



C Commands

This chapter describes the Cisco NX-OS security commands that begin with C.

class (policy map)

To specify a control plane class map for a control plane policy map, use the **class** command. To delete a control plane class map from a control plane policy map, use the **no** form of this command.

```
class { class-map-name [insert-before class-map-name2] | class-default }
```

```
no class class-map-name
```

Syntax Description	
<i>class-map-name</i>	Name of the class map.
insert-before <i>class-map-name2</i>	(Optional) Inserts the control plane class map ahead of another control plane class map for the control plane policy map.
class-default	Specifies the default class.

Defaults	None
-----------------	------

Command Modes	Policy map configuration
----------------------	--------------------------

SupportedUserRoles	network-admin vdc-admin
---------------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to configure a class map for a control plane policy map:

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)
```

This example shows how to delete a class map from a control plane policy map:

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# no class ClassMapA
```

Related Commands

Command	Description
policy-map type control-plane	Specifies a control plane policy map and enters policy map configuration mode.
show policy-map type control-plane	Displays configuration information for control plane policy maps.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

class-map type control-plane

To create or specify a control plane class map and enter class map configuration mode, use the **class-map type control-plane** command. To delete a control plane class map, use the **no** form of this command.

```
class-map type control-plane [match-all | match-any] class-map-name
```

```
no class-map type control-plane [match-all | match-any] class-map-name
```

Syntax Description		
match-all	(Optional)	Specifies to match all match conditions in the class map.
match-any	(Optional)	Specifies to match any match conditions in the class map.
<i>class-map-name</i>		Name of the class map. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.

Defaults	
match-any	

Command Modes	
Global configuration	

Supported User Roles	
network-admin vdc-admin	

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	
You cannot use match-all, match-any, or class-default as names for control plane class maps.	
You can use this command only in the default virtual device context (VDC).	
This command does not require a license.	

Examples	
This example shows how to specify a control plane class map and enter class map configuration mode:	

```
switch# config t
switch(config)# class-map type control-plane ClassMapA
switch(config-cmap)#
```

This example shows how to delete a control plane class map:

```
switch# config t
switch(config)# no class-map type control-plane ClassMapA
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	show class-map type control-plane	Displays control plane policy map configuration information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear access-list counters

To clear the counters for all IPv4 and MAC access control lists (ACLs) or a single ACL, use the **clear access-list counters** command.

```
clear access-list counters [access-list-name]
```

Syntax Description	<i>access-list-name</i> (Optional) Name of the ACL whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters.
---------------------------	--

Defaults	None
-----------------	------

Command Modes	Privileged EXEC
----------------------	-----------------

Supported User Roles	network-admin vdc-admin
-----------------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples This example shows how to clear counters for all IPv4 and MAC ACLs:

```
switch# clear access-list counters
switch#
```

This example shows how to clear counters for an IPv4 ACL named acl-ipv4-01:

```
switch# clear access-list counters acl-ipv4-01
switch#
```

Related Commands	Command	Description
	clear ip access-list counters	Clears counters for IPv4 ACLs.
	clear mac access-list counters	Clears counters for MAC ACLs.
	show access-lists	Displays information about one or all IPv4 and MAC ACLs.

Send document comments to nexus7k-docfeedback@cisco.com

clear accounting log

To clear the accounting log, use the **clear accounting log** command.

clear accounting log

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Any command mode

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines The command operates only in the default virtual device context (VDC 1).
This command does not require a license.

Examples This example shows how to clear the accounting log:

```
switch# clear accounting log
```

Related Commands	Command	Description
	show accounting log	Displays the accounting log contents.

Send document comments to nexus7k-docfeedback@cisco.com

clear copp statistics

To clear control plane policing (CoPP) statistics, use the **clear copp statistics** command.

```
clear copp statistics
```

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Any configuration mode

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines You can use this command only in the default virtual device context (VDC).
This command does not require a license.

Examples This example shows how to specify a control plane class map and enter class map configuration mode:

```
switch# clear copp statistics
```

Related Commands	Command	Description
	show policy-map interface control-plane	Displays the CoPP statistics for interfaces.

Send document comments to nexus7k-docfeedback@cisco.com

clear dot1x

To clear 802.1X authenticator instances, use the **clear dot1x** command.

```
clear dot1x {all | interface ethernet slot/port}
```

Syntax Description	all Specifies all 802.1X authenticator instances.						
	interface ethernet slot/port Specifies the 802.1X authenticator instances for a specified interface.						
Defaults	None						
Command Modes	Any command mode						
Supported User Roles	network-admin vdc-admin						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(1)	This command was introduced.		
Release	Modification						
4.0(1)	This command was introduced.						
Usage Guidelines	You must use the feature dot1x command before you configure 802.1X. This command does not require a license.						
Examples	<p>This example shows how to clear all 802.1X authenticator instances:</p> <pre>switch# clear dot1x all</pre> <p>This example shows how to clear the 802.1X authenticator instances for an interface:</p> <pre>switch# clear dot1x interface ethernet 1/1</pre>						
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>feature dot1x</td> <td>Enables the 802.1X feature.</td> </tr> <tr> <td>show dot1x all</td> <td>Displays all 802.1X information.</td> </tr> </tbody> </table>	Command	Description	feature dot1x	Enables the 802.1X feature.	show dot1x all	Displays all 802.1X information.
Command	Description						
feature dot1x	Enables the 802.1X feature.						
show dot1x all	Displays all 802.1X information.						

Send document comments to nexus7k-docfeedback@cisco.com

clear eou

To clear Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) sessions, use the **clear eou** command.

