Cisco TrustSec Switch Configuration Guide

For Cisco Catalyst Switches

Updated: July 28, 2016

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: OL-22192-02

Cisco TrustSec Switch Configuration Guide

Preface

Revised: October 16, 2013, OL-22192-02

Organization

This guide includes the following chapters and appendixes:

Chapter or Appendix Title	Description
Chapter 1, “Cisco TrustSec Overview”	Describes the elements and processes that create the Cisco TrustSec network.
Chapter 2, “Configuring the Cisco TrustSec Solution”	Provides an overview of configuration tasks required to implement a Cisco TrustSec Network.
Chapter 3, “Configuring Identities, Connections, and SGTs”	Provides NDAC and TrustSec seed device configuration procedures.
Chapter 4, “Configuring SGACL Policies”	Provides Security Group ACL configuration procedures from the switch CLI.
Chapter 5, “Cisco TrustSec SGACL High Availability,”	Provides information about the SGACLs high availability functionality in switches that support the Cisco StackWise technology. This technology provides stateful redundancy and allows a switch stack to enforce and process access control entries.
Chapter 6, “Configuring SGT Exchange Protocol”	Provides SGT over TCP Protocol (SXP) configuration procedures.
Chapter 7, “Cisco TrustSec VRF-Aware SGT,”	Provides information about the Cisco TrustSec VRF-Aware SGT feature that binds an SXP connection with a VRF instance.
Chapter 11, “Configuring Endpoint Admission Control”	Provides 802.1X, MAB, and WebAuth configuration procedures for a TrustSec context.
Chapter 12, “Cisco TrustSec Command Summary”	Provides a list of Cisco TrustSec CLI commands with brief descriptions.

Chapter or Appendix Title	Description
Appendix A, "Notes for Catalyst 3000 and 2000 Series Switches and Wireless LAN Controller 5700 Series"	Describes constraints, limitations, or considerations pertaining to TrustSec implementation of Catalyst 3000 and 2000 Series Switches and WLC 5700 Series Wireless LAN Controllers.
Appendix B, "Notes for Catalyst 4500 Series Switches"	Describes constraints, limitations, or considerations pertaining to TrustSec implementation of Catalyst 4500 Series Switches.
Appendix C, "Notes for Catalyst 6500 Series Switches"	Describes constraints, limitations, or considerations pertaining to TrustSec implementation of Catalyst 6500 Series Switches.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem.*

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

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Cisco TrustSec Overview

Revised: September 02, 2015

This chapter contains the following topics:

Restrictions for Cisco TrustSec

- Protected access credential (PAC) provisioning fails and remains in hung state, when an invalid device ID is specified. Even after clearing the PAC, and configuring the correct device ID and password, PAC still fails.
  As a workaround, in the Cisco Identity Services Engine (ISE), uncheck the Suppress Anomalous Clients option in the Administration> System> Settings> Protocols> Radius menu for PAC to work.

Information About Cisco TrustSec Architecture

The Cisco TrustSec security architecture builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and data-path replay protection mechanisms. Cisco TrustSec uses the device and user credentials acquired during authentication for classifying the packets by security groups (SGs) as they enter the network. This packet classification is maintained by tagging packets on ingress to the Cisco TrustSec network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, called the security group tag (SGT), allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic.

Note Cisco TrustSec IEEE 802.1X links are not supported on platforms supported in the Cisco IOS XE Denali and Everest releases, and hence only the Authenticator is supported; the Supplicant is not supported.

The Cisco TrustSec architecture incorporates three key components:

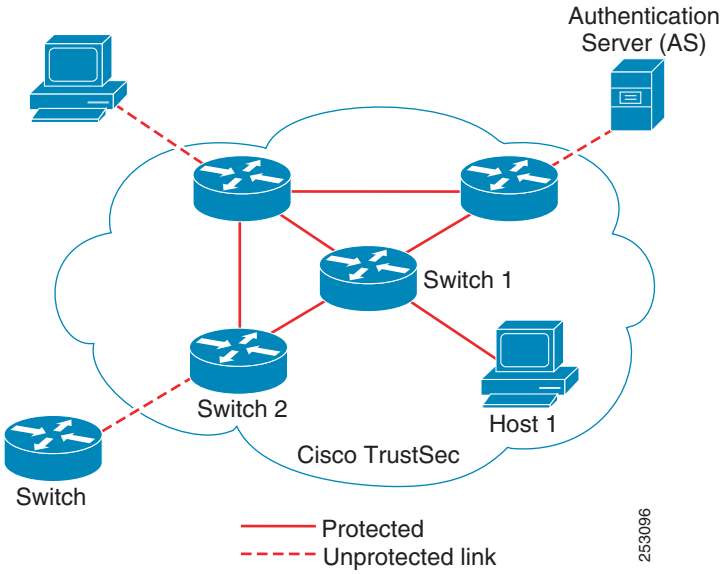
- Authenticated networking infrastructure—After the first device (called the seed device) authenticates with the authentication server to begin the Cisco TrustSec domain, each new device added to the domain is authenticated by its peer devices already within the domain. The peers act as

intermediaries for the domain's authentication server. Each newly-authenticated device is categorized by the authentication server and assigned a security group number based on its identity, role, and security posture.

- Security group-based access control—Access policies within the Cisco TrustSec domain are topology-independent, based on the roles (as indicated by security group number) of source and destination devices rather than on network addresses. Individual packets are tagged with the security group number of the source.
- Secure communication—With encryption-capable hardware, communication on each link between devices in the domain can be secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms.

Figure 1-1 shows an example of a Cisco TrustSec domain. In this example, several networking devices and an endpoint device are inside the Cisco TrustSec domain. One endpoint device and one networking device are outside the domain because they are not Cisco TrustSec-capable devices or because they have been refused access. The authentication server is considered to be outside of the Cisco TrustSec domain; it is either a Cisco Identities Service Engine (Cisco ISE), or a Cisco Secure Access Control System (Cisco ACS).

Figure 1-1 Cisco TrustSec Network Domain Example



Each participant in the Cisco TrustSec authentication process acts in one of the following roles:

- Supplicant—An unauthenticated device connected to a peer within the Cisco TrustSec domain, and attempting to join the Cisco TrustSec domain.
- Authentication server—The server that validates the identity of the supplicant and issues the policies that determine the supplicant's access to services within the Cisco TrustSec domain.

- Authenticator—An authenticated device that is already part of the Cisco TrustSec domain and can authenticate new peer supplicants on behalf of the authentication server.

When the link between a supplicant and an authenticator first comes up, the following sequence of events typically occurs:

1. Authentication (802.1X)—The supplicant is authenticated by the authentication server, with the authenticator acting as an intermediary. Mutual authentication is performed between the two peers (supplicant and authenticator).
2. Authorization—Based on the identity information of the supplicant, the authentication server provides authorization policies, such as security group assignments and ACLs, to each of the linked peers. The authentication server provides the identity of each peer to the other, and each peer then applies the appropriate policy for the link.
3. Security Association Protocol (SAP) negotiation—When both sides of a link support encryption, the supplicant and the authenticator negotiate the necessary parameters to establish a security association (SA).

When all three steps are complete, the authenticator changes the state of the link from the unauthorized (blocking) state to the authorized state, and the supplicant becomes a member of the Cisco TrustSec domain.

Cisco TrustSec uses ingress tagging and egress filtering to enforce access control policy in a scalable manner. Packets entering the domain are tagged with a security group tag (SGT) containing the assigned security group number of the source device. This packet classification is maintained along the data path within the Cisco TrustSec domain for the purpose of applying security and other policy criteria. The final Cisco TrustSec device on the data path, either the endpoint or network egress point, enforces an access control policy based on the security group of the Cisco TrustSec source device and the security group of the final Cisco TrustSec device. Unlike traditional access control lists based on network addresses, Cisco TrustSec access control policies are a form of role-based access control lists (RBACLs) called security group access control lists (SGACLs).

Note Ingress refers to packets entering the first Cisco TrustSec-capable device encountered by a packet on its path to the destination and egress refers to packets leaving the last Cisco TrustSec-capable device on the path.

Authentication

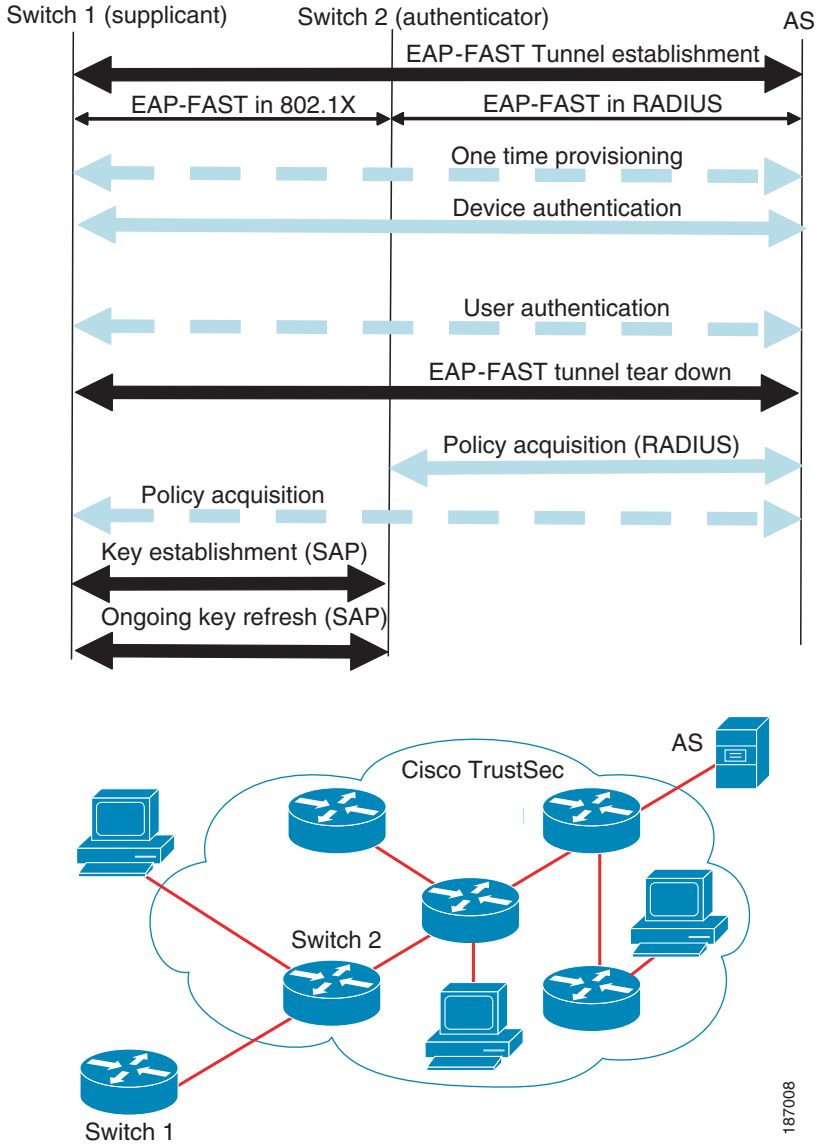
This section includes the following topics:

Cisco TrustSec and Authentication

Using Network Device Admission Control (NDAC), Cisco TrustSec authenticates a device before allowing it to join the network. NDAC uses 802.1X authentication with Extensible Authentication Protocol Flexible Authentication via Secure Tunnel (EAP-FAST) as the Extensible Authentication Protocol (EAP) method to perform the authentication. EAP-FAST conversations provide for other EAP method exchanges inside the EAP-FAST tunnel using chains. Administrators can use traditional

user-authentication methods, such as Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2), while still having security provided by the EAP-FAST tunnel. During the EAP-FAST exchange, the authentication server creates and delivers to the supplicant a unique protected access credential (PAC) that contains a shared key and an encrypted token to be used for future secure communications with the authentication server. Figure 1-2 shows the EAP-FAST tunnel and inner methods as used in Cisco TrustSec.

Figure 1-2 Cisco TrustSec Authentication



This section includes the following topics:

Cisco TrustSec Enhancements to EAP-FAST

The implementation of EAP-FAST for Cisco TrustSec has the following enhancements:

- Authenticate the authenticator—Securely determines the identity of the authenticator by requiring the authenticator to use its PAC to derive the shared key between itself and the authentication server. This feature also prevents you from configuring RADIUS shared keys on the authentication server for every possible IP address that can be used by the authenticator.
- Notify each device of the identity of its peer—By the end of the authentication exchange, the authentication server has identified both the supplicant and the authenticator. The authentication server conveys the identity of the authenticator, and whether the authenticator is Cisco TrustSec-capable, to the supplicant by using additional type-length-value parameters (TLVs) in the protected EAP-FAST termination. The authentication server also conveys the identity of the supplicant, and whether the supplicant is Cisco TrustSec-capable, to the authenticator by using RADIUS attributes in the Access- Accept message. Because each device knows the identity of its peer, it can send additional RADIUS Access-Requests to the authentication server to acquire the policy to be applied on the link.

802.1X Role Selection

In 802.1X, the authenticator must have IP connectivity with the authentication server because it has to relay the authentication exchange between the supplicant and the authenticator using RADIUS over UDP/IP. When an endpoint device, such as a PC, connects to a network, it is obvious that it should function as a supplicant. However, in the case of a Cisco TrustSec connection between two network devices, the 802.1X role of each network device might not be immediately apparent to the other network device.

Instead of requiring manual configuration of the authenticator and supplicant roles for two adjacent switches, Cisco TrustSec runs a role-selection algorithm to automatically determine which switch functions as the authenticator and which functions as the supplicant. The role-selection algorithm assigns the authenticator role to the switch that has IP reachability to a RADIUS server. Both switches start both the authenticator and supplicant state machines. When a switch detects that its peer has access to a RADIUS server, it terminates its own authenticator state machine and assumes the role of the supplicant. If both switches have access to a RADIUS server, the first switch to receive a response from the RADIUS server becomes the authenticator and the other switch becomes the supplicant.

Cisco TrustSec Authentication Summary

By the end of the Cisco TrustSec authentication process, the authentication server has performed the following actions:

- Verified the identities of the supplicant and the authenticator.
- Authenticated the user if the supplicant is an endpoint device.

At the end of the Cisco TrustSec authentication process, both the authenticator and the supplicant know the following:

- Device ID of the peer
- Cisco TrustSec capability information of the peer
- Key used for the SAP

Device Identities

Cisco TrustSec does not use IP addresses or MAC addresses as device identities. Instead, you assign a name (device ID) to each Cisco TrustSec-capable switch to identify it uniquely in the Cisco TrustSec domain. This device ID is used for the following:

- Looking up the authorization policy
- Looking up passwords in the databases during authentication

Device Credentials

Cisco TrustSec supports password-based credentials. Cisco TrustSec authenticates the supplicants through passwords and uses MSCHAPv2 to provide mutual authentication.

The authentication server uses these credentials to mutually authenticate the supplicant during the EAP-FAST phase 0 (provisioning) exchange where a PAC is provisioned in the supplicant. Cisco TrustSec does not perform the EAP-FAST phase 0 exchange again until the PAC expires, and only performs EAP-FAST phase 1 and phase 2 exchanges for future link bringups. The EAP-FAST phase 1 exchange uses the PAC to mutually authenticate the authentication server and the supplicant. Cisco TrustSec uses the device credentials only during the PAC provisioning (or reprovisioning) steps.

When the supplicant first joins the Cisco TrustSec domain, the authentication server authenticates the supplicant and pushes a shared key and encrypted token to the supplicant with the PAC. The authentication server and the supplicant use this key and token for mutual authentication in all future EAP-FAST phase 0 exchanges.

User Credentials

Cisco TrustSec does not require a specific type of user credential for endpoint devices. You can choose any type of user authentication method that is supported by the authentication server, and use the corresponding credentials. For example, the Cisco Secure Access Control System (ACS) version 5.1 supports MSCHAPv2, generic token card (GTC), or RSA one-time password (OTP).

Security Group-Based Access Control

This section includes the following topics:

Security Groups and SGTs

A security group is a grouping of users, endpoint devices, and resources that share access control policies. Security groups are defined by the administrator in the Cisco ISE or Cisco Secure ACS. As new users and devices are added to the Cisco TrustSec domain, the authentication server assigns these new entities to appropriate security groups. Cisco TrustSec assigns to each security group a unique 16-bit security group number whose scope is global within a Cisco TrustSec domain. The number of security groups in the switch is limited to the number of authenticated network entities. You do not have to manually configure security group numbers.

Once a device is authenticated, Cisco TrustSec tags any packet that originates from that device with a security group tag (SGT) that contains the security group number of the device. The packet carries this SGT throughout the network within the Cisco TrustSec header. The SGT is a single label that determines the privileges of the source within the entire enterprise.

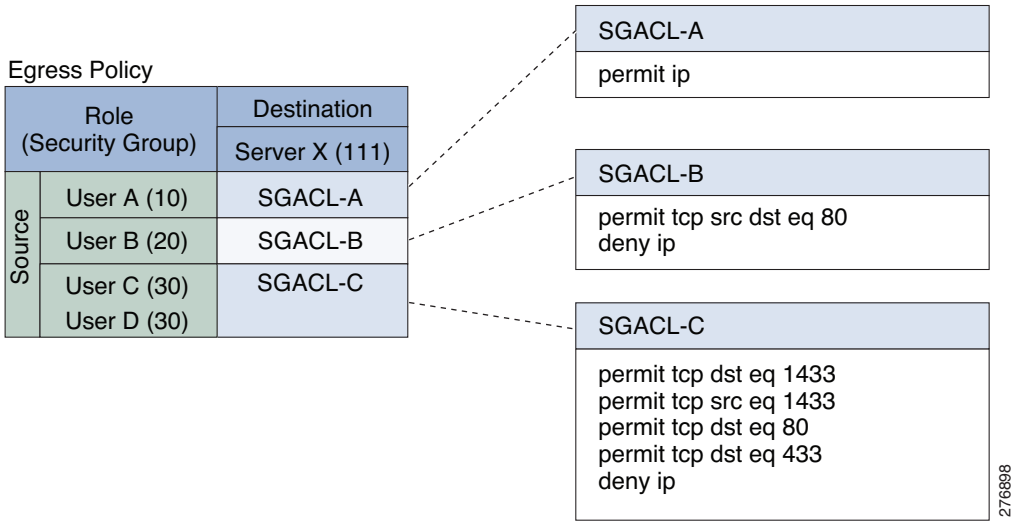
Because the SGT contains the security group of the source, the tag can be referred to as the source SGT. The destination device is also assigned to a security group (the destination SG) that can be referred to for simplicity as the destination group tag (DGT), although the actual Cisco TrustSec packet tag does not contain the security group number of the destination device.

SGACL Policies

Using security group access control lists (SGACLs), you can control the operations that users can perform based on the security group assignments of users and destination resources. Policy enforcement within the Cisco TrustSec domain is represented by a permissions matrix, with source security group numbers on one axis and destination security group numbers on the other axis. Each cell in the body of the matrix can contain an ordered list of SGACLs which specifies the permissions that should be applied to packets originating from the source security group and destined for the destination security group.

Figure 1-3 shows an example of a Cisco TrustSec permissions matrix for a simple domain with three defined user roles and one defined destination resource. Three SGACL policies control access to the destination server based on the role of the user.

Figure 1-3 SGACL Policy Matrix Example



By assigning users and devices within the network to security groups and applying access control between the security groups, Cisco TrustSec achieves role-based topology-independent access control within the network. Because SGACLs define access control policies based on device identities instead of IP addresses as in traditional ACLs, network devices are free to move throughout the network and change IP addresses. As long as the roles and the permissions remain the same, changes to the network topology do not change the security policy. When a user is added to the switch, you simply assign the user to an appropriate security group and the user immediately receives the permissions of that group.

Note SGACL policies are applied to traffic that is generated between two host devices, not to traffic that is generated from a switch to an end host device.

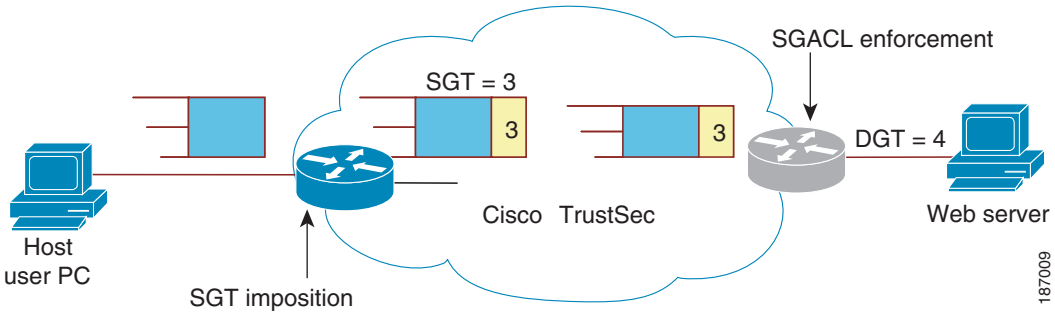
Using role-based permissions greatly reduces the size of ACLs and simplifies their maintenance. With Cisco TrustSec, the number of access control entries (ACEs) configured is determined by the number of permissions specified, resulting in a much smaller number of ACEs than in a traditional IP network. The use of SGACLs in Cisco TrustSec typically results in a more efficient use of TCAM resources compared with traditional ACLs.

Ingress Tagging and Egress Enforcement

Cisco TrustSec access control is implemented using ingress tagging and egress enforcement. At the ingress point to the Cisco TrustSec domain, traffic from the source is tagged with an SGT containing the security group number of the source entity. The SGT is propagated with the traffic across the domain. At the egress point of the Cisco TrustSec domain, an egress device uses the source SGT and the security group number of the destination entity (the destination SG, or DGT) to determine which access policy to apply from the SGACL policy matrix.

Figure 1-4 shows how the SGT assignment and the SGACL enforcement operate in a Cisco TrustSec domain.

Figure 1-4 SGT and SGACL in a Cisco TrustSec Domain



Step 1 The host PC transmits a packet to the web server. Although the PC and the web server are not members of the Cisco TrustSec domain, the data path of the packet includes the Cisco TrustSec domain.

Step 2 The Cisco TrustSec ingress switch modifies the packet to add an SGT with security group number 3, the security group number assigned by the authentication server for the host PC.

Step 3 The Cisco TrustSec egress switch enforces the SGACL policy that applies to source group 3 and destination group 4, the security group number assigned by the authentication server for the web server.

Step 4 If the SGACL allows the packet to be forwarded, the Cisco TrustSec egress switch modifies the packet to remove the SGT and forwards the packet to the web server.

Determining the Source Security Group

A network device at the ingress of Cisco TrustSec domain must determine the SGT of the packet entering the Cisco TrustSec domain so that it can tag the packet with that SGT when it forwards it into the Cisco TrustSec domain. The egress network device must determine the SGT of the packet in order to apply an SGACL.

The network device can determine the SGT for a packet in one of the following methods:

- Obtain the source SGT during policy acquisition—After the Cisco TrustSec authentication phase, a network device acquires policy information from the authentication server, which indicates whether the peer device is trusted or not. If a peer device is not trusted, then the authentication server can also provide an SGT to apply to all packets coming from the peer device.
- Obtain the source SGT from the packet—If a packet comes from a trusted peer device, the packet carries the SGT. This applies to a network device that is not the first network device in Cisco TrustSec domain for the packet.
- Look up the source SGT based on the source identity—With Identity Port Mapping (IPM), you can manually configure the link with the identity of the connected peer. The network device requests policy information, including SGT and trust state, from the authentication server.
- Look up the source SGT based on the source IP address—In some cases, you can manually configure the policy to decide the SGT of a packet based on its source IP address. The SGT Exchange Protocol (SXP) can also populate the IP-address-to-SGT mapping table.

Determining the Destination Security Group

The egress network device in a Cisco TrustSec domain determines the destination group (DGT) for applying the SGACL. The network device determines the destination security group for the packet using the same methods used for determining the source security group, with the exception of obtaining the group number from a packet tag. The destination security group number is not included in a packet tag.

In some cases, ingress devices or other non-egress devices might have destination group information available. In those cases, SGACLs might be applied in these devices rather than egress devices.

SGACL Enforcement on Routed and Switched Traffic

SGACL enforcement is applied only on IP traffic, but enforcement can be applied to either routed or switched traffic.

For routed traffic, SGACL enforcement is performed by an egress switch, typically a distribution switch or an access switch with a routed port connecting to the destination host. When you enable SGACL enforcement globally, enforcement is automatically enabled on every Layer 3 interface except for SVI interfaces.

For switched traffic, SGACL enforcement is performed on traffic flowing within a single switching domain without any routing function. An example would be SGACL enforcement performed by a data center access switch on server-to-server traffic between two directly connected servers. In this example, the server-to-server traffic would typically be switched. SGACL enforcement can be applied to packets switched within a VLAN or forwarded to an SVI associated with a VLAN, but enforcement must be enabled explicitly for each VLAN.

SGACL Logging and ACE Statistics

Note Applies to Catalyst 4500-E Series Switches, Catalyst 4500-X Series Switches, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F Series Switches.

When logging is enabled in SGACL, the switch logs the following information:

- The source security group tag (SGT) and destination SGT
- The SGACL policy name
- The packet protocol type
- The action performed on the packet

The log option applies to individual ACEs and causes packets that match the ACE to be logged. The first packet logged by the log keyword generates a syslog message. Subsequent log messages are generated and reported at five-minute intervals. If the logging-enabled ACE matches another packet (with characteristics identical to the packet that generated the log message), the number of matched packets is incremented (counters) and then reported.

To enable logging, use the **log** keyword in front of the ACE definition in the SGACL configuration. For example, **permit ip log**.

The following is a sample log, displaying source and destination SGTs, ACE matches (for a permit or deny action), and the protocol, that is, TCP, UDP, IGMP, and ICMP information:

```
*Jun  2 08:58:06.489: %C4K_IOSINTF-6-SGACLHIT: list deny_udp_src_port_log-30 Denied
udp 24.0.0.23(100) -> 28.0.0.91(100), SGT8 DGT 12
```

In addition to the existing 'per cell' SGACL statistics, which can be displayed using the **show cts role-based counters** command, you can also display ACE statistics, by using the **show ip access-list** *sgacl_name* command. No additional configuration is required for this.

The following example shows how you can use the **show ip access-list** command to display the ACE count:

```
Switch # show ip access-control deny_udp_src_port_log-30
Role-based IP access list deny_udp_src_port_log-30 (downloaded)
    10 deny udp src eq 100 log (283 matches)
    20 permit ip log (50 matches)
```

VRF-aware SGACL Logging

The SGACL system logs will include VRF information. In addition to the fields that are currently logged the logging information will include the VRF name. The updated logging information will be as shown below:

```
*Nov 15 02:18:52.187: %RBM-6-SGACLHIT_V6: ingress_interface='GigabitEthernet1/0/15'
sgacl_name='IPV6_TCP_DENY' action='Deny' protocol='tcp' src-vrf='CTS-VRF'
src-ip='25::2' src-port='20' dest-vrf='CTS-VRF' dest-ip='49::2' dest-port='30'
sgt='200' dgt='500' logging_interval_hits='1'
```

SGACL Monitor Mode

During the pre-deployment phase of Cisco TrustSec, an administrator will use the monitor mode to test the security policies without enforcing them to make sure that the policies function as intended. If the security policies do not function as intended, the monitor mode provides a convenient mechanism for identifying that and provides an opportunity to correct the policy before enabling SGACL enforcement. This enables administrators to have increased visibility to the outcome of the policy actions before they enforce it, and confirm that the subject policy meets the security requirements (access is denied to resources if users are not authorized).

