



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](#) , on page 1
- [Licensing Requirements for Cisco TrustSec](#) , on page 10
- [Prerequisites for Cisco TrustSec](#) , on page 10
- [Guidelines and Limitations for Cisco TrustSec](#) , on page 10
- [Default Settings for Cisco TrustSec Parameters](#), on page 11
- [Configuring Cisco TrustSec](#) , on page 12
- [Verifying the Cisco TrustSec Configuration](#), on page 43
- [Configuration Examples for Cisco TrustSec](#), on page 44
- [Additional References for Cisco TrustSec](#), on page 47
- [Feature History for Cisco TrustSec](#), on page 48

Information About Cisco TrustSec

This section provides information about Cisco TrustSec.

Cisco TrustSec Architecture

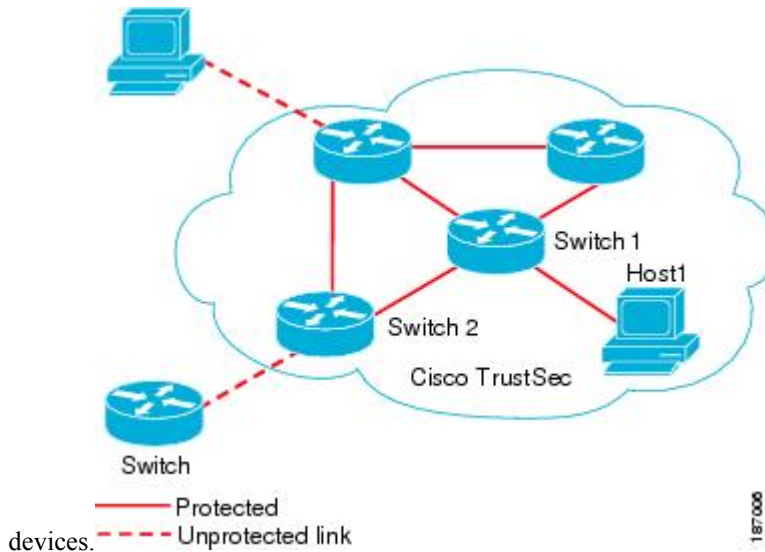
The Cisco TrustSec security architecture builds secure networks by establishing clouds of trusted network devices. Cisco TrustSec also uses the device information acquired during authentication for classifying, or coloring, the packets as they enter the network. This packet classification is maintained 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 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.



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 a per-packet basis using the source tags on each packet.

A Cisco TrustSec network has the following entities:

Authenticators (AT)

Devices that are already part of a Cisco TrustSec network.

Authorization server (AS)

Servers that may provide authentication information, authorization information, or both.

When the link first comes up, authorization occurs in which each side of the link obtains policies, such as SGT and ACLs, that apply to the link.

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.

