Cisco TrustSec Configuration Guide

First Published: 2025-08-25

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

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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Read Me First

Only supported features are documented. To confirm or clarify all the supported features for a platform, go to Cisco Feature Navigator.

CONTENTS

PREFACE

CHAPTER 1

CHAPTER 2

CHAPTER 1

Cisco TrustSec

Feature History for Cisco TrustSec

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 17.18.1	Cisco TrustSec: Cisco TrustSec builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers, and communication between devices is secured with encryption, message integrity checks, and data-path replay protection.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Cisco TrustSec

Cisco TrustSec builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers, and communication between devices is secured with encryption, message integrity checks, and data-path replay protection.

Key components of Cisco TrustSec

Cisco TrustSec architecture incorporates these 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 roup number) of source and destination devices rather than on network addresses. Individual packets are tagged with the security group number of the source.

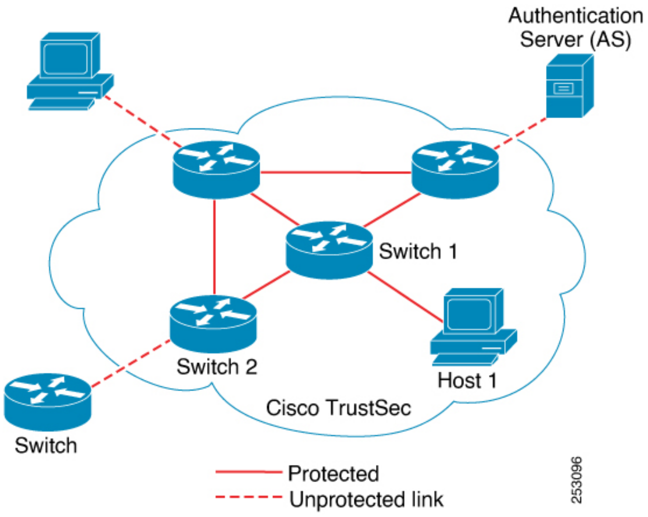
- Secure communication:

  With encryption-capable hardware, communication on each link between devicesin the domain can be secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms.

Figure shows a Cisco TrustSec domain with

- An endpoint device and several networking devices within the Cisco TrustSec domain.
- An endpoint device and one networking device outside the Cisco TrustSec domain. This is because they are either not Cisco TrustSec-capable devices or they have been refused access.
- The authentication server outside of the Cisco TrustSec domain. The authentication server can either be a Cisco Identities Service Engine (Cisco ISE), or a Cisco Secure Access Control System (Cisco ACS)

Figure 1: Cisco TrustSec Domain



Roles in the Cisco TrustSec authentication process

In the Cisco TrustSec authentication process, there are these roles:

- Supplicant

  An unauthenticated device that is connected to a peer within the Cisco TrustSec domain and is attempting to gain access to the domain.

- Authentication Server

  The system responsible for verifying the supplicant's identity and assigning policies that control the supplicant's access to services within the Cisco TrustSec domain.

- Authenticator

  An authenticated device that is already a member of the Cisco TrustSec domain and is authorized to authenticate new supplicant peers on behalf of the authentication server.

Authentication Process Sequence

When a connection is established between a supplicant and an authenticator, the process typically follows these steps:

1. Authentication (802.1X):

   The supplicant's credentials are verified by the authentication server, with the authenticator serving as an intermediary. Mutual authentication takes place between the supplicant and the authenticator.

2. Authorization:

   Based on the supplicant's identity, the authentication server issues authorization policies, such as security group assignments and access control lists (ACLs), to both connected peers. The server also shares each peer's identity with the other, enabling the appropriate policies to be applied to the link.

3. Security Association Protocol (SAP) Negotiation:

   If both ends of the link support encryption, the supplicant and authenticator negotiate parameters to establish a security association.

Once all three steps are successfully completed, the authenticator transitions the link from an unauthorized (blocking) state to an authorized state, allowing the supplicant to join the Cisco TrustSec domain.

Identities and Credentials

The following sections describe these foundational elements—Device Identities, Device Credentials, User Credentials, and Protected Access Credentials (PACs)—and how they interact in a TrustSec deployment.

Device Identities

Cisco TrustSec uses assigned device names (device IDs) instead of IP or MAC addresses to uniquely identify switches. These device IDs are used for authorization policy lookups and password lookups during authentication.

Device Credentials

Cisco TrustSec supports password-based credentials and uses MSCHAPv2 for mutual authentication.

Device credentials are used during EAP-FAST phase 0 (PAC provisioning) exchanges. Subsequent link bring-ups use EAP-FAST phase 1 and 2, leveraging the provisioned PAC.

User Credentials

Cisco TrustSec does not require a specific type of user credential for endpoint devices. Any authentication method supported by the authentication server (for example, MSCHAPv2, GTC, RSA OTP for Cisco ACS 5.1) can be used.

Protected Access Credential

A PAC is a unique shared credential for mutual client and server authentication, eliminating the need for Public Key Infrastructure (PKI) and digital certificates.

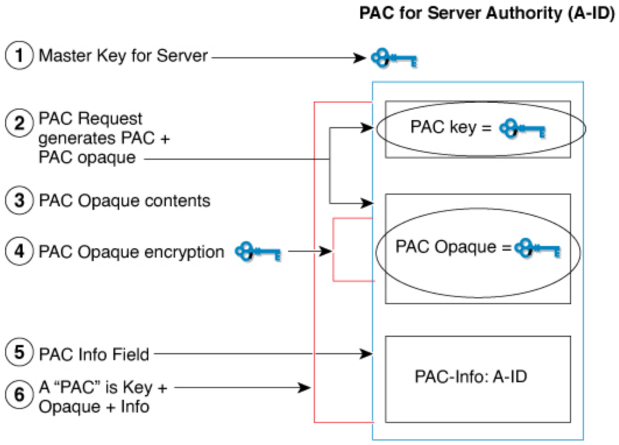
PAC Creation Steps

1. The server's Authority Identity (A-ID) maintains a local master key.
2. When a client, initiator identity (I-ID), requests a PAC, the server generates a unique PAC key and PAC-Opaque field.
3. The PAC-Opaque field contains the PAC key, I-ID, and key lifetime, encrypted with the master key.
4. A PAC-Info field containing the A-ID is created.
5. The PAC is automatically distributed or imported to the client.

Note The server does not maintain the PAC or PAC key, enabling a stateless EAP-FAST server.

The figure below describes the PAC's construction. A PAC consists of the PAC-Opaque, PAC Key, and PAC-Info fields. The PAC-Info field contains the A-ID.

Figure 2: PAC's Process Flow



PAC Provisioning

- In Secure RADIUS, the PAC key is provisioned into each device during authentication to derive the shared secret.
- Clients send an additional RADIUS attribute containing the PAC-Opaque field, which the server interprets to recover information and validate identity.
- EAP-FAST Phase 0 is used for automatic PAC provisioning.

PAC-less Authentication

PAC-less mode simplifies the deployment of Cisco TrustSec policies by eliminating the need for a Protected Access Credential (PAC), which is typically required for secure communication between devices and the Identity Services Engine (ISE). This approach is particularly advantageous in environments with multiple ISE nodes, as devices can seamlessly connect to a secondary ISE node if the primary becomes unavailable, without the need to re-establish the PAC, thus reducing service interruptions.

Benefits

By removing the dependency on PACs, AAA PAC-less authentication streamlines the authentication process. This enhances scalability, improves the user experience, and enables support for modern authentication approaches consistent with Zero Trust security principles.

PAC-less Authentication Workflow

1. In PAC-less mode, devices begin authentication by sending a RADIUS request that includes the Cisco TrustSec username, password, and an EAP attribute message.
2. The ISE replies with a RADIUS access-challenge to initiate an EAP-FAST session.
3. Once the EAP-FAST session is established, the ISE provides the PAC opaque and PAC information. The PAC opaque contains the PAC key and user identity, encrypted using the EAP-FAST server master key. The PAC information includes the server identity and Time-to-Live timers.

4. The PAC opaque is then embedded in the Message-Authenticator field of subsequent Cisco TrustSec RADIUS requests to the ISE. This enables the secure download of environment data and Security Group Access Control List (SGACL) policies.

Guidelines for Cisco TrustSec

General Guidelines

- Cisco TrustSec is not supported in FIPS mode.
- Cisco TrustSec cannot be configured on a pure bridging domain with the IPSG enabled.

Guidelines for Identities and Credentials

- Protected access credential (PAC) provisioning fails and remains in hung state, when an invalid device ID is specified. Even after clearing the PAC, and configuring the correct device ID and password, PAC still fails.

  As a workaround, in the Cisco Identity Services Engine (ISE), uncheck the Suppress Anomalous Clients option in the **Administration** > **System** > **Settings** > **Protocols** > **Radius** menu for PAC to work.

Configure Cisco TrustSec Credentials

This task allows you to configure your device with device ID, password and authentication method.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted

Step 2 **cts credentials id** *cts-id* **password** *password*

Example:

```
Device# cts credentials id ctsid password abcd
```

Configures the Cisco TrustSec device ID for this device to use when authenticating with other Cisco TrustSec devices with EAP-FAST because Cisco TrustSec requires each device in the network to identity itself uniquely.

- The *cts-id* argument has a maximum length of 32 characters and is case sensitive.
- The *password* argument is the password or this device to use when authenticating with other Cisco TrustSec devices with EAP-FAST.

Step 3 **configure terminal**

Example:

```
Device(config)# configure terminal
```

Enters global configuration mode.

Step 4 **aaa new-model**

Example:

```
Device(config)# aaa new-model
```

Enables new RADIUS and AAA access control commands and functions and disables old commands.

Step 5 **aaa authentication dot1x default group radius**

Example:

```
Device(config)# aaa authentication dot1x default group radius
```

Specifies that RADIUS servers are used for authentication on interfaces running IEEE 802.1X.

Step 6 **cts authorization list network** *list-name*

Example:

```
Device(config)# cts authorization list network cts-mlist
```

Specifies a list of AAA servers for the Cisco TrustSec seed device to use.

Step 7 **aaa authorization network** *list-name* **group radius**

Example:

```
Device(config)# aaa authorization network cts-mlist group radius
```

Specifies the Cisco TrustSec authorization list name for allnetwork-related service requests from RADIUS servers.

Step 8 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode.

Step 9 **show cts server-list**

Example:

```
Device# show cts server-list
```

Displays the RADIUS the server configurations for Cisco TrustSec seed devices

Step 10 **show cts credentials**

Example:

```
Device# show cts credentials
```

Display sthe Cisco TrustSec device ID. The stored password is never displayed.

Security Groups and Security Group Tags

These sections provide information about security groups and security group tags.

Security Groups

A security group is a collection of users, endpoint devices, and resources that share common access control policies. Administrators define these groups in Cisco ISE or Cisco Secure ACS. When new users or devices join the Cisco TrustSec domain, the authentication server automatically assigns them to the appropriate security groups. Each group receives a unique 16-bit security group number, which is globally recognized within the Cisco TrustSec domain. The total number of security groups is determined by the number of authenticated network entities, and administrators do not need to manually configure these group numbers.

Security Group Tags and Packet Tagging

After a device is authenticated, Cisco TrustSec tags every packet originating from that device with a Security Group Tag (SGT). This tag includes the device's assigned security group number and travels with the packet across the network within the Cisco TrustSec header. The SGT acts as a single label that defines the source's access privileges throughout the enterprise network.

