



CHAPTER 7

Cisco TrustSec Command Summary

Revised: April 26, 2013, OL-22192-01

Cisco TrustSec Privileged EXEC Commands

cts change-password	Initiate password change with AAA server.
cts credentials	Inserts CTS device ID and password into the keystore.
cts refresh	Refresh environment, peer and RBACL policies.
cts rekey	CTS SAP rekey
cts role-based policy trace	TrustSec SGT and SGACL trace utility.

Cisco TrustSec Global Configuration Commands

cts authorization list	Configures CTS global authorization configuration.
cts cache	Enables caching of TrustSec authorization and environment-data information to DRAM and NVRAM.
cts manual	Define CTS keystore behavior
cts policy layer3	Specifies traffic and exception policies for CTS Layer 3 Transport gateway interfaces.
cts role-based	Maps IP addresses, L3 interfaces, and VRFs to SGTs; enables CTS 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.

CTS Flexible NetFlow Commands

match flow cts	
--------------------------------	--

CTS Interface Configuration Commands

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

CTS dot1x Submode Commands

<code>default (cts dot1x interface configuration submode)</code>	Restores defaults for CTS dot1x commands.
<code>propagate (cts dot1x submode)</code>	Enables/disables SGT propagation in dot1x mode.
<code>sap (cts dot1x interface submode)</code>	Configures CTS SAP for dot1x mode.
<code>timer (cts dot1x interface submode)</code>	Configures the CTS timer.

CTS Manual Interface Configuration Submode Commands

<code>default (cts manual interface configuration submode)</code>	Restores default configurations for CTS manual mode.
<code>policy (cts manual interface configuration submode)</code>	Configures CTS policy for manual mode
<code>propagate (cts manual interface configuration submode)</code>	Configures CTS SGT Propagation configuration for manual mode
<code>sap (cts manual interface submode)</code>	Configures CTS SAP for manual mode.

Cisco TrustSec Clear Commands

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

Cisco TrustSec Show Commands	
<code>show cts authorization entries</code>	Displays the authorization entries.
<code>show cts credentials</code>	Displays credentials used for CTS authentication.
<code>show cts environment-data</code>	Displays the CTS environment data.
<code>show cts interface</code>	Displays CTS states and statistics per interface.
<code>show cts macsec</code>	Displays crypto ASIC packet counters per interface.
<code>show cts pacs</code>	Displays the A-ID and PAC-info for PACs in the keystore.
<code>show cts policy peer</code>	Displays the peer authorization policies of TrustSec peers.
<code>show cts policy layer3</code>	Displays the traffic and exception policies used in CTS Layer3 Transport.
<code>show cts provisioning</code>	Displays outstanding CTS provisioning jobs
<code>show cts role-based sgt-map</code>	Displays IP address to Security Group Tag mappings.
<code>show cts role-based counters</code>	Displays role-based access control enforcement statistics for SGTs and DGTs.
<code>show cts role-based sgt-map</code>	Displays IP to SGT bindings, permission lists, and NetFlow statistics.
<code>show cts server-list</code>	Displays lists of AAA servers and load balancing configurations.
<code>show cts sxp</code>	Displays CTS SXP protocol information.
<code>show platform cts reflector</code>	Displays the status of CTS reflector per interface.
Commands to Configure Endpoint Admission Control (EAC)	
<code>aaa accounting</code>	
<code>aaa authorization</code>	
<code>aaa authentication</code>	
<code>order</code>	
<code>priority</code>	
<code>event</code>	
<code>periodic</code>	
<code>timer</code>	
<code>host-mode</code>	
<code>authorization</code>	
<code>accounting</code>	
<code>radius-server host</code>	
<code>authentication port-control</code>	

Debug Commands

debug authentication event	
debug authentication feature	
debug condition cts peer-id	
debug condition cts	Filters CTS debugging messages by interface name, peer-id, peer-SGT or Security Group name.
debug condition cts peer-id	
debug condition cts security-group	
debug cts aaa	
debug cts authentication events	
debug cts authorization	
debug cts authorization events	
debug cts authorization rbacl	
debug cts authorization snmp	
debug cts cache	
debug cts coa events	
debug cts dp errors	
debug cts dp info	
debug cts dp packets	
debug cts environment-data	
debug cts environment-data events	
debug cts error	
debug cts fips	
debug cts ha	
debug cts ha core	
debug cts ha infra	
debug cts ifc	
debug cts ifc cache	
debug cts ifc events	
debug cts ifc snmp	
debug cts layer3-trustsec	
debug cts provisioning	
debug cts provisioning event	
debug cts provisioning pak	
debug cts relay event	
debug cts relay pak	
debug cts sap events	
debug cts sap packets	
debug cts sap pakdump	

debug cts server-list	
debug cts states	
debug cts sxp	
debug cts sxp conn	
debug cts sxp error	
debug cts sxp internal	
debug cts sxp mdb	
debug cts sxp message	
debug dot.lx	
debug epm	
debug event	
debug mab	
debug radius	
debug rbm api	
debug rbm cli	
debug rbm bindings	
debug rbm dp errors	
debug rbm dp events	
debug rbm dp packets	
debug rbm platform	
debug rbm policy	

cts authorization list

To specify a list of AAA servers to use by the TrustSec seed device, use the **cts authorization** command on the 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	<i>server_list</i> Specifies a Cisco TrustSec AAA server group.	
Defaults	None	
Command Modes	Global configuration (config)	
Supported User Roles	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: <pre> Router# cts credentials id Switch1 password Cisco123 Router# configure terminal Router(config)# aaa new-model Router(config)# aaa authentication dot1x default group radius Router(config)# aaa authorization network MLIST group radius Router(config)# cts authorization list MLIST Router(config)# aaa accounting dot1x default start-stop group radius Router(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key AbCe1234 Router(config)# radius-server vsa send authentication Router(config)# dot1x system-auth-control Router(config)# exit </pre>	
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** global configuration 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 CTS 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: <i>dir</i>		Specifies bootflash dir as the nv-storage location.
disk0: <i>dir</i>		Specifies disk 0 directory as the nv-storage location.
disk1: <i>dir</i>		Specifies disk 1 directory as the nv-storage location.
sup-bootflash: <i>image</i>		Specifies a supervisor bootflash directory as the nv-storage location.

Defaults The default is caching disabled.

