Cisco TrustSec Integration

Table 1: Feature History

Feature Name	Release Information	Description
Support for SGT Propagation with Cisco TrustSec Integration	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature enables Cisco IOS XE Catalyst SD-WAN edge devices to propagate Security Group Tag (SGT) inline tags that are generated by Cisco TrustSec-enabled switches in the branches to other edge devices in the Cisco Catalyst SD-WAN network. While Cisco TrustSec-enabled switches do classification, propagation (inline SGT tagging) and enforcement on the branches, Cisco IOS XE Catalyst SD-WAN device devices carry the inline tags across the edge devices.
Enhanced SGACL Logging	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This feature enhances SGACL logging capability on Cisco IOS XE Catalyst SD-WAN devices by utilizing High Speed Logging (HSL). HSL offers a more efficient and scalable method for logging security events, ideal for high-traffic network environments.
SGT Propagation with Cisco TrustSec Integration using Configuration Groups	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	With this feature you can configure SGT propagation using TrustSec feature under **Other Profile** in a configuration group in Cisco SD-WAN Manager.

This chapter contains the following sections:

- Support for SGT Propagation with Cisco TrustSec Integration, on page 2
- SGT Propagation Using Inline Tagging, on page 2
- SGT Propagation Using SXP, on page 10
- SGACL for Cisco TrustSec, on page 20
- SGT Enforcement, on page 28
- Monitor SXP Connections and SGT Enforcement, on page 30

Support for SGT Propagation with Cisco TrustSec Integration

Cisco TrustSec is an end-to-end network infrastructure that provides a scalable architecture for the enforcement of role-based access control, identity-aware networking, and data confidentiality to secure the network and its resources. Cisco TrustSec uses Security Group Tag (SGT) to represent user and device groups. The switches, routers, and firewalls inspect these tags and enforce SGT-based traffic policies.

Cisco TrustSec is defined in three phases—classification, propagation, and enforcement. After traffic is classified, the SGT is propagated from where classification took place, to where enforcement action is invoked. This process is called propagation. Cisco TrustSec offers two types of SGT propagation, Inline tagging and Security Group Tag Exchange Protocol (SXP).

With inline tagging, a special Ethernet frame is used to propagate these SGTs between network hops where the policies are enforced based on the SGT policy. After the introduction of this feature, Cisco IOS XE Catalyst SD-WAN devices support propagation of SGT. See Configure SGT Inline Tagging Using Feature Templates, on page 6

When Inline tagging is not used (or not possible), an SXP protocol can be used to dynamically exchange IP address binding to SGT between Cisco IOS XE Catalyst SD-WAN devices. You can also manually configure IP address to SGT binding, statically, in Cisco SD-WAN Manager. See SGT Propagation Using SXP, on page 10

Enforcement of SGT is achieved using Security Group Access Control Lists (SGACL) where policies can be dynamically or statically configured and applied to the egress traffic on the network. See SGT Enforcement, on page 28

Benefits of Cisco TrustSec

- Provides secure access to network services and applications based on user and device identity.
- Applies policies across the network using tags instead of IP addresses.
- Enforces policies easily. SGT propagation simplifies network access and security operations with software-defined segmentation.
- Scales fast and enforces policies consistently across the network. SGT propagation helps streamline security policy management across domains.
- Reduces risk and segments devices without redesigning the network. You can easily manage access to enterprise resources and restrict lateral movement of threats with microsegmentation.

SGT Propagation Using Inline Tagging

One of the SGT propagation methods is using Inline tagging where a special Ethernet frame is used to propagate these SGTs between network hops where the policies are enforced based on the SGT policy. For more information see, SGT Propagation in Cisco Catalyst SD-WAN, on page 3

Prerequisites

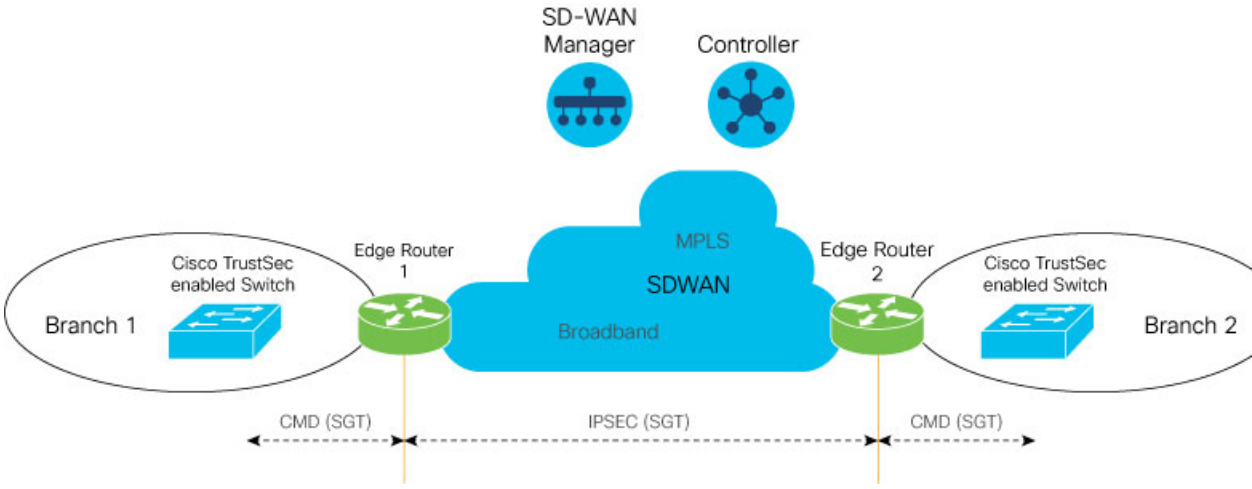
- Branches must be equipped with Cisco TrustSec-enabled switches that are capable of handling SGT inline tagging.

• Cisco IOS XE Catalyst SD-WAN devices running on Cisco IOS XE Catalyst SD-WAN device and later.

SGT Propagation in Cisco Catalyst SD-WAN

The following image illustrates how SGT is propagated in Cisco Catalyst SD-WAN from one branch to another.

