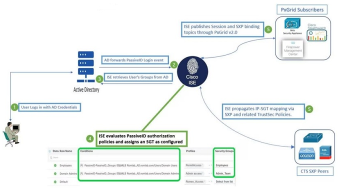
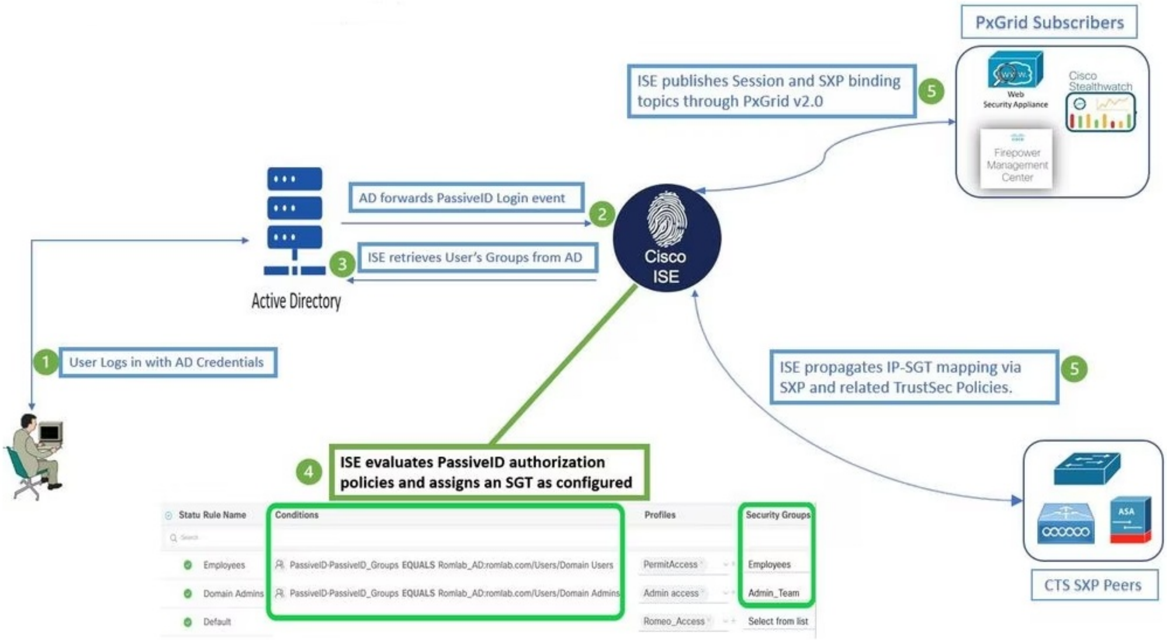

PxGrid Subscribers
ISE publishes Session and SXP binding topics through PxGrid v2.0
5
Web Security Appliance
Cisco Stealthwatch
Firepower Management Center
AD forwards PassiveID Login event
2
ISE retrieves User's Groups from AD
3
Cisco ISE
Active Directory
1
User Logs in with AD Credentials
ISE propagates IP-SGT mapping via SXP and related TrustSec Policies.
5
4
ISE evaluates PassiveID authorization policies and assigns an SGT as configured
Statu Rule Name
Conditions
Profiles
Security Groups
Employees
PassiveID-PassiveID_Groups EQUALS Romlab_AD:romlab.com/Users/Domain Users
PermitAccess
Employees
Domain Admins
PassiveID-PassiveID_Groups EQUALS Romlab_AD:romlab.com/Users/Domain Admins
Admin access
Admin_Team
Default
Romeo_Access
Select from list
ASA
CTS SXP Peers

CISCO Configuring Security Group Tag Mapping User Guide

Contents

CISCO Configuring Security Group Tag Mapping



1 User Logs in with AD Credentials

2 AD forwards PassiveID Login event

3 ISE retrieves User's Groups from AD

4 ISE evaluates PassiveID authorization policies and assigns an SGT as configured

5 ISE publishes Session and SXP binding topics through PxGrid v2.0

5 ISE propagates IP-SGT mapping via SXP and related TrustSec Policies.

Statu	Rule Name	Conditions	Profiles	Security Groups
	Employees	PassiveID-PassiveID_Groups EQUALS Romlab_AD:romlab.com/Users/Domain Users	PermitAccess	Employees
	Domain Admins	PassiveID-PassiveID_Groups EQUALS Romlab_AD:romlab.com/Users/Domain Admins	Admin access	Admin_Team
	Default		Romeo_Access	Select from list

Product Information

The product allows for configuring security group tag (SGT) mapping. This feature binds an SGT to all host addresses of a specified subnet. Once this mapping is implemented, Cisco TrustSec imposes the SGT on any incoming packet that has a source IP address that belongs to the specified subnet.