Source and Destination Group Tags

The SGT represents the security group of the packet's source, so it is often called the source SGT. The device receiving the packet is also assigned to a security group, known as the destination security group (SG). For simplicity, this may be referred to as the destination group tag (DGT), although the Cisco TrustSec packet itself does not include the destination device's security group number.

Determining the Source Security Group Tag

When a packet enters a Cisco TrustSec domain, the network device at the ingress point must identify the source SGT so it can tag the packet appropriately before forwarding it into the TrustSec environment. Similarly, the egress device needs to determine the packet's SGT to enforce Security Group Access Control Lists (SGACLs).

There are several ways a network device can determine the SGT for a packet:

1. Policy Acquisition from the Authentication Server

   After the Cisco TrustSec authentication process, the network device obtains policy information from the authentication server. This information includes whether the peer device is trusted. If the device is not trusted, the authentication server provides an SGT, which the network device applies to all packets received from that peer.

2. SGT Included in the Packet

   If the packet is received from a trusted peer device, it will already carry the SGT. This situation applies to devices that are not the initial entry point in the Cisco TrustSec domain for the given packet.

3. Identity Port Mapping (IPM)

With Identity Port Mapping, the network administrator can manually assign an identity to the link connected to the peer device. The network device then requests policy details, including the SGT and trust status, from the authentication server.

4. Source IP Address Lookup

   In certain scenarios, policies can be configured to assign an SGT to a packet based on its source IP address. The SGT Exchange Protocol (SXP) can also be used to automatically populate the mapping table between IP addresses and SGTs.

Determining the Destination Security Group Tag

The egress network device in a Cisco TrustSec domain is responsible for identifying the destination security group (DGT) in order to enforce SGACLs. To determine the destination security group for a packet, the network device uses the same methods as those used for determining the source security group, except that it cannot extract the group number from a packet tag—since the destination group number is not included in the packet's tag.

In certain scenarios, ingress devices or other intermediate network devices may have access to destination group information. When this occurs, SGACLs can be enforced at these devices rather than solely at the egress point.

Link Security

When both ends of a link support 802.1AE Media Access Control Security (MACsec), a SAP negotiation is initiated. During this process, an Extensible Authentication Protocol over LAN (EAPOL) key exchange takes place between the supplicant and authenticator to:

- Negotiate a cipher suite
- Exchange security parameters
- Manage cryptographic keys

Once all these steps are successfully completed, a security association is established.

Depending on your software version, crypto licensing, and hardware capabilities, SAP negotiation can operate in one of the following modes:

Mode	Description
Galois/Counter Mode (GCM)	Provides both authentication and encryption
GCM Authentication (GMAC)	Provides authentication without encryption
No Encapsulation	Transmits data in clear text, with no encapsulation
Null	Applies encapsulation, but without authentication or encryption

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

Configure SAP-PMK for Link Security

To configure SAP-PML for link security, perform this procedure.

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **interface** *type number*

Example:

```
Device(config)# interface TenGigabitEthernet 1/1/4
```

Configures an interface and enters interface configuration mode.

Step 4 **switchport mode trunk**

Example:

```
Device(config-if)# switchport mode trunk
```

Specifies a trunking VLAN Layer 2 interface.

Step 5 **cts manual**

Example:

```
Device(config-if)# cts manual
```

Enters Cisco TrustSec manual configuration mode.

Step 6 **no propogate sgt**

Example:

```
Device(config-if-cts-manual)# no propagate sgt
```

Use the **no** form of this command when the peer is incapable of processing a SGT. The **no propagate sgt** command prevents the interface from transmitting the SGT to the peer.

Step 7 **sap pmk** *key* [**mode-list** *mode1* [*mode2* [*mode3* [*mode4*]]]]

Example:

```
Device(config-if-cts-manual)# sap pmk
00000000000000000000000000000000000000000000000000001234567890 mode-list gcm-encrypt gmac
```

Configures the SAP pairwise master key (PMK) and operation mode.

Note
SAP is disabled by default in Cisco TrustSec manual mode.

key: A hexadecimal value with an even number of characters and a maximum length of 32 characters.

The SAP operation mode options are described below:

- **gcm-encrypt**: Authentication and encryption

  Note
  Select this mode for MACsec authentication and encryption if your software license supports MACsec encryption.

- **gmac**: Authentication, no encryption
- **no-encap**: No encapsulation
- **null**: Encapsulation, no authentication or encryption

Note
If the interface is not capable of data link encryption, the no-encap command is the default and the only available SAP operating mode. SGT is not supported.

Step 8 **end**

Example:

```
Device(config-if-cts-manual)# end
```

Exits Cisco TrustSec manual configuration mode and returns to privileged EXEC mode.

CHAPTER 2

Security Group ACL

Feature History for SGACL

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 17.18.1	SGACL: Security Group Access Control Lists (SGACLs) enable administrators to enforce policies that control what operations users can perform based on their assigned security groups and the resources they are accessing.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Security Group ACL

Security Group Access Control Lists (SGACLs) enable administrators to enforce policies that control what operations users can perform based on their assigned security groups and the resources they are accessing.

SGACLs provide a stateless access control mechanism, relying on security group tags rather than traditional IP addresses and filters.

There are three primary ways to provision SGACL policies:

- Static Policy Provisioning:

  Administrators manually define SGACL policies using the **cts role-based permission** command.

- Dynamic Policy Provisioning:

  SGACL policies are centrally managed and configured through Cisco Secure ACS or Cisco Identity Services Engine (ISE) policy management functions.

- Change of Authorization (CoA):

  When an SGACL policy is updated on Cisco ISE, the new policy is pushed to the TrustSec device via CoA. The device's data plane applies the new policy to the CoA packets, which are then forwarded to the control plane for further enforcement.

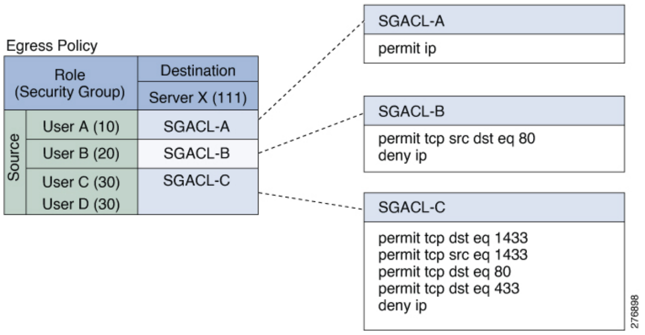
Role-Based Access Control with SGACL Policies

SGACLs enable precise control over the actions users can perform, based on their assigned security groups and the resources they access.

Within the Cisco TrustSec domain, policy enforcement is managed through a permissions matrix: source security group numbers are listed on one axis and destination security group numbers on the other. Each cell in the matrix holds an ordered list of SGACLs, specifying which permissions apply to packets traveling from a given source security group to a particular destination security group.

The following figure 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 3: SGACL Policy Matrix Example



Egress Policy

	Role (Security Group)	Destination
		Server X (111)
Source	User A (10)	SGACL-A
	User B (20)	SGACL-B
	User C (30) User D (30)	SGACL-C

SGACL-A

```
permit ip
```

SGACL-B

```
permit tcp src dst eq 80
deny ip
```

SGACL-C

```
permit tcp dst eq 1433
permit tcp src eq 1433
permit tcp dst eq 80
permit tcp dst eq 433
deny ip
```

Benefits of SGACLs in Cisco TrustSec

By assigning users and devices to security groups and controlling access between these groups, Cisco TrustSec provides role-based, topology-independent access control. Unlike traditional access control lists (ACLs) that rely on IP addresses, SGACLs use device identities. This means devices can move or change IP addresses anywhere in the network, and security policies remain unchanged as long as their roles and permissions stay the same. When a new user or device is added, simply assign it to the appropriate security group and it immediately inherits the group's permissions.

Simplified Policy Management and Resource Efficiency

SGACLs streamline access control by reducing the number and complexity of access control entries (ACEs). The total number of ACEs is determined by the number of distinct permissions, which is typically much lower than in traditional IP-based ACLs. This role-based approach not only simplifies ongoing maintenance but also makes more efficient use of hardware resources, such as TCAM, on network devices. Cisco TrustSec supports up to 5,000 SGACL policies.

Device Authentication and Link Authorization in Cisco TrustSec

After device authentication is complete, both the supplicant and authenticator receive security policy information from the authentication server. The two devices then perform link authorization and enforce the appropriate link security policy based on their Cisco TrustSec device IDs.

The link authentication method can be configured as either 802.1X or manual authentication:

- 802.1X Authentication:

  Each device uses its device ID, as provided by the authentication server.

- Manual Authentication:

  Device IDs must be manually assigned to each peer.

The authentication server supplies the following policy attributes:

- Cisco TrustSec Trust:

  Specifies whether the peer device is trusted to insert the Security Group Tag (SGT) into packets.

- Peer SGT:

  Identifies the security group to which the peer belongs. If the peer is not trusted, all packets from that device are tagged with this SGT. If the device is unsure whether there are SGACLs associated with the peer's SGT, it may send a follow-up request to the authentication server to retrieve the necessary SGACLs.

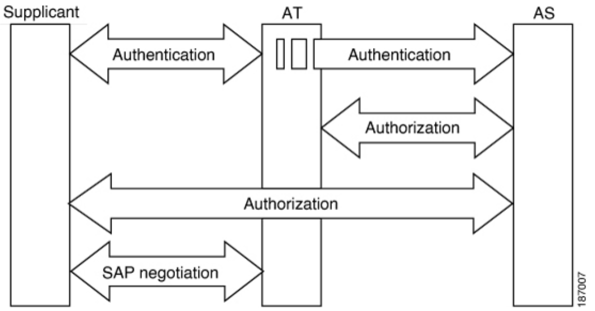
- Authorization Expiry Time:

  Indicates how many seconds the authorization and policy are valid. Devices should refresh their policy and authorization before expiration. Cached authentication and policy data can be reused after a reboot, provided it has not expired.

Note 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 the following figure:

Figure 4: NDAC and SAP Negotiation



SGACL - Layer 2 Enforcement

Enforcement at Layer 2 is done by applying SGACL policies on interfaces or VLANs, filtering traffic based on SGTs carried in the packets. This allows segmentation and control within the same Layer 2 domain.

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.

- Routed Traffic:

  SGACL enforcement applies only to IP traffic and is performed by an egress switch (for esample a distribution switch or an access switch with a routed port). When globally enabled, it's automatic on Layer 3 interfaces (except SVI).

- Switched Traffic:

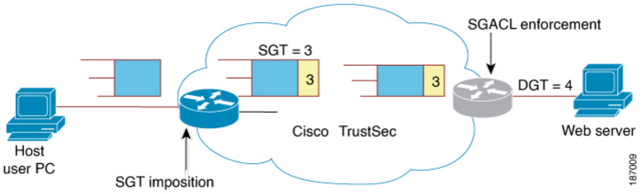
  Enforcement is on traffic within a single switching domain without routing. It can apply to packets switched within a VLAN or forwarded to an SVI associated with a VLAN, but must be explicitly enabled per VLAN.

Ingress Tagging and Egress Enforcement in Cisco TrustSec

Cisco TrustSec enforces access control through a combination of ingress tagging and egress enforcement. When traffic enters the Cisco TrustSec domain, the ingress device tags the packets with a SGT that identifies the security group number of the source. This SGT remains with the traffic as it traverses the TrustSec domain. At the egress point, the egress device evaluates both the source SGT and the security group number of the destination (also known as the destination group tag or DGT). Using this information, the egress device references the SGACL policy matrix to determine and enforce the appropriate access policy for the traffic.

