



## **Cisco TrustSec Configuration Guide, Cisco IOS Release 15E**

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

#### Enabling Bidirectional SXP Support 1

- Finding Feature Information 1
- Prerequisites for Bidirectional SXP Support 1
- Restrictions for Bidirectional SXP Support 2
- Information About Bidirectional SXP Support 2
  - Bidirectional SXP Support Overview 2
- How to Enable Bidirectional SXP Support 3
  - Configuring Bidirectional SXP Support 3
  - Verifying Bidirectional SXP Support Configuration 5
- Configuration Examples for Bidirectional SXP Support 6
  - Example: Configuring Bidirectional SXP Support 6
- Additional References for Bidirectional SXP Support 7
- Feature Information for Bidirectional SXP Support 8

---

### CHAPTER 2

#### Enablement of Security Group ACL at Interface Level 11

- Finding Feature Information 11
- Restrictions for Enablement of Security Group ACL at Interface Level 12
- Information About Enablement of Security Group ACL at Interface Level 12
  - Security Group ACL Overview 12
  - Guidelines to Configure Security Group ACL 13
- How to Configure Security Group ACL at Interface Level 13
  - Configuring Security Group ACL at Interface Level 13
- Configuration Examples for Enablement of Security Group ACL at Interface Level 14
  - Example: Configuring Security Group ACL at Interface Level 14
  - Example: Verifying Security Group ACL at Interface Level 14
- Additional References for Enablement of Security Group ACL at Interface Level 15
- Feature Information for Enablement of Security Group ACL at Interface Level 16

---

**CHAPTER 3****IPv6 Support for SGT and SGACL 17**

- Finding Feature Information 17
- Restrictions for IPv6 Support for SGT and SGACL 17
- Information About IPv6 Support for SGT and SGACL 18
  - Components of IPv6 Dynamic Learning 18
- How to Configure IPv6 Support for SGT and SGACL 18
  - Generating IPv6 Addresses for IP-SGT Bindings 18
  - Configuring IPv6 IP-SGT Binding Using Local Binding 21
  - Configuring IPv6 IP-SGT Binding Using a VLAN 23
  - Verifying IPv6 Support for SGT and SGACL 25
- Configuration Examples for IPv6 Support for SGT and SGACL 26
  - Example: Generating IPv6 Addresses for IP-SGT Bindings 26
  - Example: Configuring IPv6 IP-SGT Binding Using Local Binding 26
  - Example: Configuring IPv6 IP-SGT Binding Using a VLAN 27
- Additional References for IPv6 Support for SGT and SGACL 27
- Feature Information for IPv6 Support for SGT and SGACL 28

---

**CHAPTER 4****Cisco TrustSec Network Device Admission Control 31**

- Information About Cisco TrustSec Network Device Admission Control 31
  - Cisco TrustSec NDAC Authentication for an Uplink Interface 31
- How to Configure Cisco TrustSec Network Device Admission Control 32
  - Configuring AAA for Cisco TrustSec NDAC Devices 32
    - Configuring AAA on Cisco TrustSec Seed Devices 32
    - Configuring AAA on Cisco TrustSec Non-seed Devices 35
- Configuration Examples for Cisco TrustSec Network Device Admission Control 36
  - Example: Configuring AAA for Cisco TrustSec NAC Devices 36
- Additional References 37
- Feature Information for Cisco TrustSec Network Device Admission Control 38

---

**CHAPTER 5****Cisco TrustSec Critical Authentication 39**

- Finding Feature Information 39
- Prerequisites for Cisco TrustSec Critical Authentication 39
- Restrictions for Cisco TrustSec Critical Authentication 40
- Information About Cisco TrustSec Critical Authentication 40

Critical Authentication Overview	40
How to Configure Cisco TrustSec Critical Authentication	42
Configuring Critical Authentication	42
Troubleshooting Tips	44
Verifying Critical Authentication	44
Configuration Examples for Cisco TrustSec Critical Authentication	45
Example: Configuring Critical Authentication	45
Additional References for Cisco TrustSec Critical Authentication	46
Feature Information for Cisco TrustSec Critical Authentication	47





## CHAPTER

# 1

## Enabling Bidirectional SXP Support

---

The Bidirectional SXP Support feature enhances the functionality of Cisco TrustSec with SXP version 4 by adding support for Security Group Tag (SGT) Exchange Protocol (SXP) bindings that can be propagated in both directions between a speaker and a listener over a single connection.

- [Finding Feature Information, page 1](#)
- [Prerequisites for Bidirectional SXP Support, page 1](#)
- [Restrictions for Bidirectional SXP Support, page 2](#)
- [Information About Bidirectional SXP Support, page 2](#)
- [How to Enable Bidirectional SXP Support, page 3](#)
- [Configuration Examples for Bidirectional SXP Support, page 6](#)
- [Additional References for Bidirectional SXP Support, page 7](#)
- [Feature Information for Bidirectional SXP Support, page 8](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

### Prerequisites for Bidirectional SXP Support

- Ensure that Cisco TrustSec is configured on the device. For more information, see the “Cisco TrustSec Support for IOS” chapter in the *Cisco TrustSec Configuration Guide*.

## Restrictions for Bidirectional SXP Support

- The peers at each end of the connection must be configured as a bidirectional connection using the **both** keyword. It is a wrong configuration to have one end configured as a bidirectional connection using the **both** keyword and the other end configured as a speaker or listener (unidirectional connection).

## Information About Bidirectional SXP Support

### Bidirectional SXP Support Overview

Cisco TrustSec builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. The peer that produces data is the speaker and the corresponding peer is the listener.

With the support for bidirectional Security Group Tag (SGT) Exchange Protocol (SXP) configuration, a peer can act as both a speaker and a listener and propagate SXP bindings in both directions using a single connection.

The bidirectional SXP configuration is managed with one pair of IP addresses. On either end, only the listener initiates the SXP connection and the speaker accepts the incoming connection.

**Figure 1: Bidirectional SXP Connection**



In addition, SXP version 4 (SXPv4) continues to support the loop detection mechanism (to prevent stale binding in the network).



# How to Enable Bidirectional SXP Support

## Configuring Bidirectional SXP Support

### SUMMARY STEPS

1. enable
2. configure terminal
3. cts sxp enable
4. cts sxp default password
5. cts sxp default source-ip
6. cts sxp connection peer *ipv4-address* {source | password} {default | none} mode {local | peer} both [*vrf vrf-name*]
7. cts sxp speaker hold-time *minimum-period*
8. cts sxp listener hold-time *minimum-period maximum-period*
9. exit

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>cts sxp enable</b>  <b>Example:</b> Device(config)# cts sxp enable	Enables the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4) on a network device.
Step 4	<b>cts sxp default password</b>  <b>Example:</b> Device(config)# cts sxp default password Cisco123	(Optional) Specifies the Cisco TrustSec SGT SXP default password.