Restrictions for SGT Mapping

The following command is not supported for host IP configuration: `Device(config)#cts role-based sgt-map 0.0.0.0 sgt 1000`

Overview of Subnet-to-SGT Mapping

- Subnet-to-SGT mapping binds an SGT to all host addresses of a specified subnet. Cisco TrustSec imposes the SGT on an incoming packet when the packet's source IP address belongs to the specified subnet. The subnet and SGT are specified in the CLI with the`cts role-based sgt-map net_address/prefix sgt sgt_number` global configuration command. A single host may also be mapped with this command.
- In IPv4 networks, Security Exchange Protocol (SXP)v3, and more recent versions, can receive and parse subnet net_address/prefix strings from SXPv3 peers. Earlier SXP versions convert the subnet prefix into its set of host bindings before exporting them to an SXP listener peer.
- Subnet bindings are static, there is no learning of active hosts. They can be used locally for SGT imposition and SGACL enforcement. Packets tagged by subnet-to-SGT mapping can be propagated on Layer 2 or Layer 3 Cisco TrustSec links.
- For IPv6 networks, SXPv3 cannot export subnet bindings to SXPv2 or SXPv1 peers.

Overview of VLAN-to-SGT Mapping

- The VLAN-to-SGT mapping feature binds an SGT to packets from a specified VLAN. This simplifies the migration from legacy to Cisco TrustSec-capable networks.
- The VLAN-to-SGT binding is configured with the `cts role-based sgt-map vlan-list` global configuration command.
- When a VLAN is assigned a gateway that is a switched virtual interface (SVI) on a Cisco TrustSec-capable switch, and IP Device Tracking is enabled on that switch, then Cisco TrustSec can create an IP-to-SGT binding

for any active host on that VLAN mapped to the SVI subnet.

- IP-SGT bindings for the active VLAN hosts are exported to SXP listeners. The bindings for each mapped VLAN are inserted into the IP-to-SGT table associated with the VRF the VLAN is mapped to by either its SVI or by the `cts role-based l2-vrf` command.
- VLAN-to-SGT bindings have the lowest priority of all binding methods and are ignored when bindings from other sources are received, such as from SXP or CLI host configurations. Binding priorities are listed in the Binding Source Priorities section.

Product Usage Instructions

Configuring Subnet-to-SGT Mapping

1. Access the device's CLI interface.
2. Enter the configuration mode using the `config` command.
3. Execute the following command to configure subnet-to-SGT mapping:

```
cts role-based sgt-map net_address/prefix sgt sgt_number
```

1. Replace `net_address/prefix` with the subnet address and prefix length you want to map (e.g., 192.168.1.0/24).
2. Replace `sgt_number` with the desired security group tag number.
3. Press Enter to apply the configuration.
4. Exit the configuration mode.

Configuring VLAN-to-SGT Mapping

1. Access the device's CLI interface.
2. Enter the configuration mode using the `config`command.
3. Execute the following command to configure VLAN-to-SGT mapping:

```
cts role-based sgt-map vlan-list
```

1. Specify the VLANs to be mapped to SGTs.
2. Press Enter to apply the configuration.
3. Exit the configuration mode.

Specifications

- Supported Networks: IPv4, IPv6
- Supported Protocols: Security Exchange Protocol (SXP)v3
- Supported Binding Methods: Subnet-to-SGT Mapping, VLAN-to-SGT Mapping

Frequently Asked Questions (FAQ)

- **Q: Can subnet bindings be exported to SXPv2 or SXPv1 peers in IPv6 networks?**

A: No, subnet bindings can only be exported to SXPv3 peers in IPv6 networks.

- **Q: What is the priority of VLAN-to-SGT bindings?**

  A: VLAN-to-SGT bindings have the lowest priority among all binding methods and are ignored when bindings from other sources are received.

Subnet to security group tag (SGT) mapping binds an SGT to all host addresses of a specified subnet. Once this mapping is implemented, Cisco TrustSec imposes the SGT on any incoming packet that has a source IP address that belongs to the specified subnet.

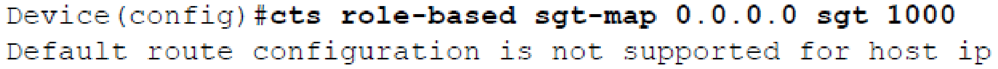
Restrictions for SGT Mapping

Restrictions for Subnet-to-SGT Mapping

- An IPv4 subnetwork with a /31 prefix cannot be expanded.
- Subnet host addresses cannot be bound to Security Group Tags (SGT)s when the network-map bindings parameter is less than the total number of subnet hosts in the specified subnets, or when the bindings is 0.
- IPv6 expansions and propagation only occurs when the Security Exchange Protocol (SXP) speaker and listener are running SXPv3 or more recent versions.

Restriction for Default Route SGT Mapping

- Default route configuration is accepted only with the subnet /0. Entering only the host-ip without the subnet /0 displays the following message:



```
Device(config)#cts role-based sgt-map 0.0.0.0 sgt 1000
Default route configuration is not supported for host ip
```

Information About SGT Mapping

This section provides information about SGT mapping.

