Crypto Commands

aaa authorization (IKEv2 profile)

To specify the authentication, authorization, and accounting (AAA) authorization for a local or external group policy, use the **aaa authorization** command in IKEv2 profile configuration mode. To remove the AAA authorization, use the **no** form of this command.

aaa authorization { **group** { **cert list** | **eap list** | **psk list** } | **user** { **cert list** | **eap list** | **psk list** } { *aaa-listname* | [*aaa-username* | [**local**] | **name-mangler** *mangler-name*] | [**password** *password*] } }
no aaa authorization { **group** { **cert list** | **eap list** | **psk list** } | **user** { **cert list** | **eap list** | **psk list** } { *aaa-listname* | [*aaa-username* | [**local**] | **name-mangler** *mangler-name*] | [**password** *password*] } }

Syntax Description

group	Specifies the AAA authorization for local or external group policy.
local	(Optional) Specifies the authorization policy that is used through a local method.
user	Specifies the AAA authorization for each user policy.
cert	Specifies the AAA method list that is used when the remote authentication method is certificate based.
eap	Specifies the AAA method list that is used when the remote authentication method is Extensible Authentication Protocol (EAP).
psk	Specifies the AAA method list that is used when the remote authentication method is preshared key.
list	Specifies the AAA method list for the remote authentication method.
aaa-listname	The AAA list name.
aaa-username	The AAA username.
name-mangler *mangler-name*	Derives the name mangler from the **crypto ikev2 name-mangler** command.
password *password*	Specifies the AAA password. This *password* argument defines the following values: • **0**—Specifies that the password is unencrypted. • **6**—Specifies that the password is encrypted. • *password*—Specifies an unencrypted user password.

Command Default

AAA authorization is not specified.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE aaa authorization (IKEv2 profile) command.

Examples

The following example shows how to configure the AAA authorization for a local group policy.

```
\
Router(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Router(config-ikev2-profile)# aaa authorization group psk list default li_policy
```

address (IKEv2 keyring)

To specify an IPv4 address or the range of the peer in an Internet Key Exchange Version 2 (IKEv2) keyring, use the **address** command in IKEv2 keyring peer configuration mode. To remove the IP address, use the **no** form of this command.

address *ipv4-address*
no address

Syntax Description

ipv4-address	IPv4 address of the remote peer.

Command Default

There is no default IP address.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE address (IKEv2 keyring) command.

Examples

The following examples show how to specify the preshared key of an IP Security (IPsec) peer:

```
Router(config)#  crypto ikev2 keyring if-ipsec256-ikev2-keyring
Router(config-ikev2-keyring)# peer if-ipsec256-ikev2-keyring-peer
Router(config-ikev2-keyring-peer)# address 172.16.93.1
Router(config-ikev2-keyring-peer)# pre-shared-key cisco123
```

authentication (IKEv2 profile)

To specify the local and remote authentication methods in an Internet Key Exchange Version 2 (IKEv2) profile, use the **authentication** command in IKEv2 profile configuration mode. To delete the authentication method, use the **no** form of this command.

authentication { **local** { **rsa-sig** | **pre-share** [**key**] | **ecdsa-sig** } | **remote** { **anyconnect-eap** | **rsa-sig** | **pre-share** [**key**] } }
no authentication { **local** { **rsa-sig** | **pre-share** [**key**] | **ecdsa-sig** } | **remote** { **anyconnect-eap** | **rsa-sig** | **pre-share** [**key**] } }

Syntax Description

local	Specifies the local authentication method.
rsa-sig	Specifies Rivest, Shamir, and Adelman (RSA) signature as the authentication method.
pre-share	Specifies preshared key as the authentication method.
key	Specifies a preshared key.
ecdsa-sig	Specifies Elliptic Curve Digital Signature Algorithm (ECDSA) signature (ECDSA-sig) as the authentication method.
anyconnect-eap	Specifies Extensible Authentication Protocol (EAP) as the authentication method.
remote	Specifies the remote authentication method.

Command Default

The default local and remote authentication method is not configured.

Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE authentication (IKEv2 profile) command.

Examples

The following example shows how to specify an authentication method in an IKEv2 profile:

```
Device(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Device(config-ikev2-profile)# aaa authorization group psk list default li_policy
Device(config-ikev2-profile)# authentication local pre-share
Device(config-ikev2-profile)# authentication remote pre-share
Device(config-ikev2-profile)# no config-exchange request
Device(config-ikev2-profile)# keyring local if-ipsec256-ikev2-keyring
Device(config-ikev2-profile)# lifetime 86400
Device(config-ikev2-profile)# match identity remote address 172.16.93.2
!
```

In the above example, the profile if-ipsec256-ikev2-profile specifies preshare as the local authentication method and as the remote authentication method that use keyring if-ipsec256-ikev2-keyring.

config-exchange

To enable the configuration exchange options, use the **config-exchange** command in IKEv2 profile configuration mode. To disable sending, use the **no** form of this command.

config-exchange {**request** | **set** {**accept** | **send**}}
no config-exchange {**request** | **set** {**accept** | **send**}}

Syntax Description

request	Enables configuration exchange request.
set	Enables configuration exchange request set options.
accept	Accepts configuration exchange request set.
send	Enables sending of configuration exchange set.

