Cisco TrustSec Command Summary

Revised: August 3, 2016

Cisco TrustSec Privileged EXEC Commands	
cts change-password	Initiates password change with AAA server. **Note** Effective with Cisco IOS Release 15.1(1)SY, this command is not available in Cisco IOS software.
cts credentials	Inserts Cisco TrustSec device ID and password into the keystore.
cts refresh	Refreshes environment, peer and RBACL policies.
cts rekey	Regenerates the Pairwise Master Key used by the Security Association Protocol (SAP),
cts role-based policy trace	TrustSec SGT and SGACL trace utility.

Cisco TrustSec Global Configuration Commands	
cts authorization list	Configures Cisco TrustSec global authorization configuration.
cts cache	Enables caching of TrustSec authorization and environment-data information to DRAM and NVRAM.
cts manual	Defines Cisco TrustSec keystore behavior.
cts policy layer3	Specifies traffic and exception policies for Cisco TrustSec Layer 3 Transport gateway interfaces.
cts role-based	Maps IP addresses, Layer 3 interfaces, and VRFs to SGTs. Enables Cisco TrustSec caching and SGACL enforcement.
cts server	Configures RADIUS server list configuration.
cts sgt	Configures local device security group tag.

cts sxp	Configures SGT exchange over TCP.
Cisco TrustSec Flexible NetFlow Commands	
match flow cts	Adds Cisco TrustSec flow objects to a Flexible NetFlow flow record.

Cisco TrustSec Interface Configuration Commands

cts dot1x	Enters CTS dot1x Interface Configuration mode (config-if-cts-dot1x).
cts layer3	Enables and applies traffic and exception policies to Cisco TrustSec Layer 3 Transport gateway interfaces.
cts manual	Supplies local configuration for Cisco TrustSec parameters.
platform cts	Enables the TrustSec egress or ingress reflector.

Cisco TrustSec dot1x Submode Commands

default (cts dot1x)	Restores defaults for Cisco TrustSec dot1x commands.
propagate sgt (cts dot1x)	Enables/disables SGT propagation in dot1x mode.
sap (cts dot1x)	Configures Cisco TrustSec SAP for dot1x mode.
timer (cts do1x)	Configures the Cisco TrustSec timer.

Cisco TrustSec Manual Interface Configuration Submode Commands

default (cts manual)	Restores default configurations for Cisco TrustSec manual mode.
policy (cts manual)	Configures Cisco TrustSec policy for manual mode
propagate sgt (cts manual)	Configures Cisco TrustSec SGT Propagation configuration for manual mode
sap (cts manual)	Configures Cisco TrustSec SAP for manual mode.

Cisco TrustSec Clear Commands

clear cts cache	Clears TrustSec cache file by type, filename or all cache files.
clear cts counter	Clears counters for a single TrustSec interface or for all interfaces
clear cts credentials	Clears all Cisco TrustSec credentials, including all PACs.
clear cts environment-data	Clears TrustSec environment data from cache.
clear cts macsec	Clears MACsec counters for a specified interface.
clear cts pac	Clears a PAC or all PACs from the keystore.
clear cts policy	Clears the peer authorization policy of a TrustSec peer.
clear cts role-based counters	Displays role-based access control enforcement statistics for SGTs and DGTs.
clear cts server	Removes the specified authentication server.

Cisco TrustSec Show Commands	
show cts authorization entries	Displays the authorization entries.
show cts credentials	Displays credentials used for Cisco TrustSec authentication.
show cts environment-data	Displays the Cisco TrustSec environment data.
show cts interface	Displays Cisco TrustSec states and statistics per interface.
show cts macsec	Displays MACSec counters information.
show cts pacs	Displays the A-ID and PAC-info for PACs in the keystore.
show cts policy peer	Displays the peer authorization policies of TrustSec peers.
show cts policy layer3	Displays the traffic and exception policies used in Cisco TrustSec Layer 3 Transport.
show cts provisioning	Displays outstanding Cisco TrustSec provisioning jobs.
show cts rbacl	Displays the Cisco TrustSec RBACL policy.
show cts role-based sgt-map	Displays IP address-to-Security Group Tag mappings.
show cts role-based counters	Displays role-based access control enforcement statistics for SGTs and DGTs.
show cts role-based flow	Displays IP-to-SGT bindings, permission lists, and NetFlow statistics.
show cts role-based permissions	Displays Permissions lists (Role-based ACLs).
show cts server-list	Displays lists of AAA servers and load balancing configurations.
show cts sxp	Displays Cisco TrustSec SXP protocol information.
show cts keystore	Displays the contents of the keystore.
show platform cts reflector	Displays the status of Cisco TrustSec reflector per interface.
Commands to Configure Endpoint Admission Control (EAC)	
aaa accounting	Enables authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa authorization	Sets the parameters that restrict user access to a network,
aaa authentication	Sets authentication parameters.
radius-server host	Specifies a RADIUS server host.
authentication port-control	Configures the authorization state of a controlled port.
dot1x pae	Sets the Port Access Entity (PAE) type.

Debug Commands	
debug authentication event	Displays debugging information about Authentication Manager events.
debug authentication feature	Displays debugging information about specific features.
debug condition cts	Filters Cisco TrustSec debugging messages by interface name, peer ID, peer-SGT or Security Group name.
debug condition cts peer-id	Filters Cisco TrustSec debugging messages by the Peer ID.
debug condition cts security-group	Filters Cisco TrustSec debugging messages by the security group name.
debug cts	Enables the debugging of Cisco TrustSec operations.

cts authorization list

To specify a list of authentication, authorization, and accounting (AAA) servers to use by the TrustSec seed device, use the **cts authorization list** command on the Cisco TrustSec seed device in global configuration mode. Use the **no** form of the command to stop using the list during authentication.

cts authorization list *server_list*

no cts authorization list *server_list*

Syntax Description

server_list	Cisco TrustSec AAA server group.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2 (33)SXI3	This command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

This command is only for the seed device. Non-seed devices obtain the TrustSec AAA server list from their TrustSec authenticator peer as a component of their TrustSec environment data.

Examples

The following example displays an AAA configuration of a TrustSec seed device:

```
Switch# cts credentials id Switch1 password Cisco123
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# aaa authorization network MLIST group radius
Switch(config)# cts authorization list MLIST
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key
AbCe1234
Switch(config)# radius-server vsa send authentication
Switch(config)# dot1x system-auth-control
Switch(config)# exit
```

Related Commands

Command	Description
show cts server-list	Displays RADIUS server configurations.

cts cache

To enable caching of TrustSec authorization and environment data information to DRAM and NVRAM, use the **cts cache** command. Use the **no** form of the command to disable caching.

[**no**] **cts cache** {**enable | nv-storage** {**bootflash:** [*dir*] **| disk0:** [*dir*] **| disk1:** [*dir*] **| sup-bootflash:** [*image*]}}

Syntax Description

enable	Enables Cisco TrustSec cache support
nv-storage	Causes DRAM cache updates to be written to non-volatile storage and enables DRAM cache to be initially populated from nv-storage when the network device boots.
bootflash: *dir*	Specifies bootflash directory as the nv-storage location.
disk0: *dir*	Specifies disk 0 directory as the nv-storage location.
disk1: *dir*	Specifies disk 1 directory as the nv-storage location.
sup-bootflash: *image*	Specifies a supervisor bootflash directory as the nv-storage location.

Defaults

Caching is disabled.

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Catalyst 6500 series switches.
12.2(50)SY	PMK caching support was added for the Catalyst 6500 series switches.

Usage Guidelines

The **cts cache** command enables caching of authentication, authorization and environment-data information to DRAM. Caching is for the maintenance and reuse of information obtained through authentication and authorization. Keystore provides for secure storage of a device's own credentials (passwords, certificates, PACs) either in the software or on a specialized hardware component. In the absence of a dedicated hardware keystore, a software emulation keystore is created using DRAM and NVRAM.

Cisco TrustSec creates a secure cloud of devices in a network by requiring that each device authenticate and authorize its neighbors with a trusted AAA server (Cisco Secure ACS 5.1 or more recent) before being granted access to the TrustSec network. Once the authentication and authorization is complete, the information could be valid for some time. If caching is enabled, that information can be reused, allowing the network device to bring up links without having to connect with the ACS. And expediting the formation of the Cisco TrustSec cloud upon reboot, improving network availability, and reducing the load on the ACS. Caching can be stored in volatile memory (information does not survive a reboot) or nonvolatile memory (information survives a reboot).

Examples

The following example shows how to enable cache support:

```
Switch# configure terminal
Switch(config)# cts cache nv-storage disk0:
Switch(config)# cts cache enable
```

Related Commands

Command	Description
clear cts cache	Clears the content of the keystore.
show cts keystore	Displays the content of the keystore.
cts rekey	Regenerates the Pairwise Master Key used by the Security Association Protocol (SAP).
cts credentials	Specifies the TrustSec ID and password of the network device.

cts change-password

Note Effective with Cisco IOS Release 15.1(1)SY, the **cts change-password** command is not available in Cisco IOS software.

To change the password between the local device and the authentication server, use the **cts change-password** privileged EXEC command.

cts change-password server *ipv4_address udp_port* {**a-id** *hex_string* | **key** *radius_key*} [**source** *interface_list*]

Syntax Description

server	Specifies the authentication server.
ipv4_address	IP address of the authentication server.
udp_port	UPD port of the authentication server.
a-id *hex_string*	Specifies the identification string of the ACS server.
key	Specifies the RADIUS key to be used for provisioning.
source	Specifies the interface for source address in request packets.S
interface_list	Interface type and its identifying parameters as per the displayed list.

Defaults

None.

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on the Catalyst 6500 Series Switches.
15.1(1)SY	This command was removed.

Usage Guidelines

The **cts change-password** command allows an administrator to change the password used between the local device and the Cisco Secure ACS authentication server, without having to reconfigure the authentication server.

Note The **cts change-password** is supported on Cisco Secure ACS, 5.1 and later versions.

For Catalyst 6500 switches with dual-supervisor chassis, the hardware-based keystores must be manually synchronized when inserting a second supervisor linecard. A password change process may be invoked to make both active and standby supervisors have the same device password.

Examples

The following example shows how to change the Cisco TrustSec password between a Catalyst 6500 switch and a Cisco Secure ACS:

```
switch# cts change-password server 192.168.2.2 88 a-id ffef
```

cts credentials

Use the **cts credentials** command in privileged EXEC mode to specify the TrustSec ID and password of the network device. Use the **clear cts credentials** command to delete the credentials.

cts credentials id *cts_id* **password** *cts_pwd*

Syntax Description

credentials id *cts_id*	Specifies the Cisco TrustSec device ID for this device to use when authenticating with other Cisco TrustSec devices with EAP-FAST. The *cts-id* variable has a maximum length of 32 characters and is case sensitive.
password *cts_pwd*	Specifies the password for this device to use when authenticating with other Cisco TrustSec devices with EAP-FAST.

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.

Usage Guidelines

The **cts credentials** command specifies the Cisco TrustSec device ID and password for this switch to use when authenticating with other Cisco TrustSec devices with EAP-FAST. The Cisco TrustSec credentials state retrieval is not performed by the nonvolatile generation process (NVGEN) because the Cisco TrustSec credential information is saved in the keystore, and not in the startup configuration. The device can be assigned a Cisco TrustSec identity by the Cisco Secure Access Control Server (ACS), or a new password auto-generated when prompted to do so by the ACS. These credentials are stored in the keystore, eliminating the need to save the running configuration. To display the Cisco TrustSec device ID, use the **show cts credentials** command. The stored password is never displayed.

To change the device ID or the password, reenter the command. To clear the keystore, use the **clear cts credentials** command.

Note When the Cisco TrustSec device ID is changed, all Protected Access Credentials (PACs) are flushed from the keystore because PACs are associated with the old device ID and are not valid for a new identity.

Examples

The following example shows how to configure the Cisco TrustSec device ID and password:

```
Switch# cts credentials id cts1 password password1
CTS device ID and password have been inserted in the local keystore. Please make sure that
the same ID and password are configured in the server database.
```

The following example show how to change the Cisco TrustSec device ID and password to cts_new and password123, respectively:

```
Switch# cts credentials id cts_new pacssword password123
A different device ID is being configured.
This may disrupt connectivity on your CTS links.
Are you sure you want to change the Device ID? [confirm] y

TS device ID and password have been inserted in the local keystore. Please make sure that
the same ID and password are configured in the server database.
```

The following sample output displays the Cisco TrustSec device ID and password state:

```
Switch# show cts credentials

CTS password is defined in keystore, device-id = cts_new
```

Related Commands

Command	Description
clear cts credentials	Clears the Cisco TrustSec device ID and password.
show cts credentials	Displays the state of the current Cisco TrustSec device ID and password.
show cts keystore	Displays contents of the hardware and software keystores.

cts dot1x

To configure the Cisco TrustSec reauthentication timer on an interface, and to enter the CTS dot1x interface configuration mode (config-if-cts-dot1x), use the **cts dot1x** command. Use the **no** form of the command to disable the timers on an interface.

[**no**] **cts dot1x**

Syntax Description

This command has no arguments or keywords.

Defaults

CTS dot1x configuration on the interface is disabled.

Command Modes

Interface configuration (config-if)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2 (33)SXI3	This command was introduced on Catalyst 6500 series switches.

Usage Guidelines

Before configuring the TrustSec dot1x reauthentication timer, configure dot1x globally from the interface. The Cisco TrustSec dot1x configuration governs TrustSec NDAC, and not TrustSec EAC processes.

Examples

The following example shows a Catalyst 6500 Series switch enter Cisco TrustSec configuration mode without first enabling dot1x in interface configuration mode:

```
Switch(config-if)# cts dot1x
Warning: Global dot1x is not configured, CTS will not run until dot1x is enabled
. (Gi3/1)

Switch(config-if-cts-dot1x)# ?
CTS dot1x configuration commands:
  default  Set a command to its defaults
  exit     Exit from CTS dot1x sub mode
  no       Negate a command or set its defaults
  timer    CTS timer configuration
```

Related Commands

Command	Description
default timer reauthentication (cts interface)	Resets the Cisco TrustSec dot1x reauthentication timer to the default value.
timer reauthentication (cts interface)	Sets the Cisco TrustSec dot1x reauthentication timer.
show cts interface	Displays Cisco TrustSec interface status and configurations.
show dot1x interface	Displays IEEE 802.1x configurations and statistics.

default timer reauthentication (cts interface)

Use the **default timer reauthentication** command in CTS interface configuration mode to reset the Cisco TrustSec dot1x reauthentication timer to the default value.

default timer reauthentication

Syntax Description

timer reauthentication	Sets the Cisco TrustSec reauthentication timer to the default values.

Defaults

3600 seconds

Command Modes

CTS interface configuration (config-if-cts-dot1x)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.

Usage Guidelines

The default value of the Cisco TrustSec reauthentication timer is 3600 seconds. When this timer expires, the device reauthenticates to the Cisco TrustSec network (NDAC).

Examples

The following example shows how to reset the Cisco TrustSec reauthentication timer to the global default values:

```
Switch # configure terminal
Switch(config)# interface gigabitEthernet 3/1
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# default timer reauthentication
```

Related Commands

Command	Description
cts dot1x	Enters Cisco TrustSec dot1x interface configuration mode (config-if-cts-dot1x).
timer reauthentication (cts interface)	Sets the Cisco TrustSec reauthentication timer.
show cts interface	Displays Cisco TrustSec interface status and configurations.
show dot1x interface	Displays IEEE 802.1x configurations and statistics.

timer reauthentication (cts interface)

Use the **timer reauthentication** command in CTS interface configuration mode to set the reauthentication timer. Use the **no** form of the command to disable the timer.

[**no**] **timer reauthentication** *seconds*

Syntax Description

reauthentication *seconds*	Sets the reauthentication timer in seconds.

Defaults

The reauthentication timer is not configured.

Command Modes

CTS interface configuration (config-if-cts-dot1x)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.

Usage Guidelines

This command sets the TrustSec reauthentication timer. When this timer expires, the device reauthenticates to the Cisco TrustSec network (NDAC).

Examples

The following example shows how to set the reauthentication timer to 44 seconds:

```
Switch(config-if-cts-dot1x)# timer reauthentication 44
```

Related Commands

Command	Description
cts dot1x	Enters Cisco TrustSec dot1x interface configuration mode (config-if-cts-dot1x).
default timer reauthentication (cts interface)	Resets the Cisco TrustSec dot1x reauthentication timer to the default value.
show cts interface	Displays Cisco TrustSec interface status and configurations.
show dot1x interface	Displays IEEE 802.1x configurations and statistics.

cts layer3

To enable Cisco TrustSec Layer 3 transport gateway interfaces, and to apply exception and traffic policies to the interfaces, use the **cts layer 3** interface configuration command.

cts layer3 {**ipv4** | **ipv6**} {**policy** | **trustsec forwarding**}

Syntax Description

ipv4 | **ipv6**	Specifies IPv4 or IPv6.
policy	Applies the traffic and exception policies on the gateway interface.
trustsec forwarding	Enables Cisco TrustSec Layer 3 transport on the gateway interface.

Defaults

Cisco TrustSec Layer3 Transport is not enabled.

Command Modes

Interface configuration (config-if)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.
Cisco IOS XE Release 3.3.0 SG	This command was implemented on Catalyst 4000 Series switches.
15.0(1)SE	This command was implemented on Catalyst 3750(X) Series switches.

Usage Guidelines

Use the **cts policy layer3** global configuration command to specify which traffic and exception commands to apply to the Cisco TrustSec Layer 3 gateway. Use the **cts layer3** interface configuration command to enable the Cisco TrustSec Layer 3 gateway interface and to apply the traffic and exception policies.

