CHAPTER 10

# Configuring Cisco TrustSec

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

This chapter includes the following sections:



# Information About Cisco TrustSec

This section includes the following topics:



## Cisco TrustSec Architecture

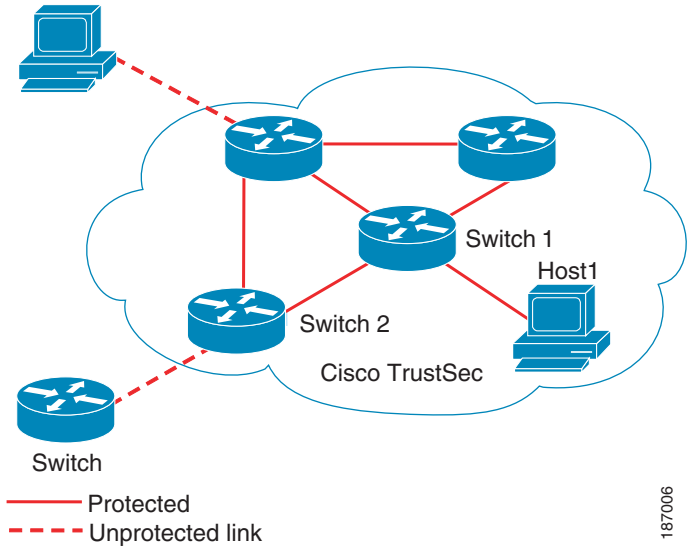
The Cisco TrustSec security architecture builds secure networks by establishing clouds of trusted network devices. Each device in the cloud is authenticated by its neighbors. Communication on the links between devices in the cloud is secured with a combination of encryption, message integrity checks,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

data-path replay protection mechanisms. Cisco TrustSec also 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 10-1 shows an example of a Cisco TrustSec cloud. In this example, several networking devices and an endpoint device are inside the Cisco TrustSec 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.

***Figure 10-1 Cisco TrustSec Network Cloud Example***




The Cisco TrustSec architecture consists of the following major components:

- Authentication—Verifies the identity of each device before allowing them to join the Cisco TrustSec network.
- Authorization—Decides the level of access to the Cisco TrustSec network resources for a device based on the authenticated identity of the device.
- Access Control—Applies access policies on 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 three entities:

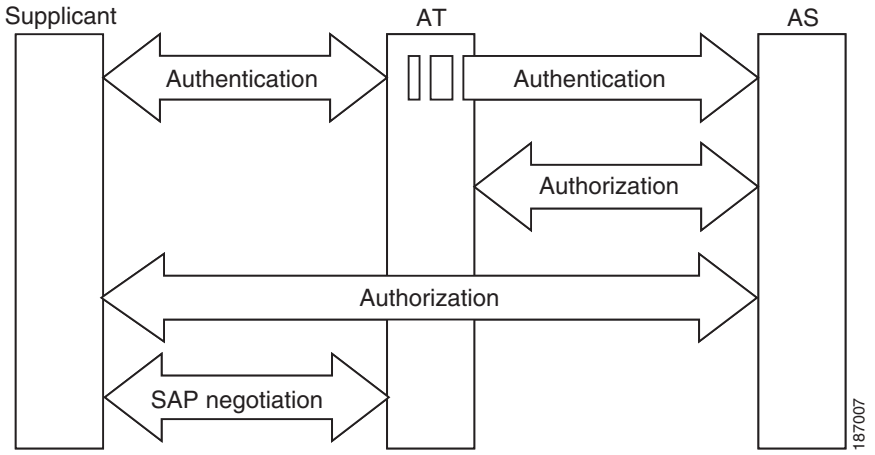
- Supplicants—Devices that attempt to join a Cisco TrustSec network.
- Authenticators (AT)—Devices that are already part of a Cisco TrustSec network.
- Authorization server—Servers that may provide authentication information, authorization information, or both.

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

1. Authentication (802.1X)—The authentication server performs the authentication of the supplicant or the authentication completes trivially if you configure the devices to unconditionally authenticate each other.
2. Authorization—Each side of the link obtains policies, such as SGT and ACLs, that to apply to the link. A supplicant may need to use the AT as a relay if it has no other Layer 3 route to the authentication server.
3. Security Association Protocol (SAP) 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).

Ports stay in unauthorized state (blocking state) until the SAP negotiation completes (see Figure 10-2).

***Figure 10-2 SAP Negotiation***




SAP 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 via Secure Tunnel (EAP-FAST) as the Extensible Authentication Protocol (EAP) method to perform the authentication.

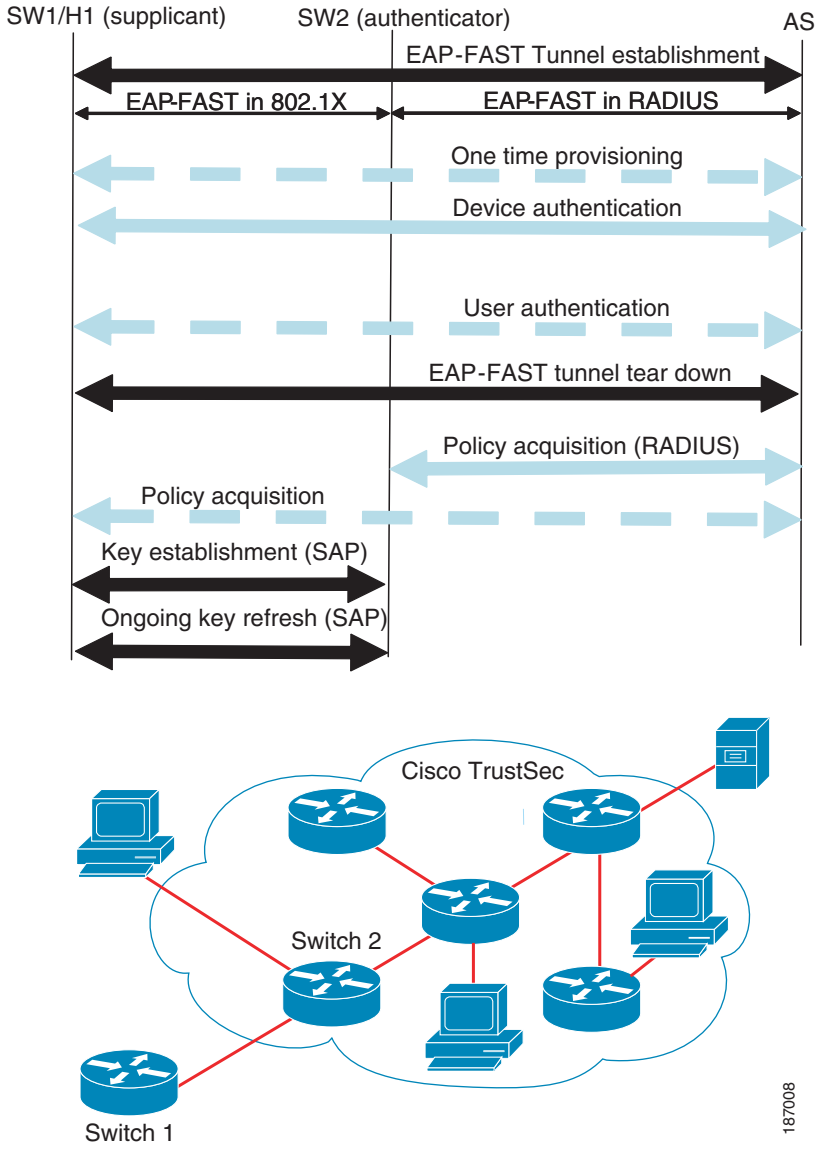
This section includes the following topics:

- Device Credentials, page 10-6
- User Credentials, page 10-6


## Cisco TrustSec and Authentication

Cisco TrustSec uses EAP-FAST for authentication. EAP-FAST conversations allow for other EAP method exchanges inside the EAP-FAST tunnel using chains. This 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 10-3 shows the EAP-FAST tunnel and inner methods as used in Cisco TrustSec.

