



# System Management Commands

---

- [arp](#), on page 4
- [boot](#), on page 5
- [cat](#), on page 6
- [copy](#), on page 7
- [copy startup-config tftp:](#), on page 8
- [copy tftp: startup-config](#), on page 9
- [debug voice diagnostics mac-address](#), on page 10
- [debug platform condition feature multicast controlplane](#), on page 11
- [debug platform condition mac](#), on page 13
- [debug platform rep](#), on page 14
- [debug ilpower powerman](#), on page 15
- [delete](#), on page 18
- [dir](#), on page 19
- [emergency-install](#), on page 21
- [exit](#), on page 23
- [factory-reset](#), on page 24
- [flash\\_init](#), on page 29
- [help](#), on page 30
- [hostname](#), on page 31
- [install](#), on page 33
- [install add file activate reloadfast commit](#), on page 47
- [ip http banner](#), on page 49
- [ip http banner-path](#), on page 50
- [ip ssh bulk-mode](#), on page 51
- [l2 traceroute](#), on page 52
- [license air level](#), on page 53
- [license boot level](#), on page 55
- [license smart \(global config\)](#), on page 58
- [license smart \(privileged EXEC\)](#), on page 70
- [line auto-consolidation](#), on page 79
- [location](#), on page 81
- [location plm calibrating](#), on page 84
- [mac address-table move update](#), on page 85

- [mgmt\\_init](#), on page 86
- [mkdir](#), on page 87
- [more](#), on page 88
- [no debug all](#), on page 89
- [reload fast](#), on page 90
- [rename](#), on page 92
- [request consent-token accept-response shell-access](#), on page 93
- [request consent-token generate-challenge shell-access](#), on page 94
- [request consent-token terminate-auth](#), on page 95
- [request platform software console attach switch](#), on page 96
- [reset](#), on page 98
- [rmdir](#), on page 99
- [sdm prefer](#), on page 100
- [service private-config-encryption](#), on page 101
- [set](#), on page 102
- [show avc client](#), on page 105
- [show bootflash:](#), on page 106
- [show cable-diagnostics tdr](#), on page 109
- [show consistency-checker mcast](#), on page 111
- [show consistency-checker mcast l3m](#), on page 113
- [show consistency-checker objects](#), on page 117
- [show consistency-checker run-id](#), on page 119
- [show debug](#), on page 121
- [show env](#), on page 122
- [show env xps](#), on page 124
- [show flow monitor](#), on page 128
- [show install](#), on page 130
- [show license all](#), on page 132
- [show license authorization](#), on page 140
- [show license data conversion](#), on page 145
- [show license eventlog](#), on page 146
- [show license history message](#), on page 148
- [show license reservation](#), on page 149
- [show license rum](#), on page 150
- [show license status](#), on page 158
- [show license summary](#), on page 167
- [show license tech](#), on page 171
- [show license udi](#), on page 189
- [show license usage](#), on page 191
- [show location](#), on page 195
- [show logging onboard switch uptime](#), on page 197
- [show logging process ios module](#), on page 200
- [show mac address-table](#), on page 203
- [show mac address-table move update](#), on page 208
- [show parser encrypt file status](#), on page 209
- [show platform hardware fpga](#), on page 210

- [show platform integrity](#), on page 211
- [show platform software audit](#), on page 212
- [show platform software fed switch punt cause](#), on page 216
- [show platform software fed switch punt cpuq](#), on page 218
- [show platform software sl-infra](#), on page 221
- [show platform sudi certificate](#), on page 222
- [show romvar](#), on page 224
- [show running-config](#), on page 226
- [show sdm prefer](#), on page 232
- [show tech-support confidential](#), on page 234
- [show tech-support monitor](#), on page 235
- [show tech-support platform](#), on page 236
- [show tech-support platform evpn\\_vxlan](#), on page 240
- [show tech-support platform fabric](#), on page 242
- [show tech-support platform igmp\\_snooping](#), on page 246
- [show tech-support platform layer3](#), on page 249
- [show tech-support platform mld\\_snooping](#), on page 257
- [show tech-support port](#), on page 264
- [show tech-support pvlan](#), on page 267
- [show tech-support resource](#), on page 268
- [show version](#), on page 273
- [system env temperature threshold yellow](#), on page 280
- [test cable-diagnostics tdr](#), on page 282
- [traceroute mac](#), on page 283
- [traceroute mac ip](#), on page 286
- [type](#), on page 288
- [unset](#), on page 289
- [upgrade rom-monitor capsule](#), on page 291
- [version](#), on page 293

# arp

To display the contents of the Address Resolution Protocol (ARP) table, use the **arp** command in boot loader mode.

**arp** [*ip\_address*]

---

<b>Syntax Description</b>	<i>ip_address</i> (Optional) Shows the ARP table or the mapping for a specific IP address.
---------------------------	--

---

<b>Command Default</b>	No default behavior or values.
------------------------	--------------------------------

<b>Command Modes</b>	Boot loader
----------------------	-------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

---

<b>Usage Guidelines</b>	The ARP table contains the IP-address-to-MAC-address mappings.
-------------------------	--

<b>Examples</b>	This example shows how to display the ARP table:
-----------------	--

```
Device: arp 172.20.136.8
arp'ing 172.20.136.8...
172.20.136.8 is at 00:1b:78:d1:25:ae, via port 0
```

# boot

To load and boot an executable image and display the command-line interface (CLI), use the **boot** command in boot loader mode.

```
boot [-post | -n | -p | flag] filesystem:/file-url...
```

Syntax Description	
<b>-post</b>	(Optional) Run the loaded image with an extended or comprehensive power-on self-test (POST). Using this keyword causes POST to take longer to complete.
<b>-n</b>	(Optional) Pause for the Cisco IOS Debugger immediately after launching.
<b>-p</b>	(Optional) Pause for the JTAG Debugger right after loading the image.
<i>filesystem:</i>	Alias for a file system. Use <b>flash:</b> for the system board flash device; use <b>usbflash0:</b> for USB memory sticks.
<i>/file-url</i>	Path (directory) and name of a bootable image. Separate image names with a semicolon.

**Command Default** No default behavior or values.

**Command Modes** Boot loader

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines**

When you enter the **boot** command without any arguments, the device attempts to automatically boot the system by using the information in the BOOT environment variable, if any.

If you supply an image name for the *file-url* variable, the **boot** command attempts to boot the specified image.

When you specify boot loader **boot** command options, they are executed immediately and apply only to the current boot loader session.

These settings are not saved for the next boot operation.

Filenames and directory names are case sensitive.

## Example

This example shows how to boot the device using the *new-image.bin* image:

```
Device: set BOOT flash:/new-images/new-image.bin  
Device: boot
```

After entering this command, you are prompted to start the setup program.

# cat

To display the contents of one or more files, use the **cat** command in boot loader mode.

**cat** *filesystem:/file-url...*

---

## Syntax Description

*filesystem:* Specifies a file system.

---

*/file-url* Specifies the path (directory) and name of the files to display. Separate each filename with a space.

---

## Command Default

No default behavior or values.

## Command Modes

Boot loader

---

## Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

---

## Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

---

## Examples

This example shows how to display the contents of an image file:

```
Device: cat flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

# copy

To copy a file from a source to a destination, use the **copy** command in boot loader mode.

```
copy filesystem:/source-file-url filesystem:/destination-file-url
```

## Syntax Description

<i>filesystem:</i>	Alias for a file system. Use <b>usbflash0:</b> for USB memory sticks.
<i>/source-file-url</i>	Path (directory) and filename (source) to be copied.
<i>/destination-file-url</i>	Path (directory) and filename of the destination.

## Command Default

No default behavior or values.

## Command Modes

Boot loader

## Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

## Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 127 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

If you are copying a file to a new directory, the directory must already exist.

## Examples

This example shows how to copy a file at the root:

```
Device: copy usbflash0:test1.text usbflash0:test4.text
File "usbflash0:test1.text" successfully copied to "usbflash0:test4.text"
```

You can verify that the file was copied by entering the **dir filesystem:** boot loader command.

## copy startup-config tftp:

To copy the configuration settings from a switch to a TFTP server, use the **copy startup-config tftp:** command in Privileged EXEC mode.

**copy startup-config tftp:** *remote host {ip-address}/{name}*

<b>Syntax Description</b>	<i>remote host {ip-address}/{name}</i> Host name or IP-address of Remote host.
---------------------------	--

<b>Command Default</b>	No default behavior or values.
------------------------	--------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 16.1	This command was introduced.

<b>Usage Guidelines</b>	To copy your current configurations from the switch, run the command <b>copy startup-config tftp:</b> and follow the instructions. The configurations are copied onto the TFTP server.
-------------------------	--

Then, login to another switch and run the command **copy tftp: startup-config** and follow the instructions. The configurations are now copied onto the other switch.

<b>Examples</b>	This example shows how to copy the configuration settings onto a TFTP server:
-----------------	---

```
Device: copy startup-config tftp:
Address or name of remote host []?
```



## copy tftp: startup-config

To copy the configuration settings from a TFTP server onto a new switch, use the **copy tftp: startup-config** command in Privileged EXEC mode on the new switch.

**copy tftp: startup-config** *remote host {ip-address}/{name}*

<b>Syntax Description</b>	<i>remote host {ip-address}/{name}</i> Host name or IP-address of Remote host.
---------------------------	--

<b>Command Default</b>	No default behavior or values.
------------------------	--------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 16.1	This command was introduced.

<b>Usage Guidelines</b>	After the configurations are copied, to save your configurations, use <b>write memory</b> command and then either reload the switch or run the <b>copy startup-config running-config</b> command.
-------------------------	---

<b>Examples</b>	This example shows how to copy the configuration settings from the TFTP server onto a switch:
-----------------	---

```
Device: copy tftp: startup-config
Address or name of remote host []?
```

## debug voice diagnostics mac-address

To enable debugging of voice diagnostics for voice clients, use the **debug voice diagnostics mac-address** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

**debug voice diagnostics mac-address** *mac-address1* **verbose** **mac-address** *mac-address2* **verbose**  
**nodebug voice diagnostics mac-address** *mac-address1* **verbose** **mac-address** *mac-address2* **verbose**

Syntax Description		
<b>voice diagnostics</b>		Configures voice debugging for voice clients.
<b>mac-address</b> <i>mac-address1</i> <b>mac-address</b> <i>mac-address2</i>		Specifies MAC addresses of the voice clients.
<b>verbose</b>		Enables verbose mode for voice diagnostics.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

The following is sample output from the **debug voice diagnostics mac-address** command and shows how to enable debugging of voice diagnostics for voice client with MAC address of 00:1f:ca:cf:b6:60:

```
Device# debug voice diagnostics mac-address 00:1f:ca:cf:b6:60
```

# debug platform condition feature multicast controlplane

To enable radioactive tracing for the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) snooping features, use the **debug platform condition feature multicast controlplane** command in privileged EXEC mode. To disable radioactive tracing, use the **no** form of this command.

**debug platform condition feature multicast controlplane** {{igmp-debug | pim} group-ip {ipv4 address / ipv6 address} | {mld-snooping | igmp-snooping} mac mac-address ip {ipv4 address / ipv6 address} vlan vlan-id } level {debug | error | info | verbose | warning}

**no debug platform condition feature multicast controlplane** {{igmp-debug | pim} group-ip {ipv4 address / ipv6 address} | {mld-snooping | igmp-snooping} mac mac-address ip {ipv4 address / ipv6 address} vlan vlan-id } level {debug | error | info | verbose | warning}

Syntax	Description
<b>igmp-debug</b>	Enables IGMP control radioactive tracing.
<b>pim</b>	Enables Protocol Independent Multicast (PIM) control radioactive tracing.
<b>mld-snooping</b>	Enables MLD snooping control radioactive tracing.
<b>igmp-snooping</b>	Enables IGMP snooping control radioactive tracing.
<b>mac mac-address</b>	MAC address of the receiver.
<b>group-ip {ipv4 address / ipv6 address}</b>	IPv4 or IPv6 address of the igmp-debug or pim group.
<b>ip {ipv4 address / ipv6 address}</b>	IPv4 or IPv6 address of the mld-snooping or igmp-snooping group.
<b>vlan vlan-id</b>	VLAN ID. The range is from 1 to 4094.
<b>level</b>	Enables debug severity levels.
<b>debug</b>	Enables debugging level.
<b>error</b>	Enables error debugging.
<b>info</b>	Enables information debugging.
<b>verbose</b>	Enables detailed debugging.
<b>warning</b>	Enables warning debugging.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

The following example shows how to enable radioactive tracing for IGMP snooping:

```
Device# debug platform condition feature multicast controlplane igmp-snooping mac
000a.f330.344a ip 10.1.1.10 vlan 550 level warning
```

Related Commands	Command	Description
	<b>clear debug platform condition all</b>	Removes the debug conditions applied to a platform.
	<b>debug platform condition</b>	Filters debugging output for <b>debug</b> commands on the basis of specified conditions.
	<b>debug platform condition start</b>	Starts conditional debugging on a system.
	<b>debug platform condition stop</b>	Stops conditional debugging on a system.
	<b>show platform condition</b>	Displays the currently active debug configuration.

# debug platform condition mac

To enable radioactive tracing for MAC learning, use the **debug platform condition mac** command in privileged EXEC mode. To disable radioactive tracing for MAC learning, use the **no** form of this command.

**debug platform condition mac** {*mac-address* {**control-plane** | **egress** | **ingress**} | **access-list** *access-list name* {**egress** | **ingress**}}  
**no debug platform condition mac** {*mac-address* {**control-plane** | **egress** | **ingress**} | **access-list** *access-list name* {**egress** | **ingress**}}

Syntax Description		
<b>mac</b> <i>mac-address</i>		Filters output on the basis of the specified MAC address.
<b>access-list</b> <i>access-list name</i>		Filters output on the basis of the specified access list.
<b>control-plane</b>		Displays messages about the control plane routines.
<b>egress</b>		Filters output on the basis of outgoing packets.
<b>ingress</b>		Filters output on the basis of incoming packets.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

The following example shows how to filter debugging output on the basis of a MAC address:

```
Device# debug platform condition mac bc16.6509.3314 ingress
```

Related Commands	Command	Description
	<b>show platform condition</b>	Displays the currently active debug configuration.
	<b>debug platform condition</b>	Filters debugging output for <b>debug</b> commands on the basis of specified conditions.
	<b>debug platform condition start</b>	Starts conditional debugging on a system.
	<b>debug platform condition stop</b>	Stops conditional debugging on a system.
	<b>clear debug platform condition all</b>	Removes the debug conditions applied to a platform.

# debug platform rep

To enable debugging of Resilient Ethernet Protocol (REP) functions, use the **debug platform rep** command in privileged EXEC mode. To remove the specified condition, use the **no** form of this command.

**debug platform rep** {all | error | event | packet | verbose}  
**no debug platform rep** {all | error | event | packet | verbose}

Syntax Description		
	<b>all</b>	Enables all REP debugging functions.
	<b>error</b>	Enables REP error debugging.
	<b>event</b>	Enables REP event debugging.
	<b>packet</b>	Enables REP packet debugging.
	<b>verbose</b>	Enables REP verbose debugging.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

The following example shows how to enable debugging for all functions:

```
Device# debug platform rep all

debug platform rep verbose debugging is on
debug platform rep control pkt handle debugging is on
debug platform rep error debugging is on
debug platform rep event debugging is on
```

Related Commands	Command	Description
	<b>show platform condition</b>	Displays the currently active debug configuration.
	<b>debug platform condition</b>	Filters debugging output for <b>debug</b> commands on the basis of specified conditions.
	<b>debug platform condition start</b>	Starts conditional debugging on a system.
	<b>debug platform condition stop</b>	Stops conditional debugging on a system.
	<b>clear debug platform condition all</b>	Removes the debug conditions applied to a platform.

# debug ilpower powerman

To enable debugging of the power controller and Power over Ethernet (PoE) system, use the **debug ilpower powerman** command in privileged EXEC mode. Use the no form of this command to disable debugging.

**Command Default** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows the output for the **debug ilpower powerman** command for releases prior to Cisco IOS XE Gibraltar 16.10.1:

```
Device# debug ilpower powerman
1. %ILPOWER-3-CONTROLLER_PORT_ERR: Controller port error, Interface
Gix/y/z: Power Controller reports power Imax error detected
Mar 8 16:35:17.801: ilpower_power_assign_handle_event: event 0, pwrassign
is done by proto CDP
Port Gil/0/48: Selected Protocol CDP
Mar 8 16:35:17.801: Ilpowerinterface (Gil/0/48) process tlvfrom cdpINPUT:

Mar 8 16:35:17.801: power_consumption= 2640, power_request_id= 1,
power_man_id= 2,
Mar 8 16:35:17.801: power_request_level[] = 2640 0 0 0 0
Mar 8 16:35:17.801:
Mar 8 16:35:17.801: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: Ilpowerinterface (Gil/0/48) power negotiation:
consumption = 2640, alloc_power= 2640
Mar 8 16:35:17.802: Ilpowerinterface (Gil/0/48) setting ICUT_OFF threshold
to 2640.
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:18.115: ILP:: posting ilpslot 1 port 48 event 5 class 0
Mar 8 16:35:18.115: ILP:: Gil/0/48: State=NGWC_ILP_LINK_UP_S-6,
Event=NGWC_ILP_IMAX_FAULT_EV-5
Mar 8 16:35:18.115: ilpowerdelete power from pdlinkdownGil/0/48
Mar 8 16:35:18.115: Ilpowerinterface (Gil/0/48), delete allocated power
2640
Mar 8 16:35:18.116: Ilpowerinterface (Gil/0/48) setting ICUT_OFF threshold
to 0.
Mar 8 16:35:18.116: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:18.116: ilpower_notify_lldp_power_via_mdltlvGil/0/48 pwralloc0
Mar 8 16:35:18.116: Gil/0/48 AUTO PORT PWR Alloc130 Request 130
Mar 8 16:35:18.116: Gil/0/48: LLDP NOTIFY TLV:
```

```
(curr/prev) PSE Allocation: 13000/0
(curr/prev) PD Request : 13000/0
(curr/prev) PD Class : Class 4/
(curr/prev) PD Priority : low/unknown
(curr/prev) Power Type : Type 2 PSE/Type 2 PSE
(curr/prev) mdi_pwr_support: 7/0
(curr/prevPower Pair) : Signal/
(curr/prev) PSE PwrSource : Primary/Unknown
```

This example shows the output for the **debug ilpower powerman** command starting Cisco IOS XE Gibraltar 16.10.1. Power Unit (mW) has been added to the `power_request_level`, PSE Allocation and PD Request. `Power_request_level` has been enhanced to display only non-zero values.

```
Device# debug ilpower powerman
1. %ILPOWER-3-CONTROLLER_PORT_ERR: Controller port error, Interface
Gix/y/z: Power Controller reports power Imax error detected
Mar 8 16:35:17.801: ilpower_power_assign_handle_event: event 0, pwrassign
  is done by proto CDP
Port Gil/0/48: Selected Protocol CDP
Mar 8 16:35:17.801: Ilpowerinterface (Gil/0/48) process tlvfrom cdpINPUT:

Mar 8 16:35:17.801: power_consumption= 2640, power_request_id= 1,
power_man_id= 2,
Mar 8 16:35:17.801: power_request_level(mW) = 2640
<----- mW unit added, non-zero value display
Mar 8 16:35:17.801:
Mar 8 16:35:17.801: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: Ilpowerinterface (Gil/0/48) power negotiation:
consumption = 2640, alloc_power= 2640
Mar 8 16:35:17.802: Ilpowerinterface (Gil/0/48) setting ICUT_OFF threshold
to 2640.
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:18.115: ILP:: posting ilpslot 1 port 48 event 5 class 0
Mar 8 16:35:18.115: ILP:: Gil/0/48: State=NGWC_ILP_LINK_UP_S-6,
Event=NGWC_ILP_IMAX_FAULT_EV-5
Mar 8 16:35:18.115: ilpowerdelete power from pdlinkdownGil/0/48
Mar 8 16:35:18.115: Ilpowerinterface (Gil/0/48), delete allocated power
2640
Mar 8 16:35:18.116: Ilpowerinterface (Gil/0/48) setting ICUT_OFF threshold
to 0.
Mar 8 16:35:18.116: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:18.116: ilpower_notifylldp_power_via_mdi_tlvGil/0/48 pwralloc0
Mar 8 16:35:18.116: Gil/0/48 AUTO PORT PWR Alloc130 Request 130
Mar 8 16:35:18.116: Gil/0/48: LLDP NOTIFY TLV:
(curr/prev) PSE Allocation (mW): 13000/0
<----- mW unit added
(curr/prev) PD Request (mW) : 13000/0
<----- mW unit added
```



```
(curr/prev) PD Class : Class 4/  
(curr/prev) PD Priority : low/unknown  
(curr/prev) Power Type : Type 2 PSE/Type 2 PSE  
(curr/prev) mdi_pwr_support: 7/0  
(curr/prevPower Pair) : Signal/  
(curr/prev) PSE PwrSource : Primary/Unknown
```

# delete

To delete one or more files from the specified file system, use the **delete** command in boot loader mode.

**delete** *filesystem:/file-url...*

## Syntax Description

*filesystem*: Alias for a file system. Use **usbflash0**: for USB memory sticks.

*/file-url...* Path (directory) and filename to delete. Separate each filename with a space.

## Command Default

No default behavior or values.

## Command Modes

Boot loader

## Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

## Usage Guidelines

Filenames and directory names are case sensitive.

The device prompts you for confirmation before deleting each file.

## Examples

This example shows how to delete two files:

```
Device: delete usbflash0:test2.text usbflash0:test5.text
Are you sure you want to delete "usbflash0:test2.text" (y/n)?y
File "usbflash0:test2.text" deleted
Are you sure you want to delete "usbflash0:test5.text" (y/n)?y
File "usbflash0:test2.text" deleted
```

You can verify that the files were deleted by entering the **dir usbflash0**: boot loader command.

# dir

To display the list of files and directories on the specified file system, use the **dir** command in boot loader mode.

**dir** *filesystem:/file-url*

<b>Syntax Description</b>	<i>filesystem</i> : Alias for a file system. Use <b>flash</b> : for the system board flash device; use <b>usbflash0</b> : for USB memory sticks.				
	<i>/file-url</i> (Optional) Path (directory) and directory name that contain the contents you want to display. Separate each directory name with a space.				
<b>Command Default</b>	No default behavior or values.				
<b>Command Modes</b>	Boot Loader Privileged EXEC				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.5.1a</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.5.1a	This command was introduced.				
<b>Usage Guidelines</b>	Directory names are case sensitive.				
<b>Examples</b>	This example shows how to display the files in flash memory:				

```
Device: dir flash:
Directory of flash:/
  2  -rwx      561   Mar 01 2013 00:48:15  express_setup.debug
  3  -rwx    2160256  Mar 01 2013 04:18:48  c2960x-dmon-mz-150-2r.EX
  4  -rwx      1048   Mar 01 2013 00:01:39  multiple-fs
  6  drwx      512   Mar 01 2013 23:11:42  c2960x-universalk9-mz.150-2.EX
645 drwx      512   Mar 01 2013 00:01:11  dc_profile_dir
647 -rwx      4316   Mar 01 2013 01:14:05  config.text
648 -rwx        5    Mar 01 2013 00:01:39  private-config.text

96453632 bytes available (25732096 bytes used)
```

**Table 1: dir Field Descriptions**

Field	Description
2	Index number of the file.
-rwx	File permission, which can be any or all of the following: <ul style="list-style-type: none"> <li>• d—directory</li> <li>• r—readable</li> <li>• w—writable</li> <li>• x—executable</li> </ul>

Field	Description
1644045	Size of the file.
<date>	Last modification date.
env_vars	Filename.

# emergency-install

To perform an emergency installation on your system, use the **emergency-install** command in boot loader mode.

**emergency-install** *url://<url>*

<b>Syntax Description</b>	<i>&lt;url&gt;</i> URL and name of the file containing the emergency installation bundle image.
---------------------------	---

<b>Command Default</b>	No default behavior or values.
------------------------	--------------------------------

<b>Command Modes</b>	Boot loader
----------------------	-------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

<b>Usage Guidelines</b>	The boot flash is erased during the installation operation. After you perform the emergency install operation, set the BOOT variable in the ROMMON prompt by using the <b>set BOOT flash:packages.conf</b> command, and run the <b>boot flash:packages.conf</b> command manually in boot loader mode to boot the system. If the BOOT variable is not set in the ROMMON prompt, once the system has booted, set the BOOT variable in the device prompt by using the <b>boot system flash:packages.conf</b> command in global configuration mode.
-------------------------	---

## Example

This example shows how to perform the emergency install operation using the contents of an image file:

```
Device: emergency-install tftp:<url>
The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery (tftp:<url> ...
Reading full image into memory.....done
Nova Bundle Image
-----
Kernel Address      : 0x6042d5c8
Kernel Size         : 0x317ccc/3243212
Initramfs Address   : 0x60745294
Initramfs Size      : 0xdc6774/14444404
Compression Format   : .mzip

Bootable image at @ ram:0x6042d5c8
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range \
[0x80180000, 0x90000000].
#####
File "sda9:c3850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)
```

```
Initiating Emergency Installation of bundle
tftp:<url>
```

```
Downloading bundle tftp:<url>...
```

```
Validating bundle tftp:<url>...
```

```
Installing bundle tftp:<url>...
```

```
Verifying bundle tftp:<url>...
```

```
Package cat3k_caa-base.SPA.03.02.00SE.pkg is Digitally Signed
```

```
Package cat3k_caa-drivers.SPA.03.02.00.SE.pkg is Digitally Signed
```

```
Package cat3k_caa-infra.SPA.03.02.00SE.pkg is Digitally Signed
```

```
Package cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg is Digitally Signed
```

```
Package cat3k_caa-platform.SPA.03.02.00.SE.pkg is Digitally Signed
```

```
Package cat3k_caa-wcm.SPA.10.0.100.0.pkg is Digitally Signed
```

```
Preparing flash...
```

```
Syncing device...
```

```
Emergency Install successful... Rebooting
```

```
Restarting system.\ufffd
```

```
Booting...(use DDR clock 667 MHz)Initializing and Testing RAM
```

```
+++@@@###...++@@++@@++@@++@@++@@++@@++@@done.
```

```
Memory Test Pass!
```

```
Base ethernet MAC Address: 20:37:06:ce:25:80
```

```
Initializing Flash...
```

```
flashfs[7]: 0 files, 1 directories
```

```
flashfs[7]: 0 orphaned files, 0 orphaned directories
```

```
flashfs[7]: Total bytes: 6784000
```

```
flashfs[7]: Bytes used: 1024
```

```
flashfs[7]: Bytes available: 6782976
```

```
flashfs[7]: flashfs fsck took 1 seconds....done Initializing Flash.
```

```
The system is not configured to boot automatically. The
following command will finish loading the operating system
software:
```

```
boot
```

# exit

To return to the previous mode or exit from the CLI EXEC mode, use the **exit** command.

## exit

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** No default behavior or values.

---

**Command Modes** Privileged EXEC  
Global configuration

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

---

This example shows how to exit the configuration mode:

```
Device(config)# exit  
Device#
```

# factory-reset

To erase all customer-specific data and restore a device to its factory configuration, use the **factory-reset** command in privileged EXEC mode.



**Note** The erasure is consistent with the clear method, as described in NIST SP 800-88 Rev. 1.

## Standalone Device

```
factory-reset { all [ secure ] [3-pass] | boot-vars | config }
```

## Stacked Device

```
factory-reset { all [secure 3-pass] | boot-vars | config | switch switch_number | all { all [secure 3-pass] | boot-vars | config } }
```

### Syntax Description

<b>all</b>	Erases all the content from the NVRAM, all Cisco IOS images, including the current boot image, boot variables, startup and running configuration data, and user data.
<b>all secure</b>	Performs data sanitization and securely resets the device.  <b>Note</b> This option implements guidelines for media sanitization as described in NIST SP 800-88 Rev. 1.
<b>secure 3-pass</b>	Erases all the content from the device with 3-pass overwrite. <ul style="list-style-type: none"> <li>• Pass 1: Overwrites all addressable locations with binary zeroes.</li> <li>• Pass 2: Overwrites all addressable locations with binary ones.</li> <li>• Pass 3: Overwrites all addressable locations with a random bit pattern.</li> </ul>
<b>boot-vars</b>	Erases only the user-added boot variables.
<b>config</b>	Erases only the startup configurations.
<b>switch</b> { <i>switch_number</i>   <b>all</b> }	Erases content on the selected switch: <ul style="list-style-type: none"> <li>• <i>switch-number</i>: Specifies the switch number. The range is from 1 to 16.</li> <li>• <b>all</b>: Selects all the switches in the stack.</li> </ul>

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.



Release	Modification
Cisco IOS XE Amsterdam 17.2.1	The <b>secure 3-pass</b> and <b>switch</b> keyword was introduced.
Cisco IOS XE Dublin 17.10.1	The <b>all secure</b> option was introduced.

### Usage Guidelines

The **factory-reset** command is used in the following scenarios:

- To return a device to Cisco for Return Material Authorization (RMA), use this command to remove all the customer-specific data before obtaining an RMA certificate for the device.
- If the key information or credentials that are stored on a device is compromised, use this command to reset the device to factory configuration, and then reconfigure the device.

After the factory reset process is successfully completed, the device reboots and enters ROMMON mode.

### Examples

The following example shows how to erase all the content from a device using the **factory-reset all** command:

```
Device> enable
Device# factory-reset all

The factory reset operation is irreversible for all operations. Are you sure? [confirm]
The following will be deleted as a part of factory reset:
1: Crash info and logs
2: User data, startup and running configuration
3: All IOS images, including the current boot image
4: OBFL logs
5: User added rommon variables
6: Data on Field Replaceable Units(USB/SSD/SATA)
The system will reload to perform factory reset.
It will take some time to complete and bring it to rommon.
You will need to load IOS image using USB/TFTP from rommon after
this operation is completed.
DO NOT UNPLUG THE POWER OR INTERRUPT THE OPERATION
Are you sure you want to continue? [confirm]
```

The following examples show how to perform a factory reset on stacked devices:

```
Device> enable
Device# factory-reset switch all all

The factory reset operation is irreversible for all operations. Are you sure? [confirm]
The following will be deleted as a part of factory reset:
1: Crash info and logs
2: User data, startup and running configuration
3: All IOS images, including the current boot image
4: OBFL logs
5: User added rommon variables
6: Data on Field Replaceable Units(USB/SSD/SATA)
The system will reload to perform factory reset.
It will take some time to complete and bring it to rommon.
You will need to load IOS image using USB/TFTP from rommon after
this operation is completed.
DO NOT UNPLUG THE POWER OR INTERRUPT THE OPERATION
Are you sure you want to continue? [confirm]
Chassis 1 reloading, reason - Factory Reset

Protection key not found
9300L#Oct 25 09:53:05.740: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload
fp action requested
Oct 25 09:53:07.277: %PMAN-5-EXITACTION:vp: Process manager is exiting: rp processes exit
```

with reload switch code

```

Enabling factory reset for this reload cycle
Switch booted with
tftp://10.5.40.45/cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20191007_224933_V17_2_0_21_2.SSA.bin
Switch booted via
//10.5.40.45/cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20191007_224933_V17_2_0_21_2.SSA.bin
% FACTORYRESET - Started Cleaning Up...

% FACTORYRESET - Unmounting sd1
% FACTORYRESET - Cleaning Up sd1 [0]
% FACTORYRESET - erase In progress.. please wait for completion...
% FACTORYRESET - write zero...
% FACTORYRESET - finish erase

% FACTORYRESET - Making File System sd1 [0]
Discarding device blocks: done
Creating filesystem with 409600 4k blocks and 102544 inodes
Filesystem UUID: fcf01664-7c6f-41ce-99f0-6dfd1d941701e
Superblock backups stored on blocks:
 32768, 98304, 163840, 229376, 294912

Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done

% FACTORYRESET - Mounting Back sd1 [0]
% FACTORYRESET - Handling Mounted sd1
% FACTORYRESET - Factory Reset Done for sd1

% FACTORYRESET - Unmounting sd3
% FACTORYRESET - Cleaning Up sd3 [0]
% FACTORYRESET - erase In progress.. please wait for completion...
% FACTORYRESET - write zero...

Chassis 2 reloading, reason - Factory Reset
Dec 12 01:02:12.500: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp
action requested
De
Enabling factory reset for this reload cycle
Switch booted with
tftp://10.5.40.45/cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20191007_224933_V17_2_0_21_2.SSA.bin
Switch booted via
//10.5.40.45/cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20191007_224933_V17_2_0_21_2.SSA.bin
% FACTORYRESET - Started Cleaning Up...
% FACTORYRESET - Unmounting sd1
% FACTORYRESET - Cleaning Up sd1 [0]
% FACTORYRESET - erase In progress.. please wait for completion...
% FACTORYRESET - write zero...

```

After this the switch will come to boot prompt. Then the customer has to boot the device from TFTP.

The following example shows how to erase all the content from a device using the **factory-reset all secure** command:

```

Device# factory-reset all secure
The factory reset operation is irreversible for securely reset all. Are you sure? [confirm]

```

```

The following will be deleted as a part of factory reset: NIST SP-800-88r1
1: Crash info and logs
2: User data, startup and running configuration
3: All IOS images, excluding the current boot image
4: OBFL logs
5: User added rommon variables
6: Data on Field Replaceable Units(SSD/SATA)
7: License usage log files
Note:
Secure erase logs/reports will be stored in flash.
The system will reload to perform factory reset.
It will take some time to complete and bring it to rommon.
DO NOT UNPLUG THE POWER OR INTERRUPT THE OPERATION
Are you sure you want to continue? [confirm]
Protection key not found
Switch#
Chassis 1 reloading, reason - Factory Reset
Sep 18 06:18:01.632: %PMAN-5-EXITACTION: C0/0: pvp: Process manager is exiting: reload cc
action requested
Sep 18 06:18:01.657: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp
action requested
Sep 18 06

Enabling factory reset for this reload cycle
Switch booted with
flash:cat9k_lite_iosxe.BLD_V1710_THROTTLE_LATEST_20220912_071947_QU_C.SSA.bin
Switch booted via cat9k_lite_iosxe.BLD_V1710_THROTTLE_LATEST_20220912_071947_QU_C.SSA.bin
FACTORY-RESET-RESTORE-IMAGE Taking backup of
flash:cat9k_lite_iosxe.BLD_V1710_THROTTLE_LATEST_20220912_071947_QU_C.SSA.bin
FACTORY-RESET-RESTORE-IMAGE Searching for
cat9k_lite_iosxe.BLD_V1710_THROTTLE_LATEST_20220912_071947_QU_C.SSA.bin on flash
factory-reset-restore-image copying
/flash/cat9k_lite_iosxe.BLD_V1710_THROTTLE_LATEST_20220912_071947_QU_C.SSA.bin image to
/tmp/factory_reset
% FACTORYRESET - Started Data Sanitization...
% FACTORYRESET - Unmounting sd1
% FACTORYRESET - Unmounting sd3
% FACTORYRESET - Unmounting sd4
% FACTORYRESET - Unmounting sd5
% FACTORYRESET - Unmounting sd6
Executing Data Sanitization...
MTD Data Sanitization started ...
!!! Please, wait - Reading MTD Info !!!
!!! Please, wait - Validating Erase for/dev/mtd3 !!!
!!! Please, wait - Validating Erase for/dev/mtd4 !!!
MTD Data Sanitization completed ...
eMMC Data Sanitization started ...
!!! Please, wait - Reading EXT_CSD !!!
!!! Please, wait - Reading EXT_CSD !!!
!!! Please, wait - sanitizing !!!
!!! Please, wait - Validating Erase for/dev/mmcblk0p1 !!!
!!! Please, wait - Reading EXT_CSD !!!
!!! Please, wait - Reading EXT_CSD !!!
!!! Please, wait - sanitizing !!!
!!! Please, wait - Validating Erase for/dev/mmcblk0p3 !!!
!!! Please, wait - Reading EXT_CSD !!!
!!! Please, wait - Reading EXT_CSD !!!
!!! Please, wait - sanitizing !!!
!!! Please, wait - Validating Erase for/dev/mmcblk0p4 !!!
!!! Please, wait - Reading EXT_CSD !!!
!!! Please, wait - Reading EXT_CSD !!!
!!! Please, wait - sanitizing !!!
!!! Please, wait - Validating Erase for/dev/mmcblk0p5 !!!
!!! Please, wait - Reading EXT_CSD !!!

```

```
!!! Please, wait - Reading EXT_CSD !!!
!!! Please, wait - sanitizing !!!
!!! Please, wait - Validating Erase for/dev/mmcblk0p6 !!!
eMMC Data Sanitization completed ...
Data Sanitization Success! Exiting...
% FACTORYRESET - Data Sanitization Success...
% FACTORYRESET - Making File System sd1 [0]
mke2fs 1.43-WIP (18-May-2015)
Discarding device blocks: done
Creating filesystem with 204800 4k blocks and 51296 inodes
Filesystem UUID: 8aae2120-0c5f-4c05-82d0-1be3ea5f5f1a
Superblock backups stored on blocks:
    32768, 98304, 163840
Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done
% FACTORYRESET - Mounting Back sd6 [0]
% FACTORYRESET - Factory Reset Done for sd6
% FACTORYRESET - Lic Clean UP
% act2 export - ROMMON_BOARDID=800
act2 cleaning Starting...
% act2 cleaning success
act2 logging Starting...
% act2 logging success
% FACTORYRESET - Restore lic0 Files
Factory reset Secure Completed ...
% FACTORYRESET - Secure Successfull
ReloadReason=Factory Reset
FACTORY-RESET-RESTORE-IMAGE Copying back image from /tmp/factory_reset onto /bootflash/
FACTORY-RESET-RESTORE-IMAGE Copying image is successful.
% FACTORYRESET - md5sum : e4394cc1f436bcb7fc518600d3f0254f
/bootflash/cat9k_lite_iosxe.BLD_V1710_THROTTLE_LATEST_20220912_071947_QU_C.SSA.bin
Factory reset successful. Rebooting...
```

# flash\_init

To initialize the flash: file system, use the **flash\_init** command in boot loader mode.

## **flash\_init**

---

**Syntax Description**

This command has no arguments or keywords.

---

**Command Default**

The flash: file system is automatically initialized during normal system operation.

---

**Command Modes**

Boot loader

---

**Command History**

<b>Release</b>	<b>Modification</b>
Cisco IOS XE Everest 16.5.1a	This command was introduced.

---

**Usage Guidelines**

During the normal boot process, the flash: file system is automatically initialized.

Use this command to manually initialize the flash: file system. For example, you use this command during the recovery procedure for a lost or forgotten password.

# help

To display the available commands, use the **help** command in boot loader mode.

## help

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** No default behavior or values.

---

**Command Modes** Boot loader

---

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

---

## Example

This example shows how to display a list of available boot loader commands:

```
Device:help
? -- Present list of available commands
arp -- Show arp table or arp-resolve an address
boot -- Load and boot an executable image
cat -- Concatenate (type) file(s)
copy -- Copy a file
delete -- Delete file(s)
dir -- List files in directories
emergency-install -- Initiate Disaster Recovery
...
...
...
unset -- Unset one or more environment variables
version -- Display boot loader version
```

# hostname

To specify or modify the hostname for the network server, use the **hostname** command in global configuration mode.

**hostname** *name*

<b>Syntax Description</b>	<i>name</i>	New hostname for the network server.
---------------------------	-------------	--------------------------------------

**Command Default** The default hostname is switch.

**Command Modes** Global configuration (config)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** The hostname is used in prompts and default configuration filenames.

Do not expect case to be preserved. Uppercase and lowercase characters look the same to many internet software applications. It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, refer to RFC 1178, *Choosing a Name for Your Computer* .

The name must also follow the rules for ARPANET hostnames. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names must be 63 characters or fewer. Creating an all numeric hostname is not recommended but the name will be accepted after an error is returned.

```
Device(config)#hostname 123
% Hostname contains one or more illegal characters.
123(config)#
```

A hostname of less than 10 characters is recommended. For more information, refer to RFC 1035, *Domain Names--Implementation and Specification* .

On most systems, a field of 30 characters is used for the hostname and the prompt in the CLI. Note that the length of your hostname may cause longer configuration mode prompts to be truncated. For example, the full prompt for service profile configuration mode is:

```
(config-service-profile)#
```

However, if you are using the hostname of “Switch,” you will only see the following prompt (on most systems):

```
Switch(config-service-profil)#
```

If the hostname is longer, you will see even less of the prompt:

```
Basement-rtr2(config-service)#
```

Keep this behavior in mind when assigning a name to your system (using the **hostname** global configuration command). If you expect that users will be relying on mode prompts as a CLI navigation aid, you should assign hostnames of no more than nine characters.

The use of a special character such as \" (backslash) and a three or more digit number for the character setting like **hostname**, results in incorrect translation:

```
Device(config)#
Device(config)#hostname \\99
% Hostname contains one or more illegal characters.
```

## Examples

The following example changes the hostname to “host1”:

```
Device(config)# hostname host1
host1(config)#
```



# install

To install Software Maintenance Upgrade (SMU) packages, use the **install** command in privileged EXEC mode.

```
install {abort | activate | file {bootflash: | flash: | harddisk: | webui:} [{auto-abort-timer timer timer
prompt-level {all | none}}]} | add file {bootflash: | flash: | ftp: | harddisk: | http: | https: | rcp: | scp:
| tftp: | webui:} [{activate [{auto-abort-timer timer prompt-level {all | none}commit}]}] | commit |
auto-abort-timer stop | deactivate file {bootflash: | flash: | harddisk: | webui:} | label id{description
description | label-name name} | remove {file {bootflash: | flash: | harddisk: | webui:} | inactive } |
rollback to {base | committed | id {install-ID } | label {label-name}}}
```

Syntax Description		
<b>abort</b>		Terminates the current install operation.
<b>activate</b>		Validates whether the SMU is added through the <b>install add</b> command.  This keyword runs a compatibility check, updates package status, and if the package can be restarted, triggers post-install scripts to restart the necessary processes, or triggers a reload for nonrestartable packages.
<b>file</b>		Specifies the package to be activated.
{bootflash:   flash:   harddisk:   webui:}		Specifies the location of the installed package.
<b>auto-abort-timer</b> <i>timer</i>		(Optional) Installs an auto-abort timer.
<b>prompt-level</b> {all   none}		(Optional) Prompts a user about installation activities.  For example, the <b>activate</b> keyword automatically triggers a reload for packages that require a reload. Before activating the package, a message prompts users about wanting to continue or not.  The <b>all</b> keyword allows you to enable prompts. The <b>none</b> keyword disables prompts.
<b>add</b>		Copies files from a remote location (through FTP or TFTP) to a device and performs SMU compatibility check for the platform and image versions.  This keyword runs base compatibility checks to ensure that a specified package is supported on a platform.
{ bootflash:   flash:   ftp:   harddisk:   http:   https:   rcp:   scp:   tftp:   webui: }		Specifies the package to be added.

<b>commit</b>	Makes SMU changes persistent over reloads.  You can perform a commit after activating a package while the system is up, or after the first reload. If a package is activated, but not committed, it remains active after the first reload, but not after the second reload.
<b>auto-abort-timer stop</b>	Stops the auto-abort timer.
<b>deactivate</b>	Deactivates an installed package.  <b>Note</b> Deactivating a package also updates the package status and might trigger a process restart or reload.
<b>label <i>id</i></b>	Specifies the ID of the install point to label.
<b>description</b>	Adds a description to the specified install point.
<b>label-name <i>name</i></b>	Adds a label name to the specified install point.
<b>remove</b>	Removes the installed packages.  The <b>remove</b> keyword can only be used on packages that are currently inactive.
<b>inactive</b>	Removes all the inactive packages from the device.
<b>rollback</b>	Rolls back the data model interface (DMI) package SMU to the base version, the last committed version, or a known commit ID.
<b>to base</b>	Returns to the base image.
<b>committed</b>	Returns to the installation state when the last commit operation was performed.
<b>id <i>install-ID</i></b>	Returns to the specific install point ID. Valid values are from 1 to 4294967295.

**Command Default**

Packages are not installed.

**Command Modes**

Privileged EXEC (#)

**Command History**

<b>Release</b>	<b>Modification</b>
Cisco IOS XE Everest 16.6.1	This command was introduced.
Cisco IOS XE Fuji 16.9.1	Hot-patching support is introduced. Sample output updated with hot SMU outputs.

## Usage Guidelines

An SMU is a package that can be installed on a system to provide a patch fix or security resolution to a released image. This package contains a minimal set of files for patching the release along with metadata that describes the contents of the package.

Packages must be added before the SMU is activated.

A package must be deactivated before it is removed from Flash. A removed packaged must be added again.

The following example shows how to add an install package to a device:

```
Device# install add file
flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin

install_add: START Mon Mar  5 21:48:51 PST 2018
install_add: Adding SMU

--- Starting initial file syncing ---
Info: Finished copying
flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin to the
selected switch(es)
Finished initial file syncing

Executing pre scripts....

Executing pre scripts done.
--- Starting SMU Add operation ---
Performing SMU_ADD on all members
  [1] SMU_ADD package(s) on switch 1
  [1] Finished SMU_ADD on switch 1
Checking status of SMU_ADD on [1]
SMU_ADD: Passed on [1]
Finished SMU Add operation

SUCCESS: install_add
/flash/cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin Mon
Mar  5 21:49:00 PST 2018
```

The following example shows how to activate an install package:

```
Device# install activate file
flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin

install_activate: START Mon Mar  5 21:49:22 PST 2018
install_activate: Activating SMU
Executing pre scripts....

Executing pre sripts done.

--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on all members
  [1] SMU_ACTIVATE package(s) on switch 1
  [1] Finished SMU_ACTIVATE on switch 1
Checking status of SMU_ACTIVATE on [1]
SMU_ACTIVATE: Passed on [1]
Finished SMU Activate operation

SUCCESS: install_activate
/flash/cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin Mon
Mar  5 21:49:34 PST 2018
```

The following example shows how to commit an installed package:

```

Device# install commit

install_commit: START Mon Mar  5 21:50:52 PST 2018
install_commit: Committing SMU
Executing pre scripts....

Executing pre sripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on all members
  [1] SMU_COMMIT package(s) on switch 1
  [1] Finished SMU_COMMIT on switch 1
Checking status of SMU_COMMIT on [1]
SMU_COMMIT: Passed on [1]
Finished SMU Commit operation

SUCCESS: install_commit
/flash/cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin Mon
Mar  5 21:51:01 PST 2018

```

The following example shows how to change a device running in bundle boot mode to install mode:

```

Device# install add file boot flash:cat9k_iosxe.17.04.01.SSA.bin activate commit

install_add_activate_commit: START Sun Jun 14 22:31:41 PDT 2020

install_add_activate_commit: Adding PACKAGE

install_add_activate_commit: Checking whether new add is allowed ....

--- Starting initial file syncing ---

[1]: Copying flash:cat9k_iosxe.17.04.01.SSA.bin from switch 1 to switch 2
[2]: Finished copying to switch 2

Info: Finished copying flash:cat9k_iosxe.17.04.01.SSA.bin to the selected switch(es)

Finished initial file syncing

--- Starting Add ---

Performing Add on all members
  [1] Add package(s) on switch 1
  [1] Finished Add on switch 1
  [2] Add package(s) on switch 2
  [2] Finished Add on switch 2

Checking status of Add on [1 2]

Add: Passed on [1 2]

Finished Add

Image added. Version: 17.4.01.0.87954

install_add_activate_commit: Activating PACKAGE

Following packages shall be activated:

/flash/cat9k-wlc.17.04.01.SSA.pkg

/flash/cat9k-webui.17.04.01.SSA.pkg

```

```
/flash/cat9k-srdriver.17.04.01.SSA.pkg
/flash/cat9k-sipsa.17.04.01.SSA.pkg
/flash/cat9k-sipbase.17.04.01.SSA.pkg
/flash/cat9k-rpboot.17.04.01.SSA.pkg
/flash/cat9k-rpbase.17.04.01.SSA.pkg
/flash/cat9k-lni.17.04.01.SSA.pkg
/flash/cat9k-guestshell.17.04.01.SSA.pkg
/flash/cat9k-espbase.17.04.01.SSA.pkg
/flash/cat9k-cc_srdriver.17.04.01.SSA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---

Performing Activate on all members

  [1] Activate package(s) on switch 1

  [1] Finished Activate on switch 1

  [2] Activate package(s) on switch 2

  [2] Finished Activate on switch 2

Checking status of Activate on [1 2]
Activate: Passed on [1 2]

Finished Activate

Building configuration...