Command Default

The configuration exchange options is enabled by default.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE config-exchange command.

Examples

The following example show how to set the acceptance of configuration exchange request for the IKEv2 profile “if-ipsec256-ikev2-profile”:

```
Router(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Router(config-ikev2-profile)# config-exchange set accept
```

crypto ikev2 authorization policy

To configure an IKEv2 authorization policy, use the **crypto ikev2 authorization policy** command in global configuration mode. To remove this command and all associated subcommands from your configuration, use the **no** form of this command.

crypto ikev2 authorization policy *policy-name*
no crypto ikev2 authorization policy *policy-name*

Syntax Description

policy-name	Group definition that identifies which policy is enforced for users.

Command Default

None.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto ikev2 authorization policy command.

Examples

In this example, the policy is enforced for users that matches the group name “li_policy.”

```
crypto ikev2 authorization policy
li_policy
  exit
```

crypto ikev2 diagnose

To enable Internet Key Exchange Version 2 (IKEv2) error diagnostics, use the **crypto ikev2 diagnose** command in global configuration mode. To disable the error diagnostics, use the **no** form of this command.

crypto ikev2 diagnose error *number*
no crypto ikev2 diagnose error

Syntax Description

error	Enables the IKEv2 error path tracing.
number	Specifies the maximum number of errors allowed in the exit path entry. The range is 1 to 1000.

Command Default

IKEv2 error diagnostics is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto ikev2 diagnose command.

Examples

The following example shows that error diagnostics is disabled:

```
Router(config)# no crypto ikev2 diagnose error
```

crypto ikev2 keyring

To configure an Internet Key Exchange version 2 (IKEv2) key ring, use the **crypto ikev2 keyring** command in the global configuration mode. To delete an IKEv2 keyring, use the **no** form of this command.

crypto ikev2 keyring *keyring-name*
no crypto ikev2 keyring *keyring-name*

Syntax Description

keyring-name	Name of the keyring.

Command Default

There is no default key ring.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto ikev2 keyring command.

Examples

The following example shows how to configure a keyring:

```
Router(config)# crypto ikev2 keyring if-ipsec256-ikev2-keyring
Router(config-ikev2-keyring)# peer if-ipsec256-ikev2-keyring-peer
Router(config-ikev2-keyring-peer)# address 172.16.93.1
Router(config-ikev2-keyring-peer)# pre-shared-key cisco123
!
!
```

crypto ikev2 policy

To configure an Internet Key Exchange Version 2 (IKEv2) policy, use the **crypto ikev2 policy** command in global configuration mode. To delete a policy, use the **no** form of this command. To return the policy to its default value, use the **default** form of this command.

crypto ikev2 policy *name*
no crypto ikev2 policy *name*
default crypto ikev2 policy

Syntax Description

name	Name of the IKEv2 policy.

Command Default

A default IKEv2 policy is used only in the absence of any user-defined IKEv2 policy. The default IKEv2 policy will have the default IKEv2 proposal and will match all local addresses in a global VPN Routing and Forwarding (VRF).

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto ikev2 policy command.

Examples

The following example show how to configure a policy:

```
Router(config)# crypto ikev2 policy policy1-global
Router(config-ikev2-policy)# proposal p1-global
```

crypto ikev2 profile

To configure an Internet Key Exchange Version 2 (IKEv2) profile, use the **crypto ikev2 profile** command in global configuration mode. To delete the profile, use the **no** form of this command.

crypto ikev2 profile *profile-name*
no crypto ikev2 profile *profile-name*

Syntax Description

profile-name	The name of the IKEv2 profile.

Command Default

There is no default IKEv2 profile. However, there are default values for some commands under the profile, such as lifetime.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto ikev2 profilecommand.

Examples

The following example show an IKEv2 profile matched on a remote identity.

IKEv2 Profile Matched on Remote Identity

The following profile caters to peers that identify using a remote address and authenticate with pre-share. The local node authenticates with pre-share using keyring, if-ipsec256-ikev2-keyring.

```
Router(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
```

```
Router(config-ikev2-profile)# aaa authorization group psk list default li_policy
Router(config-ikev2-profile)# authentication local pre-share
Router(config-ikev2-profile)# authentication remote pre-share
Router(config-ikev2-profile)# no config-exchange request
Router(config-ikev2-profile)# keyring local if-ipsec256-ikev2-keyring
Router(config-ikev2-profile)# lifetime 86400
Router(config-ikev2-profile)# match identity remote address 172.16.93.2
!
```

crypto ikev2 proposal

To configure an Internet Key Exchange Version 2 (IKEv2) proposal, use the **crypto ikev2 proposal** command in global configuration mode. To delete an IKEv2 proposal, use the **no** form of this command. To return the proposal to its default value, use the **default** form of this command.

crypto ikev2 proposal *name*
no crypto ikev2 proposal *name*
default crypto ikev2 proposal

Syntax Description

name	Name of the proposal. The proposals are attached to IKEv2 policies using the **proposal** command.