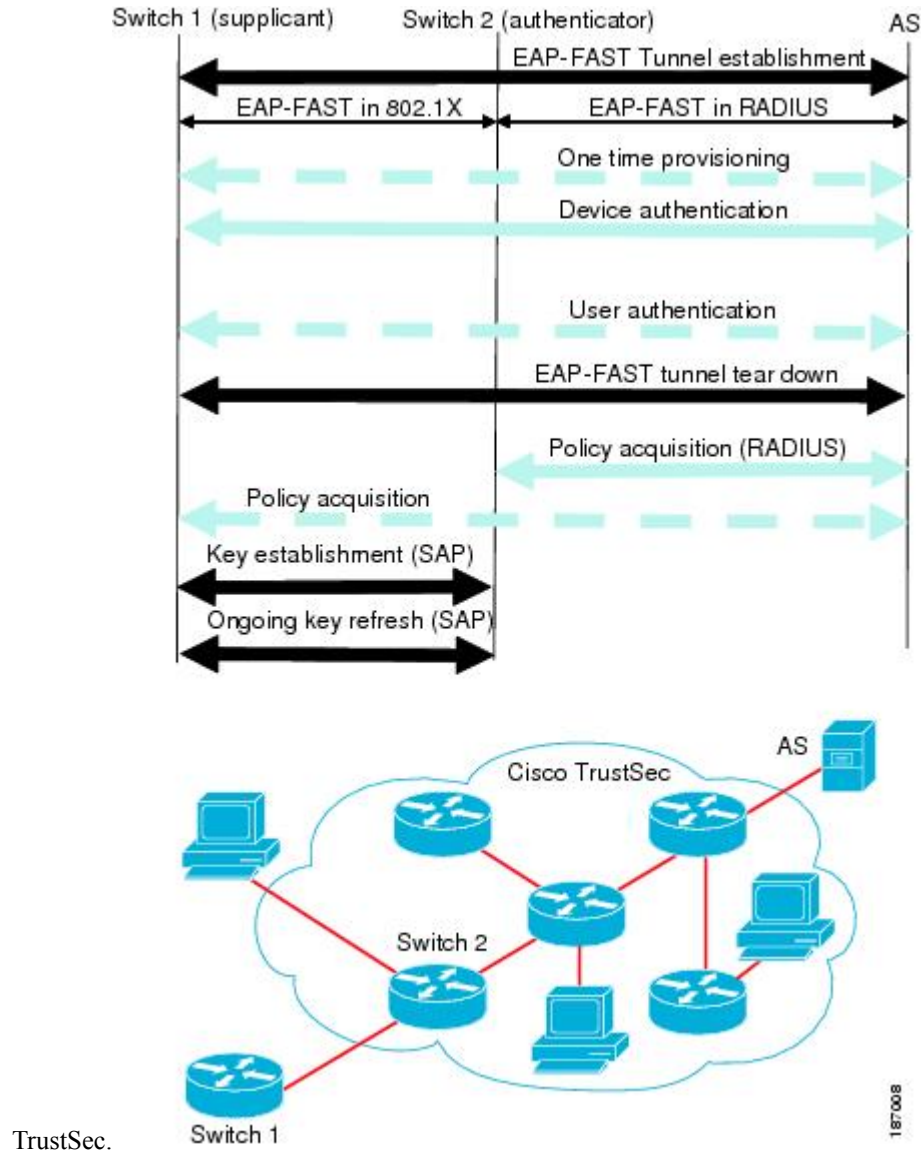
Cisco TrustSec and Authentication

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 2: Cisco TrustSec Authentication

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



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.

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.

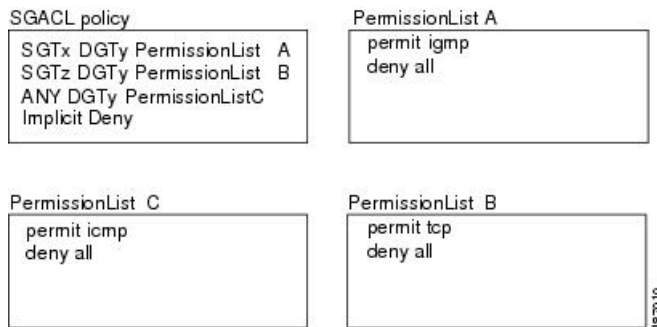
The management server derives the SGTs based on the security policy configuration. You do not have to configure them manually.

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.

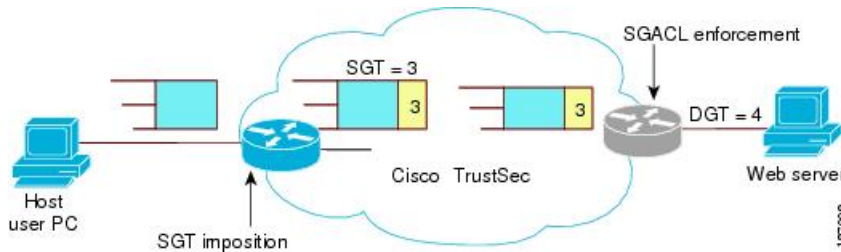
Cisco TrustSec defines access control policies between the security groups. By assigning devices within the network to security groups and applying access control between and within the security groups, Cisco TrustSec essentially achieves access control within the network.

Figure 3: SGACL Policy Example

This figure shows an example of an SGACL policy.

