
# Configuring SGT Exchange Protocol

**Revised: January 29, 2016**
You can use the SGT Exchange Protocol (SXP) to propagate the Security Group Tags (SGTs) across network devices that do not have hardware support for Cisco TrustSec. This module describes how to configure Cisco TrustSec SXP on switches in your network.

This section includes the following topics:



# Cisco TrustSec SGT Exchange Protocol Feature Histories

For a list of supported Cisco TrustSec features per platform and the minimum required IOS release, see the *Cisco TrustSec Platform Support Matrix* at the following URL:

http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html

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

# Prerequisites for SGT Exchange Protocol

The Cisco TrustSec-SGT Over Exchange Protocol (SXP) network needs to be established before implementing SXP. This network has the following prerequisites:

- To use the Cisco TrustSec functionality on your existing device, ensure that you have purchased one of the followng security licenses:
  - IP Base License
  - IP Service License

**Note** Starting with Cisco IOS XE Release 16.5.1a, LAN Base License will support SXP configuration on Cisco Catalyst 3850 and Cisco Catalyst 3650 platforms.

- Cisco TrustSec SXP software must run on all network devices.
- Connectivity should exist between all network devices..

# Restrictions for SGT Exchange Protocol

**Note** Cisco TrustSec Exchange Protocol is supported only on physical interfaces and not on logical interfaces.

The following restrictions are applicable when running Cisco TrustSec in enforcement mode or inline tagging mode. These restrictions do not apply when these switches are used as an SXP speaker:

- An IP subnet address cannot be statically mapped to a Security Group Tag (SGT). You can only map IP addresses to an SGT. While configuring IP address-to-SGT mappings, the IP address prefix must be 32. (Applicable to Catalyst 3560-X and 3750-X Series Switches)
- If a port is configured in multi-authentication mode, all hosts connecting to that port must be assigned the same SGT. When a host tries to authenticate, it must be assigned the same SGT as the SGT assigned to a previously authenticated host. If a host tries to authenticate, and it has a different SGT to that of a previously authenticated host, the VLAN port to which these hosts belong is error-disabled. (Applicable to Catalyst 3560-X and 3750-X Series Switches)
- Cisco TrustSec enforcement mode on a VLAN trunk line supports only up to eight VLANs. If more than eight VLANs are configured on a VLAN trunk link and Cisco TrustSec is enabled on those VLANs, the switch ports on those VLAN trunk links will be error-disabled. (Applicable to Catalyst 3560-X, 3750-X, and 3850 Series Switches)
- Switches can assign SGT and apply the corresponding Security Group access control list (SGACL) to end hosts based on SGT Exchange Protocol (SXP) listening only if the end hosts are Layer 2 adjacent to the switch. (Applicable to Catalyst 3560-X and 3750-X Series Switches)

# Information About SGT Exchange Protocol



## SGT Exchange Protocol Overview

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

The Security Group Tag (SGT) Exchange Protocol (SXP) is one of several protocols that supports Cisco TrustSec. SXP is a control protocol for propagating IP-to-SGT binding information across network devices that do not have the capability to tag packets. Cisco TrustSec filters packets at the egress interface. During endpoint authentication, a host accessing the Cisco TrustSec domain (the endpoint IP address) is associated with an SGT at the access device through Dynamic Host Control Protocol (DHCP)

snooping and IP device tracking. The access device transmits that association or binding through SXP to Cisco TrustSec hardware-capable egress devices. These devices maintain a table of source IP-to-SGT bindings. Packets are filtered on the egress interface by Cisco TrustSec hardware-capable devices by applying security group access control lists (SGACLs). SXP passes IP-to-SGT bindings from authentication points to upstream devices in the network. This process allows security services on switches, routers, or firewalls to learn identity information from access devices.

SGTs can be assigned through any of the following Endpoint Admission Control (EAC) access methods:

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

SXP uses TCP as the transport protocol, and the TCP port 64999 for connection initiation. SXP uses Message Digest 5 (MD5) for authentication and integrity check. It has two defined roles—speaker (initiator) and listener (receiver).