Command Modes Global configuration (config)

Supported User Roles 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 is 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 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, thus expediting the

formation of the CTS 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 enables cache support:

```
Router# config t
Router(config)# cts cache nv-storage disk0:
Router(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	
cts credentials	

cts change-password

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.
<i>ipv4_address</i>		The IP address of the authentication server.
<i>udp_port</i>		The UPD port of the authentication server.
a-id <i>hex_string</i>		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
<i>interface_list</i>		Specify the interface type and its identifying parameters per the displayed list.

Defaults	There is no default for this command.
-----------------	---------------------------------------

Command Modes	Privileged EXEC (#)
----------------------	---------------------

SupportedUserRoles	Administrator
---------------------------	---------------

Command Types	Use the following command syntax
----------------------	----------------------------------

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

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

**Note**

The **cts change-password** is supported on Cisco Secure ACS, 5.1 and more recent 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.

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

Defaults None

Command Modes Privileged EXEC (#)

Supported User Roles Administrator

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

Usage Guidelines For use in TrustSec Network Device Admission Control (NDAC) authentication, 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 CTS credentials state retrieval is not performed by the nonvolatile generation process (NVGEN) because the CTS credential information is saved in the keystore, not in the startup-config. The device can be assigned a CTS identity by the Cisco Secure Access Control Server (ACS), or auto-generate a new password when prompted to do so by the ACS. Those credentials are stored in the keystore, eliminating the need to save the running-config. To display the CTS 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 CTS device ID is changed, all Protected Access Credentials (PACs) are flushed from the keystore because the PACs are associated with the old device ID and are not valid for a new identity.

Examples

The following example configures himalaya and cisco as the CTS device ID and password:

```
Router# cts credentials id himalaya password cisco
```

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 changes the CTS device ID and password to atlas and cisco123:

```
Router# cts credentials id atlas password cisco123
```

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 example displays the CTS device ID and password state:

```
Router# show cts credentials
```

CTS password is defined in keystore, device-id = atlas

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

Use the **cts dot1x** command to enter CTS dot1x interface configuration mode (config-if-cts-dot1x) to configure the TrustSec reauthentication timer on an interface. 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 by default.				
Command Modes	Interface configuration (config-if)				
Supported User Roles	Administrator				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>12.2 (33) SXI3</td><td>This command was introduced on the Catalyst 6500 series switches.</td></tr> </table>	Release	Modification	12.2 (33) SXI3	This command was introduced on the Catalyst 6500 series switches.
Release	Modification				
12.2 (33) SXI3	This command was introduced on the Catalyst 6500 series switches.				
Usage Guidelines	Before configuring the TrustSec dot1x reauthentication timer, configure dot1x globally from the interface from the Interface Configuration mode. The CTS dot1x configuration governs TrustSec NDAC, not TrustSec EAC processes.				

Examples

In the following example, a Catalyst 6500 Series switch enters CTS configuration mode without first enabling dot1x in interface configuration mode:

```

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

Router(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 CTS dot1x reauthentication timer to the default value.
	timer reauthentication (cts interface)	Sets the CTS dot1x reauthentication timer.
	show cts interface	Displays CTS interface status and configurations.
	show dotx 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 CTS dot1x reauthentication timer to the default value.

default timer reauthentication

Syntax Description	timer reauthentication Sets the CTS reauthentication timer to the default values.	
Defaults	3600 seconds	
Command Modes	CTS interface configuration (config-if-cts-dot1x)	
Supported User Roles	Administrator	
Command History	Release	Modification
	12.2(33) SXI	This command was introduced on the Catalyst 6500 series switches.
Usage Guidelines	The default value of the CTS reauthentication timer is the global dot1x reauthentication default (3600 seconds). When this timer expires, the device reauthenticates to the CTS network (NDAC).	
Examples	The following example resets the CTS reauthentication timer to the global default values: <pre>Router # configure terminal Router(config)# interface gigabitEthernet 3/1 Router(config-if)# cts dot1x Router(config-if-cts-dot1x)# default timer reauthentication</pre>	
Related Commands	Command	Description
	cts dot1x	Enters CTS dot1x interface configuration mode (config-if-cts-dot1x).
	timer reauthentication (cts interface)	Sets the CTS reauthentication timer.
	show cts interface	Displays CTS interface status and configurations.
	show dotx 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 <i>seconds</i> Sets the reauthentication timer.	
Defaults	None	
Command Modes	CTS interface configuration (config-if-cts-dot1x)	
Supported User Roles	Administrator	
Command History	Release	Modification
	12.2(33) SXI	This command was introduced on the Catalyst 6500 series switches.
Usage Guidelines	This command sets the TrustSec reauthentication timer. When this timer expires, the device reauthenticates to the CTS network (NDAC).	
Examples	The following example sets the reauthentication timer to 44 seconds:	
	Router(config-if-cts-dot1x)# timer reauthentication 44	
Related Commands	Command	Description
	cts dot1x	Enters CTS dot1x interface configuration mode (config-if-cts-dot1x).
	default timer reauthentication (cts interface)	Resets the CTS dot1x reauthentication timer to the default value.
	show cts interface	Displays CTS interface status and configurations.
	show dotx interface	Displays IEEE 802.1x configurations and statistics.

cts layer3

Use the **cts layer 3** interface configuration command to enable CTS Layer3 Transport gateway interfaces, and to apply exception and traffic policies to them.

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

Syntax Description	ipv4 ipv6	Specify IPv4 or IPv6
	policy	Applies the traffic and exception policies on the gateway interface.
	trustsec forwarding	Enables CTS Layer3 Transport on the gateway interface.

Defaults CTS Layer3 Transport is not enabled by default.

Command Modes Interface configuration (config-if)

SupportedUserRoles Administrator

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

Usage Guidelines Use the **cts policy layer3** global configuration command to specify which traffic and exception commands to apply to the CTS Layer3 gateway. Use the **cts layer3** interface configuration command to enable the CTS Layer3 gateway interface and to apply the traffic and exception policies. See [cts policy layer3](#) for further information on traffic and exception policies.

