CHAPTER 3

Configuring Identities, Connections, and SGTs

Revised: October 7, 2013, OL-22192-02

This section includes the following topics:

Cisco TrustSec Identity Configuration Feature Histories

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

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

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

Configuring Credentials and AAA for a Cisco TrustSec Seed Device

A Cisco TrustSec-capable device that is directly connected to the authentication server, or indirectly connected but is the first device to begin the TrustSec domain, is called the seed device. Other Cisco TrustSec network devices are non-seed devices.

To enable NDAC and AAA on the seed switch so that it can begin the Cisco TrustSec domain, perform these steps:

Detailed Steps for Catalyst 6500, Catalyst 3K

	Command	Purpose
Step 1	`Router# cts credentials id device-id password password`	Specifies the Cisco TrustSec device ID and password for this switch to use when authenticating with other Cisco TrustSec devices with EAP-FAST. The *device-id* argument has a maximum length of 32 characters and is case sensitive.
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# aaa new-model`	Enables AAA.
Step 4	`Router(config)# aaa authentication dot1x default group radius`	Specifies the 802.1X port-based authentication method as RADIUS.
Step 5	`Router(config)# aaa authorization network mlist group radius`	Configures the switch to use RADIUS authorization for all network-related service requests. • *mlist*—The Cisco TrustSec AAA server group.
Step 6	`Router(config)# cts authorization list mlist`	Specifies a Cisco TrustSec AAA server group. Non-seed devices will obtain the server list from the authenticator.
Step 7	`Router(config)# aaa accounting dot1x default start-stop group radius`	Enables 802.1X accounting using RADIUS.
Step 8	`Router(config)# radius-server host ip-addr auth-port 1812 acct-port 1813 pac key secret`	Specifies the RADIUS authentication server host address, service ports, and encryption key. • *ip-addr*—The IP address of the authentication server. • *secret*—The encryption key shared with the authentication server.
Step 9	`Router(config)# radius-server vsa send authentication`	Configures the switch to recognize and use vendor-specific attributes (VSAs) in RADIUS Access-Requests generated by the switch during the authentication phase.
Step 10	`Router(config)# dot1x system-auth-control`	Globally enables 802.1X port-based authentication.
Step 11	`Router(config)# exit`	Exits configuration mode.

Note You must also configure the Cisco TrustSec credentials for the switch on the Cisco Identity Services Engine (Cisco ISE) or the Cisco Secure Access Control Server (Cisco ACS).

Configuration Examples for Seed Device

Catalyst 6500 configured as a Cisco TrustSec seed device:

```
Router# cts credentials id Switch1 password Cisco123
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# aaa authorization network MLIST group radius
Router(config)# cts authorization list MLIST
Router(config)# aaa accounting dot1x default start-stop group radius
Router(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key AbCe1234
Router(config)# radius-server vsa send authentication
Router(config)# dot1x system-auth-control
Router(config)# exit
```

Configuring Credentials and AAA for a Cisco TrustSec Non-Seed Device

To enable NDAC and AAA on a non-seed switch so that it can join the Cisco TrustSec domain, perform these steps:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router# cts credentials id` *device-id* `password` *password*	Specifies the Cisco TrustSec device ID and password for this switch to use when authenticating with other Cisco TrustSec devices with EAP-FAST. The *device-id* argument has a maximum length of 32 characters and is case sensitive.
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# aaa new-model`	Enables AAA.
Step 4	`Router(config)# aaa authentication dot1x default group radius`	Specifies the 802.1X port-based authentication method as RADIUS.
Step 5	`Router(config)# aaa authorization network` *mlist* `group radius`	Configures the switch to use RADIUS authorization for all network-related service requests. • *mlist*—Specifies a Cisco TrustSec AAA server group.
Step 6	`Router(config)# aaa accounting dot1x default start-stop group radius`	Enables 802.1X accounting using RADIUS.