**Figure 4: 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
```

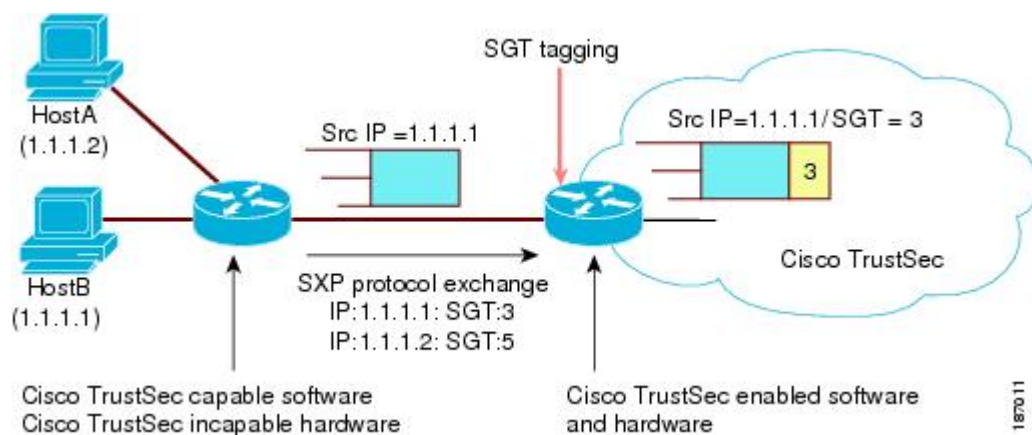
SXP for SGT Propagation Across Legacy Access Networks

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 5: 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.

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.

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.

Licensing Requirements for Cisco TrustSec

The following table shows the licensing requirements for this feature:

Table 1: Licensing Requirements for Cisco TrustSec

Product	License Requirement
Cisco NX-OS	<p>Beginning with Cisco NX-OS Release 6.1, Cisco TrustSec requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you.</p> <p>For releases earlier than Cisco NX-OS 6.1, Cisco TrustSec requires an Advanced Services license. Cisco TrustSec licensing does not have a grace period. You must obtain and install an Advanced Services license before you can use Cisco TrustSec.</p> <p>Note For an explanation of the Cisco NX-OS licensing scheme and how to obtain and apply licenses, see the Cisco NX-OS Licensing Guide.</p>

Prerequisites for Cisco TrustSec

Cisco TrustSec has the following prerequisites:

- You must install the Advanced Services license if your device is running a release earlier than Cisco NX-OS Release 6.1.
- 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:

- Cisco TrustSec uses RADIUS for 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.
- Clearing policies does not take affect immediately; it requires a flap to occur. In addition, the way policies are cleared depends on whether the SGT is static or dynamic. For a static SGT, the SGT is reset to 0 after the flap occurs. For dynamic SGT, the SGT is downloaded again from the RADIUS server after the flap occurs.

- Cisco TrustSec supports management switch virtual interfaces (SVIs), not routed SVIs.
- The 802.1X feature must be enabled before you enable the Cisco TrustSec feature. However, none of the 802.1X interface level features are available. The 802.1X feature is only used for the device to authenticate with RADIUS.
- RBACL is only implemented on bridged Ethernet traffic and cannot be enabled on a routing VLAN or routing interface.
- The determination of whether a peer is trusted or not and its capability to propagate SGTs on egress are made at the physical interface level.
- Cisco TrustedSec interface configurations on port channel members must be exactly the same. If a port channel member is inconsistent with the other port channel members, it will be error disabled.
- In a vPC domain, use the configuration synchronization mode (config-sync) to create switch profiles to ensure that the Cisco TrustSec configuration is synchronized between peers. If you configure the same vPC differently on two peer switches, traffic is treated differently.
- The maximum number of RBACL TCAM entries is 128, with 4 entries used by default, and the remaining 124 entries user-configurable.
- Cisco TrustSec is not supported on Layer 3 interfaces or Virtual Routing and Forwarding (VRF) interfaces.
- The **cts-manual**, **cts trusted mode**, and **no-propagate sgt** configurations must be consistent among all FEX ports or vEthernet ports on the same fabric port. If these configurations are inconsistent, the interfaces are err-disabled.
- The **cts-manual**, **sgt value**, **cts trusted mode**, and **no-propagate sgt** configurations must be consistent among all port channel members on the same port channel. If these configurations are inconsistent, the interfaces are err-disabled.

Default Settings for Cisco TrustSec Parameters

This table lists the default settings for Cisco TrustSec parameters.

Table 2: 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)
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.

Before you begin

Ensure that you have installed the Advanced Services license, if your device is running a release earlier than Cisco NX-OS Release 6.1.

Procedure

	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: switch(config)# exit switch#	Exits global configuration mode.
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.

	Command or Action	Purpose
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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	cts device-id <i>name</i> password <i>password</i> Example: switch(config)# cts device-id MyDevice1 password Cisc0321	Configures a unique device ID and password. The <i>name</i> 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.

	Command or Action	Purpose
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 12

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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } key [0 7] key pac Example: <pre>switch(config)# radius-server host 10.10.1.1 key L1a0K2s9 pac</pre>	Configures a RADIUS server host with a key and PAC. The <i>hostname</i> argument is alphanumeric, case sensitive, and has a maximum of 256 characters. The <i>key</i> 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: <pre>switch# show radius-server</pre>	Displays the RADIUS server configuration.
Step 4	aaa group server radius <i>group-name</i> Example: <pre>switch(config)# aaa group server radius Rad1 switch(config-radius)#</pre>	Specifies the RADIUS server group and enters RADIUS server group configuration mode.