```
clear eou { all | authentication { clientless | eap | static } | interface ethernet slot/port | ip-address
ipv4-address | mac-address mac-address | posturetoken type }
```

Syntax Description		
all		Specifies all EAPoUDP sessions.
authentication		Specifies EAPoUDP authentication
clientless		Specifies sessions authenticated using clientless posture validation.
eap		Specifies sessions authenticated using EAPoUDP.
static		Specifies sessions authenticated using statically configured exception lists.
interface ethernet <i>slot/port</i>		Specifies an interface.
ip-address <i>ipv4-address</i>		Specifies an IPv4 address. in the A.B.C.D format.
mac-address <i>mac-address</i>		Specifies a MAC address.
posturetoken <i>type</i>		Specifies a posture token name.

Defaults None

Command Modes Any command mode

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines You must enable EAPoUDP by using the **feature eou** command before using the **clear eou** command. This command does not require a license.

Examples This example shows how to clear all the EAPoUDP sessions:

```
switch# clear eou all
```

This example shows how to clear the statically authenticated EAPoUDP sessions:

```
switch# clear eou authentication static
```

Send document comments to nexus7k-docfeedback@cisco.com

This example shows how to clear the EAPoUDP sessions for an interface:

```
switch# clear eou interface ethernet 1/1
```

This example shows how to clear the EAPoUDP sessions for an IP address:

```
switch# clear eou ip-address 10.10.1.1
```

This example shows how to clear the EAPoUDP sessions for a MAC address:

```
switch# clear eou mac-address 0019.076c.dac4
```

This example shows how to clear the EAPoUDP sessions with a posture token type of checkup:

```
switch# clear eou posturetoken healthy
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
show eou	Displays EAPoUDP information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear hardware rate-limiter

To clear rate-limit statistics, use the **clear hardware rate-limiter** command.

```
clear rate-limiter {access-list-log | all | copy | layer-2 {port-security | storm-control} | layer-3
                  {control | glean | mtu | multicast {directly-connected | local-groups | rpf-leak} | ttl} |
                  receive}
```

Syntax	Description
access-list-log	Clears rate-limit statistics for access-list logging packets.
all	Clears all rate-limit statistics.
copy	Clears rate-limit statistics for copy packets.
layer-2	Specifies Layer 2 packets rate limits.
port-security	Clears rate-limit statistics for Layer 2 port-security packets.
storm-control	Clears rate-limit statistics for Layer 2 storm-control packets.
layer-3	Specifies Layer 3 packets rate limits.
control	Clears rate-limit statistics for Layer 3 control packets.
glean	Clears rate-limit statistics for Layer 3 glean packets.
mtu	Clears rate-limit statistics for Layer 3 maximum transmission unit (MTU) packets.
multicast	Specifies Layer 3 multicast rate limits.
directly-connected	Clears rate-limit statistics for Layer 3 directly connected multicast packets.
local-groups	Clears rate-limit statistics for Layer 3 local group multicast packets.
rpf-leak	Clears rate-limit statistics for Layer 3 reverse path forwarding (RPF) leak multicast packets.
ttl	Clears rate-limit statistics for Layer 3 time-to-live (TTL) packets.
receive	Clears rate-limit statistics for receive packets.

Defaults None

Command Modes Any command mode

Supported User Roles network-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(3)	Added the port-security keyword.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

You can use the command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to clear all the rate-limit statistics:

```
switch# clear hardware rate-limiter all
```

This example shows how to clear the rate-limit statistics for access-list logging packets:

```
switch# clear hardware rate-limiter access-list-log
```

This example shows how to clear the rate-limit statistics for Layer 2 storm-control packets:

```
switch# clear hardware rate-limiter layer-2 storm-control
```

This example shows how to clear the rate-limit statistics for Layer 3 glean packets:

```
switch# clear hardware rate-limiter layer-3 glean
```

This example shows how to clear the rate-limit statistics for Layer 3 directly connected multicast packets:

```
switch# clear hardware rate-limiter layer-3 multicast directly-connected
```

This example shows how to clear the rate-limit statistics for received packets:

```
switch# clear hardware rate-limiter receive
```

Related Commands

Command	Description
platform rate-limit	Configures rate limits.
show hardware rate-limit	Displays rate-limit information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ip access-list counters

