Configuring Cisco TrustSec

This chapter describes how to configure Cisco TrustSec on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About Cisco TrustSec

This section provides information about Cisco TrustSec.

Cisco TrustSec Architecture

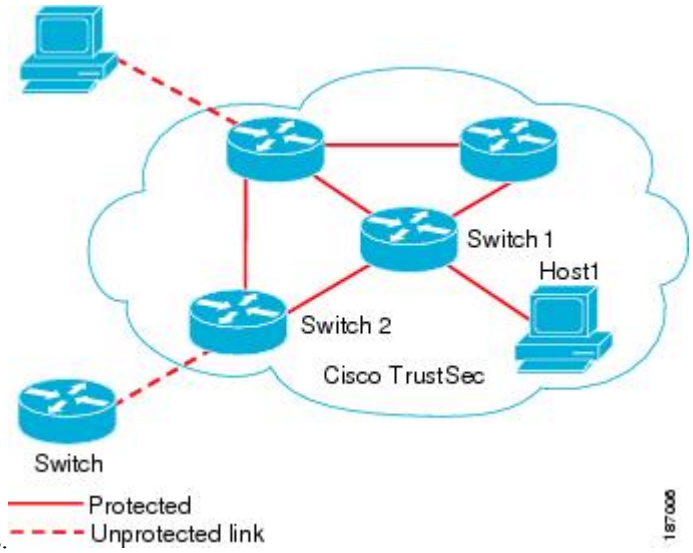
The Cisco TrustSec security architecture builds secure networks by establishing clouds of trusted network devices. Each device in a cloud is authenticated by its neighbors. Communication on the links between devices

in the cloud is secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms. Cisco TrustSec uses the device and user identification information acquired during authentication for classifying, or coloring, the packets as they enter the network. This packet classification is maintained by tagging packets on ingress to the Cisco TrustSec network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic.

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

Figure 1: Cisco TrustSec Network Cloud Example

This figure shows an example of a Cisco TrustSec network cloud. In this example, several networking devices and an endpoint device are inside the cloud. One endpoint device and one networking device are outside the cloud because they are not Cisco TrustSec-capable devices or they have been refused access.



The Cisco TrustSec architecture consists of the following major components:

Authentication
Verifies the identity of each device before allowing it to join the Cisco TrustSec network

Authorization
Decides the level of access to the Cisco TrustSec network resources for a device based on its authenticated identity

Access Control
Applies access policies on a per-packet basis using the source tags on each packet

Secure communication
Provides encryption, integrity, and data-path replay protection for the packets that flow over each link in the Cisco TrustSec network

A Cisco TrustSec network has the following entities:

Supplicants
Devices that attempt to join a Cisco TrustSec network

Authenticators (AT)
Devices that are already part of a Cisco TrustSec network

Authorization Server
Servers that might provide authentication information, authorization information, or both

When the link between the supplicant and the AT comes up, the following sequence of events might occur:

Authentication (802.1X)
The authentication server authenticates the supplicant or the authentication is completed if you configure the devices to unconditionally authenticate each other.

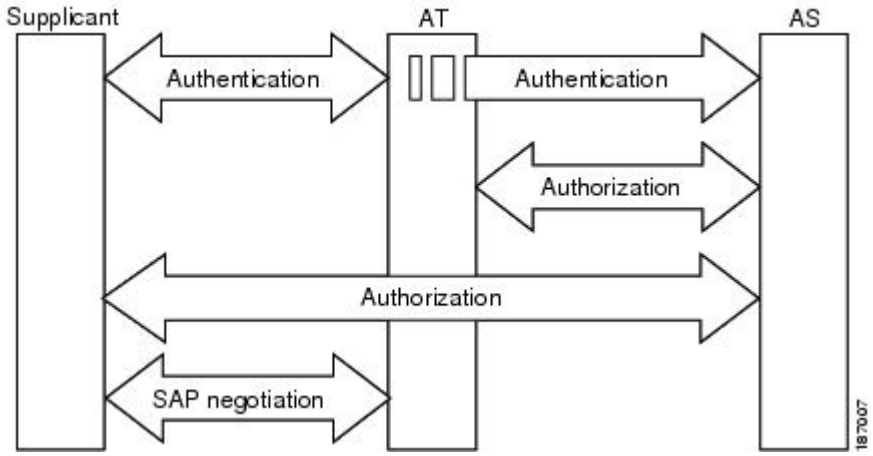
Authorization
Each side of the link obtains policies, such as SGT and ACLs, that apply to the link. A supplicant might need to use the AT as a relay if it has no other Layer 3 route to the authentication server.

Security Association Protocol Negotiation
The EAPOL-Key exchange occurs between the supplicant and the AT to negotiate a cipher suite, exchange security parameter indexes (SPIs), and manage keys. Successful completion of all three tasks results in the establishment of a security association (SA).

The ports stay in the unauthorized state (blocking state) until the SA protocol negotiation is complete.

Figure 2: SA Protocol Negotiation

This figure shows the SA protocol negotiation, including how the ports stay in unauthorized state until the SA protocol negotiation is complete.



SA protocol negotiation can use any of the following modes of operation:

- Galois/Counter Mode (GCM) encryption
- GCM authentication (GMAC)
- No encapsulation (clear text)
- Encapsulation with no encryption or authentication

Based on the IEEE 802.1AE standard, Cisco TrustSec uses ESP-128 GCM and GMAC.

Authentication

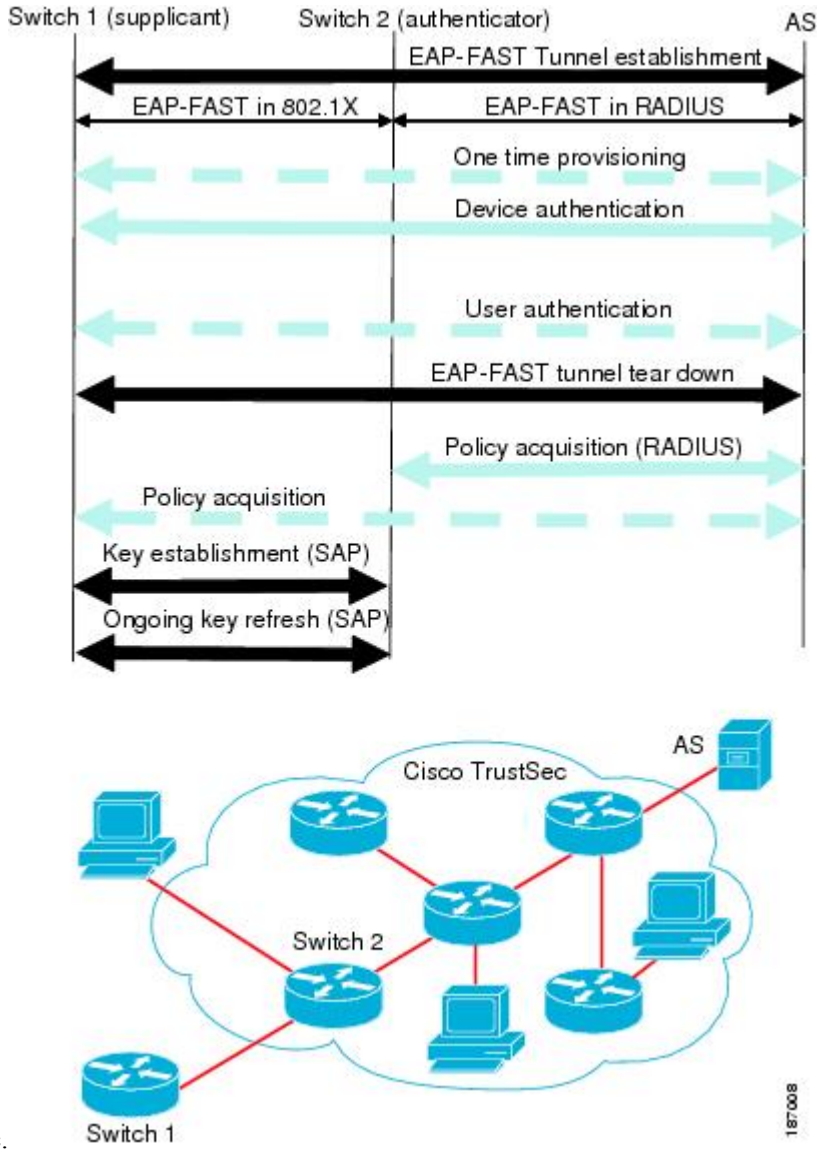
Cisco TrustSec authenticates a device before allowing it to join the network. Cisco TrustSec uses 802.1X authentication with Extensible Authentication Protocol Flexible Authentication through Secure Tunnel (EAP-FAST) as the Extensible Authentication Protocol (EAP) method to perform the authentication.

Cisco TrustSec and Authentication

Cisco TrustSec uses EAP-FAST for authentication. EAP-FAST conversations allow other EAP method exchanges inside the EAP-FAST tunnel using chains, which allows administrators to use traditional user authentication methods, such as Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2), while still having security provided by the EAP-FAST tunnel.

Figure 3: Cisco TrustSec Authentication

This figure shows the EAP-FAST tunnel and inner methods used in Cisco TrustSec.



Cisco TrustSec Enhancements to EAP-FAST

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

Authenticate the authenticator
Securely determines the identity of the AT by requiring the AT to use its protected access credential (PAC) to derive the shared secret between itself and the authentication server. This feature also prevents you from configuring RADIUS shared secrets on the authentication server for every possible IP address that can be used by the AT.

Notify each peer of the identity of its neighbor
By the end of the authentication exchange, the authentication server has identified the supplicant and the AT. The authentication server conveys the identity of the AT, and whether the AT is Cisco TrustSec-capable, to the supplicant by using additional type-length-value parameters (TLVs) in the protected EAP-FAST termination. The authentication server also conveys the identity of the supplicant and whether the supplicant is Cisco TrustSec-capable to the AT by using RADIUS attributes in the Access-Accept message. Because each peer knows the identity of its neighbor, it can send additional RADIUS Access-Requests to the authentication server to acquire the policy to be applied on the link.

AT posture evaluation
The AT provides its posture information to the authentication server whenever it starts the authentication exchange with the authentication server on behalf of the supplicant.

802.1X Role Selection

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

Instead of requiring manual configuration of the AT and supplicant roles for the Cisco NX-OS devices, Cisco TrustSec runs a role-selection algorithm to automatically determine which Cisco NX-OS device acts as the AT and which device acts as the supplicant. The role-selection algorithm assigns the AT role to the device that has IP reachability to a RADIUS server. Both devices start both the AT and supplicant state machines. When a Cisco NX-OS device detects that its peer has access to a RADIUS server, it terminates its own AT state machine and assumes the role of the supplicant. If both Cisco NX-OS devices have access to a RADIUS server, the algorithm compares the MAC addresses used as the source for sending the EAP over LAN (EAPOL) packets. The Cisco NX-OS device that has the MAC address with the higher value becomes the AT and the other Cisco NX-OS device becomes the supplicant.

Cisco TrustSec Authentication Summary

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

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

At the end of the Cisco TrustSec authentication process, the AT and the supplicant have the following information:

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

Device Identities

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

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

Device Credentials

Cisco TrustSec supports password-based credentials. The authentication servers may use self-signed certificates instead. Cisco TrustSec authenticates the supplicants through passwords and uses MSCHAPv2 to provide mutual authentication even if the authentication server certificate is not verifiable.

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

The authentication server uses a temporarily configured password to authenticate the supplicant when the supplicant first joins the Cisco TrustSec network. When the supplicant first joins the Cisco TrustSec network, the authentication server authenticates the supplicant using a manufacturing certificate and then generates a strong password and pushes it to the supplicant with the PAC. The authentication server also keeps the new password in its database. The authentication server and the supplicant use this password for mutual authentication in all future EAP-FAST phase 0 exchanges.

User Credentials

Cisco TrustSec does not require a specific type of user credentials for endpoint devices. You can choose any type of authentication method for the user (for example, MSCHAPv2, LEAP, generic token card (GTC), or OTP) and use the corresponding credentials. Cisco TrustSec performs user authentication inside the EAP-FAST tunnel as part of the EAP-FAST phase 2 exchange.

Native VLAN Tagging on Trunk and FabricPath Ports

MACSec is supported over FabricPath through native VLAN tagging on trunk and FabricPath ports feature. Native VLAN tagging can be configured either globally or on an interface for control packets and data packets. Use the following commands to enable native VLAN tagging globally:

- **vlan dot1q tag native exclude control**
- **vlan dot1q tag native fabricpath**
- **vlan dot1q tag native fabricpath exclude control**

Use the following commands to enable native VLAN tagging on FabricPath ports:

- **switchport trunk native vlan tag exclude control**
- **switchport fabricpath native vlan tag**

- **switchport fabricpath native vlan tag exclude control**

Native VLAN tagging provides support for tagged and untagged modes when sending or receiving packets. The following table explains the mode for a packet on a global configuration or port configuration for the above commands.

Tagging Configuration	TX-Control	TX-Data (Native VLAN)	RX-Control	RX-Data
Global trunk port tagging	Untagged	Tagged	Untagged and tagged	Tagged
Global FabricPath tagging	Untagged	Untagged	Untagged and tagged	Untagged and tagged
Global FabricPath tagging for data packets	Untagged	Tagged	Untagged and tagged	Tagged
Port-level trunk port tagging	Untagged	Tagged	Untagged and tagged	Tagged
Port-level Fabricpath tagging	Untagged	Untagged	Untagged and tagged	Untagged and tagged
Port-level FabricPath tagging for data packets	Untagged	Tagged	Untagged and tagged	Tagged

SGACLs and SGTs

In security group access lists (SGACLs), you can control the operations that users can perform based on assigned security groups. The grouping of permissions into a role simplifies the management of the security policy. As you add users to a Cisco NX-OS device, you simply assign one or more security groups and they immediately receive the appropriate permissions. You can modify security groups to introduce new privileges or restrict current permissions.

Cisco TrustSec assigns a unique 16-bit tag, called the security group tag (SGT), to a security group. The number of SGTs in a Cisco NX-OS device is limited to the number of authenticated network entities. The SGT is a single label that indicates the privileges of the source within the entire enterprise. Its scope is global within a Cisco TrustSec network.

The management server derives the SGTs based on the security policy configuration. You do not have to configure them manually.

Once authenticated, Cisco TrustSec tags any packet that originates from a device with the SGT that represents the security group to which the device is assigned. The packet carries this SGT throughout the network within the Cisco TrustSec header. Because this tag represents the group of the source, the tag is referred to as the source SGT. At the egress edge of the network, Cisco TrustSec determines the group that is assigned to the packet destination device and applies the access control policy.

Cisco TrustSec defines access control policies between the security groups. By assigning devices within the network to security groups and applying access control between and within the security groups, Cisco TrustSec essentially achieves access control within the network.

Figure 4: SGACL Policy Example

This figure shows an example of an SGACL policy.

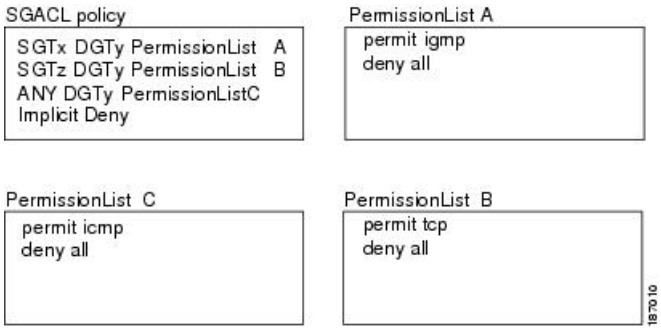
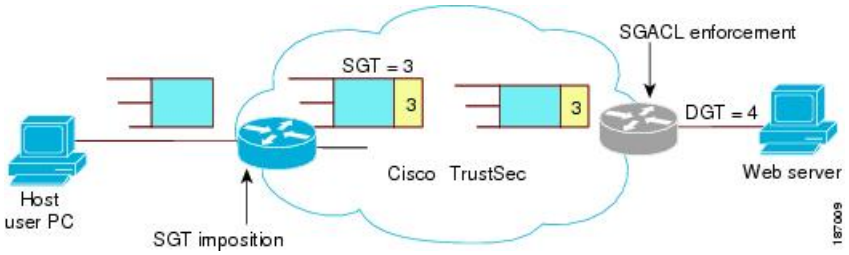


Figure 5: SGT and SGACL in Cisco TrustSec Network

This figure shows how the SGT assignment and the SGACL enforcement operate in a Cisco TrustSec network.



The Cisco NX-OS device defines the Cisco TrustSec access control policy for a group of devices as opposed to IP addresses in traditional ACLs. With such a decoupling, the network devices are free to move throughout the network and change IP addresses. Entire network topologies can change. As long as the roles and the permissions remain the same, changes to the network do not change the security policy. This feature greatly reduces the size of ACLs and simplifies their maintenance.

In traditional IP networks, the number of access control entries (ACEs) configured is determined as follows:

Number of ACEs = (number of sources specified) X (number of destinations specified) X (number of permissions specified)

Cisco TrustSec uses the following formula:

Number of ACEs = number of permissions specified

For information about SGACL policy enforcement with SGT caching, see SGACL Policy Enforcement With Cisco TrustSec SGT Caching.

Determining the Source Security Group

A network device at the ingress of the Cisco TrustSec network cloud needs to determine the SGT of the packet entering the Cisco TrustSec network cloud so that it can tag the packet with that SGT when it forwards it into the Cisco TrustSec network cloud. The egress network device needs to determine the SGT of the packet so that it can apply the SGACLs.

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

- Obtain the source SGT during policy acquisition—After the Cisco TrustSec authentication phase, a network device acquires a policy from an authentication server. The authentication server indicates

whether the peer device is trusted or not. If a peer device is not trusted, the authentication server can also provide an SGT to apply to all packets coming from the peer device.

- Obtain the source SGT field from the Cisco TrustSec header—If a packet comes from a trusted peer device, the Cisco TrustSec header carries the correct SGT field if the network device is not the first network device in the Cisco TrustSec network cloud for the packet.
- Look up the source SGT based on the source IP address—In some cases, you can manually configure the policy to decide the SGT of a packet based on the source IP address. The SGT Exchange Protocol (SXP) can also populate the IP-address-to-SGT mapping table.

Determining the Destination Security Group

The egress network device in a Cisco TrustSec network cloud determines the destination group for applying the SGACL. In some cases, ingress devices or other nonegress devices might have destination group information available. In those cases, SGACLs might be applied in these devices rather than in egress devices.

Cisco TrustSec determines the destination group for the packet in the following ways:

- Destination SGT of the egress port obtained during the policy acquisition
- Destination SGT lookup based on the destination IP address

Do not configure the destination SGT to enforce Cisco TrustSec on egress broadcast, multicast, and unknown unicast traffic on Fabric Extender (FEX) or vEthernet ports. Instead, set the DST to zero (unknown). The following is an example of the correct configuration:

```
cts role-based access-list acl-on-fex-egress
     deny udp
     deny ip
cts role-based sgt 9 dst 0 access-list acl-on-fex-egress
```

SGACL Detailed Logging

From Cisco NX-OS Release 7.3(0)D1(1), you can use the SGACL detailed logging feature to observe the effects of SGACL policies after their enforcement at the egress point. You can check the following:

- Whether a flow is permitted or denied
- Whether a flow is monitored or enforced by the SGACL

By default, the SGACL detailed logging feature is disabled.

Note SGACL monitoring mode requires SGACL detailed logging to be enabled. To disable SGACL detailed logging, make sure that SGACL monitoring mode is disabled.

From Cisco NX-OS Release 7.3(1)D1(1), the SGACL detailed logging feature is supported on the Cisco Nexus M2 and M3 series modules. However, the SGACL detailed logging information for traffic arriving on interfaces of the Cisco M2 series modules is supported when the following conditions are met:

- The source SGT for traffic is derived locally on the enforcement device.
- The interfaces of the Cisco M2 series modules do not have any port-SGT configuration.

Note The SGACL detailed logging feature is not supported on the Cisco Nexus M1 series modules.