Step 5	server { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } Example: <pre>switch(config-radius)# server 10.10.1.1</pre>	Specifies the RADIUS server host address.
Step 6	use-vrf <i>vrf-name</i> Example: <pre>switch(config-radius)# use-vrf management</pre>	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: <pre>switch(config-radius)# exit switch(config)#</pre>	Exits RADIUS server group configuration mode.

	Command or Action	Purpose
Step 8	aaa authentication dot1x default group <i>group-name</i> Example: <pre>switch(config)# aaa authentication dot1x default group Rad1</pre>	Specifies the RADIUS server groups to use for 802.1X authentication.
Step 9	aaa authorization cts default group <i>group-name</i> Example: <pre>switch(config)# aaa authentication cts default group Rad1</pre>	Specifies the RADIUS server groups to use for Cisco TrustSec authorization.
Step 10	exit Example: <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 11	(Optional) show radius-server groups <i>[group-name]</i> Example: <pre>switch# show radius-server group rad1</pre>	Displays the RADIUS server group configuration.
Step 12	(Optional) show aaa authentication Example: <pre>switch# show aaa authentication</pre>	Displays the AAA authentication configuration.
Step 13	(Optional) show aaa authorization Example: <pre>switch# show aaa authorization</pre>	Displays the AAA authorization configuration.
Step 14	(Optional) show cts pacs Example: <pre>switch# show cts pacs</pre>	Displays the Cisco TrustSec PAC information.
Step 15	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

[Enabling the Cisco TrustSec SGT Feature](#) , on page 12

[Configuring AAA on Cisco TrustSec Nonseed Cisco NX-OS Devices](#) , on page 17

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.

Procedure

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

Related Topics

[Enabling the Cisco TrustSec SGT Feature](#) , on page 12

[Configuring AAA on a Seed Cisco NX-OS Device in a Cisco TrustSec Network](#), on page 14

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:

Procedure

-
- Step 1** Enable the Cisco TrustSec feature. See [Enabling the Cisco TrustSec SGT Feature](#) , on page 12.
 - Step 2** Enable Cisco TrustSec authentication. See [Enabling Cisco TrustSec Authentication](#) , on page 18.
 - Step 3** Enable 802.1X authentication for Cisco TrustSec on the interfaces. See [Enabling the 802.1X Feature](#).
-

Related Topics

- [Enabling the Cisco TrustSec SGT Feature](#) , on page 12
- [Enabling Cisco TrustSec Authentication](#) , on page 18

Enabling Cisco TrustSec Authentication

You must enable Cisco TrustSec authentication on the interfaces.



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.

Procedure

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

	Command or Action	Purpose
	<code>switch(config)# interface ethernet 2/2</code> <code>switch(config-if)#</code>	
Step 3	cts dot1x Example: <code>switch(config-if)# cts dot1x</code> <code>switch(config-if-cts-dot1x)#</code>	Enables 802.1X authentication for Cisco TrustSec and enters Cisco TrustSec 802.1X configuration mode.
Step 4	(Optional) no replay-protection Example: <code>switch(config-if-cts-dot1x)# no</code> <code>replay-protection</code>	Disables replay protection. The default is enabled.
Step 5	exit Example: <code>switch(config-if-cts-dot1x)# exit</code> <code>switch(config-if)#</code>	Exits Cisco TrustSec 802.1X configuration mode.
Step 6	shutdown Example: <code>switch(config-if)# shutdown</code>	Disables the interface.
Step 7	no shutdown Example: <code>switch(config-if)# no shutdown</code>	Enables the interface and enables Cisco TrustSec authentication on the interface.
Step 8	exit Example: <code>switch(config-if)# exit</code> <code>switch(config)#</code>	Exits interface configuration mode.
Step 9	(Optional) show cts interface {all ethernet slot/port} Example: <code>switch(config)# show cts interface all</code>	Displays the Cisco TrustSec configuration on the interfaces.
Step 10	(Optional) copy running-config startup-config Example: <code>switch(config)# copy running-config</code> <code>startup-config</code>	Copies the running configuration to the startup configuration.

Related Topics

[Enabling the Cisco TrustSec SGT Feature](#) , on page 12

Configuring Data-Path Replay Protection for Cisco TrustSec on Interfaces

By default, the Cisco NX-OS software enables the data-path replay 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.



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.

Procedure

	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:	Enables the interface and disables the data-path replay protection feature on the interface.

	Command or Action	Purpose
	<code>switch(config-if)# no shutdown</code>	
Step 8	exit Example: <code>switch(config-if)# exit</code> <code>switch(config)#</code>	Exits interface configuration mode.
Step 9	(Optional) show cts interface {all ethernet slot/port} Example: <code>switch(config)# show cts interface all</code>	Displays the Cisco TrustSec configuration on the interface.
Step 10	(Optional) copy running-config startup-config Example: <code>switch(config)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

Related Topics

[Enabling Cisco TrustSec Authentication](#) , on page 18

Configuring SGT Propagation for Cisco TrustSec on Interfaces

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.