Overview

Overview of Subnet-to-SGT Mapping

Subnet-to-SGT mapping binds an SGT to all host addresses of a specified subnet. Cisco TrustSec imposes the SGT on an incoming packet when the packet's source IP address belongs to the specified subnet. The subnet and SGT are specified in the CLI with the cts role-based sgt-map net_address/prefix sgt sgt_number global configuration command. A single host may also be mapped with this command. In IPv4 networks, Security Exchange Protocol (SXP)v3, and more recent versions, can receive and parse subnet net_address/prefix strings from SXPv3 peers. Earlier SXP versions convert the subnet prefix into its set of host bindings before exporting them to an SXP listener peer.

For example, the IPv4 subnet 192.0.2.0/24 is expanded as follows (only 3 bits for host addresses):

- Host addresses 198.0.2.1 to 198.0.2.7—tagged and propagated to SXP peer.
- Network and broadcast addresses 198.0.2.0 and 198.0.2.8—not tagged and not propagated.

To limit the number of subnet bindings SXPv3 can export, use the cts sxp mapping network-map global configuration command. Subnet bindings are static, there is no learning of active hosts. They can be used locally for SGT imposition and SGACL enforcement. Packets tagged by subnet-to-SGT mapping can be propagated on

Layer 2 or Layer 3 Cisco TrustSec links. For IPv6 networks, SXPv3 cannot export subnet bindings to SXPv2 or SXPv1 peers.

Overview of VLAN-to-SGT Mapping
The VLAN-to-SGT mapping feature binds an SGT to packets from a specified VLAN. This simplifies the migration from legacy to Cisco TrustSec-capable networks as follows:

- Supports devices that are not Cisco TrustSec-capable but are VLAN-capable, such as, legacy switches, wireless controllers, access points, VPNs, etc.
- Provides backward compatibility for topologies where VLANs and VLAN ACLs segment the network, such as, server segmentation in data centers.
- The VLAN-to-SGT binding is configured with the cts role-based sgt-map vlan-list global configuration command.
- When a VLAN is assigned a gateway that is a switched virtual interface (SVI) on a Cisco TrustSec-capable switch, and IP Device Tracking is enabled on that switch, then Cisco TrustSec can create an IP-to-SGT binding for any active host on that VLAN mapped to the SVI subnet.
- IP-SGT bindings for the active VLAN hosts are exported to SXP listeners. The bindings for each mapped VLAN are inserted into the IP-to-SGT table associated with the VRF the VLAN is mapped to by either its SVI or by the cts role-based l2-vrf command.
- VLAN-to-SGT bindings have the lowest priority of all binding methods and are ignored when bindings from other sources are received, such as from SXP or CLI host configurations. Binding priorities are listed in the Binding Source Priorities section.

Binding Source Priorities

Cisco TrustSec resolves conflicts among IP-SGT binding sources with a strict priority scheme. For example, an SGT may be applied to an interface with the policy {dynamic identity peer-name | static sgt tag} Cisco Trustsec Manual interface mode command (Identity Port Mapping). The current priority enforcement order, from lowest (1) to highest (7), is as follows:

1. **VLAN:** Bindings learned from snooped ARP packets on a VLAN that has VLAN-SGT mapping configured.
2. **CLI:** Address bindings configured using the IP-SGT form of the cts role-based sgt-map global configuration command.
3. **SXP:** Bindings learned from SXP peers.
4. **IP_ARP:** Bindings learned when tagged ARP packets are received on a CTS-capable link.
5. **LOCAL:** Bindings of authenticated hosts which are learned via EPM and device tracking. This type of binding also includes individual hosts that are learned via ARP snooping on L2 [I] PM-configured ports.
6. **INTERNAL:** Bindings between locally configured IP addresses and the device’s own SGT.

Note
If the source IP address matches multiple subnet prefixes with different assigned SGTs, then the longest prefix SGT takes precedence unless priority differs.

Default Route SGT

- Default Route Security Group Tag (SGT) assigns an SGT number to default routes.
- Default Route is that route that does not match a specified route and therefore is the route to the last resort

destination. Default routes are used to direct packets addressed to networks not explicitly listed in the routing table.

How to Configure SGT Mapping

This section describes how to configure SGT mapping.

Configuring a Device SGT Manually

In normal Cisco TrustSec 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

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.
	Example: Device# **enable**	• 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 1234**	Enables SXP for Cisco TrustSec.
Step 4	**exit** **Example:** Device(config)# **exit**	Exits global configuration mode and returns to privileged EXEC mode

Configuring Subnet-to-SGT Mapping

Procedure

	Command or Action	Purpose
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 mapping network-map** bindings **Example:** Device(config)# **cts sxp mapping network-ma p 10000**	• Configures the Subnet to SGT Mapping host c ount constraint. The bindings argument specifie s the maximum number of subnet IP hosts that c an be bound to SGTs and exported to the SXP li stener. • bindings—(0 to 65,535) default is 0 (no expan sions performed)
Step 4	**cts role-based sgt-map** ipv4_address/prefix **sgt** number **Example:** Device(config)# **cts role-based sgt-map 10.10.10.10/29 sgt 1234**	(IPv4) Specifies a subnet in CIDR notation. • Use the no form of the command to unconfigure the Subnet to SGT mapping. The number of bindings specified in Step 2 should m atch or exceed the number of host addresses in the subnet (excluding network and broadcast ad dresses). The sgt number keyword specifies the Security