	Command	Purpose
Step 7	`Router(config)# radius-server vsa send authentication`	Configures the switch to recognize and use vendor-specific attributes (VSAs) in RADIUS Access-Requests generated by the switch during the authentication phase.
Step 8	`Router(config)# dot1x system-auth-control`	Globally enables 802.1X port-based authentication.
Step 9	`Router(config)# exit`	Exits configuration mode.

Note You must also configure the Cisco TrustSec credentials for the switch on the Cisco Identity Services Engine, or the Cisco Secure ACS.

Configuration Examples for Non-Seed Device

Catalyst 6500 example:

```
Router# cts credentials id Switch2 password Cisco123
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# aaa authorization network MLIST group radius
Router(config)# aaa accounting dot1x default start-stop group radius
Router(config)# radius-server vsa send authentication
Router(config)# dot1x system-auth-control
Router(config)# exit
```

Catalyst 3850/3650 example for access VLAN, where propagate SGT is not the default:

```
switch(config-if)# switchport access vlan 222
switch(config-if)# switchport mode access
switch(config-if)# authentication port-control auto
switch(config-if)# dot1x pae authenticator
switch(config-if)# cts dot1x
switch(config-if)# propagate sgt
```

Enabling Cisco TrustSec Authentication and MACsec in 802.1X Mode on an Uplink Port

You must enable Cisco TrustSec authentication on each interface that will connect to another Cisco TrustSec device. To configure Cisco TrustSec authentication with 802.1X on an uplink interface to another Cisco TrustSec device, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# interface type slot/port`	Enters interface configuration mode for the uplink interface.
Step 3	`Router(config-if)# cts dot1x`	Configures the uplink interface to perform NDAC authentication.
Step 4	`Router(config-if-cts-dot1x)# [no] sap mode-list mode1 [mode2 [mode3 [mode4]]]`	(Optional) Configures 802.1AE MACsec with the SAP operation mode on the interface. The interface will negotiate with the peer for a mutually-acceptable mode. List the acceptable modes in your order of preference. Choices for *mode* are: • **gcm**— Authentication and encryption • **gmac**— Authentication, no encryption • **no-encap**— No encapsulation • **null**— Encapsulation, no authentication, no encryption **Note** MACsec with SAP is not supported on the Catalyst 3K switches. **Note** If the interface is not capable of SGT insertion or data link encryption, **no-encap** is the default and the only available SAP operating mode.
Step 5	`Router(config-if-cts-dot1x)# [no] timer reauthentication seconds`	(Optional) Configures a reauthentication period to be used if the authentication server does not specify a period. If no reauthentication period is specified, the default period is 86400 seconds.
Step 6	`Router(config-if-cts-dot1x)# [no] propagate sgt`	(Optional) The **no** form of this command is used when the peer is incapable of processing an SGT. The **no propagate sgt** command prevents the interface from transmitting the SGT to the peer.
Step 7	`Router(config-if-cts-dot1x)# exit`	Exits Cisco TrustSec 802.1X interface configuration mode.
Step 8	`Router(config-if)# shutdown`	Disables the interface.

	Command	Purpose
Step 9	`Router(config-if)# no shutdown`	Enables the interface and enables Cisco TrustSec authentication on the interface.
Step 10	`Router(config-if)# exit`	Exits interface configuration mode.