SGACL Monitor Mode

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

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

From Cisco NX-OS Release 7.3(1)D1(1), the SGACL monitor mode feature is supported on the Cisco Nexus M2 and M3 series modules. However, the SGACL monitor mode feature is not supported on the Cisco Nexus M1 series modules.

Note The SGACL monitor mode feature is supported on the Cisco Nexus M2 series modules for all scenarios, and flows are allowed or denied based on the SGACL monitor mode configuration and policy actions. However, the support for SGACL detailed logging information is limited. For more information, see SGACL Detailed Logging, on page 9.

Overview of SGACL Egress Policy Overwrite

In releases earlier than Cisco NX-OS Release 8.0 (1), SGACLs from only one source was valid. Consider the following scenarios:

- SGACL is configured using CLI followed by SGACL downloaded from Integrated Services Engine (ISE). In this case, the SGACL downloaded from ISE is ignored.
- SGACL is downloaded from ISE followed by SGACL configured using CLI. In this case, the SGACL downloaded from ISE is overwritten.

From Cisco NX-OS Release 8.0 (1), the SGACLs downloaded using ISE and SGACLs configured using CLI can coexist. You can prioritize whether to use SGACLs downloaded from ISE or SGACLs configured by using CLI. Use the **[no] cts role-based priority-static** command to choose the install priority between the SGACLs configured by using CLI or SGACLs downloaded by ISE. By default, the SGACLs configured by using CLI have higher priority in Cisco NX-OS.

SGACL Policy Enforcement With Cisco TrustSec SGT Caching

This section discusses about the special cases that needs to be considered when you enable SGT Caching feature with Cisco TrustSec SGACL policy enforcement. Specifically, the SGT Caching mode for **sgt=any**,**dgt=any**, and **sgt=0,dgt=0**.

The SGT Caching feature mandates the installation of two main SGACL policies, that is, <**sgt = any, dgt = any**> and <**sgt = 0, dgt = 0**> in the hardware. If these SGACL policies are not configured by using CLI, then CTS manager creates and installs the reserved SGACL policies: <**sgt = any, dgt= any, permit all log**> and <**sgt = 0, dgt = 0, permit all**>.

Prior to Cisco NX-OS Release 8.0(1), if the SGT Caching feature is enabled with Cisco TrustSec SGACL policy enforcement, the following changes are observed:

- The reserved SGACL created by SGT caching is considered as SGACL configured by CLI. The SGACL policy with values <**sgt =any, dgt = any, ise_user_rbacl**> downloaded from ISE is ignored, because SGACLs configured by using CLI are given higher priority. Therefore, the reserved SGACL with values <**sgt=any dgt=any, permit all log**> is installed in hardware, when SGACL with <**sgt =any, dgt = any**> is not configured by the user by using CLI and only available in ISE.
- SGACL traffic counters are not supported for the reserved SGACLs. Therefore, the SGACL traffic counters are not supported for the default Any-Any policy, when SGT-caching with enforcement is enabled and there is no SGACL with <**sgt=any , dgt=any**> configured by using CLI.
- If you configure an SGACL with values <**sgt=any,dgt=any,user_rbacl** by using CLI, the **permit all log** is appended with the **user_rbacl** ACE and installed in hardware. SGACL traffic counters are supported as usual for this user installed with Any-Any policy by using CLI.

Starting from Cisco NX-OS Release 8.0(1), the rules that apply to CLI installed Any-Any SGACLs with SGT-caching feature in prior releases, are also applicable to the ISE downloaded SGACLs. In case of coexistence of the Any-Any SGACL from both CLI and ISE, the policy that needs to be used is decided based on the priority selection. SGACL traffic counters for the default policy are supported as long as the Any-Any policy from either CLI or ISE is available.

SGACL Egress Policy Overwrite With Monitor Mode

The following table provides information about how SGACLs from different sources (CLI or ISE) are selected and installed based on the "install priority" and "monitor mode" configuration.

Priority Configured	Monitor Mode Status	CLI SGACL Only	CLI Monitored SGACL Only	ISE SGACL Only	ISE Monitored SGACL Only	CLI SGACL and ISE SGACL	CLI and ISE Monitored SGACL	CLI Monitored SGACL and ISE SGACL	CLI Monitored SGACL and ISE Monitored SGACL
no cts role-based priority-static	Disabled	Install CLI SGACL	Install CLI SGACL	Install ISE SGACL	No Install	Install ISE SGACL	Install CLI SGACL	Install ISE SGACL	No Install
cts role-based priority-static	Disabled	Install CLI SGACL	Install CLI SGACL	Install ISE SGACL	No Install	Install CLI SGACL	Install CLI SGACL	Install CLI SGACL	Install CLI SGACL

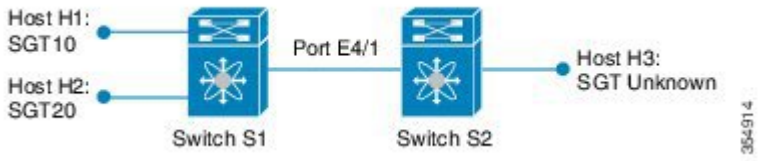
Priority Configured	Monitor Mode Status	CLI SGACL Only	CLI Monitored SGACL Only	ISE SGACL Only	ISE Monitored SGACL Only	CLI SGACL and ISE SGACL	CLI and ISE Monitored SGACL	CLI Monitored SGACL and ISE SGACL	CLI Monitored SGACL and ISE Monitored SGACL
no cts role-based priority-static	Enabled	Install CLI SGACL	Install CLI Monitored SGACL	Install ISE SGACL	Install CLI Monitored SGACL	Install ISE SGACL	Install ISE Monitored SGACL	Install ISE SGACL	Install ISE Monitored SGACL
cts role-based priority-static	Enabled	Install CLI SGACL	Install CLI Monitored SGACL	Install ISE SGACL	Install CLI Monitored SGACL	Install CLI SGACL	Install CLI SGACL	Install CLI Monitored SGACL	Install CLI Monitored SGACL

Overview of SGACL Policy Enforcement Per Interface

From Cisco NX-OS Release 8.0(1), you can enable or disable SGACL policy enforcement on Layer 3 (L3) physical interfaces and port-channels.

Consider the following scenario with two Cisco Nexus 7000 series switches. This scenario provides an overview about using the SGACL policy enforcement per interface.

Figure 6: SGACL Policy Enforcement Per Interface Enabled



The following table provides information about the SGACL policies.

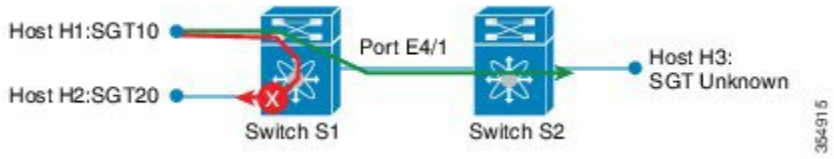
SGT Information	SGT10	SGT20	SGT Unknown
SGT10	Permit	Deny	Deny
SGT20	Deny	Permit	Deny

When SGACLs are applied on this setup, hosts with SGT10 cannot communicate with SGT20 and Unknown SGT hosts, because SGACL policy drops the packets. However, when you disable the SGACL policy enforcement on the port E4/1:

- The host H1 cannot communicate with the host H2 because this network traffic is subjected to the SGT 10 DGT 20 Deny policy.
- The host H1 can communicate with host H3 even if this network traffic is subjected to the SGT 10 DGT unknown Deny policy. This communication is possible because the packet is exiting through the port E4/1 on which the SGACL policy enforcement is disabled.

The following figure shows the packet routes between different hosts after the SGACL policy enforcement is disabled on the port E4/1.

Figure 7: SGACL Policy Enforcement Per Interface Disabled



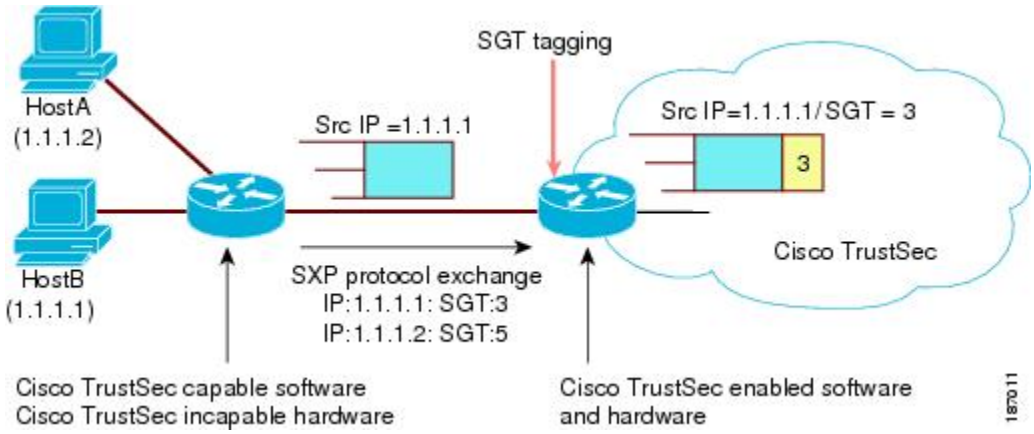
SXP for SGT Propagation Across Legacy Access Networks

The Cisco NX-OS device hardware in the access layer supports Cisco TrustSec. Without the Cisco TrustSec hardware, the Cisco TrustSec software cannot tag the packets with SGTs. You can use SXP to propagate the SGTs across network devices that do not have hardware support for Cisco TrustSec.

SXP operates between access layer devices and distribution layer devices. The access layer devices use SXP to pass the IP addresses of the Cisco TrustSec-authenticated devices with their SGTs to the distribution switches. Distribution devices with both Cisco TrustSec-enabled software and hardware can use this information to tag packets appropriately and enforce SGACL policies.

Figure 8: Using SXP to Propagate SGT Information

This figure shows how to use SXP to propagate SGT information in a legacy network.



Tagging packets with SGTs requires hardware support. You might have devices in your network that cannot tag packets with SGTs. To allow these devices to send IP address-to-SGT mappings to a device that has Cisco TrustSec-capable hardware, you must manually set up the SXP connections. Manually setting up an SXP connection requires the following:

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

Cisco TrustSec with SXPv3

The Security Group Tag (SGT) Exchange Protocol (SXP) is a control protocol, which propagates IP address-SGT binding information across network devices. From Cisco NX-OS Release 7.3(0)D1(1), the SXP version 3 (SXPv3) feature provides support to transport the IPv4 subnet to the SGT bindings.

By using the subnet for SGT bindings, you can minimize the forward information base (FIB) entries needed for storing the mapping, which allows users to increase the scale of the TrustSec deployments. In many scenarios, you can use subnet-SGT bindings instead of the L3 interface-SGT.

Note

- SXPv2 is not supported in the Cisco NX-OS Release 7.3(0)D1(1).
- SXPv3 does not support IPv6.

SXPv3 Subnet Expansion

The SXPv3 protocol allows you to configure the expansion limit for a subnet binding. SXP expands a subnet binding to host address bindings when a connection is set up with a peer with a version earlier than Version 3. SXP binding expansion is applicable only to IPv4 subnet binding.

The characteristics of subnet expansion are as follows:

- When expanding the bindings for overlapping IP addresses with different SGT values, the mapping is obtained from the IP address with the longest prefix length.
- If the subnet expansion reaches the configured limit, a system log is generated for the subnet that cannot be expanded.
- Binding expansion does not expand broadcast IP addresses in a subnet. Also, note that SXP does not summarize host IP addresses to subnet bindings. In the SXP propagation path, if there is a node that does not understand subnet binding, the bindings are expanded and propagated through the rest of the propagation path as host IP binding even though there is a node that understands subnet binding.
- The default expansion limit is zero (0) and the maximum allowed expansion limit is 65535. You can set the expansion limit as 0 when you do not have any devices supporting a lower version of SXP, in the network.

You can use the **cts sxp mapping network-map** [*num_bindings*] command to expand the network limit. The *num_bindings* parameter can accept value from 0 to 65535. The value zero (0) indicates that no expansion is allowed and 65535 is the maximum expansion limit allowed. The default value is zero (0).

Consider an example when the expansion limit is set to 67 and the subnet is /24. Cisco NX-OS expands the first 67 IP addresses for the first subnet SGT known to Cisco TrustSec. Since subnet /24 contains more hosts, it will never be fully expanded, and a syslog is generated.

Note When you set the maximum expansion limit as 65535, Cisco NX-OS supports the mapping of every IP in a /16 subnet. However, you must consider the hardware or software impact of setting the expansion limit to the maximum limit.

SXP Version Negotiation

The SXP session is established between speaker devices and listener devices. By default, the Cisco TrustSec device advertises the highest supported SXP version. The negotiation is made based on the highest common version supported by the speaker and listener devices. A standalone Cisco TrustSec-supported device can establish SXP session with different versions, with its peer devices, depending on the SXP versions of the peer devices.

Note Configure the SXP default source IP address on an SXP device only when all its peer SXP devices are configured to connect to this configured default source IP address. If the default source IP address configuration is not used on an SXP device, configure the source IP address that the SXP device should use with the **cts sxp connection peer** command.

The following table provides information about version negotiation for interoperability in different scenarios.

Table 1: SXP Version Negotiation Cases

Case Number	Speaker	Listener	SXP Session Status
1	SXPv1	SXPv1	SXPv1 session is established.
2	SXPv1	SXPv2	SXPv1 session is established.
3	SXPv1	SXPv3	SXPv1 session is established.
4	SXPv2	SXPv1	SXPv1 session is established.
5	SXPv2	SXPv2	Not possible because a Cisco Nexus 7000 device does not support SXPv2.
6	SXPv2	SXPv3	If a Cisco Nexus 7000 device with SXPv3 is interoperating with another Cisco SXP device having SXPv2, the Cisco Nexus 7000 device ensures that the connection is established as SXPv1.
7	SXPv3	SXPv1	SXP session is established.
8	SXPv3	SXPv2	If a Cisco Nexus 7000 device with SXPv3 is interoperating with another Cisco SXP device having SXPv2, the Cisco Nexus 7000 device ensures that the connection is established as SXPv1.
9	SXPv3	SXPv3	SXPv3 session is established.
10	SXPv1	SXPv4	SXPv1 session is established.
11	SXPv2	SXPv4	If a Cisco Nexus 7000 device with SXPv4 is interoperating with another Cisco SXP device having SXPv2, the Cisco Nexus 7000 device ensures that the connection is established as SXPv1.
12	SXPv3	SXPv4	SXPv3 session is established.
13	SXPv4	SXPv1	SXPv1 session is established.

Case Number	Speaker	Listener	SXP Session Status
14	SXPv4	SXPv2	If a Cisco Nexus 7000 device with SXPv4 is interoperating with another Cisco SXP device having SXPv2, the Cisco Nexus 7000 device ensures that the connection is established as SXPv1.
15	SXPv4	SXPv3	SXPv3 session is established.
16	SXPv4	SXPv4	SXPv4 session is established.

SXP Support for Default Route SGT Bindings

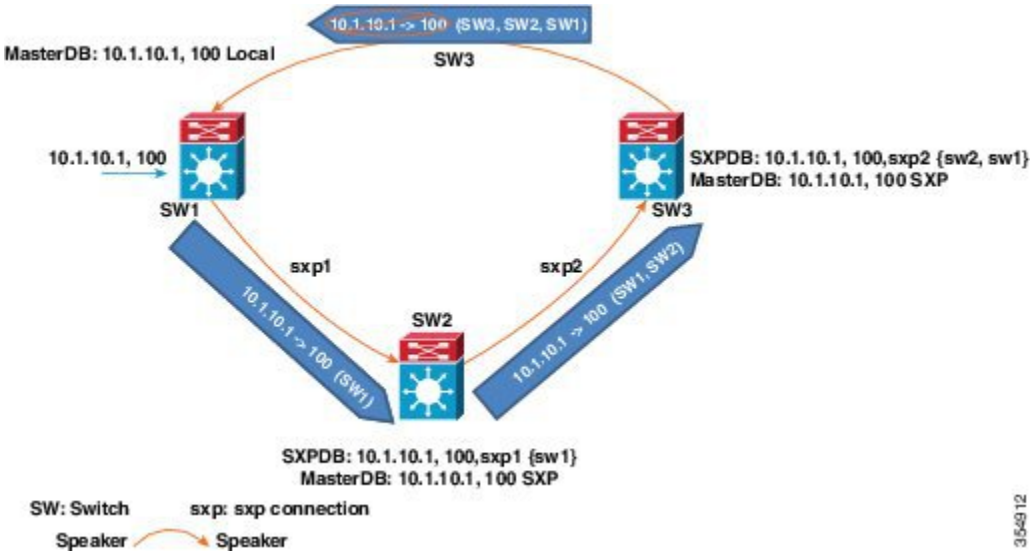
You can provide the default route for SGT bindings, when IP-SGT for the source IP address or destination IP address is not configured. In this scenario, SGT is derived from the default route entry. Note that you can use the default route only for the listener device with SXPv3. By default, the transport of SGT bindings through the default route by using SXP, is disabled. You can enable the transport of SGT bindings through the default route by using the **cts sxp allow default-route-sgt** command. Use the **no** form of this command to disable the default route of the SGT bindings.

Overview of Cisco TrustSec with SXPv4

Cisco TrustSec SXP version 4 (SXPv4) enhances the functionality of SXP by adding a loop detection mechanism to prevent stale binding in the network. SXP connections can be enabled such that the binding forwarded by one switch for an SXP connection can be received from another SXP connection, resulting in SXP connection loops. SXP loop topology might, however, result in stale binding in the network. SXPv4' s built-in loop detection and prevention mechanism addresses the stale binding issue whenever there is a loop between SXP nodes.

Loop prevention is achieved by adding SXP propagation path information when propagating (adding or deleting) bindings. Propagation path information keeps track of the network devices (via their node IDs) that the binding travels in an ordered manner. All nodes that participate in the network with looped SXP connections must run SXPv4 to function correctly. Loop detection is a mandatory capability in SXPv4.

Figure 9: SXPv4 Loop Detection



In the figure above there are three network devices: SW1, SW2, and SW3. There are also three SXP connections: SXP1, SXP2, and SXP3, together which create an SXP connection loop. A binding (10.1.10.1, 100) is learned at SW1 through local authentication. The binding is exported by SW1 to SW2 together with the path information (that is, SW1, from where the binding is forwarded).

Upon receiving the binding, SW2 exports it to SW3, again prepending the path information (SW2, SW1). Similarly, SW3 forwards the binding to SW1 with path information SW3, SW2, SW1. When SW1 receives the binding, the path information is checked. If its own path attribute is in the binding update received, then a propagation loop is detected. This binding is dropped and not stored in the SXP binding database.

If the binding is removed from SW1, (for example, if a user logs off), a binding deletion event is sent. The deletion event goes through the same path as above. When it reaches SW1, no action will be taken as no such binding exists in the SW1 binding database.

Loop detection is done when a binding is received by an SXP but before it is added to the binding database.

SXP Node ID

An SXP node ID is used to identify the individual devices within the network. The node ID is a four-octet integer that can be configured by the user. If it is not configured by the user, Cisco TrustSec assigns the router ID on the default VRF as the node ID, in the same manner that EIGRP generates its router ID, which is the first IP address on Cisco Nexus 7000 series switches.

The SXP loop detection mechanism drops binding propagation packets based on finding its own node ID in the peer sequence attribute. Changing a node ID in a loop detection-running SXP network could break SXP loop detection functionality and therefore needs to be handled carefully.

The bindings that are associated with the original node ID have to be deleted in all SXP nodes before the new node ID is configured. This can be done by disabling the SXP feature on the network device where you desire to change the node ID. Before you change the node ID, wait until the SXP bindings that are propagated with the particular node ID in the path attribute are deleted.

The node ID configuration is blocked or restricted when SXP is in the enabled state. Router-ID changes in the switch do not affect the SXP node ID, while SXP is enabled. A syslog is generated to indicate that the router ID of the system has changed and this may affect SXP loop detection functionality.

Note Disabling the SXP feature brings down all SXP connections on the device.

Keepalive and Hold-Time Negotiation with SXPv4

SXP uses a TCP-based, keepalive mechanism to determine if a connection is live. SXPv4 adds an optional negotiated keepalive mechanism within the protocol to provide more predictable and timely detection of connection loss.