	Command or Action	Purpose
<b>Step 5</b>	<b>cts sxp default source-ip</b>  <b>Example:</b>  <pre>Device(config)# cts sxp default source-ip 10.20.2.2</pre>	(Optional) Configures the Cisco TrustSec SGT SXP source IPv4 address.
<b>Step 6</b>	<b>cts sxp connection peer <i>ipv4-address</i> {source   password} {default   none} mode {local   peer} both [<i>vrf vrf-name</i>]</b>  <b>Example:</b>  <pre>Device(config)# cts sxp connection peer 10.20.2.2 password default mode local both</pre>	<p>Configures the Cisco TrustSec SXP peer address connection for a bidirectional SXP configuration. The <b>both</b> keyword configures the bidirectional SXP configuration.</p> <p>The <b>source</b> keyword specifies the IPv4 address of the source device. If no address is specified, the connection uses the default source address, if configured, or the address of the port.</p> <p>The <b>password</b> keyword specifies the password that Cisco TrustSec SXP uses for the connection using the following options:</p> <ul style="list-style-type: none"> <li>• <b>default</b>—Use the default Cisco TrustSec SXP password you configured using the <b>cts sxp default password</b> command.</li> <li>• <b>none</b>—A password is not used.</li> </ul> <p>The <b>mode</b> keyword specifies the role of the remote peer device:</p> <ul style="list-style-type: none"> <li>• <b>local</b>—The specified mode refers to the local device.</li> <li>• <b>peer</b>—The specified mode refers to the peer device.</li> <li>• <b>both</b>—Specifies that the device is both the speaker and the listener in the bidirectional SXP connection.</li> </ul> <p>The optional <b>vrf</b> keyword specifies the VRF to the peer. The default is the default VRF.</p>
<b>Step 7</b>	<b>cts sxp speaker hold-time <i>minimum-period</i></b>  <b>Example:</b>  <pre>Device(config)# cts sxp speaker hold-time 950</pre>	(Optional) Configures the global hold time (in seconds) of a speaker network device for Cisco TrustSec SGT SXPv4. The valid range is from 1 to 65534. The default is 120.
<b>Step 8</b>	<b>cts sxp listener hold-time <i>minimum-period</i> <i>maximum-period</i></b>  <b>Example:</b>  <pre>Device(config)# cts sxp listener hold-time 750 1500</pre>	<p>(Optional) Configures the global hold time (in seconds) of a listener network device for Cisco TrustSec SGT SXPv4. The valid range is from 1 to 65534. The default is 90 to 180.</p> <p><b>Note</b> The <i>maximum-period</i> value must be greater than or equal to the <i>minimum-period</i> value.</p>

	Command or Action	Purpose
Step 9	<b>exit</b>  <b>Example:</b> Device(config)# exit	Exits global configuration mode.

## Verifying Bidirectional SXP Support Configuration

### SUMMARY STEPS

1. **enable**
2. **show cts sxp {connections | sgt-map} [brief | vrf vrf-name]**

### DETAILED STEPS

#### Step 1

**enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

**Example:**

```
Device> enable
```

#### Step 2

**show cts sxp {connections | sgt-map} [brief | vrf vrf-name]**

Displays Cisco TrustSec Exchange Protocol (SXP) status and connections.

**Example:**

```
Device# show cts sxp connections
```

```
SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
-----
Peer IP : 2.0.0.2
Source IP : 1.0.0.2
Conn status : On (Speaker) :: On (Listener)
Conn version : 4
Local mode : Both
Connection inst# : 1
TCP conn fd : 1(Speaker) 3(Listener)
TCP conn password: default SXP password
```

```
Duration since last state change: 1:03:38:03 (dd:hr:mm:sec) :: 0:00:00:46 (dd:hr:mm:sec)
```

```
Device# show cts sxp connection brief
```

```
SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
-----
Peer_IP Source_IP Conn Status Duration
-----
2.0.0.2 1.0.0.2 On(Speaker)::On(Listener) 0:00:37:17 (dd:hr:mm:sec)::0:00:37:19 (dd:hr:mm:sec)
```

The following table describes the various scenarios for the connection status output.

**Table 1: Connection Status Output Scenarios**

Node1	Node2	Node1 CLI Output for Connection Status	Node2 CLI Output for Connection Status
Both	Both	On (Speaker) On (Listener)	On (Speaker) On (Listener)
Speaker	Listener	On	On
Listener	Speaker	On	On

## Configuration Examples for Bidirectional SXP Support

### Example: Configuring Bidirectional SXP Support

The following example shows how to enable bidirectional CTS-SXP and configure the SXP peer connection on Device\_A to connect to Device\_B:

```
Device_A> enable
Device_A# configure terminal
Device_A(config)# cts sxp enable
Device_A(config)# cts sxp default password Cisco123
Device_A(config)# cts sxp default source-ip 10.10.1.1
Device_A(config)# cts sxp connection peer 10.20.2.2 password default mode local both
Device_A(config)# exit
```

The following example shows how to configure the bidirectional CTS-SXP peer connection on Device\_B to connect to Device\_A:

```
Device_B> enable
Device_B# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Password123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local both
Device_B(config)# exit
```

## Additional References for Bidirectional SXP Support

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
Security commands	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Security Command Reference: Commands A to C</a></li> <li>• <a href="#">Cisco IOS Security Command Reference: Commands D to L</a></li> <li>• <a href="#">Cisco IOS Security Command Reference: Commands M to R</a></li> <li>• <a href="#">Cisco IOS Security Command Reference: Commands S to Z</a></li> </ul>
Cisco TrustSec configuration	"Cisco TrustSec Support for IOS" chapter in the <i>Cisco TrustSec Configuration Guide</i>

**Technical Assistance**

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></p>

## Feature Information for Bidirectional SXP Support

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 2: Feature Information for Bidirectional SXP Support**

Feature Name	Releases	Feature Information
Bidirectional SXP Support	Cisco IOS 15.2(2)E	<p>The Bidirectional SXP Support feature enhances the functionality of Cisco TrustSec with SXP version 4 by adding support for Security Group Tag (SGT) Exchange Protocol (SXP) bindings that can be propagated in both directions between a speaker and a listener over a single connection.</p> <p>In Cisco IOS Release 15.2(2)E, this feature is supported on the following platforms:</p> <ul style="list-style-type: none"><li>• Cisco Catalyst 3750-X Series Switches</li><li>• Cisco Catalyst 3560-X Series Switches</li></ul> <p>The following command was introduced or modified: <b>cts sxp connection peer</b>.</p>







## Enablement of Security Group ACL at Interface Level

---

The Enablement of Security Group ACL at Interface Level feature controls and manages the Cisco TrustSec access control on a network device based on an attribute-based access control list. When a security group access control list (SGACL) is enabled globally, the SGACL is enabled on all interfaces in the network by default; use the Enablement of Security Group ACL at Interface Level feature to disable the SGACL on a Layer 3 interface.

- [Finding Feature Information, page 11](#)
- [Restrictions for Enablement of Security Group ACL at Interface Level, page 12](#)
- [Information About Enablement of Security Group ACL at Interface Level, page 12](#)
- [How to Configure Security Group ACL at Interface Level, page 13](#)
- [Configuration Examples for Enablement of Security Group ACL at Interface Level, page 14](#)
- [Additional References for Enablement of Security Group ACL at Interface Level, page 15](#)
- [Feature Information for Enablement of Security Group ACL at Interface Level, page 16](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

# Restrictions for Enablement of Security Group ACL at Interface Level

- The Enablement of Security Group ACL at Interface Level feature is effective only if the security group access control list (SGACL) enforcement is enabled globally.
- Disabling per-interface SGACL enforcement also disables Security Group Tag (SGT) caching on the specific interface.
- Per-interface SGACL enforcement is not supported on Layer 3 port channel interfaces.
- Per-interface SGACL enforcement is not supported on Layer 2 interfaces.