Command Default

The default IKEv2 proposal is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto ikev2 proposal command.

Examples

The following example shows how to configure a proposal:

```
Device(config)# crypto ikev2 proposal p1-global
Device(config-ikev2-proposal)# encryption aes-cbc-128 aes-cbc-256
Device(config-ikev2-proposal)# group 14 15 16 2
Device(config-ikev2-proposal)# integrity sha1 sha256 sha384 sha512
!
```

crypto ipsec profile

To define the IP Security (IPsec) parameters that are to be used for IPsec encryption between two IPsec routers and to enter IPsec profile configuration mode, use the **crypto ipsec profile** command in global configuration

mode. To delete an IPsec profile, use the **no** form of this command. To return the IPsec profile to its default value, use the **default** form of this command.

crypto ipsec profile *name*
no crypto ipsec profile *name*

Syntax Description

name	Profile name.

Command Default

The default IPsec profile is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto ipsec profile command.

Examples

The following example shows how to configure a crypto map that uses an IPsec profile:

```
crypto ipsec profile if-ipsec256-ipsec-profile
 set ikev2-profile if-ipsec256-ikev2-profile
 set pfs group16
 set transform-set if-ipsec256-ikev2-transform
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 3600
 set security-association replay window-size 512
!
```

crypto ipsec transform-set

To define a transform set—an acceptable combination of security protocols and algorithms—use the **crypto ipsec transform-set** command in global configuration mode. To delete a transform set, use the **no** form of this command. To return the transform-set to its default value, use the **default** form of this command.

crypto ipsec transform-set *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
no crypto ipsec transform-set *transform-set-name*

Syntax Description

transform-set-name	Name of the transform set to create (or modify).
transform1 transform2 transform3 transform4	Type of transform set. You may specify up to four “transforms”: one Authentication Header (AH), one Encapsulating Security Payload (ESP) encryption, one ESP authentication, and one compression. These transforms define the IP Security (IPSec) security protocols and algorithms. Accepted transform values are available in the usage guidelines.

Command Default

The default transform-set is used.

Command Modes

Global configuration

This command invokes the crypto transform configuration mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto ipsec transform-set command.

Examples

The following example defines a transform set. The transform set will be used with an IPSec peer that supports the esp-gcm protocols.

```
Router (config)# crypto ipsec transform-set if-ipsec256-ikev2-transform esp-gcm 256
Router (cfg-crypto-trans)# mode tunnel
!
```

Examples

crypto isakmp aggressive-mode disable

To block all Internet Security Association and Key Management Protocol (ISAKMP) aggressive mode requests to and from a device, use the **crypto isakmp aggressive-mode disable** command in global configuration mode. To disable the blocking, use the **no** form of this command.

crypto isakmp aggressive-mode disable
no crypto isakmp aggressive-mode disable

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not configured, Cisco IOS software will attempt to process all incoming ISAKMP aggressive mode security association (SA) connections. In addition, if the device has been configured with the **crypto isakmp peer address** and the **set aggressive-mode password**or **set aggressive-mode client-endpoint**commands, the device will initiate aggressive mode if this command is not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto isakmp aggressive-mode disable command.

Examples

The following example shows that all aggressive mode requests to and from a device are blocked:

```
Router (config)# crypto isakmp aggressive-mode disable
```

crypto pki import

To import Rivest, Shamir, and Adleman (RSA) keys, use the **crypto pki import pkcs12 password** command in privileged EXEC mode. To remove any of the configured parameters, use the no form of this command

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto pki import command.

Examples

In the following example, an RSA key pair that has been associated with the trustpoint named **test2** is to be imported:

```
Device# crypto pki import test2 pkcs12 bootflash:router1.p12 password cisco123
% Importing pkcs12...Reading file from bootflash:router1.p12
CRYPTO_PKI: Imported PKCS12 file successfully.
```

crypto pki trustpoint

To declare the trustpoint that your router should use, use the **crypto pki trustpoint** command in global configuration mode. To delete all identity information and certificates associated with the trustpoint, use the **no** form of this command.

crypto pki trustpoint *name*
no crypto pki trustpoint *name*

Syntax Description

name	Creates a name for the trustpoint. (If you previously declared the trustpoint and just want to update its characteristics, specify the name you previously created.)

Command Default

Your router does not recognize any trustpoints until you declare a trustpoint using this command.

Your router uses unique identifiers during communication with Online Certificate Status Protocol (OCSP) servers, as configured in your network.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto pki trustpoint command.

