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 Manually, on page 1
- How to Configure SGT Mapping, on page 3
- Verifying SGT Mapping, on page 10
- Configuration Examples for SGT Mapping, on page 10
- Feature Information for SGT 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 (SGT)s 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.

Information About SGT Mapping Manually

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 12-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 listing in the Binding Source Priorities section.

**Overview of Layer 3 Logical Interface-to-SGT Mapping (L3IF–SGT Mapping)**

L3IF-SGT mapping can directly map SGTs to traffic of any of the following Layer 3 interfaces regardless of the underlying physical interface:

- Routed port
- SVI (VLAN interface)
- Layer 3 subinterface of a Layer 2 port
• Tunnel interface

Use the cts role-based sgt-map interface global configuration command to specify either a specific SGT number, or a Security Group Name (whose SGT association is dynamically acquired from a Cisco ISE or a Cisco ACS access server).

In cases where Identity Port Mapping (cts interface manual sub mode configuration) and L3IF-SGT require different IP to SGT bindings, IPM takes precedence. All other conflicts among IP to SGT binding are resolved according to the priorities listing 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. Layer 3 Interface—(L3IF) Bindings added due to FIB forwarding entries that have paths through one or more interfaces with consistent L3IF-SGT mapping or Identity Port Mapping on routed ports.
4. SXP—Bindings learned from SXP peers.
5. IP_ARP—Bindings learned when tagged ARP packets are received on a CTS capable link.
6. LOCAL—Bindings of authenticated hosts which are learned via EPM and device tracking. This type of binding also include individual hosts that are learned via ARP snooping on L2 [I]PM configured ports.
7. INTERNAL—Bindings between locally configured IP addresses and the device own SGT.

**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:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. cts sgt tag
4. exit
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> cts sgt tag</td>
<td>Enables SXP for Cisco TrustSec.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# cts sgt 1234</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits global configuration mode and returns to privileged EXEC mode</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Subnet-to-SGT Mapping

#### Summary Steps

1. enable
2. configure terminal
3. cts sxp mapping network-map bindings
4. cts role-based sgt-map ipv4_address/prefix sgt number
5. cts role-based sgt-map ipv6_address::prefix sgt number
6. exit

#### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> cts sxp mapping network-map bindings</td>
<td>• Configures the Subnet to SGT Mapping host count constraint. The bindings argument specifies the maximum number of subnet IP hosts that can be bound to SGTS and exported to the SXP listener.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# cts sxp mapping network-map 10000</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bindings</strong>—(0 to 65,535) default is 0 (no expansions performed)</td>
<td></td>
</tr>
<tr>
<td><strong>cts role-based sgt-map ipv4_address/prefix sgt number</strong></td>
<td>(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 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.</td>
</tr>
<tr>
<td><strong>ipv4_address</strong>—Specifies the IPv4 network address in dotted decimal notation.</td>
<td></td>
</tr>
<tr>
<td><strong>prefix</strong>—(0 to 30) Specifies the number of bits in the network address.</td>
<td></td>
</tr>
<tr>
<td><strong>sgt number</strong>—(0–65,535) Specifies the Security Group Tag (SGT) number.</td>
<td></td>
</tr>
<tr>
<td><strong>cts role-based sgt-map ipv6_address::prefix sgt number</strong></td>
<td>(IPv6) Specifies a subnet in colon hexadecimal notation. Use the no form of the command to unconfigure the Subnet to SGT mapping. The number of bindings specified in Step 2 should 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.</td>
</tr>
<tr>
<td><strong>ipv6_address</strong>—Specifies IPv6 network address in colon hexadecimal notation.</td>
<td></td>
</tr>
<tr>
<td><strong>prefix</strong>—(0 to 128) Specifies the number of bits in the network address.</td>
<td></td>
</tr>
<tr>
<td><strong>sgt number</strong>—(0–65,535) Specifies the Security Group Tag (SGT) number.</td>
<td></td>
</tr>
<tr>
<td><strong>exit</strong></td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### Configuring VLAN-to-SGT Mapping

#### Task Flow for Configuring VLAN-SGT Mapping

- Create a VLAN on the TrustSec device with the same VLAN_ID of the incoming VLAN.
• Create an SVI for the VLAN on the TrustSec device to be the default gateway for the endpoint clients.
• Configure the TrustSec device to apply an SGT to the VLAN traffic.
• Enable IP Device tracking on the TrustSec device.
• Verify that VLAN-to-SGT mapping occurs on the TrustSec device.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. vlan vlan_id
4. [no] shutdown
5. exit
6. interface type slot/port
7. ip address slot/port
8. [no] shutdown
9. exit
10. cts role-based sgt-map vlan-list vlan_id sgt sgt_number
11. ip device tracking probe [count count | delay seconds | interval length ]
12. exit
13. show cts role-based sgt-map {ipv4_netaddr | ipv4_netaddr/prefix | ipv6_netaddr | ipv6_netaddr/prefix | all | ipv4 | ipv6 | host {ipv4_addr | ipv6_addr | ipv6addr | ipv6_addr/prefix} | summary {ipv4 | ipv6}]
14. show ip device tracking {all | interface | ip | mac}