Examples

The following example shows how to enable a Cisco TrustSec Layer 3 Transport gateway interface:

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# cts layer3 ipv4 trustsec forwarding
Switch(config-if)# cts layer3 ipv4 trustsec
Switch(config-if)# cts layer3 ipv4 policy
```

Related Commands

Command	Description
cts policy layer3	Specifies traffic and exception policies for Cisco TrustSec Layer 3 Transport.
show cts policy layer3	Displays the name of traffic and exception polices used for Cisco TrustSec Layer 3 transport configurations.

cts manual

To enter Cisco TrustSec manual mode, use the **cts manual** command in interface configuration mode.

cts manual

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Interface configuration (config-if)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.
Cisco IOS XE Release 3.3.0 SG	This command was implemented on Catalyst 4000 Series switches.
15.0(1)SE	This command was implemented on Catalyst 3750(X) Series switches.

Usage Guidelines

Use the **cts manual** command to enter the TrustSec manual interface configuration in which policies and the Security Association Protocol (SAP) are configured on the link. If the **sap** or **policy** sub-commands are not configured, it is as if the interface is not configured for TrustSec.

When **cts manual** command is configured, 802.1X authentication is not performed on the link. Use the **policy** subcommand to define and apply policies on the link. By default no policy is applied. To configure MACsec link-to-link encryption, the SAP negotiation parameters must be defined. By default SAP is not enabled. The same SAP Pairwise master key (PMK) should be configured on both sides of the link (that is, a shared secret).

Examples

The following example shows how to enter the Cisco TrustSec manual mode:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface giga 2/1
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# ?
CTS manual configuration commands:
  default    Set a command to its defaults
  exit       Exit from CTS manual sub mode
  no         Negate a command or set its defaults
  policy     CTS policy for manual mode
  propagate  CTS SGT Propagation configuration for manual mode
  sap        CTS SAP configuration for manual mode
```

Related Commands

Command	Description
policy (cts manual)	Applies a policy to a manually configured Cisco TrustSec link.
sap (cts manual)	Manually specifies the PMK and the SAP authentication and encryption modes to negotiate MACsec link encryption between two interfaces.
show cts interface	Displays Cisco TrustSec interface configuration statistics.

cts policy layer3

To specify traffic and exception policies for Cisco TrustSec Layer 3 transport on a system when a Cisco Secure ACS is not available, use the **cts policy layer3** global configuration command. To disable the configuration use the **no** form of this command.

cts policy layer3 ipv4 {[**exception** *access_list*] | [**traffic** *access_list*]}

[**no**] **cts policy layer3 ipv6** {[**exception** *access_list*] | [**traffic** *access_list*]}

Syntax Description

ipv4 exception *access_list*	(Optional) Specifies an already defined access control list (ACL) that defines exceptions to the IPv4 Level 3 traffic policy.
ipv4 traffic *access_list*	Specifies an already defined ACL listing the IPv4 Trustsec-enabled subnets and gateways.
ipv6 exception *access_list*	(Optional) Specifies an already defined ACL that defines exceptions to the IPv6 Level 3 traffic policy.
ipv6 traffic *access_list*	Specifies an already defined ACL listing the IPv6 Trustsec-enabled subnets and gateways.

Defaults

No policy is configured.

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on the Catalyst 6500 Series Switches.
Cisco IOS XE Release 3.3.0 SG	This command was implemented on the Catalyst 4000 Series switches.
15.0(1)SE	This command was implemented on the Catalyst 3750(X) Series switches.

Usage Guidelines

The Cisco TrustSec Layer 3 transport permits Layer 2 SGT-tagged traffic from TrustSec-enabled network segments to be transported over non-TrustSec network segments by the application and removal of a Layer 3 encapsulation at specified Cisco TrustSec Layer 3 gateways. A traffic policy is an access list that lists all the TrustSec-enabled subnets and their corresponding gateway addresses. An exception policy is an access list that lists the traffic on which the Cisco TrustSec Layer 3 transport encapsulation must not be applied.

Specify the traffic and exception policies with the **cts policy layer3 {ipv4 | ipv6} traffic** *access_list* and the **cts policy layer3 {ipv4 | ipv6} exception** *access_list* global configuration commands. Apply the traffic and exception policies on the Cisco TrustSec Level 3 gateway interface with the **cts layer3 {ipv4 | ipv6} policy** interface configuration command. Enable the Cisco TrustSec Level 3 gateway interface with the **cts layer3 {ipv4 | ipv6} trustsec forwarding** interface configuration command.

Configure Cisco TrustSec Layer 3 SGT transport with these usage guidelines and restrictions:

- The Cisco TrustSec Layer 3 SGT transport feature can be configured only on ports that support hardware encryption.
- Traffic and exception policies for Cisco TrustSec Layer 3 SGT transport have the following restrictions:
  - The policies must be configured as IP extended or IP-named extended ACLs.
  - The policies must not contain **deny** entries.
  - If the same ACE is present in both the traffic and exception policies, the exception policy takes precedence. No Cisco TrustSec Layer 3 encapsulation will be performed on packets matching that ACE.
- Traffic and exception policies can be downloaded from the authentication server (if supported by your Cisco IOS Release) or manually configured on the device with the **ip access-list global** configuration command. The policies will be applied based on these rules:
  - If a traffic policy or an exception policy is downloaded from the authentication server, it will take precedence over any manually configured traffic or exception policy.
  - If the authentication server is not available but both a traffic policy and an exception policy have been manually configured, the manually configured policies will be used.
  - If the authentication server is not available but a traffic policy has been configured with no exception policy, no exception policy is applied. Cisco TrustSec Layer 3 encapsulation will be applied on the interface based on the traffic policy.
  - If the authentication server is not available and no traffic policy has been manually configured, no Cisco TrustSec Layer 3 encapsulation will be performed on the interface.

Examples

The following example shows how to configure Layer 3 SGT transport to a remote Cisco TrustSec domain:

```
Switch# configure terminal
Switch(config)# ip access-list extended traffic-list
Switch(config-ext-nacl)# permit ip any 10.1.1.0 0.0.0.255
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended exception-list
Switch(config-ext-nacl)# permit ip any 10.2.2.0 0.0.0.255
Switch(config-ext-nacl)# exit
Switch(config)# cts policy layer3 ipv4 traffic traffic-sgt
Switch(config)# cts policy layer3 ipv4 exception exception-list
Switch(config)# interface gi2/1
Switch(config-if)# cts layer3 trustsec ipv4 forwarding
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# exit
```

Related Commands

Command	Description
cts layer3	Enables and applies traffic and exception policies to Cisco TrustSec Layer 3 Transport gateway interfaces.
show cts policy layer3	Displays the traffic and exception policies used in Cisco TrustSec Layer3 Transport.

cts refresh

To refresh the TrustSec peer authorization policy of all or specific Cisco TrustSec peers, or to refresh the SGACL policies downloaded to the switch by the authentication server, use the **cts refresh** command in privileged EXEC mode.

cts refresh {**environment-data | policy** {**peer** [*peer_id*] **| sgt** [*sgt_number* | **default** | **unknown**]}}

Syntax Description

environment-data	Refreshes environment data.
peer *Peer-ID*	(Optional) If a *peer-id* is specified, only policies related to the specified peer connection are refreshed.
sgt *sgt_number*	Performs an immediate refresh of the SGACL policies from the authentication server. If an SGT number is specified, only policies related to that SGT are refreshed.
default	Refreshes the default SGACL policy.
unknown	Refreshes the unknown SGACL policy.

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced as **cts policy refresh** on the Catalyst 6500 series switches.
12.2(50)SY	This command was changed to **cts refresh policy** on the Catalyst 6500 series switches. The **sgt**, **default**, and **unknown** keywords were added.

Usage Guidelines

To refresh the Peer Authorization Policy on all TrustSec peers, enter **cts policy refresh** without specifying a peer ID.

The peer authorization policy is initially downloaded from the Cisco ACS at the end of the EAP-FAST NDAC authentication success. The Cisco ACS is configured to refresh the peer authorization policy, but the **cts policy refresh** command can force immediate refresh of the policy before the Cisco ACS timer expires. This command is relevant only to TrustSec devices that can impose Security Group Tags (SGTs) and enforce Security Group Access Control Lists (SGACLs).

Examples

The following example shows how to refresh the TrustSec peer authorization policy of all peers:

```
Switch# cts policy refresh
Policy refresh in progress
```

The following sample output displays the TrustSec peer authorization policy of all peers:

```
VSS-1# show cts policy peer

CTS Peer Policy
===============
device-id of the peer that this local device is connected to
Peer name: VSS-2T-1
Peer SGT: 1-02
Trusted Peer: TRUE
Peer Policy Lifetime = 120 secs
Peer Last update time = 12:19:09 UTC Wed Nov 18 2009
Policy expires in 0:00:01:51 (dd:hr:mm:sec)
Policy refreshes in 0:00:01:51 (dd:hr:mm:sec)
Cache data applied = NONE
```

Related Commands

Command	Description
clear cts policy	Clears all Cisco TrustSec policies, or by the peer ID or SGT.
show cts policy peer	Displays peer authorization policy for all or specific TrustSec peers.

cts rekey

To regenerate the Pairwise Master Key used by the Security Association Protocol (SAP), use the **cts rekey** privileged EXEC command.

cts rekey interface type *slot*/*port*

Syntax Description

interface type *slot*/*port*	Specifies the Cisco TrustSec interface on which to regenerate the SAP key.

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.
Cisco IOS XE Release 3.3.0 SG	This command was implemented on Catalyst 4500 Series Switches.
15.0(1)SE	This command was implemented on Catalyst 3000 Series Switches.

Usage Guidelines

SAP Pair-wise Master Key key (PMK) refresh ordinarily occurs automatically, triggered by combinations of network events and non-configurable internal timers related to dot1X authentication. The ability to manually refresh encryption keys is often part of network administration security requirements. To manually force a PMK refresh use the **cts rekey** command.

TrustSec supports a manual configuration mode where dot1X authentication is not required to create link-to-link encryption between switches. In this case, the PMK is manually configured on devices on both ends of the link with the **sap pmk** Cisco TrustSec manual interface configuration command.

Cisco TrustSec NDAC/SAP is supported only on K10 switch which has XgStub2. It is supported on both uplink (where K10 acts as supplicant) and down link with linecard that has XgStub2 (where K10 acts as authenticator).

Examples

The following example shows how to regenerate the PMK on a specified interface.

```
switch# cts rekey interface gigabitEthernet 2/1
```

Related Commands

Command	Description
sap (cts manual)	Configures Cisco TrustSec SAP for manual mode.

cts role-based policy trace

To troubleshoot Security Group Tag (SGT) and Security Group access control list (SGACL) behavior in TrustSec network devices, use the **cts role-based policy trace** privileged EXEC command.

cts role-based policy trace {**ipv4** | **ipv6**} {**tcp** | **udp**} **source_host** *ip_address* **eq** {protocol name | *wellknown_port_num*} **dest_host** *ip_address* **eq** {protocol name | *wellknown_port_num*} [**interface** type *slot*/*port* | **security-group** {**sgname** *sg_name* | **sgt** *sgt_num*} | **vlan** *vlan_id* | vrf *vrf_name*]

cts role-based policy trace {**ipv4** | **ipv6**} {*ip_port_num* | **icmp** | **ip**} **source_host** *ip_address* **dest_host** *ip_address* [**interface** type *slot*/*port* | **security-group** {**sgname** *sg_name* | **sgt** *sgt_num*} | **vlan** *vlan_id* | vrf *vrf_name*]

Syntax Description

ipv4 | **ipv6**	Specifies IPv4 or IPv6 IP encapsulation.
ip_port_num | **icmp** | **ip** | **tcp** | **udp**	Specifies the Internet Protocol or its number. Supported protocols and their IP numbers are as follows: • **0** to **255**—Range of possible Internet Protocol numbers. • **icmp**—Internet Control Message Protocol • **ip**—Internet Protocol • **tcp**—Transmission Control Protocol • **udp**—User Datagram Protocol
source_host *ip_address*	Specifies the IP address of the source host.

protocol name | *wellknown_port_num*	Specifies either the host-to-host protocol name or its well-known port number when UDP or TCP is selected as the Internet Protocol. Supported protocols and their associated well-known port numbers are as follows: • **0** to **65535**—Protocol Port number space. • **biff**—Biff (mail notification, comsat, 512) • **bootpc**—Bootstrap Protocol (BOOTP) client (68) • **bootps**—Bootstrap Protocol (BOOTP) server (67) • **discard**—Discard (9) • **dnsix**—DNSIX security protocol auditing (195) • **domain**—Domain Name Service (DNS, 53) • **echo**—Echo (7) • **isakmp**—Internet Security Association and Key Management Protocol (500) • **mobile-ip**—Mobile IP registration (434) • **nameserver**—IEN116 name service (obsolete, 42) • **netbios-dgm**—NetBios datagram service (138) • **netbios-ns**—NetBios name service (137) • **netbios-ss**—NetBios session service (139) • **non500-isakmp**—Internet Security Association and Key Management Protocol (4500) • **ntp**—Network Time Protocol (123) • **pim-auto-rp**—PIM Auto-RP (496) • **rip**—Routing Information Protocol (router, in.routed, 520) • **snmp**—Simple Network Management Protocol (161) • **snmptrap**—SNMP Traps (162) • **sunrpc**—Sun Remote Procedure Call (111) • **syslog**—System Logger (514) • **tacacs**—TAC Access Control System (49) • **talk**—Talk (517) • **tftp**—Trivial File Transfer Protocol (69) • **time**—Time (37) • **who**—Who service (rwho, 513) • **xdmcp**—X Display Manager Control Protocol (177)
eq	Boolean operator (equals). Matches packets with the specified host-to-host protocol or well-known port number from the specified host or interface. Used only for TCP and UDP packets.
dest_host *ip_address*	Specifies the IP address and port of the destination host.
interface type *slot*/*port*	(Optional) Specifies the source interface type, slot, and physical port number.

security-group {**sgname** *sg_name* | **sgt** *sgt_num*}	(Optional) Specifies the Security Group name or the Security Group Tag number.
vlan *vlan_id*	(Optional) 0 to 4094. Specifies the VLAN identifier.
vrf *vrf_name*	(Optional) Specifies the virtual routing and forwarding instance name.

Command Default None

Command Modes Privileged EXEC (#)

SupportedUserRoles Administrator

Command History

Release	Modification
15.1(1)SY1	This feature was introduced on Catalyst 6500 Series Switches.

Usage Guidelines The **cts role-based policy trace** procedure is summarized as follows:

1. Discover the network path.

   Know the topology of the entire TrustSec network before executing the command. Standard network discovery methods such as IP traceroute, Cisco Discovery Protocol, or other methods can be used to obtain this information.

2. Starting from the host and continuing to the farthest node; log-in to each device in the path.
3. Execute the **cts role-based policy trace** command on each device.

   Based on the input arguments, the command output reports the outgoing SGT value and SGACL entry/ACE. Apply the SGT value from the output as the input SGT on the next switch in the path.

   If you do not provide the (optional) SGT argument in the command line, the output reports the SGT assigned to the packet along with any available binding information.

   For example, a packet may be dropped because a device is blocking UDP packets, which may indicate a problem with an SGACL configuration or SGACL refresh obtained from another device, such as the Cisco Integrated Services Engine (Cisco ISE). The **policy trace** command would identify on which device the SGACL was enforced and which ACE was blocking.

Examples The following example shows how to specify a source interface on the source host for an xdmcp over UDP packet.

```
switch# cts role-based policy trace ipv4 udp host 10.2.2.1 eq 177 host 10.1.1.2 eq 80 int
giga 1/1

Input Qualifiers:
====================
 Input Interface          : Gi 1/1
```

```
Packet Parameters:
====================
 Protocol                : UDP
 Source IP Address       : 10.2.2.1
 Source Port             : 177
 Destination IP Address  : 10.1.1.2
 Destination Port        : 80

Result:
==========
 Source SGT mapped to Int Gi 1/1 : 6
 Destination IP: 10.1.1.2  SGT: 5  Source:CLI

 For <SGT, DGT> pair <6, 5> :
  Applicable RBACL : deny_v4_udp-10
    10 deny udp
```

The following example traces an HTTP over UDP packet from an IPv6 host:

```
switch# cts role-based policy trace ipv6 udp host 2001::3 eq 80 host 2003::4 eq 90

Input Qualifiers:
====================

Packet Parameters:
====================
 Protocol                : UDP
 Source IP Address       : 2001::3
 Source Port             : 80
 Destination IP Address  : 2003::4
 Destination Port        : 90

Result:
==========
 Source      IP: 5111::3  SGT: 16  Source:CLI
 Destination IP: 13::4  SGT: 17  Source:CLI

 For <SGT, DGT> pair <16, 17> :
  Applicable RBACL : deny_v6_tcp_udp-10
    deny udp sequence 20
```

Related Commands

Command	Description
show cts role-based counters	Displays Security Group ACL enforcement statistics.

cts role-based

Use the **cts role-based** global configuration command to manually configure SGT impositions, TrustSec NetFlow parameters, and SGACL enforcement. Use the **no** form of the command to remove the configurations.