Examples The following example enables a CTS Layer3 Transport gateway interface:

```
Router# config t
Router(config)# interface gigabitEthernet 6/1
Router(config-if)# cts layer3 ipv4 trustsec forwarding
Router(config-if)# cts layer3 ipv4 trustsec
Router(config-if)# cts layer3 ipv4 policy
```

Related Commands	Command	Description
	cts policy layer3	Specifies traffic and exception policies for CTS Layer 3 Transport.
	show cts policy layer3	Displays the name of traffic and exception polices used for CTS Layer3 Transport configurations.

cts manual

Use the **cts manual** interface configuration command to enter the TrustSec manual interface configuration submode.

cts manual

Syntax Description	There is no syntax for this command
---------------------------	-------------------------------------

Defaults	There is no default for this command.
-----------------	---------------------------------------

Command Modes	Interface configuration (config-if)
----------------------	-------------------------------------

SupportedUserRoles	Administrator
---------------------------	---------------

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

Usage Guidelines	Use the cts manual interface configuration command to enter the TrustSec manual interface configuration submode 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 mode is configured, 802.1X authentication is not performed on the link. Use the **policy** subcommand to define and apply policy on the link. The default is no policy. To configure MACsec link-to-link encryption, the SAP negotiation parameters must be defined. The default is no SAP. The same SAP PMK should be configured on both sides of the link (that is, a shared secret).

Examples	The following example demonstrates how to enter cts manual mode:
-----------------	--

```
router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# interface giga 2/1
router(config-if)# cts manual
router(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 interface configuration submode)	
sap (cts manual interface submode)	
show cts interface	

cts policy layer3

To specify traffic and exception policies for CTS Layer 3 Transport on a system when a Cisco Secure ACS is not available, use the **cts policy layer3** global configuration command.

```
[no] 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 ACL defining exceptions to the IPv4 L3 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 defining exceptions to the IPv6 L3 traffic policy.
	ipv6 traffic access_list Specifies an already defined ACL listing the IPv6 Trustsec-enabled subnets and gateways

Defaults No policy is the default.

Command Modes Global configuration (config)

Supported User Roles Administrator

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

Usage Guidelines The CTS Layer 3 Transport feature 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 CTS 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 not to apply the CTS Layer 3 Transport encapsulation. For example, the RADIUS packets used to acquire the policy should be sent in the clear.

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 CTS L3 gateway interface with the **cts layer3 {ipv4 | ipv6} policy** interface configuration command. Enable the CTS L3 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:

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

Related Commands

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

cts refresh

To refresh the TrustSec peer authorization policy and of all or specific CTS 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

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

Syntax Description	environment-data	Refreshes environment data.
	peer <i>Peer-ID</i>	(Optional). If a <i>peer-id</i> is specified, only the policies related to the specified peer connection are refreshed. To refresh all peer policies, press Enter without specifying an ID.
	sgt <i>sgt_number</i>	Performs an immediate refresh of the SGACL policies from the authentication server. If an SGT number is specified, only the policies related to that SGT are refreshed. To refresh all security group tag policies, press Enter without specifying an SGT number.
	default	Refreshes the default SGACL policy.
	unknown	Refreshes 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 refreshes the TrustSec peer authorization policy of all peers:

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

The following example 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
cts refresh	
clear cts policy	Clears all CTS policies, or singly by 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.

Syntax Description

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

Defaults

There is no default value.

Command Modes

Privileged EXEC (#)

Supported User Roles

Administrator

Command History

Release	Modification
12.2(50) SY	This command was introduced on the Catalyst 6500 Series Switches.
IOS-XE 3.3.0 SG	This command was introduced on the Catalyst 4500 Series Switches.
IOS 15.0(1) SE	This command was introduced on the 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** CTS manual interface configuration command.

Examples

The following example regenerates the PMK on the specified interface.

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

Related Commands

Command	Description
sap (cts manual interface submode)	
show cts	

cts role-based policy trace

To troubleshoot SGT and 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.
	<i>ip_port_num</i> 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 —Any Internet Protocol tcp —Transmission Control Protocol udp —User Datagram Protocol
	source_host <i>ip_address</i>	Specifies the IP address of the source host.

<i>protocol name wellknown_port_num</i>	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 <i>sg_name</i> sgt <i>sgt_num</i> }	Optional. Specifies the Security Group name or the Security Group Tag number.
vlan <i>vlan_id</i>	Optional. 0 to 4094. Specifies the VLAN identifier.
vrf <i>vrf_name</i>	Optional. Specifies the Virtual Routing and Forwarding instance name.

Command Default There are no defaults.

Command Modes Privileged EXEC

SupportedUserRoles Administrator

Command History	Release	Modification
	15.1(1)SY1	This feature was introduced on the 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, CDP 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 specifies 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 {ipv4_netaddress | ipv6_netaddress} | sgt sgt_number

[no] cts role-based sgt-map {ipv4_netaddress/prefix | ipv6_netaddress/prefix} | sgt sgt_number

[no] cts role-based sgt-map host {ipv4_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 <i>instance_name</i>		(Optional) Specifies Layer 2 VRF instance name.
enforcement		Enables SGACL enforcement on the local device for all Layer 3 CTS interfaces.
interface <i>interface_type</i>		The specified SGT is mapped to traffic from this logical or physical Layer 3 interface.
vlan-list <i>vlan-ids</i>		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 <i>ipv4_netaddress ipv6_netaddress</i>		(Optional) Specifies the network to be associated with an SGT. Enter IPv4 address in dot decimal notation; IPv6 in colon hexadecimal notation.

sgt-map <i>ipv4_netaddress/prefix</i> <i>ipv6_netaddress/prefix</i>	(Optional) Specifies that the SGT will be mapped 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 <i>ipv4_hostaddress</i> <i>ipv6_hostaddress</i>	Binds the specified host IP address with the specified SGT. Enter the IPv4 address in dot decimal notation; IPv6 in colon hexadecimal notation.
sgt <i>sgt_number</i>	(0–65,535). Specifies the Security Group Tag (SGT) number.
vrf <i>instance_name</i>	Specifies a VRF instance, previously created on the device.

Defaults

None

Command Modes

Global configuration (config)

Supported User Roles

Administrator

Command History

Release	Modification
12.2 (33) SXI3	This command was introduced on the Catalyst 6500 series switches.
12.2 (50) SG7	This command was introduced on the Catalyst 4000 series switches.
12.2 (53) SE2	This command was introduced on the 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 ARP inspection, DHCP snooping, or Host Tracking available to 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** *ipv4_netaddress* | *ipv6_netaddress* and **cts role-based sgt-map** *ipv4_subnetaddress/prefix* | *ipv6_subnetaddress/prefix* commands bind 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.

VRF to SGT Bindings

The **vrf** keyword specifies a Virtual Routing and Forwarding table previously defined with the **vrf definition** global configuration command. The configuration of VRF contexts is outside the scope of this document. 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.

