Cisco TrustSec Network Device Admission Control

The Cisco TrustSec Network Device Admission Control (NDAC) feature creates an independent layer of trust between Cisco TrustSec devices to prohibit rogue devices from being allowed on the network.

- Information About Cisco TrustSec Network Device Admission Control, page 1
- How to Configure Cisco TrustSec Network Device Admission Control, page 1
- Configuration Examples for Cisco TrustSec Network Device Admission Control, page 8
- Additional References, page 9
- Feature Information for Cisco TrustSec Network Device Admission Control, page 10

Information About Cisco TrustSec Network Device Admission Control

Cisco TrustSec NDAC Authentication for an Uplink Interface

Cisco TrustSec NDAC authentication with 802.1X must be enabled on each uplink interface that connects to another Cisco TrustSec device.

How to Configure Cisco TrustSec Network Device Admission Control

Configuring AAA for Cisco TrustSec NDAC Devices

Configure authentication, authorization, and accounting (AAA) on both seed and non-seed Network Device Admission Control (NDAC) devices.

Configuring AAA on Cisco TrustSec Seed Devices

SUMMARY STEPS

1. **enable**
2. **cts credentials id** *cts-id* **password** *cts-password*
3. **configure terminal**
4. **aaa new-model**
5. **aaa session-id common**
6. **radius server** *radius-server-name*
7. **address ipv4** {*hostname* | *ipv4address*} [**acct-port** *port* | **alias** {*hostname* | *ipv4address*} | **auth-port** *port* [**acct-port** *port*]]
8. **pac key** *encryption-key*
9. **exit**
10. **radius-server vsa send authentication**
11. **aaa group server radius** *group-name*
12. **server name** *radius-server-name*
13. **exit**
14. **aaa authentication dot1x default group** *group-name*
15. **aaa authorization network default group** *group-name*
16. **aaa authorization network** *list-name* **group** *group-name*
17. **cts authorization list** *list-name*
18. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**cts credentials id** *cts-id* **password** *cts-password* **Example:** `Device# cts credentials id CTS-One password cisco123`	Specifies the Cisco TrustSec ID and password of the network device.
Step 3	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 4	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables new RADIUS and AAA access control commands and functions and disables old commands.
Step 5	**aaa session-id common** **Example:** `Device(config)# aaa session-id common`	Ensures that the same session identification (ID) information is used for each AAA accounting service type within a given call.
Step 6	**radius server** *radius-server-name* **Example:** `Device(config)# radius server cts-aaa-server`	Specifies the name for the RADIUS server configuration for Protected Access Credential (PAC) provisioning and enters RADIUS server configuration mode.
Step 7	**address ipv4** {*hostname* | *ipv4address*} [**acct-port** *port* | **alias** {*hostname* | *ipv4address*} | **auth-port** *port* [**acct-port** *port*]] **Example:** `Device(config-radius-server)# address ipv4 192.0.2.1 auth-port 1812 acct-port 1813`	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.
Step 8	**pac key** *encryption-key* **Example:** `Device(config-radius-server)# pac key cisco123`	Specifies the PAC encryption key.
Step 9	**exit** **Example:** `Device(config-radius-server)# exit`	Exits RADIUS server configuration mode and enters global configuration mode.
Step 10	**radius-server vsa send authentication** **Example:** `Device(config)# radius-server vsa send authentication`	Configures the network access server (NAS) to recognize and use only authentication vendor-specific attributes (VSAs).
Step 11	**aaa group server radius** *group-name* **Example:** `Device(config)# aaa group server radius cts_sg`	Groups different RADIUS server hosts into distinct lists and distinct methods and enters RADIUS group server configuration mode.
Step 12	**server name** *radius-server-name* **Example:** `Device(config-sg-radius)# server name cts-aaa-server`	Specifies a RADIUS server.

	Command or Action	Purpose
Step 13	**exit** **Example:** `Device(config-sg-radius)# exit`	Exits RADIUS group server configuration mode and enters global configuration mode.
Step 14	**aaa authentication dot1x default group** *group-name* **Example:** `Device(config)# aaa authentication dot1x default group cts_sg`	Specifies the RADIUS server to use for authentication on interfaces running IEEE 802.1X.
Step 15	**aaa authorization network default group** *group-name* **Example:** `Device(config)# aaa authorization network default group cts_sg`	Specifies that the RADIUS server method is the default method for authorization into a network.
Step 16	**aaa authorization network** *list-name* **group** *group-name* **Example:** `Device(config)# aaa authorization network cts-mlist group cts_sg`	Specifies that the RADIUS server method is part of the list of authorization methods to use for authorization into a network.
Step 17	**cts authorization list** *list-name* **Example:** `Device(config)# cts authorization list cts-mlist`	Specifies a list of AAA servers for the Cisco TrustSec seed device.
Step 18	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring AAA on Cisco TrustSec Non-seed Devices