[**no**] **cts role-based enforcement** [**vlan-list** {*vlan-ids* | **all**}]

[**no**] **cts role-based** {**ip** | **ipv6**} **flow monitor fnf-ubm dropped**

[**no**] **cts role-based ipv6-copy**

[**no**] **cts role-based l2-vrf** *instance_name* **vlan-list** *vlan-ids* [**all**]

[**no**] **cts role-based permissions default** {*access-list* | **ipv4** | **ipv6**} *access-list access-list . . .*

[**no**] **cts role-based permissions from** {*sgt* | **unknown to** {*sgt* | **unknown**}} {*access-list* | **ipv4** | **ipv6**} *access-list . access-list, . . .*

[**no**] **cts role-based sgt-caching vlan-list** {*vlan_ids* | **all**}

[**no**] **cts role-based sgt-caching with-enforcement**

[**no**] **cts role-based sgt-map** {i*pv4_netaddress* | *ipv6_netaddress*} | **sgt** *sgt_number*

[**no**] **cts role-based sgt-map** {i*pv4_netaddress/prefix* | *ipv6_netaddress/prefix*} | **sgt** *sgt_number*

[**no**] **cts role-based sgt-map host** {i*pv4_hostaddress* | *ipv6_hostaddress* | **sgt** *sgt_number*

[**no**] **cts role-based sgt-map vrf** *instance_name* {*ip4_netaddress* | *ipv6_netaddress* | **host** {*ip4_address* | *ip6_address*}}] **sgt** *sgt_number*

[**no**] **cts role-based sgt-map interface** interface_type *slot/port* {**security-group** | **sgt**} *sgt_number*

[**no**] **cts role-based sgt-map vlan-list** [*vlan_ids*| **all**] *slot/port* **sgt** *sgt_number*

[**no**] **cts role-based**

Syntax Description

l2-vrf *instance_name*	(Optional) Specifies Layer 2 virtual routing and forwarding (VRF) instance name.
enforcement	Enables SGACL enforcement on the local device for all Layer 3 Cisco TrustSec interfaces.
interface interface_type	The specified SGT is mapped to traffic from this logical or physical Layer 3 interface.
vlan-list *vlan-ids*	Specifies VLAN IDs. Individual VLAN IDs are separated by commas, a range of IDs specified with a hyphen.
all	(Optional) Specifies all VLAN IDs.
with-enforcement	Enables SGT caching where SGACL enforcement is enabled.

sgt-map *ipv4_netaddress* | *ipv6_netaddress*	(Optional) Specifies the network to be associated with an SGT. Enter IPv4 address in dot decimal notation; IPv6 in colon hexadecimal notation.
sgt-map *ipv4_netaddress/prefix* | *ipv6_netaddress/prefix*	(Optional) Maps the SGT to all hosts of the specified subnet address (IPv4 or IPv6). IPv4 is specified in dot decimal CIDR notation, IPv6 in colon hexadecimal notation. *(0-128)*
sgt-map host *ipv4_hostaddress* | *ipv6_hostaddress*	Binds the specified host IP address with the SGT. Enter the IPv4 address in dot decimal notation; IPv6 in colon hexadecimal notation.
sgt *sgt_number*	Specifies the Security Group Tag (SGT) number. Valid values are from 0 to 65,535.
vrf *instance_name*	Specifies a VRF instance, previously created on the device.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2 (33)SXI3	This command was introduced on Catalyst 6500 series switches.
12.2 (50)SG7	This command was implemented on Catalyst 4000 series switches.
12.2 (53)SE2	This command was implemented on Catalyst 3750(E), 3560(E), and 3750(X) series switches (without **vrf** or IPv6 support).
12.2(50)SY	The following keywords were added for the Catalyst 6500 series switches: • [**no**] **cts role-based enforcement** • [**no**] **cts role-based ip flow monitor user-defined-monitor dropped** • [**no**] **cts role-based ipv6 flow monitor user-defined-monitor dropped** • [**no**] **cts role-based ipv6 copy** • [**no**] **cts role-based permissions**
15.0(0) SY	The following keywords were added for the Catalyst 6500 series switches: • [**no**] **cts role-based sgt-map interface** • [**no**] **cts role-based sgt-map vlan-list**

Usage Guidelines

If you do not have a Cisco Identity Services Engine, Cisco Secure ACS, dynamic Address Resolution Protocol (ARP) inspection, Dynamic Host Control Protocol (DHCP) snooping, or Host Tracking available on your switch to automatically map SGTs to source IP addresses, you can manually map an SGT to the following with the **cts role-based sgt-map** command:

- A single host IPv4 or IPv6 address
- All hosts of an IPv4 or IPv6 network or subnetwork
- VRFs
- Single or multiple VLANs
- A Layer 3 physical or logical interface

Single Host Address-to-SGT Binding

The **cts role-based sgt-map host** command binds the specified SGT with incoming packets when the IP source address is matched by the specified host address. This IP-SGT binding has the lowest priority and is ignored in the presence of any other dynamically discovered bindings from other sources (such as, SXP or locally authenticated hosts). The binding is used locally on the switch for SGT imposition and SGACL enforcement. It is exported to SXP peers if it is the only binding known for the specified host IP address.

Network or Subnetwork Addresses-to-SGT Binding

The **cts role-based sgt-map** command binds the specified SGT with packets that fall within the specified network address.

SXP exports an exhaustive expansion of all possible individual IP–SGT bindings within the specified network or subnetwork. IPv6 bindings and subnet bindings are exported only to SXP listener peers of SXP version 2 or later. The expansion does not include host bindings which are known individually or are configured or learnt from SXP for any nested subnet bindings.

VRF-to-SGT Bindings

The **vrf** keyword specifies a virtual routing and forwarding table previously defined with the **vrf definition** global configuration command. The IP-SGT binding specified with the **cts role-based sgt-map vrf** global configuration command is entered into the IP-SGT table associated with the specified VRF and the IP protocol version which is implied by the type of IP address entered.

VLAN-to-SGT Mapping

The **cts role-based sgt-map vlan-list** command binds an SGT with a specified VLAN or a set of VLANs. The keyword **all** is equivalent to the full range of VLANs supported by the switch and is not preserved in the nonvolatile generation (NVGEN) process. The specified SGT is bound to incoming packets received in any of the specified VLANs.

The system uses discovery methods such as DHCP and/or ARP snooping (a.k.a. IP device tracking) to discover active hosts in any of the VLANs mapped by this command. Alternatively, the system could map the subnet associated with the SVI of each VLAN to the specified SGT. SXP shall export the resulting bindings as appropriate for the type of binding.

The bindings for each mapped VLAN is inserted into the IP-SGT table that is associated with the VRF, the VLAN is mapped to by either its SVI or by the **cts role-based l2-vrf** command.

Layer 3 Interface Mapping (L3IF)

The **cts role-based sgt-map interface** command binds a specified Layer 3 logical interface to a security group name or to an SGT. A security group information table that maps SGTs to security group names is downloaded from the authentication server with the TrustSec environment data. The **cts role-based sgt-map interface security-group** command is rejected if a security group name table is not available.

Whenever a security group table is downloaded for the first time or refreshed, all L3IF mappings are reprocessed. IP–SGT bindings are added, updated, or deleted for all network prefixes that have output paths through the specified interface.

IP-SGT binding configured through the CLI has lower priority than any other binding. The CLI binding is ignored in the presence of any other dynamically discovered binding from other sources such as SXP or locally authenticated hosts.The binding is used locally on the system for SGT imposition and SGACL enforcement and is exported to SXP peers if it is the only binding known for the given host IPv4 or IPv6 address.

IPv6 bindings and subnet bindings are exported by SXP only to SXP peers capable of handling them. SXP listeners which support SXP version 2 are capable of handling IPv6 and subnet bindings. SXP expands the IPv4 subnet bindings to all possible individual host bindings and exports them to SXP peers running version 1 of SXP protocol. The expansion shall not include host bindings which are known individually or are configured or learnt from SXP for any nested subnet bindings.

The keyword **vrf** when entered must be followed by a name of an already defined VRF. The binding specified by this command is entered into the IP-SGT table associated with the specified VRF and the IP protocol version entered.

The following error message is shown when the VRF name entered does not exist:

```
%VPN Routing/Forwarding table <VRF name> does not exist
```

The following error message is shown when the specified VRF name does exists but the IP protocol version implied is not enabled in the VRF:

```
%IPv4/IPv6 protocol is not enabled in VRF <VRF name>
```

Binding Source Priorities

TrustSec resolves conflicts among IP-SGT binding sources in the master binding database with a strict priority scheme. For example, an SGT may also be applied to an interface with the **policy** {**dynamic identity** *peer-name* | **static sgt** *tag*} command (Identity Port Mapping). The current priority enforcement order, from lowest to highest, is as follows:

1. VLAN—Bindings learned from snooped ARP packets on a VLAN that has VLAN-SGT mapping configured.
2. CLI— Address bindings configured using the IP-SGT form of the **cts role-based sgt-map** global configuration command.
3. Layer 3 Interface—(L3IF) Bindings added due to FIB forwarding entries that have paths through one or more interfaces with consistent L3IF-SGT mapping or Identity Port Mapping on routed ports.
4. SXP—Bindings learned from SXP peers.
5. IP_ARP—Bindings learned when tagged ARP packets are received on a Cisco TrustSec-capable link.
6. LOCAL—Bindings of authenticated hosts which are learned via EPM and device tracking. This type of binding also include individual hosts that are learned via ARP snooping on L2 [I]PM configured ports.
7. INTERNAL—Bindings between locally configured IP addresses and the device own SGT.

Layer 2 VRF Assignment

For the [**no**] **cts role-based l2-vrf vrf-name vlan-list** {**vlan-list** | **all**} global configuration command, the **vlan-list** argument can be a single VLAN ID, a list of comma-separated VLAN IDs, or hyphen-separated VLAN ID ranges.

The keyword **all** is equivalent to the full range of VLANs supported by the network device. The keyword **all** is not preserved in the nonvolatile generation (NVGEN) process.

If the **cts role-based l2-vrf** command is issued more than once for the same VRF, each successive command entered adds the VLAN IDs to the specified VRF.

The VRF assignments configured by the **cts role-based l2-vrf** command are active as long as a VLAN remains a Layer 2 VLAN. The IP–SGT bindings learned while a VRF assignment is active are also added to the Forwarding Information Base (FIB) table associated with the VRF and the IP protocol version. If an SVI becomes active for a VLAN, the VRF-to-VLAN assignment becomes inactive and all the bindings learned on the VLAN are moved to the FIB table associated with the VRF of the SVI.

The VRF-to-VLAN assignment is retained even when the assignment becomes inactive. It is reactivated when the SVI is removed or when the SVI IP address is changed. When reactivated, the IP–SGT bindings are moved back from the FIB table associated with the VRF of the SVI to the FIB table associated with the VRF assigned by the **cts role-based l2-vrf** command.

Role-based Enforcement

Use the [**no**] **cts role-based enforcement** command to globally enable or disable SGACL enforcement for Cisco TrustSec-enabled Layer 3 interfaces in the system.

Note The terms Role-based Access Control and Role-based ACLs that appear in the Cisco TrustSec CLI command description is equivalent to Security Group Access Control List (SGACL) in Cisco TrustSec documentation.

VLAN Enforcement

Use the [**no**] **cts role-based enforcement vlan-list** {*vlan-ids* | **all**} command to enable or disable SGACL enforcement for Layer 2 switched packets and for Layer 3 switched packets on an SVI interface.

The *vlan-ids* argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges.

The keyword **all** is equivalent to the full range of VLANs supported by the platform (For example, the Catalyst 6500 VLAN range is from 1 to 4094). SGACLs are enforced on all VLANs of all specified lists. The keyword **all** is not preserved in the nonvolatile generation (NVGEN) process.

Note SGACL enforcement is not enabled by default on VLANs. The **cts role-based enforcement vlan-list** command must be issued to enable SGACL enforcement on VLANs.

Note When a VLAN in which a role-based access control (RBAC) is enforced has an active SVI, the RBAC is enforced for both Layer 2 and Layer3 switched packets within that VLAN. Without an SVI, the RBAC is enforced only for Layer 2 switched packets, because no Layer 3 switching is possible within a VLAN without an SVI.

```
Switch(config)# cts role-based sgt-map 41.15.20.93 sgt 11
Switch(config)# cts role-based sgt-map host 41.15.20.93 sgt 11
Switch(config)# cts role-based l2-vrf l2ipv4 vlan-list 57, 89-101
```

Defining an IPv4 RBACL

A management system (For example, the Cisco Secure ACS) is typically used to define and manage RBACLs globally within the enterprise. However, local definition of RBACLs is used primarily for testing or as a fallback policy in the absence of a dynamic downloaded policy from ACS. The following command defines an RBACL that could be applied to IPv4 traffic and enters role-based access list configuration mode:

```
Switch(config)# ip access-list role-based name
Switch(config-rb-acl)#
```

Defining an IPv4 RBACL ACE

Following commands are used to define ACEs of an IPv4 RBACL.

- `Switch(config-rb-acl)# [sequence-number | no] {permit | deny} protocol [option option-name] {[precedence precedence] [tos tos] | [dscp dscp]} [log] [fragments]`
- `Switch(config-rb-acl)# [sequence-number | no] [permit | deny] icmp [icmp-type [icmp-code] | icmp-message] {[precedence precedence] [tos tos] | [dscp dscp]} [log] [fragments]`
- `Switch(config-rb-acl)# [sequence-number | no] {permit | deny} tcp [src operator {src-port}+] [dst operator {dst-port}+] {[precedence precedence] [tos tos] | [dscp dscp]} [log] [fragments] [established | {{match-any | match-all} {{+ | -}flag-name}+]`
- `Switch(config-rb-acl)# [sequence-number | no] {permit | deny} udp [src operator {src-port}+] [dst operator {dst-port}+] {[precedence precedence] [tos tos] | [dscp dscp]} [log] [fragments]`
- `Switch(config-rb-acl)# [sequence-number | no] {permit | deny} igmp [igmp-type] {[precedence precedence] [tos tos] | [dscp dscp]} [log] [fragments]`

Definin an IPv6 RBACL

The following command defines an RBACL that could be applied to IPv6 traffic and enters IPv6 role-based access list configuration mode:

```
Switch(config)# ipv6 access-list role-based name
Switch(config-ipv6rb-acl)#
```

Defining an IPv6 RBACL ACE

Following commands are used to define ACEs of an IPv6 RBACL.

- Switch(config-ipv6rb-acl)# [no] {permit | deny} protocol [dest-option | dest-option-type {doh-number | doh-type}] [dscp cp-value] [flow-label fl-value] [mobility | mobility-type {mh-number | mh-type}] [routing | routing-type routing-number] [fragments] [log | log-input] [sequence seqno]
- Switch(config-ipv6rb-acl)# [no] [permit | deny] icmp [icmp-type [icmp-code] | icmp-message] [dest-option | dest-option-type {doh-number | doh-type}] [dscp cp-value] [flow-label fl-value] [mobility | mobility-type {mh-number | mh-type}] [routing | routing-type routing-number] [fragments] [log | log-input] [sequence seqno]
- Switch(config-ipv6rb-acl)# [no] {permit | deny} tcp [src operator {src-port}+] [dst operator {dst-port}+] [established | [ack] [rst]] [fin] [psh] [syn] [urg] [dest-option | dest-option-type {doh-number | doh-type}] [dscp cp-value] [flow-label fl-value] [mobility | mobility-type {mh-number | mh-type}] [routing | routing-type routing-number] [fragments] [log | log-input] [sequence seqno]
- Switch(config-ipv6rb-acl)# [no] {permit | deny} udp [src operator {src-port}+] [dst operator {dst-port}+] [dest-option | dest-option-type {doh-number | doh-type}] [dscp cp-value] [flow-label fl-value] [mobility | mobility-type {mh-number | mh-type}] [routing | routing-type routing-number] [fragments] [log | log-input] [sequence seqno]

Attaching SGACL Policies

Use the [**no**] **cts role-based permissions** command to define, replace, or delete the list of RBACLs for a given <SGT, DGT> pair. This policy is in effect as long as there is no dynamic policy for the same DGT or SGT.

Note Static policies can be defined for individual cells in the SGT matrix. Dynamic policies from ACS, however, are defined for the entire row or column. Dynamic and static policies cannot be used together.

Assuming both row and column are downloaded, the static cell <SGT, DGT> will be overridden by the dynamic policy for SGT or DGT even if those policies do not have an explicit cell for <SGT, DGT>.

The statically configured policy defined by this command is restored after connectivity with ACS is lost and not regained before a covering policy from ACS is expired. This command is intended as a fallback policy or during testing or experimenting with RBACL enforcement.

- The **from** clause specifies the source SGT and the **to** clause specifies the destination SGT. Both a **from** clause and a **to** clause must be specified. Either clause can specify numeric value for SGT in the range from 0 to 65533 or one of the keywords **unknown**, or **multicast-unknown**.
- **unknown**—Selects RBACLs that are applied for unicast packets whose source SGT or destination SGT cannot be determined by the system.
- **multicast-unknown**—Selects RBACLs of a multicast send or multicast receive policy when the SGT of the multicast stream cannot be determined.
- **rbacl name**—Name of an RBACL already defined. The RBACL could be an RBACL that was defined by CLI (using ip access-list role-based name) or an RBACL that was defined by policy downloaded from ACS.
- **ipv4** (optional) keyword indicates that RBACLs attached by this command are IPv4 RBACLs. This is the default and if neither IPv4 nor IPv6 are specified, the command will expect each of the given <rbacl name> to be an IPv4 RBACL.
- **ipv6** keyword indicates that the RBACLs attached by this command are IPv6 RBACLs. It is mandatory to specify the keyword **ipv6** when attaching IPv6 RBACLs. The command will not make an attempt to figure out on its own the IP protocol version from the attached RBACLs.

The **cts role-based permissions default** [**ipv4 | ipv6**] <*rbacl name*>+ command defines, replaces, or deletes the list of RBACLs of the unicast default policy. This policy remains in effect as long as no dynamic unicast default policy is downloaded from ACS.

The **cts role-based permissions multicast-send-default** <*rbacl name*>+ command defines, replaces, or deletes the list of RBACLs of the multicast send default policy. This policy remains in effect as long as no dynamic multicast send default policyis downloaded from ACS.

The **cts role-based permissions multicast-receive-default** <*rbacl name*> command defines, replaces, or deletes the single RBACL of the multicast receive default policy. This policy remains in effect as long as no dynamic multicast receive default policy has been downloaded from ACS.

Flexible Net Flow

Flexible NetFlow can account for packets dropped by SGACL enforcement when SGT and DGT flow objects are configured in the flow record with the standard 5-tuple flow objects.

Use the **flow record** and **flow exporter** global configuration commands to configure a flow record, and a flow exporter, then use the **flow monitor** command add them to a flow monitor.

To collect only SGACL dropped packets, use the [**no**] **cts role-based** {**ip | ipv6**} **flow monitor dropped** global configuration command.