[OK]--- Starting Commit ---

Performing Commit on all members

  [1] Commit package(s) on switch 1

  [1] Finished Commit on switch 1

  [2] Commit package(s) on switch 2

  [2] Finished Commit on switch 2

Checking status of Commit on [1 2]
Commit: Passed on [1 2]

Finished Commit

Send model notification for install_add_activate_commit before reload

[1 2]: Performing Upgrade_Service

300+0 records in
```

```

300+0 records out
307200 bytes (307 kB, 300 KiB) copied, 0.194027 s, 1.6 MB/s
AppGigabitEthernet port has the latest Firmware
mount: /tmp/microcode_update/boot_pkg: WARNING: device write-protected, mounted read-only.
SUCCESS: Upgrade_Service finished
Install will reload the system now!
SUCCESS: install_add_activate_commit Sun Jun 14 22:40:55 PDT 2020
The following example shows how to avoid prompt during reboot process:
Device# install add file boot flash:cat9k_iosxe.17.04.01.SSA.bin activate commit prompt-level
none
install_add_activate_commit: START Wed Jun 17 03:57:53 PDT 2020
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....
--- Starting initial file syncing ---
[1]: Copying flash:cat9k_iosxe.17.04.01.SSA.bin from switch 1 to switch 2 3
[2 3]: Finished copying to switch 2 switch 3
Info: Finished copying flash:cat9k_iosxe.17.04.01.SSA.bin to the selected switch(es)
Finished initial file syncing
--- Starting Add ---
Performing Add on all members
  [1] Add package(s) on switch 1
  [1] Finished Add on switch 1
  [2] Add package(s) on switch 2
  [2] Finished Add on switch 2
  [3] Add package(s) on switch 3
  [3] Finished Add on switch 3
Checking status of Add on [1 2 3]
Add: Passed on [1 2 3]
Finished Add
Image added. Version: 17.4.01.0.115072
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.17.04.01.SSA.pkg

```

```
/flash/cat9k-webui.17.04.01.SSA.pkg
/flash/cat9k-srdriver.17.04.01.SSA.pkg
/flash/cat9k-sipspa.17.04.01.SSA.pkg
/flash/cat9k-sipbase.17.04.01.SSA.pkg
/flash/cat9k-rpboot.17.04.01.SSA.pkg
/flash/cat9k-rpbase.17.04.01.SSA.pkg
/flash/cat9k-lni.17.04.01.SSA.pkg
/flash/cat9k-guestshell.17.04.01.SSA.pkg
/flash/cat9k-espbase.17.04.01.SSA.pkg
/flash/cat9k-cc_srdriver.17.04.01.SSA.pkg
--- Starting Activate ---
Performing Activate on all members
  [1] Activate package(s) on switch 1
  [1] Finished Activate on switch 1
  [2] Activate package(s) on switch 2
  [2] Finished Activate on switch 2
  [3] Activate package(s) on switch 3
  [3] Finished Activate on switch 3
Checking status of Activate on [1 2 3]
Activate: Passed on [1 2 3]
Finished Activate

Building configuration...
[OK]--- Starting Commit ---
Performing Commit on all members
  [1] Commit package(s) on switch 1
  [1] Finished Commit on switch 1
  [2] Commit package(s) on switch 2
  [2] Finished Commit on switch 2
  [3] Commit package(s) on switch 3
  [3] Finished Commit on switch 3
Checking status of Commit on [1 2 3]
```

```
Commit: Passed on [1 2 3]

Finished Commit

Send model notification for install_add_activate_commit before reload

[1 2 3]: Performing Upgrade_Service

300+0 records in

300+0 records out

307200 bytes (307 kB, 300 KiB) copied, 0.194692 s, 1.6 MB/s

AppGigabitEthernet port has the latest Firmware

mount: /tmp/microcode_update/boot_pkg: WARNING: device write-protected, mounted read-only.

  SUCCESS: Upgrade_Service finished

Install will reload the system now!

SUCCESS: install_add_activate_commit Wed Jun 17 04:05:25 PDT 2020
```

The following example shows how to avoid deleting files used for installation process:

```
Device# install remove inactive
install_remove: START Wed Jun 17 06:23:26 PDT 2020

Cleaning up unnecessary package files

No path specified, will use booted path flash:packages.conf

Cleaning flash:

  Scanning boot directory for packages ... done.

  Preparing packages list to delete ...

    cat9k-cc_srdriver.17.04.01.SSA.pkg
      File is in use, will not delete.

    cat9k-cc_srdriver.17.04.01.SSA.pkg
      File is in use, will not delete.

    cat9k-espbase.17.04.01.SSA.pkg
      File is in use, will not delete.

    cat9k-espbase.17.04.01.SSA.pkg
      File is in use, will not delete.

    cat9k-guestshell.17.04.01.SSA.pkg
      File is in use, will not delete.

    cat9k-guestshell.17.04.01.SSA.pkg
      File is in use, will not delete.
```



```
cat9k-lni.17.04.01.SSA.pkg
    File is in use, will not delete.
cat9k-rpbase.17.04.01.SSA.pkg
    File is in use, will not delete.
cat9k-rpbase.17.04.01.SSA.pkg
    File is in use, will not delete.
cat9k-rpboot.17.04.01.SSA.pkg
    File is in use, will not delete.
cat9k-sipbase.17.04.01.SSA.pkg
    File is in use, will not delete.
cat9k-sipbase.17.04.01.SSA.pkg
    File is in use, will not delete.
cat9k-sipspa.17.04.01.SSA.pkg
    File is in use, will not delete.
cat9k-sipspa.17.04.01.SSA.pkg
    File is in use, will not delete.
cat9k-srdriver.17.04.01.SSA.pkg
    File is in use, will not delete.
cat9k-srdriver.17.04.01.SSA.pkg
    File is in use, will not delete.
cat9k-webui.17.04.01.SSA.pkg
    File is in use, will not delete.
cat9k-webui.17.04.01.SSA.pkg
    File is in use, will not delete.
cat9k-wlc.17.04.01.SSA.pkg
    File is in use, will not delete.
cat9k-wlc.17.04.01.SSA.pkg
    File is in use, will not delete.
packages.conf
    File is in use, will not delete.
done.
```

```
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat9k-cc_srdriver.17.04.01.SSA.pkg
      File is in use, will not delete.
    cat9k-espbase.17.04.01.SSA.pkg
      File is in use, will not delete.
    cat9k-guestshell.17.04.01.SSA.pkg
      File is in use, will not delete.
    cat9k-lni.17.04.01.SSA.pkg
      File is in use, will not delete.
    cat9k-rpbase.17.04.01.SSA.pkg
      File is in use, will not delete.
    cat9k-rpboot.17.04.01.SSA.pkg
      File is in use, will not delete.
    cat9k-sipbase.17.04.01.SSA.pkg
      File is in use, will not delete.
    cat9k-sipspa.17.04.01.SSA.pkg
      File is in use, will not delete.
    cat9k-srdriver.17.04.01.SSA.pkg
      File is in use, will not delete.
    cat9k-webui.17.04.01.SSA.pkg
      File is in use, will not delete.
    cat9k-wlc.17.04.01.SSA.pkg
      File is in use, will not delete.
  packages.conf
      File is in use, will not delete.
done.

Cleaning up unnecessary package files
```

No path specified, will use booted path flash:packages.conf

Cleaning flash:

Scanning boot directory for packages ... done.

Preparing packages list to delete ...

cat9k-cc\_srdriver.17.04.01.SSA.pkg

File is in use, will not delete.

cat9k-espbase.17.04.01.SSA.pkg

File is in use, will not delete.

cat9k-guestshell.17.04.01.SSA.pkg

File is in use, will not delete.

cat9k-lni.17.04.01.SSA.pkg

File is in use, will not delete.

cat9k-rpbase.17.04.01.SSA.pkg

File is in use, will not delete.

cat9k-rpboot.17.04.01.SSA.pkg

File is in use, will not delete.

cat9k-sipbase.17.04.01.SSA.pkg

File is in use, will not delete.

cat9k-sipspa.17.04.01.SSA.pkg

File is in use, will not delete.

cat9k-srdriver.17.04.01.SSA.pkg

File is in use, will not delete.

cat9k-webui.17.04.01.SSA.pkg

File is in use, will not delete.

cat9k-wlc.17.04.01.SSA.pkg

File is in use, will not delete.

packages.conf

File is in use, will not delete.

done.

The following files will be deleted:

[switch 1]:

```
/flash/cat9k-lni.17.04.01.SSA.pkg
/flash/cat9k-rpboot.17.04.01.SSA.pkg
/flash/cat9k_iosxe.17.04.01.SSA.bin
/flash/cat9k_iosxe.17.04.01.SSA.conf
/flash/cat9k_iosxe.17.04.01.SSA.conf
[switch 2]:
/flash/cat9k-cc_srdriver.17.04.01.SSA.pkg
/flash/cat9k-espbases.17.04.01.SSA.pkg
/flash/cat9k-guestshell.17.04.01.SSA.pkg
/flash/cat9k-lni.17.04.01.SSA.pkg
/flash/cat9k-rpbases.17.04.01.SSA.pkg
/flash/cat9k-rpboot.17.04.01.SSA.pkg
/flash/cat9k-sipbases.17.04.01.SSA.pkg
/flash/cat9k-sipspace.17.04.01.SSA.pkg
/flash/cat9k-srdriver.17.04.01.SSA.pkg
/flash/cat9k-webui.17.04.01.SSA.pkg
/flash/cat9k-wlc.17.04.01.SSA.pkg
/flash/cat9k_iosxe.17.04.01.SSA.bin
/flash/cat9k_iosxe.17.04.01.SSA.conf
/flash/cat9k_iosxe.17.04.01.SSA.conf
[switch 3]:
/flash/cat9k-cc_srdriver.17.04.01.SSA.pkg
/flash/cat9k-espbases.17.04.01.SSA.pkg
/flash/cat9k-guestshell.17.04.01.SSA.pkg
/flash/cat9k-lni.17.04.01.SSA.pkg
/flash/cat9k-rpbases.17.04.01.SSA.pkg
/flash/cat9k-rpboot.17.04.01.SSA.pkg
/flash/cat9k-sipbases.17.04.01.SSA.pkg
/flash/cat9k-sipspace.17.04.01.SSA.pkg
/flash/cat9k-srdriver.17.04.01.SSA.pkg
/flash/cat9k-webui.17.04.01.SSA.pkg
/flash/cat9k-wlc.17.04.01.SSA.pkg
```

```
/flash/cat9k_iosxe.17.04.01.SSA.bin
/flash/cat9k_iosxe.17.04.01.SSA.conf
/flash/cat9k_iosxe.17.04.01.SSA.conf

Do you want to remove the above files? [y/n]y

[switch 1]:

Deleting file flash:cat9k-lni.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-rpboot.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k_iosxe.17.04.01.SSA.bin ... done.
Deleting file flash:cat9k_iosxe.17.04.01.SSA.conf ... done.
Deleting file flash:cat9k_iosxe.17.04.01.SSA.conf ... done.

SUCCESS: Files deleted.

[switch 2]:

Deleting file flash:cat9k-cc_srdriver.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-espbase.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-guestshell.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-lni.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-rpbase.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-rpboot.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-sipbase.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-sipspa.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-srdriver.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-webui.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-wlc.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k_iosxe.17.04.01.SSA.bin ... done.
Deleting file flash:cat9k_iosxe.17.04.01.SSA.conf ... done.
Deleting file flash:cat9k_iosxe.17.04.01.SSA.conf ... done.

SUCCESS: Files deleted.

[switch 3]:

Deleting file flash:cat9k-cc_srdriver.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-espbase.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-guestshell.17.04.01.SSA.pkg ... done.
```

```

Deleting file flash:cat9k-lni.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-rpbase.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-rpboot.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-sipbase.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-sipsa.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-srdriver.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-webui.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k-wlc.17.04.01.SSA.pkg ... done.
Deleting file flash:cat9k_iosxe.17.04.01.SSA.bin ... done.
Deleting file flash:cat9k_iosxe.17.04.01.SSA.conf ... done.
Deleting file flash:cat9k_iosxe.17.04.01.SSA.conf ... done.

SUCCESS: Files deleted.

--- Starting Post_Remove_Cleanup ---

Performing Post_Remove_Cleanup on all members

  [1] Post_Remove_Cleanup package(s) on switch 1
  [1] Finished Post_Remove_Cleanup on switch 1

  [2] Post_Remove_Cleanup package(s) on switch 2
  [2] Finished Post_Remove_Cleanup on switch 2

  [3] Post_Remove_Cleanup package(s) on switch 3
  [3] Finished Post_Remove_Cleanup on switch 3

Checking status of Post_Remove_Cleanup on [1 2 3]

Post_Remove_Cleanup: Passed on [1 2 3]

Finished Post_Remove_Cleanup

SUCCESS: install_remove Wed Jun 17 06:24:59 PDT 2020

```

**Related Commands**

Command	Description
<b>show install</b>	Displays information about the install packages.

# install add file activate reloadfast commit

To upgrade a standalone switch or stacked switch with the new software image using Extended Fast Software Upgrade, use the **install add file activate reloadfast commit** command in privileged EXEC mode.

**install add file** *image* **activate reloadfast commit**

<b>Syntax Description</b>	<i>image</i> Installs the software image. The keyword includes the location of the file (TFTP, HTTP, flash drives) and the image name.				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 17.3.2a</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.
Release	Modification				
Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.				
<b>Usage Guidelines</b>	<p>The <b>install add file activate reloadfast commit</b> command upgrades the standalone switch or stacked switch using Extended Fast Software Upgrade. The Extended Fast Software Upgrade reduces traffic downtime to less than 30 seconds depending on the switch configuration.</p> <p>For a Border Gateway Protocol-configured (BGP-configured) standalone switch, use the <b>bgp graceful-restart</b> command to enable Nonstop Forwarding (NSF) awareness before upgrading the software.</p> <p>For a Border Gateway Protocol-configured (BGP-configured) stacked switch, use the <b>bgp graceful-restart all</b> command to enable Nonstop Forwarding (NSF) awareness before upgrading the switch.</p> <p>For an Open Shortest Path First Version 3-configured (OSPFv3-configured) standalone switch, use the <b>ipv6 nd reachable-time</b> command to set the timeout limit, and the <b>snmp ifmib ifindex persist</b> command to enable Simple Network Management Protocol (SNMP) interface index (ifIndex) persistence globally, and the <b>interface-id snmp-if-index</b> command to enable SNMP ifIndex persistence on the interface, before upgrading the software.</p> <p>For an Intermediate System-to-Intermediate System-configured (IS-IS-configured) stacked switch, use either the <b>nsf cisco</b> or <b>nsf ietf</b> command before upgrading the switch.</p>				

## Examples

### Standalone Switch

The following example shows how to upgrade a standalone switch for a configuration other than BGP or OSPFv3:

```
Device> enable
Device# install add file bootflash: cat9k_iosxe.17.03.02.SPA.bin activate reloadfast commit
```

The following example shows how to upgrade a standalone switch for a BGP configuration:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bgp graceful-restart
Device(config-router)# end
Device# write memory
Device# install add file bootflash: cat9k_iosxe.17.03.02.SPA.bin activate reloadfast commit
```

The following example shows how to upgrade a standalone switch for an OSPFv3 configuration:

```

Device> enable
Device# configure terminal
Device(config)# ipv6 nd reachable-time 3600000
Device(config)# snmp ifmib ifindex persist
Device(config)# router OSPFv3 1
Device(config-router)# router-id 192.0.2.5
Device(config-router)# interface-id snmp-if-index
Device(config-router)# end
Device# write memory
Device# install add file bootflash: cat9k_iosxe.17.03.02.SPA.bin activate reloadfast commit

```

### Stacked Switch

The following example shows how to upgrade a stacked switch for a configuration other than BGP or OSPFv3:

```

Device> enable
Device# install add file bootflash: cat9k_iosxe.17.03.02.SPA.bin activate reloadfast commit

```

The following example shows how to upgrade a stacked switch for a BGP configuration:

```

Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bgp graceful-restart all
Device(config-router)# end
Device# write memory
Device# install add file bootflash: cat9k_iosxe.17.03.02.SPA.bin activate reloadfast commit

```

The following example shows how to upgrade a stacked switch for an IS-IS configuration:

```

Device> enable
Device# configure terminal
Device(config)# router isis tag1
Device(config-router)# nsf cisco
Device(config-router)# end
Device# write memory
Device# install add file bootflash: cat9k_iosxe.17.03.02.SPA.bin activate reloadfast commit

```



# ip http banner



**Note** The **ip http banner** command is not available in Cisco IOS XE Cupertino 17.9.6 release and later Cisco IOS XE Cupertino 17.9.x releases.

To enable the HTTP or HTTP Secure (HTTPS) server banner, use the **ip http banner** command in global configuration mode. To disable the HTTP or HTTPS server banner, use the **no** form of this command.

**ip http banner**  
**no ip http banner**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The HTTP or HTTPS server banner is not enabled.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.
	Cisco IOS XE Cupertino 17.9.6	This command was removed. It is not available in Cisco IOS XE Cupertino 17.9.6 release and later Cisco IOS XE Cupertino 17.9.x releases.

**Usage Guidelines** While the HTTP server processes a request, if the session ID is invalid or expired, the server redirects the user to a banner page. The banner page allows the user to log in with credentials. The server validates the credentials and processes the request.

**Examples** The following example shows how to enable the HTTP or HTTPS server banner:

```
Device> enable
Device# configure terminal
Device(config)# ip http banner
Device(config)# end
```

Related Commands	Command	Description
	<b>ip http banner-path</b>	Sets a custom path for the HTTP or HTTPS banner page.

# ip http banner-path



**Note** The **ip http banner-path** command is not available in Cisco IOS XE Cupertino 17.9.6 release and later Cisco IOS XE Cupertino 17.9.x releases.

To set a custom path for the HTTP or HTTP Secure (HTTPS) banner page, use the **ip http banner-path** command in global configuration mode. To disable the custom path for the HTTP or HTTPS banner page, use the **no** form of this command.

**ip http banner-path** *path-name*  
**no ip http banner-path** *path-name*

## Syntax Description

<i>path-name</i>	Custom path for the HTTP or HTTPS banner.
------------------	---

## Command Default

The custom path for the HTTP or HTTPS banner is not set.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.
Cisco IOS XE Cupertino 17.9.6	This command was removed. It is not available in Cisco IOS XE Cupertino 17.9.6 release and later Cisco IOS XE Cupertino 17.9.x releases.

## Usage Guidelines

Use the **ip http banner-path** command to direct the user to the banner path.

If the command is not configured or if the custom banner path does not exist, the server directs the user to the default banner page.

## Examples

The following example shows how to set the path to the HTTP or HTTPS banner page:

```
Device> enable
Device# configure terminal
Device(config)# ip http banner-path welcome
Device(config)# end
```

## Related Commands

Command	Description
<b>ip http banner</b>	Enables the HTTP or HTTPS server banner.

# ip ssh bulk-mode

To enable the Secure Shell (SSH) bulk data transfer mode, use the **ip ssh bulk-mode** command in global configuration mode. To disable this mode, use the **no** form of this command.

```
ip ssh bulk-mode [ window-size ]
no ip ssh bulk-mode [ window-size ]
```

<b>Syntax Description</b>	<i>window-size</i> (Optional) The SSH window size. The range is from 131072 to 1073741824. The default is 131072.								
<b>Command Default</b>	SSH bulk mode is enabled.								
<b>Command Modes</b>	Global configuration (config)								
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 17.2.1</td> <td>This command was introduced.</td> </tr> <tr> <td>Cisco IOS XE Bengaluru 17.6.1</td> <td>This command was modified. The <i>window-size</i> variable option was introduced.</td> </tr> <tr> <td>Cisco IOS XE Dublin 17.10.1</td> <td>SSH bulk mode is enabled by default.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Amsterdam 17.2.1	This command was introduced.	Cisco IOS XE Bengaluru 17.6.1	This command was modified. The <i>window-size</i> variable option was introduced.	Cisco IOS XE Dublin 17.10.1	SSH bulk mode is enabled by default.
Release	Modification								
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.								
Cisco IOS XE Bengaluru 17.6.1	This command was modified. The <i>window-size</i> variable option was introduced.								
Cisco IOS XE Dublin 17.10.1	SSH bulk mode is enabled by default.								
<b>Usage Guidelines</b>	<p>SSH bulk mode enables optimizing the throughput performance of procedures that involve the transfer of large amounts of data. The Secure Copy feature has been enhanced to leverage bulk mode optimizations.</p> <p>Beginning from Cisco IOS XE Dublin 17.10.1, SSH bulk mode is enabled by default with the default window size of 128KB.</p>								



- Note**
- Bulk data transfer mode does not support the time or volume-based SSH rekey functionality.
  - Bulk data transfer mode is not supported with SSH Version 1.

## Examples

The following example shows how to enable bulk data transfer mode on an SSH server:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh bulk-mode
Device(config)# exit
```

# I2 traceroute

To enable the Layer 2 traceroute server, use the **I2 traceroute** command in global configuration mode. Use the **no** form of this command to disable the Layer 2 traceroute server.

**I2 traceroute**  
**no I2 traceroute**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Global configuration (config#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	The command was introduced.

**Usage Guidelines** Layer 2 traceroute is enabled by default and opens a listening socket on User Datagram Protocol (UDP) port 2228. To close the UDP port 2228 and disable Layer 2 traceroute, use the **no I2 traceroute** command in global configuration mode.

The following example shows how to configure Layer 2 traceroute using the **I2 traceroute** command.

```
Device# configure terminal
Device(config)# I2 traceroute
```

# license air level

To configure AIR licenses on a wireless controller that is connected to Cisco Catalyst Access, Core, and Aggregation Switches, enter the **license air level** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

**license air level** { **air-network-advantage** [ **addon air-dna-advantage** ] | **air-network-essentials** [ **addon air-dna-essentials** ] }

**no license air level**

Syntax Description							
<b>air-network-advantage</b>	Configures the AIR network advantage license level.						
<b>addon air-dna-advantage</b>	(Optional) Configures the add-on AIR DNA advantage license level. This add-on option is available with the AIR network advantage license, and is the default license.						
<b>air-network-essentials</b>	Configures the AIR network essential license level.						
<b>addon air-dna-essentials</b>	(Optional) Configures the add-on AIR DNA essentials license level. This add-on option is available with the AIR network essential license.						
Command Default	AIR DNA Advantage is the default license						
Command Modes	Global configuration (Device(config)# )						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced.</td> </tr> <tr> <td>Cisco IOS XE Amsterdam 17.3.2a</td> <td>This command continues to be available and applicable with the introduction of Smart Licensing Using Policy in this release. See the <i>Usage Guidelines</i> section below for details.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.	Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available and applicable with the introduction of Smart Licensing Using Policy in this release. See the <i>Usage Guidelines</i> section below for details.
Release	Modification						
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.						
Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available and applicable with the introduction of Smart Licensing Using Policy in this release. See the <i>Usage Guidelines</i> section below for details.						

**Usage Guidelines** In the Smart Licensing Using Policy environment, you can use the **license air level** command to change the license level being used on the product instance, or to additionally configure an add-on license on the product instance. The change is effective after a reload.

The licenses that can be configured are:

- AIR Network Essential
- AIR Network Advantage
- AIR DNA Essential
- AIR DNA Advantage

You can configure AIR DNA Essential or AIR DNA Advantage license level, and on term expiry, you can move to the Network Advantage or Network Essentials license level, if you do not want to renew the DNA license.

Every connecting Access Point requires a Cisco DNA Center License to leverage the unique value properties of the controller.

For more information, see the [Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide](#) for the required release.

### Examples

The following example shows how to configure the AIR DNA Essential license level:

```
Device# configure terminal
Device(config)# license air level network-essentials addon air-dna-essentials
```

The following example shows how to configure the AIR DNA Advantage license level:

```
Device# configure terminal
Device(config)# license air level air-network-advantage addon air-dna-advantage
```

# license boot level

To boot a new software license on the device, use the **license boot level** command in global configuration mode. Use the **no** form of this command to remove all software licenses from the device.

```
license boot level { network-advantage [ addon dna-advantage ] | network-essentials [ addon dna-essentials ] }
```

```
no license boot level
```

Syntax Description		
<b>network-advantage</b> [ <b>addon dna-advantage</b> ]		Configures the Network Advantage license. Optionally, you can also configure the Digital Networking Architecture (DNA) Advantage license.
<b>network-essentials</b> [ <b>addon dna-essentials</b> ]		Configures the Network Essentials license. Optionally, you can also configure the Digital Networking Architecture (DNA) Essentials license.

**Command Default** Network Essentials

**Command Modes** Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Fuji 16.9.1	This command was introduced.
	Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available and applicable with the introduction of Smart Licensing Using Policy in this release. See the <i>Usage Guidelines</i> section below for details.

**Usage Guidelines** The software features available on Cisco Catalyst 9000 Series Switches fall under these base or add-on license levels:

Base Licenses:

- Network Essentials
- Network Advantage—Includes features available with the Network Essentials license and more.

Add-on Licenses:

- DNA Essentials
- DNA Advantage—Includes features available with the Network Essentials license and more.

Base licenses are permanent or perpetual licenses.

Add-on licenses are subscription or term licenses and can be purchased for a three, five, or seven year period. Base licenses are a prerequisite for add-on licenses. See the release notes for more information about this.

The sections below provide information about using the **license boot level** command in the earlier Smart Licensing environment, and in the Smart Licensing Using Policy environment.

**Smart Licensing:** If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, Smart Licensing is enabled by default and you can use the **license boot level** command for these purposes:

- Downgrade or upgrade licenses
- Enable or disable an evaluation or extension license
- Clear an upgrade license

This command forces the licensing infrastructure to boot the configured license level instead of the license hierarchy maintained by the licensing infrastructure for a given module:

- When the switch reloads, the licensing infrastructure checks the configuration in the startup configuration for licenses, if any. If there is a license in the configuration, the switch boots with that license. If there is no license, the licensing infrastructure follows the image hierarchy to check for licenses.
- If the forced boot evaluation license expires, the licensing infrastructure follows the regular hierarchy to check for licenses.
- If the configured boot license has already expired, the licensing infrastructure follows the hierarchy to check for licenses.

**Smart Licensing Using Policy:** If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, Smart Licensing Using Policy is enabled by default and you can use the **license boot level** command for these purposes:

- To change the base or add-on license levels being used on the product instance.

For example, if you are using Network Essentials and you want to use Network Advantage with the next reload, or if you are using DNA Advantage and you want to use DNA Essentials with the next reload.

- To add or remove add-on license levels being used on the product instance.

For example, if you are using only Network Essentials and you want to use DNA Essentials with the next reload, or if you are using DNA Advantage and you do not want to use the add-on after the next reload.

The notion of evaluation or expired licenses does not exist in Smart Licensing Using Policy.

After the command is configured, the configured license is effective after the next reload. License usage continues to be recorded on device and this changed licensing consumption information may have to be sent via the next Resource Utilization Measurement Report (RUM report), to CSSM. The reporting requirements and frequency are determined by the policy that is applied. See the *Usage Reporting*: section of the **show license status** command output. For more information about Smart Licensing Using Policy, in the software configuration guide of the required release, see *System Management > Smart Licensing Using Policy*.

## Examples

The following example shows how to configure the Network Essentials license at the next reload:

```
Device# configure terminal
Device(config)# license boot level network-essentials
Device(config)# exit
Device# copy running-config startup-config
Device# reload
```



The following example shows how to activate the DNA Essentials license at the next reload:

```
Device# configure terminal  
Device(config)# license boot level network-essentials add-on dna-essentials  
Device(config)# exit  
Device# copy running-config startup-config  
Device# reload
```

## license smart (global config)

To configure licensing-related settings such as the mode of transport and the URL that the product instance uses to communicate with Cisco Smart Software Manager (CSSM), or Cisco Smart Licensing Utility (CSLU), or Smart Software Manager On-Prem (SSM On-Prem), to configure the usage reporting interval, to configure the information that must be excluded or included in a license usage report (RUM report), enter the **license smart** command in global configuration mode. Use the **no** form of the command to revert to default values.

```
license smart { custom_id ID | enable | privacy { all | hostname | version } | proxy { address
address_hostname | port port } | reservation | server-identity-check | transport { automatic | callhome
| cslu | off | smart } | url { url | cslu cslu_or_on-prem_url | default | smart smart_url | utility secondary_url
} | usage { customer-tags { tag1 | tag2 | tag3 | tag4 } tag_value | interval interval_in_days } | utility [
customer_info { city city | country country | postalcode postalcode | state state | street street } ] }
```

```
no license smart { custom_id | enable | privacy { all | hostname | version } | proxy { address
address_hostname | port port } | reservation | server-identity-check | transport | url { url | cslu
cslu_or_on-prem_url | default | smart smart_url | utility secondary_url } | usage { customer-tags { tag1
| tag2 | tag3 | tag4 } tag_value | interval interval_in_days } | utility [ customer_info { city city | country
country | postalcode postalcode | state state | street street } ] }
```

Syntax Description		
<b>custom_id</b> <i>ID</i>		Although available on the CLI, this option is not supported.
<b>enable</b>		Although visible on the CLI, configuring this keyword has no effect. Smart licensing is always enabled.

---

**privacy** { **all** | **hostname** | **version** }

Sets a privacy flag to prevent the sending of the specified data privacy related information.

When the flag is disabled, the corresponding information is sent in a message or offline file created by the product instance.

Depending on the topology this is sent to one or more components, including CSSM, CSLU, and SSM On-Prem.

*All data privacy settings are disabled by default.* You must configure the option you want to exclude from all communication:

- **all**: All data privacy related information is excluded from any communication.

The **no** form of the command causes all data privacy related information to be sent in a message or offline file.

**Note** The Product ID (PID) and serial number are *included in the RUM report* regardless of whether data privacy is enabled or not.

- **hostname**: Excludes hostname information from any communication. When hostname privacy is enabled, the *UDI* of the product instance is displayed on the applicable user interfaces (CSSM, CSLU, and SSM On-Prem).

The **no** form of the command causes hostname information to be sent in a message or offline file. The hostname is displayed on the applicable user interfaces (CSSM, CSLU, and SSM On-Prem).

- **version**: Excludes the Cisco IOS-XE software version running on the product instance and the Smart Agent version from any communication.

The **no** form of the command causes version information to be sent in a message or offline file.

---

---

**proxy** { **address** *address\_hostname* | **port** *port* } Configures a proxy for license usage synchronization with CSLU or CSSM. This means that you can use this option to configure a proxy only if the transport mode is **license smart transport smart** (CSSM), or **license smart transport cslu** (CSLU).

However, you cannot configure a proxy for license usage synchronization in an SSM On-Prem deployment, which also uses **license smart transport cslu** as the transport mode.

Configure the following options:

- **address** *address\_hostname*: Configures the proxy address.

For *address\_hostname*, enter the IP address or hostname of the proxy.

- **port***port*: Configures the proxy port.

For *port*, enter the proxy port number.

---

**reservation**

Enables or disables a license reservation feature.

**Note** Although available on the CLI, this option is not applicable because license *reservation* is not applicable in the Smart Licensing Using Policy environment.

---

**server-identity-check**

Enables or disables the HTTP secure server identity check.

---

**transport** { **automatic** | **callhome** | **cslu** | **off** | **smart** } Configures the mode of transport the product instance uses to communicate with CSSM. Choose from the following options:

- **automatic**: Sets the transport mode **cslu**.
- **callhome**: Enables Call Home as the transport mode.
- **cslu**: Enables CSLU as the transport mode. This is the default transport mode.

The same keyword applies to both CSLU *and* SSM On-Prem, but the URLs are different. See **cslucslu\_or\_on-prem\_url** in the following row.

- **off**: Disables all communication from the product instance.
  - **smart**: Enables Smart transport.
-

---

```
url { url | cslu cslu_url | default | smart  
smart_url | utility secondary_url }
```

---

Sets a URL for the configured transport mode. Choose from the following options:

- **url**: If you have configured the transport mode as **callhome**, configure this option. Enter the CSSM URL exactly as follows:

```
https://tools.cisco.com/its/service/odbe/services/DDCEService
```

The **no license smart url url** command reverts to the default URL.

- **cslu cslu\_or\_on-prem\_url**: If you have configured the transport mode as **cslu**, configure this option, with the URL for CSLU or SSM On-Prem, as applicable:

- If you are using CSLU, enter the URL as follows:

```
http://<cslu_ip_or_host>:8182/cslu/v1/pi
```

For **<cslu\_ip\_or\_host>**, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.

The **no license smart url cslu**

**cslu\_or\_on-prem\_url** command reverts to

```
http://cslu-local:8182/cslu/v1/pi
```

- If you are using SSM On-Prem, enter the URL as follows:

```
http://<ip>/cslu/v1/pi/<tenant ID>
```

For **<ip>**, enter the hostname or the IP address of the server where you have installed SSM On-Prem. The **<tenantID>** must be the default local virtual account ID.

**Tip**

You can retrieve the entire URL from SSM On-Prem. In the software configuration guide of the required release (17.3.x onwards), see *System Management > Smart Licensing Using Policy > Task Library for Smart Licensing Using Policy > Retrieving the Transport URL (SSM On-Prem UI)*.

The **no license smart url cslu**

**cslu\_or\_on-prem\_url** command reverts to

```
http://cslu-local:8182/cslu/v1/pi
```

- **default**: Depends on the configured transport mode. Only the **smart** and **cslu** transport modes are supported with this option.

If the transport mode is set to **cslu**, and you configure

**license smart url default**, the CSLU URL is configured automatically

(<https://cslu-local:8182/cslu/v1/pi>).

If the transport mode is set to **smart**, and you configure **license smart url default**, the Smart URL is configured automatically

(<https://smartreceiver.cisco.com/licservice/license>).

- **smart smart\_url**: If you have configured the transport type as **smart**, configure this option. Enter the URL exactly as follows:

<https://smartreceiver.cisco.com/licservice/license>

When you configure this option, the system automatically creates a duplicate of the URL in **license smart url url**. You can ignore the duplicate entry, no further action is required.

The **no license smart url smartsmart\_url** command reverts to the default URL.

- **utility smart\_url**: Although available on the CLI, this option is not supported.
-

---

**usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag\_value* | **interval** *interval\_in\_days* } Configures usage reporting settings. You can set the following options:

- **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag\_value*: Defines strings for inclusion in data models, for telemetry. Up to 4 strings (or tags) may be defined.

For *tag\_value*, enter the string value for each tag that you define.

- **interval** *interval\_in\_days*: Sets the reporting interval in days. By default the RUM report is sent every 30 days. The valid value range is 1 to 3650.

If you set the value to zero, RUM reports are not sent, regardless of what the applied policy specifies - this applies to topologies where CSLU or CSSM may be on the receiving end.

If you set a value that is greater than zero and the transport type is set to **off**, then, between the *interval\_in\_days* and the policy value for `Ongoing reporting frequency(days):`, the lower of the two values is applied. For example, if *interval\_in\_days* is set to 100, and the value in the policy says `Ongoing reporting frequency (days):90`, RUM reports are sent every 90 days.

If you do not set an interval, and the default is effective, the reporting interval is determined entirely by the policy value. For example, if the default value is effective and only unenforced licenses are in use, if the policy states that reporting is not required, then RUM reports are not sent.

---

**utility** [ **customer\_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* } ] Although visible on the CLI, this option is not supported on any of the Cisco Catalyst Access, Core, and Aggregation Switches.

---



---

#### Command Default

Cisco IOS XE Amsterdam 17.3.1 or earlier: Smart Licensing is enabled by default

Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy is enabled by default.

---

#### Command Modes

Global config (Device(config)# )

---

#### Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

---



Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	<p>The following keywords and variables were introduced with Smart Licensing Using Policy:</p> <ul style="list-style-type: none"> <li>Under the <b>url</b> keyword, these options were introduced:           <pre>{ cslu cslu_url   smart smart_url }</pre> </li> <li>Under the <b>transport</b> keyword, these options were introduced:           <pre>{ cslu   off }</pre> <p>Further, the default transport type was changed from <b>callhome</b>, to <b>cslu</b>.</p> </li> <li><b>usage { customer-tags { tag1   tag2   tag3   tag4 } tag_value   interval interval_in_days }</b></li> </ul> <p>The following keywords and variables under the <b>license smart</b> global command are deprecated and no longer available on the CLI: <b>enableand conversion automatic</b>.</p>
Cisco IOS XE Amsterdam 17.3.3	<p>SSM On-Prem support was introduced. For product instance-initiated communication in an SSM On-Prem deployment, the existing <b>[no ]license smart url cslu cslu_or_on-prem_url</b> command supports the configuration of a URL for SSM On-Prem as well. But the required URL format for SSM On-Prem is:  <pre>http://&lt;ip&gt;/cslu/v1/pi/&lt;tenant ID&gt;</pre> </p> <p>The corresponding transport mode that must be configured is also an existing command (<b>license smart transport cslu</b>).</p>
Cisco IOS XE Cupertino 17.7.1	<p>If version privacy is disabled (<b>no license smart privacy version</b> global configuration command), the Cisco IOS-XE software version running on the product instance and the Smart Agent version is <i>included</i> in the RUM report.</p> <p>To exclude version information from the RUM report, version privacy must be enabled (<b>license smart privacy version</b>).</p>
Cisco IOS XE Cupertino 17.9.1	<ul style="list-style-type: none"> <li>Support for sending hostname information was introduced.           <p>If the privacy setting for the hostname is disabled (<b>no license smart privacy hostname</b> global configuration command), hostname information is sent from the product instance, in a separate sync message, or offline file. Depending on the topology you have implemented, the hostname information is received by CSSM, CSLU, or SSM On-Prem. It is also displayed on the corresponding user interface.</p> </li> <li>A new mechanism to send all data privacy related information was introduced. This information is no longer included in a RUM report.           <p>If data privacy is disabled (<b>no license smart privacy {all   hostname   version}</b> global configuration command), data privacy related information is sent in a separate sync message or offline file.</p> </li> </ul>

When you disable a privacy setting, the topology you have implemented determines the recipient and how the information reaches its destination:

- The recipient of the information may be one or more of the following: CSSM, CSLU, and SSM On-Prem. The privacy setting has no effect on a controller (Cisco DNA Center).

In case of the **hostname** keyword, after the hostname information is received by CSSM, CSLU, or SSM On-Prem, it is also displayed on the corresponding UIs – as applicable. If you then *enable* privacy the corresponding UIs revert to displaying the UDI of the product instance.

- How the information is sent.
  - In case of a topology where the product instance initiates communication, the product instance initiates the sending of this information in a message, to CSSM, or CSLU, or SSM On-Prem.
 

The product instance sends the hostname sent every time one of the following events occur: the product instance boots up, the hostname changes, there is a switchover in a High Availability set-up.
  - In case of a topology where CSLU or SSM On-Prem initiate communication, the corresponding component initiates the retrieval of privacy information from the product instance.
 

The hostname is retrieved at the frequency you configure in CSLU or SSM On-Prem, to retrieve information.
  - In case of a topology where the product instance is in an air-gapped network, privacy information is included in the offline file that is generated when you enter the **license smart save usage** privileged EXEC command.




---

**Note** For all topologies, data privacy related information is *not* included in the RUM report.

---

Data privacy related information it is not stored by the product instance *prior* to sending or saving. This ensures that if and when information is sent, it is consistent with the data privacy setting at the time of sending or saving.

### Communication failure and reporting

The reporting interval that you configure (**license smart usage interval** *interval\_in\_days* command), determines the date and time at which the product instance sends out the RUM report. If the scheduled interval coincides with a communication failure, the product instance attempts to send out the RUM report for up to four hours after the scheduled time has expired. If it is still unable to send out the report (because the communication failure persists), the system resets the interval to 15 minutes. Once the communication failure is resolved, the system reverts the reporting interval to the value that you last configured.

The system message you may see in case of a communication failure is %SMART\_LIC-3-COMM\_FAILED. For information about resolving this error and restoring the reporting interval value, in the software configuration guide of the required release (17.3.x onwards), see *System Management > Smart Licensing Using Policy > Troubleshooting Smart Licensing Using Policy*.

### Proxy server acceptance

When configuring the **license smart proxy** {**address** *address\_hostname* | **port***port*} command, note the change in the criteria for the acceptance of proxy servers, starting with Cisco IOS XE Bengaluru 17.6.1: only the status code of the proxy server response is verified by the system and not the reason phrase. The RFC

format is `status-line = HTTP-version SP status-code SP reason-phrase CRLF`, where the status code is a three-digit numeric code. For more information about the status line, see [section 3.1.2 of RFC 7230](#).

- [Examples for Data Privacy, on page 67](#)
- [Examples for Transport Type and URL, on page 68](#)
- [Examples for Usage Reporting Options, on page 68](#)

### Examples for Data Privacy

The following examples show how to configure data privacy related information using **license smart privacy** command in global configuration mode. The accompanying **show license status** output displays configured information.




---

**Note** The output of the **show** command only tells you if a particular option is enabled or disabled.

---

Here, no data privacy related information is sent:

```
Device# configure terminal
Device(config)# license smart privacy all
Device(config)# exit
Device# show license status
<output truncated>
Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: ENABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED

Transport:
  Type: Callhome
<output truncated>
```

Here, hostname is included and version information is excluded in the message initiated from the product instance. The product instance is directly connected to CSSM (transport type is **smart**, with the corresponding URL).

```
Device# configure terminal
Device(config)# license smart privacy version
Device(config)# no license smart privacy hostname
Device(config)# exit

Device# show license all
<output truncated>

Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
```

```
VRF:
  Not Configured

<output truncated>
```

### Examples for Transport Type and URL

The following examples show how to configure some of the transport types using the **license smart transport** and the **license smart url** commands in global configuration mode. The accompanying **show license all** output displays configured information.

Transport: **cslu**:

```
Device# configure terminal
Device(config)# license smart transport cslu
Device(config)# license smart url default
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  Proxy:
    Not Configured
<output truncated>
```

Transport: **smart**:

```
Device# configure terminal
Device(config)# license smart transport smart
Device(config)# license smart url smart https://smartreceiver.cisco.com/licservice/license
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
    Not Configured
<output truncated>
```

### Examples for Usage Reporting Options

The following examples show how to configure some of the usage reporting settings using the **license smart usage** command in global configuration mode. The accompanying **show running-config** output displays configured information.

Configuring the **customer-tag** option:

```
Device# configure terminal
Device(config)# license smart usage customer-tags tag1 SA/VA:01
Device(config)# exit
Device# show running-config | include tag1
license smart usage customer-tags tag1 SA/VA:01
```

Configuring a narrower reporting interval than the currently applied policy:

```
Device# show license status
<output truncated>
Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Dec 21 12:02:21 2020 PST
Reporting push interval: 30 days
```

```
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 22 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>
```

```
Device# configure terminal
Device(config)# license smart usage interval 20
Device(config)# exit
Device# show license status
<output truncated>
```

```
Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Nov 22 12:02:21 2020 PST
Reporting push interval: 20 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 12 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>
```

## license smart (privileged EXEC)

To configure licensing functions such as requesting or returning authorization codes, saving Resource Utilization Measurement reports (RUM reports), importing a file on to a product instance, establishing trust with Cisco Smart Software Manager (CSSM), synchronizing the product instance with CSSM, or Cisco Smart License Utility (CSLU), or Smart Software Manager On-Prem (SSM On-Prem), and removing licensing information from the product instance, enter the **license smart** command in privileged EXEC mode with the corresponding keyword or argument.

```
license smart { authorization { request { add | replace | save path } feature_name { all | local } | return
{ all | local } { offline [ path ] | online } } | clear eventlog | export return { all | local } feature_name
| factory reset | import file_path | save { trust-request filepath_filename | usage { all | days days | rum-id
rum-ID | unreported } { file file_path } } | sync { all | local } | trust idtoken id_token_value { local | all
} [ { force } ] }
```

Syntax Description	smart	Provides options for Smart Licensing.
	<b>authorization</b>	Provides the option to request for, or return, authorization codes.  Authorization codes are required <i>only</i> if you use licenses with enforcement type: export-controlled or enforced.
	<b>request</b>	Requests an authorization code from CSSM, CSLU (CSLU in-turn fetches it from CSSM), or SSM On-Prem and installs it on the product instance.
	<b>add</b>	Adds the requested license to the existing authorization code. The new authorization code will contain all the licenses of the existing authorization code and the requested license.
	<b>replace</b>	Replaces the existing authorization code. The new authorization code will contain only the requested license. All licenses in the current authorization code are returned.  When you enter this option, the product instance verifies if licenses that correspond to the authorization codes that will be removed, are in-use. If licenses are being used, an error message tells you to first disable the corresponding features.
	<b>save filepath_filename</b>	Saves the authorization code request to a file.  For <i>filepath_filename</i> , specify the absolute path to the file, including the filename.
	<i>feature_name</i>	Name of the license for which you are requesting an authorization code.
	<b>all</b>	Performs the action for all product instances in a High Availability or stacking set-up.
	<b>local</b>	Performs the action for the <i>active</i> product instance. This is the default option.
	<b>return</b>	Returns an authorization code back to the license pool in CSSM.

<b>offline</b> <i>filepath_filename</i>	<p>Means the product instance is not connected to CSSM. The authorization code is returned offline. This option requires you to print the return code to a file.</p> <p>Optionally, you can also specify a path to save the file. The file format can be any readable format, such as <code>.txt</code>.</p> <p>If you choose the offline option, you must complete the additional step of copying the return code from the CLI or the saved file and entering it in CSSM.</p>
<b>online</b>	Means that the product instance is in a connected mode. The authorization code is returned to CSLU or CSSM directly.
<b>clear eventlog</b>	Clears all event log files from the product instance.
<b>export return</b>	Although visible on the CLI, this command is not applicable in the Smart Licensing Using Policy environment. Use the <b>license smart authorization return</b> privileged EXEC command to return an authorization code instead.
<b>factory reset</b>	Clears all saved licensing information from the product instance.
<b>import</b> <i>filepath_filename</i>	<p>Imports a file on to the product instance. The file may be that of an authorization code, a trust code, or, or a policy.</p> <p>For <i>filepath_filename</i>, specify the location, including the filename.</p>
<b>save</b>	Provides options to save RUM reports or trust code requests.
<b>trust-request</b> <i>filepath_filename</i>	<p>Saves the trust code request for the active product instance in the specified location.</p> <p>For <i>filepath_filename</i>, specify the absolute path to the file, including the filename.</p>
<b>usage</b> { <b>all</b>   <b>days</b> <i>days</i>   <b>rum-id</b> <i>rum-ID</i>   <b>unreported</b> } { <b>file</b> <i>file_path</i> }	<p>Saves RUM reports (license usage information) in the specified location. You must specify one of these options:</p> <ul style="list-style-type: none"> <li>• <b>all</b>: Saves all RUM reports.</li> <li>• <b>days</b> <i>days</i>: Saves RUM report for the last <i>n</i> number of days (excluding the current day). Enter a number. The valid range is 0 to 4294967295. For example, if you enter 3, RUM reports of the last three days are saved.</li> <li>• <b>rum-Id</b> <i>rum-ID</i>: Saves a specified RUM ID. The valid value range is 0 to 18446744073709551615.</li> <li>• <b>unreported</b>: Saves all unreported RUM reports.</li> </ul> <p><b>file</b> <i>filepath_filename</i>: Saves the specified usage information to a file. Specify the absolute path to the file, including the filename.</p>

---

**sync** { **all** | **local** } Synchronizes with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. This includes uploading pending RUM reports, downloading the ACK response, any pending authorization codes, trust codes, and policies for the product instance.

Specify the product instance by entering one of these options:

- **all**: Performs synchronization for all the product instances in a High Availability or stacking set-up. If you choose this option, the product instance also sends the list of all the UDIs in the synchronization request.
- **local**: Performs synchronization only for the active product instance sending the request, that is, its own UDI. This is the default option.

---

**trust idtoken**  
*id\_token\_value* Establishes a trusted connection with CSSM.  
To use this option, you must first generate a token in the CSSM portal. Provide the generated token value for *id\_token\_value*.

---

**force** Submits a trust code request even if a trust code already exists on the product instance.  
  
A trust code is node-locked to the UDI of a product instance. If the UDI is already registered, CSSM does not allow a new registration for the same UDI. Entering the **force** keyword overrides this behavior.

---



---

#### Command Default

Cisco IOS XE Amsterdam 17.3.1 and earlier: Smart Licensing is enabled by default.

Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy is enabled by default.

---

#### Command Modes

Privileged EXEC (Device# )

---

#### Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

---



Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	<p>The following keywords and variables were introduced with Smart Licensing Using Policy:</p> <ul style="list-style-type: none"> <li>• <b>authorization</b> { <b>request</b> { <b>add</b>   <b>replace</b> } <i>feature_name</i> { <b>all</b>   <b>local</b> }   <b>return</b> { <b>all</b>   <b>local</b> } { <b>offline</b> [ <i>path</i> ]   <b>online</b> } }</li> <li>• <b>import</b> <i>file_path</i></li> <li>• <b>save</b> { <b>trust-request</b> <i>filepath_filename</i>   <b>usage</b> { <b>all</b>   <b>days</b> <i>days</i>   <b>rum-id</b> <i>rum-ID</i>   <b>unreported</b> } { <b>file</b> <i>file_path</i> } }</li> <li>• <b>sync</b> { <b>all</b>   <b>local</b> }</li> <li>• <b>trust idtoken</b> <i>id_token_value</i> { <b>local</b>   <b>all</b> } [ <b>force</b> ]</li> </ul> <p>The following keywords and variables under the <b>license smart</b> command are deprecated and no longer available on the CLI:</p> <ul style="list-style-type: none"> <li>• <b>register idtoken</b> <i>token_id</i> [ <b>force</b> ]</li> <li>• <b>deregister</b></li> <li>• <b>renew id</b> { <b>ID</b>   <b>auth</b> }</li> <li>• <b>debug</b> { <b>error</b>   <b>debug</b>   <b>trace</b>   <b>all</b> }</li> <li>• <b>mfg reservation</b> { <b>request</b>   <b>install</b>   <b>install file</b>   <b>cancel</b> }</li> <li>• <b>conversion</b> { <b>start</b>   <b>stop</b> }</li> </ul>
Cisco IOS XE Amsterdam 17.3.3	Support for SSM On-Prem was introduced. You can perform licensing-related tasks such as saving Resource Utilization Measurement reports (RUM reports), importing a file on to a product instance, synchronizing the product instance, returning authorization codes, and removing licensing information from the product instance in an SSM On-Prem deployment.
Cisco IOS XE Bengaluru 17.6.2	Support for the Export Control Key for High Security (HSECK9 key) was introduced on the Cisco Catalyst 9300X Series Switches. The authorization code related commands ( <b>license smart authorization request</b> and <b>license smart authorization return</b> ) can be used to request and return the Smart Licensing Authorization Code (SLAC) for the HSECK9 key, on supported platforms.
Cisco IOS XE Cupertino 17.7.1	<p>The following enhancements were introduced in this release:</p> <ul style="list-style-type: none"> <li>• The <b>save path</b> keyword and variable were added to the <b>license smart authorization request</b> command string. You can use this option to generate a SLAC request and save it to a file. The new options are displayed as follows: <ul style="list-style-type: none"> <li><b>license smart authorization request</b> { <b>add</b>   <b>replace</b>   <b>save path</b> } <i>feature_name</i> { <b>all</b>   <b>local</b> } <i>request_count</i></li> </ul> </li> <li>• The existing <b>license smart save usage</b> command was enhanced to automatically include a trust code request if it doesn't already exist.</li> </ul>

Release	Modification
Cisco IOS XE Cupertino 17.8.1	<p>The authorization code related commands (<b>license smart authorization request</b> and <b>license smart authorization return</b>) were implemented on the following products:</p> <ul style="list-style-type: none"> <li>• Cisco Catalyst 9600 Series 40-Port 50G, 2-Port 200G, 2-Port 400G Line Card (C9600-LC-40YL4CD)</li> <li>• Cisco Catalyst 9500X Series Switches</li> </ul> <p>You can use the above commands to request and return the Smart Licensing Authorization Code (SLAC) for the HSECK9 key on supported platforms.</p>

## Usage Guidelines

### Requesting a Trust Code in an Air-Gapped Network

Starting with Cisco IOS XE Cupertino 17.7.1 if a trust code is not available on the product instance, the product instance automatically includes a trust code request in the RUM report when you enter the **license smart save usage** command. This is supported in a standalone set-up, as well as a High Availability and stacking set-up. In a High Availability and stacking set-up, the active product instance requests and installs the trust code for all members or standbys where a trust code is missing. CSSM includes the trust code in the ACK which is available for download from the CSSM Web UI. You then have to install the ACK on the product instance. You can verify trust code installation by entering the **show license status** command in privileged EXEC mode - check for the updated timestamp in the `Trust Code Installed` field.

### Overwriting a Trust Code

Use cases for the **force** option when configuring the **license smart trust idtoken** command:

- You use same token for all the product instances that are part of one Virtual Account. If the product instance has moved from one account to another (for instance, because it was added to a High Availability set-up, which is part of another Virtual Account), then there may be an existing trust code you have to overwrite.
- There is already a factory-installed trust code on the product instance, but you want to implement a topology where the product instance is directly connected to CSSM. A factory-installed trust code cannot be used for secure communication with CSSM. You must generate an ID token in the CSSM Web UI and download a trust code file. When you install this new trust code, you must overwrite the existing factory-installed trust code.

### Removing Licensing Information

Entering the **license smart factory reset** command removes all licensing information (except the licenses in-use) from the product instance, including any authorization codes, RUM reports etc. Therefore, we recommend the use of this command only if the product instance is being returned (Return Material Authorization, or RMA), or being decommissioned permanently. We also recommend that you return any authorization codes and send a RUM report to CSSM, before you remove licensing information from the product instance - this is to ensure that CSSM has up-to-date usage information.

### Requesting and Returning Authorization Codes:

- Requesting and returning SLAC - when the product instance is connected to CSSM, or CSLU or SSM On-Prem:
  - Use the following command to request SLAC on supported product instances. In a stacking set-up, you can request SLAC for either the active (**local**), or the entire stack (**all**). You cannot request

SLAC for just one member or standby. Here the product instance is connected to CSSM, or CSLU or SSM On-Prem. For air-gapped networks, you must enter the required details directly in CSSM to generated SLAC.

**license smart authorization request { add | replace } feature\_name { all | local }**

- Use the following command to return a SLAC or an SLR authorization code:

**license smart authorization return { all | local } { online }**

- Requesting and returning a SLAC when the product instance is in an air-gapped network.
  - Starting from Cisco IOS XE Cupertino 17.7.1

You can request and install a SLAC without having to enter the required PIDs or generating a SLAC in the CSSM Web UI. Instead, save a SLAC request in a file by configuring the **license smart authorization request { add | replace } feature\_name { all | local }**, followed by the **license smart authorization request save [path]** commands.

Upload the SLAC request file, to the CSSM Web UI (in the same location and just as you would, a RUM report). After the request is processed, a SLAC file is available on the CSSM Web UI. Download, and import the SLAC file into the product instance.

Similarly, to return a SLAC configure the **license smart authorization return** command with the **offline [path]** option to save the file. Upload the file to the CSSM Web UI in the same location and just as you would, a RUM report).

- Prior to Cisco IOS XE Cupertino 17.7.1:

To request SLAC on a product instance in an air-gapped network, you must enter the required details directly in the CSSM Web UI to generate SLAC.

To return a SLAC or an SLR authorization code:

**license smart authorization return { all | local } { offline [ path ] | online }**

Copy the return code that is displayed on the CLI and enter it in CSSM. If you save the return code to a file, you can copy the code from the file and enter the same in CSSM.

For SLR authorization codes in the Smart Licensing Using Policy environment, note that you cannot request a new SLR in the Smart Licensing Using Policy environment, because the notion of “reservation” does not apply. If you are in an air-gapped network, the *No Connectivity to CSSM and No CSLU* topology applies instead.

### Authorization Codes in an SSM On-Prem Deployment

When requesting SLAC in an SSM On-Prem Deployment, ensure that you meet the following prerequisites before you configure the **license smart authorization request** command:

- The product instance must be added to SSM On-Prem. The process of addition validates and maps the product instance to the applicable Smart Account and Virtual account in CSSM.
- The authorization codes required for export-controlled and enforced licenses must be generated in CSSM and imported into SSM On-Prem.

## Examples

- [Example for Requesting SLAC \(Connected Directly to CSSM\), on page 76](#)
- [Example for Saving Licensing Usage Information, on page 77](#)
- [Example for Installing a Trust Code, on page 77](#)
- [Example for Returning an SLR Authorization Code, on page 78](#)

### Example for Requesting SLAC (Connected Directly to CSSM)

The following example shows how you can request and install SLAC on a product instance that is directly connected to CSSM. This example is of a stacking set-up with an active, a standby, and a member - all the devices in the stack are C9300X and support the HSECK9 key and IPsec. IPsec is a cryptographic feature which requires the HSECK9 key. A SLAC is requested for all the product instances in the set-up.

