Cisco TrustSec

aaa authorization network

To set authorization for all network-related service requests, use the **aaa authorization network** command in global configuration mode.

aaa authorization network *authorization-list-name* [{ **group** }] *group_name*

Syntax Description

authorization-list-name	Character string used to name the list of authorization methods activated when a user logs in.
group	Uses a subset of RADIUS servers for authentication as defined by the server group **group-name**
group_name	Server group name.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Examples

The following example shows how to set an authorization method list to the RADIUS server group in local web authentication

```
Device# config-transaction
Device(config)# aaa authorization network webauth_radius group ISE_group
Device(config)#
```

aaa group server radius

To group different RADIUS server hosts into distinct lists and distinct methods, enter the **aaa group server radius** command in global configuration mode. To remove a group server from the configuration list, enter the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE aaa group server radius

Examples

The following example shows the configuration of an AAA group server named radgroup1 that comprises three member servers:

```
Device# config-transaction
Device(config)# aaa group server radius radgroup1
Device(config-sg-radius)#server-private 10.251.1.1 timeout 5 retransmit 3 pac key 6
JTfGZMb[edH[G_V[MfQYKN^N]QeeBbLeB
Device(config-sg-radius)#ip radius source-interface GigabitEthernet0/0/1.100
Device(config-sg-radius)#ip vrf forwarding 1
Device(config-sg-radius)#
```

Note If auth-port and acct-port are not specified, the default value of auth-port is 1812 and the default value of acct-port is 1813.

aaa server radius dynamic-author

To configure a device as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server, use the **aaa server radius dynamic-author**command in global configuration mode. To remove this configuration, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE aaa server radius dynamic-author

Examples

The following example configures the ISG to act as a AAA server when interacting with the client at IP address 10.12.12.12:

```
Device# config-transaction
Device#(config)# aaa server radius dynamic-author
Device#(config-locsvr-da-radius)# client 10.12.12.12 vrf 1 server-key 6
PhHSFDUiS_abVCScDPYgYPJgXYXP[A^DY
Device#(config-locsvr-da-radius)#
```

accept-lifetime

To set the time period during which the authentication key on a key chain is received as valid, use the **accept-lifetime**command inkey chain key configuration mode. To revert to the default value, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE accept-lifetime

Examples

The following show how to specify the time entered in Cisco vManage for which the key is valid to be accepted for TCP-AO authentication.

Specify the start-time in the local time zone. By default, the start-time corresponds to UTC time. The end-time can be specified in 3 ways - infinite (no expiry), duration (1- 2147483646 sec), exact time – either UTC or local.

```
Device# config-transaction
Device(config)#key chain key6 tcp
Device(config-keychain)# key 2000
Device(config-keychain-key)# accept-lifetime local 18:00:00 Jan 12 2021 06:00:00 Jan 12
2022
Device(config-keychain-key)#
```

client

To specify a RADIUS client from which a device will accept Change of Authorization (CoA) and disconnect requests, use the **client** command in dynamic authorization local server configuration mode. To remove this specification, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE client

Examples

The following example configures the router to accept requests from the RADIUS client at IP address 10.0.0.1:

```
Device# config-transaction
Device#(config)# aaa server radius dynamic-author
Device#(config-locsvr-da-radius)# client 10.0.0.1 vrf 1 server-key 6
gWTLbecJKOQcFcIbJNR[]WKP_g^TRacRF
Device#(config)#
```

cryptographic-algorithm

To specify the TCP cryptographic algorithm for a TCP-AO key, use the **cryptographic-algorithm** command in key chain key configuration mode. To disable this feature, use the **no** form of this command.

cryptographic-algorithm *algorithm*

no cryptographic-algorithm *algorithm*

Syntax Description

algorithm	Specify one of the following authentication algorithms: • `aes-128-cmac`- AES-128-CMAC algorithm • `hmac-sha-1`- HMAC-SHA-1 algorithm • `hmac-sha-256`- HMAC-SHA-256 algorithm

Command Default

No algorithm is specified.

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the **key chain** command, you enter key chain configuration mode.