The following figure shows how the SGT assignment and the SGACL enforcement operate in a Cisco TrustSec domain.

Figure 5: SGT and SGACL in a Cisco TrustSec Domain



This is how packet flow with SGT and SGACL enforcement works:

1. The host PC sends a packet to the web server. While neither the PC nor the web server are members of the Cisco TrustSec domain, the packet's path passes through the Cisco TrustSec network.
2. The Cisco TrustSec ingress device receives the packet and adds a SGT with security group number 3, as assigned to the host PC by the authentication server.
3. The Cisco TrustSec egress device examines the packet and applies the SGACL policy that governs traffic from source group 3 (host PC) to destination group 4 (web server), with group 4 being the security group assigned to the web server by the authentication server.
4. If the SGACL permits the traffic, the Cisco TrustSec egress switch removes the SGT from the packet and forwards it to the web server.

SGACL Logging

SGACL Logging in Cisco TrustSec records detailed information about traffic matching SGACLs. When SGACL logging is enabled, the device logs the following details:

- The source and destination Security Group Tags (SGTs)
- The name of the SGACL policy
- The protocol type of the packet
- The action taken on the packet

The logging option can be applied to individual ACEs, so only packets matching those ACEs will be logged. The first packet that triggers the log keyword generates a syslog message. After that, log messages are reported every five minutes. If the same ACE logs another packet with identical characteristics, the device increments the match counter and includes this information in the next report.

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

When SGACL logging is enabled, ICMP Request messages from the device to the client are not logged for IPv4 and IPv6 protocols. However; ICMP Response messages from the client to the device are logged.

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

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

SGACL Logging and Message Control

Devices can generate logging messages for packets that are permitted or denied by a standard IP access list or an SGACL. Whenever a packet matches an SGACL entry, an informational message is sent to the console. The volume of messages displayed on the console is managed using the **logging console** command, which controls syslog output.

SGACL logging has been enhanced to use NetFlow hardware, which allows much larger logging rates.

When the first packet triggers an SGACL entry, a flow is created, and logging occurs based on NetFlow timeouts: 30 seconds for inactive flows and 1 minute for active flows. After this initial period, subsequent packets are counted and summarized, with logging messages generated every 5 minutes.

Each log message includes:

- The access list number
- Whether the packet was permitted or denied
- The source and destination IP addresses
- The ingress interface
- The number of packets permitted or denied from the same source during the previous 5-minute interval

SGACL Cell Statistics

SGACL Cell Statistics provide granular visibility into the enforcement of SGACL policies. The enforcement matrix is organized by source and destination SGT pairs, with each cell representing the permissions applied between those groups. Administrators can view per-cell statistics showing how many packets were allowed or denied by the SGACLs for each SGT pair.

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

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

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

SGACL Monitor Mode

SGACL Monitor Mode is designed for the pre-deployment phase of Cisco TrustSec, allowing administrators to test security policies without enforcing them. This mode helps verify that policies behave as expected before actual enforcement begins. If any policies do not work as intended, monitor mode makes it easy to identify and correct issues, ensuring that security requirements, such as denying unauthorized access, are met before enforcement is enabled.

Monitoring operates at the SGT-DGT (Source Group Tag–Destination Group Tag) pair level. When SGACL monitor mode is enabled, any deny action in the policy is treated as a permit on the device's line cards. This ensures that SGACL counters and logging provide visibility into policy behavior, showing how traffic would be handled if enforcement were active. Since all monitored traffic is allowed, there is no disruption of service during the testing phase.

Restrictions for SGACL

These restrictions are applicable to all switches:

- Due to hardware limitations, Cisco TrustSec SGACLs cannot be enforced for punt (CPU bound) traffic in hardware. SGACL enforcement in software is bypassed for CPU-bound traffic for switch virtual interface (SVI) and Layer 2 and Layer 3 Location Identifier Separation Protocol (LISP), and loopback interfaces.
- When configuring SGACL policies, if you change the IP version dynamically from IPv4 or IPv6 to Agnostic (applies to both IPv4 and IPv6) and vice-versa, the corresponding SGACL policies for IPv4 and IPv6 are not downloaded completely through the management VRF interface.
- When configuring SGACL policies, if you change the existing IP version to any other version (IPv4, IPv6, or Agnostic) and vice-versa, Change of Authorization (CoA) from Cisco Identity Services Engine (ISE) cannot be performed using RADIUS. Instead, use SSH and run the **cts refresh policy** command to perform a manual policy refresh.
- When using an allowed SGT model with default action as **deny all**, in some cases, Cisco TrustSec policies are only partially downloaded from the ISE server after a device reload.

  To prevent this, define a static policy on the device. Even if the deny all option is applied, the static policy permits traffic that allows the device to download policies from the ISE server and overwrite the defined static policies. For device SGT, configure the following commands in global configuration mode:

  - **cts role-based permissions from** *sgt_num* **to unknown**
  - **cts role-based permissions from unknown to** *sgt_num*

These restrictions are applicable to Cisco C9610 Series Smart Switches.

- The same set of ACLs cannot be used for both regular SGACL cell permissions and SGACL default permissions. Use a unique set of ACLs for default permission instead.
- Cell permit and deny counters are supported only for the first 511 cells.
- Counters are not supported for default permissions.

How to Configure SGACLs

These sections provide configuration information about SGACLs.

SGACL Policy Configuration Process

Follow these steps to configure and enable SGACL policies:

Procedure

Step 1 Configuration of SGACL policies should be done primarily through the Policy Management function of the Cisco Secure Access Control Server (ACS) or the Cisco Identity Services Engine (ISE).

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.

Note
An SGACL policy that is 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.

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

Enable 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:

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts role-based enforcement**

Example:

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

Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.

Step 4 **end**

Example:

```
Device(config)# end
```

Exits global configuration mode and returns to privileged EXEC mode.

Enable SGACL Policy Enforcement Per Interface

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

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

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **interface** *type slot/port*

Example:

```
Device(config)# interface gigabitethernet 6/2
```

Configures an interface and enters interface configuration mode.

Step 4 **cts role-based enforcement**

Example:

```
Device(config-if)# cts role-based enforcement
```

Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.

Step 5 **end**

Example:

```
Device(config-if)# end
```

Exits interface configuration mode and returns to privileged EXEC mode.

Enable 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:

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts role-based enforcement vlan-list** *vlan-list*

Example:

```
Device(config)# cts role-based enforcement vlan-list 31-35,41
```

Enables Cisco TrustSec SGACL policy enforcement on the VLAN or VLAN list.

Step 4 **end**

Example:

```
Device(config)# end
```

Exits global configuration mode and returns to privileged EXEC mode.

Configure SGACL Monitor Mode

To configure SGACL monitor mode, follow this procedure:

Before you begin

Before configuring SGACL monitor mode, ensure the following:

- Cisco TrustSec is enabled
- Counters are enabled

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts role-based monitor all**

Example:

```
Device(config)# cts role-based monitor all
```

Enables global monitor mode.

Step 4 **cts role-based monitor permissions from** {*sgt_num*} **to** {*dgt_num*} [**ipv4** | **ipv6**]

Example:

```
Device(config)# cts role-based permissions from 2 to 3 ipv4
```

Enables monitor mode for IPv4 or IPv6 Role-Based Access Control List (RBACL).

- *sgt_num*: Security Group Tag
- *dgt_num*: Destination Group Tag

Step 5 **end**

Example:

```
Device(config)# end
```

Exits global configuration mode and returns to privileged EXEC mode.

Configure SGACL policies manually

A role-based access control list (ACL) that is applied to a range of Source Group Tags (SGTs) and Destination Group Tags (DGTs) becomes an SGACL, which is a Cisco TrustSec policy enforced on egress traffic. The recommended approach for configuring SGACL policies is to use the policy management features of Cisco Identity Services Engine (ISE) or Cisco Secure ACS.

For local (manual) configuration, you can create a role-based ACL and bind it to a specific range of SGTs. This allows you to define and enforce access control policies directly on the device.

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

Configure and Apply IPv4 SGACL Policies

To configure and apply IPv4 SGACL policies, perform this procedure:

Before you begin

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

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **ip access-list role-based** *rbacl-name*

Example:

```
Device(config)# ip access-list role-based allow_webtraff
```

Creates an RBACL and enters Role-based ACL configuration mode.

Step 4 {[*sequence-number*] | **default** | **permit** | **deny** | **remark**}

Example:

```
Device(config-rb-acl)# 10 permit tcp dst allowed in extended named access list eq 80 dst
eq 20
```

Specifies the access control entries (ACEs) for the RBACL.

You can use most of the commands and options allowed in extended named access list configuration mode, with the source and destination fields omitted.

The following ACE keywords are not supported:

- reflect
- evaluate
- time-range

Step 5 **exit**

Example:

```
Device(config-rb-acl)# exit
```

Creates an RBACL and enters Role-based ACL configuration mode.

Step 6 **ip access-list role-based** *rbacl-name*

Example:

```
Device(config)# ip access-list role-based allow_webtraff
```

Exits role-based ACL configuration mode and returns to global configuration mode.

Step 7 **cts role-based permissions** {**default** | [**from** { *sgt_num* | **unknown**} **to** {*dgt_num* | **unknown**}] {*rbacls* **ipv4** *rbacls*}

Example:

```
Device(config)# cts role-based permissions from 55 to 66 allow_webtraff
```

Binds SGTs and DGTs to the RBACL. The configuration is analogous to populating the permissionmatrix configured on Cisco ISE or Cisco Secure ACS.

- **default**: Default permissions list.
- *sgt_num*: 0 to 65,519. Source Group Tag.
- *dgt_num*: 0 to 65,519. Destination Group Tag.
- **unknown**: SGACL applies to packets where the security group (source or destination) cannot be determined.
- **ipv4**: Indicates the RBACLs are IPv4.
- *rbacls*: Names of RBACLs.

Step 8 **end**

Example:

```
Device(config)# end
```

Exits global configuration mode and returns to privileged EXEC mode.

Configure IPv6 SGACL Policies

To manually configure IPv6 SGACL policies, perform this task:

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **ipv6 access-list role-based** *sgacl-name*

Example:

```
Device(config)# ipv6 access-list role-based sgaclname
```

Creates a named IPv6 SGACL and enters IPv6 role-based ACL configuration mode.

Step 4 {**permit** | **deny**} *protocol* [**dest-option** | **dest-option-type** {*doh-number* | *doh-type*}] [**dscp** *cp-value*] [**flow-label** *fl-value*] [**mobility** | **mobility-type** {*mh-number* | *mh-type*}] [**routing** | **routing-type** *routing-number*] [**fragments**] [**log** | **log-input**] [**sequence** *seqno*]

Example:

```
Device(config-ipv6rb-acl)# permit 33 dest-option dscp af11
```

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.

The following ACE keywords are not supported:

- **reflect**
- **evaluate**
- **time-range**

Step 5 **end**

Example:

```
Device(config-ipv6rb-acl)# end
```

Exits IPv6 role-based ACL configuration mode and returns to privileged EXEC mode.

Apply SGACL policies manually

To manually apply SGACL policies, perform this task:

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts role-based permissions default** [**ipv4** | **ipv6**] [*sgacl-name1* [*sgacl-name2* [*sgacl-name3* ...]]]