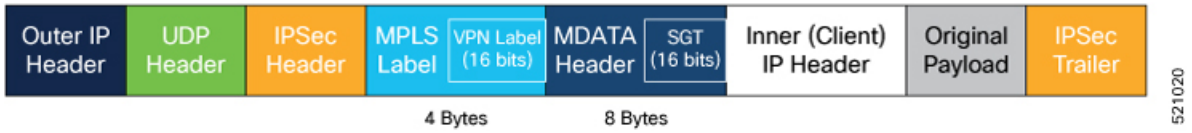
Figure 1: SGT Propagation in Cisco Catalyst SD-WAN



In this illustration, Branch 1 and Branch 2 are equipped with Cisco TrustSec-enabled switches, and these branches are connected to the Cisco IOS XE Catalyst SD-WAN devices. The Cisco TrustSec switch in Branch 1 performs SGT Inline tagging in the Ethernet CMD frame toward Edge Router 1. Edge Router 1 then de-encapsulates the CMD frame, extracts the SGT, and propagates it over Cisco Catalyst SD-WAN IPSec or GRE tunnels. The Edge Router 2 on Cisco Catalyst SD-WAN extracts the SGT from Cisco Catalyst SD-WAN, generates the Ethernet CMD frame, and copied the SGT that is recieved. The Cisco TrustSec switch on Branch 2 inspects the SGT, and looks it up against the destination SGT to determine if the traffic must be allowed or denied.

The following image is an illustration of SGT being carried through in a Cisco Catalyst SD-WAN packet and an additional eight bytes of data is added to it.

Figure 2: SGT Propagation



The following table describes how SGT propagation between edge devices in the Cisco Catalyst SD-WAN network varies based on the type of edge device and software release installed on the device.

Table 2: SGT Propagation with Cisco IOS XE Catalyst SD-WAN Devices of Different Releases Interconnected in Cisco Catalyst SD-WAN

Cisco IOS XE Catalyst SD-WAN Device at Source	Cisco Catalyst SD-WAN Device at Destination	Result
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Cisco IOS XE Catalyst SD-WAN device with Cisco IOS XE Catalyst SD-WAN Release 17.3.1a or later	• Traffic with SGT is forwarded to the Cisco IOS XE Catalyst SD-WAN device. • If Cisco TrustSec is enabled on the Cisco IOS XE Catalyst SD-WAN device, traffic with SGT along with the CMD header is forwarded to the switch. If Cisco TrustSec is not enabled on the Cisco IOS XE Catalyst SD-WAN device, traffic without the SGT and CMD header is forwarded to the switch.
	Cisco IOS XE Catalyst SD-WAN device with Cisco IOS XE Catalyst SD-WAN Release Amsterdam 17.2.x and earlier.	Traffic without SGT is forwarded to the Cisco IOS XE Catalyst SD-WAN device.
	Cisco vEdge device	Traffic without SGT is forwarded to the Cisco vEdge device.

Supported Platforms and NIMs

Supported Platforms

The following devices support propagation of SGT inline tagging:

- Cisco 1100 Integrated Services Router
- Cisco CSR 1000v Series Cloud Services Router
- Cisco 4300 Integrated Services Router
- Cisco 4400 Integrated Services Router
- Cisco ASR 1001-X Router
- Cisco ASR 1001-HX Router
- Cisco ASR 1002-X Router
- Cisco ASR 1002-HX Router
- Cisco 5000 Series Enterprise Network Compute System
- Cisco Catalyst 8000V Router

- Cisco Catalyst 8200 Router
- Cisco Catalyst 8300 Router
- Cisco Catalyst 8500 Router

Supported NIMs

The following WAN NIMs are supported for Cisco 4000 Series Integrated Services Routers platforms:

- NIM-1GE-CU-SFP
- NIM-2GE-CU-SFP
- SM-X-4x1G-1x10G
- SM-X-6X1G

The following WAN NIMs are supported on Cisco Catalyst 8200 Router and Cisco Catalyst 8300 Router platforms:

- C-NIM-2T
- C-NIM-1M
- C-NIM-1X

Limitations for SGT Propagation

- Enabling the **cts manual** command momentarily causes the interface to flap. Therefore, we recommend that you configure Cisco TrustSec manual on the Cisco IOS XE Catalyst SD-WAN device before configuring it on the switch.
- You cannot enable Cisco TrustSec by using the **cts manual** command on port-channel sub-interfaces.
- TrustSec inline tagging is not supported on service-side port channels.
- If you are configuring subinterfaces on a Cisco IOS XE Catalyst SD-WAN device, Cisco TrustSec must be enabled on the physical interface and on all the subinterfaces.
- Only devices on Cisco IOS XE Catalyst SD-WAN Release 17.3.1a support propagation of SGT.
- Inline tagging is supported only on the L3 (WAN) ports of the Cisco IOS XE Catalyst SD-WAN devices, and not on switch ports.
- For releases prior to Cisco IOS XE Release 17.3.3, Cisco Catalyst SD-WAN multicast overlay traffic is not supported on interfaces enabled with the Cisco TrustSec feature.

Configure SGT Inline Tagging Using Configuration Groups

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure the **Ethernet Interface** feature in both the Transport and Management and Service profile.

Step 3 Enable SGT propagation.

Field	Description
Enable SGT Propogation	Enable this option to use the Cisco TrustSec Security Group Tag (SGT) propagation feature.
Propagate	Enable this option to propagate SGT in Cisco Catalyst SD-WAN.
Security Group Tag	Enter a value that can be used as a tag. Range: 2 to 65519
Trusted	Enable the trusted option. When you enable this option, the SGT value received in the Ethernet packet on this interface is trusted and is used by the device for any security group aware policy enforcement.
Enable Enforced Propagation	Enable this option to start SGT enforcement on the interface.
Enforced Security Group Tag	Enter a value that can be used as a tag for enforcement. Range: 2 to 65519

What to do next

Also see Deploy a configuration group.

Configure SGT Inline Tagging Using Feature Templates

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Choose a Cisco IOS XE Catalyst SD-WAN device from the list.
4. Choose one of the available Cisco VPN Interface templates, for example, **Cisco VPN Interface Ethernet** .

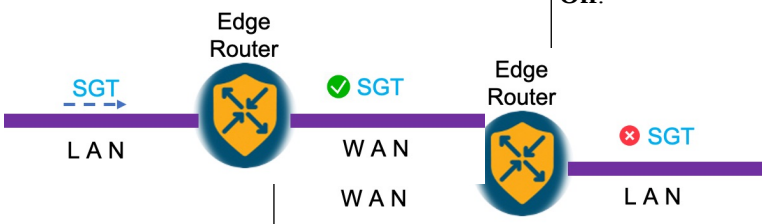
5. Enter a name and a description for the feature template.
6. To enable SGT propagation, use the following options:
   - For Transport interface (VPN 0):
     a. Click **Tunnel**.
     b. In the **CTS SGT Propagation** field, click **On** to enable SGT propagation for inline tagging. By default, this option is disabled.
   - For service-side interface (VPN x):
     a. Click **TrustSec**.
     b. From the **Enable SGT Propagation** drop-down list, choose **Global**, and then click **On**. Additional propagation options are displayed.
     c. To propagate SGT in Cisco Catalyst SD-WAN, set **Propagate** to **On**.

The following table displays the SGT propagation options, and the LAN to WAN and WAN to LAN behavior based on the option you choose for SGT propagation. The options are displayed in the following table and available to you only if you set the **Enable SGT Propagation** to **On**.