The following example configures a simple key chain for a TCP-AO enabled connection.

```
Device#config-transaction
Device(config)# key chain kc1 tcp
Device(config-keychain)# key 7890
Device(config-keychain-key)# send-id 215
Device(config-keychain-key)# recv-id 215
Device(config-keychain-key)# key-string klomn
Device(config-keychain-key)# cryptographic-algorithm hmac-sha-1
Device(config-keychain-key)#
```

cts authorization list network

To specify a list of AAA servers for the Cisco TrustSec (CTS) seed device to use, use the **cts authorization list network** command in global configuration mode. To stop using the list during authentication, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts authorization list network

Examples

The following example shows how to specify a list of AAA servers for a CTS seed device:

```
Device# config-transaction
Device(config)# aaa group server radius radgroup1
Device(config-sg-radius)#server-private 10.251.1.1 timeout 5 retransmit 3 pac key 6
JTfGZMb[edH[G_V[MfQYKN^N]QeeBbLeB
Device(config-sg-radius)#ip radius source-interface GigabitEthernet0/0/1.100
```

```
Device(config-sg-radius)#ip vrf forwarding 1
Device(config-sg-radius)#
```

```
Device# config-transaction
Device(config)# aaa authentication enable default enable
Device(config)# aaa authentication login default local group radius-1
Device(config)# aaa authorization console
Device(config)# aaa authorization exec default local group radius-1
Device(config)# aaa authorization network cts-mlist group radius-1
Device(config)#
```

```
Device# config-transaction
Device(config)# cts authorization list cts-mlist
Device(config)#
```

cts credentials

To specify the Cisco TrustSec (CTS) ID and password of the network device, use the **cts credentials** command in privileged EXEC mode. To delete the CTS credentials, use the **clear cts credentials** command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts credentials

Examples

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

```
Device# 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:

```
Device# 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:

```
Device# show cts credentials

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

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.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts role-based enforcement

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

```
Device# config-transaction
Device(config)# interface gigabitethernet 1/1/3
Device(config-if)# cts role-based enforcement
Device(config-if)#
```

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** | [{ *source-sgt* }] | **to** | [{ *dest-sgt* }] }] } }

no cts role-based permissions { { [{ **default** | **from** | [{ *source-sgt* }] | **to** | [{ *dest-sgt* }] }] } }

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.
source-sgt	Security Group Tag (SGT). Valid values are from 0 to 65519.
dest-sgt	Security Group Tag (SGT). Valid values are from 2 to 65519.

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 Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

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** 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.

Examples

The following example shows how to enter CTS manual interface configuration mode on an interface:

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

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.

Supported Parameters

interface-type	Specifies the type of interface. For example, ethernet. The specified SGT is mapped to traffic from this logical or physical Layer 3 interface.
sgtsgt-number	Specifies the SGT number from 0-65535.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts role-based sgt-map

Examples

The following example shows how to manually map a source IP address to an SGT on a Cisco ASR 1000 series router:

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

cts sgt

To manually assign a Security Group Tag (SGT) number to a network device, use the **cts sgt** command in global configuration mode. Use the **no** form of the command to remove the tag.

cts sgt *tag-number*
no cts sgt *tag-number*

Supported Parameters

tag-number	Configures the SGT for packets sent from this device. The *tag-number* argument is in decimal format. The range is from 1 to 65533.

Command Default

No SGT number is assigned

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines In Cisco TrustSec, the authentication server assigns an SGT to the device for packets originating from the device. You can manually configure an SGT to be used if the authentication server is not accessible, but an authentication server-assigned SGT will take precedence over a manually assigned SGT.

Examples The following example shows how to enter CTS manual interface configuration mode on an interface:

```
Device# config-transaction
Device(config)# cts sgt 1234
Device(config)#
```

cts sxp connection peer

Use the **cts sxp connection peer** command in global configuration mode to specify

- the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) peer IP address
- if a password is used for the peer connection or a TCP key-chain should be used to provide TCP-AO authentication
- the global hold-time period for a listener or speaker device
- if the connection is bidirectional.

To remove these configurations for a peer connection, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines For more information about this command, see the Cisco IOS XE cts sxp connection peer

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 with the password option for TCP MD5 authentication: :

```
Device_A> enable
Device_A# config-transaction
Device_A#(config)# cts sxp enable
Device_A#(config)#cts sxp node-id ipv4 10.30.1.1
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
hold-time 0 vrf 7
Device_A#(config)#
```

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# config-transaction
Device_B(config)# cts sxp enable
Device_B#(config)#cts sxp node-id ipv4 10.30.1.2
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
hold-time 0 vrf 7
Device_B#(config)#
```

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.