Examples

The following example shows a self-signed certificate being designated for a trustpoint named local using the enrollment selfsigned subcommand of the crypto pki trustpoint command:

```
crypto pki trustpoint TP-self-signed-3865005142
enrollment selfsigned
```

encryption (IKEv2 proposal)

To specify one or more encryption algorithms for an Internet Key Exchange Version 2 (IKEv2) proposal, use the **encryption** command in IKEv2 proposal configuration mode. To remove the encryption algorithm, use the **no** form of this command.

encryption { **des** | **3des** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** }
no encryption

Syntax Description

des	Specifies 56-bit Data Encryption Standard (DES)-CBC as the encryption algorithm.
3des	Specifies 168-bit DES (3DES) as the encryption algorithm.
aes-cbc-128	Specifies 128-bit Advanced Encryption Standard (AES) as the encryption algorithim.
aes-cbc-192	Specifies 192-bit AES as the encryption algorithim.
aes-cbc-256	Specifies 256-bit AES as the encryption algorithim.

Command Default

The encryption algorithm is not specified.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE encryption (IKEv2 proposal) command.

Examples

The following example configures an IKE proposal with the aes-cbc-128 and aes-cbc-256 encryption algorithm (all other parameters are set to the defaults):

```
crypto ikev2 proposal p1-global
encryption aes-cbc-128 aes-cbc-256
```

enrollment selfsigned

To specify self-signed enrollment for a trustpoint, use the **enrollment self** command in ca-trustpoint configuration mode. To delete self-signed enrollment from a trustpoint, use the **no** form of this command.

enrollment self
no enrollment self

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE enrollment selfsigned command.

Examples

The following example shows a self-signed certificate being designated for a trustpoint named local:

```
crypto pki trustpoint local
 enrollment self
```

group (IKEv2 proposal)

To specify one or more Diffie-Hellman (DH) group identifier(s) for use in an Internet Key Exchange Version 2 (IKEv2) proposal, use the **group**command in IKEv2 proposal configuration mode. To reset the DH group identifier to the default value, use the **no** form of this command.

group *group type*
no group

Syntax Description

group type	Specifies the DH group.

Command Default

DH group 2 and 5 in the IKEv2 proposal.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE group (IKEv2 proposal command.

Examples

The following example shows how to configure an IKEv2 proposal with the 2048-bit, 3072-bit, 4096-bit, and 1024-bit DH group:

```
Device(config)#  crypto ikev2 proposal p1-global
Device(config-ikev2-proposal)# group 1 2 5 14 15 16 19 20 21 24
```

integrity

To specify one or more integrity algorithms for an Internet Key Exchange Version 2 (IKEv2) proposal, use the **integrity** command in IKEv2 proposal configuration mode. To remove the configuration of the hash algorithm, use the **no** form of this command.

integrity *integrity type*
no integrity

Syntax Description

integrity type	Specifies the hash algorithm.

Command Default

The default integrity algorithm is used.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE integrity command.

Examples

The following example configures an IKEv2 proposal with the sha1, sha256, sha384, and sha512 integrity algorithms:

```
Device(config)#  crypto ikev2 proposal p1-global
Device(config-ikev2-proposal)# integrity md5 sha1 sha256 sha384 sha512
```

keyring (IKEv2 profile)

To specify a locally defined or accounting, authentication and authorization (AAA)-based keyring, use the **keyring** command in IKEv2 profile configuration mode. To delete the keyring, use the **no** form of this command.

keyring { **local** *keyring-name* | **aaa** *list-name* [**name-mangler** *mangler-name* | **password** *password*] }
no keyring

Syntax Description

local	Specifies the local keyring.
keyring-name	The keyring name for a locally defined keyring.
aaa	Specifies the AAA-based preshared keys list name.
list-name	The AAA method list name.
name-mangler	Derives the username from the peer identity in the preshared key lookup on the AAA list.
mangler-name	(Optional) Globally defined name mangler.
password *password*	Specifies a password for the password. This argument defines the following values: • **0**—Specifies that the password is unencrypted. • **6**—Specifies that the password is encrypted. • *password*—Specifies an unencrypted user password.

Command Default

A keyring is not specified.

Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE keyring (IKEv2 profile) command.

Examples

The following example shows how to configure a locally defined keyring:

```
Router(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Router(config-ikev2-profile)# keyring local if-ipsec256-ikev2-keyring
```

lifetime (IKEv2 profile)

To specify the lifetime for an Internet Key Exchange Version 2 (IKEv2) security association (SA), use the **lifetime** command in IKEv2 profile configuration mode . To reset the SA lifetime to the default value, use the **no** form of this command.

lifetime *seconds*
no lifetime

Syntax Description

seconds	The time that each IKE SA should exist before expiring. Use an integer from 60 to 86,400 seconds.

Command Default

The default is 86,400 seconds (one day).