		Group Tag to be bound to every host address in the specified subnet. • ipv4_address—Specifies the IPv4 network ad dress in dotted decimal notation. • prefix—(0 to 30) Specifies the number of bits i n the network address. • **sgt** number—(0–65,535) Specifies the Securit y Group Tag (SGT) number.
Step 5	**cts role-based sgt-map** ipv6_address::prefix **sgt** number **Example:** Device(config)# **cts role-based sgt-map 2020::/64 sgt 1234**	(IPv6) Specifies a subnet in colon hexadecimal notation. Use the no form of the command to un configure the Subnet to SGT mapping. The number of bindings specified in Step 2 shou ld match or exceed the number of host addresses in the subnet (excluding network and broadcast addresses). The sgt number keyword specifies the Security Group Tag to be bound to every host address in the specified subnet. • ipv6_address—Specifies IPv6 network addres s in colon hexadecimal notation. • prefix—(0 to128) Specifies the number of bits i n the network address. • **sgt** number—(0–65,535) Specifies the Securit y Group Tag (SGT) number.
Step 6	**exit** **Example:** Device(config)# **exit**	Exits global configuration mode and returns to p rivileged EXEC mode..

Configuring VLAN-to-SGT Mapping

Task Flow for Configuring VLAN-SGT Mapping on a Cisco TrustSec device.

- Create a VLAN on the device with the same VLAN_ID of the incoming VLAN.
- Create an SVI for the VLAN on the device to be the default gateway for the endpoint clients.
- Configure the device to apply an SGT to the VLAN traffic.
- Enable IP Device tracking on the device.
- Attach a device tracking policy to a VLAN.

Note

In a multi-switch network, SISF-based device tracking provides the capability to distribute binding table entries between switches running the feature. This assumes that binding entries are created on the switches where the host appears on an access port, and no entry is created for a host that appears over a trunk port. To achieve this in a multi-switch setup, we recommend that you configure another policy and attach it to the trunk port, as described in the Configuring a Multi-Switch Network to Stop Creating Binding Entries from a Trunk Port procedure, in the Configuring SISF-Based Device Tracking chapter of the Security Configuration Guide.

- Verify that VLAN-to-SGT mapping occurs on the device.

Procedure

	Command or Action	**Purpose**
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	**vlan** vlan_id **Example:** Device(config)# **vlan 100**	Creates VLAN 100 on the TrustSec-capable ga teway device and enters VLAN configuration mode.
Step 4	[**no**] **shutdown** **Example:** Device(config-vlan)# **no shutdown**	Provisions VLAN 100.
Step 5	**exit** **Example:** Device(config-vlan)# **exit**	Exits VLAN configuration mode and returns to global configuration mode.
Step 6	**interface** type slot/port **Example:** Device(config)# **interface vlan 100**	Specifies the interface type and enters interfac e configuration mode.
Step 7	**ip address** slot/port **Example:** Device(config-if)# **ip address 10.1.1.2 255.0.0.0**	Configures Switched Virtual Interface (SVI) for VLAN 100.

Step 8	[**no**] **shutdown** **Example:** Device(config-if)# **no shutdown**	Enables the SVI.
Step 9	**exit** **Example:** Device(config-if)# **exit**	Exits interface configuration mode and returns to global configuration mode.
Step 10	**cts role-based sgt-map vlan-list** vlan_id **sgt** sgt_number **Example:** Device(config)# **cts role-based sgt-map vlan-list 100 sgt 10**	Assigns the specified SGT to the specified VLAN.
Step 11	**device-tracking policy** policy-name **Example:** Device(config)# **device-tracking policy policy1**	Specifies the policy and enters device-tracking policy configuration mode.
Step 12	**tracking enable** **Example:** Device(config-device-tracking)# **tracking enable**	Overrides the default device tracking settings for the policy attribute.
Step 13	**exit** **Example:** Device(config-device-tracking)# **exit**	Exits device-tracking policy configuration mode and returns to global configuration mode.
Step 14	**vlan configuration** vlan_id **Example:** Device(config)# **vlan configuration 100**	Specifies the VLAN to which the device tracking policy will be attached, and enters the VLAN configuration mode.
Step 15	**device-tracking attach-policy** policy-name **Example:** Device(config-vlan-config)# **device-tracking attach-policy policy1**	Attaches a device tracking policy to the specified VLAN.

