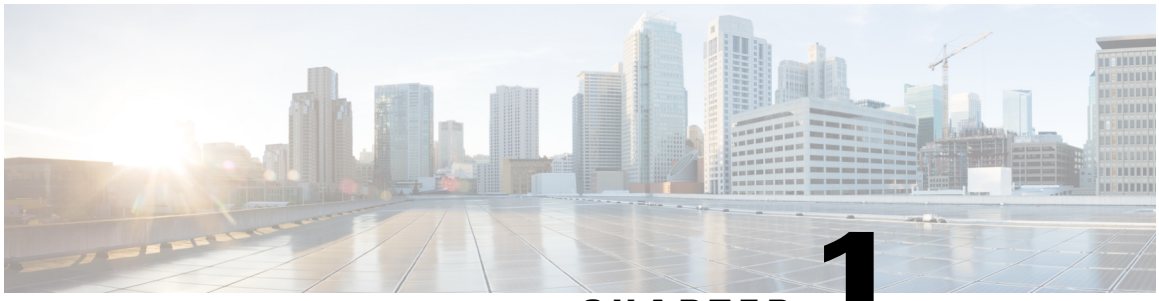
Cisco TrustSec Configuration Guide, Cisco IOS XE Release 3E

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

CONTENTS



CHAPTER 1

TrustSec SGT Handling: L2 SGT Imposition and Forwarding

First Published: July 25, 2011

Cisco TrustSec (CTS) builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and data-path replay protection mechanisms.

The TrustSec SGT Handling: L2 SGT Imposition and Forwarding feature allows the interfaces in a router to be manually enabled for CTS so that the router can insert the Security Group Tag (SGT) in the packet to be carried throughout the network in the CTS header.

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. An account on Cisco.com is not required.

Prerequisites for TrustSec SGT Handling: L2 SGT Imposition and Forwarding

The CTS network needs to be established with the following prerequisites before implementing the TrustSec SGT Handling: L2 SGT Imposition and Forwarding feature:

- Connectivity exists between all network devices
- Cisco Secure Access Control System (ACS) 5.1 operates with a CTS-SXP license
- Directory, DHCP, DNS, certificate authority, and NTP servers function within the network
- Configure the **retry open timer** command to a different value on different routers.

Information about TrustSec SGT Handling: L2 SGT Imposition and Forwarding

Security Groups and SGTs

A security group is a grouping of users, endpoint devices, and resources that share access control policies. Security groups are defined by the administrator in the ACS. As new users and devices are added to the Cisco TrustSec (CTS) domain, the authentication server assigns these new entities to appropriate security groups. CTS assigns to each security group a unique 16-bit security group number whose scope is global within a CTS domain. The number of security groups in the router is limited to the number of authenticated network entities. Security group numbers do not need to be manually configured.

Once a device is authenticated, CTS tags any packet that originates from that device with an SGT that contains the security group number of the device. The packet carries this SGT throughout the network within the CTS header. The SGT is a single label that determines the privileges of the source within the entire CTS domain. The SGT is identified as the source because it contains the security group of the source. The destination device is assigned a destination group tag (DGT).

Note The CTS packet tag does not contain the security group number of the destination device.

How to Configure TrustSec SGT Handling: L2 SGT Imposition and Forwarding

Manually Enabling TrustSec SGT Handling: L2 SGT Imposition and Forwarding on an Interface

Perform the following steps to manually enable an interface on the device for Cisco TrustSec (CTS) so that the device can add Security Group Tag (SGT) in the packet to be propagated throughout the network and to implement a static authorization policy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**GigabitEthernet***port* | **Vlan** *number*}
4. **cts manual**
5. **policy static sgt** *tag* [**trusted**]
6. **end**
7. **show cts interface** [**GigabitEthernet***port* | **Vlan** *number* | **brief** | **summary**]

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** {**GigabitEthernet***port*	**Vlan** *number*} **Example:** `Device(config)# interface gigabitethernet 0`	Enters the interface on which CTS SGT authorization and forwarding is enabled
Step 4	**cts manual** **Example:** `Device(config-if)# cts manual`	Enables the interface for CTS SGT authorization and forwarding, and enters CTS manual interface configuration mode.

	Command or Action	Purpose
Step 5	**policy static sgt** *tag* [**trusted**] **Example:** `Device(config-if-cts-manual)# policy static sgt 100 trusted`	Configures a static authorization policy for a CTS security group with a tagged packet that defines the trustworthiness of the SGT.
Step 6	**end** **Example:** `Device(config-if-cts-manual)# end`	Exits CTS manual interface configuration mode and enters privileged EXEC mode.
Step 7	**show cts interface** [**GigabitEthernet***port* | **Vlan** *number* | **brief** | **summary**] **Example:** `Device# show cts interface brief`	Displays CTS configuration statistics for the interface.