SXP connections are asymmetric with almost all of the protocol messages (except for open/open_resp and error messages) sent from an SXP speaker to an SXP listener. The SXP listener can keep a potentially large volume of state per connection, which includes all the binding information learned on a connection. Therefore, it is only meaningful to have a keepalive mechanism that allows a listener to detect the loss of connection with a speaker.

The mechanism is based on two timers:

- **Hold timer**—Used by a listener for detection of elapsing time without successive keepalive or update messages from a speaker
- **Keepalive timer**—Used by a speaker to trigger the dispatch of keepalive messages during intervals when no other information is exported through update messages

The hold-time for the keepalive mechanism may be negotiated during the open or open_resp exchange at connection setup. The following information is important during the negotiation:

- A listener may have desirable range for the hold-time period locally configured or have a default of 90 to 180 seconds. A value of 0xFFFF..0xFFFF indicates that the keepalive mechanism is not used.
- A speaker may have a minimum acceptable hold-time period locally configured or have a default of 120 seconds. This is the shortest period of time a speaker is willing to send keepalive messages for keeping the connection alive. Any shorter hold-time period would require a faster keepalive rate than the rate the speaker is ready to support.
- A value of 0xFFFF implies that the keepalive mechanism is not used.
- The negotiation succeeds when the speaker's minimum acceptable hold-time falls below or within the desirable hold-time range of the listener. If one end turns off the keepalive mechanism, the other end should also turn it off to make the negotiation successful.
- The negotiation fails when the speaker's minimum acceptable hold-time is greater than the upper bound of the listener's hold-time range.
- The selected hold-time period of a successful negotiation is the maximum of the speaker's minimum acceptable hold-time and the lower bound of the listener's hold-time range.
- The speaker calculates the keepalive time to one-third of the selected hold-time by default unless a different keepalive time is locally configured.
- Larger Minimum listener hold-time values are recommended on systems with large number of bindings or connections. Also, these values are recommended if there is a requirement to hold the bindings on the listener during network maintenance events.

For more information about the hold-time negotiation process, see the Cisco TrustSec Configuration Guide, Cisco IOS Release 15M&T.

Bidirectional SXP Support Overview

The Bidirectional SXP Support feature enhances the functionality of Cisco TrustSec with SXP version 4 by adding support for SXP bindings that can be propagated in both directions between a speaker and a listener over a single connection.

With the support for bidirectional SXP configuration, a peer can act as both a speaker and a listener and propagate SXP bindings in both directions using a single connection.

The bidirectional SXP configuration is managed with one pair of IP addresses, thereby reducing operational complexity. On either end, only the listener initiates the SXP connection and the speaker accepts the incoming connection.

Figure 10: Bidirectional SXP Connection

In addition, bidirectional SXP uses the underlying loop-detection benefits of SXPv4 to avoid replay of updates back and forth across the same connection.

Note The peers at each end of the connection must be configured as a bidirectional connection using the **both** keyword. It is an incorrect configuration to have one end configured as a bidirectional connection using the **both** keyword and the other end configured as a speaker or listener (unidirectional connection). The system will not be able to detect the mismatch in configuration leading to unpredictable SXP connectivity.

Guidelines and Limitations for SXPv4

Cisco TrustSec SXPv4 has the following guidelines and limitations:

- The Bidirectional SXP Support feature enhances the functionality of Cisco TrustSec with SXPv4 by adding support for SXP bindings that can be propagated in both directions between a speaker and a listener over a single connection.
- IPV6 bindings are not learned or transported by the Cisco Nexus 7000 series switches over SXPv4 connections. However, the SXPv4 peering with speakers transporting IPv6 bindings are still supported.
- Cisco Nexus 7000 series switches only expand Subnet-SGT bindings over SXPv3 connections.
- After upgrading to the Cisco Nexus Release 8.0(1), the default version SXPv4 is advertised by a switch. The appropriate connection versions are re-negotiated with the peers.
- Ensure that there are no overlapping node IDs configured in the network or the node IDs that are configured in the network do not overlap with IP addresses used elsewhere in the network.
- Ensure that there are no overlapping IP addresses to avoid unintentional reuse of default node IDs in the network.
- Before modifying IP addresses in the switch or a router, ensure that the old and the new IP addresses have not been used as default node IDs locally or remotely in the network.

- Ensure that the speaker and listener hold-time values per connection or global or default for each speaker-listener pair are compatible.
- Note that using the hold-time value as 65535 on speaker or listener disables the in-built keepalive mechanism and avoids the staling of bindings upon connectivity loss on SXPv4 devices. Administrative connection resets are required to clear these bindings.
- When migrating existing unidirectional connections to bidirectional connections, ensure that the global hold times are compatible and the bindings learnt in both directions are within the supported scale limits. Also, ensure that the global or default hold-time values on speaker and listener are compatible, since you cannot configure hold-time values for these connections on a per-connection basis.

Cisco TrustSec Subnet-SGT Mapping

Subnet-SGT mapping binds an SGT to all the host addresses of a specified subnet. After this mapping is implemented, Cisco TrustSec imposes SGT on incoming packets having a source IP address that belongs to the specified subnet. This enables you to enforce the Cisco TrustSec policy on the traffic flowing through data center hosts. You can configure IPv4 subnet-SGT bindings under a VRF instance.

In IPv4 networks, SXPv3 and later versions can receive and parse subnet network address or prefix strings from SXPv3 peers.

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

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

Note Use the **cts sxp mapping network-map** global configuration command to limit the number of subnet binding expansions exported to an SXPv1 peer.

Subnet bindings are static, which means that active hosts are not learned. They can be used locally for SGT imposition and SGACL enforcement. Packets tagged by subnet-SGT mapping can be propagated on Layer 2 or Layer 3 TrustSec links. Additionally, you can use the **cts sxp allow default-route-sgt** command to enable the transport of SGT bindings through the default route, that is, unknown IP address 0.0.0.0.

SGT Tagging Exemption for Layer 2 Protocols

The Layer 2 (L2) control plane protocols are responsible for creating and maintaining operational states between devices connected through the Cisco TrustSec-enabled links. SGT tagging is enabled by default on Cisco TrustSec-enabled links. A Cisco TrustSec-enabled device applies SGT tags for almost all the L2 packets egressing an interface. The L2 peers on the ingress interfaces process the SGT packets. However, some peers cannot process the SGT-tagged control packets tagged due to limitations. For example, Cisco F3 Series modules do not accept the packets with an SGT tag in the port ingress when the IEEE 802.1Q tag is missing in front of the SGT tag. This causes a peer to drop the L2 control packets such as Cisco Discovery Protocol, Link Level Discovery Protocol (LLDP), Link Aggregation Control Protocol (LACP), or bridge protocol data units (BPDU) with SGT.

From Cisco NX-OS Release 8.1(1), Cisco TrustSec provides the following enhancements to exempt SGT tagging for the L2 control packets:

1. By default, Cisco NX-OS assigns null SGT for the L2 control packets even if the device SGT is non-zero.
2. Cisco Nexus line card modules perform the following action after receiving null SGT and L2 packet from the Supervisor module:
   - Cisco Nexus F Series modules do not tag null SGT for the L2 control packets.
   - Cisco Nexus M Series modules tag null SGT for the L2 control packets. In this case, you can prevent the Cisco Nexus M series modules from tagging null SGT by using the **no propagate-sgt l2-control** command. This exemption ensures that the L2 control protocols are transmitted without any SGT tags from the Cisco TrustSec-enabled ports.

Use the **no propagate-sgt l2-control** command to exempt the SGT tagging of the L2 control plane protocols for an interface. By default, the SGT tagging is not exempted for the L2 control plane protocols. For example, if the Cisco M3 series module has to interoperate with the Cisco F3 series module by using the Cisco TrustSec enabled link, then enable the **no propagate-sgt l2-control** command for the M3 series module. This ensures that the control packets are accepted by the Cisco F3 series module.

You can also enable or disable the SGT tagging of the L2 control plane protocols under a port profile or a port channel.

Note

- The **no propagate-sgt l2-control** command is supported only on the Cisco M3 Series module ports without Cisco TrustSec MACSec.
- You can also enable or disable SGT tagging of the L2 control packets under a port profile and a port channel.

Authorization and Policy Acquisition

After authentication ends, the supplicant and AT obtain the security policy from the authentication server. The supplicant and AT enforce the policy against each other. Both the supplicant and AT provide the peer device ID that each receives after authentication. If the peer device ID is not available, Cisco TrustSec can use a manually configured peer device ID.

The authentication server returns the following policy attributes:

Cisco TrustSec Trust
Indicates whether the neighbor device is to be trusted for the purpose of putting the SGT in the packets.

Peer SGT
Indicates the security group that the peer belongs to. If the peer is not trusted, all packets received from the peer are tagged with the SGT configured on the ingress interface. If enforcement is enabled on this interface, the SGACLs that are associated with the peer SGT are downloaded. If the device does not know if the SGACLs are associated with the peer's SGT, the device might send a follow-up request to fetch the SGACLs.

Authorization expiry time
Indicates the number of seconds before the policy expires. The Cisco-proprietary attribute-value (AV) pairs indicate the expiration time of an authorization or policy response to a Cisco TrustSec device. A Cisco TrustSec device should refresh its policy and authorization before it times out.

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

Change of Authorization

Cisco TrustSec uses the RADIUS Change of Authorization feature to automatically download policies from Cisco Identity Services Engine (ISE) server to a switch, after an administrator updates the AAA profile on the server.

Note The feature works with Cisco ISE only and not with Cisco Secure Access Control Server (ACS).

Environment Data Download

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

Note If you have manually configured the Cisco TrustSec device ID, but not using the AAA server for a Cisco TrustSec deployment, you should remove the Cisco TrustSec device ID by using the **no cts device-id** command. Otherwise, the following false syslog error is generated:

```
ENVIRONMENT_DATA_DOWNLOAD_FAILURE:  Environment data download failed from AAA
```

The **no cts device-id** command is supported from Cisco NX-OS Release 7.2. If you are using Cisco NX-OS Release 6.2.6 or a later release, you can disable only by disabling Cisco TrustSec and reapplying Cisco TrustSec configurations without the **cts device-id** configuration.

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

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

Server lists
: List of servers that the client can use for future RADIUS requests (for both authentication and authorization)

Device SGT
: Security group to which the device itself belongs

Expiry timeout
: Interval that controls how often the Cisco TrustSec device should refresh its environment data

RADIUS Relay Functionality

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

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

SGT Support for Virtual Port Channel

Effective with Cisco NX-OS Release 7.2(0)D1(1), Cisco TrustSec is supported on over Virtual Port Channel (vPC) and vPC+. The following Cisco TrustSec configurations on both vPC or vPC+ peers must be consistent:

- Port-SGT configuration on all interfaces of a vPC (SGT and trust mode)
- IP-SGT configuration
- VLAN-SGT configuration
- SXP peer connections configuration
- SGT caching configuration
- AAA/RADIUS configuration
- SGACL policy configuration
- Enforcing SGACL on VLAN and VRF configuration

Note

- No warning will be generated for inconsistent configuration and no compatibility checks will be enforced.
- The vPC peer-link should be configured in trusted mode with SGT propagation enabled using the **propagate-sgt** and **policy static sgt** commands in the Cisco TrustSec manual configuration mode (after the **cts manual** command is executed).
- IP-SGT learning is not supported on fabricpath ports, but inline SGT tagging is supported on fabricpath links. If Cisco TrustSec is enabled on fabricpath ports, the **propagate-sgt** and **policy static sgt** commands must be enabled on the ports.

Binding Source Priorities

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

1. Cisco Fabric Services—Cisco TrustSec IP-SGT bindings learned on vPC peer. This is applicable only to vPC peer devices.
2. VLAN-SGT—Bindings learned from snooped ARP or DHCP packets on a VLAN that is configured with a VLAN-SGT mapping.
3. SGT-caching—IP-SGT bindings learned on a VLAN or VRF, where SGT-caching is configured.
4. SXP—Bindings learned from SXP peers.
5. Learned on interface—Bindings of authenticated hosts, which are learned through EPM and device tracking. This type of binding also includes individual hosts that are learned through ARP snooping on L2 [I]PM configured ports.
6. CLI—Address bindings configured using the IP-SGT form of the **cts role-based sgt-map** global configuration command.
7. Port ASIC—SGT bindings derived inline or directly from the port, based on CTS trusted or untrusted configuration.

Virtualization Support

Cisco TrustSec configuration and operation are local to the virtual device context (VDC). For more information on VDCs, see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide.

Prerequisites for Cisco TrustSec

Cisco TrustSec has the following prerequisites:

- You must enable the 802.1X feature before you enable the Cisco TrustSec feature. Although none of the 802.1X interface level features are available, 802.1X is required for the device to authenticate with RADIUS.

Guidelines and Limitations for Cisco TrustSec

Cisco TrustSec has the following guidelines and limitations:

- Traffic generated from any supervisor is tagged with device-SGT provided that a non-zero value is configured or downloaded and SGT propagation is enabled on the egress interface. However, even if the SGACL enforcement is enabled on the corresponding VRF or VLAN, this traffic would not be subject to SGACL enforcement, if the destination for this traffic is the next hop device.
- Cisco TrustSec stops tagging traffic when Netflow is configured on the same interface which is used for tagging. Do not configure Netflow on the same interface if the matrix does not specify that the Netflow is supported with SGT. The workaround for this issue is to remove Netflow from the interface which is used for tagging and use a different interface to send the Netflow (with no relation to the Cisco TrustSec).
- The Cisco Nexus 7000 series switch does not support multiple SGACLs for the same source and destination pair. It is recommended that the multi line single SGACL is used.

- Cisco TrustSec MACSec—The following set of requirements must be used when deploying MACSec over SP-provided pseudowire connections. These requirements help to ensure the right service, quality, or characteristics are ordered from the SP.

  The Cisco Nexus 7000 series switch supports MACSec over Point-to-Point links, including those using DWDM, as well as non-PtP links such as EoMPLS where the following conditions are met:

  - There is no re-ordering or buffering of packets on the MACSec link.
  - No additional frames can be injected to the MACSec link.
  - There must be end-to-end link event notification—if the edge device or any intermediate device loses a link then there must be notifications sent so that the user is aware of the link failure as the service will be interrupted.

- For MACsec links that have a bandwidth that is greater than or equal to 40G, multiple security associations (SCI/AN pairs) are established with each SA protocol exchange.
- Cisco TrustSec SGT supports IPv4 addressing only.
- Cisco TrustSec SGT in-line tagging is not supported over OTV, VXLAN, FCoE, or Programmable Fabric.
- SXP cannot use the management (mgmt 0) interface.
- You cannot enable Cisco TrustSec on interfaces in half-duplex mode.
- If SGACL is applied to the packets being routed through SVI, SGACL has to be enabled on all the VLANs and the VRF instance involved.
- You cannot configure both Cisco TrustSec and 802.1X on an interface; you can configure only one or the other. However, you must enable the 802.1X feature for Cisco TrustSec to use EAP-FAST authentication.
- AAA authentication and authorization for Cisco TrustSec is only supported by the Cisco Secure ACS and Cisco ISE.
- To download sgname tables or refresh the environment data, you must use the Cisco ISE Release 1.0 or a later release. The Cisco Secure ACS does not support these features.
- Cisco TrustSec supports 200,000 IP-SGT maps. This is subject to the FIB TCAM space availability on each of the modules. Note that the CLI rollback is not supported when more than 100,000 IP-SGT mappings are manually configured. For more information, see Cisco Nexus 7000 Series NX-OS Verified Scalability Guide.
- The CISCO-TRUSTSEC-SXP-MIB does not provide an instance number. The object *ctsxSxpConnInstance* does not provide the instance number of the Cisco TrustSec SXP connection. Currently this number is not maintained and cannot be displayed.
- Reloading with Cisco TrustSec configuration on the Non-default VDC triggers a syslog message. When the Cisco TrustSec enforcement is enabled on the VLANs, and if a VDC reload occurs, Cisco TrustSec attempts twice to disable the enforcement on the VLANs. On the second attempt, the following syslog message appears:

  ```
  CTS-2-RBACL_ENFORCEMENT_FAILED:Failed to disable RBACL enf on vdc reload
  ```

  This syslog message can be ignored for the VDC reload because the VLANs are deleted on reload and Cisco TrustSec also deletes the enforcement configurations for those VLANs.

- The Cisco TrustSec configuration commands are not available. The **no cts dev-id pswd dev-pswd** command is currently not supported in NX-OS software. When the **cts dev-id pass** command is configured, the command configuration can be replaced using the same command, but it cannot be deleted.
- When you change the Cisco TrustSec MACSec port mode from Cache Engine (CE) mode to FabricPath mode, CRC errors are displayed in the Cisco TrustSec MACsec link until native VLAN tagging is disabled on the FabricPath core port. Such configuration changes that occur on a Cisco TrustSec port should be flapped. However, this could cause possible traffic disruptions. In such circumstances, to avoid the display of CRC errors and traffic disruptions, perform the following steps:
  1. Disable the cache engine port while having the Cisco TrustSec MACsec enabled.
  2. Change the port mode to FabricPath mode.
  3. Disable the native VLAN tagging on the FabricPath core port.
  4. Enable the port.
- The subnet-to-SGT bindings are not expanded by default. To enable expansion, the **cts sxp mapping network-map**command must be set to a non-zero value.
- An SGT that is associated with a longer prefix is always selected even if a corresponding SGT binding exists. For example, consider the hosts 12.1.0.0/16 with the subnet-SGT binding 10 and 12.1.1.1 with IP-SGT binding 20. SGT 20 is selected for the host 12.1.1.1 even though the parent prefix SGT is 10. Similarly, if VLAN 121 is designated to the subnet 12.1.0.0/16 and configured with a VLAN-SGT binding of 30, host 12.1.1.1 will continue to have the SGT value of 20 and the host 12.1.1.2 will have an SGT value of 10, because the subnet-SGT binding is considered a longer match than a VLAN-SGT mapping.
- To enable the monitoring mode, enable the **cts role-based detailed-logging** command. You can enable or disable logging at the ACE level, as being done currently.
- Monitoring at a per-RBACL or per-ACE level is not supported.
- The monitor mode counter statistics and logging output might not match because the logging output count is rate limited, while counter statistics are directly obtained from the hardware.
- When you enable **monitor all** by using CLI, ISE, or both, the monitoring for all SGT-DGT pairs is turned on, independent of per-pair configuration.
- When you disable the monitor mode feature, the switch reverts to the default behavior. The monitored SGACLs from ISE will not be installed. All the CLI-installed SGACLS will begin to enforce or deny the policies as configured.
- The traffic hitting SGACL Access Control Entry (ACE) with the log option set is punted to the supervisor, causing network congestion in the supervisor and the packets originated from supervisor such as ping, OSPF hello, and SXP may fail leading to control plane disruption. Therefore, we recommend that you enable log option only for troubleshooting or validation purposes.
- The following guidelines and limitations are applicable for the SGACL Egress Policy Overwrite feature:
  - If overlapping RBACL exists from both the sources (CLI and ISE) for an sgt-dgt pair, the respective RBACL is programmed in to the hardware based on the configured priority. The RBACL is programmed as conventional or monitored based on the monitor mode property.
  - If RBACL exists only from a single source, irrespective of configured priority, the RBACL is programmed as conventional or monitored based on the monitor mode property.

- Irrespective of the configured priority, RBACL always get updated into the PSS. However, hardware programming is based on the priority and monitor mode property.
- SGACLs are monitored when you enable monitor mode globally and set monitor all. However, based on the install priority set by using the **cts role-based priority-static** command, either the SGACLs downloaded from ISE or the SGACLs configured by using CLI are monitored.
- When SGACL exists only from a single source, that is, either from ISE or CLI, the existing SGACL is used irrespective of the configured install priority of SGACLs.
- When you set **monitor all** by using CLI, ISE, or both, the monitoring for all SGT-DGT pairs is turned on, independent of per-pair configuration.
- Based on the set priority, the monitoring is enabled for the SGACL configured by using CLI or SGACL downloaded from ISE.
- When you disable the monitor mode feature, the switch reverts to the default behavior. The monitored SGACLs from ISE will not be installed. All the CLI-installed SGACLS will begin to enforce or deny the policies as configured.