Example:

```
Device(config)# cts role-based permissions default MYDEFAULTSGACL
```

Specifies the default SGACL. The default policies are applied when no explicit policy exists between the source and destination security groups.

Step 4 **cts role-based permissions from** {*source-sgt* | **unknown**} to {*dest-sgt* | **unknown**} [**ipv4** | **ipv6**] *sgacl-name1* [*sgacl-name2* [*sgacl-name3* ...]]]

Example:

```
Device(config)# cts role-based permissions from 3 to 5 SRB3 SRB5
```

Specifies the SGACLs to be applied for an SGT anda DGT.

- *source-sgt*: The range is from 1 to 65533.
- *dest-sgt* : The range is from 1 to 65533.
- **from**: Specifies the source SGT.
- **to**: Specifies the destination security group.
- **unknown**: SGACL applies to packets where the security group (source or destination) cannot be determined.

Note

- By default, SGACLs are considered to be IPv4.
- An SGACL policy downloaded dynamically from the ACS will override conflicting manual policies, if any.

Step 5 **end**

Example:

```
Device(config)# end
```

Exits global configuration mode and returns to privileged EXEC mode.

Refresh the SGACL Policies

To refresh the SGACL policies, perform this task.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password, if prompted.

Step 2	**cts refresh policy** {**peer** [*peer-id*] | **sgt** [*sgt_number* | **default** | **unknown**]}
	Example:
	`Device# cts refresh policy peer my_cisco_ise`
		Performs an immediate refresh of the SGACL policies from the authentication server.
		• If a *peer-id* is specified, only the policies related to the specified peer connection are refreshed.
		To refresh all the peer policies, press Enter without specifying an ID.
		• If an SGT number is specified, only the policies related to that SGT are refreshed.
		• To refresh all the SGT policies, press Enter without specifying an SGT number.
		• Select **default** to refresh the default policy.
		• Select **unknown** to refresh an unknown policy.

Step 3	**exit** **Example:** `Device# exit`	Exits privileged EXEC mode

Monitoring and Viewing SGACL Policies

Command	Description
show cts interface	Displays Cisco TrustSec states and statistics per interface.
show cts role-based counters [ipv4 | ipv6]	Displays all the SGACL enforcement statistics for IPv4 and IPv6 events.
show cts role-based permissions	Displays permission to RBACL configurations.

Command	Description
show cts role-based permissions from {*source-sgt* | unknown} to {*dest-sgt* | unknown}] [ipv4 | ipv6 | details]	Displays the SGACL policies and details about the monitor mode functionality foreach pair. The command output displays if per-cell monitor mode is enabled for the *SGT-DGT* pair. • By using or omitting 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.
show ip access-lists {*rbacls* | ipv4 *rbacls*}	Displays ACEs of all RBACLs or a specified RBACL.
show cts role-based permissions default [ipv4 | ipv6 | details]	Displays the list of SGACL, of the default policy.

Configuration Examples for Security Group ACL Policies

The following sections provide examples of various SGACL policy configurations.

Example: Enable SGACL Policy Enforcement Globally

The following example shows how to enable SGACL policy enforcement globally:

```
Device> enable
Device# configure terminal
Device(config)# cts role-based enforcement
```

Example: Enable SGACL Policy Enforcement Per Interface

The following example shows how to enable SGACL policy enforcement per interface:

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

Example: Enable SGACL Policy Enforcement on VLANs

The following example shows how to enable SGACL policy enforcement on VLANs:

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

Example: Configure SGACL Monitor Mode

The following example shows how to configure SGACL monitor mode:

```
Device# configure terminal
Device(config)# cts role-based monitor enable
Device(config)# cts role-based permissions from 2 to 3 ipv4
Device# show cts role-based permissions from 2 to 3 ipv4

IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00

Device# show cts role-based permissions from 2 to 3 ipv4 details

IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00
Details:
Role-based IP access list denytcpudpicmp-10 (downloaded)
        10 deny tcp
        20 deny udp
        30 deny icmp
Role-based IP access list Permit IP-00 (downloaded)
        10 permit ip

Device# show cts role-based counters ipv4

Role-based IPv4 counters
From     To     SW-Denied  HW-Denied  SW-Permitt  HW_Permitt  SW-Monitor  HW-Monitor
*         *     0          0          8           18962       0           0
2         3     0          0          0           0           0           341057
```

Example: Configure SGACL Policies Manually

```
Device# configure terminal
Device(config)# ip access role allow_webtraff
Device(config-rb-acl)# 10 permit tcp dst eq 80
Device(config-rb-acl)# 20 permit tcp dst eq 443
Device(config-rb-acl)# 30 permit icmp
Device(config-rb-acl)# 40 deny ip
Device(config-rb-acl)# exit
Device(config)# cts role-based permissions from 55 to 66 allow_webtraff
Device# 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
Device# show show cts role-based permissions from 50 to 70
```

Example: Apply SGACLs Manually

The following example shows how to manually apply SGACL policies:

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

Example: View SGACL Policies

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

```
Device# 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
```

CHAPTER 3

SGT Exchange Protocol

Feature History for SXP

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 17.18.1	SGT Exchange Protocol: The SGT Exchange Protocol (SXP) enables the propagation of Security Group Tags across network devices that do not natively support Cisco Group-Based Policy (GBP) hardware tagging.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

SGT Exchange Protocol

The Security Group Tag (SGT) Exchange Protocol (SXP) enables the propagation of SGTs across network devices that do not natively support Cisco Group-Based Policy (GBP) hardware tagging. This protocol allows organizations to extend Security Group Tagging functionality throughout the network, even on devices without direct hardware support.

Cisco Group-Based Policy

Cisco Group-Based Policy creates secure network domains made up of trusted devices, where each device is authenticated by its peers. Communication within these domains is safeguarded using encryption, message integrity checks, and data-path replay protection mechanisms.

How SGTs Are Used in the Network

When a device or user is authenticated, SXP (Security Group Tag Exchange Protocol) uses the acquired credentials to classify packets into security groups (SGs) as they enter the network. Packets are tagged at the ingress to ensure they can be identified for policy enforcement, such as access control, as they traverse the data path. The SGT enables endpoint devices and network infrastructure to filter and control traffic based on assigned tags. Additionally, static port identification can be used to determine the SGT value for endpoints connected to specific ports.

SGT Assignment Mechanisms

SGTs can be assigned to packets at the port level under various scenarios:

- Packets with SGT on Trusted Ports

  If a packet arrives on a trusted port with an SGT tag, the tag is accepted as the source SGT.

- Packets with SGT on Untrusted Ports

  If a tagged packet comes through an untrusted port, the packet is ignored and the source SGT is set according to the port’s configuration.

- Packets without SGT

  If a packet does not have an SGT, the source SGT is set as configured on the port.

SGT Assignment Methods

Security Group Tags can be assigned through various Endpoint Admission Control (EAC) methods, such as:

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

- Web Authentication

Supported SGT Assignment Methods

The following methods are supported for assigning SGTs in the network:

- Endpoint Admission Control (EAC)

  Includes 802.1X, MAB, and Web Authentication.
- VLAN-to-SGT Mapping

  Assigns a static SGT to IP addresses learned within a VLAN through IP device tracking; this is a lower priority classification method.
- SXP Listener

  Receives SGT information from other devices using the SGT Exchange Protocol.
- IP SGT

  Assigns SGTs based on IP addresses.
- Subnet SGT

  Assigns SGTs based on IP subnets.
- Port SGT

  Assigns SGTs at the port level.
- Caching SGT

  Stores and reuses previously assigned SGTs for efficiency.

Endpoint Authentication and SGT Association

During endpoint authentication, the access device associates the endpoint’s IP address with an SGT using methods like DHCP snooping and IP device tracking. This binding is then communicated via SXP to hardware-capable egress devices, which maintain a table of source IP-to-SGT bindings. At the egress interface, these devices enforce security policies using Security Group Access Control Lists (SGACLs).

Role of SXP in Security Group Tag Propagation

SXP functions as a control protocol, propagating IP-to-SGT binding information from authentication points to upstream network devices. This process ensures that security services on switches, routers, and firewalls can learn and utilize identity information from access devices. SXP is especially valuable in network segments that lack packet tagging capabilities.

SXP Protocol Details

SXP uses TCP as its transport protocol, specifically TCP port 64999 for connection initiation. For authentication and integrity, SXP employs:

- Message Digest 5 (MD5)
- TCP Authentication Option (TCP-AO)

The protocol defines two operational roles:

- Speaker: Initiates the connection
- Listener: Receives the connection

SXP Version 5

SXP Version 5 enhances the scalability and flexibility of SGT propagation in environments using Virtual Routing and Forwarding (VRF). In previous versions, expanding the number of VRFs required a proportional increase in SXP connections and IP-SGT mappings. SXP Version 5 addresses this limitation by allowing the export and import of SXP mappings between designated SXP peers across multiple VRFs using a single connection.

SXP Version 5 Mappings

The following are the SXP Version 5 mappings:

- Exporting Mappings:

  On the SXP speaker side, SXP Version 5 can export specific IP-SGT bindings based on the binding source type or associated VRF.

- Importing Mappings:

  On the SXP listener side, SXP Version 5 imports the relevant mappings into the specified VRF.

SXP Operation Mode

You can specify which VRF-associated IP-SGT bindings to export to remote peer devices according to your configuration. When an SXP connection is established between two devices that both support SXP Version 5, the connection operates in Version 5 mode. If either device supports only an earlier version, the connection defaults to the lowest common supported version.

To control which VRFs or list of VRF tables export IP-SGT bindings to peer devices, use the **cts sxp** global configuration command.

Guidelines to configure SXP

- The Cisco SGT Exchange Protocol (SXP) network needs to be established before implementing SXP. This network has the following prerequisites:
  - To use the Cisco Group-Based Policy functionality on your existing device, ensure that you have purchased a Cisco Group-Based Policy security license. If the device is being ordered and needs the Cisco Group-Based Policy functionality, ensure that this license is pre-installed on your device before it is shipped to you.
  - Group-Based Policy functionality, ensure that this license is pre-installed on your device before it is shipped to you
  - Cisco Group-Based Policy SXP software must run on all network devices.
  - Connectivity should exist between all network devices.
- Cisco Group-Based Policy Exchange Protocol is not supported on logical interfaces; supported only on physical interfaces.
- When the Dynamic Host Control Protocol (DHCP) snooping is enabled, Cisco Group-Based Policy enforcement for DHCP packets are passed by enforcement polices.
- Modifying a peer list under an SXP group is not supported when the peer connection configuration is present.
- Modifying an export list or import list under the speaker or listener export-import group is not allowed when an SXP connection configuration is present for any of the peers in the group. To modify the configuration under the export-import group, the corresponding peer SXP connection configuration must be removed. You can also shut down SXP by using the **no cts sxp enable** command.
- One peer cannot be configured under multiple export-import groups in the same direction, that is, a peer can be a part of the speaker export-import group as well as the listener export-import group but cannot be a part of a second speaker or listener group at the same time.
- Global export-import group configuration and per peer export-import group configuration are mutually exclusive.

How to Configure SXP

These sections provide configuration information on how to configure SXP.

Configure a Device SGT Manually

In a normal Cisco Group-Based Policy 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:

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts sgt** *tag*

Example:

```
Device(config)# cts sgt tag
```

Configures the SGT for packets sent from the device.

tag: The tag argument is in decimal format. The range is from 1 to 65533.