## Information About Enablement of Security Group ACL at Interface Level

### Security Group ACL Overview

The attribute-based access control list organizes and manages the Cisco TrustSec access control on a network device. The security group access control list (SGACL) is a Layer 3-4 access control list to filter access based on the value of the security group tag (SGT). The filtering usually occurs at an egress port of the Cisco TrustSec domain. SGT is a Layer 2 tag that is used to classify traffic based on role, and SGT tagging occurs at ingress of the CTS domain.

The terms role-based ACL (RBACL) and SGACL can be used interchangeably, and they refer to a topology-independent ACL used in an attribute-based access control (ABAC) policy model. ABAC is an access control mechanism that uses subject attributes, resource attributes, and environment attributes.

- Subject attributes (S) are associated with a subject—be it a user or an application—that defines the identity and characteristics of that subject.
- Resource attributes (R) are associated with a resource, such as a web service, a system function, or data.
- Environment attributes (E) describe the operational, technical, or situational environment or context in which information is accessed.

ABAC policy rules are generated as Boolean functions of S, R, and E attributes, and these rules decide whether a subject S can access a resource R in a particular environment E. Access control policy is defined between security groups and consists of traditional security ACLs but without IP source and destination addresses.

Because networks are bidirectional, access control is applied both between the subject (user) and the object (resource or server) and between the object and the subject. This requires the subjects to be grouped together into security groups and the objects to be likewise grouped together into security groups. Rules based on subject and object attributes group the subjects and objects into security groups.

Once SGACL is enabled globally, it is automatically enabled on every Layer 3 interface on the device, and you can disable SGACL on specific Layer 3 interfaces. Granular disablement at interface level is effective

only if SGACL is enabled globally. This feature is applicable even if packets sent or received are not tagged with SGT at the source device of the packet.

Enabling or disabling per-interface SGACL enforcement enables or disables SGACL monitor mode on that interface.

## Guidelines to Configure Security Group ACL

The security group access control list (SGACL) can be configured by the administrator in Cisco Identity Service Engine (ISE) or in Cisco Secure Access Control System (ACS).

You can also configure the SGACL in the device using the **ip access-list role-based** *sgacl-name* command in global configuration mode. Use the **show cts role-based permissions** command or the **show cts rbacl** command in privileged EXEC mode to view the SGACLs configured on the device. For more information about the security commands, see the *Cisco IOS Security Command Reference*.



**Note** Ensure that the SGACL name begins with an alphabetic character to prevent ambiguity with numbered access lists. These names cannot contain a space or quotation mark.

## How to Configure Security Group ACL at Interface Level

### Configuring Security Group ACL at Interface Level

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **cts role-based enforcement**
5. **end**
6. **show running-config interface** *type number*

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.

	Command or Action	Purpose
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<b>interface <i>type number</i></b>  <b>Example:</b> Device(config)# <code>interface gigabitethernet 2/5/3</code>	Enters interface configuration mode.
Step 4	<b>cts role-based enforcement</b>  <b>Example:</b> Device(config-if)# <code>cts role-based enforcement</code>	Enables a security group access control list (SGACL) for the interface.
Step 5	<b>end</b>  <b>Example:</b> Device(config-if)# <code>end</code>	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	<b>show running-config interface <i>type number</i></b>  <b>Example:</b> Device# <code>show running-config interface gigabitethernet 2/5/3</code>	Displays whether the SGACL is disabled on a specific interface.

## Configuration Examples for Enablement of Security Group ACL at Interface Level

### Example: Configuring Security Group ACL at Interface Level

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/3
Device(config-if)# cts role-based enforcement
Device(config-if)# end
```

### Example: Verifying Security Group ACL at Interface Level

```
Device# show running-config interface gigabitethernet 2/5/3

Building configuration...

Current configuration : 175 bytes
!
interface GigabitEthernet2/5/3
no switchport
ip address 192.0.2.2 255.255.255.0
```