The monitoring capability is provided at the SGT-DGT pair level. When you enable the SGACL monitoring mode feature, the deny action is implemented as an ACL permit on the line cards. This allows the SGACL counters and logging to display how connections are handled by the SGACL policy. Since all the monitored traffic is permitted, there is no disruption of service due to SGACLs while in the SGACL monitor mode.

Authorization and Policy Acquisition

After device authentication ends, both the supplicant and authenticator obtain the security policy from the authentication server. The two peers then perform link authorization and enforce the link security policy against each other based on their Cisco TrustSec device IDs. The link authentication method can be configured as either 802.1X or manual authentication. If the link security is 802.1X, each peer uses a device ID received from the authentication server. If the link security is manual, you must assign the peer device IDs.

The authentication server returns the following policy attributes:

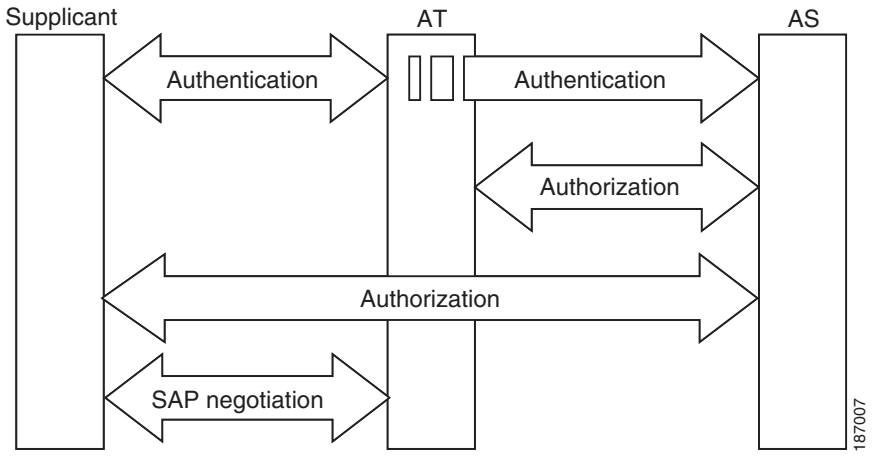
- Cisco TrustSec trust—Indicates whether the peer device is to be trusted for the purpose of putting the SGT in the packets.

- Peer SGT—Indicates the security group to which the peer belongs. If the peer is not trusted, all packets received from the peer are tagged with this SGT. If the device does not know whether any SGACLs are associated with the peer's SGT, the device may send a follow-up request to the authentication server to download the SGACLs.
- Authorization expiry time—Indicates the number of seconds before the policy expires. A Cisco TrustSec device should refresh its policy and authorization before it times out. The device can cache the authentication and policy data and reuse it after a reboot if the data has not expired. In Cisco IOS Release 12.2(33)SXI, only policy data and environment data is cached.

Tip Each Cisco TrustSec device should support some minimal default access policy in case it is not able to contact the authentication server to get an appropriate policy for the peer.

The NDAC and SAP negotiation process is shown in Figure 1-5.

Figure 1-5 NDAC and SAP Negotiation



Environment Data Download

The Cisco TrustSec environment data is a collection of information or policies that assists a device to function as a Cisco TrustSec node. The device acquires the environment data from the authentication server when the device first joins a Cisco TrustSec domain, although you might also manually configure some of the data on a device. For example, you must configure the seed Cisco TrustSec device with the authentication server information, which can later be augmented by the server list that the device acquires from the authentication server.

The device must refresh the Cisco TrustSec environment data before it expires. The device can also cache the environment data and reuse it after a reboot if the data has not expired.

The device uses RADIUS to acquire the following environment data from the authentication server:

- Server lists—List of servers that the client can use for future RADIUS requests (for both authentication and authorization).
- Device SG—Security group to which the device itself belongs.
- Expiry timeout—Interval that controls how often the Cisco TrustSec device should refresh its environment data.

RADIUS Relay Functionality

The switch that plays the role of the Cisco TrustSec authenticator in the 802.1X authentication process has IP connectivity to the authentication server, allowing the switch to acquire the policy and authorization from the authentication server by exchanging RADIUS messages over UDP/IP. The supplicant device may not have IP connectivity with the authentication server. In such cases, Cisco TrustSec allows the authenticator to act as a RADIUS relay for the supplicant.

The supplicant sends a special EAPOL message to the authenticator that contains the RADIUS server IP address and UDP port and the complete RADIUS request. The authenticator extracts the RADIUS request from the received EAPOL message and sends it over UDP/IP to the authentication server. When the RADIUS response returns from the authentication server, the authenticator forwards the message back to the supplicant, encapsulated in an EAPOL frame.

Link Security

When both sides of a link support 802.1AE Media Access Control Security (MACsec), a security association protocol (SAP) negotiation is performed. An EAPOL-Key exchange occurs between the supplicant and the authenticator to negotiate a cipher suite, exchange security parameters, and manage keys. Successful completion of all three tasks results in the establishment of a security association (SA).

Depending on your software version, crypto licensing, and link hardware support, SAP negotiation can use one of the following modes of operation:

- Galois/Counter Mode (GCM)—Specifies authentication and encryption
- GCM authentication (GMAC)—Specifies authentication and no encryption
- No Encapsulation—Specifies no encapsulation (clear text)
- Null—Specifies encapsulation, no authentication and no encryption

All modes except No Encapsulation require Cisco TrustSec-capable hardware.

For Cisco Catalyst 6500 series switches, Cisco IOS Release 12.2(50)SY and later releases, Cisco TrustSec uses AES-128 GCM and GMAC, compliant with the IEEE 802.1AE standard.

Using Cisco TrustSec-Incapable Devices and Networks in a Cisco TrustSec Network

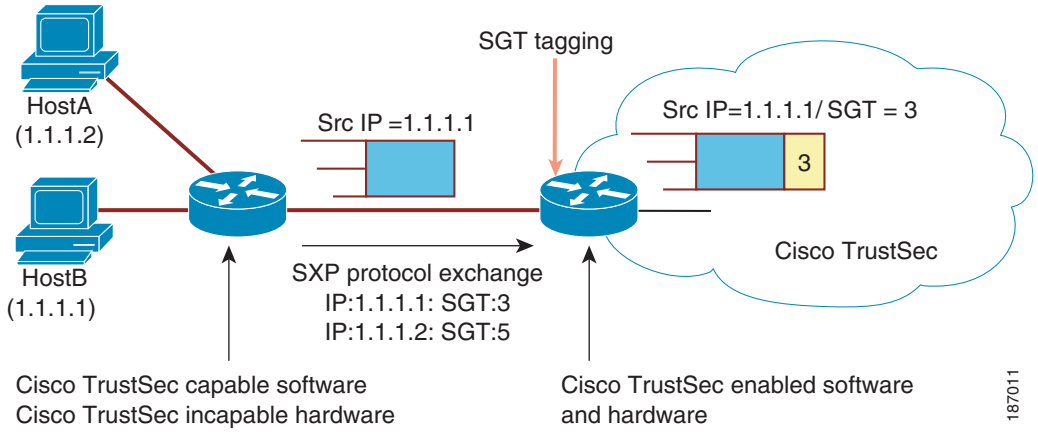
This section includes the following topics:

SXP for SGT Propagation Across Legacy Access Networks

Tagging packets with SGTs requires hardware support. You might have devices in your network that, while capable of participating in Cisco TrustSec authentication, lack the hardware capability to tag packets with SGTs. By using the SGT Exchange Protocol (SXP), these devices can pass IP-address-to-SGT mappings to a Cisco TrustSec peer device that has Cisco TrustSec-capable hardware.

SXP typically operates between ingress access layer devices at the Cisco TrustSec domain edge and distribution layer devices within the Cisco TrustSec domain. The access layer device performs Cisco TrustSec authentication of external source devices to determine the appropriate SGTs for ingress packets. The access layer device learns the IP addresses of the source devices using IP device tracking and (optionally) DHCP snooping, then uses SXP to pass the IP addresses of the source devices along with their SGTs to the distribution switches. Distribution switches with Cisco TrustSec-capable hardware can use this IP-to-SGT mapping information to tag packets appropriately and to enforce SGACL policies (see Figure 1-6).

Figure 1-6 SXP Protocol to Propagate SGT Information



You must manually configure an SXP connection between a peer without Cisco TrustSec hardware support and a peer with Cisco TrustSec hardware support. The following tasks are required when configuring the SXP connection:

- If you require SXP data integrity and authentication, you must configure the same SXP password on both peer devices. You can configure the SXP password either explicitly for each peer connection or globally for the device. Although an SXP password is not required, we recommend its use.
- You must configure each peer on the SXP connection as either an SXP speaker or an SXP listener. The speaker device distributes the IP-to-SGT mapping information to the listener device.
- You can specify a source IP address to use for each peer relationship or you can configure a default source IP address for peer connections where you have not configured a specific source IP address. If you do not specify any source IP address, the device will use the interface IP address of the connection to the peer.

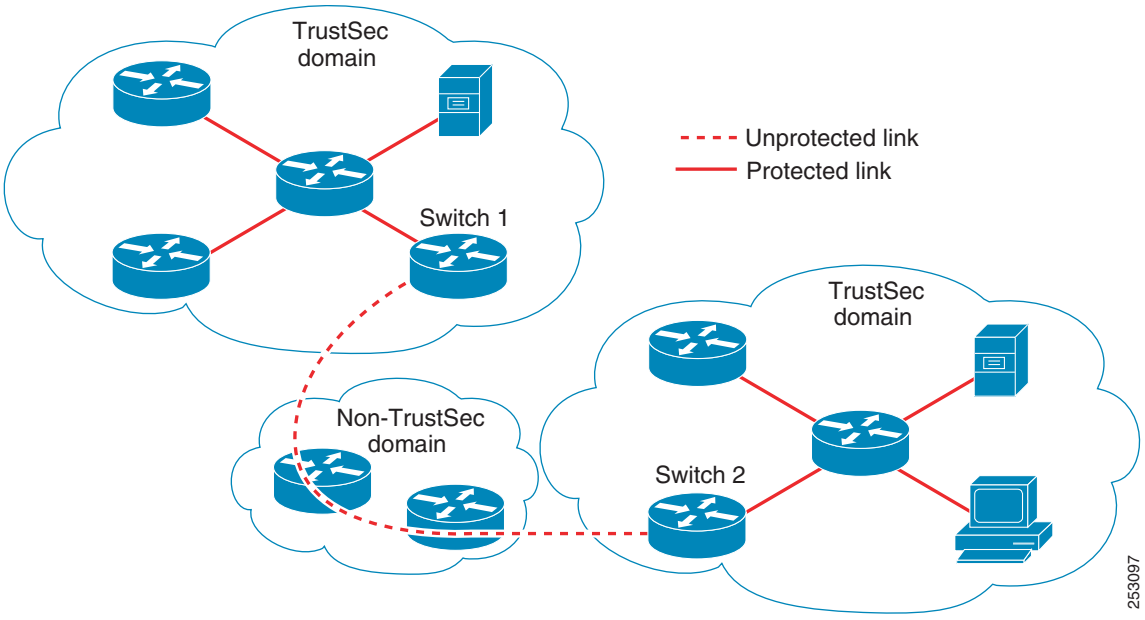
SXP allows multiple hops. That is, if the peer of a device lacking Cisco TrustSec hardware support also lacks Cisco TrustSec hardware support, the second peer can have an SXP connection to a third peer, continuing the propagation of the IP-to-SGT mapping information until a hardware-capable peer is reached. A device can be configured as an SXP listener for one SXP connection as an SXP speaker for another SXP connection.

A Cisco TrustSec device maintains connectivity with its SXP peers by using the TCP keepalive mechanism. To establish or restore a peer connection, the device will repeatedly attempt the connection setup using a configurable retry period until the connection is successful or until the connection is removed from the configuration.

Layer 3 SGT Transport for Spanning Non-TrustSec Regions

When a packet leaves the Cisco TrustSec domain for a non-TrustSec destination, the egress Cisco TrustSec device removes the Cisco TrustSec header and SGT before forwarding the packet to the outside network. If, however, the packet is merely traversing a non-TrustSec domain on the path to another Cisco TrustSec domain, as shown in Figure 1-7, the SGT can be preserved by using the Cisco TrustSec Layer 3 SGT Transport feature. In this feature, the egress Cisco TrustSec device encapsulates the packet with an ESP header that includes a copy of the SGT. When the encapsulated packet arrives at the next Cisco TrustSec domain, the ingress Cisco TrustSec device removes the ESP encapsulation and propagates the packet with its SGT.

Figure 1-7 Spanning a Non-TrustSec domain



To support Cisco TrustSec Layer 3 SGT Transport, any device that will act as a Cisco TrustSec ingress or egress Layer 3 gateway must maintain a traffic policy database that lists eligible subnets in remote Cisco TrustSec domains as well as any excluded subnets within those regions. You can configure this database manually on each device if they cannot be downloaded automatically from the Cisco Secure ACS.

A device can send Layer 3 SGT Transport data from one port and receive Layer 3 SGT Transport data on another port, but both the ingress and egress ports must have Cisco TrustSec-capable hardware.

Note Cisco TrustSec does not encrypt the Layer 3 SGT Transport encapsulated packets. To protect the packets traversing the non-TrustSec domain, you can configure other protection methods, such as IPsec.

Cisco TrustSec Reflector for Cisco TrustSec-Incapable Switching Modules

A Catalyst 6500 series switch in a Cisco TrustSec domain may contain any of these types of switching modules:

- Cisco TrustSec-capable—Hardware supports insertion and propagation of SGT.
- Cisco TrustSec-aware—Hardware does not support insertion and propagation of SGT, but hardware can perform a lookup to determine the source and destination SGTs for a packet.
- Cisco TrustSec-incapable—Hardware does not support insertion and propagation of SGT and cannot determine the SGT by a hardware lookup.

If your switch contains a Cisco TrustSec-capable supervisor engine, you can use the Cisco TrustSec reflector feature to accommodate legacy Cisco TrustSec-incapable switching modules within the same switch. Available in Cisco IOS Release 12.2(50)SY and later releases, Cisco TrustSec reflector uses SPAN to reflect traffic from a Cisco TrustSec-incapable switching module to the supervisor engine for SGT assignment and insertion.

Two mutually exclusive modes, ingress and egress, are supported for the Cisco TrustSec reflector. The default is pure mode, in which neither reflector is enabled. A Cisco TrustSec ingress reflector is configured on an access switch facing a distribution switch, while a Cisco TrustSec egress reflector is configured on a distribution switch.

Supported TrustSec Reflector Hardware

For further discussion of the Cisco TrustSec Reflector feature and a list of supported hardware, see the document, "*Cisco Catalyst 6500 Series with Supervisor Engine 2T: Enabling Cisco TrustSec with Investment Protection,*" at the following URL:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11-658388.html

Ingress Reflector

A Cisco TrustSec ingress reflector is implemented on an access switch, where the Cisco TrustSec-incapable switching module is on the Cisco TrustSec domain edge and the Cisco TrustSec-capable supervisor engine uplink port connects to a Cisco TrustSec-capable distribution switch.

The following conditions must be met before the Cisco TrustSec ingress reflector configuration is accepted:

- The supervisor engine must be Cisco TrustSec-capable.
- Any Cisco TrustSec-incapable DFCs must be powered down.
- A Cisco TrustSec egress reflector must not be configured on the switch.
- Before disabling the Cisco TrustSec ingress reflector, you must remove power from the Cisco TrustSec-incapable switching modules.

Egress Reflector

A Cisco TrustSec egress reflector is implemented on a distribution switch with Layer 3 uplinks, where the Cisco TrustSec-incapable switching module faces an access switch. The Cisco TrustSec egress reflector is supported only on Layer 3 uplinks, and is not supported on Layer 2 interfaces, SVIs, subinterfaces, or tunnels, and is not supported for NAT traffic.

The following conditions must be met before the Cisco TrustSec egress reflector configuration is accepted:

- The supervisor engine or DFC switching module must be Cisco TrustSec-capable.
- Cisco TrustSec must not be enabled on non-routed interfaces on the supervisor engine uplink ports or on the Cisco TrustSec-capable DFC switching modules.
- Before disabling the Cisco TrustSec egress reflector, you must remove power from the Cisco TrustSec-incapable switching modules.
- A Cisco TrustSec ingress reflector must not be configured on the switch.

VRF-Aware SXP

The SXP implementation of Virtual Routing and Forwarding (VRF) binds an SXP connection with a specific VRF. It is assumed that the network topology is correctly configured for Layer 2 or Layer 3 VPNs, with all VRFs configured before enabling Cisco TrustSec.

SXP VRF support can be summarized as follows:

- Only one SXP connection can be bound to one VRF.
- Different VRFs may have overlapping SXP peer or source IP addresses.
- IP–SGT mappings learned (added or deleted) in one VRF can be updated only in the same VRF domain. The SXP connection cannot update a mapping bound to a different VRF. If no SXP connection exits for a VRF, IP–SGT mappings for that VRF won't be updated by SXP.
- Multiple address families per VRF is supported. Therefore, one SXP connection in a VRF domain can forward both IPV4 and IPV6 IP-SGT mappings.
- SXP has no limitation on the number of connections and number of IP–SGT mappings per VRF.

Layer 2 VRF-Aware SXP and VRF Assignment

VRF to Layer 2 VLANs assignments are specified with the **cts role-based l2-vrf vrf-name vlan-list** global configuration command. A VLAN is considered a Layer 2 VLAN as long as there is no switch virtual interface (SVI) with an IP address configured on the VLAN. The VLAN becomes a Layer 3 VLAN once an IP address is configured on its SVI.

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.

Configuring the Cisco TrustSec Solution

Revised: July 13, 2012

This chapter includes the following topics:

Configuration Overview

This guide documents elementary Cisco TrustSec configuration procedures for Cisco Catalyst switches and includes a TrustSec command reference.

For network-wide deployment configurations, see the section, "Cisco TrustSec Configuration How-to Documents."

A network-wide deployment includes the configuration, interoperability, and management of multiple devices, which may include the Cisco Identity Services Engine (Cisco ISE), The Cisco Secure Access Control System (Cisco ACS), Cisco IP Telephones, Cisco routers, Cisco network appliances, etc.

White papers and presentations explaining the Cisco TrustSec Solution are at the following URL: http://www.cisco.com/en/US/netsol/ns1051/index.html

Cisco TrustSec Configuration How-to Documents

A series of "How-to" configuration documents provides deployment guidelines and best practices for proven network architectures in complex scenarios:

Cisco TrustSec How-to Guide: ISE Profiling Design Guide includes the following topics:

- Introduction
- Cisco ISE Profiling Services
- Profiling Service Requirements
- Profiling Services Global Configuration
- Configuring Probes
- Device Sensor
- Configuring Profiling Policies

- Profiling Design and Best Practices

Supported Hardware and Software

For a list of TrustSec supported hardware and software per TrustSec release, see, *Release Notes for Cisco TrustSec General Availability Releases* at the following URL: http://www.cisco.com/en/US/docs/switches/lan/trustsec/release/notes/rn_cts_crossplat.html

See also, the Release Notes, Configuration Guides, and Command References for your device.

Prerequisites for Cisco TrustSec

The following are the prerequisites for establishing a TrustSec network with Catalyst switches:

- TrustSec software on all network devices
- Connectivity between all network devices
- Network availability of the Cisco Secure ACS 5.1, or Cisco ISE operating with a TrustSec license
- Directory, DHCP, DNS, certificate authority, and NTP servers functioning in the network

Cisco TrustSec Guidelines and Limitations

Cisco TrustSec has the following guidelines and limitations for Catalyst switches:

- AAA for Cisco TrustSec uses RADIUS and is supported only by the Cisco Secure Access Control System (ACS), version 5.1 or later.
- You must enable the 802.1X feature globally for Cisco TrustSec to perform NDAC authentication. If you disable 802.1X globally, you will disable NDAC.
- Cisco TrustSec is supported only on physical interfaces, not on logical interfaces.
- Cisco TrustSec does not support IPv6 in the releases referenced in this guide.
- If the default password is configured on a switch, the connection on that switch should configure the password to use the default password. If the default password is not configured on a switch, the connection on that switch should also not configure a password. The configuration of the password option should be consistent across the deployment network.
- Configure the **retry open timer** command to a different value on different switches.
- SXP conveys IP-SGT mapping to RBACL enforcing switches in the network. If the access layer switch is in a different NAT domain than the RBACL enforcing switch, then clearly the IP-SGT map it uploads will be meaningless because the IP address included in the map will belong to the wrong NAT domain. The RBACL enforcing switch will never see the source IP address enumerated in the map and therefore IP-SGT database lookup will yield nothing. This means it will not be possible to apply RBACL

Default Settings

Table 2-1 lists the default settings for Cisco TrustSec parameters.

Table 2-1 Default Cisco TrustSec Parameters

Parameters	Default
Cisco TrustSec	Disabled.
SXP	Disabled.
SXP default password	None.
SXP reconciliation period	120 seconds (2 minutes).
SXP retry period	60 seconds (1 minute).
Cisco TrustSec Caching	Disabled.

Additional Documentation

Release-Specific Documents

Release-Specific Document Title	TrustSec Topics
Release Notes for Cisco TrustSec General Availability Releases	• Open and resolved caveats • Current hardware and software support

Platform-Specific Documents

Platform-Specific Document Title	TrustSec Topics
Catalyst 3000 Series Switches	
Release Notes for Catalyst 3560 and 3750 Switches	Open and resolved caveats; supported features
Catalyst 3560 Software Configuration Guides	802.1x configuration procedures
Catalyst 3750-E and 3560-E Switch Software Configuration Guide	
Cisco Catalyst 3560-X Series Switches Software Configuration Guides	
Catalyst 3750 Metro Series Switches Software Configuration Guides	
Cisco Catalyst 3750-X Series Switches Software Configuration Guides	
Catalyst 4500 Series Switches	

Platform-Specific Document Title	TrustSec Topics
Cisco Catalyst 4500 Series Switches Release Notes	Open and resolved caveats, supported features
Catalyst 4500 Series Switches Software Configuration Guides	802.1x configuration procedures
Catalyst 6500 Series Switches	
Cisco Catalyst 6500 Series Switches Release Notes	Open and resolved caveats, supported features
Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide	802.1x configuration procedures
Catalyst 6500 Release 12.2SY Software Configuration Guide	
Catalyst 6500 Release 15.0SY Software Configuration Guide	
Nexus 7000 Series Switches	
Cisco Nexus 7000 Series Switches Release Notes	Open and resolved caveats
Cisco Nexus 7000 Series Switches Configuration Guides	• TrustSec feature configurations for Cisco Nexus 7000 series switches, Release 4.1 and later • 802.1X configuration procedures
Cisco Secure Access Control System and Cisco Identity Services Engine	
Cisco Secure Access Control System Release Notes	Open and resolved caveats
Cisco Secure Access Control System End-User Guides	TrustSec configurations for Cisco ACS 5.1 and later
Cisco Identity Services Engine	TrustSec Configurations. TrustSec is referred to as SGA, or Security Group Access in ISE documentation.

Cisco IOS TrustSec Documentation Set

Cisco IOS Document Title
Cisco TrustSec Configuration Guide, Cisco IOS Release 15SY
Cisco IOS Security Command Reference

Configuring Identities, Connections, and SGTs

Revised: August 31, 2017

This section includes the following topics:

Cisco TrustSec Identity Configuration Feature Histories

For a list of supported TrustSec features per platform and the minimum required IOS release, see the *Cisco TrustSec Platform Support Matrix* at the following URL:

http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html

Otherwise, see product release notes for detailed feature introduction information.

Configuring Credentials and AAA for a Cisco TrustSec Seed Device

A Cisco TrustSec-capable device that is directly connected to the authentication server, or indirectly connected but is the first device to begin the TrustSec domain, is called the seed device. Other Cisco TrustSec network devices are non-seed devices.

To enable NDAC and AAA on the seed switch so that it can begin the Cisco TrustSec domain, perform these steps:

Release	Feature History
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).

Detailed Steps

	Command	Purpose
Step 1	`Device# cts credentials id device-id password password`	Specifies the Cisco TrustSec device ID and password for this switch to use when authenticating with other Cisco TrustSec devices with EAP-FAST. The *device-id* argument has a maximum length of 32 characters and is case sensitive.
Step 2	`Device# configure terminal`	Enters global configuration mode.
Step 3	`Device(config)# aaa new-model`	Enables AAA.
Step 4	`Device(config)# aaa authentication dot1x default group radius`	Specifies the 802.1X port-based authentication method as RADIUS.
Step 5	`Device(config)# aaa authorization network mlist group radius`	Configures the switch to use RADIUS authorization for all network-related service requests. • *mlist*—The Cisco TrustSec AAA server group.
Step 6	`Device(config)# cts authorization list mlist`	Specifies a Cisco TrustSec AAA server group. Non-seed devices will obtain the server list from the authenticator.
Step 7	`Device(config)# aaa accounting dot1x default start-stop group radius`	Enables 802.1X accounting using RADIUS.
Step 8	`Device(config)# radius-server host ip-addr auth-port 1812 acct-port 1813 pac key secret`	Specifies the RADIUS authentication server host address, service ports, and encryption key. • *ip-addr*—The IP address of the authentication server. • *secret*—The encryption key shared with the authentication server.

	Command	Purpose
Step 9	`Device(config)# radius-server vsa send authentication`	Configures the switch to recognize and use vendor-specific attributes (VSAs) in RADIUS Access-Requests generated by the switch during the authentication phase.
Step 10	`Device(config)# dot1x system-auth-control`	Globally enables 802.1X port-based authentication.
Step 11	`Device(config)# exit`	Exits configuration mode.

Note You must also configure the Cisco TrustSec credentials for the switch on the Cisco Identity Services Engine (Cisco ISE) or the Cisco Secure Access Control Server (Cisco ACS).

Configuration Examples for Seed Device

Catalyst 6500 configured as a Cisco TrustSec seed device:

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

Configuring Credentials and AAA for a Cisco TrustSec Non-Seed Device

Release	Feature History
12.2(33) SXI3	This feature was introduced on the Catalyst 6500 series switches.
IOS-XE 3.3.0 SG	This feature was introduced on the Catalyst 4000 series switches.
15.0(1)SE	This feature was introduced on the Catalyst 3750-E, 3560-E, and 3750-X series switches.