Configuration Examples for 802.1X on Uplink Port

Catalyst 6500 Cisco TrustSec authentication in 802.1X mode on an interface using GCM as the preferred SAP mode; the authentication server did not provide a reauthentication timer:

```
Router# configure terminal
Router(config)# interface gi2/1
Router(config-if)# cts dot1x
Router(config-if-cts-dot1x)# sap mode-list gcm null no-encap
Router(config-if-cts-dot1x)# timer reauthentication 43200
Router(config-if-cts-dot1x)# propagate sgt
Router(config-if-cts-dot1x)# exit
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

Configuring Cisco TrustSec and MACsec in Manual Mode on an Uplink Port

You can manually configure Cisco TrustSec on an interface. You must manually configure the interfaces on both ends of the connection. No authentication occurs; policies can be statically configured or dynamically downloaded from an authentication server by specifying the server's device identity.

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# interface` *type slot/port*	Enters interface configuration mode for the uplink interface.
Step 3	`Router(config-if)# cts manual`	Enters Cisco TrustSec manual configuration mode.

	Command	Purpose
Step 4	`Router(config-if-cts-manual)# [no] sap pmk key [mode-list mode1 [mode2 [mode3 [mode4]]]]`	(Optional) Configures the SAP pairwise master key (PMK) and operation mode. SAP is disabled by default in Cisco TrustSec manual mode. • *key*—A hexadecimal value with an even number of characters and a maximum length of 32 characters. The SAP operation *mode* options are: • **gcm**— Authentication and encryption • **gmac**— Authentication, no encryption • **no-encap**— No encapsulation • **null**— Encapsulation, no authentication or encryption **Note** MACsec with SAP is not supported on the Catalyst 3K switches. **Note** If the interface is not capable of SGT insertion or data link encryption, **no-encap** is the default and the only available SAP operating mode.
Step 5	`Router(config-if-cts-manual)# [no] policy dynamic identity peer-name`	(Optional) Configures Identity Port Mapping (IPM) to allow dynamic authorization policy download from authorization server based on the identity of the peer. See the additional usage notes following this task. • *peer-name*—The Cisco TrustSec device ID for the peer device. The peer name is case sensitive. **Note** Ensure that you have configured the Cisco TrustSec credentials (see "Configuring Credentials and AAA for a Cisco TrustSec Seed Device" section on page 3-2).
	`Router(config-if-cts-manual)# [no] policy static sgt tag [trusted]`	(Optional) Configures a static authorization policy. See the additional usage notes following this task. • *tag*—The SGT in decimal format. The range is 1 to 65533. • **trusted**—Indicates that ingress traffic on the interface with this SGT should not have its tag overwritten.
Step 6	`Router(config-if-cts-manual)# [no] propagate sgt`	(Optional) The **no** form of this command is used when the peer is incapable of processing an SGT. The **no propagate sgt** command prevents the interface from transmitting the SGT to the peer.
Step 7	`Router(config-if-cts-manual)# exit`	Exits Cisco TrustSec manual interface configuration mode.
Step 8	`Router(config-if)# shutdown`	Disables the interface.

	Command	Purpose
Step 9	`Router(config-if)# no shutdown`	Enables the interface and enables Cisco TrustSec authentication on the interface.
Step 10	`Router(config-if)# exit`	Exits interface configuration mode.

Identity Port Mapping (IPM) configures a physical port such that a single SGT is imposed on all traffic entering the port; this SGT is applied on all IP traffic exiting the port until a new binding is learned. IPM is configured as follows:

- CTS Manual interface configuration mode with the **policy static sgt** *tag* command
- CTS Manual interface configuration mode with the **policy dynamic identity** *peer-name* command where *peer-name* is designated as non-trusted in the Cisco ACS or Cisco ISE configuration.

IPM is supported for the following ports:

- Routed ports
- Switchports in access mode
- Switchports in trunk mode

When manually configuring Cisco TrustSec on an interface, consider these usage guidelines and restrictions:

- If no SAP parameters are defined, no Cisco TrustSec encapsulation or encryption will be performed.
- If the selected SAP mode allows SGT insertion and an incoming packet carries no SGT, the tagging policy is as follows:
  - If the **policy static** command is configured, the packet is tagged with the SGT configured in the **policy static** command.
  - If the **policy dynamic** command is configured, the packet is not tagged.
- If the selected SAP mode allows SGT insertion and an incoming packet carries an SGT, the tagging policy is as follows:
  - If the **policy static** command is configured without the **trusted** keyword, the SGT is replaced with the SGT configured in the **policy static** command.
  - If the **policy static** command is configured with the **trusted** keyword, no change is made to the SGT.
  - If the **policy dynamic** command is configured and the authorization policy downloaded from the authentication server indicates that the packet source is untrusted, the SGT is replaced with the SGT specified by the downloaded policy.
  - If the **policy dynamic** command is configured and the downloaded policy indicates that the packet source is trusted, no change is made to the SGT.

Configuration Examples for Manual Mode and MACsec on an Uplink Port

Catalyst 6500 TrustSec interface configuration in manual mode:

```
Router# configure terminal
Router(config)# interface gi 2/1
Router(config-if)# cts manual
Router(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm null no-encap
Router(config-if-cts-manual)# policy static sgt 111
Router(config-if-cts-manual)# exit
```

```
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# end
```

Catalyst 3850 TrustSec interface configuration in manual mode:

```
Switch# configure terminal
Switch(config)# interface gig 1/0/5
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# policy dynamic identity my_cisco_ise_id
Switch(config-if-cts-manual)# exit
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
Router(config-if)# end
```

Regenerating SAP Key on an Interface

The ability to manually refresh encryption keys is often part of network administration security requirements. SAP key refresh ordinarily occurs automatically, triggered by combinations of network events and non-configurable internal timers.

Detailed Steps for Catalyst 6500, Catalyst 3850/3650

	Command	Purpose
Step 1	**cts rekey interface** interface_type *slot/port* **Example:** c6500switch# **cts rekey int gig 1/1**	Forces renegotiation of SAP keys on MACsec link.

Verifying the Cisco TrustSec Interface Configuration

To view the TrustSec-relate interface configuration, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	**show cts interface** [**interface_type** *slot/port* | **brief** | **summary**] **Example:** c6500switch# **show cts interface brief**	Displays TrustSec-related interface configuration.

Example: Show Cisco 6500 TrustSec interface configuration:

```
Router# show cts interface interface gi3/3

Global Dot1x feature is Enabled
Interface GigabitEthernet3/3:
    CTS is enabled, mode:    DOT1X
    IFC state:               OPEN
    Authentication Status:   SUCCEEDED
```

```
        Peer identity:       "sanjose"
        Peer's advertised capabilities: ""
        802.1X role:         Supplicant
        Reauth period applied to link:  Not applicable to Supplicant role
    Authorization Status:    SUCCEEDED
        Peer SGT:            11
        Peer SGT assignment: Trusted
    SAP Status:              NOT APPLICABLE
        Configured pairwise ciphers:
            gcm-encrypt
            null

        Replay protection:      enabled
        Replay protection mode: OUT-OF-ORDER

        Selected cipher:

    Cache Info:
        Expiration            : 23:32:40 PDT Jun 22 2009
        Cache applied to link : NONE
        Expiration            : 23:32:40 PDT Jun 22 2009

    Statistics:
        authc success:              1
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                0
        sap fail:                   0
        authz success:              1
        authz fail:                 0
        port auth fail:             0

Dot1x Info for GigabitEthernet3/1
-----------------------------------
PAE                       = SUPPLICANT
StartPeriod               = 30
AuthPeriod                = 30
HeldPeriod                = 60
MaxStart                  = 3
Credentials profile       = CTS-ID-profile
EAP profile               = CTS-EAP-profile
Dot1x Info for GigabitEthernet3/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = FORCE_AUTHORIZED
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 55
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