```
load-interval 30
ipv6 address 2001:DB8::1
ipv6 enable
no cts role-based enforcement
end
```



**Note** The **no cts role-based enforcement** line in the command output indicates that the security group access control list (SGACL) is disabled at the interface level.

## Additional References for Enablement of Security Group ACL at Interface Level

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
Security commands	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Security Command Reference: Commands A to C</a></li> <li>• <a href="#">Cisco IOS Security Command Reference: Commands D to L</a></li> <li>• <a href="#">Cisco IOS Security Command Reference: Commands M to R</a></li> <li>• <a href="#">Cisco IOS Security Command Reference: Commands S to Z</a></li> </ul>
Cisco TrustSec switches	<i>Cisco TrustSec Switch Configuration Guide</i>

### 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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for Enablement of Security Group ACL at Interface Level

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 3: Feature Information for Enablement of Security Group ACL at Interface Level**

Feature Name	Releases	Feature Information
Enablement of Security Group ACL at Interface Level	Cisco IOS 15.2(2)E	<p>The Enablement of Security Group ACL at Interface Level feature controls and manages the Cisco TrustSec access control on a network device based on an attribute-based access control policy. This feature provides the flexibility of enabling and disabling a security group access control list (SGACL) on specific Layer 3 interfaces with assigned security groups.</p> <p>In Cisco IOS Release 15.2(2)E, this feature is supported on the following platforms:</p> <ul style="list-style-type: none"> <li>• Cisco Catalyst 3750-X Series Switches</li> <li>• Cisco Catalyst 3560-X Series Switches</li> </ul> <p>The following command was introduced: <b>cts role-based enforcement</b>.</p>



## IPv6 Support for SGT and SGACL

---

The IPv6 Support for SGT and SGACL feature facilitates dynamic learning of mappings between IP addresses and Security Group Tags (SGTs) for IPv6 addresses. The SGT is later used to derive the Security Group Access Control List (SGACL).

- [Finding Feature Information, page 17](#)
- [Restrictions for IPv6 Support for SGT and SGACL, page 17](#)
- [Information About IPv6 Support for SGT and SGACL, page 18](#)
- [How to Configure IPv6 Support for SGT and SGACL, page 18](#)
- [Configuration Examples for IPv6 Support for SGT and SGACL, page 26](#)
- [Additional References for IPv6 Support for SGT and SGACL, page 27](#)
- [Feature Information for IPv6 Support for SGT and SGACL, page 28](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

### Restrictions for IPv6 Support for SGT and SGACL

Enforcement of IPv6 addresses is not supported by this feature.

# Information About IPv6 Support for SGT and SGACL

## Components of IPv6 Dynamic Learning

Dynamic learning of IPv6 addresses require three components:

- Switch Integrated Security Features (SISF)—An infrastructure built to take care of security, address assignment, address resolution, neighbor discovery, exit point discovery, and so on.
- Cisco Enterprise Policy Manager (EPM)—A solution that registers to SISF to receive IPv6 address notifications. The Cisco EPM then uses these IPv6 addresses and the Security Group Tags (SGTs) downloaded from the Cisco Identity Services Engine (ISE) to generate IP-SGT bindings.
- Cisco TrustSec—A solution that protects devices from unauthorized access. Cisco TrustSec assigns an SGT to the ingress traffic of a device and enforces the access policy based on the tag anywhere in the network.

Learning of IPv6 addresses can be done using the following methods, which are listed starting from lowest priority (1) to highest priority (7):

- 1 VLAN—Bindings learned from snooped Address Resolution Protocol (ARP) packets on a VLAN that has VLAN-SGT mapping.
- 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 forwarding information base (FIB ) forwarding entries that have paths through one or more interfaces with consistent L3IF-SGT mapping or identity port mapping (IPM) on routed ports.
- 4 SXP—Bindings learned from SGT Exchange Protocol (SXP) peers.
- 5 IP\_ARP—Bindings learned when tagged ARP packets are received on a CTS-capable link.
- 6 Local—Bindings of authenticated hosts that are learned via EPM and device tracking.
- 7 Internal—Bindings between locally configured IP addresses and the device's own SGT.

## How to Configure IPv6 Support for SGT and SGACL

### Generating IPv6 Addresses for IP-SGT Bindings

Switch Integrated Security Features (SISF) is a feature that generates IPv6 addresses for use in IP-SGT bindings.



## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 snooping policy** *policy-name*
4. **tracking enable**
5. **exit**
6. **ipv6 dhcp pool** *dhcp-pool-name*
7. **address prefix** *ipv6-address/prefix*
8. **exit**
9. **interface vlan** *interface-number*
10. **ipv6 enable**
11. **no ipv6 address**
12. **ipv6 address** *ipv6-address/prefix*
13. **ipv6 address autoconfiguration**
14. **ipv6 dhcp server** *dhcp-pool-name*
15. **end**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ipv6 snooping policy</b> <i>policy-name</i>  <b>Example:</b> Device(config)# ipv6 snooping policy policy1	Generates IPv6 addresses for IP-SGT bindings and enters IPv6 snooping configuration mode.
<b>Step 4</b>	<b>tracking enable</b>  <b>Example:</b> Device(config-ipv6-snooping)# tracking enable	Overrides the default tracking policy on a port.
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> Device(config-ipv6-snooping)# exit	Exits IPv6 snooping configuration mode and returns to global configuration mode.

	Command or Action	Purpose
<b>Step 6</b>	<code>ipv6 dhcp pool <i>dhcp-pool-name</i></code>  <b>Example:</b> Device(config)# ipv6 dhcp pool dhcp-pool	Assigns an IPv6 DHCP pool to the DHCP server and enters IPv6 DHCP pool configuration mode.
<b>Step 7</b>	<code>address prefix <i>ipv6-address/prefix</i></code>  <b>Example:</b> Device(config-dhcpv6)# address prefix 2001:DB8::1/64	Sets the IPv6 address for an end host.
<b>Step 8</b>	<code>exit</code>  <b>Example:</b> Device(config-dhcpv6)# exit	Exits IPv6 DHCP pool configuration mode and returns to global configuration mode.
<b>Step 9</b>	<code>interface vlan <i>interface-number</i></code>  <b>Example:</b> Device(config)# interface vlan 20	Creates a VLAN interface and enters interface configuration mode.
<b>Step 10</b>	<code>ipv6 enable</code>  <b>Example:</b> Device(config-if)# ipv6 enable	Enables IPv6 on an interface.
<b>Step 11</b>	<code>no ipv6 address</code>  <b>Example:</b> Device(config-if)# no ipv6 address	Removes the existing IPv6 address set for an interface.
<b>Step 12</b>	<code>ipv6 address <i>ipv6-address/prefix</i></code>  <b>Example:</b> Device(config-if)# ipv6 address 2001:DB8:1:1::1/64	Assigns an IPv6 address for the interface.
<b>Step 13</b>	<code>ipv6 address autoconfiguration</code>  <b>Example:</b> Device(config-if)# ipv6 address autoconfiguration	Enables stateless autoconfiguration on an interface.
<b>Step 14</b>	<code>ipv6 dhcp server <i>dhcp-pool-name</i></code>  <b>Example:</b> Device(config-if)# ipv6 dhcp server dhcp-pool	Assigns an IPv6 DHCP pool to the DHCP server.
<b>Step 15</b>	<code>end</code>  <b>Example:</b> Device(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

**What to Do Next**

Configure IPv6-SGT binding by using either local binding or a VLAN.

**Configuring IPv6 IP-SGT Binding Using Local Binding**

In local binding, the Security Group Tag (SGT) value is downloaded from the Identity Services Engine (ISE).

**Before You Begin**

- An IPv6 address must be generated through Switch Integrated Security Features (SISF) to configure an IP-SGT binding.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **policy-map type control subscriber** *control-policy-name*
4. **event session-started match-all**
5. *priority-number* **class always do-until-failure**
6. *action-number* **authenticate using mab**
7. **end**
8. **configure terminal**
9. **interface gigabitethernet** *interface-number*
10. **description** *interface-description*
11. **switchport access vlan** *vlan-id*
12. **switchport mode access**
13. **ipv6 snooping attach-policy** *policy-name*
14. **access-session port-control auto**
15. **mab eap**
16. **dot1x pae authenticator**
17. **service-policy type control subscriber** *policy-name*
18. **end**
19. **show cts role-based sgt-map all ipv6**

**DETAILED STEPS**

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.

	Command or Action	Purpose
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>policy-map type control subscriber <i>control-policy-name</i></b>  <b>Example:</b> Device(config)# policy-map type control subscriber policy1	Defines a control policy for subscriber sessions and enters control policy-map configuration mode.
Step 4	<b>event session-started match-all</b>  <b>Example:</b> Device(config-event-control-policymap)# event session-started match-all	Specifies the type of event that triggers actions in a control policy if conditions are met.
Step 5	<b><i>priority-number</i> class always do-until-failure</b>  <b>Example:</b> Device(config-class-control-policymap)# 10 class always do-until-failure	Associates a control class with one or more actions in a control policy and enters action control policy-map configuration mode.  • A named control class must first be configured before specifying it with the <i>control-class-name</i> argument.
Step 6	<b><i>action-number</i> authenticate using mab</b>  <b>Example:</b> Device(config-action-control-policymap)# 10 authenticate using mab	Initiates the authentication of a subscriber session using the specified method.
Step 7	<b>end</b>  <b>Example:</b> Device(config-action-control-policymap)# end	Exits action control policy-map configuration mode and returns to privileged EXEC mode.
Step 8	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 9	<b>interface gigabitethernet <i>interface-number</i></b>  <b>Example:</b> Device(config)# interface gigabitethernet 1/0/1	Enters interface configuration mode.
Step 10	<b>description <i>interface-description</i></b>  <b>Example:</b> Device(config-if)# description downlink to ipv6 clients	Describes the configured interface.

	Command or Action	Purpose
Step 11	<b>switchport access vlan</b> <i>vlan-id</i>  <b>Example:</b> Device(config-if)# switchport access vlan 20	Sets access mode characteristics of the interface and configures VLAN when the interface is in access mode.
Step 12	<b>switchport mode access</b>  <b>Example:</b> Device(config-if)# switchport mode access	Sets the trunking mode to access mode.
Step 13	<b>ipv6 snooping attach-policy</b> <i>policy-name</i>  <b>Example:</b> Device(config-if)# ipv6 snooping attach-policy snoop	Applies a policy to the IPv6 snooping feature.
Step 14	<b>access-session port-control auto</b>  <b>Example:</b> Device(config-if)# access-session port-control auto	Sets the authorization state of a port.
Step 15	<b>mab eap</b>  <b>Example:</b> Device(config-if)# mab eap	Uses Extensible Authentication Protocol (EAP) for MAC authentication bypass.
Step 16	<b>dot1x pae authenticator</b>  <b>Example:</b> Device(config-if)# dot1x pae authenticator	Enables dot1x authentication on the port.
Step 17	<b>service-policy type control subscriber</b> <i>policy-name</i>  <b>Example:</b> Device(config-if)# service-policy type control subscriber policy	Specifies the policy map that is used for sessions that come up on this interface. The policy map has rules for authentication and authorization.
Step 18	<b>end</b>  <b>Example:</b> Device(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.
Step 19	<b>show cts role-based sgt-map all ipv6</b>  <b>Example:</b> Device# show cts role-based sgt-map all ipv6	Displays active IPv6 IP-SGT bindings.

## Configuring IPv6 IP-SGT Binding Using a VLAN

In a VLAN, a network administrator assigns a Security Group Tag (SGT) value to a particular VLAN.

**Before You Begin**

- An IPv6 address must be generated through Switch Integrated Security Features (SISF) to configure an IP-SGT binding.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. cts role-based sgt-map vlan-list *vlan-id* sgt *sgt-value*
4. end
5. show cts role-based sgt-map all ipv6

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	enable  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	configure terminal  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	cts role-based sgt-map vlan-list <i>vlan-id</i> sgt <i>sgt-value</i>  <b>Example:</b> Device(config)# cts role-based sgt-map vlan-list 20 sgt 3	Assigns an SGT value to the configured VLAN.  <b>Note</b> The range of the <i>sgt-value</i> argument must be from 2 to 65519.
<b>Step 4</b>	end  <b>Example:</b> Device(config)# end	Exits global configuration mode and returns to privileged EXEC mode.
<b>Step 5</b>	show cts role-based sgt-map all ipv6  <b>Example:</b> Device# show cts role-based sgt-map all ipv6	Displays active IPv6 IP-SGT bindings.

## Verifying IPv6 Support for SGT and SGACL

### SUMMARY STEPS

1. enable
2. show cts role-based sgt-map all
3. show cts role-based sgt-map all ipv6

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Device&gt; <b>enable</b></p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<p><b>show cts role-based sgt-map all</b></p> <p><b>Example:</b> Device# <b>show cts role-based sgt-map all</b></p> <pre>Active IPv4-SGT Bindings Information IP Address                SGT      Source ===== 192.0.2.1                  8        INTERNAL 192.0.2.2                  8        INTERNAL 192.0.2.3                  11       LOCAL  IP-SGT Active Bindings Summary ===== Total number of LOCAL    bindings = 1 Total number of INTERNAL bindings = 2 Total number of active   bindings = 3  Active IPv6-SGT Bindings Information IP Address                SGT      Source ===== 2001:DB8:0:ABCD::1       8        INTERNAL 2001:DB8:1::1            11       LOCAL 2001:DB8:1::1            11       LOCAL  IP-SGT Active Bindings Summary ===== Total number of LOCAL    bindings = 2 Total number of INTERNAL bindings = 1 Total number of active   bindings = 3</pre>	<p>Displays active IPv4 and IPv6 IP-SGT bindings.</p>
Step 3	<p><b>show cts role-based sgt-map all ipv6</b></p> <p><b>Example:</b> Device# <b>show cts role-based sgt-map all ipv6</b></p> <pre>Active IP-SGT Bindings Information</pre>	<p>Displays active IPv6 IP-SGT bindings.</p>

Command or Action	Purpose
<pre> IP Address                                     SGT      Source ===== 2001:DB8:1::1                                10       CLI 2001:DB8:1:FFFF::1                           27       VLAN 2001:DB8:9798:8294:753F::1                    5        LOCAL 2001:DB8:8E99:DA94:8A6A::2                    5        LOCAL 2001:DB8:104:2001::139                         27       VLAN 2001:DB8:104:2001:14FE:9798:8294:753F         5        LOCAL  IP-SGT Active Bindings Summary ===== Total number of VLAN      bindings = 2 Total number of CLI       bindings = 1 Total number of LOCAL     bindings = 3 Total number of active    bindings = 6 </pre>	

## Configuration Examples for IPv6 Support for SGT and SGACL

### Example: Generating IPv6 Addresses for IP-SGT Bindings

