Send comments to nexus5k-docfeedback@cisco.com

Cisco Nexus 5000 Series NX-OS TrustSec Command Reference

Cisco NX-OS Release 5.x

First Published: November 2011
Last Modified: July 2012

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

Text Part Number: OL-25830-01

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

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

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

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

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

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

Cisco Nexus 5000 Series NX-OS TrustSec Command Reference

CONTENTS

Preface

This preface describes the audience, organization, and conventions of the *Cisco Nexus 5000 Series NX-OS TrustSec Command Reference*. It also provides information on how to obtain related documentation.

This preface includes the following sections:

- Audience, page vii
- Supported Switches, page vii
- Organization, page viii
- Document Conventions, page viii
- Related Documentation, page ix
- Obtaining Documentation and Submitting a Service Request, page xi

Audience

This publication is for experienced users who configure and maintain Cisco NX-OS devices.

Supported Switches

This section includes the following topics:

- Cisco Nexus 5500 Platform Switches, page vii

Cisco Nexus 5500 Platform Switches

Table 1 lists the Cisco switches supported in the Cisco Nexus 5500 Platform.

Note For more information on these switches, see the *Cisco Nexus 5500 Platform and Cisco Nexus 5000 Platform Hardware Installation Guide* available at the following URL: http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

Table 1 Supported Cisco Nexus 5500 Platform Switches

Switch	Description
Cisco Nexus 5548P Switch	The Cisco Nexus 5548P switch is the first switch in the Cisco Nexus 5500 Platform. It is a one-rack-unit (1 RU), 10-Gigabit Ethernet and Fibre Channel over Ethernet (FCoE) switch that offers up to 960-Gbps throughput and up to 48 ports.
Cisco Nexus 5596P Switch	The Cisco Nexus 5596P switch is a top-of-rack, 10-Gigabit Ethernet and FCoE switch offering up to 1920-Gigabit throughput and up to 96 ports.

Organization

This document is organized as follows:

Chapter Title	Description
New and Changed Information	Describes the new and changed information for the new Cisco NX-OS software releases.
A Commands	Describes the Cisco NX-OS TrustSec commands that begin with A.
C Commands	Describes the Cisco NX-OS TrustSec commands that begin with C.
F Commands	Describes the Cisco NX-OS TrustSec commands that begin with F.
P Commands	Describes the Cisco NX-OS TrustSec commands that begin with P.
Show Commands	Describes the Cisco NX-OS TrustSec **show** commands.

Document Conventions

Command descriptions use these conventions:

Convention	Description
boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
{x | y | z}	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use these conventions:

`screen font`	Terminal sessions and information that the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.

`italic screen font`	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means reader *be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

Documentation for Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extender is available at the following URL:

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

The following are related Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Fabric Extender documents:

Release Notes

Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes

Cisco Nexus 5000 Series Switch Release Notes

Configuration Guides

Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 5.0(2)N1(1)

Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 4.2(1)N1(1) and Release 4.2(1)N2(1)

Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide

Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide

Cisco Nexus 5000 Series NX-OS Multicast Routing Configuration Guide

Cisco Nexus 5000 Series NX-OS Quality of Service Configuration Guide

Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide

Cisco Nexus 5000 Series NX-OS Security Configuration Guide

Cisco Nexus 5000 Series NX-OS System Management Configuration Guide

Cisco Nexus 5000 Series NX-OS Unicast Routing Configuration Guide

Cisco Nexus 5000 Series Switch NX-OS Software Configuration Guide

Cisco Nexus 5000 Series Fabric Manager Configuration Guide, Release 3.4(1a)

Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x

Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide

Maintain and Operate Guides

Cisco Nexus 5000 Series NX-OS Operations Guide

Installation and Upgrade Guides

Cisco Nexus 5000 Series and Cisco Nexus 5500 Platform Hardware Installation Guide

Cisco Nexus 2000 Series Hardware Installation Guide

Cisco Nexus 5000 Series NX-OS Software Upgrade and Downgrade Guide, Release 4.2(1)N1(1)

Regulatory Compliance and Safety Information for the Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders

Licensing Guide

Cisco NX-OS Licensing Guide

Command References

Cisco Nexus 5000 Series NX-OS FabricPath Command Reference

Cisco Nexus 5000 Series NX-OS Fabric Extender Command Reference

Cisco Nexus 5000 Series NX-OS Fibre Channel Command Reference

Cisco Nexus 5000 Series NX-OS Fundamentals Command Reference

Cisco Nexus 5000 Series NX-OS Layer 2 Interfaces Command Reference

Cisco Nexus 5000 Series NX-OS Multicast Routing Command Reference

Cisco Nexus 5000 Series NX-OS QoS Command Reference

Cisco Nexus 5000 Series NX-OS Security Command Reference

Cisco Nexus 5000 Series NX-OS System Management Command Reference

Cisco Nexus 5000 Series NX-OS TrustSec Command Reference

Cisco Nexus 5000 Series NX-OS Unicast Routing Command Reference

Cisco Nexus 5000 Series NX-OS vPC Command Reference

Technical References

Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Fabric Extender MIBs Reference

Error and System Messages

Cisco NX-OS System Messages Reference

Troubleshooting Guide

Cisco Nexus 5000 Troubleshooting Guide

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 5000 Series NX-OS TrustSec Command Reference*. The latest version of this document is available at the following Cisco website:

http://www.cisco.com/en/US/products/ps9670/prod_command_reference_list.html

To check for additional information about this Cisco NX-OS Release, see the *Cisco Nexus 5000 Series Switch Release Notes* available at the following Cisco website:

http://www.cisco.com/en/US/products/ps9670/prod_release_notes_list.html

New and Changed Information for Cisco NX-OS Releases

This section includes the following topics:

- New and Changed Information for Cisco NX-OS Release 5.2(1)N1(1), page xiii
- New and Changed Information for Cisco NX-OS Release 5.1(3)N1(1), page xiii

New and Changed Information for Cisco NX-OS Release 5.2(1)N1(1)

There are no new or changed features in this release.

New and Changed Information for Cisco NX-OS Release 5.1(3)N1(1)

Table 1 summarizes the new and changed features for Cisco NX-OS Release 5.1(3)N1(1) and tells you where they are documented.

Table 1 New and Changed Information for Release 5.1(3)N1(1)

Feature	Description	Changed in Release	Where Documented
Cisco TrustSec	This feature was introduced.	5.1(3)N1(1)	A Commands C Commands D Commands F Commands P Commands Show Commands

A Commands

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

aaa authentication cts default group

To configure the default authentication, authorization, and accounting (AAA) RADIUS server groups for Cisco TrustSec authentication, use the **aaa authentication cts default group** command. To remove a server group from the default AAA authentication server group list, use the **no** form of this command.

aaa authentication cts default group *group-list*

no aaa authentication cts default group *group-list*

Syntax Description

group-list	Space-separated list of RADIUS server groups that can include the following: • **radius** for all configured RADIUS servers. • Any configured RADIUS server group name. The maximum number of names in the list is eight.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.1(3)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 *group-list* refers to a set of previously defined RADIUS servers. Use the **radius-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa groups** command to display the RADIUS server groups on the device. See the *Cisco Nexus 5000 Series NX-OS Security Command Reference* for information on these commands.

If you specify more than one server group, the Cisco NX-OS software checks each group in the order that you specify in the list.

This command does not require a license.

Examples

This example shows how to configure the default AAA authentication RADIUS server group for Cisco TrustSec:

```
switch# configure terminal
swtich(config)# aaa authentication cts default group RadGroup
swtich(config)#
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature on the switch.
radius-server host	Configures RADIUS servers.
show aaa authentication	Displays the AAA authentication configuration.
show aaa groups	Displays the AAA server groups.

aaa authorization cts default group

To configure the default authentication, authorization, and accounting (AAA) RADIUS server groups for Cisco TrustSec authorization, use the **aaa authorization cts default group** command. To remove a server group from the default AAA authorization server group list, use the **no** form of this command.

aaa authorization cts default group *group-list*

no aaa authorization cts default group *group-list*

Syntax Description

group-list	Space-separated list of RADIUS server groups that can include the following: • **radius** for all configured RADIUS servers. • Any configured RADIUS server group name. The maximum number of names in the list is eight.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

To use the **aaa authorization cts default group** command, you must enable the Cisco TrustSec feature using the **feature cts** command.

The *group-list* refers to a set of previously defined RADIUS servers. Use the **radius-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa groups** command to display the RADIUS server groups on the device. See the *Cisco Nexus 5000 Series NX-OS Security Command Reference* for information on these commands.

If you specify more than one server group, the Cisco NX-OS software checks each group in the order that you specify in the list.

This command does not require a license.

Examples

This example shows how to configure the default AAA authorization RADIUS server group for Cisco TrustSec:

```
switch# configure terminal
swtich(config)# aaa authorization cts default group RadGroup
swtich(config)#
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show aaa authorization	Displays the AAA authorization configuration.
show aaa groups	Displays the AAA server groups.

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
5.1(3)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
5.1(3)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
5.1(3)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
5.1(3)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
5.1(3)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
5.1(3)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
5.1(3)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
5.1(3)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
5.1(3)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
5.1(3)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
5.1(3)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
5.1(3)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
5.1(3)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
5.1(3)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
5.1(3)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
5.1(3)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.

D Commands

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

deny

To configure a deny action in the security group access control list (SGACL), use the **deny** command. To remove the action, use the **no** form of this command.

deny {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**dest** | **dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**log**]

no deny {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**dest** | **dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**log**]

Syntax Description

all	Specifies all traffic.
icmp	Specifies Internet Control Message Protocol (ICMP) traffic.
igmp	Specifies Internet Group Management Protocol (IGMP) traffic.
ip	Specifies IP traffic.
tcp	Specifies TCP traffic.
udp	Specifies User Datagram Protocol (UDP) traffic.
dest	Specifies the destination port number.
dst	Specifies the destination port number.
src	Specifies the source port number.
eq	Specifies equal to the port number.
gt	Specifies greater than the port number.
lt	Specifies less than the port number.
neq	Specifies not equal to the port number.
port-number	Port number for TCP or UDP. The range is from 0 to 65535.
range	Specifies a port range for TCP or UDP.
port-number1	First port in the range. The range is from 0 to 65535.
port-number2	Last port in the range. The range is from 0 to 65535.
log	(Optional) Specifies that packets matching this configuration be logged.

Command Default

None

Command Modes

role-based access control list (RBACL)

Command History

Release	Modification
5.1(3)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 enable RBACL logging, you must enable RBACL policy enforcement on the VLAN. You must also enable Cisco TrustSec counters using the **cts role-based counters enable** command.

This command does not require a license.

Examples

This example shows how to add a deny action to an SGACL and enable RBACL logging:

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

This example shows how to remove a deny action from an SGACL:

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

Related Commands

Command	Description
cts role-based access-list	Configures Cisco TrustSec SGACLs.
cts role-based counters	Enables RBACL counters.
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature on the switch.
permit	Configures permit actions in an SGACL.
show cts role-based access-list	Displays the Cisco TrustSec SGACL configuration.

F Commands

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

feature cts

To enable the Cisco TrustSec feature, use the **feature cts** command. To revert to the default, use the **no** form of this command.

feature cts

no feature cts

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature dot1x** command.

This command does not require a license.

Examples

This example shows how to enable the Cisco TrustSec feature:

```
switch# configure terminal
switch(config)# feature cts
switch(config)#
```

This example shows how to disable the Cisco TrustSec feature:

```
switch# configure terminal
switch(config)# no feature cts
switch(config)#
```

Related Commands

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

feature dot1x

To enable the 802.1X feature, use the **feature dot1x** command. To revert to the default setting, use the **no** form of this command.

feature dot1x

no feature dot1x

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you enable the Cisco TrustSec feature on the switch by using the **feature cts** command.

This command does not require a license.

