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

This section describes 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 device 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* **Example:** `Device# cts credentials id device1 password Cisco123`	Specifies the Cisco TrustSec device ID and password for this device 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** **Example:** `Device# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 3	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 4	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 5	**aaa authentication dot1x default group radius** **Example:** `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** **Example:** `Device(config)# aaa authorization network mlist group radius`	Configures the device to use RADIUS authorization for all network-related service requests. • *mlist*—The Cisco TrustSec AAA server group.
Step 7	**cts authorization list** *mlist* **Example:** `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** **Example:** `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* **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. • *secret*—The encryption key shared with the authentication server.
Step 10	**radius-server vsa send authentication** **Example:** `Device(config)# radius-server vsa send authentication`	Configures the device to recognize and use vendor-specific attributes (VSAs) in RADIUS Access-Requests generated by the device during the authentication phase.
Step 11	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Globally enables 802.1X port-based authentication.
Step 12	**exit** **Example:** `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 device on the Cisco Identity Services Engine, or the Cisco Secure ACS.

To enable NDAC and AAA on a non-seed device 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* **Example:** `Device# cts credentials id device-id password password`	Specifies the Cisco TrustSec device ID and password for this device 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** **Example:** `Device# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 3	**configure terminal** **Example:**	Enters global configuration mode..

	Command or Action	Purpose
	`Device# configure terminal`	
Step 4	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 5	**aaa authentication dot1x default group radius** **Example:** `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** **Example:** `Device(config)# aaa authorization network mlist group radius`	Configures the device to use RADIUS authorization for all network-related service requests. • *mlist*— Specifies a Cisco TrustSec AAA server group.
Step 7	**aaa accounting dot1x default start-stop group radius** **Example:** `Device(config)# aaa accounting dot1x default start-stop group radius`	Enables 802.1X accounting using RADIUS.
Step 8	**radius-server vsa send authentication** **Example:** `Device(config)# radius-server vsa send authentication`	Configures the device to recognize and use vendor-specific attributes (VSAs) in RADIUS Access-Requests generated by the device during the authentication phase.
Step 9	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Globally enables 802.1X port-based authentication.
Step 10	**exit** **Example:** `Device(config)# exit`	Exits configuration mode.

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* **Example:** `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 device and the Cisco TrustSec server, perform one or more of these tasks:

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 server deadtime** *seconds* **Example:** `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**] **Example:** `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. The **ignore-preferred-server** keyword instructs the device not to try to use the same server throughout a session.
Step 5	**cts server test** {*server-IP-address* | **all**} {**deadtime** *seconds* | **enable** | **idle-time** *seconds* } **Example:** `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** **Example:** `Device(config)# exit`	Exits configuration mode.

	Command or Action	Purpose
Step 7	**show cts server-list** **Example:** `Device# show cts server-list`	Displays status and configuration details of a list of Cisco TrustSec servers.

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**

```
Device# show cts interface gigabitethernet 1/1/1

Global Dot1x feature is Disabled
```

```
Interface GigabitEthernet1/1/1:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Interface Active for 00:54:01.936
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: "sap"
    Authorization Status:    SUCCEEDED
        Peer SGT:            18
        Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
        Version:             2
        Configured pairwise ciphers:
            gcm-encrypt

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

    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:                3
        sap fail:                   0
        authz success:              4
        authz fail:                 0
        port auth fail:             0

    L3 IPM:   disabled.
```

Feature History for Identities, Connections, and SGTs

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Fuji 16.9.2	Identities, Connections, and SGTs	A Cisco TrustSec-capable device that is directly connected to the authentication server, or indirectly connected but is the first device to begin the Cisco TrustSec domain, is called the seed device. Other Cisco TrustSec network devices are non-seed devices.

Use 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.