```
Device# license smart authorization request add hseck9 all
Device#
Oct 19 15:49:47.888: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization
code was successfully installed on PID:C9300X-24HX,SN:FOC2519L8R7
Oct 19 15:49:47.946: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization
code was successfully installed on PID:C9300X-48HXN,SN:FOC2524L39P
Oct 19 15:49:48.011: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization
code was successfully installed on PID:C9300X-48HX,SN:FOC2516LC92

Device# show license authorization
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
    Status: SMART AUTHORIZATION INSTALLED on Oct 19 15:49:47 2021 UTC
    Last Confirmation code: 4e740fb8
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
    Status: SMART AUTHORIZATION INSTALLED on Oct 19 15:49:47 2021 UTC
    Last Confirmation code: 086d28d7
  Member: PID:C9300X-48HX,SN:FOC2516LC92
    Status: SMART AUTHORIZATION INSTALLED on Oct 19 15:49:48 2021 UTC
    Last Confirmation code: beb51aa1

Authorizations:
C9K HSEC (Cat9K HSEC):
  Description: HSEC Key for Export Compliance on Cat9K Series Switches
  Total available count: 3
  Enforcement type: EXPORT RESTRICTED
  Term information:
    Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Authorization type: SMART AUTHORIZATION INSTALLED
      License type: PERPETUAL
      Term Count: 1
    Standby: PID:C9300X-48HXN,SN:FOC2524L39P
      Authorization type: SMART AUTHORIZATION INSTALLED
      License type: PERPETUAL
      Term Count: 1
    Member: PID:C9300X-48HX,SN:FOC2516LC92
      Authorization type: SMART AUTHORIZATION INSTALLED
      License type: PERPETUAL
      Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

**Example: Requesting a SLAC and Returning a SLAC (No Connectivity to CSSM and No CSLU)**

The following examples show you how to generate and save a SLAC request on the product instance and also how to return a SLAC to the CSSM Web UI, for a product instance in an air-gapped network. The software version running on the product instance is Cisco IOS XE Cupertino 17.7.1, which introduces support for a more simplified way of requesting and returning SLAC in an air-gapped network.

Requesting a SLAC

```
Device# license smart authorization request add hseck9 local
Device# license smart authorization request save bootflash:slac-request.txt
```

After the above steps, upload the file to the CSSM Web UI. From the CSSM Web UI, download the file containing the SLAC. To import and install the file on the product instance, enter the following commands:

```
Device# copy tftp://10.8.0.6/user01/slac_code.txt bootflash:
Device# license smart import bootflash:slac_code.txt
```

Returning a SLAC

```
Device# license smart authorization return local offline bootflash:auth_return.txt
```

After the above step, upload the file to the CSSM Web UI. A file is available for download after this, but import and installation of this file is optional.

**Example for Saving Licensing Usage Information**

The following example shows how you can save license usage information on the product instance. You can use this option to fulfil reporting requirements in an air-gapped network. In the example, the file is first save to flash memory and then copied to a TFTP location:

```
Device> enable
Device# license smart save usage unreported file flash:RUM-unrep.txt
Device# copy flash:RUM-unrep.txt tftp://192.168.0.1//auto/tftp-user/user01/
Address or name of remote host [192.168.0.1]?
Destination filename [//auto/tftp-user/user01/RUM-unrep.txt]?
!!
15128 bytes copied in 0.161 secs (93963 bytes/sec)
```

After you save RUM reports to a file, you must upload it to CSSM (from a workstation that has connectivity to the internet, and Cisco).

**Example for Installing a Trust Code**

The following example shows how to install a trust code even if one is already installed on the product instance. This requires connectivity to CSSM. The accompanying **show license status** output shows sample output after successful installation:

Before you can install a trust code, you must generate a token and download the corresponding file from CSSM.

Use the **show license status** command (Trust Code Installed:) to verify results.

```
Device> enable
Device# license smart trust idtoken
NGMwMjk5mYtNZaxMS00NzZmtgWm local force
Device# show license status
<output truncated>
```

```
Trust Code Installed:
  Active: PID:C9500-24Y4C,SN:CAT2344L4GH
         INSTALLED on Sep 04 01:01:46 2020 EDT
  Standby: PID:C9500-24Y4C,SN:CAT2344L4GJ
         INSTALLED on Sep 04 01:01:46 2020 EDT
<output truncated>
```

### Example for Returning an SLR Authorization Code

The following example shows how to remove and return an SLR authorization code. Here the code is returned offline (no connectivity to CSSM). The accompanying **show license all** output shows sample output after successful return:

```
Device> enable
Device# license smart authorization return local offline
Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:C9500-16X,SN:FCW2233A5ZV
Return code: Cr9JHx-L1x5Rj-ftwzgl-h9QZAU-LE5DT1-babWeL-FABPt9-Wr1Dn7-Rp7
Device# configure terminal
Device(config)# no license smart reservation

Device# show license all
<output truncated>
License Authorizations
=====
Overall status:
  Active: UDI: PID:C9500-16X,SN:FCW2233A5ZV
         Status: NOT INSTALLED
         Last return code: Cr9JHx-L1x5Rj-ftwzgl-h9QZAU-LE5DT1-babWeL-FABPt9-Wr1Dn7-Rp7
<output truncated>
```

Since the product instance is in an air-gapped network, you must copy the return code from the CLI, locate the product instance in the CSSM Web UI and enter the return code there to complete the return process.

# line auto-consolidation

To consolidate multiple line configurations of the same submode into a single line, use the **line auto-consolidation** command in global configuration mode. Auto-consolidation of line configurations is enabled by default. Starting with the Cisco IOS XE Bengaluru 17.4.1 you can disable auto consolidation by using the **no** form of the command.

**line auto-consolidation**  
**no line auto-consolidation**

<b>Syntax Description</b>	<b>auto-consolidation</b>	Consolidates multiple line configurations of the same submode into a single line.
<b>Command Default</b>	Autoconsolidation is enabled by default.	
<b>Command Modes</b>	Global configuration mode (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.4.1	The command was introduced.

The following example shows the nonvolatile generation (NVGEN) process output with **line auto-consolidation** configured:

```
Device# show run | sec line
line con 0
stopbits 1
line vty 0 4
transport input ssh
line vty 5 9
transport input all
Device# configure terminal
Device(config)# line vty 10 15
Device(config-line)# transport input all
Device(config-line)# end
Device# show run | sec line
line con 0
stopbits 1
line vty 0 4
transport input ssh
line vty 5 15
transport input all
```

The following example shows the nonvolatile generation (NVGEN) process output after **no line auto-consolidation** is configured:

```
Device# show run | sec line
line con 0
stopbits 1
line vty 0 4
transport input ssh
line vty 5 9
transport input all
Device# configure terminal
```

```
Device(config)#no line auto-consolidation
Device(config)# line vty 10 15
Device(config-line)# transport input all
Device(config-line)# end
Device# show run | sec line
no line auto-consolidation
line con 0
stopbits 1
line vty 0 4
transport input ssh
line vty 5 9
transport input all
line vty 10 15
transport input all
```



# location

To configure location information for an endpoint, use the **location** command in global configuration mode. To remove the location information, use the **no** form of this command.

```
location {admin-tag string | civic-location identifier {hostid} | civic-location identifier {hostid} |
elin-location {string | identifier id} | geo-location identifier {hostid} | prefer {cdp weight
priority-value | lldp-med weight priority-value | static config weight priority-value}
no location {admin-tag string | civic-location identifier {hostid} | civic-location identifier {hostid} |
elin-location {string | identifier id} | geo-location identifier {hostid} | prefer {cdp weight
priority-value | lldp-med weight priority-value | static config weight priority-value}
```

Syntax Description		
<b>admin-tag</b>	<i>string</i>	Configures administrative tag or site information. Site or location information in alphanumeric format.
<b>civic-location</b>		Configures civic location information.
<b>identifier</b>		Specifies the name of the civic location, emergency, or geographical location.
<b>host</b>		Defines the host civic or geo-spatial location.
<i>id</i>		Name of the civic, emergency, or geographical location.  <b>Note</b> The identifier for the civic location in the LLDP-MED switch TLV is limited to 250 bytes or less. To avoid error messages about available buffer space during switch configuration, be sure that the total length of all civic-location information specified for each civic-location identifier does not exceed 250 bytes.
<b>elin-location</b>		Configures emergency location information (ELIN).
<b>geo-location</b>		Configures geo-spatial location information.
<b>prefer</b>		Sets location information source priority.

**Command Default** No default behavior or values.

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** After entering the **location civic-location identifier** global configuration command, you enter civic location configuration mode. After entering the **location geo-location identifier** global configuration command, you enter geo location configuration mode.

The civic-location identifier must not exceed 250 bytes.

The host identifier configures the host civic or geo-spatial location. If the identifier is not a host, the identifier only defines a civic location or geo-spatial template that can be referenced on the interface.

The **host** keyword defines the device location. The civic location options available for configuration using the **identifier** and the **host** keyword are the same. You can specify the following civic location options in civic location configuration mode:

- **additional-code**—Sets an additional civic location code.
- **additional-location-information**—Sets additional civic location information.
- **branch-road-name**—Sets the branch road name.
- **building**—Sets building information.
- **city**—Sets the city name.
- **country**—Sets the two-letter ISO 3166 country code.
- **county**—Sets the county name.
- **default**—Sets a command to its defaults.
- **division**—Sets the city division name.
- **exit**—Exits from the civic location configuration mode.
- **floor**—Sets the floor number.
- **landmark**—Sets landmark information.
- **leading-street-dir**—Sets the leading street direction.
- **name**—Sets the resident name.
- **neighborhood**—Sets neighborhood information.
- **no**—Negates the specified civic location data and sets the default value.
- **number**—Sets the street number.
- **post-office-box**—Sets the post office box.
- **postal-code**—Sets the postal code.
- **postal-community-name**—Sets the postal community name.
- **primary-road-name**—Sets the primary road name.
- **road-section**—Sets the road section.
- **room**—Sets room information.
- **seat**—Sets seat information.
- **state**—Sets the state name.
- **street-group**—Sets the street group.
- **street-name-postmodifier**—Sets the street name postmodifier.
- **street-name-premodifier**—Sets the street name premodifier.
- **street-number-suffix**—Sets the street number suffix.
- **street-suffix**—Sets the street suffix.
- **sub-branch-road-name**—Sets the sub-branch road name.
- **trailing-street-suffix**—Sets the trailing street suffix.
- **type-of-place**—Sets the type of place.
- **unit**—Sets the unit.

You can specify the following geo-spatial location information in geo-location configuration mode:

- **altitude**—Sets altitude information in units of floor, meters, or feet.
- **latitude**—Sets latitude information in degrees, minutes, and seconds. The range is from -90 degrees to 90 degrees. Positive numbers indicate locations north of the equator.

- **longitude**—Sets longitude information in degrees, minutes, and seconds. The range is from -180 degrees to 180 degrees. Positive numbers indicate locations east of the prime meridian.
- **resolution**—Sets the resolution for latitude and longitude. If the resolution value is not specified, default value of 10 meters is applied to latitude and longitude resolution parameters. For latitude and longitude, the resolution unit is measured in meters. The resolution value can also be a fraction.
- **default**—Sets the geographical location to its default attribute.
- **exit**—Exits from geographical location configuration mode.
- **no**—Negates the specified geographical parameters and sets the default value.

Use the **no lldp med-tlv-select location information** interface configuration command to disable the location TLV. The location TLV is enabled by default.

This example shows how to configure civic location information on the switch:

```
Device(config)# location civic-location identifier 1
Device(config-civic)# number 3550
Device(config-civic)# primary-road-name "Cisco Way"
Device(config-civic)# city "San Jose"
Device(config-civic)# state CA
Device(config-civic)# building 19
Device(config-civic)# room C6
Device(config-civic)# county "Santa Clara"
Device(config-civic)# country US
Device(config-civic)# end
```

You can verify your settings by entering the **show location civic-location** privileged EXEC command.

This example shows how to configure the emergency location information on the switch:

```
Device(config)# location elin-location 14085553881 identifier 1
```

You can verify your settings by entering the **show location elin** privileged EXEC command.

The example shows how to configure geo-spatial location information on the switch:

```
Device(config)# location geo-location identifier host
Device(config-geo)# latitude 12.34
Device(config-geo)# longitude 37.23
Device(config-geo)# altitude 5 floor
Device(config-geo)# resolution 12.34
```

You can use the **show location geo-location identifier** command to display the configured geo-spatial location details.

# location plm calibrating

To configure path loss measurement (CCX S60) request for calibrating clients, use the **location plm calibrating** command in global configuration mode.

**location plm calibrating** {**multiband** | **uniband**}

Syntax Description	
<b>multiband</b>	Specifies the path loss measurement request for calibrating clients on the associated 802.11a or 802.11b/g radio.
<b>uniband</b>	Specifies the path loss measurement request for calibrating clients on the associated 802.11a/b/g radio.

**Command Default** No default behavior or values.

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** The uniband is useful for single radio clients (even if the radio is a dual band and can operate in the 2.4-GHz and the 5-GHz bands). The multiband is useful for multiple radio clients.

This example shows how to configure the path loss measurement request for calibrating clients on the associated 802.11a/b/g radio:

```
Device# configure terminal
Device(config)# location plm calibrating uniband
Device(config)# end
```

# mac address-table move update

To enable the MAC address table move update feature, use the **mac address-table move update** command in global configuration mode on the switch stack or on a standalone switch. To return to the default setting, use the **no** form of this command.

```
mac address-table move update {receive | transmit}
no mac address-table move update {receive | transmit}
```

## Syntax Description

<b>receive</b>	Specifies that the switch processes MAC address-table move update messages.
<b>transmit</b>	Specifies that the switch sends MAC address-table move update messages to other switches in the network if the primary link goes down and the standby link comes up.

## Command Default

By default, the MAC address-table move update feature is disabled.

## Command Modes

Global configuration

## Command History

### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

## Usage Guidelines

The MAC address-table move update feature allows the switch to provide rapid bidirectional convergence if a primary (forwarding) link goes down and the standby link begins forwarding traffic.

You can configure the access switch to send the MAC address-table move update messages if the primary link goes down and the standby link comes up. You can configure the uplink switches to receive and process the MAC address-table move update messages.

## Examples

This example shows how to configure an access switch to send MAC address-table move update messages:

```
Device# configure terminal
Device(config)# mac address-table move update transmit
Device(config)# end
```

This example shows how to configure an uplink switch to get and process MAC address-table move update messages:

```
Device# configure terminal
Device(config)# mac address-table move update receive
Device(config)# end
```

You can verify your setting by entering the **show mac address-table move update** privileged EXEC command.

# mgmt\_init

To initialize the Ethernet management port, use the **mgmt\_init** command in boot loader mode.

## **mgmt\_init**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** No default behavior or values.

---

**Command Modes** Boot loader

---

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

---



---

**Usage Guidelines** Use the **mgmt\_init** command only during debugging of the Ethernet management port.

---

**Examples** This example shows how to initialize the Ethernet management port:

```
Device: mgmt_init
```

# mkdir

To create one or more directories on the specified file system, use the **mkdir** command in boot loader mode.

**mkdir** *filesystem:/directory-url...*

<b>Syntax Description</b>	<i>filesystem:</i> Alias for a file system. Use <b>usbflash0:</b> for USB memory sticks.
	<i>/directory-url...</i> Name of the directories to create. Separate each directory name with a space.

<b>Command Default</b>	No default behavior or values.
------------------------	--------------------------------

<b>Command Modes</b>	Boot loader
----------------------	-------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

<b>Usage Guidelines</b>	<p>Directory names are case sensitive.</p> <p>Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.</p>
-------------------------	---

## Example

This example shows how to make a directory called Saved\_Configs:

```
Device: mkdir usbflash0:Saved_Configs
Directory "usbflash0:Saved_Configs" created
```

## more

To display the contents of one or more files, use the **more** command in boot loader mode.

**more** *filesystem:/file-url...*

---

### Syntax Description

*filesystem:* Alias for a file system. Use **flash:** for the system board flash device.

*/file-url...* Path (directory) and name of the files to display. Separate each filename with a space.

---



---

### Command Default

No default behavior or values.

---

### Command Modes

Boot loader

---

### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

---



---

### Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

---

### Examples

This example shows how to display the contents of a file:

```
Device: more flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```



# no debug all

To disable debugging on a switch, use the **no debug all** command in Privileged EXEC mode.

## **no debug all**

---

**Command Default** No default behavior or values.

---

**Command Modes** Privileged EXEC

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 16.1	This command was introduced.

---

---

**Examples** This example shows how to disable debugging on a switch.

```
Device: no debug all
All possible debugging has been turned off.
```

# reload fast

To reload a standalone switch or stacked switch with the software image using Extended Fast Software Upgrade, use the **reload fast** command in privileged EXEC mode.

## reload fast

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.

### Usage Guidelines

The **reload fast** command reloads the standalone switch or stacked switch using Extended Fast Software Upgrade, which reduces traffic downtime to less than 30 seconds depending on the switch configuration.

For a Border Gateway Protocol-configured (BGP-configured) standalone switch, use the **bgp graceful-restart** command to enable Nonstop Forwarding (NSF) awareness before reloading the switch.

For a Border Gateway Protocol-configured (BGP-configured) stacked switch, use the **bgp graceful-restart all** command to enable Nonstop Forwarding (NSF) awareness before reloading the switch.

For an Open Shortest Path First Version 3-configured (OSPFv3-configured) standalone switch, use the **ipv6 nd reachable-time** command to set the timeout limit, and the **snmp ifmib ifindex persist** command to enable Simple Network Management Protocol (SNMP) interface index (ifIndex) persistence globally, and the **interface-id snmp-if-index** command to enable SNMP ifIndex persistence on the interface before reloading the switch.

For an Intermediate System-to-Intermediate System-configured (IS-IS-configured) stacked switch, use either the **nsf cisco** or **nsf ietf** command before reloading the switch.

### Examples

#### Standalone Switch

The following example shows how to reload a standalone switch for a configuration other than BGP or OSPFv3:

```
Device> enable
Device# reload fast
```

The following example shows how to reload a standalone switch for a BGP configuration:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bgp graceful-restart
Device(config-router)# end
Device# write memory
Device# reload fast
```

The following example shows how to reload a standalone switch for an OSPFv3 configuration:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 nd reachable-time 3600000
Device(config)# snmp ifmib ifindex persist
Device(config)# router OSPFv3 1
```

```
Device(config-router)# router-id 192.0.2.5  
Device(config-router)# interface-id snmp-if-index  
Device(config-router)# end  
Device# write memory  
Device# reload fast
```

### Stacked Switch

The following example shows how to reload a stacked switch for a configuration other than BGP or OSPFv3:

```
Device> enable  
Device# reload fast
```

The following example shows how to reload a stacked switch for a BGP configuration:

```
Device> enable  
Device# configure terminal  
Device(config)# router bgp 65000  
Device(config-router)# bgp graceful-restart all  
Device(config-router)# end  
Device# write memory  
Device# reload fast
```

The following example shows how to reload a stacked switch for an IS-IS configuration:

```
Device> enable  
Device# configure terminal  
Device(config)# router isis tag1  
Device(config-router)# nsf cisco  
Device(config-router)# end  
Device# write memory  
Device# reload fast
```

# rename

To rename a file, use the **rename** command in boot loader mode.

```
rename filesystem:/source-file-url filesystem:/destination-file-url
```

Syntax Description	
<i>filesystem:</i>	Alias for a file system. Use <b>usbflash0:</b> for USB memory sticks.
<i>/source-file-url</i>	Original path (directory) and filename.
<i>/destination-file-url</i>	New path (directory) and filename.

**Command Default** No default behavior or values.

**Command Modes** Boot loader

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** Filenames and directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 127 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

## Examples

This example shows a file named *config.text* being renamed to *config1.text*:

```
Device: rename usbflash0:config.text usbflash0:config1.text
```

You can verify that the file was renamed by entering the **dir** *filesystem:* boot loader command.

# request consent-token accept-response shell-access

To submit the Consent Token response to a previously generated challenge, use the **request consent-token accept-response shell-access** command.

**request consent-token accept-response shell-access** *response-string*

## Syntax Description

Syntax	Description
<i>response-string</i>	Specifies the character string representing the response.

**Command Modes** Privileged EXEC mode (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

**Usage Guidelines** You must enter the response string within 30 minutes of challenge generation. If it is not entered, the challenge expires and a new challenge must be requested.

## Example

The following is sample output from the **request consent-token accept-response shell-access** *response-string* command:

```
Device# request consent-token accept-response shell-access
% Consent token authorization success
*Jan 18 02:51:37.807: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (authentication success:
Shell access 0).
```



# request consent-token terminate-auth

To terminate the Consent Token based authorization to system shell, use the **request consent-token terminate-auth** command.

## **request consent-token terminate-auth**

**Command Modes** Privileged EXEC mode (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

**Usage Guidelines** In system shell access scenario, exiting the shell does not terminate authorization until the authorization timeout occurs.

We recommend that you force terminate system shell authorization by explicitly issuing the **request consent-token terminate-auth** command once the purpose of system shell access is complete.

If the current authentication is terminated using the **request consent-token terminate-auth** command, the user will have to repeat the authentication process to gain access to system shell.

### **Example**

The following is sample output from the **request consent-token terminate-auth** command:

```
Device# request consent-token terminate-auth shell-access
% Consent token authorization termination success

Device#
*Mar 13 01:45:39.197: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (terminate authentication:
Shell access 0).
Device#
```

# request platform software console attach switch

To start a session on a member switch, use the **request platform software console attach switch** command in privileged EXEC mode.



**Note** On stacking switches (Catalyst 3650/3850/9200/9300 switches), this command can only be used to start a session on the standby console. On Catalyst 9500 switches, this command is supported only in a stackwise virtual setup. You cannot start a session on member switches. By default, all consoles are already active, so a request to start a session on the active console will result in an error.

**request platform software console attach switch** { *switch-number* | **active** | **standby** } { **0/0** | **R0** }

## Syntax Description

*switch-number* Specifies the switch number. The range is from 1 to 9.

**active** Specifies the active switch.

**Note** This argument is not supported on Catalyst 9500 switches.

**standby** Specifies the standby switch.

**0/0** Specifies that the SPA-Inter-Processor slot is 0, and bay is 0.

**Note** Do not use this option with stacking switches. It will result in an error.

**R0** Specifies that the Route-Processor slot is 0.

## Command Default

By default, all switches in the stack are active.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

## Usage Guidelines

To start a session on the standby switch, you must first enable it in the configuration.

## Examples

This example shows how to session to the standby switch:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device(config-r-mc)# end
```



```
Device# request platform software console attach switch standby R0
#
# Connecting to the IOS console on the route-processor in slot 0.
# Enter Control-C to exit.
#
Device-stby> enable
Device-stby#
```

# reset

To perform a hard reset on the system, use the **reset** command in boot loader mode. A hard reset is similar to power-cycling the device; it clears the processor, registers, and memory.

## reset

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** Boot loader

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

## Examples

This example shows how to reset the system:

```
Device: reset
Are you sure you want to reset the system (y/n)? y
System resetting...
```

# rmdir

To remove one or more empty directories from the specified file system, use the **rmdir** command in boot loader mode.

**rmdir** *filesystem:/directory-url...*

<b>Syntax Description</b>	<p><i>filesystem:</i> Alias for a file system. Use <b>usbflash0:</b> for USB memory sticks.</p> <p><i>/directory-url...</i> Path (directory) and name of the empty directories to remove. Separate each directory name with a space.</p>				
<b>Command Default</b>	No default behavior or values.				
<b>Command Modes</b>	Boot loader				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.5.1a</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.5.1a	This command was introduced.				

**Usage Guidelines**

Directory names are case sensitive and limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Before removing a directory, you must first delete all of the files in the directory.

The device prompts you for confirmation before deleting each directory.

## Example

This example shows how to remove a directory:

```
Device: rmdir usbflash0:Test
```

You can verify that the directory was deleted by entering the **dir** *filesystem:* boot loader command.

# sdm prefer

To specify the SDM template for use on the switch, use the **sdm prefer** command in global configuration mode.

```
sdm prefer
{ access }
```

---

**Syntax Description**      **access** Specifies the SDM access template.

---



---

**Command Default**      No default behavior or values.

---



---

**Command Modes**      Global configuration

---



---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

---



---

**Usage Guidelines**      In a stack, all stack members must use the same SDM template that is stored on the active .

When a new is added to a stack, the SDM configuration that is stored on the active overrides the template configured on an individual .

## Example

This example shows how to configure the access template:

```
Device(config)# sdm prefer access
Device(config)# exit
Device# reload
```

# service private-config-encryption

To enable private configuration file encryption, use the **service private-config-encryption** command. To disable this feature, use the **no** form of this command.

**service private-config-encryption**  
**no service private-config-encryption**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.

## Examples

The following example shows how to enable private configuration file encryption:

```
Device> enable
Device# configure terminal
Device(config)# service private-config-encryption
```

## Related Commands

Command	Description
<b>show parser encrypt file status</b>	Displays the private configuration encryption status.

# set

To set or display environment variables, use the **set** command in boot loader mode. Environment variables can be used to control the boot loader or any other software running on the device.

**set** *variable value*

## Syntax Description

<i>variable</i>	Use one of the following keywords for <i>variable</i> and the appropriate value for <i>value</i> :
<i>value</i>	<p><b>MANUAL_BOOT</b>—Decides whether the device boots automatically or manually.</p> <p>Valid values are 1/Yes and 0/No. If it is set to 0 or No, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the device from the boot loader mode.</p> <hr/> <p><b>BOOT</b> <i>filesystem:/file-url</i>—Identifies a semicolon-separated list of executable files to try to load and execute when automatically booting.</p> <p>If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash: file system.</p> <hr/> <p><b>ENABLE_BREAK</b>—Allows the automatic boot process to be interrupted when the user presses the <b>Break</b> key on the console.</p> <p>Valid values are 1, Yes, On, 0, No, and Off. If set to 1, Yes, or On, you can interrupt the automatic boot process by pressing the <b>Break</b> key on the console after the flash: file system has initialized.</p> <hr/> <p><b>HELPER</b> <i>filesystem:/file-url</i>—Identifies a semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.</p> <hr/> <p><b>PS1</b> <i>prompt</i>—Specifies a string that is used as the command-line prompt in boot loader mode.</p> <hr/> <p><b>CONFIG_FILE</b> <b>flash:</b> <i>/file-url</i>—Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.</p> <hr/> <p><b>BAUD</b> <i>rate</i>—Specifies the number of bits per second (b/s) that is used for the baud rate for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting. The range is from 0 to 128000 b/s. Valid values are 50, 75, 110, 150, 300, 600, 1200, 1800, 2000, 2400, 3600, 4800, 7200, 9600, 14400, 19200, 28800, 38400, 56000, 57600, 115200, and 128000.</p> <p>The most commonly used values are 300, 1200, 2400, 9600, 19200, 57600, and 115200.</p> <hr/> <p><b>SWITCH_NUMBER</b> <i>stack-member-number</i>—Changes the member number of a stack member.</p> <hr/> <p><b>SWITCH_PRIORITY</b> <i>priority-number</i>—Changes the priority value of a stack member.</p>

## Command Default

The environment variables have these default values:

MANUAL\_BOOT: No (0)

BOOT: Null string

ENABLE\_BREAK: No (Off or 0) (the automatic boot process cannot be interrupted by pressing the **Break** key on the console).

HELPER: No default value (helper files are not automatically loaded).

PS1 device:

CONFIG\_FILE: config.text

BAUD: 9600 b/s

SWITCH\_NUMBER: 1

SWITCH\_PRIORITY: 1



**Note** Environment variables that have values are stored in the flash: file system in various files. Each line in the files contains an environment variable name and an equal sign followed by the value of the variable.

A variable has no value if it is not listed in these files; it has a value if it is listed even if the value is a null string. A variable that is set to a null string (for example, “”) is a variable with a value.

Many environment variables are predefined and have default values.

#### Command Modes

Boot loader

#### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

#### Usage Guidelines

Environment variables are case sensitive and must be entered as documented.

Environment variables that have values are stored in flash memory outside of the flash: file system.

Under typical circumstances, it is not necessary to alter the setting of the environment variables.

The MANUAL\_BOOT environment variable can also be set by using the **boot manual** global configuration command.

The BOOT environment variable can also be set by using the **boot system filesystem:/file-url** global configuration command.

The ENABLE\_BREAK environment variable can also be set by using the **boot enable-break** global configuration command.

The HELPER environment variable can also be set by using the **boot helper filesystem: /file-url** global configuration command.

The CONFIG\_FILE environment variable can also be set by using the **boot config-file flash: /file-url** global configuration command.

The SWITCH\_NUMBER environment variable can also be set by using the **switch current-stack-member-number renumber new-stack-member-number** global configuration command.

The SWITCH\_PRIORITY environment variable can also be set by using the device *stack-member-number* **priority** *priority-number* global configuration command.

The boot loader prompt string (PS1) can be up to 120 printable characters not including the equal sign (=).

### Example

This example shows how to set the SWITCH\_PRIORITY environment variable:

```
Device: set SWITCH_PRIORITY 2
```

You can verify your setting by using the **set** boot loader command.



# show avc client

To display information about top number of applications, use the **show avc client** command in privileged EXEC mode.

```
show avc client client-mac top n application [aggregate | upstream | downstream]
```

## Syntax Description

**client** *client-mac* Specifies the client MAC address.

**top n application** Specifies the number of top "N" applications for the given client.

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

### Release Modification

This command was introduced.

The following is sample output from the **show avc client** command:

```
# sh avc client 0040.96ae.65ec top 10 application aggregate
```

Cumulative Stats:

No.	AppName	Packet-Count	Byte-Count	AvgPkt-Size	usage%
1	skinny	7343	449860	61	94
2	unknown	99	13631	137	3
3	dhcp	18	8752	486	2
4	http	18	3264	181	1
5	tftp	9	534	59	0
6	dns	2	224	112	0

Last Interval (90 seconds) Stats:

No.	AppName	Packet-Count	Byte-Count	AvgPkt-Size	usage%
1	skinny	9	540	60	100

## show bootflash:

To display information about the bootflash: file system, use the **show bootflash:** command in user EXEC or privileged EXEC mode.

**show bootflash:** [{all | filesys | namesort | sizesort | timesort }]

Syntax Description	
<b>all</b>	(Optional) Displays all possible Flash information.
<b>filesys</b>	(Optional) Displays Flash system information.
<b>namesort</b>	(Optional) Sorts the output by file name.
<b>sizesort</b>	(Optional) Sorts the output by file size.
<b>timesort</b>	(Optional) Sorts the output by time stamp.

Command Default	
	User EXEC (>)
	Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.
	Cisco IOS XE Amsterdam 17.3.1	The following keywords were introduced: <ul style="list-style-type: none"> <li>• <b>namesort</b></li> <li>• <b>sizesort</b></li> <li>• <b>timesort</b></li> </ul>

### Example:

The following is a sample output from the **show bootflash: all** command:

```
Device# show bootflash: all
-#- --length-- -----date/time----- path
2      4096 May 11 2020 16:49:01.0000000000 +00:00 .installer
3      4096 Feb 27 2020 15:03:50.0000000000 +00:00 .installer/issu_crash
4          12 May 05 2020 22:06:48.0000000000 +00:00 .installer/issu_crash/fru_crash
5          50 May 11 2020 16:40:40.0000000000 +00:00 .installer/last_pkgconf_shasum
6           6 Feb 27 2020 16:33:59.0000000000 +00:00 .installer/install_issu_pid
7          13 Feb 27 2020 21:05:35.0000000000 +00:00 .installer/install_issu_prev_state
8          17 Feb 27 2020 21:05:36.0000000000 +00:00 .installer/install_issu_state
9          13 May 11 2020 16:41:12.0000000000 +00:00 .installer/watchlist
```

```
10      8 Feb 28 2020 18:04:31.0000000000 +00:00 .installer/crdu_frus
11      0 Mar 01 2020 18:01:09.0000000000 +00:00 .installer/.install_add_pkg_list.prev.txt
12     1729 Mar 01 2020 18:02:54.0000000000 +00:00 .installer/install_add_oper.log
13      5 May 11 2020 16:40:40.0000000000 +00:00 .installer/install_global_trans_lock
14     10 May 11 2020 16:40:40.0000000000 +00:00 .installer/install_state
15 33554432 May 11 2020 16:42:37.0000000000 +00:00 nvram_config
16     396 May 11 2020 16:41:02.0000000000 +00:00 boothelper.log
17    4096 May 11 2020 16:40:42.0000000000 +00:00 rpr
18     80 May 11 2020 16:40:42.0000000000 +00:00 rpr/RPR_log.txt
19     80 May 05 2020 22:10:45.0000000000 +00:00 rpr/RPR_log_prev.txt
20    2183 May 11 2020 16:40:42.0000000000 +00:00 bootloader_evt_handle.log
21    4096 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh
22     965 Dec 24 2019 15:23:55.0000000000 +00:00 .ssh/ssh_host_key
23     630 Dec 24 2019 15:23:55.0000000000 +00:00 .ssh/ssh_host_key.pub
24    1675 Dec 24 2019 15:23:56.0000000000 +00:00 .ssh/ssh_host_rsa_key
25     382 Dec 24 2019 15:23:56.0000000000 +00:00 .ssh/ssh_host_rsa_key.pub
26     668 Dec 24 2019 15:23:56.0000000000 +00:00 .ssh/ssh_host_dsa_key
27     590 Dec 24 2019 15:23:56.0000000000 +00:00 .ssh/ssh_host_dsa_key.pub
28     492 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh/ssh_host_ecdsa_key
29     162 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh/ssh_host_ecdsa_key.pub
30     387 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh/ssh_host_ed25519_key
31     82 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh/ssh_host_ed25519_key.pub
32    4096 Dec 24 2019 15:24:41.0000000000 +00:00 core
33    4096 May 11 2020 16:41:29.0000000000 +00:00 core/modules
34    4096 May 05 2020 22:11:47.0000000000 +00:00 .prst_sync
35    4096 Mar 01 2020 18:17:15.0000000000 +00:00 .rollback_timer
36    4096 Mar 06 2020 21:01:11.0000000000 +00:00 gs_script
37    4096 Mar 06 2020 21:01:11.0000000000 +00:00 gs_script/sss
38    4096 Apr 24 2020 18:56:40.0000000000 +00:00 tech_support
39 15305 May 11 2020 16:41:01.0000000000 +00:00 tech_support/igmp-snooping.tcl
40    1612 May 11 2020 16:41:01.0000000000 +00:00 tech_support/igmpsn_dump.tcl
.
```

## show bootflash:

.

.

The following is a sample output from the **show bootflash: sizesort** command:

Device# **show bootflash: sizesort**

```

-#- --length-- -----date/time----- path
126 968337890 Mar 27 2020 18:06:17.0000000000 +00:00 cat9k_iosxe.CSCvt37598.bin
136 967769293 May 05 2020 21:50:33.0000000000 +00:00 cat9k_iosxe.CSCvu05574
124 967321806 Mar 23 2020 18:48:45.0000000000 +00:00 cat9k_ts_2103.bin
133 951680494 Apr 13 2020 19:46:35.0000000000 +00:00
cat9k_iosxe.2020-04-13_17.34_rakoppak.SSA.bin
130 950434163 Apr 09 2020 09:03:47.0000000000 +00:00
cat9k_iosxe.2020-04-09_13.49_rakoppak.SSA.bin
132 950410332 Apr 09 2020 07:29:57.0000000000 +00:00
cat9k_iosxe.2020-04-09_12.28_rakoppak.SSA.bin
134 948402972 Apr 17 2020 23:02:04.0000000000 +00:00 cat9k_iosxe.tla.bin
77 810146146 Feb 27 2020 15:41:42.0000000000 +00:00 cat9k_iosxe.16.12.01c.SPA.bin
88 701945494 Feb 27 2020 16:23:55.0000000000 +00:00 cat9k_iosxe.16.09.03.SPA.bin
101 535442436 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-rpbase.16.12.01c.SPA.pkg
86 88884228 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-espbase.16.12.01c.SPA.pkg
104 60167172 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-sipspa.16.12.01c.SPA.pkg
102 43111770 Mar 01 2020 18:02:07.0000000000 +00:00 cat9k-rpboot.16.12.01c.SPA.pkg
15 33554432 May 11 2020 16:42:37.0000000000 +00:00 nvram_config
131 33554432 May 11 2020 16:42:39.0000000000 +00:00 nvram_config_bkup
103 31413252 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-sipbase.16.12.01c.SPA.pkg
105 22676484 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-srdriver.16.12.01c.SPA.pkg
85 14226440 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-cc_srdriver.16.12.01c.SPA.pkg
.
.
.

```

# show cable-diagnostics tdr

To display the Time Domain Reflector (TDR) results, use the **show cable-diagnostics tdr** command in privileged EXEC mode.

```
show cable-diagnostics tdr interface interface-id
```

## Syntax Description

*interface-id* Specifies the interface on which TDR is run.

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

## Usage Guidelines

TDR is supported only on 10/100/100 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports and small form-factor pluggable (SFP) module ports.

## Examples

This example shows the output from the **show cable-diagnostics tdr interface *interface-id*** command on a device:

```
Device# show cable-diagnostics tdr interface gigabitethernet1/0/23
TDR test last run on: March 01 00:04:08
Interface  Speed  Local pair  Pair length          Remote pair  Pair status
-----
Gi1/0/23  1000M  Pair A     1 +/- 1 meters      Pair A      Normal
           Pair B     1 +/- 1 meters      Pair B      Normal
           Pair C     1 +/- 1 meters      Pair C      Normal
           Pair D     1 +/- 1 meters      Pair D      Normal
```

**Table 2: Field Descriptions for the show cable-diagnostics tdr Command Output**

Field	Description
Interface	The interface on which TDR is run.
Speed	The speed of connection.
Local pair	The name of the pair of wires that TDR is testing on the local interface.

Field	Description
Pair length	The location of the problem on the cable, with respect to your device. TDR can only find the location in one of these cases: <ul style="list-style-type: none"> <li>• The cable is properly connected, the link is up, and the interface speed is 1000 Mb/s.</li> <li>• The cable is open.</li> <li>• The cable has a short.</li> </ul>
Remote pair	The name of the pair of wires to which the local pair is connected. TDR can learn about the remote pair only when the cable is properly connected and the link is up.
Pair status	The status of the pair of wires on which TDR is running: <ul style="list-style-type: none"> <li>• Normal—The pair of wires is properly connected.</li> <li>• Not completed—The test is running and is not completed.</li> <li>• Not supported—The interface does not support TDR.</li> <li>• Open—The pair of wires is open.</li> <li>• Shorted—The pair of wires is shorted.</li> <li>• ImpedanceMis—The impedance is mismatched.</li> <li>• Short/Impedance Mismatched—The impedance mismatched or the cable is short.</li> <li>• InProgress—The diagnostic test is in progress.</li> </ul>

This example shows the output from the **show interface** *interface-id* command when TDR is running:

```
Device# show interface gigabitethernet1/0/2
gigabitethernet1/0/2 is up, line protocol is up (connected: TDR in Progress)
```

This example shows the output from the **show cable-diagnostics tdr interface** *interface-id* command when TDR is not running:

```
# show cable-diagnostics tdr interface gigabitethernet1/0/2
% TDR test was never issued on gigabitethernet1/0/2
```

If an interface does not support TDR, this message appears:

```
% TDR test is not supported on device 1
```

## show consistency-checker mcast

To run a consistency-checker and detect inconsistent states of software entries on Layer 2 multicast forwarding tables and Layer 3 multicast forwarding tables, run the **show consistency-checker mcast** command in privileged EXEC mode.

```
show consistency-checker mcast { l2m | l3m } start { all | vlan vlan-id { ipv4-address |
ipv6-address } } [{ recursive }]
```

Syntax Description		
<b>l2m</b>		Layer 2 multicast forwarding tables are selected to run a consistency-checker.
<b>l3m</b>		Layer 3 multicast forwarding tables are selected to run a consistency-checker.
<b>start</b>		Starts the consistency-checker for Layer 2 multicast. <ul style="list-style-type: none"> <li>• <b>all</b> : Starts the checker for entire table</li> <li>• <b>vlan vlan-id { ipv4-address   ipv6-address }</b>: Starts the checker for the specified VLAN.</li> </ul>
<b>all</b>		Starts the checker for entire table.
<b>vlan vlan-id { ipv4-address   ipv6-address }</b>		Starts the checker for the specified VLAN.
<b>recursive</b>		Runs a recursive consistency-checker.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Bengaluru 17.6.1	This command was introduced.
	Cisco IOS XE Cupertino 17.7.1	The keyword <b>l3m</b> was introduced to run consistency checker on Layer 3 multicast forwarding tables.

**Usage Guidelines** The consistency checker has the following limitations:

- There is no command to abort or terminate the consistency checker. It will stop only once the full report has been displayed.
- FED hardware checks are partially implemented. Only errors in programming hardware will be reported.
- False Positive cases: When the consistency checker is running and a large number of feature table entry delete/add/modify actions occur (triggered via clear \* or relearn), the consistency checker may report inconsistent or missing entries across processes. It can also switch off the stale reporting due to a large number of changes in table entries.

**Example**

The following is a sample output for the **show consistency-checker mcast l2m** command:

```
Device# show consistency-checker mcast l2m start vlan 900 229.1.1.1 recursive
Single entry scan started with Run_id: 2

*Feb 17 06:54:09.880: %IOSXE_FMANRP_CCK-6-FMANRP_COMPLETED: Consistency Check for Run-Id 2
is completed. Check 'show consistency-checker run-id 2'.
Device#
Device# show consistency-checker run 2
Process: IOSD
  Object-Type   Start-time           Entries   Exceptions
  l2m_vlan      2021/02/17 06:54:01     1         0
  l2m_group     2021/02/17 06:54:01     1         0

Process: FMAN-FP
  *Statistics(A/I/M/S/O): Actual/Inherited/Missing/Stale/Others

  Object-Type   Start-time           State      A / I / M / S / O
  l2m_vlan      1970/01/01 00:10:03   Consistent  0/ 0/ 0/ 0/ 0
  l2m_group     1970/01/01 00:10:03   Consistent  0/ 0/ 0/ 0/ 0

Process: FED
  *Statistics(A/I/M/S/HW/O): Actual/Inherited/Missing/Stale/Hardware/Others

  Object-Type   Start-time           State      A / I / M / S / HW/ O
  l2m_vlan      2021/02/17 06:54:01   Inconsistent  1/ 0/ 0/ 0/ 0/ 0
  l2m_group     2021/02/17 06:54:01   Inconsistent  0/ 1/ 0/ 0/ 0/ 0

Device#
```

The following is a sample output for the **show consistency-checker mcast l3m** command:

```
Device# show consistency-checker mcast l2m start vlan 900 229.1.1.1 recursive
Single entry scan started with Run_id: 2

*Feb 17 06:54:09.880: %IOSXE_FMANRP_CCK-6-FMANRP_COMPLETED: Consistency Check for Run-Id 2
is completed. Check 'show consistency-checker run-id 2'.
Device#
Device# show consistency-checker run 2
Process: IOSD
  Object-Type   Start-time           Entries   Exceptions
  l2m_vlan      2021/02/17 06:54:01     1         0
  l2m_group     2021/02/17 06:54:01     1         0

Process: FMAN-FP
  *Statistics(A/I/M/S/O): Actual/Inherited/Missing/Stale/Others

  Object-Type   Start-time           State      A / I / M / S / O
  l2m_vlan      1970/01/01 00:10:03   Consistent  0/ 0/ 0/ 0/ 0
  l2m_group     1970/01/01 00:10:03   Consistent  0/ 0/ 0/ 0/ 0

Process: FED
  *Statistics(A/I/M/S/HW/O): Actual/Inherited/Missing/Stale/Hardware/Others

  Object-Type   Start-time           State      A / I / M / S / HW/ O
  l2m_vlan      2021/02/17 06:54:01   Inconsistent  1/ 0/ 0/ 0/ 0/ 0
  l2m_group     2021/02/17 06:54:01   Inconsistent  0/ 1/ 0/ 0/ 0/ 0

Device#
```



## show consistency-checker mcast l3m

To run a consistency-checker and detect inconsistent states of software entries on the Layer 3 multicast forwarding tables, run the **show consistency-checker mcast l3m** command in privileged EXEC mode.

```
show consistency-checker mcast l3m start { all | vrf vrf-name { ipv4-address | ipv6-address } }
[ { recursive } ]
```

Syntax Description	start	Starts the consistency-checker for Layer 3 multicast.
		<ul style="list-style-type: none"> <li>• <b>all</b> : Starts the checker for entire table</li> <li>• <b>vrf vrf-name { ipv4-address   ipv6-address }</b> : Starts the checker for the specified VRF.</li> </ul>
	<b>all</b>	Starts the checker for entire table.
	<b>vrf vrf-name { ipv4-address   ipv6-address }</b>	Starts the checker for the specified VRF.
	<b>recursive</b>	Runs a recursive consistency-checker.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Cupertino 17.7.1	This command was introduced.