Examples

This example shows how to enable 802.1X:

```
switch# configure terminal
switch(config)# feature dot1x
switch(config)#
```

This example shows how to disable 802.1X:

```
switch# configure terminal
switch(config)# no feature dot1x
switch(config)#
```

Related Commands

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

P Commands

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

permit

To configure a permit action in a security group access control list (SGACL), use the **permit** command. To remove the action, use the **no** form of this command.

permit {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**dest** | **dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**log**]

no permit {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**dest** | **dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**log**]

Syntax Description

all	Specifies all traffic.
icmp	Specifies Internet Control Message Protocol (ICMP) traffic.
igmp	Specifies Internet Group Management Protocol (IGMP) traffic.
ip	Specifies IP traffic.
tcp	Specifies TCP traffic.
udp	Specifies User Datagram Protocol (UDP) traffic.
dest	Specifies the destination port number.
dst	Specifies the destination port number.
src	Specifies the source port number.
eq	Specifies equal to the port number.
gt	Specifies greater than the port number.
lt	Specifies less than the port number.
neq	Specifies not equal to the port number.
port-number	Port number for TCP or UDP. The range is from 0 to 65535.
range	Specifies a port range for TCP or UDP.
port-number1	First port in the range. The range is from 0 to 65535.
port-number2	Last port in the range. The range is from 0 to 65535.
log	(Optional) Specifies that packets matching this configuration be logged.

Defaults

None

Command Modes

role-based access control list (RBACL)

Command History

Release	Modification
5.1(3)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 enable RBACL logging, you must enable RBACL policy enforcement on the VLAN. You must also enable Cisco TrustSec counters using the **cts role-based counters enable** command.

This command does not require a license.

Examples

This example shows how to add a permit action to an SGACL and enable RBACL logging:

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

This example shows how to remove a permit action from an SGACL:

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

Related Commands

Command	Description
cts role-based access-list	Configures Cisco TrustSec SGACLs.
cts role-based counters	Enables RBACL counters.
deny	Configures deny actions in an SGACL.
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.

policy

To manually configure a Cisco TrustSec authentication policy on an interface with either a Cisco TrustSec device identifier or security group tag (SGT), use the **policy** command. To revert to the default, use the **no** form of this command.

policy {**dynamic identity** *device-id* | **static sgt** *sgt-value* [**trusted**]}

no policy {**dynamic** | **static**}

Syntax Description

dynamic identity	Specifies a dynamic policy using a Cisco TrustSec device identifier.
device-id	Cisco TrustSec device identifier. The device identifier is case sensitive.
static sgt	Specifies a static policy using an SGT.
sgt-value	Cisco TrustSec SGT. The format is **0x***hhhh.* The range is 0x2 to 0xffef.
trusted	(Optional) Specifies that traffic coming on the interface with the SGT should not have its tag overridden.

Command Default

None

Command Modes

Cisco TrustSec manual configuration mode

Command History

Release	Modification
5.1(3)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 manually configure a dynamic Cisco TrustSec policy on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy dynamic identity DeviceB
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

This example shows how to remove a manually configured dynamic Cisco TrustSec policy from an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# no policy dynamic
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

This example shows how to manually configure a static Cisco TrustSec policy on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy static sgt 0x100
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

This example shows how to remove a manually configured static Cisco TrustSec policy on an interface:

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

Related Commands

Command	Description
cts manual	Enters Cisco TrustSec manual configuration mode for an interface.
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature on the switch.
show cts interface	Displays the Cisco TrustSec configuration for interfaces.

propagate-sgt

To enable security group tag (SGT) propagation on Layer 2 Cisco TrustSec interfaces, use the **propagate-sgt** command. To disable SGT propagation, use the **no** form of this command.

propagate-sgt

no propagate-sgt

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled if manual configuration is enabled on the interface.

Disabled if manual configuration is disabled on the interface.

Command Modes

Global configuration mode

Command History

Release	Modification
5.1(3)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 disable the SGT propagation feature on an interface if the peer device connected to the interface can not handle Cisco TrustSec packets tagged with an SGT.

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 disable SGT propagation:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts manual
switch(config-if-cts-manual)# no propagate-sgt
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

This example shows how to enable SGT propagation:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts manual
switch(config-if-cts-manual)# propagate-sgt
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

Related Commands

Command	Description
cts manual	Enables Cisco TrustSec manual configuration on an interface.
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature on the switch.
show cts interface	Displays the Cisco TrustSec configuration for interfaces.