To clear the counters for all IPv4 access control lists (ACLs) or a single IPv4 ACL, use the **clear ip access-list counters** command.

```
clear ip access-list counters [access-list-name]
```

Syntax Description	<i>access-list-name</i> (Optional) Name of the IPv4 ACL whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters.										
Defaults	None										
Command Modes	Privileged EXEC										
Supported User Roles	network-admin vdc-admin										
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(1)	This command was introduced.						
Release	Modification										
4.0(1)	This command was introduced.										
Usage Guidelines	This command does not require a license.										
Examples	<p>This example shows how to clear counters for all IPv4 ACLs:</p> <pre>switch# clear ip access-list counters switch#</pre> <p>This example shows how to clear counters for an IP ACL named acl-ipv4-101:</p> <pre>switch# clear ip access-list counters acl-ipv4-101 switch#</pre>										
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>clear access-list counters</td> <td>Clears counters for IPv4 and MAC ACLs.</td> </tr> <tr> <td>clear mac access-list counters</td> <td>Clears counters for MAC ACLs.</td> </tr> <tr> <td>show access-lists</td> <td>Displays information about one or all IPv4 and MAC ACLs.</td> </tr> <tr> <td>show ip access-lists</td> <td>Displays information about one or all IPv4 ACLs.</td> </tr> </tbody> </table>	Command	Description	clear access-list counters	Clears counters for IPv4 and MAC ACLs.	clear mac access-list counters	Clears counters for MAC ACLs.	show access-lists	Displays information about one or all IPv4 and MAC ACLs.	show ip access-lists	Displays information about one or all IPv4 ACLs.
Command	Description										
clear access-list counters	Clears counters for IPv4 and MAC ACLs.										
clear mac access-list counters	Clears counters for MAC ACLs.										
show access-lists	Displays information about one or all IPv4 and MAC ACLs.										
show ip access-lists	Displays information about one or all IPv4 ACLs.										

Send document comments to nexus7k-docfeedback@cisco.com

clear ip arp inspection log

To clear the Dynamic ARP Inspection (DAI) logging buffer, use the **clear ip arp inspection log** command.

clear ip arp inspection log

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Any command mode

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to clear the DAI logging buffer:

```
switch# clear ip arp inspection log
switch#
```

Related Commands	Command	Description
	ip arp inspection log-buffer	Configures the DAI logging buffer size.
	show ip arp inspection	Displays the DAI configuration status.
	show ip arp inspection log	Displays the DAI log configuration.
	show ip arp inspection statistics	Displays the DAI statistics.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ip arp inspection statistics vlan

To clear the Dynamic ARP Inspection (DAI) statistics for a specified VLAN, use the **clear ip arp inspection statistics vlan** command.

clear ip arp inspection statistics vlan *vlan-list*

Syntax Description	vlan <i>vlan-list</i>	Specifies the VLANs whose DAI statistics this command clears. The <i>vlan-list</i> argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges (see the “Examples” section). Valid VLAN IDs are from 1 to 4094.
---------------------------	------------------------------	---

Defaults	None
-----------------	------

Command Modes	Any command mode
----------------------	------------------

Supported User Roles	network-admin vdc-admin
-----------------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples This example shows how to clear the DAI statistics for VLAN 2:

```
switch# clear ip arp inspection statistics vlan 2
switch#
```

This example shows how to clear the DAI statistics for VLANs 5 through 12:

```
switch# clear ip arp inspection statistics vlan 5-12
switch#
```

This example shows how to clear the DAI statistics for VLAN 2 and VLANs 5 through 12:

```
switch# clear ip arp inspection statistics vlan 2,5-12
switch#
```

clear ip arp inspection statistics vlan***Send document comments to nexus7k-docfeedback@cisco.com***

Related Commands	Command	Description
	clear ip arp inspection log	Clears the DAI logging buffer.
	ip arp inspection log-buffer	Configures the DAI logging buffer size.
	show ip arp inspection	Displays the DAI configuration status.
	show ip arp inspection vlan	Displays DAI status for a specified list of VLANs.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ip device tracking

To clear IP device tracking information, use the **clear ip device tracking** command.

```
clear ip device tracking { all | interface ethernet slot/port | ip-address ipv4-address | mac-address mac-address }
```

Syntax Description		
all		Clears all IP device tracking information.
interface ethernet <i>slot/port</i>		Clears IP device tracking information for an interface.
ip-address <i>ipv4-address</i>		Clears IP device tracking information for an IPv4 address in the A.B.C.D format.
mac-address <i>mac-address</i>		Clears IP tracking information for a MAC address in the XXXX.XXXX.XXXX format.