# Security Group Tagging

Security Group Tag is a unique 16 bit tag that is assigned to a unique role. It represents the privilege of the source user, device, or entity and is tagged at the ingress of the Cisco TrustSec domain.

SXP uses the device and user credentials acquired during authentication for classifying packets by security groups (SGs) as they enter a network. This packet classification is maintained by tagging packets on the ingress to the Cisco TrustSec network so that they can be identified for the purpose of applying security and other policy criteria along the data path. 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. Static port Identification is used to lookup the SGT value for a particular endpoint connected to a port.

# SGT Assignment

The Security Group Tag (SGT) of a packet can be assigned at the port level when the packet comes tagged on a Cisco TrustSec link, or when a single endpoint authenticates on a port.

SGT of an incoming packet is determined in the following ways:

- When a packet that is tagged with an SGT comes on a trust port, the tag of the packet is considered as the SGT of the packet.
- When a packet is tagged with an SGT, but comes on an untrusted port, the SGT of the packet is ignored and the peer SGT is configured for the port.
- When a packet does not have an SGT, the peer SGT is configured for a port.
- Cisco TrustSec only allows a single host device to authenticate on a port (except for voice and data using separate VLANs). When a host is directly connected to a port, only a single peer SGT exists for that port. All packet from that port is assigned the same SGT.

The following methods of assigning SGTs are supported:

- IPM (dot1x, MAB, and Web Authentication)
- VLAN-to-SGT mapping Established when an authentication method provides an SGT for an authenticated entry already has an assigned IP address. A switch process monitors endpoint sessions and detects changes or removal of IP-to-SGT binding.

- SXP (SGT Exchange Protocol) Listener

# Layer 3 SGT Transport Between Cisco TrustSec Domains

**Note** This feature is supported only on Cisco Catalyst 6500 Series Switches.

You can configure Layer 3 SGT Transport on Cisco TrustSec gateway devices on the edges of a network domain that has no Cisco TrustSec-capable devices.

When configuring Cisco TrustSec Layer 3 SGT transport, consider these usage guidelines and restrictions:

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

# How to Configure SGT Exchange Protocol

- Creating Syslogs to Capture Changes of IP Address-to-SGT Mapping Learned Through SXP, page 6-9
- Configuring Layer 3 SGT Transport Between Cisco TrustSec Domains, page 6-10

To configure Cisco TrustSec SXP, follow these steps:

**Step 1** Enable the Cisco TrustSec feature (see the "Configuring Identities, Connections, and SGTs" chapter).

**Step 2** Enable Cisco TrustSec SXP (see the "Enabling Cisco TrustSec SXP" section on page 6-5).

**Step 3** Configure SXP peer connections (see the "Configuring an SXP Peer Connection" section on page 6-5).

# Enabling Cisco TrustSec SXP

You must enable Cisco TrustSec SXP before you can configure peer connections. To enable Cisco TrustSec SXP, perform this task:

### Detailed Stepss

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch# enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 1** | `Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | `Switch(config)# [no] cts sxp enable` | Enables SXP for Cisco TrustSec. |
| **Step 3** | `Switch(config)# end` | Exits global configuration mode and returns to privileged EXEC mode |

# Configuring an SXP Peer Connection

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

**Note** If a default SXP source IP address is not configured and you do not configure an SXP source address in the connection, the Cisco TrustSec software derives the SXP source IP address from existing local IP addresses. The SXP source address might be different for each TCP connection initiated from the switch.