***Figure 10-3 Cisco TrustSec Authentication***



This section includes the following topics:



### Cisco TrustSec Enhancements to EAP-FAST

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

- Authenticate the authenticator—Securely determines the identity of the 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 both 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 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, both the AT and the supplicant know following:

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

## Device Identities

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

# 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 the 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 the 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 10-4 shows an example of an SGACL policy.

***Figure 10-4 SGACL Policy Example***

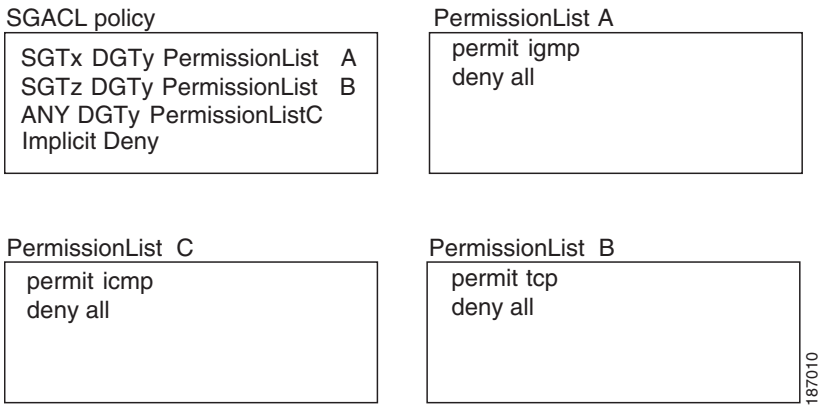
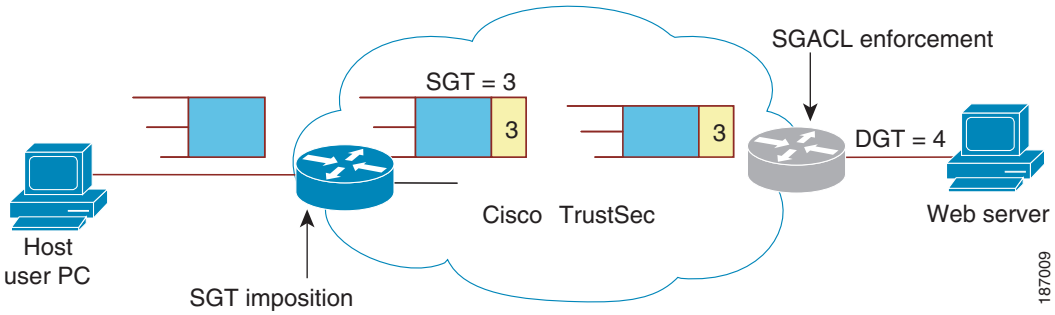



Figure 10-5 shows how the SGT assignment and the SGACL enforcement operate in a Cisco TrustSec network.

***Figure 10-5 SGT and SGACL in Cisco TrustSec Network***



The Cisco NX-OS device defines 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 greatly reduces size of ACLs and simplifies their maintenance.

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

# of ACEs = (# of sources specified) X (# of destinations specified) X (# of permissions specified)

In Cisco TrustSec uses the following formula:

# of ACEs = # of permissions specified

This section includes the following topics:



## Determining the Source Security Group

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

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

- Obtain the source SGT during policy acquisition—After Cisco TrustSec authentication phase, network device acquires policy from authentication server. Authentication server indicates whether the peer device is trusted or not. If a peer device is not trusted then the authentication server can also provide an SGT to apply to all packets coming from the peer device.
- Obtain the source SGT field from the Cisco TrustSec header—If a packet comes from a trusted peer device, the Cisco TrustSec header carries the correct SGT field. This applies to a network device which is not the first network device in Cisco TrustSec cloud for the packet.
- Look up the source SGT based on source IP Address—In some cases, you can manually configure the policy to decide the SGT of a packet based on 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 cloud determines the destination group for applying the SGACL. In some cases, ingress devices or other non-egress devices might have destination group information available. In those cases SGACLs might be applied in these devices rather than egress devices.

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

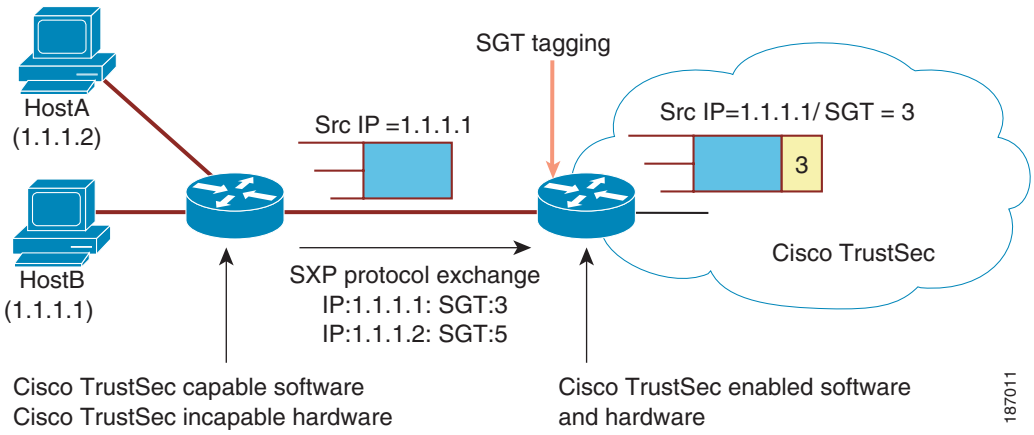
- Destination SGT of the egress port obtained during policy acquisition
- Destination SGT lookup based on the destination IP address

## 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 along with their SGTs to the distribution switches. Distribution devices with both Cisco TrustSec-enable software and hardware can use this information to tag packets appropriately and enforce SGACL policies (see Figure 10-6).

*Figure 10-6 SXP Protocol to Propagate SGT information*




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 both 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.

# Authorization and Policy Acquisition

After authentication ends, both 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 this SGT. If the device does not know if the SGACLs are associated with the peer's SGT, the device may 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 indicates 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.

# 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 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.

The device must refresh the Cisco TrustSec environment data before it expires.

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.

## 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, Release 4.1*.

# Licensing Requirements for Cisco TrustSec

The following table shows the licensing requirements for this feature:

| Product | License Requirement |
|---|---|
| Cisco NX-OS | Configuring Cisco TrustSec requires an Advanced Services license. For a complete explanation of the Cisco NX-OS licensing scheme and how to obtain and apply licenses, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.1*.<br>**Note** Cisco TrustSec licensing does not have a grace period. You must obtain and install an Advanced Services license before you can use Cisco TrustSec. |

# Prerequisites for Cisco TrustSec

Cisco TrustSec has the following prerequisites:

- You must install the Advance Service license.
- You must enable the 802.1X feature.

# Guidelines and Limitations

Cisco TrustSec has the following guidelines and limitations:

- Cisco TrustSec uses RADIUS for authentication.
- 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 Access Control Server (ACS).
- Cisco TrustSec supports IPv4 addressing only.
- SXP cannot use the management (mgmt 0) interface.
- You cannot enable Cisco TrustSec on interfaces in half-duplex mode.
- Do not perform simultaneous in-service software upgrades (ISSUs) on Cisco NX-OS devices you have connected using Cisco TrustSec. Wait until the ISSU for one device completes before you upgrade the other device.

# Configuring Cisco TrustSec

This section includes the following topics:



## Enabling the Cisco TrustSec Feature

You must enable both the 802.1X and Cisco TrustSec features 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.

### BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

### SUMMARY STEPS

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

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal**<br><br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters configuration mode. |
| Step 2 | **feature dot1x**<br><br>**Example:**<br>`switch(config)# feature dot1x` | Enables the 802.1X feature. |

| | Command | Purpose |
|---|---|---|
| Step 3 | **feature cts**<br><br>**Example:**<br>switch(config)# feature cts | Enables the Cisco TrustSec feature. |
| Step 4 | **exit**<br><br>**Example:**<br>switch(config)# exit<br>switch# | Exits configuration mode. |
| Step 5 | **show feature**<br><br>**Example:**<br>switch# show feature | (Optional) Displays the enabled status of the feature. |
| Step 6 | **copy running-config startup-config**<br><br>**Example:**<br>switch# copy running-config startup-config | (Optional) 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 *Configuration Guide for the Cisco Secure ACS*).

## BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

## SUMMARY STEPS

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

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal**<br><br>**Example:**<br>switch# configure terminal<br>switch(config)# | Enters configuration mode. |
| Step 2 | **cts device-id** *name* **password** *password*<br><br>**Example:**<br>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. |
| Step 3 | **exit**<br><br>**Example:**<br>switch(config)# exit<br>switch# | Exits configuration mode. |
| Step 4 | **show cts**<br><br>**Example:**<br>switch# show cts | (Optional) Displays the Cisco TrustSec configuration. |
| Step 5 | **copy running-config startup-config**<br><br>**Example:**<br>switch# copy running-config startup-config | (Optional) Copies the running configuration to the startup configuration. |

# 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-enable 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 VRF to communicate with the Cisco Secure ACS.

**Note** Only the Cisco Secure ACS supports Cisco TrustSec.

For more information on configuring RADIUS servers, see Chapter 3, “Configuring RADIUS.” For information on configuring RADIUS server groups, see Chapter 2, “Configuring AAA.”

This section includes the following sections:

- Configuring AAA on the Cisco TrustSec Seed Cisco NX-OS Device, page 10-15
- Configuring AAA on Cisco TrustSec Nonseed Cisco NX-OS Devices, page 10-17

## Configuring AAA on the Cisco TrustSec Seed Cisco NX-OS Device

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. If you use the management VRF, no further configuration is necessary for the nonseed devices in the network cloud. If you use a different VRF, you must configure the nonseed devices with that VRF (see the Configuring AAA on Cisco TrustSec Nonseed Cisco NX-OS Devices, page 10-17).

### BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Obtain the IPv4 or IPv6 address or hostname for the Cisco ACS.

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

### SUMMARY STEPS

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **password** *password* **pac**
3. **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. **show radius-server groups** [*group-name*]
12. **show aaa authentication**
13. **show aaa authorization**
14. **show cts pacs**
15. **copy running-config startup-config**

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>switch# configure terminal<br>switch(config)# | Enters global configuration mode. |
| **Step 2** | **radius-server host** {*ipv4-address* \| *ipv6-address* \| *hostname*} **password** *password* **pac**<br><br>**Example:**<br>switch(config)# radius-server host 10.10.1.1 password L1a0K2s9 pac | Configures a RADIUS server host with a password and PAC. |
| **Step 3** | **show radius-server**<br><br>**Example:**<br>switch# show radius-server | (Optional) Displays the RADIUS server configuration. |
| **Step 4** | **aaa group server radius** *group-name*<br><br>**Example:**<br>switch(config)# aaa group server radius Rad1<br>switch(config-radius)# | Specifies the RADIUS server group and enters RADIUS server group configuration mode. |
| **Step 5** | **server** {*ipv4-address* \| *ipv6-address* \| *hostname*}<br><br>**Example:**<br>switch(config-radius)# server 10.10.1.1 | Specifies the RADIUS server host address. |
| **Step 6** | **use-vrf** *vrf-name*<br><br>**Example:**<br>switch(config-radius)# use-vrf management | Specifies the management VRF for the AAA server group.<br>**Note** If you use the management VRF, no further configuration is necessary for the nonseed devices in the network cloud. If you use a different VRF, you must configure the nonseed devices with that VRF (see the Configuring AAA on Cisco TrustSec Nonseed Cisco NX-OS Devices, page 10-17). |
| **Step 7** | **exit**<br><br>**Example:**<br>switch(config-radius)# exit<br>switch(config)# | Exits RADIUS server group configuration mode. |
| **Step 8** | **aaa authentication dot1x default group** *group-name*<br><br>**Example:**<br>switch(config)# aaa authentication dot1x default group Rad1 | Specifies the RADIUS server groups to use for 802.1X authentication. |

| | Command | Purpose |
|---|---|---|
| Step 9 | **aaa authorization cts default group** *group-name*<br><br>**Example:**<br>switch(config)# aaa authentication cts default group Rad1 | Specifies the RADIUS server groups to use for Cisco TrustSec authorization. |
| Step 10 | **exit**<br><br>**Example:**<br>switch(config)# exit<br>switch# | Exits configuration mode. |
| Step 11 | **show radius-server groups** [*group-name*]<br><br>**Example:**<br>switch# show radius-server group rad2 | (Optional) Displays the RADIUS server group configuration. |
| Step 12 | **show aaa authentication**<br><br>**Example:**<br>switch# show aaa authentication | (Optional) Displays the AAA authentication configuration. |
| Step 13 | **show aaa authorization**<br><br>**Example:**<br>switch# show aaa authorization | (Optional) Displays the AAA authorization configuration. |
| Step 14 | **show cts pacs**<br><br>**Example:**<br>switch# show show cts pacs | (Optional) Displays the Cisco TrustSec PAC information. |
| Step 15 | **copy running-config startup-config**<br><br>**Example:**<br>switch# copy running-config startup-config | (Optional) Copies the running configuration to the startup configuration. |

## 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 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, you must change the aaa-private-sg on the nonseed Cisco NX-OS device to use the correct VRF.

### BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

Ensure that you have configured a seed Cisco NX-OS device in your network (see Configuring AAA on the Cisco TrustSec Seed Cisco NX-OS Device, page 10-15).

### SUMMARY STEPS

1. **configure terminal**
2. **aaa group server radius aaa-private-sg**

3. **use-vrf** *vrf-name*
4. **exit**
5. **show radius-server groups** [*group-name*]
6. **copy running-config startup-config**

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>switch# configure terminal<br>switch(config)# | Enters global configuration mode. |
| **Step 2** | **aaa group server radius aaa-private-sg**<br><br>**Example:**<br>switch(config)# aaa group server radius aaa-private-sg<br>switch(config-radius)# | Specifies the RADIUS server group aaa-private-sg and enters RADIUS server group configuration mode. |
| **Step 3** | **use-vrf** *vrf-name*<br><br>**Example:**<br>switch(config-radius)# use-vrf MyVRF | Specifies the management VRF for the AAA server group. |
| **Step 4** | **exit**<br><br>**Example:**<br>switch(config-radius)# exit<br>switch(config)# | Exits configuration mode. |
| **Step 5** | **show radius-server groups aaa-private-sg**<br><br>**Example:**<br>switch(config)# show radius-server groups aaa-private-sg | (Optional) Displays the RADIUS server group configuration for the default server group. |
| **Step 6** | **copy running-config startup-config**<br><br>**Example:**<br>switch(config)# copy running-config startup-config | (Optional) Copies the running configuration to the startup configuration. |

# Configuring Cisco TrustSec Authentication, Authorization, SAP, and Data Path Security

This section includes the following topics:

## 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 the "Enabling the Cisco TrustSec Feature" section on page 10-12).

**Step 2** Enable Cisco TrustSec authentication (see the "Enabling Cisco TrustSec Authentication" section on page 10-19).

**Step 3** Enable 802.1X authentication for Cisco TrustSec on the interfaces (see the "Enabling Cisco TrustSec Authentication" section on page 10-19).