For Flexible NetFlow overview and configuration information, see the following documents:

Getting Started with Configuring Cisco IOS Flexible NetFlow

http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/get_start_cfg_fnflow.html

Cisco IOS Flexible NetFlow Configuration Guide, Release 15.0SY

http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/15-0sy/fnf-15-0sy-book.html

Examples

In the following example, a Catalyst 4500 series switch binds host IP address 10.1.2.1 to SGT 3 and 10.1.2.2 to SGT 4. These bindings are forwarded by SXP to an SGACL enforcement switch.

```
Switch# (config)# cts role-based sgt-map host 10.1.2.1 sgt 3
Switch(config)# cts role-based sgt-map host 10.1.2.2 sgt 4

Switch# show cts role-based sgt-map all

Active IP-SGT Bindings Information

IP Address    SGT  Source
============================================
10.1.2.1       3   CLI
10.1.2.2       4   CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 2
Total number of active   bindings = 2
```

In the following example, VLAN 57, and 89 through 101 is added to VRF l2ipv4. The VRF was created with the **vrf** global configuration command.

```
Switch(config)# cts role-based l2-vrf l2ipv4 vlan-list 57, 89-101
```

Related Commands

Command	Description
cts sxp	Configures SXP on a network device.
cts sgt	Configures local device security group tag.
show cts role-based flow	Displays role-based access control information

cts server

To configure RADIUS server group load balancing, use the **cts server** command in global configuration mode. Use the **no** form of the command to disable load balancing.

[**no**] **cts server deadtime** *timer_secs*

[**no**] **cts server key-wrap enable**

[**no**] **cts server load-balance method least-outstanding** [**batch-size** *transactions*] [**ignore-preferred-server**]

Syntax Description

deadtime *timer_secs*	Specifies how long a server in the group should not be selected for service once it has been marked as dead. The default is 20 seconds; the range is from 1 to 864000.
load-balance method least-outstanding	Enables RADIUS load balancing for the Cisco TrustSec private server group and chooses the server with the least outstanding transactions. By default, no load balancing is applied.
batch-size *transactions*	(Optional) The number of transactions to be assigned per batch. The default is 25. **Note** Batch size may impact throughput and CPU load. It is recommended that the default batch size, 25, be used because it is optimal for high throughput, without adversely impacting CPU load.
ignore-preferred-server	(Optional) Instructs the switch not to use the same server throughout a session.
key-wrap enable	Enables AES Key Wrap encryption for Trustsec RADIUS server communications.

Defaults

Deadtime	20 seconds
Batch-size	25 transactions

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.
12.2(50)SY	The **key-wrap** keyword was added on Catalyst 6500 series switches.

Usage Guidelines

Use the **key-wrap** keyword when operating the switch in FIPS mode.

Examples

The following example shows how to configure server settings and how to display the Cisco TrustSec server list:

```
Switch# configure terminal
Switch(config)# cts server load-balance method least-outstanding batch-size 50
ignore-preferred-server
Switch(config)# exit

Switch# show cts server-list

CTS Server Radius Load Balance = ENABLED
  Method     = least-outstanding
  Batch size = 50
  Ignore preferred server
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Preferred list, 1 server(s):
 *Server: 10.15.20.102, port 1812, A-ID  87B3503255C4384485BB808DC24C6F55
               Status = ALIVE
               auto-test = TRUE, idle-time = 120 mins, deadtime = 20 secs
Installed list: SL1-1E6E6AE57D4E2A9B320D1844C68BA291, 3 server(s):
 *Server: 10.15.20.102, port 1812, A-ID  87B3503255C4384485BB808DC24C6F55
               Status = ALIVE
               auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.15.20.101, port 1812, A-ID 255C438487B3503485BBC6F55808DC24
               Status = ALIVE
               auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
Installed list: SL2-1E6E6AE57D4E2A9B320D1844C68BA293, 3 server(s):
 *Server: 10.0.0.1, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
               Status = ALIVE
               auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.0.0.2, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
               Status = DEAD
               auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
```

Related Commands

Command	Description
show cts server-list	Displays lists of AAA servers and load-balancing configurations.

cts server test

To configure an automated test for liveness check on a RADIUS server, use the **cts server test** command in global configuration mode. Use the **no** form of the command to disable the liveness check.

cts server test {*ipv4_address* | **all**} {**deadtime** *seconds* | **enable** | **idle-time** *minutes*}

no cts server test {*ipv4_address* | **all**} {**deadtime** | **enable** | **idle-time**}

Syntax Description

ipv4_address	Configures the server-liveness test for a specified IP address.
all	Configures the server-liveness test for all servers on the dynamic server list.
deadtime *seconds*	Specifies how long a server in the group should not be selected for service once it has been marked as dead. The default is 20 seconds; the range is from 1 to 864000.
enable	Enables the server-liveness automated test.
idle-time *minutes*	Configures how often to send an automated test message. The default is 60 seconds; the range is from 1 to 14400 seconds.

Defaults

Test is enabled for all servers.

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.
Cisco IOS XE Denali 16.1.1	This command was implemented on Catalyst 3650 and 3850 Series Switches.

Usage Guidelines

Because the server-liveness is enabled by default, you may receive failed authentication messages from the user CTS-Test-Server. The server-liveness probes a specified RADIUS server or all servers in the dynamic server list, and when a RADIUS server does not respond, the switch will mark it as down and sends the failed authentication message. You can disable these messages by using the **no cts server test** command.

To configure a password for the CTS-Test-Server user, configure the **username** command in global configuration mode.

Examples

The following example shows how to configure server settings and how to display the Cisco TrustSec server list:

```
Switch# configure terminal
Switch(config)# cts server load-balance method least-outstanding batch-size 50
ignore-preferred-server
Switch(config)# cts server test all deadtime 20
Switch(config)# cts server test all enable
Switch(config)# cts server test 10.15.20.102 idle-time 120
Switch(config)# exit

Switch# show cts server-list

CTS Server Radius Load Balance = ENABLED
  Method     = least-outstanding
  Batch size = 50
  Ignore preferred server
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Preferred list, 1 server(s):
 *Server: 10.15.20.102, port 1812, A-ID  87B3503255C4384485BB808DC24C6F55
                Status = ALIVE
                auto-test = TRUE, idle-time = 120 mins, deadtime = 20 secs
Installed list: SL1-1E6E6AE57D4E2A9B320D1844C68BA291, 3 server(s):
 *Server: 10.15.20.102, port 1812, A-ID  87B3503255C4384485BB808DC24C6F55
                Status = ALIVE
                auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.15.20.101, port 1812, A-ID 255C438487B3503485BBC6F55808DC24
                Status = ALIVE
                auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
Installed list: SL2-1E6E6AE57D4E2A9B320D1844C68BA293, 3 server(s):
 *Server: 10.0.0.1, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
                Status = ALIVE
                auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.0.0.2, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
                Status = DEAD
                auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
```

The following example shows how to configure a password for the CTS-Test-Server user:

```
Switch(config)# username CTS-Test-Server password 0 Password123
```

Related Commands

Command	Description
show cts server-list	Displays lists of AAA servers and load-balancing configurations.
username	Configures an username for authentication.

cts sgt

To manually assign a Security Group Tag (SGT) number to a network device, use the **cts sgt** command in global configuration mode. Use the **no** form of the command to remove the tag.

[**no**] **cts sgt** *tag-number*

Syntax Description

tag-number	Configures the SGT for packets sent from this device. The *tag* argument is in decimal format. The range is from 1 to 65533.

Defaults

No SGT number is assigned.

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2 (33)SXI3	This command was introduced on Catalyst 6500 Series Switches.
12.2 (50)SG7	This command was implemented on Catalyst 4000 Series Switches.
12.2 (53)SE2	This command was implemented on Catalyst 3750(E) and 3560(E) Series Switches.
12.2 (53)SE2	This command was implemented on Catalyst 3750(X) Series Switches.

Usage Guidelines

In Cisco TrustSec, the authentication server assigns an SGT to the device for packets originating from the device. You can manually configure an SGT to be used if the authentication server is not accessible, but an authentication server-assigned SGT will take precedence over a manually assigned SGT.

Examples

The following example shows how to manually configure an SGT on the network device:

```
Switch# configure terminal
Switch(config)# cts sgt 1234
Switch(config)# exit
```

Related Commands

Command	Description
show cts environment-data	Displays the Cisco TrustSec environment data.

cts sxp

To configure SXP on a network device, use the **cts sxp** global configuration command. Use the **no** form of this command to disable SXP configurations.

[**no**] **cts sxp connection peer** *ip4_address* **password** {**default | none**} **mode** {**local | peer**} [**speaker | listener**] [**vrf** *vrf_name*]

[**no**] **cts sxp connection peer** *ip4_address* **source** *ip4_address* **password** {**default | none**} **mode** {**local | peer**} [**speaker | listener**] [**vrf** *vrf_name*]

[**no**] **cts sxp default password** {**0** *unencrypted_pwd* **| 6** *encrypted_key* **| 7** *encrypted_key* **|** *cleartext_pwd*}

[**no**] **cts sxp default source-ip** *ip4_address*

[**no**] **cts sxp enable**

[**no**] **cts sxp log binding-changes**

[**no**] **cts sxp mapping network-map** *bindings*

[**no**] **cts sxp reconciliation period** *seconds*

[**no**] **cts sxp retry period** *seconds*

Syntax Description

connection peer *ip4_address*	Specifies the peer SXP address.
password {default | none}	Specifies the password that SXP uses for peer connection using the following options: • **default**—Use the default SXP password configured using the **cts sxp default password** command. • **none**—Do not use a password. Maximum password length is 32 characters.
mode {local | peer}	Specifies the role of the remote peer device: • **local**—The specified mode refers to the local device. • **peer**—The specified mode refers to the peer device.
network-map *bindings*	Specifies the maximum number of subnet host address-to-SGT bindings permitted when expanding subnets for IP–SGT tagging and export. Enter 0 for no expansion. Valid values are from 0 to 65535.
speaker | listener	**speaker**—Default. Specifies that the device is the speaker in the connection. **listener**—Specifies that the device is the listener in the connection.
vrf *vrf_name*	(Optional) Specifies the VRF to the peer. Default is the default VRF.

default password **0** *unencrypted_pwd* | **6** *encrypted_key* | **7** *encrypted_key* | *cleartext_pwd*	Configures the SXP default password. You can enter either a clear text password (using the **0** or no option) or an encrypted password (using the **6** or **7** option). The maximum password length is 32 characters.
source-ip *ip4_address*	(Optional) Specifies the IPv4 address of the source device. If no address is specified, the connection uses the default source address (if configured), or the address of the port.
enable	Enables SGT Exchange Protocol over TCP (SXP) for Cisco TrustSec.
log binding-changes	Enables logging for IP-to-SGT binding changes. Default is off.
reconciliation period *seconds*	Changes the SXP reconciliation timer. The range is from 0 to 64000. Default is 120 seconds (2 minutes).
retry period *seconds*	Changes the SXP retry timer. The range is from 0 to 64000. Default is 120 seconds (2 minutes).

Defaults

sxp	Disabled by default
log binging-changes	off
password	none
reconciliation period	120 seconds
retry period	60 seconds
source-ip	Default source IP address (if configured) or the port address
vrf	Default VRF name

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI3	This command was introduced on Catalyst 6500 series switches.
12.2(50)SG7	This command was implemented on Catalyst 4000 series switches.
12.2(53)SE2	This command was implemented on Catalyst 3750(E) and 3560(E) series switches (without **log binding-changes** keyword).

Release	Modification
12.2(53)SE2	This command was implemented on Catalyst 3750(X) series switches without **log binding-changes** keyword).
12.2(50)SY	The **mapping** keyword was added.

Usage Guidelines

This command enables SXP, determines the SXP password, the peer speaker/listener relationship, and the reconciliation period.

When an SXP connection to a peer is configured with the **cts sxp connection peer** command, only the connection mode can be changed. The **vrf** keyword is optional. If a VRF name is not provided or a VRF name is provided with name "default," the connection is set up in the default routing or forwarding domain.

The default setting for an SXP connection password is **none**. Because SXP connection is configured per IP address, a device with many peers can have many SXP connections. The **cts sxp default password** command sets the default SXP password to be optionally used for all SXP connections configured on the device. The SXP password can be cleartext or encrypted. The default is type 0 (cleartext). If the encryption type is 6 or 7, the encryption password argument must be a valid type 6 or type 7 ciphertext. Use the **no cts sxp default password** command to delete the SXP password.

The **cts sxp default source-ip** command sets the default source IP address that SXP uses for all new TCP connections when a source IP address is not specified. Pre-existing TCP connections are not affected when this command is entered. If neither the default nor the peer-specific source IP address is configured, then the source-IP address will be derived from existing local IP addresses and could potentially be different for each TCP connection initiated from the device.

SXP connections are governed by three timers:

- Retry timer
- Delete Hold Down timer
- Reconciliation timer

Retry Timer

The Retry timer is triggered if at least one SXP connection that is not up. A new SXP connection is attempted when this timer expires. Use the **cts sxp retry period** command to configure this timer value. The default value is 120 seconds. The range is from 0 to 64000 seconds. A zero value results in no retry being attempted.

Delete Hold Down Timer

The Delete Hold Down timer value is not configurable and is set to 120 seconds. This timer is triggered when an SXP listener connection goes down. The IP-SGT mappings learned from the down connection are deleted when this timer expires. If the down connection is restored before the Delete Hold Down timer expires, the Reconciliation timer is triggered.

Reconciliation Timer

After a peer terminates an SXP connection, an internal Delete Hold-down timer starts. If the peer reconnects before the Delete Hold Down timer expires, the SXP Reconciliation timer starts. While the SXP Reconciliation period timer is active, the Cisco TrustSec software retains the SGT mapping entries learned from the previous connection and removes invalid entries. The default value is 120 seconds (2 minutes). Setting the SXP reconciliation period to 0 seconds disables the timer and causes all entries from the previous connection to be removed. Use the **cts sxp reconciliation period** command to configure this timer.

Examples

The following example shows how to enable SXP, and configure the SXP peer connection on SwitchA, a speaker, for connection to SwitchB, a listener:

```
SwitchA# configure terminal
SwitchA#(config)# cts sxp enable
SwitchA#(config)# cts sxp default password Cisco123
SwitchA#(config)# cts sxp default source-ip 10.10.1.1
SwitchA#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

The following example shows how to configure the SXP peer connection on SwitchB, a listener, for connection to SwitchA, a speaker:

```
SwitchB# configure terminal
SwitchB(config)# cts sxp enable
SwitchB(config)# cts sxp default password Cisco123
SwitchB(config)# cts sxp default source-ip 10.20.2.2
SwitchB(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

Related Commands

Command	Description
show cts sxp	Displays status of all SXP configurations.

clear cts cache

To clear TrustSec cache, use the **clear cts counter** command in privileged EXEC mode.

clear cts cache authorization-policies [**peer** | **sgt**]

clear cts cache environment-data

clear cts cache filename *file*

clear cts cache interface-controller [**type** *slot*/*port*]

Syntax Description

authorization-policies [peer | sgt]	Clears all cached SGT and peer authorization policies.
environment-data	Clears environment data cache file.
filename *file*	Specifies filename of cache file to clear.
interface-controller type *slot*/*port*	Specifies the interface controller cache to clear.

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.
12.2(50)SY	The **interface-controller** keyword was added on Catalyst 6500 series switches.

Examples

The following example deletes environment data from the cache:

```
Switch# clear cts cache environment-data
```

Note Clearing peer authorization and SGT policies are relevant only to TrustSec devices capable of enforcing SGACLs.

Related Commands

Command	Description
cts cache	Enables caching of TrustSec authorization and environment data information to DRAM and NVRAM.

clear cts counter

To clear Cisco TrustSec statistics on a specified interface, use the **clear cts counter** command in privileged EXEC mode.

clear cts counter [**type** *slot*/*port*]

Syntax Description

type *slot*/*port*	(Optional) Specifies the interface type, slot, and port of the interface to clear.

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.

Usage Guidelines

The **clear cts counter** command clears the Cisco TrustSec counters specific to the selected interface. If no interface is specified, all of the TrustSec counters on all TrustSec interfaces are cleared.

Examples

The following example shows how to clear Cisco TrustSec statistics for GigabitEthernet interface 3/1, and then verify with the **show cts interface** command (a fragment of the **show** command output is displayed):

```
Switch# clear cts counter gigabitEthernet3/1
Switch# show cts interface  gigabitEthernet3/1

Global Dot1x feature is Disabled
Interface GigabitEthernet3/1:
<snip>

    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        authz success:              0
        authz fail:                 0
        port auth fail:             0
<snip>
```

Related Commands

Command	Description
show cts interface	Displays Cisco TrustSec interface status and configurations.

clear cts credentials

To delete the Cisco Trustsec device ID and password, use the **clear cts credentials** command in privileged EXEC mode.

clear cts credentials

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Catalyst 6500 series switches.

Examples

```
Switch# clear cts credentials
Switch# show cts environment-data

CTS Environment Data
====================
Current state = START
Last status = Cleared
Environment data is empty
State Machine is running
Retry_timer (60 secs) is running
```

Related Commands

Command	Description
cts credentials	Specifies the TrustSec ID and password.

clear cts environment-data

To delete the TrustSec environment data from cache, use the **clear cts environment-data** command in privileged EXEC mode.

clear cts environment-data

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.

Examples

The following example shows how to clear environment data from cache:

```
Switch# clear cts environment-data
```

Related Commands

Command	Description
show cts environment-data	Displays the Cisco TrustSec environment data.

clear cts macsec

To clear the MACsec counters for a specified interface, use the **clear cts macsec counters** command in privileged EXEC mode.

clear cts macsec counters interface type *slot*/*port*

Syntax Description

interface type *slot*/*port*	Specifies the interface.

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.

Examples

The following example shows how to clear the counters on a GigabitEthernet interface on a Catalyst 6500 series switch:

```
Switch# clear cts macsec counters interface gigabitEthernet 6/2
```

Related Commands

Command	Description
show cts macsec	Displays MACSEC counters information.
show cts interface	Displays TrustSec interface configuration statistics.

clear cts pac

To clear Cisco TrustSec Protected Access Credential (PAC) information from the keystore, use the **clear cts pac** command in privileged EXEC mode.

clear cts pac {**A-ID** *hexstring* | **all**}

Syntax Description

A-ID *hexstring*	Specifies the authenticator ID (A-ID) of the PAC to be removed from the keystore.
all	Specifies that all PACs on the device be deleted.

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.