<table>
<tr><td><b>Step 16</b></td><td><b>end</b>
<b>Example:</b>
Device(config-vlan-config)# <b>end</b></td><td>Exits VLAN configuration mode and returns to privileged EXEC mode.</td></tr>
<tr><td><b>Step 17</b></td><td><b>show cts role-based sgt-map</b> {ipv4_netaddr
| ipv4_netaddr/prefix | ipv6_netaddr | ipv6_netaddr/prefix |<b>all</b> [<b>ipv4</b> |<b>ipv6</b>] |<b>host</b> { ipv4 addr |ipv6_addr } |<b>summary</b> [<b>ipv4</b>
|<b>ipv6</b>]
<b>Example:</b>
Device# <b>show cts role-based sgt-map all</b></td><td>(Optional) Displays the VLAN-to-SGT mappings.</td></tr>
<tr><td><b>Step 18</b></td><td><b>show device-tracking policy</b> policy-name
<b>Example:</b>
Device# <b>show device-tracking policy policy 1</b></td><td>(Optional) Displays the current policy attributes.</td></tr>
</table>

Emulating the Hardware Keystore

In cases where a hardware keystore is not present or is unusable, you can configure the switch to use a software emulation of the keystore. To configure the use of a software keystore, perform this task:

Procedure

	Command or Action	Purpose
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 keystore emulate** **Example:** Device(config)# **cts keystore emulate**	Configures the switch to use a software emulati on of the keystore instead of the hardware keyst ore.
Step 4	**exit** **Example:** Device(config)# **exit**	Exits configuration mode.
Step 5	**show keystore** **Example:** Device# **show keystore**	Displays the status and contents of the keystore . The stored secrets are not displayed.

Configuring Default Route SGT

Before you begin

Ensure that you have already created a default route on the device using the ip route 0.0.0.0 command. Otherwise, the default route (which comes with the Default Route SGT) gets an unknown destination and therefore the last resort destination will point to CPU.

Procedure

	Command or Action	Purpose
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 role-based sgt-map 0.0.0.0/0 sgt** number **Example:** Device(config)# cts role-based sgt-map 0.0.0.0/0 sgt 3	Specifies the SGT number for the default route. Valid values are from 0 to 65,519. **Note** • The **host_address/subnet** can be either IPv4 address (0.0.0.0/0) or IPv6 address (0:0::/0) • The default route configuration is accepted only with the subnet **/0** . Entering only the host-ip without the subnet /0 displays the following message: Device(config)#**cts role-based sgt-map** **0.0.0.0 sgt 1000** Default route configuration is not supported for host ip
Step 4	**exit** **Example:** Device(config)# exit	Exits global configuration mode.

Verifying SGT Mapping

The following sections show how to verify SGT mapping:

Verifying Subnet-to-SGT Mapping Configuration

To display Subnet-to-SGT Mapping configuration information, use one of the following show commands:

Command	Purpose
show cts sxp connections	Displays the SXP speaker and listener connections with their operational status.
show cts sxp sgt-map	Displays the IP to SGT bindings exported to the SXP listeners.
show running-config	Verifies that the subnet-to-SGT configurations commands are in the running configuration file.

Verifying VLAN-to-SGT Mapping

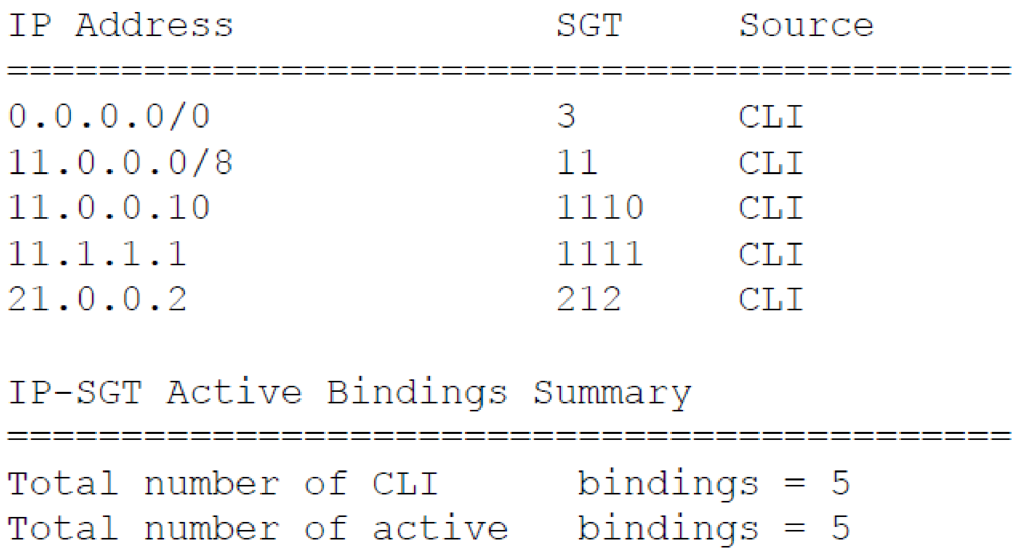
To display VLAN-to-SGT configuration information, use the following show commands:

Table 1:

Command	Purpose
show device-tracking policy	Displays the current policy attributes of the device trac king policy.
show cts role-based sgt-map	Displays IP address-to-SGT bindings.

