F through H

filter-hash

Note Effective with Cisco IOS Release 15.2(4)M, the **filter-hash** command is not available in Cisco IOS software.

To specify the hash for verification and validation of decrypted contents, use the **filter-hash** command in Flexible Packet Matching (FPM) encryption filter configuration mode.

filter-hash *hash-value*

Syntax Description

hash-value	Hash value obtained from the encrypted traffic classification definition file (eTCDF).

Command Default

No hash value is specified.

Command Modes

FPM encryption filter configuration (c-map-match-enc-config)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Usage Guidelines

If you have access to an eTCDF or if you know valid values to configure encrypted FPM filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **filter-hash** command to specify the hash for verification and validation of decrypted contents.

Examples

The following example shows how to specify the hash value from the eTCDF file for verification and validation of decrypted contents:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# filter-hash AABBCCDD11223344
Router(c-map-match-enc-config)#
```

Related Commands

Command	Description
class-map type	Creates a class map to be used for matching packets to a specified class.
match encrypted	Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode.

filter-id

Note Effective with Cisco IOS Release 15.2(4)M, the **filter-id** command is not available in Cisco IOS software.

To specify a filter-level ID for encrypted filters, use the **filter-id** command in FPM match encryption filter configuration mode.

filter-id *id-value*

Syntax Description

id-value	Filter-level ID value.

Command Default

No filter ID is specified.

Command Modes

FPM match encryption filter configuration (c-map-match-enc-config)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Usage Guidelines

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **filter-id** command to specify a filter-level ID for encrypted filters.

Examples

The following example shows how to specify the filter ID value for an encrypted filter:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# filter-id id2
Router(c-map-match-enc-config)#
```

Related Commands

Command	Description
class-map type	Creates a class map to be used for matching packets to a specified class.
match encrypted	Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode.

filter-version

Note Effective with Cisco IOS Release 15.2(4)M, the **filter-version** command is not available in Cisco IOS software.

To specify the filter-level version value for the encrypted filter, use the **filter-version** command in FPM match encryption filter configuration mode.

filter-version *version*

Syntax Description

version	Filter-level version value of the encrypted filter.

Command Default

No filter version is specified.

Command Modes

FPM match encryption filter configuration (c-map-match-enc-config)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Usage Guidelines

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **filter-version** command to specify the filter-level version value for the encrypted filter.

Examples

The following example shows how to specify the filter version for the encrypted filter:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# filter-version v1
Router(c-map-match-enc-config)#
```

Related Commands

Command	Description
class-map type	Creates a class map to be used for matching packets to a specified class.
match encrypted	Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode.

filter tunnel

To configure a SSL VPN tunnel access filter, use **filter tunnel** command in webvpn group policy configuration mode. To remove the tunnel access filter, use the **no** form of this command.

filter tunnel {*extended-acl* *acl-name*}
no filter tunnel

Syntax Description

extended-acl	Defines the filter on the basis of an extended access list (ACL). A named, numbered, or expanded access list is entered.
acl -name	Specifies the name for the access list.

Command Default

A SSL VPN tunnel access filter is not configured.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The tunnel access filter is used to control network- and application-level access.

Examples

The following example shows how to configure a deny access filter for any host from the 192.0.2.0/24 network:

```
Device(config)# access-list 101 deny ip 192.0.2.0 0.0.0.255 any
Device(config)# webvpn context context1
Device(config-webvpn-context)# policy group ONE
Device(config-webvpn-group)# filter tunnel 101
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

fingerprint

To preenter a fingerprint that can be matched against the fingerprint of an untrusted certification authority (CA) certificate during authentication, use the **fingerprint** command in crypto pki trustpoint configuration mode. To remove the preentered fingerprint, use the **no** form of this command.

fingerprint *ca-fingerprint*
no fingerprint *ca-fingerprint*

Syntax Description

ca-fingerprint	Certificate fingerprint.

Command Default

A fingerprint is not preentered for a trustpoint, and if the authentication request is interactive, you must verify the fingerprint that is displayed during authentication of the CA certificate. If the authentication request is noninteractive, the certificate will be rejected without a preentered fingerprint.

Command Modes

pki trustpoint configuration

Command History

Release	Modification
12.3(12)	This command was introduced. This release supports only message digest algorithm 5 (MD5) fingerprints.
12.3(13)T	Support was added for Secure Hash Algorithm 1 (SHA1), but only for Cisco IOS T releases.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Note An authentication request made using the CLI is considered an interactive request. An authentication request made using HTTP or another management tool is considered a noninteractive request.

Note The fingerprint check is performed only while authenticating the certificate of the first untrusted Certificate authority in a given CA hierarchy. In other words, Subordinate-CA certificates are not subjected to fingerprint checking if the Root-CA certificate is trusted already, however in the absence of the Root-CA certificate, authenticating the Subordinate CA's certificate first will result in fingerprint checking.This is as per the current design.

Preenter the fingerprint if you want to avoid responding to the verify question during CA certificate authentication or if you will be requesting authentication noninteractively. The preentered fingerprint may be either the MD5 fingerprint or the SHA1 fingerprint of the CA certificate.

If you are authenticating a CA certificate and the fingerprint was preentered, if the fingerprint matches that of the certificate, the certificate is accepted. If the preentered fingerprint does not match, the certificate is rejected.

If you are requesting authentication noninteractively, the fingerprint must be preentered or the certificate will be rejected. The verify question will not be asked when authentication is requested noninteractively.

If you are requesting authentication interactively without preentering the fingerprint, the fingerprint of the certificate will be displayed, and you will be asked to verify it.

Examples

The following example shows how to preenter an MD5 fingerprint before authenticating a CA certificate:

```
Router(config)# crypto pki trustpoint myTrustpoint
Router(ca-trustpoint)# fingerprint 6513D537 7AEA61B7 29B7E8CD BBAA510B
Router(ca-trustpoint) exit
Router(config)# crypto pki authenticate myTrustpoint
Certificate has the following attributes:
       Fingerprint MD5: 6513D537 7AEA61B7 29B7E8CD BBAA510B
      Fingerprint SHA1: 998CCFAA 5816ECDE 38FC217F 04C11F1D DA06667E
Trustpoint Fingerprint: 6513D537 7AEA61B7 29B7E8CD BBAA510B
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
Router (config)#
```