```

Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy-name
Device(config-ipv6-snooping)# tracking enable
Device(config-ipv6-snooping)# exit
Device(config)# ipv6 dhcp pool dhcp-pool
Device(config-dhcpv6)# address prefix 2001:DB8::1/64
Device(config-dhcpv6)# exit
Device(config)# interface vlan 20
Device(config-if)# no ip address
Device(config-if)# ipv6 address 2001:DB8::2/64
Device(config-if)# ipv6 address autoconfiguration
Device(config-if)# ipv6 enable
Device(config-if)# ipv6 dhcp server dhcp-pool
Device(config-if)# end

```

### Example: Configuring IPv6 IP-SGT Binding Using Local Binding

```

Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy-name
Device(config-ipv6-snooping)# tracking enable
Device(config-ipv6-snooping)# exit
Device(config)# ipv6 dhcp pool dhcp-pool
Device(config-dhcpv6)# address prefix 2001:DB8::1/64
Device(config-dhcpv6)# exit
Device (config)# interface vlan 20
Device(config-if)# no ip address
Device(config-if)# ipv6 address 2001:DB8::2/64
Device(config-if)# ipv6 address autoconfiguration

```



```

Device(config-if)# ipv6 enable
Device(config-if)# ipv6 dhcp server dhcp-pool
Device(config-if)# exit
Device(config)# policy-map type control subscriber policy1
Device(config-event-control-policymap)# event session match-all
Device(config-class-control-policymap)# 10 class always do-until-failure
Device(config-action-control-policymap)# 10 authenticate using mab
Device(config-action-control-policymap)# end
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# description downlink to ipv6 clients
Device(config-if)# switchport access vlan 20
Device(config-if)# switchport mode access
Device(config-if)# ipv6 snooping attach-policy snoop
Device(config-if)# access-session port-control auto
Device(config-if)# mab eap
Device(config-if)# dot1x pae authenticator
Device(config-if)# service-policy type control subscriber example
Device(config-if)# end

```

## Example: Configuring IPv6 IP-SGT Binding Using a VLAN