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vlan vlan_id</td>
<td>Creates VLAN 100 on the TrustSec-capable gateway device and enters VLAN configuration submode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# vlan 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> [no] shutdown</td>
<td>Provisions VLAN 100.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-vlan)# no shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits VLAN configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>Device(config-vlan)# exit</code></td>
<td>Enters interface configuration mode.</td>
</tr>
</tbody>
</table>

**Step 6**  
`interface type slot/port`  
**Example:**  
`Device(config)# interface vlan 100`  
Configures Switched Virtual Interface (SVI) for VLAN 100.

**Step 7**  
`ip address slot/port`  
**Example:**  
`Device(config-if)# ip address 10.1.1.2 255.0.0.0`  
Enables the SVI.

**Step 8**  
`[no ] shutdown`  
**Example:**  
`Device(config-if)# no shutdown`  
Exits VLAN interface configuration mode and returns to global configuration mode.

**Step 9**  
`exit`  
**Example:**  
`Device(config-if)# exit`  
Assigns the specified SGT to the specified VLAN.

**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`  
Enables IP device tracking. When active hosts are detected, the device adds the following entries to an IP Device tracking table:

- IP address of host
- MAC address of host
- VLAN of the host
- The interface on which the device detected the host
- The state of the host (active or inactive)

The host added to the IP Device tracking table is monitored with periodic ARP probes. Hosts that fail to respond are removed from the table.

**Step 12**  
`exit`  
**Example:**  
`Device(config)# exit`  
(Optional) Displays the VLAN-to-SGT mappings.
### Configuring L3IF-to-SGT Mapping

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts role-based sgt-map interface** *type slot/port* [*security-group name | sgt number*]
4. **exit**
5. **show cts role-based sgt-map all**

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  Example:  
  Device# enable |
| **Step 2** configure terminal | Enters global configuration mode.  
  Example:  
  Device# configure terminal |
| **Step 3** cts role-based sgt-map interface *type slot/port* [*security-group name | sgt number*] | An SGT is imposed on ingress traffic to the specified interface.  
  Example:  
  Device(config)# cts role-based sgt-map interface gigabitEthernet 1/1 sgt 77  
  • interface *type slot/port* — Displays list of available interfaces.  
  • security-group *name* — Security Group name to SGT pairings are configured on the Cisco ISE or Cisco ACS.  
  • sgt *number* — (0 to 65,535). Specifies the Security Group Tag (SGT) number. |
| **Step 4** exit | Exits configuration mode.  
  Example:  
  Device(config)# exit |
| **Step 5** show cts role-based sgt-map all | Verify that ingressing traffic is tagged with the specified SGT.  
  Example:  
  Device(config)# show cts role-based sgt-map all |
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:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `cts keystore emulate`
4. `exit`
5. `show keystore`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>cts keystore emulate</code></td>
<td>Configures the switch to use a software emulation of the keystore instead of the hardware keystore.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>cts keystore emulate</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# <code>cts keystore emulate</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>exit</code></td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>exit</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# <code>exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>show keystore</code></td>
<td>Displays the status and contents of the keystore. The stored secrets are not displayed.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>show keystore</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# <code>show keystore</code></td>
<td></td>
</tr>
</tbody>
</table>
Verifying SGT Mapping

Verifying Subnet-to-SGT Mapping Configuration

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show cts sxp connections</code></td>
<td>Displays the SXP speaker and listener connections with their operational status.</td>
</tr>
<tr>
<td><code>show cts sxp sgt-map</code></td>
<td>Displays the IP to SGT bindings exported to the SXP listeners.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verifies that the subnet-to-SGT configurations commands are in the running configuration file.</td>
</tr>
</tbody>
</table>

Verifying VLAN-to-SGT Mapping

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

Table 1:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip device tracking</code></td>
<td>Displays the status of IP Device Tracking which identifies the IP addresses of active hosts on a VLAN.</td>
</tr>
<tr>
<td><code>show cts role-based sgt-map</code></td>
<td>Displays IP address-to-SGT bindings.</td>
</tr>
</tbody>
</table>