Defaults None

Command Modes Any command mode

SupportedUserRoles network-admin
vdc-admin
VDC user

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to clear all the IP device tracking information:

```
switch# clear ip device tracking all
```

This example shows how to clear the IP device tracking information for an interface:

```
switch# clear ip device tracking interface ethernet 1/1
```

This example shows how to clear the IP device tracking information for an IP address:

```
switch# clear ip device tracking ip-address 10.10.1.1
```

This example shows how to clear the IP device tracking information for a MAC address:

```
switch# clear ip device tracking mac-address 000c.30da.86f4
```

clear ip device tracking

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	ip device tracking	Enables IP device tracking.
	show ip device tracking	Displays IP device tracking information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ip dhcp snooping binding

To clear the DHCP snooping binding database, use the **clear ip dhcp snooping binding** command.

clear ip dhcp snooping binding

clear ip dhcp snooping binding [**vlan** *vlan-id* **mac** *mac-address* **ip** *ip-address* **interface ethernet** *slot/port*[*.subinterface-number*]]

clear ip dhcp snooping binding [**vlan** *vlan-id* **mac** *mac-address* **ip** *ip-address* **interface port-channel** *channel-number*[*.subchannel-number*]]

Syntax Description	
vlan <i>vlan-id</i>	(Optional) Clears the DHCP snooping binding database for an entry identified with the VLAN ID specified by the <i>vlan-id</i> argument and the additional keywords and arguments that follow.
mac-address <i>mac-address</i>	Specifies the MAC address of the binding database entry to be cleared. Enter the <i>mac-address</i> argument in dotted hexadecimal format.
ip <i>ip-address</i>	Specifies the IPv4 address of the binding database entry to be cleared. Enter the <i>ip-address</i> argument in dotted decimal format.
interface ethernet <i>slot/port</i>	(Optional) Specifies the Ethernet interface of the binding database entry to be cleared.
<i>.subinterface-number</i>	(Optional) Number of the Ethernet-interface subinterface. Note The dot separator is required between the <i>port</i> and <i>subinterface-number</i> arguments.
interface port-channel <i>channel-number</i>	(Optional) Specifies the Ethernet port-channel of the binding database entry to be cleared.
<i>.subchannel-number</i>	(Optional) Number of the Ethernet port-channel subchannel. Note The dot separator is required between the <i>channel-number</i> and <i>subchannel-number</i> arguments.

Defaults None

Command Modes Any command mode

Supported User Roles network-admin
vdc-admin
VDC user

Send document comments to nexus7k-docfeedback@cisco.com

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(3)	This command was modified to support clearing a specific binding database entry. The optional vlan keyword and the arguments and keywords that follow it were added.

Usage Guidelines This command does not require a license.

Examples This example shows how to clear the DHCP snooping binding database:

```
switch# clear ip dhcp snooping binding
switch#
```

This example shows how to clear a specific entry from the DHCP snooping binding database:

```
switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9 interface
ethernet 2/11
switch#
```

Related Commands	Command	Description
	ip dhcp snooping	Globally enables DHCP snooping on the device.
	show ip dhcp snooping	Displays general information about DHCP snooping.
	show ip dhcp snooping binding	Displays IP-MAC address bindings, including the static IP source entries.
	show ip dhcp snooping statistics	Displays DHCP snooping statistics.
	show running-config dhcp	Displays DHCP snooping configuration, including the IP Source Guard configuration.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear mac access-list counters

To clear the counters for all MAC access control lists (ACLs) or a single MAC ACL, use the **clear mac access-list counters** command.

```
clear mac access-list counters [access-list-name]
```

Syntax Description	<i>access-list-name</i> (Optional) Name of the MAC ACL whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters.
---------------------------	--

Defaults	None
-----------------	------

Command Modes	Privileged EXEC
----------------------	-----------------

Supported User Roles	network-admin vdc-admin
-----------------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples This example shows how to clear counters for all MAC ACLs:

```
switch# clear mac access-list counters
switch#
```

This example shows how to clear counters for a MAC ACL named acl-mac-0060:

```
switch# clear mac access-list counters acl-ipv4-0060
switch#
```

Related Commands	Command	Description
	clear access-list counters	Clears counters for IPv4 and MAC ACLs.
	clear ip access-list counters	Clears counters for IPv4 ACLs.
	show access-lists	Displays information about one or all IPv4 and MAC ACLs.
	show mac access-lists	Displays information about one or all MAC ACLs.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear port-security

To clear a single, dynamically learned, secure MAC address or to clear all dynamically learned, secure MAC addresses for a specific interface, use the **clear port-security** command.

```
clear port-security {dynamic} {interface ethernet slot/port | address address} [vlan vlan-id]
```

Syntax Description	dynamic	Specifies that you want to clear dynamically learned, secure MAC addresses.
	interface ethernet <i>slot/port</i>	Specifies the interface of the dynamically learned, secure MAC addresses that you want to clear.
	address <i>address</i>	Specifies a single MAC address to be cleared, where <i>address</i> is the MAC address.
	vlan <i>vlan-id</i>	Specifies the VLAN of the secure MAC addresses to be cleared. Valid VLAN IDs are from 1 to 4096.

Defaults dynamic

Command Modes Any command mode

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines You must enable port security by using the **feature port-security** command before you can use the **clear port-security** command.