Table 3: SGT Propagation options

SGT Propagation Options	LAN to WAN	WAN to LAN	Notes
Propagate = On **Security Group Tag** = <SGT Value> **Trusted** = On	SGT is propagated from LAN to WAN.	SGT is propagated from WAN to LAN.	This is the most common configuration. Usually, the SGT value is 2
Propagate = On **Security Group Tag** = <SGT Value> **Trusted** = Off	SGT is propagated from LAN to WAN with a configured SGT value.	SGT is propagated from WAN to LAN. No effect to the incoming SGT.	Overrides the incoming SGT from LAN to WAN because **Trusted** is set to **Off**

SGT Propagation Options	LAN to WAN	WAN to LAN	Notes
Propagate = Off **Security Group Tag** = <SGT Value> **Trusted** = Off	SGT is propagated from LAN to WAN with a configured SGT value.	SGT is not added to the LAN packets. SGT is not propagated to	Overrides the incoming SGT from LAN to WAN because **Trusted** is set to **Off**.
Propagate = On	SGT propagated from LAN to WAN with SGT value	SGT is propagated from WAN to LAN with SGT value 0.	This can be configured only on a physical interface if there are existing sub interfaces.
Propagate = Off **Security Group Tag** = <SGT Value> **Trusted** = On	NA	NA	This configuration is not supported.



Note

- Enterprise Network Compute System (ENCS) LAN and WAN ports allow propagation of SGT tags on its physical ports. The LAN interfaces must be connected to the LAN side and the WAN interfaces must be connected to the WAN side of the network. You must deploy Cisco Catalyst 8000V router or Integrated Services Virtual router to process the tagging.

7. Click **Save**.
8. Configure the routing protocols using the Cisco SD-WAN Manager templates. You can choose to use any of the routing protocols. For BGP template, see Configure BGP Using Cisco SD-WAN Manager templates.
9. Attach the feature template to the device template.

Configure SGT Inline Tagging Using CLI

The following example shows SGT propagation configured on a Cisco IOS XE Catalyst SD-WAN device . In this example:

- A network connection is established between a switch in the branch and a Cisco IOS XE Catalyst SD-WAN device.
- Two VRF instances, and subinterfaces are configured on the Cisco IOS XE Catalyst SD-WAN device.
- SGT propagation is enabled on the subinterfaces.
- SGT propagation is configured on the network using BGP.

```
! VRF 1
vrf definition 1
 rd 1:1
 !

! VRF 2
vrf definition 2
 rd 1:2
 !

! Link between switch and router
interface GigabitEthernet0/0/2
 no ip address
 no ip redirects
 negotiation auto
 ip mtu  1504
 mtu 1504
cts manual
!

! sub-interface on VRF 1
interface GigabitEthernet0/0/2.2
 encapsulation dot1Q 2
 vrf forwarding 1
 ip address 77.27.9.2 255.255.255.0
 ip mtu 1500
 cts manual
  policy static sgt 2 trusted
!

! sub-interface on VRF 2
interface GigabitEthernet0/0/2.3
 encapsulation dot1Q 3
 vrf forwarding 2
 ip address 77.27.19.2 255.255.255.0
 ip mtu 1500
 cts manual
  policy static sgt 2 trusted
!

! BGP configuration
router bgp 64005
 bgp log-neighbor-changes
 distance bgp 20 200 20
 !
 ! BGP neighbor VRF 1
 address-family ipv4 vrf 1
  network 77.27.9.0 mask 255.255.255.0
  redistribute connected
  redistribute static
  redistribute omp
  neighbor 77.27.9.1 remote-as 64006
  neighbor 77.27.9.1 activate
  neighbor 77.27.9.1 send-community both
```

```
exit-address-family
!
! BGP neighbor VRF 2
address-family ipv4 vrf 2
 redistribute connected
 redistribute static
 redistribute omp
 neighbor 77.27.19.1 remote-as 64006
 neighbor 77.27.19.1 activate
 neighbor 77.27.19.1 send-community both
exit-address-family
!
```

View SGT Propagation Configuration

To view Cisco TrustSec SGT Propagation configuration, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices.
3. Click **Real Time** in the left pane.
4. From **Device Options** drop-down list, choose **Interface TrustSec** to view SGT propagation configuration.

SGT Propagation Using SXP

Table 4: Feature History

Feature Name	Release Information	Description
SGT Propagation Using SXP and SGACL Enforcement	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	With this feature, Cisco IOS XE Catalyst SD-WAN devices can exchange SGT over the overlay network using SXP. Use SXP when your hardware does not support Inline propagation of SGTs. This feature also extends support for SGACL enforcement on Cisco IOS XE Catalyst SD-WAN devices by configuring SGACL policies.

You can use SXP to propagate SGTs across network devices if your hardware does not support inline tagging. Using Cisco Identity Services Engine (ISE), you can create an IP-to-SGT binding (Dynamic IP-SGT) and then download IP-SGT binding using SXP to a Cisco IOS XE Catalyst SD-WAN device for propagation of the SGT over the Cisco Catalyst SD-WAN network. See Configure SXP for Dynamic IP-SGT Binding Using Feature Templates, on page 15.

Alternatively, you have the option to manually configure IP-SGT binding (Static IP-SGT) and then push the configuration to a Cisco IOS XE Catalyst SD-WAN device using a CLI Add-On template to propagate SGT over the Cisco Catalyst SD-WAN network. See Configure Static IP-SGT Binding Using Cisco SD-WAN Manager, on page 18.

Prerequisites

- You must enable Cisco TrustSec and propagation through SXP on the devices in a Cisco Catalyst SD-WAN network.
- Cisco ISE version must be 2.6 or later.

Points to Consider

- Cisco ISE has a limit on the number of SXP sessions it can handle. Therefore, as an alternative, you can use SXP reflector for horizontal scaling.
- Static IP-SGT configuration is based on the CLI Add-On template and not using a Feature template in Cisco SD-WAN Manager.
- From Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, Cisco vManage Release 20.5.1, we recommend that you use an SXP reflector to establish an SXP peering with Cisco IOS XE Catalyst SD-WAN devices. This is because when you use an SXP Reflector, the SXP filtering option ensures that only relevant IP-SGT bindings for the local service side networks are pushed down to the Cisco IOS XE Catalyst SD-WAN device. Overlapping or remote entries coming though SXP can have an adverse effect on the Overlay routing. See SXP Reflectors, on page 13

Limitations for SGT Propagation Using SXP

- 802.1x-based SGT assignment is not supported.
- SGACL policies cannot be downloaded using HTTP.
- SXP filter is not supported.
- Static SGACLs using IPv6 is not supported through CLI or Cisco SD-WAN Manager.
- SGACL policies cannot be enforced on the ingress traffic, only on egress traffic in a Cisco Catalyst SD-WAN network.
- The option to cache SGT is not available.
- An SXP connection with an IPv6 version is not supported.
- You cannot have overlapping of OMP routes for the prefixes bound to SGTs.
- SXP Node ID must be explicitly configured preferably with a system IP.
- Cisco TrustSec feature is not supported with Federal Information Processing Standard (FIPS) mode enabled. If FIPS mode is enabled, download of Protected Access Credential (PAC) key fails.
- Cisco TrustSec feature is not supported for more than 24K SGT Policies in controller mode.
- SXP connections over NAT-enabled interfaces are not supported when using the default password. This results in connection failures and flapping. Instead, use password as **`none`** for SXP over NAT.