Show Commands

This chapter describes the Cisco NX-OS TrustSec **show** commands.

show cts

To display the global Cisco TrustSec configuration, use the **show cts** command.

show cts

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the Cisco TrustSec global configuration:

```
switch# show cts
CTS Global Configuration
==============================
  CTS support            : enabled
  CTS device identity    : not configured
  SGT                    : 0
  CTS caching support    : disabled

  Number of CTS interfaces in
    DOT1X mode : 0
    Manual mode : 1

switch#
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts credentials

To display the Cisco TrustSec device credentials configuration, use the **show cts credentials** command.

show cts credentials

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the Cisco TrustSec credentials configuration:

```
switch# show cts credentials
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts environment-data

To display the global Cisco TrustSec environment data, use the **show cts environment-data** command.

show cts environment-data

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

The Cisco NX-OS device downloads the Cisco TrustSec environment data from the ACS after you have configured the Cisco TrustSec credentials for the device and configured authentication, authorization, and accounting (AAA).

This command does not require a license.

Examples

This example shows how to display the Cisco TrustSec environment data:

```
switch# show cts environment-data
CTS Environment Data
==============================
  Current State           : CTS_ENV_DNLD_ST_INIT_STATE
  Last Status             : CTS_ENV_INCOMPLETE
  Local Device SGT        : 0x0000
  Transport Type          : CTS_ENV_TRANSPORT_DIRECT
  Data loaded from cache  : FALSE
  Env Data Lifetime       :
  Last Update Time        : Never
  Server List             :
     AID: IP: Port:

switch#
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

Send comments to nexus5k-docfeedback@cisco.com

show cts interface

To display the Cisco TrustSec information for interfaces, use the **show cts interface** command.

show cts interface {**all** | **ethernet** *slot*/*port* | **vethernet** *veth-num*}

Syntax Description

all	Displays Cisco TrustSec information for all interfaces.
ethernet *slot*/*port*	Displays Cisco TrustSec information for the specific Ethernet interface. The slot number is from 1 to 255 and the port number is from 1 to 48.
vethernet *veth-num*	Displays Cisco TrustSec information for the specific virtual Ethernet (vEthe) interface. The virtual Ethernet interface number is from 1 to 1048575.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

You must enable the Cisco Virtual Machine on the switch by using the **feature-set virtualization** command to see the **vethernet** keyword.

This command does not require a license.

Examples

This example shows how to display the Cisco TrustSec configuration for a specific interface:

```
switch# show cts interface ethernet 1/5
CTS Information for Interface Ethernet1/5:
    CTS is enabled, mode:   CTS_MODE_MANUAL
    IFC state:              Unknown
    Authentication Status:  CTS_AUTHC_INIT
      Peer Identity:
      Peer is:              Unknown in manual mode
      802.1X role:          CTS_ROLE_UNKNOWN
      Last Re-Authentication:
    Authorization Status:   CTS_AUTHZ_INIT
      PEER SGT:             3
      Peer SGT assignment:  Not Trusted
    SAP Status:             CTS_SAP_INIT
      Configured pairwise ciphers:
      Replay protection:
      Replay protection mode:
      Selected cipher:
      Current receive SPI:
      Current transmit SPI:
```

```
    Propagate SGT: Enabled

switch#
```

This example shows how to display the Cisco TrustSec configuration for all interfaces:

```
switch# show cts interface all
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
feature-set virtualization	Enables the Cisco Virtual Machine features on the switch.

show cts pacs

To display the Cisco TrustSec protect access credentials (PACs) provisioned by EAP-FAST, use the **show cts pacs** command.

show cts pacs

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the Cisco TrustSec global configuration:

```
switch# show cts pacs
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts role-based access-list

To display the global Cisco TrustSec security group access control list (SGACL) configuration, use the **show cts role-based access-list** command.

show cts role-based access-list [*list-name*]

Syntax Description

list-name	(Optional) SGACL name.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the Cisco TrustSec SGACL configuration:

```
switch# show cts role-based access-list
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts role-based counters

To display the configuration status of role-based access control list (RBACL) statistics and list the statistics for all RBACL policies, use the **show cts role-based counters** command.

show cts role-based counters

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(3)N1(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 also enable Cisco TrustSec counters using the **cts role-based counters enable** command.