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.

Binding Source Priorities

TrustSec resolves conflicts among IP-SGT binding sources in the master binding data-base 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}** cts interface 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 CTS 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.

L2 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 specified 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 SVI's VRF.

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 deconfigured. When reactivated, the IP-SGT bindings are moved back from the FIB table associated with the SVI's VRF 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 CTS-enabled Layer 3 interfaces in the system.



Note

The terms Role-based Access Control and Role-based ACLs that appear in the CTS 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 L3 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. Separate multiple entries with a hyphen “-” or a comma “,”.

The keyword **all** is equivalent to the full range of VLANs supported by the platform (For example, the Catalyst 6500 VLAN range is 1–4094). Issuing multiple commands has an additive effect. SGACLs are enforced on all the VLANs of all the lists specified. 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.

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. Use the **show flow** show commands to verify your configurations.

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, then verifies with a **show** command. These bindings will be forwarded by SXP to an SGACL enforcement switch.

```
cat4k# (config)# cts role-based sgt-map host 10.1.2.1 sgt 3
cat4k(config)#cts role-based sgt-map host 10.1.2.2 sgt 4
```

```
cat4k# 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, a Catalyst 6500 series includes VLAN 57, and 89 through 101 to VRF 12ipv4. The VRF was created with the **vrf** global configuration command.

```
Cat6k(config)# cts role-based 12-vrf 12ipv4 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 sgt-map	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 deadline *timer_secs*

[no] cts server key-wrap enable

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

[no] cts server test {*ip4_address* | **all**} {**deadline** *seconds* | **enable** | **idle-time** *minutes*}

Syntax Description

deadline <i>timer_secs</i>	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 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 <i>transactions</i>	(Optional) The number of transactions to be assigned per batch. The default <i>transactions</i> 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 try to use the same server throughout a session.
test { <i>ip4_address</i> all } { deadline <i>seconds</i> enable idle-time <i>minutes</i> }	Configures the server-liveliness test for a specified RADIUS server or for all servers on the dynamic server list. By default, the test is enabled for all servers. The default deadline is 20 seconds; the range is 1 to 864000 seconds. The default idle-time is 60 seconds; the range is from 1 to 14400 seconds.
key-wrap enable	Enables AES Key Wrap encryption for Trustsec RADIUS server communications.

Defaults

Deadtime	20 seconds
Batch-size	25 transactions
test idle-time	60 seconds

Command Modes Global configuration (config)

Supported User Roles Administrator

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

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

Information on RADIUS server load balancing is available at the following URL:
http://www.cisco.com/en/US/docs/ios/12_2sb/feature/guide/sbrldbl.html

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

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

```
Router# 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 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	<i>tag-number</i>	Configures the SGT for packets sent from this device. The <i>tag</i> argument is in decimal format. The range is 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 the Catalyst 6500 series switches.
	12.2 (50) SG7	This command was introduced on the Catalyst 4000 series switches.
	12.2 (53) SE2	This command was introduced on the Catalyst 3750(E) and 3560(E) series switches.
	12.2 (53) SE2	This command was introduced on the Catalyst 3750(X) series switches.

Usage Guidelines	In normal Cisco TrustSec operation, 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:
-----------------	---

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

Related Commands	Command	Description
	show cts environment-data	Displays the CTS environment data.

cts sxp

To configure SXP on a network device, use the **cts sxp** global configuration command. This command enables SXP, determines the SXP password, the peer speaker/listener relationship, and the reconciliation period. It also toggles the binding changes log on or off. Use the **no** form of the 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 <i>ip4_address</i>	Specifies the peer SXP address.
password { default none }	Specifies the password that SXP will use for the peer connection using the following options: default—Use the default SXP password you 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 <i>bindings</i>	0–65535. Maximum number of Subnet host address to SGT bindings permitted when expanding subnets for IP–SGT tagging and export. Enter 0 for no expansion.
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 <i>vrf_name</i>	(Optional) Specifies the VRF to the peer. Default is the default VRF.

default password 0 <i>unencrypted_pwd</i> 6 <i>encrypted_key</i> 7 <i>encrypted_key</i> <i>cleartext_pwd</i>	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 <i>ip4_address</i>	(Optional) Specifies the IPv4 address of the source device. If no address is specified, the connection will use 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	Turns on logging for IP to SGT binding changes. Default is off.
reconciliation period <i>seconds</i>	Changes the SXP reconciliation timer. The range is from 0 to 64000. Default is 120 seconds (2 minutes).
retry period <i>seconds</i>	Changes the SXP retry timer. The range is from 0 to 64000. Default value is 120 seconds (2 minutes).

Defaults

sxp	Disabled by default
log binding-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)

Supported User Roles

Administrator

Command History

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

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

Usage Guidelines

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 an SXP connection is configured per IP address, a device with many peers can have as 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 with the **0 | 7 | 6 encrypted_key** encryption type options. 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 where a source IP address is not specified. Pre-existing TCP connections are not affected when this command is entered. SXP connections are governed by three timers:

- Retry timer
- Delete Hold Down timer
- Reconciliation timer

Retry Timer

The Retry timer is triggered if there is 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 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 authorization and use the **clear cts counter** Privileged EXEC command.

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

Defaults None

Command Modes Privileged EXEC (#)

Supported User Roles Administrator

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

Examples The following example deletes environment data from cache:

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



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

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 the Catalyst 6500 series switches.

Usage Guidelines	The clear cts counter command clears the CTS 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 clears CTS statistics for GigabitEthernet interface 3/1, then confirms with the show cts interface command (a fragment of the show command output is displayed):
----------	--

```
Router# clear cts counter gigabitEthernet3/1
Router# 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 CTS interface status and configurations.

clear cts credentials

To delete the 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	<pre>Router# clear cts credentials Router# clear cts environment-data Router# 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</pre>	
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 the Catalyst 6500 series switches.