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE lifetime (IKEv2 profile) command

Examples

The following example configures an IKEv2 profile with a security association lifetime of 86400 seconds, and all other parameters are set to the defaults:

```
Router(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Router(config-ikev2-profile)# lifetime 86400
```

match identity remote

To define the remote identity match statement, use the **match identity remote** command in IKEv2-profile configuration mode. To remove the remote identity match statement, use the **no** form of this command.

match identity remote { **address** *ipv4-address* | **any** | **email** { *email-address* | **domain** *domain-name* } | **fqdn** { **domain** *domain-name domain-name* } | **key-id** *opaque-string* }
no match identity remote { **address** *ipv4-address* | **any** | **email** { *email-address* | **domain** *domain-name* } | **fqdn** { **domain** *domain-name domain-name* } | **key-id** *opaque-string* }

Syntax Description

address *ipv4-address*	Matches peer identity based on remote IPv4 address.
any	Matches any peer identity.
email *email-address*	Matches peer identity based on email address.
domain *domain-name*	Specifies to match peer identity based on domain.
fqdn	Matches peer identity based on FQDN.
domain-string	Specifies the domain string to match.
key-id *opaque-string*	Matches peer identity based on remote key ID.

Command Default

No default behavior or values.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)#

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco vManage CLI templates.

Usage Guidelines

An IKEv2 profile is a repository of the nonnegotiable parameters of the IKE security association, such as local or remote identities and authentication methods and the services that are available to the authenticated peers that match the profile. An IKEv2 profile must be attached to either a crypto map or an IPSec profile on both IKEv2 initiator and IKEv2 responder. During IKE AUTH Internet Security Association and Key Management Protocol (ISAKMP) negotiations, the peers must identify themselves to each other.

An IKEv2 profile must contain a match identity or a match certificate statement. An IKEv2 profile can have more than one match identity or match certificate statements.

This command can be used to define the remote identity match statement.

Examples

The following example shows how to define the IKEv2 profile if-ipsec256-ikev2-profile to match the peer identity based on IPv4 address:

```
Device(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Device(config-ikev2-profile)# match identity remote address 172.16.93.2
```

The following example shows how to define the IKEv2 profile if-ipsec256-ikev2-profile to match any peer identity:

```
Device(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Device(config-ikev2-profile)# match identity remote any
```

The following example shows how to define the IKEv2 profile if-ipsec256-ikev2-profile to match the peer identity based on FQDN. To match the entire domain, use the domain keyword:

```
Device(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Device(config-ikev2-profile)# match identity remote fqdn remote.cisco.com
Device(config-ikev2-profile)# match identity remote fqdn domain cisco.com
```

The following example shows how to define the IKEv2 profile if-ipsec256-ikev2-profile to match the peer identity based on email. To match the entire domain, use the domain keyword:

```
Device(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Device(config-ikev2-profile)# match identity remote email remote@cisco.com
Device(config-ikev2-profile)# match identity remote email domain cisco.com
```

The following example shows how to define the IKEv2 profile if-ipsec256-ikev2-profile to match the peer identity based on key-ID:

```
Device(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Device(config-ikev2-profile)# match identity remote key-id cisco
```

mode (IPSec)

To change the mode for a transform set, use the **mode** command in crypto transform configuration mode. To reset the mode to the default value of tunnel mode, use the **no** form of this command.

mode { **tunnel** | **transport** }
no mode

Syntax Description

tunnel | **transport**	Specifies the mode for a transform set: either tunnel or transport mode. If neither **tunnel** nor **transport** is specified, the default (tunnel mode) is assigned.

Command Default

Tunnel mode

Command Modes

Crypto transform configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE mode (IPSec) command.

Examples

The following example defines a transform set and changes the mode to transport mode. The mode value only applies to IP traffic with the source and destination addresses at the local and remote IPSec peers.

```
crypto ipsec transform-set if-ipsec256-ikev2-transform esp-gcm 256
mode transport
exit
```

multi-tenancy

To enable multi-tenancy as a global parameter map, use the **multi-tenancy** command in parameter-map type inspect configuration mode. To disable multi-tenancy as a global parameter map, use the **no** form of this command.

multi-tenancy
no multi-tenancy

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Parameter-map type inspect configuration (config-profile).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A parameter map allows you to specify parameters that control the behavior of actions and match criteria sthat are specified under a policy map and a class map respectively, for zone-based firewall policies.

Examples

The following example shows how to enable multi-tenancy as a global parameter map:

```
Device(config)# parameter-map type inspect-global
Device(config-profile)# multi-tenancy
```

parameter-map type inspect-global

To configure a global parameter map and enter parameter-map type inspect configuration mode, use the **parameter-map type inspect-global** command in global configuration mode. To delete a global parameter map, use the **no** form of this command.

parameter-map type inspect-global
no parameter-map type inspect-global

Syntax Description

This comand has no keywords or arguments.

Command Default

Global parameter maps are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

After you enter the **parameter-map type inspect-global** command, you can enter the commands listed in the table below in parameter-map type inspect-global configuration modes.

Command	Description
aggressive-aging	Enables aggressive aging of half-opened firewall sessions.
alert on	Enables Cisco IOS stateful packet inspection alert messages.
inspect	Enables and disables audit trail messages.
log {**dropped-packets** | **flow-export**}	Logs the dropped packets.
max-incomplete {**low** | **high**} *number-of-connections*	Defines the number of existing half-open sessions that will cause the software to start and stop deleting half-open sessions.
multi-tenancy	Enables Cisco vManage for multitenancy.
vpn zone security	Inspects traffic exchange between multiple service VPNs.