Verifying Default Route SGT Configuration

Verify the Default Route SGT configuration:
device# show role-based sgt-map all Active IPv4-SGT Bindings Information



```
IP Address                SGT     Source
============================================
0.0.0.0/0                 3       CLI
11.0.0.0/8                11      CLI
11.0.0.10                 1110    CLI
11.1.1.1                  1111    CLI
21.0.0.2                  212     CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI       bindings = 5
Total number of active    bindings = 5
```

Configuration Examples for SGT Mapping

The following sections show configuration examples of SGT mapping:

Example: Configuring a Device SGT Manually

- Device# configure terminal
- Device(config)# cts sgt 1234
- Device(config)# exit

Example: Configuration for Subnet-to-SGT Mapping
The following example shows how to configure IPv4 Subnet-to-SGT Mapping between devices running SXPv3 (Device1 and Device2):

1. **Configure SXP speaker/listener peering between devices.**
    - Device1# configure terminal
    - Device1(config)# cts sxp enable

   - Device1(config)# cts sxp default source-ip 1.1.1.1
   - Device1(config)# cts sxp default password 1syzygy1
   - Device1(config)# cts sxp connection peer 2.2.2.2 password default mode local speaker

2. **Configure Device2 as SXP listener of Device1.**
   - Device2(config)# cts sxp enable
   - Device2(config)# cts sxp default source-ip 2.2.2.2
   - Device2(config)# cts sxp default password 1syzygy1
   - Device2(config)# cts sxp connection peer 1.1.1.1 password default mode local listener
3. **On Device2, verify that the SXP connection is operating:**

   Device2# show cts sxp connections brief | include 1.1.1.1 1.1.1.1 2.2.2.2 On 3:22:23:18 (dd:hr:mm:sec)
4. **Configure the subnetworks to be expanded on Device1.**
   - Device1(config)# cts sxp mapping network-map 10000
   - Device1(config)# cts role-based sgt-map 10.10.10.0/30 sgt 101
   - Device1(config)# cts role-based sgt-map 11.11.11.0/29 sgt 11111
   - Device1(config)# cts role-based sgt-map 192.168.1.0/28 sgt 65000
5. On Device2, verify the subnet-to-SGT expansion from Device1. There should be two expansions for the 10.10.10.0/30 subnetwork, six expansions for the 11.11.11.0/29 subnetwork, and 14 expansions for the 192.168.1.0/28 subnetwork.

   Device2# show cts sxp sgt-map brief | include 101|11111|65000
   - IPv4,SGT: <10.10.10.1 , 101>
   - IPv4,SGT: <10.10.10.2 , 101>
   - IPv4,SGT: <11.11.11.1 , 11111>
   - IPv4,SGT: <11.11.11.2 , 11111>
   - IPv4,SGT: <11.11.11.3 , 11111>
   - IPv4,SGT: <11.11.11.4 , 11111>
   - IPv4,SGT: <11.11.11.5 , 11111>
   - IPv4,SGT: <11.11.11.6 , 11111>
   - IPv4,SGT: <192.168.1.1 , 65000>
   - IPv4,SGT: <192.168.1.2 , 65000>
   - IPv4,SGT: <192.168.1.3 , 65000>
   - IPv4,SGT: <192.168.1.4 , 65000>
   - IPv4,SGT: <192.168.1.5 , 65000>
   - IPv4,SGT: <192.168.1.6 , 65000>
   - IPv4,SGT: <192.168.1.7 , 65000>
   - IPv4,SGT: <192.168.1.8 , 65000>
   - IPv4,SGT: <192.168.1.9 , 65000>
   - IPv4,SGT: <192.168.1.10 , 65000>
   - IPv4,SGT: <192.168.1.11 , 65000>
   - IPv4,SGT: <192.168.1.12 , 65000>
   - IPv4,SGT: <192.168.1.13 , 65000>
   - IPv4,SGT: <192.168.1.14 , 65000>
6. **Verify the expansion count on Device1:**

   Device1# show cts sxp sgt-map

    - IP-SGT Mappings expanded:22
    - There are no IP-SGT Mappings

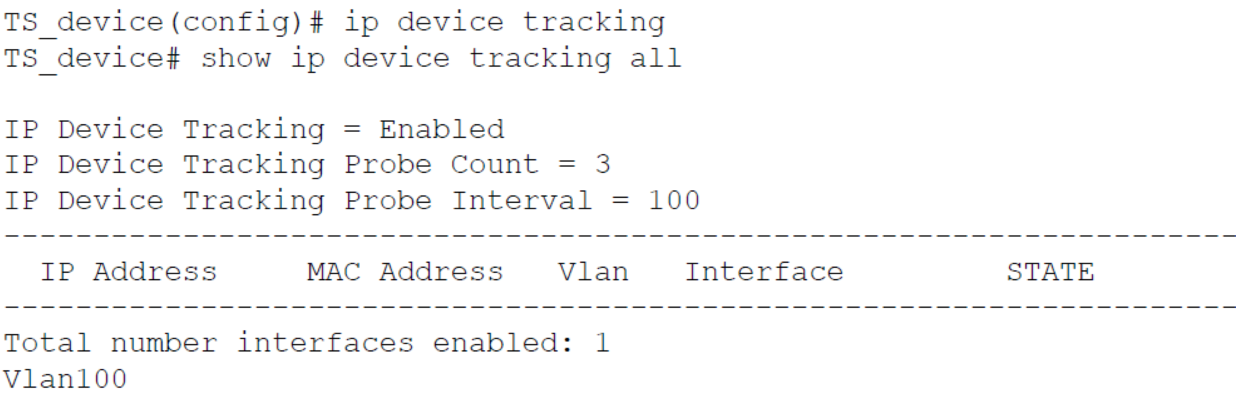
7. **Save the configurations on Device1 and Device2 and exit global configuration mode.**