The following is an example for Cisco Release 12.3(12). Note that the SHA1 fingerprint is not displayed because it is not supported by this release.

```
Router(config)# crypto ca trustpoint myTrustpoint
Router(ca-trustpoint)# fingerprint 6513D537 7AEA61B7 29B7E8CD BBAA510B
Router(ca-trustpoint)# exit
Router(config)# crypto ca authenticate myTrustpoint
Certificate has the following attributes:
           Fingerprint: 6513D537 7AEA61B7 29B7E8CD BBAA510B
Trustpoint Fingerprint: 6513D537 7AEA61B7 29B7E8CD BBAA510B
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
Router(config)#
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto ca trustpoint	Declares the CA that your router should use.

firewall

To specify secure virtual LAN (VLAN) groups and to attach them to firewall modules, use the **firewall** command in global configuration mode. To disable the configuration, use the **no** form of this command.

firewall {**autostate** | **module** *number* **vlan-group** *number* | **multiple-vlan-interfaces** | **vlan-group** *number vlan-range*}
no firewall {**autostate** | **module** *number* **vlan-group** *number* | **multiple-vlan-interfaces** | **vlan-group** *number vlan-range*}

Syntax Description

autostate	Enables auto state.
module	Specifies the module number to which a VLAN group is attached.
number	Module number. Valid values are from 1 to 6.
vlan-group	Specifies the secure group to which the VLANs are attached.
number	Group number. The range is from 1 to 65535.
multiple-vlan-interfaces	Enables multiple VLAN interfaces mode for firewall modules.
vlan-range	VLAN range. Valid values are from 2 to 1001 and 1006 to 4094.

Command Default

No secure VLAN groups are attached to firewall modules.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Examples

The following example shows how to configure a VLAN group:

```
Router(config)# firewall vlan-group 34 1-20
```

Related Commands

Command	Description
show firewall vlan-group	Displays secure VLANs attached to a secure group.

flow restrict

To restrict the traffic coming from Cisco Easy VPN inside interface to go out in clear text when a VPN tunnel is down, use the **flow restrict** command in Cisco Easy VPN Remote configuration mode. To allow traffic in a VPN connection, use the **no** form of this command.

flow restrict
no flow restrict

Syntax Description

This command has no keywords or arguments.

Command Default

If this command is not used, all traffic will go out in clear text when a VPN connection is down.

Command Modes

Cisco Easy VPN Remote configuration (config-crypto-ezvpn)

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Before you configure the **flow restrict** command, you must use the **crypto ipsec client ezvpn** command to place the device in the Cisco Easy VPN remote configuration mode.

Example

```
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!
!
crypto ipsec transform-set 3DES-SHA esp-3des esp-sha-hmac
!
!
!
crypto ipsec client ezvpn customer-vpn
 connect auto
 group vpntest key cisco
 mode network-extension
 peer 10.198.16.132 default
 flow restrict
 virtual-interface 2
 username cisco password cisco
 xauth userid mode local
crypto ipsec client ezvpn aap01651
 connect auto
 group vpntest key cisco
 mode network-extension
 peer 10.198.16.153
 flow restrict
 virtual-interface 1
 username cisco password cisco
 xauth userid mode local
```

Related Commands

Command	Description
crypto ipsec client ezvpn	Creates a Cisco Easy VPN remote configuration.

fpm package-group

Note Effective with Cisco IOS Release 15.2(4)M, the **fpm package-group** command is not available in Cisco IOS software.

To configure flexible packet matching (fpm) package support, use the **fpm package-group** command in global configuration mode. To disable fpm package support, use the **no** form of this command.

fpm package-group [**fpm-group-name**]
no fpm package-group [**fpm-group-name**]

Syntax Description

fpm-group-name	Specifies the fpm package group name.

Command Default

FPM groups are not configured by default.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Examples

The following example enables fpm package-group:

```
Router(config)# fpm package-group fpm-group-76
```

Related Commands

Command	Description
fpm package-info	Enables fpm package transfer.

fpm package-info

Note Effective with Cisco IOS Release 15.2(4)M, the **fpm package-info** command is not available in Cisco IOS software.

To configure flexible packet matching (FPM) package transfer from an FPM server to a local server, use the **fpm package-info** command in global configuration mode. To disable fpm packet transfer, use the **no** form of this command.

fpm package-info
no fpm package-info

Syntax Description

This command has no keywords or arguments.

Command Default

The command is not configured by default.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Examples

The following example enables fpm package transfer:

```
Router(config)# fpm package-info
```

Related Commands

Command	Description
fpm package-group	Configures fpm package group support.
show fpm package-group	Displays fpm package matching support configuration details.
show fpm package-info	Displays fpm package transfer configuration details.

fqdn (IKEv2 profile)

To derive the name mangler from the remote identity of type Fully Qualified Domain Name (FQDN), use the **fqdn** command in IKEv2 name mangler configuration mode. To remove the name derived from FQDN, use the **no** form of this command.

fqdn {**all** | **domain** | **hostname**}
no fqdn

Syntax Description

all	Derives the name mangler from the entire FQDN.
domain	Derives the name mangler from the domain name of FQDN.
hostname	Derives the name mangler from the hostname of FQDN.

Command Default

No default behavior or values.

Command Modes

IKEv2 name mangler configuration (config-ikev2-name-mangler)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to derive the name mangler from the remote identity of type FQDN.

Examples

The following example shows how to derive a name for the name mangler from the hostname of FQDN:

```
Router(config)# crypto ikev2 name-mangler mangler2
Router(config-ikev2-name-mangler)# fqdn hostname
```

Related Commands

Command	Description
crypto ikev2 name mangler	Defines a name mangler.

grant auto rollover

To enable automatic granting of certificate reenrollment requests for a Cisco IOS subordinate certificate authority (CA) server or registration authority (RA) mode CA, use the **grant auto rollover** command in certificate server configuration mode. To disable automatic granting of certificate reenrollment requests for a Cisco IOS subordinate or RA-mode CA server, use the **no** form of this command.

grant auto rollover {**ca-cert** | **ra-cert**}
no grant auto rollover {**ca-cert** | **ra-cert**}

Syntax Description

ca-cert	Specifies that auto renewal is enabled for the subordinate CA rollover certificate.
ra-cert	Specifies that auto renewal is enabled for the RA-mode CA rollover certificate.

Command Default

Automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA-mode CA reenrollment requests is not enabled. Reenrollment requests will have to be granted manually.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

The first time a CA is enabled, a certificate request is sent to its superior CA. This initial request must be granted manually. The **grant auto rollover**command allows subsequent renewal certificate grant requests to be automatically processed by the CA for either a subordinate CA certificate (by designating the **ca-cert** keyword) or an RA-mode CA (by designating the **ra-cert** keyword), thereby eliminating the need for operator intervention.

Examples

The following example shows how the user can enable automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server:

```
Router(config)#crypto pki server CA
Router(cs-server)#grant auto rollover ca-cert
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crl (cs-server)	Specifies the CRL PKI CS.

Command	Description
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials
database archive	Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.
database level	Controls what type of data is stored in the certificate enrollment database.
database url	Specifies the location where database entries for the CS is stored or published.
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.
default (cs-server)	Resets the value of the CS configuration command to its default.
grant auto trustpoint	Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.
grant none	Specifies all certificate requests to be rejected.
grant ra-auto	Specifies that all enrollment requests from an RA be granted automatically.
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.
issuer-name	Specifies the DN as the CA issuer name for the CS.
lifetime (cs-server)	Specifies the lifetime of the CA or a certificate.