Step 4 **exit**

Example:

```
Device(config)# exit
```

Exits configuration mode.

Configure 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, or you can also set both speaker and listener in both the devices. 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 Group-Based Policy 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 device.

Toconfigure an SXP peer connection, perform this task:

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts sxp connection peer** *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** {**default** | **none**} **mode** {**local** | **peer**} {**speaker** | **listener**} {**vrf** *vrf-name*}

Example:

```
Device(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

Configuresthe SXP address connection.

The optional **source** keyword specifies the IPv4 address of the source device. If no address is specified, the connection will use the default source address, if configured, or the address of the port.

The **password** keyword specifies the password that SXP will use for the connection using the following options:

- **default**: Use the default SXP password you configured using the **cts sxp default password** command.
- **none**: Do not use a password.

The **mode** keyword specifies the role of the remote peer device:

- **local**: The specified mode refers to the local device.
- **peer**: The specified mode refers to the peer device.
- **speaker**: Default. Specifies that the deviceis the speaker in the connection.
- **listener**: Specifies that the device is the listener in the connection.

The optional **vrf** keyword specifies the VRF to the peer. The default is the default VRF.

Step 4 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode and returns to privileged EXEC mode

Step 5 **show cts sxp connections**

Example:

```
Device# show cts sxp connections
```

(Optional) Displays the SXP connection information.

Configure the Default SXP Password

By default, SXP uses no password when setting up connections.

To configure a default SXP password, perform this task:

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts sxp default password** [**0** | **6** | **7**] *passeword*

Example:

```
Device(config)# cts sxp default password 0 hello
```

Configures the SXP default password.

You can enter

- a clear text password (using the **0** or no option)
- an encrypted password (using the **6** or **7** option).

The maximum password length is 32 characters.

Step 4 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode and returns to privileged EXEC mode

Configure 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:

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts sxp default source-ip** *src-ip-addr*

Example:

```
Device(config)# cts sxp default source-ip 10.0.1.2
```

Configures the SXP default source IP address.

Step 4 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode and returns to privileged EXEC mode.

Change 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 Group-Based Policy software retains the SGT mapping entries learned from the previous connection and removes invalid entries.

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:

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts sxp reconciliation period** *seconds*

Example:

```
Device(config)# cts sxp reconciliation period 360
```

Changes the SXP reconciliation timer.

seconds: The range is from 0 to 64000. The default value is 120 seconds (2 minutes).

Step 4 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode and returns to privileged EXEC mode.

Change the SXP Retry Period

The SXP retry period determines how often the Cisco Group-Based Policy software retries an SXP connection. When an SXP connection is not successfully set up, the Cisco Group-Based Policy software makes a new attempt to set up the connection after the SXP retry period timer expires. 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:

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts sxp retry period** *vlan-list*

Example:

```
Device(config)# cts sxp retry period 360
```

Changes the SXP retry timer.

seconds: The range is from 0 to 64000. The default value is 120 seconds (2 minutes).

Step 4 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode and returns to privileged EXEC mode.

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

When the **cts sxp log binding-changes** command is configured in global configuration mode, SXP syslogs (sev 5 syslog) are generated whenever a change to IP address to SGT binding occurs (add, delete, change).

These changes are learned and propagated on the SXP connection. The default is **no cts sxp log binding-changes**.

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

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts sxp log binding-changes**

Example:

```
Device(config)# cts sxp log binding-changes
```

Enables logging for IP to SGT binding changes.

Step 4 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode and returns to privileged EXEC mode.

Configure an SXP Export List

To configure an SXP export list, perform this task.

Note Export-list configurations cannot be removed if they are associated with an SXP group. To remove it, you must first disable the SXP connection.

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts sxp export-list** *export_list_name*

Example:

```
Device(config)# cts sxp export-list export_list_1
```

Configures an SXP export list, and enters export-list configuration mode.

Step 4 **binding-source-type** {**all** | **caching** | **cli** | **l3if** | **lisp-local-host** | **lisp-remote-host** | **local** | **omp** | **vlan**}

Example:

```
Device(config-export-list)# binding-source-type all
```

(Optional) Configures the bindings of the corresponding source type that are to be exported to the peer.

- **all**: Exports all bindings.
- **caching**: Exports cached bindings to a peer
- **cli**: Exports CLI bindings to a peer.
- **l3if**: Exports L3IF bindings to a peer.
- **lisp-local-host**: Exports LISP local bindings to a peer.
- **lisp-remote-host**: Exports LISP remote bindings to a peer.
- **local**: Exports local bindings to a peer.
- **omp**: Exports OMP bindings to a peer.
- **vlan**: Exports VLAN bindings to a peer.

Step 5 **vrf** {*instance_name* | **Default-vrf** | **all**}

Example:

```
Device(config-export-list)# vrf all
```

(Optional) Configures the VRF used to import the bindings.

- *instance_name*: Specifies a VPN routing and forwarding instance name.
- **Default-vrf**: Exports default VRF bindings.
- **all**: Exports all IP-SGT bindings.

Note
vrf and **vrf** *instance_name* configuration are mutually exclusive.

Step 6 **end**

Example:

```
Device(config-export-list)# end
```

Exits export list configuration mode, and returns to privileged EXEC mode.

Configure an SXP Import List

To configure an SXP import list, perform this task:

Note Import-list configurations cannot be removed if they are associated with an SXP group. To remove an import-list configuration, you must first disable the corresponding SXP connection.

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts sxp import-list** *import_list_name*

Example:

```
Device(config)# cts sxp import-list import_list_1
```

Configures an SXP import list, and enters import list configuration mode.

Step 4 **vlan-list**

Example:

```
Device(config-import-list)# vlan-list
```

(Optional) Configures import VRF based on the VLAN in the received binding update.

Note
If there is no VRF mapping in the device for a VLAN received in the update, the bindings that are received are added to the default VRF table.

Step 5 **vrf** {*instance_name* | **Default-vrf**}}

Example:

```
Device(config-import-list)# vrf vrf_1
```

(Optional) Configures the VRF used to import the bindings.

- *instance_name*: Specifies a VPN routing and forwarding instance name.
- **Default-vrf**: Configures the default VPN routing and forwarding instance.

Note
vrf *instance_name* and **vlan-list** configuration are mutually exclusive.

Step 6 **end**

Example:

```
Device(config-import-list)# end
```

Exits export list configuration mode, and returns to privileged EXEC mode

Configure an SXP Export-Import Group

The export-import groups are defined as either speaker or listener groups that control the export or import of SXP bindings for a group.

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts sxp export-import-group** {**listener** | **speaker**} {**global** | *list_name*}

Example:

```
Device(config)# cts sxp export-import-group listener group_1
```

Configures an SXP export-import group, and enters export-import-group configuration mode.

- **global**: Configures either an SXP listener global import group or an SXP speaker global export group. Global speaker or listener export-import group is applied to all the SXP connections configured in the device.
- *list_name*: Specifies the default VPN routing and forwarding instance name.

Step 4 **import-list** *list_name*

Example:

```
Device(config-export-import-group)# import-list import_1
```

(Optional) Specifies the import list name to be applied to the export-import group.

An empty import list or export list cannot be attachedto a listener or speaker export-import group respectively.

Step 5 **export-list** *list_name*

Example:

```
Device(config-export-import-group)# export-list export_1
```

Optional) Specifies the export list name to be applied to the export-import group.

An empty import list or export list cannot be attachedto a listener or speaker export-import group respectively.

Step 6 **peer** *address_name*

Example:

```
Device(config-export-import-group)# peer 1.1.1.1 2.2.2.2
```

(Optional) Configures a list of peers to be applied to the export-import group. A maximum of eight peers can be configured.

Step 7 **end**

Example:

```
Device(config-export-import-group)# end
```

Exits export-import-group configuration mode, and returns to privileged EXEC mode.

Verify SGT Exchange Protocol Connections

Table 1:

Command	Description
show cts sxp connections	Displays detailed information about the SXP status and connections.
show cts sxp connections [brief]	Displays brief information about the SXP status and connections.
show cts sxp export-list	Displays the list of VRFs associated with a specific export list or all the export lists.
show cts sxp import-list	Displays the list of VRFs associated with a specific import list name or all the import lists.
show cts sxp export-import-group [detailed]	Displays the export list or import list applied with a specific export-import group along with the list of peers that are a part of this export-import group.

Configuration Examples for SXP

These sections provide configuration examples for SXP.

Example: Enable Cisco Group-Based Policy SXP and an SXP Peer Connection

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

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

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

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

Example: Configure the Default SXP Password and Source IP Address

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

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

Example: Verify SGT Exchange Protocol Connections

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

```
Device# show cts sxp connections

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

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

```
Device# show cts sxp connections brief

SXP                      : Enabled
Default Password         : Set
Default Source IP        : Not Set
Connection retry open period: 120 secs
Reconcile period         : 120 secs
Retry open timer is not running
-----------------------------------------------------------------------------
Peer_IP          Source_IP          Conn Status    Duration
```

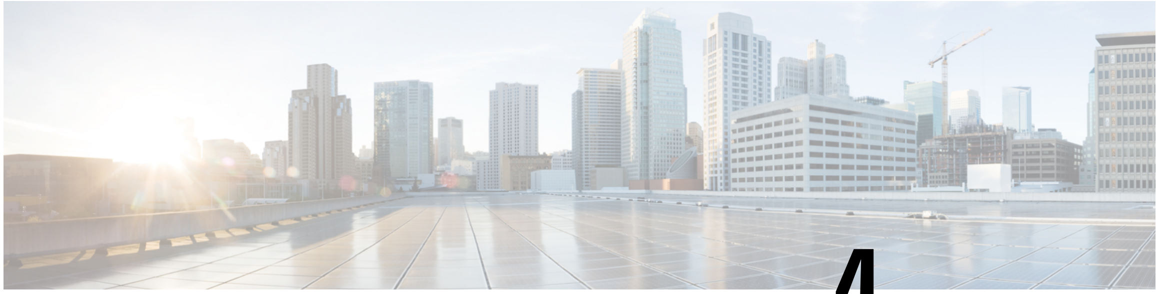
```
------------------------------------------------------------------------------
10.1.3.1          10.1.3.2           On            6:00:09:13 (dd:hr:mm:sec)
Total num of SXP Connections = 1
```

The following is a sample output of the **show cts sxp export-list** command displaying the list of VRFs associated with a specific export list or all the export lists configured on the device:

```
Device# show cts sxp export-list export_list_1

   Export-list-name: export_list_1
   vrf red_vrf
   vrf blue_vrf

Device# show cts sxp export-list

   Export-list-name: export_list_1
       vrf red_vrf
       vrf blue_vrf
       vrf green_vrf
   Export-list-name: export_list_2
       vrf all
```

The following is a sample output of the **show cts sxp export-import-group** command displaying the export list or import list applied to a specific export-import group along with the list of peers that are a part of this export-import group. The **show cts sxp export-import-group** command also lists the details of all the export-import groups configured on the device. Use the **detailed** keyword to display the export list or import list contents along with the export list or import list name and the list of peers. The **global** keyword displays the details of only the global listener and speaker.

```
Device# show cts sxp export-import-group speaker group_1

   Export-import-group: group_1
   Export-list-name: export_list_1
   Peer-list: 1.1.1.1, 2.2.2.2, 3.3.3.3

Device# show cts sxp export-import-group listener

Global Listener export-import-group: Not configured

   Export-import-group: group_1
   Export-list-name:  export_list_1
   Peer-list: 1.1.1.1, 2.2.2.2, 3.3.3.3

   Export-import-group: group_2
   Import-list-name: import_list_1
   Peer-list: 4.4.4.4, 5.5.5.5, 6.6.6.6


Device# show cts sxp export-import-group speaker group_1 detailed

    Export-import-group: group_1
    Export-list-name: export_list_1
    Export-list-content:
       vrf Red_vrf
       vrf Blue_vrf
    Peer-list: 1.1.1.1, 2.2.2.2, 3.3.3.3

Device# show cts sxp export-import-group listener detailed

    Global Listener export-import-group: Not configured

    Export-import-group: group_1
    Import-list-name: import_list_1
    Import-list-content:
       vlan-list
    Peer-list: 1.1.1.1, 2.2.2.2, 3.3.3.3

Device# show cts sxp export-import-group global

   Global Listener export-import-list Name: group_1
   Global Speaker export-import-list Name: group_2
```



CHAPTER 4

IPv6 Support for SGT and SGACL

Feature History for IPv6 support SGT and SGACL

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 17.18.1	IPv6 support SGT and SGACL: The IPv6 Support for Security Group Tags (SGT) and Security Group Access Control Lists (SGACL) enables seamless mapping between IPv6 addresses and SGTs.	Cisco C9610 Series Smart Switches

IPv6 Support for SGT and SGACL

The IPv6 Support for Security Group Tags (SGT) and Security Group Access Control Lists (SGACL) feature enables seamless mapping between IPv6 addresses and SGTs. These mapped SGTs play a crucial role in enforcing security policies via SGACLs.