## 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 SAP operating mode is GCM-encrypt.

**Caution** For the Cisco TrustSec authentication configuration to take affect, 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 SAP on the interface.

### BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

### SUMMARY STEPS

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

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>switch# configure terminal<br>switch(config)# | Enters global configuration mode. |
| **Step 2** | **interface ethernet** *slot*/*port* [**-** *port2*]<br><br>**Example:**<br>switch(config)# interface ethernet 2/2<br>switch(config-if)# | Specifies a single port or a range of ports and enters interface configuration mode. |
| **Step 3** | **cts dot1x**<br><br>**Example:**<br>switch(config-if)# cts dot1x<br>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**<br><br>**Example:**<br>switch(config-if-cts-dot1x)# no replay-protection | (Optional) Disables replay protection. The default is enabled. |
| **Step 5** | **sap modelist** {**gcm-encrypt** \| **gmac** \| **no-encap** \| **null**}<br><br>**Example:**<br>switch(config-if-cts-dot1x)# sap modelist gcm-encrypt | (Optional) Configures the SAP operation mode on the interface.<br>• **gcm-encrypt**—GCM encryption<br>• **gmac**—GCM authentication only<br>• **no-encap**— No encapsulation for SAP and no SGT insertion<br>• **null**— Encapsulation without authentication or encryption<br>The default is **gcm-encrypt**. |
| **Step 6** | **exit**<br><br>**Example:**<br>switch(config-if-cts-dot1x)# exit<br>switch(config-if)# | Exits Cisco TrustSec 802.1X configuration mode. |
| **Step 7** | **shutdown**<br><br>**Example:**<br>switch(config-if)# shutdown | Disables the interface. |
| **Step 8** | **no shutdown**<br><br>**Example:**<br>switch(config-if)# no shutdown | Enables the interface and enables Cisco TrustSec authentication on the interface. |
| **Step 9** | **exit**<br><br>**Example:**<br>switch(config-if)# exit<br>switch(config)# | Exits interface configuration mode. |

| | Command | Purpose |
|---|---|---|
| Step 10 | **show cts interface all**<br><br>**Example:**<br>switch(config)# show cts interface all | (Optional) Displays the Cisco TrustSec configuration on the interfaces. |
| Step 11 | **copy running-config startup-config**<br><br>**Example:**<br>switch(config)# copy running-config startup-config | (Optional) Copies the running configuration to the startup configuration. |

## Configuring Data-Path Replay Protection for Cisco TrustSec on Interfaces

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 SAP.

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

### BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec authentication on the interface (see the "Enabling Cisco TrustSec Authentication" section on page 10-19).

### 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. **show cts interface all**
10. **copy running-config startup-config**

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface ethernet** *slot*/*port* [**-** *port2*]<br><br>**Example:**<br>`switch(config)# interface ethernet 2/2`<br>`switch(config-if)#` | Specifies a single port or a range of ports and enters interface configuration mode. |
| **Step 3** | **cts dot1x**<br><br>**Example:**<br>`switch(config-if)# cts dot1x`<br>`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**<br><br>**Example:**<br>`switch(config-if-cts-dot1x)# no replay-protection` | Disables data-path replay protection. The default is enabled.<br><br>Use the **replay-protection** command to enable data-path replay protection on the interface. |
| **Step 5** | **exit**<br><br>**Example:**<br>`switch(config-if-cts-dot1x)# exit`<br>`switch(config-if)#` | Exits Cisco TrustSec 802.1X configuration mode. |
| **Step 6** | **shutdown**<br><br>**Example:**<br>`switch(config-if)# shutdown` | Disables the interface. |
| **Step 7** | **no shutdown**<br><br>**Example:**<br>`switch(config-if)# no shutdown` | Enables the interface and disables the data-path reply protection feature on the interface. |
| **Step 8** | **exit**<br><br>**Example:**<br>`switch(config-if)# exit`<br>`switch(config)#` | Exits interface configuration mode. |
| **Step 9** | **show cts interface all**<br><br>**Example:**<br>`switch(config)# show cts interface all` | (Optional) Displays the Cisco TrustSec configuration on the interface. |
| **Step 10** | **copy running-config startup-config**<br><br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

## Configuring SAP Operation Modes for Cisco TrustSec on Interfaces

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

**Caution** For the SAP operation mode configuration to take affect, you must enable and disable the interface which disrupts traffic on the interface.

### BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec authentication on the interface (see the "Enabling Cisco TrustSec Authentication" section on page 10-19).

### SUMMARY STEPS

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

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal**<br><br>**Example:**<br>switch# configure terminal<br>switch(config)# | Enters global configuration mode. |
| Step 2 | **interface ethernet** *slot*/*port* [**-** *port2*]<br><br>**Example:**<br>switch(config)# interface ethernet 2/2<br>switch(config-if)# | Specifies a single interface or a range of interfaces and enters interface configuration mode. |

| | Command | Purpose |
|---|---|---|
| Step 3 | **cts dot1x**<br><br>**Example:**<br>`switch(config-if)# cts dot1x`<br>`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**<br><br>**Example:**<br>`switch(config-if-cts-dot1x)# sap modelist gcm-encrypt` | Configures GCM encryption mode for SAP on the interface.<br><br>The default is **gcm-encrypt**. |
| | **sap modelist gmac**<br><br>**Example:**<br>`switch(config-if-cts-dot1x)# sap modelist gmac` | Configures GCM authentication only mode for SAP on the interface. |
| | **sap modelist no-encap**<br><br>**Example:**<br>`switch(config-if-cts-dot1x)# sap modelist no-encap` | Configures no encapsulation for SAP on the interface and does not insert an SGT. |
| | **sap modelist null**<br><br>**Example:**<br>`switch(config-if-cts-dot1x)# sap modelist null` | Configures encapsulation without authentication or encryption for SAP on the interface. Only the SGT is encapsulated. |
| Step 5 | **exit**<br><br>**Example:**<br>`switch(config-if-cts-dot1x)# exit`<br>`switch(config-if)#` | Exits Cisco TrustSec 802.1X configuration mode. |
| Step 6 | **shutdown**<br><br>**Example:**<br>`switch(config-if)# shutdown` | Disables the interface. |
| Step 7 | **no shutdown**<br><br>**Example:**<br>`switch(config-if)# no shutdown` | Enables the interface and SAP operation mode on the interface. |
| Step 8 | **exit**<br><br>**Example:**<br>`switch(config-if)# exit`<br>`switch(config)#` | Exits interface configuration mode. |
| Step 9 | **show cts interface all**<br><br>**Example:**<br>`switch(config)# show cts interface all` | (Optional) Displays the Cisco TrustSec configuration on the interface. |
| Step 10 | **copy running-config startup-config**<br><br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

## Configuring SGT Propagation for Cisco TrustSec on Interfaces

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 can not handle Cisco TrustSec packets tagged with an SGT.

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

### BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec authentication on the interface (see the "Enabling Cisco TrustSec Authentication" section on page 10-19).

