SGT Exchange Protocol

Feature History for SXP

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

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

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

SGT Exchange Protocol

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

Cisco Group-Based Policy

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

How SGTs Are Used in the Network

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

SGT Assignment Mechanisms

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

- Packets with SGT on Trusted Ports

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

- Packets with SGT on Untrusted Ports

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

- Packets without SGT

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

SGT Assignment Methods

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

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

- Web Authentication

Supported SGT Assignment Methods

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

- Endpoint Admission Control (EAC)

  Includes 802.1X, MAB, and Web Authentication.

- VLAN-to-SGT Mapping

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

- SXP Listener

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

- IP SGT

  Assigns SGTs based on IP addresses.

- Subnet SGT

  Assigns SGTs based on IP subnets.

- Port SGT

  Assigns SGTs at the port level.

- Caching SGT

  Stores and reuses previously assigned SGTs for efficiency.

Endpoint Authentication and SGT Association

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

Role of SXP in Security Group Tag Propagation

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

SXP Protocol Details

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

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

The protocol defines two operational roles:

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

SXP Version 5

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

SXP Version 5 Mappings

The following are the SXP Version 5 mappings:

- Exporting Mappings:

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

- Importing Mappings:

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

SXP Operation Mode

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

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

Guidelines to configure SXP

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

How to Configure SXP

These sections provide configuration information on how to configure SXP.

Configure a Device SGT Manually

In a normal Cisco Group-Based Policy operation, the authentication server assigns an SGT to the device for packets originating from the device. You can manually configure an SGT to be used if the authentication server is not accessible, but an authentication server-assigned SGT will take precedence over a manually-assigned SGT.

To manually configure an SGT on the device, perform this task:

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **cts sgt** *tag*

Example:

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

Configures the SGT for packets sent from the device.

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

Step 4 **exit**

Example:

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

Exits configuration mode.

Configure an SXP Peer Connection

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

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

Toconfigure an SXP peer connection, perform this task:

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

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

Example:

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

Configuresthe SXP address connection.

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

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

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

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

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

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

Step 4 **exit**

Example:

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

Exits global configuration mode and returns to privileged EXEC mode

Step 5 **show cts sxp connections**

Example:

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

(Optional) Displays the SXP connection information.

Configure the Default SXP Password

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

To configure a default SXP password, perform this task:

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

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

Example:

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

Configures the SXP default password.

You can enter

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

The maximum password length is 32 characters.

Step 4 **exit**

Example:

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

Exits global configuration mode and returns to privileged EXEC mode

Configure the Default SXP Source IP Address

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

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

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

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

Example:

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

Configures the SXP default source IP address.

Step 4 **exit**

Example:

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

Exits global configuration mode and returns to privileged EXEC mode.

Change the SXP Reconciliation Period

After a peer terminates an SXP connection, an internal hold-down timer starts. If the peer reconnects before the internal hold-down timer expires, the SXP reconciliation period timer starts. While the SXP reconciliation period timer is active, the Cisco Group-Based Policy software retains the SGT mapping entries learned from the previous connection and removes invalid entries.

Setting the SXP reconciliation period to 0 seconds disables the timer and causes all entries from the previous connection to be removed.

To change the SXP reconciliation period, perform this task:

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

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

Example:

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

Changes the SXP reconciliation timer.

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

Step 4 **exit**

Example:

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

Exits global configuration mode and returns to privileged EXEC mode.

Change the SXP Retry Period

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

To change the SXP retry period, perform this task:

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

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

Example:

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

Changes the SXP retry timer.

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

Step 4 **exit**

Example:

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

Exits global configuration mode and returns to privileged EXEC mode.

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

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

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

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

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

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

Example:

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

Enables logging for IP to SGT binding changes.

Step 4 **exit**

Example:

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

Exits global configuration mode and returns to privileged EXEC mode.

Configure an SXP Export List

To configure an SXP export list, perform this task.

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

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

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

Example:

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

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

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

Example:

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

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

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

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

Example:

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

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

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

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

Step 6 **end**

Example:

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

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

Configure an SXP Import List

To configure an SXP import list, perform this task:

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

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

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

Example:

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

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

Step 4 **vlan-list**

Example:

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

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

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

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

Example:

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

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

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

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

Step 6 **end**

Example:

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

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

Configure an SXP Export-Import Group

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

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

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

Example:

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

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

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

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

Example:

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

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

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

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

Example:

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

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

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

Step 6 **peer** *address_name*

Example:

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

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

Step 7 **end**

Example:

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

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

Verify SGT Exchange Protocol Connections

Table 1:

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

Configuration Examples for SXP

These sections provide configuration examples for SXP.

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

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

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

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

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

Example: Configure the Default SXP Password and Source IP Address

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

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

Example: Verify SGT Exchange Protocol Connections

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

```
Device# show cts sxp connections

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

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

```
Device# show cts sxp connections brief

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

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

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

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

   Export-list-name: export_list_1
   vrf red_vrf
   vrf blue_vrf

Device# show cts sxp export-list

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

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

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

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

Device# show cts sxp export-import-group listener

Global Listener export-import-group: Not configured

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

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


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

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

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

    Global Listener export-import-group: Not configured

    Export-import-group: group_1
    Import-list-name: import_list_1
    Import-list-content:
```

```
       vlan-list
    Peer-list: 1.1.1.1, 2.2.2.2, 3.3.3.3

Device# show cts sxp export-import-group global

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