Cisco TrustSec Commands

cts authorization list

To specify a list of authentication, authorization, and accounting (AAA) servers to be used by the TrustSec seed device, use the **cts authorization list** command on the Cisco TrustSec seed device in global configuration mode. Use the **no** form of the command to stop using the list during authentication.

cts authorization list *server_list*

no cts authorization list *server_list*

Syntax Description

server_list	Cisco TrustSec AAA server group.

Command Default

None

Command Modes

Global configuration (config)

Supported User Roles

Administrator

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

This command is only for the seed device. Non-seed devices obtain the TrustSec AAA server list from their TrustSec authenticator peer as a component of their TrustSec environment data.

The following example displays an AAA configuration of a TrustSec seed device:

```
Device# cts credentials id Device1 password Cisco123
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
Device(config)# aaa authorization network MLIST group radius
Device(config)# cts authorization list MLIST
Device(config)# aaa accounting dot1x default start-stop group radius
Device(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key
AbCe1234
Device(config)# radius-server vsa send authentication
Device(config)# dot1x system-auth-control
Device(config)# exit
```

Related Commands

Command	Description
show cts server-list	Displays RADIUS server configurations.

cts credentials

Use the **cts credentials** command in privileged EXEC mode to specify the TrustSec ID and password of the network device. Use the **clear cts credentials** command to delete the credentials.

cts credentials id *cts_id* **password** *cts_pwd*

Syntax Description

credentials id *cts_id*	Specifies the Cisco TrustSec device ID for this device to use when authenticating with other Cisco TrustSec devices with EAP-FAST. The *cts-id* variable has a maximum length of 32 characters and is case sensitive.

password *cts_pwd*	Specifies the password for this device to use when authenticating with other Cisco TrustSec devices with EAP-FAST.

Command Default

None

Command Modes

Privileged EXEC (#)

Supported User Roles

Administrator

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

The **cts credentials** command specifies the Cisco TrustSec device ID and password for this device to use when authenticating with other Cisco TrustSec devices with EAP-FAST. The Cisco TrustSec credentials state retrieval is not performed by the nonvolatile generation process (NVGEN) because the Cisco TrustSec credential information is saved in the keystore, and not in the startup configuration. The device can be assigned a Cisco TrustSec identity by the Cisco Secure Access Control Server (ACS), or a new password auto-generated when prompted to do so by the ACS. These credentials are stored in the keystore, eliminating the need to save the running configuration. To display the Cisco TrustSec device ID, use the **show cts credentials** command. The stored password is never displayed.

To change the device ID or the password, reenter the command. To clear the keystore, use the **clear cts credentials** command.

Note When the Cisco TrustSec device ID is changed, all Protected Access Credentials (PACs) are flushed from the keystore because PACs are associated with the old device ID and are not valid for a new identity.

The following example shows how to configure the Cisco TrustSec device ID and password:

```
Device# cts credentials id cts1 password password1
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 show how to change the Cisco TrustSec device ID and password to cts_new and password123, respectively:

```
Device# cts credentials id cts_new pacssword password123
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 sample output displays the Cisco TrustSec device ID and password state:

```
Device# show cts credentials
```

```
CTS password is defined in keystore, device-id = cts_new
```

Related Commands

Command	Description
clear cts credentials	Clears the Cisco TrustSec device ID and password.
show cts credentials	Displays the state of the current Cisco TrustSec device ID and password.
show cts keystore	Displays contents of the hardware and software keystores.

cts refresh

To refresh the TrustSec peer authorization policy of all or specific Cisco TrustSec peers, or to refresh the SGACL policies downloaded to the device by the authentication server, use the **cts refresh** command in privileged EXEC mode.

cts refresh {**peer** [*peer_id*] | **sgt** [{*sgt_number* | **default** | **unknown**}]}

Syntax Description

environment-data	Refreshes environment data.
peer *Peer-ID*	(Optional) If a peer-id is specified, only policies related to the specified peer connection are refreshed.
sgt *sgt_number*	(Optional) Performs an immediate refresh of the SGACL policies from the authentication server. If an SGT number is specified, only policies related to that SGT are refreshed.
default	(Optional) Refreshes the default SGACL policy.
unknown	(Optional) Refreshes the unknown SGACL policy.

Command Default

None

Command Modes

Privileged EXEC (#)

Supported User Roles

Administrator

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

To refresh the Peer Authorization Policy on all TrustSec peers, enter **cts policy refresh** without specifying a peer ID.

The peer authorization policy is initially downloaded from the Cisco ACS at the end of the EAP-FAST NDAC authentication success. The Cisco ACS is configured to refresh the peer authorization policy, but the **cts policy refresh** command can force immediate refresh of the policy before the Cisco ACS timer expires. This command is relevant only to TrustSec devices that can impose Security Group Tags (SGTs) and enforce Security Group Access Control Lists (SGACLs).

The following example shows how to refresh the TrustSec peer authorization policy of all peers:

```
Device# cts policy refresh
Policy refresh in progress
```

The following sample output displays the TrustSec peer authorization policy of all peers:

```
VSS-1# show cts policy peer

CTS Peer Policy
===============
device-id of the peer that this local device is connected to
Peer name: VSS-2T-1
Peer SGT: 1-02
Trusted Peer: TRUE
Peer Policy Lifetime = 120 secs
Peer Last update time = 12:19:09 UTC Wed Nov 18 2009
Policy expires in 0:00:01:51 (dd:hr:mm:sec)
Policy refreshes in 0:00:01:51 (dd:hr:mm:sec)
Cache data applied = NONE
```

Related Commands

Command	Description
clear cts policy	Clears all Cisco TrustSec policies, or by the peer ID or SGT.
show cts policy peer	Displays peer authorization policy for all or specific TrustSec peers.

cts rekey

To regenerate the Pairwise Master Key used by the Security Association Protocol (SAP), use the **cts rekey** privileged EXEC command.

cts rekey interface type *slot/port*

Syntax Description

interface type *slot/port*	Specifies the Cisco TrustSec interface on which to regenerate the SAP key.