- The following guidelines and limitations are applicable for the SGACL Egress Policy Overwrite feature:
  - Irrespective of whether SGT and DGT are known or unknown for a given network traffic, or an SGACL policy exists for a given SGT and DGT, SGACL policy enforcement disablement on an interface does bypass all SGACLs.
  - Per Interface SGACL Bypass feature is configured on an L3 physical interface as well as an L3 port-channel. However, port-channel member ports cannot be configured for this feature.
  - SGACL policy enforcement feature is removed from an interface when the IP address is removed.
  - When an L3 interface is converted to an L2 interface, the IP configuration is erased. Thereby, the SGACL policy enforcement feature is also erased for the L2 interface.
  - When you change a VRF, all L3 configurations are erased on an L3 interface. Thereby, the SGACL policy enforcement feature is also erased for the L3 interface.

- When you enable or disable the Cisco TrustSec SGT Caching feature, by default, Cisco TrustSec reprograms all the RBACLs to add or remove the log option for all the ACEs. Due to this reprogramming, the previously known statistics are deleted for a RBACL and they are not displayed in the **show cts role-based counters** command output.
- The following guidelines and limitations are applicable to SGT tagging exemption for L2 protocols feature:
  - You can exempt SGT tagging only on the following control packets by using the **no propagate-sgt l2-control** command:
    - Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP)
    - IEEE Standard 802.3 Slow Protocols such as Link Aggregation Control Protocol (LACP), Operation, Administration, and Maintenance (OAM), and Link Level Discovery Protocol (LLDP)
    - IEEE 802.1X Extensible Authentication Protocol over LAN (EAPOL)

  - Cisco Discovery Protocol, Virtual Terminal Protocol (VTP), Dynamic Trunking Protocol (DTP), Port Aggregation Protocol (PAgP), or Unidirectional Link Detection (UDLD)
  - Per VLAN Spanning Tree Plus (PVST+)
  - IEEE 802.3 Full Duplex PAUSE Frame

- If the Cisco M3 Series module has to interoperate with the Cisco F3 Series module by using the Cisco TrustSec enabled link, then enable the **no propagate-sgt l2-control** command for the Cisco M3 Series module. This ensures that the control packets are accepted by the Cisco F3 Series module.
- By default, Cisco NX-OS exempts SGT tagging for any L2 control packets for the Cisco F2e series module and Cisco F3 series module because packets are not tagged with null SGT. Therefore, Cisco F2e Series modules interoperating with Cisco F3 Series modules or Cisco F3 Series modules interoperating with another Cisco F3 Series modules work without enabling the **no propagate-sgt l2-control** command on the Cisco TrustSec enabled links.
- Currently, Cisco Nexus F3 Series modules do not support SGT tagging with regard to the following Cisco products unless these products support the SGT tagging exemption feature for Layer 2 protocols.
  - Cisco Catalyst 3000 Series Switches
  - Cisco Catalyst 4500 Series Switches
  - Cisco Catalyst 6500 Series Switches
  - Cisco 4000 Series Integrated Services Routers
  - Cisco ASR 1000 Series Routers
  - Cisco Integrated Services Router Generation 2
- This table provides information about the support for port interoperability for the Cisco TrustSec-enabled links between the Cisco Nexus modules:

Table 2: Support for port interoperability for the Cisco TrustSec-enabled links between the Cisco Nexus modules

Cisco Nexus Modules	Port Interoperability for Cisco TrustSec Enabled Link With SGT Propagation and Without MACSec	Port Interoperability for Cisco TrustSec Enabled Link Without SGT Propagation and Without MACSec	Port Interoperability for Cisco TrustSec Enabled Link With SGT Propagation and With MACSec	Port Interoperability for Cisco TrustSec Enabled Link Without SGT Propagation and With MACSec
Cisco M3 Series and Cisco F3 Series modules	Enable SGT tagging exemption on the Cisco M3 Series module port.	Interoperate by default.	Not interoperable.	Interoperate by default.

Cisco Nexus Modules	Port Interoperability for Cisco TrustSec Enabled Link With SGT Propagation and Without MACSec	Port Interoperability for Cisco TrustSec Enabled Link Without SGT Propagation and Without MACSec	Port Interoperability for Cisco TrustSec Enabled Link With SGT Propagation and With MACSec	Port Interoperability for Cisco TrustSec Enabled Link Without SGT Propagation and With MACSec
Cisco M2 Series and Cisco F3 Series modules	Not interoperable because SGT tagging exemption is not supported on Cisco M2 Series modules.	Interoperate by default.	Not interoperable.	Interoperate by default.
Cisco F3 Series and Cisco F2e Series modules	Interoperate by default.	Interoperate by default.	Interoperate by default.	Interoperate by default.
Cisco M3 Series and Cisco F2e Series modules	Interoperate by default.	Interoperate by default.	Interoperate by default.	Interoperate by default.
Cisco M2 Series and Cisco F2e Series modules	Interoperate by default.	Interoperate by default.	Interoperate by default.	Interoperate by default.
Cisco M3 Series and Cisco M2 Series modules	Interoperate by default.	Interoperate by default.	Interoperate by default.	Interoperate by default.

Default Settings for Cisco TrustSec Parameters

This table lists the default settings for Cisco TrustSec parameters.

Table 3: Default Cisco TrustSec Parameters Settings

Parameter	Default
Cisco TrustSec	Disabled
SXP	Disabled
SXP default password	None
SXP reconcile period	120 seconds (2 minutes)
SXP retry period	60 seconds (1 minute)

Parameter	Default
Caching	Disabled

Configuring Cisco TrustSec

This section provides information about the configuration tasks for Cisco TrustSec.

Enabling the Cisco TrustSec SGT Feature

You must enable both the 802.1X feature and the Cisco TrustSec feature on the Cisco NX-OS device before you can configure Cisco TrustSec.

Note You cannot disable the 802.1X feature after you enable the Cisco TrustSec feature.

SUMMARY STEPS

1. **configure terminal**
2. **feature dot1x**
3. **feature cts**
4. **exit**
5. (Optional) **show cts**
6. (Optional) **show feature**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**feature dot1x** **Example:** `switch(config)# feature dot1x`	Enables the 802.1X feature.
Step 3	**feature cts** **Example:** `switch(config)# feature cts`	Enables the Cisco TrustSec feature.
Step 4	**exit** **Example:**	Exits global configuration mode.

	Command or Action	Purpose
	`switch(config)# exit` `switch#`	
Step 5	(Optional) **show cts** **Example:** `switch# show cts`	Displays the Cisco TrustSec configuration.
Step 6	(Optional) **show feature** **Example:** `switch# show feature`	Displays the enabled status for features.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Cisco TrustSec Device Credentials

You must configure unique Cisco TrustSec credentials on each Cisco TrustSec-enabled Cisco NX-OS device in your network. Cisco TrustSec uses the password in the credentials for device authentication.

Note You must also configure the Cisco TrustSec credentials for the Cisco NX-OS device on the Cisco Secure ACS. See the documentation at:

http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-installation-and-configuration-guides-list.html

Before you begin

Ensure that you have enabled Cisco TrustSec.

SUMMARY STEPS

1. **configure terminal**
2. **cts device-id** *name* **password** *password*
3. **exit**
4. (Optional) **show cts**
5. (Optional) **show cts environment**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
Step 2	**cts device-id** *name* **password** *password* **Example:** `switch(config)# cts device-id MyDevice1 password CiscO321`	Configures a unique device ID and password. The *name* argument has a maximum length of 32 characters and is case sensitive. **Note** To remove the configuration of device ID and the password, use the **no** form of the command.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	(Optional) **show cts** **Example:** `switch# show cts`	Displays the Cisco TrustSec configuration.
Step 5	(Optional) **show cts environment** **Example:** `switch# show cts environment`	Displays the Cisco TrustSec environment data.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30

Configuring Native VLAN Tagging

Configuring Native VLAN Tagging Globally

Perform this task to configure native VLAN tagging globally.

Before you begin

Ensure that you enabled Cisco TrustSec.

SUMMARY STEPS

1. **configure terminal**
2. **vlan dot1q tag native** {**fabricpath**} **exclude control**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal`	Enters global configuration mode.
Step 2	**vlan dot1q tag native** {**fabricpath**} **exclude control** **Example:** `switch(config)# vlan do1q tag native exclude control`	Tags control and data packets as appropriate. • Use **exclude control** keyword to tag data packets only. • Use **fabricpath** keyword to tag control and data packets on fabricpath ports.

Configuring Native VLAN Tagging on an Interface

Perform this task to configure native VLAN tagging globally.

Before you begin

Ensure that you enabled Cisco TrustSec.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type slot/port*
3. **vlan dot1q tag native** {**fabricpath**} **exclude control**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *type slot/port* **Example:** `switch(config)# interface ethernet 1/4`	Specifies the interface that you want to add to a channel group, and enters the interface configuration mode.
Step 3	**vlan dot1q tag native** {**fabricpath**} **exclude control** **Example:** `switch(config-if)# vlan do1q tag native exclude control`	Tags control and data packets as appropriate. • Use **exclude control** keyword to tag data packets only. • Use **fabricpath** keyword to tag control and data packets on fabricpath ports.

Configuring AAA for Cisco TrustSec

You can use Cisco Secure ACS for Cisco TrustSec authentication. You must configure RADIUS server groups and specify the default AAA authentication and authorization methods on one of the Cisco TrustSec-enabled Cisco NX-OS devices in your network cloud. Because Cisco TrustSec supports RADIUS relay, you need to configure AAA only on a seed Cisco NX-OS device that is directly connected to a Cisco Secure ACS. For all the other Cisco TrustSec-enabled Cisco NX-OS devices, Cisco TrustSec automatically provides a private AAA server group, aaa-private-sg. The seed Cisco NX-OS devices uses the management virtual routing and forwarding (VRF) instance to communicate with the Cisco Secure ACS.

Note Only the Cisco Secure ACS supports Cisco TrustSec.

Configuring AAA on a Seed Cisco NX-OS Device in a Cisco TrustSec Network

This section describes how to configure AAA on the seed Cisco NX-OS device in your Cisco TrustSec network cloud.

Note When you configure the AAA RADIUS server group for the seed Cisco NX-OS device, you must specify a VRF instance. If you use the management VRF instance, no further configuration is necessary for the nonseed devices in the network cloud. If you use a different VRF instance, you must configure the nonseed devices with that VRF instance.

Before you begin

- Obtain the IPv4 or IPv6 address or hostname for the Cisco Secure ACS.
- Ensure that you enabled Cisco TrustSec.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **key** [**0** | **7**] *key* **pac**
3. (Optional) **show radius-server**
4. **aaa group server radius** *group-name*
5. **server** {*ipv4-address* | *ipv6-address* | *hostname*}
6. **use-vrf** *vrf-name*
7. **exit**
8. **aaa authentication dot1x default group** *group-name*
9. **aaa authorization cts default group** *group-name*
10. **exit**
11. (Optional) **show radius-server groups** [*group-name*]
12. (Optional) **show aaa authentication**
13. (Optional) **show aaa authorization**
14. (Optional) **show cts pacs**
15. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **key** [**0** | **7**] *key* **pac** **Example:** `switch(config)# radius-server host 10.10.1.1 key L1a0K2s9 pac`	Configures a RADIUS server host with a key and PAC. The *hostname* argument is alphanumeric, case sensitive, and has a maximum of 256 characters. The *key* argument is alphanumeric, case sensitive, and has a maximum length of 63 characters. The **0** option indicates that the key is in clear text. The **7** option indicates that the key is encrypted. The default is clear text.
Step 3	(Optional) **show radius-server** **Example:** `switch# show radius-server`	Displays the RADIUS server configuration.

Step 4	**aaa group server radius** *group-name*
	Example:
	`switch(config)# aaa group server radius Rad1`
	`switch(config-radius)#`
		Specifies the RADIUS server group and enters RADIUS server group configuration mode.

Step 5	**server** {*ipv4-address* | *ipv6-address* | *hostname*} **Example:** `switch(config-radius)# server 10.10.1.1`	Specifies the RADIUS server host address.
Step 6	**use-vrf** *vrf-name* **Example:** `switch(config-radius)# use-vrf management`	Specifies the management VRF instance for the AAA server group. **Note** If you use the management VRF instance, no further configuration is necessary for the nonseed devices in the network cloud. If you use a different VRF instance, you must configure the nonseed devices with that VRF instance.

Step 7	**exit**
	Example:
	`switch(config-radius)# exit`
	`switch(config)#`
		Exits RADIUS server group configuration mode.

Step 8	**aaa authentication dot1x default group** *group-name* **Example:** `switch(config)# aaa authentication dot1x default group Rad1`	Specifies the RADIUS server groups to use for 802.1X authentication.

	Command or Action	Purpose
Step 9	**aaa authorization cts default group** *group-name* **Example:** `switch(config)# aaa authentication cts default group Rad1`	Specifies the RADIUS server groups to use for Cisco TrustSec authorization.

Step 10	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 11	(Optional) **show radius-server groups** [*group-name*] **Example:** `switch# show radius-server group rad1`	Displays the RADIUS server group configuration.
Step 12	(Optional) **show aaa authentication** **Example:** `switch# show aaa authentication`	Displays the AAA authentication configuration.
Step 13	(Optional) **show aaa authorization** **Example:** `switch# show aaa authorization`	Displays the AAA authorization configuration.
Step 14	(Optional) **show cts pacs** **Example:** `switch# show cts pacs`	Displays the Cisco TrustSec PAC information.
Step 15	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30
Configuring AAA on Cisco TrustSec Nonseed Cisco NX-OS Devices , on page 36

Configuring AAA on Cisco TrustSec Nonseed Cisco NX-OS Devices

Cisco TrustSec configures an AAA server group named aaa-private-sg on the nonseed Cisco NX-OS devices in the network cloud. By default, the aaa-private-sg server group uses the management VRF instance to communicate with the Cisco Secure ACS and no further configuration is required on the nonseed Cisco NX-OS devices. However, if you choose to use a different VRF instance, you must change the aaa-private-sg on the nonseed Cisco NX-OS device to use the correct VRF instance.

Before you begin

Ensure that you enabled Cisco TrustSec.

Ensure that you have configured a seed Cisco NX-OS device in your network.

SUMMARY STEPS

1. **configure terminal**
2. **aaa group server radius aaa-private-sg**
3. **use-vrf** *vrf-name*
4. **exit**
5. (Optional) **show radius-server groups aaa-private-sg**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**aaa group server radius aaa-private-sg**
	Example:
	`switch(config)# aaa group server radius aaa-private-sg`
	`switch(config-radius)#`
		Specifies the RADIUS server group aaa-private-sg and enters RADIUS server group configuration mode.

Step 3	**use-vrf** *vrf-name* **Example:** `switch(config-radius)# use-vrf MyVRF`	Specifies the management VRF instance for the AAA server group.

Step 4	**exit**
	Example:
	`switch(config-radius)# exit`
	`switch(config)#`
		Exits RADIUS server group configuration mode.

Step 5	(Optional) **show radius-server groups aaa-private-sg** **Example:** `switch(config)# show radius-server groups aaa-private-sg`	Displays the RADIUS server group configuration for the default server group.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30
Configuring AAA on a Seed Cisco NX-OS Device in a Cisco TrustSec Network, on page 34

Configuring Cisco TrustSec Authentication, Authorization, and Data Path Security

This section provides information about the configuration tasks for Cisco TrustSec authentication, authorization, and data path security.

Cisco TrustSec Configuration Process for Cisco TrustSec Authentication and Authorization

Follow these steps to configure Cisco TrustSec authentication and authorization:

Step 1 Enable the Cisco TrustSec feature. See Enabling the Cisco TrustSec SGT Feature , on page 30.

Step 2 Enable Cisco TrustSec authentication. See Enabling Cisco TrustSec Authentication , on page 38.

Step 3 Enable 802.1X authentication for Cisco TrustSec on the interfaces.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30
Enabling Cisco TrustSec Authentication , on page 38

Enabling Cisco TrustSec Authentication

You must enable Cisco TrustSec authentication on the interfaces. By default, the data path replay protection feature is enabled and the SA protocol operating mode is GCM-encrypt.

Caution For the Cisco TrustSec authentication configuration to take effect, you must enable and disable the interface, which disrupts traffic on the interface.

Note Enabling 802.1X mode for Cisco TrustSec automatically enables authorization and SA protocol on the interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port* [- *port2*]
3. **cts dot1x**
4. (Optional) **no replay-protection**
5. (Optional) **sap modelist** {**gcm-encrypt** | **gcm-encrypt-256** | **gmac** | **no-encap** | **null**}
6. **exit**
7. **shutdown**
8. **no shutdown**
9. **exit**
10. (Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot/port*}
11. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**interface ethernet** *slot*/*port* [- *port2*]
	Example:
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		Specifies a single port or a range of ports and enters interface configuration mode.

Step 3	**cts dot1x**
	Example:
	`switch(config-if)# cts dot1x`
	`switch(config-if-cts-dot1x)#`
		Enables 802.1X authentication for Cisco TrustSec and enters Cisco TrustSec 802.1X configuration mode.

Step 4	(Optional) **no replay-protection** **Example:** `switch(config-if-cts-dot1x)# no replay-protection`	Disables replay protection. The default is enabled.
Step 5	(Optional) **sap modelist** {**gcm-encrypt** | **gcm-encrypt-256** | **gmac** | **no-encap** | **null**} **Example:** `switch(config-if-cts-dot1x)# sap modelist gcm-encrypt`	Configures the SAP operation mode on the interface. Use the **gcm-encrypt** keyword for GCM encryption. This option is the default. Use the **gcm-encrypt-256** keyword for 256-bit GCM encryption. Use the **gmac** keyword for GCM authentication only. Use the **no-encap** keyword for no encapsulation for SA protocol and no SGT insertion. Use the **null** keyword for encapsulation without authentication or encryption.

Step 6	**exit**
	Example:
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Exits Cisco TrustSec 802.1X configuration mode.

Step 7	**shutdown** **Example:** `switch(config-if)# shutdown`	Disables the interface.
Step 8	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Enables the interface and enables Cisco TrustSec authentication on the interface.

	Command or Action	Purpose

Step 9	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 10	(Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*} **Example:** `switch(config)# show cts interface all`	Displays the Cisco TrustSec configuration on the interfaces.
Step 11	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30

Configuring Data-Path Replay Protection for Cisco TrustSec on Interfaces and Port Profiles

By default, the Cisco NX-OS software enables the data-path reply protection feature. You can disable the data-path replay protection feature on the interfaces for Layer 2 Cisco TrustSec if the connecting device does not support SA protocol.

When this task is configured on a port profile, any port profile that joins the group inherits the configuration.

Caution For the data-path replay protection configuration to take effect, you must enable and disable the interface, which disrupts traffic on the interface.

Before you begin

Ensure that you enabled Cisco TrustSec authentication on the interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot*/*port* [**-** *port2*]
3. **cts dot1x**
4. **no replay-protection**
5. **exit**
6. **shutdown**
7. **no shutdown**
8. **exit**
9. (Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*}
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**interface ethernet** *slot*/*port* [- *port2*]
	Example:
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		Specifies a single port or a range of ports and enters interface configuration mode.

Step 3	**cts dot1x**
	Example:
	`switch(config-if)# cts dot1x`
	`switch(config-if-cts-dot1x)#`
		Enables 802.1X authentication for Cisco TrustSec and enters Cisco TrustSec 802.1X configuration mode.

Step 4	**no replay-protection** **Example:** `switch(config-if-cts-dot1x)# no replay-protection`	Disables data-path replay protection. The default is enabled. Use the **replay-protection** command to enable data-path replay protection on the interface.

Step 5	**exit**
	Example:
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Exits Cisco TrustSec 802.1X configuration mode.

Step 6	**shutdown** **Example:** `switch(config-if)# shutdown`	Disables the interface.
Step 7	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Enables the interface and disables the data-path reply protection feature on the interface.