Verifying L3IF-to-SGT Mapping

To display L3IF-to-SGT configuration information, use the following show command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show cts role-based sgt-map all</code></td>
<td>Displays all IP address-to-SGT bindings.</td>
</tr>
</tbody>
</table>

Configuration Examples for SGT Mapping

Example: Configurating 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 l1syzygy1
   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 l1syzygy1
   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
   ```

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 access port are omitted in this example.

     access_device(config)# interface gigabitEthernet 6/3
     access_device(config-if)# switchport
     access_device(config-if)# switchport mode access
     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

     IP Device Tracking = Enabled
Example: Configuration for L3IF-to-SGT Mapping on an Ingress Port

In the following example a Layer 3 interface of a device linecard is configured to tag all ingressing traffic with SGT 3. Prefixes of attached subnets are already known.

1. Configure the interface.

   Device# configure terminal
   Device(config)# interface gigabitEthernet 6/3 sgt 3
   Device(config)# exit

2. Verify that the ingressing traffic to the interface is tagged appropriately.

   Device# show cts role-based sgt-map all

   IP Address  SGT  Source
   --------------------------
   15.1.1.15  4  INTERNAL
   17.1.1.0/24  3  L3IF
   21.1.1.2  4  INTERNAL
   31.1.1.0/24  3  L3IF
   31.1.1.2  4  INTERNAL
   43.1.1.0/24  3  L3IF
   49.1.1.0/24  3  L3IF
   50.1.1.0/24  3  L3IF
   50.1.1.2  4  INTERNAL
   51.1.1.1  4  INTERNAL
   52.1.1.0/24  3  L3IF
   81.1.1.1  5  CLI
   102.1.1.1  4  INTERNAL
   105.1.1.1  3  L3IF
   111.1.1.1  4  INTERNAL

   Example: Configuration for L3IF-to-SGT Mapping on an Ingress Port

   In the following example a Layer 3 interface of a device linecard is configured to tag all ingressing traffic with SGT 3. Prefixes of attached subnets are already known.

   1. Configure the interface.

      Device# configure terminal
      Device(config)# interface gigabitEthernet 6/3 sgt 3
      Device(config)# exit

   2. Verify that the ingressing traffic to the interface is tagged appropriately.

      Device# show cts role-based sgt-map all

      IP Address  SGT  Source
      --------------------------
      15.1.1.15  4  INTERNAL
      17.1.1.0/24  3  L3IF
      21.1.1.2  4  INTERNAL
      31.1.1.0/24  3  L3IF
      31.1.1.2  4  INTERNAL
      43.1.1.0/24  3  L3IF
      49.1.1.0/24  3  L3IF
      50.1.1.0/24  3  L3IF
      50.1.1.2  4  INTERNAL
      51.1.1.1  4  INTERNAL
      52.1.1.0/24  3  L3IF
      81.1.1.1  5  CLI
      102.1.1.1  4  INTERNAL
      105.1.1.1  3  L3IF
      111.1.1.1  4  INTERNAL

   Example: Configuration for L3IF-to-SGT Mapping on an Ingress Port

   In the following example a Layer 3 interface of a device linecard is configured to tag all ingressing traffic with SGT 3. Prefixes of attached subnets are already known.

   1. Configure the interface.

      Device# configure terminal
      Device(config)# interface gigabitEthernet 6/3 sgt 3
      Device(config)# exit

   2. Verify that the ingressing traffic to the interface is tagged appropriately.

      Device# show cts role-based sgt-map all

      IP Address  SGT  Source
      --------------------------
      15.1.1.15  4  INTERNAL
      17.1.1.0/24  3  L3IF
      21.1.1.2  4  INTERNAL
      31.1.1.0/24  3  L3IF
      31.1.1.2  4  INTERNAL
      43.1.1.0/24  3  L3IF
      49.1.1.0/24  3  L3IF
      50.1.1.0/24  3  L3IF
      50.1.1.2  4  INTERNAL
      51.1.1.1  4  INTERNAL
      52.1.1.0/24  3  L3IF
      81.1.1.1  5  CLI
      102.1.1.1  4  INTERNAL
      105.1.1.1  3  L3IF
      111.1.1.1  4  INTERNAL
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):

<table>
<thead>
<tr>
<th>Index</th>
<th>Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>S</td>
<td>CTS-password</td>
</tr>
<tr>
<td>1</td>
<td>P</td>
<td>ECF05BB8DFAD854E8376DEA4EF6171CF</td>
</tr>
</tbody>
</table>
```

Feature Information for SGT Mapping

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

```
Table 2: Feature Information for SGT Mapping
```

Total number of INTERNAL bindings = 7
Total number of active bindings = 15