Command	Description
mode ra	Enters the PKI server into RA certificate server mode.
mode sub-cs	Enters the PKI server into sub-certificate server mode
redundancy (cs-server)	Specifies that the active CS is synchronized to the standby CS.
serial-number (cs-server)	Specifies whether the router serial number should be included in the certificate request.
show (cs-server)	Displays the PKI CS configuration.
shutdown (cs-server)	Allows a CS to be disabled without removing the configuration.

grant auto trustpoint

To specify the certification authority (CA) trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests, use the **grant auto trustpoint**command in certificate server configuration mode. To remove the name of the trustpoint holding the trusted CA certificate, use the **no** form of this command.

grant auto trustpoint *label*
no grant auto trustpoint *label*

Syntax Description

label	Name of the non-Cisco IOS CA trustpoint.

Command Default

No default behavior or values.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

After the network administrator for the server configures and authenticates a trustpoint for the CA of another vendor, the **grant auto trustpoint** command is issued to reference the newly created trustpoint and enroll the router with a Cisco IOS CA.

Note The newly created trustpoint can only be used one time (which occurs when the router is enrolled with the Cisco IOS CA). After the initial enrollment is successfully completed, the credential information will be deleted from the enrollment profile.

The Cisco IOS certificate server will automatically grant only the requests from clients who were already enrolled with the CA of another vendor. All other requests must be manually granted--unless the server is set to be in auto grant mode (through the **grant automatic**command).

Caution The **grant automatic**command can be used for testing and building simple networks and should be disabled before the network is accessible by the Internet. However, it is recommended that you do not issue this command if your network is generally accessible .

Examples

The following example shows how to configure a client router and a Cisco IOS certificate server to exchange enrollment requests through a certificate enrollment profile:

```
! Define the trustpoint “msca-root” that points to the non-Cisco IOS CA and enroll and !
authenticate the client with the non-Cisco IOS CA.
crypto pki trustpoint msca-root
 enrollment mode ra
 enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
 ip-address FastEthernet2/0
 revocation-check crl
!
! Configure trustpoint “cs” for Cisco IOS CA.
crypto pki trustpoint cs
 enrollment profile cs1
 revocation-check crl
!
! Define enrollment profile “cs1,” which points to Cisco IOS CA and mention (via the !
enrollment credential command) that “msca-root” is being initially enrolled with the ! Cisco
 IOS CA.
crypto pki profile enrollment cs1
 enrollment url  http://cs:80
 enrollment credential  msca-root!
! Configure the certificate server, and issue the grant auto trustpoint command to ! instruct
 the certificate server to accept enrollment request only from clients who are ! already
enrolled with trustpoint “msca-root.”
crypto pki server cs
 database level minimum
 database url nvram:
 issuer-name CN=cs
 grant auto trustpoint msca-root
!
crypto pki trustpoint cs
 revocation-check crl
rsakeypair cs
!
crypto pki trustpoint msca-root
 enrollment mode ra
 enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
 revocation-check crl
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crl (cs-server)	Specifies the CRL PKI CS.
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials
database archive	Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.

Command	Description
database level	Controls what type of data is stored in the certificate enrollment database.
database url	Specifies the location where database entries for the CS is stored or published.
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.
default (cs-server)	Resets the value of the CS configuration command to its default.
grant auto rollover	Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.
grant none	Specifies all certificate requests to be rejected.
grant ra-auto	Specifies that all enrollment requests from an RA be granted automatically.
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.
issuer-name	Specifies the DN as the CA issuer name for the CS.
lifetime (cs-server)	Specifies the lifetime of the CA or a certificate.
mode ra	Enters the PKI server into RA certificate server mode.
mode sub-cs	Enters the PKI server into sub-certificate server mode
redundancy (cs-server)	Specifies that the active CS is synchronized to the standby CS.
serial-number (cs-server)	Specifies whether the router serial number should be included in the certificate request.

Command	Description
show (cs-server)	Displays the PKI CS configuration.
shutdown (cs-server)	Allows a CS to be disabled without removing the configuration.

grant none

To specify all certificate requests to be rejected, use the **grant none** command in certificate server configuration mode. To disable automatic rejection of certificate enrollment, use the **no** form of this command.

grant none
no grant none

Syntax Description

This command has no arguments or keywords.

Command Default

Certificate enrollment is manual; that is, authorization is required.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

Examples

The following example shows how to automatically reject all certificate enrollment requests for the certificate server "myserver":

```
Router#(config) ip http server
Router#(config) crypto pki server myserver
Router#(cs-server) database level minimum
Router#(cs-server)#
grant none
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crl (cs-server)	Specifies the CRL PKI CS.
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials

Command	Description
database archive	Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.
database level	Controls what type of data is stored in the certificate enrollment database.
database url	Specifies the location where database entries for the CS is stored or published.
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.
default (cs-server)	Resets the value of the CS configuration command to its default.
grant auto rollover	Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.
grant auto trustpoint	Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.
grant ra-auto	Specifies that all enrollment requests from an RA be granted automatically.
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.
issuer-name	Specifies the DN as the CA issuer name for the CS.
lifetime (cs-server)	Specifies the lifetime of the CA or a certificate.
mode ra	Enters the PKI server into RA certificate server mode.

Command	Description
mode sub-cs	Enters the PKI server into sub-certificate server mode
redundancy (cs-server)	Specifies that the active CS is synchronized to the standby CS.
serial-number (cs-server)	Specifies whether the router serial number should be included in the certificate request.
show (cs-server)	Displays the PKI CS configuration.
shutdown (cs-server)	Allows a CS to be disabled without removing the configuration.

grant ra-auto

To specify that all enrollment requests from a Registration Authority (RA) be granted automatically, use the **grant ra-auto** command in certificate server configuration mode. To disable automatic certificate enrollment, use the **no** form of this command.

grant ra-auto
no grant ra-auto

Syntax Description

This command has no arguments or keywords.

Command Default

Certificate enrollment is manual; that is, authorization is required.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

When grant ra-auto mode is configured on the issuing certificate server, ensure that the RA mode certificate server is running in manual grant mode so that enrollment requests are authorized individually by the RA.

Note For the **grant ra-auto** command to work, you have to include “cn=ioscs RA” or “ou=ioscs RA” in the subject name of the RA certificate.

