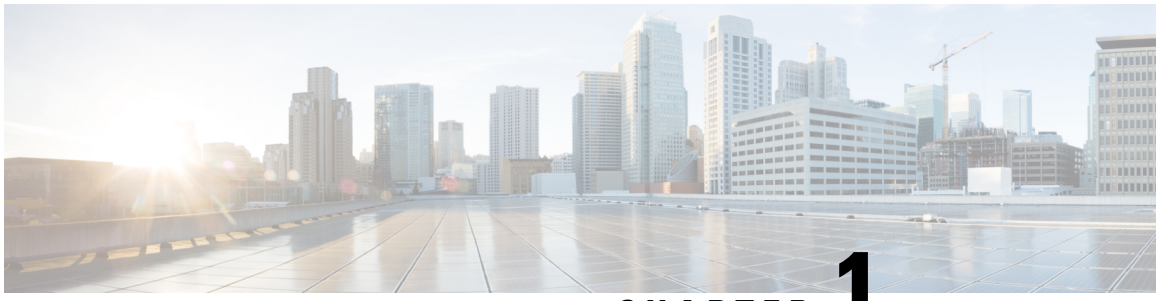
Cisco TrustSec Configuration Guide, Cisco IOS Release 15SY

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

Cisco TrustSec Support for IOS

Cisco TrustSec (CTS) is a system that provides security for CTS-enabled network devices at each routing hop. In this system, each network device works to authenticate and authorize its neighbor devices and next applies some level of security (group tagging, role-based access control lists (ACLs), encryption, and so on) to traffic between the devices.

The Cisco TrustSec Support for IOS feature involves using Secure RADIUS to prescribe a process of authentication, authorization, session association, encryption, and traffic filtering. Secure RADIUS uses automatic Protected Access Credential (PAC) provisioning as a low overhead method to send PAC metadata and control information to clients. PAC provisioning is used with Extensible Authentication Protocol-Flexible Authentication through Secure Tunneling (EAP-FAST) to establish a Transport Layer Security (TLS) tunnel in which client credentials are verified.

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 Cisco TrustSec Support for IOS

To use the Cisco TrustSec functionality on your existing router, ensure that you have purchased a Cisco TrustSec security license. If the router is being ordered and needs the Cisco TrustSec functionality, ensure that this license is preinstalled on your router before it is shipped to you.

The Cisco Identity Services Engine 1.0 is required for authentication. The Secure Access Control Server (ACS) Express Appliance server can also be used for authentication; however, not all ACS features are supported by CTS.

Restrictions for Cisco TrustSec Support for IOS

- The Cisco TrustSec Support for IOS feature is supported on the Cisco Integrated Services Router Generation 2 (ISR G2) only.
- EAP-FAST only supports Phase 0 where the PAC is initially distributed to the client. EAP-FAST Phase 1 (the PAC is used to establish a secure tunnel) and Phase 2 (client is authenticated through the secure tunnel) are not supported.

Information About Cisco TrustSec Support for IOS

Cisco TrustSec Device Enrollment

Any device that participates in the CTS network requires it to be authenticated and trusted. New devices that connect to the CTS network use an enrollment process to obtain CTS authentication credentials and receive general information about the CTS environment to facilitate the authentication process. Device enrollment can happen either directly with an Authentication Server (AS) provided the device has L3 connectivity to AS or through a peer Authenticator (AT) device, such as a switch or router that facilitates enrollment with an AS.

Access switches or routers are the authentication points in typical branch access scenarios and have direct connectivity to the AS. They authenticate endpoints through EAP-FAST Phase 0 for dynamic PAC provisioning or RADIUS and EAP exchange. When endpoints are successfully authenticated, they receive user-specific AAA attributes that include the SGT, which in turn is relayed to a router using SXP. The router initiates EAP-FAST Phase 0 exchange with the available AS and obtains a PAC. This is accomplished by a local PAC-provisioning driver, which acts as a pass-through authenticator to the supplicant EAP-FAST engine running on the router.

Secure RADIUS

The RADIUS protocol requires a secret to be shared between a client and a server. Shared secrets are used to verify that RADIUS messages are sent by a RADIUS enabled device that is configured with the same shared secret. Shared secrets also verify that the RADIUS message has not been modified in transit (message integrity). The message integrity is checked by including the Message Authenticator attribute in the RADIUS messages. This attribute is a Hash-based Message Authentication Code-Message Digest 5 (HMAC-MD5) of the entire radius message using the shared secret as the key. The shared secret is also used to encrypt some RADIUS attributes, such as User-Password and Tunnel-Password.

EAP-FAST

EAP-FAST is a publicly accessible IEEE 802.1X extensible authentication protocol type that is used to support customers who cannot enforce a strong password policy. EAP-FAST is used for the following reasons:

- Digital certificates are not required.
- A variety of database types for usernames and passwords are supported.
- Password expiration and change are supported.
- EAP-FAST is flexible, easy to deploy and manage.

Note Lightweight Directory Access Protocol (LDAP) users cannot be automatically PAC provisioned and must be manually provisioned.

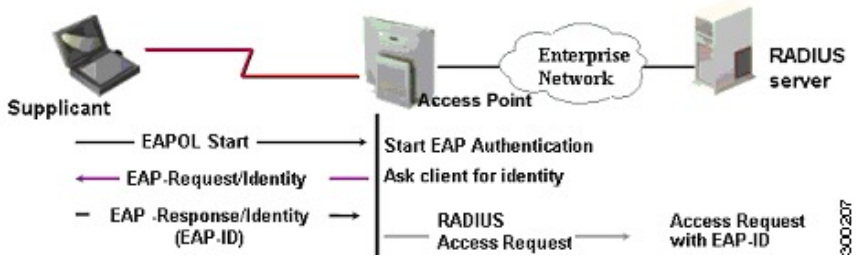
EAP-FAST comprises three basic phases, but only Phase 0 is supported. Phase 0 initially distributes the PAC to the client device.

Note Unsupported EAP-FAST Phase 1 uses the PAC to establish a secure tunnel and Phase 2 authenticates the client through a secure tunnel.

Phase 0 or auto-provisioning (also called in-band provisioning) component of EAP-FAST permits the secure distribution of the user PAC to each device. With some other authentication protocols, it is necessary to establish a network connection or manually install a file in order to distribute credentials to the device. Phase 0 in EAP-FAST permits a PAC to be distributed to the device during an encrypted session after the device's credentials are authenticated. This device authentication uses a challenge-handshake protocol to authenticate the device and to validate the server response. This authentication mechanism guards against potential interception and reforwarding of provisioning requests for the purpose of intercepting a user PAC.

The end result of Phase 0 is PAC distribution. After successful PAC distribution, the server issues an authentication failure to the access point and the device is disassociated from the network. Then the device reinitiates an EAP-FAST authentication with the network using the newly provisioned PAC and the device's credentials.

The figure below shows an overview of EAP-FAST authentication.



Protected Access Credential (PAC)

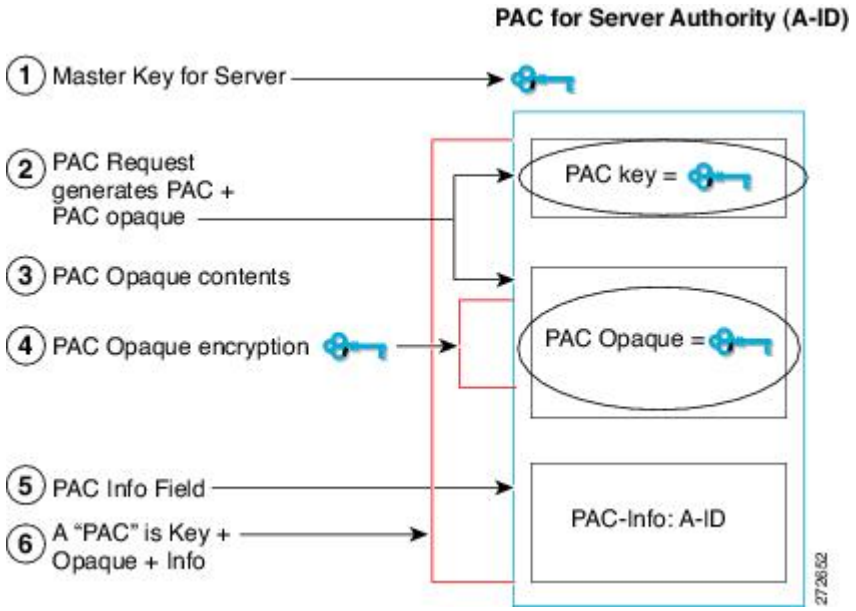
The PAC is a unique shared credential used to mutually authenticate client and server. It is associated with a specific client username and a server authority identifier (A-ID). A PAC removes the need for Public Key Infrastructure (PKI) and digital certificates.

Creating a PAC consists of the following steps:

1. Server A-ID maintains a local key (master key) that is only known by the server.
2. When a client, which is referred to in this context as an initiator identity (I-ID), requests a PAC from the server, the server generates a randomly unique PAC key and PAC-Opaque field for this client.
3. The PAC-Opaque field contains the randomly generated PAC key along with other information such as an I-ID and key lifetime.
4. PAC Key, I-ID, and Lifetime in the PAC-Opaque field are encrypted with the master key.
5. A PAC-Info field that contains the A-ID is created.
6. The PAC is distributed or imported to the client automatically.

Note The server does not maintain the PAC or the PAC key, enabling the EAP-FAST server to be stateless.

The figure below describes the PAC's construction. A PAC consists of the PAC-Opaque, PAC Key, and PAC-Info fields. The PAC-Info field contains the A-ID.



PAC Provisioning

In Secure RADIUS, the PAC key is provisioned into each device during authentication to derive the shared secret. Since the RADIUS ACS does not store the PAC key for each device, the clients must also send an

additional RADIUS attribute containing the PAC-Opaque field, which is a variable length field that can only be interpreted by the server to recover the required information and validate the peer's identity and authentication. For example, the PAC-Opaque field may include the PAC key and the PAC's peer identity.

The PAC-Opaque field format and contents are specific to the PAC server on which it is issued. The RADIUS server obtains the PAC Key from the PAC-Opaque field and derives the shared secret the same way clients do. Secure RADIUS only modifies the way shared secret is derived and not its usage.

EAP-FAST Phase 0 is used to automatically provision a client with a PAC.

Deploying Devices in High Availability Setup

Perform the following steps when deploying devices in an HA setup:

1. Clear the credentials from all the devices which are part of the HA setup.
2. Boot the stack setup and establish the device roles (active, standby, and members).
3. Configure the credentials on the active device. Use the **cts credentials id** *id* **password** *password* command to configure the credentials.

Note While adding a new device to an existing stack, ensure that you clear the credentials on the fresh device and then add it to the existing stack setup.

How to Provide Cisco TrustSec Support for IOS

Installing the Cisco TrustSec Security License

To use the Cisco TrustSec functionality on your existing router, ensure that you have purchased a Cisco TrustSec security license. If the router is being ordered and needs the Cisco TrustSec functionality, ensure that this license is preinstalled on your router before it is shipped to you.

Perform this task to manually install the Cisco TrustSec security license:

SUMMARY STEPS

1. **enable**
2. **license install** *stored-location-url*
3. **license boot module** *module-name* **technology-package** *package-name*
4. **reload**
5. **show license udi**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**license install** *stored-location-url* **Example:** `Router# license install tftp://mytftpserver/mylicensefile.lic`	Installs the license on the router.
Step 3	**license boot module** *module-name* **technology-package** *package-name* **Example:** `Router# license boot module c2900 technology-package securityk9`	Specifies the security software license to boot. • The *module-name* argument is the router or module to be configured. • The **technology-package** keyword and *package-name* argument upgrades the security software license package from which the router should boot. • Accept the end-user license agreement when prompted.
Step 4	**reload** **Example:** `Router# reload`	Restarts the router to enable the new software with the securityk9 license containing the Cisco TrustSec license.
Step 5	**show license udi** **Example:** `Router# show license udi`	Displays all the UDI values that are licensed in the system, and verifies that your Cisco TrustSec security license has installed successfully.

What to do next

See the "Configuring Cisco TrustSec Credentials" section to configure the basic parameters needed to make Cisco TrustSec operational on your router.

Configuring Cisco TrustSec Credentials

Perform this task for CTS to work on your router.