Example:

The following is sample output for the **show cts interface brief**command.

Cisco ASR 1000 Series Aggregation Services Routers and Cisco Cloud Services Router 1000V Series

```
Device# show cts interface brief

Global Dot1x feature is Disabled
 Interface GigabitEthernet0/1/0:
     CTS is enabled, mode:    MANUAL
     IFC state:               OPEN
     Interface Active for 00:00:40.386
     Authentication Status:   NOT APPLICABLE
         Peer identity:       "unknown"
         Peer's advertised capabilities: ""
     Authorization Status:    NOT APPLICABLE
     SAP Status:              NOT APPLICABLE
     Propagate SGT:           Enabled
     Cache Info:
         Cache applied to link : NONE
```

Cisco 4400 Series Integrated Services Routers

```
Device# show cts interface brief

Interface GigabitEthernet0/1/0
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             100
        Peer SGT assignment:  Trusted
```

Disabling CTS SGT Propagation on an Interface

Follow these steps to disable CTS SGT Propagation on an interface in an instance when a peer device is not capable of receiving an SGT.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**GigabitEthernet***port* | **Vlan** *number*}
4. **cts manual**
5. **no propagate sgt**
6. **end**
7. **show cts interface** [**GigabitEthernet***port* | **Vlan** *number* | **brief** | **summary**]

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** {**GigabitEthernet***port*	**Vlan** *number*} **Example:** `Device(config)# interface gigabitethernet 0`	Enters the interface on which CTS SGT authorization and forwarding is enabled
Step 4	**cts manual** **Example:** `Device(config-if)# cts manual`	Enables the interface for CTS SGT authorization and forwarding. CTS manual interface configuration mode is entered where CTS parameters can be configured.
Step 5	**no propagate sgt** **Example:** `Device(config-if-cts-manual)# no propagate sgt`	Disables CTS SGT propagation on an interface in situations where a peer device is not capable of receiving an SGT. **Note** CTS SGT propagation is enabled by default. The **propagate sgt** command can be used if CTS SGT propagation needs to be turned on again for a peer device. Once the **no propagate sgt** command is entered, the SGT tag is not added in the L2 header.
Step 6	**end** **Example:** `Device(config-if-cts-manual)# end`	Exits CTS manual interface configuration mode and enters privileged EXEC mode.

	Command or Action	Purpose

Step 7	**show cts interface** [**GigabitEthernet***port* | **Vlan** *number* | **brief** | **summary**]
	
	Example:
	
	`Device# show cts interface brief`
	`Global Dot1x feature is Disabled`
	`Interface GigabitEthernet0:`
	`CTS is enabled, mode: MANUAL`
	`IFC state: OPEN`
	`Authentication Status: NOT APPLICABLE`
	`Peer identity: "unknown"`
	`Peer's advertised capabilities: ""`
	`Authorization Status: NOT APPLICABLE`
	`SAP Status: NOT APPLICABLE`
	`Propagate SGT: Disabled`
	`Cache Info:`
	`Cache applied to link : NONE`
		Displays CTS configuration statistics to verify that CTS SGT propagation was disabled on interface.

Additional References for TrustSec SGT Handling: L2 SGT Imposition and Forwarding

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command 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 switches	Cisco TrustSec Switch Configuration Guide

MIBs

MIB	MIBs Link
CISCO-TRUSTSEC-SXP-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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

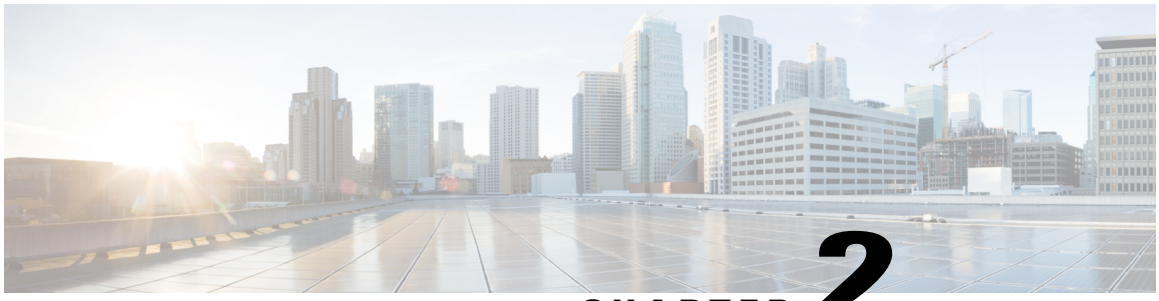
Feature Information for TrustSec SGT Handling: L2 SGT Imposition and Forwarding

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 . An account on Cisco.com is not required.