Supported Platforms and NIMs

Supported Platforms

The following devices support propagation of SGT using SXP:

- Cisco 1000 Series Integrated Services Router
- Cisco 1100 Integrated Services Router (on L3 [WAN] ports)
- Cisco Integrated Services Virtual Router (on L3 [WAN] ports)
- Cisco CSR 1000v Series Cloud Services Router
- Cisco 4300 Integrated Services Router
- Cisco 4331 Integrated Services Router
- Cisco 4351 Integrated Services Router
- Cisco 4400 Integrated Services Router
- Cisco ASR 1001-X Router
- Cisco ASR 1001-HX Router
- Cisco ASR 1002-X Router
- Cisco ASR 1002-HX Router
- Cisco ASR 1006-X Router
- Cisco Catalyst 8000V Router
- Cisco Catalyst 8200 Router
- Cisco Catalyst 8300 Router
- Cisco Catalyst 8500 Router

Supported NIMs

The following WAN NIMs are supported on Cisco 4000 Series Integrated Services Routers platforms:

- NIM-1GE-CU-SFP
- NIM-2GE-CU-SFP
- SM-X-4x1G-1x10G
- SM-X-6X1G

Propagate SGT Using SXP

If hardware does not support SGT propagation through inline tagging, you can propagate SGT using SXP.

If a branch is equipped with Cisco TrustSec-enabled hardware, the branch is referred to as a TrustSec branch. You can propagate SGTs to a TrustSec branch through inline tagging. For information about Inline Tagging, see SGT Propagation in Cisco Catalyst SD-WAN, on page 3.

If a branch is not equipped with Cisco TrustSec-enabled hardware, the branch is referred to as a non-TrustSec branch. You can propagate SGT to a non-TrustSec branch using SXP.

In the case of a non-TrustSec branch, for SD-WAN ingress, a Cisco IOS XE Catalyst SD-WAN device performs SGT tagging based on source IP address of the packet and IP-SGT binding dynamically learned from ISE using SXP or based on static IP-SGT binding configuration. For SD-WAN egress, the Cisco IOS XE Catalyst SD-WAN device performs a destination SGT lookup based on the destination IP address using IP-SGT bindings (received through SXP or static configuration), and the SGT is determined. Policies for the SGT traffic on SD-WAN egress is enforced either by downloading SGACL policies from ISE or by configuring static SGACL policies.

SXP Reflectors

SXP reflectors are used when you need to have multiple connections to communicate information about IP-SGT bindings over a network. Because Cisco ISE has a limit on the number of SXP sessions it can handle, as an alternative, you can use Cisco ASR1000 routers, with the SXP reflector functionality enabled for horizontal scaling between ISE and the Cisco IOS XE Catalyst SD-WAN device.

You can configure an SXP connection to an SXP reflector the same way you configure an SXP connection to ISE. For information about configuring SXP reflector, see Configure SXP Reflector Using the CLI, on page 20.

We recommend an SXP reflector to establish SXP peering with Cisco IOS XE Catalyst SD-WAN devices. When you use an SXP reflector, the SXP filtering configuration ensures that only relevant IP-SGT bindings for the local service-side networks are pushed down to the Cisco IOS XE Catalyst SD-WAN devices. Overlapping or remote entries coming through an SXP can have an adverse effect on overlay routing.

Configure SXP for Dynamic IP-SGT Binding Using Configuration Groups

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a TrustSec feature in the Other profile.

a) Enter the details for setting up an SXP connection.

Field	Description
Enable Enforcement	Enable enforcement at a global level.
Device SGT	Enter a value to configure the SGT for packets sent from a device. Range: 2 to 65519.

Field	Description
Device ID	Enter a TrustSec ID for the device. This ID must be the same as that in ISE and must not exceed 32 characters.
Device Password	Enter a clean text password for the device with length of 24 characters.

b) Configure SXP for dynamic IP/SGT.

Field	Description
Enable SXP	Enable an SXP connection on the device.
Source IP	Enter an IPv4 address to set up a source IP address for SXP.
Preshared Key	
Password	Enter a clean text password for the device with length of 24 characters.
Key chain name	Enter a key chain name that you configured in the Fabric Security feature under System profile.

c) Add a new SXP peer connection.

Field	Description
(Optional) **VPN ID**	Enter a VPN or VRF ID for the SXP connection. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.
Peer IP	Configure a peer IPv4 address for SXP.
Source IP	Configure a source IPv4 address for SXP.
Preshared Key	Choose a preshared key type.
Mode	Choose a connection mode. **Local** refers to the local device, and **Peer** refers to a peer device.
Mode type	Choose a role for the device.
(Optional) **Min. Hold Time**	Enter time (in seconds) to configure the minimum hold time for the SXP connection.
(Optional) **Max. Hold Time**	Enter time (in seconds) to configure the maximum hold time for the SXP connection.

Note

Maximum Hold Time and **Minimum Hold Time** can be configured only when you choose **Mode** as **Local** and **Mode Type** as **Listener**, or when **Mode** is **Peer** and **Mode Type** is **Speaker**.

Only **Minimum Hold Time** is configurable when **Mode** is **Local** and **Mode Type** is **Speaker** or when **Mode** is **Peer** and **Mode Type** is **Listener**.

Hold time cannot be configured if you choose **Mode Type** as **Both** (that is Listener and Speaker).

Step 3 Click **Save** to save the configuration for an SXP connection.

What to do next

Also see Deploy a configuration group.

Configure SXP for Dynamic IP-SGT Binding Using Feature Templates

You can configure an SXP connection for downloading the IP-SGT binding from Cisco ISE to a Cisco IOS XE Catalyst SD-WAN device.

To configure an SXP connection in Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Choose the device for which you are creating the template.
4. Under **OTHER TEMPLATES** section, choose **TrustSec**.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 - 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any of the characters and spaces.
7. Enter the details for setting up an SXP connection:

Parameter Name	Description
Device SGT	Enter a value to configure the SGT for packets sent from a device. Range: 2 to 65519.
Credentials ID	Enter a TrustSec ID for the device. This ID must be the same as that in ISE and must not exceed 32 characters.
Credentials Password	Enter a TrustSec password for the device.