The following example shows how to configure the CTS-SXP peer connection on Device_A, a speaker, for connection to Device_B, a listener without a password or key chain option:

```
Device_A(config)# cts sxp connection peer 10.51.51.1 source 10.51.51.2 password none mode
local speaker hold-time 0 vrf 7
Device_A(config)#
```

```
Device_B(config)# cts sxp connection peer 10.51.51.2 source 10.51.51.1 password none mode
local listener hold-time 0 vrf 7
Device_B(config)#
```

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# config-transaction
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp node-id ipv4 10.30.1.1
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)#cts sxp connection peer 10.20.2.2 password default mode local both vrf 7
Device_A#(config)#
```

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

```
Device_A> enable
Device_A# config-transaction
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp node-id ipv4 10.30.1.2
Device_A#(config)# cts sxp default key-chain sxp_1
Device_A#(config)# cts sxp connection peer 10.2.2.2 password key-chain mode local speaker
hold-time 0 vrf 7
Device_A#(config)#
```

cts sxp default key-chain

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

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp default key-chain

Example

In the following example, a TCP-AO key chain named sxp_1 is configured as the default key chain for CTS SXP sessions using TCP-AO.

```
Device> enable
Device# config-transaction
Device(config)# cts sxp default key-chain key6
Device(config)# cts sxp connection peer 10.30.1.1 source 10.201.1.2 password key-chain mode
 local speaker hold-time 0 vrf 1
Device(config)# cts sxp enable
Device(config)# cts sxp node-id ipv4 10.30.1.1
Device(config)#
```

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.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp default password

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# config-transaction
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 node-id ipv4 10.30.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
Device_A#(config)#
```

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# config-transaction
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 node-id ipv4 10.30.1.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
Device_B#(config)#
```

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.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp default source-ip

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# config-transaction
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 node-id ipv4 10.30.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
Device_A#(config)#
```

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# config-transaction
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 node-id ipv4 10.30.1.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
Device_B#(config)#
```

cts sxp enable

To enable the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) on a device, use the **cts sxp enable** command in global configuration mode. To disable the CTS-SXP on a device, use the **no** form of this command

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp enable

Examples

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

```
Device_A# config-transaction
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp node-id ipv4 10.30.1.1
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
Device_A#(config)#
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# config-transaction
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B#(config)# cts sxp node-id ipv4 10.30.1.2
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
Device_B(config)#
```

cts sxp listener hold-time

To configure the global hold-time period of a listener network device in a Cisco TrustSec Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4) network, use the **cts sxp listener hold-time** command in global configuration mode. To remove the hold time from the listener device, use the **no** form of this command.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp listener hold-time

The following example shows how to configure the hold time period of a listener device for a minimum of 300 seconds and a maximum of 500 seconds:

```
Device> enable
Device# config-transaction
Device(config)# cts sxp listener hold-time 300 500
Device(config)#
```

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.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp log binding-changes

Examples

The following example shows how to enable logging for IP-to-Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) binding changes:

```
Device# config-transaction
Device#(config)# cts sxp log binding-changes
Device#(config)#
```

cts manual

To manually enable an interface for Cisco TrustSec Security (CTS), use the **cts manual** command in interface configuration mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts manual

Examples

The following example shows how to enter CTS manual interface configuration mode on an interface:

```
Device# config-transaction
Device(config)# interface gigabitethernet 0
Device(config-if)# cts manual
Device(config-if-cts-manual))#
```

The following example shows how to remove the CTS manual configuration from an interface:

```
Device# config-transaction
Device(config)# interface gigabitethernet 0
Device(config-if)# no cts manual
Device(config-if)#
```

cts sxp node-id

To configure the node ID of a network device for Cisco TrustSec (CTS) Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4), use the **cts sxp node-id** command in global configuration mode. To remove the node ID, use the **no** form of this command.

When you need to change a Node ID, you must first disable SXP and then push the template to the device. Then, you change the Node ID, and then push the template to the device again.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp node-id

The following example shows how to configure the node ID of a network device for Cisco TrustSec (CTS) Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4).