   ```
   Device1(config)# copy running-config startup-config
   Device1(config)# exit
   Device2(config)# copy running-config startup-config
   Device2(config)# exit
   ```

Example:
Configuration for VLAN-to-SGT Mapping for a Single Host Over an Access Link.

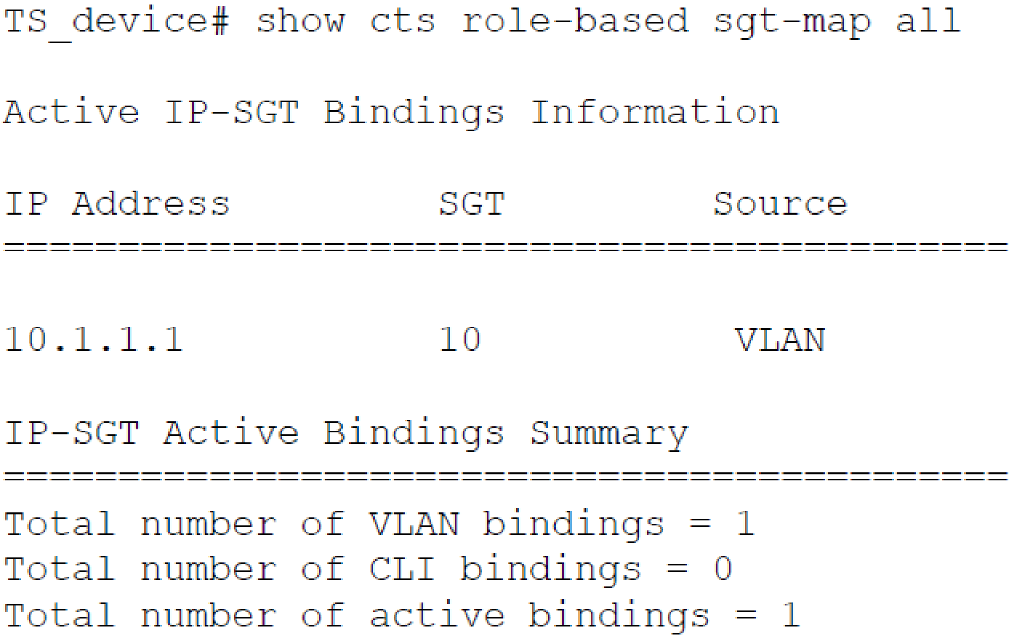
In the following example, a single host connects to VLAN 100 on an access device. A switched virtual interface on the TrustSec device is the default gateway for the VLAN 100 endpoint (IP Address 10.1.1.1). The TrustSec device imposes Security Group Tag (SGT) 10 on packets from VLAN 100.

1. **Create VLAN 100 on an access device.**
    - access_device# configure terminal
    - access_device(config)# vlan 100
    - access_device(config-vlan)# no shutdown
    - access_device(config-vlan)# exit
    - access_device(config)#
2. **Configure the interface to the TrustSec device as an access link. Configurations for the endpoint**
    1. access port are omitted in this example.
    2. access_device(config)# interface gigabitEthernet 6/3
    3. access_device(config-if)# switchport
    4. access_device(config-if)# switchport mode access
    5. access_device(config-if)# switchport access vlan 100
3. **Create VLAN 100 on the TrustSec device.**
    - TS_device(config)# vlan 100
    - TS_device(config-vlan)# no shutdown
    - TS_device(config-vlan)# end
    - TS_device#
4. **Create an SVI as the gateway for incoming VLAN 100.**
    - TS_device(config)# interface vlan 100
    - TS_device(config-if)# ip address 10.1.1.2 255.0.0.0
    - TS_device(config-if)# no shutdown
    - TS_device(config-if)# end
    - TS_device(config)#
5. **Assign Security Group Tag (SGT) 10 to hosts on VLAN 100.**
    - TS_device(config)# cts role-based sgt-map vlan 100 sgt 10
6. **Enable IP Device Tracking on the TrustSec device. Verify that it is operating.**
    - TS_device(config)# ip device tracking
    - TS_device# show ip device tracking all



```
TS_device(config)# ip device tracking
TS_device# show ip device tracking all

IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 100
----------------------------------------------------------------------
  IP Address     MAC Address   Vlan   Interface          STATE
----------------------------------------------------------------------
Total number interfaces enabled: 1
Vlan100
```