Examples

The following command clears all PACs in the keystore:

```
Switch# clear cts pac all
```

Related Commands

Command	Description
show cts pacs	Displays the A-ID and PAC-info for PACs in the keystore.
show cts keystore	Displays the contents of the keystore.

clear cts policy

To delete the peer authorization policy of a Cisco TrustSec peer, use the **clear cts policy** command in privileged EXEC mode.

clear cts policy {**peer** [*peer_id*] | **sgt** [*sgt*]}

Syntax Description

peer *peer_id*	Specifies the peer ID of the TrustSec peer device.
sgt *sgt*	Specifies the Security Group Tag (SGT) of the TrustSec peer device in hexadecimal.

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33) SXI	This command was introduced on Catalyst 6500 series switches.

Usage Guidelines

To clear the peer authorization policy of all TrustSec peers, use the **clear cts policy peer** command without specifying a peer ID. To clear the Security Group tag of the TrustSec peer, use the **clear cts policy sgt** command.

Examples

The following example shows how to clear the peer authorization policy of the TrustSec peer with the peer ID peer1:

```
Switch# clear cts policy peer peer1
Delete all peer policies? [confirm] y
```

Related Commands

Command	Description
cts refresh	Forces refresh of peer authorization policies.
show cts policy peer	Displays the peer authorization policies of TrustSec peers.

clear cts role-based counters

To reset Security Group ACL statistic counters, use the **clear cts role-based counters** command in user EXEC or privileged EXEC mode.

clear cts role-based counters default [**ipv4** | **ipv6**]

clear cts role-based counters from {*sgt_num* | **unknown**} [**ipv4** | **ipv6** | **to** {*sgt_num* | **unknown**} [**ipv4** | **ipv6**]]

clear cts role-based counters to {*sgt_num* | **unknown**} [**ipv4** | **ipv6**]

clear cts role-based counters [**ipv4** | **ipv6**]

Syntax Description

default	Specifies default policy counters.
from	Specifies the source security group.
ipv4	Specifies security groups on IPv4 networks.
ipv6	Specifies security groups on IPv6 networks.
to	Specifies the destination security group.
sgt_num	Specifies the Security Group Tag number. Valid values are from 0 to 65533.
unknown	Specifies all source groups.

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.

Usage Guidelines

Use the **clear cts role-based counters** command to clear the Security Group ACL (SGACL) enforcement counters.

Specify the source SGT with the **from** keyword and the destination SGT with the **to** keyword. The counters for the entire permission matrix are cleared when both the **from** and **to** keywords are omitted.

The **default** keyword clears the statistics of the default unicast policy.

Examples

The following example shows how to clear all role-based counters:

```
Switch# clear cts role-based counters ipv4
```

```
Switch# show cts role-based counters

Role-based counters
From    To      SW-Denied       HW-Denied       SW-Permitted    HW_Permitted
2       5       129                89762              421      7564328
3       5        37               123456             1325     12345678
3       7         0                65432              325      2345678
```

Related Commands

Command	Description
cts role-based	Manually maps a source IP address to a Security Group Tag (SGT) on either a host or a VRF as well as enabling SGACL enforcement.
show cts role-based counters	Displays statistics of SGACL enforcement events.

clear cts server

To remove a server configuration from the Cisco TrustSec authentication, authorization, and accounting (AAA) server list, use the **clear cts server** command.

clear cts server *ip-address*

Syntax Description

ip-address	IPv4 address of the AAA server to be removed from the server list.

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 Series Switches.

Usage Guidelines

This command removes a server configuration from the list of Cisco Trustsec AAA servers configured using the **cts authorization list** command, or the AAA server list provisioned by the Cisco TrustSec authenticator peer.

Examples

The following example removes the AAA server 10.10.10.1 from the Cisco TrustSec AAA server list.

```
Switch# clear cts server 10.10.10.1
```

Related Commands

Command	Description
cts server	Configures RADIUS server-group load balancing.
show cts server-list	Displays the list of RADIUS servers available to TrustSec seed and nonseed devices.

default (cts dot1x)

To restore all Cisco TrustSec dot1x configurations to their default value, use the **default** command in CTS dot1x interface configuration mode.

default propagate sgt

default sap

default timer reauthentication

Syntax Description

propagate sgt	Restores the default propagate SGT.
sap	Restores the default; **sap modelist gcm-encrypt null**.
timer	Restores the default 86,400 seconds for the dot1x reauthentication period.

Defaults

None

Command Modes

CTS dot1x interface configuration mode (config-if-cts-dot1x)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.

Examples

The following example re-enables SGT propagation:

```
Switch# configure terminal
Switch(config)# interface gigabit 6/1
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# default propagate sgt
```

Related Commands

Command	Description
propagate sgt (cts dot1x)	Enables/disables SGT propagation in dot1x mode.
sap (cts dot1x)	Configures Cisco TrustSec SAP for dot1x mode.
timer (cts do1x)	Configures the Cisco TrustSec timer.

debug condition cts

To set match criteria (conditions) to filter TrustSec debug messages on a Peer ID, Security Group Tag (SGT), or Security Group Name (SGN), use the **debug condition cts** command. Use the **no** form of the command to remove debug condtions.

[**no**] **debug condition cts** {**peer-id** *peer-id* | **security-group** {**name** *sg_name* | **tag** *tag_number*}}

Syntax Description

peer-id *peer-id*	Specifies the Peer ID to match.
security-group *sg_name*	Specifies the Security Group Name (SGN) to match.
tag *tag_number*	Specifies the Security Group Tag (SGT) to match.

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modifications
15.1(1)SY1	This command was introduced on Catalyst 6500 series switches.

Usage Guidelines

When any of the **debug cts** commands are enbled, debugging messages for the specified Cisco TrustSec service is logged. The **debug condition cts** command filters these debugging messages by setting match conditions for Peer ID, SGT or Security Group Name.

For SXP messages, debug conditions can be set for source and destination IP addresses. To filter by VRF, or IP-to-SGT bindings, use the conditional debug commands—**debug condition ip**, and **debug condition vrf**.

The debug conditions are not saved in the running-configuration file.

Examples

In following example, messages for **debug cts ifc events** and **debug cts authentication details** are filtered by peer-id, SGT, and SGN. Interface Controller (ifc) and Authentication debug messages are displayed only if the messages contain the peer-id="Zoombox" or security-group tag = 7 or security-group name="engineering":

```
switch# debug condition cts peer-id Zoombox
Condition 1 set
switch# show debug condition
     Condition 1: cts peer-id Zoombox (0 flags triggered)

switch# debug condition cts security-group tag 7
Condition 2 set

switch# debug condition cts security-group name engineering
    Condition 3 set

switch# show debug condition
```

```
    Condition 1: cts peer-id Zoombox (0 flags triggered)
    Condition 2: cts security-group tag 7 (0 flags triggered)
    Condition 3: cts security-group name engineering (0 flags triggered)
switch# debug cts ifc events
switch# debug cts authentication details
```

In the following example, SXP connection and mapping database messages are filtered by IP address and SGT. Only SXP debug messages that contain IP address 10.10.10.1, or security-group tag = 8, or security-group name = “engineering” are displayed.

```
switch# debug condition ip 10.10.10.1
    Condition 1 set
switch# debug condition cts security-group tag 8
    Condition 2 set
switch# debug condition cts security-group name engineering
    Condition 3 set

switch# show debug condition

    Condition 1: ip 10.10.10.1 (0 flags triggered)
    Condition 2: cts security-group tag 8 (0 flags triggered)
    Condition 3: cts security-group name engineering (0 flags triggered)

switch# debug cts sxp conn
switch# debug cts sxp mdb
```

Related Commands

Command	Description
show debug condition	Displays all conditions set for debug commands.

default (cts manual)

To restore all Cisco TrustSec manual configurations to their default values, use the **default** command in CTS manual interface configuration mode.

default policy dynamic identity

default policy static sgt

default propagate sgt

default sap

Syntax Description

dynamic identity	Defaults to the peer policy downloaded from the AAA server.
policy static sgt	Defaults to no policy. That is, no SGT is applied to the ingress traffic.
policy propagate sgt	Changes SGT propagation mode to ON.
sap	Specifies default SAP values. (GCM-Encrypt, null)

Command Modes

CTS manual interface configuration mode (config-if-cts-manual)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.

Usage Guidelines

To restore the Cisco TrustSec manual interface configuration mode parameters to default values, use the **default** command.

Examples

The following example shows how to restore the default dynamic policy and SGT propagation policies of a Cisco TrustSec-enabled interface:

```
Switch# config t
Switch(config)# interface gigbitEthernet 6/1
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# default policy dynamic identity
Switch(config-if-cts-manual)# default propagate sgt
```

Related Commands

Command	Description
policy (cts manual)	Configures Cisco TrustSec policy for manual mode.
propagate sgt (cts manual)	Configures Cisco TrustSec SGT Propagation configuration for manual mode.
sap (cts manual)	Configures Cisco TrustSec SAP for manual mode.

match flow cts

To add Cisco TrustSec flow objects to a Flexible NetFlow flow record, use the **match flow cts** command in global configuration mode. To disable the configuration, use the **no** form of this command.

[**no**] **match flow cts destination group-tag**

[**no**] **match flow cts source group-tag**

Syntax Description

destination group-tag	Matches destination fields for the Cisco TrustSec Security Group Tag (SGT).
source group-tag	Matches source fields for the Cisco TrustSec Security Group Tag (SGT).

Defaults

None

Command Modes

Flexible NetFlow record configuration (config-flow-record)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.

Usage Guidelines

Flexible NetFlow accounts for packets dropped by SGACL enforcement when SGT and DGT flow objects are configured in the flow record with standard 5-tuple flow objects.

Use the **flow record** and **flow exporter** global configuration commands to configure a flow record, and a flow exporter, then use the **flow monitor** command to add them to a flow monitor.

To collect only SGACL dropped packets, use the [**no**] **cts role-based** {**ip** | **ipv6**} **flow monitor dropped** global configuration command.

Examples

The following example configures an IPV4 Flow Record (5-tuple, direction, SGT, DGT):

```
Switch(config)# flow record cts-record-ipv4
Switch(config-flow-record)# match ipv4 protocol
Switch(config-flow-record)# match ipv4 source address
Switch(config-flow-record)# match ipv4 destination address
Switch(config-flow-record)# match transport source-port
Switch(config-flow-record)# match transport destination-port
Switch(config-flow-record)# match flow direction
Switch(config-flow-record)# match flow cts source group-tag
Switch(config-flow-record)# match flow cts destination group-tag
Switch(config-flow-record)# collect counter packets
```

Related Commands

Command	Description
show flow monitor	Displays the status and statistics for a Flexible NetFlow flow monitor.
cts role-based	For Flexible NetFlow, this command has the option to attach the flow monitor to all Layer 3 interfaces to collect statistics of traffic dropped by SGACLs.

platform cts

To enable the TrustSec egress or ingress reflector, use the **platform cts** command in global configuration mode. Use the **no** form of the command to disable the reflector.

[**no**] **platform cts** {**egress** | **ingress**}

Syntax Description

egress	Specifies the egress TrustSec reflector to be enabled or disabled.
ingress	Specifies the ingress TrustSec reflector to be enabled or disabled.

Defaults

Ingress or egress reflectors are not configured.

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.

Examples

The following example shows how to enable the Cisco TrustSec ingress reflector on a Catalyst 6500 switch:

```
switch(config)# platform cts egress
```

The following example shows how to disable the Cisco TrustSec ingress reflector on a Catalyst 6500 switch:

```
switch(config)# no platform cts egress
```

Related Commands

Command	Description
show platform cts reflector	Displays the status of the Cisco TrustSec reflector mode.

policy (cts manual)

To apply a policy to a manually configured Cisco TrustSec link, use the **policy** command in CTS interface manual mode. Use the **no** form of the command to remove a policy.

[**no**] **policy dynamic identity** *peer_deviceID*

[**no**] **policy static sgt** *sgt_number* [**trusted**]

Syntax Description

dynamic	Obtains policy from the authorization server.
identity *peer_deviceID*	Specifies the peer device name or symbolic name in the authentication server policy database associated with the policy to be applied to the peer.
static	Specifies an Security Group Tag (SGT) policy to incoming traffic on the link.
sgt *sgt_number*	SGT number to apply to incoming traffic from peer.
trusted	Indicates that the SGT of the ingress traffic on the interface with the SGT specified in the command should not be overwritten. Untrusted is the default.

Defaults

Policy is not configured.

Command Modes

CTS interface manual mode (config-if-cts-manual)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.
Cisco IOS XE Release 3.3.0 SG	This feature was implemented on Catalyst 4000 Series Switches.
15.0(1)SE	This feature was implemented on Catalyst 3750(X) Series Switches.

Usage Guidelines

Use the **policy** command to apply a policy when manually configuring a TrustSec link. The default is **no policy** which passes all traffic without applying an SGT. The **sap** cts manual mode command must also be configured to bring up a TrustSec link.

If the selected SAP mode allows SGT insertion and an incoming packet carries no SGT, the tagging policy is as follows:

- If the **policy static** command is configured, the packet is tagged with the SGT configured in the **policy static** command.
- If the **policy dynamic** command is configured, the packet is not tagged.

If the selected SAP mode allows SGT insertion and an incoming packet carries an SGT, the tagging policy is as follows:

- If the **policy static** command is configured without the **trusted** keyword, the SGT is replaced with the SGT configured in the **policy static** command.
- If the **policy static** command is configured with the **trusted** keyword, no change is made to the SGT.
- If the **policy dynamic** command is configured and the authorization policy downloaded from the authentication server indicates that the packet source is untrusted, the SGT is replaced with the SGT specified by the downloaded policy.

  The authorization policy can specify the peer's SGT, peer SGT assignment trust state, RBACLs for the associated peer SGT, or an interface ACL.
- If the **policy dynamic** command is configured and the downloaded policy indicates that the packet source is trusted, no change is made to the SGT.

For statically configured SGTs no RBACL is applied, but traditional interface ACL can be configured separately for traffic filtering if required.

Examples

The following example shows how to apply SGT 3 to incoming traffic from the peer, except for traffic already tagged (the interface that has no communication with a Cisco Secure ACS server):

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm null no-encap
Switch(config-if-cts-manual)# policy static sgt 3 trusted
Switch(config-if-cts-manual)# exit
Switch(config-if)# no shutdown
Switch(config-if)# end

Switch# show cts interface GigabitEthernet 2/1

Global Dot1x feature is Enabled
Interface GigabitEthernet2/1:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: "sap"
    Authorization Status:    SUCCEEDED
        Peer SGT:            3
        Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
        Version:             1
        Configured pairwise ciphers:
            gcm-encrypt
            null

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

    Propagate SGT:           Enabled
    Cache Info:
        Cache applied to link : NONE

    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
```

```
authc logoff:                0
sap success:                 1
sap fail:                    0
authz success:               5
authz fail:                  0
port auth fail:              0
Ingress:
    control frame bypassed: 0
    sap frame bypassed:     0
    esp packets:            0
    unknown sa:             0
    invalid sa:             0
    inverse binding failed: 0
    auth failed:            0
    replay error:           0
Egress:
    control frame bypassed: 0
    esp packets:            0
    sgt filtered:           0
    sap frame bypassed:     0
    unknown sa dropped:     0
    unknown sa bypassed:    0
```

Related Commands

Command	Description
show cts interface	Displays TrustSec configuration statistics per interface.
default (cts manual)	Restores default configurations for Cisco TrustSec manual mode.
policy (cts manual)	Configures Cisco TrustSec policy for manual mode.
propagate sgt (cts manual)	Configures Cisco TrustSec SGT Propagation configuration for manual mode.
sap (cts manual)	Configures Cisco TrustSec SAP for manual mode.

propagate sgt (cts dot1x)

To enable or disable the SGT propagation on a Cisco TrustSec interface, use the **propagate sgt** command in CTS dot1x interface configuration mode.

[**no**] **propagate sgt**

Syntax Description

This command has no arguments or keywords.

Defaults

SGT propagation is enabled by default in CTS dot1x and CTS manual interface configuration modes.

Command Modes

CTS dot1x interface configuration mode (config-if-cts-dot1x)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.
Cisco IOS XE Release 3.3.0 SG	This feature was implemented on Catalyst 4000 Series Switches.
15.0(1) SE	This feature was implemented on Catalyst 3750(X) Series Switches.

Usage Guidelines

SGT propagation (SGT tag encapsulation) is enabled by default in both CTS dot1x and CTS manual interface configuration modes. A TrustSec-capable port can support Layer-2 MACsec and SGT encapsulation, and negotiates the most secure mode with the peer for the transmittal of the SGT tag and data.

MACsec is an 802.1AE standard-based link-to-link protocol used by switches and servers. A peer can support MACsec, but not SGT encapsulation. In such a case, it is recommended that this Layer 2 SGT propagation be disabled with the **no propagate sgt** CTS dot1x interface configuration command.

To re-enable the SGT propagation enter the **propagate sgt** command. Use the **show cts interface** command to verify the state of SGT propagation. Only the disabled state is saved in the nonvolatile generation (NVGEN) process.

Examples

The following example shows how to disable SGT propagation on a TrustSec-capable interface:

```
Switch(config) interface gigabitethernet 6/1
Switch(config-if) cts dot1x
Switch(config-if-cts-dot1x)# no propagate sgt
```

```
Switch# show cts interface gigabitethernet 6/1

Global Dot1x feature is Enabled
Interface GigabitEthernet6/1:
    CTS is enabled, mode:    DOT1X
    IFC state:               INIT

<snip> . . . SAP Status:              UNKNOWN
Configured pairwise ciphers:
    gcm-encrypt
    null

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:

    Propagate SGT:           Disabled
<snip> . . .
```

Related Commands

Command	Description
show cts interface	Displays Cisco TrustSec states and statistics per interface.
sap (cts dot1x)	Configures Cisco TrustSec SAP for dot1x mode.
timer (cts do1x)	Configures the Cisco TrustSec timer.

propagate sgt (cts manual)

To enable or disable the ability of an interface to propagate a Security Group Tag, use the **propagate sgt** command in interface manual configuration mode.

[**no**] **propagate sgt**

Syntax Description This command has no keywords or arguments.

Defaults SGT is propagated.

Command Modes CTS manual interface configuration mode (config-if-cts-manual)

SupportedUserRoles Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.

Usage Guidelines Security Group Tag propagation is enabled by default in both CTS dot1x and CTS manual modes. To disable SGT processing, enter the **no propagate sgt** command. To re-enable SGT, enter the **propagate sgt** command. Only the **no propagate sgt** state is saved when issuing a CLI command that invokes the nonvolatile generation (NVGEN) process (for example, **copy system running-config**).

A TrustSec-capable interface can support MACsec (Layer 2 802.1AE security) and SGT tagging. In a manual CTS interface configuration, disable SGT propagation on the Cisco TrustSec-capable interface if you are only implementing MACsec.

A Cisco TrustSec capable port can extract and accept SGT from packets, and it can assign a default to SGT to untagged packets received, or ignore a received SGT tag and override it with a configured default SGT.

The precise behavior is affected by the Cisco TrustSec mode (dot1x or manual), the type of policy in manual mode (static or dynamic), and the trust attribute configured or downloaded in peer policy or dynamic policy.

This behavior is governed by the following table:

Table 3.2: SGT Propagate Behavior Table

Table 11-1

Mode	Policy	Trusted	Propagate	SGT				Notes
				RX			TX	
				From Packet	Default	Overide		
Manual	Static	No	No	Ignored	Config	Yes	No	• no propagate; explicitly configured. • Learn every IP on port (IPM)
Manual	Static	No	Yes	Ignored	Config	Yes	Yes	• propagate behavior assumed. • Learn every IP on port (IPM)
Manual	Static	Yes	No	N/A	N/A	N/A	N/A	Unsupported combination
Manual	Static	Yes	Yes	Taken	Config	No	Yes	propagate behavior is assumed.
Manual	None		No	Ignored	FFFF	Yes	No	• no propagate configured without any policy • Port default FFFF allowing forwarding HW to assign SGT.
Manual	None		Yes	Ignored	FFFF	Yes	Yes	Neither no propagate nor policy are configured.
Manual	Dynamic	Yes	Yes	Taken	FFFF	No	Yes	Default behavior without no propagate.
Manual	Dynamic	Yes	No	Ignored	FFFF	Yes	No	no propagate configured
Manual	Dynamic	No	No	Ignored	Policy	Yes	No	• no propagate configured. • Learn every IP on port (IPM)
Manual	Dynamic	No	Yes	Ignored	Policy	Yes	Yes	• propagate behavior assumed. • Learn every IP on port (IPM)
Dot1x	Peer	Yes	Yes	Taken	FFFF	No	Yes	Default behavior without no propagate
Dot1x	Peer	Yes	No	Ignored	FFFF	Yes	No	no propagate configured

Table 11-1

Mode	Policy	Trusted	Propagate	SGT				Notes
Dot1x	Peer	No	No	Ignored	FFFF	Yes	No	• no propagate configured. • Do not learn every IP on port (IPM)
Dot1x	Peer	No	Yes	Ignored	Policy	Yes	Yes	• propagate behavior assumed. • Learn every IP on port (IPM)

Examples

The following example shows how to disable SGT tagging on a manually-configured TrustSec-capable interface:

```
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk FFFE
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# exit
Switch(config)# exit
Switch# show running-config
. . .
interface GigabitEthernet6/2
 ip address 172.16.4.12 255.255.255.0
cts manual
  no propagate sgt
  sap pmk 00000000000000000000000000000000000000000000000000000000000000000000FFFE
. . .
```

Related Commands

Command	Description
show cts interface	Displays Cisco TrustSec states and statistics per interface.
show running-config	Displays the current system configuration.

sap (cts dot1x)

Use the **sap mode-list** command to select the Security Association Protocol (SAP) authentication and encryption modes to negotiate link encryption between two interfaces. Use the **no** form of this command to remove a modelist and revert to the default.

[**no**] **sap mode-list** {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**]

Syntax Description

mode-list	Lists the advertised SAP authentication and encryption modes (prioritized from the highest to the lowest).
gcm-encrypt	Specifies the Galois Message Authentication Code (GMAC) authentication with Galois Counter Mode (GCM) encryption.
gmac	Specifies GMAC authentication without any encryption.
no-encap	Specifies no encapsulation.
null	Specifies that no encapsulation, authentication, and encryption is required.

Defaults

The default encryption is **sap modelist gcm-encrypt null**. When a peer interface do not support dot1x, 802.1AE MACsec, or 802.REV layer-2 link encryption, the default encryption is **null.**

Command Modes

CTS dot1x interface mode (config-if-cts-dot1x)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.
Cisco IOS XE Release 3.3.0 SG	This command was implemented on Catalyst 4500 Series Switches.
15.0(1)SE	This command was implemented on Catalyst 3000 Series Switches.

Usage Guidelines

Use the **sap mode-list** command to specify the authentication and encryption method to use during dot1x authentication.

The Security Association Protocol (SAP) is an encryption key derivation and exchange protocol based on a draft version of the 802.11i IEEE protocol. SAP is used to establish and maintain the 802.1AE link-to-link encryption (MACsec) between interfaces that support MACsec.

After a dot1x authentication, before the SAP exchange begins, both sides (supplicant and authenticator) receives the Pairwise Master Key (PMK) and the MAC address of the peer's port from the Cisco Secure Access Control Server (Cisco Secure ACS). If 802.1X authentication is not possible, SAP, and the PMK can be manually configured between two interfaces in CTS manual configuration mode.

If a device is running Cisco TrustSec-aware software but the hardware is not Cisco TrustSec-capable, disable encapsulation with the **sap modelist no-encap** command.

Use the **timer reauthentication** command to configure the reauthentication period to be applied to the Cisco TrustSec link in case the period is not available from the Cisco Secure ACS. The default reauthentication period is 86,400 seconds.

Note Because TrustSec NDAC, and SAP are supported only on a switch-to-switch link, dot1x must be configured in multihost mode. The authenticator PAE starts only when **dot1x system-auth-control** is enabled globally.

Examples

The following example shows how to specify that SAP is negotiating the use of Cisco TrustSec encapsulation with GCM cipher, or null-cipher as a second choice, but cannot accept Cisco TrustSec encapsulation if the peer does not support Cisco TrustSec encapsulation in hardware.

```
Switch(config-if-cts-dot1x)# sap modelist gcm-encrypt null no-encap
```

Related Commands

Command	Description
propagate sgt (cts dot1x)	Enables/disables SGT propagation in dot1x mode.
sap (cts dot1x)	Configures Cisco TrustSec SAP for dot1x mode.
timer (cts do1x)	Configures the Cisco TrustSec timer.

sap (cts manual)

Use the **sap** command to manually specify the Pairwise Master Key (PMK) and the Security Association Protocol (SAP) authentication and encryption modes to negotiate MACsec link encryption between two interfaces. Use the **no** form of the command to disable the configuration.

[**no**] **sap pmk** *hex_value* [**modelist** {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**]

Syntax Description

pmk *hex_value*	Specifies the Hex-data PMK (without leading 0x; enter even number of hex characters, or else the last character is prefixed with 0.).
modelist	Specifies the list of advertised modes (prioritized from highest to lowest).
gcm-encrypt	Specifies the Galois Message Authentication Code (GMAC) authentication with Galois Counter Mode (GCM) encryption.
gmac	Specifies the GCM authentication without any encryption.
no-encap	Specifies no encapsulation.
null	Specifies that encapsulation, authentication, and encryption are not present.

Defaults

The default encryption is **sap modelist gcm-encrypt null**. When the peer interface does not support dot1x, 802.1AE MACsec, or 802.REV layer-2 link encryption, the default encryption is **null.**

Command Modes

CTS manual interface configuration mode (config-if-cts-manual)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.
Cisco IOS XE Release 3.3.0SG	This command was implemented on Catalyst 4500 Series Switches.
IOS 15.0(1)SE	This command was implemented on Catalyst 3000 Series Switches.

Usage Guidelines

The Security Association Protocol (SAP) is an encryption key derivation and exchange protocol based on a draft version of the 802.11i IEEE protocol. In a TrustSec configuration, keys are used for MACsec link-to-link encryption between two interfaces.

If 802.1X authentication is not possible, SAP, and the Pairwise Master Key (PMK) can be manually configured between two interfaces with the **sap pmk** command. When using 802.1X authentication, both sides (supplicant and authenticator) receive the PMK and the MAC address of the peer's port from the Cisco Secure Access Control Server.

Examples

The following example shows how to configure SAP on a Gigabit Ethernet interface:

```
Switch(config)# interface gigabitEthernet 2/1
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk FFFEE mode-list gcm-encrypt
```

Related Commands

Command	Description
default (cts manual)	Restores default configurations for Cisco TrustSec manual mode.
policy (cts manual)	Configures Cisco TrustSec policy for manual mode
propagate sgt (cts manual)	Configures Cisco TrustSec SGT Propagation configuration for manual mode
show cts interface	Displays TrustSec configuration statistics per interface.

show cts

To display states and statistics related to Cisco TrustSec, use the **show cts** command in privileged EXEC mode.

show cts [**authorization entries** | **credentials** | **environment-data** | **interface** {type *slot/port* | **vlan** *vlan_number* | **keystore** | **macsec counters interface** type *slot/port* [**delta**] | **pacs** | **policy layer3** [**ipv4** | **ipv6**] | **policy peer** *peer_id* | **provisioning** | **role-based counters** | **role-based flow** | **role-based permissions** | **role-based sgt-map** | **server-list** | **sxp connections** | **sxp sgt-map**]

Syntax Description

authorization	Displays the authorization entries.
credentials	Displays credentials used for Cisco TrustSec authentication.
environment-data	Displays the Cisco TrustSec environment data.
interface	Displays Cisco TrustSec interface status and configuration.
keystore	Displays keystore information.
macsec	Displays MACSec counters information.
pacs	Displays A-ID and PAC-info for PACs in the key store.
policy	Displays the Cisco TrustSec policy.
provisioning	Displays outstanding Cisco TrustSec provisioning jobs.
role-based	Displays Role-based Access Control information (SGACL information).
server-list	Displays the Cisco TrustSec server lists.
sxp	Displays Cisco TrustSec SXP protocol information.

Defaults

None

Command Modes

EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.

Examples

The following is sample output from the **show cts** command:

```
Switch# show cts

Global Dot1x feature: Enabled
CTS device identity: "dcas1"
CTS caching support: disabled
```

```
Number of CTS interfaces in DOT1X mode:  19,    MANUAL mode: 5
Number of CTS interfaces in LAYER3 TrustSec mode: 0

Number of CTS interfaces in corresponding IFC state
  INIT            state:  19
  AUTHENTICATING  state:  0
  AUTHORIZING     state:  0
  SAP_NEGOTIATING state:  0
  OPEN            state:  5
  HELD            state:  0
  DISCONNECTING   state:  0
  INVALID         state:  0

CTS events statistics:
  authentication success: 14
  authentication reject : 19
  authentication failure: 0
  authentication logoff : 1
  authentication no resp: 0
  authorization success : 19
  authorization failure : 3
  sap success           : 12
  sap failure           : 0
  port auth failure     : 0
```

Related Commands

Command	Description
cts credentials	Specifies the TrustSec ID and password.

show cts authorization entries

To display TrustSec Network Device Admission Control (NDAC) authorization entries, use the **show cts authorization entries** command in user EXEC or privileged EXEC mode.

show cts authorization entries

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.

Examples

The following is sample output from the **show cts authorization entries** command:

```
Switch# show cts authorization entries

Authorization Entries Info
 Peer-name                = peer1
Peer-SGT                 = 7-1F05D8C1
Entry State              = COMPLETE
Entry last refresh       = 01:19:37 UTC Sat Dec 8 2007
Session queuesize        = 1
  Interface:       Gi2/3
  status:          SUCCEEDED
Peer policy last refresh = 01:19:37 UTC Sat Dec 8 2007
SGT policy last refresh = 01:19:37 UTC Sat Dec 8 2007
Peer policy refresh time = 2000
Policy expires in     0:00:28:26 (dd:hr:mm:sec)
Policy refreshes in  0:00:28:26 (dd:hr:mm:sec)
Retry_timer                  = not running
Cache data applied           = NONE
Entry status                 = SUCCEEDED

Peer-name = Unknown-0000
Peer-SGT = 0-AD23BDF78
Entry State = COMPLETE
Entry last refresh       = 01:30:37 UTC Sat Dec 8 2007
session queuesize = 0
Peer policy last refresh = 01:30:37 UTC Sat Dec 8 2007
SGT policy last refresh = 01:30:37 UTC Sat Dec 8 2007
Peer policy refresh time = 0
```

```
SGT policy refresh time = 2000
Policy expires in    0:00:29:27 (dd:hr:mm:sec)
Policy refreshes in 0:00:29:27 (dd:hr:mm:sec)
Retry_timer                  = not running
Cache data applied      = NONE
Entry status                 = SUCCEEDED

Peer-name = Unknown-FFFF
Peer-SGT = FFFF-ABC876234
Entry State = COMPLETE
Entry last refresh       = 01:30:37 UTC Sat Dec 8 2007
session queuesize = 0
Peer policy last refresh = 00:20:37 UTC Sat Dec 8 2007
SGT policy last refresh = 01:30:37 UTC Sat Dec 8 2007
Peer policy refresh time = 0
SGT policy refresh time = 2000
Policy expires in    0:00:29:27 (dd:hr:mm:sec)
Policy refreshes in 0:00:29:27 (dd:hr:mm:sec)
Retry_timer                  = not running
Cache data applied       = NONE
Entry status                  = SUCCEEDED
```

Related Commands

Command	Description
cts credentials	Specifies the TrustSec ID and password.

show cts credentials

To display the TrustSec device ID, use the **show cts credentials** command in user EXEC or privileged EXEC mode.

show cts credentials

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.

Examples

This following sample output displays the type of credentials that is used for Cisco TrustSec authentication.

```
Switch# show cts credentials

CTS password is defined in keystore, device-id = r4
```

Related Commands

Command	Description
cts credentials	Specifies the TrustSec ID and password.

show cts environment-data

To display the TrustSec environment data, use the **show cts environment-data** command in user EXEC or privileged EXEC mode.

show cts environment-data

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.

Examples

The following sample outputs displays the environment data on a Cisco Catalyst 6500 series switch:

```
Switch# show cts environment-data

CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 11-ea7f3097b64bc9f8
Server List Info:
Preferred list, 0 server(s):
Installed list: SL1-15A25AC3633E7F074FF7E0B45861DF15, 1 server(s):
 *Server: 43.1.1.3, port 1812, A-ID 05181D8147015544BC20F0119BE8717E
          Status = ALIVE
          auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
  Multicast Group Addresses:
Multicast Group SGT Table:
  Name = mcg_table_2-4ff532e525a3efe4
  Multicast SGT:
Transport type = CTS_TRANSPORT_IP_UDP
Environment Data Lifetime = 2000 secs
Last update time = 21:43:28 UTC Mon Aug 27 2007
Data loaded from cache = FALSE
Refresh timer is running
State Machine is running

Switch# show cts environment-data
CTS Environment Data
```

```
====================
Current state = WAITING_RESPONSE
Last status = Failed
Environment data is empty
State Machine is running
Retry_timer (60 secs) is running

Switch# show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 15- 6b674e447b810692
Server List Info:
Installed list: SL1-1E6E6AE57D4E2A9B320D1844C68BA291, 3 server(s):
 *Server: 17.15.20.102, port 1812, A-ID 87B3503255C4384485BB808DC24C6F55
          Status = ALIVE
          auto-test = FALSE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 17.15.20.101, port 1812, A-ID 255C438487B3503485BBC6F55808DC24
          Status = ALIVE
          auto-test = FALSE, idle-time = 60 mins, deadtime = 20 secs
Installed list: SL2-1E6E6AE57D4E2A9B320D1844C68BA293, 3 server(s):
 *Server: 20.0.0.1, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
          Status = ALIVE
          auto-test = FALSE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 20.0.0.2, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
          Status = ALIVE
          auto-test = FALSE, idle-time = 60 mins, deadtime = 20 secs
  Multicast Group Addresses:
Multicast Group SGT Table:
  Name = MSGT1-1e6e6ae57d4e2a9b320d1844c68ba201
  Multicast SGT:
    0.0.0.0:224.0.1.40 -> 2-7F9509E0
    0.0.0.0:224.0.1.50 -> 3-8B1F05D
Transport type = CTS_TRANSPORT_IP_UDP
Environment Data Lifetime = 600 secs
Last update time = 16:43:39 PDT Fri Dec 7 2007
Env-data expires in         0:00:08:27 (dd:hr:mm:sec)
Env-data refreshes in      0:00:08:27 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

Related Commands

Command	Description
clear cts environment-data	Clears TrustSec environment data from cache.

show cts interface

To display Cisco TrustSec interface configuration statistics, use the **show cts interface** command in user EXEC or privileged EXEC mode.

show cts interface [**type** *slot/port*] | [**brief**] | [**summary**]

Syntax Description

type *slot/port*	(Optional) Specifies an interface type and slot and port number. A verbose output for this interface is returned.
brief	(Optional) Displays abbreviated status for all Cisco TrustSec interfaces.
summary	(Optional) Displays a tabular summary of all Cisco TrustSec interfaces with 4 or 5 key status fields for each interface.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.

Usage Guidelines

Use the **show cts interface** command without keywords to display verbose status for all Cisco TrustSec interfaces.