```
Device# config-transaction
Device(config)# cts sxp node-id ipv4 10.16.1.3
Device(config)#
```

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.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp reconciliation period

Examples

The following example shows how to change the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) reconciliation period:

```
Device# config-transaction
Device#(config)# cts sxp reconciliation period 120
Device(config)#
```

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.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp retry period

Examples

The following example shows how to change the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) retry period timer:

```
Device# config-transaction
Device#(config)# cts sxp retry period 60
Device(config)#
```

cts sxp speaker hold-time

To configure the global hold-time period of a speaker network device in a Cisco TrustSec Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4) network, use the **cts sxp speaker hold-time** command in global configuration mode. To remove the hold time from the speaker device, use the **no** form of this command.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp speaker hold-time

The following example shows how to configure the minimum hold time period of a speaker device for 300 seconds:

```
config-transaction
Device(config)# cts sxp speaker hold-time 300
Device(config)#
```

domain stripping

To configure domain stripping at the server group level, use the **domain-stripping** command in server group RADIUS configuration mode. To disable the configuration, use the **no** form of this command.

Supported Parameters

right-to-left	(Optional) Terminates the string at the first delimiter going from right to left.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE domain stripping

Examples

The following example shows how to configure domain stripping at the server group level:

```
Device# configure transaction
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 77.251.1.1 vrf 1 server-key 0
$CRYPT_CLUSTER$8p6dnAgrJ00J5nT2ibIz+A==$7hds/zxmCbjtkbAJlKynPQ==
Device(config-locsvr-da-radius)# domain stripping right-to-left
Device(config-locsvr-da-radius)#
```

ip radius source-interface

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the **ip radius source-interface**command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the no form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE ip radius source-interface

Examples

The following example shows how to configure RADIUS to use the IP address of subinterface s2 for all outgoing RADIUS packets:

```
Device# config-transaction
Device(config)# aaa group server radius radgroup1
Device#(config-sg-radius)# ip radius source-interface GigabitEthernet0/0/1.100
Device#(config-sg-radius)#
```

ip vrf forwarding

To associate a Virtual Private Network (VPN) routing and forwarding (VRF) instance with a Diameter peer, use the **ip vrf forwarding** command in Diameter peer configuration mode. To enable Diameter peers to use the global (default) routing table, use the no form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE ip vrf forwarding

Examples

The following example shows how to configure a VRF:

```
config-transaction
Device(config)# aaa group server radius radius-1
Device# (config-sg-radius)# ip vrf forwarding 1
Device(config-sg-radius)#
```

key

To identify an authentication key on a key chain, use the **key** command in key-chain configuration mode. To remove the key from the key chain, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE key

Examples

You configure TCP Authentication Option (TCP-AO) for SXP where you configure keys on both the peers communicating through a TCP connection.

This example shows how to create a key with the specified key-id.

```
Device# config-transaction
Device(config)#key chain key6 tcp
Device(config-keychain)# key 2000
Device(config-keychain-key)#
```

key chain

To define an authentication key chain needed to enable authentication for routing protocols and enter key-chain configuration mode, use the **key chain** command in global configuration mode. To remove the key chain, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE key chain

Examples

You configure TCP Authentication Option (TCP-AO) for SXP where you configure the key chain on both the peers communicating through a TCP connection.

This example shows how to create a TCP-AO key chain with the specified name.

```
Device# config-transaction
Device(config)#key chain key6 tcp
Device(config-keychain)#
```

key-string

To specify the authentication string for a key, use the **key-string**command in key chain key configuration mode. To remove the authentication string, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE key-string

Examples

This example show how to specify the master-key for deriving traffic keys.

The master-keys must be identical on both peers. If the master-keys do not match, authentication fails and segments may be rejected by the receiver.