IPv6 Dynamic Learning Components

Dynamic learning of IPv6 addresses relies on three core components:

- Switch Integrated Security Features (SISF):

  An infrastructure responsible for security, address assignment, resolution, neighbor discovery, and exit point discovery.

- Cisco Enterprise Policy Manager (EPM):

  Registers with SISF to receive IPv6 address notifications. EPM then uses IPv6 addresses and SGTs obtained from Cisco Identity Services Engine (ISE) to create IP-SGT bindings.

- Cisco TrustSec:

  Protects devices from unauthorized access by assigning SGTs to incoming traffic and enforcing access policies based on these tags across the network.

IPv6 address-to-SGT mapping priorities

IPv6 address-to-SGT mapping can be achieved through several methods, prioritized as follows (from lowest to highest):

1. VLAN:

   IPv6 addresses learned through SISF on VLANs with SGT-VLAN mappings, using ICMPv6 Neighbor Discovery.

2. CLI:

   Manual address bindings set using the **cts role-based sgt-map** global configuration command (IP-SGT format).

3. Layer 3 Interface:

   Bindings created from FIB forwarding entries traversing interfaces with consistent Layer 3 interface-SGT or identity port mapping (IPM).

4. SXP:

   Bindings received from SGT Exchange Protocol (SXP) peers.

5. Local:

   Bindings for authenticated hosts, identified through EPM and device tracking (SISF).

6. Internal:

   Bindings between locally configured IP addresses and the device's SGT.

How to Configure IPv6 Support for SGT and SGACL

This section describes how to configure IPv6 support for SGT and SGACL.

Learn IPv6 Addresses for IP-SGT Bindings

SISF is a feature that learns IPv6 addresses for use in IP-SGT bindings.

To learn IPv6 addresses for IP-SGT bindings, configure this task.

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts role-based sgt-map** *host-address/prefix* **sgt** *sgt-value*

Example:

```
Device(config)# cts role-based sgt-map 2001::db8::1/64 sgt 120
```

Manually maps a source IPv6 address to an SGT on either a host or a virtual routing and forwarding (VRF) instance.

Step 4 **device-tracking policy** *policy-name*

Example:

```
Device(config)# device-tracking policy policy1
```

Enables device tracking and enters device tracking configuration mode.

Step 5 **tracking enable**

Example:

```
Device(config-device-tracking)# tracking enable
```

Overrides the default tracking policy on a port.

Step 6 **end**

Example:

```
Device(config-device-tracking)# end
```

Exits device tracking configuration mode and returns to privileged EXEC mode.

Configure IPv6 IP-SGT Binding Using Local Binding

To configure IPv6 IP-SGT Binding Using Local Binding, perform this task.

Before you begin

- In local binding, SGT values are downloaded from Cisco Identity Service Engine (ISE). For more information, see the *Configuring Cisco Security Group Access Policies* document.
- SISF must be enabled and populated before IPv6 address can be generated.

Note This task uses Cisco Identity Based Networking Services (IBNS) Version 2.0.

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **policy-map type control subscriber** *control-policy-name*

Example:

```
Device(config)# policy-map type control subscriber policy1
```

Defines a control policy for subscriber sessions and enters control policy-map configuration mode.

Step 4 **event session-started match-all**

Example:

```
Device(config-event-control-policymap)# event session-started match-all
```

Specifies the type of event that triggers actions in a control policy if conditions are met.

Step 5 *priority-number* **class always do-until-failure**

Example:

```
Device(config-class-control-policymap)# 10 class always do-until-failure
```

Associates a control class with one or more actions in a control policy and enters action control policy-map configuration mode.

A named control class must first be configuredbefore specifying it with the *control-class-name* argument.

Step 6 *action-number* **authenticate using mab**

Example:

```
Device(config-action-control-policymap)# 10 authenticate using mab
```

Initiates the authentication of a subscriber session using the specified method.

Step 7 **exit**

Example:

```
Device(config-action-control-policymap)# exit
```

Exits action control policy-map configuration mode and returns to global configuration mode.

Step 8 **interface gigabitethernet** *interface-number*

Example:

```
Device(config)# interface gigabitethernet 1/0/1
```

Configures an interface and enters interface configuration mode.

Step 9 **description** *interface-description*

Example:

```
Device(config-if)# description downlink to ipv6 clients
```

Describes the configured interface.

Step 10 **switchport access vlan** *vlan-id*

Example:

```
Device(config-if)# switchport access vlan 20
```

Sets access mode characteristics of the interfaceand configures VLAN when the interface is in access mode.

Step 11 **switchport mode access**

Example:

```
Device(config-if)# switchport mode access
```

Sets the trunking mode to access mode.

Step 12 **device-tracking attach-policy** *policy-name*

Example:

```
Device(config-if)# device-tracking attach-policy snoop
```

Applies a policy to the IPv6 Snooping feature.

Step 13 **access-session port-control auto**

Example:

```
Device(config-if)# access-session port-control auto
```

Sets the authorization state of a port.

Step 14 **mab eap**

Example:

```
Device(config-if)# mab eap
```

Uses Extensible Authentication Protocol (EAP) for MAC authentication bypass.

Step 15 **dot1x pae authenticator**

Example:

```
Device(config-if)# dot1x pae authenticator
```

Enables dot1x authentication on the port.

Step 16 **service-policy type control subscriber** *policy-name*

Example:

```
Device(config-if)# service-policy type control subscriber policy
```

Specifies the policy map that is used for sessionsthat come up on this interface. The policy map has rules for authentication and authorization.

Step 17 **end**

Example:

```
Device(config-if)# end
```

Exits interface configuration mode and returns to privileged EXEC mode.

Step 18 **show cts role-based sgt-map all ipv6**

Example:

```
Device# show cts role-based sgt-map all ipv6
```

Displays active IPv6 IP-SGT bindings.

Configure IPv6 IP-SGT Binding Using a VLAN

In a VLAN, a network administrator assigns SGT values to a particular VLAN.

To configure IPv6 IP-SGT BindinguUsing a VLAN, perform this task.

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts role-based sgt-map vlan-list** *vlan-id* **sgt** *sgt-value*

Example:

```
Device(config)# cts role-based sgt-map vlan-list 20 sgt 3
```

Assigns an SGT value to the configured VLAN.

sgt-value: The range must be from 2 to 65519.

Step 4 **end**

Example:

```
Device(config)# end
```

Exits global configuration mode and returns to privileged EXEC mode.

Verify IPv6 Support for SGT and SGACL

Command	Description
show cts role-based sgt-map all	Displays active IPv4 and IPv6 IP-SGT bindings.
show cts role-based sgt-map all ipv6	Displays active IPv6 IP-SGT bindings.

Configuration Examples for IPv6 Support for SGT and SGACL

The following sections show how to configure IPv6 Support for SGT and SGACL.

Example: Learn IPv6 Addresses for IP-SGT Bindings

The following example shows how to learn IPv6 addresses for IP-SGT bindings:

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map 2001::db8::1/64 sgt 120
Device(config)# device-tracking policy policy1
Device(config-device-tracking)# tracking enable
Device(config-device-tracking)# end
```

Example: Configure IPv6 IP-SGT Binding Using Local Binding

The following example uses IBNS Version 2.0

```
Device> enable
Device# configure terminal
Device(config)# policy-map type control subscriber policy1
Device(config-event-control-policymap)# event session-started match-all
Device(config-class-control-policymap)# 10 class always do-until-failure
Device(config-action-control-policymap)# 10 authenticate using mab
Device(config-action-control-policymap)# exit
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# description downlink to ipv6 clients
Device(config-if)# switchport access vlan 20
Device(config-if)# switchport mode access
Device(config-if)# device-tracking attach-policy snoop
Device(config-if)# access-session port-control auto
Device(config-if)# mab eap
Device(config-if)# dot1x pae authenticator
Device(config-if)# service-policy type control subscriber policy
Device(config-if)# end
```

Example: Configure IPv6 IP-SGT Binding Using a VLAN

The following example shows how to configure IP-SGT binding using a VLAN:

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map vlan-list 20 sgt 3
Device(config)# end
```

CHAPTER 5

TrustSec Security Group Name Download

Feature History for TrustSec Security Group Name Download

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 17.18.1	TrustSec Security Group Name Download: The TrustSec Security Group Name Download feature improves the SGT policy by enabling network access devices to receive not only the SGT number and SGACL policy, but also the associated SGT name.	Cisco C9610 Series Smart Switches

TrustSec Security Group Name Download

The TrustSec Security Group Name Download feature improves the Security Group Tag (SGT) policy by enabling network access devices to receive not only the SGT number and Security Group Access Control List (SGACL) policy, but also the associated SGT name.

SGT Mapping to Layer 3 Logical interface

With this feature, SGTs can be directly mapped to traffic on any of the following Layer 3 interfaces, regardless of the underlying physical interface:

- Routed port
- Switch Virtual Interface (SVI or VLAN interface)
- Layer 3 subinterface of a Layer 2 port
- Tunnel interface

The **cts role-based sgt-map interface** global configuration command allows you to specify either a particular SGT number or a Security Group Name. The association between the Security Group Name and its SGT is dynamically obtained from a Cisco Identity Services Engine (ISE) or Cisco Access Control Server (ACS).

Configure TrustSec Security Group Name Download

To configure TrustSec security group name download, perform this task.

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts role-based sgt-map interface** *type slot/port* [**security-group** *name* | **sgt** *number*]

Example:

```
Device(config)# cts role-based sgt-map interface gigabitEthernet 1/1 sgt 77
```

An SGT is imposed on ingress traffic to the specified interface.

- **interface** *type slot/port*: Displays list of available interfaces.
- **security-group** *name*: Security Group name to SGT pairings are configured on the Cisco ISE or Cisco ACS.
- **sgt** *number*: Specfies the SGT number. The range is from 0 to 65,535.

Step 4 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode.