Examples	The following example clears environment data from cache: Router# clear cts environment-data
-----------------	--

Related Commands	Command	Description
	show cts environment-data	Displays the CTS environment data.

clear cts macsec

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

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

Syntax Description	interface type <i>slot/port</i>	Specifies the interface.
Command Modes	Privileged EXEC	
Supported User Roles	Administrator	
Command History	Release	Modification
	12.2(50) SY	This command was introduced on the Catalyst 6500 Series Switches.
Examples	The following example clears the counters on a gigabitEthernet interface on a Catalyst 6500 series switch: <pre>Router# clear cts macsec counters interface gigabitEthernet 6/2</pre>	
Related Commands	Command	Description
	show cts macsec	
	show cts interface	

clear cts pac

To clear 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 <i>hexstring</i>	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 (#)
---------------	---------------------

Supported User Roles	Administrator
----------------------	---------------

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

Examples	The following command clears all PACs in the keystore: Router# 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 TrustSec peer, use the the **clear cts policy** command in privileged EXEC mode.

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

Syntax Description	peer <i>peer_id</i>	Specifies the peer ID of the TrustSec peer device.
	sgt <i>sgt</i>	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 the Catalyst 6500 series switches.

Usage Guidelines

ExamplesTo 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. Use the **show cts policy peer** command to verify.

The following example clears the peer authorization policy of the TrustSec peer with the peer ID atlas2:

```
Router# clear cts policy peer atlas2
Delete all peer policies? [confirm] y
Router#
```

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 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	Default policy counters
from	Specifies the source security group
ipv4	Specifies security groups on IP version 4 networks
ipv6	Specifies security groups on IP version 6 networks
to	Specifies the destination security group
sgt_num	(0–65533) Specifies the Security Group Tag number
unknown	Specifies all Source Groups

Command Modes

EXEC (>); Privileged EXEC (#)

Supported User Roles

Administrator

Command History

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

Usage Guidelines

Use the **clear cts role-based counters** command to clear the Security Group ACL (SGACL) enforcement counters within the scope you specify. The **show cts role-based counters** tabulates the statistics accumulated since the last clear command was issued, as shown in [Example 7-1](#).

Example 7-1 Tabulated SGACL Output from show role-based counters

```
router# 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
```

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.

When neither **ipv4** nor **ipv6** are specified the command clears only IPv4 counters.

Examples

The following example clears all role-based counters compiling statics for SGACL enforcements on IPv4 traffic:

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

Related Commands

clear cts server

To remove a server from the CTS AAA server list, use the **clear cts server** command.

clear cts server *ip_address*

Syntax Description	<i>ip_address</i>	IPv4 address of the AAA server to be removed from the server list.
Command Modes	Privileged EXEC (#)	
Supported User Roles	Administrator	
Command History	Release	Modification
	12.2(33) SXI	This command was introduced on the Catalyst 6500 Series Switches.
Usage Guidelines	This command removes a server from the list of CTS AAA servers configured with the cts authorization list global configuration command, or the AAA server list provisioned by the CTS authenticator peer.	
Examples	The following example removes the AAA server 10.10.10.1 from the CTS AAA server list. <pre>router# clear cts server 1.1.1.1</pre>	
Related Commands	Command	Description
	show cts server-list	
	cts server	

default (cts dot1x interface configuration submode)

To restore any of the **cts dot1x** configurations to their default values, use the **default** command in CTS dot1x interface configuration submode.

default propagate sgt

default sap

default timer reauthentication

Syntax Description	propagate sgt	Restores default to enabled for propagate sgt.
	sap	Restores default to sap modelist gcm-encrypt null .
	timer	Restores default 86,400 seconds for the dot1x reauthentication period.

Defaults There is no default for this command.

Command Modes CTS dot1x interface configuration submode (config-if-cts-dot1x)

SupportedUserRoles Administrator

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

Examples The following example re-enables SGT propagation:

```
router# config t
router(config)# interface gigabit 6/1
router(config-if)# cts dot1x
router(config-if-cts-dot1x)# default propagate sgt
```

Related Commands	Command	Description
	propagate (cts dot1x submode)	Enables/disables SGT propagation in dot1x mode.
	sap (cts dot1x interface submode)	Configures CTS SAP for dot1x mode.
	timer (cts dot1x interface submode)	Configures the CTS timer.

debug condition cts

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

```
[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 SGN to match.
	tag tag_number	Specifies the SGT to match.

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

SupportedUserRoles	Administrator
--------------------	---------------

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

Usage Guidelines

Enabling any of the **debug cts** commands returns debugging messages for the specified cts service for all TrustSec links to the device. The **debug condition cts** command can filter those 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 non-cts 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 will be 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 interface configuration submode)

To restore any of the **cts manual** configurations to their default values, use the **default** command in CTS manual interface configuration submode.

- 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 ingress traffic.
	policy propagate sgt	Specifies SGT propagation mode of On.
	sap	Specifies default SAP values. (GCM-Encrypt, null)

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

SupportedUserRoles	Administrator
--------------------	---------------

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

Usage Guidelines	To restore the CTS manual interface configuration submode parameters to default values, use the default subcommand.
------------------	--

Examples	The following example restores the default dynamic policy and SGT propagation policies of a Catalyst 6500 series switch CTS-enabled interface: <pre> router# config t router(config)# interface gigbitEthernet 6/1 router(config-if)# cts manual router(config-if-cts-manual)# default policy dynamic identity router(config-if-cts-manual)# default propagate sgt </pre>
----------	---

Related Commands	Command	Description
	policy (cts manual interface configuration submode)	Configures CTS policy for manual mode
	sap (cts manual interface submode)	Configures CTS SAP for manual mode.

match flow cts

To add the Cisco TrustSec flow objects to a Flexible NetFlow flow record, use the **match flow cts** record configuration 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	There are no defaults for this command.
-----------------	---

Command Modes	Flexible NetFlow record configuration (config-flow-record)
----------------------	--

SupportedUserRoles	Administrator
---------------------------	---------------

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

Usage Guidelines	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 to add them to a flow monitor. Use the show flow show commands to verify your configurations..
	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 Catalyst 6500 Release 12.2SY Software Configuration Guide http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/netflow_hw_support.html

Examples

The following example configures an IPv4 Flow Record (5-tuple, direction, SGT, DGT):

```
router(config)# flow record cts-record-ipv4
router(config-flow-record)# match ipv4 protocol
router(config-flow-record)# match ipv4 source address
router(config-flow-record)# match ipv4 destination address
router(config-flow-record)# match transport source-port
router(config-flow-record)# match transport destination-port
router(config-flow-record)# match flow direction
router(config-flow-record)# match flow cts source group-tag
router(config-flow-record)# match flow cts destination group-tag
router(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** global config command. 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	The default is no ingress or egress reflector.
----------	--

Command Modes	Global configuration (config)
---------------	-------------------------------

Supported User Roles	Administrator
----------------------	---------------

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

Examples	The following example enables the CTS ingress reflector on a Catalyst 6500 switch: switch(config)# platform cts egress
	The following example disables the CTS 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 interface configuration submode)

To apply a policy to a manually configured TrustSec link, use the **policy** interface manual submode command. 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 <i>peer_deviceID</i>	The peer device name or symbolic name in the authentication server's policy database associated with the policy to be applied to the peer.
static	Specifies an SGT policy to incoming traffic on the link.
sgt <i>sgt_number</i>	Security Group Tag number to apply to incoming traffic from peer.
trusted	Indicates that ingress traffic on the interface with the SGT specified in the command, should not have its SGT overwritten. Untrusted is the default.