Examples

The following output shows that the issuing certificate server is configured to issue a certificate automatically if the request comes from an RA:

```
Router (config)# crypto pki server myserver
Router-ca (cs-server)# grant ra-auto
% This will cause all certificate requests that are already authorized by known RAs to be
automatically granted.
Are you sure you want to do this? [yes/no]:yes
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crl (cs-server)	Specifies the CRL PKI CS.

Command	Description
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials
database archive	Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.
database level	Controls what type of data is stored in the certificate enrollment database.
database url	Specifies the location where database entries for the CS is stored or published.
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.
default (cs-server)	Resets the value of the CS configuration command to its default.
grant auto rollover	Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.
grant auto trustpoint	Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.
grant none	Specifies all certificate requests to be rejected.
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.
issuer-name	Specifies the DN as the CA issuer name for the CS.
lifetime (cs-server)	Specifies the lifetime of the CA or a certificate.

Command	Description
mode ra	Enters the PKI server into RA certificate server mode.
mode sub-cs	Enters the PKI server into sub-certificate server mode
redundancy (cs-server)	Specifies that the active CS is synchronized to the standby CS.
serial-number (cs-server)	Specifies whether the router serial number should be included in the certificate request.
show (cs-server)	Displays the PKI CS configuration.
shutdown (cs-server)	Allows a CS to be disabled without removing the configuration.

group (firewall)

To enter redundancy application group configuration mode, use the **group** command in redundancy application configuration mode. To remove the group configuration, use the **no** form of this command.

group *id*
no group *id*

Syntax Description

id	Redundancy group ID. Valid values are 1 and 2.

Command Default

No group is configured.

Command Modes

Redundancy application configuration (config-red-app)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure a redundancy group with group ID 1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)#
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.

group (authentication)

To specify the authentication, authorization, and accounting (AAA) TACACS+ server group to use for preauthentication, use the **group** command in AAA preauthentication configuration mode. To remove the **group** command from your configuration, use the **no** form of this command.

group tacacs+ *server-group*
no group tacacs+ *server-group*

Syntax Description

tacacs+	Uses a TACACS+ server for authentication.
server-group	Name of the server group to use for authentication.

Command Default

No method list is configured.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must configure the **group** command before you configure any other AAA preauthentication command (**clid**, **ctype**, **dnis**, or **dnis bypass**).

Examples

The following example enables Dialed Number Identification Service (DNIS) preauthentication using the abc123 server group and the password aaa-DNIS:

```
aaa preauth
 group abc123
 dnis password aaa-DNIS
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication mode.
dnis (authentication)	Enables AAA preauthentication using DNIS.

group (IKE policy)

To specify one or more Diffie-Hellman (DH) group identifier(s) for use in an Internet Key Exchange (IKE) policy, which defines a set of parameters to be used during IKE negotiation , use the **group**command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. To reset the DH group identifier to the default value, use the **no** form of this command.

group {**1** | **2** | **5** | **14** | **15** | **16** | **19** | **20** | **24**}
no group

Syntax Description

1	Specifies the 768-bit DH group.
2	Specifies the 1024-bit DH group.
5	Specifies the 1536-bit DH group.
14	Specifies the 2048-bit DH group.
15	Specifies the 3072-bit DH group.
16	Specifies the 4096-bit DH group.
19	Specifies the 256-bit elliptic curve DH (ECDH) group.
20	Specifies the 384-bit ECDH group.
21	Specifies the 521-bit elliptic curve DH (ECDH) group.
24	Specifies the 2048-bit DH/DSA group.

Command Default

DH group 1

Command Modes

ISAKMP policy configuration (config-isakmp)

Command History

Release	Modification
11.3 T	This command was introduced.
12.1(1.3)T	Support was added for DH group 5.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.2	Support was added for DH groups 14, 15, and 16 on the Cisco ASR 1000 series routers.

Release	Modification
15.1(2)T	This command was modified. The **14**, **15**, **16**, **19**, and **20** keywords were added.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

The group chosen must be strong enough (have enough bits) to protect the IPsec keys during negotiation. A generally accepted guideline recommends the use of a 2048-bit group after 2013 (until 2030). Either group 14 or group 24 can be selected to meet this guideline. Even if a longer-lived security method is needed, the use of Elliptic Curve Cryptography is recommended, but group 15 and group 16 can also be considered.

The ISAKMP group and the IPsec perfect forward secrecy (PFS) group should be the same if PFS is used. If PFS is not used, a group is not configured in the IPsec crypto map.

Examples

The following example shows how to configure an IKE policy with the 1024-bit DH group (all other parameters are set to the defaults):

```
Router(config)# crypto isakmp policy 15
Router(config-isakmp) group 2
Router(config-isakmp)
 exit
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

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
15.1(1)T	This command was introduced.
15.1(2)T	This command was modified. The **14**, **15**, **16**, **19**, and **20** keywords were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

The group type can be one of the following:

Group Type	Description
1	Specifies the 768-bit DH group.
2	Specifies the 1024-bit DH group.
5	Specifies the 1536-bit DH group.
14	Specifies the 2048-bit DH group
15	Specifies the 3072-bit DH group.
16	Specifies the 4096-bit DH group.
19	Specifies the 256-bit elliptic curve DH (ECDH) group.

Group Type	Description
20	Specifies the 384-bit ECDH group.
21	Specifies the 521-bit elliptic curve DH (ECDH) group.
24	Specifies the 2048-bit DH/DSA group.

The group chosen must be strong enough (have enough bits) to protect the IPsec keys during negotiation. A generally accepted guideline recommends the use of a 2048-bit group after 2013 (until 2030). Either group 14 or group 24 can be selected to meet this guideline. Even if a longer-lived security method is needed, the use of Elliptic Curve Cryptography is recommended, but group 15 and group 16 can also be considered.

Examples

The following example shows how to configure an IKEv2 proposal with the 1024-bit DH group:

```
Device(config)# crypto ikev2 proposal proposal1
Device(config-ikev2-proposal)# group 2
Device(config-ikev2-proposal)# exit
```

Related Commands

Command	Description
crypto ikev2 proposal	Defines an IKEv2 proposal.
encryption (ikev2 proposal)	Specifies the encryption algorithm in an IKEv2 proposal.
integrity (ikev2 proposal)	Specifies the integrity algorithm in an IKEv2 proposal.
show crypto ikev2 proposal	Displays the algorithms configured in each IKEv2 proposal.

group (local RADIUS server)

To enter user group configuration mode and to configure shared settings for a user group, use the **group**command in local RADIUS server configuration mode. To remove the group configuration from the local RADIUS server, use the **no** form of this command.

group *group-name*
no group *group-name*

Syntax Description

group-name	Name of user group.

Command Default

No default behavior or values

Command Modes

Local RADIUS server configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following example shows that shared settings are being configured for group “team1”:

```
group team1
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.

Command	Description
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

group (RADIUS)

To specify the authentication, authorization, and accounting (AAA) RADIUS server group to use for preauthentication, use the **group** command in AAA preauthentication configuration mode. To remove the **group** command from your configuration, use the **no** form of this command.

group *server-group*
no group *server-group*

Syntax Description

server-group	Specifies a AAA RADIUS server group.