**Usage Guidelines** The consistency checker has the following limitations:

- There is no command to abort or terminate the consistency checker. It will stop only once the full report has been displayed.
- FED hardware checks are partially implemented. Only errors in programming hardware will be reported.
- False Positive cases: When the consistency checker is running and a large number of feature table entry delete/add/modify actions occur (triggered via clear \* or relearn), the consistency checker may report inconsistent or missing entries across processes. It can also switch off the stale reporting due to a large number of changes in table entries.

You can run an end to end consistency checker using the **show diagnostic content switch all** command for Layer 2 multicast and Layer 3 multicast.

### Example

The following is a sample output for the **show consistency-checker mcast l3m start all** command:

## show consistency-checker mcast l3m

```

Device# show consistency-checker mcast l3m start all
L3 multicast Full scan started. Run_id: 1
Use 'show consistency-checker run-id 1 status' for completion status.

SF-2043#
*Apr  2 17:30:01.831: %IOSXE_FMANRP_CCK-6-FMANRP_COMPLETED: Consistency Check for Run-Id 1
  is completed. Check 'show consistency-checker run-id 1'.
SF-2043#
SF-2043#
SF-2043#
SF-2043#
SF-2043#
SF-2043#sh consi
SF-2043#sh consistency-checker
SF-2043#sh consistency-checker run-id 1
Process: IOSD
Flags:      F - Full Table Scan, S - Single Entry Run
           RE - Recursive Check, GD - Garbage Detector
           Hw - Hardware Check, HS - Hardware Shadow Copy
Object-Type  Start-time                Entries  Exceptions  Flags
l3m_entry    2021/04/02 17:29:35                8        0          F GD Hw HS

Process: FMAN-FP
*Statistics(A/I/M/S/Oth): Actual/Inherited/Missing/Stale/Others

Object-Type  Start-time                State          A/  I/  M/  S/Oth
l3m_entry    2021/04/02 17:29:35      Consistent    0/  0/  0/  0/  0

Process: FED
*Statistics(A/I/M/S/HW/Oth): Actual/Inherited/Missing/Stale/Hardware/Others

Object-Type  Start-time                State          A/  I/  M/  S/ HW/Oth
l3m_entry    2021/04/02 17:29:35      Consistent    0/  0/  0/  0/  0/  0

```

The following is a sample output for the **show consistency-checker mcast l3m** command running a recursive consistency checker:

```

Device# sh consistency-checker mcast l3m start 225.1.1.1 recursive
Single entry scan started with Run_id: 2
Use 'show consistency-checker run-id 2 status' for completion status.

Device#show consistency-checker run-id 2 detail
Process: IOSD
Object-Type:l2m_vlan  Start-time:2021/03/31 15:22:44
  Key/data                Reason
  (Ipv4, vlan:100)        Success
  snoop:on stp_tcn:off flood:off pimsn:off

Object-Type:l2m_group  Start-time:2021/03/31 15:22:44
  Key/data                Reason
  (Ipv4, vlan:100, (*,225.1.1.1))  Success
  Fo1/0/3

Object-Type:l3m_entry  Start-time:2021/03/31 15:22:44
  Key/data                Reason
  (Ipv4, (*,225.1.1.1))  Success
  Entry flags: C
  Total entries: 1
  Obj_id: F80004A1 Flags:  F

Process: FMAN-FP
Object-Type:l3m_entry  Start-time:2021/03/31 15:22:44
Status:Completed      State:Inconsistent
  Key/data                Reason

```

```

      (Ipv4, vrf:0, ((*,225.1.1.1)))          Inherited
      Entry Flags: C
      Total entries: 1
      Obj_id: f80004a1 Flags:  F
-----Recursion-level-1-----
Object-Type:l2m_group  Start-time:2021/03/31 15:22:44
Status:Completed  State:Inconsistent
Key/data          Reason
(Ipv4, vlan:100, ((*,225.1.1.1)))          Inherited
      Group ports: total entries: 1
      FortyGigabitEthernet1/0/3
-----Recursion-level-2-----
Object-Type:l2m_vlan  Start-time:2021/03/31 15:22:44
Status:Completed  State:Inconsistent
Key/data          Reason
(Ipv4, vlan:100)          Inconsistent
      snoop:on stp_tcn:off flood:off pimsn:off

Process: FED
      Object-Type:l3m_entry  Start-time:2021/03/31 15:22:44
      Status:Completed  State:Inconsistent
      Key/data          Reason
      (Ipv4, vrf:0 (*,225.1.1.1))          Inherited
      Entry Flags: C
      Total entries: 1
      Obj_id: f80004a1 Flags:  F
-----Recursion-level-1-----
Object-Type:l2m_group  Start-time:2021/03/31 15:22:44
Status:Completed  State:Inconsistent
      Key/data          Reason
      (Ipv4, vlan:100 (*,225.1.1.1))          Inherited
      Group ports: total entries: 1
      FortyGigabitEthernet1/0/3
-----Recursion-level-2-----
Object-Type:l2m_vlan  Start-time:2021/03/31 15:22:44
Status:Completed  State:Inconsistent
      Key/data          Reason
      (Ipv4, vlan: 100)          Inconsistent
      snoop:on stp_tcn:off flood:off pimsn:off

```

The following is a sample output for the **show consistency-checker mcast l3m** command for a specified VRF:

```

Device#show consistency-checker mcast l3m start vrf vrf3001 229.1.1.1
Single entry scan started with Run_id: 5
Use 'show consistency-checker run-id 5 status' for completion status.

Stark#
*May 26 13:21:18.689: %IOSXE_FMANRP_CCK-6-FMANRP_COMPLETED: Consistency Check for Run-Id 5
is completed. Check 'show consistency-checker run-id 5'.
Stark#
Stark#
Stark#
Stark#sh consistency-checker run-id 5 detail
Process: IOSD
      Object-Type:l3m_entry  Start-time:2021/05/26 13:21:07
      Key/data          Reason
      (Ipv4, vrf:vrf3001, (*,229.1.1.1))          Success
      Entry flags: C
      Total entries: 2
      Obj_id: 4D Obj_flags: A
      Obj_id: F80004B1 Obj_flags: F

```

## show consistency-checker mcast l3m

```

Process: FMAN-FP
Object-Type:l3m_entry Start-time:2021/05/26 13:21:07
Status:Completed State:Inconsistent
Key/data Reason
(Ipv4, vrf:4, ((*,229.1.1.1))) Inconsistent
Entry Flags: C
Total entries: 2
Obj_id: 6e Obj_flags: A
Obj_id: f80004b1 Obj_flags: F

```

```

Process: FED
Object-Type:l3m_entry Start-time:2021/05/26 13:21:07
Status:Completed State:Inconsistent
Key/data Reason
(Ipv4, vrf:4 (*,229.1.1.1)) Inconsistent
Entry Flags: C
Total entries: 2
Obj_id: 6e Obj_flags: A
Obj_id: f80004b1 Obj_flags: F

```

The following is a sample output for the **show diagnostic content switch all** command:

```

Device#show diagnostic content switch all
switch 2 module 1:

```

```

Diagnostics test suite attributes:
M/C/* - Minimal bootup level test / Complete bootup level test / NA
B/* - Basic ondemand test / NA
P/V/* - Per port test / Per device test / NA
D/N/* - Disruptive test / Non-disruptive test / NA
S/* - Only applicable to standby unit / NA
X/* - Not a health monitoring test / NA
F/* - Fixed monitoring interval test / NA
E/* - Always enabled monitoring test / NA
A/I - Monitoring is active / Monitoring is inactive

```

ID	Test Name	Attributes	Test Interval day hh:mm:ss.ms	Thre- shold
1)	TestGoldPktLoopback	*BPN*X**I	not configured	n/a
2)	TestOBFL	*B*N*X**I	not configured	n/a
3)	TestFantray	*B*N****A	000 00:01:40.00	1
4)	TestPhyLoopback	*BPD*X**I	not configured	n/a
5)	TestThermal	*B*N****A	000 00:01:30.00	1
6)	TestScratchRegister	*B*N****A	000 00:01:30.00	5
7)	TestPortTxMonitoring	*BPN****A	000 00:02:30.00	1
8)	TestConsistencyCheckL2	*B*N****A	000 00:01:30.00	1
9)	TestConsistencyCheckL3	*B*N****A	000 00:01:30.00	1
10)	TestConsistencyCheckMcast	*B*N****A	000 00:01:30.00	1
11)	TestConsistencyCheckL2m	*B*N****A	000 00:01:30.00	1
12)	TestConsistencyCheckL3m	*B*N****A	000 00:01:30.00	1 □

This gives the status of consistency check for multicast

# show consistency-checker objects

To run a consistency-checker and detect inconsistent states of software entries on objects, run the **show consistency-checker objects** command in privileged EXEC mode.

```
show consistency-checker objects { adjacency | interface | l2m_group | l2m_vlan | l3_entry | l3m_entry } [{ run-id }] [{ detail }]
```

## Syntax Description

<b>adjacency</b>	Runs the consistenc-checker on adjacency entries.
<b>interface</b>	Runs the consistenc-checker on interface entries.
<b>l2m_group</b>	Runs the consistenc-checker on Layer 2 Multicast group entries.
<b>l2m_vlan</b>	Runs the consistenc-checker on Layer 2 Multicast VLAN entries.
<b>l3_entry</b>	Runs the consistenc-checker on Layer 3 Unicast entries.
<b>l3m_entry</b>	Runs the consistenc-checker on Layer 3 Multicast entries.
<i>run-id</i>	Runs the consistency-checker by run ID.
<b>detail</b>	Displays detailed output for the run ID.

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

## Usage Guidelines

The consistency checker has the following limitations:

- There is no command to abort or terminate the consistency checker. It will stop only once the full report has been displayed.
- FED hardware checks are partially implemented. Only errors in programming hardware will be reported.
- False Positive cases: When the consistency checker is running and a large number of feature table entry delete/add/modify actions occur (triggered via clear \* or relearn), the consistency checker may report inconsistent or missing entries across processes. It can also switch off the stale reporting due to a large number of changes in table entries.

## Example

The following is sample output for the **show consistency-checker objects l2m\_group** command:

```
Device# show consistency-checker objects l2m_group
Process: IOSD
```

## show consistency-checker objects

Run-id	Start-time	Exception
1	2021/02/17 05:20:42	0
2	2021/02/17 06:19:05	0

Process: FMAN-FP

\*Statistics(A/I/M/S/Oth): Actual/Inherited/Missing/Stale/Others

Run-id	Start-time	State	A/	I/	M/	S/Oth
1	2021/02/17 05:20:42	Consistent	0/	0/	0/	0/ 0
2	2021/02/17 06:19:05	Consistent	0/	0/	0/	0/ 0

Process: FED

\*Statistics(A/I/M/S/HW/Oth): Actual/Inherited/Missing/Stale/Hardware/Others

Run-id	Start-time	State	A/	I/	M/	S/	HW/Oth
1	2021/02/17 05:20:42	Consistent	0/	0/	0/	0/	0/ 0
2	2021/02/17 06:19:05	Inconsistent	4/	0/	2/	0/	0/ 0

Device#

# show consistency-checker run-id

To run a consistency-checker and detect inconsistent states of software entries by run ID, run the **show consistency-checker run-id** *run-id* command in privileged EXEC mode.

```
show consistency-checker run-id run-id [{ detail | | status }]
```

Syntax Description	
<i>run-id</i>	Specifies the run ID.
<b>detail</b>	Displays detailed output for the run ID.
<b>status</b>	Displays the completion status of the checker.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

**Usage Guidelines** The consistency checker has the following limitations:

- There is no command to abort or terminate the consistency checker. It will stop only once the full report has been displayed.
- FED hardware checks are partially implemented. Only errors in programming hardware will be reported.
- False Positive cases: When the consistency checker is running and a large number of feature table entry delete/add/modify actions occur (triggered via clear \* or relearn), the consistency checker may report inconsistent or missing entries across processes. It can also switch off the stale reporting due to a large number of changes in table entries.

## Example

The following is sample output for the **show consistency-checker run-id** *run-id* command:

```
Device# show consistency-checker run-id 6
Process: IOSD
Flags:    F - Full Table Scan, S - Single Entry Run
          RE - Recursive Check, GD - Garbage Detector
          Hw - Hardware Check, HS - Hardware Shadow Copy
Object-Type  Start-time           Entries  Exceptions  Flags
l2m_vlan    2021/07/19 15:19:41      30       0      F Hw HS
l2m_group   2021/07/19 15:19:42      10       0      F Hw HS

Process: FMAN-FP
*Statistics (A/I/M/S/Oth): Actual/Inherited/Missing/Stale/Others

Object-Type  Start-time           State           A/  I/  M/  S/Oth
l2m_vlan    2021/07/19 15:19:41  Consistent     0/  0/  0/  0/  0
l2m_group   2021/07/19 15:19:42  Consistent     0/  0/  0/  0/  0
```

## show consistency-checker run-id

```

Process: FED
*Statistics (A/I/M/S/HW/Oth): Actual/Inherited/Missing/Stale/Hardware/Others

Object-Type      Start-time          State                A/  I/  M/  S/ HW/Oth
l2m_vlan         2021/07/19 15:19:41 Consistent           0/  0/  0/  0/  0
l2m_group        2021/07/19 15:19:42 Consistent           0/  0/  0/  0/  0

```

Device#

The following is sample output for the **show consistency-checker run-id run-id status** command:

```

Device# show consistency-checker run-id 6 status
Process: IOSD
Object-Type      Status              Time(sec)            Exceptions
l2m_vlan         Completed           13                   No
l2m_group        Completed           13                   No

Process: FMAN-FP
Object-Type      Status              Time(sec)            State
l2m_vlan         Completed           12                   Consistent
l2m_group        Completed           11                   Consistent

Process: FED
Object-Type      Status              Time(sec)            State
l2m_vlan         Completed           12                   Consistent
l2m_group        Completed           11                   Consistent

Device#

```



# show debug

To display all the debug commands available on a switch, use the **show debug** command in Privileged EXEC mode.

**show debug**

**show debug condition** *Condition identifier* / *All conditions*

<b>Syntax Description</b>	<i>Condition identifier</i>	Sets the value of the condition identifier to be used. Range is between 1 and 1000.
	<i>All conditions</i>	Shows all conditional debugging options available.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 16.1	This command was introduced.

**Usage Guidelines** Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

**Examples** This example shows the output of a **show debug** command:

```
Device# show debug condition all
```

To disable debugging, use the **no debug all** command.

# show env

To display fan, temperature, and power information for the switch (standalone switch, stack's active switch, or stack member), use the **show env** command in EXEC modes.

```
show env { all | fan | power [all | switch [switch-number]] | stack [stack-number] |
temperature [status] }
```

Syntax Description		
<b>all</b>		Displays fan, temperature and power environmental status.
<b>fan</b>		Displays the switch fan status.
<b>power</b>		Displays the power supply status.
<b>all</b>		(Optional) Displays the status for all power supplies.
<b>switch</b> <i>switch-number</i>		(Optional) Displays the power supply status for a specific switch.
<b>stack</b> <i>switch-number</i>		(Optional) Displays all environmental status for each switch in the stack or for a specified switch. The range is 1 to 9, depending on the switch member numbers in the stack.
<b>temperature</b>		Displays the switch temperature status.
<b>status</b>		(Optional) Displays the temperature status and threshold values.

**Command Default** No default behavior or values.

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** Use the **show env stack** [*switch-number*] command to display information about any switch in the stack from any member switch.

Use the **show env temperature status** command to display the switch temperature states and threshold levels.

## Examples

This example shows how to display information about stack member 1 from the active switch:

```
Device> show env stack 1
Device 1:
Device Fan 1 is OK
Device Fan 2 is OK
Device Fan 3 is OK
FAN-PS1 is OK
```

```
FAN-PS2 is NOT PRESENT
Device 1: SYSTEM TEMPERATURE is OK
Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold : 56 Degree Celsius
```

```
Device>
```

This example shows how to display temperature value, state, and threshold values:

```
Device> show env temperature status
Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold : 56 Degree Celsius
```

```
Device>
```

**Table 3: States in the show env temperature status Command Output**

State	Description
Green	The switch temperature is in the <i>normal</i> operating range.
Yellow	The temperature is in the <i>warning</i> range. You should check the external temperature around the switch.
Red	The temperature is in the <i>critical</i> range. The switch might not run properly if the temperature is in this range.

## show env xps

To display budgeting, configuration, power, and system power information for the Cisco eXpandable Power System (XPS) 2200, use the **show env xps** command in privileged EXEC mode.

```
show env xps { budgeting | configuration | port [ all | number ] | power | system |
thermal | upgrade | version }
```

### Syntax Description

<b>budgeting</b>	Displays XPS power budgeting, the allocated and budgeted power of all switches in the power stack.
<b>configuration</b>	Displays the configuration resulting from the power xps privileged EXEC commands. The XPS configuration is stored in the XPS. Enter the show env xps configuration command to retrieve the non-default configuration.
<b>port</b> [ all   number ]	Displays the configuration and status of all ports or the specified XPS port. Port numbers are from 1 to 9.
<b>power</b>	Displays the status of the XPS power supplies.
<b>system</b>	Displays the XPS system status.
<b>thermal</b>	Displays the XPS thermal status.
<b>upgrade</b>	Displays the XPS upgrade status.
<b>version</b>	Displays the XPS version details.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.2(55)SE1	This command was introduced.

### Usage Guidelines

Use the **show env xps** privileged EXEC command to display the information for XPS 2200.

### Examples

This is an example of output from the show env xps budgeting command:

```
Switch#
=====

XPS 0101.0100.0000 :
=====
Data          Current   Power    Power Port  Switch #  PS A  PS B  Role-State
Committed
Budget
-----
223          1543
----- 1 - - 715 SP-PS
```

```

2    -    -    -    SP-PS    223    223
3    -    -    -    -        -        -
4    -    -    -    -        -        -
5    -    -    -    -        -        -
6    -    -    -    -        -        -
7    -    -    -    -        -        -
8    -    -    -    -        -        -
9    1    -    1100 -    RPS-NB    223    070
XPS  -    -    1100 -    -        -        -

```

This is an example of output from the show env xps configuration command:

```

Switch# show env xps configuration
=====
XPS 0101.0100.0000 :
=====
power xps port 4 priority 5
power xps port 5 mode disable
power xps port 5 priority 6
power xps port 6 priority 7
power xps port 7 priority 8
power xps port 8 priority 9
power xps port 9 priority 4

```

This is an example of output from the show env xps port all command:

```

Switch#
XPS 010

-----
Port name      : -
Connected      : Yes
Mode           : Enabled (On)
Priority       : 1
Data stack switch # : - Configured role      : Auto-SP
Run mode       : SP-PS : Stack Power Power-Sharing Mode
Cable faults   : 0x0 XPS 0101.0100.0000 Port 2
-----
Port name      : -
Connected      : Yes
Mode           : Enabled (On)
Priority       : 2
Data stack switch # : - Configured role      : Auto-SP
Run mode       : SP-PS : Stack Power Power-Sharing Mode
Cable faults   : 0x0 XPS 0101.0100.0000 Port 3
-----
Port name      : -
Connected      : No
Mode           : Enabled (On)
Priority       : 3
Data stack switch # : - Configured role      : Auto-SP Run mode           : -
Cable faults   :
<output truncated>

```

This is an example of output from the show env xps power command:

```

=====
XPS 0101.0100.0000 :
=====
Port-Supply SW PID                               Serial#      Status      Mode Watts
-----
XPS-A          Not present
XPS-B          NG3K-PWR-1100WAC  LIT13320NTV OK          SP   1100
1-A           - -

```

## show env xps

```

1-B      - -      -      -      SP      715
2-A      - -      -      -
2-B      - -      -      -
9-A      - -      100WAC  LIT141307RK OK      RPS  1100
9-B      - -      esent

```

This is an example of output from the show env xps system command:

```
Switch#
=====
```

```
XPS 0101.0100.0000 :
```

```

=====
XPS          Cfg Cfg      RPS Switch  Current  Data Port  XPS Port Name
Mode Role    Pri Conn  Role-State  Switch #
-----
1      -          On  Auto-SP  1  Yes      SP-PS      -
2      -          On  Auto-SP  2  Yes      SP-PS      -
3      -          On  Auto-SP  3  No       -          -
4      none       On  Auto-SP  5  No       -          -
5      -          Off Auto-SP  6  No       -          -
6      -          On  Auto-SP  7  No       -          -
7      -          On  Auto-SP  8  No       -          -
8      -          On  Auto-SP  9  No       -          -
9      test       On  Auto-SP  4  Yes      RPS-NB

```

This is an example of output from the show env xps thermal command:

```
Switch#
=====
```

```
XPS 0101.0100.0000 :
```

```

=====
Fan  Status
----
1      OK
2      OK
3      NOT PRESENT PS-1  NOT PRESENT PS-2  OK Temperature is OK

```

This is an example of output from the show env xps upgrade command when no upgrade is occurring:

```
Switch# show env xps upgrade
No XPS is connected and upgrading.
```

These are examples of output from the show env xps upgrade command when an upgrade is in process:

```
Switch# show env xps upgrade
XPS Upgrade Xfer

SW Status Prog
--
1 Waiting 0%
Switch#
*Mar 22 03:12:46.723: %PLATFORM_XPS-6-UPGRADE_START: XPS 0022.bdd7.9b14 upgrade has
started through the Service Port.
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
--
1 Receiving 1%
Switch# show env xps upgrade
```

```

XPS Upgrade Xfer
SW Status Prog
-- -----
1 Receiving 5%
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- -----
1 Reloading 100%
Switch#
*Mar 22 03:16:01.733: %PLATFORM_XPS-6-UPGRADE_DONE: XPS 0022.bdd7.9b14 upgrade has
completed and the XPS is reloading.

```

This is an example of output from the show env xps version command:

```

Switch# show env xps version
=====
XPS 0022.bdd7.9b14:
=====
Serial Number: FDO13490KUT
Hardware Version: 8
Bootloader Version: 7
Software Version: 18

```

**Table 4: Related Commands**

Command	Description
power xps(global configuration command)	Configures XPS and XPS port names.
power xps(privileged EXEC command)	Configures the XPS ports and system.

# show flow monitor

To display the status and statistics for a flow monitor, use the **show flow monitor** command in privileged EXEC mode.

Syntax Description	name	(Optional) Specifies the name of a flow monitor.
	<i>monitor-name</i>	(Optional) Name of a flow monitor that was previously configured.
	<b>cache</b>	(Optional) Displays the contents of the cache for the flow monitor.
	<b>format</b>	(Optional) Specifies the use of one of the format options for formatting the display output.
	<b>csv</b>	(Optional) Displays the flow monitor cache contents in comma-separated variables (CSV) format.
	<b>record</b>	(Optional) Displays the flow monitor cache contents in record format.
	<b>table</b>	(Optional) Displays the flow monitor cache contents in table format.
	<b>statistics</b>	(Optional) Displays the statistics for the flow monitor.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** The **cache** keyword uses the record format by default.

The uppercase field names in the display output of the **show flowmonitor** *monitor-name* **cache** command are key fields that uses to differentiate flows. The lowercase field names in the display output of the **show flow monitor** *monitor-name* **cache** command are nonkey fields from which collects values as additional data for the cache.

## Examples

The following example displays the status for a flow monitor:

```
# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:      Used for basic traffic analysis
  Flow Record:     flow-record-1
  Flow Exporter:   flow-exporter-1
                  flow-exporter-2

Cache:
  Type:            normal
  Status:          allocated
  Size:            4096 entries / 311316 bytes
  Inactive Timeout: 15 secs
  Active Timeout:  1800 secs
```

This table describes the significant fields shown in the display.



**Table 5: show flow monitor monitor-name Field Descriptions**

Field	Description
Flow Monitor	Name of the flow monitor that you configured.
Description	Description that you configured or the monitor, or the default description User defined.
Flow Record	Flow record assigned to the flow monitor.
Flow Exporter	Exporters that are assigned to the flow monitor.
Cache	Information about the cache for the flow monitor.
Type	Flow monitor cache type. The value is always normal, as it is the only supported cache type.
Status	Status of the flow monitor cache. The possible values are: <ul style="list-style-type: none"> <li>• allocated—The cache is allocated.</li> <li>• being deleted—The cache is being deleted.</li> <li>• not allocated—The cache is not allocated.</li> </ul>
Size	Current cache size.
Inactive Timeout	Current value for the inactive timeout in seconds.
Active Timeout	Current value for the active timeout in seconds.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1:

This table describes the significant fields shown in the display.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1 in a table format:

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-IPv6 (the cache contains IPv6 data) in record format:

The following example displays the status and statistics for a flow monitor:

# show install

To display information about install packages, use the **show install** command in privileged EXEC mode.

**show install** {**active** | **committed** | **inactive** | **log** | **package** {**bootflash:** | **flash:** | **webui:**} | **rollback** | **summary** | **uncommitted**}

Syntax Description		
<b>active</b>		Displays information about active packages.
<b>committed</b>		Displays package activations that are persistent.
<b>inactive</b>		Displays inactive packages.
<b>log</b>		Displays entries stored in the logging installation buffer.
<b>package</b>		Displays metadata information about the package, including description, restart information, components in the package, and so on.
{ <b>bootflash:</b>   <b>flash:</b>   <b>harddisk:</b>   <b>webui:</b> }		Specifies the location of the install package.
<b>rollback</b>		Displays the software set associated with a saved installation.
<b>summary</b>		Displays information about the list of active, inactive, committed, and superseded packages.
<b>uncommitted</b>		Displays package activations that are nonpersistent.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

**Usage Guidelines** Use the show commands to view the status of the install package.

## Example

The following is sample output from the **show install package** command:

```
Device# show install package bootflash:cat3k-universalk9.2017-01-10_13.15.1.
CSCxxx.SSA.dmp.bin
Name: cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SS
Version: 16.6.1.0.199.1484082952..Everest
Platform: Catalyst3k
Package Type: dmp
Defect ID: CSCxxx
Package State: Added
Supersedes List: {}
Smu ID: 1
```

The following is sample output from the **show install summary** command:

```
Device# show install summary

Active Packages:
  bootflash:cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
Inactive Packages:
  No packages
Committed Packages:
  bootflash:cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
Uncommitted Packages:
  No packages
Device#
```

The table below lists the significant fields shown in the display.

**Table 6: show install summary Field Descriptions**

Field	Description
Active Packages	Name of the active install package.
Inactive Packages	List of inactive packages.
Committed Packages	Install packages that have saved or committed changes to the harddisk, so that the changes become persistent across reloads.
Uncommitted Packages	Intall package activations that are nonpersistent.

The following is sample output from the **show install log** command:

```
Device# show install log

[0|install_op_boot]: START Fri Feb 24 19:20:19 Universal 2017
[0|install_op_boot]: END SUCCESS Fri Feb 24 19:20:23 Universal 2017
[3|install_add]: START Sun Feb 26 05:55:31 UTC 2017
[3|install_add( FATAL)]: File path (scp) is not yet supported for this command
[4|install_add]: START Sun Feb 26 05:57:04 UTC 2017
[4|install_add]: END SUCCESS
/bootflash/cat3k-universalk9.2017-01-10_13.15.1.CSCvb12345.SSA.dmp.bin
Sun Feb 26 05:57:22 UTC 2017
[5|install_activate]: START Sun Feb 26 05:58:41 UTC 2017
```

#### Related Commands

Command	Description
<b>install</b>	Installs SMU packages.

# show license all

To display all licensing information enter the **show license all** command in privileged EXEC mode. This command displays status, authorization, UDI, and usage information, all combined.

## show license all

**Syntax Description** This command has no arguments or keywords.

**Command Default** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Fuji 16.9.1	This command was introduced.
	Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to display information relating to Smart Licensing Using Policy. Command output no longer displays Smart Account and Virtual account information.
	Cisco IOS XE Cupertino 17.7.1	The output of the command was enhanced to display the following information: <ul style="list-style-type: none"> <li>• RUM report statistics, in section <code>Usage Report Summary</code>.</li> <li>• Smart Account and Virtual Account information, in section <code>Account Information</code>.</li> </ul>

## Usage Guidelines

This command concatenates the output of other show license commands, enabling you to display different kinds of licensing information together. For field descriptions, refer to the corresponding commands.

**Smart Licensing:** If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing (whether smart licensing is enabled, all associated licensing certificates, compliance status, and so on).

**Smart Licensing Using Policy:** If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

- The `Smart Licensing Status` section corresponds with the output of the **show license status** command.
- The `License Usage` section corresponds with the output of the **show license usage** command.
- The `Product Information` section corresponds with the output of the **show license udi** command.
- The `Agent Version` section of the show license all command displays the Smart Agent version and is available only in this command.
- The `License Authorizations` section corresponds with the output of the **show license authorization** command.
- The `Usage Report Summary` section corresponds with the output in the **show license tech** command.

## Examples

- [show license all for Smart Licensing Using Policy \(Cisco Catalyst 9300 Series Switches\)](#), on page 133
- [show license all for Smart Licensing Using Policy \(Cisco Catalyst 9500 Series Switches\)](#), on page 135
- [show license all for Smart Licensing](#), on page 137

### show license all for Smart Licensing Using Policy (Cisco Catalyst 9300 Series Switches)

The following is sample output of the **show license all** command in a stacking set-up. All the product instances in the stack are C9300X switches, which support the Export Control Key for High Security (HSECK9) starting from Cisco IOS XE Bengaluru 17.6.2. An HSECK9 key is used here and the requisite Smart Licensing Authorization Code (SLAC) is installed (SMART AUTHORIZATION INSTALLED on Oct 29 17:45:28 2021 UTC).

```
Device# show license all

Smart Licensing Status
=====

Smart Licensing is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: cslu
  Cslu address: <empty>
  Proxy:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Installed On Oct 29 17:44:15 2021 UTC
  Policy name: Custom Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (Customer Policy)
    Reporting frequency (days): 0 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (Customer Policy)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
```

show license all

```

Reporting frequency (days): 90 (Customer Policy)
Report on change (days): 90 (Customer Policy)
Export (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 90 (Customer Policy)
Report on change (days): 90 (Customer Policy)

```

## Usage Reporting:

```

Last ACK received: Oct 29 17:48:51 2021 UTC
Next ACK deadline: Jan 27 17:48:51 2022 UTC
Reporting push interval: 30 days
Next ACK push check: <none>
Next report push: Oct 29 18:32:43 2021 UTC
Last report push: Oct 29 17:44:50 2021 UTC
Last report file write: <none>

```

## Trust Code Installed:

```

Active: PID:C9300X-24HX,SN:FOC2519L8R7
INSTALLED on Oct 29 17:44:15 2021 UTC
Standby: PID:C9300X-48HXN,SN:FOC2524L39P
INSTALLED on Oct 29 17:44:15 2021 UTC
Member: PID:C9300X-48HX,SN:FOC2516LC92
INSTALLED on Oct 29 17:44:15 2021 UTC

```

## License Usage

=====

## network-advantage (C9300-24 Network Advantage):

```

Description: C9300-24 Network Advantage
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: network-advantage
Feature Description: C9300-24 Network Advantage
Enforcement type: NOT ENFORCED
License type: Perpetual

```

## dna-advantage (C9300-24 DNA Advantage):

```

Description: C9300-24 DNA Advantage
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: dna-advantage
Feature Description: C9300-24 DNA Advantage
Enforcement type: NOT ENFORCED
License type: Subscription

```

## network-advantage (C9300-48 Network Advantage):

```

Description: C9300-48 Network Advantage
Count: 2
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: network-advantage
Feature Description: C9300-48 Network Advantage
Enforcement type: NOT ENFORCED
License type: Perpetual

```

## dna-advantage (C9300-48 DNA Advantage):

```

Description: C9300-48 DNA Advantage
Count: 2
Version: 1.0

```

```

Status: IN USE
Export status: NOT RESTRICTED
Feature Name: dna-advantage
Feature Description: C9300-48 DNA Advantage
Enforcement type: NOT ENFORCED
License type: Subscription

hseck9 (Cat9K HSEC):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Perpetual

Product Information
=====
UDI: PID:C9300X-24HX,SN:FOC2519L8R7

HA UDI List:
  Active:PID:C9300X-24HX,SN:FOC2519L8R7
  Standby:PID:C9300X-48HXN,SN:FOC2524L39P
  Member:PID:C9300X-48HX,SN:FOC2516LC92

Agent Version
=====
Smart Agent for Licensing: 5.1.23_rel/104

License Authorizations
=====
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
    Status: SMART AUTHORIZATION INSTALLED on Oct 29 17:45:28 2021 UTC
    Last Confirmation code: 6746c5b5
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
    Status: NOT INSTALLED
  Member: PID:C9300X-48HX,SN:FOC2516LC92
    Status: NOT INSTALLED

Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Authorization type: SMART AUTHORIZATION INSTALLED
      License type: PERPETUAL
      Term Count: 1

Purchased Licenses:
  No Purchase Information Available

```

### show license all for Smart Licensing Using Policy (Cisco Catalyst 9500 Series Switches)

The following is sample output of the **show license all** command on a Cisco Catalyst 9500 switch. The software version running on the product instance here is Cisco IOS XE Cupertino 17.7.1. Similar output is displayed on all Cisco Catalyst Access, Core, and Aggregation Switches.

```

Device# show license all

Smart Licensing Status
=====

Smart Licensing is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: <none>
  Virtual Account: <none>

Data Privacy:
  Sending Hostname: no
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: ENABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Mar 30 22:32:22 2020 EST
  Reporting push interval: 30 days
  Next ACK push check: <none>
  Next report push: Oct 19 04:39:08 2021 EST

```



```

Last report push: <none>
Last report file write: <none>

Trust Code Installed: <none>

License Usage
=====

network-advantage (C9500 Network Advantage):
  Description: C9500 Network Advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: C9500 Network Advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual

dna-advantage (C9500-40X DNA Advantage):
  Description: C9500-40X DNA Advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9500-40X DNA Advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription

Product Information
=====
UDI: PID:C9500-40X,SN:FCW2227A4NC

Agent Version
=====
Smart Agent for Licensing: 5.3.9_rel/22

License Authorizations
=====
Overall status:
  Active: PID:C9500-40X,SN:FCW2227A4NC
  Status: NOT INSTALLED

Purchased Licenses:
  No Purchase Information Available

Derived Licenses:
  Entitlement Tag:
regid.2017-03.com.cisco.advantagek9-Nyquist-C9500,1.0_f1563759-2e03-4a4c-bec5-5feec525a12c
  Entitlement Tag:
regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9

Usage Report Summary:
=====
Total: 26, Purged: 0
Total Acknowledged Received: 0, Waiting for Ack: 0
Available to Report: 26 Collecting Data: 2

```

### show license all for Smart Licensing

The following is sample output from the **show license all** command:

## show license all

Device# **show license all**

Smart Licensing Status

=====

Smart Licensing is ENABLED

Registration:

Status: REGISTERED

Smart Account: CISCO Systems

Virtual Account: NPR

Export-Controlled Functionality: Allowed

Initial Registration: SUCCEEDED on Jul 13 09:30:40 2018 EDT

Last Renewal Attempt: None

Next Renewal Attempt: Jan 09 09:30:40 2019 EDT

Registration Expires: Jul 13 09:25:31 2019 EDT

License Authorization:

Status: AUTHORIZED on Jul 13 09:30:45 2018 EDT

Last Communication Attempt: SUCCEEDED on Jul 13 09:30:45 2018 EDT

Next Communication Attempt: Aug 12 09:30:45 2018 EDT

Communication Deadline: Oct 11 09:25:40 2018 EDT

Utility:

Status: DISABLED

Data Privacy:

Sending Hostname: yes

Callhome hostname privacy: DISABLED

Smart Licensing hostname privacy: DISABLED

Version privacy: DISABLED

Transport:

Type: Callhome

License Usage

=====

C9300 DNA Advantage (C9300-24 DNA Advantage):

Description: C9300-24P DNA Advantage

Count: 3

Version: 1.0

Status: AUTHORIZED

C9300 Network Advantage (C9300-24 Network Advantage):

Description: C9300-24P Network Advantage

Count: 3

Version: 1.0

Status: AUTHORIZED

Product Information

=====

UDI: PID:C9300-24U,SN:FCW2125L046

HA UDI List:

Active:PID:C9300-24U,SN:FCW2125L046

Standby:PID:C9300-24U,SN:FCW2125L03U

Member:PID:C9300-24U,SN:FCW2125G01T

Agent Version

=====

Smart Agent for Licensing: 4.4.13\_rel/116

Component Versions: SA:(1\_3\_dev)1.0.15, SI:(dev22)1.2.1, CH:(rel15)1.0.3, PK:(dev18)1.0.3

```
Reservation Info
=====
License reservation: DISABLED
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show license status</b>	Displays compliance status of a license.
<b>show license authorization</b>	Displays authorization code-related information.
<b>show license summary</b>	Displays summary of all active licenses.
<b>show license udi</b>	Displays UDI.
<b>show license usage</b>	Displays license usage information
<b>show license tech support</b>	Displays the debug output.

# show license authorization

To display authorization-related information for (export-controlled and enforced) licenses, enter the **show license authorization** command in privileged EXEC mode.

## show license authorization

This command has no arguments or keywords.

---

**Command Modes** Privileged EXEC (Device#)

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.

---



---

**Usage Guidelines** Use this command to display information about authorization codes. This includes SLR authorization codes and Smart Licensing Authorization Codes (SLAC).

## Examples

For information about fields shown in the display, see [Table 7: show license authorization Field Descriptions, on page 141](#).

For sample outputs, see:

- [Displaying SLAC, on page 143](#)
- [Displaying SLR Authorization Code, on page 143](#).

Table 7: show license authorization Field Descriptions

Field	Description
Overall Status	<p>Header for UDI information for all product instances in the set-up, the type of authorization that is installed, and configuration errors, if any.</p> <p>In a High Availability set-up, all UDIs in the set-up are listed.</p>
Active: Status:	<p>The active product instance UDI, followed by the status of the authorization code installation for this UDI.</p> <p>If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.</p>
Standby: Status:	<p>The standby product instance UDI, followed by the status of the authorization code installation for this UDI.</p> <p>If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.</p>
Member: Status:	<p>The member product instance UDI, followed by the status of the authorization code installation for this UDI.</p> <p>If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.</p>
ERROR:	<p>Configuration errors or discrepancies in the High Availability set-up, if any.</p>

Field	Description
Authorizations	<p>Header for detailed license authorization information. All licenses, their enforcement types, and validity durations are displayed. Errors are displayed for each product instance if its authorization or mode does not match what is installed on the active.</p> <p>This section is displayed only if the product instance is using a license with an authorization code.</p>
():	License name and a shortened form of the license name.
Description	License description.
Total available count:	<p>Total count of licenses that are <i>available</i> to consume.</p> <p>This includes licenses of all durations (perpetual and subscription), including expired subscription licenses, for all the product instances in a High Availability setup.</p>
Enforcement type	<p>Enforcement type for the license. This may be one of the following:</p> <ul style="list-style-type: none"> <li>• Enforced</li> <li>• Not enforced</li> <li>• Export-Controlled</li> </ul>
Term information:	<p>Header providing license duration information. The following fields maybe included under this header:</p> <ul style="list-style-type: none"> <li>• Active: The active product instance UDI, followed by the status of the authorization code installation for this UDI.</li> <li>• Authorization type: Type of authorization code installed and date of installation. The type can be: SLAC, UNIVERSAL, SPECIFIED, PAK, RTU.</li> <li>• Start Date: Displays validity start date if the license is for a specific term or time period.</li> <li>• Start Date: Displays validity end date if the license is for a specific term or time period.</li> <li>• Term Count: License count.</li> <li>• Subscription ID: Displays ID if the license is for a specific term or time period.</li> <li>• License type: License duration. This can be: SUBSCRIPTION or PERPETUAL.</li> <li>• Standby: The standby product instance UDI, followed by the status of the authorization code installation for this UDI.</li> <li>• Member: The member product instance UDI, followed by the status of the authorization code installation for this UDI.</li> </ul>

Field	Description
Purchased Licenses	Header for license purchase information.
Active:	The active product instance and its the UDI.
Count:	License count.
Description:	License description.
License type:	License duration. This can be: SUBSCRIPTION or PERPETUAL.
Standby:	The standby product instance UDI.
Member:	The member product instance UDI.

### Displaying SLAC

The following is sample output of the **show license authorization** command on a C9300X model switch. Here SLAC is installed only on the active product instance in a stacking set-up:

```
Device# show license authorization
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
           Status: SMART AUTHORIZATION INSTALLED on Oct 29 17:45:28 2021 UTC
           Last Confirmation code: 6746c5b5
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
           Status: NOT INSTALLED
  Member: PID:C9300X-48HX,SN:FOC2516LC92
           Status: NOT INSTALLED

Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Authorization type: SMART AUTHORIZATION INSTALLED
      License type: PERPETUAL
      Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

### Displaying SLR Authorization Code

The following is sample output of the **show license authorization** command showing SLR authorization codes (Last Confirmation code:). An SLR authorization code is supported after upgrade to Smart Licensing Using Policy. While existing SLRs are carried over after upgrade, you cannot request a new SLR in the Smart Licensing Using Policy environment. If you are in an air-gapped network, the *No Connectivity to CSSM and No CSLU* topology applies instead.

```
Device# show license authorization

Overall status:
  Active: PID:C9500-16X,SN:FCW2233A5ZV
```

## show license authorization

```

Status: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
Last Confirmation code: 184ba6d6
Standby: PID:C9500-16X,SN:FCW2233A5ZY
Status: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
Last Confirmation code: 961d598f

Specified license reservations:
C9500 Network Advantage (C9500 Network Advantage):
  Description: C9500 Network Advantage
  Total reserved count: 2
  Enforcement type: NOT ENFORCED
  Term information:
    Active: PID:C9500-16X,SN:FCW2233A5ZV
      Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
      License type: PERPETUAL
      Term Count: 1
    Standby: PID:C9500-16X,SN:FCW2233A5ZY
      Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
      License type: PERPETUAL
      Term Count: 1
C9500-DNA-16X-A (C9500-16X DNA Advantage):
  Description: C9500-DNA-16X-A
  Total reserved count: 2
  Enforcement type: NOT ENFORCED
  Term information:
    Active: PID:C9500-16X,SN:FCW2233A5ZV
      Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
      License type: PERPETUAL
      Term Count: 1
    Standby: PID:C9500-16X,SN:FCW2233A5ZY
      Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
      License type: PERPETUAL
      Term Count: 1

Purchased Licenses:
  No Purchase Information Available

Derived Licenses:
  Entitlement Tag:
  regid.2017-03.com.cisco.advantagek9-Nyquist-C9500,1.0_f1563759-2e03-4a4c-bec5-5feec525a12c
  Entitlement Tag:
  regid.2017-07.com.cisco.C9500-DNA-16X-A,1.0_ef3574d1-156b-486a-864f-9f779ff3ee49

```



# show license data conversion

To display license data conversion information, enter the **show license data** command in privileged EXEC mode.

**show license data conversion**

## Syntax Description

This command has no keywords or arguments

## Command Modes

Privileged EXEC (Device#)

## Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to display information relating to Smart Licensing Using Policy.  Command output no longer displays Smart Account and Virtual account information.

## Usage Guidelines

**Smart Licensing:** If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

**Smart Licensing Using Policy:** If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Device-led conversion is not supported on Cisco Catalyst Access, Core, and Aggregation Switches.

# show license eventlog

To display event logs relating to Smart Licensing Using Policy, enter the **show license eventlog** command in privileged EXEC mode.

**show license eventlog** [ *days* ]

<b>Syntax Description</b>	<i>days</i> Enter the number of days for which you want to display event logs. The valid value range is from 0 to 2147483647.
---------------------------	---

<b>Command Modes</b>	Privileged EXEC (Device#)
----------------------	---------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Fuji 16.9.1	This command was introduced.
	Cisco IOS XE Amsterdam 17.3.2a	Additional events were added with the introduction of Smart Licensing Using Policy: <ul style="list-style-type: none"> <li>• Installation and removal of a policy</li> <li>• Request, installation and removal of an authorization code.</li> <li>• Installation and removal of a trust code.</li> <li>• Addition of authorization source information for license usage.</li> </ul>

## Usage Guidelines

**Smart Licensing:** If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

**Smart Licensing Using Policy:** If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

## Examples

[show license eventlog for One Day, for Smart Licensing Using Policy, on page 146](#)

[show license eventlog for All Events, for Smart Licensing Using Policy, on page 147](#)

### show license eventlog for One Day, for Smart Licensing Using Policy

The following is sample output from the **show license eventlog** command on a Cisco Catalyst 9500 switch. Similar output is displayed on all supported Cisco Catalyst Access, Core, and Aggregation Switches. The command is configured to display events for one day.

```
Device# show license eventlog 1
**** Event Log ****
```

```
2020-09-11 00:50:17.693 EDT SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_ERM_RESET" MSG="ERM-Reset: Client 0, AP-GROUP group, 2 features
air-network-advantage,air-dna-advantage"
2020-09-11 00:50:17.695 EDT SAEVT_ENDPOINT_USAGE count="0"
```

```

entitlementTag="regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896"
2020-09-11 00:50:17.695 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790"
2020-09-11 00:50:50.175 EDT SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
2020-09-11 08:50:17.694 EDT SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_ERM_RESET" MSG="ERM-Reset: Client 0, AP-GROUP group, 2 features
air-network-advantage,air-dna-advantage"
2020-09-11 08:50:17.696 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896"
2020-09-11 08:50:17.696 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790"
2020-09-11 08:50:52.804 EDT SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"

```

### show license eventlog for All Events, for Smart Licensing Using Policy

The following is sample output from the **show license eventlog** command on a Cisco Catalyst 9500 switch. Similar output is displayed on all supported Cisco Catalyst Access, Core, and Aggregation Switches. The command is configured to display all events.

```
Device# show license eventlog
```

```

**** Event Log ****

2020-09-01 15:43:42.300 UTC SAEVT_INIT_START version="4.13.14_rel/41"
2020-09-01 15:43:42.301 UTC SAEVT_INIT_CRYPT0 success="False" error="Crypto Initialization
has not been completed"
2020-09-01 15:43:42.301 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHarmfRegister"
2020-09-01 15:43:45.055 UTC SAEVT_READY
2020-09-01 15:43:45.055 UTC SAEVT_ENABLED
2020-09-01 15:43:45.088 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_SYSDATA_FAIL" MSG="Get-SDL: not the active switch"
2020-09-01 15:43:45.089 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_SYSDATA_FAIL" MSG="Get-SDL: not the active switch"
2020-09-01 15:43:45.089 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_SYSDATA_FAIL" MSG="Get-SDL: not the active switch"
2020-09-01 15:43:45.089 UTC SAEVT_LICENSE_USAGE count="0" type="destroy"
entitlementTag="regid.2018-01.com.cisco.C9500-24Y4C-A,1.0_6b065611-6552-472a-8859-ab3339550166"
2020-09-01 15:43:45.098 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_SYSDATA_FAIL" MSG="Get-SDL: not the active switch"

```

## show license history message

To display communication history between the product instance and CSSM or CSLU (as the case may be), enter the **show license history message** command in privileged EXEC mode. The output of this command is used by the technical support team, for troubleshooting.

### show license history message

<b>Syntax Description</b>	This command has no keywords or arguments.	
<b>Command Modes</b>	Privileged EXEC (Device#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.
<b>Usage Guidelines</b>	When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: <b>show license tech support</b> , <b>show license history message</b> , and the <b>show platform software sl-infra all</b> privileged EXEC commands.	

# show license reservation

To display license reservation information, enter the **show license reservation** command in privileged EXEC mode.

## show license reservation

This command has no arguments or keywords.

---

### Command Modes

Privileged EXEC (Device#)

---

### Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	The command continues to be available on the CLI, but is no longer applicable because the notion of reservation does not exist in the Smart Licensing Using Policy environment.

---

### Usage Guidelines

The command continues to be available on the CLI and corresponding output is displayed, but with the introduction of Smart Licensing Using Policy, the notion of reservation is no longer applicable. Use the **show license all** command in privileged EXEC mode, to display *migrated* SLR licenses instead (the SLR authorization code is migrated to Smart Licensing Using Policy).

## show license rum

To display information about Resource Utilization Measurement reports (RUM report) available on the product instance, including report IDs, the current processing state of a report, error information (if any), and to save the detailed or summarized view that is displayed, enter the **show license rum** command in privileged EXEC mode.

```
show license rum { feature { license_name | all } | id { rum_id | all } } [ detail ] [ save path ]
```

### Syntax Description

<b>feature</b> { <i>license_name</i>   <b>all</b> }	Displays RUM report information based on the license name.  Specify a particular license name to display all RUM reports for that license, or use the <b>all</b> keyword to display all RUM reports available on the product instance.
<b>id</b> { <i>rum_id</i>   <b>all</b> }	Displays RUM report information based on the RUM report ID.  Specify a report ID to display information for a single report, or use the <b>all</b> keyword to display all RUM reports available on the product instance.
<b>detail</b>	Displays detailed RUM report information.  You can use this to display detailed information by license name and detailed information by RUM report ID.
<b>save path</b>	Saves the information that is displayed. This can be the simplified or detailed version and depends on the preceding keywords you have entered.  Information about 200 RUM reports can be displayed. If there are more 200 RUM reports on the product instance, you can view information about all the RUM reports by saving it to a text (.txt) file.  <b>Note</b> This option saves the information <i>about</i> RUM reports and is not for reporting purposes. It does not save the RUM report, which is an XML file containing usage information.

### Command Modes

Privileged EXEC (Device#)

### Command History

Release	Modification
Cisco IOS XE Cupertino 17.7.1	This command was introduced.

### Usage Guidelines

A RUM report is a license usage report, which the product instance generates, to fulfil reporting requirements as specified by the policy. An acknowledgement (ACK) is a response from CSSM and provides information about the status of a RUM report. Once the ACK for a report is available on the product instance, it indicates

that the corresponding RUM report is no longer required and can be deleted. You can use the **show license rum** command to:

- Display information about the available RUM reports on the product instance - filtered by ID or license name.
- Display a short summary of the information or display a detailed view of the information.
- Track a RUM report throughout its lifecycle (from the time it is first generated until its acknowledgement from CSSM). By displaying the current processing state and condition of a report you can ascertain if and when there is a problem in the reporting workflow.
- Save the displayed information. The CLI displays information about up to 200 reports. If there are more than 200 reports on the product instance and you want to view information about all of them, save the displayed info in a .txt file and export to the desired location to view.