Defaults

No policy is the default.

Command Modes

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

Supported User Roles

Administrator

Command History

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

Usage Guidelines

Use the **policy** command to apply policy when manually configuring a TrustSec link. The default is **no policy** which passes all traffic through without applying an SGT. The **sap** cts manual mode subcommand 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's SGT assignment trust state, RBACLs for the associated peer SGT and 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 applies an 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):

```
Router# configure terminal
Router(config)# interface gi2/1
Router(config-if)# cts manual
Router(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm null no-encap
Router(config-if-cts-manual)# policy static sgt 3 trusted
Router(config-if-cts-manual)# exit
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

```
Router# 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 interface configuration submode)	Restores default configurations for CTS manual mode.
policy (cts manual interface configuration submode)	Configures CTS policy for manual mode.
sap (cts manual interface submode)	Configures CTS SAP for manual mode.

propagate (cts dot1x submode)

To enable and disable the SGT propagation on a Cisco TrustSec interface, use the `propagate sgt` command in CTS dot1x interface configuration submode.

[no] propagate sgt

Syntax Description	sgt	Specifies CTS SGT propagation.
---------------------------	------------	--------------------------------

Defaults	.SGT propagation is enabled by default in CTS dot1x and CTS manual interface configuration submodes.
-----------------	--

Command Modes	CTS Dot1x interface configuration submode (config-if-cts-dot1x)
----------------------	---

SupportedUserRoles	Administrator
---------------------------	---------------

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

Usage Guidelines	SGT propagation (SGT tag encapsulation) is enabled by default in both CTS dot1x and CTS manual interface configuration submodes. 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 disables SGT propagation on a TrustSec-capable interface:
-----------------	---

```

router(config) interface gigabit 6/1
router(config-if) cts dot1x
router(config-if-cts-dot1x)# no propagate sgt

router# show cts interface gigabit 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 interface submode)	Configures CTS SAP for dot1x mode.
timer (cts do1x interface submode)	Configures the CTS timer.

To enable and disable an interface's ability to propagate a Security Group Tag on a interface, use the **cts propagate** cts interface manual configuration submode command.

Syntax Description	sgt	Specifies the Security Group Tag
---------------------------	-----	----------------------------------

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

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

A TrustSec-capable interface can support MACsec (Layer2 802.1AE security) and SGT tagging. A TrustSec-capable interface attempts to negotiate the most secure mode with its peer. The peer may be capable of MACsec but not capable of SGT processing. In a manual CTS interface configuration, disable the SGT propagation on the CTS-capable interface if you are only implementing the MACsec feature.

[illegible]

Related Commands	Command	Description
	show cts interface	Displays Cisco TrustSec states and statistics per interface.
	show running-config	Displays current system configurations.

sap (cts dot1x interface submode)

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 the 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 advertised SAP authentication and encryption modes (prioritized from highest to lowest)
	gcm-encrypt	Specifies GMAC authentication, GCM encryption
	gmac	Specifies GMAC authentication only, no encryption
	no-encap	Specifies no encapsulation
	null	Specifies encapsulation present, no authentication, no encryption

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 dot1x interface submode(config-if-cts-dot1x)

SupportedUserRoles Administrator

Command History	Release	Modification
	12.2(50) SY	This command was introduced on the Catalyst 6500 Series Switches.
	IOS-XE 3.3.0 SG	This command was introduced on the Catalyst 4500 Series Switches.
	IOS 15.0(1) SE	This command was introduced on the 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.

Before the SAP exchange begins after a Dot1x authentication, both sides (supplicant and authenticator) have received 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 CTS-aware software but the hardware is not CTS-capable, disallow encapsulation with the **sap modelist no-encap** command.

Use the **timer reauthentication** command to configure the reauthentication period to be applied to the CTS 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 multi-hosts mode. The authenticator PAE starts only when **dot1x system-auth-control** is enabled globally.

Examples

The following example specifies that SAP is to negotiate the use of CTS encapsulation with GCM cipher, or null-cipher as a second choice, but can accept no CTS encapsulation if the peer does not support CTS encapsulation in hardware.

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

Related Commands

Command	Description
propagate (cts dot1x submode)	Enables/disables SGT propagation in dot1x mode.
sap (cts dot1x interface submode)	Configures CTS SAP for dot1x mode.
timer (cts dot1x interface submode)	Configures the CTS timer.

sap (cts manual interface submode)

Use the **sap mode-list** 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 revert to the default.

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

Syntax Description	pmk <i>hex_value</i>	Hex-data PMK (without leading 0x; enter even number of hex chars else last char prefixed with 0)
	modelist	List of advertised modes (prioritized from highest to lowest)
	gcm-encrypt	Specifies GCM authentication, GCM encryption
	gmac	Specifies GCM authentication, no encryption
	no-encap	Specifies no encapsulation
	null	Specifies encapsulation present, no authentication, no encryption

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 submode (config-if-cts-manual)

SupportedUserRoles Administrator

Command History	Release	Modification
	12.2(50) SY	This command was introduced on the Catalyst 6500 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, the 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 a SAP configuration for a Gigabit Ethernet interface:

```

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

```

Related Commands	Command	Description
	default (cts manual interface configuration submode)	Restores default configurations for CTS manual mode.
	policy (cts manual interface configuration submode)	Configures CTS policy for manual mode
	propagate (cts manual interface configuration submode)	Configures CTS 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** Privileged EXEC command.