Ensure that you configure the **parameter-map type inspect-global** command with **vpn zone security** command to enable zone-based firewall.

For more information on usage guidelines, see the Cisco IOS XE parameter-map type inspect-global command.

Examples

The following example shows a sample parameter-map type inspect-global configuration:

```
Device(config)# parameter-map type inspect-global
Device(config)# alert on
Device(config-profile)# log dropped-packets
Device(config-profile)# multi-tenancy
Device(config-profile)# vpn zone security allow dia
```

peer

To define the peer or peer group and enter the IKEv2 keyring peer configuration mode, use the **peer** command in IKEv2 keyring configuration mode. To remove the peer or peer group, use the **no** form of this command.

peer *name*
no peer *name*

Syntax Description

name	Defines the name of the peer or peer group.

Command Default

No default behavior or values.

Command Modes

IKEv2 keyring configuration (config-ikev2-keyring)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco vManage CLI templates.

Usage Guidelines

IKEv2 supports crypto map-and tunnel protection-based crypto interfaces. An IKEv2 keyring is a repository of symmetric and asymmetric preshared keys and is independent of the IKEv1 keyring. The IKEv2 keyring is associated with an IKEv2 profile and hence, caters to a set of peers that match the IKEv2 profile. IKEv2 keyring keys must be configured in the peer configuration submode that defines a peer subblock. An IKEv2 keyring can have multiple peer subblocks. A peer subblock contains a single symmetric or asymmetric key pair for a peer or peer group identified by any combination of hostname, identity, and IP address. This command can be used to set the name of the peer or peer group.

Examples

The following example shows setting the peer name to if-ipsec256-ikev2-keyring-peer and entering the IKEv2 keyring peer configuration mode:

```
Device(config)# crypto ikev2 keyring if-ipsec256-ikev2-keyring
Device(config-ikev2-keyring)# peer if-ipsec256-ikev2-keyring-peer
Device(config-ikev2-keyring-peer)#
```

Related Commands

Command	Description
address	Specifies an IPv4 or IPv6 address or range for the peer.
description	Specifies the description for the peer.
hostname	Specifies the peer using a hostname.
identity	Identifies the IKEv2 peer.ßß:
pre-shared-key	Specifies the preshared key for the peer.

pre-shared-key

To define the preshared key, use the **pre-shared-key** command in IKEv2 keyring peer configuration mode. To remove the preshared key, use the **no** form of this command.

pre-shared-key *key*
no pre-shared-key

Syntax Description

key	Defines the pre-shared key.

Command Default

By default, the preshared key is symmetric.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

IKEv2 supports crypto map-and tunnel protection-based crypto interfaces. An IKEv2 keyring is a repository of symmetric and asymmetric preshared keys and is independent of the IKEv1 keyring. The IKEv2 keyring is associated with an IKEv2 profile and hence, caters to a set of peers that match the IKEv2 profile. IKEv2 keyring keys must be configured in the peer configuration submode that defines a peer subblock. An IKEv2 keyring can have multiple peer subblocks. A peer subblock contains a single symmetric or asymmetric key pair for a peer or peer group identified by any combination of hostname, identity, and IP address. Use the **pre-shared-key** command to specify the preshared key for the peer.

Examples

The following example shows setting the IKEv2 Keyring with Asymmetric Preshared Keys. The local preshared key is encrypted and named key1. The remote preshared key is unencrypted and named key2:

```
Device(config)# crypto ikev2 keyring if-ipsec256-ikev2-keyring
Device(config-ikev2-keyring)# peer if-ipsec256-ikev2-keyring-peer
Device(config-ikev2-keyring-peer)# hostname if-ipsec256-ikev2-keyring-peer
Device(config-ikev2-keyring-peer)# address 10.0.0.1 255.255.255.0
Device(config-ikev2-keyring-peer)# identity address 10.0.0.5
Device(config-ikev2-keyring-peer)# pre-shared-key cisco123
```

Table 1: Related Commands

Command	Description
address	Specifies an IPv4 or an IPv6 address or range for the peer.
description	Specifies the description for the peer.

Command	Description
hostname	Specifies the peer using a hostname.
identity	Identifies the IKEv2 peer.

proposal

To attach a proposal to an IKEv2 policy, use the **proposal** command in IKEv2 policy configuration mode. To remove a proposal from an IKEv2 policy, use the **no** form of this command.

proposal *name*
no proposal *name*

Syntax Description

name	Specifies the name of the proposal in an IKEv2 policy

Command Default

No default behavior or values.

Command Modes

IKEv2 policy configuration (config-ikev2-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco vManage CLI templates.

Usage Guidelines

An IKEv2 policy contains proposals that are used to negotiate the encryption, integrity, PRF algorithms, and DH group in SA_INIT exchange. It can have match statements which are used as selection criteria to select a policy during negotiation. An IKEv2 proposal is a collection of transforms used in the negotiation of IKE security associations as part of the IKE_SA_INIT exchange. Each profile can have multiple proposals and are prioritized in the order of listing. The default proposal is used if no proposals have been attached. This command can be used to attach a proposal to an IKEv2 policy.