To display a statistical view of RUM report information (the total number of reports on the product instance, the number of reports that have a corresponding ACK, the number of reports waiting for an ACK etc.) refer to the `Usage Report Summary`: section of the **show license all** and **show license tech** privileged EXEC commands.

The **show license tech** command also provides RUM report related information that the Cisco technical support team can use to troubleshoot, if there are problems with RUM reporting.

### Examples

For information about fields shown in the display, see [Table 8: show license rum \(simplified view\) Field Descriptions, on page 151](#) and [Table 9: show license rum \(detailed view\) Field Descriptions, on page 153](#)

For examples of the **show license rum** command, see:

- [show license rum feature: Simplified and Detailed View, on page 154](#)
- [Saving RUM Report View, on page 157](#)

**Table 8: show license rum (simplified view) Field Descriptions**

Field Name	Description
Report Id	A numeric field that identifies a RUM report. The product instance automatically assigns an ID to every RUM report it generates. An ID may be up to 20 characters long.

Field Name	Description
State	<p>This field displays the current processing state of a RUM report, and can be only one of the following:</p> <ul style="list-style-type: none"> <li>• OPEN: This means new measurements are being added to this report.</li> <li>• CLOSED: This means no further measurements can be added to this report, and the report is ready for communication to CSSM.</li> <li>• PENDING: This is a transitional status that you may see if you display a report while it is being transmitted.</li> <li>• UNACK: This means the report was transmitted and is waiting for confirmation from CSSM, that it is processed.</li> <li>• ACK: This means the report was processed or acknowledged by CSSM and is eligible for deletion.</li> </ul>
Flag	<p>Indicates the condition of the RUM report, and is displayed in the form of a character. Each character represents a specific condition, and can be only one of the following values:</p> <ul style="list-style-type: none"> <li>• N: Normal; This means no errors have been detected and the report is going through normal operation.</li> <li>• P: Purged; This means the report was removed due to system resource limitation, and can refer to a shortage of disk space or insufficient memory. If this flag is displayed, refer to the <code>State Change Reason</code> field in the detailed view for more information.</li> <li>• E: Error; This means an error was detected in the RUM report. If this flag is displayed, refer to the detailed view for more information. Possible workflow issues include and are not limited to the following: <ul style="list-style-type: none"> <li>• RUM report was dropped by CSSM. If this is the issue, the <code>State</code> field displays value <code>ACK</code>, but the <code>State Change Reason</code> does not change to <code>ACKED</code>.</li> <li>• RUM Report data is missing. If this is the issue, the <code>Storage State</code> field displays value <code>MISSING</code>.</li> <li>• Tracking information is missing. If this is the case the <code>State</code> field displays value <code>UNACK</code> and the <code>Transaction ID</code> field has no information.</li> </ul> </li> </ul> <p><b>Note</b> Occasional errors in RUM reports do not require any action from you and are not an indication of a problem. It is only if you see a large number of reports (greater than 10) with errors that you must contact the Cisco technical support team.</p>
Feature Name	The name of the license that the RUM report applies to.



Table 9: show license rum (detailed view) Field Descriptions

Field Name	Description
Report Id	A numeric field that identifies a RUM report. The product instance automatically assigns an ID to every RUM report it generates. An ID may be up to 20 characters long.
Metric Name:	Shows the type of data that is recorded. For a RUM report, the only possible value is ENTITLEMENT, and refers to measurement of license usage.
Feature Name:	The name of the license that the RUM report applies to.
Metric Value	A unique identifier for the data that is recorded. This is the same as the “Entitlement Tag” in the output of the <b>show license tech</b> command and it displays information about the license being tracked.
UDI	Composed of the Product ID (PID) and serial number of the product instance.
Previous Report Id:	ID of the previous RUM report that the product instance generated for a license.
Next Report Id:	The ID that the product instance will use for the next RUM report it generates for a license.
State:	Displays the current processing state of a RUM report. The value displayed here is always the same as the value displayed in the simplified view. For the list of possible values see <a href="#">Table 8: show license rum (simplified view) Field Descriptions, on page 151</a> above.
State Change Reason:	Displays the reason for a RUM report state change. Not all state changes provide a reason. <ul style="list-style-type: none"> <li>• NONE: This means the RUM report is going through its normal lifecycle (for instance, from OPEN → CLOSED → ACK). This state change reason is usually accompanied by an N flag (meaning Normal) in the simplified view and requires no action from you.</li> <li>• ACKED: RUM report was processed normally by CSSM.</li> <li>• REMOVED: RUM report was received and requested to be removed by CSSM.</li> <li>• RELOAD: RUM report state was changed due to some type of device reload.</li> <li>• DECONFIG: License was removed from configuration.</li> </ul>
Start Time:	Timestamps for measurement start and measurement end for a RUM report.
End Time:	Together, the start time and end time provide the time duration that the measurements cover.

Field Name	Description
Storage State:	<p>Displays current storage state of the RUM report and can be one of the following values:</p> <ul style="list-style-type: none"> <li>• <b>EXIST</b>: This means the data for the RUM report is located in storage.</li> <li>• <b>DELETED</b>: This means the data was intentionally deleted. Refer to the <code>Storage State Change Reason</code> in the output of the <b>show license tech</b> command for more information about this storage state.</li> <li>• <b>PURGED</b>: This means the data was deleted due to a system resource limitation. Refer to the <code>Storage State Change Reason</code> in the output of the <b>show license tech</b> command for more information about this storage state.</li> <li>• <b>MISSING</b>: This means data is missing from storage. If reports are identified as missing, there is no recovery process.</li> </ul>
Transaction ID:	<p>Contains tracking information for the RUM report. This information can be either polling information or ACK import information.</p> <p>The Transaction Message contains the error message, if the product instance receives one when importing an ACK.</p> <p>The information in these fields is used by the Cisco technical support team when troubleshooting problems with RUM reports.</p>
Transaction Message:	

### show license rum feature: Simplified and Detailed View

The following is sample output of the **show license rum feature *license-name*** and **show license rum feature *license-name* detail** commands on a Cisco Catalyst 9500 Series Switch. Similar output is displayed on all other Catalyst switches.

The output is filtered to display all RUM reports for the DNA Advantage license, followed by a detailed view of all RUM reports for the DNA Advantage license.

```
Device# show license rum feature dna-advantage
```

```
Smart Licensing Usage Report:
```

```
=====
```

```
Report Id,      State,   Flag,  Feature Name
1574560487     CLOSED  N      dna-advantage
1574560489     CLOSED  N      dna-advantage
1574560491     CLOSED  N      dna-advantage
1574560493     CLOSED  N      dna-advantage
1574560495     CLOSED  N      dna-advantage
1574560497     CLOSED  N      dna-advantage
1574560499     CLOSED  N      dna-advantage
1574560501     CLOSED  N      dna-advantage
1574560503     CLOSED  N      dna-advantage
1574560505     CLOSED  N      dna-advantage
1574560507     CLOSED  N      dna-advantage
1574560509     CLOSED  N      dna-advantage
1574560511     OPEN    N      dna-advantage
```

```
Device# show license rum feature dna-advantage detail
```

```
Smart Licensing Usage Report Detail:
```

```
=====  
Report Id: 1574560487  
Metric Name: ENTITLEMENT  
Feature Name: dna-advantage  
Metric Value:  
regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9  
UDI: PID:C9500-40X,SN:FCW2227A4NC  
Previous Report Id: 0, Next Report Id: 1574560489  
State: CLOSED, State Change Reason: None  
Start Time: Sep 02 00:11:55 2020 EST, End Time: Sep 02 20:12:04 2020 EST  
Storage State: EXIST  
Transaction ID: 0  
Transaction Message: <none>  
  
Report Id: 1574560489  
Metric Name: ENTITLEMENT  
Feature Name: dna-advantage  
Metric Value:  
regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9  
UDI: PID:C9500-40X,SN:FCW2227A4NC  
Previous Report Id: 1574560487, Next Report Id: 1574560491  
State: CLOSED, State Change Reason: None  
Start Time: Sep 02 20:24:46 2020 EST, End Time: Sep 02 22:24:56 2020 EST  
Storage State: EXIST  
Transaction ID: 0  
Transaction Message: <none>  
  
Report Id: 1574560491  
Metric Name: ENTITLEMENT  
Feature Name: dna-advantage  
Metric Value:  
regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9  
UDI: PID:C9500-40X,SN:FCW2227A4NC  
Previous Report Id: 1574560489, Next Report Id: 1574560493  
State: CLOSED, State Change Reason: None  
Start Time: Sep 02 22:34:27 2020 EST, End Time: Sep 03 14:34:37 2020 EST  
Storage State: EXIST  
Transaction ID: 0  
Transaction Message: <none>  
  
Report Id: 1574560493  
Metric Name: ENTITLEMENT  
Feature Name: dna-advantage  
Metric Value:  
regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9  
UDI: PID:C9500-40X,SN:FCW2227A4NC  
Previous Report Id: 1574560491, Next Report Id: 1574560495  
State: CLOSED, State Change Reason: None  
Start Time: Sep 03 14:45:16 2020 EST, End Time: Sep 03 15:30:49 2020 EST  
Storage State: EXIST  
Transaction ID: 0  
Transaction Message: <none>  
  
Report Id: 1574560495  
Metric Name: ENTITLEMENT  
Feature Name: dna-advantage  
Metric Value:  
regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9  
UDI: PID:C9500-40X,SN:FCW2227A4NC  
Previous Report Id: 1574560493, Next Report Id: 1574560497  
State: CLOSED, State Change Reason: None  
Start Time: Sep 03 15:47:29 2020 EST, End Time: Dec 21 17:02:39 2020 EST  
Storage State: EXIST  
Transaction ID: 0
```

```

Transaction Message: <none>

Report Id: 1574560497
Metric Name: ENTITLEMENT
Feature Name: dna-advantage
Metric Value:
regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9
UDI: PID:C9500-40X,SN:FCW2227A4NC
Previous Report Id: 1574560495, Next Report Id: 1574560499
State: CLOSED, State Change Reason: None
Start Time: Jan 05 14:02:34 2021 EST, End Time: Feb 19 21:02:21 2021 EST
Storage State: EXIST
Transaction ID: 0
Transaction Message: <none>

Report Id: 1574560499
Metric Name: ENTITLEMENT
Feature Name: dna-advantage
Metric Value:
regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9
UDI: PID:C9500-40X,SN:FCW2227A4NC
Previous Report Id: 1574560497, Next Report Id: 1574560501
State: CLOSED, State Change Reason: None
Start Time: Feb 19 21:17:57 2021 EST, End Time: Jul 05 14:03:07 2021 EST
Storage State: EXIST
Transaction ID: 0
Transaction Message: <none>

Report Id: 1574560501
Metric Name: ENTITLEMENT
Feature Name: dna-advantage
Metric Value:
regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9
UDI: PID:C9500-40X,SN:FCW2227A4NC
Previous Report Id: 1574560499, Next Report Id: 1574560503
State: CLOSED, State Change Reason: None
Start Time: Jul 05 14:19:30 2021 EST, End Time: Jul 06 14:34:40 2021 EST
Storage State: EXIST
Transaction ID: 0
Transaction Message: <none>

Report Id: 1574560503
Metric Name: ENTITLEMENT
Feature Name: dna-advantage
Metric Value:
regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9
UDI: PID:C9500-40X,SN:FCW2227A4NC
Previous Report Id: 1574560501, Next Report Id: 1574560505
State: CLOSED, State Change Reason: None
Start Time: Jul 06 14:39:42 2021 EST, End Time: Jul 06 15:10:14 2021 EST
Storage State: EXIST
Transaction ID: 0
Transaction Message: <none>

Report Id: 1574560505
Metric Name: ENTITLEMENT
Feature Name: dna-advantage
Metric Value:
regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9
UDI: PID:C9500-40X,SN:FCW2227A4NC
Previous Report Id: 1574560503, Next Report Id: 1574560507
State: CLOSED, State Change Reason: RELOAD
Start Time: Jul 06 15:25:36 2021 EST, End Time: Aug 05 15:55:46 2021 EST
Storage State: EXIST

```

```

Transaction ID: 0
Transaction Message: <none>

Report Id: 1574560507
Metric Name: ENTITLEMENT
Feature Name: dna-advantage
Metric Value:
regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9
UDI: PID:C9500-40X,SN:FCW2227A4NC
Previous Report Id: 1574560505, Next Report Id: 1574560509
State: CLOSED, State Change Reason: REPORTING
Start Time: Aug 05 16:15:11 2021 EST, End Time: Aug 05 16:15:14 2021 EST
Storage State: EXIST
Transaction ID: 0
Transaction Message: <none>

Report Id: 1574560509
Metric Name: ENTITLEMENT
Feature Name: dna-advantage
Metric Value:
regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9
UDI: PID:C9500-40X,SN:FCW2227A4NC
Previous Report Id: 1574560507, Next Report Id: 1574560511
State: CLOSED, State Change Reason: REPORTING
Start Time: Aug 05 16:15:14 2021 EST, End Time: Aug 05 19:38:43 2021 EST
Storage State: EXIST
Transaction ID: 0
Transaction Message: <none>

Report Id: 1574560511
Metric Name: ENTITLEMENT
Feature Name: dna-advantage
Metric Value:
regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9
UDI: PID:C9500-40X,SN:FCW2227A4NC
Previous Report Id: 1574560509, Next Report Id: 0
State: OPEN, State Change Reason: None
Start Time: Aug 05 19:38:43 2021 EST, End Time: Oct 18 02:53:39 2021 EST
Storage State: EXIST
Transaction ID: 0
Transaction Message: <none>

```

### Saving RUM Report View

The following example shows you how to save a simplified view of the **show license rum feature all** command.

By using the **feature** and **all** keywords, the output is filtered to display all RUM reports for all licenses being used on the product instance. You can then transfer it to a location from where you can open the text file and view the information.

```

Device# show license rum feature all save bootflash:all-rum-stats.txt
Device# copy bootflash:all-rum-stats.txt tftp://10.8.0.6/user01/

```

# show license status

To display information about licensing settings such as data privacy, policy, transport, usage reporting and trust codes, enter the **show license status** command in privileged EXEC mode.

## show license status

**Syntax Description** This command has no arguments or keywords.

**Command Default** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Fuji 16.9.1	This command was introduced.
	Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. This includes <code>Trust code installed:</code> , <code>Policy in use</code> , <code>Policy name:</code> , reporting requirements as in the policy, and <code>Usage Reporting:</code> .  Command output no longer displays Smart Account and Virtual account information.
	Cisco IOS XE Cupertino 17.7.1	Command output was updated to display Smart Account and Virtual account information.

**Usage Guidelines** **Smart Licensing:** If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

**Smart Licensing Using Policy:** If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

### Account Information in the output

Starting with Cisco IOS XE Cupertino 17.7.1, every ACK includes the Smart Account and Virtual Account that was reported to, in CSSM. When it receives the ACK, the product instance securely stores only the latest version of this information - as determined by the timestamp in the ACK. The Smart Account and Virtual Account information that is displayed in the `Account Information` section of this command's output is therefore always as per the latest available ACK on the product instance.

If a product instance is moved from one Smart Account and Virtual Account to another, the next ACK after the move will have this updated information. The output of this command is updated once this ACK is available on the product instance.

The ACK may be received directly (where the product instance is connected to CSSM), or indirectly (where the product instance is connect to CSSM through CSLU, Cisco DNA Center, or SSM On-Prem), or by manually importing the ACK (where a product instance is in an air-gapped network).

## Examples

For information about fields shown in the display, see [Table 10: show license status Field Descriptions for Smart Licensing Using Policy, on page 159](#)

For sample outputs, see:

- [show license status for Smart Licensing Using Policy, on page 164](#)
- [show license status for Smart Licensing, on page 165](#)

**Table 10: show license status Field Descriptions for Smart Licensing Using Policy**

Field	Description	
Utility	Header for utility settings that are configured on the product instance.	
	Status:	Status
	Utility report:	Last attempt:
	Customer Information:	The following fields are displayed: <ul style="list-style-type: none"> <li>• Id:</li> <li>• Name:</li> <li>• Street</li> <li>• City:</li> <li>• State:</li> <li>• Country:</li> <li>• Postal Code:</li> </ul>
Smart Licensing Using Policy:	Header for policy settings on the product instance.	
	Status:	Indicates if Smart Licensing Using Policy is enabled.  Smart Licensing Using Policy is supported starting from Cisco IOS XE Amsterdam 17.3.2 and is always enabled on supported software images.
Account Information:	Header for account information that the product instance belongs to, in CSSM.  This section is displayed only if the software version on the product instance is Cisco IOS XE Cupertino 17.7.1 or a later release.  If an ACK is not installed on the product instance, these fields display <none>.	
	Smart Account:	The Smart Account that the product instance is part of. This information is always as per the latest available ACK on the product instance.
	Virtual Account:	The Virtual Account that the product instance is part of. This information is always as per the latest available ACK on the product instance.

Field	Description
Data Privacy:	Header for privacy settings that are configured on the product instance.
Sending Hostname:	A <i>yes</i> or <i>no</i> value which shows if the hostname is sent in usage reports.
Callhome hostname privacy:	Indicates if the Call Home feature is configured as the mode of transport for reporting. If configured, one of these values is displayed: <ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>
Smart Licensing hostname privacy:	One of these values is displayed: <ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>
Version privacy:	One of these values is displayed: <ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>
Transport:	Header for transport settings that are configured on the product instance.
Type:	Mode of transport that is in use. Additional fields are displayed for certain transport modes. For example, if transport type is set to CSLU, the CSLU address is also displayed.



Field	Description
Policy:	Header for policy information that is applicable to the product instance.
Policy in use:	<p>Policy that is applied</p> <p>This can be one of the following: Cisco default, Product default, Permanent License Reservation, Specific License Reservation, PAK license, Installed on &lt;date&gt;, Controller.</p>
Policy name:	Name of the policy
Reporting ACK required:	A <i>yes</i> or <i>no</i> value which specifies if the report for this product instance requires CSSM acknowledgement (ACK) or not. The default policy is always set to “yes”.
Unenforced/Non-Export Perpetual Attributes	<p>Displays policy values for perpetual licenses.</p> <ul style="list-style-type: none"> <li>• First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name.</li> <li>• Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name.</li> <li>• Report on change (days): he maximum amount of time available to send a report in case of a change in license usage, followed by policy name</li> </ul>
Unenforced/Non-Export Subscription Attributes	<p>Displays policy values for subscription licenses.</p> <ul style="list-style-type: none"> <li>• First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name.</li> <li>• Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name.</li> <li>• Report on change (days): he maximum amount of time available to send a report in case of a change in license usage, followed by policy name</li> </ul>
Enforced (Perpetual/Subscription) License Attributes	

Field		Description
		<p>Displays policy values for enforced licenses.</p> <ul style="list-style-type: none"> <li>• First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name.</li> <li>• Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name.</li> <li>• Report on change (days): The maximum amount of time available to send a report in case of a change in license usage, followed by policy name</li> </ul>
	Export (Perpetual/Subscription) License Attributes	<p>Displays policy values for export-controlled licenses.</p> <ul style="list-style-type: none"> <li>• First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name.</li> <li>• Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name.</li> <li>• Report on change (days): The maximum amount of time available to send a report in case of a change in license usage, followed by policy name</li> </ul>
Miscellaneous	Header for custom ID.	
	Custom Id:	ID

Field	Description
Usage Reporting:	Header for usage reporting (RUM reports) information.
Last ACK received:	Date and time of last ACK received, in the local time zone.
Next ACK deadline:	Date and time for next ACK. If the policy states that an ACK is not required then this field displays <code>none</code> .  <b>Note</b> If an ACK is required and is not received by this deadline, a syslog is displayed.
Reporting Interval:	Reporting interval in days  The value displayed here depends on what you configure in the <b>license smart usage interval</b> <code>interval_in_days</code> and the policy value. For more information, see the corresponding Syntax Description: <a href="#">Table 10: show license status Field Descriptions for Smart Licensing Using Policy, on page 159</a> .
Next ACK push check:	Date and time when the product instance will submit the next polling request for an ACK. Date and time are in the local time zone.  This applies only to product instance- initiated communication to CSSM or CSLU. If the reporting interval is zero, or if no ACK polling is pending, then this field displays <code>none</code> .
Next report push:	Date and time when the product instance will send the next RUM report. Date and time are in the local time zone. If the reporting interval is zero, or if there are no pending RUM reports, then this field displays <code>none</code> .
Last report push:	Date and time for when the product instance sent the last RUM report. Date and time are in the local time zone.
Last report file write:	Date and time for when the product instance last saved an offline RUM report. Date and time are in the local time zone.
Last report pull:	Date and time for when usage reporting information was retrieved using data models. Date and time are in the local time zone.

Field	Description
Trust Code Installed:	Header for trust code-related information. Displays date and time if trust code is installed. Date and time are in the local time zone. If a trust code is not installed, then this field displays <i>none</i> .
Active:	Active product instance. In a High Availability set-up, the the UDIs of all product instances in the set-up, along with corresponding trust code installation dates and times are displayed.
Standby:	Standby product instance.
Member:	Member product instance

### show license status for Smart Licensing Using Policy

The following is sample output of the **show license status** command on a Cisco Catalyst 9500 switch where the software version running on the product instance is Cisco IOS XE Cupertino 17.7.1. Note the Smart Account and Virtual Account fields in the output starting from this release.

An ACK has not been installed on this product instance (Last ACK received: <none>). The account information fields therefore display <none>:

```
Device# show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: <none>
  Virtual Account: <none>

Data Privacy:
  Sending Hostname: no
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: ENABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
```

```

Unenforced/Non-Export Subscription Attributes:
  First report requirement (days): 90 (CISCO default)
  Reporting frequency (days): 90 (CISCO default)
  Report on change (days): 90 (CISCO default)
Enforced (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 0 (CISCO default)
Export (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 0 (CISCO default)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Mar 30 22:32:22 2020 EST
  Reporting push interval: 30 days
  Next ACK push check: <none>
  Next report push: Oct 21 04:39:08 2021 EST
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

```

### show license status for Smart Licensing

The following is sample output of the **show license status** command.

```

Device# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: REGISTERED
  Smart Account: Cisco Systems
  Virtual Account: NPR
  Export-Controlled Functionality: Allowed
  Initial Registration: First Attempt Pending
  Last Renewal Attempt: SUCCEEDED on Jul 19 14:49:49 2018 IST
  Next Renewal Attempt: Jan 15 14:49:47 2019 IST
  Registration Expires: Jul 19 14:43:47 2019 IST

License Authorization:
  Status: AUTHORIZED on Jul 28 07:02:56 2018 IST
  Last Communication Attempt: SUCCEEDED on Jul 28 07:02:56 2018 IST
  Next Communication Attempt: Aug 27 07:02:56 2018 IST
  Communication Deadline: Oct 26 06:57:50 2018 IST

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show license all</b>	Displays entitlements information.
<b>show license authorization</b>	Displays authorization code-related information.
<b>show license summary</b>	Displays summary of all active licenses.
<b>show license udi</b>	Displays UDI.
<b>show license usage</b>	Displays license usage information
<b>show tech-support license</b>	Displays the debug output.

# show license summary

To display a brief summary of license usage, which includes information about licenses being used, the count, and status, use the **show license summary** command in privileged EXEC mode.

## show license summary

**Syntax Description** This command has no arguments or keywords.

**Command Default** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Fuji 16.9.1	This command was introduced.
	Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect valid license status for Smart Licensing Using Policy. Valid license statuses are now only <code>IN USE</code> , <code>NOT IN USE</code> , <code>NOT AUTHORIZED</code> .  Command output was also updated to remove registration and authorization information.  Command output no longer displays Smart Account and Virtual account information.
	Cisco IOS XE Cupertino 17.7.1	Command output was updated to display Smart Account and Virtual account information.

## Usage Guidelines

**Smart Licensing:** If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

**Smart Licensing Using Policy:** If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

### License status

- The **unenforced licenses** that are available on Cisco Catalyst Access, Core, and Aggregation Switches are `never NOT AUTHORIZED OR NOT IN USE`.
- The **export-controlled license**, Export Control Key for High Security (HSECK9 key), which is supported on the switches listed below, displays status `NOT IN USE` if an HSECK9 key is available on the product instance and the requisite Smart Licensing Authorization Code (SLAC) is installed, but the cryptographic feature that requires the HSECK9 key is not configured.
  - Cisco Catalyst 9300X Series Switches, from Cisco IOS XE Bengaluru 17.6.2
  - Cisco Catalyst 9600 Series 40-Port 50G, 2-Port 200G, 2-Port 400G Line Card (C9600-LC-40YL4CD) from Cisco IOS XE Cupertino 17.8.1
  - Cisco Catalyst 9500X Series Switches from Cisco IOS XE Cupertino 17.8.1

Configure the applicable cryptographic feature for the count and status fields to change to 1 and IN USE respectively.

For more detailed license usage information, see the output of the **show license usage** privileged EXEC command.

### Usage Count

In a stacking setup, even if you install SLAC on more than one device, the usage count remains 1. This is because only one HSECK9 key is used at a given point in time - the one on the active. The license on the standby comes into effect when a switchover occurs. The count remains 1 with the new active as well, because it is still only one HSECK9 key that is being used.

In case of a modular chassis, the usage count must display only 1 because only one HSECK9 key is required for each chassis UDI - regardless of the number of supervisors installed.

### Account information in the output

Starting with Cisco IOS XE Cupertino 17.7.1, every ACK includes the Smart Account and Virtual Account that was reported to, in CSSM. When it receives the ACK, the product instance securely stores only the latest version of this information - as determined by the timestamp in the ACK. The Smart Account and Virtual Account information that is displayed in the `Account Information` section of this command's output is therefore always as per the latest available ACK on the product instance.

If a product instance is moved from one Smart Account and Virtual Account to another, the next ACK after the move will have this updated information. The output of this command is updated once this ACK is available on the product instance.

The ACK may be received directly (where the product instance is connected to CSSM), or indirectly (where the product instance is connect to CSSM through CSLU, Cisco DNA Center, or SSM On-Prem), or by manually importing the ACK (where a product instance is in an air-gapped network).

### Examples

For information about fields shown in the display, see [Table 11: show license summary Field Descriptions for Smart Licensing Using Policy, on page 168](#)

For sample outputs, see:

- [show license summary \(Cisco Catalyst 9500 Series Switches\), on page 169](#)
- [show license summary \(Cisco Catalyst 9300X Series Switches\), on page 169](#)

**Table 11: show license summary Field Descriptions for Smart Licensing Using Policy**

Field	Description
Account Information:	The Smart Account and Virtual Account that the product instance is part of. This information is always as per the latest available ACK on the product instance.
Smart Account:	This field is displayed only if the software version on the product instance is Cisco IOS XE Cupertino 17.7.1 or a later release.  If an ACK is not installed on the product instance, these fields display <code>&lt;none&gt;</code> .
Virtual Account:	
License	Name of the licenses in use
Entitlement Tag	Short name for license



Field	Description
Count	License count
Status	<p>License status can be one of the following</p> <ul style="list-style-type: none"> <li>• In-Use: Valid license, and in-use.</li> <li>• Not In-Use: An HSECK9 key is available on the product instance and the requisite Smart Licensing Authorization Code (SLAC) is installed, but the cryptographic feature that requires the HSECK9 key is disabled or not configured.</li> </ul> <p>This status is a prerequisite when you want to <i>return</i> the SLAC for an HSECK9 license to CSSM.</p> <ul style="list-style-type: none"> <li>• Not Authorized: Means that the license requires installation of SLAC before use.</li> </ul>

### show license summary (Cisco Catalyst 9500 Series Switches)

The following is sample output of the **show license summary** command, on a product instance where the software version is Cisco IOS XE Cupertino 17.7.1. Note the account information fields displayed from this release onwards:

```
Device# show license summary
```

```
Account Information:
  Smart Account: Eg-SA
  Virtual Account: Eg-VA
```

```
License Usage:
```

License	Entitlement Tag	Count	Status
network-advantage_250M	(ESR_P_250M_A)	1	IN USE
dna-advantage_250M	(DNA_P_250M_A)	1	IN USE

### show license summary (Cisco Catalyst 9300X Series Switches)

The following are sample outputs of the **show license summary** command, on a C9300X stack.

The Status and Count columns here, display `NOT IN USE` and `0` for the HSECK9 key. This means the HSECK9 key is available and SLAC is installed, but the cryptographic feature that requires the license is not configured:

```
Device# show license summary
```

```
License Usage:
```

License	Entitlement Tag	Count	Status
network-advantage	(C9300-24 Network Advan...)	1	IN USE
dna-advantage	(C9300-24 DNA Advantage)	1	IN USE
network-advantage	(C9300-48 Network Advan...)	2	IN USE
dna-advantage	(C9300-48 DNA Advantage)	2	IN USE
<b>C9K HSEC</b>	<b>(Cat9K HSEC)</b>	<b>0</b>	<b>NOT IN USE</b>

The Status and Count columns here display `IN USE` and `1` for the HSECK9 key. This means the cryptographic feature, which requires an HSECK9 key, is configured.

```
Device# show license summary
```

```
License Usage:
```

## show license summary

License	Entitlement Tag	Count	Status
network-advantage	(C9300-24 Network Advan...)	1	IN USE
dna-advantage	(C9300-24 DNA Advantage)	1	IN USE
network-advantage	(C9300-48 Network Advan...)	2	IN USE
dna-advantage	(C9300-48 DNA Advantage)	2	IN USE
<b>hseck9</b>	<b>(Cat9K HSEC)</b>	<b>1</b>	<b>IN USE</b>

## show license tech

To display licensing information to help the technical support team troubleshoot a problem, enter the **show license tech** command in privileged EXEC mode. The output for this command includes outputs of several other **show license** commands and more.

```
show license tech { message | rum { feature { license_name | all } | id { rum_id | all } } [ detail ] [ save_path ] | support }
```

Syntax Description	message	rum { feature { license_name   all }   id { rum_id   all } } [ detail ] [ save_path ]	support
	Displays messages concerning trust establishment, usage reporting, result polling, authorization code requests and returns, and trust synchronization.  This is the same information as displayed in the output of the <b>show license history message</b> command.	Displays information about Resource Utilization Measurement reports (RUM reports) on the product instance, including report IDs, the current processing state of a report, error information (if any), and an option save the displayed RUM report information.  <b>Note</b> This option saves the information <i>about</i> RUM reports and is not for reporting purposes. It does not save the RUM report, which is an XML file containing usage information.	Displays licensing information that helps the technical support team to debug a problem.

**Command Modes** Privileged EXEC (Device#)

Command History	Release	Modification
	Cisco IOS XE Fuji 16.9.1	This command was introduced.
	Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy.

Release	Modification
Cisco IOS XE Cupertino 17.7.1	<p>The <b>rum</b> keyword and additional options under this keyword were added:</p> <pre>{ feature { license_name   all }   id { rum_id   all } }</pre> <p>The output of the <b>show license tech support</b> command was enhanced to display the following information:</p> <ul style="list-style-type: none"> <li>• RUM report information, in section <code>License Usage</code> and <code>Usage Report Summary</code>.</li> <li>• Smart Account and Virtual account information, in section <code>Account Information</code>.</li> </ul> <p>The <b>data conversion</b>, <b>eventlog</b> and <b>reservation</b> keywords were removed from this command. They continue to be available as separate show commands, that is, <b>show license data</b>, <b>show license eventlog</b>, and <b>show license reservation</b> respectively.</p>

## Usage Guidelines

**Smart Licensing:** If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing (whether smart licensing is enabled, all associated licensing certificates, compliance status, and so on).

**Smart Licensing Using Policy:** If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

- Troubleshooting with a Support Representative

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra all** privileged EXEC commands.

- RUM Report Information in the output
  - The output of the **show license tech support** command displays the following sections pertaining to RUM reports:

[Table 12: show license tech support: Field Descriptions for Header "License Usage", on page 172](#)

```
License Usage
=====
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 1
    Current Report: 1574560510          Previous: 1574560508
```

**Table 12: show license tech support: Field Descriptions for Header "License Usage"**

Field Name	Description
Interval:	This is a fixed measurement duration and is always 15 minutes.
Current Value:	Information about the current license count.

Field Name	Description
Current Report:	ID of the currently OPEN report for the license.
Previous:	ID of the last OPEN report for the license. This report will have state CLOSED now.

Table 13: show license tech support: Field Descriptions for Header "Usage Report Summary", on page 173

```
Usage Report Summary:
=====
Total: 26, Purged: 0(0)
Total Acknowledged Received: 0, Waiting for Ack: 0(26)
Available to Report: 26 Collecting Data: 2
Maximum Display: 26 In Storage: 26, MIA: 0(0)
```

Table 13: show license tech support: Field Descriptions for Header "Usage Report Summary"

Field Name	Description
Total:	Total number of reports that the product instance has ever generated.  <b>Note</b> This total does not refer to the total number of reports <i>currently available</i> on and being tracked by the product instance. For this you must sum up the <code>Total Acknowledged Received:</code> and <code>Available to Report</code> fields.
Purged:	The number of reports deleted due to a system resource limitation. This number includes RUM reports where the product instance no longer has tracking information.
Total Acknowledged Received:	The number of RUM reports acknowledged on this product instance.
Waiting for Ack:	The number of RUM reports waiting for an ACK. This is the total number of reports in an <code>UNACK</code> state, where the product instance still has tracking information.
Available to Report:	The number of RUM reports that are available to send to CSSM. This is the total number of reports in an <code>OPEN</code> or <code>CLOSED</code> state, where the product instance still has tracking information.
Collecting Data:	Number of reports where the product instance is currently collecting measurements.
Maximum Display:	Number of reports available for display in a <code>show</code> command's output.
In Storage:	Number of reports currently stored on the disk
MIA:	The number of reports missing.

- The output of the **show license tech rum** command displays the following fields pertaining to RUM reports: [Table 14: show license tech rum: Field Descriptions for Header "Smart Licensing Usage Report Detail", on page 174](#)

The options available under the **show license tech rum** keyword are the same as the options available with the **show license rum** privileged EXEC command. The sample output that is displayed in the *simplified view* is also the same. But if you use the **detail** keyword (for example if you enter **show license tech rum feature license\_name detail**), the detailed view is displayed and this has a few *additional* fields when compared to **show license rum**.

```
Smart Licensing Usage Report Detail:
=====
Report Id: 1574560509
  Metric Name: ENTITLEMENT
  Feature Name: dna-advantage
  Metric Value:
regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9
  UDI: PID:C9500-40X,SN:FCW2227A4NC
  Previous Report Id: 1574560507,   Next Report Id: 1574560511
Version: 2.0
  State: CLOSED,           State Change Reason: REPORTING
  Start Time: Aug 05 16:15:14 2021 EST,   End Time: Aug 05 19:38:43 2021 EST
Storage State: EXIST,   Storage State Change Reason: None
Transaction ID: 0
Transaction Message: <none>
Report Size: 1086(1202)
```

**Table 14: show license tech rum: Field Descriptions for Header "Smart Licensing Usage Report Detail"**

Field Name	Description
Version:	Displays the format of the report during transmission. Starting with Cisco IOS XE Cupertino 17.7.1, RUM reports are stored in a new format that reduces processing time. This field indicates if the product instance is using the old format or the new format.
Storage State:	Indicates if a given report is currently in storage. In addition to the displaying the current storage state of the RUM report, with these possible values: EXIST, DELETED, PURGED, MISSING, if a "(1)" is displayed next to the label (Storage State (1)), this means the RUM report is in the older (pre-17.7.1 format) and will be processed accordingly. If the RUM report is in the new format, the field is displayed as Storage State - without any extra information.

Field Name	Description
Storage State Change Reason:	<p>Displays the reason for the change in the storage state change. Not all state changes provide a reason.</p> <ul style="list-style-type: none"> <li>• NONE: This means no reason was recorded for the the storage state change.</li> <li>• PROCESSED: This means the RUM report was deleted after CISCO has processed the data.</li> <li>• LIMIT_STORAGE: This means the RUM report was deleted because the product instance reached it's storage limit.</li> <li>• LIMIT_TIME: This means the RUM report was deleted because the report reached the persisted time limit.</li> </ul>
Transaction ID: Transaction Message:	<p>If the transaction ID displays a correlation ID and an error status is displayed, the product instance displays the error code field in this section. If there are no errors, no data is displayed here.</p>
Report Size	<p>This field displays two numbers. The first number is the size of raw report for communication, in bytes. The second number is the disk space used for saving the report, also in bytes. The second number is displayed only if report is stored in the new format.</p>

## Examples

### Example: show license tech support (Cisco Catalyst 9400 Series Switches)

The following is sample output from the **show license tech support** command on a Cisco Catalyst 9400 switch running software version Cisco IOS XE Cupertino 17.7.1. Similar output is displayed on all supported Cisco Catalyst Access, Core, and Aggregation Switches.

```
Device# show license tech support

Smart Licensing Tech Support info

Smart Licensing Status
=====

Smart Licensing is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
```

```

Status: ENABLED

Account Information:
  Smart Account: Eg-SA
  Virtual Account: Eg-VA

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Address: <empty>
    Port: <empty>
    Username: <empty>
    Password: <empty>
  Server Identity Check: True
  VRF: <empty>

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Installed On Nov 20 12:10:02 2021 PDT
  Policy name: SLE Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 111 (Customer Policy)
    Report on change (days): 111 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)

Usage Reporting:
  Last ACK received: Dec 03 12:12:10 2021 PDT
  Next ACK deadline: Feb 01 12:12:10 2022 PDT
  Reporting push interval: 30 days State(4) InPolicy(60)
  Next ACK push check: Dec 04 04:12:06 2021 PDT
  Next report push: Dec 03 20:08:05 2021 PDT
  Last report push: Dec 03 12:08:08 2021 PDT
  Last report file write: <none>

License Usage
=====
Handle: 1
  License: network-advantage
  Entitlement Tag:
  regid.2017-05.com.cisco.advantagek9-C9400,1.0_61a546cd-1037-47cb-bbe6-7cad3217a7b3
  Description: C9400 Network Advantage
  Count: 2

```



```
Version: 1.0
Status: IN USE(15)
Status time: Nov 20 19:07:28 2021 PDT
Request Time: Nov 20 19:08:05 2021 PDT
Export status: NOT RESTRICTED
Feature Name: network-advantage
Feature Description: C9400 Network Advantage
Enforcement type: NOT ENFORCED
License type: Perpetual
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 2
    Current Report: 1637348082          Previous: 1637348080
Soft Enforced: True

Handle: 2
License: dna-essentials
Entitlement Tag:
regid.2017-05.com.cisco.dna_essentials-C9400,1.0_74d47865-1bf3-4f00-a06b-edbe18b049b3
Description: C9400 DNA Essentials
Count: 1
Version: 1.0
Status: IN USE(15)
Status time: Nov 20 19:07:28 2021 PDT
Request Time: Nov 20 19:07:28 2021 PDT
Export status: NOT RESTRICTED
Feature Name: dna-essentials
Feature Description: C9400 DNA Essentials
Enforcement type: NOT ENFORCED
License type: Subscription
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 1
    Current Report: 1637348083          Previous: 1637348081
Soft Enforced: True

Handle: 7
License: air-network-advantage
Entitlement Tag:
regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896
Description: air-network-advantage
Count: 0
Version: 1.0
Status: NOT IN USE(1)
Status time: Dec 03 20:07:35 2021 PDT
Request Time: None
Export status: NOT RESTRICTED
Feature Name: air-network-advantage
Feature Description: air-network-advantage
Enforcement type: NOT ENFORCED
License type: Perpetual
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 0
    Current Report: 0          Previous: 0
Soft Enforced: True

Handle: 8
License: air-dna-advantage
Entitlement Tag: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790
```

```

Description: air-dna-advantage
Count: 0
Version: 1.0
Status: NOT IN USE(1)
Status time: Dec 03 20:07:35 2021 PDT
Request Time: None
Export status: NOT RESTRICTED
Feature Name: air-dna-advantage
Feature Description: air-dna-advantage
Enforcement type: NOT ENFORCED
License type: Subscription
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 0
    Current Report: 0      Previous: 0
  Soft Enforced: True

```

#### Product Information

```
=====
```

```
UDI: PID:C9407R,SN:FXS2119Q2U7
```

#### HA UDI List:

```

Active:PID:C9407R,SN:FXS2119Q2U7
Standby:PID:C9407R,SN:FXS2119Q2U7

```

#### Agent Version

```
=====
```

```
Smart Agent for Licensing: 5.3.16_rel/55
```

#### Upcoming Scheduled Jobs

```
=====
```

```

Current time: Dec 03 22:58:47 2021 PDT
Daily: Dec 04 19:07:31 2021 PDT (20 hours, 8 minutes, 44 seconds remaining)
Authorization Renewal: Expired Not Rescheduled
Init Flag Check: Expired Not Rescheduled
Reservation configuration mismatch between nodes in HA mode: Expired Not Rescheduled
Retrieve data processing result: Dec 04 04:12:06 2021 PDT (5 hours, 13 minutes, 19 seconds
remaining)
Start Utility Measurements: Dec 03 23:08:06 2021 PDT (9 minutes, 19 seconds remaining)
Send Utility RUM reports: Dec 04 20:08:05 2021 PDT (21 hours, 9 minutes, 18 seconds remaining)
Save unreported RUM Reports: Dec 03 23:53:16 2021 PDT (54 minutes, 29 seconds remaining)
Process Utility RUM reports: Dec 04 12:17:10 2021 PDT (13 hours, 18 minutes, 23 seconds
remaining)
Data Synchronization: Expired Not Rescheduled
External Event: Jan 19 11:53:19 2022 PDT (46 days, 12 hours, 54 minutes, 32 seconds remaining)
Operational Model: Expired Not Rescheduled

```

#### Communication Statistics:

```
=====
```

```
Communication Level Allowed: DIRECT
```

```
Overall State: <empty>
```

#### Trust Establishment:

```
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
```

```
Last Response: <none>
```

```
Failure Reason: <none>
```

```
Last Success Time: <none>
```

```
Last Failure Time: <none>
```

#### Trust Acknowledgement:

```
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
```

```
Last Response: <none>
```

```
Failure Reason: <none>
```

```
Last Success Time: <none>
```

```
Last Failure Time: <none>
```

```
Usage Reporting:
  Attempts: Total=45, Success=22, Fail=23 Ongoing Failure: Overall=1 Communication=1
  Last Response: NO REPLY on Dec 03 20:08:05 2021 PDT
  Failure Reason: <none>
  Last Success Time: Dec 03 12:08:07 2021 PDT
  Last Failure Time: Dec 03 20:08:05 2021 PDT
Result Polling:
  Attempts: Total=85, Success=25, Fail=60 Ongoing Failure: Overall=3 Communication=3
  Last Response: NO REPLY on Dec 03 20:12:19 2021 PDT
  Failure Reason: <none>
  Last Success Time: Dec 03 12:29:18 2021 PDT
  Last Failure Time: Dec 03 20:12:19 2021 PDT
Authorization Request:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Authorization Confirmation:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Authorization Return:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Trust Sync:
  Attempts: Total=5, Success=1, Fail=4 Ongoing Failure: Overall=0 Communication=0
  Last Response: OK on Nov 20 19:17:37 2021 PDT
  Failure Reason: <none>
  Last Success Time: Nov 20 19:17:37 2021 PDT
  Last Failure Time: Nov 20 19:17:02 2021 PDT
Hello Message:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>

License Certificates
=====
Production Cert: True
Not registered. No certificates installed

HA Info
=====
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless
Message Flow Allowed: False

Reservation Info
=====
License reservation: DISABLED

Overall status:
  Active: PID:C9407R,SN:FXS2119Q2U7
```

```

Reservation status: NOT INSTALLED
Request code: <none>
Last return code: <none>
Last Confirmation code: <none>
Reservation authorization code: <none>
Standby: PID:C9407R,SN:FXS2119Q2U7
Reservation status: NOT INSTALLED
Request code: <none>
Last return code: <none>
Last Confirmation code: <none>
Reservation authorization code: <none>

```

Specified license reservations:

```

Purchased Licenses:
  No Purchase Information Available

```

Usage Report Summary:

=====

```

Total: 137, Purged: 0(0)
Total Acknowledged Received: 98, Waiting for Ack: 34(39)
Available to Report: 4 Collecting Data: 2
Maximum Display: 137 In Storage: 59, MIA: 0(0)
Report Module Status: Ready

```

Other Info

=====

```

Software ID: regid.2017-05.com.cisco.C9400,v1_ad928212-d182-407e-ac85-29e213602efa
Agent State: authorized
TS enable: True
Transport: Smart
  Default URL: https://smartreceiver.cisco.com/licservice/license
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type:: Production
sizeof(char)   : 1
sizeof(int)    : 4
sizeof(long)   : 4
sizeof(char *) : 8
sizeof(time_t) : 4
sizeof(size_t) : 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: True
Message Version: 1.3
connect_info.name: <empty>
connect_info.version: <empty>
connect_info.additional: <empty>
connect_info.prod: False
connect_info.capabilities: <empty>
agent.capabilities: UTILITY, DLC, AppHA, MULTITIER, EXPORT_2, OK_TRY_AGAIN, POLICY_USAGE
Check Point Interface: True
Config Management Interface: False
License Map Interface: True
HA Interface: True
Trusted Store Interface: True
Platform Data Interface: True
Crypto Version 2 Interface: False
SAPuginMgmtInterfaceMutex: True
SAPuginMgmtIPDomainName: True
SmartTransportVRFSupport: True

```

```

SmartAgentClientWaitForServer: 2000
SmartAgentCmRetrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
SmartTransportServerIdCheck: True
SmartTransportProxySupport: True
SmartAgentPolicyDisplayFormat: 0
SmartAgentReportOnUpgrade: False
SmartAgentIndividualRUMEncrypt: 2
SmartAgentMaxRumMemory: 50
SmartAgentConcurrentThreadMax: 10
SmartAgentPolicyControllerModel: False
SmartAgentPolicyModel: True
SmartAgentFederalLicense: True
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: False
conversionAllowed: False
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
HighAvailabilityOverrideEvent: UnknownPlatformEvent
platformIndependentOverrideEvent: UnknownPlatformEvent
platformOverrideEvent: SmartAgentSystemDataListChanged
WaitForHaRole: False
standbyIsHot: True
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150
traceAlwaysOn: True
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 58 KB
P:C9407R,S:FXS2119Q2U7: P:C9407R,S:FXS2119Q2U7, state[2], Trust Data INSTALLED TrustId:412
P:C9407R,S:FXS2119Q2U7: P:C9407R,S:FXS2119Q2U7, state[2], Trust Data INSTALLED TrustId:412
Overall Trust: INSTALLED (2)
Clock sync-ed with NTP: True

Platform Provided Mapping Table
=====
C9407R: Total licenses found: 198
Enforced Licenses:
P:C9407R,S:FXS2119Q2U7:
No PD enforced licenses

```

### show license tech support for Smart Licensing Using Policy (Cisco Catalyst 9500 Series Switches)

The following is sample output from the **show license tech support** command on a Cisco Catalyst 9500 switch. Similar output is displayed on all supported Cisco Catalyst Access, Core, and Aggregation Switches.