Example: Cisco 3850 TrustSec interface query:

```
Edison24U> show cts interface gig 1/0/6
Global Dot1x feature is Disabled
Interface GigabitEthernet1/0/6:
    CTS is enabled, mode:    MANUAL
    IFC state:               INIT
    Authentication Status:   NOT APPLICABLE
```

```
    Peer identity:       "unknown"
    Peer's advertised capabilities: ""
Authorization Status:    NOT APPLICABLE
SAP Status:              NOT APPLICABLE
Propagate SGT:           Enabled
Cache Info:
    Expiration            : N/A
    Cache applied to link : NONE

Statistics:
    authc success:              0
    authc reject:               0
    authc failure:              0
    authc no response:          0
    authc logoff:               0
    sap success:                0
    sap fail:                   0
    authz success:              0
    authz fail:                 0
    port auth fail:             0

L3 IPM:   disabled.
```

Manually Configuring a Device SGT

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:

Detailed Steps for Catalyst 6500, 3850, 3750-X

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# cts sgt` *tag*	Configures the SGT for packets sent from the device. The *tag* argument is in decimal format. The range is 1 to 65533.
Step 3	`Switch(config)# exit`	Exits configuration mode.

Configuration Examples for Manually Configuring a Device SGT

Catalyst 6500, Catalyst 3850, and Catalyst 3750-X:

```
Switch# configure terminal
Switch(config)# cts sgt 1234
Switch(config)# exit
```

Manually Configuring IP-Address-to-SGT Mapping

This section discusses SGTs to source IP address mapping as follows:

For Identity Port Mapping in cts interface manual mode, see the following section:

Subnet to SGT Mapping

Subnet to SGT mapping binds an SGT to all host addresses of a specified subnet. 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, SXPv3, 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 198.1.1.0/29 is expanded as follows (only 3 bits for host addresses):

- Host addresses 198.1.1.1 to 198.1.1.7–tagged and propagated to SXP peer.
- Network and broadcast addresses 198.1.1.0 and 198.1.1.8— 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 TrustSec links.

For IPv6 networks, SXPv3 cannot export subnet bindings to SXPv2 or SXPv1 peers.

Default Settings

There are no default settings for this feature.

Configuring Subnet to SGT Mapping

This section includes the following topics:

Restrictions

- An IPv4 subnetwork with a /31 prefix cannot be expanded.
- Subnet host addresses cannot be bound to 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 SXP speaker and listener are running SXPv3, or more recent versions.

Detailed Steps for Catalyst 6500

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **cts sxp mapping network-map** *bindings* **Example:** `switch(config)# cts sxp mapping network-map 10000`	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. • *bindings*—(0 to 65,535) default is 0 (no expansions performed)
Step 3	[**no**] **cts role-based sgt-map** *ipv4_address/prefix* **sgt** *number* **Example:** `switch(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 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. • *ipv4_address*—Specifies the IPv4 network address in dotted decimal notation. • *prefix*—(0 to 30). Specifies the number of bits in the network address. • **sgt** *number* (0–65,535). Specifies the Security Group Tag (SGT) number.

	Command	Purpose
Step 4	[**no**] **cts role-based sgt-map** *ipv6_address::prefix* **sgt** *number* **Example:** switch(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 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. • *ipv6_address*—Specifies IPv6 network address in colon hexadecimal notation. • *prefix*—(0 to128). Specifies the number of bits in the network address. • **sgt** *number*—(0 to 65,535). Specifies the Security Group Tag (SGT) number.
Step 5	**exit** **Example:** switch(config)# exit switch#	Exits global configuration mode.
Step 6	**show running-config** | include *search_string* **Example:** switch# show running-config | include sgt 1234 switch# show running-config | include network-map	Verifies that the **cts role-based sgt-map** and the **cts sxp mapping network-map** commands are in the running configuration.
Step 7	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Verifying Subnet to SGT Mapping Configuration

To display Subnet to SGT Mapping configuration information, perform one of the following tasks:

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.

For detailed information about the fields in the output from these commands, refer to Chapter 7, "Cisco TrustSec Command Summary."