SUMMARY STEPS

1. **enable**
2. **cts credentials id** *cts-id* **password** *cts-password*
3. **configure terminal**
4. **aaa new-model**
5. **aaa session-id common**
6. **radius-server vsa send authentication**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**cts credentials id** *cts-id* **password** *cts-password* **Example:** `Device# cts credentials id CTS-One password cisco123`	Specifies the Cisco TrustSec ID and password of the network device.
Step 3	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 4	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables new RADIUS and AAA access control commands and functions and disables old commands.
Step 5	**aaa session-id common** **Example:** `Device(config)# aaa session-id common`	Ensures that the same session identification (ID) information is used for each AAA accounting service type within a given call.
Step 6	**radius-server vsa send authentication** **Example:** `Device(config)# radius-server vsa send authentication`	Configures the network access server (NAS) to recognize and use only authentication vendor-specific attributes (VSAs).
Step 7	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Cisco TrustSec NDAC Authentication for an Uplink Interface

Before You Begin

Configure authentication, authorization, and accounting (AAA) on both seed and non-seed Network Device Admission Control (NDAC) devices. For more information, see the "Configuring AAA for Cisco TrustSec NDAC Devices" section in this chapter.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **cts dot1x**
5. **sap mode-list** {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**]
6. **timer reauthentication** *seconds*
7. [**no**] **propagate sgt**
8. **exit**
9. **no shutdown**
10. **exit**

DETAILED STEPS

	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	**interface** *type slot/port* **Example:** `Device(config)# interface gigabitEthernet 3/1`	Enters interface configuration mode for the uplink interface.
Step 4	**cts dot1x** **Example:** `Device(config-if)# cts dot1x`	Configures the uplink interface for NDAC authentication and enters CTS dot1x interface configuration mode.

	Command or Action	Purpose
Step 5	**sap mode-list** {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**] **Example:** `Device(config-if-cts-dot1x)# sap mode-list gcm`	(Optional) Configures the Security Association Protocol (SAP) authentication and encryption modes to negotiate link encryption between two interfaces. The interface negotiates with the peer for a mutually-acceptable mode. List the acceptable modes in the desired order of preference. Choices for the *mode* argument are: • **gcm-encrypt—**Specifies GMAC authentication and GCM encryption. • **gmac—**Specifies GMAC authentication only, no encryption. • **no-encap—**Specifies no encapsulation. • **null—**Specifies encapsulation present, no authentication, no encryption. **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 6	**timer reauthentication** *seconds* **Example:** `Device(config-if-cts-dot1x)# timer reauthentication 100`	(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 7	[**no**] **propagate sgt** **Example:** `Device(config-if-cts-dot1x)# no propagate sgt`	(Optional) Security Group Tag (SGT) processing propagation is enabled by default. 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 8	**exit** **Example:** `Device(config-if-cts-dot1x)# exit`	s Exits Cisco TrustSec 802.1X interface configuration mode.
Step 9	**no shutdown** **Example:** `Device(config-if)# no shutdown`	Enables the interface and enables Cisco TrustSec authentication on the interface.
Step 10	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.

Configuration Examples for Cisco TrustSec Network Device Admission Control

Example: Configuring AAA for Cisco TrustSec NAC Devices

Example: Configuring AAA on Cisco TrustSec Seed Devices

```
Device> enable
Device# cts credentials id CTS-One password cisco123
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa session-id common
Device(config)# radius server cts-aaa-server
Device(config-radius-server)# address ipv4 192.0.2.1 auth-port 1812 acct-port 1813
Device(config-radius-server)# pac key cisco123
Device(config-radius-server)# exit
Device(config)# radius-server vsa send authentication
Device(config)# aaa group server radius cts_sg
Device(config-sg-radius)# server name cts-aaa-server
Device(config-sg-radius)# exit
Device(config)# aaa authentication dot1x default group cts_sg
Device(config)# aaa authorization network default group cts_sg
Device(config)# aaa authorization network cts-mlist group cts_sg
Device(config)# cts authorization list cts-mlist
Device(config)# exit
```

Example: Configuring AAA on Cisco TrustSec Non-seed Devices

```
Device> enable
Device# cts credentials id CTS-One password cisco123
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa session-id common
Device(config)# radius-server vsa send authentication
Device(config)# exit
```

Example: Configuring Cisco TrustSec NDAC Authentication for an Uplink Interface

This example shows how to enable 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:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 3/1
Device(config-if)# cts dot1x
Device(config-if-cts-dot1x)# sap mode-list gcm null no-encap
Device(config-if-cts-dot1x)# timer reauthentication 43200
Device(config-if-cts-dot1x)# exit
Device(config-if)# no shutdown
Device(config-if)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands	• Cisco IOS Security Command Reference Commands A to C • Cisco IOS Security Command Reference Commands D to L • Cisco IOS Security Command Reference Commands M to R • Cisco IOS Security Command Reference Commands S to Z
Cisco TrustSec and SXP configuration	Cisco TrustSec Switch Configuration Guide
IPsec configuration	Configuring Security for VPNs with IPsec
IKEv2 configuration	Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site
Cisco Secure Access Control Server	Configuration Guide for the Cisco Secure ACS

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco TrustSec Network Device Admission Control

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 1: Feature Information for Cisco TrustSec Network Device Admission Control

Feature Name	Releases	Feature Information
Cisco TrustSec Network Device Admission Control	Cisco IOS XE Release 3.7E	The Cisco TrustSec Network Device Admission Control (NDAC) feature creates an independent layer of trust between Cisco TrustSec devices to prohibit rogue devices from being allowed on the network. The following commands were introduced or modified: **cts dot1x**, **propagate sgt (config-if-cts-dot1x)** , **sap mode-list**, **timer reauthentication**.