```

Device# show license tech support
Smart Licensing Tech Support info

Smart Licensing Status
=====

Smart Licensing is ENABLED
License Reservation is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Transport Off

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Jan 27 09:49:33 2021 PST
  Reporting push interval: 30 days State(2) InPolicy(90)
  Next ACK push check: <none>
  Next report push: Oct 29 09:51:33 2020 PST
  Last report push: <none>
  Last report file write: <none>

License Usage
=====
Handle: 1
  License: network-advantage

```

```
Entitlement Tag:
regid.2017-03.com.cisco.advantagek9-Nyquist-C9500,1.0_f1563759-2e03-4a4c-bec5-5feec525a12c
Description: network-advantage
Count: 2
Version: 1.0
Status: IN USE(15)
Status time: Oct 29 09:48:54 2020 PST
Request Time: Oct 29 09:49:18 2020 PST
Export status: NOT RESTRICTED
Feature Name: network-advantage
Feature Description: network-advantage
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 2
  Soft Enforced: True

Handle: 2
License: dna-advantage
Entitlement Tag:
regid.2017-07.com.cisco.C9500-DNA-16X-A,1.0_ef3574d1-156b-486a-864f-9f779ff3ee49
Description: C9500-16X DNA Advantage
Count: 2
Version: 1.0
Status: IN USE(15)
Status time: Oct 29 09:48:54 2020 PST
Request Time: Oct 29 09:49:18 2020 PST
Export status: NOT RESTRICTED
Feature Name: dna-advantage
Feature Description: C9500-16X DNA Advantage
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 2
  Soft Enforced: True

Handle: 7
License: air-network-advantage
Entitlement Tag:
regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896
Description: air-network-advantage
Count: 0
Version: 1.0
Status: IN USE(15)
Status time: Oct 29 10:49:09 2020 PST
Request Time: None
Export status: NOT RESTRICTED
Feature Name: air-network-advantage
Feature Description: air-network-advantage
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 0
  Soft Enforced: True

Handle: 8
License: air-dna-advantage
Entitlement Tag: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790

Description: air-dna-advantage
Count: 0
Version: 1.0
Status: IN USE(15)
Status time: Oct 29 10:49:09 2020 PST
```

```

Request Time: None
Export status: NOT RESTRICTED
Feature Name: air-dna-advantage
Feature Description: air-dna-advantage
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 0
    Soft Enforced: True

Product Information
=====
UDI: PID:C9500-16X,SN:FCW2233A5ZV

HA UDI List:
  Active:PID:C9500-16X,SN:FCW2233A5ZV
  Standby:PID:C9500-16X,SN:FCW2233A5ZY

Agent Version
=====
Smart Agent for Licensing: 5.0.5_rel/42

Upcoming Scheduled Jobs
=====
Current time: Oct 29 11:04:46 2020 PST
Daily: Oct 30 09:48:56 2020 PST (22 hours, 44 minutes, 10 seconds remaining)
Init Flag Check: Expired Not Rescheduled
Reservation configuration mismatch between nodes in HA mode: Nov 05 09:52:25 2020 PST (6
days, 22 hours, 47 minutes, 39 seconds remaining)
Start Utility Measurements: Oct 29 11:19:09 2020 PST (14 minutes, 23 seconds remaining)
Send Utility RUM reports: Oct 30 09:53:10 2020 PST (22 hours, 48 minutes, 24 seconds
remaining)
Save unreported RUM Reports: Oct 29 12:04:19 2020 PST (59 minutes, 33 seconds remaining)
Process Utility RUM reports: Oct 30 09:49:33 2020 PST (22 hours, 44 minutes, 47 seconds
remaining)
Data Synchronization: Expired Not Rescheduled
External Event: Nov 28 09:49:33 2020 PST (29 days, 22 hours, 44 minutes, 47 seconds remaining)
Operational Model: Expired Not Rescheduled

Communication Statistics:
=====
Communication Level Allowed: INDIRECT
Overall State: <empty>
Trust Establishment:
  Attempts: Total=0, Success=0, Fail=0   Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Trust Acknowledgement:
  Attempts: Total=0, Success=0, Fail=0   Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Usage Reporting:
  Attempts: Total=0, Success=0, Fail=0   Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Result Polling:
  Attempts: Total=0, Success=0, Fail=0   Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>

```



```

    Failure Reason: <none>
    Last Success Time: <none>
    Last Failure Time: <none>
Authorization Request:
    Attempts: Total=0, Success=0, Fail=0   Ongoing Failure: Overall=0 Communication=0
    Last Response: <none>
    Failure Reason: <none>
    Last Success Time: <none>
    Last Failure Time: <none>
Authorization Confirmation:
    Attempts: Total=0, Success=0, Fail=0   Ongoing Failure: Overall=0 Communication=0
    Last Response: <none>
    Failure Reason: <none>
    Last Success Time: <none>
    Last Failure Time: <none>
Authorization Return:
    Attempts: Total=0, Success=0, Fail=0   Ongoing Failure: Overall=0 Communication=0
    Last Response: <none>
    Failure Reason: <none>
    Last Success Time: <none>
    Last Failure Time: <none>
Trust Sync:
    Attempts: Total=0, Success=0, Fail=0   Ongoing Failure: Overall=0 Communication=0
    Last Response: <none>
    Failure Reason: <none>
    Last Success Time: <none>
    Last Failure Time: <none>
Hello Message:
    Attempts: Total=0, Success=0, Fail=0   Ongoing Failure: Overall=0 Communication=0
    Last Response: <none>
    Failure Reason: <none>
    Last Success Time: <none>
    Last Failure Time: <none>

```

```

License Certificates
=====
Production Cert: True
Not registered. No certificates installed

```

```

HA Info
=====
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless
Message Flow Allowed: False

```

```

Reservation Info
=====
License reservation: ENABLED

```

```

Overall status:
  Active: PID:C9500-16X,SN:FCW2233A5ZV
    Reservation status: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
    Request code: <none>
    Last return code: <none>
    Last Confirmation code: 184ba6d6
    Reservation authorization code:

```

```

<tagDisplayName>C9500 Network</tagDisplayName><tagDescription>C9500 Network
Network Advantage</displayName><tagDescription>C9500 Network

```

## show license tech

```

Standby: PID:C9500-16X,SN:FCW2233A5ZY
Reservation status: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
Request code: <none>
Last return code: <none>
Last Confirmation code: 961d598f
Reservation authorization code:
Network Advantage</displayName><tagDescription>C9500 Network

```

## Specified license reservations:

```

C9500 Network Advantage (C9500 Network Advantage):
Description: C9500 Network Advantage
Total reserved count: 2
Enforcement type: NOT ENFORCED
Term information:
  Active: PID:C9500-16X,SN:FCW2233A5ZV
  Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
  License type: PERPETUAL
  Start Date: <none>
  End Date: <none>
  Term Count: 1
  Subscription ID: <none>
  Standby: PID:C9500-16X,SN:FCW2233A5ZY
  Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
  License type: PERPETUAL
  Start Date: <none>
  End Date: <none>
  Term Count: 1
  Subscription ID: <none>
C9500-DNA-16X-A (C9500-16X DNA Advantage):
Description: C9500-DNA-16X-A
Total reserved count: 2
Enforcement type: NOT ENFORCED
Term information:
  Active: PID:C9500-16X,SN:FCW2233A5ZV
  Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
  License type: PERPETUAL
  Start Date: <none>
  End Date: <none>
  Term Count: 1
  Subscription ID: <none>
  Standby: PID:C9500-16X,SN:FCW2233A5ZY
  Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
  License type: PERPETUAL
  Start Date: <none>
  End Date: <none>
  Term Count: 1
  Subscription ID: <none>

```

## Purchased Licenses:

```
No Purchase Information Available
```

## Other Info

```
=====
```

```

Software ID: regid.2017-05.com.cisco.C9500,v1_7435cf27-0075-4bfb-b67c-b42f3054e82a
Agent State: authorized
TS enable: True
Transport: Transport Off
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True

```

```
Privacy Send IP: True
Build type:: Production
sizeof(char) : 1
sizeof(int) : 4
sizeof(long) : 4
sizeof(char *): 8
sizeof(time_t): 4
sizeof(size_t): 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: False
Message Version: 1.3
connect_info.name: <empty>
connect_info.version: <empty>
connect_info.additional: <empty>
connect_info.prod: False
connect_info.capabilities: <empty>
agent.capabilities: UTILITY, DLC, AppHA, MULTITIER, EXPORT_2, OK_TRY_AGAIN, POLICY_USAGE
Check Point Interface: True
Config Management Interface: False
License Map Interface: True
HA Interface: True
Trusted Store Interface: True
Platform Data Interface: True
Crypto Version 2 Interface: False
SAPPluginMgmtInterfaceMutex: True
SAPPluginMgmtIPDomainName: True
SmartAgentClientWaitForServer: 2000
SmartAgentCmRetrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
SmartTransportServerIdCheck: False
SmartTransportProxySupport: False
SmartAgentMaxRumMemory: 50
SmartAgentConcurrentThreadMax: 10
SmartAgentPolicyControllerModel: False
SmartAgentPolicyModel: True
SmartAgentFederalLicense: True
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: False
conversionAllowed: False
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
HighAvailabilityOverrideEvent: UnknownPlatformEvent
platformIndependentOverrideEvent: UnknownPlatformEvent
platformOverrideEvent: SmartAgentSystemDataListChanged
WaitForHaRole: False
standbyIsHot: True
chkPtType: 2
delayCommInit: False
```

```
roleByEvent: True
maxTraceLength: 150
traceAlwaysOn: True
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 109 KB
P:C9500-16X,S:FCW2233A5ZV: No Trust Data
P:C9500-16X,S:FCW2233A5ZY: No Trust Data
Overall Trust: No ID
```

Platform Provided Mapping Table

```
=====
C9500-16X: Total licenses found: 143
Enforced Licenses:
P:C9500-16X,S:FCW2233A5ZV:
  No PD enforced licenses
P:C9500-16X,S:FCW2233A5ZY:
  No PD enforced licenses
```

# show license udi

To display Unique Device Identifier (UDI) information for a product instance, enter the **show license udi** command in Privileged EXEC mode. In a High Availability set-up, the output displays UDI information for all connected product instances.

## show license udi

### Syntax Description

This command has no arguments or keywords.

### Command Default

Privileged EXEC (#)

### Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	The command continues to be available and applicable in the Smart Licensing Using Policy environment.

### Usage Guidelines

**Smart Licensing:** If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

**Smart Licensing Using Policy:** If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

In a High Availability or stacking set-up, the output of the **show license udi** command displays the UDI information for all connected product instances.

### Examples

[show licensing udi for Smart Licensing Using Policy, on page 189](#)

[show license udi for Smart Licensing, on page 189](#)

#### show licensing udi for Smart Licensing Using Policy

The following is sample output of the **show license udi** command for a High Availability set-up on a Catalyst 9500 switch. Similar output is displayed on all supported Cisco Catalyst Access, Core, and Aggregation Switches.

```
Device# show license udi

UDI: PID:C9500-16X,SN:FCW2233A5ZV
HA UDI List:
Active:PID:C9500-16X,SN:FCW2233A5ZV
Standby:PID:C9500-16X,SN:FCW2233A5ZY
```

#### show license udi for Smart Licensing

The following is sample output of the **show license udi** command:

```
Device# show license udi
UDI: PID:C9300-24U,SN:FCW2125L046
```

```
HA UDI List:  
Active:PID:C9300-24U,SN:FCW2125L046  
Standby:PID:C9300-24U,SN:FCW2125L03U  
Member:PID:C9300-24U,SN:FCW2125G01T
```

# show license usage

To display license usage information such as status, a count of licenses being used, and enforcement type, enter the **show license usage** command in privileged EXEC mode.

## show license usage

This command has no arguments or keywords.

### Command Default

Privileged EXEC (#)

### Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. This includes the <code>Status</code> , <code>Enforcement type</code> fields.  Command output was also updated to remove reservation related information, authorization status information, and export status information.

### Usage Guidelines

**Smart Licensing:** If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

**Smart Licensing Using Policy:** If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

#### License status

- The **unenforced licenses** that are available on Cisco Catalyst Access, Core, and Aggregation Switches are `never NOT AUTHORIZED OR NOT IN USE`.
- The **export-controlled license**, Export Control Key for High Security (HSECK9 key), which is supported on the switches listed below, displays status `NOT IN USE` if an HSECK9 key is available on the product instance and the requisite Smart Licensing Authorization Code (SLAC) is installed, but the cryptographic feature that requires the HSECK9 key is not configured.
  - Cisco Catalyst 9300X Series Switches, from Cisco IOS XE Bengaluru 17.6.2
  - Cisco Catalyst 9600 Series 40-Port 50G, 2-Port 200G, 2-Port 400G Line Card (C9600-LC-40YL4CD) from Cisco IOS XE Cupertino 17.8.1
  - Cisco Catalyst 9500X Series Switches from Cisco IOS XE Cupertino 17.8.1

Configure the applicable cryptographic feature for the count and status fields to change to 1 and `IN USE` respectively.

#### Usage Count

In a stacking setup, even if you install SLAC on more than one device, the usage count remains 1. This is because only one HSECK9 key is used at a given point in time - the one on the active. The license on the

standby comes into effect when a switchover occurs. The count remains 1 with the new active as well, because it is still only one HSECK9 key that is being used.

In case of a modular chassis, the usage count must display only 1 because only one HSECK9 key is required for each chassis UDI - regardless of the number of supervisors installed.

### Examples

See [Table 15: show license usage Field Descriptions for Smart Licensing Using Policy, on page 192](#) for information about fields shown in the display.

[show license usage for Smart Licensing Using Policy, on page 193](#)

[show license usage for Smart Licensing, on page 193](#)

**Table 15: show license usage Field Descriptions for Smart Licensing Using Policy**

Field	Description
License Authorization: Status:	Displays overall authorization status.
():	Name of the license as in CSSM. If this license is one that requires an authorization code, the name of the license includes the code.
Description	Description of the license as in CSSM.
Count	License count. If the license is not in-use, the count is reflected as zero.
Version	Version.
Status	License status can be one of the following <ul style="list-style-type: none"> <li>• In-Use: Valid license, and in-use.</li> <li>• Not In-Use: An HSECK9 key is available on the product instance and a Smart Licensing Authorization Code (SLAC) is installed, but the key that requires the HSECK9 key is disabled or not configured. This status is a prerequisite when you want to <i>return</i> the SLAC for use to CSSM.</li> <li>• Not Authorized: The license requires installation of a SLAC before use.</li> </ul>
Export Status:	Indicates if the license is export-controlled or not. Accordingly, one of the following is displayed: <ul style="list-style-type: none"> <li>• RESTRICTED - ALLOWED</li> <li>• RESTRICTED - NOT ALLOWED</li> <li>• NOT RESTRICTED</li> </ul>
Feature name	Name of the feature that uses this license.



Field	Description
Feature Description:	Description of the feature that uses this license.
Utility Subscription id:	ID Not applicable, because the corresponding configuration option is not
Enforcement type	Enforcement type status for the license. This may be one of the following: <ul style="list-style-type: none"> <li>• ENFORCED: A license, which requires authorization before use.</li> <li>• NOT ENFORCED: A license, which does not require authorization.</li> <li>• EXPORT RESTRICTED - ALLOWED: An export-controlled license that requires authorization, that is, a SLAC is installed.</li> <li>• EXPORT RESTRICTED - NOT ALLOWED: An export-controlled license that does not require the required authorization. An export-controlled license requires use.</li> </ul>

### show license usage for Smart Licensing Using Policy

The following is sample output of the **show license usage** command on a Cisco Catalyst 9500 switch. Unenforced licenses are in-use here. Similar output is displayed on all supported Cisco Catalyst Access, Core, and Aggregation Switches.

```
Device# show license usage
License Authorization:
  Status: Not Applicable
network-advantage (C9500 Network Advantage):
  Description: network-advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
dna-advantage (C9500-16X DNA Advantage):
  Description: C9500-16X DNA Advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9500-16X DNA Advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription
```

### show license usage for Smart Licensing

This example shows a sample output from the **show license usage** command:

```
Device# show license usage
License Authorization:
  Status: AUTHORIZED on Jul 17 09:47:28 2018 EDT

C9300 DNA Advantage (C9300-24 DNA Advantage):
```

**show license usage**

```

Description: C9300-24P DNA Advantage
Count: 3
Version: 1.0
Status: AUTHORIZED

```

```

C9300 Network Advantage (C9300-24 Network Advantage):
Description: C9300-24P Network Advantage
Count: 3
Version: 1.0
Status: AUTHORIZED

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show license all</b>	Displays entitlements information.
<b>show license status</b>	Displays compliance status of a license.
<b>show license summary</b>	Displays summary of all active licenses.
<b>show license udi</b>	Displays UDI.
<b>show tech-support license</b>	Displays the debug output.

# show location

To display location information for an endpoint, use the **show location** command in privileged EXEC mode.

## show location

```
[{admin-tag | civic-location{identifier identifier-string | interface type number | static} |
custom-location{identifier identifier-string | interface type number | static} | elin-location{identifier
identifier-string | interface type number | static} | geo-location{identifier identifier-string | interface
type number | static} | host}]
```

Syntax Description		
<b>admin-tag</b>		Displays administrative tag or site information.
<b>civic-location</b>		Specifies civic location information.
<b>identifier</b> <i>identifier-string</i>		Information identifier of the civic location, custom location, or geo-spatial location.
<b>interface</b> <i>type number</i>		Interface type and number.  For information about the numbering syntax for your device, use the question mark (?) online help function.
<b>static</b>		Displays configured civic, custom, or geo-spatial location information.
<b>custom-location</b>		Specifies custom location information.
<b>elin-location</b>		Specifies emergency location information (ELIN).
<b>geo-location</b>		Specifies geo-spatial location information.
<b>host</b>		Specifies the civic, custom, or geo-spatial host location information.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

The following sample output of the **show location civic-location** command displays civic location information for the specified identifier (*identifier 1*):

```
Device# show location civic-location identifier 1
Civic location information
-----
Identifier           : 1
County              : Santa Clara
Street number       : 3550
Building            : 19
Room                : C6
Primary road name   : Example
```

**show location**

```
City           : San Jose
State          : CA
Country        : US
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>location</b>	Configures location information for an endpoint.

# show logging onboard switch uptime

To display a history of all reset reasons for all modules or switches in a system, use the **show logging onboard switch uptime** command.

**show logging onboard switch** { *switch-number* | **active** | **standby** } **uptime** [ [ **continuous** | **detail** ] [ **start** *hour day month* [*year*] [ **end** *hour day month year* ] ] ] | **summary** ]

Syntax Description		
<b>switch</b> <i>switch-number</i>		Specifies a switch. Enter the switch number.
<b>active</b>		Specifies the active instance.
<b>standby</b>		Specifies the standby instance.
<b>continuous</b>		(Optional) Displays continuous data.
<b>detail</b>		(Optional) Displays detailed data.
<b>start</b> <i>hour day month year</i>		(Optional) Specifies the start time to display data.
<b>end</b> <i>hour day month year</i>		(Optional) Specifies the end time to display data.
<b>summary</b>		(Optional) Displays summary data.

**Command Modes** Privileged EXEC(#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was implemented on the Cisco Catalyst 9300 Series Switches
	Cisco IOS XE Gibraltar 16.10.1	The output of this command was updated to display the reload reasons for members in a stack.

## Examples:

The following is a sample output from the **show logging onboard switch active uptime continuous** command:

```
Device# show logging onboard switch active uptime continuous
-----
UPTIME CONTINUOUS INFORMATION
-----
Time Stamp          | Reset              | Uptime
MM/DD/YYYY HH:MM:SS | Reason            | years weeks days hours minutes
-----
06/17/2018 19:42:56 | Reload            | 0   0   0   0   5
06/17/2018 19:56:31 | Reload            | 0   0   0   0   5
06/17/2018 20:10:46 | Reload            | 0   0   0   0   5
06/17/2018 20:23:48 | Reload            | 0   0   0   0   5
06/17/2018 20:37:20 | Reload Command    | 0   0   0   0   5
06/18/2018 17:09:23 | Reload Command    | 0   0   0   20  5
06/18/2018 17:18:39 | redundancy force-switchover | 0   0   0   0   5
06/18/2018 18:33:33 | Reload            | 0   0   0   1   5
06/18/2018 19:03:05 | Reload            | 0   0   0   0   5
```

## show logging onboard switch uptime

```

06/18/2018 19:40:30 Reload 0 0 0 0 5
06/18/2018 20:37:47 Reload 0 0 0 0 5
06/18/2018 20:51:13 Reload 0 0 0 0 5
06/18/2018 21:04:08 Reload 0 0 0 0 5
06/18/2018 21:18:23 Reload 0 0 0 0 5
06/18/2018 21:31:25 Reload 0 0 0 0 5
06/18/2018 21:45:15 Reload 0 0 0 0 5
06/18/2018 21:59:02 Reload 0 0 0 0 5
06/18/2018 22:11:41 Reload 0 0 0 0 5
06/18/2018 22:24:27 Reload 0 0 0 0 5
06/18/2018 22:39:14 Reload Command 0 0 0 0 4
06/19/2018 00:01:59 Reload Command 0 0 0 1 5
06/19/2018 00:13:21 redundancy force-switchover 0 0 0 0 5
06/19/2018 01:05:42 redundancy force-switchover 0 0 0 0 5
06/20/2018 02:37:16 redundancy force-switchover 0 0 1 1 5
06/20/2018 02:50:03 redundancy force-switchover 0 0 0 0 5
06/20/2018 03:02:13 redundancy force-switchover 0 0 0 0 5
06/20/2018 03:14:26 redundancy force-switchover 0 0 0 0 5
06/20/2018 03:26:44 redundancy force-switchover 0 0 0 0 5
06/20/2018 03:38:58 redundancy force-switchover 0 0 0 0 5
06/20/2018 03:52:43 redundancy force-switchover 0 0 0 0 5
06/20/2018 04:05:16 redundancy force-switchover 0 0 0 0 5
.
.
.

```

The following is a sample output from the **show logging onboard switch active uptime detail** command:

```
Device# show logging onboard switch active uptime detail
```

```
-----
UPTIME SUMMARY INFORMATION
-----
```

```

First customer power on : 06/10/2017 09:28:22
Total uptime           : 0 years 50 weeks 4 days 13 hours 38 minutes
Total downtime        : 0 years 15 weeks 4 days 11 hours 52 minutes
Number of resets       : 75
Number of slot changes : 9
Current reset reason   : PowerOn
Current reset timestamp : 09/17/2018 10:59:57
Current slot           : 1
Chassis type           : 0
Current uptime         : 0 years 0 weeks 0 days 0 hours 0 minutes
-----

```

```
-----
UPTIME CONTINUOUS INFORMATION
-----
```

Time Stamp	Reset Reason	Uptime
MM/DD/YYYY HH:MM:SS	Reason	years weeks days hours minutes
06/10/2017 09:28:22	Reload	0 0 0 0 0
<snip>		
09/17/2018 09:07:44	PowerOn	0 0 3 15 5
09/17/2018 10:16:26	Reload Command	0 0 0 1 5
09/17/2018 10:59:57	PowerOn	0 0 0 0 5

The following is a sample output from the **show logging onboard switch standby uptime detail** command:

```
Device# show logging onboard switch standby uptime detail
```

```
-----
UPTIME SUMMARY INFORMATION
-----
```

```

First customer power on : 06/10/2017 11:51:26
Total uptime           : 0 years 46 weeks 0 days 11 hours 44 minutes
Total downtime        : 0 years 20 weeks 1 days 10 hours 45 minutes
Number of resets       : 79
Number of slot changes : 13
Current reset reason   : PowerOn
Current reset timestamp : 09/17/2018 10:59:57
Current slot           : 2
Chassis type           : 0
Current uptime         : 0 years 0 weeks 0 days 0 hours 5 minutes

```

---

UPTIME CONTINUOUS INFORMATION

---

Time Stamp	Reset	Uptime
MM/DD/YYYY HH:MM:SS	Reason	years weeks days hours minutes
06/10/2017 11:51:26	Reload	0 0 0 0 0
<snip>		
08/10/2018 09:13:58	LocalSoft	0 0 2 5 4
08/28/2018 14:21:42	Reload Slot Command	0 0 0 3 5
08/28/2018 14:34:29	System requested reload	0 0 0 0 0
09/11/2018 09:08:15	Reload	0 0 1 8 5
09/11/2018 19:15:06	redundancy force-switchover	0 0 0 9 4
09/13/2018 16:50:18	Reload Command	0 0 1 21 6
09/17/2018 10:55:09	PowerOn	0 0 0 0 5

The following is a sample output from the **show logging onboard switch active uptime summary** command:

```
Device# show logging onboard switch active uptime summary
```

---

UPTIME SUMMARY INFORMATION

---

```

First customer power on : 04/26/2018 21:45:39
Total uptime           : 0 years 20 weeks 2 days 12 hours 22 minutes
Total downtime        : 0 years 2 weeks 2 days 8 hours 40 minutes
Number of resets       : 1900
Number of slot changes : 18
Current reset reason   : Reload Command
Current reset timestamp : 09/26/2018 20:43:15
Current slot           : 1
Chassis type           : 91
Current uptime         : 0 years 0 weeks 5 days 22 hours 5 minutes

```

# show logging process ios module

To display btrace logs for an IOS module, use the **show logging process ios module** command in the EXEC mode.

**show logging process ios module** *module-name*

<b>Syntax Description</b>	<i>module-name</i> Displays the logs for the specified IOS module.
---------------------------	--

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

## Usage Guidelines

The following example shows how to display the logs for the IPSLA Sender module:

```
Device# show logging process ios module ipsla_s
Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
executing cmd on chassis local ...
Collecting files on current[local] chassis.
# of files collected = 2

2019/10/07 09:07:47.799791 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [1000] Starting
echo operation
2019/10/07 09:07:47.799840 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [1000] Starting
control phase
2019/10/07 09:07:47.803366 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [1000] Socket setup
& registered with XDM - fd: 0
2019/10/07 09:07:47.804934 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): Socket send udp-echo
packet
2019/10/07 09:07:47.804982 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [1000] Socket send
successful - fd: 0
2019/10/07 09:07:47.805009 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [udp-echo:1000]
Received response SendTime=32867803, RecvTime=32867804, delta=0
2019/10/07 09:07:47.805035 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [udp-echo:1000]
Probe successful - RTT: 1
2019/10/07 09:08:17.800477 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [1000] Starting
echo operation
2019/10/07 09:08:17.800527 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [1000] Starting
control phase
2019/10/07 09:08:17.803028 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [1000] Socket setup
& registered with XDM - fd: 0
2019/10/07 09:08:17.803141 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): Socket send udp-echo
packet
2019/10/07 09:08:17.803186 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [1000] Socket send
successful - fd: 0
2019/10/07 09:08:17.804660 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [udp-echo:1000]
Received response SendTime=32897803, RecvTime=32897804, delta=0
2019/10/07 09:08:17.804696 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [udp-echo:1000]
```



```

Probe successful - RTT: 1
2019/10/07 09:08:47.799809 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [1000] Starting
echo operation
2019/10/07 09:08:47.799865 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [1000] Starting
control phase
2019/10/07 09:08:47.802108 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [1000] Socket setup
& registered with XDM - fd: 0
2019/10/07 09:08:47.802284 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): Socket send udp-echo
packet
2019/10/07 09:08:47.802376 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [1000] Socket send
successful - fd: 0
2019/10/07 09:08:47.803603 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [udp-echo:1000]
Received response SendTime=32927802, RecvTime=32927803, delta=0
2019/10/07 09:08:47.803679 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [udp-echo:1000]
Probe successful - RTT: 1
2019/10/07 09:09:17.800297 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [1000] Starting
echo operation
2019/10/07 09:09:17.800341 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [1000] Starting
control phase
2019/10/07 09:09:17.802882 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [1000] Socket setup
& registered with XDM - fd: 0
2019/10/07 09:09:17.803079 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): Socket send udp-echo
packet
2019/10/07 09:09:17.803111 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [1000] Socket send
successful - fd: 0
2019/10/07 09:09:17.804366 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [udp-echo:1000]
Received response SendTime=32957803, RecvTime=32957803, delta=0
2019/10/07 09:09:17.804407 {IOSRP_R0-0}{1}: [ipsla_s] [917]: (note): [udp-echo:1000]
Probe successful - RTT: 1

```

The following example shows how to display the logs for the IPSLA Responder module:

```

Device#show logging process ios module ipsla_r
Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
executing cmd on chassis local ...
Collecting files on current[local] chassis.
# of files collected = 2

2019/10/07 09:08:25.843000 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): [192.168.12.1:64446]
Received Control message with len: 52
2019/10/07 09:08:25.843078 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): [192.168.12.1:64446]
table_id from the pktinfo
2019/10/07 09:08:25.843105 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): Ctrl-Msg Ver: 1 ID:
18 Len: 52
2019/10/07 09:08:25.843209 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): [192.168.12.1:64446]
Sending control response message back to the client with status (0) length (24)
2019/10/07 09:08:55.843812 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): [192.168.12.1:52445]
Received Control message with len: 52
2019/10/07 09:08:55.843889 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): [192.168.12.1:52445]
table_id from the pktinfo
2019/10/07 09:08:55.843917 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): Ctrl-Msg Ver: 1 ID:
19 Len: 52
2019/10/07 09:08:55.844028 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): [192.168.12.1:52445]
Sending control response message back to the client with status (0) length (24)
2019/10/07 09:09:25.843451 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): [192.168.12.1:53546]
Received Control message with len: 52
2019/10/07 09:09:25.843531 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): [192.168.12.1:53546]
table_id from the pktinfo
2019/10/07 09:09:25.843559 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): Ctrl-Msg Ver: 1 ID:
20 Len: 52
2019/10/07 09:09:25.843672 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): [192.168.12.1:53546]
Sending control response message back to the client with status (0) length (24)

```

## show logging process ios module

```
2019/10/07 09:09:55.844054 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): [192.168.12.1:60976]
Received Control message with len: 52
2019/10/07 09:09:55.844113 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): [192.168.12.1:60976]
table_id from the pktinfo
2019/10/07 09:09:55.844141 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): Ctrl-Msg Ver: 1 ID:
21 Len: 52
2019/10/07 09:09:55.844257 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): [192.168.12.1:60976]
Sending control response message back to the client with status (0) length (24)
2019/10/07 09:10:25.843479 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): [192.168.12.1:50769]
Received Control message with len: 52
2019/10/07 09:10:25.843535 {IOSRP_R0-0}{1}: [ipsla_r] [641]: (note): [192.168.12.1:50769]
table_id from the pktinfo
```

## show mac address-table

To display the MAC address table, use the **show mac address-table** command in privileged EXEC mode.

```
show mac address-table [{ address mac-addr [ interface type/number | vlan vlan-id ] | aging-time
[ routed-mac | vlan vlan-id ] | control-packet-learn | count [ summary | vlan vlan-id ] | dynamic
| secure | static ][ address mac-addr ][ interface type/number | vlan vlan-id ] | interface type/number
| learning [ vlan vlan-id ] | multicast [ count ][ igmp-snooping | mld-snooping | user ][ vlan
vlan-id ] | notification { change [ interface [ type/number ] ] | mac-move | threshold } | vlan
vlan-id }
```

Syntax	Description
<b>address</b> <i>mac-addr</i>	(Optional) Displays information about the MAC address table for a specific MAC address.
<b>interface</b> <i>type/number</i>	(Optional) Displays addresses for a specific interface.
<b>vlan</b> <i>vlan-id</i>	(Optional) Displays addresses for a specific VLAN.
<b>aging-time</b> [ <b>routed-mac</b>   <b>vlan</b> <i>vlan-id</i> ]	(Optional) Displays the aging time for the routed MAC or VLAN.
<b>control-packet-learn</b>	(Optional) Displays the controlled packet MAC learning parameters.
<b>count</b>	(Optional) Displays the number of entries that are currently in the MAC address table.
<b>dynamic</b>	(Optional) Displays only the dynamic addresses.
<b>secure</b>	(Optional) Displays only the secure addresses.
<b>static</b>	(Optional) Displays only the static addresses.
<b>learning</b>	(Optional) Displays learnings of a VLAN or interface.
<b>multicast</b>	(Optional) Displays information about the multicast MAC address table entries only.
<b>igmp-snooping</b>	(Optional) Displays the addresses learned by Internet Group Management Protocol (IGMP) snooping.
<b>mld-snooping</b>	(Optional) Displays the addresses learned by Multicast Listener Discover version 2 (MLDv2) snooping.
<b>user</b>	(Optional) Displays the manually entered (static) addresses.
<b>notification change</b>	Displays the MAC notification parameters and history table.
<b>notification mac-move</b>	Displays the MAC-move notification status.
<b>notification threshold</b>	Displays the Counter-Addressable Memory (CAM) table utilization notification status.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.
	Cisco IOS XE Gibraltar 16.12.4	The output of the <b>show mac address-table vlan <i>vlan-id</i></b> command has been updated to show the MAC addresses used for Cisco Software-Defined Access (SD-Access) solution.

**Usage Guidelines** The *mac-addr* value is a 48-bit MAC address. The valid format is H.H.H.

The interface *number* argument designates the module and port number. Valid values depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The following is sample output from the **show mac address-table** command:

```
Device# show mac address-table

          Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
All     0100.0ccc.cccc   STATIC    CPU
All     0100.0ccc.cccd   STATIC    CPU
All     0180.c200.0000   STATIC    CPU
All     0180.c200.0001   STATIC    CPU
All     0180.c200.0002   STATIC    CPU
All     0180.c200.0003   STATIC    CPU
All     0180.c200.0004   STATIC    CPU
All     0180.c200.0005   STATIC    CPU
All     0180.c200.0006   STATIC    CPU
All     0180.c200.0007   STATIC    CPU
All     0180.c200.0008   STATIC    CPU
All     0180.c200.0009   STATIC    CPU
All     0180.c200.000a   STATIC    CPU
All     0180.c200.000b   STATIC    CPU
All     0180.c200.000c   STATIC    CPU
All     0180.c200.000d   STATIC    CPU
All     0180.c200.000e   STATIC    CPU
All     0180.c200.000f   STATIC    CPU
All     0180.c200.0010   STATIC    CPU
All     0180.c200.0021   STATIC    CPU
All     ffff.ffff.ffff   STATIC    CPU
  1     780c.f0e1.1dc3   STATIC    Vl1
  51    0000.1111.2222   STATIC    Vl51
  51    780c.f0e1.1dc6   STATIC    Vl51
1021    0000.0c9f.f45c   STATIC    Vl1021
1021    0002.02cc.0002   STATIC    Gi6/0/2
1021    0002.02cc.0003   STATIC    Gi6/0/3
1021    0002.02cc.0004   STATIC    Gi6/0/4
1021    0002.02cc.0005   STATIC    Gi6/0/5
1021    0002.02cc.0006   STATIC    Gi6/0/6
1021    0002.02cc.0007   STATIC    Gi6/0/7
1021    0002.02cc.0008   STATIC    Gi6/0/8
1021    0002.02cc.0009   STATIC    Gi6/0/9
1021    0002.02cc.000a   STATIC    Gi6/0/10
```

<output truncated>

The following example shows how to display MAC address table information for a specific MAC address:

```
Device# show mac address-table address fc58.9a02.7382
```

```

          Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       fc58.9a02.7382   DYNAMIC   Te1/0/1
Total Mac Addresses for this criterion: 1

```

The following example shows how to display the currently configured aging time for a specific VLAN:

```
Device# show mac address-table aging-time vlan 1
```

```

Global Aging Time: 300
Vlan    Aging Time
----    -
1       300

```

The following example shows how to display the information about the MAC address table for a specific interface:

```
Device# show mac address-table interface TenGigabitEthernet1/0/1
```

```

          Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       fc58.9a02.7382   DYNAMIC   Te1/0/1
Total Mac Addresses for this criterion: 1

```

The following example shows how to display the MAC-move notification status:

```
Device# show mac address-table notification mac-move
```

```
MAC Move Notification: Enabled
```

The following example shows how to display the CAM-table utilization-notification status:

```
Device# show mac address-table notification threshold
```

```

      Status      limit      Interval
-----+-----+-----
enabled          50          120

```

The following example shows how to display the MAC notification parameters and history table for a specific interface:

```
Device# show mac address-table notification change interface tenGigabitEthernet1/0/1
```

```

MAC Notification Feature is Disabled on the switch
Interface                                     MAC Added Trap  MAC Removed Trap
-----

```

## show mac address-table

```
TenGigabitEthernet1/0/1      Disabled      Disabled
```

The following example shows how to display the information about the MAC-address table for a specific VLAN:



**Note** MAC addresses of the type CP\_LEARN will be displayed only if Cisco SD-Access solution is used.

```
Device# show mac address-table vlan 1021

          Mac Address Table
-----
Vlan      Mac Address      Type           Ports
----      -
1021     0000.0c9f.f45c   STATIC         Vl1021
1021     0002.02cc.0002   STATIC         Gi6/0/2
1021     0002.02cc.0003   STATIC         Gi6/0/3
1021     0002.02cc.0004   STATIC         Gi6/0/4
1021     0002.02cc.0005   STATIC         Gi6/0/5
1021     0002.02cc.0006   STATIC         Gi6/0/6
1021     0002.02cc.0007   STATIC         Gi6/0/7
1021     0002.02cc.0008   STATIC         Gi6/0/8
1021     0002.02cc.0009   STATIC         Gi6/0/9
1021     0002.02cc.000a   STATIC         Gi6/0/10
1021     0002.02cc.000b   STATIC         Gi6/0/11
1021     0002.02cc.000c   STATIC         Gi6/0/12
1021     0002.02cc.000d   STATIC         Gi6/0/13
1021     0002.02cc.000e   STATIC         Gi6/0/14
1021     0002.02cc.000f   STATIC         Gi6/0/15
1021     0002.02cc.0010   STATIC         Gi6/0/16
1021     0002.02cc.0011   STATIC         Gi6/0/17
1021     0002.02cc.0012   STATIC         Gi6/0/18
1021     0002.02cc.0013   STATIC         Gi6/0/19
1021     0002.02cc.0014   STATIC         Gi6/0/20

.
.
.

1021     0002.0100.0001   CP_LEARN       Tu0
1021     0002.0100.0002   CP_LEARN       Tu0
1021     0002.0100.0003   CP_LEARN       Tu0
1021     0002.0100.0004   CP_LEARN       Tu0
1021     0002.0100.0005   CP_LEARN       Tu0
1021     0002.0100.0006   CP_LEARN       Tu0
1021     0002.0100.0007   CP_LEARN       Tu0
1021     0002.0100.0008   CP_LEARN       Tu0
1021     0002.0100.0009   CP_LEARN       Tu0
1021     0002.0100.000a   CP_LEARN       Tu0
Total Mac Addresses for this criterion: 114
```

The table below describes the significant fields shown in the **show mac address-table** display.

*Table 16: show mac address-table Field Descriptions*

Field	Description
VLAN	VLAN number.
Mac Address	MAC address of the entry.
Type	Type of address.
Ports	Port type.
Total MAC addresses	Total MAC addresses in the MAC address table.

**Related Commands**

Command	Description
<b>clear mac address-table</b>	Deletes dynamic entries from the MAC address table.

# show mac address-table move update

To display the MAC address-table move update information on the device, use the **show mac address-table move update** command in EXEC mode.

## show mac address-table move update

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	M
	Cisco IOS XE Everest 16.5.1a	Th

## Example

This example shows the output from the **show mac address-table move update** command:

```
Device# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```



# show parser encrypt file status

To view the private configuration encryption status, use the **show parser encrypt file status** command.

## show parser encrypt file status

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** User EXEC

Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.

## Examples

The following command output indicates that the feature is available and the file is encrypted. The file is in 'cipher text' format.

```
Device> enable
Device# show parser encrypt file status
Feature:                Enabled
File Format:            Cipher text
Encryption Version:    ver1
```

## Related Commands

Command	Description
<b>service private-config-encryption</b>	Enables private configuration file encryption.

# show platform hardware fpga

To display the system field-programmable gate array (FPGA) settings, use the **show platform hardware fpga** command in privileged EXEC mode.

## show platform hardware fpga

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Fuji 16.9.1	This command was introduced.

## Example

The following is a sample output from the **show platform hardware fpga** command on a Cisco Catalyst 9300 Series switch:

```
Device# show platform hardware fpga

Register Addr          FPGA Reg Description          Value
-----
0x00000000             Board ID                      0x00006053
0x00000004             FPGA Version                  0x00000206
0x00000008             Reset Reg1                    0x00010204
0x0000000c             Reset Reg2                    0x00000000
0x00000028             FRU LED DATA Reg1          0x00001008
0x0000002c             FRU LED DATA Reg2          0x00001008
0x00000030             FRU Control Reg              0x0000c015
0x00000034             Doppler Misc Reg             0x00000311
0x00000010             SBC Enable                    0x0000000f
<snip>
```

The following is a sample output from the **show platform hardware fpga** command on a Cisco Catalyst 9500 Series switch:

```
Device# show platform hardware fpga

Register Addr          FPGA Reg Description          Value
-----
0x00000000             FPGA Version                  0x00000110
0x00000040             FRU Power Cntrl Reg          0x00000112
0x00000020             System Reset Cntrl Reg       0x00000000
0x00000024             Beacon LED Cntrl Reg         0x00000000
0x00000044             1588 Sync Pulse Reg         0x00000000
0x00000048             Mainboard Misc Cntrl Reg     0x0000000a
0x00000038             DopplerD Misc Cntrl Reg     0x000000ff
<snip>
```

# show platform integrity

To display checksum record for the boot stages , use the **show platform integrity** command in privileged EXEC mode.

```
show platform integrity [sign [nonce <nonce>]]
```

<b>Syntax Description</b>	<b>sign</b>	(Optional) Show signature
	<b>nonce</b>	(Optional) Enter a nonce value
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
		This command was introduced.

## Examples

This example shows how to view the checksum record for boot stages :

```
Device# show platform integrity sign

PCR0: EE47F8644C2887D9BD4DE3E468DD27EB93F4A606006A0B7006E2928C50C7C9AB
PCR8: E7B61EC32AFA43DA1FF4D77F108CA266848B32924834F5E41A9F6893A9CB7A38
Signature version: 1
Signature:
816C5A29741BBAC1961C109FFC36DA5459A44DBF211025F539AFB4868EF91834C05789
5DAFBC7474F301916B7D0D08ABE5E05E66598426A73E921024C21504383228B6787B74
8526A305B17DAD3CF8705BACFD51A2D55A333415CABC73DAFDEEFD8777AA77F482EC4B
731A09826A41FB3EFC46DC02FBA666534DBEC7DCC0C029298DB8462A70DBA26833C2A
1472D1F08D721BA941CB94A418E43803699174572A5759445B3564D8EAE57D64AE304
EE1D2A9C53E93E05B24A92387E261199CED8D8A0CE7134596FF8D2D6E6DA773757C70C
D3BA91C43A591268C248DF32658999276FB972153ABE823F0ACFE9F3B6F0AD1A00E257
4A4CC41C954015A59FB8FE
Platform: WS-C3650-12X48UZ
```

# show platform software audit

To display the SE Linux Audit logs, use the **show platform software audit** command in privileged EXEC mode.

```
show platform software audit {all | summary | [switch {switch-number | active | standby}]
{0 | F0 | R0 | {FP | RP} {active}}}
```

## Syntax Description

<b>all</b>	Shows the audit log from all the slots.
<b>summary</b>	Shows the audit log summary count from all the slots.
<b>switch</b>	Shows the audit logs for a slot on a specific switch.
<i>switch-number</i>	Selects the switch with the specified switch number.
<b>switch active</b>	Selects the active instance of the switch.
<b>standby</b>	Selects the standby instance of the switch.
<b>0</b>	Shows the audit log for the SPA-Inter-Processor slot 0.
<b>F0</b>	Shows the audit log for the Embedded-Service-Processor slot 0.
<b>R0</b>	Shows the audit log for the Route-Processor slot 0.
<b>FP active</b>	Shows the audit log for the active Embedded-Service-Processor slot.
<b>RP active</b>	Shows the audit log for the active Route-Processor slot.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

## Usage Guidelines

This command was introduced in the Cisco IOS XE Gibraltar 16.10.1 as a part of the SELinux Permissive Mode feature. The **show platform software audit** command displays the system logs containing the access violation events.

In Cisco IOS XE Gibraltar 16.10.1, operation in a permissive mode is available - with the intent of confining specific components (process or application) of the IOS-XE platform. In the permissive mode, access violation events are detected and system logs are generated, but the event or operation itself is not blocked. The solution operates mainly in an access violation detection mode.

The following is a sample output of the **show software platform software audit summary** command:

```
Device# show platform software audit summary
```

```
=====
AUDIT LOG ON switch 1
-----
AVC Denial count: 58
=====
```

The following is a sample output of the **show software platform software audit all** command:

```
Device# show platform software audit all
```

```
=====
AUDIT LOG ON switch 1
-----
===== START =====
type=AVC msg=audit(1539222292.584:100): avc: denied { read } for pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc: denied { getattr } for pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sdal" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc: denied { getattr } for pid=14028 comm="ls"
path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc: denied { read } for pid=14028 comm="ls"
name="crashinfo" dev="tmpfs" ino=58407 scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438600.896:119): avc: denied { execute } for pid=8300 comm="sh"
name="id" dev="loop0" ino=6982 scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:bin_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438600.897:120): avc: denied { execute_no_trans } for pid=8300
comm="sh"
path="/tmp/sw/mount/cat9k-rpbase.2018-10-02_00.13_mhungund.SSA.pkg/nyquist/usr/bin/id"
dev="loop0" ino=6982 scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:bin_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438615.535:121): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438624.916:122): avc: denied { execute_no_trans } for pid=8600
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438648.936:123): avc: denied { execute_no_trans } for pid=9307
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438678.649:124): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438696.969:125): avc: denied { execute_no_trans } for pid=10057
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438732.973:126): avc: denied { execute_no_trans } for pid=10858
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438778.008:127): avc: denied { execute_no_trans } for pid=11579
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
```

```

type=AVC msg=audit(1539438800.156:128): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438834.099:129): avc: denied { execute_no_trans } for pid=12451
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539440246.697:149): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539440299.119:150): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
===== END =====
=====

```

The following is a sample output of the **show software platform software audit switch** command:

```
Device# show platform software audit switch active R0
```

```

===== START =====
type=AVC msg=audit(1539222292.584:100): avc: denied { read } for pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc: denied { getattr } for pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc: denied { getattr } for pid=14028 comm="ls"
path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc: denied { read } for pid=14028 comm="ls"
name="crashinfo" dev="tmpfs" ino=58407 scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438624.916:122): avc: denied { execute_no_trans } for pid=8600
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438648.936:123): avc: denied { execute_no_trans } for pid=9307
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438678.649:124): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438696.969:125): avc: denied { execute_no_trans } for pid=10057
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438732.973:126): avc: denied { execute_no_trans } for pid=10858
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438778.008:127): avc: denied { execute_no_trans } for pid=11579
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438800.156:128): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438834.099:129): avc: denied { execute_no_trans } for pid=12451
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0

```

```
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438860.907:130): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
===== END =====
=====
```

## show platform software fed switch punt cause

To display information about why the packets received on an interface are punted to the Router Processor (RP), use the **show platform software fed switch punt cpuq cause** command in privileged EXEC mode.

```
show platform software fed switch {switch-number | active | standby} punt {cause_id | clear | summary}
```

### Syntax Description

<b>switch</b> { <i>switch-number</i>   <b>active</b>   <b>standby</b> }	Displays information about the switch. You have the following options: <ul style="list-style-type: none"> <li>• <i>switch-number</i>.</li> <li>• <b>active</b>—Displays information relating to the active switch.</li> <li>• <b>standby</b>—Displays information relating to the standby switch, if available.</li> </ul> <p><b>Note</b> This keyword is not supported.</p>
---	--

<i>cause_id</i>	Specifies the ID of the cause for which the details have to be displayed.
-----------------	---

<b>clear</b>	Clears the statistics for all the causes. Clearing the causes might result in inconsistent statistics.
--------------	--

<b>summary</b>	Displays a high-level overview of the punt reason.
----------------	--

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Usage Guidelines

None

### Example

The following is sample output from the **show platform software fed switch active punt cause summary** command.

```
Device# show platform software fed switch active punt cause summary
Statistics for all causes
```

Cause	Cause Info	Rcvd	Dropped
7	ARP request or response	1	0
21	RP<->QFP keepalive	22314	0
55	For-us control	12	0
60	IP subnet or broadcast packet	21	0
96	Layer2 control protocols	133808	0



-----  
The following is sample output from the **show platform software fed switch active punt cause** *cause-id* command.

Device# **show platform software fed switch active punt cause 21**  
Detailed Statistics

Sub Cause	Rcvd	Dropped
0	22363	0

# show platform software fed switch punt cpuq

To display information about the punt traffic on CPU queues, use the **show platform software fed switch punt cpuq** command in privileged EXEC mode.

**show platform software fed switch** {*switch-number* | **active** | **standby**} **punt cpuq** {*cpuq\_id* | **all** | **brief** | **clear** | **rates**}

## Syntax Description

<b>switch</b> { <i>switch-number</i> <b>active</b> <b>standby</b> }	Displays information about the switch. You have the following options: <ul style="list-style-type: none"> <li>• <i>switch-number</i>.</li> <li>• <b>active</b>—Displays information relating to the active switch.</li> <li>• <b>standby</b>—Displays information relating to the standby switch, if available.</li> </ul> <p><b>Note</b> This keyword is not supported.</p>
<b>punt</b>	Displays the punt information.
<b>cpuq</b>	Displays information about the CPU receive queue.
<i>cpuq_id</i>	Specifies details specific to a particular CPU queue.
<b>all</b>	Displays the statistics for all the CPU queues.
<b>brief</b>	Displays summarized statistics for all the queues like details about punt packets received and dropped.
<b>clear</b>	Clears the statistics for all the CPU queues. Clearing the CPU queue might result in inconsistent statistics.
<b>rates</b>	Displays the rate at which the packets are punted.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

## Usage Guidelines

None

**Example**

The following is sample output from the **show platform software fed switch active punt cpuq brief** command.

```
Device#show platform software fed switch active punt cpuq brief
```

```
Punt CPU Q Statistics Brief
```

```
=====
```

Q no	Queue Name	Rx prev	Rx cur	Rx delta	Drop prev	Drop cur	Drop delta
0	CPU_Q_DOT1X_AUTH	0	0	0	0	0	0
1	CPU_Q_L2_CONTROL	0	6772	6772	0	0	0
2	CPU_Q_FORUS_TRAFFIC	0	0	0	0	0	0
3	CPU_Q_ICMP_GEN	0	0	0	0	0	0
4	CPU_Q_ROUTING_CONTROL	0	12	12	0	0	0
5	CPU_Q_FORUS_ADDR_RESOLUTION	0	1	1	0	0	0
6	CPU_Q_ICMP_REDIRECT	0	0	0	0	0	0
7	CPU_Q_INTER_FED_TRAFFIC	0	0	0	0	0	0
8	CPU_Q_L2LVX_CONTROL_PKT	0	0	0	0	0	0
9	CPU_Q_EWLC_CONTROL	0	0	0	0	0	0
10	CPU_Q_EWLC_DATA	0	0	0	0	0	0
11	CPU_Q_L2LVX_DATA_PKT	0	0	0	0	0	0
12	CPU_Q_BROADCAST	0	21	21	0	0	0
13	CPU_Q_LEARNING_CACHE_OVFL	0	0	0	0	0	0
14	CPU_Q_SW_FORWARDING	0	0	0	0	0	0
15	CPU_Q_TOPOLOGY_CONTROL	0	127300	127300	0	0	0
16	CPU_Q_PROTO_SNOOPING	0	0	0	0	0	0
17	CPU_Q_BFD_LOW_LATENCY	0	0	0	0	0	0
18	CPU_Q_TRANSIT_TRAFFIC	0	0	0	0	0	0
19	CPU_Q_RPF_FAILED	0	0	0	0	0	0
20	CPU_Q_MCAST_END_STATION_SERVICE	0	0	0	0	0	0
21	CPU_Q_LOGGING	0	0	0	0	0	0
22	CPU_Q_PUNT_WEBAUTH	0	0	0	0	0	0
23	CPU_Q_HIGH_RATE_APP	0	0	0	0	0	0
24	CPU_Q_EXCEPTION	0	0	0	0	0	0
25	CPU_Q_SYSTEM_CRITICAL	0	0	0	0	0	0
26	CPU_Q_NFL_SAMPLED_DATA	0	0	0	0	0	0
27	CPU_Q_LOW_LATENCY	0	0	0	0	0	0
28	CPU_Q_EGR_EXCEPTION	0	0	0	0	0	0
29	CPU_Q_FSS	0	0	0	0	0	0
30	CPU_Q_MCAST_DATA	0	0	0	0	0	0
31	CPU_Q_GOLD_PKT	0	0	0	0	0	0

```
=====
```

The table below describes the significant fields shown in the display.

**Table 17: show platform software fed switch active punt cpuq brief Field Descriptions**

Field	Description
Q no	ID of the queue.
Queue Name	Name of the queue.
Rx	Number of packets received.

Field	Description
Drop	Number of packets dropped.