```

Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy-name
Device(config-ipv6-snooping)# tracking enable
Device(config-ipv6-snooping)# exit
Device(config)# ipv6 dhcp pool dhcp-pool
Device(config-dhcpv6)# address prefix 2001:DB8::1/64
Device(config-dhcpv6)# domain name domain.com
Device(config-dhcpv6)# exit
Device (config)# interface vlan 20
Device(config-if)# no ip address
Device(config-if)# ipv6 address 2001:DB8::2/64
Device(config-if)# ipv6 address autoconfiguration
Device(config-if)# ipv6 enable
Device(config-if)# ipv6 nd other-config-flag
Device(config-if)# ipv6 dhcp server dhcp-pool
Device(config-if)# end

```

## Additional References for IPv6 Support for SGT and SGACL

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>

Related Topic	Document Title
Security commands	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Security Command Reference Commands A to C</a></li> <li>• <a href="#">Cisco IOS Security Command Reference Commands D to L</a></li> <li>• <a href="#">Cisco IOS Security Command Reference Commands M to R</a></li> <li>• <a href="#">Cisco IOS Security Command Reference Commands S to Z</a></li> </ul>
Security group ACL	“Enablement of Security Group ACL at Interface Level” module of <i>Cisco TrustSec Configuration Guide</i>
IEEE 802.1X authentication	“Configuring IEEE 802.1X Port-Based Authentication” module of <i>802.1X Authentication Services Configuration Guide</i>
MAC Authentication Bypass	“Configuring MAC Authentication Bypass” module of <i>Authentication Authorization and Accounting Configuration Guide</i>

### Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature Information for IPv6 Support for SGT and SGACL

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 4: Feature Information for IPv6 Support for SGT and SGACL**

Feature Name	Releases	Feature Information
IPv6 Support for SGT and SGACL	Cisco IOS 15.2(2)E	<p>The IPv6 Support for SGT and SGACL feature introduces dynamic learning of mappings between IP addresses and Security Group Tags (SGTs) for IPv6 addresses. The SGT is later used to derive the Security Group Access Control List (SGACL).</p> <p>In Cisco IOS Release 15.2(2)E, this feature was supported on the following platforms:</p> <ul style="list-style-type: none"> <li>• Cisco Industrial Ethernet 3000 Series Switches</li> <li>• Cisco Industrial Ethernet 2000 Series Switches</li> <li>• Catalyst 2960-S Series Switches</li> <li>• Catalyst 2960-Plus Series Switches</li> <li>• Catalyst 2960-C Series Switches</li> <li>• Catalyst 3560-C Series Switches</li> <li>• Catalyst 3750-X Series Switches</li> <li>• Catalyst 3560-X Series Switches</li> <li>• Catalyst 2960-X Series Switches</li> <li>• Catalyst 2960-X Series Switches</li> </ul> <p>The following command was modified: <b>cts role-based sgt-map</b>.</p>





# 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 31](#)
- [How to Configure Cisco TrustSec Network Device Admission Control, page 32](#)
- [Configuration Examples for Cisco TrustSec Network Device Admission Control, page 36](#)
- [Additional References, page 37](#)
- [Feature Information for Cisco TrustSec Network Device Admission Control, page 38](#)

## 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	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

	Command or Action	Purpose
<b>Step 2</b>	<b>cts credentials id</b> <i>cts-id</i> <b>password</b> <i>cts-password</i>  <b>Example:</b> Device# cts credentials id CTS-One password cisco123	Specifies the Cisco TrustSec ID and password of the network device.
<b>Step 3</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 4</b>	<b>aaa new-model</b>  <b>Example:</b> Device(config)# aaa new-model	Enables new RADIUS and AAA access control commands and functions and disables old commands.
<b>Step 5</b>	<b>aaa session-id common</b>  <b>Example:</b> 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.
<b>Step 6</b>	<b>radius server</b> <i>radius-server-name</i>  <b>Example:</b> 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.
<b>Step 7</b>	<b>address ipv4</b> { <i>hostname</i>   <i>ipv4address</i> } [ <b>acct-port</b> <i>port</i>   <b>alias</b> { <i>hostname</i>   <i>ipv4address</i> }   <b>auth-port</b> <i>port</i> [ <b>acct-port</b> <i>port</i> ]]  <b>Example:</b> 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.
<b>Step 8</b>	<b>pac key</b> <i>encryption-key</i>  <b>Example:</b> Device(config-radius-server)# pac key cisco123	Specifies the PAC encryption key.
<b>Step 9</b>	<b>exit</b>  <b>Example:</b> Device(config-radius-server)# exit	Exits RADIUS server configuration mode and enters global configuration mode.
<b>Step 10</b>	<b>radius-server vsa send authentication</b>  <b>Example:</b> Device(config)# radius-server vsa send authentication	Configures the network access server (NAS) to recognize and use only authentication vendor-specific attributes (VSAs).

	Command or Action	Purpose
<b>Step 11</b>	<b>aaa group server radius</b> <i>group-name</i>  <b>Example:</b> 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.
<b>Step 12</b>	<b>server name</b> <i>radius-server-name</i>  <b>Example:</b> Device(config-sg-radius)# server name cts-aaa-server	Specifies a RADIUS server.
<b>Step 13</b>	<b>exit</b>  <b>Example:</b> Device(config-sg-radius)# exit	Exits RADIUS group server configuration mode and enters global configuration mode.
<b>Step 14</b>	<b>aaa authentication dot1x default group</b> <i>group-name</i>  <b>Example:</b> Device(config)# aaa authentication dot1x default group cts_sg	Specifies the RADIUS server to use for authentication on interfaces running IEEE 802.1X.
<b>Step 15</b>	<b>aaa authorization network default group</b> <i>group-name</i>  <b>Example:</b> Device(config)# aaa authorization network default group cts_sg	Specifies that the RADIUS server method is the default method for authorization into a network.
<b>Step 16</b>	<b>aaa authorization network list-name group</b> <i>group-name</i>  <b>Example:</b> 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.
<b>Step 17</b>	<b>cts authorization list</b> <i>list-name</i>  <b>Example:</b> Device(config)# cts authorization list cts-mlist	Specifies a list of AAA servers for the Cisco TrustSec seed device.
<b>Step 18</b>	<b>exit</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>cts credentials id <i>cts-id</i> password <i>cts-password</i></b>  <b>Example:</b> Device# cts credentials id CTS-One password cisco123	Specifies the Cisco TrustSec ID and password of the network device.
<b>Step 3</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 4</b>	<b>aaa new-model</b>  <b>Example:</b> Device(config)# aaa new-model	Enables new RADIUS and AAA access control commands and functions and disables old commands.
<b>Step 5</b>	<b>aaa session-id common</b>  <b>Example:</b> 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.
<b>Step 6</b>	<b>radius-server vsa send authentication</b>  <b>Example:</b> Device(config)# radius-server vsa send authentication	Configures the network access server (NAS) to recognize and use only authentication vendor-specific attributes (VSAs).

	Command or Action	Purpose
Step 7	<b>exit</b>  <b>Example:</b> Device(config)# exit	Exits global configuration mode and returns to privileged EXEC 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

```

# Additional References

## Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
Security commands	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Security Command Reference Commands A to C</a></li> <li>• <a href="#">Cisco IOS Security Command Reference Commands D to L</a></li> <li>• <a href="#">Cisco IOS Security Command Reference Commands M to R</a></li> <li>• <a href="#">Cisco IOS Security Command Reference Commands S to Z</a></li> </ul>
Cisco TrustSec and SXP configuration	<a href="#">Cisco TrustSec Switch Configuration Guide</a>
IPsec configuration	<a href="#">Configuring Security for VPNs with IPsec</a>
IKEv2 configuration	<a href="#">Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site</a>
Cisco Secure Access Control Server	<a href="#">Configuration Guide for the Cisco Secure ACS</a>

## 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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

# 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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 5: Feature Information for Cisco TrustSec Network Device Admission Control**

Feature Name	Releases	Feature Information
Cisco TrustSec Network Device Admission Control	Cisco IOS 15.0(1)SE Cisco IOS 15.1(1)SG Cisco IOS 15.2(3)E	<p>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.</p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p> <p>The following commands were introduced or modified: <b>cts dot1x</b>, <b>propagate sgt (config-if-cts-dot1x)</b> , <b>sap mode-list</b>, <b>timer reauthentication</b>.</p>



## Cisco TrustSec Critical Authentication

The Cisco TrustSec Critical Authentication feature ensures that the Network Device Admission Control (NDAC)-authenticated 802.1X links between Cisco TrustSec devices are in an open state even when the Authentication, Authorization, and Accounting (AAA) server is not reachable.