Examples

The following example shows how to create the proposal p1-global and attach it to the IKEv2 policy policy1-global:

```
Device(config)# crypto ikev2 proposal p1-global
Device(config-ikev2-proposal)# encryption aes-cbc-128
Device(config-ikev2-proposal)# integrity md5
Device(config-ikev2-proposal)# exit
Device(config)# crypto ikev2 policy policy1-global
Device(config-ikev2-policy)# proposal p1-global
```

revocation-check

To check the revocation status of a certificate, use the **revocation-check crl** command in ca-trustpoint configuration mode. To disable this functionality, use the **revocation-check none** command.

revocation-check crl
revocation-check none

Syntax Description

none	Certificate checking is disabled.

Command Default

After a trustpoint is enabled, the default is set to **revocation-check crl**, which means that CRL checking is mandatory.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE revocation check command.

Examples

The following example shows how revocation check is ignored:

```
Device(config)# crypto pki trustpoint TP-self-signed-3865005142
Device(ca-trustpoint)# revocation-check none
```

set ikev2-profile

To attach an IKEv2 profile to an IPSec profile, use the **set ikev2-profile** command in IPSec profile configuration mode. To remove the IKEv2 profile from an IPSec profile, use the no form of this command.

set ikev2-profile *profile-name*
no set ikev2-profile

Syntax Description

profile-name	Specifies the IKEv2 profile name

Command Default

No default behavior or values.

Command Modes

IPSec profile configuration (ipsec-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco vManage CLI templates.

Usage Guidelines

An IKEv2 profile is a repository of the nonnegotiable parameters of the IKE security association, such as local or remote identities and authentication methods and the services that are available to the authenticated peers that match the profile. An IKEv2 profile must be attached to either crypto map or IPSec profile on both IKEv2 initiator and responder. An IPSec profile defines the IPsec parameters that are to be used for IPsec encryption between two IPsec devices. This command can be used to attach an IKEv2 profile to an IPSec profile.

Examples

The following example shows how to create the prerequisites — IKEv2 keyring, PKI Trustpoint, IKEv2 profile and how to attach the IKEv2 profile to the IPSec profile if-ipsec256-ipsec-profile:

```
Device(config)# crypto ikev2 keyring if-ipsec256-ikev2-keyring
Device(config-ikev2-keyring)# peer if-ipsec256-ikev2-keyring-peer
Device(config-ikev2-keyring-peer)# hostname if-ipsec256-ikev2-keyring-peer
Device(config-ikev2-keyring-peer)# address 10.0.0.1 255.255.255.0
Device(config-ikev2-keyring-peer)# identity address 10.0.0.5
Device(config-ikev2-keyring-peer)# pre-shared-key cisco123
Device(config-ikev2-keyring-peer)# exit
Device(config-ikev2-keyring)# exit

Device(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Device(config-ikev2-profile)# authentication local ecdsa-sig
Device(config-ikev2-profile)# aaa authorization group cert list list1
Device(config-ikev2-profile)# keyring local if-ipsec256-ikev2-keyring
Device(config-ikev2-profile)# lifetime 86400
Device(config-ikev2-profile)# match address local 10.10.10.10
Device(config-ikev2-profile)# exit

Device(config)# crypto ipsec profile if-ipsec256-ipsec-profile
Device(ipsec-profile)# set ikev2-profile if-ipsec256-ikev2-profile
```

Related Commands

Command	Description
setidentity	Specifies which identity can be used
setisakmp-profile	Specifies which isakmp-profile can be used
setmixed-mode	Specifies which mixed-mode can be used
setpfs	Specifies which pfs can be used
setreverse-route	Specifies which reverse-route can be used
setsecurity-association	Specifies which security-association can be used
setsecurity-policy	Specifies which security-policy can be used
settransform-set	Specifies which transform sets can be used

set pfs

To optionally specify that IP security (IPsec) requests the perfect forward secrecy (PFS) Diffie-Hellman (DH) prime modulus group identifier when requesting new security associations (SAs) for a crypto map entry or

when IPsec requires PFS when receiving requests for new SAs, use the **set pfs** command in crypto m ap configuration mode. To specify that IPsec should not request PFS during the DH exchange, use the **no** form of this command.

set pfs [group1 | group2 | group5 | group14 | group15 | group16 | group19 | group20 | group21 | group24]
no set pfs

Syntax Description

group1	Specifies the 768-bit DH identifier.
group2	Specifies the 1024-bit DH identifier.
group5	Specifies the 1536-bit DH identifier.
group14	Specifies the 2048-bit DH identifier.
group15	Specifies the 3072-bit DH identifier.
group16	Specifies the 4096-bit DH identifier.
group19	Specifies the 256-bit elliptic curve DH (ECDH) identifier.
group20	Specifies the 384-bit ECDH identifier.
group21	Specifies the 521-bit DH identifier.
group24	Specifies the 2048-bit DH identifier.