The following is sample output from the **show platform software fed switch active punt cpuq cpuq\_id** command.

```
Device#show platform software fed switch active punt cpuq 1
```

```
Punt CPU Q Statistics
```

```
=====
```

```
CPU Q Id                : 1
CPU Q Name              : CPU_Q_L2_CONTROL
Packets received from ASIC : 6774
Send to IOSd total attempts : 6774
Send to IOSd failed count  : 0
RX suspend count        : 0
RX unsuspend count      : 0
RX unsuspend send count  : 0
RX unsuspend send failed count : 0
RX consumed count       : 0
RX dropped count         : 0
RX non-active dropped count : 0
RX conversion failure dropped : 0
RX INTACK count         : 6761
RX packets dq'd after intack : 0
Active RxQ event        : 6761
RX spurious interrupt    : 0
```

```
Replenish Stats for all rxq:
```

```
-----
Number of replenish      : 61969
Number of replenish suspend : 0
Number of replenish un-suspend : 0
-----
```

## show platform software sl-infra

To display troubleshooting information and for debugging, enter the **show platform software sl-infra** command in privileged EXEC mode. The output of this command is used by the technical support team, for troubleshooting and debugging.

```
show platform software sl-infra { all | current | debug | stored }
```

### Syntax Description

**all** Displays current, debugging, and stored information.

**current** Displays current license-related information.

**debug** Enables debugging

**stored** Displays information that is stored on the product instance.

### Command Modes

Privileged EXEC (Device#)

### Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.

### Usage Guidelines

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra all** privileged EXEC commands.

# show platform sudi certificate

To display checksum record for the specific SUDI, use the **show platform sudi certificate** command in privileged EXEC mode.

**show platform sudi certificate** [**sign** [**nonce** <nonce> ]]

<b>Syntax Description</b>	<b>sign</b>	(Optional) Show signature
	<b>nonce</b>	(Optional) Enter a nonce value
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
		This command was introduced.

## Examples

This example shows how to view the checksum record for a specific SUDI :

```
# show platform sudi certificate

-----BEGIN CERTIFICATE-----
MIIDQzCCAiuqAwIBAgIQX/h7KctU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAYv8CrLqUccda8bnuoqrpu0hWISEwDovyD0My5jOamaHBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJsZR2tKys7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFU14F1pyXOWWqCZe+36ufijXWLBvLdT6ZeYpzPEApk0E5tziVMW/VgpSDH
jWn0f84bcN5wGyDWbs2mAg8EtKpP6BrXruOIIt6ke01a06g58QBdKhTcYtKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwtzALBGNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBGNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhIsjQal8dwy3U8pORFbi71R803UXHOjgkxhLtv5M0hmBvRbW7hmW
Yqpao2TB9k5UM8Z3/sUcuVdJcr18JOagEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpxYgyc81WhJdTsd9i7rp77rMKsSH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe00caEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdx41Id
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAYsGAWIBAgIKYQ1ufQAAAAAADANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQKEw1DaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIEENBmIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAM5l3THIx9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477Aks
5XAtUs5oxDYvt/zEbs1Zq3+LR6qrqKQVU6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPc1M4iYKHuMQMqmgmg+
xghHIooWS80BOccdiynEbeP5rZ7qRuewKmp11TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdg13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sX1XtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBbRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgnVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWBf2nsvqjBDBGNVHR8EPDA6MDiNgA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZW51cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
```

```

BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2l1zY28uY29tL3N1Y3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEAAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2l1zY28uY29tL3N1Y3VyXR5
L3BraS9wb2xpY2l1cy9pbmRleC5odG1sMBIGAlUdEwEB/wQIMAYBAf8CAQAwdQYJ
KoZlIhvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcC101Ju0a9zTXA9w47H9/t61eduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOwryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2P1As8YyjoNpK/urSRI14WdI1plR1nH7KND15618yfVp
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDhjCCAm6gAwIBAgIDctWkMA0GCSqGSIb3DQEBCwUAMCcxDjAMBgNVBAoTBUNp
c2NvMRUwEwYDVQQDEwxQ1QyIFNVREkgQ0EwHhcNMTUwODA2MDgwODI5WhcNMjUw
ODA2MDgwODI5WjBzMSwwKgYDVQQFEyNQSUQ6V1MtQzM2NTAtMTJYNdhVWjBTtjPjG
RE8xOTMyWDAwQzEOMAwGA1UEChMFQ2l1zY28xGDAwBGNVBAStD0FDVC0yIExpDGUg
U1VESTZMBcGA1UEAxMQV1MtQzM2NTAtMTJYNdhVWjCCASIdQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBANZxOGYI0eUl4HcSwjL4HO75qTj19C2BHG3ufce9ikkN
xwGXi8qq8vKxub9tRYRaJC5bP1Wmoq7+ZJtQA079xE4X14soNbkq5NaUhh7RB1wD
iRUJvTfCOzVICbNfbzvtB30I75tCarFNmpd0K6AFrIa41U988QGqaCj7R1JrYNaj
nc73UXXM/hc0HtNR5mhyqer5Y2qjjzo6tHZYqrrx2eS1X0a262ZSQriAxmaH/KLC
K97ywyRBdJlxBRX3hGtKlog8nASB8WpXqB9NVCERzUajwU3L/kg2BsCqw9Y2m7HW
U1cerTxgthuyUkdNI+Jg6iGAp2+s8E9hsHPBPMCdIsCAwEAAANvMG0wDgYDVR0P
AQH/BAQDAgXgMAwGA1UdEwEB/wQCMAAwTQYDVR0RBeywRKBCBgkrBgEAAQkVAgOg
NRMzQ2hpcE1EPVVZSk5ORmRRR1FvN1ZIVmxJRTlqZENBeU9DQXhPRG93T1RveE1T
QVg5eWc9MA0GCSqGSIb3DQEBCwUAA4IBAQBKicTRZbVCRjVIR5MQcWXUT086v6Ej
HahDHTts3YpQoyAVfioNg2x8J6EXcEau4voyVu+eMUuoNL4szPhmmDcULfiCGBcA
/R3EFuoVMIzNT0geziytsCf728KGw1oGuosgvjNGOOahUELu4+F/My7bIJNbh+PD
KjIFmhJpJg0F3q17yClAeXvd13g3W393i35d0Lm5L1WbBfQTyBaOLAbxsHvutrX
ulVZ5sdqSTwTkk09vKMaQjh7a8J/AmJi93jvzM69pe5711P1zqZfYfpiJ3cyJ0xf
I4brQ1smdczl0FD4asF7A+1vor5e4VDBP0ppmeFAJvCQ52JTpj0M0o1D
-----END CERTIFICATE-----

```

## show romvar

To view all ROMMON environment variables, use the **show romvar** command. To view environmental variable for a specific resource, use the **show romvar | i resource\_name**.

### show romvar

**Command Default** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows the output from the **show romvar** command:

```
Device# show romvar
ROMMON variables:
  PS1="switch: "
  TERMLINES="0"
  MOTHERBOARD_ASSEMBLY_NUM="73-18506-02"
  MOTHERBOARD_REVISION_NUM="05"
  MODEL_REVISION_NUM="P2B"
  POE1_ASSEMBLY_NUM="73-16123-03"
  POE1_REVISION_NUM="A0"
  POE1_SERIAL_NUM="FOC21387NKP"
  POE2_ASSEMBLY_NUM="73-16123-03"
  POE2_REVISION_NUM="A0"
  POE2_SERIAL_NUM="FOC21387NKT"
  IMAGE_UPGRADE="no"
  BOARDID="24666"
  MAC_ADDR="F8:B7:E2:4F:37:80"
  MODEL_NUM="C9300-48UN"
  MOTHERBOARD_SERIAL_NUM="FOC213901T4"
  SYSTEM_SERIAL_NUM="FCW2144L00V"
  USB_SERIAL_NUM="FOC21416472"
  STKPWR_SERIAL_NUM="FOC21432WPT"
  STKPWR_ASSEMBLY_NUM="73-11956-08"
  STKPWR_REVISION_NUM="B0"
  USB_ASSEMBLY_NUM="73-16167-02"
  USB_REVISION_NUM="A0"
  TAN_NUM="68-101202-01"
  TAN_REVISION_NUMBER="25"
  VERSION_ID="P2B"
  CLEI_CODE_NUMBER="ABCDEFGHJIJ"
  ECI_CODE_NUMBER="123456"
  TAG_ID="E2003412012AFC00062B095E"
  TFTP_SERVER="10.8.0.6"
  TFTP_BLKSIZE="8192"
  TEMPLATE="access"
  LICENSE_BOOT_LEVEL="network-essentials,all:C9300_48P;"
  DC_COPY="yes"
  ENABLE_BREAK="yes"
  IP_ADDRESS="172.21.227.57"
  IP_SUBNET_MASK="255.255.254.0"
  DEFAULT_GATEWAY="172.21.226.1"
  BAUD="115200"
```



```
AUTOREBOOT_RESTORE="0"  
SWITCH_NUMBER="5"  
CRASHINFO="crashinfo:crashinfo_RP_00_00_20180704-001833-UTC"  
BOOT="flash:packages.conf;"  
ABNORMAL_RESET_COUNT="0"  
RET_2_RTS="15:25:49 IST Fri Jul 13 2018"  
ROMMON_AUTOBOOT_ATTEMPT="3"  
BSI="0"  
RET_2_RCALTS=""  
RANDOM_NUM="1931842665"  
MANUAL_BOOT="yes"
```

## show running-config

To display the contents of the current running configuration file or the configuration for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or virtual circuit (VC) class, use the **show running-config** command in privileged EXEC mode.

**show running-config** [*options*]

---

### Syntax Description

*options* (Optional) Keywords used to customize output. You can enter more than one keyword.

- **aaa** [**accounting** | **attribute** | **authentication** | **authorization** | **diameter** | **group** | **ldap** | **miscellaneous** | **radius-server** | **server** | **tacacs-server** | **user-name** | **username**]: Displays AAA configurations.
  - **all**: Expands the output to include the commands that are configured with default parameters. If the **all** keyword is not used, the output does not display commands configured with default parameters.
  - **bridge-domain** {**id** | **parameterized vlan**}: Displays the running configuration for bridge domains.
  - **brief**: Displays the configuration without certification data and encrypted filter details.
  - **class-map** [*name*] [**linenum**]: Displays class map information.
  - **cts** [**interface** | **policy-server** | **rbm-rbac** | **server** | **sxp**]: Displays Cisco TrustSec configurations.
  - **deprecated**: Displays deprecated configuration along with the running configuration.
  - **eap** {**method** | **profiles**}: Displays EAP method configurations and profiles.
  - **flow** {**exporter** | **monitor** | **record**}: Displays global flow configuration commands.
  - **full**: Displays the full configuration.
  - **identity** {**policy** | **profile**}: Displays identity profile or policy information.
-

- **interface** *type number*: Displays interface-specific configuration information. If you use the **interface** keyword, you must specify the interface type and the interface number (for example, **interface GigabitEthernet 1/0/1**). Use the **show run interface ?** command to determine the interfaces available on your system.
- **ip dhcp pool** [*name*]: Displays IPv4 DHCP pool configuration.
- **ipv6 dhcp pool** [*name*]: Displays IPv6 DHCP pool configuration.
- **linenum** [**brief** | **full** | **partition**]: Displays line numbers in the output.
- **map-class** [**atm** | **dialer** | **frame-relay**] [*name*]: Displays map class information.
- **mdns-sd** [**gateway** | **location-group** | **service-definition** | **service-list** | **service-peer** | **service-policy**]: Displays Multicast DNS Service Discovery (mDNS-SD) configurations.
- **partition** {**access-list** | **class-map** | **common** | **global-cdp** | **interface** | **ip-as-path** | **ip-community** | **ip-prefix-list** | **ip-static-routes** | **line** | **policy-map** | **route-map** | **router** | **snmp** | **tacacs**}: Displays the configuration corresponding to a partition.
- **policy-map** [*name*] [**linenum**]: Displays policy map information.
- **switch** *number*: Displays configuration for the specified switch.
- **view** [**full**]: Enables the display of a full running configuration. This is for view-based users who typically can only view the configuration commands that they are entitled to access for that particular view.
- **vlan** [*vlan-id*]: Displays the specific VLAN information; valid values are from 1 to 4094.
- **vrf** [*vrf-name*]: Displays the Virtual routing and forwarding (VRF)-aware configuration module number .

**Command Default**

The default syntax, **show running-config**, displays the contents of the running configuration file, except commands configured using the default parameters.

**Command Modes**

Privileged EXEC (#)

**Command History**

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines**

The **show running-config** command is technically a command alias (substitute or replacement syntax) of the **more system:running-config** command. Although the use of more commands is recommended (because of their uniform structure across platforms and their expandable syntax), the **show running-config** command remains enabled to accommodate its widespread use, and to allow typing shortcuts such as **show run**.

The **show running-config interface** command is useful when there are multiple interfaces and you want to look at the configuration of a specific interface.

The **linenum** keyword causes line numbers to be displayed in the output. This option is useful for identifying a particular portion of a very large configuration.

You can enter additional output modifiers in the command syntax by including a pipe character (|) after the optional keyword. For example, **show running-config interface GigabitEthernet 1/0/1 linenum | begin 3**.

To display the output modifiers that are available for a keyword, enter `| ?` after the keyword. Depending on the platform you are using, the keywords and the arguments for the *options* argument may vary.

The **show running-config all** command displays complete configuration information, including the default settings and values. For example, if the Cisco Discovery Protocol (abbreviated as CDP in the output) hold-time value is set to its default of 180:

- The **show running-config** command does not display this value.
- The **show running-config all** displays the following output: `cdp holdtime 180`.

If the Cisco Discovery Protocol holdtime is changed to a nondefault value (for example, 100), the output of the **show running-config** and **show running-config all** commands is the same; that is, the configured parameter is displayed.

The **show running-config** command displays ACL information. To exclude ACL information from the output, use the **show running | section exclude ip access | access list** command.

## Examples

The following example shows the configuration for GigabitEthernet0/0 interface. The fields are self-explanatory.

```
Device# show running-config interface gigabitEthernet0/0

Building configuration...

Current configuration : 130 bytes
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 ip address 10.5.20.10 255.255.0.0
 negotiation auto
 ntp broadcast
end
```

The following example shows how to set line numbers in the command output and then use the output modifier to start the display at line 10. The fields are self-explanatory.

```
Device# show running-config linenum | begin 10

10 : boot-start-marker
11 : boot-end-marker
12 : !
13 : no logging buffered
14 : enable password #####
15 : !
16 : spe 1/0 1/7
17 :  firmware location bootflash:mica-modem-pw.10.16.0.0.bin
18 : !
19 : !
20 : resource-pool disable
21 : !
22 : no aaa new-model
23 : ip subnet-zero
24 : ip domain name cisco.com
25 : ip name-server 172.16.11.48
26 : ip name-server 172.16.2.133
27 : !
28 : !
29 : isdn switch-type primary-5ess
30 : !
.
```

```
.
.
126 : end
```

In the following sample output from the **show running-config** command, the **shape average** command indicates that the traffic shaping overhead accounting for ATM is enabled. The BRAS-DSLAM encapsulation type is qinq and the subscriber line encapsulation type is snap-rbe based on the ATM adaptation layer 5 (AAL5) service. The fields are self-explanatory.

```
Device# show running-config
.
.
.
subscriber policy recording rules limit 64
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
controller T1 2/0
framing sf
linecode ami
!
controller T1 2/1
framing sf
linecode ami
!
!
policy-map unit-test
class class-default
shape average percent 10 account qinq aal5 snap-rbe
!
```

The following is sample output from the **show running-config class-map** command. The fields in the display are self-explanatory.

```
Device# show running-config class-map

Building configuration...

Current configuration : 2157 bytes
!
class-map match-any system-cpp-police-ewlc-control
  description EWLC Control
class-map match-any system-cpp-police-topology-control
  description Topology control
class-map match-any system-cpp-police-sw-forward
  description Sw forwarding, L2 LVX data packets, LOGGING, Transit Traffic
class-map match-any system-cpp-default
  description EWLC Data, Inter FED Traffic
class-map match-any system-cpp-police-sys-data
  description Openflow, Exception, EGR Exception, NFL Sampled Data, RPF Failed
class-map match-any system-cpp-police-punt-webauth
  description Punt Webauth
class-map match-any system-cpp-police-l2lvx-control
  description L2 LVX control packets
class-map match-any system-cpp-police-forus
  description Forus Address resolution and Forus traffic
class-map match-any system-cpp-police-multicast-end-station
  description MCAST END STATION
class-map match-any system-cpp-police-high-rate-app
  description High Rate Applications
class-map match-any system-cpp-police-multicast
  description MCAST Data
class-map match-any system-cpp-police-l2-control
  description L2 control
```

```

class-map match-any system-cpp-police-dot1x-auth
  description DOT1X Auth
class-map match-any system-cpp-police-data
  description ICMP redirect, ICMP_GEN and BROADCAST
class-map match-any system-cpp-police-stackwise-virt-control
  description Stackwise Virtual OOB
...

```

The following example shows that the teletype (tty) line 2 is reserved for communicating with the second core:

```

Device# show running

Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname device
!
enable password lab
!
no ip subnet-zero
!
!
!
interface Ethernet0
 ip address 10.25.213.150 255.255.255.128
 no ip directed-broadcast
 no logging event link-status
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
ip default-gateway 10.25.213.129
ip classless
ip route 0.0.0.0 0.0.0.0 10.25.213.129
!
!
line con 0
 transport input none
line 1 6
 no exec
 transport input all
line 7
 no exec
 exec-timeout 300 0
 transport input all
line 8 9
 no exec
 transport input all

```

```

line 10
  no exec
  transport input all
  stopbits 1
line 11 12
  no exec
  transport input all
line 13
  no exec
  transport input all
  speed 115200
line 14 16
  no exec
  transport input all
line aux 0
line vty 0 4
  password cisco
  login
!
end

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration. (Command alias for the <b>copy system:running-config nvram:startup-config</b> command.)
<b>show startup-config</b>	Displays the contents of NVRAM (if present and valid) or displays the configuration file pointed to by the CONFIG_FILE environment variable. (Command alias for the <b>more:nvram startup-config</b> command.)

# show sdm prefer

To display information about the templates that can be used to maximize system resources for a particular feature, use the **show sdm prefer** command in privileged EXEC mode. To display the current template, use the command without a keyword.

**show sdm prefer** [ **access** ]

<b>Syntax Description</b>	<b>access</b> (Optional) Displays information on the access template.
---------------------------	---

<b>Command Default</b>	No default behavior or values.
------------------------	--------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

<b>Usage Guidelines</b>	If you did not reload the device after entering the <b>sdm prefer</b> global configuration command, the <b>show sdm prefer</b> privileged EXEC command displays the template currently in use and not the newly configured template.
-------------------------	--

The numbers displayed for each template represent an approximate maximum number for each feature resource. The actual number might vary, depending on the actual number of other features configured. For example, in the default template if your device had more than 16 routed interfaces (subnet VLANs), the number of possible unicast MAC addresses might be less than 6000.

## Example

The following is sample output from the **show sdm prefer** command:

```
Device# show sdm prefer
Showing SDM Template Info

This is the Access template.
Number of VLANs:                4094
Unicast MAC addresses:          32768
Overflow Unicast MAC addresses: 1024
L2 Multicast entries:           8192
Overflow L2 Multicast entries:   512
L3 Multicast entries:           8192
Overflow L3 Multicast entries:   512
Directly connected routes:      24576
Indirect routes:                 8192
STP Instances:                  1024
Security Access Control Entries: 5120
QoS Access Control Entries:      5120
Policy Based Routing ACEs:       1024
Netflow Input ACEs:              256
Netflow Output ACEs:             768
```



```
Ingress Netflow ACEs:                256
Egress Netflow ACEs:                 768
Flow SPAN ACEs:                      1024
Tunnels:                             512
LISP Instance Mapping Entries:       512
Control Plane Entries:               512
Input Netflow flows:                 32768
Output Netflow flows:                32768
SGT/DGT (or) MPLS VPN entries:       8192
SGT/DGT (or) MPLS VPN Overflow entries: 512
Wired clients:                       2048
MACSec SPD Entries:                  256
MPLS L3 VPN VRF:                     255
MPLS Labels:                         2048
MPLS L3 VPN Routes VRF Mode:         7168
MPLS L3 VPN Routes Prefix Mode:      3072
MVPN MDT Tunnels:                    256
L2 VPN EOMPLS Attachment Circuit:    256
MAX VPLS Bridge Domains :             128
MAX VPLS Peers Per Bridge Domain:    32
MAX VPLS/VPWS Pseudowires :          1024
```

These numbers are typical for L2 and IPv4 features.  
Some features such as IPv6, use up double the entry size;  
so only half as many entries can be created.  
\* values can be modified by sdm cli.

# show tech-support confidential

To hide confidential information from the **show tech-support** output, use the **show tech-support confidential** command in privileged EXEC mode.

**show tech-support confidential output** *file-name*

<b>Syntax Description</b>	<b>output</b> <i>file-name</i>	Specifies the output file where the tech-support data is to be saved.
<b>Command Default</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.
<b>Usage Guidelines</b>	<p>The <b>show tech-support confidential</b> command will hide sensitive data like MAC addresses, IP addresses, and passwords. The output will be the same as that of the <b>show tech-support</b> command with all the customer-specific data masked.</p> <p>The output from the <b>show tech-support confidential</b> command is very long. To better manage this output, you can redirect the output to a file in the local writable storage file system or the remote file system by using the <b>show tech-support confidential output</b> <i>location:filename</i> ). Redirecting the output to a file also makes sending the output to your Cisco Technical Assistance Center (TAC) representative easier.</p> <pre>Device# show tech-support confidential output flash:tech_confidential Collecting tech-support without confidential info, it will take few min..</pre> <p>To view the output of the redirected file, use the command <b>more</b> <i>location:filename</i>.</p>	

# show tech-support monitor

To display the SPAN monitor information, use the **show tech-support monitor** command in privileged EXEC mode.

**show tech-support monitor** [**{switch** *switch-number* | **active** | **standby**}]

Syntax Description		
	<i>switch-number</i>	Specifies the switch.
	<b>active</b>	Specifies the active instance of the switch.
	<b>standby</b>	Specifies the standby instance of the switch.

**Command Default** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

**Usage Guidelines** The output from the **show tech-support monitor** command is very long. To better manage this output, you can redirect the output to a file (for example, **show tech-support monitor** [**switch** *switch-number* | **active** | **standby**] | **redirect location:filename**) in the local writable storage file system or the remote file system. Redirecting the output to a file also makes sending the output to your Cisco Technical Assistance Center (TAC) representative easier.

To view the output of the redirected file, use the command **more location:filename**.

# show tech-support platform

To display detailed information about a platform for use by technical support, use the **show tech-support platform** command in privileged EXEC mode.

## show tech-support platform

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

**Usage Guidelines** This command is used for platform-specific debugging. The output provides detailed information about a platform, such as CPU usage, Ternary Content Addressable Memory (TCAM) usage, capacity, and memory usage.

The output of the **show tech-support platform** command is very long. To better manage this output, you can redirect the output to an external file (for example, **show tech-support platform | redirect flash:filename**) in the local writable storage file system or remote file system.

The output of the **show tech-support platform** command displays a list commands and their output. These commands may differ based on the platform.

## Examples

The following is sample output from the **show tech-support platform** command:

```
Device# show tech-support platform
.
.
.
----- show platform hardware capacity -----

Load Average
  Slot  Status  1-Min  5-Min 15-Min
1-RP0 Healthy  0.25  0.17  0.12

Memory (kB)
  Slot  Status  Total      Used (Pct)   Free (Pct)  Committed (Pct)
1-RP0 Healthy 3964428 2212476 (56%) 1751952 (44%) 3420472 (86%)

CPU Utilization
  Slot  CPU   User System  Nice  Idle  IRQ  SIRQ  IOwait
1-RP0  0    1.40  0.90  0.00  97.60 0.00  0.10  0.00
      1    2.00  0.20  0.00  97.79 0.00  0.00  0.00
      2    0.20  0.00  0.00  99.80 0.00  0.00  0.00
      3    0.79  0.19  0.00  99.00 0.00  0.00  0.00
      4    5.61  0.50  0.00  93.88 0.00  0.00  0.00
      5    2.90  0.40  0.00  96.70 0.00  0.00  0.00

*: interface is up
```

IHQ: pkts in input hold queue      IQD: pkts dropped from input queue  
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue  
 RXBS: rx rate (bits/sec)            RXPS: rx rate (pkts/sec)  
 TXBS: tx rate (bits/sec)            TXPS: tx rate (pkts/sec)  
 TRTL: throttle count

Interface			IHQ	IQD	OHQ	OQD	RXBS	RXPS
TXBS	TXPS	TRTL						
Vlan1			0	0	0	0	0	0
0	0	0						
* GigabitEthernet0/0			0	10179	0	0	2000	4
0	0	0						
GigabitEthernet1/0/1			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/2			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/3			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/4			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/5			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/6			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/7			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/8			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/9			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/10			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/11			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/12			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/13			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/14			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/15			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/16			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/17			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/18			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/19			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/20			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/21			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/22			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/23			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/24			0	0	0	0	0	0
0	0	0						
GigabitEthernet1/0/25			0	0	0	0	0	0
0	0	0						

## show tech-support platform

```

GigabitEthernet1/0/26      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/27      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/28      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/29      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/30      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/31      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/32      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/33      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/34      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/35      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/36      0      0      0      0      0      0
0      0      0
Tel/0/37                   0      0      0      0      0      0
0      0      0
Tel/0/38                   0      0      0      0      0      0
0      0      0
Tel/0/39                   0      0      0      0      0      0
0      0      0
Tel/0/40                   0      0      0      0      0      0
0      0      0
Tel/0/41                   0      0      0      0      0      0
0      0      0
Tel/0/42                   0      0      0      0      0      0
0      0      0
Tel/0/43                   0      0      0      0      0      0
0      0      0
Tel/0/44                   0      0      0      0      0      0
0      0      0
Tel/0/45                   0      0      0      0      0      0
0      0      0
Tel/0/46                   0      0      0      0      0      0
0      0      0
Tel/0/47                   0      0      0      0      0      0
0      0      0
Tel/0/48                   0      0      0      0      0      0
0      0      0
Tel/1/1                    0      0      0      0      0      0
0      0      0
Tel/1/2                    0      0      0      0      0      0
0      0      0
Tel/1/3                    0      0      0      0      0      0
0      0      0
Tel/1/4                    0      0      0      0      0      0
0      0      0

```

## ASIC 0 Info

```

-----
ASIC 0 HASH Table 0 Software info: FSE 0
MAB 0: Unicast MAC addresses srip 0 1
MAB 1: Unicast MAC addresses srip 0 1
MAB 2: Unicast MAC addresses srip 0 1
MAB 3: Unicast MAC addresses srip 0 1
MAB 4: Unicast MAC addresses srip 0 1
MAB 5: Unicast MAC addresses srip 0 1
MAB 6: Unicast MAC addresses srip 0 1

```

```

MAB 7: Unicast MAC addresses srip 0 1
ASIC 0 HASH Table 1 Software info: FSE 0
MAB 0: Unicast MAC addresses srip 0 1
MAB 1: Unicast MAC addresses srip 0 1
MAB 2: Unicast MAC addresses srip 0 1
MAB 3: Unicast MAC addresses srip 0 1
MAB 4: Unicast MAC addresses srip 0 1
MAB 5: Unicast MAC addresses srip 0 1
MAB 6: Unicast MAC addresses srip 0 1
MAB 7: Unicast MAC addresses srip 0 1
ASIC 0 HASH Table 2 Software info: FSE 1
MAB 0: L3 Multicast entries srip 2 3
MAB 1: L3 Multicast entries srip 2 3
MAB 2: SGT_DGT          srip 0 1
MAB 3: SGT_DGT          srip 0 1
MAB 4: (null)           srip
MAB 5: (null)           srip
MAB 6: (null)           srip
MAB 7: (null)           srip
.
.
.

```

Output fields are self-explanatory.

#### Related Commands

Command	Description
<b>show tech-support platform evpn_vxlan</b>	Displays EVPN-VXLAN-related platform information.
<b>show tech-support platform fabric</b>	Displays detailed information about the switch fabric.
<b>show tech-support platform igmp_snooping</b>	Displays IGMP snooping information about a group.
<b>show tech-support platform layer3</b>	Displays Layer 3 platform forwarding information.
<b>show tech-support platform mld_snooping</b>	Displays MLD snooping information about a group.

## show tech-support platform evpn\_vxlan

To display Ethernet VPN (EVPN)-Virtual eXtensible LAN (VXLAN)-related platform information for use by technical support, use the **show tech-support platform evpn\_vxlan** command in privileged EXEC mode.

**show tech-support platform evpn\_vxlan switch** *switch-number*

<b>Syntax Description</b>	<b>switch</b> <i>switch-number</i>	Displays information for the specified switch. Valid values are from 1 to 9.
---------------------------	------------------------------------	--

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

<b>Usage Guidelines</b>	The output of this command is very long. To better manage this output, you can redirect the output to an external file (for example, <b>show tech-support platform evpn_vxlan switch 1   redirect flash:filename</b> ) in the local writable storage file system or remote file system.
-------------------------	---

### Examples

The following is sample output from the **show tech-support platform evpn\_vxlan** command:

```
Device# show tech-support platform evpn_vxlan switch 1
.
.
.
    "show clock"
    "show version"
    "show running-config"switch no: 1

----- sh sdm prefer -----

Showing SDM Template Info

This is the Advanced template.
Number of VLANs:                               4094
Unicast MAC addresses:                         32768
Overflow Unicast MAC addresses:                512
L2 Multicast entries:                          4096
Overflow L2 Multicast entries:                 512
L3 Multicast entries:                          4096
Overflow L3 Multicast entries:                 512
Directly connected routes:                    16384
Indirect routes:                               7168
STP Instances:                                4096
Security Access Control Entries:               3072
QoS Access Control Entries:                    2560
Policy Based Routing ACEs:                     1024
Netflow ACEs:                                  768
Flow SPAN ACEs:                                512
Tunnels:                                       256
LISP Instance Mapping Entries:                 256
Control Plane Entries:                         512
```



```

Input Netflow flows:                8192
Output Netflow flows:              16384
SGT/DGT (or) MPLS VPN entries:     4096
SGT/DGT (or) MPLS VPN Overflow entries: 512
Wired clients:                     2048
MACSec SPD Entries:                256
MPLS L3 VPN VRF:                   127
MPLS Labels:                       2048
MPLS L3 VPN Routes VRF Mode:      7168
MPLS L3 VPN Routes Prefix Mode:   3072
MVPN MDT Tunnels:                  256
L2 VPN EOMPLS Attachment Circuit:  256
MAX VPLS Bridge Domains :          64
MAX VPLS Peers Per Bridge Domain:  8
MAX VPLS/VPWS Pseudowires :       256

```

These numbers are typical for L2 and IPv4 features.  
Some features such as IPv6, use up double the entry size;  
so only half as many entries can be created.  
\* values can be modified by sdm cli.

```
----- show platform software fed switch 1 ifm interfaces nve -----
```

```
----- show platform software fed switch 1 ifm interfaces efp -----
```

```
----- show platform software fed switch 1 matm macTable -----
```

```

Total Mac number of addresses:: 0
*a_time=aging_time(secs) *e_time=total_elapsed_time(secs)
Type:
MAT_DYNAMIC_ADDR          0x1  MAT_STATIC_ADDR          0x2  MAT_CPU_ADDR
0x4  MAT_DISCARD_ADDR    0x8
MAT_ALL_VLANS             0x10 MAT_NO_FORWARD           0x20  MAT_IPMULT_ADDR
0x40  MAT_RESYNC         0x80
MAT_DO_NOT_AGE           0x100 MAT_SECURE_ADDR         0x200  MAT_NO_PORT
0x400  MAT_DROP_ADDR     0x800
MAT_DUP_ADDR             0x1000 MAT_NULL_DESTINATION    0x2000  MAT_DOT1X_ADDR
0x4000  MAT_ROUTER_ADDR  0x8000
MAT_WIRELESS_ADDR        0x10000 MAT_SECURE_CFG_ADDR    0x20000  MAT_OPQ_DATA_PRESENT
0x40000  MAT_WIRED_TUNNEL_ADDR 0x80000
MAT_DLR_ADDR             0x100000 MAT_MRP_ADDR            0x200000  MAT_MSRRP_ADDR
0x400000  MAT_LISP_LOCAL_ADDR 0x800000
MAT_LISP_REMOTE_ADDR    0x1000000 MAT_VPLS_ADDR           0x2000000
Device#

```

Output fields are self-explanatory.

#### Related Commands

Command	Description
<b>show tech-support platform</b>	Displays detailed information about a platform for use by technical support.

# show tech-support platform fabric

To display information about the switch fabric, use the **show tech-support platform fabric** command in privileged EXEC mode.

```
show tech-support platform fabric [{display-cli | vrf vrf-name {ipv4 display-cli | ipv6 display-cli |
source instance-id instance-id {ipv4 ip-address/ip-prefix | ipv6 ipv6-address/ipv6-prefix | mac mac-address}
{dest instance-id instance-id} {ipv4 ip-address/ip-prefix | ipv6 ipv6-address/ipv6-prefix | mac mac-address}
[ {display-cli} ]}]
```

Syntax Description		
<b>display-cli</b>		(Optional) Displays the list of show commands available in the output of this command.
<b>vrf</b> <i>vrf-name</i>		(Optional) Displays fabric-related information for the specified virtual routing and forwarding (VRF) instance.
<b>ipv4</b> <i>ip-address/ip-prefix</i>		(Optional) Displays fabric-related information for the source or destination IP VRF.
<b>ipv6</b> <i>ipv6-address/ipv6-prefix</i>		(Optional) Displays fabric-related information for the source or destination IPv6 VRF.
<b>source</b>		(Optional) Displays fabric-related information for the source VRF.
<b>instance-id</b> <i>instance-id</i>		(Optional) Displays information about the endpoint identifier (EID) of the source.
<b>mac</b> <i>mac-address</i>		(Optional) Displays fabric-related information for the source and destination MAC VRF for Layer 2 extension deployments.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

**Usage Guidelines** The output of this command is very long. To better manage this output, you can redirect the output to an external file (for example, **show tech-support platform fabric | redirect flash:filename**) in the local writable storage file system or remote file system.

The output of this command displays a list commands and their output. These commands may differ based on the platform.

## Examples

The following is sample output from the **show tech-support platform fabric vrf source instance-id ipv4 dest instance-id ipv4** command:

```
Device# show tech-support platform fabric vrf DEFAULT_VN source instance-id
4098 ipv4 10.1.1.1/32 dest instance-id 4098 ipv4 10.12.12.12/32

.
.
.
-----show ip lisp eid-table vrf DEFAULT_VN forwarding eid remote 10.12.12.12-----

Prefix          Fwd action  Locator status bits  encap_iid
10.12.12.12/32  encap       0x00000001           N/A
  packets/bytes 1/576
  path list 7F44EEC2C188, 4 locks, per-destination, flags 0x49 [shble, rif, hwn]
  ifnums:
    LISP0.4098(78): 192.0.2.2
  1 path
    path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4
      nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2
7F44F8E86CE8
  1 output chain
    chain[0]: IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8
              IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378

-----show lisp instance-id 4098 ipv4 map-cache-----

LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries
0.0.0.0/0, uptime: 02:46:01, expires: never, via static-send-map-request
  Encapsulating to proxy ETR
10.1.1.0/24, uptime: 02:46:01, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR
10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
Locator Uptime  State      Pri/Wgt  Encap-IID
192.0.2.2 02:45:54 up        10/10    -

-----show lisp instance-id 4098 ipv4 map-cache detail-----

LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries
0.0.0.0/0, uptime: 02:46:01, expires: never, via static-send-map-request
  Sources: static-send-map-request
  State: send-map-request, last modified: 02:46:01, map-source: local
  Exempt, Packets out: 2(676 bytes) (~ 02:45:38 ago)
  Configured as EID address space
  Encapsulating to proxy ETR
10.1.1.0/24, uptime: 02:46:01, expires: never, via dynamic-EID, send-map-request
  Sources: NONE
  State: send-map-request, last modified: 02:46:01, map-source: local
  Exempt, Packets out: 0(0 bytes)
  Configured as EID address space
  Configured as dynamic-EID address space
  Encapsulating dynamic-EID traffic
  Encapsulating to proxy ETR
```

```

10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
Sources: map-reply
State: complete, last modified: 02:45:54, map-source: 10.0.1.2
Idle, Packets out: 1(576 bytes) (~ 02:45:38 ago)
Locator Uptime State Pri/Wgt Encap-IID
192.0.2.2 02:45:54 up 10/10 -
Last up-down state change: 02:45:54, state change count: 1
Last route reachability change: 02:45:54, state change count: 1
Last priority / weight change: never/never
RLOC-probing loc-status algorithm:
Last RLOC-probe sent: 02:45:54 (rtt 1ms)

```

```
-----show lisp instance-id 4098 ipv4 map-cache 10.12.12.12/32-----
```

```
LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries
```

```

10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
Sources: map-reply
State: complete, last modified: 02:45:54, map-source: 10.0.1.2
Idle, Packets out: 1(576 bytes) (~ 02:45:38 ago)
Locator Uptime State Pri/Wgt Encap-IID
192.0.2.2 02:45:54 up 10/10 -
Last up-down state change: 02:45:54, state change count: 1
Last route reachability change: 02:45:54, state change count: 1
Last priority / weight change: never/never
RLOC-probing loc-status algorithm:
Last RLOC-probe sent: 02:45:54 (rtt 1ms)

```

```
-----show ip cef vrf DEFAULT_VN 10.12.12.12/32 internal-----
```

```

10.12.12.12/32, epoch 1, flags [sc, lisp elig], refcnt 6, per-destination sharing
sources: LISP, IPL
feature space:
  Broker: linked, distributed at 1st priority
subblocks:
  SC owned,sourced: LISP remote EID - locator status bits 0x00000001
  LISP remote EID: 1 packets 576 bytes fwd action encap, cfg as EID space
  LISP source path list
    path list 7F44EEC2C188, 4 locks, per-destination, flags 0x49 [shble, rif, hwc]
    ifnums:
      LISP0.4098(78): 192.0.2.2
    1 path
      path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4
      nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2
7F44F8E86CE8
    1 output chain
      chain[0]: IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8
        IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378
      Dependent covered prefix type LISP, cover 0.0.0.0/0
    2 IPL sources [no flags]
  ifnums:
    LISP0.4098(78): 192.0.2.2
  path list 7F44EEC2C188, 3 locks, per-destination, flags 0x49 [shble, rif, hwc]
    path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4
    nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8

output chain:
  PushCounter(LISP:10.12.12.12/32) 7F44F3C8B8D8
  IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8
  IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378

```

```

switch no: 1
.
.
.

Device# show tech-support platform fabric vrf Campus_VN source instance-id 8189
mac 00b7.7128.00a1 dest instance-id 8189 mac 00b7.7128.00a0 | i show

----- show clock -----
----- show version -----
----- show running-config -----
----- show device-tracking database -----
----- show lisp site -----
----- show mac address-table address 00B7.7128.00A0-----
----- show ip arp vrf Campus_VN-----
Device#

```

Output fields are self-explanatory.

#### Related Commands

Command	Description
<b>show tech-support platform</b>	Displays detailed information about a platform for use by technical support.

## show tech-support platform igmp\_snooping

To display Internet Group Management Protocol (IGMP) snooping information about a group, use the **show tech-support platform igmp\_snooping** command in privileged EXEC mode.

```
show tech-support platform igmp_snooping [{Group_ipAddr ipv4-address} [{vlan vlan-ID}]]
```

Syntax Description	Group_ipAddr	(Optional) Displays snooping information about the specified group address.
	<i>ipv4-address</i>	(Optional) IPv4 address of the group.
	<b>vlan</b> <i>vlan-ID</i>	(Optional) Displays IGMP snooping VLAN information. Valid values are from 1 to 4094.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

The output of this command is very long. To better manage this output, you can redirect the output to a file (for example, **show tech-support platform igmp\_snooping | redirect flash:filename**) in the local writable storage file system or remote file system.

### Examples

The following is sample output from the **show tech-support platform igmp\_snooping** command:

```
Device# show tech-support platform igmp_snooping GroupIPAddr 226.6.6.6 vlan
.
.
.
----- show ip igmp snooping groups | i 226.6.6.6 -----
5          226.6.6.6          user          Gi1/0/8, Gi1/0/27, Gi1/0/28,

----- show ip igmp snooping groups count -----
Total number of groups:  2

----- show ip igmp snooping mrouter -----

Vlan      ports
-----  -----
   23     Router
   24     Router
```

25 Router

----- show ip igmp snooping querier -----

Vlan	IP Address	IGMP Version	Port
23	10.1.1.1	v2	Router
24	10.1.2.1	v2	Router
25	10.1.3.1	v2	Router

----- show ip igmp snooping vlan 5 -----

Global IGMP Snooping configuration:

```

-----
IGMP snooping           : Enabled
Global PIM Snooping    : Disabled
IGMPv3 snooping        : Enabled
Report suppression     : Enabled
TCN solicit query      : Disabled
TCN flood query count  : 2
Robustness variable    : 2
Last member query count : 2
Last member query interval : 1000

```

Vlan 5:

```

-----
IGMP snooping           : Enabled
Pim Snooping           : Disabled
IGMPv2 immediate leave : Disabled
Explicit host tracking  : Enabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
Robustness variable    : 2
Last member query count : 2
Last member query interval : 1000

```

----- show ip igmp snooping groups vlan 5 -----

Vlan	Group	Type	Version	Port List
5	226.6.6.6	user		Gi1/0/8, Gi1/0/27, Gi1/0/28, Gi2/0/7, Gi2/0/8, Gi2/0/27, Gi2/0/28
5	238.192.0.1	user		Gi2/0/28

----- show platform software fed active ip igmp snooping vlan 5 -----

Vlan 5

```

-----
IGMPSN Enabled : On
PIMSN Enabled  : Off
Flood Mode     : On
I-Mrouter      : Off
Oper State     : Up

```

**show tech-support platform igmp\_snooping**

```

STP TCN Flood   : Off
Routing Enabled : Off
PIM Enabled     : Off
PVLAN           : No
In Retry        : 0x0
L3mcast Adj     :
Mrouter PortQ   :
Flood PortQ     :

```

```
----- show platform software fed active ip igmp snooping groups | begin 226.6.6.6 -----
```

```
Vlan:5 Group:226.6.6.6
```

```

-----
Member ports   :
CAPWAP ports   :
Host Type Flags: 0
Failure Flags  : 0
DI handle      : 0x7f11151cbad8
REP RI handle  : 0x7f11151cc018
SI handle      : 0x7f11151cd198
HTM handle     : 0x7f11151cd518

```

```
si hdl : 0x7f11151cd198 rep ri hdl : 0x7f11151cc018 di hdl : 0x7f11151cbad8 htm hdl :
0x7f11151cd518
```

```
.
.
.
```

```
Device#
```

Output fields are self-explanatory.

**Related Commands**

Command	Description
<b>ip igmp snooping</b>	Enables IGMP snooping globally or on an interface.
<b>show ip igmp snooping</b>	Displays the IGMP snooping configuration of a device.
<b>show tech-support platform</b>	Displays detailed information about a platform for use by technical support.



# show tech-support platform layer3

To display Layer 3 platform forwarding information, use the **show tech-support platform layer3** command in privileged EXEC mode.

```
show tech-support platform layer3 {multicast Group_ipAddr ipv4-address switch switch-number srcIP
ipv4-address | unicast {dstIP ipv4-address srcIP ipv4-address | vrf vrf-name destIP ipv4-address srcIP
ipv4-address}}
```

Syntax Description		
	<b>multicast</b>	Displays multicast information.
	<b>Group_ipv6Addr</b> <i>ipv4-address</i>	Displays information about the specified multicast group address.
	<b>switch</b> <i>switch-number</i>	Displays information about the specified switch. Valid values are from 1 to 9.
	<b>srcIP</b> <i>ipv4-address</i>	Displays information about the specified source address.
	<b>unicast</b>	Displays unicast-related information.
	<b>dstIP</b> <i>ipv4-address</i>	Displays information about the specified destination address.
	<b>vrf</b> <i>vrf-name</i>	Displays unicast-related virtual routing and forwarding (VRF) information.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

**Usage Guidelines** The output of this command is very long. To better manage this output, you can redirect the output to an external file (for example, **show tech-support platform layer3 multicast group 224.1.1.1 switch 1 srcIP 10.10.0.2 | redirect flash:filename**) in the local writable storage file system or remote file system.

**Examples** The following is sample output from the **show tech-support platform layer3 multicast group** command:

```
Device# show tech-support platform layer3 multicast group_ipAddr 224.1.1.1
switch 1 srcIP 10.10.0.2

.
.
.
destination IP: 224.1.1.1
source IP: 10.10.0.2
```

## show tech-support platform layer3

```

switch no: 1

----- show ip mroute 224.1.1.1 10.10.0.2 -----

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group, c - PFP-SA cache created entry
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(10.10.0.2, 224.1.1.1), 00:00:22/00:02:37, flags: LFT
  Incoming interface: GigabitEthernet1/0/10, RPF nbr 0.0.0.0, Registering
  Outgoing interface list:
    Vlan20, Forward/Sparse, 00:00:22/00:02:37, A

----- show ip mfib 224.1.1.1 10.10.0.2 -----

Entry Flags:   C - Directly Connected, S - Signal, IA - Inherit A flag,
               ET - Data Rate Exceeds Threshold, K - Keepalive
               DDE - Data Driven Event, HW - Hardware Installed
               ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
               MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
               MS - MoFRR Entry in Sync, MC - MoFRR entry in MoFRR Client.
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
                MA - MFIB Accept, A2 - Accept backup,
                RA2 - MRIB Accept backup, MA2 - MFIB Accept backup

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:  FS Pkt Count/PS Pkt Count
Default
(10.10.0.2,224.1.1.1) Flags: HW
  SW Forwarding: 0/0/0/0, Other: 1/1/0
  HW Forwarding:  NA/NA/NA/NA, Other: NA/NA/NA
  GigabitEthernet1/0/10 Flags: A
  Vlan20 Flags: F IC
    Pkts: 0/0
  Tunnel0 Flags: F
    Pkts: 0/0

----- show platform software fed switch 1 ip multicast interface summary -----

Multicast Interface database

```

VRF	Interface SVI	IF ID	PIM Status	State	RI Handle
0	GigabitEthernet1/0/10 0x00007fb414b1f108 false	0x000000000000005f	enabled	0x0000000000000010	
0	Vlan20 0x00007fb414b31a98 true	0x0000000000000060	enabled	0x0000000000000010	

----- show platform software fed switch 1 ip multicast groups summary -----

Multicast Groups database

Mvrf\_id: 0 Mroute: (\*, 224.0.1.40/32) Flags: C IC  
 Htm: 0x00007fb414b23ce8 Si: 0x00007fb414b23a08 Di: 0x00007fb414b240e8 Rep\_ri:  
 0x00007fb414b245f8

Mvrf\_id: 0 Mroute: (\*, 224.0.0.0/4) Flags: C  
 Htm: 0x00007fb4143549e8 Si: 0x00007fb414b20a48 Di: 0x00007fb414b1fe78 Rep\_ri:  
 0x00007fb414b20428

Mvrf\_id: 0 Mroute: (\*, 224.1.1.1/32) Flags: C IC  
 Htm: 0x00007fb414b2cc98 Si: 0x00007fb414b2b678 Di: 0x00007fb414b2ab98 Rep\_ri:  
 0x00007fb414b2b0c8

Mvrf\_id: 0 Mroute: (10.10.0.2, 224.1.1.1/32) Flags: IC  
 Htm: 0x00007fb414b2f348 Si: 0x00007fb414b321d8 Di: 0x00007fb414b2dba8 Rep\_ri:  
 0x00007fb414b30ed8

----- show platform software fed switch 1 ip multicast groups count -----

Total Number of entries:4

----- show platform software fed switch 1 ip multicast groups 224.1.1.1/32  
 source 10.10.0.2 detail -----

MROUTE ENTRY vrf 0 (10.10.0.2, 224.1.1.1/32)  
 HW Handle: 140411418055080 Flags: IC  
 RPF interface: GigabitEthernet1/0/10(95):  
 HW Handle:140411418055080 Flags:A  
 Number of OIF: 3  
 Flags: 0x4 Pkts : 0  
 OIF Details:  
 Tunnel0 Adj: 0xf8000636 F  
 Vlan20 Adj: 0xf8000601 F IC  
 GigabitEthernet1/0/10 A  
 Htm: 0x7fb414b2f348 Si: 0x7fb414b321d8 Di: 0x7fb414b2dba8 Rep\_ri: 0x7fb414b30ed8

DI details

-----  
 Handle:0x7fb414b2dba8 Res-Type:ASIC\_RSC\_DI Res-Switch-Num:255 Asic-Num:255  
 Feature-ID:AL\_FID\_L3\_  
 MULTICAST\_IPV4 Lkp-ftr-id:LKP\_FEAT\_INVALID ref\_count:1  
 priv\_ri/priv\_si Handle:(nil) Hardware Indices/Handles: index0:0x538e  
 mtu\_index/l3u\_ri\_index0:0x0 index1:0x538e mtu\_index/l3u\_ri\_index1:0x0

## show tech-support platform layer3

```

Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00
00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Detailed Resource Information (ASIC# 0)
-----

Destination Index (DI) [0x538e]
portMap = 0x00000000          0
cmil = 0x385
rcpPortMap = 0

al_rsc_cmi
CPU Map Index (CMI) [0x385]
ctiLo0 = 0x9
ctiLo1 = 0
ctiLo2 = 0
cpuQNum0 = 0x9e
cpuQNum1 = 0
cpuQNum2 = 0
npuIndex = 0
strip_seg = 0x0
copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
-----

Destination Index (DI) [0x538e]
portMap = 0x00000000          0
cmil = 0x385
rcpPortMap = 0

al_rsc_cmi
CPU Map Index (CMI) [0x385]
ctiLo0 = 0x9
ctiLo1 = 0
ctiLo2 = 0
cpuQNum0 = 0x9e
cpuQNum1 = 0
cpuQNum2 = 0
npuIndex = 0
strip_seg = 0x0
copy_seg = 0x0

=====

RI details
-----
Handle:0x7fb414b30ed8 Res-Type:ASIC_RSC_RI_REP Res-Switch-Num:255 Asic-Num:255 Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: index0:0x5 mtu_index/13u_ri_index0:0x0

index1:0x5 mtu_index/13u_ri_index1:0x0
Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00
00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Detailed Resource Information (ASIC# 0)
-----

Detailed Resource Information (ASIC# 1)
-----

=====

```

```

SI details
-----
Handle:0x7fb414b321d8 Res-Type:ASIC_RSC_SI_STATS Res-Switch-Num:255 Asic-Num:255 Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: index0:0x4004 mtu_index/l3u_ri_index0:
0x0 sm handle 0:0x7fb414b2df98 index1:0x4004 mtu_index/l3u_ri_index1:0x0
Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00
00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Detailed Resource Information (ASIC# 0)
-----
Detailed Resource Information (ASIC# 1)
-----

=====

HTM details
-----
Handle:0x7fb414b2f348 Res-Type:ASIC_RSC_HASH_TCAM Res-Switch-Num:0 Asic-Num:255 Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_SG ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: handle0:0x7fb414b2f558
Detailed Resource Information (ASIC# 0)
-----
Number of HTM Entries: 1

Entry #0: (handle 0x7fb414b2f558)

KEY - src_addr:10.10.0.2 starg_station_index: 16387
MASK - src_addr:0.0.0.0 starg_station_index: 0
AD: use_starg_match: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0 rpf_valid: 1 rpf_le_ptr: 0

afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1 cpp_type: 0 dest_mod_index: 0
rp_index:
0 priority: 5 rpf_le: 36 station_index: 16388 capwap_mgid_present: 0 mgid 0

=====

```

The following is sample output from the **show tech-support platform layer3 unicast vrf** command:

```

Device# show tech-support platform layer3 unicast vrf vr1 dstIP 10.0.0.20
srcIP 10.0.0.10

```

```

.
.
.
destination IP: 10.0.0.20
source IP: 10.0.0.10
vrf name :

```

```

Switch/Stack Mac Address : 5006.ab89.0280 - Local Mac Address
Mac persistency wait time: Indefinite

```

Switch#	Role	Mac Address	Priority	H/W Version	Current State
*1	Active	5006.ab89.0280	1	V02	Ready

```

----- show switch -----

```

## show tech-support platform layer3

```
10.0.0.10 -> 10.0.0.20 =>IP adj out of GigabitEthernet1/0/7, addr 10.0.0.20
```

```
----- show ip cef exact-route platform 10.0.0.10 10.0.0.20 -----
```

```
nexthop is 10.0.0.20
```

```

Protocol Interface Address
IP GigabitEthernet1/0/7 10.0.0.20(8)
0 packets, 0 bytes
epoch 0
sourced in sev-epoch 0
Encap length 14
00211BFDE6495006AB8902C00800
L2 destination address byte offset 0
L2 destination address byte length 6
Link-type after encap: ip
ARP

```

```
----- show adjacency 10.0.0.20 detail -----
```

```

Routing entry for 10.0.0.0/24
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
* directly connected, via GigabitEthernet1/0/7
Route metric is 0, traffic share count is 1

```

```
----- show ip route 10.0.0.20 -----
```

```

10.0.0.20/32, epoch 3, flags [attached]
Adj source: IP adj out of GigabitEthernet1/0/7, addr 10.0.0.20 FF90E67820
Dependent covered prefix type adjfib, cover 10.0.0.0/24
attached to GigabitEthernet1/0/7

```

```
----- show ip cef 10.0.0.20 detail -----
```

```
ip prefix: 10.0.0.20/32
```

```
Forwarding Table
```

```

10.0.0.20/32 -> OBJ_ADJACENCY (29), urpf: 30
Connected Interface: 31
Prefix Flags: Directly L2 attached
OM handle: 0x10205416d8

```

```
----- show platform software ip switch 1 R0 cef prefix 10.0.0.20/32 detail -----
```

```
OBJ_ADJACENCY found: 29
```

```
Number of adjacency objects: 5
```

```
Adjacency id: 0x1d (29)
```

```
Interface: GigabitEthernet1/0/7, IF index: 31, Link Type: MCP_LINK_IP  
Encap: 0:21:1b:fd:e6:49:50:6:ab:89:2:c0:8:0  
Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500  
Flags: no-l3-inject  
Incomplete behavior type: None  
Fixup: unknown  
Fixup_Flags_2: unknown  
Nexthop addr: 10.0.0.20  
IP FRR MCP_ADJ_IPFRR_NONE 0  
OM handle: 0x1020541348
```

```
----- show platform software adjacency switch 1 R0 index 29 -----
```

```
Forwarding Table
```

```
10.0.0.20/32 -> OBJ_ADJACENCY (29), urpf: 30  
Connected Interface: 31  
Prefix Flags: Directly L2 attached  
aom id: 393, HW handle: (nil) (created)
```

```
----- show platform software ip switch 1 F0 cef prefix 10.0.0.20/32 detail -----
```

```
OBJ_ADJACENCY found: 29
```

```
Number of adjacency objects: 5
```

```
Adjacency id: 0x1d (29)
```

```
Interface: GigabitEthernet1/0/7, IF index: 31, Link Type: MCP_LINK_IP  
Encap: 0:21:1b:fd:e6:49:50:6:ab:89:2:c0:8:0  
Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500  
Flags: no-l3-inject  
Incomplete behavior type: None  
Fixup: unknown  
Fixup_Flags_2: unknown  
Nexthop addr: 10.0.0.20  
IP FRR MCP_ADJ_IPFRR_NONE 0  
aom id: 391, HW handle: (nil) (created)
```

```
----- show platform software adjacency switch 1 F0 index 29 -----
```

```
found aom id: 391
```

**show tech-support platform layer3**

```
Object identifier: 391
  Description: adj 0x1d, Flags None
  Status: Done, Epoch: 0, Client data: 0xc6a747a8
```

```
----- show platform software object-manager switch 1 F0 object 391 -----
```

```
Object identifier: 66
  Description: intf GigabitEthernet1/0/7, handle 31, hw handle 31, HW dirty: NONE AOM dirty
  NONE
  Status: Done
```

```
----- show platform software object-manager switch 1 F0 object 391 parents -----
```

```
Object identifier: 393
  Description: PREFIX 10.0.0.20/32 (Table id 0)
  Status: Done
```

```
.
.
.
```

Output fields are self-explanatory.

**Related Commands**

Command	Description
<b>show tech-support platform</b>	Displays detailed information about a platform for use by technical support.



# show tech-support platform mld\_snooping

To display Multicast Listener Discovery (MLD) snooping information about a group, use the **show tech-support platform mld\_snooping** command in privileged EXEC mode.