Step 5 **show cts role-based sgt-map all**

Example:

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

Verify that ingressing traffic is tagged with the specified SGT.

Example: Configure TrustSec Security Group Name Download

The following example shows the SGT download configuration for the ingress interface:

```
Device# config terminal
Device(config)# cts role-based sgt-map interface gigabitEthernet 6/3 sgt 3
Device (config)# exit
```

Example: Verify TrustSec Security Group Name Download Configuration

The following example shows a sample output of the **show cts role-based sgt-map all** command.

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

IP Address             SGT     Source

============================================

15.1.1.15              4       INTERNAL

17.1.1.0/24            3       L3IF

21.1.1.2               4       INTERNAL

31.1.1.0/24            3       L3IF

31.1.1.2               4       INTERNAL

43.1.1.0/24            3       L3IF

49.1.1.0/24            3       L3IF

50.1.1.0/24            3       L3IF

50.1.1.2               4       INTERNAL

51.1.1.1               4       INTERNAL
```

```
52.1.1.0/24             3       L3IF
81.1.1.1                5       CLI
102.1.1.1               4       INTERNAL
105.1.1.1               3       L3IF
111.1.1.1               4       INTERNAL
IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of L3IF     bindings = 7
Total number of INTERNAL bindings = 7
Total number of active   bindings = 15
```

CHAPTER 6

Layer 2 SGT Imposition and Forwarding

Feature History for Layer 2 SGT Imposition and Forwarding

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 17.18.1	Layer 2 SGT Imposition and Forwarding: Layer 2 SGT Imposition and Forwarding enables interfaces on a switch to be manually configured for Cisco TrustSec, allowing the switch to insert a SGT into network packets	Cisco C9610 Series Smart Switches

Layer 2 SGT Imposition and Forwarding

Layer 2 SGT Imposition and Forwarding features enables interfaces on a switch to be manually configured for Cisco TrustSec, allowing the switch to insert a SGT into network packets. The SGT is carried throughout the network in the Cisco TrustSec header, enabling consistent security group policy enforcement across the infrastructure.

Guidelines to configure Layer 2 SGT Imposition and Forwarding

The Cisco Trustsec network needs to be established with the following prerequisites before implementing the Layer 2 SGT Imposition and Forwarding feature:

- Connectivity exists between all network devices
- Cisco Secure Access Control System (ACS) 5.1 operates with a Cisco TrustSec -SXP license
- Directory, DHCP, DNS, certificate authority, and NTP servers function within the network
- Configure the retry open timer command to a different value on different routers.

How to Configure SGT Handling: L2 SGT Imposition and Forwarding

These sections provide configuration information for SGT Handling: L2 SGT Imposition and Forwarding.

Enable Layer 2 SGT Imposition and Forwarding Manually on an Interface

Perform this task to manually enable an interface on the device for Cisco TrustSec so that the device can add SGT in the packet to be propagated throughout the network and to implement a static authorization policy.

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **interface** {**GigabitEthernet** *port* | **Vlan** *number*}

Example:

```
Device(config)# interface gigabitethernet 0
```

Enters the interface on which CTS SGT authorization and forwarding is enabled.

Step 4 **cts manual**

Example:

```
Device(config-if)# cts manual
```

Enables the interface for CTS SGT authorization and forwarding, and enters CTS manual interface configuration mode.

Step 5 **policy static sgt** *tag* [**trusted**]

Example:

```
Device(config-if-cts-manual)# policy static sgt 100 trusted
```

Configures a static authorization policy for a CTS security group with a tagged packet that defines the trustworthiness of the SGT.

Step 6 **end**

Example:

```
Device(config-if-cts-manual)# end
```

Exits CTS manual interface configuration mode and enters privileged EXEC mode

Step 7 **show cts interface** [**GigabitEthernet** *port* | **Vlan** *number* | **brief** | **summary**]

Example:

```
Device# show cts interface brief
```

Displays CTS configuration statistics for the interface.

Disable CTS SGT Propagation on an Interface

Follow these steps to disable CTS SGT Propagation on an interface in an instance when a peer device is not capable of receiving an SGT.

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **interface** {**GigabitEthernet** *port* | **Vlan** *number*}

Example:

```
Device(config)# interface gigabitethernet 0
```

Enters the interface on which CTS SGT authorization and forwarding is enabled

Step 4 **cts manual**

Example:

```
Device(config-if)# cts manual
```

Enables the interface for CTS SGT authorization and forwarding.

CTS manual interface configuration mode is entered where CTS parameters can be configured.

Step 5 **no propagate sgt**

Example:

```
Device(config-if-cts-manual)# no propagate sgt
```

Disables CTS SGT propagation on an interface in situations where a peer device is not capable of receiving an SGT.

Note
CTS SGT propagation is enabled by default. The **propagate sgt** command can be used if CTS SGT propagation needs to be turned on again for a peer device.

Once the **no propagate sgt** command is entered, the SGT tag is not added in the L2 header.

Step 6 **end**

Example:

```
Device(config-if-cts-manual)# end
```

Exits CTS manual interface configuration mode and enters privileged EXEC mode.

Step 7 **show cts interface** [**GigabitEthernet** *port* | **Vlan** *number* | **brief** | **summary**]

Example:

```
Device# show cts interface brief
```

Displays CTS configuration statistics to verify that CTS SGT propagation was disabled on interface.

CHAPTER 7

SGT Inline Tagging

Feature History for SGT Inline Tagging

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 17.18.1	SGT Inline Tagging: SGT inline tagging enables Cisco TrustSec to propagate security group identity information directly within Ethernet frames, allowing network devices to enforce security policies efficiently based on the source's security group membership.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Layer 2 SGT Imposition

Cisco TrustSec-capable devices have hardware support to send and receive packets with SGT embedded at the MAC (Layer 2) level. This capability, known as Layer 2 (L2) SGT Imposition, enables Ethernet interfaces to insert the SGT directly into packets, which are then forwarded to neighboring Ethernet devices. The SGT-over-Ethernet method allows hop-by-hop, clear-text propagation of the SGT, providing scalable and efficient identity tagging without adding control plane overhead.

SGT Handling with SXPv4

The Cisco TrustSec solution, with SGT Exchange Protocol Version 4 (SXPv4), supports metadata-based L2-SGT. When a packet enters a TrustSec-enabled interface, the device references its IP-SGT mapping database—built dynamically via SXP or statically by configuration—to determine the correct SGT based on the source IP address. This SGT is then inserted into the packet and carried throughout the TrustSec domain.

SGT Handling with SGACL

At the network's egress edge, the group of the packet's destination is determined, and access control can be enforced. Security Group Access Control Lists (SGACLs) define whether to permit or restrict communication between different security groups. Each packet's policy enforcement is determined by its source and destination security group tags.

SGT Propagation and Use Cases

- Trusted Interface Propagation: SGTs received from trusted interfaces are propagated across the network and can be utilized for identity-based firewall classification.
- IPsec Integration: When IPsec is used, the SGT received in a packet can be shared with IPsec for proper SGT tagging.

Determining the SGT of a Packet

When a device at the ingress of the Cisco TrustSec domain receives a packet, it must determine the appropriate SGT to tag the packet. This can be done in two primary ways:

- SGT Field in TrustSec Header:

  If the packet arrives from a trusted peer device, the SGT field in the Cisco TrustSec header is assumed to be accurate.

- SGT Lookup by Source IP:

  Administrators can manually configure policies or leverage the SXP protocol to populate an IP-to-SGT mapping table for assigning SGTs based on source IP addresses.

SGT Inline Tagging on NAT-Enabled Devices

This section describes how SGT values are determined and enforced for packets traversing from a primary device, which has Network Address Translation (NAT) enabled on both ingress and egress ports, to a secondary device.

Note All ports involved in the flow must have Cisco TrustSec (CTS) manual and trusted mode configured on both devices

Inline Tagging Enabled, SGT Tag Not Changed via CLI

- On the primary device, Cisco TrustSec enforces the SGT tag corresponding to the packet's original source IP.
- After NAT translation, the NAT IP is associated with the same SGT tag.
- On the secondary device, Cisco TrustSec enforces the SGT tag based on the source IP (as represented by the SGT tag).

Example

A packet arrives at the primary device with source IP 192.0.2.5 and SGT tag 133.

- Cisco TrustSec enforces SGT tag 133 on the primary device.
- After NAT, the packet's IP changes to 198.51.100.10 but remains tagged with SGT 133.
- The secondary device receives the packet with IP 198.51.100.10 and SGT 133, and enforces TrustSec policy based on SGT 133.

Inline Tagging Enabled, SGT Tag Changed via CLI

- On the primary device, Cisco TrustSec enforces the SGT tag based on the packet's original source IP.
- The SGT tag may be changed via CLI, but the NAT IP is still tagged with the original source IP's SGT.
- On the secondary device, TrustSec continues to enforce policy according to the SGT tag corresponding to the packet's original source IP.

Example

A packet arrives at the primary device with source IP 192.0.2.5 and SGT tag 133.

- SGT tag is changed to 200 via CLI, but after NAT (IP changes to 198.51.100.10), the packet is still tagged with SGT 133.
- The secondary device receives the packet with IP 198.51.100.10 and SGT 133, and enforces TrustSec policy based on SGT 133.

Inline Tagging Disabled, SGT Learned via SXP Protocol and Changed via CLI

- On the primary device, TrustSec enforces the SGT tag based on the original source IP.
- The SGT for the post-NAT IP is defined through CLI and learned on the primary device.
- On the secondary device, if there is no direct TrustSec link, IP-to-SGT bindings are learned through the SXP protocol, and TrustSec is enforced based on the SGT associated with the NAT IP.

Example

A packet arrives at the primary device with source IP 192.0.2.5 and SGT tag 133.

- After NAT, the source IP becomes 198.51.100.10, and the SGT for this IP is set to 200 via CLI.
- TrustSec enforces SGT 133 on the primary device.

- On the secondary device, the IP-to-SGT binding (198.51.100.10—200) is learned via SXP, and TrustSec is enforced using SGT 200.

SGT Inline Tagging with IPv6 Multicast Traffic

Layer 2 inline tagging is also supported for IPv6 multicast traffic, provided the multicast packets originate from unicast IPv6 source addresses.

Guidelines for SGT Inline Tagging

This restriction is applicable to all switches:

Cisco TrustSec manual configurations and 802.1x configurations can coexist only if Security Association Protocol is not configured.

This restriction is applicable to Cisco C9610 Series Smart Switches.

- System generated packets for the egress interface are not sent with Cisco TrustSec tag on the Cisco TrustSec enabled interface.
- VLAN-based SGT assignment and VLAN-based enforcement is not supported.
- Q-in-QVLAN tagging is not supported with Cisco TrustSec header.
- In a multisite VXLAN fabric, handoff is not supported.
- Flexible NetFlow, Policy-based Routing (PBR), Quality of Service (QoS), etc SGT features are not supported.
- Broadcast, unknown unicast, and multicast (BUM) traffic will not be tagged with a SGT or Cisco TrustSec header.
- With the Dynamic Host Control Protocol (DHCP) Snooping enabled, DHCP packets ingress on Cisco TrustSec enabled ports will be discarded.
- Irrespective of the **cts manual** configuration on the egress interface, the device neither adds nor removes the Cisco MetaData header for Layer 2 traffic.

Configure SGT Inline Tagging

To configure SGT inline tagging, perform this task.

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **interface** {**gigabitethernet port** | **vlan** *number*}

Example:

```
Device(config)# interface gigabitethernet 1/0/1
```

Configures the interface on which Cisco TrustSec SGT authorization and forwarding is enabled, and enters interface configuration mode.

Step 4 **cts manual**

Example:

```
Device(config-if)# cts manual
```

Enables Cisco TrustSec SGT authorization and forwarding on the interface, and enters Cisco TrustSec manual interface configuration mode.

Step 5 **propagate sgt**

Example:

```
Device(config-if-cts-manual)# propagate sgt
```

Enables Cisco TrustSec SGT propagation on an interface.

Note
Use this command in situations where the peer device is capable of receiving SGT over Ethernet packets (that is, when a peer device support Cisco Ethertype CMD 0x8909 frame format).

Step 6 **policy static sgt** *tag* [**trusted**]

Example:

```
Device(config-if-cts-manual)# policy static sgt 77 trusted
```

Configures a static SGT ingress policy on the interface and defines the trustworthiness of an SGT received on the interface.

Note
The **trusted** keyword indicates that the interface is trustworthy for Cisco TrustSec. The SGT value received in the Ethernet packet on this interface is trusted and will be used by the device for any SG-aware policy enforcement or for the purpose of egress-tagging.

Step 7 **end**

Example:

```
Device(config-if-cts-manual)# end
```

Exits Cisco TrustSec manual interface configuration mode and enters privileged EXEC mode.

Example: Configure SGT Static Inline Tagging

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

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

CHAPTER 8

SGACL High Availability

Feature History for SGACL High Availability

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 17.18.1	SGACL High Availability: Cisco TrustSec Security Group Access Control Lists (SGACLs) support high availability on switches equipped with Cisco StackWise technology	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Cisco TrustSec SGACL High Availability

Cisco TrustSec Security Group Access Control Lists (SGACLs) support high availability on switches equipped with Cisco StackWise technology. StackWise provides stateful redundancy, allowing a switch stack to enforce and process access control entries (ACEs) even during failover events.

High Availability Operation in Switch Stacks

Within a switch stack, the stack manager designates the switch with the highest priority as the active switch, and the next highest as the standby. During a stateful switchover, whether automatic or CLI-initiated, the standby switch becomes active, while the next in line assumes the standby role.

Operational data is synchronized from the active to the standby switch during system bootup, when operational data changes (such as Change of Authorization [CoA]), or during an operational data refresh.

Deploying Devices in High Availability Setup

Perform the following steps when deploying devices in an high availability setup:

1. Remove any existing credentials from all devices that will be part of the high availability setup.
2. Power up the stack and assign device roles (active, standby, and member switches).
3. On the active device, set up the credentials using the **cts credentials id** *id* **password** *password* command.

Data Synchronization and Switchover Process

When a stateful switchover occurs, the new active switch requests and downloads the necessary operational data. Environment data (ENV-data) and Role-Based Access Control Lists (RBACLs) are updated only after the refresh period completes.

The following are the different types of operational data that are downloaded to the active switch.

Operational Data	Description
Environment Data (ENV-data)	Contains a preferred server list for retrieving RBACL information during refresh or initialization.
Protected Access Credential (PAC)	A unique shared secret between the switch and the authenticator, used to secure Extensible Authentication Protocol Flexible Authentication via Secure Tunneling (EAP-FAST).
Role-Based Policy (RBACL or SGACL)	A variable-length list defining policies for all Security Group Tag (SGT) mappings on the switch.

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

Verify Cisco TrustSec SGACL High Availability

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

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

```
Device# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
        default_sgacl-01
        Deny IP-00
```

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

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

```
Device-stby# show cts role-based permissions

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

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

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

```
Device# show cts pacs

AID: A3B6D4D8353F102346786CF220FF151C
PAC-Info:
    PAC-type = Cisco Trustsec
    AID: A3B6D4D8353F102346786CF220FF151C
    I-ID: CTS_ED_21
    A-ID-Info: Identity Services Engine
    Credential Lifetime: 17:22:32 IST Mon Mar 14 2016
PAC-Opaque:
000200B80003000100040010A3B6D4D8353F102346786CF220FF151C0006009C00030100E044B2650D8351FD06
F23623C470511E0000001356DEA96C00093A80538898D40F633C368B053200D4C9D2422A7FEB4837EA9DBB89D1
E51DA4E7B184E66D3D5F2839C11E5FB386936BB85250C61CA0116FDD9A184C6E96593EEAF5C39BE08140AFBB19
4EE701A0056600CFF5B12C02DD7ECEAA3CCC8170263669C483BD208052A46C31E39199830F794676842ADEECBB
A30FC4A5A0DEDA93
Refresh timer is set for 01:00:05
```

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

```
Device# show cts environment-data

CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0:Unknown
Server List Info:
Installed list: CTSServerList1-000D, 1 server(s):
  *Server: 10.78.105.47, port 1812, A-ID A3B6D4D8353F102346786CF220FF151C
  Status = ALIVE
  auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
0001-45 :
  0-00:Unknown
  2-ba:SGT_2
  3-00:SGT_3
  4-00:SGT_4
  5-00:SGT_5
  6-00:SGT_6
  7-00:SGT_7
  8-00:SGT_8
  9-00:SGT_9
  10-16:SGT_10
!
!
!
Environment Data Lifetime = 3600 secs
Last update time = 14:32:53 IST Mon Mar 14 2016
Env-data expires in 0:00:10:04 (dd:hr:mm:sec)
Env-data refreshes in 0:00:10:04 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
```

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

```
Device# show cts role-based permissions

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

CHAPTER 9

Bidirectional SXP Support

Feature History for Bidirectional SXP Support

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 17.18.1	Bidirectional SXP Support: With bidirectional SXP support, a single peer can function as both a speaker and a listener, allowing SXP bindings to flow in both directions over a single connection.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Cisco TrustSec and SXP Roles

Cisco TrustSec establishes secure network domains where devices authenticate one another. Within this system, the device originating data is called the "speaker," while the receiving device is the "listener."

Bidirectional SXP Support

With bidirectional SXP support, a single peer can function as both a speaker and a listener, allowing SXP bindings to flow in both directions over a single connection. This setup requires only one pair of IP addresses, with the listener initiating the connection and the speaker accepting it.

SXPv4 Loop Detection

SXP version 4 maintains support for loop detection, helping to prevent stale bindings within the network.

Configure Bidirectional SXP Support

To configure bidirectional SXP support, perform this task.

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts sxp enable**

Example:

```
Device(config)# cts sxp enable
```

Enables the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4).

Step 4 **cts sxp default password** *password*

Example:

```
Device(config)# cts sxp default password Cisco123
```

(Optional) Specifies the Cisco TrustSec SGT SXP default password.

Step 5 **cts sxp default source-ip** *ipv4-address*

Example:

```
Device(config)# cts sxp default source-ip 10.20.2.2
```

(Optional) Configures the Cisco TrustSec SGT SXP source IPv4 address.

Step 6 **cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} **both** [**vrf** *vrf-name*]

Example:

```
Device(config)# cts sxp connection peer 10.20.2.2 password default mode local both
```

Configures the Cisco TrustSec SXP peer address connection for a bidirectional SXP configuration.

- The **both** keyword configures the bidirectional SXP configuration.
- The **source** keyword specifies the IPv4 address of the source device. If no address is specified, the connection uses the default source address, if configured, or the address of the port.
- The **password** keyword specifies the password that Cisco TrustSec SXP uses for the connection using the following options:
    - **default**: Use the default Cisco TrustSec SXP password you configured using the cts sxp default password command.
    - **none**: A password is not used.
- The **mode** keyword specifies the role of the remote peer device:
    - **local**: The specified mode refers to the local device.
    - **peer**: The specified mode refers to the peer device.
    - **both**: Specifies that the device is both the speaker and the listener in the bidirectional SXP connection.
- The **optional** vrf keyword specifies the VRF to the peer. The default is the default VRF.

Step 7 **cts sxp speaker** *hold-time minimum-period*

Example:

```
Device(config)# cts sxp speaker hold-time 950
```

(Optional) Configures the global hold time (in seconds) of a speaker network device for Cisco TrustSec SGT SXPv4.

The valid range is from 1 to 65534. The default is 120.

Step 8 **cts sxp listener hold-time** *minimum-period maximum-period*

Example:

```
Device(config)# cts sxp listener hold-time 750 1500
```

(Optional) Configures the global hold time (in seconds) of a listener network device for Cisco TrustSec SGT SXPv4.

The valid range is from 1 to 65534. The default is 90 to 180.

Note
The *maximum-period* value must be greater than or equal to the minimum-period value.

Step 9 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode.

Step 10 **show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*]

Example:

```
Device# show cts sxp connections
```

Displays Cisco TrustSec Exchange Protocol (SXP) status and connections.

Configuration Examples for Bidirectional SXP Support

These sections provide configuration examples for Bidirectional SXP support.

Example: Configure Bidirectional SXP Support

The following example shows how to enable bidirectional CTS-SXP and configure the SXP peer connection on Device-A to connect to Device-B:

```
Device-A> enable
Device-A# configure terminal
Device-A(config)# cts sxp enable
Device-A(config)# cts sxp default password Cisco123
Device-A(config)# cts sxp default source-ip 10.10.1.1
Device-A(config)# cts sxp connection peer 10.20.2.2 password default mode local both
Device-A(config)# exit
```

The following example shows how to configure the bidirectional CTS-SXP peer connection on Device-B to connect to Device-A:

```
Device-B> enable
Device-B# configure terminal
Device-B(config)# cts sxp enable
Device-B(config)# cts sxp default password Password123
Device-B(config)# cts sxp default source-ip 10.20.2.2
Device-B(config)# cts sxp connection peer 10.10.1.1 password default mode local both
Device-B(config)# exit
```

Example: Verify Bidirectional SXP Support

The followinge example is a sample output of the **show cts sxp connections** command.

```
Device# show cts sxp connections

        SXP : Enabled
        Highest Version Supported: 4
        Default Password : Set
        Default Source IP: Not Set
        Connection retry open period: 120 secs
        Reconcile period: 120 secs
        Retry open timer is running
        ----------------------------------------------
        Peer IP : 2.0.0.2
        Source IP : 1.0.0.2
        Conn status : On (Speaker) :: On (Listener)
        Conn version : 4
        Local mode : Both
        Connection inst# : 1
        TCP conn fd : 1(Speaker) 3(Listener)
        TCP conn password: default SXP password
        Duration since last state change: 1:03:38:03 (dd:hr:mm:sec) :: 0:00:00:46
(dd:hr:mm:sec)
```

The followinge example is a sample output of the **show cts sxp connections brief** command.

```
        Device# show cts sxp connection brief

        SXP : Enabled
        Highest Version Supported: 4
        Default Password : Set
        Default Source IP: Not Set
        Connection retry open period: 120 secs
        Reconcile period: 120 secs
        Retry open timer is running
        -----------------------------------------------------
        Peer_IP Source_IP Conn Status Duration
        ---------------------------------------------------
        2.0.0.2 1.0.0.2 On(Speaker)::On(Listener) 0:00:37:17 (dd:hr:mm:sec)::0:00:37:19
(dd:hr:mm:sec)
```

The following table describes the various scenarios for the connection status output.

Node1	Node2	Node1 CLI Output for Connection Status	Node2 CLI Output for Connection Status
Both	Both	On (Speaker) On (Listener)	On (Listener) On (Speaker)
Speaker	Listener	On	On
Listener	Speaker	On	On