SUMMARY STEPS

1. **enable**
2. **cts credentials id** *cts-id* **password** *password*
3. **configure terminal**
4. **aaa new-model**
5. **aaa authentication dot1x default group radius**
6. **cts authorization list network** *list-name*
7. **aaa authorization network** *list-name* **group radius**

8. **exit**
9. **show cts server-list**
10. **show cts credentials**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**cts credentials id** *cts-id* **password** *password* **Example:** `Router# cts credentials id ctsid password abcd`	Specifies the CTS device ID for this device to use when authenticating with other CTS devices with EAP-FAST because CTS requires each device in the network to identity itself uniquely. • The *cts-id* argument has a maximum length of 32 characters and is case sensitive. • The *password* argument is the password for this device to use when authenticating with other CTS devices with EAP-FAST.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 4	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables new RADIUS and AAA access control commands and functions and disables old commands.
Step 5	**aaa authentication dot1x default group radius** **Example:** `Router(config)# aaa authentication dot1x default group radius`	Specifies that RADIUS servers are used for authentication on interfaces running IEEE 802.1X.
Step 6	**cts authorization list network** *list-name* **Example:** `Router(config)# cts authorization list network cts-mlist`	Specifies a list of AAA servers for the CTS seed device to use.
Step 7	**aaa authorization network** *list-name* **group radius** **Example:**	Specifies the CTS authorization list name for all network-related service requests from RADIUS servers.

	Command or Action	Purpose
	`Router(config)# aaa authorization network cts-mlist group radius`	
Step 8	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 9	**show cts server-list** **Example:** `Router# show cts server-list`	Displays the RADIUS the server configurations for CTS seed devices.
Step 10	**show cts credentials** **Example:** `Router# show cts credentials`	Displays the CTS device ID. The stored password is never displayed.

Configuring Secure RADIUS Automatic PAC Provisioning

In seed devices, the PAC-Opaque field has to be provisioned so that all RADIUS exchanges can use the PAC-Opaque field to make the server it communicates with capable of automatic PAC provisioning. All non-seed devices obtain the PAC-Opaque field during the authentication phase of a link initialization.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius server** *name*
5. **address ipv4** *hostname* [**acct-port** *port* | **alias** *name* | **auth-port** *port* [**acct-port** *port*]]
6. **pac key** *encryption-key*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables new RADIUS and AAA access control commands and functions and disables old commands.
Step 4	**radius server** *name* **Example:** `Router(config)# radius server myserver`	Specifies a name for the RADIUS server PAC provisioning configuration and enters RADIUS server configuration mode.
Step 5	**address ipv4** *hostname* [**acct-port** *port* | **alias** *name* | **auth-port** *port* [**acct-port** *port*]] **Example:** `Router(config-radius-server)# address ipv4 10.0.0.1 acct-port 1813 auth-port 1812`	Configures the RADIUS server accounting and authentication parameters for PAC provisioning. • The *hostname* argument is the RADIUS server IPv4 address or Domain Name System (DNS) name. • The **acct-port** keyword and *port* argument specify the UDP port for the RADIUS accounting server for accounting requests. The default port is 1646. • The **alias** keyword and *name* argument specify an alias for this server. The alias can be an IPv4 address or host name. Up to 8 aliases can be configured for this server. • The **auth-port** keyword and *port* argument specify the UDP port for RADIUS authentication server. The default port is 1645.
Step 6	**pac key** *encryption-key* **Example:** `Router(config-radius-server)# pac key 7 mypackey`	Specifies the PAC encryption key (overrides the default). • The *encryption-key* can be **0** (specifies that an unencrypted keys follows), **7** (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.

What to do next

Note Automatic PAC Provisioning can also be triggered by Secure RADIUS when the server has no PAC or when an Access-Reject message is received from the Autonomous System (AS) says “PAC Expired”.

Configuration Examples for Cisco TrustSec Support for IOS

Configuring the CTS Device ID and Password: Example

The following example configures himalaya and cisco as the CTS device ID and password:

```
Router# cts credentials id himalaya password cisco

CTS device ID and password have been inserted in the local keystore. Please make sure that
 the same ID and password are configured in the server database.
```

The following example changes the CTS device ID and password to atlas and cisco123:

```
Router# cts credentials id atlas password cisco123
A different device ID is being configured.
This may disrupt connectivity on your CTS links.
Are you sure you want to change the Device ID? [confirm] y
TS device ID and password have been inserted in the local keystore. Please make sure that
the same ID and password are configured in the server database.
```

The following example displays the CTS device ID and password state:

```
Router# show cts credentials
CTS password is defined in keystore, device-id = atlas
```

Configuring AAA for a CTS Seed Device and Automatic PAC Provisioning: Example

The following example configures the AAA configuration for a CTS seed device and automatic PAC provisioning on the router:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# aaa authorization network cts-mlist group radius
Router(config)# cts authorization list cts-mlist
Router(config)# aaa accounting dot1x default start-stop group radius
Router(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key AbCe1234
Router(config)# radius-server vsa send authentication
Router(config)# dot1x system-auth-control
Router(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
EAP Flexible Authentication via Secured Tunnel (EAP-FAST) authentication protocol deployment in wireless networks	EAP-FAST Deployment Guide
Cisco TrustSec switches	Cisco TrustSec Switch Configuration Guide

MIBs

Description	Link
CISCO-TRUSTSEC-SXP-MIB	To locate and download MIBs for selected platforms, Cisco IOS 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

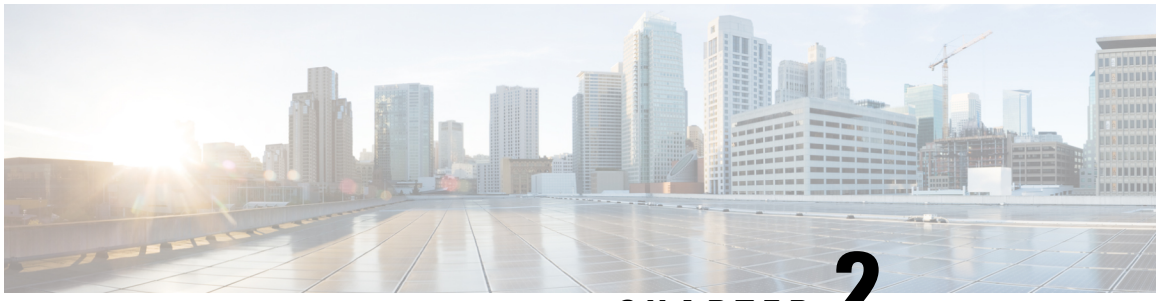
Feature Information for Cisco TrustSec Support for IOS

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Cisco TrustSec Support for IOS

Feature Name	Releases	Feature Information
Support for Cisco TrustSec Solution on ISR Platforms.	12.2(33)SXI 15.2(2)T	This feature involves using secure RADIUS to prescribe a process of authentication, authorization, session association, encryption, and traffic filtering. Secure RADIUS uses automatic PAC provisioning as a low overhead method to send PAC metadata and control information to clients. PAC provisioning is used with EAP-FAST to establish a TLS tunnel in which client credentials are verified. In Cisco IOS Release 12.2(33)SXI, this feature was introduced on Cisco IOS software. This feature was integrated into Cisco IOS Release 15.2(2)T software. The following commands were introduced or modified: **address ipv4 (config-radius-server)**, **cts authorization list network**, **pac keyradius-server host**, **show cts credentials**, **show cts server-list**.



CHAPTER 2

Cisco TrustSec Subnet to SGT Mapping

Subnet to security group tag (SGT) mapping binds an SGT to all host addresses of a specified subnet. Once this mapping is implemented, Cisco TrustSec imposes the SGT on any incoming packet that has a source IP address which belongs to the specified subnet.

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 Cisco TrustSec Subnet to SGT Mapping

- An IPv4 subnetwork with a /31 prefix cannot be expanded.
- Subnet host addresses cannot be bound to SGTs when the **cts sxp mapping network-map** command *bindings* argument is less than the total number of subnet hosts in the specified subnets or when the number of bindings is 0.
- IPv6 expansions and propagation only occurs when SXP speaker and listener are running SXPv3, or more recent versions.

Information About Cisco TrustSec Subnet to SGT Mapping

In IPv4 networks, SXPv3, and more recent versions, can receive and parse subnet network address/prefix strings from SXPv3 peers. Earlier SXP versions convert the subnet prefix into its set of host bindings before exporting them to an SXP listener peer.

For example, the IPv4 subnet 198.1.1.0/29 is expanded as follows (only 3 bits for host addresses):

- Host addresses 198.1.1.1 to 198.1.1.7 are tagged and propagated to SXP peer.
- Network and broadcast addresses 198.1.1.0 and 198.1.1.8 are not tagged and not propagated.

Note To limit the number of subnet bindings SXPv3 can export, use the **cts sxp mapping network-map** global configuration command.

Subnet bindings are static, which means that active hosts are not learned. They can be used locally for SGT imposition and SGACL enforcement. Packets tagged by subnet to SGT mapping can be propagated on Layer 2 or Layer 3 TrustSec links.

Note For IPv6 networks, SXPv3 cannot export subnet bindings to SXPv2 or SXPv1 peers.

How to Configure Cisco TrustSec Subnet to SGT Mapping

Configuring Subnet to SGT Mapping

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp mapping network-map** *bindings*
4. **cts role-based sgt-map** *ipv4-address* **sgt** *number*
5. **cts role-based sgt-map** *ipv6-address::prefix* **sgt** *number*
6. **exit**
7. **show running-config | include** *search-string*
8. **show cts sxp connections**
9. **show cts sxp sgt-map**
10. **copy running-config startup-config**

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 mapping network-map** *bindings* **Example:** `Device(config)# cts sxp mapping network-map 10000`	Configures the subnet to SGT mapping host count constraint. The *bindings* argument specifies the maximum number of subnet IP hosts from 0 to 65,535 that can be bound to SGTs and exported to the SXP listener. The default is 0 (no expansions performed).
Step 4	**cts role-based sgt-map** *ipv4-address* **sgt** *number* **Example:** `Device(config)# cts role-based sgt-map 10.10.10.10/29 sgt 1234`	(IPv4) Specifies an IPv4 subnet in CIDR notation. The number of bindings specified in step 3 should match or exceed the number of host addresses in the subnet (excluding network and broadcast addresses). The **sgt** *number* keyword pair specifies the SGT number that is to be bound to every host address in the specified subnet. • *ipv4-address*—Specifies the IPv4 network address in dotted decimal notation. • *prefix*—(0 to 30). Specifies the number of bits in the network address. • **sgt** *number* (0-65,535). Specifies the SGT number.
Step 5	**cts role-based sgt-map** *ipv6-address::prefix* **sgt** *number* **Example:** `Device(config)# cts role-based sgt-map 2020::/64 sgt 1234`	(IPv6) Specifies an IPv6 subnet in hexadecimal notation. The number of bindings specified in step 3 should match or exceed the number of host addresses in the subnet (excluding network and broadcast addresses). The **sgt** *number* keyword pair specifies the SGT number that is to be bound to every host address in the specified subnet. • *ipv6-address*—Specifies the IPv4 network address in dotted decimal notation. • *prefix*—(0 to 30). Specifies the number of bits in the network address. • **sgt** *number*—(0-65,535). Specifies the SGT number.
Step 6	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

	Command or Action	Purpose

Step 7	**show running-config** | **include** *search-string*
	Example:
	`Device# show running-config | include sgt 1234`
	`Device# show running-config | include network-map`
		Verifies that the **cts role-based sgt-map** and the **cts sxp mapping network-map** commands are in the running configuration.

