C Commands

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

clear cts policy

To clear the Cisco TrustSec security group access control list (SGACL) policies, use the **clear cts policy** command.

clear cts policy {**all** | **peer** *device-id* | **sgt** *sgt-value*}

Syntax Description

all	Clears all the Cisco TrustSec SGACL policies on the local device.
peer *device-id*	Clears the Cisco TrustSec SGACL policies for a peer device on the local device.
sgt *sgt-value*	Clears the Cisco TrustSec SGACL policies for a security group tag (SGT) on the local device.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must first enable the 802.1X feature by using the **feature dot1x** command and then enable the Cisco TrustSec feature using the **feature cts** command.

When you clear the SGACL policies, the operation does not take effect until the interface is flapped. If the interface is a static SGT interface, the SGT value is set to zero (0) after the flapping. To undo this operation, use the following commands:

```
switch(config-if-cts-manual)# no policy static
switch(config-if-cts-manual)# policy static sgt sgt-value
switch(config-if-cts-manual)#
```

If the interface is a dynamic SGT interface, the SGT is downloaded again from the RADIUS server after the flapping.

This command does not require a license.

Examples

This example shows how to clear all the Cisco TrustSec SGACL policies on the device:

```
switch# clear cts policy all
switch#
```

Related Commands

Command	Description
cts role-based sgt	Maps SGTs to a SGACL.
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature.
policy	Configures an authentication policy on an interface.
show cts role-based policy	Displays Cisco TrustSec SGACL policy information.

clear cts role-based counters

To clear the role-based access control list (RBACL) statistics so that all counters are reset to 0, use the **clear cts role-based counters** command.

clear cts role-based counters

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear the RBACL statistics:

```
switch# clear cts role-based counters
switch#
```

Related Commands

Command	Description
cts role-based counters enable	Enables the RBACL statistics.
show cts role-based counters	Displays the configuration status of RBACL statistics and lists statistics for all RBACL policies.

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

device-id	Cisco TrustSec device identifier name. The name is alphanumeric and case-sensitive. The maximum length is 32 characters.
password	Specifies the password (in clear text or encrypted) to use during EAP-FAST processing.
7	(Optional) Specifies that the password is in encrypted text.
password	Password for the Cisco TrustSec device. It contains up to 32 alphanumeric, case-sensitive characters.

Command Default

No Cisco TrustSec device identifier
Clear text password

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must first enable the 802.1X feature by using the **feature dot1x** command and then enable the Cisco TrustSec feature using the **feature cts** command.

The Cisco TrustSec device identifier name must be unique.

This command does not require a license.

Examples

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

```
switch# configure terminal
swtich(config)# cts device-id DeviceA password Cisco321
swtich(config)#
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature.
show cts credentials	Displays the Cisco TrustSec credentials information.

cts manual

To enter the 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.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must first enable the 802.1X feature by using the **feature dot1x** command and then enable the Cisco TrustSec feature using the **feature cts** command.

After using this command, you must enable and disable the interface using the **shutdown** and **no shutdown** command sequence for the configuration to take effect.

This command does not require a license.

Examples

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

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

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

Command	Description
feature dot1x	Enables the 802.1X feature.
show cts interface	Displays Cisco TrustSec configuration information for interfaces.

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

list-name	Name for the SGACL. The name is alphanumeric and case-sensitive. The maximum length is 32 characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must first enable the 802.1X feature by using the **feature dot1x** command and then enable the Cisco TrustSec feature using the **feature cts** command.

When you remove an SGACL, the access list can no longer be referenced by any SGT-DGT pair in the system.

This command does not require a license.

Examples

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

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

This example shows how to remove a Cisco TrustSec SGACL:

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

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature on the switch.
show cts role-based access-list	Displays the Cisco TrustSec SGACL configuration.

cts role-based counters enable

To enable role-based access control list (RBACL) statistics, use the **cts role-based counters enable** command. To disable RBACL statistics, use the **no** form of this command.

cts role-based counters enable

no cts role-based counters enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must first enable the 802.1X feature by using the **feature dot1x** command and then enable the Cisco TrustSec feature using the **feature cts** command.

To use this command, you must enable RBACL policy enforcement on the VLAN.

When you enable RBACL statistics, each policy requires one entry in the hardware. If you do not have enough space remaining in the hardware, an error message appears, and you cannot enable the statistics.

RBACL statistics are lost during an ISSU or when an access control entry is added to or removed from a RBACL.

This command does not require a license.

Examples

This example shows how to enable RBACL statistics:

```
switch# configure terminal
switch(config)# cts role-based counters enable
Note: Clearing previously collected counters...
switch(config)#
```

This example shows how to disable RBACL statistics:

```
switch# configure terminal
switch(config)# no cts role-based counters enable
switch(config)#
```

Related Commands

Command	Description
clear cts role-based counters	Clears the RBACL statistics so that all counters are reset to 0.
feature dot1x	Enables the 802.1X feature on the switch.
show cts role-based counters	Displays the configuration status of RBACL statistics and lists statistics for all RBACL policies.

cts role-based enforcement

To enable role-based access control list (RBACL) enforcement on a VLAN, use the **cts role-based enforcement** command. To disable RBACL enforcement on a VLAN, 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.

Command Default

Disabled

Command Modes

VLAN configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must first enable the 802.1X feature by using the **feature dot1x** command and then enable the Cisco TrustSec feature using the **feature cts** command.

RBACL enforcement is enabled on per-VLAN basis. RBACL enforcement cannot be enabled on routed VLANs or interfaces. For RBACL enforcement changes to take effect, you must exit from the VLAN configuration mode.

This command does not require a license.

Examples

This example shows how to enable RBACL enforcement on a VLAN and verifies the status:

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# cts role-based enforcement
switch(config-vlan)# exit
switch(config)# show cts role-based enable
vlan:102
switch(config)#
```

This example shows how to disable RBACL enforcement on a VLAN:

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# no cts role-based enforcement
switch(config-vlan)#
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature on the switch.
show cts role-based enable	Displays the VLANs that has RBACL enabled.

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* | **any** | **unknown**} **access-list** *list-name*

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

Syntax Description

sgt-value	Source SGT value. The range is from 0 to 65519.
any	Specifies any SGT or destination SGT.
unknown	Specifies an unknown SGT.
dgt	Specifies the destination SGT.
dgt-value	Destination SGT value. The range is from 0 to 65519.
access-list *list-name*	Specifies the name for the SGACL.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must first enable the 802.1X feature by using the **feature dot1x** command and then enable the Cisco TrustSec feature using the **feature cts** command.

You must configure the SGACL before you can configure SGT mapping.

This command does not require a license.

Examples

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

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

This example shows how to configure any SGT mapping to any destination SGT:

```
switch# configure terminal
switch(config)# cts role-based sgt any dgt any access-list MySGACL
switch(config)#
```

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

```
switch# configure terminal
switch(config)# no cts role-based sgt 3 dgt 10
switch(config)#
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature on the switch.
show cts role-based policy	Displays the Cisco TrustSec SGT mapping for an SGACL.

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

ipv4-address	IPv4 address. The format is *A.B.C.D*
sgt-value	SGT value. The range is 1 to 65519.

Command Default

None

Command Modes

Global configuration mode
VLAN configuration mode
VRF configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must first enable the 802.1X feature by using the **feature dot1x** command and then enable the Cisco TrustSec feature using the **feature cts** command.

You can use only IPv4 addressing with Cisco TrustSec.

This command does not require a license.

Examples

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

```
switch# configure terminal
switch(config)# cts role-based sgt-map 10.10.1.1 3
switch(config)#
```

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

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

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

Command	Description
feature dot1x	Enables the 802.1X feature on the switch.
show cts role-based sgt-map	Displays the Cisco TrustSec SGT mapping.

cts sgt

To configure the security group tag (SGT) for Cisco TrustSec, use the **cts sgt** command. To revert to the default settings, use the **no** form of this command.

cts sgt *tag*

no cts sgt

Syntax Description

tag	Local SGT for the device that is a hexadecimal value with the format **0x***hhhh*. The range is from 0x2 to 0xffef.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must first enable the 802.1X feature by using the **feature dot1x** command and then enable the Cisco TrustSec feature using the **feature cts** command.

This command does not require a license.

Examples

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

```
switch# configure terminal
switch(config)# cts sgt 0x3
switch(config)#
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature on the switch.
show cts environment-data	Displays the Cisco TrustSec environment data.