Command Default

None.

Command Modes

Privileged EXEC (#)

Supported User Roles

Administrator

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

SAP Pair-wise Master Key key (PMK) refresh ordinarily occurs automatically, triggered by combinations of network events and non-configurable internal timers related to dot1X authentication. The ability to manually refresh encryption keys is often part of network administration security requirements. To manually force a PMK refresh, use the **cts rekey** command.

TrustSec supports a manual configuration mode where dot1X authentication is not required to create link-to-link encryption between switches. In this case, the PMK is manually configured on devices on both ends of the link with the **sap pmk** Cisco TrustSec manual interface configuration command.

The following example shows how to regenerate the PMK on a specified interface:

```
Device# cts rekey interface gigabitEthernet 2/1
```

Related Commands

Command	Description
sap mode-list (cts manual)	Configures Cisco TrustSec SAP for manual mode.

cts role-based enforcement

To enable role-based access control globally and on specific Layer 3 interfaces using Cisco TrustSec, use the **cts role-based enforcement** command in global configuration mode and interface configuration mode respectively. To disable the enforcement of role-based access control at an interface level, use the **no** form of this command.

cts role-based enforcement
no cts role-based enforcement

Syntax Description

This command has no keywords or arguments.

Command Default

Enforcement of role-based access control at an interface level is disabled globally.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

The **cts role-based enforcement** command in global configuration mode enables role-based access control globally. Once role-based access control is enabled globally, it is automatically enabled on every Layer 3 interface on the device. To disable role-based access control on specific Layer 3 interfaces, use the **no** form of the command in interface configuration mode. The **cts role-based enforcement** command in interface configuration mode enables enforcement of role-based access control on specific Layer 3 interfaces.

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. The terms role-based access control list (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.

The following example shows how to enable role-based access control on a Gigabit Ethernet interface:

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

cts role-based l2-vrf

To select a virtual routing and forwarding (VRF) instance for Layer 2 VLANs, use the **cts role-based l2-vrf** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cts role-based l2-vrf *vrf-name* **vlan-list** {**all** *vlan-ID*} [{**,**}] [{**-**}]
no cts role-based l2-vrf *vrf-name* **vlan-list** {**all** *vlan-ID*} [{**,**}] [{**-**}]

Syntax Description

vrf-name	Name of the VRF instance.
vlan-list	Specifies the list of VLANs to be assigned to a VRF instance.
all	Specifies all VLANs.
vlan-ID	VLAN ID. Valid values are from 1 to 4094.
,	(Optional) Specifies another VLAN separated by a comma.
-	(Optional) Specifies a range of VLANs separated by a hyphen.

Command Default

VRF instances are not selected.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

The *vlan-list* argument can be a single VLAN ID, a list of comma-separated VLAN IDs, or hyphen-separated VLAN ID ranges.

The **all** keyword is equivalent to the full range of VLANs supported by the network device. The **all** keyword is not preserved in the nonvolatile generation (NVGEN) process.

If the **cts role-based l2-vrf** command is issued more than once for the same VRF, each successive command entered adds the VLAN IDs to the specified VRF.

The VRF assignments configured by the **cts role-based l2-vrf** command are active as long as a VLAN remains a Layer 2 VLAN. The IP–SGT bindings learned while a VRF assignment is active are also added to the Forwarding Information Base (FIB) table associated with the VRF and the IP protocol version. If an Switched Virtual Interface (SVI) becomes active for a VLAN, the VRF-to-VLAN assignment becomes inactive and all bindings learned on the VLAN are moved to the FIB table associated with the VRF of the SVI.

Use the **interface vlan** command to configure an SVI interface, and the **vrf forwarding** command to associate a VRF instance to the interface.

The VRF-to-VLAN assignment is retained even when the assignment becomes inactive. It is reactivated when the SVI is removed or when the SVI IP address is changed. When reactivated, the IP–SGT bindings are moved back from the FIB table associated with the VRF of the SVI to the FIB table associated with the VRF assigned by the **cts role-based l2-vrf** command.

The following example shows how to select a list of VLANS to be assigned to a VRF instance:

```
Device(config)# cts role-based l2-vrf vrf1 vlan-list 20
```

The following example shows how to configure an SVI interface and associate a VRF instance:

```
Device(config)# interface vlan 101
Device(config-if)# vrf forwarding vrf1
```

Related Commands

Command	Description
interface vlan	Configures a VLAN interface.
vrf forwarding	Associates a VRF instance or a virtual network with an interface or subinterface.
show cts role-based permissions	Displays the SGACL permission list.

cts role-based monitor

To enable role-based (security-group) access list monitoring, use the **cts role-based monitor** command in global configuration mode. To remove role-based access list monitoring, use the **no** form of this command.

cts role-based monitor {**all** | **permissions** {**default** [{**ipv4** | **ipv6**}] | **from** {*sgt* | **unknown**} **to** {*sgt* | **unknown**} [{**ipv4** | **ipv6**}]}}
no cts role-based monitor {**all** | **permissions** {**default** [{**ipv4** | **ipv6**}] | **from** {*sgt* | **unknown**} **to** {*sgt* | **unknown**} [{**ipv4** | **ipv6**}]}}

Syntax Description

all	Monitors permissions for all source tags to all destination tags.
permissions	Monitors permissions from a source tags to a destination tags.

default	Monitors the default permission list.
ipv4	(Optional) Specifies the IPv4 protocol.
ipv6	(Optional) Specifies the IPv6 protocol.
from	Specifies the source group tag for filtered traffic.
sgt	Security Group Tag (SGT). Valid values are from 2 to 65519.
unknown	Specifies an unknown source or destination group tag (DST).