Step 8	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 9	(Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*} **Example:** `switch(config)# show cts interface all`	Displays the Cisco TrustSec configuration on the interface.
Step 10	(Optional) **copy running-config startup-config** **Example:**	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	`switch(config)# copy running-config startup-config`	

Related Topics

Enabling Cisco TrustSec Authentication , on page 38

Configuring SA Protocol Operation Modes for Cisco TrustSec on Interfaces and Port Profiles

You can configure the SA protocol operation mode on the interfaces for Layer 2 Cisco TrustSec. The default SA protocol operation mode is GCM-encrypt.

When this task is configured on a port profile, any port profile that joins the group inherits the configuration.

Caution For the SA protocol operation mode configuration to take effect, you must enable and disable the interface, which disrupts traffic on the interface.

Before you begin

Ensure that you enabled Cisco TrustSec authentication on the interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot*/*port* [- *port2*]
3. **cts dot1x**
4. **sap modelist** [**gcm-encrypt** | **gcm-encrypt-256** | **gmac** | **no-encap** | **null**]
5. **exit**
6. **shutdown**
7. **no shutdown**
8. **exit**
9. (Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*}
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**interface ethernet** *slot*/*port* [- *port2*]
	Example:
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		Specifies a single interface or a range of interfaces and enters interface configuration mode.

	Command or Action	Purpose

Step 3	**cts dot1x**
	Example:
	`switch(config-if)# cts dot1x`
	`switch(config-if-cts-dot1x)#`
		Enables 802.1X authentication for Cisco TrustSec and enters Cisco TrustSec 802.1X configuration mode.

Step 4	**sap modelist** [**gcm-encrypt** | **gcm-encrypt-256** | **gmac** | **no-encap** | **null**] **Example:** `switch(config-if-cts-dot1x)# sap modelist gmac`	Configures the SA protocol authentication mode on the interface. Use the **gcm-encrypt** keyword for GCM encryption. This option is the default. Use the **gcm-encrypt-256** keyword for 256-bit GCM encryption. Use the **gmac** keyword for GCM authentication only. Use the **no-encap** keyword for no encapsulation for SA protocol on the interface and no SGT insertion. Use the **null** keyword for encapsulation without authentication or encryption for SA protocol on the interface. Only the SGT is encapsulated.

Step 5	**exit**
	Example:
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Exits Cisco TrustSec 802.1X configuration mode.

Step 6	**shutdown** **Example:** `switch(config-if)# shutdown`	Disables the interface.
Step 7	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Enables the interface and SA protocol operation mode on the interface.

Step 8	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 9	(Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*} **Example:** `switch(config)# show cts interface all`	Displays the Cisco TrustSec configuration on the interface.
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling Cisco TrustSec Authentication , on page 38

Configuring SGT Propagation for Cisco TrustSec on Interfaces and Port Profiles

The SGT propagation feature on the Layer 2 interface is enabled by default. You can disable the SGT propagation feature on an interface if the peer device connected to the interface cannot handle Cisco TrustSec packets tagged with an SGT.

When this task is configured on a port profile, any port profile that joins the group inherits the configuration.

Caution For the SGT propagation configuration to take effect, you must enable and disable the interface, which disrupts traffic on the interface.

Before you begin

Ensure that you enabled Cisco TrustSec authentication on the interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot*/*port* [**-** *port2*]
3. **cts dot1x**
4. **no propagate-sgt**
5. **exit**
6. **shutdown**
7. **no shutdown**
8. **exit**
9. (Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*}
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**interface ethernet** *slot*/*port* [**-** *port2*]
	Example:
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		Specifies a single port or a range of ports and enters interface configuration mode.

Step 3	**cts dot1x** **Example:**	Enables 802.1X authentication for Cisco TrustSec and enters Cisco TrustSec 802.1X configuration mode.

	Command or Action	Purpose
	`switch(config-if)# cts dot1x` `switch(config-if-cts-dot1x)#`	
Step 4	**no propagate-sgt** **Example:** `switch(config-if-cts-dot1x)# no propagate-sgt`	Disables SGT propagation. The default is enabled. Use the **propagate-sgt** command to enable SGT propagation on the interface.

Step 5	**exit**
	Example:
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Exits Cisco TrustSec 802.1X configuration mode.

Step 6	**shutdown** **Example:** `switch(config-if)# shutdown`	Disables the interface.
Step 7	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Enables the interface and disables the data-path reply protection feature on the interface.

Step 8	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 9	(Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*} **Example:** `switch(config)# show cts interface all`	Displays the Cisco TrustSec configuration on the interface.
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling Cisco TrustSec Authentication , on page 38

Regenerating SA Protocol Keys on an Interface

You can trigger an SA protocol exchange to generate a new set of keys and protect the data traffic flowing on an interface.

Before you begin

Ensure that you enabled Cisco TrustSec.

SUMMARY STEPS

1. **cts rekey ethernet** *slot/port*
2. (Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot/port*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**cts rekey ethernet** *slot/port* **Example:** `switch# cts rekey ethernet 2/3`	Generates the SA protocol keys for an interface.
Step 2	(Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot/port*} **Example:** `switch# show cts interface all`	Displays the Cisco TrustSec configuration on the interfaces.

Related Topics

Enabling Cisco TrustSec Authentication , on page 38

Configuring Cisco TrustSec Authentication in Manual Mode

You can manually configure Cisco TrustSec on an interface if your Cisco NX-OS device does not have access to a Cisco Secure ACS or authentication is not needed because you have the MAC address authentication bypass feature enabled. You must manually configure the interfaces on both ends of the connection.

Note You cannot enable Cisco TrustSec on interfaces in half-duplex mode. Use the **show interface** command to determine if an interface is configured for half-duplex mode.

Caution For the Cisco TrustSec manual mode configuration to take effect, you must enable and disable the interface, which disrupts traffic on the interface.

Before you begin

Ensure that you enabled Cisco TrustSec.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface slot/port*
3. **cts manual**
4. **sap pmk** {*key* [**left-zero-padded**] [**display encrypt**] | **encrypted** *encrypted_pmk* | **use-dot1x**} [**modelist** {**gcm-encrypt** |**gcm-encrypt-256** | **gmac** | **no-encap** | **null**}]
5. (Optional) **policy dynamic identity** *peer-name*

6. (Optional) **policy static sgt** *tag* [**trusted**]
7. **exit**
8. **shutdown**
9. **no shutdown**
10. **exit**
11. (Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*}
12. (Optional) **show cts sap pmk** {**all** | **interface ethernet** *slot*/*port*}
13. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**interface** *interface slot*/*port*
	Example:
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		Specifies an interface and enters interface configuration mode.

Step 3	**cts manual**
	Example:
	`switch(config-if)# cts manual`
	`switch(config-if-cts-manual)#`
		Enters Cisco TrustSec manual configuration mode.
		Note You cannot enable Cisco TrustSec on interfaces in half-duplex mode.

Step 4	**sap pmk** {*key* [**left-zero-padded**] [**display encrypt**] | **encrypted** *encrypted_pmk* | **use-dot1x**} [**modelist** {**gcm-encrypt** |**gcm-encrypt-256** | **gmac** | **no-encap** | **null**}] **Example:** `switch(config-if-cts-manual)# sap pmk fedbaa modelist gmac`	Configures the SA protocol pairwise master key (PMK) and operation mode. SA protocol is disabled by default in Cisco TrustSec manual mode. The *key* argument is a hexadecimal value with an even number of characters and a maximum length of 32 characters. Use the **left-zero-padded** keyword to pad zeros to the left of the entered string if the PMK length is less than 32 bytes. Use the **display encrypt** keyword to specify that the configured PMK be displayed in AES-encrypted format in the running configuration. Use the **encrypted** *encrypted_pmk* keyword to specify an encrypted PMK string of 64 bytes (128 hexadecimal characters). Use the **use-dot1x** keyword when the peer device does not support Cisco TrustSec 802.1X authentication or authorization but does support SA protocol data path encryption and authentication.

	Command or Action	Purpose
		The mode list configures the cipher mode for the data path encryption and authentication as follows: Use the **gcm-encrypt** keyword for GCM encryption. This option is the default. Use the **gcm-encrypt-256** keyword for GCM encryption. Use the **gmac** keyword for GCM authentication. Use the **no-encap** keyword for no encapsulation and no SGT insertion. Use the **null** keyword for encapsulation of the SGT without authentication or encryption.
Step 5	(Optional) **policy dynamic identity** *peer-name* **Example:** `switch(config-if-cts-manual)# policy dynamic identity MyDevice2`	Configures a dynamic authorization policy download. The *peer-name* argument is the Cisco TrustSec device ID for the peer device. The peer name is case sensitive. **Note** Ensure that you have configured the Cisco TrustSec credentials and AAA for Cisco TrustSec. **Note** The **policy dynamic** and **policy static** commands are mutually exclusive. Only one can be applied at a time. To change from one to the other, you must use the **no** form of the command to remove the configuration before configuring the other command.
Step 6	(Optional) **policy static sgt** *tag* [**trusted**] **Example:** `switch(config-if-cts-manual)# policy static sgt 0x2`	Configures a static authorization policy. The *tag* argument is a decimal value or a hexadecimal value in the format **0x***hhhh*. The decimal range is from 2 to 65519, and the hexadecimal range is from 0x2 to 0xffef. The **trusted** keyword indicates that traffic coming on the interface with this SGT should not have its tag overridden. **Note** The **policy dynamic** and **policy static** commands are mutually exclusive. Only one can be applied at a time. To change from one to the other, you must use the **no** form of the command to remove the configuration before configuring the other command.

Step 7	**exit**
	Example:
	`switch(config-if-cts-manual)# exit`
	`switch(config-if)#`
		Exits Cisco TrustSec manual configuration mode.

Step 8	**shutdown** **Example:** `switch(config-if)# shutdown`	Disables the interface.

	Command or Action	Purpose
Step 9	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Enables the interface and enables Cisco TrustSec authentication on the interface.

Step 10	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 11	(Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*} **Example:** `switch# show cts interface all`	Displays the Cisco TrustSec configuration for the interfaces.
Step 12	(Optional) **show cts sap pmk** {**all** | **interface ethernet** *slot*/*port*} **Example:** `switch# show cts sap pmk all`	Displays the hexadecimal value of the configured PMK for all interfaces or a specific Ethernet interface.
Step 13	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30

Configuring SGACL Policies

This section provides information about the configuration tasks for SGACL policies.

SGACL Policy Configuration Process

Follow these steps to configure Cisco TrustSec SGACL policies:

Step 1 To improve performance, globally enable SGACL batch programming.

Step 2 For Layer 2 interfaces, enable SGACL policy enforcement for the VLANs with Cisco TrustSec-enabled interfaces.

Step 3 For Layer 3 interfaces, enable SGACL policy enforcement for the VRF instances with Cisco TrustSec-enabled interfaces.

Step 4 If you are not using AAA on a Cisco Secure ACS to download the SGACL policy configuration, manually configure the SGACL mapping and policies.

Enabling SGACL Batch Programming

Perform the following task to enable batching of Security Group Access Control List (SGACL) programming.

Before you begin

Ensure that you enabled Cisco TrustSec.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **cts role-based policy batched-programming enable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	[**no**] **cts role-based policy batched-programming enable**	Enables batching of SGACL programming-related tasks. To disable SGACL batch programming after you have explicitly enabled the feature, use the **no** form of this command.

Enabling SGACL Policy Enforcement on VLANs

If you use SGACLs, you must enable SGACL policy enforcement in the VLANs that have Cisco TrustSec-enabled Layer 2 interfaces.

Note This operation cannot be performed on FCoE VLANs.

Before you begin

- Ensure that you enabled Cisco TrustSec.
- Ensure that you enabled SGACL batch programming.

SUMMARY STEPS

1. **configure terminal**
2. **vlan** *vlan-id*
3. **cts role-based enforcement**
4. **exit**
5. (Optional) **show cts role-based enable**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

Step 2	**vlan** *vlan-id*
	Example:
	`switch(config)# vlan 10`
	`switch(config-vlan)#`
		Specifies a VLAN and enters VLAN configuration mode.

Step 3	**cts role-based enforcement** **Example:** `switch(config-vlan)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on the VLAN. **Note** If you enable the cts role-based enforcement on a VLAN and no other configuration on ports, the traffic traversing through these ports are subject to (0,0) SGACL. You can either configure this SGACL statically or download it from Cisco ISE.

Step 4	**exit**
	Example:
	`switch(config-vlan)# exit`
	`switch(config)#`
		Saves the VLAN configuration and exits VLAN configuration mode.

Step 5	(Optional) **show cts role-based enable** **Example:** `switch(config)# show cts role-based enable`	Displays the Cisco TrustSec SGACL enforcement configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30

Enabling SGACL Policy Enforcement on VRF Instances

If you use SGACLs, you must enable SGACL policy enforcement in the VRF instances that have Cisco TrustSec-enabled Layer 3 interfaces.

Note You cannot enable SGACL policy enforcement on the management VRF instance.

Before you begin

- Ensure that you enabled Cisco TrustSec.
- Ensure that you enabled SGACL batch programming.

- Ensure that you enabled dynamic Address Resolution Protocol (ARP) inspection or Dynamic Host Configuration Protocol (DHCP) snooping.

SUMMARY STEPS

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **cts role-based enforcement**
4. **exit**
5. (Optional) **show cts role-based enable**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**vrf context** *vrf-name*
	Example:
	`switch(config)# vrf context MyVrf`
	`switch(config-vrf)#`
		Specifies a VRF instance and enters VRF configuration mode.

Step 3	**cts role-based enforcement** **Example:** `switch(config-vrf)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on the VRF instance.

Step 4	**exit**
	Example:
	`switch(config-vrf)# exit`
	`switch(config)#`
		Exits VRF configuration mode.

Step 5	(Optional) **show cts role-based enable** **Example:** `switch(config)# show cts role-based enable`	Displays the Cisco TrustSec SGACL enforcement configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30

Configuring SGACL Logging

Before you begin

Ensure that you have enabled Cisco TrustSec.

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Enable detailed logging for SGACLs:

switch(config)# **cts role-based detailed-logging**

Step 3 Enable detailed logging for the IP access list:

switch(config)# **[no] logging ip access-list detailed**

Step 4 (Optional) Change the default value of the logging level such that the ACLLOG SYSLOGs appear using the terminal monitor:

switch(config)# **logging level acllog 6**

Step 5 (Optional) Clear the cache every 15 seconds to limit the cache output to only recent connections:

switch(config)# **logging ip access-list cache interval 15**

Step 6 Exit global configuration mode:

switch(config)# **exit**

Step 7 Required: Display information about the detailed logging IP access list and ACE actions:

switch# **show logging ip access-list cache detail**

Step 8 (Optional) Display the running configuration for Cisco TrustSec:

switch# **show run cts**

Configuring SGACL Logging

This example shows a running configuration, followed by verification commands that display the detailed logging IP access list. The status of the monitor mode and ACE action are highlighted in the output. Replace the placeholders with relevant values for your setup.

```
configure terminal
 cts role-based detailed-logging
 logging ip access-list detailed
 logging level acllog 6
 logging ip access-list cache interval 15
.
.
.
switch(config)# sh logging ip access-list cache detail
SGT     Src IP        Dst IP     S-Port    D-Port    Src Intf      Protocol  Monitor
```

```
 ACL-Name  ACE-Number ACE-Action      ACL-Direction    ACL-Filter-Type    ACL Applied Intf
    Hits
------------------------------------------------------------------------------------------
40      4.1.1.2      3.1.1.1     0       0         Ethernet4/11 (1)ICMP    (1 )ON     ----
    -----       Deny           -----            -----              -----            0
   ---------------------------------------------------------------------------------
10      1.1.1.1      2.1.1.2     0       0         Ethernet4/46 (1)ICMP    (1 )ON     ----
    -----       Permit         -----            -----              -----            8

---------------------------------------------------------------------------------
20      2.1.1.2      1.1.1.1     0       0         Ethernet4/34 (1)ICMP    (0 )OFF    ----
    -----       Deny           -----            -----              -----            3

---------------------------------------------------------------------------------
30      3.1.1.1      4.1.1.2     0       0         Ethernet8/48 (1)ICMP    (0 )OFF    ----
    -----       Permit         -----            -----              -----            0

---------------------------------------------------------------------------------

Number of cache entries: 4
------------------------------------------------------------------------------------------
```

The following example displays detailed logging when **monitor all** is enabled:

```
switch(config)# show logging ip access-list  cache detail
SGT     Src IP        Dst IP     S-Port    D-Port    Src Intf      Protocol          Monitor
    ACL-Name  ACE-Number    ACE-Action    ACL-Direction    ACL-Filter-Type    ACL Applied
Intf    Hits
------------------------------------------------------------------------------------------
26      172.16.2.6       10.1.1.1           0       0         Ethernet6/14 (1)ICMP   (1 )ON
     ----     -----           Deny          -----            -----              -----
         20
---------------------------------------------------------------------------------

Number of cache entries: 1
------------------------------------------------------------------------------------------
```

Note In this output, the logs show Deny, but traffic is not denied when Monitor (1) ON is displayed.

The following example displays system log:

```
2016 Jan 22 10:48:47 xbow-vdc4 %$ VDC-4 %$ %ACLLOG-6-ACLLOG_FLOW_INTERVAL: Src IP: 172.16.2.6,
 Dst IP: 10.1.1.1, Src Port: 0, Dst Port: 0, Src Intf: Ethernet6/14, Protocol: "ICMP"(1),
Monitor: (1)"ON" , ACL Name: ---, ACE Action: Deny, Appl Intf: ---, Hit-count: 20
```

The following example displays the Cisco TrustSec policy:

```
switch# show cts  role-based  policy

sgt:26
dgt:101 rbacl:test(monitored)
        deny ip log

switch# show running-config  cts

!Command: show running-config cts
!Time: Fri Jan 22 11:01:54 2016

version 7.3(0)D1(1)
feature cts
```

```
cts role-based counters enable
cts role-based detailed-logging
cts role-based monitor enable
cts role-based monitor all
cts role-based sgt-map 10.1.1.1 101
cts role-based sgt-map 172.16.2.6 26
cts role-based access-list permit
  permit ip log
cts role-based access-list test
  deny ip log
cts role-based sgt 26 dgt 101 access-list test
cts role-based enforcement

logging level cts 6

switch(config)# show cts role-based counters

RBACL policy counters enabled
Counters last cleared: 01/22/2016 at 10:58:27 AM

sgt:26 dgt:101  [20]
rbacl:test(monitored)
        deny ip log     [20]

switch(config)# show system internal access-list output entries detail  module 6

Flags: F - Fragment entry  E - Port Expansion
       D - DSCP Expansion  M - ACL Expansion
       T - Cross Feature Merge Expansion

               VDC-4 VRF table 1 :
               ====================

INSTANCE 0x0
---------------

  Tcam 0 resource usage:
  ----------------------
  Label_a = 0x200
   Bank 0
   ------
     IPv4 Class
       Policies: Rbacl()
       Netflow profile: 0
       Netflow deny profile: 0
       Entries:
         [Index] Entry [Stats]
         ---------------------
  [0014:000a:000a] prec 3 permit ip 0.0.0.26/32 0.0.0.101/32  log  [0]
  [0015:000b:000b] prec 3 permit ip 0.0.0.0/0 0.0.0.0/0  log  [0]
  [0016:000c:000c] prec 3 permit ip 0.0.0.0/0 0.0.0.0/0   [0]


  L4 protocol cam entries usage: none

  No mac protocol cam entries are in use


INSTANCE 0x1
---------------

  Tcam 0 resource usage:
  ----------------------
  Label_a = 0x200
```

```
 Bank 0
 ------
   IPv4 Class
     Policies: Rbacl()
     Netflow profile: 0
     Netflow deny profile: 0
     Entries:
       [Index] Entry [Stats]
       ---------------------
[0014:000a:000a] prec 3 permit ip 0.0.0.26/32 0.0.0.101/32  log  [20]

[0015:000b:000b] prec 3 permit ip 0.0.0.0/0 0.0.0.0/0  log  [0]
[0016:000c:000c] prec 3 permit ip 0.0.0.0/0 0.0.0.0/0   [0]
```

Configuring SGACL Monitor Mode

Before you begin

- Ensure that you have enabled Cisco TrustSec.
- Ensure that you have enabled counters.