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*| **7** *encrypted-password*}} **mode listener** [**vrf** *vrf-name*]

no cts sxp connection peer *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** {**default** | **none** | **required** {*password* | **7** *encrypted-password*}} **mode listener** [**vrf** *vrf-name*]

Syntax Description

peer-ipv4-addr	IPv4 address of the peer device.
source *src-ipv4-addr*	(Optional) Specifies the IPv4 address of the source device.
password	Specifies the password option to use for the SXP authentication.
default	Specifies that SXP should use the default SXP password for the peer connection.
none	Specifies that SXP should not use a password.
required	Specifies the password that SXP should use for this peer connection.
password	Clear text password. The password is alphanumeric and case-sensitive. The maximum length is 32 characters.
7 *encrypted-password*	Specifies an encrypted password. The maximum length is 32 characters.
mode	Specifies the mode of the peer device.
listener	Specifies that the peer is the listener.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) instance for the peer. The VRF name can be a maximum of 32 alphanumeric characters.

Command Default

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

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must first enable the 802.1X feature by using the **feature dot1x** command and then 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.

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

This command does not require a license.

Examples

This example shows how to configure an SXP peer connection:

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

This example shows how to remove an SXP peer connection:

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

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.
feature dot1x	Enables the 802.1X feature on the switch.
show cts sxp connection	Displays the Cisco TrustSec SXP peer connection information.

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* | **7** *encrypted-password*}

no cts sxp default password

Syntax Description

password	Clear text password. The password is alphanumeric and case-sensitive. The maximum length is 32 characters.
7 *encrypted-password*	Specifies an encrypted password. The maximum length is 32 characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must first enable the 802.1X feature by using the **feature dot1x** command and then enable the Cisco TrustSec feature using the **feature cts** command.

This command does not require a license.

Examples

This example shows how to configure the default SXP password for the device:

```
switch# configure terminal
switch(config)# cts sxp default password Cisco654
switch(config)#
```

This example shows how to remove the default SXP password:

```
switch# configure terminal
switch(config)# no cts sxp default password
switch(config)#
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature on the switch.
show cts sxp	Displays the Cisco TrustSec SXP configuration information.

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

Syntax Description

ipv4-address	Default SXP IPv4 address for the device.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must first enable the 802.1X feature by using the **feature dot1x** command and then enable the Cisco TrustSec feature using the **feature cts** command.

You can use only IPv4 addressing with Cisco TrustSec.

This command does not require a license.

Examples

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

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

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

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

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature on the switch.
show cts sxp	Displays the Cisco TrustSec SXP configuration information.

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.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must first enable the 802.1X feature by using the **feature dot1x** command and then enable the Cisco TrustSec feature using the **feature cts** command.

This command does not require a license.

Examples

This example shows how to enable SXP:

```
switch# configure terminal
switch(config)# cts sxp enable
switch(config)#
```

This example shows how to disable SXP:

```
switch# configure terminal
switch(config)# no cts sxp enable
switch(config)#
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature on the switch.
show cts sxp	Displays the Cisco TrustSec SXP configuration information.

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

seconds	Number of seconds. The range is from 0 to 64000.

Command Default

120 seconds (2 minutes)

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must first enable the 802.1X feature by using the **feature dot1x** command and then 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.

Note Setting the SXP reconcile period to 0 seconds disables the timer.

This command does not require a license.

Examples

This example shows how to configure the SXP reconcile period:

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

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

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

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature on the switch.
show cts sxp connection	Displays the Cisco TrustSec SXP configuration information.

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

seconds	Number of seconds. The range is from 0 to 64000.

Command Default

60 seconds (1 minute)

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must first enable the 802.1X feature by using the **feature dot1x** command and then enable the Cisco TrustSec feature using the **feature cts** command.

The SXP retry period determines how often the Cisco NX-OS software retries an SXP connection. When an SXP connection is not successfully set up, the Cisco 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 does not require a license.

Examples

This example shows how to configure the SXP retry period:

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

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

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

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature on the switch.
show cts sxp connection	Displays the Cisco TrustSec SXP peer connection information.