Command Default

By default, PFS is not requested. If no group is specified with this command, the **group1** keyword is used as the default.

Command Modes

Crypto map configuration (config-crypto-map)

IPsec profile configuration (ipsec-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE set pfs command.

Examples

The following example specifies that PFS should be used whenever a new security association is negotiated for the crypto ipsec profile if-ipsec256-ipsec-profile:

```
 crypto ipsec profile if-ipsec256-ipsec-profile
 set ikev2-profile if-ipsec256-ikev2-profile
set pfs group16
```

set security-association lifetime

To set the TEK lifetime for a specific crypto map entry or IPsec profile that is used when negotiating IPsec security associations (SAs), use the **set security-association lifetime** command in crypto map configuration mode or IPsec profile configuration mode. To reset a lifetime to the global value, use the **no** form of this command.

set security-association lifetime {**days** *number-of-days* | **kilobytes** {*number-of-kilobytes* | **disable**} | **seconds** *number-of-seconds*}
no set security-association lifetime { **days** | **seconds** }

Syntax Description

days *number-of-days*	Lifetime in days. The range is 1 to 30.
kilobytes *number-of-kilobytes*	Volume of traffic (in kilobytes) that can pass between IPsec peers using an SA. The range is 2560 to 4294967295.
disable	Disables the SA rekey based on the traffic-volume lifetime.
seconds *number-of-seconds*	Lifetime in seconds. The range is 120 to 2592000. **Note** It is not recommended to use a lifetime value that is lower than 900 seconds in production routers.

Command Default

Global lifetime values are used.

Command Modes

IPsec profile configuration (ipsec-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE set security-association lifetime command.

Examples

The following example shows how to disable the SA rekey based on the traffic-volume lifetime for an IPsec profile named if-ipsec256-ipsec-profile:

```
Device# configure-t
Device(config)#  crypto ipsec profile if-ipsec256-ipsec-profile
Device(ipsec-profile)# set ikev2-profile if-ipsec256-ikev2-profile
Device(ipsec-profile)# set pfs group16
Device(ipsec-profile)# set transform-set if-ipsec256-ikev2-transform
Device(ipsec-profile)# set security-association lifetime kilobytes disable
```

set security-association replay window-size

To control the security associations (SAs) that are created using the policy specified by a particular crypto map, dynamic crypto map, or crypto profile, use the **set security-association replay window-size**command in crypto map configuration or crypto profile configuration mode. To reset the crypto map to follow the global configuration that was specified by the **crypto ipsec security-association replay window-size** command, use the **no** form of this command.

set security-association replay window-size [*N*]
no set security-association replay

Syntax Description

N	(Optional) Size of the window. The value can be 64, 128, 256, 512, or 1024. This value sets the window size for a particular crypto map, dynamic crypto map, or crypto profile.

Command Default

Window size is not set.

Command Modes

Crypto map configuration
Crypto profile configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows that the window size has been set to 512 for the crypto ispec profile named "if-ipsec256-ipsec-profile":

```
crypto ipsec profile if-ipsec256-ipsec-profile
set ikev2-profile if-ipsec256-ikev2-profile
set pfs group16
set transform-set if-ipsec256-ikev2-transform
set security-association lifetime seconds 3600
set security-association replay window-size 512
```

set transform-set

To specify which transform sets can be used with the crypto map entry, use the **set transform-set**command in crypto map configuration mode. To remove all transform sets from a crypto map entry, use the **no** form of this command.

set transform-set *transform-set-name*
[*transform-set2...transform-set6*]
no set transform-set

Syntax Description

transform-set-name	Name of the transform set. For an **ipsec-manual** crypto map entry, you can specify only one transform set. For an **ipsec-isakmp** or dynamic crypto map entry, you can specify up to six transform sets.

Command Default

No transform sets are included by default.

Command Modes

IPsec profile configuration (ipsec-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE set transform-set command.

Examples

The following example defines a transform set and specifies that it can be used with a crypto ispec profile.

```
 crypto ipsec transform-set if-ipsec256-ikev2-transform esp-gcm 256
mode tunnel
!
crypto ipsec profile if-ipsec256-ipsec-profilep
set ikev2-profile if-ipsec256-ikev2-profile
set pfs group16
set transform-set if-ipsec256-ikev2-transform
```

subject-name

To specify the subject name in the certificate request, use the **subject-name** command in ca-trustpoint configuration mode. To clear any subject name from the configuration, use the **no** form of this command.

subject-name *name*
no subject-name *name*

Syntax Description

name	Specifies the subject name used in the certificate request.

Command Default

If the *name* argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE subject-name command.

Examples

The following example shows how to specify the subject name for the certificate:

```
crypto pki trustpoint TP-self-signed-3865005142
  enrollment selfsigned
  revocation-check none
  subject-name     cn=IOS-Self-Signed-Certificate-3865005142
```