Command Default

No default behavior or values.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You must configure a RADIUS server group with the **aaa group server radius** command in global configuration mode before using the **group** command in AAA preauthentication configuration mode.

You must configure the **group** command before you configure any other AAA preauthentication command (**clid**, **ctype**, **dnis**, or **dnis bypass**).

Examples

The following example shows the creation of a RADIUS server group called “maestro” and then specifies that DNIS preauthentication be performed using this server group:

```
aaa group server radius maestro
 server 10.1.1.1
 server 10.2.2.2
 server 10.3.3.3
aaa preauth
 group maestro
 dnis required
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
clid	Preauthenticates calls on the basis of the CLID number.
ctype	Preauthenticates calls on the basis of the call type.
dnis (RADIUS)	Preauthenticates calls on the basis of the DNIS number.

Command	Description
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.

group-lock

The **group-lock** command attribute is used to check if a user attempting to connect to a group belongs to this group. This attribute is used in conjunction with the extended authentication (Xauth) username. The user name must include the group to which it belongs. The group is then matched against the VPN group name (ID_KEY_ID) that is passed during the Internet Key Exchange (IKE). If the groups do not match, then the client connection is terminated.

To allow the extended authentication (Xauth) username to be entered when preshared key authentication is used with IKE, use the **group-lock** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove the group lock, use the **no** form of this command.

Note Preshared keys are supported only. Certificates are not supported.

group-lock
no group-lock

Syntax Description

This command has no arguments or keywords.

Command Default

Group lock is not configured.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

The Group-Lock attribute can be used if preshared key authentication is used with IKE. When the user enables the **group-lock** command attribute, one of the following extended Xauth usernames can be entered:

name/group

name\group

name@group

name%group

where the \ / @ % are the delimiters. The group that is specified after the delimiter is then compared against the group identifier that is sent during IKE aggressive mode. The groups must match or the connection is rejected.

Caution Do not use the Group-Lock attribute if you are using RSA signature authentication mechanisms such as certificates. Use the User-VPN-Group attribute instead.

The Group-Lock attribute is configured on a Cisco IOS router or in the RADIUS profile. This attribute has local (gateway) significance only and is not passed to the client.

Note If local authentication is used, then the Group-Lock attribute is the only option.

The username in the local or RADIUS database must be of the following format:

username[/,\,%,@]group.

Examples

The following example shows how Group-Lock attribute is configured in the CLI using the **group-lock** command:

Note You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that has to be defined or changed, before enabling the **group-lock** command.

```
crypto isakmp client configuration group cisco
  group-lock
```

The following example shows how an attribute-value (AV) pair for the User-VPN-Group attribute is added in the RADIUS configuration:

Note If RADIUS is used for user authentication, then use the User-VPN-Group attribute instead of the Group-Lock attribute.

```
ipsec:group-lock=1
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

group-object

To specify a nested reference to a type of user group within an object group, use the **group-object** command in object-group identity configuration mode. To remove the user group from the object group, use the **no** form of this command.

group-object *name*
no group-object *name*

Syntax Description

name	Nested user group name.

Command Default

No nested user group is defined.

Command Modes

Object-group identity configuration (config-object-group)

Command History

Release	Modification
15.2(1)S	This command was introduced in Cisco IOS Release 15.2(1)S.
Cisco IOS XE Release 3.5	This command was introduced in Cisco IOS XE Release 3.5.

Usage Guidelines

In addition to a security group that is specified for the object group, a group object can be specified for a nested user group. The **group-object** command is used in the class map configuration of the Security Group Access (SGA) Zone-Based Policy firewall (ZBPF). Multiple nested user groups can be specified using this command.

Note A policy map must also be configured for the SGA ZBPF.

Examples

The following example shows how the **group-object** command is used in the class map configuration of the SGA ZBPF.

```
Router(config)# object-group security myobject1a
Router(config-object-group)# security-group tag-id 1
Router(config-object-group)# end
Router(config)# object-group security myobject1b
Router(config-object-group)# security-group tag-id 2
Router(config-object-group)# end
Router(config)# object-group security myobject1
Router(config-object-group)# group-object myobject1a
Router(config-object-group)# group-object myobject1b
Router(config-object-group)# end
Router(config)# class-map type inspect match-any myclass1
Router(config-cmap)# match group-object security source myobject1
Router(config-cmap)# end
```

Related Commands

Command	Description
debug object-group event	Enables debug messages for object-group events.
match group-object security	Matches traffic from a user in the security group.
object-group security	Creates an object group to identify traffic coming from a specific user or endpoint.
security-group	Specifies the membership of the security group for an object group.
show object-group	Displays the content of all user groups.

group size

To set the group size (sender ID length) for Suite B, use the **group size** command in GDOI local server configuration mode. To return a group size to the default size, use the **no** form of this command.

group size {**small** {**8** | **12** | **16**} | **medium** | **large**}
no group size [**small** [**8** | **12** | **16**] | **medium** | **large**]

Syntax Description

small {**8** | **12** | **16**}	Specifies an 8-, 12-, or 16-bit sender identifier (SID).
medium	Specifies a 24-bit SID.
large	Specifies a 32-bit SID (FIPS 140-2 operating mode).

Command Default

Medium

Command Modes

GDOI local server configuration (gdoi-local-server)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

SID lengths of 8, 12, or 16 bits ensure interoperability with the GDOI standard that is described in RFC 6054, Using Counter Modes with Encapsulating Security Payload (ESP) and Authentication Header (AH) to Protect Group Traffic.

For most deployments, a group size of medium is recommended; therefore, using this command is optional. Any group size other than medium should be used only for interoperability (for which a small 8-bit, small 12-bit, or small 16-bit size should be used) or if you need to strictly adhere to FIPS 140-2 compliance (in which case, large is required). If you use this command, you should choose the group size based on the anticipated number of key servers (KSs) and group members (GMs).

When you change the group size in a group with cooperative KSs while Suite B (meaning ESP-GCM or ESP-GMAC) is configured and while the Suite B policy has been generated, you must change the group size on all secondary KSs before changing it on the primary KS.