To enable NDAC and AAA on a non-seed switch so that it can join the Cisco TrustSec domain, perform these steps:

Detailed Steps

	Command	Purpose
Step 1	`Device# cts credentials id device-id password password`	Specifies the Cisco TrustSec device ID and password for this switch to use when authenticating with other Cisco TrustSec devices with EAP-FAST. The *device-id* argument has a maximum length of 32 characters and is case sensitive.
Step 2	`Device# configure terminal`	Enters global configuration mode.
Step 3	`Device(config)# aaa new-model`	Enables AAA.
Step 4	`Device(config)# aaa authentication dot1x default group radius`	Specifies the 802.1X port-based authentication method as RADIUS.
Step 5	`Device(config)# aaa authorization network mlist group radius`	Configures the switch to use RADIUS authorization for all network-related service requests. • *mlist*—Specifies a Cisco TrustSec AAA server group.
Step 6	`Device(config)# aaa accounting dot1x default start-stop group radius`	Enables 802.1X accounting using RADIUS.
Step 7	`Device(config)# radius-server vsa send authentication`	Configures the switch to recognize and use vendor-specific attributes (VSAs) in RADIUS Access-Requests generated by the switch during the authentication phase.
Step 8	`Device(config)# dot1x system-auth-control`	Globally enables 802.1X port-based authentication.
Step 9	`Device(config)# exit`	Exits configuration mode.

Note You must also configure the Cisco TrustSec credentials for the switch on the Cisco Identity Services Engine, or the Cisco Secure ACS.

Configuration Examples for Non-Seed Device

Catalyst 6500 example:

```
Device# cts credentials id Switch2 password Cisco123
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
Device(config)# aaa authorization network MLIST group radius
Device(config)# aaa accounting dot1x default start-stop group radius
Device(config)# radius-server vsa send authentication
Device(config)# dot1x system-auth-control
Device(config)# exit
```

Catalyst 3850/3650 example for access VLAN, where propagate SGT is not the default:

```
switch(config-if)# switchport access vlan 222
switch(config-if)# switchport mode access
switch(config-if)# authentication port-control auto
switch(config-if)# dot1x pae authenticator
switch(config-if)# cts dot1x
switch(config-if)# propagate sgt
```

Enabling Cisco TrustSec Authentication and MACsec in 802.1X Mode on an Uplink Port

Release	Feature History
12.2(33) SXI3	This feature was introduced on the Catalyst 6500 series switches.
IOS-XE 3.3.0 SG	This feature was introduced on the Catalyst 4000 series switches.
15.0(1)SE	This feature was introduced on the Catalyst 3750(X) series switches

Note This feature is not supported on platforms that support Cisco IOS XE Denali and Everest Releases.

You must enable Cisco TrustSec authentication on each interface that will connect to another Cisco TrustSec device. To configure Cisco TrustSec authentication with 802.1X on an uplink interface to another Cisco TrustSec device, perform this task:

Detailed Steps

	Command	Purpose
Step 1	`Device# configure terminal`	Enters global configuration mode.
Step 2	`Device(config)# interface` *type slot/port*	Enters interface configuration mode for the uplink interface.
Step 3	`Device(config-if)# cts dot1x`	Configures the uplink interface to perform NDAC authentication.

	Command	Purpose
Step 4	`Device(config-if-cts-dot1x)# [no] sap mode-list mode1 [mode2 [mode3 [mode4]]]`	(Optional) Configures 802.1AE MACsec with the SAP operation mode on the interface. The interface will negotiate with the peer for a mutually-acceptable mode. List the acceptable modes in your order of preference. Choices for *mode* are: • **gcm**— Authentication and encryption • **gmac**— Authentication, no encryption • **no-encap**— No encapsulation • **null**— Encapsulation, no authentication, no encryption **Note** MACsec with SAP is not supported on the Catalyst 3K switches. **Note** If the interface is not capable of SGT insertion or data link encryption, **no-encap** is the default and the only available SAP operating mode. **Note** On Cisco IOS XE 3.9.2E Catalyst 4500 Series Switch, if CTS DOT1X is configured on uplink port of the supervisor with gmac/gcm modes and CTS link is toggled from L2 to L3, traffic stops flowing. Workaround is to not use encryption.
Step 5	`Device(config-if-cts-dot1x)# [no] timer reauthentication seconds`	(Optional) Configures a reauthentication period to be used if the authentication server does not specify a period. If no reauthentication period is specified, the default period is 86400 seconds.
Step 6	`Device(config-if-cts-dot1x)# [no] propagate sgt`	(Optional) The **no** form of this command is used when the peer is incapable of processing an SGT. The **no propagate sgt** command prevents the interface from transmitting the SGT to the peer.
Step 7	`Device(config-if-cts-dot1x)# exit`	Exits Cisco TrustSec 802.1X interface configuration mode.
Step 8	`Device(config-if)# shutdown`	Disables the interface.
Step 9	`Device(config-if)# no shutdown`	Enables the interface and enables Cisco TrustSec authentication on the interface.
Step 10	`Device(config-if)# exit`	Exits interface configuration mode.

Configuration Examples for 802.1X on Uplink Port

Catalyst 6500 Cisco TrustSec authentication in 802.1X mode on an interface using GCM as the preferred SAP mode; the authentication server did not provide a reauthentication timer:

```
Device# configure terminal
Device(config)# interface gi2/1
Device(config-if)# cts dot1x
Device(config-if-cts-dot1x)# sap mode-list gcm null no-encap
```

```
Device(config-if-cts-dot1x)# timer reauthentication 43200
Device(config-if-cts-dot1x)# propagate sgt
Device(config-if-cts-dot1x)# exit
Device(config-if)# shutdown
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# exit
```

Configuring Cisco TrustSec and MACsec in Manual Mode on an Uplink Port

Note Cisco Catalyst 9400 Series Switches do not support MACsec.

Feature History for Trustsec NDAC

Feature Name	Releases	Feature Information
	15.0(1) SE	This feature was introduced on the Catalyst 3750(X) series switches
TrustSec NDAC	XE 3.3.0 SG	This feature was introduced on the Catalyst 4000 series switches.
	12.2(50) SY	This feature was introduced on the Catalyst 6500 series switches.

You can manually configure Cisco TrustSec on an interface. You must manually configure the interfaces on both ends of the connection. No authentication occurs; policies can be statically configured or dynamically downloaded from an authentication server by specifying the server's device identity.

Detailed Steps

	Command	Purpose
Step 1	`Device# configure terminal`	Enters global configuration mode.
Step 2	`Device(config)# interface` *type slot/port*	Enters interface configuration mode for the uplink interface.
Step 3	`Device(config-if)# cts manual`	Enters Cisco TrustSec manual configuration mode.

	Command	Purpose
Step 4	`Device(config-if-cts-manual)# [no] sap pmk key [mode-list mode1 [mode2 [mode3 [mode4]]]]`	(Optional) Configures the SAP pairwise master key (PMK) and operation mode. SAP is disabled by default in Cisco TrustSec manual mode. • *key*—A hexadecimal value with an even number of characters and a maximum length of 32 characters. The SAP operation *mode* options are: • **gcm**— Authentication and encryption • **gmac**— Authentication, no encryption • **no-encap**— No encapsulation • **null**— Encapsulation, no authentication or encryption **Note** MACsec with SAP is not supported on the Catalyst 3K switches. **Note** If the interface is not capable of SGT insertion or data link encryption, **no-encap** is the default and the only available SAP operating mode.
Step 5	`Device(config-if-cts-manual)# [no] policy dynamic identity peer-name`	(Optional) Configures Identity Port Mapping (IPM) to allow dynamic authorization policy download from authorization server based on the identity of the peer. See the additional usage notes following this task. • *peer-name*—The Cisco TrustSec device ID for the peer device. The peer name is case sensitive. **Note** Ensure that you have configured the Cisco TrustSec credentials (see "Configuring Credentials and AAA for a Cisco TrustSec Seed Device" section on page 3-2).
	`Device(config-if-cts-manual)# [no] policy static sgt tag [trusted]`	(Optional) Configures a static authorization policy. See the additional usage notes following this task. • *tag*—The SGT in decimal format. The range is 1 to 65533. • **trusted**—Indicates that ingress traffic on the interface with this SGT should not have its tag overwritten.
Step 6	`Device(config-if-cts-manual)# [no] propagate sgt`	(Optional) The **no** form of this command is used when the peer is incapable of processing an SGT. The **no propagate sgt** command prevents the interface from transmitting the SGT to the peer.
Step 7	`Device(config-if-cts-manual)# exit`	Exits Cisco TrustSec manual interface configuration mode.
Step 8	`Device(config-if)# shutdown`	Disables the interface.

	Command	Purpose
Step 9	`Device(config-if)# no shutdown`	Enables the interface and enables Cisco TrustSec authentication on the interface.
Step 10	`Device(config-if)# exit`	Exits interface configuration mode.

Identity Port Mapping (IPM) configures a physical port such that a single SGT is imposed on all traffic entering the port; this SGT is applied on all IP traffic exiting the port until a new binding is learned. IPM is configured as follows:

- CTS Manual interface configuration mode with the **policy static sgt** *tag* command
- CTS Manual interface configuration mode with the **policy dynamic identity** *peer-name* command where *peer-name* is designated as non-trusted in the Cisco ACS or Cisco ISE configuration.

IPM is supported for the following ports:

- Routed ports
- Switchports in access mode
- Switchports in trunk mode

When manually configuring Cisco TrustSec on an interface, consider these usage guidelines and restrictions:

- If no SAP parameters are defined, MACsec encapsulation or encryption will not be performed.
- 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.
  - 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.

Configuration Examples for Manual Mode and MACsec on an Uplink Port

Note Cisco Catalyst 9400 Series Switches do not support MACsec.

Catalyst 6500 TrustSec interface configuration in manual mode:

```
Device# configure terminal
Device(config)# interface gi 2/1
```

```
Device(config-if)# cts manual
Device(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm null no-encap
Device(config-if-cts-manual)# policy static sgt 111
Device(config-if-cts-manual)# exit
Device(config-if)# shutdown
Device(config-if)# no shutdown
Device(config-if)# end
```

Before configuring Cisco TrustSec, refer to the guidelines mentioned in Catalyst 3850, Catalyst 3650 Switches, and Wireless LAN Controller 5700 Series under Configuration Guidelines and Restrictions section.

Catalyst 3850 TrustSec interface configuration in manual mode:

```
Switch# configure terminal
Switch(config)# interface gig 1/0/5
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# policy dynamic identity my_cisco_ise_id
Switch(config-if-cts-manual)# exit
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
Device(config-if)# end
```

Regenerating SAP Key on an Interface

Feature History for SAP Key Regeneration

Feature Name	Releases	Feature Information
	15.0(1)SE	This feature was introduced on the Catalyst 3750-E, 3560-E and 3750-X series switches.
SAP Key Regeneration	IOS-XE 3.3.0 SG	This feature was introduced on the Catalyst 4000 series switches.
	12.2(50) SY	This feature was introduced on the Catalyst 6500 series switches.

The ability to manually refresh encryption keys is often part of network administration security requirements. SAP key refresh ordinarily occurs automatically, triggered by combinations of network events and non-configurable internal timers.

Detailed Steps

	Command	Purpose
Step 1	**cts rekey interface** interface_type *slot/port* **Example:** c6500switch# **cts rekey int gig 1/1**	Forces renegotiation of SAP keys on MACsec link.

Verifying the Cisco TrustSec Interface Configuration

To view the TrustSec-relate interface configuration, perform this task:

Detailed Steps

	Command	Purpose
Step 1	**show cts interface** [**interface_type** *slot/port* | **brief** | **summary**] **Example:** c6500switch# **show cts interface brief**	Displays TrustSec-related interface configuration.

Example: Show Cisco 6500 TrustSec interface configuration:

```
Device# show cts interface interface gi3/3

Global Dot1x feature is Enabled
Interface GigabitEthernet3/3:
    CTS is enabled, mode:    DOT1X
    IFC state:               OPEN
    Authentication Status:   SUCCEEDED
        Peer identity:       "sanjose"
        Peer's advertised capabilities: ""
        802.1X role:         Supplicant
        Reauth period applied to link:  Not applicable to Supplicant role
    Authorization Status:    SUCCEEDED
        Peer SGT:            11
        Peer SGT assignment: Trusted
    SAP Status:              NOT APPLICABLE
        Configured pairwise ciphers:
            gcm-encrypt
            null

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

        Selected cipher:

    Cache Info:
        Expiration            : 23:32:40 PDT Jun 22 2009
        Cache applied to link : NONE
        Expiration            : 23:32:40 PDT Jun 22 2009

    Statistics:
        authc success:              1
        authc reject:               0
        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

Dot1x Info for GigabitEthernet3/1
-----------------------------------
PAE                       = SUPPLICANT
```

```
StartPeriod              = 30
AuthPeriod               = 30
HeldPeriod               = 60
MaxStart                 = 3
Credentials profile      = CTS-ID-profile
EAP profile              = CTS-EAP-profile
Dot1x Info for GigabitEthernet3/1
-----------------------------------
PAE                      = AUTHENTICATOR
PortControl              = FORCE_AUTHORIZED
ControlDirection         = Both
HostMode                 = SINGLE_HOST
QuietPeriod              = 60
ServerTimeout            = 0
SuppTimeout              = 55
ReAuthMax                = 2
MaxReq                   = 2
TxPeriod                 = 30
```

Example: Cisco 3850 TrustSec interface query:

```
Edison24U> show cts interface gig 1/0/6
Global Dot1x feature is Disabled
Interface GigabitEthernet1/0/6:
    CTS is enabled, mode:    MANUAL
    IFC state:               INIT
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: ""
    Authorization Status:    NOT APPLICABLE
    SAP Status:              NOT APPLICABLE
    Propagate SGT:           Enabled
    Cache Info:
        Expiration            : N/A
        Cache applied to link : NONE

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

    L3 IPM:   disabled.
```

Manually Configuring a Device SGT

Feature History for Manual Device SGT

Feature Name	Releases	Feature Information
Manual Device SGT	12.2(50) SY	This feature was introduced on the Catalyst 6500 series switches.

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.

To manually configure an SGT on the device, perform this task:

Detailed Steps

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# cts sgt` *tag*	Configures the SGT for packets sent from the device. The *tag* argument is in decimal format. The range is 1 to 65533.
Step 3	`Switch(config)# exit`	Exits configuration mode.

Configuration Examples for Manually Configuring a Device SGT

Catalyst 6500, Catalyst 3850, and Catalyst 3750-X:

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

Manually Configuring IP Address-to-SGT Mapping

Feature History for IP-Address-to-SGT Mapping

Feature Name	Releases	Feature Information
IP Address-to-SGT-Mapping	15.0(0)SY	SXPv3 was introduced on the Catalyst 6500 switches. The following arguments and keyword were added to the **cts role-based sgt-map** command on the Catalyst 6500 series switches. • *ipv4-address/prefix* • *ipv6-address/prefix* • **interface**
	12.2(50) SY	This feature was introduced on the Catalyst 6500 series switches.

This section discusses SGTs-to-source IP address mapping as follows:

- Subnet-to-SGT Mapping, page 3-14
- VLAN-to-SGT Mapping, page 3-18
- Layer 3 Logical Interface-to-SGT Mapping (L3IF–SGT Mapping), page 3-24

For Identity Port Mapping in cts interface manual mode, see the following section:

- Configuring Cisco TrustSec and MACsec in Manual Mode on an Uplink Port, page 3-7

Subnet-to-SGT Mapping

Subnet-to-SGT mapping binds an SGT to all host addresses of a specified subnet. TrustSec imposes the SGT on an incoming packet when the packet's source IP address belongs to the specified subnet. The subnet and SGT are specified in the CLI with the **cts role-based sgt-map** *net_address*/*prefix* **sgt** *sgt_number* global configuration command. A single host may also be mapped with this command.

In IPv4 networks, SXPv3, and more recent versions, can receive and parse subnet *net_address*/*prefix* strings from SXPv3 peers. Earlier SXP versions convert the subnet prefix into its set of host bindings before exporting them to an SXP listener peer.

For example, the IPv4 subnet 198.1.1.0/29 is expanded as follows (only 3 bits for host addresses):

- Host addresses 198.1.1.1 to 198.1.1.7–tagged and propagated to SXP peer.
- Network and broadcast addresses 198.1.1.0 and 198.1.1.8— not tagged and not propagated.

To limit the number of subnet bindings SXPv3 can export, use the **cts sxp mapping network-map** global configuration command.

Subnet bindings are static, there is no learning of active hosts. They can be used locally for SGT imposition and SGACL enforcement. Packets tagged by subnet-to-SGT mapping can be propagated on Layer 2 or Layer 3 TrustSec links.

For IPv6 networks, SXPv3 cannot export subnet bindings to SXPv2 or SXPv1 peers.

Feature History for Subnet-to-SGT Mapping

Feature Name	Releases	Feature Information
Subnet-to-SGT Mapping	15.0(1)SY	Support for this command was introduced with SXPv3 on the Catalyst 6500 series switches. Related CLIs appeared in earlier releases.

Default Settings

There are no default settings for this feature.

Configuring Subnet-to-SGT Mapping

This section includes the following topics:

- Verifying Subnet-to-SGT Mapping Configuration, page 3-17
- Configuring Subnet-to-SGT Mapping, page 3-14

Restrictions

- An IPv4 subnetwork with a /31 prefix cannot be expanded.
- Subnet host addresses cannot be bound to SGTs when the **network-map** *bindings* parameter is less than the total number of subnet hosts in the specified subnets, or when *bindings* is 0.
- IPv6 expansions and propagation only occurs when SXP speaker and listener are running SXPv3, or more recent versions.

Restrictions for Cisco IOS XE Release 3.9.2E on Catalyst 4500

- You can assign SGT to IPv4 End-point IDs (EIDs) only.
- VRF aware SGT is applicable only to routed traffic and not bridged traffic.
- If CTS links are switchports and belong to an access/trunk VLAN, configure an SVI for the VLAN and the VLAN should be unshut.

Detailed Steps

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **cts sxp mapping network-map** *bindings* **Example:** `switch(config)# cts sxp mapping network-map 10000`	Configures the Subnet to SGT Mapping host count constraint. The *bindings* argument specifies the maximum number of subnet IP hosts that can be bound to SGTs and exported to the SXP listener. • *bindings*—(0 to 65,535) default is 0 (no expansions performed)
Step 3	[**no**] **cts role-based sgt-map** *ipv4_address/prefix* **sgt** *number* **Example:** `switch(config)# cts role-based sgt-map 10.10.10.10/29 sgt 1234`	(IPv4) Specifies a subnet in CIDR notation. Use the [**no**] form of the command to unconfigure the Subnet to SGT mapping. The number of bindings specified in Step 2 should match or exceed the number of host addresses in the subnet (excluding network and broadcast addresses). The **sgt** *number* keyword specifies the Security Group Tag to be bound to every host address in the specified subnet. • *ipv4_address*—Specifies the IPv4 network address in dotted decimal notation. • *prefix*—(0 to 30). Specifies the number of bits in the network address. • **sgt** *number* (0–65,535). Specifies the Security Group Tag (SGT) number.

	Command	Purpose
Step 4	[**no**] **cts role-based sgt-map** *ipv6_address::prefix* **sgt** *number* **Example:** `switch(config)# cts role-based sgt-map 2020::/64 sgt 1234`	(IPv6) Specifies a subnet in colon hexadecimal notation. Use the [**no**] form of the command to unconfigure the Subnet to SGT mapping. The number of bindings specified in Step 2 should match or exceed the number of host addresses in the subnet (excluding network and broadcast addresses). The **sgt** *number* keyword specifies the Security Group Tag to be bound to every host address in the specified subnet. • *ipv6_address*—Specifies IPv6 network address in colon hexadecimal notation. • *prefix*—(0 to128). Specifies the number of bits in the network address. • **sgt** *number*—(0 to 65,535). Specifies the Security Group Tag (SGT) number.

Step 5	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 6	**show running-config** | include *search_string*
	
	Example:
	`switch# show running-config | include sgt 1234`
	`switch# show running-config | include network-map`
		Verifies that the **cts role-based sgt-map** and the **cts sxp mapping network-map** commands are in the running configuration.

Step 7	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying Subnet-to-SGT Mapping Configuration

To display Subnet-to-SGT Mapping configuration information, perform one of the following tasks:

Command	Purpose
show cts sxp connections	Displays the SXP speaker and listener connections with their operational status.
show cts sxp sgt-map	Displays the IP to SGT bindings exported to the SXP listeners.
show running-config	Verifies that the Subnet to SGT configurations commands are in the running configuration file.

Configuration Examples for Subnet-to-SGT Mapping

The following example shows how to configure IPv4 Subnet-to-SGT Mapping between two Catalyst 6500 series switches running SXPv3 (Switch1 and Switch2):

Step 1 Configure SXP speaker/listener peering between Switch1 (1.1.1.1) and Switch 2 (2.2.2.2).

```
Switch1# config t
Switch1(config)# cts sxp enable
Switch1(config)# cts sxp default source-ip 1.1.1.1
Switch1(config)# cts sxp default password 1syzygy1
Switch1(config)# cts sxp connection peer 2.2.2.2 password default mode local speaker
```

Step 2 Configure Switch 2 as SXP listener of Switch1.

```
Switch2(config)# cts sxp enable
Switch2(config)# cts sxp default source-ip 2.2.2.2
Switch2(config)# cts sxp default password 1syzygy1
Switch2(config)# cts sxp connection peer 1.1.1.1 password default mode local listener
```

Step 3 On Switch2, verify that the SXP connection is operating:

```
Switch2# show cts sxp connections brief | include 1.1.1.1
     1.1.1.1          2.2.2.2          On               3:22:23:18 (dd:hr:mm:sec)
```

Step 4 Configure the subnetworks to be expanded on Switch1.

```
Switch1(config)# cts sxp mapping network-map 10000
Switch1(config)# cts role-based sgt-map 10.10.10.0/30 sgt 101
Switch1(config)# cts role-based sgt-map 11.11.11.0/29 sgt 11111
Switch1(config)# cts role-based sgt-map 192.168.1.0/28 sgt 65000
```

Step 5 On Switch2, verify the subnet-to-SGT expansion from Switch1. There should be two expansions for the 10.10.10.0/30 subnetwork, six expansions for the 11.11.11.0/29 subnetwork, and 14 expansions for the 192.168.1.0/28 subnetwork.

```
Switch2# show cts sxp sgt-map brief | include 101|11111|65000
    IPv4,SGT: <10.10.10.1 , 101>
    IPv4,SGT: <10.10.10.2 , 101>
    IPv4,SGT: <11.11.11.1 , 11111>
    IPv4,SGT: <11.11.11.2 , 11111>
    IPv4,SGT: <11.11.11.3 , 11111>
    IPv4,SGT: <11.11.11.4 , 11111>
    IPv4,SGT: <11.11.11.5 , 11111>
    IPv4,SGT: <11.11.11.6 , 11111>
    IPv4,SGT: <192.168.1.1 , 65000>
```

```
IPv4,SGT: <192.168.1.2 , 65000>
IPv4,SGT: <192.168.1.3 , 65000>
IPv4,SGT: <192.168.1.4 , 65000>
IPv4,SGT: <192.168.1.5 , 65000>
IPv4,SGT: <192.168.1.6 , 65000>
IPv4,SGT: <192.168.1.7 , 65000>
IPv4,SGT: <192.168.1.8 , 65000>
IPv4,SGT: <192.168.1.9 , 65000>
IPv4,SGT: <192.168.1.10 , 65000>
IPv4,SGT: <192.168.1.11 , 65000>
IPv4,SGT: <192.168.1.12 , 65000>
IPv4,SGT: <192.168.1.13 , 65000>
IPv4,SGT: <192.168.1.14 , 65000>
```

Step 6 Verify the expansion count on Switch1:

```
Switch1# show cts sxp sgt-map

    IP-SGT Mappings expanded:22
    There are no IP-SGT Mappings
```

Step 7 Save the configurations on Switch 1 and Switch 2 and exit global configuration mode.

```
Switch1(config)# copy running-config startup-config
Switch1(config)# exit
Switch2(config)# copy running-config startup-config
Switch2(config)# exit
```

VLAN-to-SGT Mapping

The VLAN-to-SGT mapping feature binds an SGT to packets from a specified VLAN. This simplifies the migration from legacy to TrustSec-capable networks as follows:

- Supports devices that are not TrustSec-capable but are VLAN-capable, such as, legacy switches, wireless controllers, access points, VPNs, etc.
- Provides backward compatibility for topologies where VLANs and VLAN ACLs segment the network, such as, server segmentation in data centers.

The VLAN-to-SGT binding is configured with the **cts role-based sgt-map vlan-list** global configuration command.

When a VLAN is assigned a gateway that is a switched virtual interface (SVI) on a TrustSec-capable switch, and IP Device Tracking is enabled on that switch, then TrustSec can create an IP-to-SGT binding for any active host on that VLAN mapped to the SVI subnet.

IP-SGT bindings for the active VLAN hosts are exported to SXP listeners. The bindings for each mapped VLAN are inserted into the IP-to-SGT table associated with the VRF the VLAN is mapped to by either its SVI or by the **cts role-based l2-vrf** command.

VLAN-to-SGT bindings have the lowest priority of all binding methods and are ignored when bindings from other sources are received, such as from SXP or CLI host configurations. Binding priorities are listing in the "Binding Source Priorities" section on page 3-26.

Feature History for VLAN-to-SGT Mapping

Table 3-1 Feature History for VLAN-to-SGT Mapping

Feature Name	Releases	Feature Information
VLAN-to-SGT Mapping	15.0 (1) SY	Support for this command was introduced with SXPv3 on the Catalyst 6500 series switches. Related CLIs appeared in earlier releases.
	Cisco IOS XE 3.9.2E	Introduced support for **cts role-based vrf** command on Catalyst 4500E Series Switch.

Default Settings

There are no default settings.

Configuring VLAN-to-SGT Mapping

This section includes the following topics:

- Task Flow for Configuring VLAN-SGT Mapping, page 3-19
- Configuring SISF Policy and Attaching to a Port, page 3-21

Task Flow for Configuring VLAN-SGT Mapping

- Create a VLAN on the TrustSec switch with the same VLAN_ID of the incoming VLAN.
- Create an SVI for the VLAN on the TrustSec switch to be the default gateway for the endpoint clients.
- Configure the TrustSec switch to apply an SGT to the VLAN traffic.
- Enable IP Device tracking on the TrustSec switch.
- Verify that VLAN-to-SGT mapping occurs on the TrustSec switch.

Detailed Steps for Catalyst 6500, Catalyst 4K

	Command	Purpose

Step 1	**config t**
	
	Example:
	`TS_switchswitch# config t`
	`TS_switchswitch(config)#`
		Enters global configuration mode.

Step 2	**vlan** ***vlan_id***
	
	Example:
	`TS_switch(config)# vlan 100`
	`TS_switch(config-vlan)#`
		Creates VLAN 100 on the TrustSec-capable gateway switch and enters VLAN configuration submode.