**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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.
Step 2	interface ethernet slot/port [- port2] Example: <code>switch(config)# interface ethernet 2/2</code> <code>switch(config-if)#</code>	Specifies a single port or a range of ports 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	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 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 18

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.

Procedure

	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	(Optional) policy dynamic identity peer-name Example: switch(config-if-cts-manual)# policy dynamic identity MyDevice2	Configures a dynamic authorization policy download. The <i>peer-name</i> 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.

	Command or Action	Purpose
		<p>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.</p>
Step 5	<p>(Optional) policy static sgt tag [trusted]</p> <p>Example:</p> <pre>switch(config-if-cts-manual)# policy static sgt 0x2</pre>	<p>Configures a static authorization policy. The <i>tag</i> argument is a hexadecimal value in the format 0xhhhh. The 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.</p> <p>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.</p>
Step 6	<p>exit</p> <p>Example:</p> <pre>switch(config-if-cts-manual)# exit switch(config-if)#</pre>	Exits Cisco TrustSec manual configuration mode.
Step 7	<p>shutdown</p> <p>Example:</p> <pre>switch(config-if)# shutdown</pre>	Disables the interface.
Step 8	<p>no shutdown</p> <p>Example:</p> <pre>switch(config-if)# no shutdown</pre>	Enables the interface and enables Cisco TrustSec authentication on the interface.
Step 9	<p>exit</p> <p>Example:</p> <pre>switch(config-if)# exit switch(config)#</pre>	Exits interface configuration mode.
Step 10	<p>(Optional) show cts interface {all ethernet slot/port}</p> <p>Example:</p> <pre>switch# show cts interface all</pre>	Displays the Cisco TrustSec configuration for the interfaces.

	Command or Action	Purpose
Step 11	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

[Enabling the Cisco TrustSec SGT Feature](#) , on page 12

Configuring Pause Frame Encryption or Decryption for Cisco TrustSec on Interfaces

Pause frames are MAC control frames used for Ethernet flow control. The ports on some line cards encrypt and decrypt pause frames while the ports on other line cards do not have this ability. This disparity causes interoperability issues and causes the ports to discard or ignore the pause frames.

You can determine if the pause frames are to be encrypted or clear on individual interfaces. You must configure the interfaces on both ends of the connection but can do so using either dot1x or manual mode. If two ports are connected to form a CTS link and one is clear pause capable and the other is secure (encryption or decryption) pause capable, the pause frames must be sent in the clear across the link in order for them to be correctly sent and received.



Note F1 Series modules and the N7K-M132XP-12(L) module support only clear pause frames.



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 pause frame encryption or decryption 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.

Ensure that you have enabled flow control on the interface using the **flowcontrol {send | receive}** command.

Procedure

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

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
Step 2	interface ethernet <i>slot/port</i> Example: switch(config)# interface ethernet 2/2 switch(config-if)#	Specifies an interface and enters interface configuration mode.
Step 3	cts dot1x or cts manual Example: switch(config-if)# cts dot1x switch(config-if-cts-dot1x)#	Enters Cisco TrustSec dot1x or manual configuration mode. Note You cannot enable Cisco TrustSec on interfaces in half-duplex mode.
Step 4	[no] encrypt pause-frame Example: switch(config-if-cts-dot1x)# no encrypt pause-frame	Configures pause frame encryption or decryption for Cisco TrustSec on the interface. When no encrypt pause-frame is configured, the pause frames are sent in the clear. When encrypt pause-frame is configured, pause frames are sent encrypted over the CTS link.
Step 5	exit Example: switch(config-if-cts-dot1x)# exit switch(config-if)#	Exits Cisco TrustSec dot1x or manual 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 enables pause frame encryption or decryption for Cisco TrustSec on the interface.
Step 8	exit Example: switch(config-if)# exit switch(config)#	Exits interface configuration mode.
Step 9	(Optional) show cts interface {all ethernet <i>slot/port</i>} Example: switch# show cts interface all	Displays the Cisco TrustSec configuration for the interfaces.
Step 10	(Optional) copy running-config startup-config Example:	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	switch# copy running-config startup-config	

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:

Procedure

-
- 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 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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.

	Command or Action	Purpose
Step 2	vlan <i>vlan-id</i> Example: <pre>switch(config)# vlan 10 switch(config-vlan)#</pre>	Specifies a VLAN and enters VLAN configuration mode.