Table 1: Feature Information for TrustSec SGT Handling: L2 SGT Imposition and Forwarding

Feature Name	Releases	Feature Information
TrustSec SGT Handling: L2 SGT Imposition and Forwarding	Cisco IOS XE 3.3SE Cisco IOS XE 3.6E	This feature allows the interfaces in a router to be manually enabled for CTS so that the router can insert the Security Group Tag (SGT) in the packet to be carried throughout the network in the CTS header. In Cisco IOS XE Release 3.3SE, this feature is supported on the following platforms: • Catalyst 3850 Series Switches • Catalyst 3650 Series Switches • Cisco 5700 Series Wireless LAN Controllers In Cisco IOS XE Release 3.6E, this feature is supported on the following platforms: • Cisco Catalyst 4500E Supervisor Engine 7-E • Cisco Catalyst 4500E Supervisor Engine 7L-E • Cisco Catalyst 4500-X Series Switches • Cisco Catalyst 4500E Supervisor Engine 8-E • Cisco Catalyst 3850 Series Switches • Cisco Catalyst 3650 Series Switches The following commands were introduced or modified: **cts manual**, **policy static sgt**, **propagate sgt**, **show cts interface**.



CHAPTER 2

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

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. 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	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**cts sxp enable** **Example:** `Device(config)# cts sxp enable`	Enables the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4) on a network device.
Step 4	**cts sxp default password** **Example:** `Device(config)# cts sxp default password Cisco123`	(Optional) Specifies the Cisco TrustSec SGT SXP default password.

	Command or Action	Purpose
Step 5	**cts sxp default source-ip** **Example:** `Device(config)# cts sxp default source-ip 10.20.2.2`	(Optional) Configures the Cisco TrustSec SGT SXP source IPv4 address.
Step 6	**cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} **both** [**vrf** *vrf-name*] **Example:** `Device(config)# cts sxp connection peer 10.20.2.2 password default mode local both`	Configures the Cisco TrustSec SXP peer address connection for a bidirectional SXP configuration. The **both** keyword configures the bidirectional SXP configuration. The **source** 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. The **password** keyword specifies the password that Cisco TrustSec SXP uses for the connection using the following options: • **default—**Use the default Cisco TrustSec SXP password you configured using the **cts sxp default password** command. • **none—**A password is not used. The **mode** keyword specifies the role of the remote peer device: • **local—**The specified mode refers to the local device. • **peer—**The specified mode refers to the peer device. • **both—**Specifies that the device is both the speaker and the listener in the bidirectional SXP connection. The optional **vrf** keyword specifies the VRF to the peer. The default is the default VRF.
Step 7	**cts sxp speaker hold-time** *minimum-period* **Example:** `Device(config)# cts sxp speaker hold-time 950`	(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.
Step 8	**cts sxp listener hold-time** *minimum-period maximum-period* **Example:** `Device(config)# cts sxp listener hold-time 750 1500`	(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. **Note** The *maximum-period* value must be greater than or equal to the *minimum-period* value.

	Command or Action	Purpose
Step 9	**exit** **Example:** `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 2: 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	Cisco IOS Master Command 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 configuration	"Cisco TrustSec Support for IOS" chapter in the *Cisco TrustSec Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

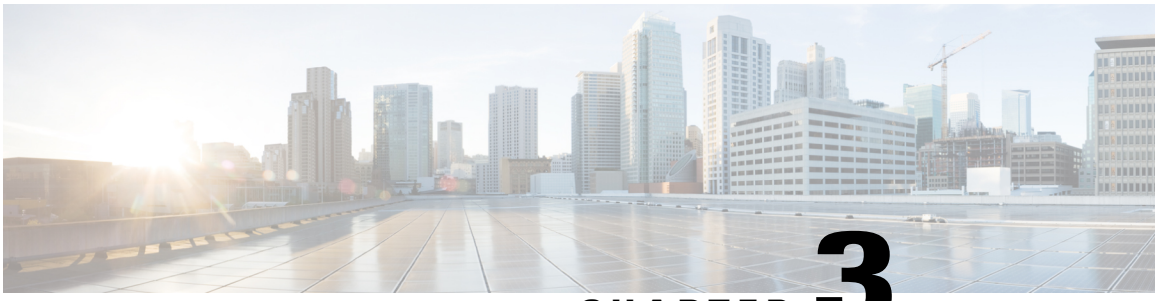
Feature Information for Bidirectional SXP Support

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 . An account on Cisco.com is not required.