Parameter Name	Description
Enable Enforcement	Click **On** to enable at a global level. Click **Off** to disable SGT enforcement. **Note** You can enable this configuration either at a global level here, or at an interface level in step 8 of Configuring SGT Enforcement at an interface level in Cisco SD-WAN Manager, but not both.

8. Configure SXP for dynamic IP/SGT.

Parameter Name	Description
Enable SXP	Click **On** to enable an SXP connection on the device. When you enable SXP, you must enter a Node ID and a Node ID type. **Note** When you change a Node ID, you must first disable SXP and then push the template to the device. Then, you change the Node ID, and then push the template to the device again.
Source IP	Enter an IP address to set up a source IP address for SXP.
Password	Enter a default password for SXP.
Key Chain Name	Enter a name to configure the key chain for SXP.
Log Binding Changes	Click **On** to enable logging for IP-to-SGT binding changes.
Reconciliation Period (seconds)	Enter a time (in seconds) to configure 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 the invalid entries. The default value is 120 seconds (2 minutes). Setting the SXP reconciliation period to 0 seconds disables the timer and causes all the entries from the previous connection to be removed.
Retry Period (seconds)	Enter a time (in seconds) to configure the retry period for SXP reconnection.
Speaker Hold Time (seconds)	Enter time (in seconds) to configure the global hold-time period for a speaker device.
Minimum Listener Hold Time (seconds)	Enter a time (in seconds) to configure the minimum allowed hold-time period for a listener device.
Maximum Listener Hold Time (seconds)	Enter a time (in seconds) to configure the maximum allowed hold-time period for a listener device.
Node ID Type	Choose a node ID type.
Node ID	Enter a node ID. A node ID is used to identify the individual devices within the network.

9. Click **New Connection** to add a new SXP peer connection details.

Parameter Name	Description
Peer IP	Configure a peer IPv4 address for SXP.
Source IP	Configure a source IPv4 address for SXP.
Preshared Key	Choose a preshared key type.
Mode	Choose a connection mode. **Local** refers to the local device, and **Peer** refers to a peer device.
Mode Type	Choose a role for the device.
Minimum Hold Time	Enter time (in seconds) to configure the minimum hold time for the SXP connection.
Maximum Hold Time	Enter time (in seconds) to configure the maximum hold time for the SXP connection.
VPN ID	Enter a VPN or VRF ID for the SXP connection.

Note **Maximum Hold Time** and **Minimum Hold Time** can be configured only when you choose **Mode** as **Local** and **Mode Type** as **Listener**, or when **Mode** is **Peer** and **Mode Type** is **Speaker**.

Only **Minimum Hold Time** is configurable when **Mode** is **Local** and **Mode Type** is **Speaker** or when **Mode** is **Peer** and **Mode Type** is **Listener**.

Hold time cannot be configured if you choose **Mode Type** as **Both** (that is **Listener** and **Speaker**).

10. Click **Save** to save your configuration for an SXP connection.

Configure SXP for Dynamic IP-SGT Binding on the CLI

Set Up an SXP Connection

```
Device(config)# cts sgt 10
Device(config)# cts credentials id cEDGE4 password 6
RX^ASQVgfFV^EOAeQWVZ]VFQ_hcLDdgJJDevice(config)# cts credentials password cts_pwd
Device(config)# cts role-based enforcement
Device(config)#
```

Configure SXP for Dynamic IP/SGT Binding

```
Device(config)# cts sxp enable
Device(config)# cts sxp default source-ip 10.29.1.1
Device(config)# cts sxp default password 6 LZcdEUScdLSVZceMAJ_R[cJgb^NbWNLLC
Device(config)# cts sxp default key-chain key1
Device(config)# cts sxp log binding-changes
Device(config)# cts sxp reconciliation period 120
Device(config)# cts sxp retry period 60
Device(config)# cts sxp speaker hold-time 120
Device(config)# cts sxp listener hold-time 60 90
Device(config)#
```

Add a New SXP Peer Connection

```
Device(config)# cts sxp connection peer 10.201.1.2 source 10.29.1.1 password key-chain mode
 local both vrf 1
```

Configure Static IP-SGT Binding Using Cisco SD-WAN Manager

To configure static IP-SGT, use the CLI add-on template in Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Choose the device for which you are creating the template.
4. Under **OTHER TEMPLATES** section, choose **CLI Add-On Template** as the feature template.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 - 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any of the characters and spaces.
7. In the **CLI Configuration** area, enter the following configuration:

```
cts role-based sgt-map vrf instance_name {ipv4_netaddress|ipv4_netaddress/prefix} sgt
sgt-number
cts role-based sgt-map vrf instance_name host {ipv4_hostaddress} sgt sgt-number
```

8. Click **Save** to save this configuration. This configuration can now be pushed to a Cisco IOS XE Catalyst SD-WAN device for propagation of the SGT over a Cisco Catalyst SD-WAN network.

Configure TCP-AO Support for SXP

Cisco TrustSec SXP peers exchange IP-SGT bindings over a TCP connection. TCP Authentication Option (TCP-AO) is used to guard against spoofed TCP segments in Cisco TrustSec SXP sessions between the peers. TCP-AO is resistant to collision attacks and provides algorithmic agility and support for key management.

To enable TCP-AO for an SXP connection, a TCP-AO key chain must be specified for the connection.

To establish an SXP peer connection with TCP-AO:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Choose the device for which you are creating the template.
4. Under **BASIC INFORMATION** section, choose **Cisco Security** as the feature template.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any of the characters and spaces.
7. Configure TCP-AO key chain and keys.

Parameter Name	Description
Keychain Name	Specify a TCP-AO key chain name. The key chain name can have a maximum of 256 characters.
Key ID	Specify a key identifier. Range: 0 to 2147483647.
Send ID	Specify the send identifier for the key. Range: 0 to 255.
Receiver ID	Specify the receive identifier for the key. Range: 0 to 255.
Include TCP Options	This field indicates whether TCP options other than TCP-AO must be used to calculate Message Authentication Codes (MACs). A MAC is computed for a TCP segment using a configured MAC algorithm, relevant traffic keys, and the TCP segment data prefixed with a pseudoheader. When options are included, the content of all options is included in the MAC with TCP-AO's **MAC field** is filled with zeroed. When the options are not included, all options other than TCP-AO are excluded from all MAC calculations.
Accept AO Mismatch	This field indicates whether the receiver must accept the segments for which the MAC in the incoming TCP-AO does not match the MAC that is generated on the receiver.
Crypto Algorithm	Specify the algorithm to be used to compute MACs for TCP segments. You can choosese one of these: • **aes-128-cmac** • **hmac-sha-1** • **hmac-sha-256**
Key String	Specify the master key for deriving the traffic keys. The master keys must be identical on both the peers. If the master keys do not match, authentication fails and segments may be rejected by the receiver. Range: 0 to 80 characters.
Send Lifetime Local	Specify the time in seconds that is entered in Cisco SD-WAN Manager for which the key to be used in TCP-AO authentication is valid. Specify the start time in the local time zone. By default, the start time corresponds to UTC time. The end time can be specified in three ways—infinite (no expiry), duration (1 to 2147483646 sec), exact time – (either UTC or local).