Step 3	cts role-based enforcement Example: <pre>switch(config-vlan)# cts role-based enforcement</pre>	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: <pre>switch(config-vlan)# exit switch(config)#</pre>	Saves the VLAN configuration and exits VLAN configuration mode.
Step 5	(Optional) show cts role-based enable Example: <pre>switch(config)# show cts role-based enable</pre>	Displays the Cisco TrustSec SGACL enforcement configuration.
Step 6	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

[Enabling the Cisco TrustSec SGT Feature](#) , on page 12

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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	vrf context <i>vrf-name</i> 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 12

Manually Configuring Cisco TrustSec SGTs

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



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 have enabled Cisco TrustSec.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	cts sgt tag Example: switch(config)# cts sgt 0x00a2	Configures the SGT for packets sent from the device. The <i>tag</i> argument is a hexadecimal value in the format 0xhhh . The range is from 0x2 to 0xffef.
Step 3	exit Example: switch(config)# exit switch#	Exits global configuration mode.
Step 4	(Optional) show cts environment-data Example: switch# show cts environment-data	Displays the Cisco TrustSec environment data information.
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 12

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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	vlan <i>vlan-id</i> Example: switch(config)# vlan 10 switch(config-vlan)#	Specifies a VLAN and enters VLAN configuration mode.
Step 3	cts role-based sgt-map <i>ipv4-address tag</i> 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 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 12

[Enabling SGACL Policy Enforcement on VLANs](#) , on page 27

[Enabling SGACL Policy Enforcement on VRF Instances](#), on page 28

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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	vrf context <i>vrf-name</i> 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 <i>ipv4-address tag</i> 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.
Step 5	(Optional) show cts role-based sgt-map 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.

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.

Procedure

	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 <i>list-name</i> 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 <i>port-number</i> , <i>port-number1</i> , and <i>port-number2</i> 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 <i>port-number</i> , <i>port-number1</i> , and <i>port-number2</i> arguments is from 0 to 65535.
Step 9	exit Example: switch(config-rbacl)# exit switch(config)#	Exits role-based access-list configuration mode.

	Command or Action	Purpose
Step 10	cts role-based sgt <i>{sgt-value any unknown}</i> dgt <i>{dgt-value any unknown}</i> access-list <i>list-name</i> Example: <pre>switch(config)# cts role-based sgt 3 dgt 10 access-list MySGACL</pre>	Maps the SGT values to the SGACL. The <i>sgt-value</i> and <i>dgt-value</i> argument values range from 0 to 65520. Note You must create the SGACL before you can map SGTs to it.
Step 11	(Optional) show cts role-based access-list Example: <pre>switch(config)# show cts role-based access-list</pre>	Displays the Cisco TrustSec SGACL configuration.
Step 12	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

[Enabling the Cisco TrustSec SGT Feature](#) , on page 12

[Enabling SGACL Policy Enforcement on VLANs](#) , on page 27

[Enabling SGACL Policy Enforcement on VRF Instances](#), on page 28

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.

Procedure

	Command or Action	Purpose
Step 1	show cts role-based access-list Example: <pre>switch# show cts role-based access-list</pre>	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 12

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.

Procedure

	Command or Action	Purpose
Step 1	cts refresh role-based-policy Example: switch# cts refresh role-based-policy	Refreshes the Cisco TrustSec SGACL policies from the Cisco Secure ACS.
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 12

Enabling Statistics for RBACL

You can request a count of the number of packets that match role-based access control list (RBACL) policies. These statistics are collected per source group tag (SGT) and destination group tag (DGT).



Note When you modify an RBACL policy, statistics for the previously assigned access control entry (ACE) are displayed, and the newly assigned ACE statistics are initialized to 0.



Note RBACL statistics are lost only when the Cisco NX-OS device reloads or you deliberately clear the statistics.

Before you begin

Ensure that you have enabled Cisco TrustSec.

If you plan to enable RBACL statistics, ensure that you have enabled RBACL policy enforcement on the VLAN and VRF instance.

When you enable RBACL statistics, each policy requires one entry in the hardware. If you do not have enough space remaining in the hardware, an error message appears, and you are unable to enable the statistics.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	[no] cts role-based counters enable Example: switch(config)# cts role-based counters enable	Enables or disables RBACL statistics. The default is disabled.