Table 3: Feature Information for Bidirectional SXP Support

Feature Name	Releases	Feature Information
Bidirectional SXP Support	Cisco IOS XE 3.6E	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. In Cisco IOS XE Release 3.6E, this feature is supported on the following platforms: • Cisco Catalyst 4500E Supervisor Engine 7-E • Cisco Catalyst 4500E Supervisor Engine 7L-E • Cisco Catalyst 4500-X Series Switches • Cisco Catalyst 4500E Supervisor Engine 8-E • Cisco Catalyst 3850 Series Switches • Cisco Catalyst 3650 Series Switches The following command was introduced or modified: **cts sxp connection peer**.



CHAPTER 3

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

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. 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	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 2/5/3`	Enters interface configuration mode.
Step 4	**cts role-based enforcement** **Example:** `Device(config-if)# cts role-based enforcement`	Enables a security group access control list (SGACL) for the interface.
Step 5	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	**show running-config interface** *type number* **Example:** `Device# show running-config interface gigabitethernet 2/5/3`	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	Cisco IOS Master Command 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 switches	*Cisco TrustSec Switch Configuration Guide*

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

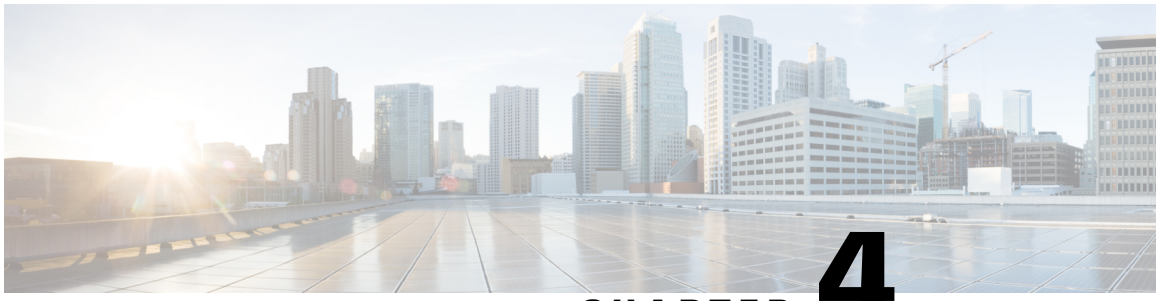
Feature Information for Enablement of Security Group ACL at Interface Level

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 . An account on Cisco.com is not required.

Table 4: 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 XE 3.6E	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. In Cisco IOS XE Release 3.6E, this feature is supported on the following platforms: • Cisco Catalyst 4500E Supervisor Engine 7-E • Cisco Catalyst 4500E Supervisor Engine 7L-E • Cisco Catalyst 4500-X Series Switches • Cisco Catalyst 4500E Supervisor Engine 8-E • Cisco Catalyst 3850 Series Switches • Cisco Catalyst 3650 Series Switches The following command was introduced: **cts role-based enforcement**.



CHAPTER 4

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

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. 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
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	**ipv6 snooping policy** *policy-name* **Example:** `Device(config)# ipv6 snooping policy policy1`	Generates IPv6 addresses for IP-SGT bindings and enters IPv6 snooping configuration mode.
Step 4	**tracking enable** **Example:** `Device(config-ipv6-snooping)# tracking enable`	Overrides the default tracking policy on a port.
Step 5	**exit** **Example:** `Device(config-ipv6-snooping)# exit`	Exits IPv6 snooping configuration mode and returns to global configuration mode.

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control subscriber** *control-policy-name* **Example:** `Device(config)# policy-map type control subscriber policy1`	Defines a control policy for subscriber sessions and enters control policy-map configuration mode.
Step 4	**event session-started match-all** **Example:** `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	*priority-number* **class always do-until-failure** **Example:** `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 *control-class-name* argument.
Step 6	*action-number* **authenticate using mab** **Example:** `Device(config-action-control-policymap)# 10 authenticate using mab`	Initiates the authentication of a subscriber session using the specified method.
Step 7	**end** **Example:** `Device(config-action-control-policymap)# end`	Exits action control policy-map configuration mode and returns to privileged EXEC mode.
Step 8	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 9	**interface gigabitethernet** *interface-number* **Example:** `Device(config)# interface gigabitehternet 1/0/1`	Enters interface configuration mode.
Step 10	**description** *interface-description* **Example:** `Device(config-if)# description downlink to ipv6 clients`	Describes the configured interface.