```

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 CTS authentication.	
environment-data	Displays the CTS environment data.	
interface	Displays CTS 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 CTS policy.	
provisioning	Displays outstanding CTS provisioning jobs.	
role-based	Displays Role-based Access Control information (SGACL information).	

server-list	Displays the CTS server lists.
sxp	Displays CTS 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 the Catalyst 6500 series switches.
	12.2(50) SY	The following keywords were added for Catalyst 6500 series switches:

Examples

The following is an example of **show cts** entered without keywords:

```
Router# 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
```

show cts

Related Commands

Command	Description
cts credentials	Specifies the TrustSec ID and password.

show cts authorization entries

To display TrustSec NDAC authorization entries, use the **show cts authorization entries** command in EXEC or privileged EXEC mode.

show cts authorization entries

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

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

Command Modes	EXEC (>); Privileged EXEC (#)
----------------------	-------------------------------

SupportedUserRoles	Administrator
---------------------------	---------------

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

Examples	The following example is show command output from a Catalyst 6500 switch:
-----------------	--

```

router# show cts authorization entries
Authorization Entries Info
  Peer-name           = annapurna
  Peer-SGT            = 7-1F05D8C1
  Entry State         = COMPLETE
  Entry last refresh   = 01:19:37 UTC Sat Dec 8 2007
  Session queue size   = 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 queue size = 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)

```

show cts authorization entries

```
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 EXEC or privileged EXEC mode.

show cts credentials

Syntax Description	This command has no commands or keywords.
---------------------------	---

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

Command Modes	EXEC (>); Privileged EXEC (#)
----------------------	-------------------------------

SupportedUserRoles	Administrator
---------------------------	---------------

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

Examples	Router# 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 EXEC or privileged EXEC mode.

show cts environment-data

Syntax Description	This command has no commands or keywords.	
Defaults	None	
Command Modes	EXEC (>); Privileged EXEC (#)	
SupportedUserRoles	Administrator	
Command History	Release	Modification
	12.2(33) SXI	This command was introduced on the Catalyst 6500 series switches.

Examples	The following example displays the environment data of a Cisco Catalyst 6500 series switch. <pre> Router# 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 </pre>
----------	---

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

show cts interface

To display TrustSec configuration statistics, use the **show cts interface** command in 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 status output for this interface is returned.
	brief	(Optional) Displays abbreviated status for all CTS interfaces.
	summary	(Optional) Displays a tabular summary of all CTS interfaces with 4 or 5 key status fields for each interface.

Defaults None

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

SupportedUserRoles Administrator

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

Usage Guidelines Use the **show cts interface** command without keywords to display verbose status for all CTS interfaces.

Examples The following example displays output without using a keyword (verbose status for all CTS interfaces):

```
Router# 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 example displays output using the **brief** keyword:

```
Router# 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 example displays output using the **summary** keyword:

```
Router# show cts interface summary
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache  Dot1x
-----
Gi4/1      DOT1X   OPEN      Authent   r1         invalid    enabled
```

Related Commands

Command	Description
cts sxp	Configures SXP on a network device.

show cts macsec

To display crypto ASIC packet counters per interface related to CTS link-to-link encryption, 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 CTS MACsec interface.
	delta	Displays counter values since the last time cleared.
Command Modes	EXEC (>); Privileged EXEC (#)	
SupportedUserRoles	Administrator	
Command History	Release	Modification
	12.2(50) SY	This command was introduced on the Catalyst 6500 Series Switches.
Usage Guidelines	This command displays the crypto ASIC packet counters per interface. If Security Associations (SA) are installed (through NDAC or sap cts interface do1x or manual subcommands), the active SA's 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 since the clear cts macsec counters interface command was issued.	
Examples	The following example displays the MACsec counters of a manually configured CTS uplink interface on a Catalyst 6500 series switch: <pre> router# 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 </pre>	

show cts macsec

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

Related Commands	Command	Description
	show cts interface	
	sap (cts dot1x interface submode)	
	sap (cts manual interface submode)	

show cts pacs

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

show cts pacs

Syntax Description	This command has no commands or keywords.
---------------------------	---

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

Command Modes	EXEC (>); Privileged EXEC (#)
----------------------	-------------------------------

SupportedUserRoles	Administrator
---------------------------	---------------

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

Usage Guidelines	Use this command to identify the NDAC authenticator and to verify NDAC completion.
-------------------------	--

Examples	The following example displays the Protected Access Credential (PAC) received from a Cisco ACS with the authenticator ID (A-ID-Info) of acs1 by the device named atlas:
-----------------	---

```
Router# show cts pacs
AID: 1100E046659D4275B644BF946EFA49CD
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: 1100E046659D4275B644BF946EFA49CD
  I-ID: atlas
  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
```

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 CTS Layer3 Transport configurations, use the **show cts policy layer3** command in 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	EXEC (>); Privileged EXEC (#)
---------------	-------------------------------

SupportedUserRoles	Administrator
--------------------	---------------

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

Usage Guidelines	A traffic or exception policy may be configured locally, or obtained from the Cisco Secure ACS. See the section, “ cts policy layer3 ” for additional information on the CTS Layer3 Transport feature.
------------------	--

Examples	The following example displays the output of the show cts policy3 command:
----------	---

```
router# 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 CTS Layer 3 Transport.
	cts layer3	Enables and applies traffic and exception policies to CTS Layer 3 Transport gateway interfaces.

show cts policy peer

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

show cts policy peer

Syntax Description This command has no commands or keywords.

Defaults None

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

SupportedUserRoles Administrator

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

Examples The following example displays the 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
```

Output Field	Explanation
Peer name	CTS device-id of the peer to which the local device is connected.
Peer SGT	The Security Group Tag of the peer.
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

show cts policy peer

Output Field	Explanation
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

Use the **show cts provisioning** command in EXEC or Privileged EXEC mode to display waiting RADIUS server CTS provisioning jobs.

show cts provisioning

Syntax Description	This command has no commands or keywords.
---------------------------	---

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

Command Modes	EXEC (>); Privileged EXEC (#)
----------------------	-------------------------------

SupportedUserRoles	Administrator
---------------------------	---------------

Command History

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

Examples	The following output displays a list of AAA servers that the CTS provisioning driver is re-trying for PAC-provisioning:
-----------------	---

```
router# 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 role-based counters

To display Security Group ACL enforcement statistics, use the **show cts role-based** counters show command. 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	Default policy counters
	from	Specifies the source security group
	ipv4	Specifies security groups on IP version 4 networks
	ipv6	Specifies security groups on IP version 6 networks
	to	Specifies the destination security group
	sgt_num	(0–65533) Specifies the Security Group Tag number
	unknown	Specifies all Source Groups

Command Modes	EXEC (>); Privileged EXEC (#)
---------------	-------------------------------

SupportedUserRoles	Administrator
--------------------	---------------

Command History	Release	Modification
	12.2(50) SY	This command was introduced on the 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 example displays all enforcement statistics for IPv4 and IPv6 events:

```
router# 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 Security Group Tag (SGT) on either a host or a VRF as well as enabling SGACL enforcement.

show cts role-based sgt-map

To display the SXP source IP to SGT bindings table (IP-SGT bindings), use the **show cts role-based sgt-map** command in 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		
	<i>ipv4_dec</i>	Specifies an IPv4 address in dot-decimal notation. For example (208.77.188.166)
	<i>ipv4_cidr</i>	Specifies an IPv4 address range in Classless Inter-Domain Routing (CIDR) For example, 35.0.0.0/8, where the /8 signifies that the 8 most significant bits identify the networks, and the 24 least-significant bits, the hosts.
	<i>ipv6_hex</i>	Specifies an IP version 6 address in hexadecimal separated by colons. For example, 2001:db8:85a3::8a2e:370:7334.
	<i>ipv6_cidr</i>	Specifies a range of IPv6 address in hexadecimal CIDR notation.
	host <i>ipv4_decimal</i> <i>ipv6_hex</i>	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 <i>instance_name</i>	Specify a VPN Routing/Forwarding instance for mappings.

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

Command Modes	EXEC (>); Privileged EXEC (#)
----------------------	-------------------------------

Supported User Roles	Administrator
-----------------------------	---------------

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

Usage Guidelines

Use this command to verify that SXP is correctly binding source IP addresses to the appropriate Security Group Tags (SGTs). VRF reports are available only from Privileged EXEC mode.

Examples

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

```
Router# show cts role-based sgt-map all
Active IP-SGT Bindings Information

IP Address      SGT Source
=====
1.1.1.1         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 maps a source IP address to a Security Group Tag (SGT).
cts sxp	Configures SXP on a network device.
show cts sxp	Displays CTS SXP protocol information

show cts server-list

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

show cts server-list

Syntax Description	This command has no commands or keywords.
Defaults	None
Command Modes	EXEC (>); Privileged EXEC (#)
SupportedUserRoles	Administrator

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

Examples	The following example displays the TrustSec RADIUS server list: <pre>Router> 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</pre>
----------	--

Related Commands	Command	Description
	cts server	Displays CTS server list configuration.

show cts sxp

To display SXP connection or SourceIP-to-SGT mapping information, use the **show cts sxp** command in EXEC or privileged EXEC mode.

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

Syntax Description	connections	Displays CTS SXP connections information.
	sgt-map	Displays the IP-SGT mappings received through SXP.
	brief	(Optional) Displays an abbreviation of the SXP information.
	vrf <i>instance_name</i>	(Optional) Displays the SXP information for the specified VRF instance name.

Defaults None

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

Supported User Roles Administrator

Command History	Release	Modification
	12.2(33) SXI	This command was introduced on the Catalyst 6500 series switches.
	12.2 (50) SG7	This command was introduced on the Catalyst 4000 series switches
	12.2 (53) SE2	This command was introduced on the Catalyst 3750(E) and 3560(E) series switches.
	12.2 (53) SE2	This command was introduced on the 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 SourceIP-to-SGT mapping database.

Examples The following example displays the default SXP configuration on a Catalyst 6500 series switch:

```
Router# 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 example displays the SXP connections on a Catalyst 6500 switch using the **brief** keyword:

```
Router# 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 example displays the SXP connections on a Catalyst 6500 series switch:

```
Router# 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 example displays output from an SXP listener with a torn down connection to the SXP speaker. SourceIP-to-SGT mappings are held for 120 seconds, the default value of the Delete Hold Down timer.

```
Router# 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 example displays the current SourceIP-to-SGT mapping database learned through SXP:

```

router# show cts sxp sgt-map
IP-SGT Mappings as follows:
IPv4,SGT: <2.2.2.1 , 7>
source   : SXP;
Peer IP  : 2.2.2.1;
Ins Num  : 1;
IPv4,SGT: <2.2.2.1 , 7>
source   : SXP;
Peer IP  : 3.3.3.1;
Ins Num  : 1;
Status   : Active;
IPv4,SGT: <3.3.3.1 , 7>
source   : SXP;
Peer IP  : 2.2.2.1;
Ins Num  : 1;

```

The following example displays the current SourceIP-to-SGT mapping database using the **brief** keyword:

```

Router# show cts sxp sgt-map brief
IP-SGT Mappings as follows:
IPv4,SGT: <2.2.2.1 , 7>
IPv4,SGT: <3.3.3.1 , 7>
IPv4,SGT: <4.4.4.1 , 7>
IPv4,SGT: <43.13.21.41 , 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 EXEC or privileged EXEC mode.

show cts keystore

Syntax Description This command has no commands or keywords.

Defaults None

Command Modes 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 .

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

Examples The following example displays the contents of a Catalyst 6500 software emulated keystore:

```
Router# 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 example displays the contents of a Catalyst 6500 hardware keystore:

```
Router# 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 Commands

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 CTS) on a specific interface, use the **show platform cts reflector** command.

```
show platformcts 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 the Catalyst 6500 Series Switches.

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

timer (cts do1x interface submode)

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

[no] timer reauthentication *seconds*

Syntax Description	reauthentication <i>seconds</i> (0–2147483) Timer in seconds. Enter 0 to disable dot1x reauthentication.	
Defaults	The default period is 86,400 seconds (24 hours).	
Command Modes	CTS dot1x interface configuration submode (config-if-cts-dot1x)	
Supported User Roles	Administrator	
Command History	Release	Modification
	12.2(33) SXI	This command was introduced on the Catalyst 6500 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 period 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 sets the 802.1X reauthentication period for 48 hours (17, 2800 seconds): <pre> router# config t router(config)# interface gigabitEthernet 6/1 router(config-if)# cts dot1x router(config-if-cts-dot1x)# timer reauthentication 172800 </pre>	
Related Commands	Command	Description
	show cts interface	Displays Cisco TrustSec states and statistics per interface.
	sap (cts dot1x interface submode)	Configures CTS SAP for dot1x mode.
	propagate (cts dot1x submode)	Enables/disables SGT propagation in dot1x mode.

■ timer (cts do1x interface submode)