Configuration Examples for Subnet to SGT Mapping

The following example shows how to configure IPv4 Subnet to SGT Mapping between two Catalyst 6500 series switches running SXPv3 (Switch1 and Switch2):

Step 1 Configure SXP speaker/listener peering between Switch1 (1.1.1.1) and Switch 2 (2.2.2.2).

```
Switch1# config t
Switch1(config)# cts sxp enable
Switch1(config)# cts sxp default source-ip 1.1.1.1
Switch1(config)# cts sxp default password 1syzygy1
Switch1(config)# cts sxp connection peer 2.2.2.2 password default mode local speaker
```

Step 2 Configure Switch 2 as SXP listener of Switch1.

```
Switch2(config)# cts sxp enable
Switch2(config)# cts sxp default source-ip 2.2.2.2
Switch2(config)# cts sxp default password 1syzygy1
Switch2(config)# cts sxp connection peer 1.1.1.1 password default mode local listener
```

Step 3 On Switch2, verify that the SXP connection is operating:

```
Switch2# 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)
```

Step 4 Configure the subnetworks to be expanded on Switch1.

```
Switch1(config)# cts sxp mapping network-map 10000
Switch1(config)# cts role-based sgt-map 10.10.10.0/30 sgt 101
Switch1(config)# cts role-based sgt-map 11.11.11.0/29 sgt 11111
Switch1(config)# cts role-based sgt-map 192.168.1.0/28 sgt 65000
```

Step 5 On Switch2, verify the subnet to SGT expansion from Switch1. 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.

```
Switch2# 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>
```

Step 6 Verify the expansion count on Switch1:

```
Switch1# show cts sxp sgt-map

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

Step 7 Save the configurations on Switch 1 and Switch 2 and exit global configuration mode.

```
Switch1(config)# copy running-config startup-config
Switch1(config)# exit
Switch2(config)# copy running-config startup-config
Switch2(config)# exit
```

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 TrustSec-capable networks as follows:

- Supports devices that are not 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 TrustSec-capable switch, and IP Device Tracking is enabled on that switch, then 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 a **cts role-based l2-vrf** cts global configuration 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 on page 3-22.

Default Settings

There are no default settings.

Configuring VLAN to SGT Mapping

This section includes the following topics:

- Task Flow for Configuring VLAN-SGT Mapping, page 3-17

Task Flow for Configuring VLAN-SGT Mapping

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

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	**config t** **Example:** TS_switchswitch# config t TS_switchswitch(config)#	Enters global configuration mode.
Step 2	**vlan** ***vlan_id*** **Example:** TS_switch(config)# vlan 100 TS_switch(config-vlan)#	Creates VLAN 100 on the TrustSec-capable gateway switch and enters VLAN configuration submode.
Step 3	[**no**] **shutdown** **Example:** TS_switch(config-vlan)# **no shutdown**	Provisions VLAN 100.
Step 4	**exit** **Example:** TS_switch(config-vlan)# exit TS_switch(config)#	Exits VLAN configuration mode into Global Configuration mode.
Step 5	**interface** type *slot/port* **Example:** TS_switch(config)# interface vlan 100 TS_switch(config-if)#	Enters interface configuration mode.
Step 6	**ip address** *slot/port* **Example:** TS_switch(config-if)# ip address 10.1.1.2 255.0.0.0	Configures Switched Virtual Interface (SVI) for VLAN 100.

	Command	Purpose
Step 7	[**no**] **shutdown** **Example:** TS_switch(config-if)# **no shutdown**	Enables the SVI.
Step 8	**exit** **Example:** TS_switch(config-if)# exit TS_switch(config)#	Exits VLAN Interface Configuration mode into Global Configuration mode.
Step 9	**cts role-based sgt-map vlan-list** *vlan_id* **sgt** *sgt_number* **Example:** TS_switch(config)# cts role-based sgt-map vlan-list 100 sgt 10	Assigns the specified SGT to the specified VLAN.
Step 10	**ip device tracking probe** [**count** *count* | **delay** *seconds* | **interval** *length*] **Example:** TS-switch(config)# **ip device tracking**	Enables IP device tracking. When active hosts are detected, the switch 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 switch 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 11	**exit** **Example:** TS_switch(config)# exit TS_switch#	Exits Global configuration mode.
Step 12	**show cts role-based sgt-map** {*ipv4_netaddr* | *ipv4_netaddr/prefix* | *ipv6_netaddr*| *ipv6_netaddr/prefix* | **all** [**ipv4** | **ipv6**] | host {*ipv4__addr* | *ipv6_addr*} | **summary** [**ipv4** | **ipv6**] **Example:** TS_switch# cts role-based sgt-map all	(Optional) Displays the VLAN to SGT mappings.

	Command	Purpose
Step 13	**show ip device tracking {all|interface|ip|mac}** **Example:** TS_switch# show ip device tracking all	(Optional) Verifies the operational status of IP Device tracking.
Step 14	**copy running-config startup-config** **Example:** TS_switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Verifying VLAN to SGT Mapping

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

Command	Purpose
show ip device tracking	Displays the status of IP Device Tracking which identifies the IP addresses of active hosts on a VLAN.
show cts role-based sgt-map	Displays IP address to SGT bindings.

For detailed information about the fields in the output from these commands, refer to Chapter 7, "Cisco TrustSec Command Summary," or the "Cisco IOS 15.0SY Security and VPN Command Reference."

Configuration Example 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 switch. The access switch has an access mode link to a Catalyst 6500 series TrustSec software-capable switch. A switched virtual interface on the TrustSec switch is the default gateway for the VLAN 100 endpoint (IP Address 10.1.1.1). The TrustSec switch imposes Security Group Tag (SGT) 10 on packets from VLAN 100.

Step 1 Create VLAN 100 on an access switch.

