# Configuring Identities, Connections, and SGTs



# Configuring Identities and Connections

This module describes the following features:

- Configuring Credentials and AAA for a Cisco TrustSec Seed Device
- Configuring Credentials and AAA for a Cisco TrustSec Non-Seed Device
- Cisco TrustSec Authentication and MACsec in 802.1X Mode on an Uplink Port
- Cisco TrustSec and MACsec in Manual Mode on an Uplink Port
- Regenerating SAP Key on an Interface

## How to Configure Identities and Connections

### 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.

**Note**

- You must also configure the Cisco TrustSec credentials for the device on the Cisco Identity Services Engine (Cisco ISE) or the Cisco Secure Access Control Server (Cisco ACS).
- The **cts authorization list** command must be configured to download the Cisco TrustSec environment data and SGACL policy from the Cisco Identity Services Engine (ISE).

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

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **cts credentials id** *device-id* **password** *password*<br>**Example:**<br>`Device# cts credentials id Switch1 password Cisco123` | 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 haracters and is case sensitive. |
| **Step 2** | **enable**<br>**Example:**<br>`Device# enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 3** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 4** | **aaa new-model**<br>**Example:**<br>`Device(config)# aaa new-model` | Enables AAA. |
| **Step 5** | **aaa authentication dot1x default group radius**<br>**Example:**<br>`Device(config)# aaa authentication dot1x default group radius` | Specifies the 802.1X port-based authentication method as RADIUS. |
| **Step 6** | **aaa authorization network** *mlist* **group radius**<br>**Example:**<br>`Device(config)# aaa authorization network mlist group radius` | Configures the switch to use RADIUS authorization for all network-related service requests.<br>• *mlist*—The Cisco TrustSec AAA server group. |
| **Step 7** | **cts authorization list** *mlist*<br>**Example:**<br>`Device(config)# cts authorization list mlist` | Specifies a Cisco TrustSec AAA server group. Non-seed devices will obtain the server list from the authenticator. |
| **Step 8** | **aaa accounting dot1x default start-stop group radius**<br>**Example:**<br>`Device(config)# aaa accounting dot1x default start-stop group radius` | Enables 802.1X accounting using RADIUS. |
| **Step 9** | **radius-server host** *ip-addr* **auth-port 1812 acct-port 1813 pac key** *secret*<br>**Example:** | Specifies the RADIUS authentication server host address, service ports, and encryption key. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key AbCe1234` | • *ip-addr*—The IP address of the authentication server.<br>• *secret*—The encryption key shared with the authentication server. |
| **Step 10** | **radius-server vsa send authentication**<br>**Example:**<br>`Device(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 11** | **dot1x system-auth-control**<br>**Example:**<br>`Device(config)# dot1x system-auth-control` | Globally enables 802.1X port-based authentication. |
| **Step 12** | **exit**<br>**Example:**<br>`Device(config)# exit` | Exits configuration mode. |

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

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

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

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **cts credentials id** *device-id* **password** *password*<br>**Example:**<br>`Device# 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** | **enable**<br>**Example:**<br>`Device# enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 3** | **configure terminal**<br>**Example:** | Enters global configuration mode.. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device# configure terminal` | |
| **Step 4** | **aaa new-model**<br>**Example:**<br>`Device(config)# aaa new-model` | Enables AAA. |
| **Step 5** | **aaa authentication dot1x default group radius**<br>**Example:**<br>`Device(config)# aaa authentication dot1x default group radius` | Specifies the 802.1X port-based authentication method as RADIUS. |
| **Step 6** | **aaa authorization network** *mlist* **group radius**<br>**Example:**<br>`Device(config)# aaa authorization network mlist group radius` | Configures the switch to use RADIUS authorization for all network-related service requests.<br>• *mlist*— Specifies a Cisco TrustSec AAA server group. |
| **Step 7** | **aaa accounting dot1x default start-stop group radius**<br>**Example:**<br>`Device(config)# aaa accounting dot1x default start-stop group radius` | Enables 802.1X accounting using RADIUS. |
| **Step 8** | **radius-server vsa send authentication**<br>**Example:**<br>`Device(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 9** | **dot1x system-auth-control**<br>**Example:**<br>`Device(config)# dot1x system-auth-control` | Globally enables 802.1X port-based authentication. |
| **Step 10** | **exit**<br>**Example:**<br>`Device(config)# exit` | Exits configuration mode. |