Command Default

Role-based access control monitoring is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

Use the **cts role-based monitor all** command to enable the global monitor mode. If the **cts role-based monitor all** command is configured, the output of the **show cts role-based permissions** command displays monitor mode for all configured policies as true.

The following examples shows how to configure SGACL monitor from a source tag to a destination tag:

```
Device(config)# cts role-based monitor permissions from 10 to 11
```

Related Commands

Command	Description
show cts role-based permissions	Displays the SGACL permission list.

cts role-based permissions

To enable permissions from a source group to a destination group, use the **cts role-based permissions** command in global configuration mode. To remove the permissions, use the **no** form of this command.

cts role-based permissions {**default** | **from** {*sgt* | **unknown**}**to** {*sgt* | **unknown**}} {*rbacl-name* | **ipv4** | **ipv6**}
no cts role-based permissions {**default** | **from** {*sgt* | **unknown**}**to** {*sgt* | **unknown**}} {*rbacl-name* | **ipv4** | **ipv6**}

Syntax Description

default	Specifies the default permissions list. Every cell (an SGT pair) for which, security group access control list (SGACL) permission is not configured statically or dynamically falls under the default category.

from	Specifies the source group tag of the filtered traffic.
sgt	Security Group Tag (SGT). Valid values are from 2 to 65519.
unknown	Specifies an unknown source or destination group tag.
rbacl-name	Role-based access control list (RBACL) or SGACL name. Up to 16 SGACLs can be specified in the configuration.
ipv4	Specifies the IPv4 protocol.
ipv6	Specifies the IPv6 protocol.

Command Default

Permissions from a source group to a destination group is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

Use the **cts role-based permissions** command to define, replace, or delete the list of SGACLs for a given source group tag (SGT), destination group tag (DGT) pair. This policy is in effect as long as there is no dynamic policy for the same DGT or SGT.

The **cts role-based permissions default** command defines, replaces, or deletes the list of SGACLs of the default policy as long as there is no dynamic policy for the same DGT.

The following example shows how to enable permissions for a destination group:

```
Device(config)# cts role-based permissions from 6 to 6 mon_2
```

Related Commands

Command	Description
show cts role-based permissions	Displays the SGACL permission list.

cts role-based sgt-map

To manually map a source IP address to a Security Group Tag (SGT) on either a host or a VRF, use the **cts role-based sgt-map** command in global configuration mode. Use the **no** form of the command to remove the mapping.

cts role-based sgt-map {*ipv4_netaddress* | *ipv6_netaddress* | *ipv4_netaddress/prefix* | *ipv6_netaddress/prefix*} **sgt** *sgt-number*
cts role-based sgt-map host {*ipv4_hostaddress* | *ipv6_hostaddress*} **sgt** *sgt-number*
cts role-based sgt-map vlan-list [{*vlan_ids* | **all**}] **sgt** *sgt-number*

cts role-based sgt-map vrf *instance_name*
{*ipv4_netaddress* | *ipv6_netaddress* | *ipv4_netaddress/prefix* | *ipv6_netaddress/prefix* | **host**
{*ipv4_hostaddress* | *ipv6_hostaddress*}} **sgt** *sgt-number*
no cts role-based sgt-map

Syntax Description

ipv4_netaddress | **ipv6_netaddress**	Specifies the network to be associated with an SGT. Enter IPv4 address in dot decimal notation; IPv6 in colon hexadecimal notation.
ipv4_netaddress/prefix | **ipv6_netaddress/prefix**	Maps the SGT to all hosts of the specified subnet address (IPv4 or IPv6). IPv4 is specified in dot decimal CIDR notation, IPv6 in colon hexadecimal notation
host {*ipv4_hostaddress* | *ipv6_hostaddress*}	Binds the specified host IP address with the SGT. Enter the IPv4 address in dot decimal notation; IPv6 in colon hexadecimal notation.
vlan-list {*vlan_ids* | **all**}	Specifies VLAN IDs. • (Optional) *vlan_ids*: Individual VLAN IDs are separated by commas, a range of IDs specified with a hyphen. • (Optional) **all**: Specifies all VLAN IDs.
vrf *instance_name*	Specifies a VRF instance, previously created on the device.
sgt *sgt-number*	Specifies the SGT number from 0 to 65,535.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

If you do not have a Cisco Identity Services Engine, Cisco Secure ACS, dynamic Address Resolution Protocol (ARP) inspection, Dynamic Host Control Protocol (DHCP) snooping, or Host Tracking available on your device to automatically map SGTs to source IP addresses, you can manually map an SGT to the following with the **cts role-based sgt-map** command:

- A single host IPv4 or IPv6 address
- All hosts of an IPv4 or IPv6 network or subnetwork
- VRFs
- Single or multiple VLANs

The **cts role-based sgt-map** command binds the specified SGT with packets that fall within the specified network address.

SXP exports an exhaustive expansion of all possible individual IP–SGT bindings within the specified network or subnetwork. IPv6 bindings and subnet bindings are exported only to SXP listener peers of SXP version 2 or later. The expansion does not include host bindings which are known individually or are configured or learnt from SXP for any nested subnet bindings.