### 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. **show cts interface all**
10. **copy running-config startup-config**

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface ethernet** *slot*/*port* [**-** *port2*]<br><br>**Example:**<br>`switch(config)# interface ethernet 2/2`<br>`switch(config-if)#` | Specifies a single port or a range of ports and enters interface configuration mode. |
| **Step 3** | **cts dot1x**<br><br>**Example:**<br>`switch(config-if)# cts dot1x`<br>`switch(config-if-cts-dot1x)#` | Enables 802.1X authentication for Cisco TrustSec and enters Cisco TrustSec 802.1X configuration mode. |

| | Command | Purpose |
|---|---|---|
| Step 4 | **no propagate-sgt**<br><br>**Example:**<br>`switch(config-if-cts-dot1x)# no propagate-sgt` | Disables SGT propagation. The default is enabled.<br><br>Use the **propagate-sgt** command to enable SGT propagation on the interface. |
| Step 5 | **exit**<br><br>**Example:**<br>`switch(config-if-cts-dot1x)# exit`<br>`switch(config-if)#` | Exits Cisco TrustSec 802.1X configuration mode. |
| Step 6 | **shutdown**<br><br>**Example:**<br>`switch(config-if)# shutdown` | Disables the interface. |
| Step 7 | **no shutdown**<br><br>**Example:**<br>`switch(config-if)# no shutdown` | Enables the interface and disables the data-path reply protection feature on the interface. |
| Step 8 | **exit**<br><br>**Example:**<br>`switch(config-if)# exit`<br>`switch(config)#` | Exits interface configuration mode. |
| Step 9 | **show cts interface all**<br><br>**Example:**<br>`switch(config)# show cts interface all` | (Optional) Displays the Cisco TrustSec configuration on the interface. |
| Step 10 | **copy running-config startup-config**<br><br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

## Regenerating SAP Keys on an Interface

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

### BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

### SUMMARY STEPS

1. **cts rekey ethernet** *slot*/*port*
2. **show cts interface all**

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **cts rekey ethernet** *slot/port*<br><br>**Example:**<br>switch# cts rekey ethernet 2/3 | Generates the SAP keys for an interface. |
| Step 1 | **show cts interface all**<br><br>**Example:**<br>switch# show cts interface all | (Optional) Displays Cisco TrustSec configuration on the interfaces. |

# 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 configure for half-duplex mode.

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

### BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

### SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **cts manual**
4. **sap pmk** {*key* | **use-dot1x**} [**modelist** {**gcm-encrypt** | **gmac** | **no-encap** | **null**}]
5. **policy dynamic identity** *peer-name*

   **policy static sgt** *tag* [**trusted**]
6. **exit**
7. **shutdown**
8. **no shutdown**
9. **exit**
10. **show cts interface all**

11. copy running-config startup-config

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal**<br><br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| Step 2 | **interface ethernet** *slot*/*port*<br><br>**Example:**<br>`switch(config)# interface ethernet 2/2`<br>`switch(config-if)#` | Specifies an interface and enters interface configuration mode. |
| Step 3 | **cts manual**<br><br>**Example:**<br>`switch(config-if)# cts manual`<br>`switch(config-if-cts-manual)#` | Enters Cisco TrustSec manual configuration mode.<br><br>**Note** You cannot enable Cisco TrustSec on interfaces in half-duplex mode. |
| Step 4 | **sap pmk** {*key* \| **use-dot1x**} [**modelist** {**gcm-encrypt** \| **gmac** \| **no-encap** \| **null**}]<br><br>**Example:**<br>`switch(config-if-cts-manual)# sap pmk fedbaa modelist gmac` | Configures the SAP pairwise master key (PMK) and operation mode. SAP is disabled by default in Cisco TrustSec manual mode.<br><br>The *key* argument is a hexadecimal value with an even number of characters and a maximum length of 32 characters.<br><br>Use the **use-dot1x** keyword when the peer device does not support Cisco TrustSec 802.1X authentication or authorization but does support SAP data path encryption and authentication.<br><br>The mode list configures the cipher mode for the data path encryption and authentication as follows:<br>• **gcm-encrypt**—GCM encryption mode<br>• **gmac**—GCM authentication mode<br>• **no-encap**—No encapsulation and no SGT insertion<br>• **null**— Encapsulation of the SGT without authentication or encryption<br><br>The default mode is **gcm-encrypt**. |

| | Command | Purpose |
|---|---|---|
| Step 5 | **policy dynamic identity** *peer-name*<br><br>**Example:**<br>`switch(config-if-cts-manual)# policy dynamic identity MyDevice2` | Configures dynamic authorization policy download. The *peer-name* argument is the Cisco TrustSec device ID for the peer device. The peer name is case sensitive.<br><br>**Note** Ensure that you have configured the Cisco TrustSec credentials (see "Configuring Cisco TrustSec Device Credentials" section on page 10-13) and AAA for Cisco TrustSec (see "Configuring AAA for Cisco TrustSec" section on page 10-14). |
| | **policy static sgt** *tag* [**trusted**]<br><br>**Example:**<br>`switch(config-if-cts-manual)# policy static sgt 0x03` | Configures a static authorization policy. The *tag* argument is in hexadecimal format and the range is from 0x0 to 0xffff. The **trusted** keyword indicates that traffic coming on the interface with this SGT should not have its tag overridden. |
| Step 6 | **exit**<br><br>**Example:**<br>`switch(config-if-cts-manual)# exit`<br>`switch(config-if)#` | Exits Cisco TrustSec manual configuration mode. |
| Step 7 | **shutdown**<br><br>**Example:**<br>`switch(config-if)# shutdown` | Disables the interface. |
| Step 8 | **no shutdown**<br><br>**Example:**<br>`switch(config-if)# no shutdown` | Enables the interface and enables Cisco TrustSec authentication on the interface. |
| Step 9 | **exit**<br><br>**Example:**<br>`switch(config-if)# exit`<br>`switch(config)#` | Exits interface configuration mode. |
| Step 10 | **show cts interface all**<br><br>**Example:**<br>`switch# show cts interface all` | (Optional) Displays the Cisco TrustSec configuration for the interfaces. |
| Step 11 | **copy running-config startup-config**<br><br>**Example:**<br>`switch# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

# Configuring SGACL Policies

This section includes the following topics:

## SGACL Policy Configuration Process

Follow these steps to configure Cisco TrustSec SGACL policies:

**Step 1** For Layer 2 interfaces, enable SGACL policy enforcement for the VLANs with Cisco TrustSec-enabled interfaces (see the "Enabling SGACL Policy Enforcement on VLANs" section on page 10-30).

**Step 2** For Layer 3 interfaces, enable SGACL policy enforcement for the VRFs with Cisco TrustSec-enabled interfaces (see the "Enabling SGACL Policy Enforcement on VRFs" section on page 10-31).

**Step 3** If you are not using AAA on a Cisco Secure ACS to download the SGACL policy configuration, manually configure the SGACL mapping and policies (see the "Manually Configuring IPv4-Address-to-SGACL SGT Mapping" section on page 10-33 and the "Manually Configuring SGACL Policies" section on page 10-35).

## 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.

### BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

### SUMMARY STEPS

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

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal**<br><br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters configuration mode. |
| Step 2 | **vlan** *vlan-id*<br><br>**Example:**<br>`switch(config)# vlan 10`<br>`switch(config-vlan)#` | Specifies a VLAN and enters VLAN configuration mode. |
| Step 3 | **cts role-based enforcement**<br><br>**Example:**<br>`switch(config-vlan)# cts role-based enforcement` | Enables Cisco TrustSec SGACL policy enforcement on the VLAN. |
| Step 4 | **exit**<br><br>**Example:**<br>`switch(config-vlan)# exit`<br>`switch(config)#` | Exits VLAN configuration mode. |
| Step 5 | **show cts role-based enable**<br><br>**Example:**<br>`switch(config)# show cts role-based enable` | (Optional) Displays the Cisco TrustSec SGACL enforcement configuration. |
| Step 6 | **copy running-config startup-config**<br><br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

## Enabling SGACL Policy Enforcement on VRFs

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

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

### BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

Ensure that you enabled dynamic Address Resolution Protocol (ARP) inspection (see Chapter 16, "Configuring Dynamic ARP Inspection") or Dynamic Host Configuration Protocol (DHCP) snooping (see Chapter 15, "Configuring DHCP Snooping").