Changing the group size causes the group to reinitialize (so that the new SID length can be used). The following prompt appears:

```
Device(gdoi-local-server)# group size large

% Changing Group Size from MEDIUM to LARGE will cause
% the group to re-initialize...

Are you sure you want to proceed? [yes/no]:
```

If the group size is decreasing and KS SIDs (KSSIDs) were configured that are not supported in the new group size (for example, 256 was configured with large and you changed it to medium, which has a maximum KSSID value of 127), the following prompt appears:

```
Device(gdoi-local-server)# group size medium

% Changing the Group Size from LARGE to MEDIUM will cause the group to
% re-initialize & the following configured Key Server SIDs will be lost:
%   256, 510-511

Are you sure you want to proceed? [yes/no]:
```

If cooperative KSs are configured, changing the group size on a secondary cooperative KS will not change the group size used and will not cause reinitialization until the primary cooperative KS changes the group size and reinitializes the group:

```
Device(gdoi-local-server)# group size large

% Secondary COOP-KS will change configured Group Size from MEDIUM to LARGE
% but will not use this Group Size until Primary COOP-KS changes as well.
```

If the group is currently reinitializing, changing the group size is denied:

```
Device(gdoi-local-server)# group size large

% Group Size Configuration Denied:
%   Please wait for group getvpn to finish re-initialization
%   and try changing the Group Size again.
```

If cooperative KSs are configured and the local KS is primary, changing the group size is denied if all of the secondary cooperative KS peers have not already changed their group size to the new group size:

```
Device(gdoi-local-server)# group size large

% Primary COOP-KS cannot change Group Size from MEDIUM to LARGE while the
% following Secondary COOP-KS peers have not changed to LARGE:
%   10.0.9.1 (Group Size: MEDIUM)
```

If cooperative KSs are configured and the local KS is primary, changing the group size is denied if all of the secondary cooperative KS peers are not alive (meaning that there is a network split):

```
Device(gdoi-local-server)# group size large

% Primary COOP-KS cannot change Group Size from MEDIUM to LARGE while
% there is a network split with the following COOP-KS peers:
%   10.0.8.1 (Role: Primary, Status: Dead)
```

Examples

The following example shows how to configure a SID length of 16-bit small:

```
Device# crypto gdoi group GETVPN
Device(config-gdoi-group) server local
Device(gdoi-local-server) group size small 16
```

Related Commands

Command	Description
crypto gdoi group	Creates a GDOI group and enters GDOI group configuration mode.

gtp

To configure the inspection parameters for General Packet Radio Service (GPRS) Tunneling Protocol (GTP), use the **gtp** command in parameter-map profile configuration mode. To disable the inspection parameters for GTP, use the **no** form of this command.

gtp {**request-queue** *elements* | **timeout** { {**gsn** | **pdp-context** | **signaling** | **tunnel**} *minutes* | **request-queue** *seconds*} | **tunnel-limit** *number*}
no gtp {**request-queue** | **timeout** {**gsn** | **pdp-context** | **signaling** | **tunnel** | **request-queue**} | **tunnel-limit**}

Syntax Description

request-queue	Specifies the queue depth of GTP requests.
elements	Number of elements in a queue. The range is from 1 to 4294967295. The default is 200.
timeout	Configures the timeout values for GTP.
gsn	Specifies the timeout value for the inactive GPRS Support Node (GSN).
minutes	Timeout in minutes. The range is from 1 to 35791. The default is 30.
pdp-context	Specifies the timeout value for inactive Packet Data Protocol (PDP) -Context.
request-queue	Specifies the timeout value for the inactive request queue.
seconds	Timeout in seconds. The range is from 1 to 2147483. The default value is 60.
signaling	Specifies the timeout value for inactive signaling.
tunnel	Specifies the timeout value for an inactive tunnel. The default value is 30 minutes.
tunnel-limit	Specifies the number of maximum allowed GTP tunnels.
number	Number of allowed GTP tunnels. The range is from 1 to 4294967295. The default is 500.

Command Default

Inspect parameters are not configured for GTP.

Command Modes

Parameter-map profile configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

The **request-queue** keyword specifies the maximum number of GTP requests that will be queued while waiting for a response. When the specified limit is reached and a new request arrives, the request that has been in the queue for the longest time is removed. After the inactivity timer has elapsed, the request will be removed from the queue.

Examples

The following examples show how to configure the maximum number of GTP requests that will be queued while waiting for a response.

```
Router(config)# parameter-map type inspect pamap1
Router(config-profile)# gtp request-queue 100
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

hardware statistics

To enable the collection of hardware statistics, use the **hardware statistics**command in IPv6or IPv4 access-list configuration mode. To disable this feature, use the **no** form of this command.

hardware statistics
no hardware statistics

Syntax Description

This commands has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

IPv6 access-list configuration (config-ipv6-acl)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The hardware statistics command affects only global access-list (ACL) counters.

Examples

The following example enables the collection of hardware statistics in an IPv6 configuration:

```
Router(config-ipv6-acl)# hardware statistics
```

hash (ca-trustpoint)

To specify the cryptographic hash algorithm function for the signature that the Cisco IOS client uses to sign its self-signed certificates, use the **hash** command in ca-trustpoint configuration mode. To return to the default cryptographic hash function, use the **no** form of this command.

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

hash {**md5** | **sha1** | **sha256** | **sha384** | **sha512**}
no hash

Syntax Description

md5	Specifies that Message-Digest algorithm 5 (MD5) hash function is used.
sha1	Specifies that Secure Hash Algorithm (SHA-1) hash function is used as the default hash algorithm for RSA keys.
sha256	Specifies that the SHA-256 hash function is used as the hash algorithm for Elliptic Curve (EC) 256 bit keys.
sha384	Specifies that the SHA-384 hash function is used as the hash algorithm for EC 384 bit keys.
sha512	Specifies that the SHA-512 hash function is used as the hash algorithm for EC 384 bit keys.

Command Default

The Cisco IOS client uses the MD5 cryptographic hash function for self-signed certificates by default.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Any specified **hash** command algorithm keyword option can be used to over-ride the default setting for the trustpoint. This setting then becomes the default cryptographic hash algorithm function for self-signed certificates by default.

Note The algorithm does not specify what kind of signature the certificate authority (CA) uses when it issues a certificate to the client.

Examples

The following example configures the trustpoint "MyTP" and sets the cryptographic hash function to SHA-384:

```
crypto pki trustpoint MyTP
   enrollment url http://MyTP
   ip-address FastEthernet0/0
   revocation-check none
   hash sha384
```

Related Commands

Command	Description
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.

hash (cs-server)

To specify the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the certificate authority (CA), use the **hash** command in certificate server configuration mode. To return to the default cryptographic hash function, use the no form of this command.

hash {**md5** | **sha1** | **sha256** | **sha384** | **sha512**}
no hash

Syntax Description

md5	Specifies that the Message-Digest algorithm 5 (MD5), the default hash function is used.
sha1	Specifies that the Secure Hash Algorithm (SHA-1) hash function is used.
sha256	Specifies that the SHA-256 hash function is used.
sha384	Specifies that the SHA-384 hash function is used.
sha512	Specifies that the SHA-512 hash function is used.

Command Default

By default, to sign certificates issued by CA, the Cisco IOS client uses the MD5 cryptographic hash function.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

The **hash** command in cs-server configuration mode sets the hash function for the signature that the Cisco IOS CA uses to sign all of the certificates issued by the server. If the CA is a root CA, it uses the hash function in its own, self-signed certificate.

Examples

The following example configures a certificate server, MyCS, and sets the cryptographic hash function to SHA-512 for the certificate server:

```
crypto pki server MyCS
database level complete
issuer-name CN=company,L=city,C=country
grant auto trustpoint
```

```
hash sha512
lifetime crl 168
```

The following is sample output from the **show crypto ca certificates** command. This output shows that the CA has been configured and that the hash function SHA-512 has been specified.