Examples

The following sample output displays verbose status for all Cisco TrustSec interfaces:

```
Switch# show cts interface

Global Dot1x feature is Enabled
Interface GigabitEthernet4/1:
    CTS is enabled, mode:    DOT1X
    IFC state:               OPEN
    Authentication Status:   SUCCEEDED
        Peer identity:       "r1"
        Peer is:             CTS capable
        802.1X role:         Authenticator
        Reauth period configured:       0 (locally not configured)
        Reauth period per policy:       3000 (server configured)
        Reauth period applied to link:  3000 (server configured)
    Authorization Status:    SUCCEEDED
        Peer SGT:            0
```

```
        Peer SGT assignment: Untrusted
    SAP Status:              NOT APPLICABLE
        Configured pairwise ciphers:
            gcm-encrypt
            null

        Replay protection:      enabled
        Replay protection mode: OUT-OF-ORDER
        SPI range:              (256, 1023)
        Pairwise Master Session Key:
             27C2DF9D 7C686B03 C930D003 95F83737
             6AC0276C 8160FE3C 0C33EF9A C01FCBAC

        Selected cipher:
        Current receive SPI:    0
        Current transmit SPI:   0
        Current Transient Session Key:
             27C2DF9D 7C686B03 C930D003 95F83737
             6AC0276C 8160FE3C 0C33EF9A C01FCBAC

        Current Offset:
             27C2DF9D 7C686B03 C930D003 95F83737
             6AC0276C 8160FE3C 0C33EF9A C01FCBAC

    Statistics:
        authc success:              1
        authc reject:               18
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                0
        sap fail:                   0
        authz success:              1
        authz fail:                 0
        port auth fail:             0
        Ingress:
            control frame bypassed: 0
            sap frame bypassed:     0
            esp packets:            0
            unknown sa:             0
            invalid sa:             0
            inverse binding failed: 0
            auth failed:            0
            replay error:           0
        Egress:
            control frame bypassed: 0
            esp packets:            0
            sgt filtered:           0
            sap frame bypassed:     0
            unknown sa dropped:     0
            unknown sa bypassed:    0

Dot1x Info for GigabitEthernet4/1
-----------------------------------
PAE                     = AUTHENTICATOR
PortControl             = AUTO
ControlDirection        = Both
HostMode                = MULTI_HOST
ReAuthentication        = Enabled
QuietPeriod             = 60
ServerTimeout           = 30
SuppTimeout             = 30
ReAuthPeriod            = 3000 (Locally configured)
ReAuthMax               = 2
```

```
MaxReq                   = 2
TxPeriod                 = 30
```

The following is sample output from the **show cts interface brief** command:

```
Switch# show cts interface brief

Global Dot1x feature is Enabled
Interface GigabitEthernet4/1:
    CTS is enabled, mode:    DOT1X
    IFC state:               OPEN
    Authentication Status:   SUCCEEDED
        Peer identity:       "r1"
        Peer is:             CTS capable
        802.1X role:         Authenticator
        Reauth period configured:       0 (locally not configured)
        Reauth period per policy:       3000 (server configured)
        Reauth period applied to link:  3000 (server configured)
    Authorization Status:    SUCCEEDED
        Peer SGT:            0
        Peer SGT assignment: Untrusted
    SAP Status:              NOT APPLICABLE

Dot1x Info for GigabitEthernet4/1
-----------------------------------
PAE                      = AUTHENTICATOR
PortControl              = AUTO
ControlDirection         = Both
HostMode                 = MULTI_HOST
ReAuthentication         = Enabled
QuietPeriod              = 60
ServerTimeout            = 30
SuppTimeout              = 30
ReAuthPeriod             = 3000 (Locally configured)
ReAuthMax                = 2
MaxReq                   = 2
TxPeriod                 = 30
```

The following is sample output from the **show cts interface summary** command:

```
Switch# show cts interface summary

Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache  Dot1x
-------------------------------------------------------------------------
Gi4/1      DOT1X   OPEN      Authent    r1         invalid    enabled
```

The following sample output shows the Cisco TrustSec information on an interface for the Authenticator role where the reauthentication period is configured on the Authentication Server and the reauthentication value acquired from the server is applied on the interface. The "Reauth starts in approx." timer indicates the time left until the next reauthentication:

```
Switch# show cts interface gigabitethernet 2/3

Global Dot1x feature is Enabled
Interface GigabitEthernet2/3:
    CTS is enabled, mode:    DOT1X
    IFC state:               OPEN
    Authentication Status:   SUCCEEDED
        Peer identity:       "peer1"
        Peer's advertised capabilities: ""
        802.1X role:         Authenticator
        Reauth period configured:       86400 (default)
        Reauth period per policy:       900 (server configured)
        Reauth period applied to link:  900 (server configured)
```

```
        Reauth starts in approx. 0:00:10:10 (dd:hr:mm:sec)
    Authorization Status:    SUCCEEDED
        Peer SGT:            7
        Peer SGT assignment: Trusted
    Cache Info:
        Expiration            : 23:47:36 PDT Jun 20 2008
        Cache applied to link : NONE

    Statistics:
        authc success:              1
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        authz success:              1
        authz fail:                 0
        port auth fail:             0

Dot1x Info for GigabitEthernet2/3
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

The following is sample output from the **show cts interface summary** command. This command displays interface information for both Layer 2 and Layer 3. IPv4 and IPv6 encapsulation and policy states are also displayed.

```
Switch# show cts interface summary

Global Dot1x feature is Disabled


CTS Layer2 Interfaces
---------------------
Interface   Mode             IFC-state  dot1x-role    peer-id        IFC-cache
-------------------------------------------------------------------------------
Te4/2       MANUAL  INIT     unknown     unknown      invalid

CTS Layer3 Interfaces
---------------------
Interface    IPv4 encap       IPv6 encap    IPv4 policy                IPv6 policy
-------------------------------------------------------------------------------------------
Te4/1       ----------------------       ----------       PENDING SETUP    -----------
Te4/3        PENDING SETUP      ----------       ------------------------    -----------
```

The following is sample output displays Cisco TrustSec interface information for the manual mode:

```
Switch# show cts interface gigabitethernet 2/2

Global Dot1x feature is Enabled
Interface GigabitEthernet2/2:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: "sap"
```

```
Authorization Status:    SUCCEEDED
    Peer SGT:            7
    Peer SGT assignment: Trusted  (or Untrusted)
SAP Status:              SUCCEEDED
    Configured pairwise ciphers:
        null    (Other modes are: gcm-encrypt, gmac, no-encap)

    Replay protection:      enabled
    Replay protection mode: OUT-OF-ORDER

    Selected cipher:        null

Cache Info:
    Expiration            : Never expires
    Cache applied to link : NONE
    Expiration            : Never expires

Statistics:
    authc success:              0
    authc reject:               0
    authc failure:              0
    authc no response:          0
    authc logoff:               0
    sap success:                3
    sap fail:                   0
    authz success:              3
    authz fail:                 0
    port auth fail:             0
```

Related Commands

Command	Description
cts sxp	Configures SXP on a network device.

show cts macsec

To display MACSec counters information, use the **show cts macsec** command.

show cts macsec counters interface *interface_type slot/port* [**delta**]

Syntax Description

interface *interface_type slot/port*	Specifies the Cisco TrustSec MACsec interface.
delta	Displays counter values since the last time the counters were cleared.

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.

Usage Guidelines

If Security Associations (SA) are installed (through NDAC or **sap** (**cts interface do1x**) or **sap (cts manual)** commands), the active SA counters are displayed. Only one SA is active at a time. Supported values for SAs are 1 and 2. The **delta** keyword lists the counter values after the **clear cts macsec counters interface** command was issued.

Examples

The following sample output displays the MACsec counters of a manually configured Cisco TrustSec uplink interface on a Catalyst 6500 series switch:

```
Switch# show cts macsec counters interface gigabitEthernet 6/2

CTS Security Statistic Counters:
                    rxL2UntaggedPkts = 0
                       rxL2NotagPkts = 0
                      rxL2SCMissPkts = 0
                        rxL2CTRLPkts = 0
                        rxL3CTRLPkts = 0
                    rxL3UnknownSAPkts = 0
                       rxL2BadTagPkts = 0
                     txL2UntaggedPkts = 0
                        txL2CtrlPkts = 0
                        txL3CtrlPkts = 0
                      txL3UnknownSA = 0
GENERIC Counters:
                      CRCAlignErrors = 0
                      UndersizedPkts = 0
                       OversizedPkts = 0
                        FragmentPkts = 0
                             Jabbers = 0
                          Collisions = 0
```

```
                        InErrors = 0
                       OutErrors = 0
                     ifInDiscards = 0
                ifInUnknownProtos = 0
                    ifOutDiscards = 0
           dot1dDelayExceededDiscards = 0
                             txCRC = 0
                      linkChange = 0
```

Related Commands

Command	Description
show cts interface	Displays Cisco TrustSec states and statistics per interface.
sap (cts dot1x)	Selects the SAP authentication and encryption modes to negotiate link encryption between two interfaces.
sap (cts manual)	Manually specifies the PMK and SAP authentication and encryption modes to negotiate MACsec link encryption between two interfaces.

show cts pacs

To display the Protected Access Credentials (PACs), use the **show cts pacs** command in user EXEC or privileged EXEC mode.

show cts pacs

Syntax Description This command has no arguments or keywords.

Defaults None

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

SupportedUserRoles Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.

Usage Guidelines Use this command to identify the Network Device Admission Control (NDAC) authenticator and to verify NDAC completion.

Examples The following sample output displays the Protected Access Credential (PAC) received from a Cisco ACS with the authenticator ID (A-ID–Info):

```
Switch# show cts pacs

  AID: 1100E046659D4275B644BF946EFA49CD
  PAC-Info:
    PAC-type = Cisco Trustsec
    AID: 1100E046659D4275B644BF946EFA49CD
    I-ID: device1
    A-ID-Info: acs1
    Credential Lifetime: 13:59:27 PDT Jun 5 2010
  PAC-Opaque: 000200B000030001000400101100E046659D4275B644BF946EFA49CD0006009400
0301008285A14CB259CA096487096D68D5F34D000000014C09A6AA00093A808ACA80B39EB656AF0B
CA91F3564DF540447A11F9ECDFA4AEC3A193769B80066832495B8C40F6B5B46B685A68411B7DF049
A32F2B03F89ECF948AC4BB85CF855CA186BEF8E2A8C69A7C0BE1BDF6EC27D826896A31821A7BA523
C8BD90072CB8A8D0334F004D4B627D33001B0519D41738F7EDDF3A
  Refresh timer is set for 00:01:24

Switch# show cts pacs

  AID: CAFECAFECAFECAFECAFECAFECAFECAFE
  PAC-Info:
    PAC-type = tunnel
```

```
    AID: CAFECAFECAFECAFECAFECAFECAFECAFE
    I-ID: kyoto
    A-ID-Info: "CTS-ACS on ACS1"
    Credential Lifetime: Apr 06 2002 01:00:31 UTC
PAC-Opaque:
000200820001000400 10DEADBEEFDEADBEEF1111111111111111000600540000000158EDE58522C8698794F2F2
4F2623F8D26D78414DE33B102E6E93EDE53B8EFF0061FC14C1E1CCF14A04F69DAC79FE9F1BCD514893AC87B0AD
B476D2CB9CBF75788C5B8C3AE89E5322E4A124D4CB6A616B306E1DDD38CCE3E634E64E17BBD31957B0579DBC
Refresh timer is set for 2w1d
```

Related Commands

Command	Description
clear cts pac	Clears a PAC or all PACs from the keystore.
cts sxp	Configures SXP on a network device.

show cts policy layer3

To display the name of traffic and exception polices used for Cisco TrustSec Layer 3 transport configurations, use the **show cts policy layer3** command in user EXEC or privileged EXEC mode.

show cts policy layer3 {**ipv4** | **ipv6**}

Syntax Description

ipv4	Specifies IPv4 policies.
ipv6	Specifies IPv6 policies

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 series switches.

Usage Guidelines

A traffic or exception policy may be configured locally, or obtained from the Cisco Secure ACS.

Examples

The following is sample output from the **show cts policy3** command:

```
Switch# show cts policy layer3 ipv4

No CTS L3 IPV4 policy received from ACS
Local CTS L3 IPv4 exception policy name  : cts-exceptions-local
Local CTS L3 IPv4 traffic policy name     : cts-traffic-local
Current CTS L3 IPv4 exception policy name: cts-exceptions-local
Current CTS L3 IPv4 traffic policy name   : cts-traffic-local
```

Related Commands

Command	Description
cts policy layer3	Specifies traffic and exception policies for Cisco TrustSec Layer 3 Transport.
cts layer3	Enables and applies traffic and exception policies to Cisco TrustSec Layer 3 transport gateway interfaces.

show cts policy peer

To display the peer authorization policy data of Cisco TrustSec peers, use the **show cts policy peer** command in user EXEC or privileged EXEC mode.

show cts policy peer

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.

Examples

The following sample output displays the Cisco TrustSec peer authorization policy of all peers:

```
VSS-1# show cts policy peer

CTS Peer Policy
===============
Peer name: VSS-2T-1
Peer SGT: 1-02
Trusted Peer: TRUE
Peer Policy Lifetime = 120 secs
Peer Last update time = 12:19:09 UTC Wed Nov 18 2009
Policy expires in 0:00:01:51 (dd:hr:mm:sec)
Policy refreshes in 0:00:01:51 (dd:hr:mm:sec)
Cache data applied = NONE
```

The following table describes the output fields.

Output Field	Explanation
Peer name	Cisco TrustSec device ID of the peer to which the local device is connected.
Peer SGT	The Security Group Tag of the peer.

Output Field	Explanation
Trusted Peer	TRUE—The local device trusts the SGT tagged in the packet coming from this peer. FALSE—The device does not trust the SGT tagged in the packet coming from this peer.
Peer Policy Lifetime	The length of time this policy is valid before it is refreshed.
Peer Last update time	The time when this policy was last refreshed
Policy expires in (dd:hr:mm:sec)	This peer policy is due to expire after this elapsed time
Policy refreshes in 0:00:01:51 (dd:hr:mm:sec)	This peer policy will be refreshed after this elapsed time
Cache data applied = NONE	This policy was not populated from cache, i.e., it was acquired from the ACS

Related Commands

Command	Description
cts refresh	Forces refresh of peer authorization policies.
clear cts policy	Clears the peer authorization policy of a TrustSec peer.

show cts provisioning

To display the Cisco TrustSec provisioning jobs waiting on the RADIUS server, use the **show cts provisioning** command in user EXEC or privileged EXEC mode.

show cts provisioning

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 Series Switches.

Usage Guidelines

Use this command to display the queue for protected access credential (PAC) provisioning jobs. Reprovisioning occurs when PACs expire or devices are reconfigured.

Examples

The following sample output displays a list of AAA servers that the Cisco TrustSec provisioning driver is retrying for PAC-provisioning:

```
Switch# show cts provisioning

A-ID: 0b2d160f3e4dcf4394262a7f99ea8f63
   Server 41.16.19.201, using existing PAC
      Req-ID EB210008: callback func 418A8990, context 290F14D0
A-ID: Unknown
   Server 41.16.19.203, using shared secret
      Req-ID 49520002: callback func 40540CF0, context AE000007
```

Related Commands

Command	Description
show cts pacs	Displays the A-ID and PAC-info for PACs in the keystore.
radius-server host	Specifies the RADIUS servers for device authentication.

show cts rbacl

To display the role-based access control list (RBACL) policy lists acquired from the Cisco Secure Access Control Server, use the **show cts rbacl** command in privileged EXEC mode.

show cts rbacl [*name-list*]

Syntax Description

name-list	(Optional) RBACL lists.

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.

Usage Guidelines

Specify the name of an RBACL to display information about it or the **show cts rbacl** command displays information about all RBACLs.

Examples

The following sample output displays information about all RBACLs:

```
Switch# show cts rbacl

CTS RBACL Policy
================
  name   = RBACLANY2ANY-4fd20415d67b012545cc7f0367d732f4
  refcnt = 3
  flag   = 0x0
  staled = FALSE
  RBACL ACEs:
    permit ip

  name   = RBACL1001-6e928b43045978b25f739d4f1562d0e6
  refcnt = 1
  flag   = 0x0
  staled = FALSE
  RBACL ACEs:
    permit icmp host-unreachable
    deny tcp
    permit udp

  name   = RBACL101-9e11409565e40823c245430be8c35144
  refcnt = 7
  flag   = 0x0
```

```
  staled = FALSE
  RBACL ACEs:
    permit icmp host-unreachable
    deny tcp
    permit udp

  name   = RBACL0099-d381deab1fa777901f9d5c2301b3d677
  refcnt = 1
  flag   = 0x0
  staled = FALSE
  RBACL ACEs:
    deny tcp
    permit udp

  name   = RBACL102-1c6ca50a2a6135972b28cf99a82027ed
  refcnt = 2
  flag   = 0x0
  staled = FALSE
  RBACL ACEs:
    permit ip

  name   = RBACL901-4241cdc840708c99a8cf8dbc271cc295
  refcnt = 6
  flag   = 0x0
  staled = FALSE
  RBACL ACEs:
    permit icmp host-unreachable
    deny tcp
    permit udp
    permit ip
```

The following sample output displays information about RBACL101:

```
Switch# show cts rbacl RBACL101

CTS RBACL Policy
================
  name   = RBACL101-9e11409565e40823c245430be8c35144
  refcnt = 1
  flag   = 0x0
  staled = FALSE
  RBACL ACEs:
    permit icmp host-unreachable
    deny tcp
    permit udp
```

show cts role-based counters

To display Security Group access control list (ACL) enforcement statistics, use the **show cts role-based counters** command in user EXEC and privileged EXEC mode. Use the **clear cts role-based counters** command to clear the counters.

show cts role-based counters

show cts role-based counters default [**ipv4** | **ipv6**]

show cts role-based counters from {*sgt_num* | **unknown**} [**ipv4** | **ipv6** |
to {*sgt_num* | **unknown**} [**ipv4** | **ipv6**]]

show cts role-based counters to {*sgt_num* | **unknown**} [**ipv4** | **ipv6** |]

show cts role-based counters [**ipv4** | **ipv6**]

Syntax Description

default	Specifies default policy counters.
from	Specifies the source security group.
ipv4	Specifies security groups on IPv4 networks.
ipv6	Specifies security groups on IPv6 networks.
to	Specifies the destination security group.
sgt_num	Security Group Tag number. Valid values are from 0 to 65533.
unknown	Specifies all source groups.

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.

Usage Guidelines

Use the **show cts role-based counters** command to display the Security Group ACL (SGACL) enforcement statistics. Use the **clear cts role-based counters** to reset all or a range of statistics.

Specify the source SGT with the **from** keyword and the destination SGT with the **to** keyword. All statistics are displayed when both the **from** and **to** keywords are omitted.

The **default** keyword displays the statistics of the default unicast policy. When neither **ipv4** nor **ipv6** are specified this command displays only IPv4 counters.

Examples

The following sample output displays all enforcement statistics for IPv4 and IPv6 events:

```
Switch# show cts role-based counters

Role-based counters

From    To      SW-Denied       HW-Denied       SW-Permitted    HW_Permitted
2       5       129                89762                421      7564328
3       5        37               123456               1325     12345678
3       7         0                65432                325      2345678
```

Related Commands

Command	Description
clear cts role-based counters	Resets Security Group ACL statistic counters.
cts role-based	Manually maps a source IP address to a SGT on either a host or a VRF as well as enabling SGACL enforcement.

show cts role-based flow

To display the Role-Based access control Flexible NetFlow information, use the **show cts role-based flow** command in privileged EXEC mode.

clear cts role-based flow

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Privileged EXEC (#)

SupportedUserRoles Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 Series Switches.

Examples The following is sample output from the **show cts role-based flow** command:

show cts role-based permissions

To display the Cisco TrustSec role-based access control list (RBACL) permissions, use the **show cts role-based permissions** command in privileged EXEC mode.

show cts role-based permissions [[**default**] [**from**] [**ipv4**] [**to**]] [**details**]

Syntax Description

default	(Optional) Displays the default permission list.
from	(Optional) Displays the source group.
ipv4	(Optional) Displays the IPv4 RBACLs.
to	(Optional) Displays the destination group.
details	(Optional) Displays the attached access control list (ACL) details.

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 Series Switches.

Usage Guidelines

This show command displays the content of the RBACL permission matrix. You can specify the source SGT by using the **from** keyword and the destination SGT by using the **to** keyword. When both **from** and **to** are specified the RBACLs of a single cell are displayed. An entire column is displayed when only the **to** keyword is used. An entire row is displayed when the **from** keyword is used.

The entire permission matrix is displayed when both the **from** clause and **to** keywords are omitted.

The command output is sorted by destination SGT as a primary key and the source SGT as a secondary key. The RBACLs for each cell is displayed in the same order they are defined in the configuration or acquired from Cisco ACS.

The **details** keyword is provided when a single cell is selected by specifying both **from** and **to** keywords. When the **details** keyword is specified the ACEs of the RBACLs of a single cell are displayed.

Examples

The following is sample output from the **show cts role-based permissions** command:

```
Switch# show cts role-based permissions

Role-based permissions from group 2 to group 5:
        srb2
        srb5
Role-based permissions from group 3 to group 5:
```

```
        srb3
        srb5
Role-based permissions from group 3 to group 7:
        srb4
```

The following is sample output from the **show cts role-based permissions from to** command:

```
Switch# show cts role-based permissions from 2 to 5

Role-based permissions from group 2 to group 5:
        srb2
        srb5
```

Related Commands

Command	Description
cts role-based	Manually configures SGT impositions, TrustSec NetFlow parameters, and SGACL enforcement.

show cts role-based sgt-map

To display the Security Group Tag (SGT) Exchange Protocol (SXP) source IP-to-SGT bindings table, use the **show cts role-based sgt-map** command in user EXEC or privileged EXEC mode.

show cts role-based sgt-map {*ipv4_dec* | *ipv4_cidr* | *ipv6_hex* | *ipv6_cidr* | **all** [**ipv4** | **ipv6**] | **host** {*ipv4_decimal* | *ipv6_dec*} | **summary** [**ipv4** | **ipv6**] | **vrf** *instance_name* {*ipv4_dec* | *ipv4_cidr* | *ipv6_dec* | *ipv6_cidr* | **all** {**ipv4** | **ipv6**} | **host** {*ipv4_decimal* | *ipv6_dec*} |**summary** {**ipv4** | **ipv6**}}

Syntax Description

ipv4_dec	IPv4 address in dot-decimal notation. For example (208.77.188.166)
ipv4_cidr	IPv4 address range in Classless Inter-Domain Routing (CIDR) For example, 10.0.0.0/8, where the /8 signifies that the 8 most significant bits identify the networks, and the 24 least-significant bits, the hosts.
ipv6_hex	IPv6 address in hexadecimal separated by colons. For example, 2001:db8:85a3::8a2e:370:7334.
ipv6_cidr	A range of IPv6 address in hexadecimal CIDR notation.
host *ipv4_decimal* | *ipv6_hex*	Specifies mappings for a specific IPv4 or IPv6 host. Use dot decimal and hex colon notation for IPv4 and IPv6 respectively.
all	Specifies all mappings to be displayed.
summary ipv4 | ipv6	Summary of IPv4 or IPv6 mappings. Displays both IPv4 and IPv6 if you do not specify a keyword.
vrf *instance_name*	Specifies a VPN routing and forwarding instance for mappings.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI3	This command was introduced on Catalyst 6500 series switches.
12.2(50)SG7	This command was implemented on Catalyst 4000 series switches (without **vrf** keyword).
12.2(53)SE2	This command was implemented on Catalyst 3750(E) and 3560(E) series switches (without **vrf** keyword).
12.2(53)SE2	This command was implemented on the Catalyst 3750(X) series switches (without **vrf** keyword).

Usage Guidelines

Use this command to verify that source IP addresses to the appropriate Security Group Tags bindings are correct. This command shows information about active IP-SGT bindings for the specified IP host address or subnet.

This command displays a single binding when host IP address is specified. It displays all the bindings for IP addresses within a given subnet if <network>/<length> is specified.

A summary of the active bindings by source is displayed at the end of the keyword all output and also if the keyword summary is entered.

Examples

The following sample output displays the bindings of IP address and SGT source names:

```
Switch# show cts role-based sgt-map all

Active IP-SGT Bindings Information

IP Address    SGT Source
============================================
10.1.1.1       7   INTERNAL
10.252.10.1   7   INTERNAL
10.252.10.10  3   LOCAL
10.252.100.1  7   INTERNAL
172.26.208.31 7   INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of INTERNAL bindings = 4
Total number of active   bindings = 5
```

Related Commands

Command	Description
cts role-based	Manually configures SGT impositions, TrustSec NetFlow parameters, and SGACL enforcement.
cts sxp	Configures SXP on a network device.
show cts sxp	Displays Cisco TrustSec SXP protocol information

show cts server-list

To display the list of RADIUS servers available to Cisco TrustSec seed and nonseed devices, use the **show cts server-list** command in user EXEC or privileged EXEC mode.

show cts server-list

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.

Examples

The following sample output displays the Cisco TrustSec RADIUS server list:

```
Switch> show cts server-list

CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Preferred list, 1 server(s):
 *Server: 10.0.1.6, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
          Status = ALIVE
          auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
Installed list: ACSServerList1-0001, 1 server(s):
 *Server: 101.0.2.61, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
          Status = ALIVE
          auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
```

Related Commands

Command	Description
cts server	Displays Cisco TrustSec server list configuration.

show cts sxp

To display Security Group Tag (SGT) Exchange Protocol (SXP) connection or source IP-to-SGT mapping information, use the **show cts sxp** command in user EXEC or privileged EXEC mode.

show cts sxp {**connections** | **sgt-map**} [**brief** | **vrf** *instance_name*]

Syntax Description

connections	Displays Cisco TrustSec SXP connections information.
sgt-map	Displays the IP-SGT mappings received through SXP.
brief	(Optional) Displays an abbreviated version of the SXP information.
vrf *instance_name*	(Optional) Displays the SXP information for the specified VRF instance name.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 series switches.
12.2(50)SG7	This command was implemented on Catalyst 4000 series switches
12.2(53)SE2	This command was implemented on Catalyst 3750(E) and 3560(E) series switches.
12.2(53)SE2	This command was integrated Catalyst 3750(X) series switches.

Usage Guidelines

Use the **cts sxp connections** command to view the status of the network device SXP configuration. Use the **cts sxp sgt-map** command to display the current source IP-to-SGT mapping database.

Examples

The following sample output displays the default SXP configuration:

```
Switch# show cts sxp connections

 SXP              : Disabled
 Default Password : Not Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
There are no SXP Connections.
```

The following sample output displays a brief summary of SXP connections:

```
Switch# show cts sxp connection brief

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running

------------------------------------------------------------------------------
Peer_IP          Source_IP        Conn Status       Duration
------------------------------------------------------------------------------
2.2.2.1          2.2.2.2          On                0:00:02:14 (dd:hr:mm:sec)
3.3.3.1          3.3.3.2          On                0:00:02:14 (dd:hr:mm:sec)

Total num of SXP Connections = 2
```

The following sample output displays all SXP connections:

```
Switch# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP          : 2.2.2.1
Source IP        : 2.2.2.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)

----------------------------------------------
Peer IP          : 3.3.3.1
Source IP        : 3.3.3.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
TCP conn fd      : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)


Total num of SXP Connections = 2
```

The following sample output is from an SXP listener with a torn down connection to the SXP speaker. Source IP-to-SGT mappings are held for 120 seconds, the default value of the Delete Hold Down timer.

```
Switch# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
```

```
----------------------------------------------
Peer IP           : 2.2.2.1
Source IP         : 2.2.2.2
Set up            : Peer
Conn status       : Delete_Hold_Down
Connection mode   : SXP Listener
Connection inst# : 1
TCP conn fd       : -1
TCP conn password: not set (using default SXP password)
Delete hold down timer is running
Duration since last state change: 0:00:00:16 (dd:hr:mm:sec)

----------------------------------------------
Peer IP           : 3.3.3.1
Source IP         : 3.3.3.2
Set up            : Peer
Conn status       : On
Connection inst# : 1
TCP conn fd       : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:05:49 (dd:hr:mm:sec)

Total num of SXP Connections = 2
```

The following sample output displays the current Source IP-to-SGT mapping database learned through SXP:

```
Switch# show cts sxp sgt-map

IP-SGT Mappings as follows:
IPv4,SGT: <10.2.2.1 , 7>
source  : SXP;
Peer IP : 10.2.2.1;
Ins Num : 1;
IPv4,SGT: <10.2.2.1 , 7>
source  : SXP;
Peer IP : 10.3.3.1;
Ins Num : 1;
Status  : Active;
IPv4,SGT: <10.3.3.1 , 7>
source  : SXP;
Peer IP : 10.2.2.1;
Ins Num : 1;
```

The following sample output displays a brief summary of the current Source IP-to-SGT mapping database:

```
Switch# show cts sxp sgt-map brief

IP-SGT Mappings as follows:
IPv4,SGT: <10.2.2.1 , 7>
IPv4,SGT: <10.3.3.1 , 7>
IPv4,SGT: <10.4.4.1 , 7>
IPv4,SGT: <10.13.21.41 , 7>
```

Related Commands

Command	Description
cts sxp	Configures SXP on a network device.

show cts keystore

To display the contents of the software or hardware encryption keystore, use the **show cts keystore** command in user EXEC or privileged EXEC mode.

show cts keystore

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Catalyst 6500 series switches as **show cts keystore**.
12.2(50)SY	This command is replaced by the **show keystore** command.

Usage Guidelines

This command shows all the records stored in the keystore. The stored secrets are not revealed.

Examples

The following sample output displays the contents of a keystore:

```
Switch# show cts keystore

No hardware keystore present, using software emulation.
Keystore contains the following records (S=Simple Secret, P=PAC, R=RSA):

Index  Type  Name
-----  ----  ----
    0     P  05181D8147015544BC20F0119BE8717E
    1     S  CTS-password
```

The following sample output displays the contents of a hardware keystore:

```
Switch# show cts keystore

CTS keystore firmware version 2.0.
Keystore contains the following records (S=Simple Secret, P=PAC, R=RSA):

Index  Type  Name
-----  ----  ----
    0     S  CTS-passwordFOX094901KW
    1     P  74656D706F72617279
```

```
Hardware Keystore error counters:
       FW Panics = 0
       FW Resets = 0
       RX FIFO underruns = 12
       RX timeouts = 0
       RX bad checksums = 0
       RX bad fragment lengths = 0
       Corruption Detected in keystore = 0
```

Related Commandsa

Command	Description
cts credentials	Specifies the TrustSec ID and password.
cts sxp	Configures SXP on a network device.

show platform cts reflector

To display the status of the Cisco TrustSec reflector mode (ingress, egress, pure, or no Cisco TrustSec) on a specific interface, use the **show platform cts reflector** command.

show platform cts reflector interface type *slot/port*

Syntax Description

interface type *slot/port*	Specifies the interface type, slot and port for which to display status.

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(50)SY	This command was introduced on Catalyst 6500 Series Switches.

Related Commands

Command	Description
platform cts	Enables the TrustSec egress or ingress reflector.

timer (cts do1x)

To set the dot1x authentication timer, use the **timer** command in CTS dot1x interface configuration mode. Use the **no** form of the command to disable dot1x reauthentication.

[**no**] **timer reauthentication** *seconds*

Syntax Description

reauthentication *seconds*	Specifies the reauthentication timer in seconds. Valid values are from 0 to 2147483. 0 disables the dot1x reauthentication.

Defaults

86,400 seconds (24 hours).

Command Modes

CTS dot1x interface configuration mode (config-if-cts-dot1x)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2(33)SXI	This command was introduced on Catalyst 6500 Series Switches.
Cisco IOS XE Release 3.3.0 SG	This command was implemented on Catalyst 4500 Series Switches.
15.0(1)SE	This command was implemented on Catalyst 3000 Series Switches.

Usage Guidelines

Use the **timer reauthentication** command to configure a dot1x reauthentication period if the authentication server does not specify a period. If no reauthentication period is specified, the default is 86,400 seconds.

To disable dot1x reauthentication, use the **no** form of the command or specify a period of 0 seconds. Use the **default timer reauthentication** command to restore the default value.

Examples

The following example shows how to set the 802.1X reauthentication period for 48 hours (17,2800 seconds):

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# timer reauthentication 172800
```

Related Commands

Command	Description
show cts interface	Displays Cisco TrustSec states and statistics per interface.
sap (cts dot1x)	Configures Cisco TrustSec SAP for dot1x mode.
propagate sgt (cts dot1x)	Enables/disables SGT propagation in dot1x mode.

debug cts

To enable the debugging of Cisco TrustSec operations, use the **debug cts aaa** command in privileged EXEC mode. To disable the debugging, use the **no** form of this command.

[no] debug cts [**aaa** | **all** | **authentication** {**details** | **events**} | **authorization** [**aaa** | **all** | **events** | **rbacl** | **snmp**] | **cache** | **coa events** | **dp** {**info** | **error** | **packets**} | **environment-data** [**aaa** | **all** | **events**] | **error** | **fips events** | **ha** {**config** | **core** | **infra**} | **ifc** {**cache** | **events** | **snmp**} | **layer3-trustsec** | **provisioning** {**events** | **packets**} | **relay** {**event** | **pak**} | **sap** {**events** | **packets** | **pakdump**} | **server-list** | **states** | **sxp** {**conn** | **error** | **internal** | **mdb** | **message**}]

Syntax Description

aaa	(Optional) Enables debugging of authentication, authorization, and accounting (AAA) parameters for Cisco TrustSec.
all	(Optional) Enables debugging of all Cisco TrustSec messages.
authentication	(Optional) Enables debugging of Cisco TrustSec authentication messages.
details	(Optional) Enables debugging of authentication details.
events	(Optional) Enables debugging of authentication events.
authorization	(Optional) Enables debugging of Cisco TrustSec authorization messages.
rbacl	(Optional) Enables debugging of role-based access control list (RBACL) policy installation events.
snmp	(Optional) Enables debugging of Cisco TrustSec policy for SNMP related events.
cache	(Optional) Enables debugging of Cisco TrustSec cache.
coa events	(Optional) Enables debugging of Change of Authorization (CoA) events.
dp	(Optional) Enables debugging of Cisco TrustSec datapath messages.
info	(Optional) Enables debugging of informational messages.
error	(Optional) Enables debugging of Cisco TrustSec errors.
packets	(Optional) Enables debugging of data packets.
environment-data	(Optional) Enables debugging of Cisco TrustSec environment data operations.
fips	(Optional) Enables debugging of Federal Information Processing Standards (FIPS) publication140-2 Cryptographic Module Validation Program (CMVP) events.
ha	(Optional) Enables debugging of high availability messages.
config	(Optional) Enables debugging of high availability configuration.
core	(Optional) Enables debugging of high availability core.
infra	(Optional) Enables debugging of high availability infra.
ifc	(Optional) Enables debugging of Cisco TrustSec Interface Controller.
layer3-trustsec	(Optional) Enables debugging of Layer 3 Cisco TrustSec policy.
provisioning	(Optional) Enables debugging of protected access credential (PAC) provisioning.
relay	(Optional) Enables debugging of Cisco TrustSec relay events.

pak	(Optional) Enables debugging of Cisco TrustSec relay packets.
sap	(Optional) Enables debugging of Cisco TrustSec Security Association Protocol (SAP).
pakdump	(Optional) Enables debugging of SAP packet dumps.
server-list	(Optional) Enables debugging of Cisco TrustSec server list operations.
states	(Optional) Enables state change debugs.
sxp	(Optional) Enables debugging of Security Group Tag (SGT) Exchange Protocol (SXP) operations.
conn	(Optional) Enables debugging of SXP connections.
message	(Optional) Enables debugging of SXP messages.

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

Release	Modification
12.2 (33) SXI3	This command was introduced on the Catalyst 6500 Series Switches..

Examples

The following example show how to enable Cisco TrustSec debugging:

```
Switch# debug cts
Default cts debugging is on
```

The following example shows how to enable debugging of environment data:

```
Switch# debug cts environment-data aaa
CTS environment data AAA messages debugging is on
```

Related Commands

Command	Description
cts cache	Enables caching of TrustSec authorization and environment data information to DRAM and NVRAM.
cts layer3	Enables Cisco TrustSec Layer 3 transport gateway interfaces, and applies exception and traffic policies to the interfaces.
cts sxp	Configures SXP on a network device.