Step 3	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.
Step 4	exit Example: switch(config)# exit switch#	Exits global configuration mode.
Step 5	(Optional) show cts role-based counters [sgt {sgt-value any unknown}] [dgt {dgt-value any unknown}] Example: switch# show cts role-based counters sgt 10 dgt 20	Displays the configuration status of RBACL statistics and lists statistics for all RBACL policies. Optionally displays the total number of packets that match RBACL policies for a specific source group tag (SGT) or destination group tag (DGT). The <i>sgt-value</i> and <i>dgt-value</i> argument values range from 0 to 65519.
Step 6	(Optional) clear cts role-based counters Example: switch# clear cts role-based counters	Clears the RBACL statistics so that all counters are reset to 0.

Clearing Cisco TrustSec SGACL Policies

You can clear the Cisco TrustSec SGACL policies.

Before you begin

Ensure that you enabled Cisco TrustSec.

Procedure

	Command or Action	Purpose
Step 1	(Optional) show cts role-based policy Example:	Displays the Cisco TrustSec RBACL policy configuration.

	Command or Action	Purpose
	<code>switch# clear cts policy all</code>	
Step 2	clear cts policy {all peer <i>device-name</i> sgt <i>sgt-value</i> } Example: <code>switch# clear cts policy all</code>	Clears the policies for Cisco TrustSec connection information.

Related Topics

[Enabling the Cisco TrustSec SGT Feature](#) , on page 12

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:

Procedure

-
- 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 27
 - [Enabling SGACL Policy Enforcement on VRF Instances](#), on page 28
 - [Manually Configuring IPv4-Address-to-SGACL SGT Mapping for a VLAN](#), on page 30
 - [Manually Configuring SGACL Policies](#), on page 32
 - [Enabling the Cisco TrustSec SGT Feature](#) , on page 12
 - [Enabling Cisco TrustSec SXP](#) , on page 37
 - [Configuring Cisco TrustSec SXP Peer Connections](#), on page 38

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.

Procedure

	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 12

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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	cts sxp connection peer <i>peer-ipv4-addr</i> [source <i>src-ipv4-addr</i> password { default none required <i>password</i> } mode { speaker listener } [vrf <i>vrf-name</i>] Example: <pre>switch(config)# cts sxp connection peer 10.10.1.1 source 20.20.1.1 password default mode listener</pre>	<p>Configures the SXP address connection.</p> <p>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.</p> <p>The password keyword specifies the password that SXP should use for the connection using the following options:</p> <ul style="list-style-type: none"> • 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. <p>The speaker and listener keywords specify the role of the remote peer device.</p> <p>The vrf keyword specifies the VRF instance to the peer. The default is the default VRF instance.</p> <p>Note You cannot use the management (mgmt 0) interface for SXP.</p>
Step 3	exit Example: <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 4	(Optional) show cts sxp connections Example: <pre>switch# show cts sxp connections</pre>	Displays the SXP connections and their status.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

[Enabling the Cisco TrustSec SGT Feature](#) , on page 12

[Enabling Cisco TrustSec SXP](#) , on page 37

[Enabling SGACL Policy Enforcement on VRF Instances](#), on page 28

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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	cts sxp default password <i>password</i> Example: switch(config)# cts sxp default password A2Q3d4F5	Configures the SXP default password.
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 12

[Enabling Cisco TrustSec SXP](#) , on page 37

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.

Procedure

	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 <i>src-ip-addr</i> 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 12

[Enabling Cisco TrustSec SXP](#) , on page 37

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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	cts sxp reconcile-period <i>seconds</i> 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 12

[Enabling Cisco TrustSec SXP](#) , on page 37

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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	cts sxp retry-period <i>seconds</i> 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 12

[Enabling Cisco TrustSec SXP](#) , on page 37

Verifying the Cisco TrustSec Configuration

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

Command	Purpose
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 {all ethernet slot/port}	Displays the Cisco TrustSec configuration for the interfaces.
show cts role-based access-list	Displays Cisco TrustSec SGACL information.
show cts pacs	Displays Cisco TrustSec authorization information and PACs in the device key store.
show cts role-based enable	Displays Cisco TrustSec SGACL enforcement status.
show cts role-based policy	Displays Cisco TrustSec SGACL policy information.
show cts role-based sgt-map	Displays the 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.

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

  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
```