- [Finding Feature Information, page 39](#)
- [Prerequisites for Cisco TrustSec Critical Authentication, page 39](#)
- [Restrictions for Cisco TrustSec Critical Authentication, page 40](#)
- [Information About Cisco TrustSec Critical Authentication, page 40](#)
- [How to Configure Cisco TrustSec Critical Authentication, page 42](#)
- [Configuration Examples for Cisco TrustSec Critical Authentication, page 45](#)
- [Additional References for Cisco TrustSec Critical Authentication, page 46](#)
- [Feature Information for Cisco TrustSec Critical Authentication, page 47](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

### Prerequisites for Cisco TrustSec Critical Authentication

- The Cisco TrustSec Network Device Admission Control feature must be configured on the device. For more information, see the “Cisco TrustSec Network Device Admission Control” chapter in the *Cisco TrustSec Configuration Guide*.

- Ensure that the RADIUS server is marked as dead before configuring the Cisco TrustSec Critical Authentication feature.

## Restrictions for Cisco TrustSec Critical Authentication

- All Cisco TrustSec 802.1X links must be part of a single port channel or must be on different VLANs. If multiple links are on the same VLAN, authentication fails because Spanning Tree Protocol (STP) drops all the packets on a blocked interface.



---

**Note** All STP forwarding ports are maintained in the open state when Cisco TrustSec critical authentication mode is enabled.

---

- If the authenticating device (authenticator) is down or if connectivity between the authenticator and Cisco Identity Services Engine (ISE) is lost, the Cisco TrustSec 802.1X links move to the critical authentication mode until connectivity is regained or until the links are reconfigured.
- The default peer security group tag (SGT) value used to configure the Cisco TrustSec 802.1X links for critical authentication must be defined in the ISE server. If the default peer-SGT value is not defined in the ISE server, the policies related to the default peer SGT are not downloaded and are not applied on the Cisco TrustSec 802.1X links. In such a situation, the default policy is applied when the links are in critical authentication mode.
- You must not refresh the environment data when connectivity to the ISE server is lost and when the Cisco TrustSec 802.1X links are in critical authentication mode. If the environment data is refreshed and fails to download, the policies on the device may get cleared.

## Information About Cisco TrustSec Critical Authentication

### Critical Authentication Overview

The Cisco TrustSec solution provides end-to-end security that is centrally managed using an Authentication, Authorization, and Accounting (AAA) server. The AAA server authenticates and authorizes each device coming into the network, and encryption is done on a per-link basis. The authentication information is downloaded to both the authenticating device (authenticator) and to the incoming device (supplicant) that are added to the CTS network. Another key component of Cisco TrustSec is the Cisco Identity Services Engine (ISE). The ISE server is the policy control point for Cisco TrustSec. The authenticator must be connected to the ISE server to ensure that the Cisco TrustSec 802.1X links are active. After authentication, the supplicant is connected to the ISE server through the authenticator.

Cisco TrustSec Network Device Admission Control helps to add network devices into trusted networks.

When the AAA server is down, Cisco TrustSec can neither add any new device into the network nor maintain the currently authenticated devices in the trusted network. This situation results in the Cisco TrustSec links going into the disconnect state.

The Cisco TrustSec Critical Authentication feature aims to prevent the Cisco TrustSec 802.1X links from going down if the AAA server is not reachable. For devices that are already in the trusted network, previously

obtained (cached) security group access control list (SGACL) policies, peer security group tag (SGT) values, and pairwise master key (PMK) values are used until the AAA server is reachable again. For new devices coming into the network, the default peer-SGT value (trusted or untrusted), default PMK value, and default SGACL policy are used until the AAA server is reachable and the full authentication and authorization policy is received from the AAA server.

All three values—SGACL policy, peer-SGT value, and PMK value—are configurable.

If a user does not want to configure the PMK value, critical authentication brings up 802.1X links without link encryption, and the Security Association Protocol (SAP) negotiation does not occur between interfaces. The default PMK value is used for all SAP negotiations.

In critical authentication mode, preference is given to cached data because it is the last valid set of values received from the AAA server. However, this is a configurable option, and the user can decide if default values should be preferred over cached values.

**Note**

---

The Cisco TrustSec Critical Authentication feature is triggered only when the AAA server is unreachable. It is not triggered if the AAA server responds to an authenticator request from a device with a failure message (Access-Reject).

Consider this example: If the entry for Device A is deleted from the AAA server and the AAA server is thus unreachable, a Device A link in authenticator state will trigger the critical authentication feature. If Device B is connected to this link, Device B will also enter into critical authentication mode, and Device B will become the authenticator. Now, if Device B has one or more other links in supplicant state that are connected to Device A, then these supplicant links will attempt to reauthenticate with the AAA server. However, the AAA server will reject Device B's request for authentication (by sending the Access-Reject message). As a result, critical authentication feature on both devices will be terminated. The other interfaces connected to both devices (with SAP negotiation on one end and 802.1x authentication on the other) will now start flapping.

This is a security mechanism to prevent unauthorized devices from assuming the role of authenticator.

---

# How to Configure Cisco TrustSec Critical Authentication

## Configuring Critical Authentication

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server dead-criteria** [**time seconds**] [**tries number-of-tries**]
4. **radius-server deadtime** *minutes*
5. **radius server** *server-name*
6. **address ipv4** {*hostname* | *ipv4address*} [**acct-port** *port* | **alias** {*hostname* | *ipv4address*} | **auth-port** *port* [**acct-port** *port*]]
7. **automate-tester username** *user* [**ignore-auth-port**] [**ignore-acct-port**] [**idle-time** *minutes*]
8. **pac key** *encryption-key*
9. **exit**
10. **cts server test** {*ipv4-address* | **all**} {**deadtime** *seconds* | **enable** | **idle-time** *minutes*}
11. **cts critical-authentication default peer-sgt** *peer-sgt-value* [**trusted**]
12. **exit**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>radius-server dead-criteria</b> [ <b>time seconds</b> ] [ <b>tries number-of-tries</b> ]  <b>Example:</b> Device(config)# radius-server dead-criteria time 15 tries 3	Configures the conditions that determine when a RADIUS server is considered unavailable or dead. <ul style="list-style-type: none"> <li>• <b>time seconds</b> - Sets the time, in seconds, during which the device does not need to get a valid response from the RADIUS server. The range is from one to 120 seconds.</li> <li>• <b>tries number-of-tries</b> - Sets the number of times that the device does not get a valid response from the RADIUS server before the server is considered unavailable.</li> </ul>