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Enable detailed logging for SGACLs:

switch(config)# **cts role-based detailed-logging**

Step 3 Depending on the requirements, perform one of the following actions:

- Enable monitoring mode for all the SGACLs:

  switch(config)# **[no] cts role-based monitor all**

- Enable monitoring for each SGT-DGT pair:

  switch(config)# **[no] cts role-based monitor permissions from** {*sgt*|**unknown**} **to** {*dgt*|**unknown**} [**ipv4**| **ipv6**]

  Monitoring is enabled for IPv4 Role-Based access control lists (RBACLs) by default. Currently, the IPv6 option is not supported.

Step 4 Required: Display the Cisco TrustSec SGACL policies and details about the monitor mode feature for each pair:

switch(config)# **show cts role-based policy**

Step 5 Required: Display the monitoring status of RBACL statistics and lists statistics for all RBACL policies:

switch(config)# **show cts role-based counters**

Note You can also use other **show** commands to display the SGACL syslogs.

Step 6 (Optional) Display the running configuration for Cisco TrustSec:

switch(config)# **show run cts**

Configuring SGACL Monitor Mode

Displaying SGACL Monitor Mode Information

This example shows a running configuration to configure the SGACL monitor mode for SGT 20 to DGT 30. Replace the placeholders with relevant values for your setup.

```
configure terminal
 cts role-based detailed-logging
 cts role-based monitor permissions from <20> to <30>
 exit
```

The following example displays the Cisco TrustSec SGACL policies and details about the monitor mode feature for each SGT-DGT pair:

```
switch(config)# sh cts role-based policy

sgt:unknown
dgt:unknown     rbacl:rbacl1
        permit ip log

sgt:10
dgt:20  rbacl:rbacl1(monitored)
        permit ip log

sgt:20
dgt:10  rbacl:rbacl2
        deny ip log

sgt:30
dgt:40  rbacl:rbacl1
        permit ip

sgt:40
dgt:30  rbacl:rbacl2(monitored)
        deny ip

sgt:any
dgt:any rbacl:rbacl1
        permit ip log
```

The following example displays the monitoring status of RBACL statistics and lists the statistics for all the RBACL policies:

```
switch(config)# sh cts role-based counters

RBACL policy counters enabled
Counters last cleared: 12/23/2015 at 01:41:46 AM

sgt:unknown dgt:unknown [0]
rbacl:rbacl1
        permit ip log   [0]

sgt:10 dgt:20   [5]
rbacl:rbacl1(monitored)
        permit ip log   [5]

sgt:20 dgt:10   [5]
rbacl:rbacl2
        deny ip log     [5]
```

```
sgt:30 dgt:40   [0]
rbacl:rbacl1
        permit ip   [0]

sgt:40 dgt:30   [0]
rbacl:rbacl2(monitored)
        deny ip     [0]

sgt:any dgt:any [0]
rbacl:rbacl1
        permit ip log   [0]
```

The following example displays a running configuration for Cisco TrustSec:

```
switch(config)# show run cts

!Command: show running-config cts
!Time: Wed Dec 23 02:01:43 2015

version 7.3(0)D1(1)
feature cts
cts role-based counters enable
cts role-based detailed-logging
cts role-based monitor enable
cts role-based sgt-map 1.1.1.1 10
cts role-based sgt-map 2.1.1.2 20
cts role-based sgt-map 3.1.1.1 30
cts role-based sgt-map 4.1.1.2 40
cts role-based access-list rbacl1
  permit ip log
cts role-based access-list rbacl2
  deny ip log
cts role-based sgt 0 dgt 0 access-list rbacl1
cts role-based sgt 10 dgt 20 access-list rbacl1
cts role-based sgt 20 dgt 10 access-list rbacl2
cts role-based sgt 30 dgt 40 access-list rbacl1
cts role-based sgt 40 dgt 30 access-list rbacl2
cts role-based sgt any dgt any access-list rbacl1
cts role-based monitor permissions from 10 to 20
cts role-based monitor permissions from 40 to 30
cts role-based enforcement
```

The following example displays the running configuration for Cisco TrustSec, that does not include the SGACL logging:

```
switch(config)# show run cts

!Command: show running-config cts
!Time: Wed Dec 23 02:01:43 2015

version 7.3(0)D1(1)
feature cts
cts role-based counters enable
cts role-based detailed-logging
cts role-based monitor enable
cts role-based sgt-map 1.1.1.1 10
cts role-based sgt-map 2.1.1.2 20
cts role-based sgt-map 3.1.1.1 30
cts role-based sgt-map 4.1.1.2 40
cts role-based access-list rbacl1
  permit ip log
cts role-based access-list rbacl2
```

```
  deny ip log
cts role-based access-list rbacl1_no_log
  permit ip
cts role-based access-list rbacl2_no_log
  deny ip
cts role-based sgt 0 dgt 0 access-list rbacl1
cts role-based sgt 10 dgt 20 access-list rbacl1
cts role-based sgt 20 dgt 10 access-list rbacl2
cts role-based sgt 30 dgt 40 access-list rbacl1_no_log
cts role-based sgt 40 dgt 30 access-list rbacl2_no_log
cts role-based sgt any dgt any access-list rbacl1
cts role-based monitor permissions from 10 to 20
cts role-based monitor permissions from 40 to 30
cts role-based enforcement
```

Manually Configuring Cisco TrustSec SGTs

You can manually configure unique Cisco TrustSec security group tags (SGTs) for the packets originating from this device.

Before you begin

Ensure that you have enabled Cisco TrustSec.

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Configure the SGT for packets sent from the device:

switch(config)# **cts sgt** *tag*

Note The *tag* argument is a decimal value or a hexadecimal value in the format **0x***hhhh*. The decimal range is from 2 to 65519, and the hexadecimal range is from 0x2 to 0xffef.

Step 3 Exit global configuration mode:

switch(config)# **exit**

Step 4 (Optional) Display the Cisco TrustSec environment data information:

switch# **show cts environment-data**

Step 5 (Optional) Copy the running configuration to the startup configuration:

switch# **copy running-config startup-config**

Manually Configuring IPv4-Address-to-SGACL SGT Mapping for a VLAN

You can manually configure an IPv4 address to SGACL SGT mapping on a VLAN if you do not have Cisco Secure ACS, dynamic ARP inspection, or DHCP snooping available on your Cisco NX-OS device.

Before you begin

- Ensure that you enabled Cisco TrustSec.

- Ensure that you enabled SGACL policy enforcement on the VLAN.

SUMMARY STEPS

1. **configure terminal**
2. **vlan** *vlan-id*
3. **cts role-based sgt-map** *ipv4-address tag*
4. **exit**
5. (Optional) **show cts role-based sgt-map** [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**vlan** *vlan-id*
	Example:
	`switch(config)# vlan 10`
	`switch(config-vlan)#`
		Specifies a VLAN and enters VLAN configuration mode.

Step 3	**cts role-based sgt-map** *ipv4-address tag* **Example:** `switch(config-vlan)# cts role-based sgt-map 10.10.1.1 100`	Configures SGT mapping for the SGACL policies for the VLAN.

Step 4	**exit**
	Example:
	`switch(config-vlan)# exit`
	`switch(config)#`
		Saves the VLAN configuration and exits VLAN configuration mode.

Step 5	(Optional) **show cts role-based sgt-map** [**summary**	**sxp peer** *peer-ipv4-addr*	**vlan** *vlan-id*	**vrf** *vrf-name*] **Example:** `switch(config)# show cts role-based sgt-map`	Displays the Cisco TrustSec SGACL SGT mapping configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30
Enabling SGACL Policy Enforcement on VLANs , on page 50

Enabling SGACL Policy Enforcement on VRF Instances, on page 51

Manually Configuring IPv4-Address-to-SGACL SGT Mapping for a VRF Instance

You can manually configure IPv4-address-to-SGACL SGT mapping on a VRF instance if a Cisco Secure ACS is not available to download the SGACL policy configuration. You can use this feature if you do not have Cisco Secure ACS, dynamic ARP inspection, or DHCP snooping available on your Cisco NX-OS device.

Before you begin

- Ensure that you enabled Cisco TrustSec.
- Ensure that you enabled SGACL policy enforcement on the VRF instance.
- Ensure that the Layer-3 module is enabled.

SUMMARY STEPS

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **cts role-based sgt-map** *ipv4-address tag*
4. **exit**
5. (Optional) **show cts role-based sgt-map** [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**vrf context** *vrf-name*
	Example:
	`switch(config)# vrf context accounting`
	`switch(config-vrf)#`
		Specifies a VRF instance and enters VRF configuration mode.

Step 3	**cts role-based sgt-map** *ipv4-address tag* **Example:** `switch(config-vrf)# cts role-based sgt-map 10.10.1.1 100`	Configures SGT mapping for the SGACL policies for the VLAN.

Step 4	**exit**
	Example:
	`switch(config-vrf)# exit`
	`switch(config)#`
		Exits VRF configuration mode.

	Command or Action	Purpose
Step 5	(Optional) **show cts role-based sgt-map** [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*] **Example:** `switch(config)# show cts role-based sgt-map`	Displays the Cisco TrustSec SGACL SGT mapping configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring VLAN to SGT Mapping

You can map VLANs to SGTs. This procedure is useful for deploying Cisco TrustSec for devices that are VLAN capable but not SGT capable. A host or server can be assigned an SGT based on the assigned VLAN, and any traffic from the VLAN would be marked with the given SGT.

Before you begin

Ensure that you enabled Cisco TrustSec.

SUMMARY STEPS

1. **configure terminal**
2. **vlan** *vlan-id*
3. **cts role-based sgt** *sgt-value*
4. **exit**
5. (Optional) **show cts role-based sgt vlan** {**all** | *vlan-id*}
6. (Optional) **show cts role-based sgt-map** [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*]
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**vlan** *vlan-id*
	Example:
	`switch(config)# vlan 10`
	`switch(config-vlan)#`
		Specifies a VLAN and enters VLAN configuration mode.

Step 3	**cts role-based sgt** *sgt-value* **Example:** `switch(config-vlan)# cts role-based sgt 3`	Maps the VLAN to an SGT. The *sgt-value* argument range is from 1 to 65519.

	Command or Action	Purpose

Step 4	**exit**
	Example:
	`switch(config-vlan)# exit`
	`switch(config)#`
		Saves the VLAN configuration and exits VLAN configuration mode.

Step 5	(Optional) **show cts role-based sgt vlan** {**all** | *vlan-id*} **Example:** `switch(config)# show cts role-based sgt vlan all`	Displays the configured SGT for the specified VLAN.
Step 6	(Optional) **show cts role-based sgt-map** [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*] **Example:** `switch(config)# show cts role-based sgt-map summary`	Displays the SGT mappings.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Manually Configuring SGACL Policies

You can manually configure SGACL policies on your Cisco NX-OS device if a Cisco Secure ACS is not available to download the SGACL policy configuration.

Before you begin

Ensure that you have enabled Cisco TrustSec.

For Cisco TrustSec logging to function, you must enable Cisco TrustSec counters or statistics.

Ensure that you have enabled SGACL policy enforcement on the VLAN and VRF instance.

SUMMARY STEPS

1. **configure terminal**
2. **cts role-based access-list** *list-name*
3. (Optional) {**deny** | **permit**} **all**
4. (Optional) {**deny** | **permit**} **icmp**
5. (Optional) {**deny** | **permit**} **igmp**
6. (Optional) {**deny** | **permit**} **ip**
7. (Optional) {**deny** | **permit**} **tcp** [{**dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}]
8. {**deny** | **permit**} **udp** [{**dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}]
9. **exit**
10. **cts role-based sgt** {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **any** | **unknown**} **access-list** *list-name*
11. (Optional) **show cts role-based access-list**
12. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**cts role-based access-list** *list-name*
	Example:
	`switch(config)# cts role-based access-list MySGACL`
	`switch(config-rbacl)#`
		Specifies an SGACL and enters role-based access list configuration mode. The *list-name* argument value is alphanumeric, case sensitive, and has a maximum length of 32 characters.

Step 3	(Optional) {**deny** | **permit**} **all** **Example:** `switch(config-rbacl)# deny all`	Denies or permits all traffic.
Step 4	(Optional) {**deny** | **permit**} **icmp** **Example:** `switch(config-rbacl)# permit icmp`	Denies or permits Internet Control Message Protocol (ICMP) traffic.
Step 5	(Optional) {**deny** | **permit**} **igmp** **Example:** `switch(config-rbacl)# deny igmp`	Denies or permits Internet Group Management Protocol (IGMP) traffic.
Step 6	(Optional) {**deny** | **permit**} **ip** **Example:** `switch(config-rbacl)# permit ip`	Denies or permits IP traffic.
Step 7	(Optional) {**deny** | **permit**} **tcp** [{**dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}] **Example:** `switch(config-rbacl)# deny tcp dst eq 100`	Denies or permits TCP traffic. The default permits all TCP traffic. The range for the *port-number*, *port-number1*, and *port-number2* arguments is from 0 to 65535.
Step 8	{**deny** | **permit**} **udp** [{**dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}] **Example:** `switch(config-rbacl)# permit udp src eq 1312`	Denies or permits UDP traffic. The default permits all UDP traffic. The range for the *port-number*, *port-number1*, and *port-number2* arguments is from 0 to 65535.

Step 9	**exit**
	Example:
	`switch(config-rbacl)# exit`
	`switch(config)#`
		Exits role-based access-list configuration mode.

Step 10	**cts role-based sgt** {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **any** | **unknown**} **access-list** *list-name* **Example:**	Maps the SGT values to the SGACL. The *sgt-value* and *dgt-value* argument values range from 0 to 65520.

	Command or Action	Purpose
	`switch(config)# cts role-based sgt 3 dgt 10 access-list MySGACL`	**Note** You must create the SGACL before you can map SGTs to it.
Step 11	(Optional) **show cts role-based access-list** **Example:** `switch(config)# show cts role-based access-list`	Displays the Cisco TrustSec SGACL configuration.
Step 12	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30
Enabling SGACL Policy Enforcement on VLANs , on page 50
Enabling SGACL Policy Enforcement on VRF Instances, on page 51

Displaying the Downloaded SGACL Policies

After you configure the Cisco TrustSec device credentials and AAA, you can verify the Cisco TrustSec SGACL policies downloaded from the Cisco Secure ACS. The Cisco NX-OS software downloads the SGACL policies when it learns of a new SGT through authentication and authorization on an interface, from SXP, or from manual IPv4 address to SGACL SGT mapping.

Before you begin

Ensure that you enabled Cisco TrustSec.

SUMMARY STEPS

1. **show cts role-based access-list**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show cts role-based access-list** **Example:** `switch# show cts role-based access-list`	Displays Cisco TrustSec SGACLs, both downloaded from the Cisco Secure ACS and manually configured on the Cisco NX-OS device.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30

Refreshing the Downloaded SGACL Policies

You can refresh the SGACL policies downloaded to the Cisco NX-OS device by the Cisco Secure ACS.

Before you begin

Ensure that you enabled Cisco TrustSec.

SUMMARY STEPS

1. **cts refresh role-based-policy sgt** {*sgt-value* | **any** | **unknown**}
2. (Optional) **show cts role-based policy**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**cts refresh role-based-policy sgt** {*sgt-value* | **any** | **unknown**}
	Example:
	`switch# cts refresh role-based-policy`
	Example:
	`switch# cts refresh role-based-policy sgt any`
		Refreshes the Cisco TrustSec SGACL policies from the Cisco Secure ACS.
		• **sgt**—Refreshes the egress policy for an SGT.
		• *sgt-value* —Refreshes the egress policy for a specified SGT.
		• **any**—Refreshes the egress policy for any SGT.
		• **unknown**—Refreshes the egress policy for an unknown SGT.

Step 2	(Optional) **show cts role-based policy** **Example:** `switch# show cts role-based policy`	Displays the Cisco TrustSec SGACL policies.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30

Refreshing the Environment Data

You can refresh the environment data download from the AAA server.

Before you begin

Ensure that you enabled Cisco TrustSec.

Ensure that you are using the Cisco Identity Services Engine (ISE) Release 1.0 or later releases.

SUMMARY STEPS

1. **cts refresh environment-data**
2. **show cts environment-data**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**cts refresh environment-data** **Example:** `switch# cts refresh environment-data`	Refreshes the environment data from the AAA server.
Step 2	**show cts environment-data** **Example:** `switch# show cts environment-data`	Displays the downloaded environment data pertaining to the local device. **Note** The SGT name table entries can be downloaded from the ISE.

Clearing Cisco TrustSec SGACL Policies

You can clear the Cisco TrustSec SGACL policies.

Before you begin

Ensure that you enabled Cisco TrustSec.

SUMMARY STEPS

1. (Optional) **show cts role-based policy**
2. **clear cts policy** {**all** | **peer** *device-name* | **sgt** *sgt-value*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) **show cts role-based policy** **Example:** `switch# clear cts policy all`	Displays the Cisco TrustSec RBACL policy configuration.
Step 2	**clear cts policy** {**all**	**peer** *device-name*	**sgt** *sgt-value*} **Example:** `switch# clear cts policy all`	Clears the policies for Cisco TrustSec connection information.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30

Manually Configuring SXP

You can use the SGT Exchange Protocol (SXP) to propagate the SGTs across network devices that do not have hardware support for Cisco TrustSec. This section describes how to configure Cisco TrustSec SXP on Cisco NX-OS devices in your network.

Cisco TrustSec SXP Configuration Process

Follow these steps to manually configure Cisco TrustSec SXP:

SUMMARY STEPS

1. Enable the Cisco TrustSec feature.
2. Enable SGACL policy enforcement on the VRF instance.
3. Enable Cisco TrustSec SXP.
4. Configure SXP peer connections.

DETAILED STEPS

Step 1 Enable the Cisco TrustSec feature.

Step 2 Enable SGACL policy enforcement on the VRF instance.

Step 3 Enable Cisco TrustSec SXP.

Step 4 Configure SXP peer connections.

Note You cannot use the management (mgmt 0) connection for SXP.

Related Topics

Enabling SGACL Policy Enforcement on VLANs , on page 50
Enabling SGACL Policy Enforcement on VRF Instances, on page 51
Manually Configuring IPv4-Address-to-SGACL SGT Mapping for a VLAN, on page 59
Manually Configuring SGACL Policies, on page 63
Enabling the Cisco TrustSec SGT Feature , on page 30
Enabling Cisco TrustSec SXP , on page 68
Configuring Cisco TrustSec SXP Peer Connections, on page 69

Enabling Cisco TrustSec SXP

You must enable Cisco TrustSec SXP before you can configure peer connections.

Before you begin

Ensure that you enabled Cisco TrustSec.

SUMMARY STEPS

1. **configure terminal**
2. **cts sxp enable**
3. **exit**
4. (Optional) **show cts sxp**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**cts sxp enable** **Example:** `switch(config)# cts sxp enable`	Enables SXP for Cisco TrustSec.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	(Optional) **show cts sxp** **Example:** `switch# show cts sxp`	Displays the SXP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30

Configuring Cisco TrustSec SXP Peer Connections

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

Note If the default SXP source IP address is not configured and you do not specify the SXP source address in the connection, the Cisco NX-OS software derives the SXP source IP address from existing local IP addresses. The SXP source address could be different for each TCP connection initiated from the Cisco NX-OS device.

Before you begin

Ensure that you enabled Cisco TrustSec.

Ensure that you enabled SXP.

Ensure that you enabled RBACL policy enforcement in the VRF instance.