This command does not require a license.

Examples This example shows how to remove dynamically learned, secure MAC addresses from the Ethernet 2/1 interface:

```
switch# config t
switch(config)# clear port-security dynamic interface ethernet 2/1
```

This example shows how to remove the dynamically learned, secure MAC address 0019.D2D0.00AE:

```
switch# config t
switch(config)# clear port-security dynamic address 0019.D2D0.00AE
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	debug port-security	Provides debugging information for port security.
	feature port-security	Enables port security globally.
	show port-security	Shows information about port security.
	switchport port-security	Enables port security on a Layer 2 interface.

Send document comments to nexus7k-docfeedback@cisco.com

clear ssh hosts

To clear the Secure Shell (SSH) host sessions for a virtual device context (VDC), use the **clear ssh hosts** command.

clear ssh hosts

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Any command mode

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to clear all SSH host sessions:

```
switch# clear ssh hosts
```

Related Commands	Command	Description
	ssh server enable	Enables the SSH server.

Send document comments to nexus7k-docfeedback@cisco.com

clear user

To clear a user session for a virtual device context (VDC), use the **clear user** command.

```
clear user user-id
```

Syntax Description	<i>user-id</i>	User identifier.
--------------------	----------------	------------------

Defaults	None
----------	------

Command Modes	Any command mode
---------------	------------------

SupportedUserRoles	network-admin vdc-admin
--------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the show users command to display the current user sessions on the device. This command does not require a license.
------------------	---

Examples	This example shows how to clear all SSH host sessions: switch# clear user user1
----------	---

Related Commands	Command	Description
	show users	Displays the user session information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

cts device-id

To configure a Cisco TrustSec device identifier, use the **cts device-id** command.

```
cts device-id device-id password [7] password
```

Syntax	Description
<i>device-id</i>	Cisco TrustSec device identifier name. The name is alphanumeric and case-sensitive. The maximum length is 32 characters.
7	(Optional) Encrypts the password.
password <i>password</i>	Specifies the password to use during EAP-FAST processing. The name is alphanumeric and case-sensitive. The maximum length is 32 characters.

Defaults
No Cisco TrustSec device identifier
Clear text password

Command Modes
Global configuration

Supported User Roles
network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines
To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command. The Cisco TrustSec device identifier name must be unique in your Cisco TrustSec network cloud. This command requires the Advanced Services license.

Examples
This example shows how to configure a Cisco TrustSec device identifier:

```
switch# config t  
switch(config)# cts device-id DeviceA password Cisco321
```

Related Commands	Command	Description
	feature cts	Enables the Cisco TrustSec feature.
	show cts credentials	Displays the Cisco TrustSec credentials information.

Send document comments to nexus7k-docfeedback@cisco.com

cts dot1x

To enable Cisco TrustSec authentication on an interface and enter Cisco TrustSec 802.1X configuration mode, use the **cts dot1x** command. To revert to the default, use the **no** form of this command.

```
cts dot1x
```

```
no cts dot1x
```

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command. After using this command, you must enable and disable the interface using the **shutdown/no shutdown** command sequence for the configuration to take effect. This command requires the Advanced Services license.

Examples This example shows how to enable Cisco TrustSec authentication on an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to disable Cisco TrustSec authentication on an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# no cts dot1x
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	feature cts	Enables the Cisco TrustSec feature.
	show cts interface	Displays Cisco TrustSec configuration information for interfaces.

Send document comments to nexus7k-docfeedback@cisco.com

cts manual

To enter Cisco TrustSec manual configuration for an interface, use the **cts manual** command. To remove the manual configuration, use the **no** form of this command.

cts manual

no cts manual

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command. After using this command, you must enable and disable the interface using the **shutdown/no shutdown** command sequence for the configuration to take effect. This command requires the Advanced Services license.

Examples This example shows how to enter Cisco TrustSec manual configuration mode for an interface:

```
switch# config t
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)#
```

This example shows how to remove the Cisco TrustSec manual configuration from an interface:

```
switch# config t
switch(config)# interface ethernet 2/4
switch(config-if)# no cts manual
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	feature cts	Enables the Cisco TrustSec feature.
	show cts interface	Displays Cisco TrustSec configuration information for interfaces.

Send document comments to nexus7k-docfeedback@cisco.com

cts refresh role-based-policy

To refresh the Cisco TrustSec security group access control list (SGACL) policies downloaded from the Cisco Secure ACS, use the **cts refresh role-based-policy** command.

cts refresh role-based-policy

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Any configuration mode

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command. This command requires the Advanced Services license.

Examples This example shows how to enter Cisco TrustSec manual configuration mode for an interface:

```
switch# cts refresh role-based-policy
```

Related Commands	Command	Description
	feature cts	Enables the Cisco TrustSec feature.
	show cts role-based policy	Displays Cisco TrustSec SGACL policy configuration.