```
access_switch# config t
access_switch(config)# vlan 100
access_switch(config-vlan)# no shutdown
access_switch(config-vlan)# exit
access_switch(config)#
```

Step 2 Configure the interface to the TrustSec switch as an access link. Configurations for the endpoint access port are omitted in this example.

```
access_switch(config)# interface gigabitEthernet 6/3
access_switch(config-if)# switchport
access_switch(config-if)# switchport mode access
access_switch(config-if)# switchport access vlan 100
```

Step 3 Create VLAN 100 on the TrustSec switch.

```
TS_switch(config)# vlan 100
TS_switch(config-vlan)# no shutdown
TS_switch(config-vlan)# end
TS_switch#
```

Step 4 Create an SVI as the gateway for incoming VLAN 100.

```
TS_switch(config)# interface vlan 100
TS_switch(config-if)# ip address 10.1.1.2 255.0.0.0
TS_switch(config-if)# no shutdown
TS_switch(config-if)# end
TS_switch(config)#
```

Step 5 Assign Security Group Tag (SGT) 10 to hosts on VLAN 100.

```
TS_switch(config)# cts role-based sgt-map vlan 100 sgt 10
```

Step 6 Enable IP Device Tracking on the TrustSec switch. Verify that it is operating.

```
TS_switch(config)# ip device tracking
TS_switch# 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
```

Step 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_switch# 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
```

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)
- Layer3 subinterface of a Layer2 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 on page 3-22.

Feature History for L3IF-SGT Mapping

Default Settings

There are no default settings.

Configuring L3IF to SGT Mapping

Detailed steps Catalyst 6500

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.

Step 2	`Router(config)# cts role-based sgt-map interface` type *slot/port* `[security-group` *name* `|` `sgt` *number*`]`
	
	`Router(config)# cts role-based sgt-map interface gigabitEthernet 1/1 sgt 77`
		An SGT is imposed on ingress traffic to the specified interface.
		• **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 3	`Router(config)# exit`	Exits configuration mode.
Step 4	`Router# show cts role-based sgt-map all`	Verify that ingressing traffic is tagged with the specified SGT.