	Command or Action	Purpose
<b>Step 4</b>	<p><b>radius-server</b> <i>deadtime minutes</i></p> <p><b>Example:</b></p> <pre>Device(config)# radius-server deadtime 10</pre>	<p>Defines time, in minutes (up to a maximum of 1440 minutes or 24 hours), a server marked as DEAD is held in that state. This command improves RADIUS response times when some servers might be unavailable, and causes the unavailable servers to be skipped immediately.</p> <p>Once the deadtime expires, the device marks the server as UP (ALIVE) and notifies the registered clients about the state change. If the server is still unreachable after the state is marked as UP and if the DEAD criteria is met, then server is marked as DEAD again for the deadtime interval.</p>
<b>Step 5</b>	<p><b>radius server</b> <i>server-name</i></p> <p><b>Example:</b></p> <pre>Device(config)# radius server RASERV-1</pre>	<p>Specifies the name for the RADIUS server configuration for Protected Access Credential (PAC) provisioning and enters RADIUS server configuration mode.</p>
<b>Step 6</b>	<p><b>address ipv4</b> {<i>hostname   ipv4address</i>} [<b>acct-port</b> <i>port   alias {hostname   ipv4address}</i>]   <b>auth-port</b> <i>port</i> [<b>acct-port</b> <i>port</i>]]</p> <p><b>Example:</b></p> <pre>Device(config-radius-server)# address ipv4 172.20.254.4 auth-port 1812 acct-port 1813</pre>	<p>Configures the IPv4 address for the RADIUS server accounting and authentication parameters.</p>
<b>Step 7</b>	<p><b>automate-tester username</b> <i>user</i> [<b>ignore-auth-port</b>] [<b>ignore-acct-port</b>] [<b>idle-time</b> <i>minutes</i>]</p> <p><b>Example:</b></p> <pre>Device(config-radius-server)# automate-tester username dummy</pre>	<p>Enables the automated testing feature for the RADIUS server.</p> <p>With this practice, the device sends periodic test authentication messages to the RADIUS server. It looks for a RADIUS response from the server. A success message is not necessary - a failed authentication suffices, because it shows that the server is alive.</p>
<b>Step 8</b>	<p><b>pac key</b> <i>encryption-key</i></p> <p><b>Example:</b></p> <pre>Device(config-radius-server)# pac key 7 mypackey</pre>	<p>Specifies the Protected Access Credential (PAC) encryption key. The <i>encryption-key</i> argument can be <b>0</b> (specifies that an unencrypted key follows), <b>6</b> (specifies that an advanced encryption scheme [AES] encrypted key follows), <b>7</b> (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.</p>
<b>Step 9</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Device(config)# exit</pre>	<p>Exits RADIUS server configuration mode and returns to global configuration mode.</p>
<b>Step 10</b>	<p><b>cts server test</b> {<i>ipv4-address   all</i>} {<b>deadtime</b> <i>seconds   enable   idle-time minutes</i>}</p>	<p>Configures the server-liveliness test for a specified RADIUS server or for all servers on the dynamic server list. By default, the test is enabled for all servers. The default <b>deadtime</b> is 20 seconds; the range is 1 to</p>

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device(config)# cts server test all idle-time 3</pre>	864000 seconds. The default <b>idle-time</b> is 60 seconds; the range is from 1 to 14400 seconds.
<b>Step 11</b>	<p><b>cts critical-authentication default peer-sgt</b> <i>peer-sgt-value</i> [<b>trusted</b>]</p> <p><b>Example:</b></p> <pre>Device(config)# cts critical-authentication default peer-sgt 5</pre>	<p>Configures the default peer security group tag (SGT) value.</p> <ul style="list-style-type: none"> <li>The peer-SGT value is used to tag new devices coming into the Cisco TrustSec network. This value must be configured before the Cisco TrustSec critical authentication mode is enabled. Use the <b>trusted</b> keyword to mark a device as trustworthy.</li> <li>The range for the <i>peer-SGT-value</i> argument is from 2 to 65519.</li> </ul>
<b>Step 12</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Device(config)# exit</pre>	Exits global configuration mode and returns to privileged EXEC mode.

## Troubleshooting Tips

- Use the **debug cts critical-auth events** and **debug cts critical-auth errors** commands in user EXEC or privileged EXEC mode to help troubleshoot issues with the critical authentication mode.
- Troubleshooting can also be done using the log messages that notify users when an interface enters critical authentication mode and when it reauthenticates.

## Verifying Critical Authentication

### SUMMARY STEPS

- enable**
- show running-config | section critical**
- show cts interface summary**

### DETAILED STEPS

- 
- Step 1**     **enable**  
Enables privileged EXEC mode.
- Enter your password if prompted.

**Example:**

```
Device> enable
```

**Step 2** **show running-config | section critical**

Displays the critical authentication configuration and the configured values.

**Example:**

```
Device# show running-config | section critical

cts critical-authentication default pmk
4444000000000000000000000000000000000000000000000000000000000000
cts critical-authentication default peer-sgt 10
cts critical-authentication fallback default
cts critical-authentication
```

**Step 3** **show cts interface summary**

Displays summary information about the configured Cisco TrustSec interfaces, including the Cisco TrustSec 802.1X links in critical authentication mode and their status.

**Example:**

```
Device# show cts interface summary
```

```
Global Dot1x feature is Enabled
```

## CTS Layer2 Interfaces

Interface	Mode	IFC-state	dot1x-role	peer-id	IFC-cache	Critical-Authentication
Gi3/0/2	DOT1X	OPEN	Authent	3k_3	valid	Cached

## CTS Layer3 Interfaces

Interface	IPv4 encap	IPv6 encap	IPv4 policy	IPv6 policy

# Configuration Examples for Cisco TrustSec Critical Authentication

## Example: Configuring Critical Authentication

```
Device> enable
Device# configure terminal
Device(config)# radius-server dead-criteria time 15 tries 3
Device(config)# radius-server deadtime 10
```

```

Device(config)# radius server RASERV-1
Device(config-radius-server)# address ipv4 172.20.254.4 auth-port 1812 acct-port 1813
Device(config-radius-server)# automate-tester username dummy
Device(config-radius-server)# pac key 7 mypackey
Device(config-radius-server)# exit
Device(config)# radius server RASERV-2
Device(config-radius-server)# address ipv4 172.20.254.8 auth-port 1645 acct-port 1646
Device(config-radius-server)# automate-tester username dummy
Device(config-radius-server)# pac key 7 mypackey
Device(config-radius-server)# exit
Device(config)# cts dot1x-server-timeout 30
Device(config)# cts dot1x-supp-timeout 30
Device(config)# cts server test all idle-time 3
Device(config)# cts critical-authentication default peer-sgt 5
Device(config)# cts critical-authentication
Device(config)# cts critical-authentication default pmk password123
Device(config)# cts cache nv-storage bootdisk:cache
Device(config)# cts critical-authentication fallback cached
Device(config)# exit

```

## Additional References for Cisco TrustSec Critical Authentication

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
Security commands	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Security Command Reference: Commands A to C</a></li> <li>• <a href="#">Cisco IOS Security Command Reference: Commands D to L</a></li> <li>• <a href="#">Cisco IOS Security Command Reference: Commands M to R</a></li> <li>• <a href="#">Cisco IOS Security Command Reference: Commands S to Z</a></li> </ul>
Cisco TrustSec configuration	“Cisco TrustSec Support for IOS” chapter in the <i>Cisco TrustSec Configuration Guide</i>

**Technical Assistance**

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p>

## Feature Information for Cisco TrustSec Critical Authentication

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 6: Feature Information for Cisco TrustSec Critical Authentication**

Feature Name	Releases	Feature Information
Cisco TrustSec Critical Authentication	Cisco IOS 15.2(2)E	<p>The Cisco TrustSec Critical Authentication feature ensures that the Network Device Admission Control (NDAC)-authenticated 802.1X links between Cisco TrustSec devices are in an open state even when the Authentication, Authorization, and Accounting (AAA) server is not reachable.</p> <p>In Cisco IOS Release 15.2(2)E, this feature is supported on the following platforms:</p> <ul style="list-style-type: none"> <li>• Cisco Catalyst 3750-X Series Switches</li> <li>• Cisco Catalyst 3560-X Series Switches</li> </ul> <p>The following command was introduced by this feature: <b>cts critical-authentication</b>.</p>