Send document comments to nexus7k-docfeedback@cisco.com

cts rekey

To rekey an interface for Cisco TrustSec policies, use the **cts rekey** command.

cts rekey ethernet slot/port

Syntax Description	ethernet slot/port	Specifies an Ethernet interface.
--------------------	--------------------	----------------------------------

Defaults	None
----------	------

Command Modes	Any command mode
---------------	------------------

Supported User Roles	network-admin vdc-admin
----------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	To use this command, you must enable the Cisco TrustSec feature using the feature cts command. This command requires the Advanced Services license.
------------------	--

Examples	This example shows how to rekey an interface for Cisco TrustSec: switch# cts rekey ethernet 2/3
----------	---

Related Commands	Command	Description
	feature cts	Enables the Cisco TrustSec feature.
	show cts interface	Displays Cisco TrustSec configuration information for interfaces.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

cts role-based access-list

To create or specify a Cisco TrustSec security group access control list (SGACL) and enter role-based access control list configuration mode, use the **cts role-based access-list** command. To remove an SGACL, use the **no** form of this command.

cts role-based access-list *list-name*

no cts role-based access-list *list-name*

Syntax Description	<i>list-name</i>	Name for the SGACL. The name is alphanumeric and case-sensitive. The maximum length is 32 characters.
---------------------------	------------------	---

Defaults	None
-----------------	------

Command Modes	Global configuration
----------------------	----------------------

SupportedUserRoles	network-admin vdc-admin
---------------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	To use this command, you must enable the Cisco TrustSec feature using the feature cts command. This command requires the Advanced Services license.
-------------------------	--

Examples	This example shows how to create a Cisco TrustSec SGACL and enter role-based access list configuration mode:
-----------------	--

```
switch# config t
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)#
```

This example shows how to remove a Cisco TrustSec SGACL:

```
switch# config t
switch(config)# no cts role-based access-list MySGACL
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	feature cts	Enables the Cisco TrustSec feature.
	show cts role-based access-list	Displays the Cisco TrustSec SGACL configuration.

Send document comments to nexus7k-docfeedback@cisco.com

cts role-based enforcement

To enable Cisco TrustSec security group access control list (SGACL) enforcement in a VLAN or Virtual Routing and Forwarding instance (VRF), use the **cts role-based enforcement** command. To revert to the default, use the **no** form of this command.

cts role-based enforcement

no cts role-based enforcement

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration
VLAN configuration
VRF configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command. This command requires the Advanced Services license.

Examples This example shows how to enable Cisco TrustSec SGACL enforcement in the default VRF:

```
switch# config t
switch(config)# cts role-based enforcement
```

This example shows how to enable Cisco TrustSec SGACL enforcement in a VLAN:

```
switch# config t
switch(config)# vlan 1
switch(config-vlan)# cts role-based enforcement
```

This example shows how to enable Cisco TrustSec SGACL enforcement in a nondefault VRF:

```
switch# config t
switch(config)# vrf context MyVRF
switch(config-vrf)# cts role-based enforcement
```

Send document comments to nexus7k-docfeedback@cisco.com

This example shows how to disable Cisco TrustSec SGACL enforcement:

```
switch# config t  
switch(config)# no cts role-based enforcement
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based enable	Displays the Cisco TrustSec SGACL policy enforcement configuration.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

cts role-based sgt

To manually configure mapping of Cisco TrustSec security group tags (SGTs) to a security group access control list (SGACL), use the **cts role-based sgt** command. To remove the SGT mapping to an SGACL, use the **no** form of this command.

```
cts role-based sgt {sgt-value | any | unknown} dgt {dgt-value | unknown}
access-list list-name
```

```
no cts role-based sgt {sgt-value | any | unknown} dgt {dgt-value | unknown}
```

Syntax Description	
<i>sgt-value</i>	Source SGT value. The range is 0 to 65533.
any	Specifies any SGT.
unknown	Specifies an unknown SGT.
dgt	Specifies the destination SGT.
<i>dgt-value</i>	Destination SGT value. The range is 0 to 65533.
access-list <i>list-name</i>	Specifies the name for the SGACL.

Defaults None

Command Modes Global configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command. You must configure the SGACL before you can configure SGT mapping. This command requires the Advanced Services license.

Examples This example shows how to configure SGT mapping for an SGACL:

```
switch# config t
switch(config)# cts role-based sgt 3 dgt 10 access-list MySGACL
```

This example shows how to remove SGT mapping for an SGACL:

```
switch# config t
switch(config)# no cts role-based sgt 3 sgt 10
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	feature cts	Enables the Cisco TrustSec feature.
	show cts role-based policy	Displays the Cisco TrustSec SGT mapping for an SGACL.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

cts role-based sgt-map

To manually configure the Cisco TrustSec security group tag (SGT) mapping to IP addresses, use the **cts role-based sgt-map** command. To remove an SGT, use the **no** form of this command.