SUMMARY STEPS

1. **configure terminal**

2. **cts sxp connection peer** *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** {**default** | **none** | **required** *password*} **mode** {**speaker** | **listener** | **local** | **peer** | **speaker**} } [**vrf** *vrf-name*]
3. **exit**
4. (Optional) **show cts sxp connections**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**cts sxp connection peer** *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** {**default** | **none** | **required** *password*} **mode** {**speaker** | **listener** | **local** | **peer** | **speaker**} } [**vrf** *vrf-name*] **Example:** `switch(config)# cts sxp connection peer 10.10.1.1 source 20.20.1.1 password default mode listener`	Configures the SXP address connection. The **source** keyword specifies the IPv4 address of the source device. The default source is IPv4 address you configured using the **cts sxp default source-ip** command. The **password** keyword specifies the password that SXP should use for the connection using the following options: • Use the **default** option to use the default SXP password that you configured using the **cts sxp default password** command. • Use the **none** option to not use a password. • Use the **required** option to use the password specified in the command. • Use the **local** keyword to use the listener as speaker and vice versa • Use the **peer** keyword to use peer device as the SXP listener. The **speaker** and **listener** keywords specify the role of the remote peer device. The **vrf** keyword specifies the VRF instance to the peer. The default is the default VRF instance. **Note** You cannot use the management (mgmt 0) interface for SXP.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

	Command or Action	Purpose
Step 4	(Optional) **show cts sxp connections** **Example:** `switch# show cts sxp connections`	Displays the SXP connections and their status.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30
Enabling Cisco TrustSec SXP , on page 68
Enabling SGACL Policy Enforcement on VRF Instances, on page 51

Configuring the Default SXP Password

By default, SXP uses no password when setting up connections. You can configure a default SXP password for the Cisco NX-OS device.

Before you begin

Ensure that you enabled Cisco TrustSec.

Ensure that you enabled SXP.

SUMMARY STEPS

1. **configure terminal**
2. **cts sxp default password** *password*
3. **exit**
4. (Optional) **show cts sxp**
5. (Optional) **show running-config cts**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**cts sxp default password** *password* **Example:** `switch(config)# cts sxp default password A2Q3d4F5`	Configures the SXP default password.

	Command or Action	Purpose

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	(Optional) **show cts sxp** **Example:** `switch# show cts sxp`	Displays the SXP configuration.
Step 5	(Optional) **show running-config cts** **Example:** `switch# show running-config cts`	Displays the SXP configuration in the running configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30
Enabling Cisco TrustSec SXP , on page 68

Configuring the Default SXP Source IPv4 Address

The Cisco NX-OS software uses the default source IPv4 address in all new TCP connections where a source IPv4 address is not specified. When you change the default source IP address, the existing SXP connections are reset and the IP-SGT bindings learned over SXP are cleared. The SXP connections, for which a source IP address has been configured, will continue to use the same IP address, while coming back up.

The SXP connections, for which a source IP address has not been configured, uses the default IP address as the source IP address. Note that for such connections, correct destination IP address configuration on the peer and the reachability to the default source IP address are the required conditions before such connections can become operational. It is recommended to ensure that these conditions are met for existing operational connections, before configuring default source IP address on a device.

Before you begin

Ensure that you enabled Cisco TrustSec.

Ensure that you enabled SXP.

SUMMARY STEPS

1. **configure terminal**
2. **cts sxp default source-ip** *src-ip-addr*
3. **exit**
4. (Optional) **show cts sxp**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**cts sxp default source-ip** *src-ip-addr* **Example:** `switch(config)# cts sxp default source-ip 10.10.3.3`	Configures the SXP default source IPv4 address.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	(Optional) **show cts sxp** **Example:** `switch# show cts sxp`	Displays the SXP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30
Enabling Cisco TrustSec SXP , on page 68

Changing the SXP Reconcile 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 reconcile period timer starts. While the SXP reconcile period timer is active, the Cisco NX-OS software retains the SGT mapping entries learned from the previous connection and removes invalid entries. The default value is 120 seconds (2 minutes). Setting the SXP reconcile period to 0 seconds disables the timer and causes all entries from the previous connection to be removed.

Before you begin

Ensure that you enabled Cisco TrustSec.

Ensure that you enabled SXP.

SUMMARY STEPS

1. **configure terminal**
2. **cts sxp reconcile-period** *seconds*
3. **exit**
4. (Optional) **show cts sxp**

5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**cts sxp reconcile-period** *seconds* **Example:** `switch(config)# cts sxp reconcile-period 180`	Changes the SXP reconcile timer period. The default value is 120 seconds (2 minutes). The range is from 0 to 64000.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	(Optional) **show cts sxp** **Example:** `switch# show cts sxp`	Displays the SXP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30
Enabling Cisco TrustSec SXP , on page 68

Changing the SXP Retry Period

The SXP retry period determines how often the Cisco NX-OS software retries an SXP connection. When an SXP connection is not successfully set up, the Cisco NX-OS software makes a new attempt to set up the connection after the SXP retry period timer expires. The default value is 60 seconds (1 minute). Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted.

Before you begin

Ensure that you enabled Cisco TrustSec.

Ensure that you enabled SXP.

SUMMARY STEPS

1. **configure terminal**
2. **cts sxp retry-period** *seconds*
3. **exit**

4. (Optional) **show cts sxp**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**cts sxp retry-period** *seconds* **Example:** `switch(config)# cts sxp retry-period 120`	Changes the SXP retry timer period. The default value is 60 seconds (1 minute). The range is from 0 to 64000.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	(Optional) **show cts sxp** **Example:** `switch# show cts sxp`	Displays the SXP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 30
Enabling Cisco TrustSec SXP , on page 68

Configuring SXPv3

Before you begin

- Ensure that you have enabled Cisco TrustSec.
- Ensure that you have enabled SXP.
- Ensure that you have configured Cisco TrustSec SXP peer connections.

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 (Optional) Expand the network limit:

switch(config)# **[no] cts sxp mapping network-map** [*num_bindings*]

Note The *num_bindings* parameter can accept a value from 0 to 65535. The value zero (0) indicates that no expansion is allowed and 65535 is the maximum expansion limit allowed. The default value is zero (0).

Step 3 Configure a subnet-SGT binding:

switch(config)# **cts role-based sgt-map** {*A.B.C.D/<0-32>*} *sgt-number*

Step 4 Required: Display the Cisco TrustSec SXP configuration details:

switch (config)# **show cts sxp**

Step 5 Required: Display the supported SXP version:

switch(config)# **show cts sxp connection**

Example: Configuring SXPv3

This example shows a running configuration, followed by verification commands that display the Cisco TrustSec SXP configuration details and the supported SXP version. Replace the placeholders with relevant values for your setup.

```
configure terminal
 cts sxp enable
 cts sxp mapping network-map <64>
 cts role-based sgt-map <10.10.10.10/29> <1032>
.
.
.
switch(config)# show cts sxp
CTS SXP Configuration:
SXP enabled
SXP retry timeout:60
SXP reconcile timeout:120
Highest supported SXP version: 3
SXP network-map limit: 64
SXP default-route-SGT transport: Enabled
Unsupported SXP version(s): 2

switch(config)# show cts sxp connection
PEER_IP_ADDR    VRF             PEER_SXP_MODE   SELF_SXP_MODE   CONNECTION STATE    VERSION
30.1.1.3        default          listener        speaker          connected           3
```

Configuring Default Route for SGT Bindings

Before you begin

- Ensure that you have enabled Cisco TrustSec.
- Ensure that you have enabled SXP.
- Ensure that you have configured Cisco TrustSec SXP peer connections.

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Required: Enable the default route for the SGT bindings:

switch(config)# **[no] cts sxp allow default-route-sgt**

Step 3 Specify the default route for the SGT bindings for a speaker:

switch(config)# **cts role-based sgt-map** {*0.0.0.0/0*} *sgt-number*

Step 4 Required: Display the Cisco TrustSec SXP configuration details:

switch(config)# **show cts sxp**

Example: Configuring a Default Route for SGT Bindings

This example shows a running configuration, followed by a verification command that displays a Cisco TrustSec SXP configuration details. Replace the placeholders with relevant values for your setup.

```
configure terminal
 cts sxp enable
 cts sxp allow default-route-sgt
 cts role-based sgt-map <0.0.0.0/0> <200>
.
.
.
switch(config)# show cts sxp
CTS SXP Configuration:
SXP enabled
SXP retry timeout:60
SXP reconcile timeout:120
Highest supported SXP version:3
Network Map expansion limit:0
Default Route SGT Propagation: Enabled
Unsupported SXP version(s):2
```

How to Configure SXPv4

Configuring the Node ID of a Network Device

Before you begin

Enable the Cisco TrustSec feature.

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Configure the node ID of a network device:

switch(config)# **cts sxp node-id** {*sxp-node-id* | **interface** *interface-type* | *ipv4-address*}

Note Use the **no** form of this command to delete a node ID.

Step 3 Exit global configuration modes:

switch(config)# **exit**

Step 4 (Optional) Display the node ID of a network device by using one of the following commands:

switch# **show cts sxp sgt-map**

switch# **show run | include node-id**

switch# **show cts sxp sgt-map detail**

Example: Configuring the Node ID of a Network Device

The following running configuration shows how to configure the node ID of a network device. Replace the placeholders with relevant values for your setup.

```
configure terminal
 cts sxp node-id <172.16.1.3>
 exit
```

The following example shows how to configure node ID as an interface.

```
switch(config)# cts sxp node-id interface ethernet 1/1
```

Note that the specified interface should have a valid IP configuration. Otherwise, you cannot configure the node ID.

The following example shows how to display the node ID.

```
switch(config)# show cts sxp sgt-map
SXP Node ID(configured):0x00006789

switch(config)# show run | include node-id
cts sxp node-id interface Eth1/1
```

Configuring the Hold-Time for the SXPv4 Protocol on a Network Device

Before you begin

Enable the Cisco TrustSec feature.

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Configure a minimum and maximum acceptable hold-time period in seconds for the listener device:

switch(config)# **cts sxp listener hold-time** *minimum-period maximum-period*

The valid range is from 1-65534 seconds. The default hold-time range for a listener is 90-180 seconds.

Note The maximum-period value must be greater than the minimum-period value.

Step 3 Configure a minimum acceptable hold-time period in seconds for the speaker device:

switch(config)# **cts sxp speaker hold-time** *minimum-period*

The valid range is 1-65534. The default hold-time for a speaker is 120 seconds.

Step 4 Exit global configuration modes:

switch(config)# **exit**

Step 5 (Optional) Display the hold-time configuration value:

switch# **show run | grep speaker**

switch# **show run | grep listener**

Example: Configuring the Hold-Time for the SXPv4 Protocol on a Network Device

The following running configuration shows how to configure the hold-time for the SXPv4 protocol on a listener device. Replace the placeholders with relevant values for your setup.

```
configure terminal
 cts sxp listener hold-time <100> <200>
 exit
```

The following running configuration shows how to configure the hold-time for the SXPv4 protocol on a speaker device. Replace the placeholders with relevant values for your setup.

```
configure terminal
 cts sxp speaker hold-time <100>
 exit
```

The following example shows how to display the hold-time configuration values.

```
switch(config)# show run | grep speaker
cts sxp speaker hold-time 456

switch(config)# show run | grep listener
cts sxp listener hold-time 20 30
```

Configuring the Hold-Time for the SXPv4 Protocol for Each Connection

The peer connection must be configured on both devices. One device is the speaker and the other is the listener. When using password protection, make sure to use the same password on both ends.

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Configure a minimum and maximum acceptable hold-time period in seconds for the listener device:

switch(config)# **cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **required** *password*} **mode [[both | local {listener | speaker} | peer {listener | speaker} | listener | speaker] hold-time** *minimum-period maximum-period*] [**vrf** *vrf-name*]]

Configures the Cisco TrustSec-SXP peer address connection.

Note A **hold-time** *maximum-period* value is required only when you use the following keywords: **peer speaker** and **local listener**. In other instances, only a **hold-time** *minimum-period* value is required.

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:

- **both** — The specified mode refers that the device is both the speaker and the listener in the bidirectional SXP connection.
- **local**—The specified mode refers to the local device.
- **peer**—The specified mode refers to the peer device.
- **listener**— Specifies that the peer device is the listener.
- **speaker**— Specifies that the peer device is the speaker.

The **hold-time** keyword allows you to specify the length of the hold-time period for the speaker or listener device. The valid range is from 0-65534 seconds. The value 0 is the global or default hold-time. You can disable the keep-alive mechanism by specifying the maximum hold-time value as 65535. If the **hold-time** option is not specified, the global hold-time value is used. However, if the global hold-time configuration is missing, the default hold-time is used.

Note A **hold-time** *maximum-period* value is required only when you use the following keywords: **peer speaker** and **local listener**. In other instances, only a **hold-time** *minimum-period* value is required.

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

You cannot use the management (mgmt 0) interface for SXP.

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

Step 3 Configure a minimum acceptable hold-time period in seconds for the speaker device:

switch(config)# **cts sxp speaker hold-time** *minimum-period*

The valid range is 1-65534. The default hold-time for a speaker is 120 seconds.

Step 4 Exit global configuration mode:

switch(config)# **exit**

Step 5 (Optional) Displays Cisco TrustSec-SXP status and connections:

switch# **show cts sxp {connections | sgt-map}** [**detail**| **vrf** *vrf-name*]

Example: Configuring the Hold-Time for the SXPv4 Protocol for Each Connection

Example: Disabling Keep-Alive Mechanism at Listener and Speaker Devices

The following running configuration shows how to configure the hold-time for the SXPv4 protocol for each connection. Replace the placeholders with relevant values for your setup.

```
configure terminal
 cts sxp connection peer <10.20.2.2> password default mode local speaker hold-time <500>
 exit
```

The following example shows how to display the hold-time for the SXPv4 protocol for a connection.

```
switch(config)# show run cts | include connection
cts sxp connection peer 1.2.3.4 source 3.4.5.6 password none mode speaker hold-time 113 314
 vrf default

switch-listener(config)# show cts sxp sgt-map detail
SXP Node ID(generated):0x14141409
IP-SGT Mappings as follows:
IPv4,SGT : <1.34.56.45/32 , 119>
Vrf      :1
Peer IP  :5.1.1.1
Status   : Active
Seq Num  : 3
Peer Seq :0b0b0b0a
IPv4,SGT : <2.3.11.0/28 , 123>
Vrf      :1
Peer IP  :5.1.1.1
Status   : Active
Seq Num  : 3
Peer Seq :0b0b0b0a,0e0e0e01
Total number of IP-SGT Mappings: 2

switch # show cts sxp connection detail

----------------------------------------------
Peer IP           :3.1.1.2
VRF               :default
PEER MODE         :speaker
Connection State  :connected
Version           :4
Node ID           :0x0e0e0e01
Capability        :UNKNOWN
Conn Hold Time    :120 seconds
```

The following example shows how to display the hold-time configuration values.

```
switch(config)# show run | grep speaker
cts sxp speaker hold-time 456

switch(config)# show run | grep listener
cts sxp listener hold-time 20 30
```

The following example shows how to disable keep-alive mechanism at listener and speaker devices by configuring maximum values for hold-time.

```
switch# configure terminal
switch(config)# cts sxp connection peer 1.2.3.4 source 3.4.5.6 password none mode speaker
hold-time 65535 65535 vrf default
switch(config)# exit

switch# configure terminal
switch(config)# cts sxp connection peer 4.5.6.7 source 6.7.8.9 password none mode listener
 hold-time 65535 vrf default
switch(config)# exit
```

Configuring Bidirectional SXP Support

Before you begin

Enable the Cisco TrustSec feature.

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Configure the Cisco TrustSec SXP peer address connection for a bidirectional SXP configuration:

switch(config)# **cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **required** *password*} **mode both** [**vrf** *vrf-name*]

Note The **both** keyword configures the bidirectional SXP configuration.

Step 3 Exit global configuration mode:

switch(config)# **exit**

Step 4 (Optional) Displays Cisco TrustSec-SXP status and connections:

switch# **show cts sxp {connections | sgt-map}** [**detail**| **vrf** *vrf-name*]

Example: Configuring Bidirectional SXP Support

The following running configuration shows how to configure bidirectional SXP support. Replace the placeholders with relevant values for your setup.

```
configure terminal
 cts sxp connection peer <3.3.3.2> source <3.3.3.1> password <none> mode both vrf <default>
Warning: The peer should also be configured as both when this peer is configured as both.
```

The following example shows how to display bidirectional SXP configuration details.

```
switch(config)# show run | include connection
cts sxp connection peer 3.3.3.2 source 3.3.3.1 password none mode both vrf default
```

The following example shows the SXP learnt SGT bindings:

```
switch(config)# show cts sxp sgt-map detail
SXP Node ID(generated):0x00000000
IP-SGT Mappings as follows:
Total number of IP-SGT Mappings: 0
```

Verifying Cisco TrustSec with SXPv4

The following table provides information about how to verify SXPv4 configuration details.

Commands	Purpose
show cts sxp sgt-map vrf *vrf-name*	Displays information about SXP connection.
show cts sxp connection	Displays detailed information about SXP connections.
show cts sxp connection detail	Displays SXP connection for the specified VRF.
show cts sxp connection vrf *vrf-name*	Displays IP address to SGT mapping.
show cts sxp sgt-map	Displays SXP learnt SGT bindings in detail.
show cts sxp sgt-map detail	Displays the SGT mapping for the specified VRF.

Configuring Subnet to SGT Mapping

Before you begin

Ensure that you have enabled Cisco TrustSec.

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Configure the subnet to SGT mapping:

switch(config)# **cts role-based sgt-map** {*ip-addr*/*prefix length*} *sgt*

Note The *sgt number* keyword pair specifies the SGT number that is to be bound to every host address in the specified subnet.

Step 3 Display all the SGT bindings:

switch(config)# **show cts role-based sgt-map**

Step 4 Exit global configuration mode:

switch(config)# **exit**

Configuring Subnet to SGT Mapping

This example shows a running configuration, followed by a verification command that displays all the SGT bindings. Replace the placeholders with relevant values for your setup.

```
configure terminal
 cts role-based sgt-map <10.10.10.8/29> <6>
.
```

```
.
.
switch(config)# show cts role-based sgt-map
IP ADDRESS                              SGT     VRF/VLAN    SGT CONFIGURATION
10.10.10.8/29                           6        vrf:1      CLI Configured
12.1.0.0/16                             10       vrf:1      CLI Configured
12.1.1.1                                20       vrf:1      CLI Configured
12.1.1.2                                30       vlan:121   CLI Configured
```

Configuring SGT Tagging Exemption for Layer 2 Protocols

Before you begin

Ensure that you have enabled Cisco TrustSec.

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Specify an interface or a port channel:

switch(config)# **interface** *interface slot/port*

switch(config)# **interface port-channel** *port-channel*

Step 3 Required: Enter Cisco TrustSec manual configuration mode:

switch(config-if)# **cts manual**

Note You cannot enable Cisco TrustSec on interfaces that are in the half-duplex mode.

Step 4 Enable SGT tagging exemption for the L2 control protocols:

switch(config-if-cts-manual)# **no propagate-sgt l2-control**

Note Use the **propagate-sgt l2-control** command to disable SGT tagging exemption for the L2 control protocols.