To configure an SXP peer connection, perform this task:

### Detailed Steps

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch# enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 1** | `Switch# configure terminal` | Enters global configuration mode. |

| | Command | Purpose |
|---|---|---|
| **Step 2** | `Switch(config)# cts sxp connection peer peer-ipv4-addr [source src-ipv4-addr] password {default \| none} mode {local \| peer} {speaker \| listener} [vrf vrf-name]` | Configures the SXP address connection.<br>The optional **source** keyword specifies the IPv4 address of the source device. If no address is specified, the connection will use the default source address, if configured, or the address of the port.<br>The **password** keyword specifies the password that SXP will 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**—Do not use a password.<br>The **mode** keyword specifies the role of the remote peer device:<br>• **local**—The specified mode refers to the local device.<br>• **peer**—The specified mode refers to the peer device.<br>• **speaker**—Default. Specifies that the device is the speaker in the connection.<br>• **listener**—Specifies that the device is the listener in the connection.<br>The optional **vrf** keyword specifies the VRF to the peer. The default is the default VRF. |
| **Step 3** | `Switch(config)# exit` | Exits global configuration mode and returns to privileged EXEC mode |
| **Step 4** | `Switch# show cts sxp connections` | (Optional) Displays the SXP connection information. |

# Configuring the Default SXP Password

By default, SXP uses no password when setting up connections. You can configure a default SXP password for the switch. In Cisco IOS Release 12.2(50)SY and later releases, you can specify an encrypted password for the SXP default password.

To configure a default SXP password, perform this task:

### Detailed Steps

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch# enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 1** | `Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | `Switch(config)# cts sxp default password [0 \| 6 \| 7] password` | Configures the SXP default password. You can enter either a clear text password (using the **0** or no option) or an encrypted password (using the **6** or **7** option). The maximum password length is 32 characters. |
| **Step 3** | `Switch(config)# end#` | Exits global configuration mode and returns to privileged EXEC mode. |

# Configuring the Default SXP Source IP Address

SXP uses the default source IP address for all new TCP connections where a source IP address is not specified. There is no effect on existing TCP connections when you configure the default SXP source IP address.

To configure a default SXP source IP address, perform this task:

### Detailed Steps

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch# enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 1** | `Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | `Switch(config)# cts sxp default source-ip src-ip-addr` | Configures the SXP default source IP address. |
| **Step 3** | `Switch(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

# Changing the SXP Reconciliation Period

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

To change the SXP reconciliation period, perform this task:

### Detailed Steps

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch# enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 1** | `Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | `Switch(config)# cts sxp reconciliation period` *seconds* | Changes the SXP reconciliation timer. The default value is 120 seconds (2 minutes). The range is from 0 to 64000. |
| **Step 3** | `Switch(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

# Changing the SXP Retry Period

The SXP retry period determines how often the Cisco TrustSec software retries an SXP connection. When an SXP connection is not successfully set up, the Cisco TrustSec software makes a new attempt to set up the connection after the SXP retry period timer expires. The default value is 120 seconds. Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted.

To change the SXP retry period, perform this task:

**Detailed Steps**

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch# enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 1** | `Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | `Switch(config)# cts sxp retry period` *seconds* | Changes the SXP retry timer. The default value is 120 seconds (2 minutes). The range is from 0 to 64000. |
| **Step 3** | `Switch(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

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

When the **cts sxp log binding-changes** command is configured in global configuration mode, SXP syslogs (sev 5 syslog) are generated whenever a change to IP address to SGT binding occurs (add, delete, change). These changes are learned and propagated on the SXP connection. The default is **no cts sxp log binding-changes**.

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

**Detailed Steps**

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch# enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 1** | `Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | `Switch(config)# cts sxp log binding-changes` | Enables logging for IP to SGT binding changes. |
| **Step 3** | `Switch(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

# Configuring Layer 3 SGT Transport Between Cisco TrustSec Domains

You can configure Layer 3 SGT Transport on Cisco TrustSec gateway devices on the edges of a network domain that has no Cisco TrustSec-capable devices.