```
cts role-based sgt-map ipv4-address sgt-value
```

```
no cts role-based sgt-map ipv4-address
```

Syntax Description	
<i>ipv4-address</i>	IPv4 address. The format is <i>A.B.C.D</i> .
<i>sgt-value</i>	SGT value. The range is 0 to 65533.

Defaults	None
----------	------

Command Modes	Global configuration VLAN configuration VRF configuration
---------------	---

Supported User Roles	network-admin vdc-admin
----------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	To use this command, you must enable the Cisco TrustSec feature using the feature cts command. You can use only IPv4 addressing with Cisco TrustSec. This command requires the Advanced Services license.
------------------	--

Examples This example shows how to configure mapping for a Cisco TrustSec SGT:

```
switch# config t
switch(config)# cts role-based sgt-map 10.10.1.1 3
switch(config-rbacl)#
```

This example shows how to remove a Cisco TrustSec SGT mapping:

```
switch# config t
switch(config)# no cts role-based sgt-map 10.10.1.1
```

Related Commands

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based sgt-map	Displays the Cisco TrustSec SGT mapping.

Send document comments to nexus7k-docfeedback@cisco.com

cts sgt

To configure the security group tag (SGT) for Cisco TrustSec, use the **cts sgt** command.

cts sgt *tag*

Syntax Description	<i>tag</i>	Local SGT for the device that is a hexadecimal value with the format 0xhhhh . The range is from 0x0 to 0xffff.
--------------------	------------	---

Defaults	None
----------	------

Command Modes	Global configuration
---------------	----------------------

Supported User Roles	network-admin vdc-admin
----------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	To use this command, you must enable the Cisco TrustSec feature using the feature cts command. This command requires the Advanced Services license.
------------------	--

Examples	This example shows how to configure the Cisco TrustSec SGT for the device:
----------	--

```
switch# config t
switch(config)# cts sgt 0x3
```

Related Commands	Command	Description
	feature cts	Enables the Cisco TrustSec feature.
	show cts environment-data	Displays the Cisco TrustSec environment data.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

cts sxp connection peer

To configure a Security Group Tag (SGT) Exchange Protocol (SXP) peer connection for Cisco TrustSec, use the **cts sxp connection peer** command. To remove the SXP connection, use the **no** form of this command.

```
cts sxp connection peer peer-ipv4-addr [source src-ipv4-addr] password [default | none | required password] mode {speaker | listener} [vrf vrf-name]
```

```
no cts sxp connection peer peer-ipv4-addr [vrf vrf-name]
```

Syntax Description		
	<i>peer-ipv4-addr</i>	IPv4 address of the peer device.
	source <i>src-ipv4-addr</i>	(Optional) Specifies the IPv4 address of the source device.
	password	Specifies the password option to use for the SXP authentication.
	default	(Optional) Specifies that SXP should use the default SXP password for the device.
	none	(Optional) Specifies that SXP should not use a password.
	required <i>password</i>	(Optional) Specifies that SXP should use this password.
	mode	Specifies the mode of the peer device.
	speaker	Specifies that the peer is the speaker.
	listener	Specifies that the peer is the listener.
	vrf <i>vrf-name</i>	(Optional) Specifies the VRF for the peer.

Defaults	
	Configured default SXP password for the device
	Configured default SXP source IPv4 address for the device
	Default VRF

Command Modes	
	Global configuration

SupportedUserRoles	
	network-admin
	vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	
	To use this command, you must enable the Cisco TrustSec feature using the feature cts command.
	You can use only IPv4 addressing with Cisco TrustSec.
	If you do not specify a source IPv4 address, you must configure a default SXP source IPv4 address using the cts sxp default source-ip command.

Send document comments to nexus7k-docfeedback@cisco.com

If you specify default as the password mode, you must configure a default SXP password using the **cts sxp default password** command.

This command requires the Advanced Services license.

Examples

This example shows how to configure an SXP peer connection:

```
switch# config t  
switch(config)# cts sxp connection peer 10.10.1.1 source 10.10.2.2 password default mode listener
```

This example shows how to remove an SXP peer connection:

```
switch# config t  
switch(config)# no cts sxp connection peer 10.10.1.1
```

Related Commands

Command	Description
cts sxp default password	Configures the default SXP password for the device.
cts sxp default source-ip	Configures the default SXP source IPv4 address for the device.
feature cts	Enables the Cisco TrustSec feature.
show cts sxp connection	Displays the Cisco TrustSec SXP peer connection information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

cts sxp default password

To configure the default Security Group Tag (SGT) Exchange Protocol (SXP) password for the device, use the **cts sxp default password** command. To remove the default, use the **no** form of this command.