Parameter Name	Description
Accept Lifetime Local	Specify the time in seconds that is entered in Cisco SD-WAN Manager for which the key to be accepted for TCP-AO authentication is valid. Specify the start time in the local time zone. By default, the start time corresponds to UTC time. The end time can be specified in three ways—infinite (no expiry), duration (1 to 2147483646 sec), exact time – (either UTC or local).

Note When you configure a key chain for an SXP connection, at least one key in the key chain must be configured with the current time. All keys in the key chain cannot be configured completely with a future time.

Configure TCP-AO Support for SXP on the CLI

```
Device(config)# key chain key1 tcp
Device(onfig-keychain)# key 1000
Device(config-keychain-key)# cryptographic-algorithm hmac-sha-256
Device(config-keychain-key)# key-string 6 _RPB[dVI]SO^BAOVNMKATgOZKMXFGXFTa
Device(config-keychain-key)# accept-lifetime local 18:00:00 Jan 12 2021 06:00:00 Jan 12
2022
Device(config-keychain-key)# send-lifetime local 18:00:00 Jan 12 2021 01:00:00 Jan 12 2022
Device(config-keychain-key)# send-id 215
Device(config-keychain-key)# recv-id 215
Device(config)#
```

Configure SXP Reflector Using the CLI

```
cts sxp filter-enable
cts sxp filter-list <device-name1>
 permit ipv4 <ip-address>
 deny ipv4 <ip-address>
 permit ipv6 <network-prefix>
 deny ipv6 <network-prefix>
cts sxp filter-list <device-name2>
 permit ipv4 <ip-address>
 deny ipv4 <ip-address>
 permit ipv6 <network-prefix>
 deny ipv6 <network-prefix>
cts sxp filter-group speaker <device-name1_spk>
 filter <device-name1>
 peer ipv4 <ip-address>
cts sxp filter-group speaker <device-name2_spk>
 filter <device-name1>
 peer ipv4 <ip-address>
!
```

SGACL for Cisco TrustSec

Security Group Access Control Lists (SGACLs) are a policy enforcement mechanism through which an administrator can control the operations performed by users based on the security group assignments and destination resources.

SGACL policies are configured in Cisco ISE and dynamically downloaded for enforcement to a Cisco IOS XE Catalyst SD-WAN device using a RADIUS server. The downloaded SGACL policies override any conflicting locally defined policies. See Download SGACL Policies to Cisco IOS XE Catalyst SD-WAN devices, on page 22.

Alternatively, you have the option of configuring SGACL policies on Cisco SD-WAN Manager. The policies can be pushed to the Cisco IOS XE Catalyst SD-WAN device using the CLI Add-On template. See Configure Static SGACL Policies in Cisco SD-WAN Manager, on page 24.

Configure SGACL for Cisco TrustSec Using a Configuration Group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a AAA feature in a System profile.

a) Configure a connection to a RADIUS server.

Table 5: RADIUS

Field	Description
Address*	Enter the IP address of the RADIUS server host.
Acct Port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server. Range: 1 - 65534. Default: 1813
Auth Port	Enter the UDP destination port to use for authentication requests to the RADIUS server. Default: 1812 Range: 1 - 65534
Retransmit	Enter the number of times the device transmits each RADIUS request to the server before giving up. Default: 3 Range: 0 - 100
Timeout	Enter the number of seconds a device waits for a reply to a RADIUS request before retransmitting the request. Default: 5 seconds Range: 1 through 1000
Key*	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the RADIUS server for authentication and encryption.

Field	Description
Key Type	Choose Protected Access Credential (PAC) key.

b) Configure TrustSec details for authorization.

Field	Description
CTS Authorization List	Specify a name of a list for authentication, authorization, and accounting (AAA) servers. The list name should be within 1-64 characters.
(Optional) **RADIUS Group**	Choose a RADIUS server.

Step 3 Click **Save.**

What to do next

Also see Deploy a configuration group.

Download SGACL Policies to Cisco IOS XE Catalyst SD-WAN devices

When configured in Cisco ISE, SGACL policies can be downloaded dynamically from Cisco ISE to a Cisco IOS XE Catalyst SD-WAN device using a RADIUS server.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Choose the device for which you are creating the template.
4. Under **Basic Information**, choose **Cisco AAA** as the feature template.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any of the characters and spaces.
7. Click **Radius** to configure a connection to a RADIUS server. The followin fields are displayed:

Parameter Name	Description
Address	Enter the IP address of the RADIUS server.

Parameter Name	Description
Authentication Port	Enter the UDP destination port to use for authentication requests to the RADIUS server. If the server is not used for authentication, configure the port number to be 0. Range: 0 to 65535.
Accounting Port	Enter the UDP port that will be used to send 802.1X and 802.11i accounting information to the RADIUS server. Range: 0 to 65535.
Timeout	Specify how long to wait to receive a reply from the RADIUS server before retransmitting a request. Range: 1 through 1000.
Retransmit Count	Specify how many times to search through the list of RADIUS servers while attempting to locate a server. Range: 1 through 1000.
Key Type	Click **PAC** as key type.
Key	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the RADIUS server for authentication and encryption. You can enter the key as a text string from—1 to 31 characters long,—and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the RADIUS server.

8. Click **Radius Group** to add a new RADIUS group. The following fields are displayed:

Parameter Name	Description
Group Name	Displays the RADIUS group name. This field is automatically populated based on the VPN ID that you configure.
VPN ID	Enter a VPN ID.
Source Interface	Set the interface that will be used to reach the RADIUS server.
Radius Server	Choose an IP address for the RADIUS server.

9. Click **Radius COA** to configure the settings to accept change of authorization (CoA) requests from a RADIUS or other authentication server, and to act on requests to a connection to the RADIUS server.

   Updated policies are downloaded to the Cisco IOS XE Catalyst SD-WAN device when SGACL policies are modified on ISE and a CoA is pushed to the Cisco IOS XE Catalyst SD-WAN device.