The **cts role-based sgt-map host** command binds the specified SGT with incoming packets when the IP source address is matched by the specified host address. This IP-SGT binding has the lowest priority and is ignored in the presence of any other dynamically discovered bindings from other sources (such as, SXP or locally authenticated hosts). The binding is used locally on the device for SGT imposition and SGACL enforcement. It is exported to SXP peers if it is the only binding known for the specified host IP address.

The **vrf** keyword specifies a virtual routing and forwarding table previously defined with the vrf definition global configuration command. The IP-SGT binding specified with the **cts role-based sgt-map vrf** global configuration command is entered into the IP-SGT table associated with the specified VRF and the IP protocol version which is implied by the type of IP address entered.

The **cts role-based sgt-map vlan-list** command binds an SGT with a specified VLAN or a set of VLANs. The keyword **all** is equivalent to the full range of VLANs supported by the device and is not preserved in the nonvolatile generation (NVGEN) process. The specified SGT is bound to incoming packets received in any of the specified VLANs. The system uses discovery methods such as DHCP and/or ARP snooping (a.k.a. IP device tracking) to discover active hosts in any of the VLANs mapped by this command. Alternatively, the system could map the subnet associated with the SVI of each VLAN to the specified SGT. SXP exports the resulting bindings as appropriate for the type of binding.

Examples

The following example shows how to manually map a source IP address to an SGT:

```
Device(config)# cts role-based sgt-map 10.10.1.1 sgt 77
```

In the following example, a device binds host IP address 10.1.2.1 to SGT 3 and 10.1.2.2 to SGT 4. These bindings are forwarded by SXP to an SGACL enforcement device.

```
Device(config)# cts role-based sgt-map host 10.1.2.1 sgt 3
Device(config)# cts role-based sgt-map host 10.1.2.2 sgt 4
```

Related Commands

Command	Description
show cts role-based sgt-map	Displays role-based access control information.

cts sxp connection peer

To enter the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) peer IP address, to specify if a password is used for the peer connection, to specify the global hold-time period for a listener or speaker device, and to specify if the connection is bidirectional, use the **cts sxp connection peer** command in global configuration mode. To remove these configurations for a peer connection, use the **no** form of this command.

cts sxp connection peer *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [{[[{**listener** | **speaker**}] [{**hold-time** *minimum-time maximum-time* | **vrf** *vrf-name*}]] | **both** [**vrf** *vrf-name*]}]

cts sxp connection peer *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [{[[{**listener** | **speaker**}] [{**hold-time** *minimum-time maximum-time* | **vrf** *vrf-name*}]] | **both** [**vrf** *vrf-name*]}]

Syntax Description

ipv4-address	SXP peer IPv4 address.
source	Specifies the source IPv4 address.
password	Specifies that an SXP password is used for the peer connection.
default	Specifies that the default SXP password is used.
none	Specifies no password is used.
mode	Specifies either the local or peer SXP connection mode.
local	Specifies that the SXP connection mode refers to the local device.
peer	Specifies that the SXP connection mode refers to the peer device.
listener	(Optional) Specifies that the device is the listener in the connection.
speaker	(Optional) Specifies that the device is the speaker in the connection.
hold-time *minimum-time maximum-time*	(Optional) Specifies the hold-time period, in seconds, for the device. The range for minimum and maximum time is from 0 to 65535. A *maximum-time* value is required only when you use the following keywords: **peer speaker** and **local listener**. In other instances, only a *minimum-time* value is required. **Note** If both minimum and maximum times are required, the *maximum-time* value must be greater than or equal to the *minimum-time* value.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) instance name to the peer.
both	(Optional) Specifies that the device is both the speaker and the listener in the bidirectional SXP connection.

Command Default

The CTS-SXP peer IP address is not configured and no CTS-SXP peer password is used for the peer connection.

The default setting for a CTS-SXP connection password is **none**.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

When a CTS-SXP connection to a peer is configured with the **cts sxp connection peer** command, only the connection mode can be changed. The **vrf** keyword is optional. If a VRF name is not provided or a VRF name is provided with the **default** keyword, then the connection is set up in the default routing or forwarding domain.

A **hold-time** *maximum-period* value is required only when you use the following keywords: **peer speaker** and **local listener**. In other instances, only a **hold-time** *minimum-period* value is required.

> **Note** The *maximum-period* value must be greater than or equal to the *minimum-period* value.

Use the **both** keyword to configure a bidirectional SXP connection. With the support for bidirectional SXP configuration, a peer can act as both a speaker and a listener and propagate SXP bindings in both directions using a single connection.

Examples

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_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 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_B> enable
Device_B# 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
```

You can also configure both peer and source IP addresses for an SXP connection. The source IP address specified in the **cts sxp connection** command overwrites the default value.

```
Device_A(config)# cts sxp connection peer 51.51.51.1 source 51.51.51.2 password none mode
local speaker
```

```
Device_B(config)# cts sxp connection peer 51.51.51.2 source 51.51.51.1 password none mode
local listener
```

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
```

Related Commands

Command	Description
cts sxp default password	Configures the Cisco TrustSec SXP default password.
cts sxp default source-ip	Configures the Cisco TrustSec SXP source IPv4 address.
cts sxp enable	Enables Cisco TrustSec SXP on a device.
cts sxp log	Enables logging for IP-to-SGT binding changes.
cts sxp reconciliation	Changes the Cisco TrustSec SXP reconciliation period.
cts sxp retry	Changes the Cisco TrustSec SXP retry period timer.
cts sxp speaker hold-time	Configures the global hold-time period of a speaker device in a Cisco TrustSec SGT SXPv4 network.
cts sxp listener hold-time	Configures the global hold-time period of a listener device in a Cisco TrustSec SGT SXPv4 network.
show cts sxp	Displays the status of all Cisco TrustSec SXP configurations.