### SUMMARY STEPS

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

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters configuration mode. |
| **Step 2** | **vrf context** *vrf-name*<br><br>**Example:**<br>`switch(config)# vrf context MyVrf`<br>`switch(config-vrf)#` | Specifies a VRF and enters VRF configuration mode. |
| **Step 3** | **cts role-based enforcement**<br><br>**Example:**<br>`switch(config-vrf)# cts role-based enforcement` | Enables Cisco TrustSec SGACL policy enforcement on the VRF. |
| **Step 4** | **exit**<br><br>**Example:**<br>`switch(config-vrf)# exit`<br>`switch(config)#` | Exits VRF configuration mode. |
| **Step 5** | **show cts role-based enable**<br><br>**Example:**<br>`switch(config)# show cts role-based enable` | (Optional) Displays the Cisco TrustSec SGACL enforcement configuration. |
| **Step 6** | **copy running-config startup-config**<br><br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

## Manually Configuring Cisco TrustSec SGTs

You can manually configure unique Cisco TrustSec security group tags (SGTs) for the packets subject to SGACL enforcement.

**Note** You must also configure the Cisco TrustSec credentials for the Cisco NX-OS device on the Cisco Secure ACS.

### BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

### SUMMARY STEPS

1. **configure terminal**
2. **cts sgt** *tag*
3. **exit**
4. **show cts environment-data**
5. **copy running-config startup-config**

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters configuration mode. |
| **Step 2** | **cts sgt** *tag*<br><br>**Example:**<br>`switch(config)# cts device-id MyDevice1 password CiscO321` | Configures the SGT for packets sent from the device. The *tag* argument is a hexadecimal value in the format **0x***hhhh*. The range is from 0x1 to 0xfffd. |
| **Step 3** | **exit**<br><br>**Example:**<br>`switch(config)# exit`<br>`switch#` | Exits configuration mode. |
| **Step 4** | **show cts environment-data**<br><br>**Example:**<br>`switch# show cts environment-data` | (Optional) Displays the Cisco TrustSec environment data information. |
| **Step 5** | **copy running-config startup-config**<br><br>**Example:**<br>`switch# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

## Manually Configuring IPv4-Address-to-SGACL SGT Mapping

You can manually configure IPv4 address to SGACL SGT mapping on either a VLAN or a VRF 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 are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

Ensure that you enabled SGACL policy enforcement on the VLAN (see the "Enabling SGACL Policy Enforcement on VLANs" section on page 10-30) or VRF (see the "Enabling SGACL Policy Enforcement on VRFs" section on page 10-31).

## SUMMARY STEPS

1. **configure terminal**
2. **vlan** *vlan-id*

   **vrf context** *vrf-name*
3. **cts role-based sgt-map** *ipv4-address tag*
4. **exit**
5. **show cts role-based enable**
6. **copy running-config startup-config**

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters configuration mode. |
| **Step 2** | **vlan** *vlan-id*<br><br>**Example:**<br>`switch(config)# vlan 10`<br>`switch(config-vlan)#` | Specifies a VLAN and enters VLAN configuration mode. |
| | **vrf context** *vrf-name*<br><br>**Example:**<br>`switch(config)# vrf context MyVrf`<br>`switch(config-vrf)#` | Specifies a VRF and enters VRF configuration mode. |
| **Step 3** | **cts role-based sgt-map** *ipv4-address tag*<br><br>**Example:**<br>`switch(config-vlan)# cts role-based sgt-map 10.10.1.1 100` | Configures SGT mapping for the SGACL policies for the VLAN. |
| | **cts role-based sgt-map** *ipv4-address tag*<br><br>**Example:**<br>`switch(config-vrf)# cts role-based sgt-map 10.10.1.1 100` | Configures SGT mapping for the SGACL policies for the VRF. |

| | Command | Purpose |
|---|---|---|
| Step 4 | **exit**<br><br>**Example:**<br>`switch(config-vlan)# exit`<br>`switch(config)#` | Exits VLAN configuration mode. |
| | **exit**<br><br>**Example:**<br>`switch(config-vrf)# exit`<br>`switch(config)#` | Exits VRF configuration mode. |
| Step 5 | **show cts role-based sgt-map**<br><br>**Example:**<br>`switch(config)# show cts role-based sgt-map` | (Optional) Displays the Cisco TrustSec SGACL SGT mapping configuration. |
| Step 6 | **copy running-config startup-config**<br><br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

## Manually Configuring SGACL Policies

You can manually configure SGACL polices 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 are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

Ensure that you enabled SGACL policy enforcement on the VLAN (see the "Enabling SGACL Policy Enforcement on VLANs" section on page 10-30) and VRF (see the "Enabling SGACL Policy Enforcement on VRFs" section on page 10-31).

### SUMMARY STEPS

1. **configure terminal**
2. **cts role-based access-list** *list-name*
3. **deny all**

   **deny icmp**

   **deny igmp**

   **deny ip**

   **deny tcp** [{**dest** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}]

   **deny udp** [{**dest** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}]
4. **permit all**

   **permit icmp**

   **permit igmp**

**permit ip**

**permit tcp** [{**dest** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}]

**permit udp** [{**dest** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}]

5. **exit**
6. **cts role-based sgt** {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **any** | **unknown**} **access-list** *list-name*
7. **show cts role-based access-list**
8. **copy running-config startup-config**

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters configuration mode. |
| **Step 2** | **cts role-based access-list** *list-name*<br><br>**Example:**<br>`switch(config)# cts role-based access-list MySGACL`<br>`switch(config-rbacl)#` | Specifies an SGACL and enters role-based access list configuration mode. The *list-name* argument is alphanumeric, case sensitive, and has a maximum length of 32 characters. |
| **Step 3** | **deny all**<br><br>**Example:**<br>`switch(config-rbacl)# deny all` | Denies all traffic. |
| | **deny icmp**<br><br>**Example:**<br>`switch(config-rbacl)# deny icmp` | Denies Internet Control Message Protocol (ICMP) traffic. |
| | **deny igmp**<br><br>**Example:**<br>`switch(config-rbacl)# deny igmp` | Denies Internet Group Management Protocol (IGMP) traffic. |
| | **deny all**<br><br>**Example:**<br>`switch(config-rbacl)# deny ip` | Denies IP traffic. |
| | **deny tcp** [{**dest** \| **src**} {{**eq** \| **gt** \| **lt** \| **neq**} *port-number* \| **range** *port-number1 port-number2*}]<br><br>**Example:**<br>`switch(config-rbacl)# deny tcp src lt 10` | Denies TCP traffic. The default denies all TCP traffic. The range for the *port-number*, *port-number1*, and *port-number2* arguments is from 0 to 65535. |
| | **deny udp** [{**dest** \| **src**} {{**eq** \| **gt** \| **lt** \| **neq**} *port-number* \| **range** *port-number1 port-number2*}]<br><br>**Example:**<br>`switch(config-rbacl)# deny udp dest eq 100` | Permits UDP traffic The default denies all UDP traffic.The range for the *port-number*, *port-number1*, and *port-number2* arguments is from 0 to 65535. |