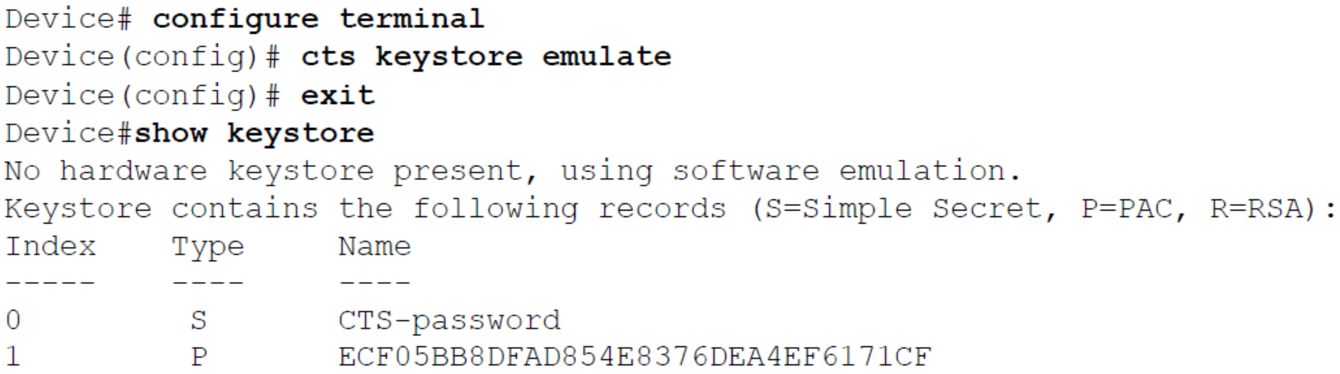
7. (Optional) PING the default gateway from an endpoint (in this example, host IP Address 10.1.1.1). Verify that SGT 10 is being mapped to VLAN 100 hosts.



```
TS_device# show cts role-based sgt-map all

Active IP-SGT Bindings Information

IP Address           SGT          Source
============================================

10.1.1.1             10            VLAN

IP-SGT Active Bindings Summary
============================================
Total number of VLAN bindings = 1
Total number of CLI bindings = 0
Total number of active bindings = 1
```

Example: Emulating the Hardware Keystore

This example shows how to configure and verify the use of a software keystore:



```
Device# configure terminal
Device(config)# cts keystore emulate
Device(config)# exit
Device#show keystore
No hardware keystore present, using software emulation.
Keystore contains the following records (S=Simple Secret, P=PAC, R=RSA):
Index    Type     Name
-----    ----     ----
0         S       CTS-password
1         P       ECF05BB8DFAD854E8376DEA4EF6171CF
```

Example: Configuring Device Route SGT

- Device# configure terminal
- Device(config)# cts role-based sgt-map 0.0.0.0/0 sgt 3
- Device(config)# exit

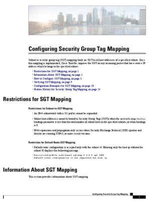
Feature History for Security Group Tag Mapping

- This table provides release and related information for the features explained in this module.
- These features are available in all the releases after the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Everest 16.5.1a	Security Group Tag Mapping	Subnet to SGT mapping binds an SGT to all host addresses of a specified subnet. Once this mapping is implemented, Cisco TrustSec imposes the SGT on any incoming packet that has a source IP address that belongs to the specified subnet.
Cisco IOS XE Gibraltar 16.11.1	Default Route SGT Classification	Default Route SGT assigns an SGT tag number to those routes that do not match a specified route.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to **http://www.cisco.com/go/cfn**.

Documents / Resources

 Configuring Security Group Tag Mapping
Subnet to security group tag (SGT) mapping binds an SGT to all host addresses of a specified subnet. Once this mapping is implemented, Cisco TrustSec imposes the SGT on any incoming packet that has a source IP address which belongs to the specified subnet.
• Restrictions for SGT Mapping, on page 1
• Information About SGT Mapping, on page 1
• How to Configure SGT Mapping, on page 3
• Verifying SGT Mapping, on page 9
• Configuration Examples for SGT Mapping, on page 10
• Feature History for Security Group Tag Mapping, on page 14
Restrictions for SGT Mapping
Restrictions for Subnet-to-SGT Mapping
• An IPv4 subnetwork with a /31 prefix cannot be expanded.
• Subnet host addresses cannot be bound to Security Group Tags (SGTs) when the network-map bindings parameter is less than the total number of subnet hosts in the specified subnets, or when bindings is 0.
• IPv6 expansions and propagation only occurs when Security Exchange Protocol (SXP) speaker and listener are running SXPv3, or more recent versions.
Restriction for Default Route SGT Mapping
• Default route configuration is accepted only with the subnet /0. Entering only the host-ip without the subnet /0 displays the following message:
`Device(config)#cts role-based sgt-map 0.0.0.0 sgt 1000`
`Default route configuration is not supported for host ip`
Information About SGT Mapping
This section provides information about SGT mapping.
Configuring Security Group Tag Mapping 1
	CISCO Configuring Security Group Tag Mapping [pdf] User Guide
	Configuring Security Group Tag Mapping, Configuring, Security Group Tag Mapping, Group Tag Mapping, Tag Mapping

References

- **User Manual**