cts sxp default password

To specify the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) default password, use the **cts sxp default password** command in global configuration mode. To remove the CTS-SXP default password, use the **no** form of this command.

cts sxp default password {**0** *unencrypted-pwd* | **6** *encrypted-key* | **7** *encrypted-keycleartext-pwd*}
no cts sxp default password {**0** *unencrypted-pwd* | **6** *encrypted-key* | **7** *encrypted-keycleartext-pwd*}

Syntax Description

0 *unencrypted-pwd*	Specifies that an unencrypted CTS-SXP default password follows. The maximum password length is 32 characters.
6 *encrypted-key*	Specifies that a 6 encryption type password is used as the CTS-SXP default password. The maximum password length is 32 characters.
7 *encrypted-key*	Specifies that a 7 encryption type password is used as the CTS-SXP default password. The maximum password length is 32 characters.
cleartext-pwd	Specifies a cleartext CTS-SXP default password. The maximum password length is 32 characters.

Command Default

Type **0** (cleartext)

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

The **cts sxp default password** command sets the CTS-SXP default password to be optionally used for all CTS-SXP connections configured on the device. The CTS-SXP password can be cleartext, or encrypted with the **0**, **7**, **6** encryption type keywords. If the encryption type is 0, then an unencrypted cleartext password follows.

Examples

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_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 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_B# 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
```

Related Commands

Command	Description
cts sxp connection peer	Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection.
cts sxp default source-ip	Configures the CTS-SXP source IPv4 address.
cts sxp enable	Enables CTS-SXP on a device.
cts sxp log	Enables logging for IP-to-SGT binding changes.
cts sxp reconciliation	Changes the CTS-SXP reconciliation period.
cts sxp retry	Changes the CTS-SXP retry period timer.
show cts sxp	Displays the status of all SXP configurations.

cts sxp default source-ip

To configure the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) source IPv4 address, use the **cts sxp default source-ip** command in global configuration mode. To remove the CTS-SXP default source IP address, use the **no** form of this command.

cts sxp default source-ip *ipv4-address*
no cts sxp default source-ip *ipv4-address*

Syntax Description

ip-address	Default source CTS-SXP IPv4 address.

Command Default

The CTS-SXP source IP address is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

The **cts sxp default source-ip** command sets the default source IP address that CTS-SXP uses for all new TCP connections where a source IP address is not specified. Preexisting TCP connections are not affected when this command is entered. CTS-SXP connections are governed by three timers:

- Retry timer
- Delete Hold Down timer
- Reconciliation timer

Examples

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_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 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_B# 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
```

Related Commands

Command	Description
cts sxp connectionpeer	Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection.
cts sxp default password	Configures the CTS-SXP default password.
cts sxp enable	Enables CTS-SXP on a device.

Command	Description
cts sxp log	Enables logging for IP-to-SGT binding changes.
cts sxp reconciliation	Changes the CTS-SXP reconciliation period.
cts sxp retry	Changes the CTS-SXP retry period timer.
show cts sxp	Displays the status of all SXP configurations.

cts sxp filter-enable

To enable filtering after creating filter lists and filter groups, use the **cts sxp filter-enable** command in global configuration mode. To disable filtering, use the **no** form of the command.

cts sxp filter-enable
no cts sxp filter-enable

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

This command can be used at any time to enable or disable filtering. Configured filter lists and filter groups can be used to implement filtering only after filtering is enabled. The filter action will only filter bindings that are exchanged after filtering is enabled; there won’t be any effect on the bindings that were exchanged before filtering was enabled.

Examples

```
Device(config)# cts sxp filter-enable
```

Related Commands

Command	Description
cts sxp filter-list	Creates a SXP filter list to filter IP-SGT bindings based on IP prefixes, SGT or a combination of both.
cts sxp filter-group	Creates a filter group for grouping a set of peers and applying a filter list to them.
show cts sxp filter-group	Displays information about the configured filter groups..
show cts sxp filter-list	Displays information about the configured filter lists.
debug cts sxp filter events	Logs events related to the creation, deletion and update of filter-lists and filter-groups

cts sxp filter-group

To create a filter group for grouping a set of peers and applying a filter list to them, use the **cts sxp filter-group** command in global configuration mode. To delete a filter group, use the **no** form of this command.

cts sxp filter-group {**listener** | **speaker**} {*filter-group-name* | **global** *filter-list-name*}
no cts sxp filter-group {**listener** | **speaker**} {*filter-group-name* | **global** *filter-list-name*}

Syntax Description

listener	Creates a filter group for a set of listeners.
speaker	Creates a filter group for a set of speakers.
global	Groups all speakers or listeners on the device.
filter-group-name	Name of the filter group.
filter-list-name	Name of the filter list.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

Issuing this command, places the device in the filter group configuration mode. From this mode, you can specify the devices to be grouped and apply a filter list to the filter group.

The command format to add devices or peers to the group is a follows:

peer ipv4 *peer-IP*

In a single command, you can add one peer. To add more peers, repeat the command as many times as required.

The command format to apply a filter list to the group is as follows:

filter *filter-list-name*

You cannot specify a peer list for the global listener and global speaker filter-group options because in this case the filter is applied to all SXP connections.

When both the global filter group and peer-based filter groups are applied, the global filter takes priority. If only a global listener or global speaker filter group is configured, then the global filtering takes precendence only in that specific direction. For the other direction, the peer-based filter group is implemented.