| | Command | Purpose |
|---|---|---|
| Step 4 | **permit all**<br><br>**Example:**<br>switch(config-rbacl)# permit all | Permits all traffic. |
| | **permit icmp**<br><br>**Example:**<br>switch(config-rbacl)# permit icmp | Permits ICMP traffic. |
| | **permit igmp**<br><br>**Example:**<br>switch(config-rbacl)# permit igmp | Permits IGMP traffic. |
| | **permit ip**<br><br>**Example:**<br>switch(config-rbacl)# permit ip | Permits IP traffic. |
| | **permit tcp** [{**dest** \| **src**} {{**eq** \| **gt** \| **lt** \| **neq**} *port-number* \| **range** *port-number1 port-number2*}]<br><br>**Example:**<br>switch(config-rbacl)# permit tcp | 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. The *port-number2* argument value must be greater than the *port-number1* argument value. |
| | **permit udp** [{**dest** \| **src**} {{**eq** \| **gt** \| **lt** \| **neq**} *port-number* \| **range** *port-number1 port-number2*}]<br><br>**Example:**<br>switch(config-rbacl)# permit udp dest ne 2000 | 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. The *port-number2* argument value must be greater than the *port-number1* argument value. |
| Step 5 | **exit**<br><br>**Example:**<br>switch(config-rbacl)# exit<br>switch(config)# | Exits role-based access-list configuration mode. |
| Step 6 | **cts role-based sgt** {*sgt-value* \| **any** \| **unknown**} **dgt** {*dgt-value* \| **any** \| **unknown**} **access-list** *list-name*<br><br>**Example:**<br>switch(config)# cts role-based sgt 3 dgt 10 access-list MySGACL | Maps the SGT values to the SGACL. The sgt-value and dgt-value arguments range from 0 to 65520.<br><br>**Note** You must create the SGACL before you can map SGTs to it. |
| Step 7 | **show cts role-based access-list**<br><br>**Example:**<br>switch(config)# show cts role-based access-list | (Optional) Displays the Cisco TrustSec SGACL configuration. |
| Step 8 | **copy running-config startup-config**<br><br>**Example:**<br>switch(config)# copy running-config startup-config | (Optional) Copies the running configuration to the startup configuration. |

## 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 download 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 are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

### SUMMARY STEPS

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

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | `show cts role-based access-list`<br><br>**Example:**<br>`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. |

## 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 are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

### SUMMARY STEPS

1. **cts refresh role-based-policy**
2. **show cts role-based policy**

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **cts refresh policy**<br><br>**Example:**<br>switch# cts refresh policy | Refreshes the Cisco TrustSec SGACL policies from the Cisco Secure ACS. |
| Step 2 | **show cts role-based policy**<br><br>**Example:**<br>switch# show cts role-based policy | (Optional) Displays the Cisco TrustSec SGACL policies. |

## Clearing Cisco TrustSec SGACL Policies

You can clear the Cisco TrustSec SGACL policies.

### BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

### SUMMARY STEPS

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

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **show cts role-based policy**<br><br>**Example:**<br>switch# clear cts policy all | (Optional) Displays the Cisco TrustSec RBACL policy configuration. |
| Step 2 | **clear cts policy** {**all** \| **peer** *device-name* \| **sgt** *sgt-value*}<br><br>**Example:**<br>switch# clear cts policy all | Clear the polices for Cisco TrustSec connection information. |

# 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.

This section includes the following topics:



## Cisco TrustSec SXP Configuration Process

Follow these steps to manually configure Cisco TrustSec SXP:

**Step 1** Enable the Cisco TrustSec feature (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

**Step 2** Enable SGACL policy enforcement on the VRF (see the "Enabling SGACL Policy Enforcement on VRFs" section on page 10-31).

**Step 3** Enable Cisco TrustSec SXP (see the "Enabling Cisco TrustSec SXP" section on page 10-40).

**Step 4** Configure SXP peer connections (see the "Configuring Cisco TrustSec SXP Peer Connections" section on page 10-41).

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

## Enabling Cisco TrustSec SXP

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

### BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

### SUMMARY STEPS

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

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal**<br><br>**Example:**<br>switch# configure terminal<br>switch(config)# | Enters configuration mode. |
| Step 2 | **cts sxp enable**<br><br>**Example:**<br>switch(config)# cts sxp enable | Enables SXP for Cisco TrustSec. |
| Step 3 | **exit**<br><br>**Example:**<br>switch(config)# exit<br>switch# | Exits configuration mode. |
| Step 4 | **show cts sxp**<br><br>**Example:**<br>switch# show cts sxp | (Optional) Displays the SXP configuration. |
| Step 5 | **copy running-config startup-config**<br><br>**Example:**<br>switch# copy running-config startup-config | (Optional) Copies the running configuration to the startup configuration. |

## Configuring Cisco TrustSec SXP Peer Connections

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

In Cisco NX-OS Release 4.1(3) and later releases, you can specify encrypted passwords for SXP peer connections.

**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 are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

Ensure that you enabled SXP (see the "Enabling Cisco TrustSec SXP" section on page 10-40).

Ensure that you enabled RBACL policy enforcement in the VRF (see the "Enabling SGACL Policy Enforcement on VRFs" section on page 10-31).

## SUMMARY STEPS

1. **configure terminal**
2. **cts sxp connection peer** *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** {**default** | **none** | **required** {*password* | **7** *encrypted-password*}} **mode** {**speaker** | **listener**} [**vrf** *vrf-name*]
3. **exit**
4. **show cts sxp**
5. **copy running-config startup-config**

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters configuration mode. |
| **Step 2** | **cts sxp connection peer** *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** {**default** \| **none** \| **required** {*password* \| **7** *encrypted-password*}] **mode** {**speaker** \| **listener**} [**vrf** *vrf-name*]<br><br>**Example:**<br>`switch(config)# cts sxp connection peer 10.10.1.1 source 20.20.1.1 password default mode speaker` | Configures the SXP address connection.<br><br>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.<br><br>The **password** keyword specifies the password that SXP should use for the connection using the following options:<br>• **default**—use the default SXP password you configured using the **cts sxp default password** command.<br>• **none**—does not use a password.<br>• **required**—uses the password specified in the command. You can enter a clear text password or an encrypted password using the **7** option. The maximum length is 32 characters.<br><br>The **vrf** keyword specifies the VRF to the peer. The default is the default VRF.<br><br>The **mode** keyword specifies the role of the remote peer device:<br>• **speaker**—Specifies that the peer is the speaker in the connection.<br>• **listener**—Specifies that the peer is the listener in the connection.<br><br>**Note** You cannot use the management (mgmt 0) interface for SXP. |

| | Command | Purpose |
|---|---|---|
| Step 3 | **exit**<br><br>**Example:**<br>switch(config)# exit<br>switch# | Exits configuration mode. |
| Step 4 | **show cts sxp**<br><br>**Example:**<br>switch# show cts sxp | (Optional) Displays the SXP configuration. |
| Step 5 | **copy running-config startup-config**<br><br>**Example:**<br>switch# copy running-config startup-config | (Optional) Copies the running configuration to the startup configuration. |

## 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.

In Cisco NX-OS Release 4.1(3) and later releases, you can specify encrypted passwords for SXP default password.

### BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

Ensure that you enabled SXP (see the "Enabling Cisco TrustSec SXP" section on page 10-40).

### SUMMARY STEPS

1. **configure terminal**
2. **cts sxp default password** {*password* | **7** *encrypted-password*}
3. **exit**
4. **show cts sxp**
5. **show running-config cts**
6. **copy running-config startup-config**

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal**<br><br>**Example:**<br>switch# configure terminal<br>switch(config)# | Enters configuration mode. |
| Step 2 | **cts sxp default password** {*password* \| **7** *encrypted-password*}<br><br>**Example:**<br>switch(config)# cts sxp default password A2Q3d4F5 | Configures the SXP default password. You can enter either a clear text password or an encrypted password using the **7** option. The maximum length is 32 characters. |
| Step 3 | **exit**<br><br>**Example:**<br>switch(config)# exit<br>switch# | Exits configuration mode. |
| Step 4 | **show cts sxp**<br><br>**Example:**<br>switch# show cts sxp | (Optional) Displays the SXP configuration. |
| Step 5 | **show running-config cts**<br><br>**Example:**<br>switch# show running-config cts | (Optional) Displays the SXP configuration in the running configuration. |
| Step 6 | **copy running-config startup-config**<br><br>**Example:**<br>switch# copy running-config startup-config | (Optional) Copies the running configuration to the startup configuration. |

## Configuring the Default SXP Source IP Address

The Cisco NX-OS software uses default source IP address in all new TCP connections where a source IP address is not specified. There is no effect on existing TCP connections when you configure the default SXP source IP address.

### BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

Ensure that you enabled SXP (see the "Enabling Cisco TrustSec SXP" section on page 10-40).

### SUMMARY STEPS

1. **configure terminal**
2. **cts sxp default source-ip** *src-ip-addr*
3. **exit**

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

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal**<br><br>**Example:**<br>switch# configure terminal<br>switch(config)# | Enters configuration mode. |
| Step 2 | **cts sxp default source-ip** *src-ip-addr*<br><br>**Example:**<br>switch(config)# cts sxp default source-ip 10.10.3.3 | Configures the SXP default source IP address. |
| Step 3 | **exit**<br><br>**Example:**<br>switch(config)# exit<br>switch# | Exits configuration mode. |
| Step 4 | **show cts sxp**<br><br>**Example:**<br>switch# show cts sxp | (Optional) Displays the SXP configuration. |
| Step 5 | **copy running-config startup-config**<br><br>**Example:**<br>switch# copy running-config startup-config | (Optional) Copies the running configuration to the startup configuration. |

## 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 are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

Ensure that you enabled SXP (see the "Enabling Cisco TrustSec SXP" section on page 10-40).

### SUMMARY STEPS

1. **configure terminal**
2. **cts sxp reconcile-period** *seconds*

3. **exit**
4. **show cts sxp**
5. **copy running-config startup-config**

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters configuration mode. |
| **Step 2** | **cts sxp reconcile-period** *seconds*<br><br>**Example:**<br>`switch(config)# cts sxp reconcile-period 180` | Changes the SXP reconcile timer. The default value is 120 seconds (2 minutes). The range is from 0 to 64000. |
| **Step 3** | **exit**<br><br>**Example:**<br>`switch(config)# exit`<br>`switch#` | Exits configuration mode. |
| **Step 4** | **show cts sxp**<br><br>**Example:**<br>`switch# show cts sxp` | (Optional) Displays the SXP configuration. |
| **Step 5** | **copy running-config startup-config**<br><br>**Example:**<br>`switch# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

## 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 are in the correct VDC (or use the **switchto vdc** command).

Ensure that you enabled Cisco TrustSec (see the "Enabling the Cisco TrustSec Feature" section on page 10-12).

Ensure that you enabled SXP (see the "Enabling Cisco TrustSec SXP" section on page 10-40).

### SUMMARY STEPS

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

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

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters configuration mode. |
| **Step 2** | **cts sxp retry-period** *seconds*<br><br>**Example:**<br>`switch(config)# cts sxp retry-period 120` | Changes the SXP retry timer. The default value is 60 seconds (1 minute). The range is from 0 to 64000. |
| **Step 3** | **exit**<br><br>**Example:**<br>`switch(config)# exit`<br>`switch#` | Exits configuration mode. |
| **Step 4** | **show cts sxp**<br><br>**Example:**<br>`switch# show cts sxp` | (Optional) Displays the SXP configuration. |
| **Step 5** | **copy running-config startup-config**<br><br>**Example:**<br>`switch# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

# Verifying Cisco TrustSec Configuration

To display Cisco TrustSec configuration information, perform one of the following tasks:

| Command | Purpose |
|---|---|
| **show feature** | Displays the enabled status of the feature. |
| **show cts** | Displays Cisco TrustSec information. |
| **show cts credentials** | Displays Cisco TrustSec credentials for EAP-FAST. |
| **show cts environment-data** | Displays Cisco TrustSec environmental data. |
| **show cts interface** | Displays the Cisco TrustSec configuration for the interfaces. |
| **show cts pacs** | Display 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** | Displays Cisco TrustSec SGACL policy information. |

| Command | Purpose |
|---|---|
| **show cts role-based sgt-map** | Displays Cisco TrustSec SGACL SGT map configuration. |
| **show cts sxp** | Displays Cisco TrustSec SXP information. |
| **show running-config cts** | Displays the Cisco TrustSec information in the running configuration. |

For detailed information about the fields in the output from this command, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.1*.

# Example Cisco TrustSec Configurations

This sections includes the following topics:



## Enabling Cisco TrustSec

The following example shows how to enable Cisco TrustSec:

```
feature dot1x
feature cts
cts device-id device1 password Cisco321
```

## 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 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
```

# 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
```

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
```

# Configuring Cisco TrustSec Authentication in Manual Mode

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

```
interface ethernet 2/1
  cts manual
    sap pmk abcdef modelist gmac
    policy static sgt 0x20
interface ethernet 2/2
  cts manual
    policy dynamic identity device2
```

# Configuring Cisco TrustSec Role-Based Policy Enforcement for the default VRF

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

```
cts role-based enforcement
```

# 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
```

# 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
```

# Configuring IPv4 Address to SGACL SGT Mapping for the Default VRF

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

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

# Configuring IPv4 Address to SGACL SGT Mapping for a Nondefault VRF

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

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

# 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
```

# Manually Configuring Cisco TrustSec SGACLs

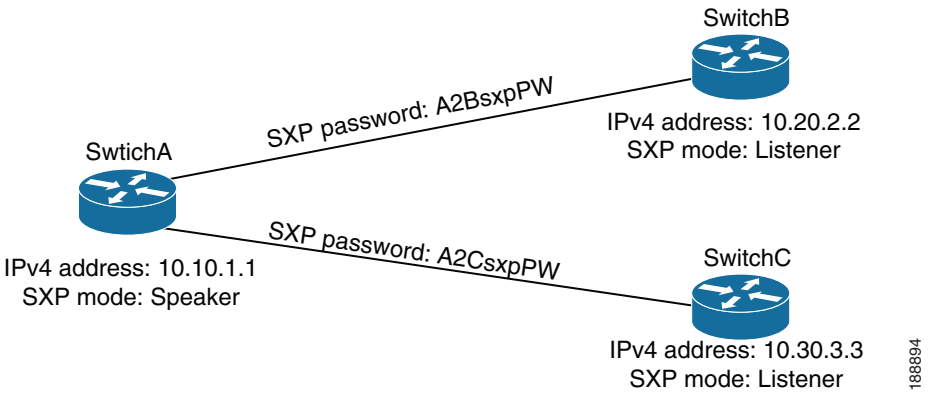
The following example shows how to manually configure Cisco TrustSec SGACLs:

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

## Manually Configuring SXP Peer Connections

Figure 10-7 shows an example of SXP peer connections over the default VRF.

*Figure 10-7 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
```

# Default Settings

Table 10-1 lists the default settings for Cisco TrustSec parameters.

*Table 10-1 Default Cisco TrustSec Parameters*

| Parameters | Default |
|---|---|
| Cisco TrustSec | Disabled. |
| SXP | Disabled. |
| SXP default password | None. |

*Table 10-1 Default Cisco TrustSec Parameters (continued)*

| Parameters | Default |
|---|---|
| SXP reconcile period | 120 seconds (2 minutes). |
| SXP retry period | 60 seconds (1 minute). |

# Additional References

For additional information related to implementing Cisco TrustSec, see the following sections:

- Related Documents, page 10-52

## Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco Secure ACS | Cisco Secure Access Control Server Engine Solution documentation |
| Command Reference | *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.1* |
| 802.1X | Chapter 8, “Configuring 802.1X” |

# Feature History for Cisco TrustSec

Table 10-2 lists the release history for this feature.

*Table 10-2 Feature History for Cisco TrustSec*

| Feature Name | Releases | Feature Information |
|---|---|---|
| SGT propagation | 4.0(3) | You can disable security group tag (SGT) propagation on Layer 2 Cisco TrustSec interfaces. |
| Cisco TrustSec manual configuration | 4.0(3) | You can configure SAP for Cisco TrustSec manual mode to use 802.1X. |
| Cisco TrustSec | 4.0(1) | This feature was introduced. |