Step 8	**show cts sxp connections** **Example:** `Device# show cts sxp connections`	Displays the SXP speaker and listener connections with their operational status.
Step 9	**show cts sxp sgt-map** **Example:** `Device# show cts sxp sgt-map`	Displays the IP to SGT bindings exported to the SXP listeners.
Step 10	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Cisco TrustSec Subnet to SGT Mapping: Examples

The following example shows how to configure IPv4 Subnet to SGT Mapping between two devices running SXPv3 (Device 1 and Device 2):

Configure SXP speaker/listener peering between Device 1 (10.1.1.1) and Device 2 (10.2.2.2).

```
Device1# configure terminal
Device1(config)# cts sxp enable
Device1(config)# cts sxp default source-ip 10.1.1.1
Device1(config)# cts sxp default password 1syzygy1
Device1(config)# cts sxp connection peer 10.2.2.2 password default mode local speaker
```

Configure Device 2 as SXP listener of Device 1.

```
Device2(config)# cts sxp enable
Device2(config)# cts sxp default source-ip 10.2.2.2
Device2(config)# cts sxp default password 1syzygy1
Device2(config)# cts sxp connection peer 10.1.1.1 password default mode local listener
```

On Device 2, verify that the SXP connection is operating:

```
Device2# show cts sxp connections brief | include 10.1.1.1

     10.1.1.1          10.2.2.2          On               3:22:23:18 (dd:hr:mm:sec)
```

Configure the subnetworks to be expanded on Device 1.

```
Device1(config)# cts sxp mapping network-map 10000
Device1(config)# cts role-based sgt-map 10.10.10.0/30 sgt 101
Device1(config)# cts role-based sgt-map 10.11.11.0/29 sgt 11111
Device1(config)# cts role-based sgt-map 172.168.1.0/28 sgt 65000
```

On Device 2, verify the subnet to SGT expansion from Device 1. There should be two expansions for the 10.10.10.0/30 subnetwork, six expansions for the 10.11.11.0/29 subnetwork, and 14 expansions for the 172.168.1.0/28 subnetwork.

```
Device2# show cts sxp sgt-map brief | include 101|11111|65000

IPv4,SGT: <10.10.10.1 , 101>
IPv4,SGT: <10.10.10.2 , 101>
IPv4,SGT: <10.11.11.1 , 11111>
IPv4,SGT: <10.11.11.2 , 11111>
IPv4,SGT: <10.11.11.3 , 11111>
IPv4,SGT: <10.11.11.4 , 11111>
IPv4,SGT: <10.11.11.5 , 11111>
IPv4,SGT: <10.11.11.6 , 11111>
IPv4,SGT: <172.168.1.1 , 65000>
IPv4,SGT: <172.168.1.2 , 65000>
IPv4,SGT: <172.168.1.3 , 65000>
IPv4,SGT: <172.168.1.4 , 65000>
IPv4,SGT: <172.168.1.5 , 65000>
IPv4,SGT: <172.168.1.6 , 65000>
IPv4,SGT: <172.168.1.7 , 65000>
IPv4,SGT: <172.168.1.8 , 65000>
IPv4,SGT: <172.168.1.9 , 65000>
IPv4,SGT: <172.168.1.10 , 65000>
IPv4,SGT: <172.168.1.11 , 65000>
IPv4,SGT: <172.168.1.12 , 65000>
IPv4,SGT: <172.168.1.13 , 65000>
IPv4,SGT: <172.168.1.14 , 65000>
```

Verify the expansion count on Device 1:

```
Device1# show cts sxp sgt-map

IP-SGT Mappings expanded:22
There are no IP-SGT Mappings
```

Save the configurations on Device 1 and Device 2 and exit global configuration mode.

```
Device1(config)# copy running-config startup-config
Device1(config)# exit

Device2(config)# copy running-config startup-config
Device2(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

Related Topic	Document Title
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

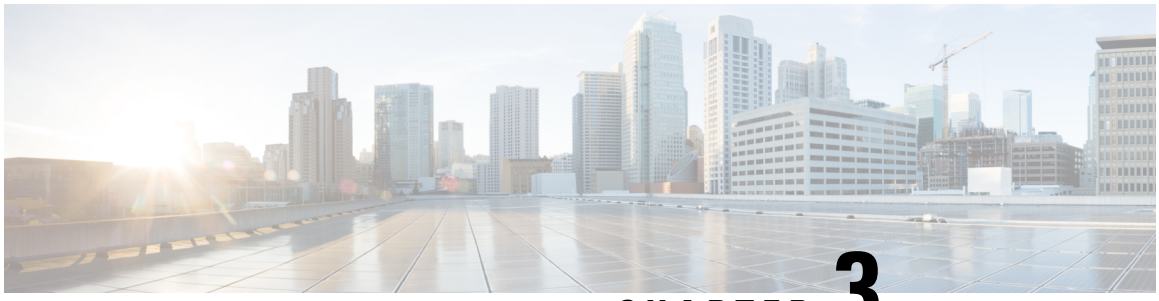
Feature Information for Cisco TrustSec Subnet to SGT Mapping

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for Cisco TrustSec Subnet to SGT Mapping

Feature Name	Releases	Feature Information
Cisco TrustSec Subnet to SGT Mapping	15.1(1)SY 15.4(2)T	Subnet to security group tag (SGT) mapping binds an SGT to all host addresses of a specified subnet. Once this mapping is implemented, Cisco TrustSec imposes the SGT on any incoming packet that has a source IP address which belongs to the specified subnet. The following command was introduced: **cts sxp mapping network-map**.



CHAPTER 3

Cisco TrustSec SGT Exchange Protocol IPv4

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 Security Group Tag (SGT) Exchange Protocol (SXP) is one of several protocols that supports CTS and is referred to in this document as CTS-SXP. CTS-SXP is a control protocol for propagating IP-to-SGT binding information across network devices that do not have the capability to tag packets. CTS-SXP passes IP to SGT bindings from authentication points to upstream devices in the network. This process allows security services on switches, routers, or firewalls to learn identity information from access devices.

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 Cisco TrustSec SGT Exchange Protocol IPv4

The CTS-SXP network needs to be established before implementing SXP. The CTS-SXP network has the following prerequisites:

- To use the Cisco TrustSec functionality on your existing router, ensure that you have purchased a Cisco TrustSec security license. If the router is being ordered and needs the Cisco TrustSec functionality, ensure that this license is pre-installed on your router before it is shipped to you.
- CTS-SXP software runs on all network devices
- Connectivity exists between all network devices
- The Cisco Identity Services Engine 1.0 is required for authentication. The Secure Access Control Server (ACS) Express Appliance server can also be used for authentication, however not all ACS features are supported by CTS. ACS 5.1 operates with a CTS-SXP license.
- Configure the **retry open timer** command to a different value on different routers.

Restrictions for Cisco TrustSec SGT Exchange Protocol IPv4

- The Cisco TrustSec Support for IOS feature is supported on the Cisco Integrated Services Router Generation 2 (ISR G2) only.
- CTS-SXP is supported only on physical interfaces, not on logical interfaces.
- CTS-SXP does not support IPv6.
- If the default password is configured on a router, the connection on that router should configure the password to use the default password. If the default password is not configured, the connection on that router should configure to not use the password configuration. The configuration of the password option should be consistent across the deployment network.

Information About Cisco TrustSec SGT Exchange Protocol IPv4

Security Group Tagging

CTS-SXP uses the device and user credentials acquired during authentication for classifying the packets by security groups (SGs) as they enter the network. This packet classification is maintained by tagging packets on ingress to the CTS-SXP network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The Security Group Tag (SGT) allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic.

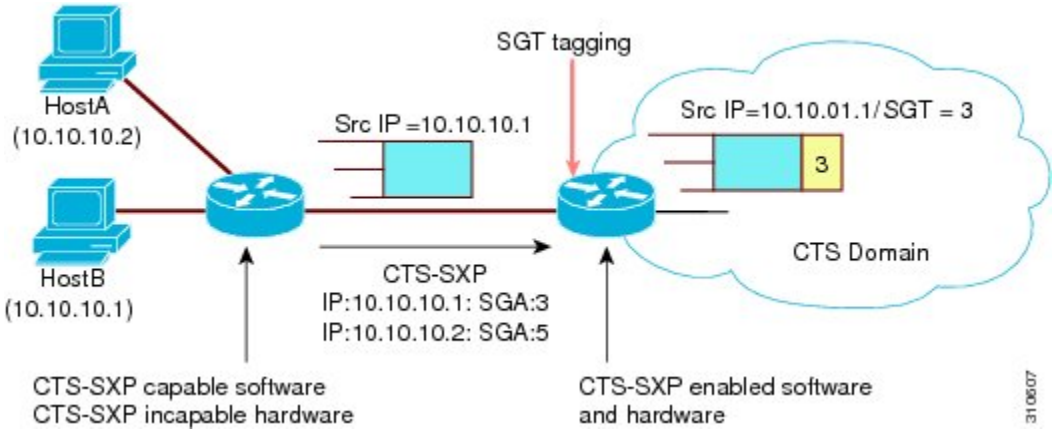
Using CTS-SXP for SGT Propagation Across Legacy Access Networks

Tagging packets with SGTs requires hardware support. There may be devices in the network that can participate in CTS authentication, but lack the hardware capability to tag packets with SGTs. However, if CTS-SXP is used, then these devices can pass IP-to-SGT mappings to a CTS peer device that has CTS-capable hardware.

CTS-SXP typically operates between ingress access layer devices at the CTS domain edge and distribution layer devices within the CTS domain. The access layer device performs CTS authentication of external source devices to determine the appropriate SGTs for ingress packets. The access layer device learns the IP addresses of the source devices using IP device tracking and (optionally) DHCP snooping, then uses CTS-SXP to pass the IP addresses of the source devices along with their SGTs to the distribution switches. Distribution switches

with CTS-capable hardware can use this IP-to-SGT mapping information to tag packets appropriately and to enforce Security Group Access Control List (SGACL) policies as shown in the figure below. An SGACL associates an SGT with a policy. The policy is enforced when SGT-tagged traffic egresses the CTS domain.

Figure 1: How CTS-SXP Propagates SGT Information



You must manually configure a CTS-SXP connection between a peer without CTS hardware support and a peer with CTS hardware support. The following tasks are required when configuring the CTS-SXP connection:

- If CTS-SXP data integrity and authentication are required, the same CTS-SXP password can be configured on both peer devices. The CTS-SXP password can be configured either explicitly for each peer connection or globally for the device. Although a CTS-SXP password is not required it is recommended.
- Each peer on the CTS-SXP connection must be configured as either a CTS-SXP speaker or CTS-SXP listener. The speaker device distributes the IP-to-SGT mapping information to the listener device.
- A source IP address can be specified to use for each peer relationship or a default source IP address can be configured for peer connections where a specific source IP address is not configured. If no source IP address is specified, then the device uses the interface IP address of the connection to the peer.

CTS-SXP allows multiple hops. That is, if the peer of a device lacking CTS hardware support also lacks CTS hardware support, the second peer can have a CTS-SXP connection to a third peer, continuing the propagation of the IP-to-SGT mapping information until a hardware-capable peer is reached. A device can be configured as a CTS-SXP listener for one CTS-SXP connection as a CTS-SXP speaker for another CTS-SXP connection.

A CTS device maintains connectivity with its CTS-SXP peers by using the TCP keepalive mechanism. To establish or restore a peer connection, the device repeatedly attempts the connection setup by using the configured retry period until the connection is successful or until the connection is removed from the configuration.

VRF-Aware CTS-SXP

The CTS-SXP implementation of Virtual Routing and Forwarding (VRF) binds a CTS-SXP connection with a specific VRF. It is assumed that the network topology is correctly configured for Layer 2 or Layer 3 VPNs, and that all VRFs are configured before enabling CTS-SXP.

CTS-SXP VRF support can be summarized as follows:

- Only one CTS-SXP connection can be bound to one VRF.

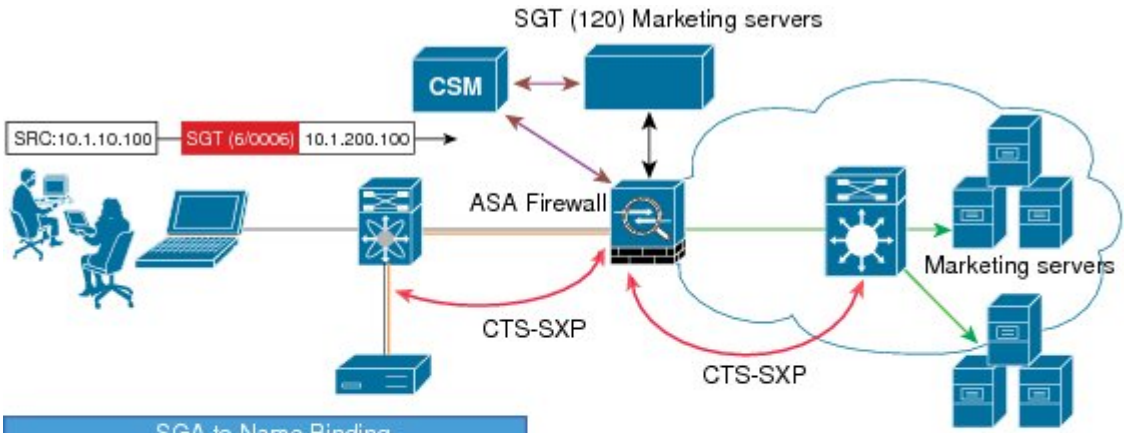
- Different VRFs may have overlapping CTS-SXP peer or source IP addresses.
- IP-to-SGT mappings learned (added or deleted) in one VRF can be updated only in the same VRF domain. The CTS-SXP connection cannot update a mapping bound to a different VRF. If no SXP connection exits for a VRF, IP-SGT mappings for that VRF will not be updated by SXP.
- CTS-SXP does not support the establishment of connections with a source IPv6 address. However, multiple address families per VRF are supported where one CTS-SXP connection in a VRF domain can forward both IPv4 and IPv6 IP-to-SGT mappings.
- CTS-SXP has no limitation on the number of connections and number of IP-to-SGT mappings per VRF.

Security Group Access Zone-Based Policy Firewall

CTS-SXP extends the deployment of network devices to additional places on the network by using the Security Group Access (SGA) Zone-Based Policy firewalls (ZBPFs). CTS-SXP is used for Identity distribution through inline devices where the identity information is learned from a primary communication path that exists across networks as shown in the figure below.

The Security Group Tag (SGT) is used by the SGA ZBPF to apply enforcement policy. IP-to-SGT mapping information is learned through CTS-SXP. When a packet arrives, source and destination IP addresses in the packet are used to derive source and destination tags. The Identity firewall applies a policy to the received IP packets based on the configured policy where the SGT is one of the attributes.

Figure 2: CTS-SXP SGA ZBPF Distribution Path Across Networks



SGA to Name Binding	
Secuirty Group Name	Secuirty Group Tag
mktg-server	120
mktg-corp-users	006
mktg-contractor	080
corp-servers	090

How to Configure Cisco TrustSec SGT Exchange Protocol IPv4

Enabling CTS-SXP

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp enable**

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 a CTS-SXP connection to any peer connection that is configured. **Note** Ensure that peer connections are configured. If peer connections are not configured, then CTS-SXP connections cannot be established with them.

Configuring a CTS-SXP Peer Connection

The CTS-SXP peer connection must be configured on both devices. One device is the speaker and the other is the listener. When using password protection, make sure to use the same password on both ends.

Note If a default CTS-SXP source IP address is not configured and you do not configure a CTS-SXP source address in the connection, the Cisco TrustSec software derives the CTS-SXP source IP address from existing local IP addresses. The CTS-SXP source IP address might be different for each TCP connection initiated from the router.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[**listener** | **speaker**] [**vrf** *vrf-name*]]
4. **exit**
5. **show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*]

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 connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[**listener** | **speaker**] [**vrf** *vrf-name*]] **Example:** `Device(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker`	Configures the CTS-SXP peer address connection. 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 CTS-SXP uses for the connection using the following options: • **default**—Use the default CTS-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. • **listener**—Specifies that the device is the listener in the connection. • **speaker**—Specifies that the device is the speaker in the connection. This is the default. The optional **vrf** keyword specifies the VRF to the peer. The default is the default VRF.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	**show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*] **Example:** `Device# show cts sxp connections`	(Optional) Displays CTS-SXP status and connections.

Configuring the Default CTS-SXP Password

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp default password** [**0** | **6** | **7**] *password*
4. **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 default password** [**0** | **6** | **7**] *password* **Example:** `Device(config)# cts sxp default password Cisco123`	Configures the CTS-SXP default password. You can enter either a clear text password (using the **0** or no option) or an encrypted password (using the **6** or **7** option). The maximum password length is 32 characters. **Note** By default, CTS-SXP uses no password when setting up connections.
Step 4	**exit** **Example:** `Device# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring the Default CTS-SXP Source IP Address

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp default source-ip** *src-ip-addr*
4. **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 default source-ip** *src-ip-addr* **Example:** `Device(config)# cts sxp default source-ip 10.20.2.2`	Configures the CTS-SXP default source IP address that is used for all new TCP connections where a source IP address is not specified. **Note** Existing TCP connections are not affected when the default CTS-SXP source IP address is configured.
Step 4	**exit** **Example:** `Device# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring the CTS-SXP Reconciliation Period

After a peer terminates a CTS-SXP connection, an internal hold-down timer starts. If the peer reconnects before the internal hold-down timer expires, the CTS-SXP reconciliation period timer starts. While the CTS-SXP reconciliation period timer is active, the CTS software retains the SGT mapping entries learned from the previous connection and removes invalid entries. The default value is 120 seconds (2 minutes). Setting the CTS-SXP reconciliation period to 0 seconds disables the timer and causes all entries from the previous connection to be removed.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **cts sxp reconciliation period** *seconds*
4. **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 reconciliation period** *seconds* **Example:** `Device(config)# cts sxp reconciliation period 150`	Sets the CTS-SXP reconciliation timer, in seconds. The range is from 0 to 64000. The default is 120.
Step 4	**exit** **Example:** `Device# exit`	Exits global configuration mode and enters privileged EXEC mode.

Configuring the CTS-SXP Retry Period

The CTS-SXP retry period determines how often the CTS software retries a CTS-SXP connection. If a CTS-SXP connection is not established successfully, then the CTS software makes a new attempt to set up the connection after the CTS-SXP retry period timer expires. The default value is 2 minutes. Setting the CTS-SXP retry period to 0 seconds disables the timer and retries are not attempted.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp retry period** *seconds*
4. **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	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**cts sxp retry period** *seconds* **Example:** `Device(config)# cts sxp retry period 160`	Sets the CTS-SXP retry timer, in seconds. The range is from 0 to 64000. The default is 120.
Step 4	**exit** **Example:** `Device# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Creating Syslogs to Capture IP-to-SGT Mapping Changes

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp log binding-changes**
4. **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 log binding-changes** **Example:** `Device(config)# cts sxp log binding-changes`	Enables logging for IP-to-SGT binding changes causing CTS-SXP syslogs (sev 5 syslog) to be generated whenever a change to IP-to-SGT binding occurs (add, delete, change). These changes are learned and propagated on the CTS-SXP connection. **Note** This logging function is disabled by default.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring a Class Map for a Security Group Access Zone-Based Policy Firewall

Perform this task to configure a class map for classifying Security Group Access (SGA) zone-based policy firewall network traffic.

Note You must perform at least one match step.

The zone-based firewall policy uses the Security Group Tag ID for filtering. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the inspect action.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **object-group security** *name*
4. **security-group tag-id** *sgt-id*
5. **group-object** *name*
6. **description** *text*
7. **exit**
8. **class-map type inspect** [**match-any** | **match-all**] *class-map-name*
9. **match group-object security source** *name*
10. **match group-object security destination** *name*
11. **end**
12. **show object-group** [*name*]

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:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**object-group security** *name* **Example:** `Device(config)# object-group security myobject1a`	Creates an object group to identify traffic coming from a specific user or endpoint and enters object-group identity mode.
Step 4	**security-group tag-id** *sgt-id* **Example:** `Device(config-object-group)# security-group tag-id 120`	Specifies the membership of a security group by using the SGT ID number. This number can be from 1 to 65535. Multiple security groups can be specified using this command.
Step 5	**group-object** *name* **Example:** `Device(config-object-group)# group-object admin`	(Optional) Specifies a nested reference to a type of user group. Multiple nested user groups can be specified using this command.
Step 6	**description** *text* **Example:** `Device(config-object-group)# description my sgtinfo`	(Optional) Defines information about the security group.
Step 7	**exit** **Example:** `Device(config-object-group)# exit`	Exits object-group identity mode and enters global configuration mode.
Step 8	**class-map type inspect** [**match-any** | **match-all**] *class-map-name* **Example:** `Device(config)# class-map type inspect match-any myclass1`	Creates a Layer 3 or Layer 4 inspect type class map and enters class-map configuration mode.
Step 9	**match group-object security source** *name* **Example:** `Device(config-cmap)# match group-object security source myobject1`	Matches traffic from a user in the security group.
Step 10	**match group-object security destination** *name* **Example:** `Device(config-cmap)# match group-object security destination myobject1`	Matches traffic for a user in the security group.

	Command or Action	Purpose
Step 11	**end** **Example:** `Device(config-cmap)# end`	Exits class-map configuration mode and enters privileged EXEC mode.
Step 12	**show object-group** [*name*] **Example:** `Device# show object-group admin`	(Optional) Displays the content of all user groups. Optionally, use the *name* argument to show information for a single group.

Creating a Policy Map for a Security Group Access Zone-Based Policy Firewall

Perform this task to create a policy map for a Security Group Access (SGA) zone-based policy firewall that is attached to zone pairs. This task also helps to configure Identity Firewall (IDFW) to work with Security Group Tag (SGT) Exchange Protocol (SXP) or L2-tagged traffic on the interfaces that belong to the security zones.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class type inspect** *class-name*
5. **inspect**
6. **exit**
7. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
8. **service-policy type inspect** *policy-map-name*
9. **end**
10. **interface** *type number*
11. **zone-member security** *zone-name*
12. **cts manual**
13. **no propagate sgt**
14. **policy static sgt** *tag* [**trusted**]
15. **exit**
16. **show policy-map type inspect zone-pair session**

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 inspect** *policy-map-name* **Example:** `Device(config)# policy-map type inspect z1z2-policy`	Creates a Layer 3 or Layer 4 inspect type policy map. • Enters policy map configuration mode.
Step 4	**class type inspect** *class-name* **Example:** `Device(config-pmap)# class type inspect cmap-1`	Specifies the traffic (class) on which an action is to be performed and enters policy-map class configuration mode.
Step 5	**inspect** **Example:** `Device(config-pmap-c)# inspect`	Enables packet inspection.
Step 6	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits policy-map class configuration mode and enters global configuration mode.
Step 7	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* **Example:** `Device(config)# zone-pair security z1z2 source z1 destination z2`	Creates a zone pair and enters security zone configuration mode. **Note** To apply a policy, you must configure a zone pair.
Step 8	**service-policy type inspect** *policy-map-name* **Example:** `Device(config-sec-zone)# service-policy type inspect z1z2-policy2`	Attaches a firewall policy map to the destination zone pair. **Note** If a policy is not configured between a pair of zones, traffic is dropped by default.
Step 9	**end** **Example:** `Device(config-sec-zone)# end`	Exits security zone configuration mode and enters global configuration mode.
Step 10	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/1/1`	Configures an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 11	**zone-member security** *zone-name* **Example:** `Device(config-if)# zone-member security Inside`	Assigns an interface to a specified security zone. **Note** When you make an interface a member of a security zone, all traffic in and out of that interface (except traffic bound for the router or initiated by the router) is dropped by default. To let traffic through the interface, you must make the zone part of a zone pair to which you should apply a policy. If the policy permits traffic, traffic can flow through that interface.
Step 12	**cts manual** **Example:** `Device(config-if)# cts manual`	Enables the interface for Cisco TrustSec Security (CTS) SGT authorization and forwarding, and enters CTS manual interface configuration mode.
Step 13	**no propagate sgt** **Example:** `Device(config-if-cts-manual)# no propagate sgt`	Disables SGT propagation at Layer 2 on CTS interfaces.
Step 14	**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 15	**exit** **Example:** `Device(config-if)# exit`	Exits security zone configuration mode and enters privileged EXEC mode.
Step 16	**show policy-map type inspect zone-pair session** **Example:** `Device# show policy-map type inspect zone-pair session`	(Optional) Displays the Cisco IOS stateful packet inspection sessions created because of the policy-map application on the specified zone pair. **Note** The information displayed under the class-map field is the traffic rate (bits per second) of the traffic that belongs to the connection-initiating traffic only. Unless the connection setup rate is significantly high and is sustained for multiple intervals over which the rate is computed, no significant data is shown for the connection.

Example:

The following sample output of the **show policy-map type inspect zone-pair session** command displays the information about the Cisco IOS stateful packet inspection sessions created because of the policy-map application on the specified zone pair:

```
Device# show policy-map type inspect zone-pair session

Zone-pair: in-out
 Service-policy inspect : test

   Class-map: test (match-any)
     Match: group-object security source sgt
     Inspect
       Established Sessions
        Session 113EF68C (192.2.2.1:8)=>(198.51.100.252:153) icmp SIS_OPEN
         Created 00:00:02, Last heard 00:00:02
         Bytes sent (initiator:responder) [360:360]


   Class-map: class-default (match-any)
     Match: any
     Drop (default action)
       310 packets, 37380 bytes
```

Configuration Examples for Cisco TrustSec SGT Exchange Protocol IPv4

Example: Enabling and Configuring a CTS-SXP Peer Connection

The following example shows how to enable CTS-SXP and configure the CTS-SXP peer connection on Device_A, a speaker, for connection to Device_B, a listener:

```
Device# 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 speaker
```

The following example shows how to configure the CTS-SXP peer connection on Device_B, a listener, for connection to Device_A, a speaker:

```
Device# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
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 listener
```

The following sample output for **show cts sxp connections** command displays CTS-SXP connections:

```
Device_B# show cts sxp connections
```

```
 SXP              : Enabled
 Default Password : Set
 Default Source IP: 10.10.1.1
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
------------------------------------------
Peer IP          : 10.20.2.2
Source IP        : 10.10.1.1
Conn status      : On
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: default SXP password
Duration since last state change: 0:00:21:25 (dd:hr:mm:sec)
Total num of SXP Connections = 1
```

Example: Configuring a Security Group Access Zone-Based Policy Firewall

The following example shows the configuration of a class map and policy map for an SGA zone-based policy firewall.