Examples

The following example shows how to create a listener group called `group_1`, and assign peers and a filter list to this group:

```
Device# configure terminal
Device(config)# cts sxp filter-group listener group_1
Device(config-filter-group)# filter filter_1
Device(config-filter-group)# peer ipv4 10.0.0.1
Device(config-filter-group)# peer ipv4 10.10.10.1
```

The following example shows how to create a global listener group called `group_2`:

```
Device# configure terminal
Device(config)# cts sxp filter-group listener global group_2
```

Related Commands

Command	Description
cts sxp filter-list	Creates a SXP filter list to filter IP-SGT bindings based on IP prefixes, SGT or a combination of both.
cts sxp filter-enable	Enables filtering.
show cts sxp filter-group	Displays information about the configured filter groups.
show cts sxp filter-list	Displays information about the configured filter lists.
debug cts sxp filter events	Logs events related to the creation, deletion and update of filter-lists and filter-groups

cts sxp filter-list

To create a SXP filter list to hold a set of filter rules for filtering IP-SGT bindings, use the **cts sxp filter-list** command in global configuration mode. To delete a filter list, use the **no** form of the command.

cts sxp filter-list *filter-list-name*
no cts sxp filter-list *filter-list-name*

Syntax Description

filter-list-name	Name of the filter-list.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

Issuing this command, places the device in the filter list configuration mode. From this mode, you can specify rules for the filter lists.

A filter rule can be based on SGT or IP Prefixes or a combination of both SGT and IP Prefixes.

The command format to add rules to the group is a follows:

sequence-number **action(permit/deny)** **filter-type(ipv4/ipv6/sgt)** *value/values*

For example, to permit SGT-IP bindings whose SGT value is 20, the rule is as follows:

```
30 permit sgt 20
```

Note that the sequence number is optional. If you do not specify a sequence number, it is generated by the system. Sequence numbers are automatically incremented by a value of 10 from the last used/configured sequence number. A new rule can be inserted by specifying a sequence number in between two existing rules.

The range of valid SGT values is between 2 and 65519. To provide multiple SGT values in a rule, seperate the values using a space. A maximum of 8 SGT values are allowed in a rule.

In a SGT and IP prefix combination rule, if there is a match for the binding in both the parts of the rule, then the action specified in the second part of the rule takes precedence. For example, in the following rule, if the SGT value of the IP prefix 10.0.0.1 is 20, the corresponding binding will be denied even if the first part of the rule permits the binding.

```
Device(config-filter-list)# 10 permit sgt 30 20 deny 10.0.0.1/24
```

Similarly, in the rule below the binding with the sgt value 20 will be permitted even if the sgt of the IP prefix 10.0.0.1 is 20, and the first action does not permit the binding.

```
Device(config-filter-list)# 10 deny 10.0.0.1/24 permit sgt 30 20
```

Examples

The following example shows how to create a filter list and add some rules to the list:

```
Device# configure terminal
Device(config)# cts sxp filter-list filter_1
Device (config-filter-list)# 10 deny ipv4 10.0.0.1/24 permit sgt 100
Device(config-filter-list)# 20 permit sgt 60 61 62 63
```

Related Commands

Command	Description
cts sxp filter-enable	Enable SXP IP-prefix and SGT-based filtering.
cts sxp filter-group	Creates a filter group for grouping a set of peers and applying a filter list to them.
show cts sxp filter-group	Displays information about the configured filter groups.
show cts sxp filter-list	Displays information about the configured filter lists.
debug cts sxp filter events	Logs events related to the creation, deletion and update of filter-lists and filter-groups.

cts sxp log binding-changes

To enable logging for IP-to-Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) binding changes, use the **cts sxp log binding-changes** command in global configuration mode. To disable logging, use the **no** form of this command.

cts sxp log binding-changes
no cts sxp log binding-changes

Command Default

Logging is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

The **cts sxp log binding-changes** command enables logging for IP-to-SGT binding changes. SXP syslogs (sev 5 syslogs) are generated whenever IP address-to-SGT binding occurs (add, delete, change). These changes are learned and propagated on the SXP connection.

Related Commands

Command	Description
cts sxp connectionpeer	Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection
cts sxp default password	Configures the CTS-SXP default password.
cts sxp default source-ip	Configures the CTS-SXP source IPv4 address.
cts sxp enable	Enables CTS-SXP on a device.
cts sxp reconciliation	Changes the CTS-SXP reconciliation period.
cts sxp retry	Changes the CTS-SXP retry period timer.
show cts sxp	Displays status of all SXP configurations.

cts sxp reconciliation period

To change the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) reconciliation period, use the **cts sxp reconciliation period** command in global configuration mode. To return the CTS-SXP reconciliation period to its default value, use the **no** form of this command.

cts sxp reconciliation period *seconds*
no cts sxp reconciliation period *seconds*

Syntax Description

seconds	CTS-SXP reconciliation timer in seconds. The range is from 0 to 64000. The default is 120.

Command Default

120 seconds (2 minutes)

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

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

Related Commands

Command	Description
cts sxp connection peer	Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection.
cts sxp default password	Configures the CTS-SXP default password.
cts sxp default source-ip	Configures the CTS-SXP source IPv4 address.
cts sxp enable	Enables CTS-SXP on a device.
cts sxp log	Turns on logging for IP to SGT binding changes.
cts sxp retry	Changes the CTS-SXP retry period timer.
show cts sxp	Displays status of all CTS-SXP configurations.

cts sxp retry period

To change the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) retry period timer, use the **cts sxp retry period** command in global configuration mode. To return the CTS-SXP retry period timer to its default value, use the **no** form of this command.

cts sxpretry period *seconds*
no cts sxpretry period *seconds*

Syntax Description

seconds	CTS-SXP retry timer in seconds. The range is from 0 to 64000. The default is 120.