Step 5 Exit Cisco TrustSec manual configuration mode, interface configuration mode, and global configuration mode:

switch(config-if-cts-manual)# **exit**

switch(config-if)# **exit**

switch(config)# **exit**

Step 6 (Optional) Display the status of SGT tagging for the L2 control protocols:

switch# **show cts propagate-status**

Step 7 (Optional) Display the Cisco TrustSec information for interfaces:

switch# **show cts interface all**

Example: Configuring SGT Tagging Exemption for L2 Protocols

This running configuration shows how to enable SGT tagging exemption for the L2 protocols. Replace the *placeholders* with relevant values for your setup.

```
configure terminal
 interface <Ethernet2/27>
  cts manual
    no propagate-sgt l2-control
    exit
   exit
 exit
```

This running configuration displays the error message when you enable the SGT tagging exemption for the L2 protocols on non-supported modules:

```
configure terminal
 interface <e7/2>
  cts manual
   no propagate-sgt l2-control
ERROR: 'no propagate-sgt l2-control' is not allowed on any port of this line card type.
```

This example displays the status of the SGT tagging for the L2 control protocols on interfaces.

```
switch(config)# show cts propagate-status
Interface: Ethernet2/13
Propagate Exemption:
        Protocols: CDP, LLDP, LACP, EAPoL, BPDUs

Interface: Ethernet2/27
Propagate Exemption:
        Protocols: CDP, LLDP, LACP, EAPoL, BPDUs

switch(config)# show cts interface all
CTS Information for Interface Ethernet2/13:
    CTS is enabled, mode:   CTS_MODE_MANUAL
    IFC state:              CTS_IFC_ST_CTS_OPEN_STATE
    Authentication Status:  CTS_AUTHC_SKIPPED_CONFIG
      Peer Identity:
      Peer is:              Unknown in manual mode
      802.1X role:          CTS_ROLE_UNKNOWN
      Last Re-Authentication:
    Authorization Status:   CTS_AUTHZ_SKIPPED_CONFIG
      PEER SGT:             0
      Peer SGT assignment:  Not Trusted
    SAP Status:             CTS_SAP_SKIPPED_CONFIG
      Version:
      Configured pairwise ciphers:
      Replay protection:
      Replay protection mode:
      Selected cipher:
    Propagate SGT: Enabled
        Propagation exempted protocols: CDP, LLDP, LACP, EAPoL, BPDUs

CTS Information for Interface Ethernet2/27:
    CTS is enabled, mode:   CTS_MODE_MANUAL
    IFC state:              CTS_IFC_ST_CTS_OPEN_STATE
    Authentication Status:  CTS_AUTHC_SKIPPED_CONFIG
      Peer Identity:
      Peer is:              Unknown in manual mode
      802.1X role:          CTS_ROLE_UNKNOWN
      Last Re-Authentication:
```

```
Authorization Status:   CTS_AUTHZ_SKIPPED_CONFIG
  PEER SGT:             0
  Peer SGT assignment:  Not Trusted
SAP Status:             CTS_SAP_SKIPPED_CONFIG
  Version:
  Configured pairwise ciphers:
  Replay protection:
  Replay protection mode:
  Selected cipher:
Propagate SGT: Enabled
    Propagation exempted protocols: CDP, LLDP, LACP, EAPoL, BPDUs
```

Configuring SGACL Egress Policy Overwrite

Use this task to configure SGACL Egress Policy Overwrite feature.

Before you begin

Enable the Cisco TrustSec feature.

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Set the install priority for SGACLs:

switch(config)# **[no] cts role-based policy priority-static** *slot/ethernet*

Note By default, the SGACLs configured by using CLI have higher priority in Cisco NX-OS. Use the **no cts role-based policy priority-static** command to set the install priority for the SGACLs downloaded from ISE.

Step 3 (Optional) Refresh the SGACL policy, if you have upgraded from a release below Cisco NX-OS Release 8.0 (1):

switch(config)# **cts refresh role-based policy**

Note You need to refresh the SGACL policy, if you have set the SGACL install priority to use the SGACLs downloaded from ISE.

Step 4 Exit the global configuration mode:

switch(config)# **exit**

Step 5 (Optional) Display the Cisco TrustSec SGACL policies and their details:

switch# **show cts role-based policy [configured| downloaded| monitored]**

The following information is displayed based on the specified filter:

- **configured** – Displays the SGACLs configured by using CLI.
- **downloaded** – Displays the SGACLs downloaded from ISE.
- **monitored** – Displays the monitored SGACLs.

Step 6 (Optional) Display the monitoring status of RBACL statistics and lists statistics for all policies:

switch# **show cts role-based counters**

Example: Configuring SGACL Egress Policy Overwrite

The following running configuration shows how to set install priority for SGACLs downloaded from ISE.

```
configure terminal
  no cts role-based policy priority-static
  exit
```

The following example displays the SGACL policies.

```
switch# show cts role-based policy
sgt:unknown
dgt:unknown     rbacl:deny_ip(Downloaded,Monitored)
deny ip
sgt:101(101)
dgt:102(102)    rbacl:rb2(Configured)
deny eigrp
sgt:101(101)
dgt:102(102)    rbacl:ise_rbacl_1_ace(Downloaded)
deny gre
```

The following example displays statistics for the enforced SGACLs.

```
switch(config)# show cts role-based counters
RBACL policy counters enabled
Counters last cleared: 08/22/2016 at 09:16:07 AM
sgt:unknown dgt:unknown [0]
rbacl:deny_ip(monitored)
        deny ip [0]
sgt:unknown dgt:2000(2000)      [0]
rbacl:Deny IP(monitored)
        deny ip [0]
sgt:10(10) dgt:20(20)   [0]
rbacl:rb1(monitored)
        deny udp        [0]
        permit tcp      [0]
        deny ip         [0]
rbacl:dummy_test (monitored)
        permit icmp     [0]
        permit tcp      [0]
        permit ip log   [0]
sgt:any dgt:any [0]
rbacl:Permit IP(monitored)
        permit ip       [0]
```

Enabling SGACL Policy Enforcement Per Interface

Use this task to enable SGACL policy enforcement per interface feature.

Before you begin

Enable the Cisco TrustSec feature.

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Specify interface or port channel by entering one of the commands:

switch(config)# **interface ethernet** *slot/ethernet*

switch(config)# **interface port-channel** *channel-number*

Step 3 Enable Cisco TrustSec SGACL policy enforcement on the routed interface or port channel:

switch(config-if)# **[no] cts role-based enforcement**

Step 4 Exit interface and global configuration modes:

switch(config-if)# **exit**

switch(config)# **exit**

Step 5 (Optional) Verify that SGACL policy enforcement is disabled on interfaces:

switch# **show cts role-based disabled-interface**

Example: Disabling SGACL Policy Enforcement Per Interface

The following running configuration shows how to disable SGACL policy enforcement per interface for ethernet 1/2. Replace the placeholders with relevant values for your setup.

```
configure terminal
 interface <ethernet 1/2>
  no cts role-based enforcement
  exit
 exit
```

The following example shows how to verify that SGACL policy enforcement is disabled on interfaces.

```
switch# show cts role-based disabled-interface
    Ethernet4/5
    Ethernet4/17
```

Cisco TrustSec Support on Port-Channel Members

Before Cisco NX-OS Release 7.2(0)D1(1), configuration compatibility on port-channel member interfaces with respect to TrustSec configuration was not enforced. Also, Cisco TrustSec configuration was not allowed on port-channel interfaces.

However, from Cisco NX-OS Release 7.2(0)D1(1), TrustSec configuration compatibility on port-channel members is enforced and also Trustsec configuration on port-channel interfaces is allowed. The following sections provide more information:

Configuration Models

The following are the configuration models:

- Cisco TrustSec configuration on port-channel interfaces:

  Any Cisco TrustSec configuration performed on a port-channel interface is inherited by all its member interfaces.

- Cisco TrustSec configuration on port-channel member interfaces:

  Port-channel compatibility parameters are not allowed to be configured on port-channel member interfaces.

  Other Cisco TrustSec configurations, such as MACSec configuration, which would not result in incompatibility, are allowed on port-channel member interfaces.

- Adding new members to a port-channel:
  - Using the **channel-group** command:

    Addition of new members is accepted, if the configuration on the port-channel and that on all members are compatible; if not, the addition is rejected.

Note If Cisco TrustSec is not configured on the port-channel and the Cisco TrustSec configuration on the members being added is compatible, the addition is accepted and the port-channel inherits the compatibility parameters from the member interfaces.

  - Using the **channel-group force** command:

    If the interfaces being added are capable of supporting the port-channel configuration, they inherit the compatibility parameters from the port-channel and the addition is accepted. However, if some interfaces being added are not capable of supporting the port-channel configuration, the addition is rejected.

User Interface Updates for Cisco NX-OS Release 7.2(0)D1(1)

The following are the updates to the user interfaces after Cisco NX-OS Release 7.2(0)D1(1):

- When the **channel group** or **channel-group force** command is issued, if there is any incompatibility in the Cisco TrustSec configuration, an error message is displayed to the user pointing to the incompatible configuration.
- The **show run** and **show start** command displays the Cisco TrustSec configuration on port-channel interfaces as well along with that on physical ethernet interfaces.
- The **show cts role-based sgt-map** command displays the port-sgt learnt mappings that was learnt on the port-channel interface, if applicable.

In-Service Software Upgrades

When In-Service Software Upgrades (ISSU) is performed from a lower version that does not support this feature, as soon as the ISSU is completed, all port-channels inherit the compatibility parameters from their first configured member interface. A warning level syslog is generated for port-channels on which the configuration incompatibility is detected.

Verifying the Cisco TrustSec Configuration

To display Cisco TrustSec configuration information, use one of the following commands:

Command	Purpose
show cts	Displays Cisco TrustSec information.
show cts capability interface {**all** | **ethernet** *slot*/*port*}	Displays the Cisco TrustSec capability of all interfaces or a specific Ethernet interface.
show cts authorization entries [**interface ethernet** *slot*/*port*.*subinterface*]	Displays the peer-policy data that is downloaded and stored as part of the Cisco TrustSec authorization for all interfaces or a specific Ethernet interface.
show cts credentials	Displays Cisco TrustSec credentials for EAP-FAST.
show cts environment-data	Displays Cisco TrustSec environmental data.
show cts interface {**all** | **brief** | **ethernet** *slot*/*port*}	Displays the Cisco TrustSec configuration for the interfaces.
show cts pacs	Displays Cisco TrustSec authorization information and PACs in the device key store.
show cts role-based access-list	Displays Cisco TrustSec SGACL information.
show cts role-based enable	Displays Cisco TrustSec SGACL enforcement status.
show cts role-based policy [[**dgt** | **sgt**]{*value* | **any** | **unknown**}]	Displays Cisco TrustSec SGACL policy information for all destination security group tag (DGT) and source security group tag (SGT) pairs or for the specified DGTs or SGTs.

Command	Purpose
show cts role-based sgt-map [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name* | **cached** | **synched**]	Displays the Cisco TrustSec SGACL SGT map configuration. • **summary**—Displays a summary of the SGT mappings. • **sxp peer**—Displays the SGT map configuration for a specific SXP peer. • **vlan**—Displays the SGT map configuration for a specific VLAN. • **vrf**—Displays the SGT map configuration for a specific VRF. • **cached**—Displays SGT maps learnt via caching. • **synched**—Displays SGT maps learnt via Cisco Fabric Services synchronization.
show cts role-based sgt vlan {**all** | *vlan-id*}	Displays the configured SGT for all VLANs or a specific VLAN.
show cts server-list	Displays only the stored list of RADIUS servers available to Cisco TrustSec seed and nonseed devices.
show cts sxp [**connection** | **sgt-map**] [**vrf** *vrf-name*]	Displays Cisco TrustSec SXP information.
show running-config cts	Displays the Cisco TrustSec information in the running configuration.

Configuration Examples for Cisco TrustSec

This section provides configuration examples for Cisco TrustSec.

Example: Enabling Cisco TrustSec

The following example shows how to enable Cisco TrustSec:

```
feature dot1x
```

```
feature cts
cts device-id device1 password Cisco321
```

Example: Configuring AAA for Cisco TrustSec on a Seed Cisco NX-OS Device

The following example shows how to configure AAA for Cisco TrustSec on the seed Cisco NX-OS device:

```
radius-server host 10.10.1.1 key Cisco123 pac
aaa group server radius Rad1
  server 10.10.1.1
  use-vrf management
aaa authentication dot1x default group Rad1
aaa authorization cts default group Rad1
```

Example: Enabling Cisco TrustSec Authentication on an Interface

The following example shows how to enable Cisco TrustSec authentication with a clear text password on an interface:

```
interface ethernet 2/1
  cts dot1x
  shutdown
  no shutdown
```

Example: Configuring Cisco TrustSec Authentication in Manual Mode

The following example shows how to configure Cisco TrustSec authentication in manual mode static policy on an interface:

```
interface ethernet 2/1
  cts manual
    sap pmk abcdef modelist gmac
    policy static sgt 0x20
```

The following example shows how to configure Cisco TrustSec authentication in manual mode dynamic policy on an interface:

```
interface ethernet 2/2
  cts manual
    policy dynamic identity device2
```

The following example shows how to specify that the configured PMK be displayed in AES-encrypted format in the running configuration:

```
 interface ethernet 2/2
   cts manual
     sap pmk fedbaa display encrypt

show cts sap pmk interface ethernet 2/2
```

```
show running-config
```

Example: Configuring Cisco TrustSec Role-Based Policy Enforcement for the Default VRF Instance

The following example shows how to enable Cisco TrustSec role-based policy enforcement for the default VRF instance:

```
cts role-based enforcement
```

Example: Configuring Cisco TrustSec Role-Based Policy Enforcement for a Nondefault VRF

The following example shows how to enable Cisco TrustSec role-based policy enforcement for a nondefault VRF:

```
vrf context test
  cts role-based enforcement
```

Example: Configuring Cisco TrustSec Role-Based Policy Enforcement for a VLAN

The following example shows how to enable Cisco TrustSec role-based policy enforcement for a VLAN:

```
vlan 10
  cts role-based enforcement
```

Example: Configuring IPv4 Address to SGACL SGT Mapping for the Default VRF Instance

The following example shows how to manually configure IPv4 address to SGACL SGT mapping for Cisco TrustSec role-based policies for the default VRF instance:

```
cts role-based sgt-map 10.1.1.1 20
```

Example: Configuring IPv4 Address to SGACL SGT Mapping for a Nondefault VRF Instance

The following example shows how to manually configure IPv4 address to SGACL SGT mapping for Cisco TrustSec role-based policies for a nondefault VRF instance:

```
vrf context test
  cts role-based sgt-map 30.1.1.1 30
```

Example: Configuring IPv4 Address to SGACL SGT Mapping for a VLAN

The following example shows how to manually configure IPv4 address to SGACL SGT mapping for Cisco TrustSec role-based policies for a VLAN:

```
vlan 10
  cts role-based sgt-map 20.1.1.1 20
```

Example: Manually Configuring Cisco TrustSec SGACLs

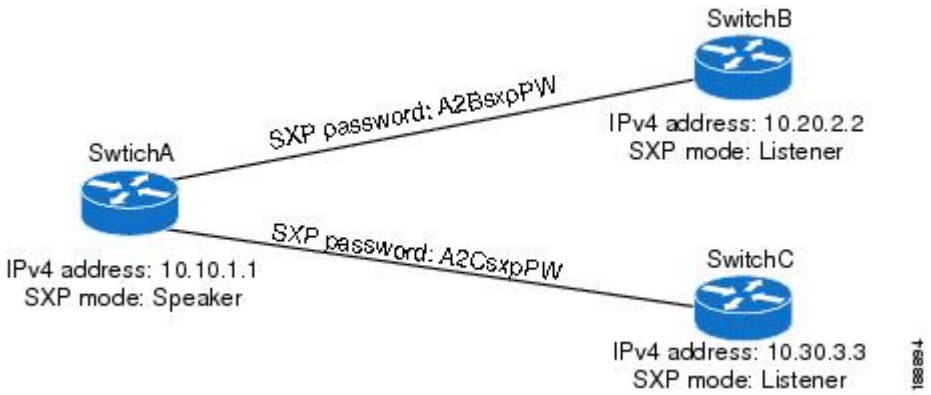
The following example shows how to manually configure Cisco TrustSec SGACLs:

```
cts role-based access-list abcd
  permit icmp
cts role-based sgt 10 dgt 20 access-list abcd
```

Example: Manually Configuring SXP Peer Connections

This figure shows an example of SXP peer connections over the default VRF instance.

Figure 11: Example SXP Peer Connections



The following example shows how to configure the SXP peer connections on SwitchA:

```
feature cts
cts role-based enforcement
cts sxp enable
cts sxp connection peer 10.20.2.2 password required A2BsxpPW mode listener
cts sxp connection peer 10.30.3.3 password required A2CsxpPW mode listener
```

The following example shows how to configure the SXP peer connection on SwitchB:

```
feature cts
cts role-based enforcement
cts sxp enable
cts sxp connection peer 10.10.1.1 password required A2BsxpPW mode speaker
```

The following example shows how to configure the SXP peer connection on SwitchC:

```
feature cts
cts role-based enforcement
cts sxp enable
cts sxp connection peer 10.10.1.1 password required A2CsxpPW mode speaker
```

Troubleshooting Cisco TrustSec

Problem: Cisco TrustSec commands fail with the following error message:

```
F: ERROR: send failed ret=-1 errno 16
```

Scenario: A VDC is shared between two different Cisco Nexus modules, such as Cisco F2E and F3 Series modules. In this setup, when you configure the IP-SGT mappings beyond the scale limit of a module, responses can be slower than usual. This slow response eventually leads to a configuration command failure, if the configured IP-SGT mappings exceed the module response rate.

Solution: To prevent the Cisco TrustSec command failure, reload the switch by performing the following task:

1. Ensure that the SGACL enforcement configuration is removed for all the VRFs or VLANs from the configuration file or the startup configuration file.
2. Reload the switch.
3. Copy the configuration file to the running configuration.
4. Enable SGACL enforcement by using the **cts role-based enforcement** command on all the required VRFs and VLANs.

Additional References for Cisco TrustSec

This sections provides additional information related to implementing Cisco TrustSec.

Related Documentation

Related Topic	Document Title
Cisco NX-OS licensing	*Cisco NX-OS Licensing Guide*
Command Reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*

Feature History for Cisco TrustSec

This table lists the release history for this feature.

Table 4: Feature History for Cisco TrustSec

Feature Name	Release	Feature Information
SGT Tagging Exemption for Layer 2 Protocols	8.1(1)	Added the functionality to exempt SGT tagging for the L2 control plane protocols. The following commands were introduced: • **no propagate-sgt l2-control** • **show cts propagate-status**
SGACL Policy Enforcement Per Interface	8.0(1)	Added the functionality to enable or disable SGACL policy enforcement on L3 physical interfaces and port-channels.
SGACL Egress Policy Overwrite	8.0(1)	Added the support for the SGACL Egress Policy Overwrite feature.
SXPv4	8.0(1)	Added the support for the SGT Exchange Protocol Version 4.
SGACL Monitoring	7.3(0)D1(1)	Added the functionality to enable monitoring of the SGACLs.
SXPv3	7.3(0)D1(1)	Added the support for the SGT Exchange Protocol Version 3.
Cisco TrustSec Subnet to SGT Mapping	7.3(0)D1(1)	Added the support for the Cisco TrustSec Subnet to SGT Mapping.
Cisco TrustSec MACsec over FabricPath on F3	7.2(1)D1(1)	Added support for Cisco TrustSec MACsec on F3 series modules on FabricPath.
Cisco TrustSec Support on Port-Channel Members	7.2(0)D1(1)	Added Cisco TrustSec Support o Port-Channel members.
Cisco TrustSec	6.2(10)	Added SGT support for F3 Series modules.
Cisco TrustSec	6.2(2)	Added the ability to map VLANs to SGTs.
Cisco TrustSec	6.2(2)	Added the ability to encrypt the SAP PMK and display the PMK in encrypted format in the running configuration.
Cisco TrustSec	6.2(2)	Added the **show cts sap pmk** command to display the hexadecimal value of the configured PMK.

Feature Name	Release	Feature Information
Cisco TrustSec	6.2(2)	Added the **show cts capability interface** command to display the Cisco TrustSec capability of interfaces.
Cisco TrustSec	6.2(2)	Enabled the **cts sgt**, **policy static sgt**, and **clear cts policy sqt** commands to accept decimal values.
Cisco TrustSec	6.2(2)	Added the ability to download sgname tables from ISE and to refresh the environment data manually and upon environment data timer expiry.
Cisco TrustSec	6.2(2)	Added optional keywords to the **show cts role-based sgt-map** command to display a summary of the SGT mappings or the SGT map configuration for a specific SXP peer, VLAN, or VRF.
Cisco TrustSec	6.2(2)	Added the **brief** keyword to the **show cts interface** command to display a brief summary for all Cisco TrustSec-enabled interfaces.
Cisco TrustSec	6.2(2)	Added SGT support for F2 and F2e Series modules.
Cisco TrustSec	6.1(1)	Removed the requirement for the Advanced Services license.
Cisco TrustSec	6.1(1)	Added MACsec support for 40G and 100G M2 Series modules.
Cisco TrustSec	6.0(1)	Updated for F2 Series modules.
Cisco TrustSec	5.2(1)	Supports pause frame encryption and decryption on interfaces.
SGACL policies	5.0(2)	Supports the enabling or disabling of RBACL logging.
SGACL policies	5.0(2)	Supports the enabling, disabling, monitoring, and clearing of RBACL statistics.
Cisco TrustSec	4.2(1)	No change from Release 4.1.