```
Device(config)# object-group security myobject1
Device(config-object-group)# security-group tag-id 1
Device(config-object-group)# exit
Device(config)# object-group security myobject2
Device(config-object-group)# security-group tag-id 2
Device(config-object-group)# exit
Device(config)# object-group security myobject3
Device(config-object-group)# security-group tag-id 3
Device(config-object-group)# exit
Device(config)# object-group security myobject4
Device(config-object-group)# security-group tag-id 4
Device(config-object-group)# exit

Device(config)# class-map type inspect match-any myclass1
Device(config-cmap)# match group-object security source myobject1
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any myclass2
Device(config-cmap)# match group-object security source myobject2
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any myclass3
Device(config-cmap)# match group-object security source myobject3
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any myclass4
Device(config-cmap)# match group-object security source myobject4
Device(config-cmap)# exit

Device(config)# policy-map type inspect InsideOutside
Device(config-pmap)# class type inspect myclass1
Device(config-pmap-c)# pass
Device(config-pmap-c)# exit
Device(config-pmap)# class type inspect myclass2
Device(config-pmap-c)# drop log
Device(config-pmap-c)# exit

Device(config)# policy-map type inspect OutsideInside
Device(config-pmap)# class type inspect myclass3
Device(config-pmap-c)# pass
Device(config-pmap-c)# exit
Device(config-pmap)# class type inspect myclass4
```

```
Device(config-pmap-c)# drop
Device(config-pmap-c)# exit

Device(config)# zone-pair security Inside
Device(config-sec-zone)# description Firewall Inside Zone
Device(config-sec-zone)# exit

Device(config)# zone-pair security Outside
Device(config-sec-zone)# description Firewall Outside Zone
Device(config-sec-zone)# exit

Device(config)# zone-pair security InsideOutside source Inside destination Outside
Device(config-sec-zone)# description Firewall ZonePair Inside Outside
Device(config-sec-zone)# service-policy type inspect InsideOutside
Device(config-sec-zone)# exit

Device(config)# zone-pair security OutsideInside source Outside destination Inside
Device(config-sec-zone)# description Firewall ZonePair Outside Inside
Device(config-sec-zone)# service-policy type inspect OutsideInside
Device(config-sec-zone)# exit

Device(config)# interface Gigabit 0/1/1
Device(config-if)# zone-member security Inside
Device(config-if)# exit
```

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 Cisco TrustSec SGT Exchange Protocol IPv4

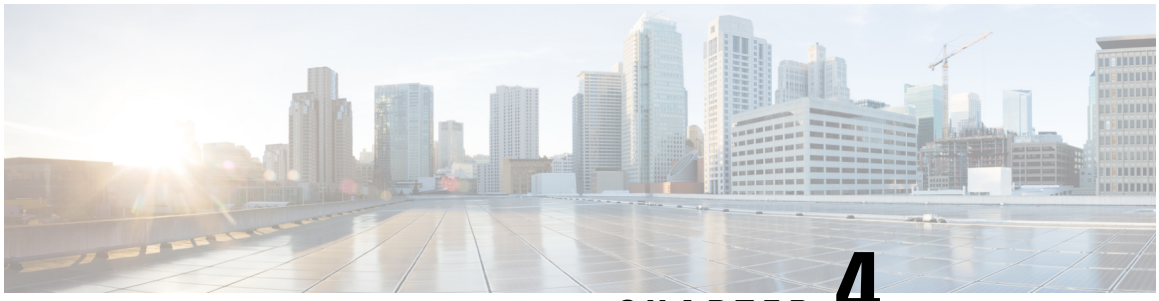
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for Cisco TrustSec SGT Exchange Protocol IPv4

Feature Name	Releases	Feature Information
Cisco TrustSec SGT Exchange Protocol IPv4	Cisco IOS 12.2(33)SXI3 Cisco IOS 15.1(3)S Cisco IOS 15.1(2)SY1	The Security Group Tag (SGT) Exchange Protocol (SXP) is one of several protocols that supports CTS and is referred to in this document as CTS-SXP. CTS-SXP is a control protocol for propagating IP-to-SGT binding information across network devices that do not have the capability to tag packets. CTS-SXP passes IP-to-SGT bindings from authentication points to upstream devices in the network. This allows security services on switches, routers, or firewalls to learn identity information from access devices. The following commands were introduced or modified: **cts sxp enable, cts sxp connection peer**, **show cts sxp**, **cts sxp default source-ip, cts sxp reconciliation period, cts sxp retry period, cts sxp log binding-changes**.

Feature Name	Releases	Feature Information
TrustSec SG Firewall Enforcement IPv4	Cisco IOS 15.2(1)S	This feature helps CTS-SXP extend the deployment of network devices through Security Group Access (SGA) Zone-Based Policy firewalls (ZBPFs). The following commands were introduced or modified: **group-object**, **match group-object security**, **object-group security**, **policy static sgt**, and **security-group**.



CHAPTER 4

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. **Note** To enable the **cts manual** command on a subinterface, you must increase the IP MTU size to accommodate the additional bytes for the Dot1Q tag. This is applicable only for releases earlier than Cisco IOS XE Release 3.17.
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**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• 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.

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

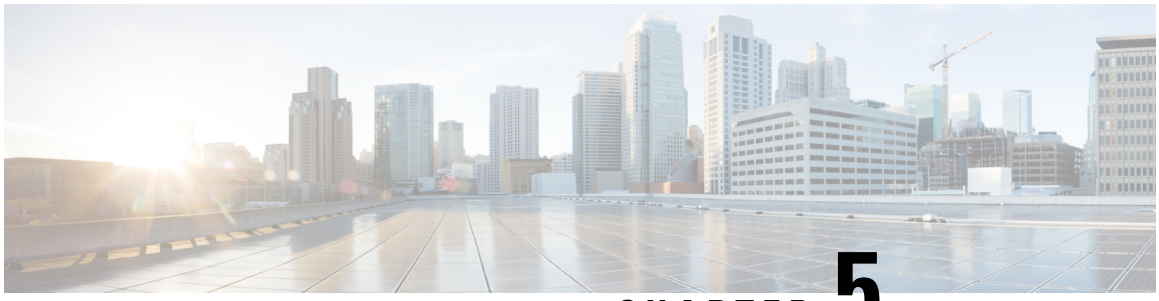
Feature Information for TrustSec SGT Handling: L2 SGT Imposition and Forwarding

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4: 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 15.1(3)S Cisco IOS 15.2(2)T Cisco IOS 15.1(2)SY1	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. The following commands were introduced or modified: **cts manual**, **policy static sgt**, **propagate sgt**, **show cts interface**.



CHAPTER 5

TrustSec Identity Port Mapping

A network device at the ingress of a Cisco TrustSec domain must have the security group tag (SGT) for the entering packet so that it can then tag it with this SGT before it forwards the packet into the domain. The egress network device determines the SGT of the packet in order to apply a security group access control list (SGACL).

The Identity Port Mapping (IPM) feature enables the ingress network device to determine the source SGT based on the source identity. IPM is implemented by configuring the link with the identity of the connected peer so that the ingress network device can request policy information, including SGT and trust state, from the authentication server.

Prerequisites for TrustSec Identity Port Mapping

IPM is supported for the following ports:

- Routed ports
- Switchports in access mode
- Switchports in trunk mode

Restrictions for TrustSec Identity Port Mapping

When manually configuring Cisco TrustSec on an interface, consider these usage guidelines and restrictions:

- If no SAP parameters are defined, Media Access Control Security (MACsec) encapsulation or encryption is not performed.
- If the selected SAP mode allows SGT insertion and an incoming packet carries an SGT, the tagging policy is as follows:

- If the **policy static** command is configured, the packet is tagged with the SGT configured in the policy static command.
- If the **policy dynamic** command is configured, the packet is not tagged.

- If the selected SAP mode allows SGT insertion and an incoming packet carries an SGT, the tagging policy is as follows:
  - If the **policy static** command is configured without the trusted keyword, the SGT is replaced with the SGT configured in the policy static command.
  - If the **policy static** command is configured with the trusted keyword, no change is made to the SGT.
  - If the **policy dynamic** command is configured and the authorization policy downloaded from the authentication server indicates that the packet source is untrusted, the SGT is replaced with the SGT specified by the downloaded policy.
  - If the**policy dynamic** command is configured and the downloaded policy indicates that the packet source is trusted, no change is made to the SGT.

Information About TrustSec Identity Port Mapping

TrustSec L2 Identity Port Mapping

TrustSec layer 2 IPM uses the **policy static sgt** command to configure a physical port so that a single SGT is imposed on all traffic entering the port. This SGT is then applied on all IP traffic exiting the port until a new binding is learned.

TrustSec L3 Identity Port Mapping

The Cisco TrustSec L3 IPM feature provides a dynamic method where the Cisco access control system (ACS) access server assigns the SGT based on the device ID mapping in the ACS for filtering at egress interfaces where no directly connected hosts (other than the next hop router) exists.

TrustSec layer 3 IPM uses the **policy dynamic identity** command to designate a peer name as non-trusted in the Cisco ACS or Cisco ISE configuration.

This feature can be used to identify places in the network egress interfaces (e.g. campus, extranet, internet) that need to be filtered so that guest access (group SGT) to the extranet (the business partner connection) is denied.

How to Configure TrustSec Identity Port Mapping

Configuring TrustSec Identity Port Mapping

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot*/*port*

4. **cts manual**
5. **policy dynamic identity** *peer-name*
6. **policy static sgt** *tag* [**trusted**]
7. **exit**
8. **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot*/*port* **Example:** `Device(config)# interface ethernet 1/0`	Enters interface configuration mode for the uplink interface.
Step 4	**cts manual** **Example:** `Device(config-if)# cts manual`	Enters Cisco TrustSec manual configuration mode.
Step 5	**policy dynamic identity** *peer-name* **Example:** `Device(config-if-cts-manual)# policy dynamic identity my_peer_device_name`	(Optional) Configures Identity Port Mapping (IPM) to allow dynamic authorization policy download from authorization server based on the identity of the peer. See the additional usage notes in the "Restrictions for Configuring TrustSec Identity" Port Mapping section. • *peer-name*—The Cisco TrustSec device ID for the peer device. The peer name is case sensitive. **Note** Ensure that you have configured the Cisco TrustSec credentials.
Step 6	**policy static sgt** *tag* [**trusted**] **Example:** `Device(config-if-cts-manual)# policy static sgt 7 trusted`	(Optional) Configures a static authorization policy. See the additional usage notes in the "Restrictions for Configuring TrustSec Identity" Port Mapping section. • *tag*— The SGT in decimal format. The range is 1 to 65533. • **trusted**—Indicates that ingress traffic on the interface with this SGT should not have its tag overwritten.
Step 7	**exit** **Example:**	Exits Cisco TrustSec manual interface configuration mode.

	Command or Action	Purpose
	`Device(config-if-cts-manual)# exit`	
Step 8	**no shutdown** **Example:** `Device(config-if)# no shutdown`	Enables the interface and enables Cisco TrustSec authentication on the interface.

TrustSec Identity Port Mapping Example

The following example shows how to configure Cisco TrustSec authentication in manual mode on an interface:

```
Device# configure terminal
Device(config)# interface gi2/1
Device(config-if)# cts manual
Device(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm null no-encap
Device(config-if-cts-manual)# exit
Device(config-if)# shutdown
Device(config-if)# no shutdown
Device(config-if)# exit
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 TrustSec Identity Port Mapping

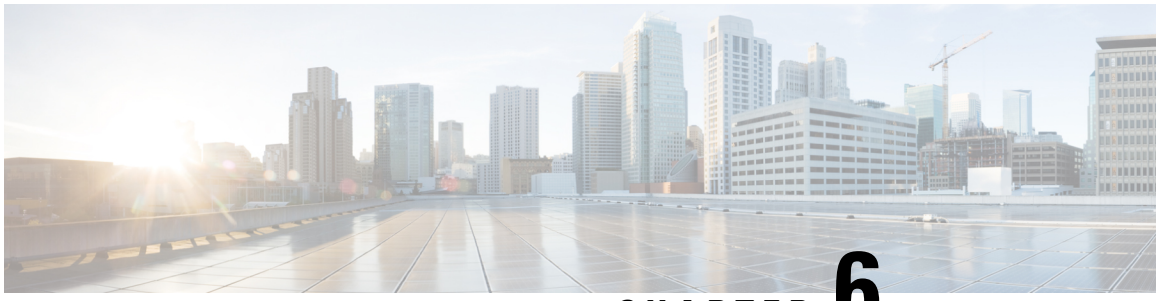
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5: Feature Information for TrustSec Identity Port Mapping

Feature Name	Releases	Feature Information
TrustSec Identity Port Mapping	15.1(1)SY	The Identity Port Mapping (IPM) feature enables the ingress network device to determine the source security group tag (SGT) based on the source identity. IPM is implemented by configuring the link with the identity of the connected peer so that the ingress network device can request policy information, including SGT and trust state, from the authentication server. The following command was introduced: **policy static sgt**.

Feature Name	Releases	Feature Information
Cisco TrustSec L3 Identity Port Mapping	15.1(1)SY	The Cisco TrustSec L3 Identity Port Mapping feature provides a dynamic method where the Cisco access control system (ACS) access server assigns the SGT based on the device ID mapping in the ACS for filtering at egress interfaces where no directly connected hosts (other than the next hop router) exists. The following command was introduced: **policy dynamic identity**.