```
CA Certificate
Status: Available
Certificate Serial Number: 01
Certificate Usage: Signature
Issuer:
cn=company
l=city
c=country
Subject:
cn=company
l=city
c=country
Validity Date:
start date: 01:32:35 GMT Aug 3 2006
end date: 01:32:35 GMT Aug 2 2009
Associated Trustpoints: MyTP
Certificate Subject:
Name: MyCS.cisco.com
IP Address: 192.168.10.2
Status: Pending Key
Usage: General Purpose
Certificate Request Fingerprint SHA1: 05080A60 82DE9395 B35607C2 38F3A0C3 50609EF8
Associated Trustpoint: MyTP
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crl (cs-server)	Specifies the CRL PKI CS.
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials
database archive	Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.
database level	Controls what type of data is stored in the certificate enrollment database.

Command	Description
database url	Specifies the location where database entries for the CS is stored or published.
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.
default (cs-server)	Resets the value of the CS configuration command to its default.
grant auto rollover	Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.
grant auto trustpoint	Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.
grant none	Specifies all certificate requests to be rejected.
grant ra-auto	Specifies that all enrollment requests from an RA be granted automatically.
issuer-name	Specifies the DN as the CA issuer name for the CS.
lifetime (cs-server)	Specifies the lifetime of the CA or a certificate.
mode ra	Enters the PKI server into RA certificate server mode.
mode sub-cs	Enters the PKI server into sub-certificate server mode
redundancy (cs-server)	Specifies that the active CS is synchronized to the standby CS.
serial-number (cs-server)	Specifies whether the router serial number should be included in the certificate request.
show (cs-server)	Displays the PKI CS configuration.

Command	Description
shutdown (cs-server)	Allows a CS to be disabled without removing the configuration.

hash (IKE policy)

To specify the hash algorithm within an Internet Key Exchange policy, use the **hash**command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the hash algorithm to the default secure hash algorithm (SHA) -1 hash algorithm, us e the **no** form of this command.

hash {**sha** | **sha256** | **sha384** | **md5**}
no hash

Syntax Description

sha	Specifies SHA-1 (HMAC variant) as the hash algorithm.
sha256	Specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm.
sha384	Specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.
md5	Specifies MD5 (HMAC variant) as the hash algorithm.

Command Default

The SHA-1 hash algorithm

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.4(4)T	IPv6 support was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(2)T	This command was modified. The **sha256** and **sha384** keywords were added.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use this command to specify the hash algorithm to be used in an IKE policy.

Examples

The following example configures an IKE policy with the MD5 hash algorithm (all other parameters are set to the defaults):

```
crypto isakmp policy 15
 hash md5
 exit
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

heading

To configure the heading that is displayed above URLs listed on the portal page of a SSL VPN, use the **heading** command in webvpn URL list configuration mode. To remove the heading, use the **no** form of this command.

heading *text-string*
no heading

Syntax Description

text-string	The URL list heading entered as a text string. The heading must be in quotation marks if it contains spaces.

Command Default

A heading is not configured.

Command Modes

Webvpn URL list configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example configures a heading for a URL list:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading "Quick Links"

Router(config-webvpn-url)#
```

Related Commands

Command	Description
url-list	Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN.

hide-url-bar

To prevent the URL bar from being displayed on the SSL VPN portal page, use the **hide-url-bar** command in webvpn group policy configuration mode. To display the URL bar on the portal page, use the **no** form of this command.

hide-url-bar
no hide-url-bar

Syntax Description

This command has no arguments or keywords.

Command Default

The URL bar is displayed on the SSL VPN portal page.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The configuration of this command applies only to clientless mode access.

Examples

The following example hides the URL bar on the SSL VPN portal page:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE

Router(config-webvpn-group)# hide-url-bar

Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

holdtime

To configure the hold time for Internet Key Exchange Version 2 (IKEv2) gateways in a Hot Standby Router Protocol (HSRP) cluster, use the **holdtime** command in IKEv2 cluster configuration mode. To restore the default hold time, use the **no** form of this command.

holdtime *milliseconds*
no holdtime

Syntax Description

milliseconds	Interval, in milliseconds, before a peer is considered dead. The range is from 100 to 120000. The default is 3000.

Command Default

The default is 3000 milliseconds if the hold time is not configured.

Command Modes

IKEv2 cluster configuration (config-ikev2-cluster)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

You must enable the **crypto ikev2 cluster** command before enabling the **holdtime** command.

Examples

The following example shows how to set the hold time to receive messages from a peer to 100 milliseconds:

```
Device(config)# crypto ikev2 cluster
Device(config-ikev2-cluster)# holdtime 100
```

Related Commands

Command	Description
crypto ikev2 cluster	Defines an IKEv2 cluster policy in an HSRP cluster.

hop-limit

To verify the advertised hop-count limit, use the **hop-limit** command in RA guard policy configuration mode.

hop-limit {**maximum** | **minimum** } *limit*

Syntax Description

maximum *limit*	Verifies that the hop-count limit is lower than that set by the *limit* argument.
minimum *limit*	Verifies that the hop-count limit is greater than that set by the *limit* argument.

Command Default

No hop-count limit is specified.

Command Modes

RA guard policy configuration
(config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **hop-limit** command enables verification that the advertised hop-count limit is greater than or less than the value set by the *limit* argument. Configuring the **minimum** *limit* keyword and argument can prevent an attacker from setting a low hop-count limit value on the hosts to block them from generating traffic to remote destinations; that is, beyond their default router. If the advertised hop-count limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Configuring the **maximum** *limit* keyword and argument enables verification that the advertised hop-count limit is lower than the value set by the *limit* argument. If the advertised hop-count limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and sets a minimum hop-count limit of 3:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# hop-limit minimum 3
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

host (webvpn url rewrite)

To select the name of the host site to be mangled on a Secure Socket Layer virtual private network (SSL VPN) gateway, use the **host** command in webvpn url rewrite configuration mode. To deselect a site, use the **no** form of this command.

host *host-name*
no host *host-name*

Syntax Description

host-name	Hostname of the site to be mangled.

Command Default

A host site is not selected.