Command Default

120 seconds (2 minutes)

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

The retry timer is triggered if there is at least one CTS-SXP connection that is not up. A new CTS-SXP connection is attempted when this timer expires. A zero value results in no retry being attempted.

Related Commands

Command	Description
cts sxp connectionpeer	Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection.
cts sxp default password	Configures the CTS-SXP default password.
cts sxp default source-ip	Configures the CTS-SXP source IPv4 address.
cts sxp enable	Enables CTS-SXP on a device.
cts sxp log	Enables logging for IP-to-SGT binding changes.
cts sxp reconciliation	Changes the CTS-SXP reconciliation period.
show cts sxp	Displays the status of all CTS-SXP configurations.

propagate sgt (cts manual)

To enable Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces, use the **propagate sgt** command in interface configuration mode. To disable SGT propagation, use the **no** form of this command.

propagate sgt

Syntax Description

This command has no arguments or keywords.

Command Default

SGT processing propagation is enabled.

Command Modes

CTS manual interface configuration mode (config-if-cts-manual)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

SGT processing propagation allows a CTS-capable interface to accept and transmit a CTS Meta Data (CMD) based L2 SGT tag. The **no propagate sgt** command can be used to disable SGT propagation on an interface in situations where a peer device is not capable of receiving an SGT, and as a result, the SGT tag cannot be put in the L2 header.

Examples

The following example shows how to disable SGT propagation on a manually-configured TrustSec-capable interface:

```
Device# configure terminal
Device(config)# interface gigabitethernet 0
Device(config-if)# cts manual
Device(config-if-cts-manual)# no propagate sgt
```

The following example shows that SGT propagation is disabled on Gigabit Ethernet interface 0:

```
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
```

Related Commands

Command	Description
cts manual	Enables an interface for CTS.
show cts interface	Displays Cisco TrustSec states and statistics per interface.

show cts credentials

To display the Cisco TrustSec (CTS) device ID, use the **show cts credentials** command in EXEC or privileged EXEC mode.

show cts credentials

Syntax Description

This command has no commands or keywords.

Command Modes

Privileged EXEC (#) User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Examples

The following example displays output:

```
Device# show cts credentials

CTS password is defined in keystore, device-id = r4
```

Related Commands

Command	Description
cts credentials	Specifies the TrustSec ID and password.

show cts interface

To display Cisco TrustSec (CTS) configuration statistics for an interface(s), use the **show cts interface** command in EXEC or privileged EXEC mode.

show cts interface [{**GigabitEthernet** *port* | **Vlan** *number* | **brief** | **summary**}]

Syntax Description

port	(Optional) Gigabit Ethernet interface number. A verbose status output for this interface is returned.
number	(Optional) VLAN interface number from 1 to 4095.
brief	(Optional) Displays abbreviated status for all CTS interfaces.
summary	(Optional) Displays a tabular summary of all CTS interfaces with 4 or 5 key status fields for each interface.

Command Default

None

Command Modes

EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

Use the **show cts interface** command without keywords to display verbose status for all CTS interfaces.

Examples

The following example displays output without using a keyword (verbose status for all CTS interfaces):

```
Device# show cts interface

Global Dot1x feature is Disabled
 Interface GigabitEthernet0/1/0:
     CTS is enabled, mode:    MANUAL
     IFC state:               OPEN
     Interface Active for 00:00:18.232
     Authentication Status:   NOT APPLICABLE
         Peer identity:       "unknown"
         Peer's advertised capabilities: ""
     Authorization Status:    NOT APPLICABLE
     SAP Status:              NOT APPLICABLE
         Configured pairwise ciphers:
             gcm-encrypt
             null

         Replay protection:      enabled
         Replay protection mode: STRICT

         Selected cipher:
```

```
     Propagate SGT:           Enabled
     Cache Info:
         Cache applied to link : NONE

     Statistics:
         authc success:              0
         authc reject:               0
         authc failure:              0
         authc no response:          0
         authc logoff:               0
         sap success:                0
         sap fail:                   0
         authz success:              0
         authz fail:                 0
         port auth fail:             0
         Ingress:
             control frame bypassed: 0
             sap frame bypassed:     0
             esp packets:            0
             unknown sa:             0
             invalid sa:             0
             inverse binding failed: 0
             auth failed:            0
             replay error:           0
         Egress:
             control frame bypassed: 0
             esp packets:            0
             sgt filtered:           0
             sap frame bypassed:     0
             unknown sa dropped:     0
             unknown sa bypassed:    0
```

The following example displays output using the **brief** keyword:

```
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
```

Related Commands

Command	Description
cts manual	Enables an interface for CTS.
cts sxp enable	Configures SXP on a network device.
propagate sgt	Enables Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces.

show cts role-based permissions

To display the role-based (security group) access control permission list, use the **show cts role-based permissions** command in privileged EXEC mode.

show cts role-based permissions [{**default** [{**details** | **ipv4 [details]** | **ipv6 [details]**}] | **from {**{*sgt* | **unknown** }[{**ipv4** | **ipv6** | **to {**{*sgt* | **unknown**}[{**details** | **ipv4 [details]** | **ipv6 [details]**}]**}}**}] | **ipv4** | **ipv6** | **platform** | **to** {*sgt* | **unknown**}[{**ipv4** | **ipv6**}]}]

Syntax Description

default	(Optional) Displays information about the default permission list.
details	(Optional) Displays attached access control list (ACL) details.
ipv4	(Optional) Displays information about the IPv4 protocol.
ipv6	(Optional) Displays information about the IPv6 protocol.
from	(Optional) Displays information about the source group.
sgt	(Optional) Security Group Tag. Valid values are from 2 to 65519.
to	(Optional) Displays information about the destination group.
unknown	(Optional) Displays information about unknown source and destination groups.
platform	(Optional) Displays information about the platform.