This command does not require a license.

Examples

This example shows how to display the configuration status of RBACL statistics:

```
switch# show cts role-based counters

RBACL policy counters enabled
Counters last cleared: Never
rbacl:ACS_1101_15
        permit icmp log                                 [0]
        permit tcp log                                  [0]
        deny udp log                                  [0]

switch#
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature on the switch.
clear cts role-based counters	Clears the RBACL statistics so that all counters are reset to 0.
cts role-based counters enable	Enables the RBACL statistics.

show cts role-based enable

To display the Cisco TrustSec security group access control list (SGACL) enable status for VLANs, use the **show cts role-based enable** command.

show cts role-based enable

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the Cisco TrustSec SGACL enforcement status:

```
switch# show cts role-based enable
vlan:102
switch#
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
cts role-based enforcement	Enables role-based access control list (RBACL) enforcement on VLANs.

show cts role-based policy

To display the global Cisco TrustSec security group access control list (SGACL) policies, use the **show cts role-based policy** command.

show cts role-based policy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the Cisco TrustSec SGACL policies:

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

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts role-based sgt-map

To display the global Cisco TrustSec Security Group Tag (SGT) mapping configuration, use the **show cts role-based sgt-map** command.

show cts role-based sgt-map

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the Cisco TrustSec SGT mapping configuration:

```
switch# show cts role-based sgt-map
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts sxp

To display the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (SXP) configuration, use the **show cts sxp** command.

show cts sxp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the Cisco TrustSec SXP configuration:

```
switch# show cts sxp
CTS SXP Configuration:
SXP enabled
SXP retry timeout:60
SXP reconcile timeout:120
switch#
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts sxp connection

To display the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (SXP) connections information, use the **show cts sxp connection** command.

show cts sxp connection

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (SXP) connections information:

```
switch# show cts sxp connection
PEER_IP_ADDR    VRF             PEER_SXP_MODE   SELF_SXP_MODE   CONNECTION STATE
192.0.2.1       default         listener        speaker         initializing
switch#
```

Related Commands

Command	Description
cts sxp connection peer	Configures a SXP peer connection.
feature cts	Enables the Cisco TrustSec feature.

show running-config cts

To display the Cisco TrustSec configuration in the running configuration, use the **show running-config cts** command.

show running-config cts

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the Cisco TrustSec configuration in the running configuration:

```
switch# show running-config cts

!Command: show running-config cts
!Time: Thu Jan  1 05:33:03 2009

version 6.0(0)N1(1)
feature cts
cts role-based counters enable
cts sxp enable
cts sxp connection peer 192.0.2.1 password none mode listener


interface Ethernet1/5
  cts manual
    policy static sgt 0x3

switch#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration information to the startup configuration file.
feature cts	Enables the Cisco TrustSec feature.

show running-config dot1x

To display 802.1X configuration information in the running configuration, use the **show running-config dot1x** command.

show running-config dotx1 [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

You must enable the 802.1X feature by using the **feature dot1x** command before using this command.

This command does not require a license.

Examples

This example shows how to display the configured 802.1X information in the running configuration:

```
switch# show running-config dot1x
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running system configuration information to the startup configuration file.
feature cts	Enables the Cisco TrustSec feature on the switch.
feature dot1x	Enables the 802.1X feature on the switch.

show startup-config cts

To display the Cisco TrustSec configuration information in the startup configuration, use the **show startup-config cts** command.

show startup-config cts

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the Cisco TrustSec information in the startup configuration:

```
switch# show startup-config cts
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration information to the startup configuration file.

show startup-config dot1x

To display 802.1X configuration information in the startup configuration, use the **show startup-config dot1x** command.

show startup-config dot1x

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

You must enable the 802.1X feature by using the **feature dot1x** command before using this command.

This command does not require a license.

Examples

This example shows how to display the 802.1X information in the startup configuration:

```
switch# show startup-config dot1x
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration information to the startup configuration file.