Command Modes

Webvpn url rewrite (config-webvpn-url-rewrite)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows that the site www.examplecompany.com is to be mangled:

```
Router (config)# webvpn context
Router (config-webvpn-context)# url rewrite
Router (config-webvpn-url-rewrite)# host www.examplecompany.com
```

Related Commands

Command	Description
ip (webvpn url rewrite)	Configures the IP address of the site to be mangled on an SSL VPN gateway.
unmatched-action (webvpn url rewrite)	Defines the action when the user request does not match the IP address or host site configuration.

hostname (IKEv2 keyring)

To specify the hostname for the peer in the Internet Key Exchange Version 2 (IKEv2) keyring, use the **hostname** command IKEv2 keyring peer configuration mode. To remove the hostname, use the **no** form of this command.

hostname *name*
no hostname

Syntax Description

name	Name for the peer.

Command Default

The hostname is not specified.

Command Modes

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

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

When configuring the IKEv2 keyring, use this command to identify the peer using hostname, which is:

- Independent of the IKEv2 identity.
- Available on an IKEv2 initiator only.
- Provided by IPsec to IKEv2 as part of a security association setup request to identify the peer.
- Used to identify the peer only with crypto maps and not with tunnel protection.

Examples

The following example shows how to configure the hostname for a peer when configuring an IKEv2 keyring:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description peer1
Router(config-ikev2-keyring-peer)# hostname peer1.example.com
```

Related Commands

Command	Description
address (ikev2 keyring)	Specifies the IPv4 address or the range of the peers in IKEv2 key.
crypto ikev2 keyring	Defines an IKEv2 keyring.
description (ikev2 keyring)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.

Command	Description
identity (ikev2 keyring)	Identifies the peer with IKEv2 types of identity.
peer	Defines a peer or a peer group for the keyring.
pre-shared-key **(ikev2 keyring)**	Defines a preshared key for the IKEv2 peer.

hostname (WebVPN)

To configure the hostname for a SSL VPN gateway, use the **hostname** command in webvpn gateway configuration mode. To remove the hostname from the SSL VPN gateway configuration, use the **no** form of this command.

hostname *name*
no hostname

Syntax Description

name	Specifies the hostname.

Command Default

The hostname is not configured.

Command Modes

Webvpn gateway configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

A hostname is configured for use in the URL and cookie-mangling process. In configurations where traffic is balanced among multiple SSL VPN gateways, the hostname configured with this command maps to the gateway IP address configured on the load-balancing device(s).

Examples

The following example configures a hostname for a SSL VPN gateway:

```
Router(config)# webvpn gateway GW_1
Router(config-webvpn-gateway)# hostname VPN_Server
```

Related Commands

Command	Description
webvpn gateway	Defines a SSL VPN gateway and enters webvpn gateway configuration mode.

http proxy-server

To direct Secure Socket Layer virtual private network (SSL VPN) user requests through a backend HTTP proxy server, use the **http proxy-server** command in webvpn policy group configuration mode. To redirect user requests to internal servers, use the **no** form of this command.

http proxy-server {*dns-nameip-address*} **port** *port-number*
no http proxy-server

Syntax Description

dns-name	Domain Name System (DNS) to be directed to the HTTP proxy server.
ip-address	IP address to be directed to the HTTP proxy server.
port *port-number*	Port number of the backend HTTP proxy server.

Command Default

User requests are routed directly to internal servers.

Command Modes

Webvpn policy group configuration (config-webvpn-group)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows that requests from IP address 10.1.1.1 are to be routed to the proxy server (port number 2034):

```
Router (config)# webvpn context e1
Router (config-webvpn-context)# policy group g1
Router (config-webvpn-group)# http proxy-server 10.1.1.1 port 2034
Router (config-webvpn-group)# exit
Router (config-webvpn-context)# default-group-policy g1
```

http-redirect

To configure HTTP traffic to be carried over secure HTTP (HTTPS), use the **http-redirect** command in webvpn gateway configuration mode. To remove the HTTPS configuration from the SSL VPN gateway, use the **no** form of this command.

http-redirect [**port** *number*]
no http-redirect

Syntax Description

port *number*	(Optional) Specifies a port number. The value for this argument is a number from 1 to 65535.

Command Default

The following default value is used if this command is configured without entering the **port** keyword:

port *number* : 80

Command Modes

Webvpn gateway configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When this command is enabled, the HTTP port is opened and the SSL VPN gateway listens for HTTP connections. HTTP connections are redirected to use HTTPS. Entering the **port**keyword and *number* argument configures the gateway to listen for HTTP traffic on the specified port. Entering the **no** form, disables HTTP traffic redirection. HTTP traffic is handled by the HTTP server if one is running.

Examples

The following example, starting in global configuration mode, redirects HTTP traffic (on TCP port 80) over to HTTPS (on TCP port 443):

```
Router(config)# webvpn gateway SSL_GATEWAY

Router(config-webvpn-gateway)# http-redirect
```

Related Commands

Command	Description
webvpn gateway	Defines a SSL VPN gateway and enters webvpn gateway configuration mode.

hw-module slot subslot only

Note This command is deleted effective with Cisco IOS Release 12.2SXI.

To change the mode of the Cisco 7600 SSC-400 card to allocate full buffers to the specified subslot, use the **hw-module slot subslot only** command in global configuration mode. If this command is not used, the total amount of buffers available is divided between the two subslots on the Cisco 7600 SSC-400.

Note This command automatically generates a reset on the Cisco 7600 SSC-400. See Usage Guidelines below for details.

hw-module slot *slot* **subslot** *subslot* **only**

Syntax Description

slot	Chassis slot number where the Cisco 7600 SSC-400 is located. Refer to the appropriate hardware manual for slot information. For SIPs and SSCs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
subslot	Secondary slot number on the SSC where the IPSec VPN SPA is installed.

Command Default

No default behavior or values.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(18)SXF2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2SXI	This command was deleted.

Usage Guidelines

Follow these guidelines and restrictions when configuring a Cisco 7600 SSC-400 and IPSec VPN SPAs using the **hw-module slot subslot only**command:

- This command is useful when supporting IP multicast over GRE on the IPSec VPN SPA.
- When this command is executed, it automatically takes a reset action on the Cisco 7600 SSC-400 and issues the following prompt to the console:

```
Module n will be reset? Confirm [n]:
```

The prompt will default to “N” (no). You must type “Y” (yes) to activate the reset action.

- When in this mode, if you manually plug in a second SPA, or if you attempt to reset the SPA (by entering a **no hw-module subslot shutdown** command, for example), a message is displayed on the router console which refers you to the customer documentation.

Examples

The following example allocates full buffers to the SPA that is installed in subslot 0 of the SIP located in slot 1 of the router and takes a reset action of the Cisco 7600 SSC-400.

```
Router(config)# hw-module slot 4 subslot 1 only
Module 4 will be reset? Confirm [no]: y
```

Note that the prompt will default to “N” (no). You must type “Y” (yes) to activate the reset action.

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing.
ip pim	Enables Protocol Independent Multicast (PIM) on an interface.