	Command	Purpose
Step 3	**[no] shutdown** **Example:** `TS_switch(config-vlan)# no shutdown`	Provisions VLAN 100.

Step 4	**exit**
	
	Example:
	`TS_switch(config-vlan)# exit`
	`TS_switch(config)#`
		Exits VLAN configuration mode and returns to global configuration mode.

Step 5	**interface** type *slot/port*
	
	Example:
	`TS_switch(config)# interface vlan 100`
	`TS_switch(config-if)#`
		Enters interface configuration mode.

Step 6	**ip address** *slot/port* **Example:** `TS_switch(config-if)# ip address 10.1.1.2 255.0.0.0`	Configures Switched Virtual Interface (SVI) for VLAN 100.
Step 7	**[no] shutdown** **Example:** `TS_switch(config-if)# no shutdown`	Enables the SVI.

Step 8	**exit**
	
	Example:
	`TS_switch(config-if)# exit`
	`TS_switch(config)#`
		Exits VLAN interface configuration mode and returns to global configuration mode.

Step 9	**cts role-based sgt-map vlan-list** *vlan_id* **sgt** *sgt_number* **Example:** `TS_switch(config)# cts role-based sgt-map vlan-list 100 sgt 10`	Assigns the specified SGT to the specified VLAN.
Step 10	Configure SISF policy before you proceed to the next step. Refer Configuring SISF Policy and Attaching to a Port.	
Step 11	**show cts role-based sgt-map** {*ipv4_netaddr* | *ipv4_netaddr/prefix* | *ipv6_netaddr*| *ipv6_netaddr/prefix* | **all** [**ipv4** | **ipv6**] | host {*ipv4__addr* | *ipv6_addr*} | **summary** [**ipv4** | **ipv6**] **Example:** `TS_switch# cts role-based sgt-map all`	(Optional) Displays the VLAN-to-SGT mappings.
Step 12	**show ip device tracking {all|interface|ip|mac}** **Example:** `TS_switch# show ip device tracking all`	(Optional) Verifies the operational status of IP Device tracking.
Step 13	**copy running-config startup-config** **Example:** `TS_switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring SISF Policy and Attaching to a Port

The Switch Integrated Security Features (SISF) policy is configured on both the VLAN and on the physical port. The SISF policy is attached to a VLAN to learn the VLAN-specific address binding. The purpose of attaching the SISF policy to a physical port is to learn IPv4 and IPv6 addresses on the physical port.

	Command	Purpose
Step 1	**device-tracking policy** *name* **Example:** `Device(config)# device-tracking policy policy1`	Configures a policy for feature device-tracking and enters device tracking configuration mode.
Step 2	**trusted-port** **Example:** `Device(config-device-tracking)# trusted-port`	Configures a port to become a trusted port.
Step 3	**limit address-count** *max-number* **Example:** `Device(config-device-tracking)# limit address-count 100`	Configures the maximum number of addresses for a port.
Step 4	**device-role node** **Example:** `Device(config-device-tracking)# device-role node`	Specifies that the device attached to the port is a node.
Step 5	**tracking enable** **Example:** `Device(config-device-tracking)# tracking enable`	Overrides default tracking behavior.
Step 6	**exit** **Example:** `Device(config-device-tracking)# exit`	Exits device tracking configuration mode and enters global configuration mode.
Step 7	**vlan configuration** *vlan_id* **Example:** `Device(config)# vlan configuration 20`	Configures the VLAN ID and enters VLAN configuration mode.
Step 8	**device-tracking attach-policy** *name* **Example:** `Device(config-vlan-config)# device-tracking attach-policy policy1`	Applies a policy for feature device-tracking on the VLAN.
Step 9	**ipv6 nd suppress** **Example:** `Device(config-vlan-config)# ipv6 nd suppress`	Applies the IPv6 neighbor discovery (ND) suppress feature on the VLAN.
Step 10	**exit** **Example:** `Device(config-vlan-config)# exit`	Exits VLAN configuration mode and enters global configuration mode.

	Command	Purpose
Step 11	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet5/2`	Configures the interface and enters interface configuration mode.
Step 12	**switchport** **Example:** `Device(config-if)# switchport`	Modifies an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.
Step 13	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Sets the interface type to access mode.
Step 14	**switchport access vlan** *vlan-id* **Example:** `Device(config-if)# switchport access vlan 20`	Sets access mode characteristics of the interface and configures VLAN when the interface is in access mode.
Step 15	**access-session host-mode multi-host** **Example:** `Device(config-if)# access-session host-mode multi-host`	Allows hosts to gain access to a controlled port and specifies that all subsequent clients are allowed access after the first client is authenticated.
Step 16	**access-session closed** **Example:** `Device(config-if)# access-session closed`	Prevents preauthentication access on a port.
Step 17	**access-session port-control auto** **Example:** `Device(config-if)# access-session port-control auto`	Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.
Step 18	**device-tracking attach-policy** *name* **Example:** `Device(config-if)# device-tracking attach-policy policy1`	Applies a policy for feature device-tracking on a port.
Step 19	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying VLAN-to-SGT Mapping

To display VLAN-to-SGT configuration information, use the following show commands:

Command	Purpose
show cts role-based sgt-map	Displays IP address to SGT bindings.
show device-tracking database	Displays the state of the IPv4 and IPv6 neighbor binding entries in a binding table.

Configuration Example for VLAN-to-SGT Mapping for a Single Host Over an Access Link

In the following example, a single host connects to VLAN 100 on an access switch. The access switch has an access mode link to a Catalyst 6500 series TrustSec software-capable switch. A switched virtual interface on the TrustSec switch is the default gateway for the VLAN 100 endpoint (IP Address 10.1.1.1). The TrustSec switch imposes Security Group Tag (SGT) 10 on packets from VLAN 100.

Step 1 Create VLAN 100 on an access switch.

```
access_switch# configure terminal
access_switch(config)# vlan 100
access_switch(config-vlan)# no shutdown
access_switch(config-vlan)# exit
access_switch(config)#
```

Step 2 Configure the interface to the TrustSec switch as an access link. Configurations for the endpoint access port are omitted in this example.

```
access_switch(config)# interface gigabitEthernet 6/3
access_switch(config-if)# switchport
access_switch(config-if)# switchport mode access
access_switch(config-if)# switchport access vlan 100
```

Step 3 Create VLAN 100 on the TrustSec switch.

```
TS_switch(config)# vlan 100
TS_switch(config-vlan)# no shutdown
TS_switch(config-vlan)# end
TS_switch#
```

Step 4 Create an SVI as the gateway for incoming VLAN 100.

```
TS_switch(config)# interface vlan 100
TS_switch(config-if)# ip address 10.1.1.2 255.0.0.0
TS_switch(config-if)# no shutdown
TS_switch(config-if)# end
TS_switch(config)#
```

Step 5 Assign Security Group Tag (SGT) 10 to hosts on VLAN 100.

```
TS_switch(config)# cts role-based sgt-map vlan 100 sgt 10
```

Step 6 (Optional) PING the default gateway from an endpoint (in this example, host IP Address 10.1.1.1). Verify that SGT 10 is being mapped to VLAN 100 hosts.

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

Active IP-SGT Bindings Information

IP Address              SGT     Source
============================================

10.1.1.1                10      VLAN

IP-SGT Active Bindings Summary
============================================
Total number of VLAN     bindings = 1
Total number of CLI      bindings = 0
Total number of active   bindings = 1
```

Step 7 (Optional) Displays the state of the IPv4 and IPv6 neighbor binding entries in a binding table.

```
TS_switch# show device-tracking database
```

```
Binding Table has 8 entries, 5 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DHCP, PKT - Other Packet, API
- API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned

Network Layer Address        Link Layer Address Interface    vlan prlvl  age   state
Time left
ARP 192.0.2.1                    001f.e21c.09b6     Gi5/2         20  0011    8s
REACHABLE  12 s
L   192.0.2.2                    c464.1395.c700     Vl20          20  0100   45s
REACHABLE
ND  2001:DB8::1                0000.0000.00fd     Gi5/2        20  0000   13s  UNKNOWN
(47 s)
L   2001:DB8::1                  c464.1395.c700     Vl20          20  0100   43s
REACHABLE
ND  2001:DB8:1::1                001f.e21c.09b6     Gi5/2         20  0011    0s
REACHABLE  20 s
ND  2001:DB8:0:ABCD::1           001f.e21c.09b6     Gi5/2         20  0011    3s
REACHABLE  17 s try 0
ND  2001:DB8::FFFE:FFFF:FFFF     001f.e21c.09b6     Gi5/2         20  0011   12s
REACHABLE  7 s try 0
L   2001:DB8::2                  c464.1395.c700     Vl20          20  0100   42s
REACHABLE
```

Layer 3 Logical Interface-to-SGT Mapping (L3IF–SGT Mapping)

L3IF-SGT mapping can directly map SGTs to traffic of any of the following Layer 3 interfaces regardless of the underlying physical interface:

- Routed port
- SVI (VLAN interface)
- Layer 3 subinterface of a Layer 2 port
- Tunnel interface

Use the **cts role-based sgt-map interface** global configuration command to specify either a specific SGT number, or a Security Group Name (whose SGT association is dynamically acquired from a Cisco ISE or a Cisco ACS access server).

In cases where Identity Port Mapping (cts interface manual sub mode configuration) and L3IF-SGT require different IP to SGT bindings, IPM takes precedence. All other conflicts among IP to SGT binding are resolved according to the priorities listing in the "Binding Source Priorities" section on page 3-26.

Feature History for L3IF-SGT Mapping

Feature Name	Releases	Feature Information
L3IF to SGT Mapping	15.0 (1) SY	Support for this command was introduced on the Catalyst 6500 series switches.

Default Settings

There are no default settings.

Configuring L3IF-to-SGT Mapping

Detailed steps Catalyst 6500

	Command	Purpose
Step 1	`Device# configure terminal`	Enters global configuration mode.

Step 2	`Device(config)# cts role-based sgt-map interface` type *slot/port* `[security-group` *name* `|` `sgt` *number*`]`
	
	`Device(config)# cts role-based sgt-map interface gigabitEthernet 1/1 sgt 77`
		An SGT is imposed on ingress traffic to the specified interface.
		• **interface** type *slot*/*port*—Displays list of available interfaces.
		• **security-group** *name*— Security Group name to SGT pairings are configured on the Cisco ISE or Cisco ACS.
		• **sgt** *number*—(0 to 65,535). Specifies the Security Group Tag (SGT) number.

Step 3	`Device(config)# exit`	Exits configuration mode.
Step 4	`Device# show cts role-based sgt-map all`	Verify that ingressing traffic is tagged with the specified SGT.

Verifying L3IF-to-SGT Mapping

To display L3IF-to-SGT configuration information, use the following show commands:

Command	Purpose
show cts role-based sgt-map all	Displays all IP address-to-SGT bindings.

Configuration Example for L3IF-to-SGT Mapping on an Ingress Port

In the following example a Layer 3 interface of a Catalyst 6500 series switch linecard is configured to tag all ingressing traffic with SGT 3. Prefixes of attached subnets are already known.

Step 1 Configure the interface.

```
Switch# config t
Switch(config)# interface gigabitEthernet 6/3 sgt 3
Switch(config)# exit
```

Step 2 Verify that the ingressing traffic to the interface is tagged appropriately.

```
Device# show cts role-based sgt-map all
IP Address              SGT     Source
============================================
15.1.1.15               4       INTERNAL
17.1.1.0/24             3       L3IF
21.1.1.2                4       INTERNAL
31.1.1.0/24             3       L3IF
31.1.1.2                4       INTERNAL
43.1.1.0/24             3       L3IF
49.1.1.0/24             3       L3IF
50.1.1.0/24             3       L3IF
50.1.1.2                4       INTERNAL
51.1.1.1                4       INTERNAL
52.1.1.0/24             3       L3IF
81.1.1.1                5       CLI
102.1.1.1               4       INTERNAL
105.1.1.1               3       L3IF
111.1.1.1               4       INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of L3IF     bindings = 7
Total number of INTERNAL bindings = 7
Total number of active   bindings = 15
```

Binding Source Priorities

TrustSec resolves conflicts among IP-SGT binding sources with a strict priority scheme. For example, an SGT may be applied to an interface with the **policy** {**dynamic identity** *peer-name* | **static sgt** *tag*} CTS Manual interface mode command (Identity Port Mapping). The current priority enforcement order, from lowest (1) to highest (7), 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.

Configuring Additional Authentication Server-Related Parameters

To configure the interaction between a switch and the Cisco TrustSec server, perform one or more of these tasks:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Device# configure terminal`	Enters global configuration mode.
Step 2	`Device(config)# [no] cts server deadtime seconds`	(Optional) 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.
Step 3	`Device(config)# [no] cts server load-balance method least-outstanding [batch-size transactions] [ignore-preferred-server]`	(Optional) 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. The default *transactions* is 25. The **ignore-preferred-server** keyword instructs the switch not to try to use the same server throughout a session.
Step 4	`Device(config)# [no] cts server test {server-IP-address | all} {deadtime seconds | enable | idle-time seconds}`	(Optional) Configures the server-liveliness test for a specified server or for all servers on the dynamic server list. By default, the test is enabled for all servers. The default **idle-time** is 60 seconds; the range is from 1 to 14400.
Step 5	`Device(config)# exit`	Exits configuration mode.
Step 6	`Device# show cts server-list`	Displays status and configuration details of a list of Cisco TrustSec servers.

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

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

Device# 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
```

Automatically Configuring a New or Replacement Password with the Authentication Server

Release	Feature History
12.2(50) SY	This feature was introduced on the Catalyst 6500 series switches.
IOS-XE 3.3.0 SG	This feature was introduced on the Catalyst 4000 series switches.
15.0(1) SE	This feature was introduced on the Catalyst 3750(X) series switches

Note This feature is not supported on Cisco Catalyst 9400 Series Switches.

As an alternative to manually configuring the password between the switch and the authentication server, you can initiate a password negotiation from the switch. To configure the password negotiation, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Device# cts change-password server ip-address port {key secret | a-id a-id}`	Initiates a password negotiation between the switch and the authentication server. • *ip-address*—The IP address of the authentication server. • *port*—The UDP port of the authentication server. • **key** *secret*—The RADIUS shared secret of the authentication server. • **a-id** *a-id*—The A-ID associated with the authentication server.

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

Emulating the Hardware Keystore

Release	Feature History
12.2(50) SY	This feature was introduced on the Catalyst 6500 series switches.

Note This feature is not supported on Cisco Catalyst 9400 Series Switches.

In cases where a hardware keystore is not present or is unusable, you can configure the switch to use a software emulation of the keystore. To configure the use of a software keystore, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Device# configure terminal`	Enters global configuration mode.
Step 2	`Device(config)# cts keystore emulate`	Configures the switch to use a software emulation of the keystore instead of the hardware keystore.
Step 3	`Device(config)# exit`	Exits configuration mode.
Step 4	`Device# show keystore`	Displays the status and contents of the keystore. The stored secrets are not displayed.

This example shows how to configure and verify the use of a software keystore:

```
Device# configure terminal
Device(config)# cts keystore emulate
Device(config)# exit
Device# show keystore

No hardware keystore present, using software emulation.
```

```
Keystore contains the following records (S=Simple Secret, P=PAC, R=RSA):

Index  Type  Name
 -----      ----     ----
     0       S  CTS-password
     1       P  ECF05BB8DFAD854E8376DEA4EF6171CF
```

Configuring SGACL Policies

Revised: January 13, 2016

This section includes the following topics:

Cisco TrustSec SGACL Feature Histories

For a list of supported TrustSec features per platform and the minimum required IOS release, see the *Cisco TrustSec Platform Support Matrix* at the following URL:

http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html

Otherwise, see product release notes for detailed feature introduction information.

Restrictions for Configuring SGACL Policies

The following restrictions apply to IPv6 SGACL enforcement:

- SGACL enforcement will be bypassed for IPv6 multicast traffic.
- SGACL enforcement will be by-passed for IPv6 packets with Link-Local IPv6 source/destination addresses

The following restriction apply to the Cisco Catalyst 3750-X Series Switches while configuring SGACL policies:

- When SXP is configured between a Catalyst 3750-X switch and another switch, SGACL policies are not enforced on Catalyst 3750-X series switches. SGACL policies are downloaded for the destination SGT, but policy statements are not applied to the traffic that is initiated from the source SGT.

  IP device tracking must be enabled on both switches and these switches should have Layer2 adjacency configured between them so that Catalyst 3750-X can tag packets with the corresponding SGT learned via the SXP protocol.

  You can enable IP device tracking on Catalyst 3750-X switches by using the **ip device tracking maximum** <*number*> command. Based on your topology, configure the number of IP clients using the *number* argument. We do not recommend configuring a high number of IP clients on ports/interfaces.

  IP device tracking is enabled by default on all ports in Cisco IOS Release 15.2(1)E, and in Catalyst 3750-X switches using this release image, SGACL policy enforcement happens.

The following restriction apply to the Cisco Catalyst 6500 Series Switches:

- CTS SGACLs are enforced for punt (CPU bound) traffic by default.

The following restriction apply to the Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches:

- CTS SGACLs cannot be enforced for punt (CPU bound) traffic due to hardware limitations.

SGACL Policy Configuration Process

Follow these steps to configure and enable Cisco TrustSec Security Group ACL (SGACL) policies:

Step 1 Configuration of SGACL policies should be done primarily through the Policy Management function of the Cisco Secure ACS or the Cisco Identity Services Engine (see the *Configuration Guide for the Cisco Secure ACS* or the *Cisco Identity Services Engine User Guide*).

If you are not using AAA on a Cisco Secure ACS or a Cisco ISE to download the SGACL policy configuration, you can manually configure the SGACL mapping and policies (see the "Manually Configuring SGACL Policies" section on page 4-7).

Note An SGACL policy downloaded dynamically from the Cisco Secure ACS or a Cisco ISE will override any conflicting locally-defined policy.

Step 2 To enable SGACL policy enforcement on egress traffic on routed ports, enable SGACL policy enforcement globally as described in the "Enabling SGACL Policy Enforcement Globally" section on page 4-2.

Step 3 To enable SGACL policy enforcement on switched traffic within a VLAN, or on traffic that is forwarded to an SVI associated with a VLAN, enable SGACL policy enforcement for specific VLANs as described in the "Enabling SGACL Policy Enforcement on VLANs" section on page 4-5.

Enabling SGACL Policy Enforcement Globally

You must enable SGACL policy enforcement globally for Cisco TrustSec-enabled routed interfaces.

The same configuration commands that are used for enforcement of IPv4 traffic apply for IPv6 traffic as well.

To enable SGACL policy enforcement on routed interfaces, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.

Configuration Examples for Enabling SGACL Policy Enforcement Globally

```
Switch(config)# cts role-based enforcement
```

Enabling SGACL Policy Enforcement Per Interface

You must first enable SGACL policy enforcement globally for Cisco TrustSec-enabled routed interfaces. This feature is not supported on Port Channel interfaces.

To enable SGACL policy enforcement on Layer 3 interfaces, perform this task:

Detailed Steps

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface gigabitethernet 6/2`	Specifies interface on which to enable or disable SGACL enforcement.
Step 3	`Switch(config-if)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.
Step 4	`Switch(config-if)# do show cts interface`	Verifies that SGACL enforcement is enabled.

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# [no] cts role-based monitor enable`	Enables device level monitor mode. By default device level monitor mode is enabled. If device monitor mode is disabled, monitor mode information is still downloaded from ISE but not applied on device until this configuration is turned on.
Step 3	`Switch(config)# [no] cts role-based monitor permissions from {sgt_num} to {dgt_num}][ipv4 | ipv6]`	Enables monitor mode for IPv4/IPv6 RBACL (SGT-DGT pair).
Step 4	`Switch(config)# show cts role-based permissions from {sgt_num} to {dgt_num}][ipv4 | ipv6] [details]`	Displays the SGACL policies and details about the monitor mode feature for each pair. The command output displays `monitored` if per cell monitor mode is enabled for the <SGT-DGT> pair
Step 5	`Switch(config)# show cts role-based counters [ipv4 | ipv6]`	Displays all SGACL enforcement statistics for IPv4 and IPv6 events.

Configuration Examples for Enabling SGACL Policy Enforcement Per Interface

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 1/0/2
Switch(config-if)# cts role-based enforcement
Switch(config-if)# end
```

Enabling SGACL Policy Enforcement on VLANs

You must enable SGACL policy enforcement on specific VLANs to apply access control to switched traffic within a VLAN, or to traffic that is forwarded to an SVI associated with a VLAN.

To enable SGACL policy enforcement on a VLAN or a VLAN list, perform this task:

Detailed Steps

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# cts role-based enforcement vlan-list` *vlan-list*	Enables Cisco TrustSec SGACL policy enforcement on the VLAN or VLAN list.

Configuration Examples for Enabling SGACL Policy Enforcement on VLANs

```
Switch# configure terminal
Switch(config)# cts role-based enforcement vlan-list 31-35,41
Switch(config)# exit
```

Configuring SGACLMonitor Mode

Before configuring SGACL monitor mode, ensure the following:

- Cisco TrustSec is enabled
- Counters are enabled

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# [no] cts role-based monitor all`	Enables device level monitor mode. By default device level monitor mode is enabled. If device monitor mode is disabled, monitor mode information is still downloaded from ISE but not applied on device until this configuration is turned on.
Step 3	`Switch(config)# [no] cts role-based monitor permissions from {sgt_num} to {dgt_num}][ipv4 | ipv6]`	Enables monitor mode for IPv4/IPv6 RBACL (SGT-DGT pair).
Step 4	`Switch(config)# show cts role-based permissions from {sgt_num} to {dgt_num}][ipv4 | ipv6] [details]`	Displays the SGACL policies and details about the monitor mode feature for each pair. The command output displays `monitored` if per cell monitor mode is enabled for the <SGT-DGT> pair
Step 5	`Switch(config)# show cts role-based counters [ipv4 | ipv6]`	Displays all SGACL enforcement statistics for IPv4 and IPv6 events.

Note The **show cts role-based counters** CLIs for IPv4 and IPv6 traffic are separate, but the displayed values for IPv4 and IPv6 are combined.

Configuration Example for Configuring SGACL Monitor Mode

```
Switch# conf t
Switch(config)# cts role-based monitor all
Switch(config)# cts role-based permissions from 2 to 3 ipv4
Switch# show cts role-based permissions from 2 to 3 ipv4
IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00
Switch# show cts role-based permissions from 2 to 3 ipv4 details
IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00
Details:
Role-based IP access list denytcpudpicmp-10 (downloaded)
    10 deny tcp
    20 deny udp
    30 deny icmp
Role-based IP access list Permit IP-00 (downloaded)
    10 permit ip
Switch# show cts role-based counters ipv4
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW_Permitt SW-Monitor HW-Monitor
*       *       0          0          8          18962      0          0
2       3       0          0          0          0          0          341057
```

Manually Configuring SGACL Policies

A role-based access control list bound to a range of SGTs and DGTs forms an SGACL, a TrustSec policy enforced on egress traffic. Configuration of SGACL policies are best done through the policy management functions of the Cisco ISE or the Cisco Secure ACS. To manually (that is, locally) configure SGACL policies, do the following:

1. Configure a role-based ACL.
2. Bind the role-based ACL to a range of SGTs.

Note An SGACL policy downloaded dynamically from the Cisco ISE or Cisco ACS overrides any conflicting manually configured policy.

Manually Configuring and Applying IPv4 SGACL Policies

Note When configuring SGACLs and Role-Based access control lists (RBACLs), the named access control lists (ACLs) must start with an alphabet.

Detailed Steps for Catalyst 3850,3650, 9300,9400,9500 switches:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	**ip access-list role-based** *rbacl-name* **Example:** `Switch(config)# ip access-list role-based allow_webtraff`	Creates a Role-based ACL and enters Role-based ACL configuration mode.
Step 3	{[*sequence-number*] | **default** | **permit** | **deny** | **remark**} **Example:** `Switch(config-rb-acl)#10 permit tcp dst eq 80 dst eq 20`	Specifies the access control entries (ACEs) for the RBACL. You can use most of the commands and options allowed in extended named access list configuration mode, with the source and destination fields omitted. Press Enter to complete an ACE and begin the next. For full explanations of ACL configuration, keywords, and options, see, Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S. The following ACE commands or keywords are not supported: • **reflect** • **evaluate** • **time-range**
Step 4	`Switch(config-rb-acl)# exit`	Exits to global configuration mode.
Step 5	[**no**] **cts role-based permissions** {**default** |[**from** {*sgt_num* | **unknown**} **to** {*dgt_num* | **unknown**}]{*rbacls* | **ipv4** *rbacls*} **Example:** `Switch(config)# cts role-based permissions from 55 to 66 allow_webtraff`	Binds SGTs and DGTs to the RBACL. The configuration is analogous to populating the permission matrix configured on the Cisco ISE or the Cisco Secure ACS. • Default—Default permissions list • *sgt_num*—0 to 65,519. Source Group Tag • *dgt_num*—0 to 65,519. Destination Group Tag • unknown—SGACL applies to packets where the security group (source or destination) cannot be determined. • ipv4—Indicates the following RBACL is IPv4. • *rbacls*—Name of RBACLs
Step 6	`Switch(config)# end`	Exits to privileged EXEC mode.
Step 7	`Switch# show cts role-based permissions`	Displays permission to RBACL configurations.
Step 8	`Switch# show ip access-lists allow_webtraff`	Displays ACEs of all RBACLs or a specified RBACL.

Configuration Examples for Manually Configuring SGACL Policies

```
Switch(config)# ip access role allow_webtraff
Switch(config-rb-acl)# 10 permit tcp dst eq 80
Switch(config-rb-acl)# 20 permit tcp dst eq 443
Switch(config-rb-acl)# 30 permit icmp
Switch(config-rb-acl)# 40 deny ip
Switch(config-rb-acl)# exit
Switch(config)# cts role-based permissions from 55 to 66 allow_webtraff
Switch# show ip access allow_webtraff

Role-based IP access list allow_webtraff
    10 permit tcp dst eq www
    20 permit tcp dst eq 443
    30 permit icmp
    40 deny ip

Switch# show show cts role-based permissions from 50 to 70
```

Configuring IPv6 Policies

To manually configure IPv6 SGACL policies, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# ipv6 access-list role-based` *sgacl-name*	Creates a named IPv6 SGACL and enters IPv6 role-based ACL configuration mode.
Step 3	`Switch(config-ipv6rb-acl)# [no] {permit | deny}` *protocol* `[dest-option | dest-option-type {`*doh-number* `|` *doh-type*`}] [dscp` *cp-value*`] [flow-label` *fl-value*`] [mobility | mobility-type {`*mh-number* `|` *mh-type*`}] [routing | routing-type` *routing-number*`] [fragments] [log | log-input] [sequence` *seqno*`]`	Specifies the access control entries (ACEs) for the IPv6 SGACL. You can use most of the commands and options allowed in extended named access list configuration mode, with the source and destination fields omitted. The following ACE commands or keywords are not supported: • **reflect** • **evaluate** • **time-range**
Step 4	`Switch(config-ipv6rb-acl)# exit`	Exits IPv6 role-based ACL configuration mode.

Manually Applying SGACL Policies

To manually apply SGACL policies, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# cts role-based permissions default [ipv4 | ipv6] sgacl-name1 [sgacl-name2 [sgacl-name3 ...]]]`	Specifies the default SGACLs. The default policies are applied when no explicit policy exists between the source and destination security groups.
Step 3	`Switch(config)# cts role-based permissions from {source-sgt | unknown} to {dest-sgt | unknown} [ipv4 | ipv6] sgacl-name1 [sgacl-name2 [sgacl-name3 ...]]]`	Specifies the SGACLs to be applied for a source security group (SGT) and destination security group (DGT). Values for *source-sgt* and *dest-sgt* range from 1 to 65533. By default, SGACLs are considered to be IPv4. • **from**—Specifies the source SGT. • **to**—Specifies the destination security group. • **unknown**—SGACL applies to packets where the security group (source or destination) cannot be determined. **Note** An SGACL policy downloaded dynamically from the ACS will override any conflicting manual policy.

Configuration Examples for Manually Applying SGACLs

Catalyst 6500—Apply default and custom SGACL policies:

```
Switch# configure terminal
Switch(config)# cts role-based permissions default MYDEFAULTSGACL
Switch(config)# cts role-based permissions from 3 to 5 SRB3 SRB5
Switch(config)# exit
```

Displaying SGACL Policies

After configuring the Cisco TrustSec device credentials and AAA, you can verify the Cisco TrustSec SGACL policies downloaded from the authentication server or configured manually. Cisco TrustSec downloads the SGACL policies when it learns of a new SGT through authentication and authorization on an interface, from SXP, or from manual IP address to SGT mapping.

To display the contents of the SGACL policies permissions matrix, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Switch# show cts role-based permissions default [ipv4 | ipv6 | details]`	Displays the list of SGACL of the default policy.
	`Switch# show cts role-based permissions [from {source-sgt | unknown}] [to {dest-sg | unknown}] [ipv4 | ipv6] [details]`	Displays the contents of the permissions matrix, including SGACLs downloaded from the authentication server and manually configured on the switch.

Using the keywords, you can display all or part of the permissions matrix:

- If the **from** keyword is omitted, a column from the permissions matrix is displayed.
- If the **to** keyword is omitted, a row from the permissions matrix is displayed.
- If the **from** and **to** keywords are omitted, the entire permissions matrix is displayed.
- If the **from** and **to** keywords are specified, a single cell from the permissions matrix is displayed and the **details** keyword is available. When **details** is entered, the ACEs of the SGACL of the single cell are displayed.

This example shows how to display the content of the SGACL policies permissions matrix for traffic sourced from security group 3:

```
Switch# show cts role-based permissions from 3

Role-based permissions from group 3 to group 5:
        SRB3
        SRB5
Role-based permissions from group 3 to group 7:
        SRB4
```

Refreshing the Downloaded SGACL Policies

Detailed Steps for Catalyst 6500, Catalyst 3850, Catalyst 3650

	Command	Purpose
Step 1	**cts refresh policy** {**peer** [*peer-id*] | **sgt** [*sgt_number*| **default**|**unknown**] } `Switch3850# cts refresh policy peer my_cisco_ise`	Performs an immediate refresh of the SGACL policies from the authentication server. • If a *peer-id* is specified, only the policies related to the specified peer connection are refreshed. To refresh all peer policies, press Enter without specifying an ID. • 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. Select default to refresh the default policy. Select unknown to refresh unknown policy.

Feature Information for SGACL Policies

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1 Feature Information for SGACL Policies

Feature Name	Releases	Feature Information
Manual SGACL Configuration	Cisco IOS Release 12.2(50)SY	This feature was introduced on the Catalyst 6500 series switches.
	Cisco IOS XE Release 3.3SE	This feature was introduced on the Catalyst 3650 and 3850 series switches.
SGACL Global Enforcement	Cisco IOS Release 12.2(50)SY	This feature was introduced on the Catalyst 6500 series switches.
SGACL Enforcement Per Interface	Cisco IOS Release 15.1(2)SY	This feature was introduced on the Catalyst 6500 series switches.
SGACL Enforcement on VLANs	Cisco IOS Release 12.2(50) SY	This feature was introduced on the Catalyst 6500 series switches.

Cisco TrustSec SGACL High Availability

Cisco TrustSec Security Group access control lists (SGACLs) support the high availability functionality in switches that support the Cisco StackWise technology. This technology provides stateful redundancy and allows a switch stack to enforce and process access control entries.

There is no Cisco TrustSec-specific configuration to enable this functionality, which is supported in Cisco IOS XE Denali 16.2.1 and later.

This chapter consists of these sections:

Prerequisites for Cisco TrustSec SGACL High Availability

This document assumes the following:

- An understanding of Cisco TrustSec and the SGACL configuration.
- Switches are configured to function as a stack. For more information, see the "*Managing Switch Stacks*" chapter of the *Software Configuration Guide, Cisco IOS XE Denali 16.1.1 (Catalyst 3850 Switches)*.
- All the switches in the stack are running an identical version of Cisco IOS XE software.

Restrictions for Cisco TrustSec SGACL High Availability

- When both active and standby switches fail simultaneously, stateful switchover of SGACL does not occur.

Information About Cisco TrustSec SGACL High Availability

High Availability Overview

In a switch stack, the stack manager assigns the switch with the highest priority as the active switch, and the switch with the next highest priority as the standby switch. During an automatic or a CLI-based stateful switchover, the standby switch becomes the active switch and the switch with the next highest priority becomes the standby switch and so on.

Operation data is synchronized from the active switch to the standby switch, during initial system bootup, changes in the operational data (also called Change of Authorization [CoA]), or operational data refresh.

During a stateful switchover, the newly active switch, requests and downloads the operation data. The environment data (ENV-data) and the Role-Based access control lists (RBACLs) are not updated until the refresh time is complete.

The following operation data is downloaded to the active switch:

- Environment Data (ENV-data)—A variable length field that consists of the preferred server list to get the RBACL information at the time of refresh or initialization.
- Protected Access Credential (PAC)—A shared secret that is mutually and uniquely shared between the switch and the authenticator to secure an Extensible Authentication Protocol Flexible Authentication via the Secure Tunneling (EAP-FAST) tunnel.
- Role-Based Policy (RBACL or SGACL)—A variable-length role-based policy list that consists of policy definitions for all the Security Group Tag (SGT) mappings on the switch.

Note Cisco TrustSec credential that consists of the device ID and password details is run as a command on the active switch.

Verifying Cisco TrustSec SGACL High Availability

To verify the Cisco TrustSec SGACL high availability configuration, run the **show cts role-based permissions** command on both the active and standby switches. The output from the command must be the same on both switches.

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

```
Device# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
        default_sgacl-01
        Deny IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 15:SGT_15:
        SGACL_3-01
IPv4 Role-based permissions from group 14:SGT_14 to group 15:SGT_15:
        multple_ace-14
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

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

```
Device-stby# show cts role-based permissions
IPv4 Role-based permissions default (monitored):
        default_sgacl-01
```

```
        Deny IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 15:SGT_15:
        SGACL_3-01
IPv4 Role-based permissions from group 14:SGT_14 to group 15:SGT_15:
        multple_ace-14
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

After a stateful switchover, run the following commands on the active switch to verify the feature:

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

```
Device# show cts pacs

AID: A3B6D4D8353F102346786CF220FF151C
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: A3B6D4D8353F102346786CF220FF151C
  I-ID: CTS_ED_21
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 17:22:32 IST Mon Mar 14 2016
PAC-Opaque:
000200B800030001000400010A3B6D4D8353F102346786CF220FF151C0006009C00030100E044B2650D8351FD06
F23623C470511E00000001356DEA96C00093A80538898D40F633C368B053200D4C9D2422A7FEB4837EA9DBB89D1
E51DA4E7B184E66D3D5F2839C11E5FB386936BB85250C61CA0116FDD9A184C6E96593EEAF5C39BE08140AFBB19
4EE701A0056600CFF5B12C02DD7ECEAA3CCC8170263669C483BD208052A46C31E39199830F794676842ADEECBB
A30FC4A5A0DEDA93
Refresh timer is set for 01:00:05
```

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

```
Device# show cts environment-data

CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0:Unknown
Server List Info:
Installed list: CTSServerList1-000D, 1 server(s):
  *Server: 10.78.105.47, port 1812, A-ID A3B6D4D8353F102346786CF220FF151C
  Status = ALIVE
  auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
0001-45 :
  0-00:Unknown
  2-ba:SGT_2
  3-00:SGT_3
  4-00:SGT_4
  5-00:SGT_5
  6-00:SGT_6
  7-00:SGT_7
  8-00:SGT_8
  9-00:SGT_9
  10-16:SGT_10
!
!
!
Environment Data Lifetime = 3600 secs
Last update time = 14:32:53 IST Mon Mar 14 2016
Env-data expires in 0:00:10:04 (dd:hr:mm:sec)
```

```
Env-data refreshes in 0:00:10:04 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
```

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

```
Device# show cts role-based permissions

IPv4 Role-based permissions default:
        default_sgacl-01
        Deny IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 15:SGT_15:
        SGACL_3-01
IPv4 Role-based permissions from group 14:SGT_14 to group 15:SGT_15:
        multple_ace-14
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

Additional References for Configuring Cisco TrustSec SGACL High Availability

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Cisco TrustSec configuration guide	*Cisco TrustSec Switch Configuration Guide*
Managing Switch Stacks	"Managing Switch Stacks" chapter in the *Software Configuration Guide, Cisco IOS XE Denali 16.1.1 (Catalyst 3850 Switches)*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco TrustSec SGACL High Availability

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1 Feature Information for Cisco TrustSec SGACL High Availability

Feature Name	Releases	Feature Information
Cisco TrustSec SGACL High Availability	Cisco IOS XE Denali 16.2.1	Cisco TrustSec Security Group access control lists (SGACLs) support the high availability functionality available on the switch stack manager. There is no Cisco TrustSec-specific configuration to enable this functionality. This functionality is only available on switches that have the stack manager architecture and use Cisco IOS XE Denali 16.2.1 and later.

Configuring SGT Exchange Protocol

Revised: January 29, 2016

You can use the SGT Exchange Protocol (SXP) to propagate the Security Group Tags (SGTs) across network devices that do not have hardware support for Cisco TrustSec. This module describes how to configure Cisco TrustSec SXP on switches in your network.

This section includes the following topics:

Cisco TrustSec SGT Exchange Protocol Feature Histories

For a list of supported Cisco TrustSec features per platform and the minimum required IOS release, see the *Cisco TrustSec Platform Support Matrix* at the following URL:

http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html

Otherwise, see product release notes for detailed feature introduction information.

Prerequisites for SGT Exchange Protocol

The Cisco TrustSec-SGT Over Exchange Protocol (SXP) network needs to be established before implementing SXP. This network has the following prerequisites:

- To use the Cisco TrustSec functionality on your existing device, ensure that you have purchased one of the followng security licenses:
  - IP Base License
  - IP Service License

Note Starting with Cisco IOS XE Release 16.5.1a, LAN Base License will support SXP configuration on Cisco Catalyst 3850 and Cisco Catalyst 3650 platforms.

- Cisco TrustSec SXP software must run on all network devices.
- Connectivity should exist between all network devices..

Restrictions for SGT Exchange Protocol

Note Cisco TrustSec Exchange Protocol is supported only on physical interfaces and not on logical interfaces.

The following restrictions are applicable when running Cisco TrustSec in enforcement mode or inline tagging mode. These restrictions do not apply when these switches are used as an SXP speaker:

- An IP subnet address cannot be statically mapped to a Security Group Tag (SGT). You can only map IP addresses to an SGT. While configuring IP address-to-SGT mappings, the IP address prefix must be 32. (Applicable to Catalyst 3560-X and 3750-X Series Switches)
- If a port is configured in multi-authentication mode, all hosts connecting to that port must be assigned the same SGT. When a host tries to authenticate, it must be assigned the same SGT as the SGT assigned to a previously authenticated host. If a host tries to authenticate, and it has a different SGT to that of a previously authenticated host, the VLAN port to which these hosts belong is error-disabled. (Applicable to Catalyst 3560-X and 3750-X Series Switches)
- Cisco TrustSec enforcement mode on a VLAN trunk line supports only up to eight VLANs. If more than eight VLANs are configured on a VLAN trunk link and Cisco TrustSec is enabled on those VLANs, the switch ports on those VLAN trunk links will be error-disabled. (Applicable to Catalyst 3560-X, 3750-X, and 3850 Series Switches)
- Switches can assign SGT and apply the corresponding Security Group access control list (SGACL) to end hosts based on SGT Exchange Protocol (SXP) listening only if the end hosts are Layer 2 adjacent to the switch. (Applicable to Catalyst 3560-X and 3750-X Series Switches)

Information About SGT Exchange Protocol

SGT Exchange Protocol Overview

Cisco TrustSec builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and data-path replay protection mechanisms.

The Security Group Tag (SGT) Exchange Protocol (SXP) is one of several protocols that supports Cisco TrustSec. SXP is a control protocol for propagating IP-to-SGT binding information across network devices that do not have the capability to tag packets. Cisco TrustSec filters packets at the egress interface. During endpoint authentication, a host accessing the Cisco TrustSec domain (the endpoint IP address) is associated with an SGT at the access device through Dynamic Host Control Protocol (DHCP)

snooping and IP device tracking. The access device transmits that association or binding through SXP to Cisco TrustSec hardware-capable egress devices. These devices maintain a table of source IP-to-SGT bindings. Packets are filtered on the egress interface by Cisco TrustSec hardware-capable devices by applying security group access control lists (SGACLs). SXP passes IP-to-SGT bindings from authentication points to upstream devices in the network. This process allows security services on switches, routers, or firewalls to learn identity information from access devices.

SGTs can be assigned through any of the following Endpoint Admission Control (EAC) access methods:

- 802.1X port-based authentication
- MAC Authentication Bypass (MAB)
- Web Authentication

SXP uses TCP as the transport protocol, and the TCP port 64999 for connection initiation. SXP uses Message Digest 5 (MD5) for authentication and integrity check. It has two defined roles—speaker (initiator) and listener (receiver).

Security Group Tagging

Security Group Tag is a unique 16 bit tag that is assigned to a unique role. It represents the privilege of the source user, device, or entity and is tagged at the ingress of the Cisco TrustSec domain.

SXP uses the device and user credentials acquired during authentication for classifying packets by security groups (SGs) as they enter a network. This packet classification is maintained by tagging packets on the ingress to the Cisco TrustSec network so that they can be identified for the purpose of applying security and other policy criteria along the data path. The Security Group Tag (SGT) allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic. Static port Identification is used to lookup the SGT value for a particular endpoint connected to a port.

SGT Assignment

The Security Group Tag (SGT) of a packet can be assigned at the port level when the packet comes tagged on a Cisco TrustSec link, or when a single endpoint authenticates on a port.

SGT of an incoming packet is determined in the following ways:

- When a packet that is tagged with an SGT comes on a trust port, the tag of the packet is considered as the SGT of the packet.
- When a packet is tagged with an SGT, but comes on an untrusted port, the SGT of the packet is ignored and the peer SGT is configured for the port.
- When a packet does not have an SGT, the peer SGT is configured for a port.
- Cisco TrustSec only allows a single host device to authenticate on a port (except for voice and data using separate VLANs). When a host is directly connected to a port, only a single peer SGT exists for that port. All packet from that port is assigned the same SGT.

The following methods of assigning SGTs are supported:

- IPM (dot1x, MAB, and Web Authentication)
- VLAN-to-SGT mapping Established when an authentication method provides an SGT for an authenticated entry already has an assigned IP address. A switch process monitors endpoint sessions and detects changes or removal of IP-to-SGT binding.

- SXP (SGT Exchange Protocol) Listener

Layer 3 SGT Transport Between Cisco TrustSec Domains

Note This feature is supported only on Cisco Catalyst 6500 Series Switches.

You can configure Layer 3 SGT Transport on Cisco TrustSec gateway devices on the edges of a network domain that has no Cisco TrustSec-capable devices.

When configuring Cisco TrustSec Layer 3 SGT transport, consider 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. The policies will be applied based on the following 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.

How to Configure SGT Exchange Protocol

- Creating Syslogs to Capture Changes of IP Address-to-SGT Mapping Learned Through SXP, page 6-9
- Configuring Layer 3 SGT Transport Between Cisco TrustSec Domains, page 6-10

To configure Cisco TrustSec SXP, follow these steps:

Step 1 Enable the Cisco TrustSec feature (see the "Configuring Identities, Connections, and SGTs" chapter).

Step 2 Enable Cisco TrustSec SXP (see the "Enabling Cisco TrustSec SXP" section on page 6-5).

Step 3 Configure SXP peer connections (see the "Configuring an SXP Peer Connection" section on page 6-5).

Enabling Cisco TrustSec SXP

You must enable Cisco TrustSec SXP before you can configure peer connections. To enable Cisco TrustSec SXP, perform this task:

Detailed Stepss

	Command	Purpose
Step 1	`Switch# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# [no] cts sxp enable`	Enables SXP for Cisco TrustSec.
Step 3	`Switch(config)# end`	Exits global configuration mode and returns to privileged EXEC mode

Configuring an SXP Peer Connection

You must configure the SXP peer connection on both of the devices. One device is the speaker and the other is the listener. When using password protection, make sure to use the same password on both ends.

Note If a default SXP source IP address is not configured and you do not configure an SXP source address in the connection, the Cisco TrustSec software derives the SXP source IP address from existing local IP addresses. The SXP source address might be different for each TCP connection initiated from the switch.

To configure an SXP peer connection, perform this task:

Detailed Steps

	Command	Purpose
Step 1	`Switch# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 1	`Switch# configure terminal`	Enters global configuration mode.

	Command	Purpose
Step 2	`Switch(config)# cts sxp connection peer peer-ipv4-addr [source src-ipv4-addr] password {default | none} mode {local | peer} {speaker | listener} [vrf vrf-name]`	Configures the SXP address connection. The optional **source** keyword 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. The **password** keyword specifies the password that SXP will use for the 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. The **mode** keyword 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. • **speaker**—Default. Specifies that the device is the speaker in the connection. • **listener**—Specifies that the device is the listener in the connection. The optional **vrf** keyword specifies the VRF to the peer. The default is the default VRF.
Step 3	`Switch(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode
Step 4	`Switch# show cts sxp connections`	(Optional) Displays the SXP connection information.

Configuring the Default SXP Password

By default, SXP uses no password when setting up connections. You can configure a default SXP password for the switch. In Cisco IOS Release 12.2(50)SY and later releases, you can specify an encrypted password for the SXP default password.

To configure a default SXP password, perform this task:

Detailed Steps

	Command	Purpose
Step 1	`Switch# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# cts sxp default password [0 | 6 | 7] password`	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.
Step 3	`Switch(config)# end#`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring the Default SXP Source IP Address

SXP uses the default source IP address for all new TCP connections where a source IP address is not specified. There is no effect on existing TCP connections when you configure the default SXP source IP address.

To configure a default SXP source IP address, perform this task:

Detailed Steps

	Command	Purpose
Step 1	`Switch# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# cts sxp default source-ip src-ip-addr`	Configures the SXP default source IP address.
Step 3	`Switch(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Changing the SXP Reconciliation Period

After a peer terminates an SXP connection, an internal hold-down timer starts. If the peer reconnects before the internal hold-down timer expires, the SXP reconciliation period 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.

To change the SXP reconciliation period, perform this task:

Detailed Steps

	Command	Purpose
Step 1	`Switch# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# cts sxp reconciliation period` *seconds*	Changes the SXP reconciliation timer. The default value is 120 seconds (2 minutes). The range is from 0 to 64000.
Step 3	`Switch(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Changing the SXP Retry Period

The SXP retry period determines how often the Cisco TrustSec software retries an SXP connection. When an SXP connection is not successfully set up, the Cisco TrustSec software makes a new attempt to set up the connection after the SXP retry period timer expires. The default value is 120 seconds. Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted.

To change the SXP retry period, perform this task:

Detailed Steps

	Command	Purpose
Step 1	`Switch# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# cts sxp retry period` *seconds*	Changes the SXP retry timer. The default value is 120 seconds (2 minutes). The range is from 0 to 64000.
Step 3	`Switch(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Creating Syslogs to Capture Changes of IP Address-to-SGT Mapping Learned Through SXP

When the **cts sxp log binding-changes** command is configured in global configuration mode, SXP syslogs (sev 5 syslog) are generated whenever a change to IP address to SGT binding occurs (add, delete, change). These changes are learned and propagated on the SXP connection. The default is **no cts sxp log binding-changes**.

To enable logging of binding changes, perform the following task:

Detailed Steps

	Command	Purpose
Step 1	`Switch# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# cts sxp log binding-changes`	Enables logging for IP to SGT binding changes.
Step 3	`Switch(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Layer 3 SGT Transport Between Cisco TrustSec Domains

You can configure Layer 3 SGT Transport on Cisco TrustSec gateway devices on the edges of a network domain that has no Cisco TrustSec-capable devices.

Note This feature is supported only on Cisco Catalyst 6500 Series Switches.

To configure Layer 3 SGT Transport, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Switch# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# [no] cts policy layer3 {ipv4 | ipv6} traffic acl-name`	(Optional) Specifies the fallback traffic policy to be applied when the authentication server is not available for downloading the traffic policy. • *acl-name*—The name of a traditional interface ACL already configured on the device. See the additional usage notes following this task.
Step 3	`Switch(config)# [no] cts policy layer3 {ipv4 | ipv6} exception acl-name`	(Optional) Specifies the fallback exception policy to be applied when the authentication server is not available for downloading the exception policy. See the additional usage notes following this task.
Step 4	`Switch(config)# interface type slot/port`	Specifies an interface and enters interface configuration mode.
Step 5	`Switch(config-if)# [no] cts layer3 {ipv4 | ipv6} trustsec forwarding`	(Configured on a Cisco TrustSec-capable physical port) Specifies that egress traffic on this interface will use Cisco TrustSec Layer 3 SGT transport encapsulation as determined by the traffic and exception policies.
	`Switch(config-if)# [no] cts layer3 {ipv4 | ipv6} policy`	(Configured on a routed port or SVI) Specifies that egress traffic on this interface will use Cisco TrustSec Layer 3 SGT transport encapsulation as determined by the traffic and exception policies.
Step 6	`Switch(config-if)# end`	Exits interface configuration and returns to privileged EXEC mode.
Step 7	`Switch# show cts policy layer3 {ipv4 | ipv6}`	(Optional) Displays the Layer 3 SGT transport configuration on the interfaces.

Configuration Examples for SGT Exchange Protocol

Example: Enabling Cisco TrustSec SXP and an SXP Peer Connection

The following example shows how to enable SXP and configure an SXP peer connection between Switch A, the speaker, and Switch B, the listener:

```
Switch# configure terminal
Switch(config)# cts sxp enable
Switch(config)# cts sxp default password Cisco123
Switch(config)# cts sxp default source-ip 10.10.1.1
Switch(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 between Switch B, the listener, and Switch A, the speaker:

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

Example: Configuring the Default SXP Password and Source IP Address

The following example shows how to configure a default SXP password and source IP address:

```
Switch# configure terminal
Switch(config)# cts sxp default password Cisco123
Switch(config)# cts sxp default source-ip 10.20.2.2
Switch(config)# end
```

Example: Configuring Layer 3 SGT Transport Between Cisco TrustSec Domains

Note This feature is supported only on Cisco Catalyst 6500 Series Switches.

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

```
Switch# configure terminal
Switch(config)# ip access-list extended traffic-list
Switch(config-ext-nacl)# permit ip any 10.1.1.0 0.0.0.255
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended exception-list
Switch(config-ext-nacl)# permit ip any 10.2.2.0 0.0.0.255
Switch(config-ext-nacl)# exit
Switch(config)# cts policy layer3 ipv4 traffic traffic-sgt
```

```
Switch(config)# cts policy layer3 ipv4 exception exception-list
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# cts layer3 trustsec ipv4 forwarding
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch#
```

Verifying SGT Exchange Protocol Connections

To view SXP connections, perform this task:

	Command	Purpose
Step 1	`Switch# show cts sxp connections`	Displays detailed information about the SXP status and connections.
Step 1	`Switch# show cts sxp connections [brief]`	Displays brief information about the SXP status and connections.

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

```
Switch# show cts sxp connections

SXP              : Enabled
Default Password : Set
Default Source IP: 10.10.1.1
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
------------------------------------------
Peer IP          : 10.20.2.2
Source IP        : 10.10.1.1
Conn status      : On
Conn Version     : 2
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: default SXP password
Duration since last state change: 0:00:21:25 (dd:hr:mm:sec)
Total num of SXP Connections = 1
```

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

```
Switch# show cts sxp connections brief

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

-------------------------------------------------------------------------------
Peer_IP          Source_IP        Conn Status       Duration
-------------------------------------------------------------------------------
10.1.3.1         10.1.3.2         On                6:00:09:13 (dd:hr:mm:sec)

Total num of SXP Connections = 1
```

Feature Information for SGT Exchange Protocol

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1 Feature Information for SGT Exchange Protocol

Feature Name	Releases	Feature Information
L3 SGT Transport	Cisco IOS Release 12.2(50) SY	This feature was introduced on the Catalyst 6500 Series Switches. **Note** This feature is only supported on Catalyst 6500 Series Switches.
SGT Exchange Protocol	Cisco IOS Release 12.2(50)SY Cisco IOS Release 15.2(3)E Cisco IOS Release 15.2(4)E1	The SGT Exchange Protocol (SXP) propagates the Security Group Tags (SGTs) across network devices that do not have hardware support for Cisco TrustSec. In Cisco IOS Release 12.2(50)SY, this feature was introduced on Cisco Catalyst 6500 Series Switches. In Cisco IOS Release 15.2(3)E, this feature was introduced on Cisco Catalyst 2960-CX Series Switches. In Cisco IOS Release 15.2(4)E1, this feature was introduced on Cisco Catalyst 3560-CX Series Switches.

Cisco TrustSec VRF-Aware SGT

Revised: July 29, 2016

The Cisco TrustSec VRF-Aware SGT feature binds a Security Group Tag (SGT) Exchange Protocol (SXP) connection with a specific virtual routing and forwarding (VRF) instance.

This module consists of these sections:

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Cisco TrustSec VRF-Aware SGT

VRF-Aware SGT

Cisco TrustSec uses security group tags (SGTs) to ensure that packets passing through the Cisco TrustSec network can be properly identified and applied with security and other access control policies.

The SGT implementation of VRF binds a Security Group Tag (SGT) Exchange Protocol (SXP) connection to a specific VRF. The assumption is that the network topology is configured for Layer 2 or Layer 3 VPNs, with all VRFs configured before enabling Cisco TrustSec.

SXP VRF support can be summarized as follows:

- The same VRF can have multiple SXP connections, with different source and peer IP address. SXP has no limitation on the number of connections and number of IP–SGT mappings per VRF.
- Different VRFs may have overlapping SXP peer or source IP addresses.
- IP–SGT mappings learned (added or deleted) in one VRF can be updated only in the same VRF domain. The SXP connection cannot update a mapping bound to a different VRF. If no SXP connection exits for a VRF, IP–SGT mappings for that VRF is not updated by SXP.
- Multiple address families per VRF is supported. Therefore, one SXP connection in a VRF domain can forward both IPV4 and IPV6 IP-SGT mappings.

You can map an SGT to a VRF using the **cts role-based sgt-map vrf** *vrf-name* command.

VRF-to-Layer 2 VLAN assignments are specified with the **cts role-based l2-vrf** *vrf-name* **vlan-list** command. A VLAN is considered a Layer 2 VLAN when there is no switch virtual interface (SVI) with an IP address configured on the VLAN. The VLAN becomes a Layer 3 VLAN once an IP address is configured on its SVI.

VRF assignments configured by the **cts role-based l2-vrf** command are active as long as a VLAN remains a Layer 2 VLAN.

Note Cisco IOS XE 3.9.2E on Catalyst 4500 Series Switch supports VRF aware SGT only for Layer 3 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 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 removed. 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.

Starting with Cisco IOS XE 3.9.2E, you can assign SGT to End-point IDs (EIDs) in LISP configuration, with the VRF aware SGT feature.

How to Configure VRF-Aware SGT

Configuring VRF-to-Layer-2-VLAN Assignments

	Command or Action	Purpose
Step 1	`Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Switch# configure terminal`	Enters global configuration mode.
Step 3	`Switch(config)# interface type number`	Enables an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	`Switch(config-if)# vrf forwarding vrf-name`	Associates a VRF instance or a virtual network with an interface or subinterface. **Note** Do not configure VRFs on the management interface.
Step 5	`Switch(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 6	`Switch(config)# cts role-based l2-vrf vrf1 vlan-list 20`	Selects a VRF instance for Layer 2 VLANs.
Step 7	`Switch(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring VRF-to-SGT Mapping

	Command or Action	Purpose
Step 1	`Switch(config)# cts role-based sgt-map vrf vrf-name {ip4_netaddress | ipv6_netaddress | host {ip4_address | ip6_address }}] sgt sgt_number`	Applies the SGT to packets in the specified VRF. The IP-SGT binding is entered into the IP-SGT table associated with the specified VRF and the IP protocol version implied by the type of IP address.
Step 2	`Switch(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuration Examples for Cisco TrustSec VRF-Aware SGT

Example: Configuring VRF-to-Layer2-VLAN Assignments

```
Device> enable
Device# configure terminal
Device(config)# interface vlan 101
Device(config-if)# vrf forwarding vrf-intf
Device(config-if)# exit
Device(config)# cts role-based l2-vrf vrf1 vlan-list 20
Device(config)# end
```

Example: Configuring VRF-to-SGT Mapping

```
Device# configure terminal
Device(config)# cts role-based sgt-map vrf red 23.1.1.2 sgt 23
Device(config)# end
```

Additional References for Configuring Cisco TrustSec VRF-Aware SGT

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Cisco TrustSec configuration guide	*Cisco TrustSec Switch Configuration Guide*
Managing Switch Stacks	"Managing Switch Stacks" chapter in the *Software Configuration Guide, Cisco IOS XE Denali 16.3.1 (Catalyst 3850 Switches)*

Standards & MIBs

MIB	MIBs Link
•	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco TrustSec VRF-Aware SGT

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1 Feature Information for Cisco TrustSec VRF-Aware SGT

Feature Name	Releases	Feature Information
Cisco TrustSec VRF-Aware SGT	Cisco IOS XE Denali 16.3.1	The Cisco TrustSec VRF-Aware SGT feature binds a Security Group Tag (SGT) Exchange Protocol (SXP) connection with a specific virtual routing and forwarding (VRF) instance. The **cts role-based l2-vrf** command was introduced on Cisco on Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches.
	Cisco IOS XE 3.9.2E	The following commands were implemented on Cisco Catalyst 4500-E Series Switches: • **cts role-based l2-vrf** • **cts role-based sgt-map vrf**

IP-Prefix and SGT-Based SXP Filtering

Revised: May 31, 2017

The Security Group Tag (SGT) Exchange Protocol (SXP) is one of the several protocols that supports Cisco TrustSec. SXP is a control protocol for propagating IP-to-SGT binding information across network devices that do not have the capability to tag packets. SXP passes IP-to-SGT bindings from authentication points to upstream devices in a network. This process allows security services on switches, routers, or firewalls to learn user identity information from access devices.

The IP-Prefix and SGT-Based SXP Filtering feature allows IP-to-SGT bindings to be filtered, when they are exported or imported. This filtering can be done based on the IP prefix, SGT, or a combination of both.

This module describes this feature and consists of these sections:

Restrictions for IP-Prefix and SGT-Based SXP Filtering

- No high availability support for the stateful synchronization of IP-SGT bindings in an SXP database between active and standby devices.
- Filters applied to an existing connection will take effect only on the subsequent bindings that are exported or imported. The filters do not apply to any bindings that have been exported or imported prior to applying the filters.
- Virtual Routing and Forwarding (VRF)-specific filtering is not supported, and a filter specified for a peer IP is applicable across all VRFs on the device.
- SGT values in filter rules will be a list of single SGT numbers. SGT ranges are not supported.

Information About IP-Prefix and SGT-Based SXP Filtering

Overview

The IP-to-SGT filtering allow systems to selectively import or export only bindings of interest. In an SXP connection, a filter can be configured on a device that acts either as a speaker or a listener, based on the filtering that happens during the export or import of bindings.

In the case of bidirectional SXP connections, filters are applied in either of the directions, based on whether a speaker or listener filter is configured. If a peer is a part of both the speaker and the listener filter groups, then filtering is applied in both directions.

Filters can be applied either on a peer-to-peer basis or globally (applicable to all SXP connections). In both cases, the filter can be applied on the speaker or the listener.

Filter Rules

A filter that needs to be applied on a device is created with a set of filter rules. Each filter rule specifies the action or actions to be taken for bindings with specific SGT values and/or IP-prefix values. Each binding is matched against the values specified in the filter rules; if a match is found, the corresponding action specified in the filter rule is applied. An action that can be applied on a selected binding is either a permit or a deny action. When a filter is enabled on the speaker or listener during the export or import of IP-SGT bindings, the bindings are filtered based on the filter rules.

If a rule is not specified for a binding in a filter list, the catch-all rule that is configured in the filter-list is executed. In the absence of a catch-all rule, the corresponding binding is implicitly denied.

Types of SXP Filtering

IP-SGT bindings are filtered in one of the following ways:

- SGT-based filtering: Filters IP-SGT bindings in an SXP connection based on the SGT value.
- IP-prefix based filtering: Filters IP-SGT bindings in an SXP connection based on the IP-prefix value.
- SGT and IP-prefix based filtering: Filter IP-SGT bindings in an SXP connection based on the SGT value and IP-prefix value.

A filter rule is applied on each of the IP-SGT binding.

How to Configure IP-Prefix and SGT-Based SXP Filtering

Configuring an SXP Filter List

In this step, a filter list is created to hold a set of rules. These rules filter the IP-SGT bindings by allowing bindings that are permitted, and blocking bindings that are denied. Each rule can be based on an SGT, IP prefix, or a combination of both the SGT and IP prefix.

If a filter list does not have a rule that matches a specific IP-SGT binding, the binding is implicitly denied unless a default or catch-all ruled is defined.

	Command or Action	Purpose
Step 1	`Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Device# configure terminal`	Enters global configuration mode.
Step 3	`Device(config)# cts sxp filter-list` *filter-name*	Configures a Cisco TrustSec filter list and enters filter-list configuration mode.
Step 4	`Device(config-filter-list)#` *sequence-number* **permit ipv4** *ip-address/prefix* **deny sgt** *sgt-value*	Configures a filter list rule.
Step 5	`Device(config-filter-list)# exit`	Exits filter-list configuration mode and returns to global configuration mode.
Step 6	`Device(config)# cts sxp filter-list` *filter-name*	Configures a Cisco TrustSec filter list and enters filter list configuration mode.
Step 7	`Device(config-filter-list)#` [*sequence-number*] **deny sgt** *sgt-value* **permit ipv6** *ipv6-address/prefix*	Configures a filter list rule.
Step 8	`Device(config-filter-list)# exit`	Exits filter-list configuration mode and returns to global configuration mode.
Step 9	`Device(config)# cts sxp filter-list` *filter-name*	Configures a Cisco TrustSec filter list and enters filter list configuration mode.
Step 10	`Device(config-filter-list)#` [*sequence-number*] **permit ipv6** *ipv6-address/prefix* **permit** *sgt-value* **permit**	Configures a filter list rule.
Step 11	`Device(config-filter-list)# end`	Exits filter-list configuration mode and returns to privileged EXEC mode.

Configuring an SXP Filter Group

In this step, a set of peers are combined into a group, and a filter list is applied to the group. A filter-group can either be defined as a speaker group or listener group. To apply the same filter list to all speakers or all listeners, you can create a global speaker filter group or a global listener filter group.

Note Only one filter list can be attached to a filter group.

	Command or Action	Purpose
Step 1	`Device# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Device# configure terminal`	Enters global configuration mode.
Step 3	`Device(config)# cts sxp filter-group listener` *listener-name*	Configures an SXP filter-group listener, and enters filter-group configuration mode.
Step 4	`Device(config-filter-group)# filter` *filter-list-name*	Configures a filter list name.
Step 5	`Device(config-filter-group)# peer` *ipv4-address*	Configures the IP address of a peer.
Step 6	`Device(config-filter-group)# exit`	Exits filter-group configuration mode and returns to global configuration mode.
Step 7	`Device(config)# cts sxp filter-group speaker` *speaker-name*	Configures a voice VLAN on a multiple VLAN access port.
Step 8	`Device(config-filter-group)# filter` *filter-list-name*	Configures a filter list name.
Step 9	`Device(config-filter-group)# peer` *ipv4-address*	Configures the IP address of a peer.
Step 10	`Device(config-filter-group)# end`	Exits filter-group configuration mode and returns to privileged EXEC mode.

Configuring a Global Listener or Speaker Filter Group

When configuring a global listener and global speaker filter group, the filter is applied to across the box for all SXP connections that are in listener or speaker mode.

When adding a filter-list to a filter group the currently configured set of filter lists on the box is displayed as a help string.

Note The **peer** command is not available for the global listener and global speaker filter-group.

	Command or Action	Purpose
Step 1	`Device# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	`Device(config)# cts sxp filter-group listener global filter-list-name`	Configures a global listener filter group.
Step 4	`Device(config)# cts sxp filter-group speaker global filter-list-name`	Configures a global speaker filter group.
Step 5	`Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Enabling SXP Filtering

After the SXP filter list and filter groups are configured, you must enable filtering.

	Command or Action	Purpose
Step 1	`Device# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Device# configure terminal`	Enters global configuration mode.
Step 3	`Device(config)# cts sxp filter enable`	Configures a source template for the interface.
Step 4	`Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	`Device# show cts sxp filter-list filter_name`	Displays the filter lists configured on the device along with the filter rules in each of the filter list.

Configuring the Default or Catch-All Rule

The default or catch-all rule is applied on IP-SGT bindings for which there was no match with any of the rules in the filter list. If a default rule is not specified, these IP-SGT bindings are denied.

Define the default or catch-all rule in the filter-list configuration mode of the corresponding filter list.

	Command or Action	Purpose
Step 1	`Device# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Device# configure terminal`	Enters global configuration mode.
Step 3	`Device(config)# cts sxp filter-list filter-name`	Configures a Cisco TrustSec filter list and enters filter-list configuration mode.
Step 4	`Device(config-filter-list)# permit ipv4 ip-address/prefix`	Permits access if the conditions are matched.
Step 5	`Device(config-filter-list)# deny ipv6 ipv6-address/prefix`	Denies access if the conditions are matched.
Step 6	`Device(config-filter-list)# permit sgt all`	Permits bindings corresponding to all SGTs.
Step 7	`Device(config-filter-list)# end`	Exits filter-list configuration mode and returns to privileged EXEC mode.

Configuration Examples for IP-Prefix and SGT-Based SXP Filtering

Example: Configuring an SXP Filter List

```
Device> enable
Device# configure terminal
Device(config)# cts sxp filter-list filter1
Device(config-filter-list)# permit ipv4 10.1.1.0/24 deny sgt 3 4
Device(config-filter-list)# exit
Device(config)# cts sxp filter-list filter2
Device(config-filter-list)# permit sgt all
Device(config-filter-list)# exit
Device(config)# cts sxp filter-list filter3
Device(config-filter-list)# deny ipv6 2001:db8::1/64 permit sgt 67
Device(config-filter-list)# end
```

Example: Configuring an SXP Filter Group

```
Device> enable
Device# configure terminal
Device(config)# cts sxp filter-group listener group1
Device(config-filter-group)# filter filter1
Device(config-filter-group)# peer 172.16.0.1 192.168.0.1
Device(config-filter-group)# exit
Device(config)# cts sxp filter-group listener global group2
Device(config)# end
```

Example: Enabling SXP Filtering

```
Device> enable
Device# configure terminal
Device(config)# cts sxp filter-enable
Device(config)# end
```

Example: Configuring the Default or Catch-All Rule

The following example shows how to create a default prefix rule that permits bindings corresponding to all IPv4 and IPv6 addresses:

```
Device(config)# cts sxp filter-list filter1
Device(config-filter-list)# permit ipv4 10.0.0.0/0
Device(config-filter-list)# deny ipv6 2001:db8::1/0
```

The following example shows how to create a default SGT rule that permits bindings corresponding to all SGTs:

```
Device(config)# cts sxp filter-list filter_1
Device(config-filter-list)# permit sgt all
```

Verifying IP-Prefix and SGT-Based SXP Filtering

To verify the configuration, use the following commands:

The **debug cts sxp filter events** command is used to log events related to the creation, removal, and update of filter-lists and filter-groups. This command is also used to capture events related to the matching actions in a filtering process.

```
Device# debug cts sxp filter events
```

The following sample output from the **show cts sxp filter-group speaker** command displays SXP speaker filter groups:

```
Device# show cts sxp filter-group speaker group1

    Filter-group: group1
    Filter-name: filter1
    Peer-list: 172.16.0.1 192.168.0.1
```

The following sample output from the **show cts sxp filter-group listener** command displays SXP listener filter groups:

```
Device# show cts sxp filter-group listener

Global Listener Filter: Not configured
    Filter-group: group1
    Filter-name: filter1
    Peer-list: 172.16.0.1 192.168.0.1
    Filter-group: group2
    Filter-name: filter1
    Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1
```

The following sample output from the **show cts sxp filter-group speaker detailed** command displays detailed information about SXP speaker filter groups:

```
Device# show cts sxp filter-group speaker group1 detailed

    Filter-group: group1
    Filter-name: filter1
    Filter-rules:
        10 deny sgt 30
        20 deny prefix 10.1.0.0/16
        30 permit sgt 60-100
    Peer-list: 172.16.0.1 192.168.0.1
```

The following sample output from the **show cts sxp filter-group** command displays information about all configured filter groups:

```
Device# show cts sxp filter-group

Global Listener Filter: Not configured

Global Speaker Filter: Not configured
```

```
Listener Group:
    Filter-group: group1
    Filter-name: filter1
    Peer-list: 172.16.0.1 192.168.0.1
    Filter-group: group2
    Filter-name: filter1
    Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1

Speaker Group:
    Filter-group: group3
    Filter-name: filter1
    Peer-list: 172.16.0.1 192.168.0.13
    Filter-group: group2
    Filter-name: filter1
    Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1
```

The following sample output from the **show sxp filter-group detailed** command displays detailed information about all configured SXP filter groups:

```
Device# show cts sxp filter-group detailed

Global Listener Filter: Configured
    Filter-name: global1
    Filter-rules:
        10 deny 192.168.0.13/32
        20 deny sgt 100-200

Global Speaker Filter: Configured
    Filter-name: global2
    Filter-rules:
        10 deny 192.168.0.13/32
        20 deny sgt 100-200

Listener Group:
    Filter-group: group1
    Filter-name: filter1
    Filter-rules:
        10 deny sgt 30
        20 deny prefix 172.16.0.0/16
        30 permit sgt 60-100
    Peer-list: 172.16.0.1, 192.168.0.13

    Filter-group: group2
    Filter-name: filter1
    Filter-rules:
        10 deny sgt 30
        20 deny prefix 172.16.0.0/16
        30 permit sgt 60-100
    Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1

Speaker Group
    Filter-group: group3
    Filter-name: filter1
    Filter-rules:
        10 deny sgt 30
        20 deny prefix 172.16.0.0/16
        30 permit sgt 60-100
    Peer-list: 10.10.10.1, 172.16.0.1, 192.168.0.13

    Filter-group: group2
    Filter-name: filter1
    Filter-rules:
        10 deny sgt 30
```

```
    20 deny prefix 172.16.0.0/16
    30 permit sgt 60-100
Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1
```

Syslog Messages for SXP Filtering

Syslog messages for SXP filtering are generated to indicate the various events related to filtering.

Syslog Messages for Filter Rules

The maximum number of rules that can be configured in a single filter is 128. The following message is generated every time the number of filter rules that is configured in a single filter increases by 20% of the limit:

```
CTS SXP filter rules exceed %[ ] threshold. Reached count of [count] out of [max] in
filter [filter-name].
```

The following message is generated when the number of rules configured in a single filter reaches 95% of the maximum number of rules allowed for a filter list:

```
CTS SXP filter rules exceed [ ] threshold. Reached count of [count] out of [max] in filter
[filter-name].
```

The following message is generated when the number of rules configured in a single filter reaches the maximum number of allowed rules, and no more rules can be added.

```
Reached maximum filter rules. Could not add new rule in filter [filter-name]
```

Syslog Messages for Filter Lists

The maximum number of filter lists that can be configured is 256. The following message is generated every time the number of filter lists that is configured increases by 20% of this limit:

```
CTS SXP filter rules exceed %[ ] threshold. Reached count of [count] out of [max] in
filter [filter-name].
```

The following message is generated when the number of filter lists that is configured reaches 95% of the maximum number of allowed filter lists:

```
CTS SXP filter rules exceed %[ ] threshold. Reached count of [count] out of [max]
```

The following message is generated when the number of filter lists that is configured reaches the maximum number of allowed filter lists, and no more filter lists can be added:

```
Reached maximum filter count. Could not add new filter
```

Feature Information for IP-Prefix and SGT-Based SXP Filtering

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for IP-Prefix and SGT-Based SXP Filtering

Feature Name	Releases	Feature Information
IP-Prefix and SGT-Based SXP Filtering	Cisco IOS Release 15.2(6)E	The IP-Prefix and SGT-Based SXP Filtering feature provides a filtering mechanism to solve the high IP-SGT bindings scale issue. The following commands were introduced: **debug cts sxp filter events**, **cts sxp filter-list**, **cts sxp filter-group**, **cts sxp filter-enable**, **show cts sxp filter-group**, **show cts sxp filter-list**.

SGT Inline Tagging

March 30, 2018

This section includes the following topics:

Information About SGT Inline Tagging

Overview of SGT Inline Tagging

Each security group in a Cisco TrustSec domain is assigned a unique 16 bit tag called the Security Group Tag (SGT). The SGT is a single label indicating the privileges of the source within the entire network. It is in turn propagated between network hops allowing any intermediary devices (switches, routers) to enforce polices based on the identity tag.

Cisco TrustSec-capable devices have built-in hardware capabilities than can send and receive packets with SGT embedded in the MAC (L2) layer. This feature is called Layer 2(L2)-SGT Imposition. It allows Ethernet interfaces on the device to be enabled for L2-SGT imposition so that the device can insert an SGT in the packet to be carried to its next hop Ethernet neighbor. SGT-over-Ethernet is a method of hop-by-hop propagation of SGT embedded in clear-text (unencrypted) Ethernet packets. The inline identity propagation is scalable, provides near line-rate performance and avoids control plane overhead.

The Cisco TrustSec with SGT Exchange Protocol V4 (SXPv4) feature supports Cisco TrustSec metadata-based L2-SGT. When a packet enters a Cisco TrustSec-enabled interface, the IP-SGT mapping database (with dynamic entries built by SXP and/or static entries built by configuration commands) is analyzed to learn the SGT corresponding to the source IP address of the packet, which is then inserted into the packet and carried throughout the network within the Cisco TrustSec header.

As the tag represents the group of the source, the tag is also referred to as the Source Group Tag (SGT). At the egress edge of the network, the group assigned to the packet's destination becomes known. At this point, access control can be applied. With Cisco TrustSec, access control policies are defined between the security groups and are referred to as Security Group Access Control Lists (SGACL). From the view of any given packet, SGACL is simply being sourced from a security group and destined for another security group.

The SGT tag received in a packet from a trusted interface is propagated to the network, and is also be used for Identity firewall classification. When IPsec support is added, the received SGT tag is shared with IPSec for SGT tagging.

A network device at the ingress of Cisco TrustSec cloud needs to determine the SGT of the packet entering the Cisco TrustSec cloud so that it can tag the packet with that SGT when it forwards it into the Cisco TrustSec cloud. The SGT of a packet can be determined with these methods:

SGT field on Cisco TrustSec header: If a packet is coming from a trusted peer device, it is assumed that the Cisco TrustSec header carries the correct SGT field. This situation applies to a network that is not the first network device in the Cisco TrustSec cloud for the packet.

SGT lookup based on source IP address: In some cases, the administrator may manually configure a policy to decide the SGT of a packet based upon the source IP address. An IP address to SGT table can also be populated by the SXP protocol.

L2 Inline Tagging is supported for IPv6 multicast traffic with unicast source IPv6 addresses.

SGT Inline Tagging on a NAT Enabled Device

Note This section is applicable only for Cisco Catalyst 9000 Series Switches beginning from Cisco IOS XE 16.8.x release.

The following scenarios explain how SGT is determined for a packet that flows from a primary device, which has Network Address Translation (NAT) enabled on both ingress and egress ports, to a secondary device:

Note All ports that are used for the flow must have **CTS manual** and trusted configured on both devices.

- If inline tagging is enabled between both devices and SGT tag is not changed with CLI:

  In this case, on the primary device Cisco TrustSec is enforced on the SGT tag corresponding to the packet's source IP. The same SGT tag is tagged to the NAT IP. On the secondary device, Cisco TrustSec is enforced on the SGT tag corresponding to the packet's source IP also.

  For example, a packet is received on the primary device with a source IP 192.0.2.5 and SGT tag 133. Cisco TrustSec is enforced for the SGT tag 133 on the primary device. After NAT translation the packet's IP changes to 198.51.100.10 and tagged to the SGT tag 133. On the secondary device, the packet is received with IP address 198.51.100.10 and SGT tag 133. Cisco TrustSec is enforced with SGT tag 133 on the secondary device.

- If inline tagging is enabled between both devices and SGT tag is changed with CLI:

  In this case, on the primary device Cisco TrustSec is enforced on the SGT tag corresponding to the packet's source IP. The SGT tag is changed by CLI but the SGT tag corresponding to the packets's source IP is tagged to the packet's NAT IP. On the secondary device, Cisco TrustSec is enforced on the SGT tag corresponding to the packet's source IP also.

  For example, a packet is received on the primary device with a source IP 192.0.2.5 and SGT tag 133. Cisco TrustSec is enforced for the SGT tag 133 on the primary device. The SGT tag is changed to 200 with CLI. After NAT translation the packet’s IP changes to 198.51.100.10 but tagged to the SGT tag 133. On the secondary device, the packet is received with IP address 198.51.100.10 and SGT tag 133. Cisco TrustSec is enforced on the SGT tag 133 on the secondary device.

- If inline tagging is disabled (SGT is populated through SXP protocol on the secondary device) and SGT tag is changed with CLI:

  In this case, on the primary device Cisco TrustSec is enforced on the SGT tag corresponding to the packet's source IP. The SGT to Post Nat IP is defined through CLI and is learnt on the primary device. On the secondary device, Cisco TrustSec is enforced on the SGT tag corresponding to the NAT IP, if there is no direct Cisco TrustSec link between primary and secondary device and IP to SGT bindings are learnt through SXP in secondary device.

  For example, a packet is received on the primary device with a source IP 192.0.2.5 and SGT tag 133. After NAT translation the source IP changes to 198.51.100.10, for which the SGT is defined through CLI as 200. Cisco TrustSec is enforced for the SGT tag 133 on the primary device. On the secondary device, IP to SGT binding is received through SXP and Cisco TrustSec is enforced on the SGT tag 200 on the secondary device.

Configuring SGT Inline Tagging

Detailed Steps

	Command	Purpose
Step 1	`Device# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Device# configure terminal`	Enters global configuration mode.
Step 3	`Device(config)# interface {gigabitethernet port | vlan number}`	Configures the interface on which Cisco TrustSec SGT authorization and forwarding is enabled, and enters interface configuration mode.
Step 4	`Device(config-if)# cts manual`	Enables Cisco TrustSec SGT authorization and forwarding on the interface, and enters Cisco TrustSec manual interface configuration mode.
Step 5	`Device(config-if-cts-manual)# propagate sgt`	Enables Cisco TrustSec SGT propagation on an interface. • Use this command in situations where the peer device is not capable of receiving SGT over Ethernet packets (that is, when a peer device does not support Cisco Ethertype CMD 0x8909 frame format).
Step 6	`Device(config-if-cts-manual)# policy static sgt tag [trusted]`	Configures a static SGT ingress policy on the interface and defines the trustworthiness of an SGT received on the interface. **Note** The **trusted** keyword indicates that the interface is trustworthy for Cisco TrustSec. The SGT value received in the Ethernet packet on this interface is trusted and will be used by the device for any SG-aware policy enforcement or for the purpose of egress-tagging

	Command	Purpose
Step 7	`Device(config-if-cts-manual)# end`	Exits Cisco TrustSec manual interface configuration mode and enters privileged EXEC mode.

Step 8	`Device# show cts interface brief`
	
	`Interface Gigabit Ethernet Gi1/0/1`
	`  Cisco TrustSec is enabled, mode: MANUAL`
	`  Propagate SGT:  Enabled`
	`  Peer SGT assignment:  Trusted`
	
	`Interface Gigabit Ethernet Gi1/0/1`
	`  Cisco TrustSec is enabled, mode: MANUAL`
	`  Propagate SGT:  Disabled`
	`  Peer SGT assignment:  Untrusted`
	
	`Interface GigabitEthernet0/3`
	`  Cisco TrustSec is disabled.`
		Displays Cisco TrustSec configuration statistics for the interface.

Configuration Examples for SGT Inline Tagging

Example: SGT Static Inline Tagging

This example shows how to enable an interface on the device for L2-SGT tagging or imposition and defines whether the interface is trusted for Cisco TrustSec

```
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# cts manual
Device(config-if-cts-manual)# propagate sgt
Device(config-if-cts-manual)# policy static sgt 77 trusted
```

Feature Information for SGT Inline Tagging

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 9-1 Feature Information for SGT Inline Tagging

Feature Name	Releases	Feature Information
SGT Inline Tagging -IPv6 enablement	Cisco IOS XE Fuji 16.8.1	Each security group in a Cisco TrustSec domain is assigned a unique 16 bit tag called the Security Group Tag (SGT). The SGT is a single label indicating the privileges of the source within the entire network. It is in turn propagated between network hops allowing any intermediary devices (switches, routers) to enforce polices based on the identity tag. This feature was introduced.

Configuring Cisco TrustSec Reflector and Caching

Revised: August 31, 2017

This module describes the Cisco TrustSec Reflector for Cisco TrustSec Reflector and the Cisco Trustsec Caching features.

Note This feature is not supported on Catalyst 3650, 3850, 9300, 9400, and 9500 Series Switches.

Note The Cisco TrustSec supervisor ingress reflector and the Cisco TrustSec egress reflector are mutually exclusive. Do not enable both functions.

Egress reflector should be disabled when ERSPAN is configured.

To configure the Cisco TrustSec supervisor ingress reflector function, perform this task.

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters configuration mode.
Step 2	`Switch(config)# [no] platform cts ingress`	Activates the Cisco TrustSec supervisor ingress reflector.
Step 3	`Switch(config)# exit`	Exits configuration mode.
Step 4	`Switch# show platform cts`	Displays Cisco TrustSec reflector mode (Ingress, Egress, Pure, or No CTS).

This example shows how to configure a Cisco TrustSec ingress reflector:

```
Switch# configure terminal
Switch(config)# platform cts ingress
Switch(config)# exit
Switch# show platform cts
 CTS Ingress mode enabled
```

Note Before disabling the Cisco TrustSec ingress reflector, you must remove power from the Cisco TrustSec-incapable switching modules.

To configure the Cisco TrustSec egress reflector function, perform this task.

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters configuration mode.
Step 2	`Switch(config)# [no] platform cts egress`	Activates the Cisco TrustSec egress reflector.
Step 3	`Switch(config)# exit`	Exits configuration mode.
Step 4	`Switch# show platform cts`	Displays Cisco TrustSec reflector mode (Ingress, Egress, Pure, or No CTS).

This example shows how to configure a Cisco TrustSec egress reflector:

```
Switch# configure terminal
Switch(config)# platform cts egress
Switch(config)# exit
Switch# show platform cts
 CTS Egress mode enabled
```

Note Before disabling the Cisco TrustSec egress reflector, you must remove power from the Cisco TrustSec-incapable switching modules.

Configuring Cisco TrustSec Caching

For quick recovery from brief outages, you can enable caching of authentication, authorization, and policy information for Cisco TrustSec connections. Caching allows Cisco TrustSec devices to use unexpired security information to restore links after an outage without requiring a full reauthentication of the Cisco TrustSec domain. The Cisco TrustSec devices will cache security information in DRAM. If non-volatile (NV) storage is also enabled, the DRAM cache information will also be stored to the NV memory. The contents of NV memory populate DRAM during a reboot.

Enabling Cisco TrustSec Caching

Note During extended outages, the Cisco TrustSec cache information is likely to become outdated.

To enable Cisco TrustSec caching, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters configuration mode.
Step 2	`Switch(config)# [no] cts cache enable`	Enables caching of authentication, authorization and environment-data information to DRAM. The default is disabled. The **no** form of this command deletes all cached information from DRAM and non-volatile storage.
Step 3	`Switch(config)# [no] cts cache nv-storage {bootdisk: | bootflash: | disk0:} [directory dir-name]`	When DRAM caching is enabled, enables DRAM cache updates to be written to non-volatile storage. Also enables DRAM cache to be initially populated from non-volatile storage when the device boots.
Step 4	`Switch(config)# exit`	Exits configuration mode.

This example shows how to configure Cisco TrustSec caching, including non-volatile storage:

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

Clearing the Cisco TrustSec Cache

To clear the cache for Cisco TrustSec connections, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Switch# clear cts cache [authorization-policies [peer] | environment-data | filename filename | interface-controller [type slot/port]]`	Clears the cache for Cisco TrustSec connection information.

This example shows how to clear the Cisco TrustSec cache:

```
Switch# clear cts cache
```

Feature Information for Cisco TrustSec Reflector and Caching

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1 Feature Information for Cisco TrustSec Reflector and Caching

Feature Name	Releases	Feature Information
Cisco TrustSec Reflector	Cisco IOS Release 12.2(50) SY	This feature was introduced on Cisco Catalyst 6500 Series Switches.
Cisco TrustSec Caching	Cisco IOS Release 12.2(50) SY	This feature was introduced on Cisco Catalyst 6500 Series Switches.

Configuring Endpoint Admission Control

Revised: May 28, 2010

This chapter contains the following sections:

Information About Endpoint Admission Control

In TrustSec networks, packets are filtered at the egress, not the ingress to the network. In TrustSec endpoint authentication, a host accessing the TrustSec domain (endpoint IP address) is associated with a Security Group Tag (SGT) at the access device through DHCP snooping and IP device tracking. The access device transmits that association (binding) through SXP-to-TrustSec hardware-capable egress devices, which maintain a continually updated table of Source IP to SGT bindings. Packets are filtered on egress by the TrustSec hardware-capable devices by applying security group ACLS (SGACLs).

Endpoint Admission Control (EAC) access methods for authentication and authorization can include the following:

- 802.1X port-based Authentication
- MAC Authentication Bypass (MAB)
- Web Authentication (WebAuth)

All port-based authentication can be enabled with the **authentication** command. Each access method must be configured individually per port. The flexible authentication sequence and failover features permit the administrator to specify the failover and fallback sequence when multiple authentication modes are configured and the active method fails. The 802.1X host mode determines how many endpoint hosts can be attached per 802.1X port.

Basic EAC Configuration Sequence

1. Configure the Cisco Secure ACS to provision SGTs to authenticated endpoint hosts.
2. Enable SXP on access switches. See the chapter, "Configuring SGT Exchange Protocol."
3. Enable any combination of 802.1X, MAB, or WebAuth authentication methods on the access switch.
4. Enable DHCP and IP device tracking on access switches.

802.1X Authentication Configuration

The following example shows the basic 802.1x configuration on a Gigabit Ethernet port:

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface GigabitEthernet2/1
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
```

Verifying the 802.1X Configuration

To verify 802.1X authentication configuration, use the **show authentication interface** command.

```
Switch# show authentication interface gigabitEthernet 2/1
*May  7 11:22:06: %SYS-5-CONFIG_I: Configured from console by console

Client list:
  Interface  MAC Address     Domain   Status         Session ID
  Gi2/1      000c.293a.048e  DATA     Authz Success  AC1AD01F0000000904BBECD8

Available methods list:
  Handle  Priority  Name
    3        0      dot1x
Runnable methods list:
  Handle  Priority  Name
    3        1      dot1x
```

And to verify the port has successfully authenticated:

```
Switch# show dot1x interface gigabitEthernet 2/1 details

Dot1x Info for GigabitEthernet2/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Authenticator Client List
-------------------------------
Supplicant                = 000c.293a.048e
Session ID                = AC1AD01F0000000904BBECD8
    Auth SM State         = AUTHENTICATED
```

```
    Auth BEND SM State    = IDLE
Port Status               = AUTHORIZED
```

MAC Authentication Bypass Configuration

MAC Authentication Bypass (MAB) enables hosts or clients that are not 802.1X capable to join 802.1X-enabled networks. It is not required to enable 802.1X authentication prior to enabling MAB.

The following example is a basic MAB configuration on a Catalyst switch:

```
switch(config)# interface GigabitEthernet2/1
switch(config-if)# authentication port-control auto
switch(config-if)# mab
```

For additional information on configuring MAB authentication, see the configuration guide for your access switch.

Verifying the MAB Configuration

To verify the MAC Authentication Bypass configuration, use the **show authentication interface** command.

```
switch# show authentication interface gigabitEthernet 2/1

Client list:
  Interface  MAC Address     Domain   Status         Session ID
  Gi2/1      000c.293a.048e  DATA     Authz Success  AC1AD01F0000000A04CD41AC

Available methods list:
  Handle  Priority  Name
    2        1      mab
Runnable methods list:
  Handle  Priority  Name
    2        0      mab
```

To verify that the port has successfully authenticated, use the **show mab interface** command.

```
switch# show mab interface gigabitEthernet 2/1 details
MAB details for GigabitEthernet2/1
-------------------------------------
Mac-Auth-Bypass           = Enabled

MAB Client List
---------------
Client MAC                = 000c.293a.048e
Session ID                = AC1AD01F0000000A04CD41AC
MAB SM state              = ACQUIRING
Auth Status               = UNAUTHORIZED
```

Web Authentication Proxy Configuration

Web Authentication Proxy (WebAuth) allows the user to use a web browser to transmit their login credentials to the Cisco Secure ACS though a Cisco IOS web server on the access device. WebAuth can be enabled independently. It does not require 802.1X or MAB to be configured.

The following example shows a basic WebAuth configuration on a Gigabit Ethernet port:

```
switch(config)# ip http server
switch(config)# ip access-list extended POLICY
switch(config-ext-nacl)# permit udp any any eq bootps
switch(config-ext-nacl)# permit udp any any eq domain
switch(config)# ip admission name HTTP proxy http
switch(config)# fallback profile FALLBACK_PROFILE
switch(config-fallback-profile)# ip access-group POLICY in
switch(config-fallback-profile)# ip admission HTTP
switch(config)# interface GigabitEthernet2/1
switch(config-if)# authentication port-control auto
switch(config-if)# authentication fallback FALLBACK_PROFILE6500(config-if)#ip access-group
POLICY in
```

Verifying Web Authentication Proxy Configuration

To verify the Web Authentication Proxy configuration, access the interface IP address with a web browser. If configured correctly, the access device generates a challenge and accepts valid login information.

To verify the Web Authentication proxy configuration with the CLI, use the **show authentication interface** command.

```
switch# show authentication interface gigabitEthernet 2/1

Client list:
  Interface  MAC Address     Domain   Status         Session ID
  Gi2/1      000c.293a.048e  DATA     Authz Success  AC1AD01F0000000904BBECD8

Available methods list:
  Handle  Priority  Name
    1        2      webauth
Runnable methods list:
  Handle  Priority  Name
    1        0      webauth
```

Flexible Authentication Sequence and Failover Configuration

Flexible Authentication Sequence (FAS) allows the access port to be configured for 802.1X, MAB, and WebAuth authentication methods, specifying the fallback sequence if one or more of the authentication methods are not available. The default failover sequence is as follows:

- 802.1X port-based Authentication
- MAC Authentication Bypass
- Web Authentication

Layer 2 authentications always occur before Layer 3 authentications. That is, 802.1X and MAB must occur before WebAuth.

The following example specifies the authentication sequence as MAB, dot1X, and then WebAuth.

```
switch(config)# interface gigabitEthernet 2/1
switch(config-if)# authentication order mab dot1x webauth
switch(config-if)^Z
```

For additional information on FAS, see the Cisco document, *Flexible Authentication Order, Priority, and Failed Authentication* at the following URL:

http://www.ciscosystems.com.pe/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/application_note_c27-573287_ps6638_Products_White_Paper.html

802.1X Host Modes

Four host classification modes can be configured per port:

- Single Host —Interface-based session with one MAC address
- Multi Host—Interface-based session with multiple MAC addresses per port
- Multi Domain—MAC + Domain (VLAN) session
- Multi Auth—MAC-based session with multiple MAC address per port

Pre-Authentication Open Access

The Pre-Authentication Open Access feature allows clients and devices to gain network access before port authentication is performed. This process is primarily required for the PXE boot scenario, where a device needs to access the network before PXE times out and download a bootable image that may contain a supplicant.

DHCP Snooping and SGT Assignment

After the authentication process, authorization of the device occurs (for example, dynamic VLAN assignment, ACL programming, etc.). For TrustSec networks, a Security Group Tag (SGT) is assigned per the user configuration in the Cisco ACS. The SGT is bound to traffic sent from that endpoint through DHCP snooping and the IP device tracking infrastructure.

The following example enables DHCP snooping and IP device tracking on an access switch:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping vlan 10
switch(config)# no ip dhcp snooping information option
switch(config)# ip device tracking
```

Verifying the SGT to Endpoint Host Binding

To verify that hosts are visible to DHCP Snooping and IP Device Tracking, use the **show ip dhcp snooping binding** and **show ip device tracking** commands.

```
switch# show ip dhcp snooping binding

MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:0C:29:3A:04:8E   10.252.10.10     84814       dhcp-snooping   10    GigabitEthernet2/1
Total number of bindings: 1


switch# show ip device tracking all

IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------
  IP Address     MAC Address       Interface          STATE
-----------------------------------------------------------
10.252.10.10    000c.293a.048e GigabitEthernet2/1     ACTIVE
```

To verify that the correct SGT is bound to an endpoint IP address, use the **show cts role-based sgt-map** command.

```
switch# 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
```

Cisco TrustSec Endpoint Access Control Feature Histories

For a list of supported platforms, supported features, and the minimum required IOS releases, see the *Cisco TrustSec Platform Support Matrix* at the following URL:

http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html

Otherwise, see product release notes for detailed feature introduction information.

Cisco TrustSec Command Summary

Revised: August 3, 2016

Cisco TrustSec Privileged EXEC Commands	
cts change-password	Initiates password change with AAA server. **Note** Effective with Cisco IOS Release 15.1(1)SY, this command is not available in Cisco IOS software.
cts credentials	Inserts Cisco TrustSec device ID and password into the keystore.
cts refresh	Refreshes environment, peer and RBACL policies.
cts rekey	Regenerates the Pairwise Master Key used by the Security Association Protocol (SAP),
cts role-based policy trace	TrustSec SGT and SGACL trace utility.
Cisco TrustSec Global Configuration Commands	
cts authorization list	Configures Cisco TrustSec global authorization configuration.
cts cache	Enables caching of TrustSec authorization and environment-data information to DRAM and NVRAM.
cts manual	Defines Cisco TrustSec keystore behavior.
cts policy layer3	Specifies traffic and exception policies for Cisco TrustSec Layer 3 Transport gateway interfaces.
cts role-based	Maps IP addresses, Layer 3 interfaces, and VRFs to SGTs. Enables Cisco TrustSec caching and SGACL enforcement.
cts server	Configures RADIUS server list configuration.
cts sgt	Configures local device security group tag.

cts sxp	Configures SGT exchange over TCP.
platform-cts	Enables subnet SGT derivation for switched (layer 2) traffic and enables Cisco Meta Data (CMD) tagging exemption for incoming and outgoing control packets.
Cisco TrustSec Flexible NetFlow Commands	
match flow cts	Adds Cisco TrustSec flow objects to a Flexible NetFlow flow record.

Cisco TrustSec Interface Configuration Commands

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

Cisco TrustSec dot1x Submode Commands

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

Cisco TrustSec Manual Interface Configuration Submode Commands

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

Cisco TrustSec Clear Commands

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

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

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

cts authorization list

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

cts authorization list *server_list*

no cts authorization list *server_list*

Syntax Description

server_list	Cisco TrustSec AAA server group.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

cts cache

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

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

Syntax Description

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

Defaults

Caching is disabled.

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

Examples

The following example shows how to enable cache support:

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

Related Commands

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

cts change-password

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

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

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

Syntax Description

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

Defaults

None.

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

cts credentials

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

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

Syntax Description

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

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

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

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

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

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

```
Switch# show cts credentials

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

Related Commands

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

cts dot1x

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

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

Syntax Description

This command has no arguments or keywords.

Defaults

CTS dot1x configuration on the interface is disabled.

Command Modes

Interface configuration (config-if)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

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

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

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

Related Commands

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

default timer reauthentication (cts interface)

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

default timer reauthentication

Syntax Description

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

Defaults

3600 seconds

Command Modes

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

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

timer reauthentication (cts interface)

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

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

Syntax Description

reauthentication *seconds*	Sets the reauthentication timer in seconds.

Defaults

The reauthentication timer is not configured.

Command Modes

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

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

cts layer3

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

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

Syntax Description

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

Defaults

Cisco TrustSec Layer3 Transport is not enabled.

Command Modes

Interface configuration (config-if)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

cts manual

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

cts manual

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Interface configuration (config-if)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

cts policy layer3

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

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

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

Syntax Description

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

Defaults

No policy is configured.

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

Related Commands

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

cts refresh

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

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

Syntax Description

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

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

```
VSS-1# show cts policy peer

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

Related Commands

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

cts rekey

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

cts rekey interface type *slot*/*port*

Syntax Description

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

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

cts role-based policy trace

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

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

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

Syntax Description

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

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

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

Command Default None

Command Modes Privileged EXEC (#)

SupportedUserRoles Administrator

Command History

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

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

1. Discover the network path.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Related Commands

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

cts role-based

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Syntax Description

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

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

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

Single Host Address-to-SGT Binding

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

Network or Subnetwork Addresses-to-SGT Binding

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

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

VRF-to-SGT Bindings

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

VLAN-to-SGT Mapping

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

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

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

Layer 3 Interface Mapping (L3IF)

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

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

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

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

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

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

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

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

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

Binding Source Priorities

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

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

Layer 2 VRF Assignment

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

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

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

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

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

Role-based Enforcement

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

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

VLAN Enforcement

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

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

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

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

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

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

Defining an IPv4 RBACL

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

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

Defining an IPv4 RBACL ACE

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

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

Definin an IPv6 RBACL

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

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

Defining an IPv6 RBACL ACE

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

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

Attaching SGACL Policies

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

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

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

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

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

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

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

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

Flexible Net Flow

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

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

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

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

Getting Started with Configuring Cisco IOS Flexible NetFlow

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

Cisco IOS Flexible NetFlow Configuration Guide, Release 15.0SY

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

Examples

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

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

Switch# show cts role-based sgt-map all

Active IP-SGT Bindings Information

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

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

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

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

Related Commands

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

cts server

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

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

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

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

Syntax Description

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

Defaults

Deadtime	20 seconds
Batch-size	25 transactions

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

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

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

Switch# show cts server-list

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

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

Related Commands

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

cts server test

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

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

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

Syntax Description

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

Defaults

Test is enabled for all servers.

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

Examples

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

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

Switch# show cts server-list

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

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

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

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

Related Commands

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

cts sgt

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

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

Syntax Description

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

Defaults

No SGT number is assigned.

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

cts sxp

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

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

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

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

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

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

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

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

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

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

Syntax Description

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

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

Defaults

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

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

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

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

Usage Guidelines

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

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

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

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

SXP connections are governed by three timers:

- Retry timer
- Delete Hold Down timer
- Reconciliation timer

Retry Timer

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

Delete Hold Down Timer

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

Reconciliation Timer

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

Examples

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

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

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

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

Related Commands

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

clear cts cache

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

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

clear cts cache environment-data

clear cts cache filename *file*

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

Syntax Description

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

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Examples

The following example deletes environment data from the cache:

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

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

Related Commands

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

clear cts counter

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

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

Syntax Description

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

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

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

clear cts credentials

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

clear cts credentials

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Examples

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

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

Related Commands

Command	Description
cts credentials	Specifies the TrustSec ID and password.

clear cts environment-data

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

clear cts environment-data

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Examples

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

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

Related Commands

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

clear cts macsec

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

clear cts macsec counters interface type *slot/port*

Syntax Description

interface type *slot/port*	Specifies the interface.

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Examples

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

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

Related Commands

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

clear cts pac

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

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

Syntax Description

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

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Examples

The following command clears all PACs in the keystore:

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

Related Commands

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

clear cts policy

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

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

Syntax Description

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

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

clear cts role-based counters

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

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

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

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

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

Syntax Description

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

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

```
Switch# show cts role-based counters

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

Related Commands

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

clear cts server

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

clear cts server *ip-address*

Syntax Description

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

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

default (cts dot1x)

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

default propagate sgt

default sap

default timer reauthentication

Syntax Description

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

Defaults

None

Command Modes

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

SupportedUserRoles

Administrator

Command History

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

Examples

The following example re-enables SGT propagation:

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

Related Commands

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

debug condition cts

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

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

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

switch# show debug condition
```

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

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

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

switch# show debug condition

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

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

Related Commands

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

default (cts manual)

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

default policy dynamic identity

default policy static sgt

default propagate sgt

default sap

Syntax Description

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

Command Modes

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

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

match flow cts

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

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

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

Syntax Description

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

Defaults

None

Command Modes

Flexible NetFlow record configuration (config-flow-record)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

platform cts

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

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

Syntax Description

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

Defaults

Ingress or egress reflectors are not configured.

Command Modes

Global configuration (config)

SupportedUserRoles

Administrator

Command History

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

Examples

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

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

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

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

Related Commands

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

policy (cts manual)

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

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

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

Syntax Description

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

Defaults

Policy is not configured.

Command Modes

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

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

Examples

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

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

Switch# show cts interface GigabitEthernet 2/1

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

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

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

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

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

Related Commands

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

platform-cts

To exempt control Protocol Data Units (PDUs) from Cisco Meta Data (CMD) tagging, or to enable subnet security group tag (SGT) derivation for switched traffic, configure the **platform-cts** command in global configuration mode. To disable either function, enter the **no** version of the command.

platform-cts {**stub l2-control-pdu cmd-exempt** | **subnet-sgt l2traffic enable**}

no platform-cts {**stub l2-control-pdu cmd-exempt** | **subnet-sgt l2traffic enable**}

Syntax Description

stub l2-control-pdu cmd-exempt	Enables exemption of control PDUs from CMD tagging.
subnet-sgt l2traffic enable	Enables SGT derivation for switched traffic.

Defaults

SGT derivation and CMD tagging exemption are both disabled by default.

Command Modes

Global configuration

SupportedUserRoles

Administrator

Command History

Release	Modification
Cisco IOS XE Release 3.8.6E and Cisco IOS XE Release 15.2(4)E6	This command was introduced Catalyst 4500 series switches.
Cisco IOS XE Release 3.9.xE and Cisco IOS XE Release 15.2(5)Ex	This command is not supported on this release train.
Cisco IOS XE Release 3.10.0E and Cisco IOS XE Release 15.2(6)E0	This command is supported again starting from this release and all later releases.
Cisco IOS XE Release 3.11.0E	The **stub l2-control-pdu cmd-exempt** keywords were introduced on the Cisco Catalyst 4500E and 4500-X Series Switches.

Usage Guidelines

SGT Derivation for Switched Traffic

With Cisco TrustSec, Catalyst 4500 switches can classify packets transmitted through the switch into different user groups. Depending on the user group of a packet, specific actions can then be imposed on the packet. The SGT enables you to impose these actions.

An SGT may be a source user group tag or a destination user group tag. A source user group tag is added by a switch that is close to the source of the packet, and a destination user group tag is added by a switch in the same network, but closer to the destination of the packet.

The addition of the source user group tag for both switched and routed packets is handled by the forwarding engine of switch, with the help of the Forward Information Base (FIB). The addition of a destination user group tag for a routed packet is also handled by the forwarding engine, but the addition of a destination user group tag for a *switched* packet is handled by the input ACL engine, with the help of input ACL TCAM entries.

When you add a new SGT binding, the new entry is programmed into the first available free space in the TCAM block - in the order of entry. For example, if you add entries in the order shown below, the generic entry (1.0.0.0/8) is programmed in the lowest index, and not the specific entry (1.0.0.1).

```
Switch(config)#cts role-based sgt-map 1.0.0.0/8 sgt 20     !!Generic entry
Switch(config)#cts role-based sgt-map 1.0.0.1 sgt 10       !!Specific entry
```

TCAM search progresses from the lowest index of the block to the highest index and search stops when the first matching entry is found. When traffic ingresses the switch, the above entries mean that for a packet with destination IP address 1.0.0.1, the TCAM lookup is matched to generic entry 1.0.0.0/8 and destination user group tag 20 is assigned, even though you have made a more specific entry for packets with the destination address 1.0.0.1.

To program TCAM entries in an optimal way and to ensure that TCAM search matches specific entries (when they are available), enter the **platform-cts subnet-sgt l2traffic enable** command in global configuration mode.

Note Before you enable or disable [**no**] **platform-cts subnet-sgt l2traffic enable**, ensure that you have disabled Cisco TrustSec global enforcement, that is, ensure that you have configured the **no cts role-based enforcement** command in global configuration mode.

The [**no**] **platform-cts subnet-sgt l2traffic enable** command applies to IPv4 and 1Pv6 addresses.

Use the **show running-config** command in privileged EXEC mode to know if **platform-cts subnet-sgt l2traffic enable** command is enabled. For example:

```
Switch(config)# platform-cts subnet-sgt l2traffic enable
Switch(config)# end
Switch# show running-config | in platform-cts
platform-cts subnet-sgt l2traffic enable
```

Exemption of Control PDUs from CMD Tagging

Cisco TrustSec-enabled devices support the enforcement of policies on packets based on a pair of SGTs. SGTs are propagated hop-by-hop, between neighboring peers. The CMD file in a packet's header carries the relevant SGT information.

In a typical layer 2 operation, the CMD header is inserted in the frame header before being sent out of a Cisco TrustSec-enabled interface. This is done by configuring the **cts manual** command in interface configuration mode, and the **propagate sgt** command in Cisco TrustSec manual interface configuration mode. After the packet is received by the peer switch, the CMD tag is parsed and the SGT, extracted.

Note When you configure the **propagate sgt** Cisco TrustSec manual interface configuration command on a link, a Catalyst 4500 switch adds the CMD header in the L2 frame header for *all* packets, control and data.

If a peer switch is unable to process a layer 2 frame (and drops such packets), then consider exempting CMD tagging by entering the **platform-cts stub l2-control-pdu cmd-exempt** command in global configuration mode. By enabling the command, you can exempt the control PDUs leaving a Catalyst 4500 switch, from CMD tagging, and also accept packets transmitted on a Cisco TrustSec-enabled link without a CMD tag.

For example, certain linecards in the Cisco Nexus 7000 Series cannot process a Layer 2 packet unless it has a 802.1Q tag. If such a line card is a peer for a Catalyst 4500 switch, you may encounter the following situation and may want to configure the command:
A trunk port on the Catalyst 4500 switch transmits selected control packets through a native VLAN. Further, the packets are transmitted with a CMD tag (because the corresponding interfaces are configured to add a CMD header), but without a 802.1Q tag (either because native VLAN tagging is not enabled or because some control packets do not support tagging), then such packets are dropped by the peer. Configure the **platform-cts stub l2-control-pdu cmd-exempt** command to prevent such pack drops.

Note For the CMD tagging exemption to work as expected, configure the **platform-cts stub l2-control-pdu cmd-exempt** command in global configuration mode first and then the **cts manual** command in interface configuration mode. If **cts manual** is already configured, then disable and reenable on the required interfaces.

The CMD tagging exemption option is not meant for, and does not serve as a workaround for these cases: Certain linecards in the Cisco Nexus 7000 Series can process a L2 frame that has a CMD tag, only if there is a 802.1Q tag. If the link between a Catalyst 4500 and a Nexus 7000 device is an *access link* then you can assume that the packet is without 802.1Q tag (on an access port on a Catalyst 4500 switch, both data and control packet go out without a 802.1Q tag).

Similarly, you cannot use this command in case of a trunk port, where data packets go out with 802.1Q tag on tagged VLANs and without 802.1Q tag on a native VLAN.

Use the **show running-config** command in privileged EXEC mode to know if **platform-cts stub l2-control-pdu cmd-exempt** command is enabled.

Related Commands

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

propagate sgt (cts dot1x)

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

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

Syntax Description This command has no arguments or keywords.

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

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

SupportedUserRoles Administrator

Command History

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

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

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

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

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

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

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

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

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

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:

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

Related Commands

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

propagate sgt (cts manual)

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

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

Syntax Description This command has no keywords or arguments.

Defaults SGT is propagated.

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

SupportedUserRoles Administrator

Command History

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

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

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

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

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

This behavior is governed by the following table:

Table 3.2: SGT Propagate Behavior Table

Table 12-1

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

Table 12-1

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

Examples

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

```
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk FFFE
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# exit
Switch(config)# exit
Switch# show running-config
. . .
interface GigabitEthernet6/2
 ip address 172.16.4.12 255.255.255.0
cts manual
  no propagate sgt
  sap pmk 00000000000000000000000000000000000000000000000000000000000000000FFFE
. . .
```

Related Commands

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

sap (cts dot1x)

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

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

Syntax Description

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

Defaults

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

Command Modes

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

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

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

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

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

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

Examples

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

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

Related Commands

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

sap (cts manual)

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

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

Syntax Description

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

Defaults

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

Command Modes

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

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

show cts

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

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

Syntax Description

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

Defaults

None

Command Modes

EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Examples

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

```
Switch# show cts

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

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

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

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

Related Commands

Command	Description
cts credentials	Specifies the TrustSec ID and password.

show cts authorization entries

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

show cts authorization entries

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Examples

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

```
Switch# show cts authorization entries

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

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

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

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

Related Commands

Command	Description
cts credentials	Specifies the TrustSec ID and password.

show cts credentials

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

show cts credentials

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Examples

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

```
Switch# show cts credentials

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

Related Commands

Command	Description
cts credentials	Specifies the TrustSec ID and password.

show cts environment-data

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

show cts environment-data

Syntax Description This command has no arguments or keywords.

Defaults None

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

SupportedUserRoles Administrator

Command History

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

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

```
Switch# show cts environment-data

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

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

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

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

Related Commands

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

show cts interface

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

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

Syntax Description

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

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

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

```
Switch# show cts interface

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

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

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

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

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

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

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

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

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

```
Switch# show cts interface brief

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

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

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

```
Switch# show cts interface summary

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

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

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

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

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

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

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

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

```
Switch# show cts interface summary

Global Dot1x feature is Disabled


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

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

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

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

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

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

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

    Selected cipher:        null

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

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

Related Commands

Command	Description
cts sxp	Configures SXP on a network device.

show cts macsec

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

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

Syntax Description

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

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

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

show cts pacs

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

show cts pacs

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

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

```
Switch# show cts pacs

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

Switch# show cts pacs

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

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

Related Commands

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

show cts policy layer3

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

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

Syntax Description

ipv4	Specifies IPv4 policies.
ipv6	Specifies IPv6 policies

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

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

```
Switch# show cts policy layer3 ipv4

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

Related Commands

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

show cts policy peer

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

show cts policy peer

Syntax Description This command has no arguments or keywords.

Defaults None

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

SupportedUserRoles Administrator

Command History

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

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

```
VSS-1# show cts policy peer

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

The following table describes the output fields.

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

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

Related Commands

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

show cts provisioning

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

show cts provisioning

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

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

```
Switch# show cts provisioning

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

Related Commands

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

show cts rbacl

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

show cts rbacl [*name-list*]

Syntax Description

name-list	(Optional) RBACL lists.

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

The following sample output displays information about all RBACLs:

```
Switch# show cts rbacl

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

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

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

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

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

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

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

The following sample output displays information about RBACL101:

```
Switch# show cts rbacl RBACL101

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

show cts role-based counters

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

show cts role-based counters

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

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

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

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

Syntax Description

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

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

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

Examples

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

```
Switch# show cts role-based counters

Role-based counters

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

Related Commands

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

show cts role-based flow

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

clear cts role-based flow

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Privileged EXEC (#)

SupportedUserRoles Administrator

Command History

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

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

show cts role-based permissions

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

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

Syntax Description

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

Defaults

None

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

```
Switch# show cts role-based permissions

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

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

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

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

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

Related Commands

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

show cts role-based sgt-map

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

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

Syntax Description

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

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Active IP-SGT Bindings Information

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

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

Related Commands

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

show cts server-list

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

show cts server-list

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Examples

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

```
Switch> show cts server-list

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

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

Related Commands

Command	Description
cts server	Displays Cisco TrustSec server list configuration.

show cts sxp

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

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

Syntax Description

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

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

The following sample output displays the default SXP configuration:

```
Switch# show cts sxp connections

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

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

```
Switch# show cts sxp connection brief

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

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

Total num of SXP Connections = 2
```

The following sample output displays all SXP connections:

```
Switch# show cts sxp connections

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

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


Total num of SXP Connections = 2
```

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

```
Switch# show cts sxp connections

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

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

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

Total num of SXP Connections = 2
```

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

```
Switch# show cts sxp sgt-map

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

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

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

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

Related Commands

Command	Description
cts sxp	Configures SXP on a network device.

show cts keystore

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

show cts keystore

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

Examples

The following sample output displays the contents of a keystore:

```
Switch# show cts keystore

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

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

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

```
Switch# show cts keystore

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

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

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

Related Commandsa

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

show platform cts reflector

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

show platform cts reflector interface type *slot/port*

Syntax Description

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

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Related Commands

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

timer (cts do1x)

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

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

Syntax Description

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

Defaults

86,400 seconds (24 hours).

Command Modes

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

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

debug cts

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

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

Syntax Description

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

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

Command Modes

Privileged EXEC (#)

SupportedUserRoles

Administrator

Command History

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

Examples

The following example show how to enable Cisco TrustSec debugging:

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

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

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

Related Commands

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

Notes for Catalyst 3000 and 2000 Series Switches and Wireless LAN Controller 5700 Series

Revised: May 18, 2014, OL-22192-02

Supported Hardware and Software

For a complete table of features, platforms, and IOS images supported, see the latest Product Bulletins at the following URL:

http://www.cisco.com/en/US/netsol/ns1051/index.html

See also, the Matrix of Cisco TrustSec-Enabled Infrastructure at the following URL:

http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html

Configuration Guidelines and Restrictions

Global Catalyst 3000 Series

- AAA for Cisco TrustSec requires RADIUS and is supported only by the Cisco Identity Services Engine (Cisco ISE), Release1.2 with patches or more recent, and Cisco Secure Access Control System (Cisco ACS), version 5.1 or more recent.
- Default for Cisco Trustsec is disabled.
- Default for SXP is disabled.

Catalyst 3850, Catalyst 3650 Switches, and Wireless LAN Controller 5700 Series

- Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.
- Cisco TrustSec for IPv6 is not supported.
- Dynamic binding of IP-SGT is not supported for hosts on Layer 3 physical routed interfaces because the IP Device Tracking feature for Layer 3 physical interfaces is not supported.
- If you configure an interface with Cisco TrustSec on Catalyst 3850 and Catalyst 3650 switches using **cts manual** command and disable the interface immediately, link flap occurs. It is recommended to disable the interface using the **shut** command before configuring Cisco TrustSec.
- Cisco TrustSec cannot be configured on a pure bridging domain with IPSG feature enabled. You must either enable IP routing or disable the IPSG feature in the bridging domain.
- Cisco TrustSec on the switch or controller supports up to 255 security group destination tags for enforcing security group ACLs.
- Cisco TrustSec MACSec for switch-to-switch security is supported only on switches running the IP base or IP services feature set. It is not supported on switches running the NPE or LAN base feature set.
- For Cisco IOS Release 3.7E and later, Cisco TrustSec VLAN-to-SGT binding cannot be enabled in pure bridging domain. You have to either manually enable IP device tracking on the ports in the VLAN, or enable SVI interface for the VLAN.

Catalyst 3750-X and Catalyst 3560-X switches

The following guidelines and limitations apply to configuring Cisco TrustSec SGT and SGACL:

- You cannot statically map an IP-subnet to an SGT. You can only map IP addresses to an SGT. When you configure IP address-to-SGT mappings, the IP address prefix must be 32.
- If a port is configured in Multi-Auth mode, all hosts connecting on that port must be assigned the same SGT. When a host tries to authenticate, its assigned SGT must be the same as the SGT assigned to a previously authenticated host. If a host tries to authenticate and its SGT is different from the SGT of a previously authenticated host, the VLAN port (VP) to which these hosts belong is error-disabled.
- Cisco TrustSec enforcement is supported only on up to eight VLANs on a VLAN-trunk link. If there are more than eight VLANs configured on a VLAN-trunk link and Cisco TrustSec enforcement is enabled on those VLANs, the switch ports on those VLAN-trunk links will be error-disabled.
- The switch can assign SGT and apply corresponding SGACL to end-hosts based on SXP listening only if the end-hosts are Layer 2 adjacent to the switch.
- SGT and SGACL are supported on Catalyst 3750-X and Catalyst 3650-X switches only with C3KX-SM-10G service module. Network modules do not support SGT and SGACL.

Notes for Catalyst 4500 Series Switches

Revised: April 24, 2013, OL-22192-02

Supported Hardware and Software

For a complete table of features, platforms, and IOS images supported see the latest Product Bulletins at the following URL:

http://www.cisco.com/en/US/netsol/ns1051/index.html

See also, the Matrix of Cisco TrustSec-Enabled Infrastructure at the following URL:

http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html

TrustSec SGT and SGACL Configuration Guidelines and Limitations

The following guidelines and limitations apply to configuring Cisco TrustSec SGT and SGACL on Catalyst WS-X45-SUP7-E/SUP7L-E and WS-C4500X-32 switches:

- Propagation of Security Group Tag in the CMD header is supported on the supervisor engine uplink ports, the WS-X47xx series line cards, and the WS-X4640-CSFP-E linecard.
- The way Destination Security tag (DGT) is derived for *switched traffic* (i.e. traffic forwarded between ports in the same VLAN or subnet) is restricted:
  - A maximum of 2000 IP-SGT mappings exists for DGT derivation. Though you can configure IP-SGT mappings above this limit, such mappings cannot be used to derive DGT for switched traffic. You can, however, use them to derive DGT for other types of traffic (e.g. routed traffic).

Note None of the previous restrictions exist for deriving either Source Security Tag for any type of traffic, or DGT for *routed traffic* (i.e. traffic forwarded between ports of different VLANs or subnets).

- The **platform-cts subnet-sgt l2traffic** command enables support for subnet based DGT derivation for switched (Layer 2) traffic. See the **platform-cts** command in the *Cisco TrustSec Command Summary* section in this document for detailed usage guidelines.
- In Cisco IOS XE 3.8.xE and earlier releases, IP-SGT mappings are not VRF-aware.

- The Time-To-Live (TTL) configuration is not supported for SGACL.
- The TCP flags supported by SGACL is similar to what the other ACLs support.
- The maximum number of access control entries (ACEs) supported in the default/(*,*) SGACL policy is 512.
- The IP-SGT mapping (based on the Source IP address in the packet) takes precedence over the SGT tag present in the CMD header of incoming traffic even if the ingress port is in trusted state. This deviates from the default behavior, which dictates that if the port is trusted the packet SGT is used for enforcing the SGACL policy.
- Every IP-SGT mapping learnt on the device is added to both the source lookup table and the destination lookup table.
- In Cisco IOS XE Release 3.9xE and later releases, a switched virtual interface (SVI) on a data VLAN is required to derive the source user group for switched (Layer 2) traffic.

  Cisco TrustSec depends on the routing table (Routing Information Base [RIB]/Forwarding Information Base [FIB]/FLC) to derive the source user group for switched traffic. Prior to Cisco IOS XE Release 3.9.xE, only one instance of the routing table was by default attached to all VLANs. In Cisco IOS XE Release 3.9.xE, with the introduction of virtual routing and forwarding (VRF) support, mapping a routing table instance to a VLAN is done only after the creation of an SVI.

  The following example shows how to configure the SVI:

```
Switch(config)# interface vlan 1
Switch(config-if)# no shutdown
```

Note An SVI is required for routed (Layer 3) IPv4/IPv6 traffic also. However, router traffic will always have an SVI that is up and running.

- In Cisco IOS XE 3.10.xE and later releases, IPv6 unicast routing must be enabled to derive source user group and destination user group for IPv6 Layer 2 traffic.

  The **ipv6 unicast-routing** command must be enabled to use Cisco TrustSec, and derive source user group and destination user group for Layer 2 clients. For IPv6 routing, routing entries are added only if the **ipv6 unicast-routing** command is enabled. This routing entry is used to derive the source user group for Layer 2 traffic. After updating the routing table, details are passed to the access control list (ACL) manager to create Content-Addressable Memory (CAM) entries to derive the destination user group for switched IPv6 traffic.

Note IPv6 unicast routing must be enabled for routed (Layer 3) IPv6 traffic also. However; for routed traffic the **ipv6 unicast-routing** command is enabled by default.

- Subnet Security Group Tag (SGT) entries will create entries with network prefix, broadcast address and matching unicast IP or IPv6 addresses in the Layer 2 destination user group derivation TCAM block, if these entries are already available in the FIB.
- The IP-SGT mapping configured on a switch takes precedence over the source user group value present in the command header of the incoming traffic, even if the ingress port is in the trusted state.
- Cisco TrustSec enforcement is not supported on logical interfaces in Cisco IOS XE Release 3.8.5E and later releases.
- The limit for Layer 2 destination user group derivation is given below:

Table B-1 In Cisco IOS XE Release 3.10.2E and Later Releases

	IPv4	IPv6
Software Hash	2500	1500
TCAM	2000	1000

Table B-2 In Cisco IOS XE Release 3.9xE and Previous Releases

	IPv4
Software Hash	2000
TACM	2000

- IPv6 Layer 2 destination user-group derivation will not work on an interface, if an IPv6 ACL that has ACEs configured with partially-masked lower 48 bit source address is applied in the ingress direction.
- By default, both IPv4 and IPv6 SGACL enforcement is disabled on all interfaces. It can be enabled by specifying a VLAN ID with the **cts role-based enforcement vlan-list** *vlan-id* command. This command will enable IPv4/IPv6 SGACL enforcement on all ports on the VLAN.
- The **cts role-based sgt-map vlan-list all** command binds the SGT with the full range of VLANs supported by the switch and is not preserved in the nonvolatile generation (NVGEN) process. The specified SGT is bound to incoming packets received in any of the specified VLANs. The system uses discovery methods such as DHCP or ARP snooping (also known as IP device tracking) to discover active hosts in any of the VLANs mapped by this command. Alternatively, the system could map the subnet associated with the SVI of each VLAN to the specified SGT.
- IPv6 SGACL enforcement and IPv6 ACEs that have partially-masked lower 48 bit source address in the egress direction cannot co-exist on an interface.
- In the case of IPv6 fragmented Cisco TrustSec packets without an encapsulating security protocol (ESP) header, there is a chance of packet parse errors happening, and packets getting dropped.
- A host that is marked as untrusted and authenticated in Cisco ISE is assigned the device SGT on the authentication switch. However, when the same host is marked as trusted, and re-authenticated, the existing device SGT mapping is not removed from the switch, and the new mapping does not come into effect until the port is shutdown and brought up again.

Notes for Catalyst 6500 Series Switches

Revised: April 26, 2013,, OL-22192-02

TrustSec Supported Hardware

TrustSec-capable supervisors and Line Cards are listed in tables 3 and 4 of "*Cisco Catalyst 6500 Series with Supervisor Engine 2T: Enabling Cisco TrustSec with Investment Protection,*" at the following URL:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11-658388.html

The Catalyst 6500 Series switches that are not TrustSec hardware-capable implement TrustSec Network Device Admission Control (NDAC) without SAP or 802.1AE link encryption.

For a complete table of features, platforms, and IOS images supported, see the latest Product Bulletins at the following URL:

http://www.cisco.com/en/US/netsol/ns1051/index.html

See also, the Matrix of Cisco TrustSec-Enabled Infrastructure at the following URL:

http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html

Flexible NetFlow Support

Release	Feature History
15.1(1)SY1	The following Flexible NetFlow flow exporter configuration subcommand was introduced on the Catalyst 6500 series switches: • **option cts-sgt-table** This option allows Flexible NetFlow to export TrustSec environmental data tables that map Security Group Tags (SGTs) to Security Group Names (SGNs).
12.2(50) SY IP Base LAN Image	The following Flexible NetFlow commands and flow objects were introduced on the Catalyst 6500 series switches: • **cts role-based** {**ip** | **ipv6**} **flow monitor** *monitor_name* **dropped** • **cts source group-tag** • **cts destination group-tag**

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:

Flexible NetFlow Configuration Guide, Cisco IOS Release 15S

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

Catalyst 6500 Release 15.0SY Software Configuration Guide

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/15_0_sy_swcg.html

Sample Configurations

Configuration Excerpt of an IPV4 Flow Record (5-tuple, direction, SGT, DGT)

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

Configuration Excerpt of an IPV6 Flow Record (5-tuple, direction, SGT, DGT)

```
Switch(config)# flow record cts-record-ipv6
Switch(config-flow-record)# match ipv6 protocol
Switch(config-flow-record)# match ipv6 source address
Switch(config-flow-record)# match ipv6 destination address
Switch(config-flow-record)# match transport source-port
Switch(config-flow-record)# match transport destination-port
Switch(config-flow-record)# match flow direction
Switch(config-flow-record)# match flow cts source group-tag
Switch(config-flow-record)# match flow cts destination group-tag
Switch(config-flow-record)# collect counter packets
```

Configuration Excerpt of an IPv4 Flow Monitor

```
Switch(config)# flow monitor cts-monitor-ipv4
Switch(config-flow-monitor)# record cts-record-ipv4
```

Configuration Excerpt of an IPv6 Flow Monitor

```
Switch(config)# flow monitor cts-monitor-ipv6
Switch(config-flow-monitor)# record cts-record-ipv6
```

Configuration Excerpt of the Global Flow Monitor (IPv4 and IPv6)

The following configuration applies the Flow Monitor to packets dropped by Role-Based Access Control Lists (RBACLs) for all TrustSec interfaces on the router or switch:

```
Switch(config)# cts role-based ip flow monitor cts-monitor-ipv4 dropped
Switch(config)# cts role-based ipv6 flow monitor cts-monitor-ipv6 dropped
```

Configuration Excerpt of the Interface Monitor

The Flow Monitor can be attached per interface, configured to filter for combinations of ingress (input), egress (output), multicast, unicast, or Layer2 switched traffic.

For IPv6, flow monitor is supported only for routed traffic in Cisco IOS Release 12.2(50)SY.

```
Switch(config)# interface TenGigabitEthernet 8/1
Switch(config-if)# ip address 192.1.1.1 255.255.255.0

;; Ingress IPv4 unicast only and egress unicast only
Switch(config-if)# ip flow monitor cts-monitor-ipv4 unicast input
Switch(config-if)# ip flow monitor cts-monitor-ipv4 unicast output

;; Ingress IPV4 L2-switched traffic only
Switch(config-if)# ip flow monitor cts-monitor-ipv4 layer2-switched input

;; Ingress Ipv4 multicast and egress IPv4 multicast traffic only
Switch(config-if)# ip flow monitor cts-monitor-ipv4 multicast input
Switch(config-if)# ip flow monitor cts-monitor-ipv4 multicast output

;; For both Unicast/multicast egress traffic
Switch(config-if)# ip flow monitor cts-monitor-ipv4 output

;; For both Unicast/multicast ingress traffic
Switch(config-if)# ip flow monitor cts-monitor-ipv4 input

;; For Ipv6 only the following are supported in Cisco IOS Release 12.2(50)SY
Switch(config-if)# ipv6 address 2022::22:1:1:11/64
Switch(config-if)# ipv6 flow monitor cts-monitor-ipv6 input
Switch(config-if)# ipv6 flow monitor cts-monitor-ipv6 unicast input
Switch(config-if)# ipv6 flow monitor cts-monitor-ipv6 output
Switch(config-if)# ipv6 flow monitor cts-monitor-ipv6 unicast output
```

Flexible NetFlow Show Commands

- **show flow record**
- **show flow monitor**
- **show flow exporter**
- **show flow interface**
- **show cts role-based counters**
- **show flow monitor** <*monitor_name*> **cache**

- **show flow monitor** <*monitor_name*> **statistics**
- **show platform flow ip**
- **show platform software flow internal fnf**
- **show platform hardware flow table flowmask**
- **show platform hardware flow table profile**
- **show platform hardware acl entry rbacl all**
- **show platform hardware acl entry tcam**
- **show platform software flow internal export**
- **show platform software flow internal export statistics**
- **show platform internal export information**
- **show platform internal export statistics**

TrustSec System Error Messages

Cisco TrustSec system error messages are listed in the Cisco Catalyst 6500 Series Switches Error and System Messages guides, found at the following URL:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_system_message_guides_list.html

The Error Message Decoder Tool is at the following URL:
http://www.cisco.com/en/US/support/tsd_most_requested_tools.html

FIPS Support

The Federal Information Processing Standard (FIPS) certification documents for Catalyst 6500 series switch software and hardware combinations are posted on the following website:

http://www.cisco.com/web/strategy/government/security_certification/net_business_benefit_seccert_fips140.html

The Catalyst 6500 Series FIPS certification documents describe the FIPS concepts and implementation per software/hardware combination.

TrustSec Considerations when Configuring FIPS

Perform initial setup, initialization, and configuration procedures of the Catalyst switch per the FIPS certification guide appropriate to your hardware and software configuration.

Licensing Requirements for FIPS

FIPS requires no licence for the Catalyst 6500 series switches.

Prerequisites for FIPS Configuration

- Disable Telnet. Users should log in using Secure Shell (SSH) only.
- Disable SNMPv1 and v2. Any existing user accounts on the device that have been configured for SNMPv3 should be configured only with SHA for authentication and AES/3DES for privacy.
- Delete all SSH server RSA1 key-pairs.

Guidelines and Limitations for FIPS

- The RADIUS keywrap feature works only with Cisco Identity Services Engine 1.1 or Cisco ACS Release 5.2 or later releases.
- HTTPS/TLS access to the module is allowed in FIPS approved mode of operation, using SSLv3.1/TLSv1.0 and a FIPS approved algorithm.
- SSH access to the module is allowed in FIPS approved mode of operation, using SSHv2 and a FIPS approved algorithm. Many SSH clients provide cryptographic libraries that can be set to FIPS Mode, making all cryptographic operations FIPS 140-2 Level 2 compliant.
- Your passwords must have a minimum of eight alphanumeric characters including at least one letter and at least one number character.

Default Settings for FIPS

The default is FIPS mode disabled, RADIUS keywrap disabled.

Revised: May 28, 2010, OL-22192-02

Numeric

802.1AE IEEE 802.1AE defines a Layer 2 hop-by-hop encryption process used between Cisco TrustSec hardware-capable devices. TrustSec uses SAP for the key management and cipher negotiation mechanism.

A

Authenticator A network device that is a member of a TrustSec network can authenticate a network device attempting to join the TrustSec network, in the role of authenticator to supplicant device. NDAC is the process by which the supplicant device is admitted into the TrustSec Network.

C

CTS Cisco Trusted Security, or Cisco TrustSec, or TrustSec.

E

EAC Endpoint Admission Control. A process of assigning SGT values to a specific IP address of the endpoint. Depending on hardware and software support, an SGT can be assigned to a source IP address with 802.1X authentication, MAC Authentication Bypass, Web Authentication Bypass, manual assignment, or IPM.

EAP Extensible Authentication Protocol. EAP-FAST is the EAP variant used in TrustSec networks for NDAC authentication.

I

IPM Identity-to-port mapping. A method for a switch to define the identity on a port to which an endpoint is connected, and to use this identity to look up a particular SGT value in the Cisco Secure ACS server.

M

MACSec Media Access Control Security based on IEEE 802.1AE to provide hop-to-hop link encryption. A TrustSec hardware-capable device can establish a MACSec link with a TrustSec hardware-capable peer.

N

NDAC Network Device Admission Control. A mutual authentication mechanism between CTS devices to authenticate and authorize its peer using an 802.1X process. EAP-FAST is used as the EAP type.

Non-seed Device Non-seed devices do not have direct IP connectivity to the Cisco Secure ACS and require other devices to authenticate and authorize them onto the TrustSec network, such as a seed device or a device already enrolled in the TrustSec network.

R

RBAC Role-based Access Control. An access control mechanism based on the role of the endpoints. RBAC is different from group based access control in a sense that RBAC can take multiple role factors to derive final policy for a particular entity.

RBACL Role-based Access Control List. Often used to characterize SGACL because TrustSec uses the RBAC features of the Cisco Secure ACS.

S

SAP Security Association Protocol, negotiates keys and cipher suite for link encryption after successful authentication and authorization for NDAC. SAP is derived from the 802.11i standard. SAP negotiation can be automatically initiated after NDAC process or the PMK can be statically configured on an interface.

Seed Device The seed device is the first TrustSec hardware-capable device to authenticate against the Cisco Secure ACS for TrustSec policy authorization. The seed device becomes the authenticator for the next TrustSec supplicant device, which in turn becomes an authenticator to its supplicant devices.

SGACL Security Group Access Control List. A Layer 3 to Layer 4 access control list that filters according to the value of SGTs. Usually, filtering occurs at an egress port of the CTS domain.

SGT Security Group Tag. A Layer-2 tag inserted in an Ethernet frame to classify traffic based on role. The tag process occurs at the ingress of the CTS domain. SGTs are defined in the Cisco Secure ACS configuration.

Supplicant In TrustSec, a network device without a direct connection to the Cisco Secure ACS which is requesting TrustSec authentication from an authenticated TrustSec network device (an authenticator) NDAC is the process by which the supplicant device is admitted into the TrustSec network.

SXP SGT Exchange Protocol. Allows devices with SXP support to build a source IP-to-SGT binding table, and then transfers the table to TrustSec hardware-capable devices through an out-of-bound TCP connection using MD5-based authentication.

T

TrustSec Trusted Security. Same as Cisco Trusted Security (CTS).

TrustSec Hardware-capable A network device that can tag traffic with SGTs, enforce SGACLs, and establish a MACSec connection with a TrustSec peer.

TrustSec Software-capable A network device that can establish NDAC and SXP connections with a TrustSec peer.

Numerics

C

D

E

F

G

I

L

M

N

P

S

T

V

W