```
cts sxp default password password
```

```
no cts sxp default password
```

Syntax Description	<i>password</i>	Default SXP password. The password is alphanumeric and case-sensitive. The maximum length is 32 characters.
Defaults	None	
Command Modes	Global configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	To use this command, you must enable the Cisco TrustSec feature using the feature cts command. This command requires the Advanced Services license.	
Examples	<p>This example shows how to configure the default SXP password for the device:</p> <pre>switch# config t switch(config)# cts sxp default password Cisco654</pre> <p>This example shows how to remove the default SXP password:</p> <pre>switch# config t switch(config)# no cts sxp default password</pre>	
Related Commands	Command	Description
	feature cts	Enables the Cisco TrustSec feature.
	show cts sxp	Displays the Cisco TrustSec SXP configuration information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

cts sxp default source-ip

To configure the default Security Group Tag (SGT) Exchange Protocol (SXP) source IPv4 address for the device, use the **cts sxp default source-ip** command. To revert to the default, use the **no** form of this command.

```
cts sxp default source-ip ipv4-address
```

```
no cts sxp default source-ip ipv4-address
```

Syntax Description	<i>ipv4-address</i>	Default SXP IPv4 address for the device.
--------------------	---------------------	--

Defaults	None
----------	------

Command Modes	Global configuration
---------------	----------------------

SupportedUserRoles	network-admin vdc-admin
--------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	To use this command, you must enable the Cisco TrustSec feature using the feature cts command. You can use only IPv4 addressing with Cisco TrustSec. This command requires the Advanced Services license.
------------------	--

Examples	This example shows how to configure the default SXP source IP address for the device:
----------	---

```
switch# config t
switch(config)# cts sxp default source-ip 10.10.3.3
```

This example shows how to remove the default SXP source IP address:

```
switch# config t
switch(config)# no cts sxp default source-ip
```

Related Commands	Command	Description
	feature cts	Enables the Cisco TrustSec feature.
	show cts sxp	Displays the Cisco TrustSec SXP configuration information.

Send document comments to nexus7k-docfeedback@cisco.com

cts sxp enable

To enable the Security Group Tag (SGT) Exchange Protocol (SXP) peer on a device, use the **cts sxp enable** command. To revert to the default, use the **no** form of this command.

cts sxp enable

no cts sxp enable

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command. This command requires the Advanced Services license.

Examples This example shows how to enable SXP:

```
switch# config t
switch(config)# cts sxp enable
```

This example shows how to disable SXP:

```
switch# config t
switch(config)# no cts sxp enable
```

Related Commands	Command	Description
	feature cts	Enables the Cisco TrustSec feature.
	show cts sxp	Displays the Cisco TrustSec SXP configuration information.

Send document comments to nexus7k-docfeedback@cisco.com

cts sxp reconcile-period

To configure a Security Group Tag (SGT) Exchange Protocol (SXP) reconcile period timer, use the **cts sxp reconcile-period** command. To revert to the default, use the **no** form of this command.

cts sxp reconcile-period *seconds*

no cts sxp reconcile-period

Syntax Description	<i>seconds</i>	Number of seconds. The range is from 0 to 64000.
--------------------	----------------	--

Defaults	60 seconds (1 minute)
----------	-----------------------

Command Modes	Global configuration
---------------	----------------------

SupportedUserRoles	network-admin vdc-admin
--------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

After a peer terminates an SXP connection, an internal hold down timer starts. If the peer reconnects before the internal hold down timer expires, the SXP reconcile period timer starts. While the SXP reconcile period timer is active, the NX-OS software retains the SGT mapping entries learned from the previous connection and removes invalid entries.



Note

Setting the SXP reconcile period to 0 seconds disables the timer and causes all entries from the previous connection to be removed.

This command requires the Advanced Services license.

Examples

This example shows how to configure the SXP reconcile period:

```
switch# config t
switch(config)# cts sxp reconcile-period 120
```

This example shows how to revert to the default SXP reconcile period value:

```
switch# config t
switch(config)# no cts sxp reconcile-period
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	feature cts	Enables the Cisco TrustSec feature.
	show cts sxp connection	Displays the Cisco TrustSec SXP configuration information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

cts sxp retry-period

To configure a Security Group Tag (SGT) Exchange Protocol (SXP) retry period timer, use the **cts sxp retry-period** command. To revert to the default, use the **no** form of this command.

cts sxp retry-period *seconds*

no cts sxp retry-period

Syntax Description	<i>seconds</i>	Number of seconds. The range is from 0 to 64000.
--------------------	----------------	--

Defaults	120 seconds (2 minutes)
----------	-------------------------

Command Modes	Global configuration
---------------	----------------------

SupportedUserRoles	network-admin vdc-admin
--------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command. The SXP retry period determines how often the NX-OS software retries an SXP connection. When an SXP connection is not successfully set up, the NX-OS software makes a new attempt to set up the connection after the SXP retry period timer expires.



Note

Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted.

This command requires the Advanced Services license.

Examples

This example shows how to configure the SXP retry period:

```
switch# config t
switch(config)# cts sxp retry-period 120
```

This example shows how to revert to the default SXP retry period value:

```
switch# config t
switch(config)# no cts sxp retry-period
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	feature cts	Enables the Cisco TrustSec feature.
	show cts sxp connection	Displays the Cisco TrustSec SXP peer connection information.