	Command or Action	Purpose
Step 11	**switchport access vlan** *vlan-id* **Example:** `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	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Sets the trunking mode to access mode.
Step 13	**ipv6 snooping attach-policy** *policy-name* **Example:** `Device(config-if)# ipv6 snooping attach-policy snoop`	Applies a policy to the IPv6 snooping feature.
Step 14	**access-session port-control auto** **Example:** `Device(config-if)# access-session port-control auto`	Sets the authorization state of a port.
Step 15	**mab eap** **Example:** `Device(config-if)# mab eap`	Uses Extensible Authentication Protocol (EAP) for MAC authentication bypass.
Step 16	**dot1x pae authenticator** **Example:** `Device(config-if)# dot1x pae authenticator`	Enables dot1x authentication on the port.
Step 17	**service-policy type control subscriber** *policy-name* **Example:** `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	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 19	**show cts role-based sgt-map all ipv6** **Example:** `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
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**cts role-based sgt-map vlan-list** *vlan-id* **sgt** *sgt-value* **Example:** `Device(config)# cts role-based sgt-map vlan-list 20 sgt 3`	Assigns an SGT value to the configured VLAN. **Note** The range of the *sgt-value* argument must be from 2 to 65519.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	**show cts role-based sgt-map all ipv6** **Example:** `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	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**show cts role-based sgt-map all**
	
	Example:
	`Device# show cts role-based sgt-map all`
	
	`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`
		Displays active IPv4 and IPv6 IP-SGT bindings.

Step 3	**show cts role-based sgt-map all ipv6**
	
	Example:
	`Device# show cts role-based sgt-map all ipv6`
	
	`Active IP-SGT Bindings Information`
		Displays active IPv6 IP-SGT bindings.

	Command or Action	Purpose
	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	

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 gigabitehternet 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	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
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
Security group ACL	"Enablement of Security Group ACL at Interface Level" module of *Cisco TrustSec Configuration Guide*
IEEE 802.1X authentication	"Configuring IEEE 802.1X Port-Based Authentication" module of *802.1X Authentication Services Configuration Guide*
MAC Authentication Bypass	"Configuring MAC Authentication Bypass" module of *Authentication Authorization and Accounting Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

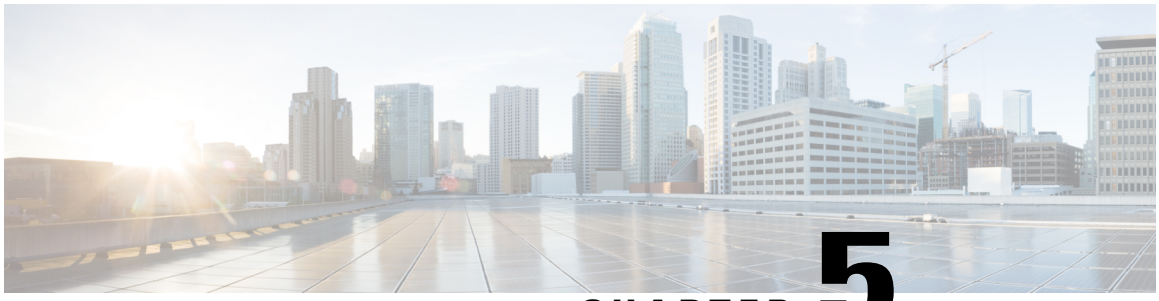
Feature Information for IPv6 Support for SGT and SGACL

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 . An account on Cisco.com is not required.

Table 5: Feature Information for IPv6 Support for SGT and SGACL

Feature Name	Releases	Feature Information
IPv6 Support for SGT and SGACL	Cisco IOS XE 3.6E	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). In Cisco IOS XE Release 3.6E, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Catalyst 3850 Series Switches • Catalyst 4500E Supervisor Engine 7L-E • Catalyst 4500-X Series Switches • Catalyst 4900 Series Switches • Catalyst 4500E Supervisor Engine 8-E The following command was modified: **cts role-based sgt-map**.



CHAPTER 5

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

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.

	Command or Action	Purpose
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** *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).

	Command or Action	Purpose
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.
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).

	Command or Action	Purpose
Step 7	**exit** **Example:** `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	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 . An account on Cisco.com is not required.

Table 6: 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 Cisco IOS XE Release 3.6E	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. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. The following commands were introduced or modified: **cts dot1x**, **propagate sgt (config-if-cts-dot1x)** , **sap mode-list**, **timer reauthentication**.