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

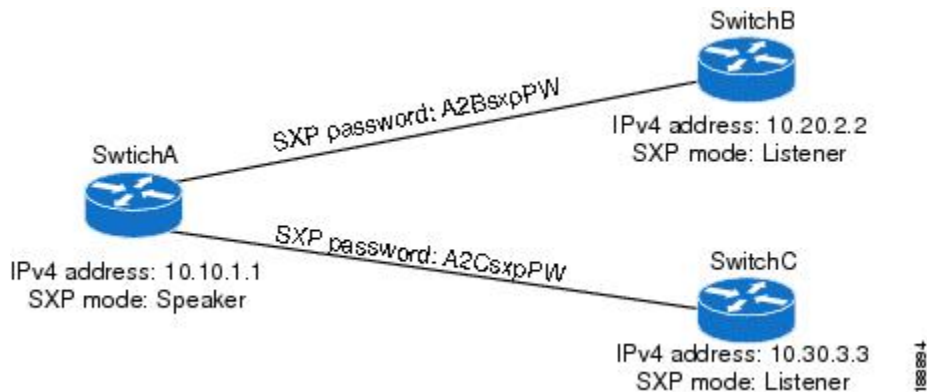
The following example shows how to manually configure Cisco TrustSec SGACLs:

```
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 6: 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
  
```

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	<i>Cisco NX-OS Licensing Guide</i>

Related Topic	Document Title
Command Reference	<i>Cisco Nexus 7000 Series NX-OS Security Command Reference</i>

Feature History for Cisco TrustSec

This table lists the release history for this feature.

Table 3: Feature History for Cisco TrustSec

Feature Name	Releases	Feature Information
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	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.