   On clicking **Radius COA**, the following fields are displayed:

Parameter Name	Description
Client	Displays the RADIUS client from which a device accepts Change of Authorization (CoA) and disconnect requests.
Domain Stripping	Configure domain stripping at the server group level. The stripping keyword compares the incoming username with the names oriented to the left of the @ domain delimiter.
Port	Specify the RADIUS Dynamic Author port. *Range:* 0 to 65535

10. Click **TrustSec** to configure more details for authorization. The following details are displayed:

Parameter Name	Description
CTS Authorization List	Specify a name of a list for authentication, authorization, and accounting (AAA) servers.
Radius group	Choose a RADIUS server.

11. Click **Save**.

Download SGACL Policies using CLI

Configure a Radius Group Server

```
Device(config)# aaa group server radius radius-1
Device(config-sg-radius)# ip radius source-interface GigabitEthernet0/0/1.100
Device(config-sg-radius)# ip vrf forwarding 1
Device(config)#
```

Configure a Radius Server

```
Device(config)# aaa group server radius radius-1
Device(config-sg-radius)# server-private 10.251.1.1 auth-port 5 acct-port 5 timeout 5
retransmit 3 pac key 6 ebKQPObGXfAKgRHQhbWe_ZXFTBCVgFOMg
Device(config)#
```

Configure a Radius CoA

```
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 10.251.1.1 vrf 1 server-key 6
gWTLbecJKOQcFcIbJNR[]WKP_g^TRacRF
Device(config-locsvr-da-radius)# domain stripping right-to-left
Device(config-locsvr-da-radius)# port 1
Device(config)#
```

Configure Other Details of Authorization

```
Device(config)# cts authorization list cts-mlist
Device(config)# aaa authorization network cts-mlist group radius-1
```

Configure Static SGACL Policies in Cisco SD-WAN Manager

To configure static SGACL policies, use the CLI Add-On template in Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Choose the device for which you are creating the template.
4. Under **OTHER TEMPLATES** section,, choose **CLI Add-On Template** as the feature template.

5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any of any characters and spaces.
7. In the CLI configuration area, enter the following configuration:

```
interface gigabitethernet 1/1/3
cts role-based enforcement
cts role-based sgt-map sgt 2
interface gigabitethernet 1/1/4
no cts role-based enforcement[no] cts role-based permissions {[ default | from |
[source-sgt] | to | [dest-sgt]]}
[no] cts role-based permissions {[ default | from | [source-sgt] | to | [dest-sgt]]}
```

8. Click **Save**.

   This configuration can now be pushed to the Cisco IOS XE Catalyst SD-WAN device for enforcement of SGACL policies.

Enhanced SGACL Logging

Information About Enhanced SGACL Logging

SGACL logging records actions that are taken by SGACLs to enforce security rules. It captures details about network traffic events, including whether traffic was allowed or blocked based on SGACL policies.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, SGACL logging on Cisco IOS XE Catalyst SD-WAN devices utilizes HSL. The enhanced SGACL logging using HSL offers a more efficient and scalable method for logging security events, which is beneficial in high-traffic network environments.

When SGACLs enforce security rules and generate log entries, these entries are stored as Cisco SYSLOG messages on the Cisco IOS XE Catalyst SD-WAN device. You can view these log messages by using the **show logging** command on the Cisco IOS XE Catalyst SD-WAN device.

Configure Enhanced SGACL Logging Using CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to configure enhanced SGACL logging.

1. Configure role-based access control with Cisco TrustSec by mapping IP addresses to SGTs, enabling enforcement, and defining SGACL permissions.

```
cts role-based sgt-map vrf vrf-value ip-address sgt SGT-value
cts role-based enforcement
cts role-based permissions from source-sgt to dest-sgt role-based-acl-name
```

2. Configure permissions for IPv4 traffic, and enable logging for TCP traffic.

```
ip access-list role-based role-based-access-list-name
 sequence-number permit tcp log-input
 sequence-number permit icmp
 sequence-number permit ip
```

3. Configure permissions for IPv6 traffic, and enable logging for UDP traffic.

```
ipv6 access-list role-based role-based-acl-name
 sequence sequence-number permit icmp
 sequence sequence-number permit udp log
 sequence sequence-number permit tcp
 sequence sequence-number permit ipv6
```

Note The log message that is produced is identical whether the **log** or the **log-input** command is used.

Here's the complete configuration example for SGACL logging for IPv4 traffic. In this example, the role-based access list named 'PERMIT' allows TCP traffic with logging enabled, while permitting ICMP and IP traffic without logging.

```
cts role-based sgt-map vrf 1 10.2.2.2 sgt 600
cts role-based enforcement
cts role-based permissions from 500 to 600 PERMIT
ip access-list role-based PERMIT
 20 permit tcp log-input
 30 permit icmp
 40 permit ip
```

Here's the complete configuration example for SGACL logging for IPv6 traffic. In this example, the role-based access list named 'PERMIT_IPv6' allows UDP traffic with logging enabled, while permitting ICMP, TCP and IPv6 traffic without logging.

```
cts role-based sgt-map vrf 1 10.2.2.2 sgt 600
cts role-based enforcement
cts role-based permissions from 500 to 600 ipv6 PERMIT_IPv6

ipv6 access-list role-based PERMIT_IPv6
 sequence 20 permit icmp
 sequence 30 permit udp log
 sequence 40 permit tcp
 sequence 50 permit ipv6
```

Note The Enhanced SGACL Logging feature can log a maximum of 512 unique traffic flows across all protocols, such as TCP, UDP, and ICMP. Flows exceeding this limit are not logged.

Verify Enhanced SGACL Logging

The following is a sample output from the **show platform hardware qfp active feature acl dp hsl configuration** command. This output displays the configuration for SGACL with HSL as set up on the device.

```
Device# show platform hardware qfp active feature acl dp hsl configuration
ACL DP HSL Config:
HSL Supported: TRUE
HSL SGACL Enabled: TRUE
```

```
SGACL HSL Setup:
Handle Session/Instance: 127/63
Version: 9
Dest Type: 3
HSL Enable: TRUE
HSL BackPressure Enable: FALSE
Base Memory Addr: <0xpXXXX>
Memory Size (bytes): 147560
Max Records: 1024
Record Threshold: 256
Memory Threshold (bytes): 32768
Record Timeout (ms): 512
Export Timeout (ms): 4
MTU Size (bytes): 1450
Template Refresh Timer: 0
Template Refresh Packets: 0
Source Id: 0x404”
Max Record Size (bytes): 104
```

The following is a sample output from the **show platform hardware qfp active feature acl control** command. This output displays whether SGACL logging is enabled or disabled. In this example, SGACL logging is enabled.

```
Device# show platform hardware qfp active feature acl control
Stats Poll Period: 0
Stats Entry Size: 16
Ha Init: 1
Fm Ready: 0
IPv4 Logging Threshold: 2147483647
IPv4 Logging Interval: 0
IPv6 Logging Threshold: 350000
IPv6 Logging Interval: 0
Maximum Aces Per Acl: 256000
Stats Update size: 180
Maximum Entries: 0
Maximum Entries per Classifier: 0
Result Bit Size: 0
Result Start Bit Pos: 0
Maximum Profiles: 0
Maximum Blocks per Profile: 0
Device Select: 0
Maximum Tree Depth: 0
Dimention: 0
Number Cuts: 0
HSL Support: TRUE // sgacl hsl logging is enabled
HSL Force Disable: FALSE
```