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

**Note** Cisco Catalyst 9400 Series Switches do not support MACsec.

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.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device# enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type slot/port*<br>**Example:**<br>`Device(config)# interface gi 2/1` | Enters interface configuration mode for the uplink interface. |
| **Step 4** | **cts manual**<br>**Example:**<br>`Device(config-if)# cts manual` | Enters Cisco TrustSec manual configuration mode. |
| **Step 5** | [**no**] **sap pmk** *key* [**mode-list** *mode1* [*mode2* [*mode3* [*mode4*]]]]<br>**Example:**<br>`Device(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm null no-encap` | (Optional) Configures the SAP pairwise master key PMK) and operation mode. SAP is disabled by default in Cisco TrustSec manual mode.<br>• *key*—A hexadecimal value with an even number of characters and a maximum length of 32 characters.<br>The SAP operation mode options are:<br>• **gcm**— Authentication and encryption<br>• **gmac**— Authentication, no encryption<br>• **no-encap**— No encapsulation<br>• **null**— Encapsulation, no authentication, no encryption<br>**Note** MACsec with SAP is not supported on the Catalyst 3K switches.<br>**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. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | [**no**] **policy dynamic identity** *peer-name*<br>**Example:**<br>`Device(config-if-cts-manual)# policy dynamic identity my_cisco_ise_id` | (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.<br>• *peer-name*—The Cisco TrustSec device ID for the peer device. The peer name is case sensitive.<br>**Note** Ensure that you have configured the Cisco TrustSec credentials (see Configuring Credentials and AAA for a Cisco TrustSec Seed Device, on page 1) |
| **Step 7** | [**no**] **policy static sgt** *tag* **[trusted]**<br>**Example:**<br>`Device(config-if-cts-manual)# policy static sgt 111` | (Optional) Configures a static authorization policy. See the additional usage notes following this task.<br>• *tag*—The SGT in decimal format. The range is 1 to 65533.<br>• **trusted**—Indicates that ingress traffic on the interface with this SGT should not have its tag overwritten. |
| **Step 8** | **[no] propagate sgt**<br>**Example:**<br>`Device(config-if-cts-manual)# 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 9** | **exit**<br>**Example:**<br>`Device(config-if-cts-manual)# exit` | Exits Cisco TrustSec manual interface configuration mode. |
| **Step 10** | **shutdown**<br>**Example:**<br>`Device(config-if)# shutdown` | Disables the interface. |
| **Step 11** | **no shutdown**<br>**Example:**<br>`Device(config-if)# no shutdown` | Enables the interface and enables Cisco TrustSec authentication on the interface. |
| **Step 12** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |

**Example**

## 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.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **cts rekey interface** *type slot/port*<br>**Example:**<br>`Device# cts rekey int gig 1/1` | Forces renegotiation of SAP keys on MACsec link. |

## 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:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device# enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **cts server deadtime** *seconds*<br>**Example:**<br>`Device(config)# cts server deadtime 20` | (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 4** | **cts server load-balance method least-outstanding** [**batch-size** *transactions* ] [**ignore-preferred-server** ]<br>**Example:**<br>`Device(config)# cts server load-balance method least-outstanding batch-size 50 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.<br>The **ignore-preferred-server** keyword instructs the switch not to try to use the same server throughout a session. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **cts server test** {*server-IP-address* \| **all**} {**deadtime** *seconds* \| **enable** \| **idle-time** *seconds* }<br>**Example:**<br>`Device(config)# cts server test 10.15.20.102 idle-time 120` | (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 6** | **exit**<br>**Example:**<br>`Device(config)# exit` | Exits configuration mode. |
| **Step 7** | **show cts server-list**<br>**Example:**<br>`Device# show cts server-list` | Displays status and configuration details of a list of Cisco TrustSec servers. |

# Configuration Examples for Identities and Connections

## Example: Configuration for Non-Seed Device

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
```

## Example: Configuration for Manual Mode and MACsec on an Uplink Port

Catalyst 3650 and 3850 Cisco TrustSec interface configuration in manual mode:

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

## Example: 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:

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

```
Device# configure terminal
Device(config)# cts server load-balance method least-outstanding batch-size 50
ignore-preferred-server
Device(config)# cts server test all deadtime 20
Device(config)# cts server test all enable
Device(config)# exit
Device#show cts server-list
CTS Server Radius Load Balance = ENABLED
    Method   = least-outstandin
    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 sec
```

## Verifying the Cisco TrustSec Interface Configuration

To view the Cisco TrustSec-related interface configuration, use the **show cts interface**

Cisco 3850 TrustSec interface query:

```
Device> show cts interface gigabitethernet 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.
```

# Feature Information for Identities, Connections, and SGTs

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 the 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 1: Feature Information for Identities, Connections, and SGTs***

| Feature Name | Release | Feature Information |
|---|---|---|
| Identities, Connections, and SGTs | Cisco IOS XE Denali 16.1.1 | This feature was introduced. |