```
Device# config-transaction
Device(config)#key chain key6 tcp
Device(config-keychain)# key 2000
Device(config-keychain-key)# key-string 6 _RPB[dVI]SO^BAOVNMKATgOZKMXFGXFTa
```

port

To specify the port on which a device listens for RADIUS requests from configured RADIUS clients, use the **port** command in dynamic authorization local server configuration mode. To restore the default, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE port

Examples

The following example specifies port 1650 as the port on which the device listens for RADIUS requests:

```
Device# config-transaction
Device#(config)# aaa server radius dynamic-author
Device#(config-locsvr-da-radius)# client 10.0.0.1
Device#(config-locsvr-da-radius)# port 1650
Device#(config-locsvr-da-radius)#
```

recv-id

To specify the receive ID for a TCP-AO key chain, use the **recv-id** command in the key chain key configuration mode. To remove the receive ID, use the **no** form of this command.

recv-id *ID*

no recv-id *ID*

Supported Parameters

ID	Specifies the receive identifier. An integer between 0 to 255.

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

The **send-id** on the device must match the **recv-id** on the other device and vice versa.

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the **key chain** command, you enter key chain configuration mode.

The following example configures a simple key chain for a TCP-AO enabled connection.

```
Device# config-transaction
Device(config)# key chain kc1 tcp
Device(config-keychain)# key 7890
Device(config-keychain-key)# send-id 215
Device(config-keychain-key)# recv-id 215
Device(config-keychain-key)# key-string klomn
Device(config-keychain-key)# cryptographic-algorithm hmac-sha-1
Device(config-keychain-key)# include-tcp-options
Device(config-keychain-key)#
```

send-id

To specify the send ID for a TCP-AO key chain, use the **send-id** command in the key chain key configuration mode. To remove the send ID, use the **no** form of this command.

send-id *ID*

no send-id *ID*

Supported Parameters

ID	Specifies the send identifier. An integer between 0 to 255.

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

The **send-id** on the device must match the **recv-id** on the other device and vice versa.

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the **key chain** command, you enter key chain configuration mode.

The following example configures a simple key chain for a TCP-AO enabled connection.

```
Device# config-transaction
Device(config)# key chain kc1 tcp
Device(config-keychain)# key 7890
Device(config-keychain-key)# send-id 215
Device(config-keychain-key)# recv-id 215
Device(config-keychain-key)# key-string klomn
Device(config-keychain-key)# cryptographic-algorithm hmac-sha-1
Device(config-keychain-key)# include-tcp-options
Device(config-keychain-key)#
```

send-lifetime

To set the time period during which an authentication key on a key chain is valid to be sent, use the **send-lifetime** command in key chain key configuration mode. To revert to the default value, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE send-lifetime

Examples

The following show how to specify the time entered in Cisco SD-WAN Manager for which the key is valid to be used for TCP-AO authentication.

Specify the start-time in the local time zone. By default, the start-time corresponds to UTC time. The end-time can be specified in 3 ways - infinite (no expiry), duration (1- 2147483646 sec), exact time – either UTC or local.

```
Device# config-transaction
Device(config)#key chain key6 tcp
Device(config-keychain)# key 2000
Device(config-keychain-key)# send-lifetime local 18:00:00 Jan 12 2021 01:00:00 Jan 12 2022
Device(config-keychain-key)#
```

server-private (RADIUS)

To configure the IP address of the private RADIUS server for the group server, use the **server-private** command in RADIUS server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

Supported Parameters

ip-address	IP address of the private RADIUS server host.
auth-port *port-number*	(Optional) User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645.
acct-port *port-number*	Optional) UDP destination port for accounting requests. The default value is 1646.

timeout *seconds*	(Optional) Time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the **radius-server timeout** command. If no timeout value is specified, the global value is used.
retransmit *retries*	(Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the **radius-server retransmit** command.
key *string*	(Optional) Authentication and encryption key used between the router and the RADIUS daemon running on the RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used. The *string* 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.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE server-private (RADIUS)

Examples

The following example shows how to define the sg_water RADIUS group server and associate private servers with it:

```
Device> enable
Device# config-transaction
Device(config)# aaa new-model
Device(config)# aaa group server radius sg_water
Device(config-sg-radius)# server-private 10.1.1.1 timeout 5 retransmit 3 key xyz
Device(config-sg-radius)# server-private 10.2.2.2 timeout 5 retransmit 3 key xyz
Device(config-sg-radius)#
```