The following is a sample output from the **show platform hardware qfp active feature acl dp hsl statistics** command. In this example, the output displays the logging statistics for SGACL HSL from the device.

```
Device# show platform hardware qfp active feature acl dp hsl statistics
Router#show platform hardware qfp active feature acl dp hsl statistic
ACL DP HSL Statistics:
HSL Supported: TRUE
HSL SGACL Enabled: TRUE

SGACL Export Statistics
-----------------------
Records sent (to HSL): 2
Records dropped (before HSL): 0
Record alloc failures: 0
Records dropped flag: Off
Records sent (by HSL): 0
```

```
Records dropped (by HSL): 0
HSL packets dropped flag: Off
HSL buffer flow-on (count): 0

SGACL HSL Statistics
--------------------
Records exported: 2
Packets exported: 2
Bytes exported: 168
Dropped records: 0
Dropped packets (inc. Punt drops): 0
Dropped bytes: 0
```

Configuration Example for Enhanced SGACL Logging

This example illustrates how role-based access control and SGACL logging are configured on a Cisco IOS XE Catalyst SD-WAN device.

```
aaa authorization network cts-mlist group radius-1
cts authorization list cts-mlist
cts credentials id admin password 6 LFAZFNeZSWRhSFQX[[_abNQU[_EGLdcdd
cts sxp default source-ip 10.20.25.16
cts sxp node-id interface GigabitEthernet5
!
interface Tunnel1
 ip unnumbered GigabitEthernet1
ipv6 unnumbered GigabitEthernet1
 cts manual
 tunnel source GigabitEthernet1
 tunnel mode sdwan
!
cts role-based sgt-map vrf 1 10.2.2.2 sgt 600
cts role-based enforcement
cts role-based permissions from 500 to 600 PERMIT
!
ip access-list role-based PERMIT
 10 permit ip log
 20 permit tcp log-input
 30 permit icmp


ipv6 access-list role-based PERMIT_IPv6
 sequence 20 permit icmp
 sequence 30 permit udp log
 sequence 40 permit tcp
 sequence 50 permit ipv6

.
```

SGT Enforcement

SGACL policies configured on Cisco ISE, or configured using the CLI Add-On template can be applied and SGT enforced on egress traffic both globally (on all the interfaces) or on a specific interface.

You can enforce SGT at a global level in the TrustSec feature template. See Configure SXP for Dynamic IP-SGT Binding Using Feature Templates, on page 15.

Configure SGT Enforcement at the Interface Level Using a Configuration Group

You enforce SGT using SGACL policies at the interface level in Cisco SD-WAN Manager using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Transport VPN feature in a Transport and Management profile or a Service VPN feature in a Service profile.

Step 3 Add an Ethernet Interface feature to the transport or service interface.

a) Configure TrustSec.

Field	Description
Enable SGT Propogation	Enable this option to use the Cisco TrustSec Security Group Tag (SGT) propagation feature.
Propagate	Enable this option to propagate SGT in Cisco Catalyst SD-WAN.
Security Group Tag	Enter a value that can be used as a tag. Range: 2 to 65519
Trusted	Enable the trusted option. When you enable this option, the SGT value received in the Ethernet packet on this interface is trusted and is used by the device for any security group aware policy enforcement.
Enable Enforced Propagation	Enable this option to start SGT enforcement on the interface.
Enforced Security Group Tag	Enter a value that can be used as a tag for enforcement. Range: 2 to 65519

Note
You can enable this configuration either at an interface level in this step, or a global level using the Enable Enforcement field in Configuring SXP for Dynamic IP/SGT using vManage, but not both.

Step 4 Click **Save**.

What to do next

Also see Deploy a configuration group.

Configure SGT Enforcement at the Interface Level in Cisco SD-WAN Manager Using Feature Templates

To enforce SGT using SGACL policies at the interface level in Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Choose the device for which you are creating the template.
4. Under **Basic Information**, choose **Cisco VPN Interface Ethernet** as the feature template.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 - 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any characters and spaces.
7. Click **TrustSec**.
8. In the **Enable Enforcement** field, click **On** to enable SGT enforcement on a particular interface.

Note You can enable this configuration either at an interface level in this step, or a global level using the **Enable Enforcement** field in Configuring SXP for Dynamic IP/SGT using Cisco SD-WAN Manager, but not both.

9. In the **Enter a SGT value** field, enter a value that can be used as a tag for enforcement .
10. Click **Save**.

Configuring SGT Enforcement at the Interface Level Using CLI

Use the following command to configure SGT enforcement:

```
Device(config)# interface <interface-type> <number>
Device(config-if)# cts role-based enforcement
```

Monitor SXP Connections and SGT Enforcement

You can monitor an SXP connection and other SGT information in Cisco SD-WAN Manager, or the WAN edge device CLI.

Using Cisco SD-WAN Manager

To monitor SXP SGT information in Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Monitor**> **Network**.
2. Choose a device from the list of devices.
3. Click **Real Time** in the left pane.
4. Choose one of the following options from the **Device Options** drop-down list to monitor SXP and SGT information:
   - **TrustSec SXP Connections**
   - **TrustSec CTS PAC**
   - **TrustSec CTS Role Based SGT Map**
   - **TrustSec CTS Role Based SGT Permission**
   - **TrustSec CTS Role Based Counters**
   - **TrustSec CTS Role Based IPv6 Permission**
   - **TrustSec CTS Role Based IPv6 Counters**
   - **TrustSec CTS Environment Data**
   - **TrustSec CTS EnvData Radius Server**

Note You can re-arrange the columns to view SXP and SGT information as per your preference by dragging the column title to the desired position. If you re-arrange the columns, we recommended the Source SGT and Destination SGT columns are set to your left hand side so that you can understand the bindings of a traffic flow.

Using CLI

Use the following commands to monitor SXP/SGT information using the CLI.

Table 6: SXP/SGT Commands

Commands	Description
show cts sxp connections	show SXP connections.
show cts role-based sgt-map	Displays role-based access control information (per VRF). (Both static and dynamic entries are shown.)
show cts role-based permissions	Displays the SGACL dynamic and static entries.
show cts role-based counters	Displays Security Group access control list (ACL) enforcement statistics.
show cts environment-data	Displays Cisco TrustSec environment data information.

Commands	Description
show cts pac	Displays Cisco TrustSec PAC information.
show aaa server	Displays the AAA server status.
Show key chain	Displays key chain information.