```
show tech-support platform mld_snooping [{Group_ipv6Addr ipv6-address }][{vlan vlan-ID}]
```

Syntax Description	Group_ipv6Addr	(Optional) Displays snooping information about the specified group address.
	<i>ipv6-address</i>	(Optional) IPv6 address of the group.
	<b>vlan</b> <i>vlan-ID</i>	(Optional) Displays MLD snooping VLAN information. Valid values are from 1 to 4094.

Command Modes	Privileged EXEC (#)
---------------	---------------------

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

**Usage Guidelines** The output of this command is very long. To better manage this output, you can redirect the output to an external file (for example, **show tech-support platform mld\_snooping | redirect flash:filename**) in the local writable storage file system or remote file system.

## Examples

The following is sample output from the **show tech-support platform mld\_snooping** command:

```
Device# show tech-support platform mld_snooping GroupIPv6Addr FF02::5:1
```

```
.
.
.
----- show running-config -----
```

```
Building configuration...
```

```
Current configuration : 11419 bytes
!
! Last configuration change at 09:17:04 UTC Thu Sep 6 2018
!
version 16.10
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
no platform punt-keepalive disable-kernel-core
!
hostname Switch
!
vrf definition Mgmt-vrf
```

```

!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
!
no aaa new-model
switch 1 provision ws-c3650-12x48uq
!
!
!
!
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email
address to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "profile-1"
  active
  destination transport-method http
  no destination transport-method email
!
!
!
!
!
ip admission watch-list expiry-time 0
!
!
!
login on-success log
!
!
!
!
no device-tracking logging theft
!
crypto pki trustpoint TP-self-signed-559433368
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-559433368
  revocation-check none
  rsakeypair TP-self-signed-559433368
!
crypto pki trustpoint SLA-TrustPoint
  enrollment pkcs12
  revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-559433368
certificate self-signed 01
  30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 35353934 33333336 38301E17 0D313531 32303331 32353432
  325A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3535 39343333
  33363830 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  AD8C9C3B FEE7FFC8 986837D2 4C126172 446C3C53 E040F798 4BA61C97 7506FDCE
  46365D0A E47E3F4F C774CA5B 73E2A8DD B72A2E98 C66DB196 94E8150F 0B669CF6
  AA5BC4CD FC2E02F6 FE08B17F 0164FC19 7DC84ABB C99D91D6 398233FF 814EF6DA
  6DC8FC20 CA12C0D6 1CB28EDA 6ADD6DFA 7E3E8281 4A189A9A AA44FCC0 BA9BD8A5
  02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D

```

```

23041830 16801448 668D668E C92914BB 69E9BA64 F61228DE 132E2030 1D060355
1D0E0416 04144866 8D668EC9 2914BB69 E9BA64F6 1228DE13 2E20300D 06092A86
4886F70D 01010505 00038181 0000F1D3 3DD1E5F1 EB714A95 D5819933 CAD0C943
59927D55 9D70CAD0 D64830EB D54380AD D2B5B613 F8AF7A5B 1F801134 246F760D
5E5515DB D098304F 5086F6CE 88E8B576 F6B93A88 F458FDCF 91A42D7E FA741908
5C892D78 600FB655 E6C5A4D0 6C1F1B9A 3AECA550 E3DC0881 01C4D004 7AB65BC3
88CF24DE DAA19474 51B535A5 0C
quit
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBA3 700A8BF7 D8F256EE
4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 COBD23CF 58BD7188
68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28
quit
!
!
!
diagnostic bootup level minimal
diagnostic monitor syslog
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
!
redundancy
mode sso
!
!
!
!
!
!
class-map match-any system-cpp-police-topology-control
description Topology control
class-map match-any system-cpp-police-sw-forward
description Sw forwarding, L2 LVX data, LOGGING
class-map match-any system-cpp-default
description EWLC control, EWLC data, Inter FED
class-map match-any system-cpp-police-sys-data
description Learning cache ovfl, High Rate App, Exception, EGR Exception, NFL SAMPLED

```



```
!  
!  
interface GigabitEthernet0/0  
  vrf forwarding Mgmt-vrf  
  no ip address  
  speed 1000  
  negotiation auto  
!  
interface GigabitEthernet1/0/1  
  switchport mode access  
  macsec network-link  
!  
interface GigabitEthernet1/0/2  
!  
interface GigabitEthernet1/0/3  
!  
interface TenGigabitEthernet1/1/1  
!  
interface TenGigabitEthernet1/1/2  
!  
interface TenGigabitEthernet1/1/3  
!  
interface TenGigabitEthernet1/1/4  
!  
interface Vlan1  
  no ip address  
  shutdown  
!  
ip forward-protocol nd  
ip http server  
ip http authentication local  
ip http secure-server  
!  
ip access-list extended AutoQos-4.0-wlan-Acl-Bulk-Data  
  permit tcp any any eq 22  
  permit tcp any any eq 465  
  permit tcp any any eq 143  
  permit tcp any any eq 993  
  permit tcp any any eq 995  
  permit tcp any any eq 1914  
  permit tcp any any eq ftp  
  permit tcp any any eq ftp-data  
  permit tcp any any eq smtp  
  permit tcp any any eq pop3  
ip access-list extended AutoQos-4.0-wlan-Acl-MultiEnhanced-Conf  
  permit udp any any range 16384 32767  
  permit tcp any any range 50000 59999  
ip access-list extended AutoQos-4.0-wlan-Acl-Scavenger  
  permit tcp any any range 2300 2400  
  permit udp any any range 2300 2400  
  permit tcp any any range 6881 6999  
  permit tcp any any range 28800 29100  
  permit tcp any any eq 1214  
  permit udp any any eq 1214  
  permit tcp any any eq 3689  
  permit udp any any eq 3689  
  permit tcp any any eq 11999  
ip access-list extended AutoQos-4.0-wlan-Acl-Signaling  
  permit tcp any any range 2000 2002  
  permit tcp any any range 5060 5061  
  permit udp any any range 5060 5061  
ip access-list extended AutoQos-4.0-wlan-Acl-Transactional-Data  
  permit tcp any any eq 443  
  permit tcp any any eq 1521
```

## show tech-support platform mld\_snooping

```

permit udp any any eq 1521
permit tcp any any eq 1526
permit udp any any eq 1526
permit tcp any any eq 1575
permit udp any any eq 1575
permit tcp any any eq 1630
permit udp any any eq 1630
permit tcp any any eq 1527
permit tcp any any eq 6200
permit tcp any any eq 3389
permit tcp any any eq 5985
permit tcp any any eq 8080
!
!
!
ipv6 access-list preauth_ipv6_acl
permit udp any any eq domain
permit tcp any any eq domain
permit icmp any any nd-ns
permit icmp any any nd-na
permit icmp any any router-solicitation
permit icmp any any router-advertisement
permit icmp any any redirect
permit udp any eq 547 any eq 546
permit udp any eq 546 any eq 547
deny ipv6 any any
!
control-plane
service-policy input system-cpp-policy
!
!
line con 0
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  login
line vty 5 15
  login
!
!
mac address-table notification mac-move
!
!
!
!
end

-----show switch | Include Ready-----

*1          Active   188b.9dfc.eb00    1          V00        Ready

----- show ipv6 mld snooping address | i FF02::5:1 -----

Vlan      Group                Type      Version    Port List
-----
123       FF02::5:1           mld      v2         Gi2/0/1

Device#

```

Output fields are self-explanatory.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ipv6 mld snooping</b>	Enables MLDv2 protocol snooping globally.
<b>show ipv6 mld snooping</b>	Displays MLDv2 snooping information.
<b>show tech-support platform</b>	Displays detailed information about a platform for use by technical support.

# show tech-support port

To display port-related information for use by technical support, use the **show tech-support port** command in privileged EXEC mode.

## show tech-support port

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Usage Guidelines

The output of the **show tech-support port** command is very long. To better manage this output, you can redirect the output to an external file (for example, **show tech-support port | redirect flash:filename**) in the local writable storage file system or remote file system.

The output of this command displays the following commands:

- **show clock**
- **show version**
- **show module**
- **show inventory**
- **show interface status**
- **show interface counters**
- **show interface counters errors**
- **show interfaces**
- **show interfaces capabilities**
- **show controllers**
- **show controllers utilization**
- **show idprom interface**
- **show controller ethernet-controller phy detail**
- **show switch**
- **show platform software fed switch active port summary**
- **show platform software fed switch ifm interfaces ethernet**
- **show platform software fed switch ifm mappings**
- **show platform software fed switch ifm mappings lpn**



- show platform software fed switch ifm mappings gpn
- show platform software fed switch ifm mappings port-le
- show platform software fed switch ifm if-id
- show platform software fed switch active port if\_id

## Examples

The following is sample output from the **show tech-support port** command:

```
Device# show tech-support port
.
.
.
----- show controllers utilization -----

Port          Receive Utilization  Transmit Utilization
Gi1/0/1       0 0
Gi1/0/2       0 0
Gi1/0/3       0 0
Gi1/0/4       0 0
Gi1/0/5       0 0
Gi1/0/6       0 0
Gi1/0/7       0 0
Gi1/0/8       0 0
Gi1/0/9       0 0
Gi1/0/10      0 0
Gi1/0/11      0 0
Gi1/0/12      0 0
Gi1/0/13      0 0
Gi1/0/14      0 0
Gi1/0/15      0 0
Gi1/0/16      0 0
Gi1/0/17      0 0
Gi1/0/18      0 0
Gi1/0/19      0 0
Gi1/0/20      0 0
Gi1/0/21      0 0
Gi1/0/22      0 0
Gi1/0/23      0 0
Gi1/0/24      0 0
Gi1/0/25      0 0
Gi1/0/26      0 0
Gi1/0/27      0 0
Gi1/0/28      0 0
Gi1/0/29      0 0
Gi1/0/30      0 0
Gi1/0/31      0 0
Gi1/0/32      0 0
Gi1/0/33      0 0
Gi1/0/34      0 0
Gi1/0/35      0 0
Gi1/0/36      0 0
Tel/0/37      0 0
Tel/0/38      0 0
Tel/0/39      0 0
Tel/0/40      0 0
Tel/0/41      0 0
Tel/0/42      0 0
Tel/0/43      0 0
Tel/0/44      0 0
```

## show tech-support port

```
Te1/0/45      0  0
Te1/0/46      0  0
Te1/0/47      0  0
Te1/0/48      0  0
Te1/1/1       0  0
Te1/1/2       0  0
Te1/1/3       0  0
Te1/1/4       0  0
```

```
Total Ports : 52
Total Ports Receive Bandwidth Percentage Utilization : 0
Total Ports Transmit Bandwidth Percentage Utilization : 0
```

```
Average Switch Percentage Utilization : 0
```

```
----- show idprom interface Gi1/0/1 -----
```

```
*Sep  7 08:57:24.249: No module is present
.
.
.
```

The output fields are self-explanatory.

# show tech-support pvlan

To display the private VLAN related information, use the **show tech-support pvlan** command in privileged EXEC mode.

```
show tech-support pvlan [{pvlan_id pvlan-id}]
```

<b>Syntax Description</b>	<b>pvlan_id</b> <i>pvlan-id</i>	Specifies the private VLAN ID.
<b>Command Default</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

**Usage Guidelines** The output from the **show tech-support pvlan** command is very long. To better manage this output, you can redirect the output to a file in the local writable storage file system or the remote file system by using the **show tech-support pvlan [ pvlan\_id pvlan-id ] | redirect location:filename** . Redirecting the output to a file also makes sending the output to your Cisco Technical Assistance Center (TAC) representative easier.

To view the output of the redirected file, use the command **more location:filename**.

# show tech-support resource

To display the switch resource information, use the **show tech-support resource** command in privileged EXEC mode.

## show tech-support resource

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

## Examples

The following is a sample output of the **show tech-support resource** command:

```
Device> enable
Device# show tech-support resource
----- show clock -----

*17:57:36.220 UTC Fri Jun 4 2021

----- show version -----

Cisco IOS XE Software, Version 17.03.03
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.3.3,
  RELEASE SOFTWARE (fc7)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Thu 04-Mar-21 12:32 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2021 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.

ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 17.5.2r, RELEASE SOFTWARE (P)

stack-nyqcr8 uptime is 3 weeks, 1 day, 19 hours, 18 minutes
Uptime for this control processor is 3 weeks, 1 day, 19 hours, 21 minutes
System returned to ROM by Reload Command
System image file is "flash:packages.conf"
Last reload reason: Reload Command
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to [export@cisco.com](mailto:export@cisco.com).

Technology Package License Information:

```

-----
Technology-package                               Technology-package
Current                                           Next reboot
-----
network-advantage   Smart License               network-advantage
dna-advantage       Subscription Smart License             dna-advantage
AIR License Level:  AIR DNA Advantage
Next reload AIR license Level:  AIR DNA Advantage

```

Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco C9300-48S (X86) processor with 1331521K/6147K bytes of memory.  
 Processor board ID FCW2315G10C  
 2 Virtual Ethernet interfaces  
 224 Gigabit Ethernet interfaces  
 36 2.5 Gigabit Ethernet interfaces  
 100 Ten Gigabit Ethernet interfaces  
 16 TwentyFive Gigabit Ethernet interfaces  
 16 Forty Gigabit Ethernet interfaces  
 48 Five Gigabit Ethernet interfaces  
 2048K bytes of non-volatile configuration memory.  
 8388608K bytes of physical memory.  
 1638400K bytes of Crash Files at crashinfo:.  
 11264000K bytes of Flash at flash:.

```

Base Ethernet MAC Address      : 4c:bc:48:97:ec:80
Motherboard Assembly Number    : 73-19406-03C
Motherboard Serial Number      : FOC23122J45
Model Revision Number          : A0
Motherboard Revision Number    : 07
Model Number                   : C9300-48S
System Serial Number           : FCW2315G10C
CLEI Code Number               : INM2900ARB

```

```

Switch Ports Model          SW Version  SW Image        Mode
-----
*   1 65    C9300-48S    17.03.03     CAT9K_IOSXE    INSTALL

```

Configuration register is 0x102

----- show running-config -----



```

revocation-check none
rsakeypair TP-self-signed-1829944574
!
crypto pki trustpoint DNAC-CA
  enrollment mode ra
  enrollment terminal
  usage ssl-client
  revocation-check crl none
!
crypto pki trustpoint SLA-TrustPoint
  enrollment pkcs12
  revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-1829944574
certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31383239 39343435 3734301E 170D3231 30353132 32323132
  33375A17 0D333130 35313232 32313233 375A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 38323939
  34343537 34308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
  0A028201 0100DDCC BF7D66CE FFE20EF3 725757F3 6FAFC721 94D4D60B 6233AD79
  E69AA12C 434C6ECE 98A34568 870DF666 CC4C09EA A80AE81C D607FAA3 A8B3022E
  0700AC7C 55B79266 C628FE55 1CA371A0 B5C47C4D 5445996A 0E6ADFB0 C1FF962D
  4F363522 A3CA9E43 736CA7A9 4C350C13 F4C2B5EC 59EDEAEC D7D74EF4 BF4ECE77
  4B625216 F5DD11C0 B667F9D4 1A6681E1 197B2C18 E7767A0A B798E120 D4616BCB
  99DD3D44 2F55BB2E ED85826F 91AE530E 968AD28F 36767EEE 4597726E 2D997AA0
  CDD33E49 7B814E3D 03C90538 C410F9F4 59147E4F 083B4143 40482C56 0CE5D3CD
  D3C6B337 E768E664 10FF3E35 93624B3F 187AD6A4 55C404BE F1993665 B18FC6A3
  4B968C9E 92E10203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
  301F0603 551D2304 18301680 14FDB525 614E9C81 4060EFC6 349A80E2 8B0F25F9
  28301D06 03551D0E 04160414 FDB52561 4E9C8140 60EFC634 9A80E28B 0F25F928
  300D0609 2A864886 F70D0101 05050003 82010100 2EACE5C4 6BB136E5 28204E25
  EE8C0514 21ECC597 24BC3B3B D72A34CB CBF950CC 82BADAE2 F58CD72B BE0A0BB9
  509946C4 F1DC5E8D 10184A79 33050AC0 8CD235DA 501C47BA 6920B007 FDF82BD3
  448A1E05 0C726EA7 6F641AA9 6A6172C0 4E2EAB90 CF758F0B 08A5F319 83D42DA1
  B0DF87FE E255864C 5DC87D26 339309D3 813E0B66 FD916E73 2319F717 6F8EF279
  5F13A7CC 2C5A6BA9 052E8D13 6D27B405 41984D8C DDB15B21 11E06F27 D36723F6
  85274D7A 994A8543 F6D8B8B1 9E94AAA9 AA660F19 951E2DB8 EA473526 89ED4161
  CCBF2032 9D03BF11 92FB4D62 8AA3A09D 374DB7DD 8566452B 4DEA0AF4 5B0D88B1
  B355144A FC6CC495 8058EFB2 4CF83651 149BA5DB
quit
crypto pki certificate chain DNAC-CA
certificate ca 43338DDB13667FF821F1D6502649F8926E67C11C
  308203A5 3082028D A0030201 02021443 338DDB13 667FF821 F1D65026 49F8926E
  67C11C30 0D06092A 864886F7 0D01010B 05003062 312D302B 06035504 030C2437
  36613236 3864642D 38393936 2D366138 322D6533 65352D34 36663366 62656137
  65306431 16301406 0355040A 0C0D4369 73636F20 53797374 656D7331 19301706
  0355040B 0C104369 73636F20 444E4120 43656E74 6572301E 170D3231 30343233
  32303431 30315A17 0D323430 31313832 30343130 315A3062 312D302B 06035504
  030C2437 36613236 3864642D 38393936 2D366138 322D6533 65352D34 36663366
  62656137 65306431 16301406 0355040A 0C0D4369 73636F20 53797374 656D7331
  19301706 0355040B 0C104369 73636F20 444E4120 43656E74 65723082 0122300D
  06092A86 4886F70D 01010105 00038201 0F003082 010A0282 010100AF 43FF5F25
  74C29B94 6E2A0FA1 A45D07B3 FD560BEC 0603B1C4 8B140AA3 A69877B8 6FAE6348
  8C7D9D3B AFDD99D2 235098C5 C5B56FD1 3EFC8258 6FD37FEE 1783B463 A490022A
  EED21295 B20CACB3 24273372 DF15FBAB A396FB54 FF348FB1 B3A34B49 59B1113A
  66595D17 EBE521A2 E3AA10BF 766F3A83 8046F031 26F0A642 609CF57D 6F6BCE6C
  5CFA6105 C783F6C6 3D414CB9 A5A572E6 FEB4CD9F D9B66208 D253F222 A2DEFEB9
  626C2AC5 6B4532DA 39429736 55D99A14 4A69D702 158469D6 5F6A6CBF A311B98F
  D459851C 5C45875A 88619DF5 22220D6C B689FE6F 989C8573 2E5492EE 9F69E108
  0892726B BB7CD254 FFE9AEAA 769395F5 1A930E7B 4AD0B5C6 603D2B02 03010001
  A3533051 301D0603 551D0E04 160414CC 002C9091 065EE9E7 003B5F10 ED1A1ED3

```

## show tech-support resource

```

76D4DD30 1F060355 1D230418 30168014 CC002C90 91065EE9 E7003B5F 10ED1A1E
D376D4DD 300F0603 551D1301 01FF0405 30030101 FF300D06 092A8648 86F70D01
010B0500 03820101 00719B9F 5D4F7FFE 29071394 1E82BF02 7F8BF38E 796BDFC7
DF2750DC 7D146E0D 094F17C6 6A8559E6 090FEA1E E2734F18 4A7D8647 A1AD4190
E0B0153A 447E9CC3 4A87B2D2 9A752F09 776CE638 4404391F F898179E 73752372
7108D675 5859CC7E C2AABAA9 C1027074 3B2E0195 02F2822C 14B7F168 EC4F91D1
A4EEEA07 73F92A61 9B6AE69F 379F3F77 CEF6A89B 0270F25F 2319E4FD 3795DFB6
C4E206FB 8E2A236A D3A2D012 DEDEB99D 8DE1C4A1 D4BE3AEC 97A2CDE3 7DB719FC
99DB5D14 4D00CBF8 EF67CE28 AC77AE17 88ECDAA5 199F7F88 9F513851 37ECCA2F
42781701 C5FC45C2 D8B0CE82 1306D4E4 7C617076 FB562A07 A3CAF126 5B860C56
582F1A97 E5AF26B5 65
quit
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
3082031B 30820203 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
2F310E30 0C060355 040A1305 43697363 6F311D30 1B060355 04031314 4C696365
6E73696E 6720526F 6F74202D 20444556 301E170D 31333034 32343231 35353433
5A170D33 33303432 34323135 3534335A 302F310E 300C0603 55040A13 05436973
636F311D 301B0603 55040313 144C6963 656E7369 6E672052 6F6F7420 2D204445
56308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201 0A028201
01009C56 7101D61E DF2EBCC3 BA7AE0DB B241B3B4 328A9B00 EB8A80D0 2AA86F5E
F1AEBFDE B67BD6AD 7DAD7B43 F582753B FFCC1CA5 A7841A07 6934D3AF 99078EF6
179196FA 4FB3F2ED 3942C756 BF1CA0A9 CC98A7A7 F9E43724 D9E61D47 89E9E792
DD9F27B4 517C2BDE D0EB5B9A 787BA085 D9BBF003 F0563BE0 A4450C8F 127B5583
3EBC1385 2D9BAD98 68D3AE07 5C27987C 6B814B99 0686E14A 5F61753C 813089E6
AEC48C68 F6D45267 0E365F44 B4456E11 96DCB950 233C8ADB 9FEEBAF1 2B5F3BB6
7CE521B5 F277EBF6 03B7B0A4 958C9C7D 5460C20B CF9CCFC7 14B80F58 B5268947
6D081172 26916B41 FB07DF42 EB9B9408 EC346138 23FBD8C4 19909697 A30845F3
01C50203 010001A3 42304030 0E060355 1D0F0101 FF040403 02010630 0F060355
1D130101 FF040530 030101FF 301D0603 551D0E04 16041443 214521B5 FB217A1A
4D1BB702 36E664CB EC8B6530 0D06092A 864886F7 0D01010B 05000382 01010085
F1B1F2AE AE7D2F9C AB0351C3 29E3F1AE 982DF11F 5E3C90F6 00B3CDED 5A1491FB
DF07E06C AA0F4325 9FB4C4AE 2080F675 8C3B7AC5 4EAAA03E C5B50A2F 670AFF87
EDA6462F CFC43967 C024AB32 EE3CCDCF A04B9DAE 1BBABBDA C8DF5587 CF51CB1C
005A282F 8B518A5A 8C6F9B3C AABA3446 32EF3A75 C2F45450 7A9BCFD3 0C8BE54A
11872DE0 CF1200D0 D1018FD9 AC685968 167E421C 9BC394ED 9BC85463 83B28146
07B2BDED DFC1605B 4D16007B 68723E25 55908512 4EEB0A70 B2A74C2A CB1EC882
C3215B87 6FC74304 241E59D7 C7C02C6D BD3042F5 196E8133 7A4446A4 81216E70
CF52CF22 50A7D23E FA9F6B07 FB0F6386 9DCC3BBC 65250693 38CF6BA6 CB8EFD
quit
!
!
license boot level network-advantage addon dna-advantage
license smart transport off
<output truncated>

```



# show version

To display information about the currently loaded software along with hardware and device information, use the **show version** command in user EXEC or privileged EXEC mode.

**show version** [{switch *node*}] [{**installed** | **provisioned** | **running**}]

Syntax Description	switch <i>node</i>	(optional) Only a single switch may be specified. Default is all switches in a stacked system.
	<b>running</b>	(optional) Specifies information on the files currently running.
	<b>provisioned</b>	(optional) Specifies information on the software files that are provisioned.
	<b>installed</b>	Specifies information on the software installed on the RP
	<b>user-interface</b>	Specifies information on the files related to the user-interface.

**Command Default** No default behavior or values.

**Command Modes** User EXEC (>)

Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** This command displays information about the Cisco IOS software version currently running on a device, the ROM Monitor and Bootflash software versions, and information about the hardware configuration, including the amount of system memory. Because this command displays both software and hardware information, the output of this command is the same as the output of the **show hardware** command. (The **show hardware** command is a command alias for the **show version** command.)

Specifically, the **show version** command provides the following information:

- Software information
  - Main Cisco IOS image version
  - Main Cisco IOS image capabilities (feature set)
  - Location and name of bootfile in ROM
  - Bootflash image version (depending on platform)
- Device-specific information
  - Device name
  - System uptime
  - System reload reason
  - Config-register setting
  - Config-register settings for after the next reload (depending on platform)

- Hardware information
  - Platform type
  - Processor type
  - Processor hardware revision
  - Amount of main (processor) memory installed
  - Amount I/O memory installed
  - Amount of Flash memory installed on different types (depending on platform)
  - Processor board ID

The output of this command uses the following format:

```
Cisco IOS Software, <platform> Software (<image-id>), Version <software-version>,
  <software-type>

Technical Support: http://www.cisco.com/techsupport
Copyright (c) <date-range> by Cisco Systems, Inc.
Compiled <day> <date> <time> by <compiler-id>

ROM: System Bootstrap, Version <software-version>, <software-type>
BOOTLDR: <platform> Software (image-id), Version <software-version>, <software-type>

<router-name> uptime is <w> weeks, <d> days, <h> hours,
<m> minutes
System returned to ROM by reload at <time> <day> <date>
System image file is "<filesystem-location>/<software-image-name>"
Last reload reason: <reload-reason>Cisco <platform-processor-type>
processor (revision <processor-revision-id>) with <free-DRAM-memory>
K/<packet-memory>K bytes of memory.
Processor board ID <ID-number>

<CPU-type> CPU at <clock-speed>Mhz, Implementation <number>, Rev <
Revision-number>, <kilobytes-Processor-Cache-Memory>KB <cache-Level> Cache
```

See the Examples section for descriptions of the fields in this output.

Entering **show version** displays the IOS XE software version and the IOS XE software bundle which includes a set of individual packages that comprise the complete set of software that runs on the switch.

The **show version running** command displays the list of individual packages that are currently running on the switch. When booted in installed mode, this is typically the set of packages listed in the booted provisioning file. When booted in bundle mode, this is typically the set of packages contained in the bundle.

The **show version provisioned** command displays information about the provisioned package set.

The following is sample output from the **show version** command on a Cisco Catalyst 9300 Series Switch:

```
Device# show version
Cisco IOS XE Software, Version BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Experimental Version
 16.10.20180903:072347
[v1610_throttle-/nobackup/mcpre/BLD-BLD_V1610_THROTTLE_LATEST_20180903_070602 183]
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Mon 03-Sep-18 11:53 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
```

All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.

ROM: IOS-XE ROMMON  
 BOOTLDR: System Bootstrap, Version 16.10.1r, RELEASE SOFTWARE (P)

C9300 uptime is 20 hours, 7 minutes  
 Uptime for this control processor is 20 hours, 8 minutes  
 System returned to ROM by Image Install  
 System image file is "flash:packages.conf"  
 Last reload reason: Image Install

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:  
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to [export@cisco.com](mailto:export@cisco.com).

Technology Package License Information:

Technology-package Current	Type	Technology-package Next reboot
network-advantage	Smart License	network-advantage
dna-advantage	Subscription Smart License	dna-advantage

Smart Licensing Status: UNREGISTERED/EVAL MODE

cisco C9300-24U (X86) processor with 1415813K/6147K bytes of memory.  
 Processor board ID FCW2125LOBH  
 8 Virtual Ethernet interfaces  
 56 Gigabit Ethernet interfaces  
 16 Ten Gigabit Ethernet interfaces  
 4 TwentyFive Gigabit Ethernet interfaces  
 4 Forty Gigabit Ethernet interfaces  
 2048K bytes of non-volatile configuration memory.  
 8388608K bytes of physical memory.  
 1638400K bytes of Crash Files at crashinfo:.  
 1638400K bytes of Crash Files at crashinfo-2:.  
 11264000K bytes of Flash at flash:.  
 11264000K bytes of Flash at flash-2:.  
 0K bytes of WebUI ODM Files at webui:.

## show version

```

Base Ethernet MAC Address      : 70:d3:79:be:6c:80
Motherboard Assembly Number   : 73-17954-06
Motherboard Serial Number     : FOC21230KPX
Model Revision Number         : A0
Motherboard Revision Number   : A0
Model Number                   : C9300-24U
System Serial Number          : FCW2125L0BH

```

Switch	Ports	Model	SW Version	SW Image	Mode
*	1 40	C9300-24U	16.10.1	CAT9K_IOSXE	INSTALL
	2 40	C9300-24U	16.10.1	CAT9K_IOSXE	INSTALL

```
Switch 02
```

```
Switch uptime : 20 hours, 8 minutes
```

```

Base Ethernet MAC Address      : 70:d3:79:84:85:80
Motherboard Assembly Number   : 73-17954-06
Motherboard Serial Number     : FOC21230KPK
Model Revision Number         : A0
Motherboard Revision Number   : A0
Model Number                   : C9300-24U
System Serial Number          : FCW2125L03W
Last reload reason            : Image Install

```

```
Configuration register is 0x102
```

In the following example, the **show version running** command is entered on a Cisco Catalyst 9300 Series Switch to view information about the packages currently running on both switches in a 2-member stack:

```

Device# show version running
Package: Provisioning File, version: n/a, status: active
  Role: provisioning file
  File: /flash/packages.conf, on: RP0
  Built: n/a, by: n/a
  File SHA1 checksum: 6a43991bae5b94de0df8083550f827a3c01756c5

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
active
  Role: rp_base
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpboot, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
active
  Role: rp_boot
  File: /flash/cat9k-rpboot.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: n/a

Package: guestshell, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: active
  Role: guestshell
  File:
/flash/cat9k-guestshell.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0/0

```

```

Built: 2018-09-03_13.11, by: mcpre
File SHA1 checksum: 10827f9f9db3b016d19a926acc6be0541440b8d7

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
active
  Role: rp_daemons
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0/0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
active
  Role: rp_iosd
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0/0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
active
  Role: rp_security
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0/0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: webui, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
active
  Role: rp_webui
  File: /flash/cat9k-webui.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0/0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 5112d7749b38fa1e122ce6ee1bfb266ad7eb553a

Package: srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
active
  Role: srdriver
  File:
/flash/cat9k-srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on:
RP0/0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: aff411e981a8dfc8de14005cc33462dc69f8bfaf

Package: cc_srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: active
  Role: cc_srdriver
  File:
/flash/cat9k-cc_srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: SIP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: e3da784f3e61ef1e153028e53d9dc94b2c9b1bf7

```

In the following example, the **show version provisioned** command is entered on a Cisco Catalyst 9300 Series Switch that is the active switch in a 2-member stack. The **show version provisioned** command displays information about the packages in the provisioned package set.

```

Device# show version provisioned
Package: Provisioning File, version: n/a, status: active
  Role: provisioning file
  File: /flash/packages.conf, on: RP0
  Built: n/a, by: n/a
  File SHA1 checksum: 6a43991bae5b94de0df8083550f827a3c01756c5

```

```
Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: rp_base
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: guestshell, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
  Role: guestshell
  File:
/flash/cat9k-guestshell.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 10827f9f9db3b016d19a926acc6be0541440b8d7

Package: rpboot, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: rp_boot
  File: /flash/cat9k-rpboot.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: n/a

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: rp_daemons
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: rp_iosd
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: rp_security
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: webui, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: rp_webui
  File: /flash/cat9k-webui.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 5112d7749b38fa1e122ce6ee1bfb266ad7eb553a

Package: wlc, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: rp_wlc
  File: /flash/cat9k-wlc.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
```

```

File SHA1 checksum: ada21bb3d57e1b03e5af2329503ed6caa7236d6e

Package: srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: srdriver
  File:
/flash/cat9k-srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on:
RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: aff411e981a8dfc8de14005cc33462dc69f8bfaf

Package: espbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: fp
  File: /flash/cat9k-espbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: ESP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 1a2317485f285a3945b31ae57aa64c56ed30a8c0

Package: sipbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: cc
  File: /flash/cat9k-sipbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: SIP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: ce821195f0c0bd5e44f21e32fca76cf9b2eed02b

Package: sipspa, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: cc_spa
  File: /flash/cat9k-sipspa.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: SIP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 54645404860b662d72f8ff7fa5e6e88cb0960e20

Package: cc_srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
  Role: cc_srdriver
  File:
/flash/cat9k-cc_srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: SIP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: e3da784f3e61ef1e153028e53d9dc94b2c9b1bf7

```

**Table 18: Table 5, show version running Field Descriptions**

Field	Description
Package:	The individual sub-package name.
version:	The individual sub-package version.
status:	Reveals if the package is active or inactive for the specific Supervisor module.
File:	The filename of the individual package file.
on:	The slot number of the Active or Standby Supervisor that this package is running on.
Built:	The date the individual package was built.

# system env temperature threshold yellow

To configure the difference between the yellow and red temperature thresholds that determines the value of yellow threshold, use the **system env temperature threshold yellow** command in global configuration mode. To return to the default value, use the **no** form of this command.

```
system env temperature threshold yellow value
no system env temperature threshold yellow value
```

## Syntax Description

*value* Specifies the difference between the yellow and red threshold values (in Celsius). The range is 10 to 25.

## Command Default

These are the default values

*Table 19: Default Values for the Temperature Thresholds*

Device	Difference between Yellow and Red	Red <sup>1</sup>
Catalyst 9300	14°C	60°C

<sup>1</sup> You cannot configure the red temperature threshold.

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

## Usage Guidelines

You cannot configure the green and red thresholds but can configure the yellow threshold. Use the **system env temperature threshold yellow** *value* global configuration command to specify the difference between the yellow and red thresholds and to configure the yellow threshold. For example, if the red threshold is 66 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 15** command. For example, if the red threshold is 60 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 9 by using the **system env temperature threshold yellow 9** command.



**Note** The internal temperature sensor in the device measures the internal system temperature and might vary  $\pm 5$  degrees C.

## Examples

This example sets 15 as the difference between the yellow and red thresholds:

```
Device(config)# system env temperature threshold yellow 15
Device(config)#
```





## test cable-diagnostics tdr

To run the Time Domain Reflector (TDR) feature on an interface, use the **test cable-diagnostics tdr** command in privileged EXEC mode.

**test cable-diagnostics tdr interface** *interface-id*

---

### Syntax Description

*interface-id* The interface on which to run TDR.

---

### Command Default

No default behavior or values.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

---

### Usage Guidelines

TDR is supported only on 10/100/100 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports or small form-factor pluggable (SFP) module ports.

After you run TDR by using the **test cable-diagnostics tdr interface** *interface-id* command, use the **show cable-diagnostics tdr interface** *interface-id* privileged EXEC command to display the results.

This example shows how to run TDR on an interface:

```
Device# test cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test started on interface Gi1/0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results
```

If you enter the **test cable-diagnostics tdr interface** *interface-id* command on an interface that has an link up status and a speed of 10 or 100 Mb/s, these messages appear:

```
Device# test cable-diagnostics tdr interface gigabitethernet1/0/3
TDR test on Gi1/0/9 will affect link state and traffic
TDR test started on interface Gi1/0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

## traceroute mac

To display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address, use the **traceroute mac** command in privileged EXEC mode.

```
traceroute mac [ interface interface-id ] source-mac-address [ interface interface-id ]
destination-mac-address [ vlan vlan-id ] [ detail ]
```

### Syntax Description

<b>interface</b> <i>interface-id</i>	(Optional) Specifies an interface on the source or destination device.
<i>source-mac-address</i>	The MAC address of the source device in hexadecimal format.
<i>destination-mac-address</i>	The MAC address of the destination device in hexadecimal format.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source device to the destination device. Valid VLAN IDs are 1 to 4094.
<b>detail</b>	(Optional) Specifies that detailed information appears.

### Command Default

No default behavior or values.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.
Cisco IOS XE Bengaluru 17.5.1	<b>aborted</b> was replaced with <b>terminated</b> in the output error message for the <b>traceroute mac</b> command.

### Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all of the devices in the network. Do not disable CDP.

When the device detects a device in the Layer 2 path that does not support Layer 2 traceroute, the device continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and an error message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN.

If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong.

If the VLAN is not specified, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port).

When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

## Examples

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Device# tracert mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5          (2.2.5.5      ) :   Gi0/0/3 => Gi0/0/1
con1          (2.2.1.1      ) :   Gi0/0/1 => Gi0/0/2
con2          (2.2.2.2      ) :   Gi0/0/2 => Gi0/0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows how to display the Layer 2 path by using the **detail** keyword:

```
Device# tracert mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 / WS-C3750E-24PD / 2.2.6.6 :
      Gi0/0/2 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
      Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
      Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
      Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination devices:

```
Device# tracert mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5          (2.2.5.5      ) :   Gi0/0/3 => Gi0/0/1
con1          (2.2.1.1      ) :   Gi0/0/1 => Gi0/0/2
con2          (2.2.2.2      ) :   Gi0/0/2 => Gi0/0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows the Layer 2 path when the device is not connected to the source device:

```
Device# tracert mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
```

```
Source 0000.0201.0501 found on con5[WS-C3750E-24TD] (2.2.5.5)
con5 / WS-C3750E-24TD / 2.2.5.5 :
    Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows the Layer 2 path when the device cannot find the destination port for the source MAC address:

```
Device# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace terminated.
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Device# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace terminated.
```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Device# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

This example shows the Layer 2 path when source and destination devices belong to multiple VLANs:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace terminated.
```

## tracert mac ip

To display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname, use the **tracert mac ip** command in privileged EXEC mode.

```
tracert mac ip { source-ip-address source-hostname } { destination-ip-address
destination-hostname } [detail]
```

### Syntax Description

<i>source-ip-address</i>	The IP address of the source device as a 32-bit quantity in dotted-decimal format.
<i>source-hostname</i>	The IP hostname of the source device.
<i>destination-ip-address</i>	The IP address of the destination device as a 32-bit quantity in dotted-decimal format.
<i>destination-hostname</i>	The IP hostname of the destination device.
<b>detail</b>	(Optional) Specifies that detailed information appears.

### Command Default

No default behavior or values.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.
Cisco IOS XE Bengaluru 17.5.1	<b>aborted</b> was replaced with <b>terminated</b> in the output error message for the <b>tracert mac ip</b> command.

### Usage Guidelines

For Layer 2 tracert to function properly, Cisco Discovery Protocol (CDP) must be enabled on each device in the network. Do not disable CDP.

When the device detects a device in the Layer 2 path that does not support Layer 2 tracert, the device continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **tracert mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet.

When you specify the IP addresses, the device uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the device uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the device sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 tracert feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port).

When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

### Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Device# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C3750E-24TD / 2.2.6.6 :
    Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
    Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Device# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5          (2.2.5.5      ) :   Gi0/0/3 => Gi0/1
con1          (2.2.1.1      ) :   Gi0/0/1 => Gi0/2
con2          (2.2.2.2      ) :   Gi0/0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

This example shows the Layer 2 path when ARP cannot associate the source IP address with the corresponding MAC address:

```
Device# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace terminated.
```

# type

To display the contents of one or more files, use the **type** command in boot loader mode.

**type** *filesystem:/file-url...*

<b>Syntax Description</b>	<i>filesystem:</i> Alias for a file system. Use <b>flash:</b> for the system board flash device; use <b>usbflash0:</b> for USB memory sticks.
---------------------------	---

<i>/file-url...</i>	Path (directory) and name of the files to display. Separate each filename with a space.
---------------------	---

<b>Command Default</b>	No default behavior or values.
------------------------	--------------------------------

<b>Command Modes</b>	Boot loader
----------------------	-------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

<b>Usage Guidelines</b>	<p>Filenames and directory names are case sensitive.</p> <p>If you specify a list of files, the contents of each file appear sequentially.</p>
-------------------------	--

<b>Examples</b>	This example shows how to display the contents of a file:
-----------------	---

```
Device: type flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```



# unset

To reset one or more environment variables, use the **unset** command in boot loader mode.

**unset** *variable*...

## Syntax Description

*variable*

Use one of these keywords for *variable*:

**MANUAL\_BOOT**—Specifies whether the device automatically or manually boots.

**BOOT**—Resets the list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash: file system.

**ENABLE\_BREAK**—Specifies whether the automatic boot process can be interrupted by using the **Break** key on the console after the flash: file system has been initialized.

**HELPER**—Identifies the semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.

**PS1**—Specifies the string that is used as the command-line prompt in boot loader mode.

**CONFIG\_FILE**—Resets the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.

**BAUD**—Resets the rate in bits per second (b/s) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting.

## Command Default

No default behavior or values.

## Command Modes

Boot loader

## Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

## Usage Guidelines

Under typical circumstances, it is not necessary to alter the setting of the environment variables.

The **MANUAL\_BOOT** environment variable can also be reset by using the **no boot manual** global configuration command.

The **BOOT** environment variable can also be reset by using the **no boot system** global configuration command.

The **ENABLE\_BREAK** environment variable can also be reset by using the **no boot enable-break** global configuration command.

The HELPER environment variable can also be reset by using the **no boot helper** global configuration command.

The CONFIG\_FILE environment variable can also be reset by using the **no boot config-file** global configuration command.

### Example

This example shows how to unset the SWITCH\_PRIORITY environment variable:

```
Device: unset SWITCH_PRIORITY
```

# upgrade rom-monitor capsule

To upgrade the read-only memory monitor (ROMMON) by using the capsule method, use the **upgrade rom-monitor capsule** command in privileged EXEC mode.

## Standalone Devices

```
upgrade rom-monitor capsule {golden | primary} [{R0 | RP active}]
```

## Device with High Availability

```
upgrade rom-monitor capsule {golden | primary} [{R0 | R1 | RP {active | standby}}]
```

## Device with StackWise Virtual

```
upgrade rom-monitor capsule {golden | primary} [{R0 | R1 | RP {active | standby} | switch {switch_number | active | standby}} {R0 | R1 | RP {active | standby}}]
```

Syntax Description		
<b>golden</b>		Specifies the golden ROMMON to be upgraded.
<b>primary</b>		Specifies the primary ROMMON to be upgraded.
<b>R0</b>		Upgrades the ROMMON of the Route Processor (RP) slot 3.
<b>R1</b>		Upgrades the ROMMON of the RP slot 4.
<b>RP {active   standby}</b>		Upgrades the ROMMON of the RP slot 1 and slot 2. <ul style="list-style-type: none"> <li>• <b>active</b>: Specifies the active instance.</li> <li>• <b>standby</b>: Specifies the standby instance.</li> </ul>
<b>switch {switch_number   active   standby}</b>		Specifies the switch. <ul style="list-style-type: none"> <li>• <i>switch_number</i>: ID of the switch. The range is from 1 to 2.</li> <li>• <b>active</b>: Specifies the active switch.</li> <li>• <b>standby</b>: Specifies the standby switch.</li> </ul>

**Command Default** This command has no default settings.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Amsterdam 17.1.1	This command was introduced.

**Usage Guidelines** To know if a ROMMON version upgrade is applicable to a software version, see the release notes of the corresponding software release:

<https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/products-release-notes-list.html>

---

**Examples**

This example shows how to upgrade the golden ROMMON on a device with StackWise Virtual:

```
Device# upgrade rom-monitor capsule golden switch active R0
```

```
This operation will reload the switch and take a few minutes to complete.
```

```
Do you want to proceed (y/n)? [confirm]y
```

```
Device#
```

```
Initializing Hardware .....
```

```
!  
!  
!
```

```
Warning : New region (type 2) access rights will be modified
```

```
Updating Block at FFFFF000h 100%
```

```
Restarting switch to complete capsule upgrade
```

```
<output truncated>
```

# version

To display the boot loader version, use the **version** command in boot loader mode.

## **version**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** No default behavior or values.

---

**Command Modes** Boot loader

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

---

---

**Examples** This example shows how to display the boot loader version on a device:

