



# **Cisco TrustSec Switch Configuration Guide**

For Cisco Catalyst Switches

Updated: October 2013

## **Americas Headquarters**

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

Text Part Number: OL-22192-02

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

*Cisco TrustSec Switch Configuration Guide*

© 2010-2013 Cisco Systems, Inc. All rights reserved.



## CONTENTS

### **Preface** ix

### **Cisco TrustSec Overview** 1-1

Information about Cisco TrustSec Architecture	1-1
Authentication	1-3
Cisco TrustSec and Authentication	1-3
Device Identities	1-6
Device Credentials	1-6
User Credentials	1-6
Security Group-Based Access Control	1-7
Security Groups and SGTs	1-7
SGACL Policies	1-7
Ingress Tagging and Egress Enforcement	1-8
Determining the Source Security Group	1-9
Determining the Destination Security Group	1-10
SGACL Enforcement on Routed and Switched Traffic	1-10
Authorization and Policy Acquisition	1-10
Environment Data Download	1-11
RADIUS Relay Functionality	1-12
Link Security	1-12
Using Cisco TrustSec-Incapable Devices and Networks in a Cisco TrustSec Network	1-13
SXP for SGT Propagation Across Legacy Access Networks	1-13
Layer 3 SGT Transport for Spanning Non-TrustSec Regions	1-14
Cisco TrustSec Reflector for Cisco TrustSec-Incapable Switching Modules	1-15
Ingress Reflector	1-16
Egress Reflector	1-16
VRF-Aware SXP	1-17
Layer 2 VRF-Aware SXP and VRF Assignment	1-17

## **Configuring the Cisco TrustSec Solution 2-1**

- Configuration Overview 2-1
  - Cisco TrustSec Configuration How-to Documents 2-1
  - Supported Hardware and Software 2-2
  - Prerequisites for Cisco TrustSec 2-2
  - Cisco TrustSec Guidelines and Limitations 2-3
  - Default Settings 2-3
- Additional Documentation 2-3
  - Release-Specific Documents 2-3
  - Platform-Specific Documents 2-4
  - Cisco IOS TrustSec Documentation Set 2-5

## **Configuring Identities, Connections, and SGTs 3-1**

- Cisco TrustSec Identity Configuration Feature Histories 3-1
- Configuring Credentials and AAA for a Cisco TrustSec Seed Device 3-2
  - Configuration Examples for Seed Device 3-3
- Configuring Credentials and AAA for a Cisco TrustSec Non-Seed Device 3-3
  - Configuration Examples for Non-Seed Device 3-4
- Enabling Cisco TrustSec Authentication and MACsec in 802.1X Mode on an Uplink Port 3-5
  - Configuration Examples for 802.1X on Uplink Port 3-6
- Configuring Cisco TrustSec and MACsec in Manual Mode on an Uplink Port 3-6
  - Configuration Examples for Manual Mode and MACsec on an Uplink Port 3-8
- Regenerating SAP Key on an Interface 3-9
- Verifying the Cisco TrustSec Interface Configuration 3-9
- Manually Configuring a Device SGT 3-11
  - Configuration Examples for Manually Configuring a Device SGT 3-11
- Manually Configuring IP-Address-to-SGT Mapping 3-12
  - Subnet to SGT Mapping 3-12
    - Default Settings 3-12
    - Configuring Subnet to SGT Mapping 3-12
    - Verifying Subnet to SGT Mapping Configuration 3-15
    - Configuration Examples for Subnet to SGT Mapping 3-15
  - VLAN to SGT Mapping 3-16
    - Default Settings 3-17
    - Configuring VLAN to SGT Mapping 3-17
    - Verifying VLAN to SGT Mapping 3-19
    - Configuration Example for VLAN to SGT Mapping for a Single Host Over an Access Link 3-19

Layer 3 Logical Interface to SGT Mapping (L3IF–SGT Mapping)	3-20
Feature History for L3IF-SGT Mapping	3-21
Default Settings	3-21
Configuring L3IF to SGT Mapping	3-21
Verifying L3IF to SGT Mapping	3-21
Configuration Example for L3IF to SGT Mapping on an Ingress Port	3-22
Binding Source Priorities	3-22
Configuring Additional Authentication Server-Related Parameters	3-23
Automatically Configuring a New or Replacement Password with the Authentication Server	3-24
<b>Configuring SGT Exchange Protocol over TCP (SXP) and Layer 3 Transport</b>	<b>4-1</b>
Cisco TrustSec SGT Exchange Protocol Feature Histories	4-1
Configuring Cisco TrustSec SXP	4-2
Enabling Cisco TrustSec SXP	4-2
Configuring an SXP Peer Connection	4-2
Configuring the Default SXP Password	4-4
Configuring the Default SXP Source IP Address	4-4
Changing the SXP Reconciliation Period	4-5
Changing the SXP Retry Period	4-5
Creating Syslogs to Capture Changes of IP Address to SGT Mapping Learned Through SXP	4-5
Verifying the SXP Connections	4-6
Configuring Layer 3 SGT Transport Between Cisco TrustSec Domains	4-6
Configuring Cisco TrustSec Reflector for Cisco TrustSec-Incapable Switching Modules	4-8
Configuring Cisco TrustSec Caching	4-9
Enabling Cisco TrustSec Caching	4-9
Clearing the Cisco TrustSec Cache	4-10
<b>Configuring SGACL Policies</b>	<b>5-1</b>
Cisco TrustSec SGACL Feature Histories	5-1
SGACL Policy Configuration Process	5-2
Enabling SGACL Policy Enforcement Globally	5-2
Configuration Examples for Enabling SGACL Policy Enforcement Globally	5-2
Enabling SGACL Policy Enforcement Per Interface	5-3
Configuration Examples for Enabling SGACL Policy Enforcement Per Interface	5-3
Enabling SGACL Policy Enforcement on VLANs	5-3
Configuration Examples for Enabling SGACL Policy Enforcement on VLANs	5-3

Manually Configuring SGACL Policies	5-4
Manually Configuring and Applying IPv4 SGACL Policies	5-4
Configuration Examples for Manually Configuring SGACL Policies	5-5
Displaying SGACL Policies	5-6
Refreshing the Downloaded SGACL Policies	5-7

## **Configuring Endpoint Admission Control** 6-1

Information About Endpoint Admission Control	6-1
Basic EAC Configuration Sequence	6-2
802.1X Authentication Configuration	6-2
Verifying the 802.1X Configuration	6-2
MAC Authentication Bypass Configuration	6-3
Verifying the MAB Configuration	6-3
Web Authentication Proxy Configuration	6-4
Verifying Web Authentication Proxy Configuration	6-4
Flexible Authentication Sequence and Failover Configuration	6-5
802.1X Host Modes	6-5
Pre-Authentication Open Access	6-5
DHCP Snooping and SGT Assignment	6-6
Verifying the SGT to Endpoint Host Binding	6-6
Cisco TrustSec Endpoint Access Control Feature Histories	6-7

## **Cisco TrustSec Command Summary** 7-1

## **Notes for Catalyst 3000 and 2000 Series Switches and WLC 5700 Series Wireless LAN Controllers** A-1

Supported Hardware and Software	A-1
Configuration Guidelines and Restrictions	A-1
Global Cat3K Restrictions	A-1
Catalyst 3850 and Catalyst 3650 Switches, and WLC 5700 Wireless LAN Controllers	A-2
Catalyst 3750-X and Catalyst 3560-X switches	A-2

## **Notes for Catalyst 4500 Series Switches** B-1

Supported Hardware and Software	B-1
TrustSec SGT and SGACL Configuration Guidelines and Limitations	B-1

## **Notes for Catalyst 6500 Series Switches C-1**

TrustSec Supported Hardware C-1

Flexible NetFlow Support C-1

Sample Configurations C-2

Configuration Excerpt of an IPV4 Flow Record (5-tuple, direction, SGT, DGT) C-2

Configuration Excerpt of an IPV6 Flow Record (5-tuple, direction, SGT, DGT) C-2

Configuration Excerpt of an IPV4 Flow Monitor C-2

Configuration Excerpt of an IPV6 Flow Monitor C-3

Configuration Excerpt of the Global Flow Monitor (IPv4 and IPv6) C-3

Configuration Excerpt of the Interface Monitor C-3

Flexible NetFlow Show Commands C-3

TrustSec System Error Messages C-4

FIPS Support C-4

TrustSec Considerations when Configuring FIPS C-4

Licensing Requirements for FIPS C-4

Prerequisites for FIPS Configuration C-5

Guidelines and Limitations for FIPS C-5

Default Settings for FIPS C-5

## **INDEX**





# Preface

---

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

## Organization

This guide includes the following chapters and appendixes:

Chapter or Appendix Title	Description
<a href="#">Chapter 1, “Cisco TrustSec Overview”</a>	Describes the elements and processes that create the Cisco TrustSec network.
<a href="#">Chapter 2, “Configuring the Cisco TrustSec Solution”</a>	Provides an overview of configuration tasks required to implement a Cisco TrustSec Network.
<a href="#">Chapter 3, “Configuring Identities, Connections, and SGTs”</a>	Provides NDAC and TrustSec seed device configuration procedures.
<a href="#">Chapter 4, “Configuring SGT Exchange Protocol over TCP (SXP) and Layer 3 Transport”</a>	Provides SGT over TCP Protocol (SXP) configuration procedures.
<a href="#">Chapter 5, “Configuring SGACL Policies”</a>	Provides Security Group ACL configuration procedures from the switch CLI.
<a href="#">Chapter 6, “Configuring Endpoint Admission Control”</a>	Provides 802.1X, MAB, and WebAuth configuration procedures for a TrustSec context.
<a href="#">Chapter 7, “Cisco TrustSec Command Summary”</a>	Provides a list of Cisco TrustSec CLI commands with brief descriptions.
<a href="#">Appendix A, “Notes for Catalyst 3000 and 2000 Series Switches and WLC 5700 Series Wireless LAN Controllers”</a>	Describes constraints, limitations, or considerations pertaining to TrustSec implementation of Catalyst 3000 and 2000 Series Switches and WLC 5700 Series Wireless LAN Controllers.
<a href="#">Appendix B, “Notes for Catalyst 4500 Series Switches”</a>	Describes constraints, limitations, or considerations pertaining to TrustSec implementation of Catalyst 4500 Series Switches.
<a href="#">Appendix C, “Notes for Catalyst 6500 Series Switches”</a>	Describes constraints, limitations, or considerations pertaining to TrustSec implementation of Catalyst 6500 Series Switches.

# Conventions

This document uses the following conventions:

Convention	Indication
<b>bold font</b>	Commands and keywords and user-entered text appear in <b>bold font</b> .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[ ]	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 <code>courier font</code> .
< >	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.





# CHAPTER 1

## Cisco TrustSec Overview

---

Revised: June 16, 2011, OL-22192-01

This chapter contains the following topics:

- [Information about Cisco TrustSec Architecture, page 1-1](#)
- [Using Cisco TrustSec-Incapable Devices and Networks in a Cisco TrustSec Network, page 1-13](#)

## Information about Cisco TrustSec Architecture

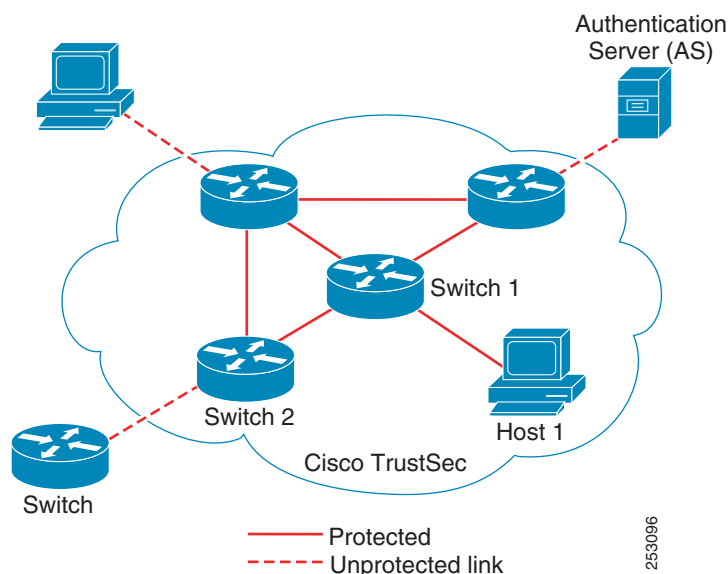
The Cisco TrustSec security architecture builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and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

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

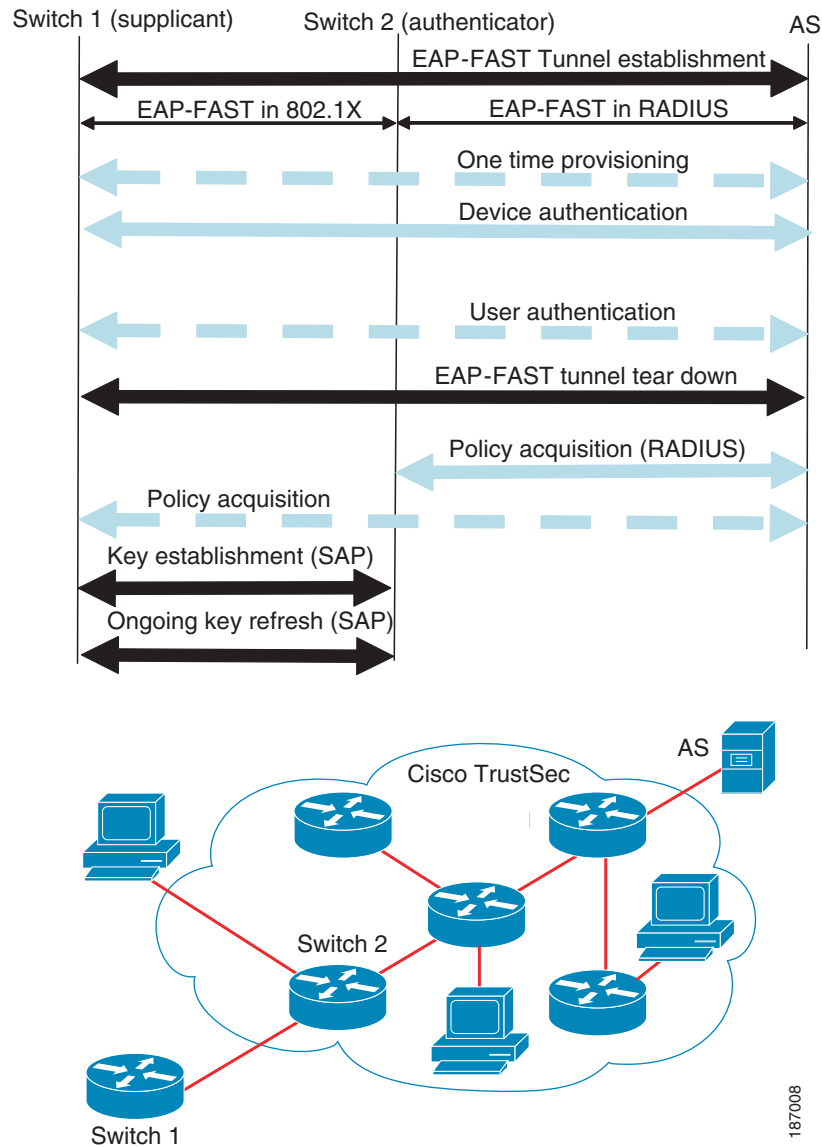
This section includes the following topics:

- [Cisco TrustSec and Authentication, page 1-3](#)
- [Device Identities, page 1-6](#)
- [Device Credentials, page 1-6](#)
- [User Credentials, page 1-6](#)

## 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, page 1-5](#)
- [802.1X Role Selection, page 1-5](#)
- [Cisco TrustSec Authentication Summary, page 1-5](#)

## 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, page 1-7](#)
- [SGACL Policies, page 1-7](#)
- [Ingress Tagging and Egress Enforcement, page 1-8](#)
- [Determining the Source Security Group, page 1-9](#)
- [Determining the Destination Security Group, page 1-10](#)
- [SGACL Enforcement on Routed and Switched Traffic, page 1-10](#)

### 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.

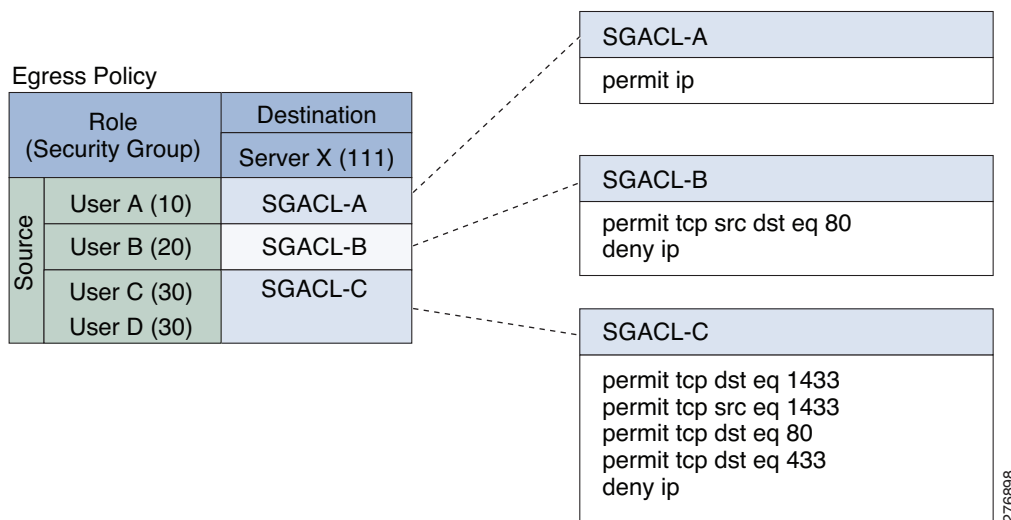
Once a device is authenticated, Cisco TrustSec tags any packet that originates from that device with a security group tag (SGT) that contains the security group number of the device. The packet carries this SGT throughout the network within the Cisco TrustSec header. The SGT is a single label that determines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

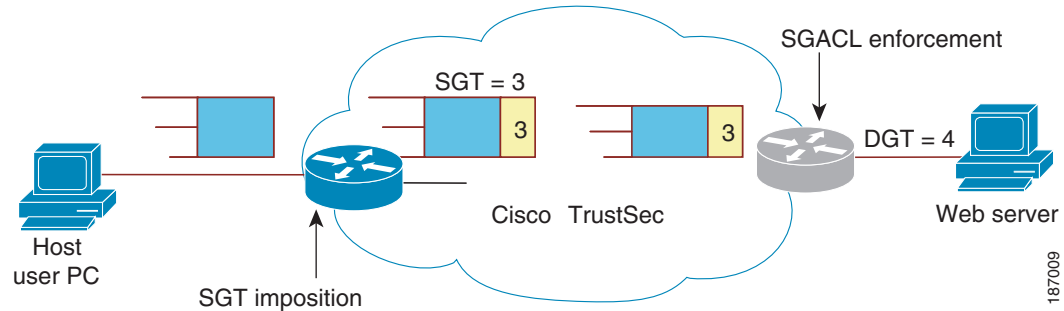
Using role-based permissions greatly reduces the size of ACLs and simplifies their maintenance. With Cisco TrustSec, the number of access control entries (ACEs) configured is determined by the number of permissions specified, resulting in a much smaller number of ACEs than in a traditional IP network. 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.

## 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:

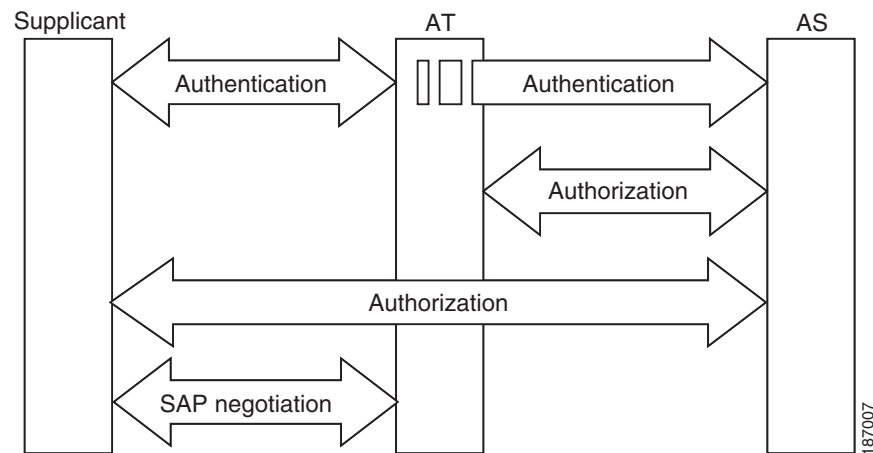
- Cisco TrustSec trust—Indicates whether the peer device is to be trusted for the purpose of putting the SGT in the packets.
- Peer SGT—Indicates the security group to which the peer belongs. If the peer is not trusted, all packets received from the peer are tagged with this SGT. If the device does not 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:

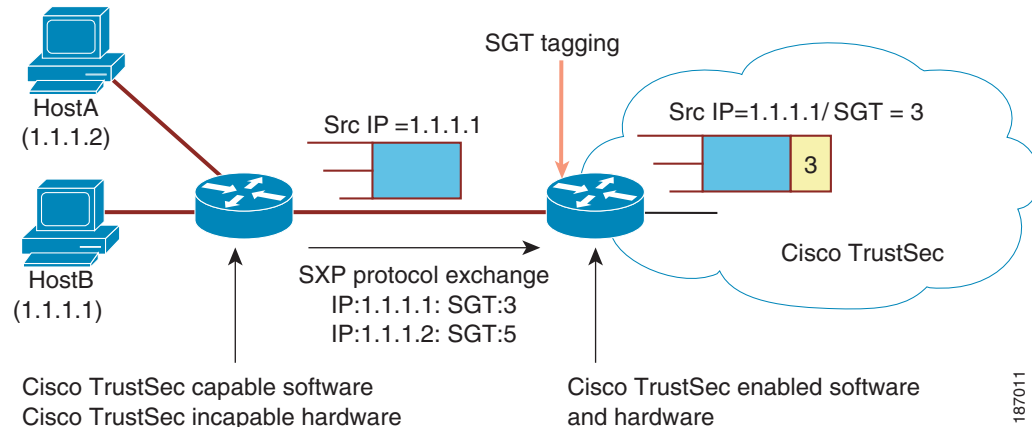
- [SXP for SGT Propagation Across Legacy Access Networks, page 1-13](#)

## 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**



187011

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:

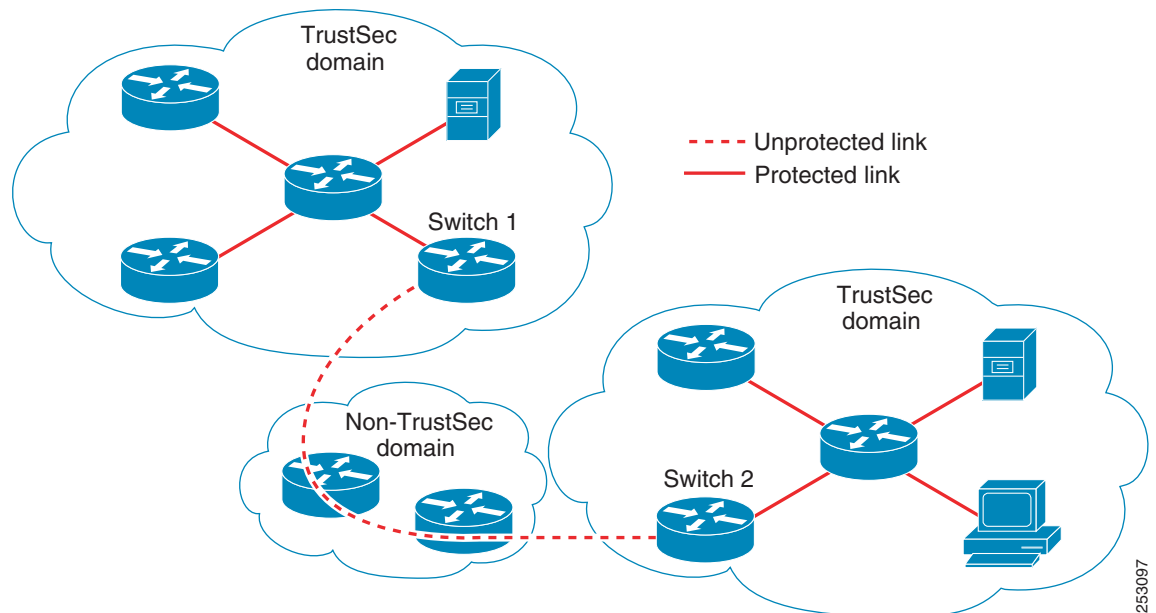
- If you require SXP data integrity and authentication, you must configure the same SXP password on both peer devices. You can configure the SXP password either explicitly for each peer connection or globally for the device. Although an SXP password is not required, we recommend its use.
- You must configure 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](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 exists 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.





## CHAPTER 2

# Configuring the Cisco TrustSec Solution

---

Revised: July 13, 2012, OL-22192-01

This chapter includes the following topics:

- [Configuration Overview, page 2-1](#)
- [Default Settings, page 2-3](#)
- [Additional Documentation, page 2-3](#)

## 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. Find all Cisco TrustSec “How-To” documents at the following URL:

[http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing\\_DesignZone\\_TrustSec.html](http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html)

TrustSec 2.1 Configuration How-to Guide topics include the following:

- Introduction
- Planning and Pre-Deployment Checklist
- ISE Base Configuration: ISE Bootstrapping
- Adding ID Stores and Creating Authentication
- Global Switch Configuration

- Base configuration for the Wireless LAN Controller
- Phased Deployment Overview
- Monitor Mode
- Migrating from Monitor Mode
- Low Impact Mode
- Closed Mode
- ISE Profiling Services
- ISE Base Configurations: Promiscuous VMware
- Central Web Authentication
- User Authentication and Authorization to Multiple Active Directory Domains
- ISE Deployment Type and Guideline
- Using Certificates to Differentiate Access
- On-boarding and Provisioning
- Server to Server Segmentation using Security Group Access
- Deploying EAP Chaining with AnyConnect NAM and Cisco ISE
- Failed Authentications & Authorizations

## 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](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.

## 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
<a href="#">Release Notes for Cisco TrustSec General Availability Releases</a>	<ul style="list-style-type: none"><li>• Open and resolved caveats</li><li>• Current hardware and software support</li></ul>

## Platform-Specific Documents

Platform-Specific Document Title	TrustSec Topics
Catalyst 3000 Series Switches	
<a href="#">Release Notes for Catalyst 3560 and 3750 Switches</a>	Open and resolved caveats; supported features
<a href="#">Catalyst 3560 Software Configuration Guides</a>	802.1x configuration procedures
<a href="#">Catalyst 3750-E and 3560-E Switch Software Configuration Guide</a>	
<a href="#">Cisco Catalyst 3560-X Series Switches Software Configuration Guides</a>	
<a href="#">Catalyst 3750 Metro Series Switches Software Configuration Guides</a>	
<a href="#">Cisco Catalyst 3750-X Series Switches Software Configuration Guides</a>	
Catalyst 4500 Series Switches	
<a href="#">Cisco Catalyst 4500 Series Switches Release Notes</a>	Open and resolved caveats, supported features
<a href="#">Catalyst 4500 Series Switches Software Configuration Guides</a>	802.1x configuration procedures
Catalyst 6500 Series Switches	
<a href="#">Cisco Catalyst 6500 Series Switches Release Notes</a>	Open and resolved caveats, supported features
<a href="#">Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide</a>	802.1x configuration procedures
<a href="#">Catalyst 6500 Release 12.2SY Software Configuration Guide</a>	
<a href="#">Catalyst 6500 Release 15.0SY Software Configuration Guide</a>	
Nexus 7000 Series Switches	
<a href="#">Cisco Nexus 7000 Series Switches Release Notes</a>	Open and resolved caveats
<a href="#">Cisco Nexus 7000 Series Switches Configuration Guides</a>	<ul style="list-style-type: none"><li>TrustSec feature configurations for Cisco Nexus 7000 series switches, Release 4.1 and later</li><li>802.1X configuration procedures</li></ul>
Cisco Secure Access Control System and Cisco Identity Services Engine	
<a href="#">Cisco Secure Access Control System Release Notes</a>	Open and resolved caveats

Platform-Specific Document Title	TrustSec Topics
<a href="#">Cisco Secure Access Control System End-User Guides</a>	TrustSec configurations for Cisco ACS 5.1 and later
<a href="#">Cisco Identity Services Engine</a>	TrustSec Configurations. TrustSec is referred to as SGA, or Security Group Access in ISE documentation.

## Cisco IOS TrustSec Documentation Set

Cisco IOS Document Title
<a href="#">Cisco IOS Security Configuration Guide: Securing User Services, Release 12.2SX</a>
<a href="#">Securing User Services Configuration Guide Library, Cisco IOS Release 15SY</a>





## CHAPTER 3

# Configuring Identities, Connections, and SGTs

---

**Revised: October 7, 2013, OL-22192-02**

This section includes the following topics:

- [Cisco TrustSec Identity Configuration Feature Histories, page 3-1](#)
- [Configuring Credentials and AAA for a Cisco TrustSec Seed Device, page 3-2](#)
- [Configuring Credentials and AAA for a Cisco TrustSec Non-Seed Device, page 3-3](#)
- [Enabling Cisco TrustSec Authentication and MACsec in 802.1X Mode on an Uplink Port, page 3-5](#)
- [Configuring Cisco TrustSec and MACsec in Manual Mode on an Uplink Port, page 3-6](#)
- [Regenerating SAP Key on an Interface, page 3-9](#)
- [Verifying the Cisco TrustSec Interface Configuration, page 3-9](#)
- [Manually Configuring a Device SGT, page 3-11](#)
- [Manually Configuring IP-Address-to-SGT Mapping, page 3-12](#)
- [Manually Configuring a Device SGT, page 3-11](#)
- [Configuring Additional Authentication Server-Related Parameters, page 3-23](#)
- [Automatically Configuring a New or Replacement Password with the Authentication Server, page 3-24](#)

## 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](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:

## Detailed Steps for Catalyst 6500, Catalyst 3K

	Command	Purpose
Step 1	Router# <b>cts credentials id</b> <i>device-id</i> <b>password</b> <i>password</i>	Specifies the Cisco TrustSec device ID and password for this switch to use when authenticating with other Cisco TrustSec devices with EAP-FAST. The <i>device-id</i> argument has a maximum length of 32 characters and is case sensitive.
Step 2	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 3	Router(config)# <b>aaa new-model</b>	Enables AAA.
Step 4	Router(config)# <b>aaa authentication dot1x default group radius</b>	Specifies the 802.1X port-based authentication method as RADIUS.
Step 5	Router(config)# <b>aaa authorization network mlist group radius</b>	Configures the switch to use RADIUS authorization for all network-related service requests. <ul style="list-style-type: none"> <li><i>mlist</i>—The Cisco TrustSec AAA server group.</li> </ul>
Step 6	Router(config)# <b>cts authorization list mlist</b>	Specifies a Cisco TrustSec AAA server group. Non-seed devices will obtain the server list from the authenticator.
Step 7	Router(config)# <b>aaa accounting dot1x default start-stop group radius</b>	Enables 802.1X accounting using RADIUS.
Step 8	Router(config)# <b>radius-server host ip-addr auth-port 1812 acct-port 1813</b> <b>pac key secret</b>	Specifies the RADIUS authentication server host address, service ports, and encryption key. <ul style="list-style-type: none"> <li><i>ip-addr</i>—The IP address of the authentication server.</li> <li><i>secret</i>—The encryption key shared with the authentication server.</li> </ul>
Step 9	Router(config)# <b>radius-server vsa send authentication</b>	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	Router(config)# <b>dot1x system-auth-control</b>	Globally enables 802.1X port-based authentication.
Step 11	Router(config)# <b>exit</b>	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:

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

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

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

### Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	Router# <b>cts credentials id</b> <i>device-id</i> <b>password</b> <i>password</i>	Specifies the Cisco TrustSec device ID and password for this switch to use when authenticating with other Cisco TrustSec devices with EAP-FAST. The <i>device-id</i> argument has a maximum length of 32 characters and is case sensitive.
Step 2	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 3	Router(config)# <b>aaa new-model</b>	Enables AAA.
Step 4	Router(config)# <b>aaa authentication dot1x default group radius</b>	Specifies the 802.1X port-based authentication method as RADIUS.
Step 5	Router(config)# <b>aaa authorization network</b> <i>mlist</i> <b>group radius</b>	Configures the switch to use RADIUS authorization for all network-related service requests. <ul style="list-style-type: none"> <li><i>mlist</i>—Specifies a Cisco TrustSec AAA server group.</li> </ul>
Step 6	Router(config)# <b>aaa accounting dot1x default start-stop group radius</b>	Enables 802.1X accounting using RADIUS.

	Command	Purpose
Step 7	Router(config)# <b>radius-server vsa send authentication</b>	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	Router(config)# <b>dot1x system-auth-control</b>	Globally enables 802.1X port-based authentication.
Step 9	Router(config)# <b>exit</b>	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:

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

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 for Catalyst 6500

	Command	Purpose
Step 1	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 2	Router(config)# <b>interface</b> <i>type slot/port</i>	Enters interface configuration mode for the uplink interface.
Step 3	Router(config-if)# <b>cts dot1x</b>	Configures the uplink interface to perform NDAC authentication.
Step 4	Router(config-if-cts-dot1x)# [ <b>no</b> ] <b>sap mode-list</b> <i>mode1 [mode2 [mode3 [mode4]]]</i>	<p>(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 <i>mode</i> are:</p> <ul style="list-style-type: none"> <li>• <b>gcm</b>— Authentication and encryption</li> <li>• <b>gmac</b>— Authentication, no encryption</li> <li>• <b>no-encap</b>— No encapsulation</li> <li>• <b>null</b>— Encapsulation, no authentication, no encryption</li> </ul> <p><b>Note</b> MACsec with SAP is not supported on the Catalyst 3K switches.</p> <p><b>Note</b> If the interface is not capable of SGT insertion or data link encryption, <b>no-encap</b> is the default and the only available SAP operating mode.</p>
Step 5	Router(config-if-cts-dot1x)# [ <b>no</b> ] <b>timer reauthentication</b> <i>seconds</i>	(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	Router(config-if-cts-dot1x)# [ <b>no</b> ] <b>propagate sgt</b>	(Optional) The <b>no</b> form of this command is used when the peer is incapable of processing an SGT. The <b>no propagate sgt</b> command prevents the interface from transmitting the SGT to the peer.
Step 7	Router(config-if-cts-dot1x)# <b>exit</b>	Exits Cisco TrustSec 802.1X interface configuration mode.
Step 8	Router(config-if)# <b>shutdown</b>	Disables the interface.

	Command	Purpose
Step 9	Router(config-if)# <b>no shutdown</b>	Enables the interface and enables Cisco TrustSec authentication on the interface.
Step 10	Router(config-if)# <b>exit</b>	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:

```
Router# configure terminal
Router(config)# interface gi2/1
Router(config-if)# cts dot1x
Router(config-if-cts-dot1x)# sap mode-list gcm null no-encap
Router(config-if-cts-dot1x)# timer reauthentication 43200
Router(config-if-cts-dot1x)# propagate sgt
Router(config-if-cts-dot1x)# exit
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

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

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 for Catalyst 6500

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

	Command	Purpose
Step 4	<pre>Router(config-if-cts-manual)# [no] sap pmk key [mode-list mode1 [mode2 [mode3 [mode4]]]]</pre>	<p>(Optional) Configures the SAP pairwise master key (PMK) and operation mode. SAP is disabled by default in Cisco TrustSec manual mode.</p> <ul style="list-style-type: none"> <li><i>key</i>—A hexadecimal value with an even number of characters and a maximum length of 32 characters.</li> </ul> <p>The SAP operation <i>mode</i> options are:</p> <ul style="list-style-type: none"> <li><b>gcm</b>— Authentication and encryption</li> <li><b>gmac</b>— Authentication, no encryption</li> <li><b>no-encap</b>— No encapsulation</li> <li><b>null</b>— Encapsulation, no authentication or encryption</li> </ul> <p><b>Note</b> MACsec with SAP is not supported on the Catalyst 3K switches.</p> <p><b>Note</b> If the interface is not capable of SGT insertion or data link encryption, <b>no-encap</b> is the default and the only available SAP operating mode.</p>
Step 5	<pre>Router(config-if-cts-manual)# [no] policy dynamic identity peer-name</pre>	<p>(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.</p> <ul style="list-style-type: none"> <li><i>peer-name</i>—The Cisco TrustSec device ID for the peer device. The peer name is case sensitive.</li> </ul> <p><b>Note</b> Ensure that you have configured the Cisco TrustSec credentials (see <a href="#">“Configuring Credentials and AAA for a Cisco TrustSec Seed Device”</a> section on page 3-2).</p>
	<pre>Router(config-if-cts-manual)# [no] policy static sgt tag [trusted]</pre>	<p>(Optional) Configures a static authorization policy. See the additional usage notes following this task.</p> <ul style="list-style-type: none"> <li><i>tag</i>—The SGT in decimal format. The range is 1 to 65533.</li> <li><b>trusted</b>—Indicates that ingress traffic on the interface with this SGT should not have its tag overwritten.</li> </ul>
Step 6	<pre>Router(config-if-cts-manual)# [no] propagate sgt</pre>	<p>(Optional) The <b>no</b> form of this command is used when the peer is incapable of processing an SGT. The <b>no propagate sgt</b> command prevents the interface from transmitting the SGT to the peer.</p>
Step 7	<pre>Router(config-if-cts-manual)# exit</pre>	Exits Cisco TrustSec manual interface configuration mode.
Step 8	<pre>Router(config-if)# shutdown</pre>	Disables the interface.

	Command	Purpose
Step 9	Router(config-if)# <b>no shutdown</b>	Enables the interface and enables Cisco TrustSec authentication on the interface.
Step 10	Router(config-if)# <b>exit</b>	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, no Cisco TrustSec encapsulation or encryption will 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

Catalyst 6500 TrustSec interface configuration in manual mode:

```
Router# configure terminal
Router(config)# interface gi 2/1
Router(config-if)# cts manual
Router(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm null no-encap
Router(config-if-cts-manual)# policy static sgt 111
Router(config-if-cts-manual)# exit
```

```
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# end
```

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
Router(config-if)# end
```

## Regenerating SAP Key on an Interface

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 for Catalyst 6500, Catalyst 3850/3650

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

## Verifying the Cisco TrustSec Interface Configuration

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

### Detailed Steps for Catalyst 6500

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

Example: Show Cisco 6500 TrustSec interface configuration:

```
Router# 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

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 for Catalyst 6500, 3850, 3750-X

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

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

- [Subnet to SGT Mapping, page 3-12](#)
- [VLAN to SGT Mapping, page 3-16](#)
- [Layer 3 Logical Interface to SGT Mapping \(L3IF–SGT Mapping\), page 3-20](#)

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 3-6](#)

## 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.

## 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 3-15](#)
- [Configuring Subnet to SGT Mapping, page 3-12](#)

## 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.

## Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	<b>config t</b>  <b>Example:</b> switch# config t switch(config)#	Enters global configuration mode.
Step 2	[no] <b>cts sxp mapping network-map</b> <i>bindings</i>  <b>Example:</b> switch(config)# cts sxp mapping network-map 10000	Configures the Subnet to SGT Mapping host count constraint. The <i>bindings</i> argument specifies the maximum number of subnet IP hosts that can be bound to SGTs and exported to the SXP listener. <ul style="list-style-type: none"> <li>• <i>bindings</i>—(0 to 65,535) default is 0 (no expansions performed)</li> </ul>
Step 3	[no] <b>cts role-based sgt-map</b> <i>ipv4_address/prefix</i> <b>sgt</b> <i>number</i>  <b>Example:</b> 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 <i>sgt number</i> keyword specifies the Security Group Tag to be bound to every host address in the specified subnet. <ul style="list-style-type: none"> <li>• <i>ipv4_address</i>—Specifies the IPv4 network address in dotted decimal notation.</li> <li>• <i>prefix</i>—(0 to 30). Specifies the number of bits in the network address.</li> <li>• <i>sgt number</i> (0–65,535). Specifies the Security Group Tag (SGT) number.</li> </ul>

	Command	Purpose
Step 4	<pre>[no] <b>cts role-based sgt-map</b>       ipv6_address::prefix <b>sgt number</b></pre> <p><b>Example:</b></p> <pre>switch(config)# cts role-based sgt-map 2020::/64 sgt 1234</pre>	<p>(IPv6) Specifies a subnet in colon hexadecimal notation. Use the <b>[no]</b> form of the command to unconfigure the Subnet to SGT mapping.</p> <p>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 <b>sgt number</b> keyword specifies the Security Group Tag to be bound to every host address in the specified subnet.</p> <ul style="list-style-type: none"> <li>• <i>ipv6_address</i>—Specifies IPv6 network address in colon hexadecimal notation.</li> <li>• <i>prefix</i>—(0 to 128). Specifies the number of bits in the network address.</li> <li>• <i>sgt number</i>—(0 to 65,535). Specifies the Security Group Tag (SGT) number.</li> </ul>
Step 5	<pre><b>exit</b></pre> <p><b>Example:</b></p> <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 6	<pre><b>show running-config</b>   include <i>search_string</i></pre> <p><b>Example:</b></p> <pre>switch# show running-config   include sgt 1234 switch# show running-config   include network-map</pre>	Verifies that the <b>cts role-based sgt-map</b> and the <b>cts sxp mapping network-map</b> commands are in the running configuration.
Step 7	<pre><b>copy running-config startup-config</b></pre> <p><b>Example:</b></p> <pre>switch# copy running-config startup-config</pre>	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
<b>show cts sxp connections</b>	Displays the SXP speaker and listener connections with their operational status.
<b>show cts sxp sgt-map</b>	Displays the IP to SGT bindings exported to the SXP listeners.
<b>show running-config</b>	Verifies that the Subnet to SGT configurations commands are in the running configuration file.

For detailed information about the fields in the output from these commands, refer to [Chapter 7, “Cisco TrustSec Command Summary.”](#)

## 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 a **cts role-based l2-vrf** cts global configuration 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 3-22.

## 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 3-17](#)

### 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

|        | Command                                                                                                                  | Purpose                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Step 1 | <b>config t</b><br><br><b>Example:</b><br>TS_switchswitch# config t<br>TS_switchswitch(config)#                          | Enters global configuration mode.                                                              |
| Step 2 | <b>vlan vlan_id</b><br><br><b>Example:</b><br>TS_switch(config)# vlan 100<br>TS_switch(config-vlan)#                     | Creates VLAN 100 on the TrustSec-capable gateway switch and enters VLAN configuration submode. |
| Step 3 | <b>[no] shutdown</b><br><br><b>Example:</b><br>TS_switch(config-vlan)# <b>no shutdown</b>                                | Provisions VLAN 100.                                                                           |
| Step 4 | <b>exit</b><br><br><b>Example:</b><br>TS_switch(config-vlan)# exit<br>TS_switch(config)#                                 | Exits VLAN configuration mode into Global Configuration mode.                                  |
| Step 5 | <b>interface type slot/port</b><br><br><b>Example:</b><br>TS_switch(config)# interface vlan 100<br>TS_switch(config-if)# | Enters interface configuration mode.                                                           |
| Step 6 | <b>ip address slot/port</b><br><br><b>Example:</b><br>TS_switch(config-if)# ip address 10.1.1.2 255.0.0.0                | Configures Switched Virtual Interface (SVI) for VLAN 100.                                      |

|         | Command                                                                                                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7  | <b>[no] shutdown</b><br><br><b>Example:</b><br>TS_switch(config-if)# <b>no shutdown</b>                                                                                                                                                                         | Enables the SVI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 8  | <b>exit</b><br><br><b>Example:</b><br>TS_switch(config-if)# <b>exit</b><br>TS_switch(config)#                                                                                                                                                                   | Exits VLAN Interface Configuration mode into Global Configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 9  | <b>cts role-based sgt-map vlan-list vlan_id sgt sgt_number</b><br><br><b>Example:</b><br>TS_switch(config)# <b>cts role-based sgt-map vlan-list 100 sgt 10</b>                                                                                                  | Assigns the specified SGT to the specified VLAN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 10 | <b>ip device tracking probe [count count   delay seconds   interval length]</b><br><br><b>Example:</b><br>TS-switch(config)# <b>ip device tracking</b>                                                                                                          | <p>Enables IP device tracking. When active hosts are detected, the switch adds the following entries to an IP Device Tracking table:</p> <ul style="list-style-type: none"> <li>• IP address of host</li> <li>• MAC address of host</li> <li>• VLAN of the host</li> <li>• The interface on which the switch detected the host</li> <li>• The state of the host (Active or Inactive)</li> </ul> <p>The host added to the IP Device Tracking table is monitored with periodic ARP probes. Hosts that fail to respond are removed from the table.</p> |
| Step 11 | <b>exit</b><br><br><b>Example:</b><br>TS_switch(config)# <b>exit</b><br>TS_switch#                                                                                                                                                                              | Exits Global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 12 | <b>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]}</b><br><br><b>Example:</b><br>TS_switch# <b>cts role-based sgt-map all</b> | (Optional) Displays the VLAN to SGT mappings.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|         | Command                                                                                                                      | Purpose                                                                   |
|---------|------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Step 13 | <code>show ip device tracking {all interface ip mac}</code><br><br><b>Example:</b><br>TS_switch# show ip device tracking all | (Optional) Verifies the operational status of IP Device tracking.         |
| Step 14 | <code>copy running-config startup-config</code><br><br><b>Example:</b><br>TS_switch# copy running-config startup-config      | (Optional) Copies the running configuration to the startup configuration. |

## Verifying VLAN to SGT Mapping

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

| Command                                  | Purpose                                                                                                |
|------------------------------------------|--------------------------------------------------------------------------------------------------------|
| <code>show ip device tracking</code>     | Displays the status of IP Device Tracking which identifies the IP addresses of active hosts on a VLAN. |
| <code>show cts role-based sgt-map</code> | Displays IP address to SGT bindings.                                                                   |

For detailed information about the fields in the output from these commands, refer to [Chapter 7, “Cisco TrustSec Command Summary,”](#) or the [“Cisco IOS 15.0SY Security and VPN Command Reference.”](#)

## 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# config t
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** Enable IP Device Tracking on the TrustSec switch. Verify that it is operating.

```
TS_switch(config)# ip device tracking
TS_switch# show ip device tracking all
```

```
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 100
```

```
-----
IP Address      MAC Address    Vlan  Interface      STATE
-----
```

```
Total number interfaces enabled: 1
Vlan100
```

**Step 7** (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
```

## 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)
- Layer3 subinterface of a Layer2 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 3-22.

## Feature History for L3IF-SGT Mapping

### Default Settings

There are no default settings.

## Configuring L3IF to SGT Mapping

### Detailed steps Catalyst 6500

	Command	Purpose
Step 1	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 2	Router(config)# <b>cts role-based sgt-map interface</b> type <i>slot/port</i> [ <b>security-group name</b>   <b>sgt number</b> ]  Router(config)# cts role-based sgt-map interface gigabitEthernet 1/1 sgt 77	An SGT is imposed on ingress traffic to the specified interface. <ul style="list-style-type: none"> <li><b>interface</b> type <i>slot/port</i>—Displays list of available interfaces.</li> <li><b>security-group name</b>— Security Group name to SGT pairings are configured on the Cisco ISE or Cisco ACS.</li> <li><b>sgt number</b>—(0 to 65,535). Specifies the Security Group Tag (SGT) number.</li> </ul>
Step 3	Router(config)# <b>exit</b>	Exits configuration mode.
Step 4	Router# <b>show cts role-based sgt-map all</b>	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
<b>show cts role-based sgt-map all</b>	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 ingress 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 ingress traffic to the interface is tagged appropriately.

```
Router# 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	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 2	Router(config)# [no] <b>cts server deadtime</b> <i>seconds</i>	(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	Router(config)# [no] <b>cts server load-balance method least-outstanding</b> [batch-size <i>transactions</i> ] [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 <i>transactions</i> is 25.  The <b>ignore-preferred-server</b> keyword instructs the switch not to try to use the same server throughout a session.
Step 4	Router(config)# [no] <b>cts server test</b> {server-IP-address   <b>all</b> } {deadtime <i>seconds</i>   <b>enable</b>   idle-time <i>seconds</i> }	(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 <b>idle-time</b> is 60 seconds; the range is from 1 to 14400.
Step 5	Router(config)# <b>exit</b>	Exits configuration mode.
Step 6	Router# <b>show cts server-list</b>	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:

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

Router# show cts server-list
CTS Server Radius Load Balance = ENABLED
Method = least-outstanding
```

```

Batch size = 50
Ignore preferred server
Server Group Deadtme = 20 secs (default)
Global Server Liveness Automated Test Deadtme = 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, deadtme = 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, deadtme = 20 secs
*Server: 10.15.20.101, port 1812, A-ID 255C438487B3503485BBC6F55808DC24
      Status = ALIVE
      auto-test = TRUE, idle-time = 60 mins, deadtme = 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, deadtme = 20 secs
*Server: 10.0.0.2, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
      Status = DEAD
      auto-test = TRUE, idle-time = 60 mins, deadtme = 20 secs

```

# Automatically Configuring a New or Replacement Password with the Authentication Server

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	Router# <b>cts change-password server</b> <i>ip-address port {key secret   a-id a-id}</i>	Initiates a password negotiation between the switch and the authentication server. <ul style="list-style-type: none"> <li>• <i>ip-address</i>—The IP address of the authentication server.</li> <li>• <i>port</i>—The UDP port of the authentication server.</li> <li>• <b>key secret</b>—The RADIUS shared secret of the authentication server.</li> <li>• <b>a-id a-id</b>—The A-ID associated with the authentication server.</li> </ul>



## CHAPTER 4

# Configuring SGT Exchange Protocol over TCP (SXP) and Layer 3 Transport

---

**Revised: May 28, 2010, OL-22192-01**

You can use the SGT Exchange Protocol (SXP) to propagate the SGTs across network devices that do not have hardware support for Cisco TrustSec. This section 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, page 4-1](#)
- [Configuring Cisco TrustSec SXP, page 4-2](#)
- [Configuring the Default SXP Password, page 4-4](#)
- [Configuring the Default SXP Source IP Address, page 4-4](#)
- [Changing the SXP Reconciliation Period, page 4-5](#)
- [Changing the SXP Retry Period, page 4-5](#)
- [Creating Syslogs to Capture Changes of IP Address to SGT Mapping Learned Through SXP, page 4-5](#)
- [Verifying the SXP Connections, page 4-6](#)
- [Configuring Layer 3 SGT Transport Between Cisco TrustSec Domains, page 4-6](#)
- [Configuring Cisco TrustSec Reflector for Cisco TrustSec-Incapable Switching Modules, page 4-8](#)
- [Configuring Cisco TrustSec Caching, page 4-9](#)

## Cisco TrustSec SGT Exchange Protocol 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: (final URL posted with TS 4.0)

[http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec\\_matrix.html](http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html)

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

# Configuring Cisco TrustSec SXP

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 4-2).
- Step 3

Configure SXP peer connections (see the “[Configuring an SXP Peer Connection](#)” section on page 4-2).

## 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 Steps for Catalyst 6500

	Command	Purpose
Step 1	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 2	Router(config)# <b>[no] cts sxp enable</b>	Enables SXP for Cisco TrustSec.
Step 3	Router(config)# <b>exit</b>	Exits configuration 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 the SXP peer connection, perform this task:

### Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 2	Router(config)# <b>cts sxp connection</b> <b>peer</b> <i>peer-ipv4-addr</i> [ <b>source</b> <i>src-ipv4-addr</i> ] <b>password</b> { <b>default</b>   <b>none</b> } <b>mode</b> { <b>local</b>   <b>peer</b> } { <b>speaker</b>   <b>listener</b> } [ <b>vrf</b> <i>vrf-name</i> ]	Configures the SXP address connection.  The optional <b>source</b> 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 <b>password</b> keyword specifies the password that SXP will use for the connection using the following options: <ul style="list-style-type: none"> <li>• <b>default</b>—Use the default SXP password you configured using the <b>cts sxp default password</b> command.</li> <li>• <b>none</b>—Do not use a password.</li> </ul> The <b>mode</b> keyword specifies the role of the remote peer device: <ul style="list-style-type: none"> <li>• <b>local</b>—The specified mode refers to the local device.</li> <li>• <b>peer</b>—The specified mode refers to the peer device.</li> <li>• <b>speaker</b>—Default. Specifies that the device is the speaker in the connection.</li> <li>• <b>listener</b>—Specifies that the device is the listener in the connection.</li> </ul> The optional <b>vrf</b> keyword specifies the VRF to the peer. The default is the default VRF.
Step 3	Router(config)# <b>exit</b>	Exits configuration mode.
Step 4	Router# <b>show cts sxp connections</b>	(Optional) Displays the SXP connection information.

This example shows how to enable SXP and configure the SXP peer connection on Switch A, a speaker, for connection to Switch B, a listener:

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

This example shows how to configure the SXP peer connection on Switch B, a listener, for connection to Switch A, a speaker:

```
Router# configure terminal
Router(config)# cts sxp enable
Router(config)# cts sxp default password Cisco123
```

```
Router(config)# cts sxp default source-ip 10.20.2.2
Router(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

## 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 for Catalyst 6500

	Command	Purpose
Step 1	Router# <b>configure terminal</b>	Enters configuration mode.
Step 2	Router(config)# <b>cts sxp default password</b> [0   6   7] <i>password</i>	Configures the SXP default password. You can enter either a clear text password (using the <b>0</b> or no option) or an encrypted password (using the <b>6</b> or <b>7</b> option). The maximum password length is 32 characters.
Step 3	Router(config)# <b>exit</b>	Exits configuration mode.

This example shows how to configure a default SXP password:

```
Router# configure terminal
Router(config)# cts sxp default password Cisco123
```

## 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 for Catalyst 6500

	Command	Purpose
Step 1	Router# <b>configure terminal</b>	Enters configuration mode.
Step 2	Router(config)# <b>cts sxp default source-ip src-ip-addr</b>	Configures the SXP default source IP address.
Step 3	Router(config)# <b>exit</b>	Exits configuration mode.

This example shows how to configure an SXP default source IP address:

```
Router# configure terminal
Router(config)# cts sxp default source-ip 10.20.2.2
```

## 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 for Catalyst 6500

	Command	Purpose
Step 1	Router# <b>configure terminal</b>	Enters configuration mode.
Step 2	Router(config)# <b>cts sxp reconciliation period seconds</b>	Changes the SXP reconciliation timer. The default value is 120 seconds (2 minutes). The range is from 0 to 64000.
Step 3	Router(config)# <b>exit</b>	Exits configuration 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 for Catalyst 6500

	Command	Purpose
Step 1	Router# <b>configure terminal</b>	Enters configuration mode.
Step 2	Router(config)# <b>cts sxp retry period seconds</b>	Changes the SXP retry timer. The default value is 120 seconds (2 minutes). The range is from 0 to 64000.
Step 3	Router(config)# <b>exit</b>	Exits configuration mode.

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

When the **cts sxp log binding-changes** global configuration command is executed, 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 for Catalyst 6500

	Command	Purpose
Step 1	Router# <b>configure terminal</b>	Enters configuration mode.
Step 2	Router(config)# <b>cts sxp log binding-changes</b>	Turns on logging for IP to SGT binding changes.

## Verifying the SXP Connections

To view the SXP connections, perform this task:

	Command	Purpose
Step 1	Router# <b>show cts sxp connections [brief]</b>	Displays SXP status and connections.

This example shows how to view the SXP connections:

```
Router# 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
```

## Configuring Layer 3 SGT Transport Between Cisco TrustSec Domains

Feature Name	Releases	Feature Information
L3 SGT Transport	12.2(50) SY	This feature was introduced on the 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.

To configure Layer 3 SGT Transport, perform this task:

### Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 2	Router(config)# <b>[no] cts policy layer3 {ipv4   ipv6} traffic acl-name</b>	(Optional) Specifies the fallback traffic policy to be applied when the authentication server is not available for downloading the traffic policy. <ul style="list-style-type: none"> <li><i>acl-name</i>—The name of a traditional interface ACL already configured on the device.</li> </ul> See the additional usage notes following this task.
Step 3	Router(config)# <b>[no] cts policy layer3 {ipv4   ipv6} exception acl-name</b>	(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	Router(config)# <b>interface type slot/port</b>	Specifies an interface and enters interface configuration mode.
Step 5	Router(config-if)# <b>[no] cts layer3 {ipv4   ipv6} trustsec forwarding</b>	(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.
	Router(config-if)# <b>[no] cts layer3 {ipv4   ipv6} policy</b>	(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	Router(config-if)# <b>end</b> Router(config)# <b>end</b>	Exits interface configuration and global configuration modes.
Step 7	Router# <b>show cts policy layer3 {ipv4   ipv6}</b>	(Optional) Displays the Layer 3 SGT transport configuration on the interfaces.

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 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.

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

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

## Configuring Cisco TrustSec Reflector for Cisco TrustSec-Incapable Switching Modules



### 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	Router# <b>configure terminal</b>	Enters configuration mode.
Step 2	Router(config)# <b>[no] platform cts ingress</b>	Activates the Cisco TrustSec supervisor ingress reflector.

	Command	Purpose
Step 3	Router(config)# <b>exit</b>	Exits configuration mode.
Step 4	Router# <b>show platform cts</b>	Displays Cisco TrustSec reflector mode (Ingress, Egress, Pure, or No CTS).

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

```
Router# configure terminal
Router(config)# platform cts ingress
Router(config)# exit
Router# 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	Router# <b>configure terminal</b>	Enters configuration mode.
Step 2	Router(config)# <b>[no] platform cts egress</b>	Activates the Cisco TrustSec egress reflector.
Step 3	Router(config)# <b>exit</b>	Exits configuration mode.
Step 4	Router# <b>show platform cts</b>	Displays Cisco TrustSec reflector mode (Ingress, Egress, Pure, or No CTS).

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

```
Router# configure terminal
Router(config)# platform cts egress
Router(config)# exit
Router# 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

### Enabling 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.

**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
<b>Step 1</b>	Router# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	Router(config)# <b>[no] cts cache enable</b>	Enables caching of authentication, authorization and environment-data information to DRAM. The default is disabled.  The <b>no</b> form of this command deletes all cached information from DRAM and non-volatile storage.
<b>Step 3</b>	Router(config)# <b>[no] cts cache nv-storage {bootdisk:   bootflash:   disk0:} [directory dir-name]</b>	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.
<b>Step 4</b>	Router(config)# <b>exit</b>	Exits configuration mode.

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

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

## Clearing the Cisco TrustSec Cache

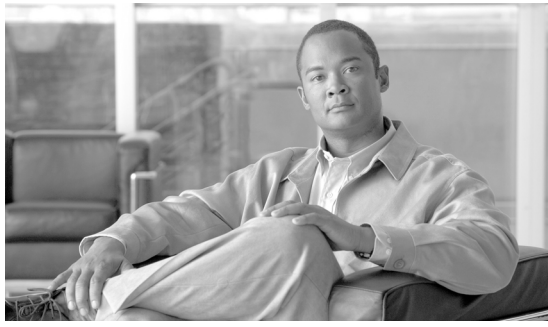
To clear the cache for Cisco TrustSec connections, perform this task:

**Detailed Steps for Catalyst 6500**

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

This example shows how to clear the Cisco TrustSec cache:

```
Router# clear cts cache
```



## CHAPTER 5

# Configuring SGACL Policies

---

**Revised: August 15, 2013, OL-22192-02**

This section includes the following topics:

- [Cisco TrustSec SGACL Feature Histories, page 5-1](#)
- [SGACL Policy Configuration Process, page 5-2](#)
- [Enabling SGACL Policy Enforcement Globally, page 5-2](#)
- [Enabling SGACL Policy Enforcement Per Interface, page 5-3](#)
- [Enabling SGACL Policy Enforcement on VLANs, page 5-3](#)
- [Manually Configuring SGACL Policies, page 5-4](#)
- [Displaying SGACL Policies, page 5-6](#)
- [Refreshing the Downloaded SGACL Policies, page 5-7](#)

## 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](http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html)

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

# SGACL Policy Configuration Process

Follow these steps to configure and enable Cisco TrustSec 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 5-4 and the “[Manually Configuring SGACL Policies](#)” section on page 5-4).



**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 5-2.
- 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 5-3.

## Enabling SGACL Policy Enforcement Globally

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

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

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

## Configuration Examples for Enabling SGACL Policy Enforcement Globally

Catalyst 6500, Catalyst 3850:

```
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 Catalyst 6500

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

## Configuration Examples for Enabling SGACL Policy Enforcement Per Interface

Catalyst 3850:

```
Switch# configure terminal
Switch(config)# interface gigabit 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 Catalyst 6500

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

## Configuration Examples for Enabling SGACL Policy Enforcement on VLANs

Catalyst 3850:

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

# 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

### Detailed Steps for Catalyst 3850

	Command	Purpose
Step 1	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 2	ip <b>access-list role-based</b> <i>rbacl-name</i>	Creates a Role-based ACL and enters Role-based ACL configuration mode.
	<b>Example:</b> Switch(config)# <b>ip access-list role-based allow_webtraff</b>	
Step 3	{ [ <i>sequence-number</i> ]   <b>default</b>   <b>permit</b>   <b>deny</b>   <b>remark</b> }	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, <a href="#">Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S</a> .  The following ACE commands or keywords are not supported: <ul style="list-style-type: none"> <li>• reflect</li> <li>• evaluate</li> <li>• time-range</li> </ul>
	<b>Example:</b> Switch(config-rb-acl)# <b>10 permit tcp dst eq 80 dst eq 20</b>	
Step 4	Switch(config-rb-acl)# <b>exit</b>	Exits to global configuration mode.

	Command	Purpose
Step 5	<pre>[no] <b>cts role-based permissions</b> {default   [from {sgt_num   unknown} to {dgt_num   unknown}]} {rbac1s   ipv4 rbac1s}</pre> <p><b>Example:</b></p> <pre>Switch(config)# <b>cts role-based permissions from 55 to 66 allow_webtraff</b></pre>	<p>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.</p> <ul style="list-style-type: none"> <li>• Default—Default permissions list</li> <li>• <i>sgt_num</i>—0 to 65,519. Source Group Tag</li> <li>• <i>dgt_num</i>—0 to 65,519. Destination Group Tag</li> <li>• unknown—SGACL applies to packets where the security group (source or destination) cannot be determined.</li> <li>• ipv4—Indicates the following RBACL is IPv4.</li> <li>• <i>rbac1s</i>—Name of RBACLs</li> </ul>
Step 6	Switch(config)# <b>end</b>	Exits to Privileged Exec mode.
Step 7	Switch# <b>show cts role-based permissions</b>	Displays permission to RBACL configurations.
Step 8	Switch# <b>show ip access-lists allow_webtraff</b>	Displays ACEs of all RBACLs or a specified RBACL.

## Configuration Examples for Manually Configuring SGACL Policies

Catalyst 3850 IPv4 Manual SGACL policy:

```
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
XXX need output XX
```

# 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	Router# <b>show cts role-based permissions default [ipv4   ipv6   details]</b>	Displays the list of SGACL of the default policy.
	Router# <b>show cts role-based permissions [from {source-sgt   unknown}] [to {dest-sg   unknown}] [ipv4   ipv6] [details]</b>	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:

```
Router# 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	<pre>cts refresh policy {peer [peer-id]   sgt [sgt_number] default unknown]}</pre>  <pre>Switch3850# cts refresh policy peer my_cisco_ise</pre>	<p>Performs an immediate refresh of the SGACL policies from the authentication server.</p> <ul style="list-style-type: none"><li>• If a <i>peer-id</i> is specified, only the policies related to the specified peer connection are refreshed. To refresh all peer policies, press Enter without specifying an ID.</li><li>• 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.</li></ul>





## CHAPTER 6

# Configuring Endpoint Admission Control

---

Revised: May 28, 2010, OL-22192-01

This chapter contains the following sections:

- [Information About Endpoint Admission Control](#)
- [Basic EAC Configuration Sequence](#)
- [802.1X Authentication Configuration](#)
- [MAC Authentication Bypass Configuration](#)
- [Web Authentication Proxy Configuration](#)
- [Flexible Authentication Sequence and Failover Configuration](#)
- [802.1X Host Modes](#)
- [Pre-Authentication Open Access](#)
- [DHCP Snooping and SGT Assignment](#)
- [Cisco TrustSec Endpoint Access Control Feature Histories](#)

## 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 over TCP \(SXP\) and Layer 3 Transport.”](#)
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:

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

For additional information on configuring 802.1x authentication, see the configuration guide for your access switch.

## Verifying the 802.1X Configuration

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

```
Router# 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:

```
Router# 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 through 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 is 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
```

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

For additional information on the **ip http server** command, see the *Cisco IOS Network Management Command Reference* entry at the following URL:

[http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm\\_08.html#wp1022387](http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_08.html#wp1022387)

## 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)#
```

For more detailed information on authentication method sequence configuration, see the configuration guide for your access switch.

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](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

For more detailed information on 802.1x Host Mode configurations, see the configuration guide for your access switch.

## 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.

For more detailed information on Pre-authentication Open Access configuration, see the configuration guide for your access switch.

## 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# conf t
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
```

For more detailed information on DHCP snooping and IP device tracking configuration, see the configuration guide for your access switch.

## 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](http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html)

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





## CHAPTER 7

# Cisco TrustSec Command Summary

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

### Cisco TrustSec Privileged EXEC Commands

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

### Cisco TrustSec Global Configuration Commands

<a href="#">cts authorization list</a>	Configures CTS global authorization configuration.
<a href="#">cts cache</a>	Enables caching of TrustSec authorization and environment-data information to DRAM and NVRAM.
<a href="#">cts manual</a>	Define CTS keystore behavior
<a href="#">cts policy layer3</a>	Specifies traffic and exception policies for CTS Layer 3 Transport gateway interfaces.
<a href="#">cts role-based</a>	Maps IP addresses, L3 interfaces, and VRFs to SGTs; enables CTS caching and SGACL enforcement.
<a href="#">cts server</a>	Configures RADIUS server list configuration.
<a href="#">cts sgt</a>	Configures local device security group tag.
<a href="#">cts sxp</a>	Configures SGT exchange over TCP.

### CTS Flexible NetFlow Commands

<a href="#">match flow cts</a>	
--------------------------------	--

**CTS Interface Configuration Commands**

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

**CTS dot1x Submode Commands**

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

**CTS Manual Interface Configuration Submode Commands**

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

**Cisco TrustSec Clear Commands**

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

### Cisco TrustSec Show Commands

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

### Commands to Configure Endpoint Admission Control (EAC)

<code>aaa accounting</code>	
<code>aaa authorization</code>	
<code>aaa authentication</code>	
<code>order</code>	
<code>priority</code>	
<code>event</code>	
<code>periodic</code>	
<code>timer</code>	
<code>host-mode</code>	
<code>authorization</code>	
<code>accounting</code>	
<code>radius-server host</code>	
<code>authentication port-control</code>	

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

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

## cts authorization list

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

**cts authorization list** *server\_list*

**no cts authorization list** *server\_list*

<b>Syntax Description</b>	<i>server_list</i> Specifies a Cisco TrustSec AAA server group.	
<b>Defaults</b>	None	
<b>Command Modes</b>	Global configuration (config)	
<b>Supported User Roles</b>	Administrator	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2 (33) SXI3	This command was introduced on the Catalyst 6500 series switches.
<b>Usage Guidelines</b>	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.	
<b>Examples</b>	<p>The following example displays an AAA configuration of a TrustSec seed device:</p> <pre> Router# cts credentials id Switch1 password Cisco123 Router# configure terminal Router(config)# aaa new-model Router(config)# aaa authentication dot1x default group radius Router(config)# aaa authorization network MLIST group radius Router(config)# cts authorization list MLIST Router(config)# aaa accounting dot1x default start-stop group radius Router(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key AbCe1234 Router(config)# radius-server vsa send authentication Router(config)# dot1x system-auth-control Router(config)# exit </pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show cts server-list</a>	Displays RADIUS server configurations.

## cts cache

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

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

Syntax Description		
<b>enable</b>		Enables CTS cache support
<b>nv-storage</b>		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.
<b>bootflash:</b> <i>dir</i>		Specifies bootflash dir as the nv-storage location.
<b>disk0:</b> <i>dir</i>		Specifies disk 0 directory as the nv-storage location.
<b>disk1:</b> <i>dir</i>		Specifies disk 1 directory as the nv-storage location.
<b>sup-bootflash:</b> <i>image</i>		Specifies a supervisor bootflash directory as the nv-storage location.

**Defaults** The default is caching disabled.

**Command Modes** Global configuration (config)

**Supported User Roles** Administrator

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

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

Cisco TrustSec creates a secure cloud of devices in a network by requiring that each device authenticate and authorize its neighbors with a trusted AAA server (Cisco Secure ACS 5.1 or more recent) before being granted access to the TrustSec network. Once the authentication and authorization is complete, the information could be valid for some time. If caching is enabled, that information can be reused, allowing the network device to bring up links without having to connect with the ACS, thus expediting the

formation of the CTS cloud upon reboot, improving network availability, and reducing the load on the ACS. Caching can be stored in volatile memory (information does not survive a reboot) or nonvolatile memory (information survives a reboot).

Examples

The following example enables cache support:

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

Related Commands

Command	Description
<a href="#">clear cts cache</a>	Clears the content of the keystore.
<a href="#">show cts keystore</a>	Displays the content of the keystore.
<a href="#">cts rekey</a>	
<a href="#">cts credentials</a>	

# cts change-password

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

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

Syntax Description		
<b>server</b>		Specifies the authentication server.
<i>ipv4_address</i>		The IP address of the authentication server.
<i>udp_port</i>		The UPD port of the authentication server.
<b>a-id</b> <i>hex_string</i>		Specifies the identification string of the ACS server
<b>key</b>		Specifies the RADIUS key to be used for provisioning
<b>source</b>		Specifies the interface for source address in request packets
<i>interface_list</i>		Specify the interface type and its identifying parameters per the displayed list.

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

**Command Modes** Privileged EXEC (#)

**Supported User Roles** Administrator

**Command Types** Use the following command syntax

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

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



**Note**

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

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

# cts credentials

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

**cts credentials id** *cts\_id* **password** *cts\_pwd*

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

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

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

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

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

**Usage Guidelines**

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

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



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

## Examples

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

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

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

The following example changes the CTS device ID and password to atlas and cisco123:

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

A different device ID is being configured.

This may disrupt connectivity on your CTS links.

```
Are you sure you want to change the Device ID? [confirm] y
```

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

The following example displays the CTS device ID and password state:

```
Router# show cts credentials
```

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

## Related Commands

Command	Description
<a href="#">clear cts credentials</a>	Clears the Cisco TrustSec device ID and password.
<a href="#">show cts credentials</a>	Displays the state of the current Cisco TrustSec device ID and password.
<a href="#">show cts keystore</a>	Displays contents of the hardware and software keystores.

# cts dot1x

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

[no] **cts dot1x**

<b>Syntax Description</b>	This command has no arguments or keywords.				
<b>Defaults</b>	CTS dot1x configuration on the interface is disabled by default.				
<b>Command Modes</b>	Interface configuration (config-if)				
<b>Supported User Roles</b>	Administrator				
<b>Command History</b>	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>12.2 (33) SXI3</td><td>This command was introduced on the Catalyst 6500 series switches.</td></tr> </table>	Release	Modification	12.2 (33) SXI3	This command was introduced on the Catalyst 6500 series switches.
Release	Modification				
12.2 (33) SXI3	This command was introduced on the Catalyst 6500 series switches.				
<b>Usage Guidelines</b>	Before configuring the TrustSec dot1x reauthentication timer, configure dot1x globally from the interface from the Interface Configuration mode. The CTS dot1x configuration governs TrustSec NDAC, not TrustSec EAC processes.				

**Examples**

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

```

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

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

```

Related Commands	Command	Description
	<a href="#">default timer reauthentication (cts interface)</a>	Resets the CTS dot1x reauthentication timer to the default value.
	<a href="#">timer reauthentication (cts interface)</a>	Sets the CTS dot1x reauthentication timer.
	<a href="#">show cts interface</a>	Displays CTS interface status and configurations.
	<b>show dotx interface</b>	Displays IEEE 802.1x configurations and statistics.

# default timer reauthentication (cts interface)

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

## default timer reauthentication

Syntax Description	<b>timer reauthentication</b> Sets the CTS 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 the Catalyst 6500 series switches.
Usage Guidelines	The default value of the CTS reauthentication timer is the global dot1x reauthentication default (3600 seconds). When this timer expires, the device reauthenticates to the CTS network (NDAC).	
Examples	<p>The following example resets the CTS reauthentication timer to the global default values:</p> <pre>Router # configure terminal Router(config)# interface gigabitEthernet 3/1 Router(config-if)# cts dot1x Router(config-if-cts-dot1x)# default timer reauthentication</pre>	
Related Commands	Command	Description
	<a href="#">cts dot1x</a>	Enters CTS dot1x interface configuration mode (config-if-cts-dot1x).
	<a href="#">timer reauthentication (cts interface)</a>	Sets the CTS reauthentication timer.
	<a href="#">show cts interface</a>	Displays CTS interface status and configurations.
	<a href="#">show dotx interface</a>	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*

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

# cts layer3

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

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

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

**Defaults** CTS Layer3 Transport is not enabled by default.

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

**SupportedUserRoles** Administrator

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

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

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

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

Related Commands	Command	Description
	<a href="#">cts policy layer3</a>	Specifies traffic and exception policies for CTS Layer 3 Transport.
	<a href="#">show cts policy layer3</a>	Displays the name of traffic and exception polices used for CTS Layer3 Transport configurations.

# cts manual

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

## cts manual

<b>Syntax Description</b>	There is no syntax for this command
---------------------------	-------------------------------------

<b>Defaults</b>	There is no default for this command.
-----------------	---------------------------------------

<b>Command Modes</b>	Interface configuration (config-if)
----------------------	-------------------------------------

<b>SupportedUserRoles</b>	Administrator
---------------------------	---------------

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

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

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

<b>Examples</b>	The following example demonstrates how to enter cts manual mode:
-----------------	--

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

Related Commands

Command	Description
<a href="#">policy (cts manual interface configuration submode)</a>	
<a href="#">sap (cts manual interface submode)</a>	
<a href="#">show cts interface</a>	

## cts policy layer3

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

```
[no] cts policy layer3 ipv4 {[exception access_list] | [traffic access_list ]}
```

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

<b>Syntax Description</b>	<b>ipv4 exception access_list</b> (Optional). Specifies an already defined ACL defining exceptions to the IPv4 L3 traffic policy.
	<b>ipv4 traffic access_list</b> Specifies an already defined ACL listing the IPv4 Trustsec-enabled subnets and gateways.
	<b>ipv6 exception access_list</b> (Optional). Specifies an already defined ACL defining exceptions to the IPv6 L3 traffic policy.
	<b>ipv6 traffic access_list</b> Specifies an already defined ACL listing the IPv6 Trustsec-enabled subnets and gateways

**Defaults** No policy is the default.

**Command Modes** Global configuration (config)

**Supported User Roles** Administrator

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

**Usage Guidelines** The CTS Layer 3 Transport feature permits Layer 2 SGT-tagged traffic from TrustSec-enabled network segments to be transported over non-TrustSec network segments by the application and removal of a Layer 3 encapsulation at specified CTS Layer 3 gateways. A traffic policy is an access list that lists all the TrustSec-enabled subnets and their corresponding gateway addresses. An exception policy is an access list that lists the traffic on which not to apply the CTS Layer 3 Transport encapsulation. For example, the RADIUS packets used to acquire the policy should be sent in the clear.

Specify the traffic and exception policies with the **cts policy layer3 {ipv4 | ipv6} traffic access\_list** and the **cts policy layer3 {ipv4 | ipv6} exception access\_list** global configuration commands. Apply the traffic and exception policies on the CTS L3 gateway interface with the **cts layer3 {ipv4 | ipv6} policy** interface configuration command. Enable the CTS L3 gateway interface with the **cts layer3 {ipv4 | ipv6} trustsec forwarding** interface configuration command.

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

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

### Examples

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

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

### Related Commands

Command	Description
<a href="#">cts layer3</a>	Enables and applies traffic and exception policies to CTS Layer 3 Transport gateway interfaces.
<a href="#">show cts policy layer3</a>	Displays the traffic and exception policies used in CTS Layer3 Transport.

# cts refresh

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

## cts refresh environment-data

**cts refresh policy** { **peer** [*peer\_id*] | **sgt** [*sgt\_number*] | **default** | **unknown** }

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

**Defaults** None

**Command Modes** Privileged EXEC (#)

**SupportedUserRoles** Administrator

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

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

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

Examples

The following example refreshes the TrustSec peer authorization policy of all peers:

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

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

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

Related Commands

Command	Description
<a href="#">cts refresh</a>	
<a href="#">clear cts policy</a>	Clears all CTS policies, or singly by peer ID or SGT.
<a href="#">show cts policy peer</a>	Displays peer authorization policy for all or specific TrustSec peers.

# cts rekey

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

## Syntax Description

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

## Defaults

There is no default value.

## Command Modes

Privileged EXEC (#)

## Supported User Roles

Administrator

## Command History

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

## Usage Guidelines

SAP Pair-wise Master Key key (PMK) refresh ordinarily occurs automatically, triggered by combinations of network events and non-configurable internal timers related to Dot1X authentication. The ability to manually refresh encryption keys is often part of network administration security requirements. To manually force a PMK refresh use the **cts rekey** command.

TrustSec supports a manual configuration mode where Dot1X authentication is not required to create link-to-link encryption between switches. In this case, the PMK is manually configured on devices on both ends of the link with the **sap pmk** CTS manual interface configuration command.

## Examples

The following example regenerates the PMK on the specified interface.

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

Related Commands

Command	Description
<a href="#">sap (cts manual interface submode)</a>	
<a href="#">show cts</a>	

# cts role-based policy trace

To troubleshoot SGT and SGACL behavior in TrustSec network devices, use the **cts role-based policy trace** privileged EXEC command.

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

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

Syntax Description		
	ipv4   ipv6	Specifies IPv4 or IPv6 IP encapsulation.
	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—Any Internet Protocol  tcp—Transmission Control Protocol  udp—User Datagram Protocol
	source_host ip_address	Specifies the IP address of the source host.

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

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

**Command Default** There are no defaults.

**Command Modes** Privileged EXEC

**SupportedUserRoles** Administrator

Command History	Release	Modification
	15.1(1)SY1	This feature was introduced on the Catalyst 6500 series switches.

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

1. Discover the network path.  
Know the topology of the entire TrustSec network before executing the command. Standard network discovery methods such as IP traceroute, CDP or other methods can be used to obtain this information.
2. Starting from the host and continuing to the farthest node; log-in to each device in the path.
3. Execute the **cts role-based policy trace** command on each device.  
Based on the input arguments, the command output reports the outgoing SGT value and SGACL entry/ACE. Apply the SGT value from the output as the input SGT on the next switch in the path.  
If you do not provide the (optional) SGT argument in the command line, the output reports the SGT assigned to the packet along with any available binding information.

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

**Examples** The following example specifies a source interface on the source host for an xdmcp over UDP packet.

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

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

Packet Parameters:
=====
```

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

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

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

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

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

Input Qualifiers:
=====

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

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

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

Related Commands

Command	Description
<a href="#">show cts role-based counters</a>	Displays Security Group ACL enforcement statistics.

## cts role-based

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

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

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

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

**[no] cts role-based l2-vrf instance\_name vlan-list vlan-ids [all]**

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

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

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

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

**[no] cts role-based sgt-map {ipv4\_netaddress | ipv6\_netaddress} | sgt sgt\_number**

**[no] cts role-based sgt-map {ipv4\_netaddress/prefix | ipv6\_netaddress/prefix} | sgt sgt\_number**

**[no] cts role-based sgt-map host {ipv4\_hostaddress | ipv6\_hostaddress} | sgt sgt\_number**

**[no] cts role-based sgt-map vrf instance\_name {ip4\_netaddress | ipv6\_netaddress | host {ip4\_address | ip6\_address}} | sgt sgt\_number**

**[no] cts role-based sgt-map interface interface\_type slot/port {security-group | sgt} sgt\_number**

**[no] cts role-based sgt-map vlan-list [vlan-ids | all] slot/port sgt sgt\_number**

**[no] cts role-based**

Syntax Description		
<b>l2-vrf</b> instance_name	(Optional) Specifies Layer 2 VRF instance name.	
<b>enforcement</b>	Enables SGACL enforcement on the local device for all Layer 3 CTS interfaces.	
<b>interface</b> interface_type	The specified SGT is mapped to traffic from this logical or physical Layer 3 interface.	
<b>vlan-list</b> vlan-ids	Specifies VLAN IDs. Individual VLAN IDs are separated by commas, a range of IDs specified with a hyphen.	
<b>all</b>	(Optional) Specifies all VLAN IDs.	
<b>with-enforcement</b>	Enables SGT caching where SGACL enforcement is enabled.	
<b>sgt-map</b> 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.	

<b>sgt-map</b> <i>ipv4_netaddress/prefix</i>   <i>ipv6_netaddress/prefix</i>	(Optional) Specifies that the SGT will be mapped to all hosts of the specified subnet address (IPv4 or IPv6). IPv4 is specified in dot decimal CIDR notation, IPv6 in colon hexadecimal notation. (0-128)
<b>sgt-map host</b> <i>ipv4_hostaddress</i>   <i>ipv6_hostaddress</i>	Binds the specified host IP address with the specified SGT. Enter the IPv4 address in dot decimal notation; IPv6 in colon hexadecimal notation.
<b>sgt</b> <i>sgt_number</i>	(0–65,535). Specifies the Security Group Tag (SGT) number.
<b>vrf</b> <i>instance_name</i>	Specifies a VRF instance, previously created on the device.

**Defaults**

None

**Command Modes**

Global configuration (config)

**Supported User Roles**

Administrator

**Command History**

Release	Modification
12.2 (33) SXI3	This command was introduced on the Catalyst 6500 series switches.
12.2 (50) SG7	This command was introduced on the Catalyst 4000 series switches.
12.2 (53) SE2	This command was introduced on the Catalyst 3750(E), 3560(E), and 3750(X) series switches (without <b>vrf</b> or IPv6 support).
12.2(50) SY	The following keywords were added for the Catalyst 6500 series switches: <ul style="list-style-type: none"> <li>[no] cts role-based enforcement</li> <li>[no] cts role-based ip flow monitor user-defined-monitor dropped</li> <li>[no] cts role-based ipv6 flow monitor user-defined-monitor dropped</li> <li>[no] cts role-based ipv6 copy</li> <li>[no] cts role-based permissions</li> </ul>
15.0(0) SY	The following keywords were added for the Catalyst 6500 series switches: <ul style="list-style-type: none"> <li>[no] cts role-based sgt-map interface</li> <li>[no] cts role-based sgt-map vlan-list</li> </ul>

**Usage Guidelines**

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

- A single host IPv4 or IPv6 address
- All hosts of an IPv4 or IPv6 network or subnetwork

- VRFs
- Single or multiple VLANs
- A Layer 3 physical or logical interface

#### Single Host Address to SGT Binding

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

#### Network or Subnetwork Addresses to SGT Binding

The **cts role-based sgt-map** *ipv4\_netaddress* | *ipv6\_netaddress* and **cts role-based sgt-map** *ipv4\_subnetaddress/prefix* | *ipv6\_subnetaddress/prefix* commands bind the specified SGT with packets that fall within the specified network address.

SXP exports an exhaustive expansion of all possible individual IP-SGT bindings within the specified network or subnetwork. IPv6 bindings and subnet bindings are exported only to SXP listener peers of SXP version 2 or later.

#### VRF to SGT Bindings

The **vrf** keyword specifies a Virtual Routing and Forwarding table previously defined with the **vrf definition** global configuration command. The configuration of VRF contexts is outside the scope of this document. The IP-SGT binding specified with the **cts role-based sgt-map vrf** global configuration command is entered into the IP-SGT table associated with the specified VRF and the IP protocol version which is implied by the type of IP address entered.

#### VLAN to SGT Mapping

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

#### Layer 3 Interface Mapping (L3IF)

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

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

#### Binding Source Priorities

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

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

### L2 VRF Assignment

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

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

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

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

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

### Role-based Enforcement

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



#### Note

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

### VLAN Enforcement

Use the **[no] cts role-based enforcement vlan-list {vlan-ids | all}** command to enable or disable SGACL enforcement for Layer 2 switched packets and for L3 switched packets on an SVI interface.

The *vlan-ids* argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges. Separate multiple entries with a hyphen “-” or a comma “,”.

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

**Note**

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

**Note**

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

### Flexible Net Flow

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

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

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

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

#### Getting Started with Configuring Cisco IOS Flexible NetFlow

[http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/get\\_start\\_cfg\\_fnflow.html](http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/get_start_cfg_fnflow.html)

#### Cisco IOS Flexible NetFlow Configuration Guide, Release 15.0SY

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

### Examples

In the following example, a Catalyst 4500 series switch binds host IP address 10.1.2.1 to SGT 3 and 10.1.2.2 to SGT 4, then verifies with a **show** command. These bindings will be forwarded by SXP to an SGACL enforcement switch.

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

```
cat4k# show cts role-based sgt-map all
Active IP-SGT Bindings Information
```

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

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

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

```
Cat6k(config)# cts role-based 12-vrf 12ipv4 vlan-list 57, 89-101
```

Related Commands	Command	Description
	<a href="#">cts sxp</a>	Configures SXP on a network device.
	<a href="#">cts sgt</a>	Configures local device security group tag.
	<a href="#">show cts role-based sgt-map</a>	Displays role-based access control information

## cts server

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


**[no] cts server deadline** *timer\_secs*

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

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

**[no] cts server test** {*ip4\_address* | **all**} {**deadline** *seconds* | **enable** | **idle-time** *minutes*}

### Syntax Description

<b>deadline</b> <i>timer_secs</i>	Specifies how long a server in the group should not be selected for service once it has been marked as dead. The default is 20 seconds; the range is 1 to 864000.
<b>load-balance method least-outstanding</b>	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.
<b>batch-size</b> <i>transactions</i>	(Optional) The number of transactions to be assigned per batch. The default <i>transactions</i> is 25.
<div>  <b>Note</b> 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.         </div>	
<b>ignore-preferred-server</b>	(Optional) Instructs the switch not to try to use the same server throughout a session.
<b>test</b> { <i>ip4_address</i>   <b>all</b> } { <b>deadline</b> <i>seconds</i>   <b>enable</b>   <b>idle-time</b> <i>minutes</i> }	Configures the server-liveliness test for a specified RADIUS server or for all servers on the dynamic server list. By default, the test is enabled for all servers. The default <b>deadline</b> is 20 seconds; the range is 1 to 864000 seconds. The default <b>idle-time</b> is 60 seconds; the range is from 1 to 14400 seconds.
<b>key-wrap enable</b>	Enables AES Key Wrap encryption for Trustsec RADIUS server communications.

### Defaults

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

**Command Modes** Global configuration (config)

**Supported User Roles** Administrator

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

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

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

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

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

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

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

Related Commands	Command	Description
	<a href="#">show cts server-list</a>	Displays lists of AAA servers and load-balancing configurations.

# cts sgt

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

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

<b>Syntax Description</b>	<i>tag-number</i>	Configures the SGT for packets sent from this device. The <i>tag</i> argument is in decimal format. The range is 1 to 65533.
---------------------------	-------------------	--

<b>Defaults</b>	No SGT number is assigned.
-----------------	----------------------------

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

<b>SupportedUserRoles</b>	Administrator
---------------------------	---------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2 (33) SXI3	This command was introduced on the Catalyst 6500 series switches.
	12.2 (50) SG7	This command was introduced on the Catalyst 4000 series switches.
	12.2 (53) SE2	This command was introduced on the Catalyst 3750(E) and 3560(E) series switches.
	12.2 (53) SE2	This command was introduced on the Catalyst 3750(X) series switches.

<b>Usage Guidelines</b>	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.
-------------------------	---

<b>Examples</b>	The following example shows how to manually configure an SGT on the network device:
-----------------	---

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show cts environment-data</a>	Displays the CTS environment data.

## cts sxp

To configure SXP on a network device, use the **cts sxp** global configuration command. This command enables SXP, determines the SXP password, the peer speaker/listener relationship, and the reconciliation period. It also toggles the binding changes log on or off. Use the **no** form of the command to disable SXP configurations.

**[no] cts sxp connection peer** *ip4\_address* **password** {**default** | **none**} **mode** {**local** | **peer**} [**speaker** | **listener**] [**vrf** *vrf\_name*]

**[no] cts sxp connection peer** *ip4\_address* **source** *ip4\_address* **password** {**default** | **none**} **mode** {**local** | **peer**} [**speaker** | **listener**] [**vrf** *vrf\_name*]

**[no] cts sxp default password** {**0** *unencrypted\_pwd* | **6** *encrypted\_key* | **7** *encrypted\_key* | *cleartext\_pwd* }

**[no] cts sxp default source-ip** *ip4\_address*

**[no] cts sxp enable**

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

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

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

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

Syntax Description	
<b>connection peer</b> <i>ip4_address</i>	Specifies the peer SXP address.
<b>password</b> { <b>default</b>   <b>none</b> }	Specifies the password that SXP will use for the peer connection using the following options: <ul style="list-style-type: none"> <li><b>default</b>—Use the default SXP password you configured using the <b>cts sxp default password</b> command.</li> <li><b>none</b>—Do not use a password.</li> </ul> Maximum password length is 32 characters.
<b>mode</b> { <b>local</b>   <b>peer</b> }	Specifies the role of the remote peer device: <ul style="list-style-type: none"> <li><b>local</b>—The specified mode refers to the local device.</li> <li><b>peer</b>—The specified mode refers to the peer device.</li> </ul>
<b>network-map</b> <i>bindings</i>	0–65535. Maximum number of Subnet host address to SGT bindings permitted when expanding subnets for IP–SGT tagging and export. Enter 0 for no expansion.
<b>speaker</b>   <b>listener</b>	<b>speaker</b> —Default. Specifies that the device is the speaker in the connection.  <b>listener</b> —Specifies that the device is the listener in the connection.
<b>vrf</b> <i>vrf_name</i>	(Optional) Specifies the VRF to the peer. Default is the default VRF.

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

## Defaults

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

## Command Modes

Global configuration (config)

## Supported User Roles

Administrator

## Command History

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

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

### Usage Guidelines

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

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

The **cts sxp default source-ip** command sets the default source IP address that SXP uses for all new TCP connections where a source IP address is not specified. Pre-existing TCP connections are not affected when this command is entered. SXP connections are governed by three timers:

- Retry timer
- Delete Hold Down timer
- Reconciliation timer

#### Retry Timer

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

#### Delete Hold Down Timer

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

#### Reconciliation Timer

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

Examples

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

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

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

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

Related Commands

Command	Description
<a href="#">show cts sxp</a>	Displays status of all SXP configurations.

# clear cts cache

To clear TrustSec authorization and use the **clear cts counter** Privileged EXEC command.

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

**clear cts cache environment-data**

**clear cts cache filename** *file*

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

## Syntax Description

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

## Defaults

None

## Command Modes

Privileged EXEC (#)

## Supported User Roles

Administrator

## Command History

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

## Examples

The following example deletes environment data from cache:

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



### Note

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

## Related Commands

Command	Description
<b>cts cache</b>	Enables caching of TrustSec authorization and environment data information to DRAM and NVRAM

# clear cts counter

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

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

Syntax Description	<b>type</b> <i>slot/port</i>	(Optional) Specifies the interface type, slot, and port of the interface to clear.
Defaults	None	
Command Modes	Privileged EXEC (#)	
SupportedUserRoles	Administrator	
Command History	Release	Modification
	12.2(33) SXI	This command was introduced on the Catalyst 6500 series switches.

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

**Examples** The following example clears CTS statistics for GigabitEthernet interface 3/1, then confirms with the **show cts interface** command (a fragment of the **show** command output is displayed):

```
Router# clear cts counter gigabitEthernet3/1
Router# show cts interface gigabitEthernet3/1
Global Dot1x feature is Disabled
Interface GigabitEthernet3/1:
<snip>

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

Related Commands	Command	Description
	<a href="#">show cts interface</a>	Displays CTS interface status and configurations.

# clear cts credentials

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

## clear cts credentials

Syntax Description	This command has no arguments or keywords.	
Defaults	None	
Command Modes	Privileged EXEC (#)	
SupportedUserRoles	Administrator	
Command History	Release	Modification
	12.2(33) SXI	This command was introduced on the Catalyst 6500 series switches.
Examples	<pre>Router# clear cts credentials Router# clear cts environment-data Router# show cts environment-data CTS Environment Data ===== Current state = START Last status = Cleared Environment data is empty State Machine is running Retry_timer (60 secs) is running</pre>	
Related Commands	Command	Description
	<a href="#">cts credentials</a>	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

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>SupportedUserRoles</b>	Administrator
---------------------------	---------------

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

<b>Examples</b>	The following example clears environment data from cache: Router# <b>clear cts environment-data</b>
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show cts environment-data</a>	Displays the CTS environment data.

# clear cts macsec

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

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

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

# clear cts pac

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

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

Syntax Description	A-ID <i>hexstring</i>	Specifies the authenticator ID (A-ID) of the PAC to be removed from the keystore.
	all	Specifies that all PACs on the device be deleted.

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

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

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

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

Examples	The following command clears all PACs in the keystore:  Router# <b>clear cts pac all</b>
----------	--

Related Commands	Command	Description
	<a href="#">show cts pacs</a>	Displays the A-ID and PAC-info for PACs in the keystore.
	<a href="#">show cts keystore</a>	Displays the contents of the keystore.

# clear cts policy

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

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

Syntax Description	peer 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 (#)
---------------	---------------------

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

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

## Usage Guidelines

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

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

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

Related Commands	Command	Description
	<a href="#">cts refresh</a>	Forces refresh of peer authorization policies.
	<a href="#">show cts policy peer</a>	Displays the peer authorization policies of TrustSec peers.

# clear cts role-based counters

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

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

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

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

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

Syntax Description

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

Command Modes

EXEC (>); Privileged EXEC (#)

Supported User Roles

Administrator

Command History

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

Usage Guidelines

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

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

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

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

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

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

---

**Examples**

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

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

---

**Related Commands**

# clear cts server

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

**clear cts server** *ip\_address*

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

## default (cts dot1x interface configuration submode)

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

**default propagate sgt**

**default sap**

**default timer reauthentication**

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

<b>Defaults</b>	There is no default for this command.
-----------------	---------------------------------------

<b>Command Modes</b>	CTS dot1x interface configuration submode (config-if-cts-dot1x)
----------------------	---

<b>SupportedUserRoles</b>	Administrator
---------------------------	---------------

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

<b>Examples</b>	The following example re-enables SGT propagation:
-----------------	---

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">propagate (cts dot1x submode)</a>	Enables/disables SGT propagation in dot1x mode.
	<a href="#">sap (cts dot1x interface submode)</a>	Configures CTS SAP for dot1x mode.
	<a href="#">timer (cts dot1x interface submode)</a>	Configures the CTS timer.

# debug condition cts

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

**[no] debug condition cts {peer-id *peer-id* | security-group {name *sg\_name* | tag *tag\_number*}}**

## Syntax Description

<b>peer-id</b> <i>peer-id</i>	Specifies the Peer ID to match.
<b>security-group</b> <i>sg_name</i>	Specifies the SGN to match.
<b>tag</b> <i>tag_number</i>	Specifies the SGT to match.

## Command Modes

Privileged EXEC

## Supported User Roles

Administrator

## Command History

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

## Usage Guidelines

Enabling any of the **debug cts** commands returns debugging messages for the specified cts service for all TrustSec links to the device. The **debug condition cts** command can filter those debugging messages by setting match conditions for Peer ID, SGT or Security Group Name.

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

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

## Examples

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

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

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

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

switch# show debug condition
```

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

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

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

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

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

**Related Commands**

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

# default (cts manual interface configuration submode)

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

- default policy dynamic identity
- default policy static sgt
- default propagate sgt
- default sap

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

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

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

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

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

Examples

The following example restores the default dynamic policy and SGT propagation policies of a Catalyst 6500 series switch CTS-enabled interface:

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

Related Commands	Command	Description
	<a href="#">policy (cts manual interface configuration submode)</a>	Configures CTS policy for manual mode
	<a href="#">sap (cts manual interface submode)</a>	Configures CTS SAP for manual mode.

# match flow cts

To add the Cisco TrustSec flow objects to a Flexible NetFlow flow record, use the **match flow cts** record configuration command.

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

Syntax Description	<b>destination group-tag</b>	Matches destination fields for the Cisco TrustSec Security Group Tag (SGT)
	<b>source group-tag</b>	Matches source fields for the Cisco TrustSec Security Group Tag (SGT)

Defaults	There are no defaults for this command.
----------	---

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

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

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

Usage Guidelines	Flexible NetFlow can account for packets dropped by SGACL enforcement when SGT and DGT flow objects are configured in the flow record with the standard 5-tuple flow objects
	Use the <b>flow record</b> and <b>flow exporter</b> global configuration commands to configure a flow record, and a flow exporter, then use the <b>flow monitor</b> command to add them to a flow monitor. Use the <b>show flow</b> show commands to verify your configurations..
	To collect only SGACL dropped packets, use the [no] <b>cts role-based {ip   ipv6} flow monitor dropped</b> global configuration command.
	For Flexible NetFlow overview and configuration information, see the following documents:
	<b>Getting Started with Configuring Cisco IOS Flexible NetFlow</b> <a href="http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/get_start_cfg_fnflow.html">http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/get_start_cfg_fnflow.html</a> <b>Catalyst 6500 Release 12.2SY Software Configuration Guide</b> <a href="http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/netflow_hw_support.html">http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/netflow_hw_support.html</a>

## Examples

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

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

## Related Commands

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

# platform cts

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

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

Syntax Description	<b>egress</b>	Specifies the egress TrustSec reflector to be enabled or disabled.
	<b>ingress</b>	Specifies the ingress TrustSec reflector to be enabled or disabled.

Defaults	The default is no ingress or egress reflector.
----------	--

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

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

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

Examples	The following example enables the CTS ingress reflector on a Catalyst 6500 switch:  switch(config)# <b>platform cts egress</b>
	The following example disables the CTS ingress reflector on a Catalyst 6500 switch:  switch(config)# <b>no platform cts egress</b>

Related Commands	<b>Command</b>	<b>Description</b>
	<a href="#">show platform cts reflector</a>	Displays the status of the Cisco TrustSec reflector mode.

## policy (cts manual interface configuration submode)

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

[no] **policy dynamic identity** *peer\_deviceID*

[no] **policy static sgt** *sgt\_number* [**trusted**]

Syntax Description		
<b>dynamic</b>		Obtains policy from the authorization server.
<b>identity</b> <i>peer_deviceID</i>		The peer device name or symbolic name in the authentication server's policy database associated with the policy to be applied to the peer.
<b>static</b>		Specifies an SGT policy to incoming traffic on the link.
<b>sgt</b> <i>sgt_number</i>		Security Group Tag number to apply to incoming traffic from peer.
<b>trusted</b>		Indicates that ingress traffic on the interface with the SGT specified in the command, should not have its SGT overwritten. Untrusted is the default.

**Defaults** No policy is the default.

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

**SupportedUserRoles** Administrator

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

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

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

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

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

- If the **policy static** command is configured without the **trusted** keyword, the SGT is replaced with the SGT configured in the **policy static** command.
- If the **policy static** command is configured with the **trusted** keyword, no change is made to the SGT.

- If the **policy dynamic** command is configured and the authorization policy downloaded from the authentication server indicates that the packet source is untrusted, the SGT is replaced with the SGT specified by the downloaded policy.

The authorization policy can specify the peer's SGT, peer's SGT assignment trust state, RBACLs for the associated peer SGT and an interface ACL.

- If the **policy dynamic** command is configured and the downloaded policy indicates that the packet source is trusted, no change is made to the SGT.

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

## Examples

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

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

```
Router# show cts interface GigabitEthernet 2/1
```

```
Global Dot1x feature is Enabled
```

```
Interface GigabitEthernet2/1:
```

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

```
Replay protection:      enabled
Replay protection mode: STRICT
```

```
Selected cipher:        gcm-encrypt
```

```
Propagate SGT:          Enabled
```

```
Cache Info:
```

```
  Cache applied to link : NONE
```

```
Statistics:
```

```
  authc success:        0
  authc reject:          0
  authc failure:         0
  authc no response:     0
  authc logoff:          0
  sap success:           1
  sap fail:              0
```

```

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

```

**Related Commands**

Command	Description
<a href="#">show cts interface</a>	Displays TrustSec configuration statistics per interface.
<a href="#">default (cts manual interface configuration submode)</a>	Restores default configurations for CTS manual mode.
<a href="#">policy (cts manual interface configuration submode)</a>	Configures CTS policy for manual mode.
<a href="#">sap (cts manual interface submode)</a>	Configures CTS SAP for manual mode.

# propagate (cts dot1x submode)

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

**[no] propagate sgt**

<b>Syntax Description</b>	<b>sgt</b>	Specifies CTS SGT propagation.
---------------------------	------------	--------------------------------

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

<b>Command Modes</b>	CTS Dot1x interface configuration submode (config-if-cts-dot1x)
----------------------	---

<b>SupportedUserRoles</b>	Administrator
---------------------------	---------------

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

<b>Usage Guidelines</b>	<p>SGT propagation (SGT tag encapsulation) is enabled by default in both CTS dot1x and CTS manual interface configuration submodes. A TrustSec-capable port can support Layer-2 MACsec and SGT encapsulation, and negotiates the most secure mode with the peer for the transmittal of the SGT tag and data. MACsec is an 802.1AE standard-based link-to-link protocol used by switches and servers. A peer can support MACsec, but not SGT encapsulation. In such a case, it is recommended that this Layer 2 SGT propagation be disabled with the <b>no propagate sgt</b> CTS Dot1x interface configuration command.</p> <p>To re-enable the SGT propagation enter the <b>propagate sgt</b> command. Use the <b>show cts interface</b> command to verify the state of SGT propagation. Only the disabled state is saved in the nonvolatile generation (NVGEN) process.</p>
-------------------------	--

<b>Examples</b>	The following example disables SGT propagation on a TrustSec-capable interface:
-----------------	---

```

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

router# show cts interface gigabit 6/1
Global Dot1x feature is Enabled
Interface GigabitEthernet6/1:
  CTS is enabled, mode:      DOT1X
  IFC state:                 INIT

<snip> . . .

```

```

SAP Status: UNKNOWN
Configured pairwise ciphers:
  gcm-encrypt
  null

  Replay protection: enabled
  Replay protection mode: STRICT

  Selected cipher:

  Propagate SGT: Disabled
<snip> . . .

```

#### Related Commands

Command	Description
<a href="#">show cts interface</a>	Displays Cisco TrustSec states and statistics per interface.
<a href="#">sap (cts dot1x interface submode)</a>	Configures CTS SAP for dot1x mode.
<a href="#">timer (cts do1x interface submode)</a>	Configures the CTS timer.

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

<b>Syntax Description</b>	sgt	Specifies the Security Group Tag
---------------------------	-----	----------------------------------

<b>Command Modes</b>	CTS manual interface configuration submode (config-if-cts-manual)
----------------------	---

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

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

[illegible]

Related Commands	Command	Description
	<a href="#">show cts interface</a>	Displays Cisco TrustSec states and statistics per interface.
	<b>show running-config</b>	Displays current system configurations.

# sap (cts dot1x interface submode)

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

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

Syntax Description

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

Defaults

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

Command Modes

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

SupportedUserRoles

Administrator

Command History

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

Usage Guidelines

Use the **sap mode-list** command to specify the authentication and encryption method to use during Dot1x authentication.

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

Before the SAP exchange begins after a Dot1x authentication, both sides (supplicant and authenticator) have received the Pairwise Master Key (PMK) and the MAC address of the peer’s port from the Cisco Secure Access Control Server (Cisco Secure ACS). If 802.1X authentication is not possible, SAP, and the PMK can be manually configured between two interfaces in CTS manual configuration mode.

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

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

**Note**

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

**Examples**

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

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

**Related Commands**

Command	Description
<a href="#">propagate (cts dot1x submode)</a>	Enables/disables SGT propagation in dot1x mode.
<a href="#">sap (cts dot1x interface submode)</a>	Configures CTS SAP for dot1x mode.
<a href="#">timer (cts dot1x interface submode)</a>	Configures the CTS timer.

# sap (cts manual interface submode)

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

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

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

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

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

**SupportedUserRoles** Administrator

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

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

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

**Examples** The following example shows a SAP configuration for a Gigabit Ethernet interface:

```

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

```

Related Commands	Command	Description
	<a href="#">default (cts manual interface configuration submode)</a>	Restores default configurations for CTS manual mode.
	<a href="#">policy (cts manual interface configuration submode)</a>	Configures CTS policy for manual mode
	<a href="#">propagate (cts manual interface configuration submode)</a>	Configures CTS SGT Propagation configuration for manual mode
	<a href="#">show cts interface</a>	Displays TrustSec configuration statistics per interface.

# show cts

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

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

Syntax Description		
authorization		Displays the authorization entries.
credentials		Displays credentials used for CTS authentication.
environment-data		Displays the CTS environment data.
interface		Displays CTS interface status and configuration.
keystore		Displays keystore information.
macsec		Displays MACSec counters information.
pacs		Displays A-ID and PAC-info for PACs in the key store.
policy		Displays the CTS policy.
provisioning		Displays outstanding CTS provisioning jobs.
role-based		Displays Role-based Access Control information (SGACL information).

server-list	Displays the CTS server lists.
sxp	Displays CTS SXP protocol information.

**Defaults** None

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

**SupportedUserRoles** Administrator

Command History	Release	Modification
	12.2(33) SXI	This command was introduced on the Catalyst 6500 series switches.
	12.2(50) SY	The following keywords were added for Catalyst 6500 series switches:

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

```
Router# show cts
Global Dot1x feature: Enabled
CTS device identity: "dcas1"
CTS caching support: disabled

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

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

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

show cts

Related Commands

Command	Description
<a href="#">cts credentials</a>	Specifies the TrustSec ID and password.

# show cts authorization entries

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

## show cts authorization entries

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC (>); Privileged EXEC (#)
----------------------	-------------------------------

<b>SupportedUserRoles</b>	Administrator
---------------------------	---------------

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

<b>Examples</b>	The following example is <b>show</b> command output from a Catalyst 6500 switch:
-----------------	--

```

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

Peer-name = Unknown-0000
Peer-SGT = 0-AD23BDF78
Entry State = COMPLETE
Entry last refresh   = 01:30:37 UTC Sat Dec 8 2007
session queue size = 0
Peer policy last refresh = 01:30:37 UTC Sat Dec 8 2007
SGT policy last refresh = 01:30:37 UTC Sat Dec 8 2007
Peer policy refresh time = 0
SGT policy refresh time = 2000
Policy expires in    0:00:29:27 (dd:hr:mm:sec)

```

show cts authorization entries

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

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

Related Commands	Command	Description
	<a href="#">cts credentials</a>	Specifies the TrustSec ID and password.

# show cts credentials

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

**show cts credentials**

<b>Syntax Description</b>	This command has no commands or keywords.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC (>); Privileged EXEC (#)
----------------------	-------------------------------

<b>SupportedUserRoles</b>	Administrator
---------------------------	---------------

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

<b>Examples</b>	Router# <b>show cts credentials</b> CTS password is defined in keystore, device-id = r4
-----------------	--

Related Commands	Command	Description
	<a href="#">cts credentials</a>	Specifies the TrustSec ID and password.

# show cts environment-data

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

## show cts environment-data

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

**Examples** The following example displays the environment data of a Cisco Catalyst 6500 series switch.

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

Related Commands	Command	Description
	<a href="#">clear cts environment-data</a>	Clears TrustSec environment data from cache.

# show cts interface

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

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

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

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

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

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

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

Usage Guidelines	Use the <b>show cts interface</b> command without keywords to display verbose status for all CTS interfaces.
------------------	--

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

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

```

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

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

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

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

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

```

The following example displays output using the **brief** keyword:

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

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

The following example displays output using the **summary** keyword:

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

Related Commands

Command	Description
<a href="#">cts sxp</a>	Configures SXP on a network device.

# show cts macsec

To display crypto ASIC packet counters per interface related to CTS link-to-link encryption, use the **show cts macsec** command.

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

## Syntax Description

<b>interface</b> <i>interface_type slot/port</i>	Specifies the CTS MACsec interface.
<b>delta</b>	Displays counter values since the last time cleared.

## Command Modes

EXEC (>); Privileged EXEC (#)

## Supported User Roles

Administrator

## Command History

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

## Usage Guidelines

This command displays the crypto ASIC packet counters per interface. If Security Associations (SA) are installed (through NDAC or **sap cts interface do1x** or manual subcommands), the active SA's counters are displayed. Only one SA is active at a time. Supported values for SAs are 1 and 2. The delta keyword lists the counter values since the **clear cts macsec counters interface** command was issued.

## Examples

The following example displays the MACsec counters of a manually configured CTS uplink interface on a Catalyst 6500 series switch:

```
router# show cts macsec counters interface gigabitEthernet 6/2
CTS Security Statistic Counters:
    rxL2UntaggedPkts = 0
    rxL2NotagPkts = 0
    rxL2SCMissPkts = 0
    rxL2CTRLPkts = 0
    rxL3CTRLPkts = 0
    rxL3UnknownSAPkts = 0
    rxL2BadTagPkts = 0
    txL2UntaggedPkts = 0
    txL2CtrlPkts = 0
    txL3CtrlPkts = 0
    txL3UnknownSA = 0

GENERIC Counters:
    CRCAlignErrors = 0
    UndersizedPkts = 0
    OversizedPkts = 0
    FragmentPkts = 0
    Jabbers = 0
    Collisions = 0
    InErrors = 0
    OutErrors = 0
```

show cts macsec

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

Related Commands	Command	Description
	<a href="#">show cts interface</a>	
	<a href="#">sap (cts dot1x interface submode)</a>	
	<a href="#">sap (cts manual interface submode)</a>	

# show cts pacs

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

**show cts pacs**

<b>Syntax Description</b>	This command has no commands or keywords.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC (>); Privileged EXEC (#)
----------------------	-------------------------------

<b>SupportedUserRoles</b>	Administrator
---------------------------	---------------

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

<b>Usage Guidelines</b>	Use this command to identify the NDAC authenticator and to verify NDAC completion.
-------------------------	--

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

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

Related Commands	Command	Description
	<a href="#">clear cts pac</a>	Clears a PAC or all PACs from the keystore.
	<a href="#">cts sxp</a>	Configures SXP on a network device.

# show cts policy layer3

To display the name of traffic and exception polices used for CTS Layer3 Transport configurations, use the **show cts policy layer3** command in EXEC or privileged EXEC mode.

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

Syntax Description	ipv4	Specifies IPv4 policies.
	ipv6	Specifies IPv6 policies

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

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

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

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

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

Examples	The following example displays the output of the <b>show cts policy3</b> command:
----------	---

```
router# show cts policy layer3 ipv4
No CTS L3 IPV4 policy received from ACS
Local CTS L3 IPV4 exception policy name : cts-exceptions-local
Local CTS L3 IPV4 traffic policy name   : cts-traffic-local
Current CTS L3 IPV4 exception policy name: cts-exceptions-local
Current CTS L3 IPV4 traffic policy name  : cts-traffic-local
```

Related Commands	Command	Description
	<a href="#">cts policy layer3</a>	Specifies traffic and exception policies for CTS Layer 3 Transport.
	<a href="#">cts layer3</a>	Enables and applies traffic and exception policies to CTS Layer 3 Transport gateway interfaces.

# show cts policy peer

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

## show cts policy peer

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

**Defaults** None

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

**SupportedUserRoles** Administrator

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

**Examples** The following example displays the TrustSec peer authorization policy of all peers:

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

Output Field	Explanation
Peer name	CTS device-id of the peer to which the local device is connected.
Peer SGT	The Security Group Tag of the peer.
Trusted Peer	TRUE—The local device trusts the SGT tagged in the packet coming from this peer. FALSE—The device does not trust the SGT tagged in the packet coming from this peer.
Peer Policy Lifetime	The length of time this policy is valid before it is refreshed.
Peer Last update time	The time when this policy was last refreshed

■ show cts policy peer

Output Field	Explanation
Policy expires in (dd:hr:mm:sec)	This peer policy is due to expire after this elapsed time
Policy refreshes in 0:00:01:51 (dd:hr:mm:sec)	This peer policy will be refreshed after this elapsed time
Cache data applied = NONE	This policy was not populated from cache, i.e., it was acquired from the ACS

Related Commands

Command	Description
<a href="#">cts refresh</a>	Forces refresh of peer authorization policies.
<a href="#">clear cts policy</a>	Clears the peer authorization policy of a TrustSec peer.

# show cts provisioning

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

## show cts provisioning

<b>Syntax Description</b>	This command has no commands or keywords.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC (>); Privileged EXEC (#)
----------------------	-------------------------------

<b>SupportedUserRoles</b>	Administrator
---------------------------	---------------

## Command History

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

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

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

Related Commands	Command	Description
	<a href="#">show cts pacs</a>	Displays the A-ID and PAC-info for PACs in the keystore.
	<a href="#">radius-server host</a>	Specifies the RADIUS servers for device authentication.

# show cts role-based counters

To display Security Group ACL enforcement statistics, use the **show cts role-based counters show** command. Use the **clear cts role-based counters** command to clear the counters.

**show cts role-based counters**

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

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

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

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

## Syntax Description

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

## Command Modes

EXEC (>); Privileged EXEC (#)

## SupportedUserRoles

Administrator

## Command History

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

## Usage Guidelines

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

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

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

When neither **ipv4** nor **ipv6** are specified this command displays only IPv4 counters.

**Examples**

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

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

**Related Commands**

Command	Description
<a href="#">clear cts role-based counters</a>	Resets Security Group ACL statistic counters.
<a href="#">cts role-based</a>	Manually maps a source IP address to a Security Group Tag (SGT) on either a host or a VRF as well as enabling SGACL enforcement.

# show cts role-based sgt-map

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

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

vrf instance_name { ipv4_dec | ipv4_cidr | ipv6_dec | ipv6_cidr | all { ipv4 | ipv6 } | host
    { ipv4_decimal | ipv6_dec } | summary { ipv4 | ipv6 } }
```

Syntax Description	<i>ipv4_dec</i>	Specifies an IPv4 address in dot-decimal notation. For example (208.77.188.166)
	<i>ipv4_cidr</i>	Specifies an IPv4 address range in Classless Inter-Domain Routing (CIDR) For example, 35.0.0.0/8, where the /8 signifies that the 8 most significant bits identify the networks, and the 24 least-significant bits, the hosts.
	<i>ipv6_hex</i>	Specifies an IP version 6 address in hexadecimal separated by colons. For example, 2001:db8:85a3::8a2e:370:7334.
	<i>ipv6_cidr</i>	Specifies a range of IPv6 address in hexadecimal CIDR notation.
	<b>host</b> <i>ipv4_decimal</i>   <i>ipv6_hex</i>	Specifies mappings for a specific IPv4 or IPv6 host. Use dot decimal and hex colon notation for IPv4 and IPv6 respectively.
	<b>all</b>	Specifies all mappings to be displayed.
	<b>summary</b> <b>ipv4</b>   <b>ipv6</b>	Summary of IPv4 or IPv6 mappings. Displays both IPv4 and IPv6 if you do not specify a keyword.
	<b>vrf</b> <i>instance_name</i>	Specify a VPN Routing/Forwarding instance for mappings.

Defaults None

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

SupportedUserRoles Administrator

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

**Usage Guidelines**

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

**Examples**

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

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

IP Address      SGT Source
=====
1.1.1.1         7    INTERNAL
10.252.10.1     7    INTERNAL
10.252.10.10    3    LOCAL
10.252.100.1    7    INTERNAL
172.26.208.31  7    INTERNAL

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

**Related Commands**

Command	Description
<a href="#">cts role-based</a>	Manually maps a source IP address to a Security Group Tag (SGT).
<a href="#">cts sxp</a>	Configures SXP on a network device.
<a href="#">show cts sxp</a>	Displays CTS SXP protocol information

# show cts server-list

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

**show cts server-list**

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

Examples	<p>The following example displays the TrustSec RADIUS server list:</p> <pre>Router&gt; show cts server-list CTS Server Radius Load Balance = DISABLED Server Group Deadtime = 20 secs (default) Global Server Liveness Automated Test Deadtime = 20 secs Global Server Liveness Automated Test Idle Time = 60 mins Global Server Liveness Automated Test = ENABLED (default)  Preferred list, 1 server(s): *Server: 10.0.1.6, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD       Status = ALIVE       auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs Installed list: ACSServerList1-0001, 1 server(s): *Server: 101.0.2.61, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD       Status = ALIVE       auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs</pre>
----------	--

Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td><a href="#">cts server</a></td><td>Displays CTS server list configuration.</td></tr> </table>	Command	Description	<a href="#">cts server</a>	Displays CTS server list configuration.
Command	Description				
<a href="#">cts server</a>	Displays CTS server list configuration.				

# show cts sxp

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

**show cts sxp** { **connections** | **sgt-map** } [**brief** | **vrf** *instance\_name*]

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

**Defaults** None

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

**SupportedUserRoles** Administrator

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(33) SXI	This command was introduced on the Catalyst 6500 series switches.
	12.2 (50) SG7	This command was introduced on the Catalyst 4000 series switches
	12.2 (53) SE2	This command was introduced on the Catalyst 3750(E) and 3560(E) series switches.
	12.2 (53) SE2	This command was introduced on the Catalyst 3750(X) series switches.

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

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

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

The following example displays the SXP connections on a Catalyst 6500 switch using the **brief** keyword:

```
Router# show cts sxp connection brief
SXP                : Enabled
Default Password   : Set
Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
```

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

Total num of SXP Connections = 2

The following example displays the SXP connections on a Catalyst 6500 series switch:

```
Router# show cts sxp connections
SXP                : Enabled
Default Password   : Set
Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
```

```
-----
Peer IP           : 2.2.2.1
Source IP         : 2.2.2.2
Set up            : Peer
Conn status       : On
Connection mode    : SXP Listener
Connection inst#   : 1
TCP conn fd       : 1
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)

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

-----
Total num of SXP Connections = 2
```

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

```
Router# show cts sxp connections
SXP                : Enabled
Default Password   : Set
Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
```

```

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

```

```

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

```

Total num of SXP Connections = 2

The following example displays the current SourceIP-to-SGT mapping database learned through SXP:

```

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

```

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

```

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

```

## Related Commands

Command	Description
<a href="#">cts sxp</a>	Configures SXP on a network device.

# show cts keystore

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

**show cts keystore**

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

**Defaults** None

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

**Supported User Roles** Administrator

Command History	Release	Modification
	12.2(33) SXI	This command was introduced on the Catalyst 6500 series switches as <b>show cts keystore</b> .

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

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

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

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

The following example displays the contents of a Catalyst 6500 hardware keystore:

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

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

```
Hardware Keystore error counters:
FW Panics = 0
FW Resets = 0
```

```
RX FIFO underruns = 12
RX timeouts = 0
RX bad checksums = 0
RX bad fragment lengths = 0
Corruption Detected in keystore = 0
```

**Related Commands**

Command	Description
<a href="#">cts credentials</a>	Specifies the TrustSec ID and password.
<a href="#">cts sxp</a>	Configures SXP on a network device.

# show platform cts reflector

To display the status of the Cisco TrustSec reflector mode (Ingress, Egress, Pure, or No CTS) on a specific interface, use the **show platform cts reflector** command.

**show platformcts reflector interface** type *slot/port*

Syntax Description	<b>interface</b> type <i>slot/port</i> Specifies the interface type, slot and port for which to display status.
--------------------	---

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

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

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

Related Commands	Command	Description
	<a href="#">platform cts</a>	Enables the TrustSec egress or ingress reflector.

## timer (cts do1x interface submode)

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

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

<b>Syntax Description</b>	<b>reauthentication</b> <i>seconds</i> (0–2147483) Timer in seconds. Enter 0 to disable dot1x reauthentication.	
<b>Defaults</b>	The default period is 86,400 seconds (24 hours).	
<b>Command Modes</b>	CTS dot1x interface configuration submode (config-if-cts-dot1x)	
<b>Supported User Roles</b>	Administrator	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(33) SXI	This command was introduced on the Catalyst 6500 Series Switches.
<b>Usage Guidelines</b>	Use the <b>timer reauthentication</b> command to configure a dot1x reauthentication period if the authentication server does not specify a period. If no reauthentication period is specified, the default period is 86,400 seconds. To disable dot1x reauthentication, use the <b>no</b> form of the command or specify a period of 0 seconds. Use the <b>default timer reauthentication</b> command to restore the default value.	
<b>Examples</b>	<p>The following example sets the 802.1X reauthentication period for 48 hours (17, 2800 seconds):</p> <pre>router# config t router(config)# interface gigabitEthernet 6/1 router(config-if)# cts dot1x router(config-if-cts-dot1x)# timer reauthentication 172800</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show cts interface</a>	Displays Cisco TrustSec states and statistics per interface.
	<a href="#">sap (cts dot1x interface submode)</a>	Configures CTS SAP for dot1x mode.
	<a href="#">propagate (cts dot1x submode)</a>	Enables/disables SGT propagation in dot1x mode.

■ timer (cts do1x interface submode)



# APPENDIX **A**

## Notes for Catalyst 3000 and 2000 Series Switches and WLC 5700 Series Wireless LAN Controllers

---

Revised: October 16, 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](http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html)

### Configuration Guidelines and Restrictions

#### Global Cat3K Restrictions

- AAA for Cisco TrustSec requires RADIUS and is supported only by the Cisco Identity Services Engine (Cisco ISE), Release 1.2 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 and Catalyst 3650 Switches, and WLC 5700 Wireless LAN Controllers

- 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 L3 physical interfaces is not currently supported.
- Cisco TrustSec can not be configured on a pure bridging domain with IPSG feature enabled, user has to either enable ip routing, or disable IPSG feature in the bridging domain.
- Cisco TrustSec only supports up to 255 security group tag.

## 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 Layer2 adjacent to the switch.
- Port-to-SGT mapping can be configured only on Cisco TrustSec links (that is, switch-to-switch links). Port-to-SGT mapping cannot be configured on host-to-switch links.
- When port-to-SGT mapping is configured on a port, an SGT is assigned to all ingress traffic on that port. There is no SGACL enforcement for egress traffic on the port.



## APPENDIX **B**

# Notes for Catalyst 4500 Series Switches

---

Revised: April 24, 2013, OL-22192-01

## 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](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).
- We cannot derive the DGT using *IP subnet to SGT mapping*. It can be derived only from *IP address (with a /32 prefix) to SGT mapping*.



### Note

None of the previous restrictions exist for deriving either Source Security Tag (SGT) for any type of traffic, or DGT for *routed traffic* (i.e. traffic forwarded between ports of different VLANs or subnets).

IP-SGT mappings are not VRF-aware.

The 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 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.



# APPENDIX C

## Notes for Catalyst 6500 Series Switches

---

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

### 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](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](http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html)

### Flexible NetFlow Support

Release	Feature History
15.1(1)SY1	<p>The following Flexible NetFlow flow exporter configuration subcommand was introduced on the Catalyst 6500 series switches:</p> <ul style="list-style-type: none"><li>• <b>option cts-sgt-table</b></li></ul> <p>This option allows Flexible NetFlow to export TrustSec environmental data tables that map Security Group Tags (SGTs) to Security Group Names (SGNs).</p>
12.2(50) SY IP Base LAN Image	<p>The following Flexible NetFlow commands and flow objects were introduced on the Catalyst 6500 series switches:</p> <ul style="list-style-type: none"><li>• <b>cts role-based {ip   ipv6} flow monitor <i>monitor_name</i> dropped</b></li><li>• <b>cts source group-tag</b></li><li>• <b>cts destination group-tag</b></li></ul>

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](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)

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

### Configuration Excerpt of an IPV6 Flow Record (5-tuple, direction, SGT, DGT)

```
router(config)# flow record cts-record-ipv6
router(config-flow-record)# match ipv6 protocol
router(config-flow-record)# match ipv6 source address
router(config-flow-record)# match ipv6 destination address
router(config-flow-record)# match transport source-port
router(config-flow-record)# match transport destination-port
router(config-flow-record)# match flow direction
router(config-flow-record)# match flow cts source group-tag
router(config-flow-record)# match flow cts destination group-tag
router(config-flow-record)# collect counter packets
```

### Configuration Excerpt of an IPv4 Flow Monitor

```
router(config)# flow monitor cts-monitor-ipv4
router(config-flow-monitor)# record cts-record-ipv4
```

## Configuration Excerpt of an IPv6 Flow Monitor

```
router(config)# flow monitor cts-monitor-ipv6
router(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:

```
router(config)# cts role-based ip flow monitor cts-monitor-ipv4 dropped
router(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.

```
router(config)# interface TenGigabitEthernet 8/1
router(config-if)# ip address 192.1.1.1 255.255.255.0

;; Ingress IPv4 unicast only and egress unicast only
router(config-if)# ip flow monitor cts-monitor-ipv4 unicast input
router(config-if)# ip flow monitor cts-monitor-ipv4 unicast output

;; Ingress IPv4 L2-switched traffic only
router(config-if)# ip flow monitor cts-monitor-ipv4 layer2-switched input

;; Ingress IPv4 multicast and egress IPv4 multicast traffic only
router(config-if)# ip flow monitor cts-monitor-ipv4 multicast input
router(config-if)# ip flow monitor cts-monitor-ipv4 multicast output

;; For both Unicast/multicast egress traffic
router(config-if)# ip flow monitor cts-monitor-ipv4 output

;; For both Unicast/multicast ingress traffic
router(config-if)# ip flow monitor cts-monitor-ipv4 input

;; For IPv6 only the following are supported in Cisco IOS Release 12.2(50)SY
router(config-if)# ipv6 address 2022::22:1:1:11/64
router(config-if)# ipv6 flow monitor cts-monitor-ipv6 input
router(config-if)# ipv6 flow monitor cts-monitor-ipv6 unicast input
router(config-if)# ipv6 flow monitor cts-monitor-ipv6 output
router(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 team
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](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](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](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.





## GLOSSARY

Revised: May 28, 2010, OL-22192-01

---

### 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.

---

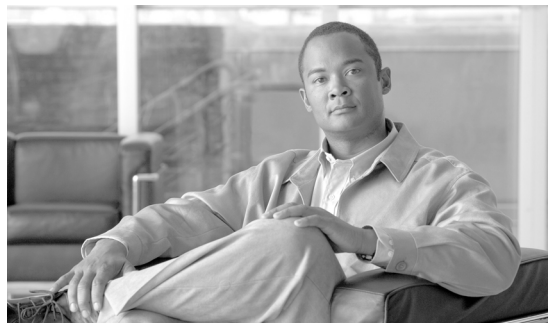
## T

**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.





## INDEX

---

### Numerics

802.1AE

See Cisco TrustSec, IEEE 802.1AE support

802.1X [6-2](#)

802.1X Host Modes [6-5](#)

---

### C

Cisco TrustSec

architecture [1-1](#)

authorization [1-10](#)

configuring [4-10](#)

configuring NDAC [1-3](#)

connection caching [4-9](#)

default values [2-3](#)

enabling [3-2, 3-3](#)

environment data download [1-11](#)

guidelines and limitations [2-3](#)

IEEE 802.1AE support [1-12](#)

link security [1-12](#)

manual mode [3-6](#)

permissions matrix [1-7](#)

policy acquisition [1-10](#)

RADIUS relay [1-12](#)

SAP negotiation [1-12](#)

seed device [1-1, 1-11, 3-2](#)

SGACLs [1-10](#)

SGTs [1-7 to 1-10, 3-11](#)

SXP [4-1](#)

Cisco TrustSec. See CTS

Cisco TrustSec authentication

description [1-6](#)

Cisco TrustSec caching

clearing [4-10](#)

enabling [4-9](#)

Cisco TrustSec device credentials

description [1-6](#)

Cisco TrustSec device identities

description [1-6](#)

Cisco TrustSec environment data

download [1-11](#)

Cisco TrustSec manual mode

configuring [3-6](#)

Cisco TrustSec Solution

configuring [2-1](#)

Cisco TrustSec user credentials

description [1-6](#)

conditional debugging [7-56](#)

CTS

configuring [4-10](#)

description [1-1](#)

CTS authentication

description [1-3](#)

cts role-based policy trace [7-25](#)

---

### D

debug condition cts [7-56](#)

DGT

See SGT, destination

DHCP Snooping [6-6](#)

Diagnostic trace [7-25](#)

---

**E**

EAP-FAST

in Cisco TrustSec authentication [1-3](#)Error Messages [C-4](#)

---

**F**FAS [6-5](#)

Fibre Channel interfaces

default settings [3-12, 3-17](#)

FIPS

Catalyst 6500 Series support [C-4](#)Flexible NetFlow [C-1](#)

---

**G**

Galois/Counter Mode. See GCM

GCM

Cisco TrustSec SAP encryption [1-12](#)

GCM authentication. See GMAC

GMAC

Cisco TrustSec SAP authentication [1-12](#)

---

**I**

Identity Port Mapping

See IPM

interfaces

default settings [3-12, 3-17](#)

IPM

configuring [3-7](#)description [1-9](#)

---

**L**L2 VRF assignment [7-32](#)L3IF-SGT mapping [3-20](#)

---

**M**MAB [6-3](#)

MACSec

See Cisco TrustSec, link security

management interfaces

default settings [3-12, 3-17](#)

Media Access Control Security

See Cisco TrustSec, link security

mgmt0 interfaces

default settings [3-12, 3-17](#)

---

**N**

NDAC

for Cisco TrustSec [1-3](#)NetFlow [C-1](#)

Network Device Admission Control

See NDAC

---

**P**

PAC

in Cisco TrustSec authentication [1-3](#)Pre-Authentication Open Access [6-5](#)

protected access credential

See PAC

---

**S**

Security Association Protocol. See SAP

security group access list

See SGACL

security group tag

See SGT

seed device

in a Cisco TrustSec network [1-1, 1-11, 3-2](#)

SGACL policies

- configuration process [5-2](#)
- displaying [5-6](#)
- displaying downloads [5-7](#)
- enabling enforcement for VLANs [5-3](#)
- enabling enforcement globally [5-2, 5-3](#)
- enabling enforcement per interface [5-3](#)
- manually configuring [5-4](#)

## SGACLs

- description [1-7, 1-10](#)

## SGACLs policies

- acquisition [1-10](#)

## SGT

- destination [1-7](#)
- source [1-7](#)

## SGT Exchange Protocol

- See SXP

## SGTs

- description [1-7 to 1-10](#)
- manually configuring [3-11](#)
- manually mapping IP addresses [3-12](#)

## Subnet to SGT mapping [3-12](#)

## SXP

- configuration process [4-2](#)
- configuring [4-1](#)
- configuring peer connections [4-2](#)
- default passwords [4-4](#)
- description [1-13](#)
- enabling [4-2](#)
- reconcile period [4-5](#)
- retry period [4-5](#)
- source IP address [4-4](#)

## Syslog Messages [C-4](#)

## System Error Messages [C-4](#)

---

## T

### Troubleshooting

- SGACL and SGT behavior [7-25](#)

### TrustSec

- SGACLs [1-7](#)

TrustSec. See CTS

---

## V

### VLANs

- enabling SGACL policy enforcement [5-3](#)

### VLAN to SGT mapping [3-19](#)

### VRF

- cts role-based command [7-93](#)
- cts sxp command [7-39](#)
- overview [1-17](#)
- Specifying for an SXP connection [4-3](#)

---

## W

### WebAuth [6-4](#)

- web-based authentication [6-4](#)