CHAPTER 6

TrustSec Security Group Name Download

The TrustSec Security Group Name Download feature enhances the Security Group Tag (SGT) policy that downloads to the network access device to include the SGT name in addition to the SGT number and Security Group Access Control List (SGACL) policy.

Information About TrustSec Security Group Download

Layer 3 Logical Interface to SGT Mapping

The TrustSec Security Group Name Download feature is used to directly map SGTs to traffic of any of the following Layer 3 interfaces regardless of the underlying physical interface:

- Routed port
- SVI (VLAN interface)
- Layer3 subinterface of a Layer2 port
- Tunnel interface

The **cts role-based sgt-map interface** global configuration command to specify either a specific SGT number, or a Security Group Name (whose SGT association is dynamically acquired from a Cisco ISE or a Cisco ACS access server).

How to Configure TrustSec Security Group Name Download

Configuring TrustSec Security Group Name Download

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts role-based sgt-map interface** *type slot/port* [**security-group** *name* | **sgt** *number*]
4. **exit**
5. **show cts role-based sgt-map all**

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 interface** *type slot/port* [**security-group** *name* | **sgt** *number*] **Example:** `Device(config)# cts role-based sgt-map interface gigabitEthernet 1/1 sgt 77`	An SGT is imposed on ingress traffic to the specified interface. • **interface** *type slot*/*port*—Displays list of available interfaces. • **security-group** *name*— Security Group name to SGT pairings are configured on the Cisco ISE or Cisco ACS. • **sgt** *number*—(0 to 65,535). Specfies the Security Group Tag (SGT) number.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.
Step 5	**show cts role-based sgt-map all** **Example:** `Device# show cts role-based sgt-map all`	Verify that ingressing traffic is tagged with the specified SGT.

TrustSec Security Group Name Download Example

The following example shows the SGT download configuration for the ingress interface:

```
Device# config terminal
Device(config)# cts role-based sgt-map interface gigabitEthernet 6/3 sgt 3
Device(config)# exit
```

The following example shows that ingressing traffic for the ingress interface is tagged appropriately:

```
Device# show cts role-based sgt-map all

IP Address              SGT     Source

============================================

15.1.1.15               4       INTERNAL

17.1.1.0/24             3       L3IF

21.1.1.2                4       INTERNAL

31.1.1.0/24             3       L3IF

31.1.1.2                4       INTERNAL

43.1.1.0/24             3       L3IF

49.1.1.0/24             3       L3IF

50.1.1.0/24             3       L3IF

50.1.1.2                4       INTERNAL

51.1.1.1                4       INTERNAL

52.1.1.0/24             3       L3IF

81.1.1.1                5       CLI

102.1.1.1               4       INTERNAL

105.1.1.1               3       L3IF

111.1.1.1               4       INTERNAL

IP-SGT Active Bindings Summary

============================================

Total number of CLI      bindings = 1

Total number of L3IF     bindings = 7

Total number of INTERNAL bindings = 7

Total number of active   bindings = 15
```

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

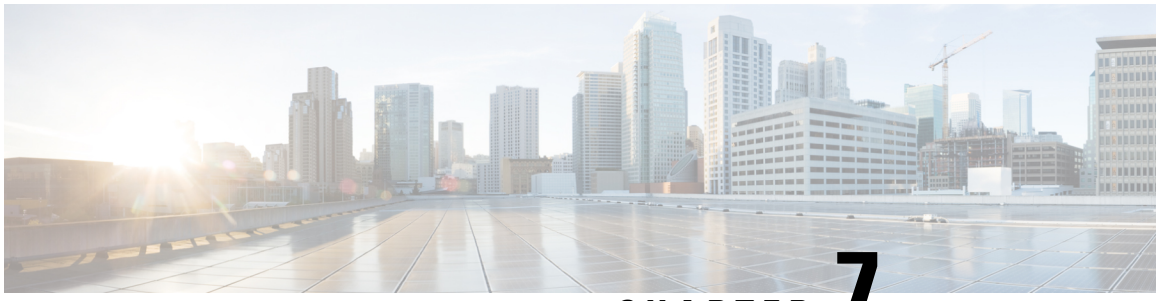
Feature Information for TrustSec Security Group Name Download

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 6: Feature Information for TrustSec Security Group Name Download

Feature Name	Releases	Feature Information
TrustSec Security Group Name Download		This feature enhances the Security Group Tag (SGT) policy that downloads to the network access device to include the SGT name in addition to the SGT number and Security Group Access Control List (SGACL) policy. The following commands were introduced or modified: **cts role-based sgt-map interface**.



CHAPTER 7

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.
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.

	Command or Action	Purpose
Step 5	**aaa session-id common** **Example:** `Device(config)# aaa session-id common`	Ensures that the same session identification (ID) information is used for each AAA accounting service type within a given call.
Step 6	**radius server** *radius-server-name* **Example:** `Device(config)# radius server cts-aaa-server`	Specifies the name for the RADIUS server configuration for Protected Access Credential (PAC) provisioning and enters RADIUS server configuration mode.
Step 7	**address ipv4** {*hostname* | *ipv4address*} [**acct-port** *port* | **alias** {*hostname* | *ipv4address*} | **auth-port** *port* [**acct-port** *port*]] **Example:** `Device(config-radius-server)# address ipv4 192.0.2.1 auth-port 1812 acct-port 1813`	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.
Step 8	**pac key** *encryption-key* **Example:** `Device(config-radius-server)# pac key cisco123`	Specifies the PAC encryption key.
Step 9	**exit** **Example:** `Device(config-radius-server)# exit`	Exits RADIUS server configuration mode and enters global configuration mode.
Step 10	**radius-server vsa send authentication** **Example:** `Device(config)# radius-server vsa send authentication`	Configures the network access server (NAS) to recognize and use only authentication vendor-specific attributes (VSAs).
Step 11	**aaa group server radius** *group-name* **Example:** `Device(config)# aaa group server radius cts_sg`	Groups different RADIUS server hosts into distinct lists and distinct methods and enters RADIUS group server configuration mode.
Step 12	**server name** *radius-server-name* **Example:** `Device(config-sg-radius)# server name cts-aaa-server`	Specifies a RADIUS server.
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:**	Specifies the RADIUS server to use for authentication on interfaces running IEEE 802.1X.

	Command or Action	Purpose
	`Device(config)# aaa authentication dot1x default group cts_sg`	
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.

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

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

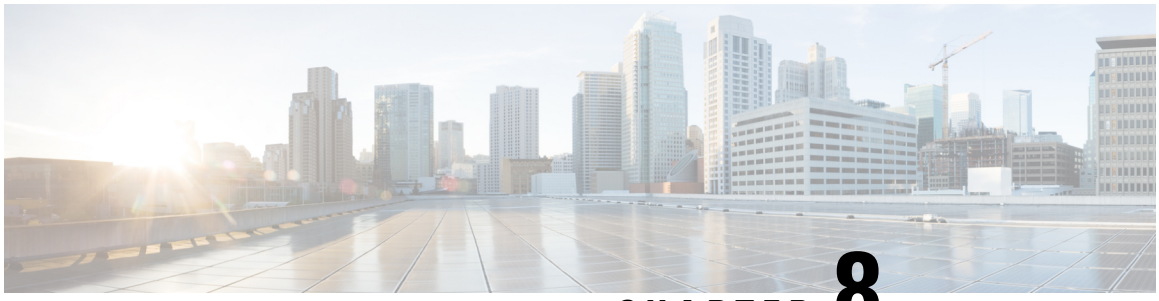
Feature Information for Cisco TrustSec Network Device Admission Control

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 7: Feature Information for Cisco TrustSec Network Device Admission Control

Feature Name	Releases	Feature Information
Cisco TrustSec Network Device Admission Control	Cisco IOS 12.2(33)SXI Cisco IOS 15.1(1)SY	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**.



CHAPTER 8

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.
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.

	Command or Action	Purpose
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

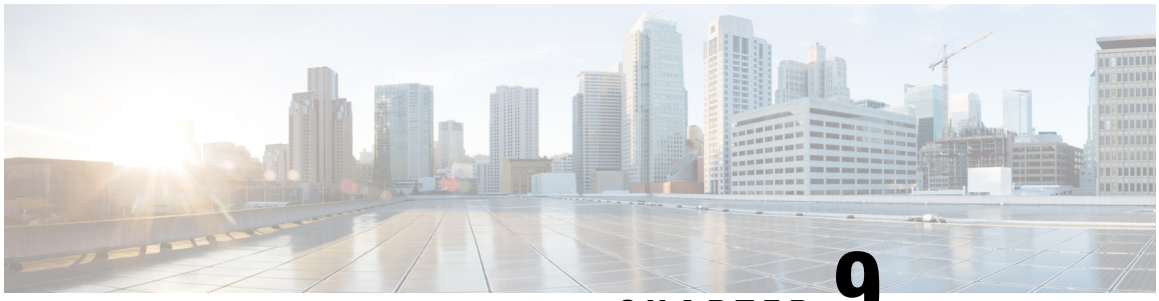
Feature Information for Enablement of Security Group ACL at Interface Level

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 8: Feature Information for Enablement of Security Group ACL at Interface Level

Feature Name	Releases	Feature Information
Enablement of Security Group ACL at Interface Level	15.1(2)SY	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. The following command was introduced: **cts role-based enforcement**.



CHAPTER 9

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

Configuring SISF Policy and Attaching to a Port

The Switch Integrated Security Features (SISF) policy is configured on both the VLAN and on the physical port. The SISF policy is attached to a VLAN to learn the VLAN-specific address binding. The purpose of attaching the SISF policy to a physical port is to learn IPv4 and IPv6 addresses on the physical port.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **device-tracking policy** *name*
4. **trusted-port**
5. **limit address-count** *max-number*
6. **device-role node**
7. **tracking enable**
8. **exit**
9. **vlan configuration** *vlan-id*

10. **device-tracking attach-policy** *name*
11. **ipv6 nd suppress**
12. **exit**
13. **interface** *type number*
14. **switchport**
15. **switchport mode access**
16. **switchport access vlan** *vlan-id*
17. **access-session host-mode multi-host**
18. **access-session closed**
19. **access-session port-control auto**
20. **device-tracking attach-policy** *name*
21. **dot1x pae authenticator**
22. **service-policy type control subscriber** *policy-name*
23. **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	**device-tracking policy** *name* **Example:** `Device(config)# device-tracking policy policy1`	Configures a policy for feature device-tracking and enters device tracking configuration mode.
Step 4	**trusted-port** **Example:** `Device(config-device-tracking)# trusted-port`	Configures a port to become a trusted port.
Step 5	**limit address-count** *max-number* **Example:** `Device(config-device-tracking)# limit address-count 100`	Configures the maximum number of addresses for a port.
Step 6	**device-role node** **Example:** `Device(config-device-tracking)# device-role node`	Specifies that the device attached to the port is a node.
Step 7	**tracking enable** **Example:** `Device(config-device-tracking)# tracking enable`	Overrides default tracking behavior.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Device(config-device-tracking)# exit`	Exits device tracking configuration mode and enters global configuration mode.
Step 9	**vlan configuration** *vlan-id* **Example:** `Device(config)# vlan configuration 20`	Configures the VLAN ID and enters VLAN configuration mode.
Step 10	**device-tracking attach-policy** *name* **Example:** `Device(config-vlan-config)# device-tracking attach-policy policy1`	Applies a policy for feature device-tracking on the VLAN.
Step 11	**ipv6 nd suppress** **Example:** `Device(config-vlan-config)# ipv6 nd suppress`	Applies the IPv6 neighbor discovery (ND) suppress feature on the VLAN.
Step 12	**exit** **Example:** `Device(config-vlan-config)# exit`	Exits VLAN configuration mode and enters global configuration mode.
Step 13	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet5/2`	Configures the interface and enters interface configuration mode.
Step 14	**switchport** **Example:** `Device(config-if)# switchport`	Modifies an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.
Step 15	**switchport mode access** **Example:** `Device(config-if)# switchport`	Sets the interface type to access mode.
Step 16	**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 17	**access-session host-mode multi-host** **Example:** `Device(config-if)# access-session host-mode multi-host`	Allows hosts to gain access to a controlled port and specifies that all subsequent clients are allowed access after the first client is authenticated.
Step 18	**access-session closed** **Example:** `Device(config-if)# access-session closed`	Prevents preauthentication access on a port.

	Command or Action	Purpose
Step 19	**access-session port-control auto** **Example:** `Device(config-if)# access-session port-control auto`	Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.
Step 20	**device-tracking attach-policy** *name* **Example:** `Device(config-if)# device-tracking attach-policy policy1`	Applies a policy for feature device-tracking on a port.
Step 21	**dot1x pae authenticator** **Example:** `Device(config-if)# dot1x pae authenticator`	Enables dot1x authentication on a port.
Step 22	**service-policy type control subscriber** *policy-name* **Example:** `Device(config-if)# service-policy type control subscriber DOT1X`	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 23	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

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.