Verifying L3IF to SGT Mapping

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

Command	Purpose
show cts role-based sgt-map all	Displays all IP address to SGT bindings.

Configuration Example for L3IF to SGT Mapping on an Ingress Port

In the following example a Layer 3 interface of a Catalyst 6500 series switch linecard is configured to tag all ingressing traffic with SGT 3. Prefixes of attached subnets are already known.

Step 1 Configure the interface.

```
Switch# config t
Switch(config)# interface gigabitEthernet 6/3 sgt 3
Switch(config)# exit
```

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

```
Router# 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

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of L3IF     bindings = 7
Total number of INTERNAL bindings = 7
Total number of active   bindings = 15
```

Binding Source Priorities

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*} CTS 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.

Configuring Additional Authentication Server-Related Parameters

To configure the interaction between a switch and the Cisco TrustSec server, perform one or more of these tasks:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# [no] cts server deadtime seconds`	(Optional) Specifies how long a server in the group should not be selected for service once it has been marked as dead. The default is 20 seconds; the range is 1 to 864000.
Step 3	`Router(config)# [no] cts server load-balance method least-outstanding [batch-size transactions] [ignore-preferred-server]`	(Optional) Enables RADIUS load balancing for the Cisco TrustSec private server group and chooses the server with the least outstanding transactions. By default, no load balancing is applied. The default *transactions* is 25. The **ignore-preferred-server** keyword instructs the switch not to try to use the same server throughout a session.
Step 4	`Router(config)# [no] cts server test {server-IP-address | all} {deadtime seconds | enable | idle-time seconds}`	(Optional) Configures the server-liveliness test for a specified server or for all servers on the dynamic server list. By default, the test is enabled for all servers. The default **idle-time** is 60 seconds; the range is from 1 to 14400.
Step 5	`Router(config)# exit`	Exits configuration mode.
Step 6	`Router# show cts server-list`	Displays status and configuration details of a list of Cisco TrustSec servers.

This example shows how to configure server settings and how to display the Cisco TrustSec server list:

```
Router# configure terminal
Router(config)# cts server load-balance method least-outstanding batch-size 50
ignore-preferred-server
Router(config)# cts server test all deadtime 20
Router(config)# cts server test all enable
Router(config)# cts server test 10.15.20.102 idle-time 120
Router(config)# exit

Router# show cts server-list
CTS Server Radius Load Balance = ENABLED
  Method     = least-outstanding
```

```
  Batch size = 50
  Ignore preferred server
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Preferred list, 1 server(s):
 *Server: 10.15.20.102, port 1812, A-ID  87B3503255C4384485BB808DC24C6F55
               Status = ALIVE
               auto-test = TRUE, idle-time = 120 mins, deadtime = 20 secs
Installed list: SL1-1E6E6AE57D4E2A9B320D1844C68BA291, 3 server(s):
 *Server: 10.15.20.102, port 1812, A-ID  87B3503255C4384485BB808DC24C6F55
               Status = ALIVE
               auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.15.20.101, port 1812, A-ID 255C438487B3503485BBC6F55808DC24
               Status = ALIVE
               auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
Installed list: SL2-1E6E6AE57D4E2A9B320D1844C68BA293, 3 server(s):
 *Server: 10.0.0.1, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
               Status = ALIVE
               auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.0.0.2, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
               Status = DEAD
               auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
```

Automatically Configuring a New or Replacement Password with the Authentication Server

As an alternative to manually configuring the password between the switch and the authentication server, you can initiate a password negotiation from the switch. To configure the password negotiation, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router#` **`cts change-password server`** *`ip-address port`* {**`key`** *`secret`* | **`a-id`** *`a-id`*}	Initiates a password negotiation between the switch and the authentication server. • *ip-address*—The IP address of the authentication server. • *port*—The UDP port of the authentication server. • **key** *secret*—The RADIUS shared secret of the authentication server. • **a-id** *a-id*—The A-ID associated with the authentication server.