Command Modes

Privileged EXE (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

This command displays the content of the SGACL permission matrix. You can specify the source security group tag (SGT) by using the **from** keyword and the destination SGT by using the **to** keyword. When both these keywords are specified RBACLs of a single cell are displayed. An entire column is displayed when only the **to** keyword is used. An entire row is displayed when the **from** keyword is used. The entire permission matrix is displayed when both the **from** and **to** keywords are omitted.

The command output is sorted by destination SGT as a primary key and the source SGT as a secondary key. SGACLs for each cell is displayed in the same order they are defined in the configuration or acquired from Cisco Identity Services Engine (ISE).

The **details** keyword is provided when a single cell is selected by specifying both **from** and **to** keywords. When the **details** keyword is specified the access control entries of SGACLs of a single cell are displayed.

The following is sample output from the **show role-based permissions** command:

```
Device# show cts role-based permissions
```

```
IPv4 Role-based permissions default (monitored):
default_sgacl-02
Permit IP-00
IPv4 Role-based permissions from group 305:sgt to group 306:dgt (monitored):
test_reg_tcp_permit-02
RBACL Monitor All for Dynamic Policies : TRUE
RBACL Monitor All for Configured Policies : FALSE
IPv4 Role-based permissions from group 6:SGT_6 to group 6:SGT_6 (configured):
  mon_1
IPv4 Role-based permissions from group 10 to group 11 (configured):
  mon_2
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

Related Commands

Command	Description
cts role-based permissions	Enables permissions from a source group to a destination group.
cts role-based monitor	Enables role-based access list monitoring.

show cts server-list

To display the list of RADIUS servers available to Cisco TrustSec (CTS) seed and nonseed devices, use the **show cts server-list** command in user EXEC or privileged EXEC mode.

show cts server-list

Syntax Description

This command has no commands or keywords.

Command Modes

Privileged EXEC (#) User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

This command is useful for gathering CTS RADIUS server address and status information.

Examples

The following example displays the CTS RADIUS server list:

```
Device> show cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)
Preferred list, 1 server(s):
 *Server: 10.0.1.6, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
          Status = ALIVE
          auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
```

```
Installed list: ACSServerList1-0001, 1 server(s):
 *Server: 101.0.2.61, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
          Status = ALIVE
          auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
```

Related Commands

Command	Description
address ipv4 (config-radius-server)	Configures the RADIUS server accounting and authentication parameters for PAC provisioning.
pac key	Specifies the PAC encryption key.

show cts sxp

To display Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) connection or source IP-to-SGT mapping information, use the **show cts sxp** command in user EXEC or privileged EXEC mode.

show cts sxp {**connections** [{**brief** | **vrf** *instance-name*}] | **filter-group** [{**detailed** | **global** | **listener** | **speaker** }] | **filter-list** *filter-list-name* | **sgt-map** [{**brief** | **vrf** *instance-name*}]} [{**brief** | **vrf** *instance-name*}]

Syntax Description

connections	Displays Cisco TrustSec SXP connections information.
brief	(Optional) Displays an abbreviation of the SXP information.
vrf *instance-name*	(Optional) Displays the SXP information for the specified Virtual Routing and Forwarding (VRF) instance name.
filter-group {**detailed | global | listener | speaker** }	(Optional) Displays filter group information.
filter-list *filter-list-name*	(Optional) Displays filter list information.
sgt-map	(Optional) Displays the IP-to-SGT mappings received through SXP.

Command Default

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Examples

The following example displays the SXP connections using the **brief** keyword:

```
Device# show cts sxp connection brief

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
-----------------------------------------------------------------------------
Peer_IP          Source_IP        Conn Status       Duration
-----------------------------------------------------------------------------
10.10.10.1          10.10.10.2          On                0:00:02:14 (dd:hr:mm:sec)
10.10.2.1          10.10.2.2          On                0:00:02:14 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

The following example displays the CTS-SXP connections:

```
Device# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP          : 10.10.10.1
Source IP        : 10.10.10.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
----------------------------------------------
Peer IP          : 10.10.2.1
Source IP        : 10.10.2.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
TCP conn fd      : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

The following example displays the CTS-SXP connections for a bi-directional connection when the device is both the speaker and listener:

```
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)
```

The following example displays output from a CTS-SXP listener with a torn down connection to the SXP speaker. Source IP-to-SGT mappings are held for 120 seconds, the default value of the delete hold down timer.

```
Device# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP          : 10.10.10.1
Source IP        : 10.10.10.2
Set up           : Peer
Conn status      : Delete_Hold_Down
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : -1
TCP conn password: not set (using default SXP password)
Delete hold down timer is running
Duration since last state change: 0:00:00:16 (dd:hr:mm:sec)
----------------------------------------------
Peer IP          : 10.10.2.1
Source IP        : 10.10.2.2
Set up           : Peer
Conn status      : On
Connection inst# : 1
TCP conn fd      : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:05:49 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

Related Commands

Command	Description
cts sxp connection peer	Enters the Cisco TrustSec SXP peer IP address and specifies if a password is used for the peer connection
cts sxp default password	Configures the Cisco TrustSec SXP default password.
cts sxp default source-ip	Configures the Cisco TrustSec SXP source IPv4 address.
cts sxp enable	Enables Cisco TrustSec SXP on a device.
cts sxp log	Enables logging for IP-to-SGT binding changes.
cts sxp reconciliation	Changes the Cisco TrustSec SXP reconciliation period.

Command	Description
cts sxp retry	Changes the Cisco TrustSec SXP retry period timer.