Before you begin

Ensure that the SISF policy is configured and attached to a Layer 2 physical interface and to a VLAN. For more information, see the “Configuring SISF Policy and Attaching to a Port” section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *dhcp-pool-name*
4. **address prefix** *ipv6-address/prefix*
5. **exit**
6. **interface vlan** *interface-number*
7. **ipv6 enable**
8. **no ipv6 address**
9. **ipv6 address** *ipv6-address/prefix*
10. **ipv6 address autoconfiguration**
11. **ipv6 dhcp server** *dhcp-pool-name*

12. **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 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 4	**address prefix** *ipv6-address/prefix* **Example:** `Device(config-dhcpv6)# address prefix 2001:DB8::1/64`	Sets the IPv6 address for an end host.
Step 5	**exit** **Example:** `Device(config-dhcpv6)# exit`	Exits IPv6 DHCP pool configuration mode and returns to global configuration mode.
Step 6	**interface vlan** *interface-number* **Example:** `Device(config)# interface vlan 20`	Creates a VLAN interface and enters interface configuration mode.
Step 7	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 on an interface.
Step 8	**no ipv6 address** **Example:** `Device(config-if)# no ipv6 address`	Removes the existing IPv6 address set for an interface.
Step 9	**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 10	**ipv6 address autoconfiguration** **Example:** `Device(config-if)# ipv6 address autoconfiguration`	Enables stateless autoconfiguration on an interface.

	Command or Action	Purpose
Step 11	**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 12	**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

- Ensure that the SISF policy is configured and attached to a Layer 2 physical interface and to a VLAN. For more information, see the "Configuring SISF Policy and Attaching to a Port" section.
- 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.
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:**	Describes the configured interface.

	Command or Action	Purpose
	`Device(config-if)# description downlink to ipv6 clients`	
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

- Ensure that the SISF policy is configured and attached to a Layer 2 physical interface and to a VLAN. For more information, see the "Configuring SISF Policy and Attaching to a Port" section.
- 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**

4. **show device-tracking database**

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`
	
	`IP Address SGT Source`
	`==========`
		Displays active IPv6 IP-SGT bindings.

	Command or Action	Purpose
	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	
Step 4	**show device-tracking database** **Example:** Device# **show device-tracking database** Binding Table has 8 entries, 5 dynamic Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DHCP, PKT - Other Packet, API - API created Preflevel flags (prlvl): 0001:MAC and LLA match 0002:Orig trunk 0004:Orig access 0008:Orig trusted trunk 0010:Orig trusted access 0020:DHCP assigned 0040:Cga authenticated 0080:Cert authenticated 0100:Statically assigned Network Layer Address Link Layer Address Interface vlan prlvl age state Time left ARP 192.0.2.1 001f.e21c.09b6 Gi5/2 20 0011 8s REACHABLE 12 s L 192.0.2.2 c464.1395.c700 Vl20 20 0100 45s REACHABLE ND 2001:DB8::1 0000.0000.00fd Gi5/2 20 0000 13s UNKNOWN (47 s) L 2001:DB8::1 c464.1395.c700 Vl20 20 0100 43s REACHABLE ND 2001:DB8:1::1 001f.e21c.09b6 Gi5/2 20 0011 0s REACHABLE 20 s ND 2001:DB8:0:ABCD::1 001f.e21c.09b6 Gi5/2 20 0011 3s REACHABLE 17 s try 0 ND 2001:DB8::FFFE:FFFF:FFFF 001f.e21c.09b6 Gi5/2 20 0011 12s REACHABLE 7 s	Displays the state of the IPv4 and IPv6 neighbor binding entries in a binding table.

	Command or Action	Purpose
	try 0 L 2001:DB8::2 c464.1395.c700 Vl20 20 0100 42s REACHABLE	

Configuration Examples for IPv6 Support for SGT and SGACL

Example: Configuring SISF Policy and Attaching to a Port

```
Device> enable
Device# configure terminal
Device(config)# device-tracking policy policy1
Device(config-device-tracking)# trusted-port
Device(config-device-tracking)# limit address-count 100
Device(config-device-tracking)# device-role node
Device(config-device-tracking)# tracking enable
Device(config-device-tracking)# exit
Device(config)# vlan configuration 20
Device(config-vlan-config)# device-tracking attach-policy policy1
Device(config-vlan-config)# ipv6 nd suppress
Device(config-vlan-config)# exit
Device(config)# interface GigabitEthernet5/2
Device(config-if)# switchport
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 20
Device(config-if)# access-session host-mode multi-host
Device(config-if)# access-session closed
Device(config-if)# access-session port-control auto
Device(config-if)# device-tracking attach-policy policy1
Device(config-if)# dot1x pae authenticator
Device(config-if)# service-policy type control subscriber DOT1X
Device(config-if)# exit
```

Example: Generating IPv6 Addresses for IP-SGT Bindings

```
Device> enable
Device# configure terminal
Device(config)# device-tracking policy policy1
Device(config-device-tracking)# trusted-port
Device(config-device-tracking)# limit address-count 100
Device(config-device-tracking)# device-role node
Device(config-device-tracking)# tracking enable
Device(config-device-tracking)# exit
Device(config)# vlan configuration 20
Device(config-vlan-config)# device-tracking attach-policy policy1
Device(config-vlan-config)# ipv6 nd suppress
Device(config-vlan-config)# exit
Device(config)# interface GigabitEthernet5/2
Device(config-if)# switchport
```

```
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 20
Device(config-if)# access-session host-mode multi-host
Device(config-if)# access-session closed
Device(config-if)# access-session port-control auto
Device(config-if)# device-tracking attach-policy policy1
Device(config-if)# dot1x pae authenticator
Device(config-if)# service-policy type control subscriber DOT1X
Device(config-if)# 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)# device-tracking policy policy1
Device(config-device-tracking)# trusted-port
Device(config-device-tracking)# limit address-count 100
Device(config-device-tracking)# device-role node
Device(config-device-tracking)# tracking enable
Device(config-device-tracking)# exit
Device(config)# vlan configuration 20
Device(config-vlan-config)# device-tracking attach-policy policy1
Device(config-vlan-config)# ipv6 nd suppress
Device(config-vlan-config)# exit
Device(config)# interface GigabitEthernet5/2
Device(config-if)# description downlink to ipv6 clients
Device(config-if)# switchport
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 20
Device(config-if)# access-session host-mode multi-host
Device(config-if)# access-session closed
Device(config-if)# access-session port-control auto
Device(config-if)# device-tracking attach-policy policy1
Device(config-if)# mab eap
Device(config-if)# dot1x pae authenticator
Device(config-if)# service-policy type control subscriber DOT1X
Device(config-if)# 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
```