**Note** This feature is supported only on Cisco Catalyst 6500 Series Switches.

To configure Layer 3 SGT Transport, perform this task:

### Detailed Steps for Catalyst 6500

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch# enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 1** | `Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | `Switch(config)# [no] cts policy layer3 {ipv4 \| ipv6} traffic acl-name` | (Optional) Specifies the fallback traffic policy to be applied when the authentication server is not available for downloading the traffic policy.<br>• *acl-name*—The name of a traditional interface ACL already configured on the device.<br>See the additional usage notes following this task. |
| **Step 3** | `Switch(config)# [no] cts policy layer3 {ipv4 \| ipv6} exception acl-name` | (Optional) Specifies the fallback exception policy to be applied when the authentication server is not available for downloading the exception policy.<br>See the additional usage notes following this task. |
| **Step 4** | `Switch(config)# interface type slot/port` | Specifies an interface and enters interface configuration mode. |
| **Step 5** | `Switch(config-if)# [no] cts layer3 {ipv4 \| ipv6} trustsec forwarding` | (Configured on a Cisco TrustSec-capable physical port) Specifies that egress traffic on this interface will use Cisco TrustSec Layer 3 SGT transport encapsulation as determined by the traffic and exception policies. |
| | `Switch(config-if)# [no] cts layer3 {ipv4 \| ipv6} policy` | (Configured on a routed port or SVI) Specifies that egress traffic on this interface will use Cisco TrustSec Layer 3 SGT transport encapsulation as determined by the traffic and exception policies. |
| **Step 6** | `Switch(config-if)# end` | Exits interface configuration and returns to privileged EXEC mode. |
| **Step 7** | `Switch# show cts policy layer3 {ipv4 \| ipv6}` | (Optional) Displays the Layer 3 SGT transport configuration on the interfaces. |

# Configuration Examples for SGT Exchange Protocol



## Example: Enabling Cisco TrustSec SXP and an SXP Peer Connection

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

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

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

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

## Example: Configuring the Default SXP Password and Source IP Address

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

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

## Example: Configuring Layer 3 SGT Transport Between Cisco TrustSec Domains

**Note** This feature is supported only on Cisco Catalyst 6500 Series Switches.

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

```
Switch# configure terminal
Switch(config)# ip access-list extended traffic-list
Switch(config-ext-nacl)# permit ip any 10.1.1.0 0.0.0.255
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended exception-list
Switch(config-ext-nacl)# permit ip any 10.2.2.0 0.0.0.255
Switch(config-ext-nacl)# exit
Switch(config)# cts policy layer3 ipv4 traffic traffic-sgt
```

```
Switch(config)# cts policy layer3 ipv4 exception exception-list
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# cts layer3 trustsec ipv4 forwarding
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch#
```

# Verifying SGT Exchange Protocol Connections

To view SXP connections, perform this task:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch# show cts sxp connections` | Displays detailed information about the SXP status and connections. |
| **Step 1** | `Switch# show cts sxp connections [brief]` | Displays brief information about the SXP status and connections. |

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

```
Switch# show cts sxp connections

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

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

```
Switch# show cts sxp connections brief

SXP              : Enabled
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running

-------------------------------------------------------------------------------
Peer_IP          Source_IP        Conn Status       Duration
-------------------------------------------------------------------------------
10.1.3.1         10.1.3.2         On                6:00:09:13 (dd:hr:mm:sec)

Total num of SXP Connections = 1
```

# Feature Information for SGT Exchange Protocol

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

**Note** Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

*Table 1 Feature Information for SGT Exchange Protocol*

| Feature Name | Releases | Feature Information |
|---|---|---|
| L3 SGT Transport | Cisco IOS Release 12.2(50) SY | This feature was introduced on the Catalyst 6500 Series Switches.<br>**Note** This feature is only supported on Catalyst 6500 Series Switches. |
| SGT Exchange Protocol | Cisco IOS Release 12.2(50)SY<br>Cisco IOS Release 15.2(3)E<br>Cisco IOS Release 15.2(4)E1 | The SGT Exchange Protocol (SXP) propagates the Security Group Tags (SGTs) across network devices that do not have hardware support for Cisco TrustSec.<br>In Cisco IOS Release 12.2(50)SY, this feature was introduced on Cisco Catalyst 6500 Series Switches.<br>In Cisco IOS Release 15.2(3)E, this feature was introduced on Cisco Catalyst 2960-CX Series Switches.<br>In Cisco IOS Release 15.2(4)E1, this feature was introduced on Cisco Catalyst 3560-CX Series Switches. |