Example: Configuring IPv6 IP-SGT Binding Using a VLAN

```
Device> enable
Device# configure terminal
Device(config)# device-tracking policy policy1
Device(config-device-tracking)# trusted-port
Device(config-device-tracking)# limit address-count 100
Device(config-device-tracking)# device-role node
Device(config-device-tracking)# tracking enable
Device(config-device-tracking)# exit
Device(config)# vlan configuration 20
Device(config-vlan-config)# device-tracking attach-policy policy1
Device(config-vlan-config)# ipv6 nd suppress
Device(config-vlan-config)# exit
Device(config)# interface GigabitEthernet5/2
Device(config-if)# switchport
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 20
Device(config-if)# access-session host-mode multi-host
Device(config-if)# access-session closed
Device(config-if)# access-session port-control auto
Device(config-if)# device-tracking attach-policy policy1
Device(config-if)# dot1x pae authenticator
Device(config-if)# service-policy type control subscriber DOT1X
Device(config-if)# 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

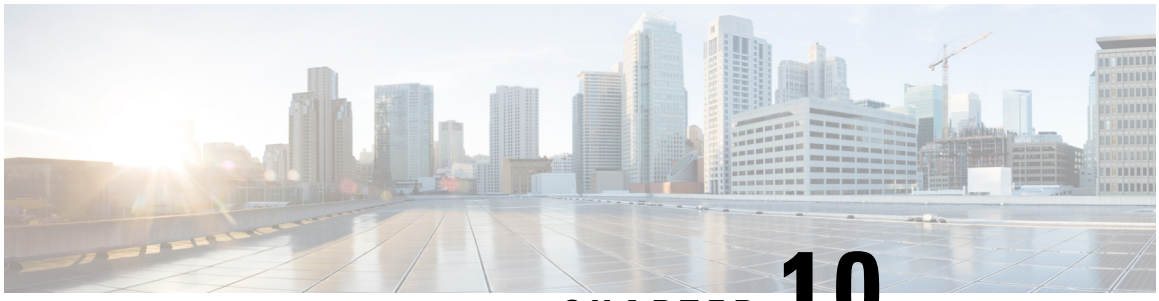
Feature Information for IPv6 Support for SGT and SGACL

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 9: Feature Information for IPv6 Support for SGT and SGACL

Feature Name	Releases	Feature Information
IPv6 Support for SGT and SGACL	Cisco IOS 15.2(1)SY	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). The following command was modified: **cts role-based sgt-map**.



CHAPTER 10

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*.
- To use the Cisco TrustSec functionality on your existing device, ensure that you have purchased one of the following security licenses:
  - IP Base License
  - LAN Base License

Note The LAN Base License is available from Cisco IOS XE Everest 16.5.1.

- IP Services License

- Connectivity must exist in all network devices.
- Cisco TrustSec SXP software must run on all network devices.

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).
- The Bidirectional SXP Support feature only supports the scalability numbers for SXP connections and IP-SGT bindings provided in the following table.

Table 10: Scalability Numbers for SXP Connections and IP-SGT Bindings

Platform	Unidirectional SXP Connections (Speaker only/Listener only)	Bidirectional SXP Connections	SXP Database IP-SGT Bindings **Note** If the number of connections are increased, ensure that the number of bindings configured per box are reduced. The number of connections should not exceed the connections documented in this table. **Note** The Role-Based IP-SGT database limit is 200K across all platforms.
ISR 2900, ISR 3900	250	125	• 180K for unidirectional SXP connections • 125K for bidirectional SXP connections
Catalyst 6000 series	500	250	100K

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 3: 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**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• 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.
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.

	Command or Action	Purpose
		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.
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 11: 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

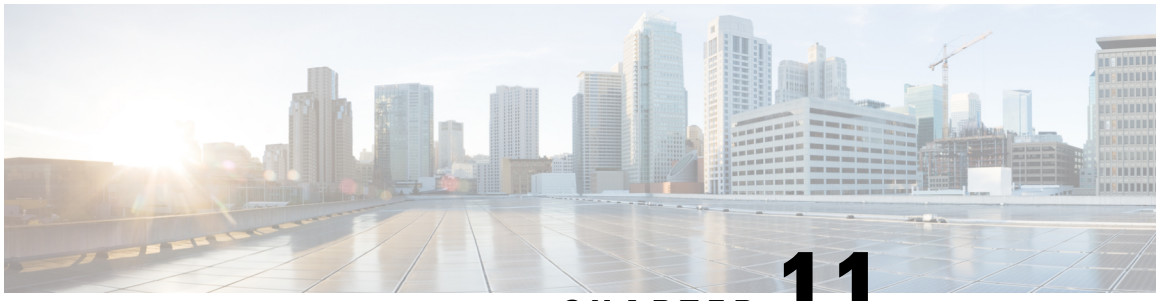
Feature Information for Bidirectional SXP Support

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 12: Feature Information for Bidirectional SXP Support

Feature Name	Releases	Feature Information
Bidirectional SXP Support	Cisco IOS 15.4(1)T Cisco IOS 15.2(1)SY	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. The following command was introduced or modified: **cts sxp connection peer**.



CHAPTER 11

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

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 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 attemp to 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
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	**radius-server dead-criteria** [**time** *seconds*] [**tries** *number-of-tries*] **Example:** `Device(config)# radius-server dead-criteria time 15 tries 3`	Configures the conditions that determine when a RADIUS server is considered unavailable or dead. • **time** *seconds* - 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. • **tries** *number-of-tries* - Sets the number of times that the device does not get a valid response from the RADIUS server before the server is considered unavailable.
Step 4	**radius-server deadtime** *minutes* **Example:** `Device(config)# radius-server deadtime 10`	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. 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.
Step 5	**radius server** *server-name* **Example:** `Device(config)# radius server RASERV-1`	Specifies the name for the RADIUS server configuration for Protected Access Credential (PAC) provisioning and enters RADIUS server configuration mode.
Step 6	**address ipv4** {*hostname* | *ipv4address*} [**acct-port** *port* | **alias** {*hostname* | *ipv4address*} | **auth-port** *port* [**acct-port** *port*]] **Example:** `Device(config-radius-server)# address ipv4 172.20.254.4 auth-port 1812 acct-port 1813`	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.

	Command or Action	Purpose
Step 7	**automate-tester username** *user* [**ignore-auth-port**] [**ignore-acct-port**] [**idle-time** *minutes*] **Example:** `Device(config-radius-server)# automate-tester username dummy`	Enables the automated testing feature for the RADIUS server. 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.
Step 8	**pac key** *encryption-key* **Example:** `Device(config-radius-server)# pac key 7 mypackey`	Specifies the Protected Access Credential (PAC) encryption key. The *encryption-key* argument can be **0** (specifies that an unencrypted key follows), **6** (specifies that an advanced encryption scheme [AES] encrypted key follows), **7** (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.
Step 9	**exit** **Example:** `Device(config)# exit`	Exits RADIUS server configuration mode and returns to global configuration mode.
Step 10	**cts server test** {*ipv4-address* | **all**} {**deadtime** *seconds* | **enable** | **idle-time** *minutes*} **Example:** `Device(config)# cts server test all idle-time 3`	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 **deadtime** is 20 seconds; the range is 1 to 864000 seconds. The default **idle-time** is 60 seconds; the range is from 1 to 14400 seconds.
Step 11	**cts critical-authentication default peer-sgt** *peer-sgt-value* [**trusted**] **Example:** `Device(config)# cts critical-authentication default peer-sgt 5`	Configures the default peer security group tag (SGT) value. • 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 **trusted** keyword to mark a device as trustworthy. • The range for the *peer-SGT-value* argument is from 2 to 65519.
Step 12	**exit** **Example:** `Device(config)# exit`	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

1. **enable**
2. **show running-config | section critical**
3. **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	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
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/cisco/web/support/index.html

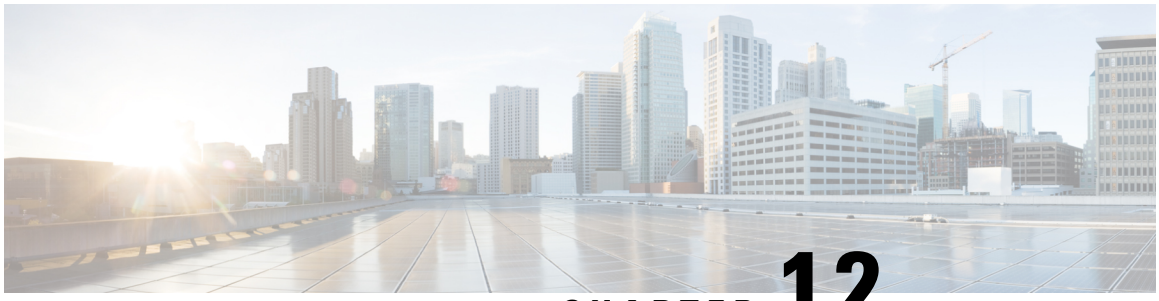
Feature Information for Cisco TrustSec Critical Authentication

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. An account on Cisco.com is not required.

Table 13: Feature Information for Cisco TrustSec Critical Authentication

Feature Name	Releases	Feature Information
Cisco TrustSec Critical Authentication	Cisco IOS 15.2(1)SY	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. The following command was introduced by this feature: **cts critical-authentication**.



CHAPTER 12

Cisco TrustSec VRF-Aware SGT

The Cisco TrustSec VRF-Aware SGT feature allows the device to communicate with the RADIUS servers through the Virtual Routing and Forwarding (VRF) interfaces. This feature allows protected access credential (PAC) and Environment-Data to be requested from the authentication device, Cisco Identity Services Engine (Cisco ISE), when Cisco ISE is in a VRF network.

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.

Information About Cisco TrustSec VRF-Aware SGT

VRF-Aware SGT

Cisco TrustSec uses security group tag (SGT) to ensure that the packets passing through the Cisco TrustSec network can be properly identified and the applied with security and other access control policies.

When Cisco Identity Services Engine (Cisco ISE) is in a Virtual Routing and Forwarding (VRF) network, information on protected access credential (PAC) and Environment-Data is obtained by opening a socket connection with Cisco ISE according to the VRF information. When an interface is configured to be on a VRF network, then the IP-SGT bindings learnt on that interface are added under the specific VRF.

How to Configure Cisco TrustSec VRF-Aware SGT

Configuring AAA and RADIUS for Cisco VRF-Aware SGT

Note Configure only one source interface on the VRF network using the **ip radius source-interface** *subinterface-name* **vrf** *vrf-name* command. Configuring more than one source interface will result in packet loss.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa session-id common**
5. **aaa authentication dot1x default group** *group-name*
6. **aaa authorization network default group** *group-name*
7. **aaa authorization network** *list-name* **group** *group-name*
8. **aaa server radius dynamic-author**
9. **radius server** *name*
10. **address ipv4** *hostname* [**acct-port** *port* | **alias** *name* | **auth-port** *port* [**acct-port** *port*]]
11. **pac key** *encryption-key*
12. **exit**
13. **aaa group server radius** *group-name*
14. **server name** *server-name*
15. **ip vrf forwarding** *vrf-name*
16. **exit**
17. **cts authorization list network** *list-name*
18. **ip radius source-interface** *subinterface-name* **vrf** *vrf-name*
19. **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.

	Command or Action	Purpose
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables new RADIUS and AAA access control commands and functions and disables old commands.
Step 4	**aaa session-id common** **Example:** `Device(config)# aaa session-id common`	Ensures that all session identification (ID) information that is sent out for a given call will be made identical.
Step 5	**aaa authentication dot1x default group** *group-name* **Example:** `Device(config)# aaa authentication dot1x default group cts-sg`	Specifies the server group used for authentication on interfaces running IEEE 802.1X.
Step 6	**aaa authorization network default group** *group-name* **Example:** `Device(config)# aaa authorization network default group cts-sg`	Specifies the default CTS authorization list for all network-related service requests from the RADIUS server group.
Step 7	**aaa authorization network** *list-name* **group** *group-name* **Example:** `Device(config)# aaa authorization network cts-mlist group cts-sg`	Specifies the CTS authorization list name for all network-related service requests from the RADIUS server group.
Step 8	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Configures a device as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server.
Step 9	**radius server** *name* **Example:** `Device(config)# radius server myserver`	Specifies a name for the RADIUS server PAC provisioning configuration and enters RADIUS server configuration mode.
Step 10	**address ipv4** *hostname* [**acct-port** *port* | **alias** *name* | **auth-port** *port* [**acct-port** *port*]] **Example:** `Device(config-radius-server)# address ipv4 10.0.0.1 acct-port 1813 auth-port 1812`	Configures the RADIUS server accounting and authentication parameters for PAC provisioning. • The *hostname* argument is the RADIUS server IPv4 address or Domain Name System (DNS) name. • The **acct-port** keyword and *port* argument specify the UDP port for the RADIUS accounting server for accounting requests. The default port is 1646. • The **alias** keyword and *name* argument specify an alias for this server. The alias can be an IPv4 address

	Command or Action	Purpose
		or host name. Up to 8 aliases can be configured for this server. • The **auth-port** keyword and *port* argument specify the UDP port for RADIUS authentication server. The default port is 1645.
Step 11	**pac key** *encryption-key* **Example:** `Device(config-radius-server)# pac key 7 mypackey`	Specifies the Protected Access Credential (PAC) encryption key. The *encryption-key* argument can be **0** (specifies that an unencrypted key follows), **6** (specifies that an advanced encryption scheme [AES] encrypted key follows), **7** (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.
Step 12	**exit** **Example:** `Device(config-radius-server)# exit`	Exits RADIUS server configuration mode and returns to global configuration mode.
Step 13	**aaa group server radius** *group-name* **Example:** `Device(config)# aaa group server radius cts-sg`	Specifies a server group and groups different RADIUS server hosts into distinct lists and distinct methods. Enters server-group RADIUS configuration mode.
Step 14	**server name** *server-name* **Example:** `Device(config-sg-radius)# server name myserver`	Configures a RADIUS server for the group server.
Step 15	**ip vrf forwarding** *vrf-name* **Example:** `Device(config-sg-radius)# ip vrf forwarding vrf-intf`	Configures the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an authentication, authorization, and accounting (AAA) RADIUS server group.
Step 16	**exit** **Example:** `Device(config-sg-radius)# exit`	Exits server-group RADIUS configuration mode and returns to global configuration mode.
Step 17	**cts authorization list network** *list-name* **Example:** `Device(config)# cts authorization list cts-mlist`	Specifies a list of AAA servers for the CTS seed device to use.
Step 18	**ip radius source-interface** *subinterface-name* **vrf** *vrf-name* **Example:**	Forces RADIUS to use the IP address of a specified interface per VRF for all outgoing RADIUS packets.

	Command or Action	Purpose
	`Device(config)# ip radius source-interface GigabitEthernet0 vrf vrf-intf`	
Step 19	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring VRF Connectivity to Cisco ISE

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask*
6. **negotiation auto**
7. **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	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet0`	Specifies an interface and enters interface configuration mode.
Step 4	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding vrf-intf`	Configures a VRF table. **Note** You can configure VRF forwarding on any VRF-Aware Software Infrastructure (VASI) interface. You need not configure VRF instances on both VASI interfaces.

	Command or Action	Purpose
Step 5	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 10.0.0.1 255.0.0.0`	Configures an IP address for an interface.
Step 6	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables the autonegotiation protocol to configure the speed, duplex, and automatic flow control of the Gigabit Ethernet interface.
Step 7	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying Cisco TrustSec VRF-Aware SGT

Before you begin

- Verify the connectivity to Cisco Identity Services Engine (Cisco ISE) through VRF
- Verify the AAA and RADIUS configuration.

SUMMARY STEPS

1. **enable**
2. **show cts pac**
3. **show cts environment-data**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Device> enable
```

Step 2 **show cts pac**

Displays all the downloaded protected access credential (PAC) information.

Example:

The following sample output from the **show cts pac** command shows all the downloaded PAC:

```
Device# show cts pac
```

```
AID: BEF6BDBA77EE27F60C8C3681D72A4889
 PAC-Info:
 PAC-type = Cisco Trustsec
 AID: BEF6BDBA77EE27F60C8C3681D72A4889
 I-ID: SW-3k-1
 A-ID-Info: ise-cts-blr4
 Credential Lifetime: 18:53:53 IST Mar 10 2014
 PAC-Opaque:
[illegible]

 Refresh timer is set for 00:01:05
```

Step 3 **show cts environment-data**

Displays the Cisco TrustSec environment data.

Example:

The following sample output from the **show cts environment-data** command shows the Cisco TrustSec environment data:

```
Device# show cts environment-data

CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 3-03:Cat6k_01
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.64.67.248, port 1812, A-ID 36B3F575DBA9ED4E782D056231DFF41C
 Status = ALIVE
 auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
 0-c2:Unknown
 2-c2:Cat6k_45
 3-c2:Cat6k_01
 4-c2:4k_active
 5-c2:cat3k_stack
 6-c2:cat3k_33
Environment Data Lifetime = 86400 secs
Last update time = 01:56:48 UTC Wed Mar 30 2011
Env-data expires in 0:23:56:37 (dd:hr:mm:sec)
Env-data refreshes in 0:23:56:37 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
```

Configuration Examples For Cisco TrustSec VRF-Aware SGT

Example: Configuring AAA and RADIUS for Cisco VRF-Aware SGT

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa session-id common
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)# aaa server radius dynamic-author
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 10.0.0.1 acct-port 1813 auth-port 1812
Device(config-radius-server)# pac key 7 mypackey
Device(config-radius-server)# exit
Device(config)# aaa group server radius cts-sg
Device(config-sg-radius)# server name myserver
Device(config-sg-radius)# ip vrf forwarding vrf-intf
Device(config-sg-radius)# exit
Device(config)# cts authorization list cts-mlist
Device(config)# ip radius source-interface GigabitEthernet0 vrf vrf-intf
Device(config)# end
```

Example: Configuring VRF Connectivity to Cisco ISE

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet0
Device(config-if)# vrf forwarding vrf-intf
Device(config-if)# ip address 10.0.0.1 255.0.0.0
Device(config-if)# negotiation auto
Device(config-if)# end
```

Additional References for Cisco TrustSec VRF-Aware SGT

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Cisco IOS 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*
Cisco TrustSec overview	Overview of TrustSec
Cisco TrustSec solution	Cisco TrustSec Security Solution

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/cisco/web/support/index.html

Feature Information for Cisco TrustSec VRF-Aware SGT

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 14: Feature Information for Cisco TrustSec VRF-Aware SGT

Feature Name	Releases	Feature Information
Cisco TrustSec VRF-Aware SGT	Cisco IOS 15.1(2)SY1	The Cisco TrustSec VRF-Aware SGT feature allows the device to communicate with the RADIUS servers through the Virtual Routing and Forwarding (VRF) interfaces. This feature allows protected access credential (PAC) and Environment-Data to be requested from the authentication device, Cisco Identity Services Engine (Cisco ISE), when Cisco ISE is in a VRF network. The following command was introduced or modified: **pac key** *encryption-key*.