

ca trust-point through clear eou

- ca trust-point, on page 3
- cabundle url, on page 5
- cache authentication profile (server group configuration), on page 7
- cache authorization profile (server group configuration), on page 8
- cache clear age, on page 9
- cache disable, on page 10
- cache expiry (server group configuration), on page 11
- cache max, on page 12
- cache refresh, on page 13
- call admission limit, on page 14
- call guard-timer, on page 15
- category (ips), on page 16
- cdp-url, on page 17
- certificate, on page 21
- chain-validation (ca-trustpool), on page 23
- chain-validation, on page 25
- cifs-url-list, on page 27
- cipherkey, on page 29
- ciphervalue, on page 30
- cisco (ips-auto-update), on page 32
- cisp enable, on page 33
- citrix enabled, on page 34
- class type inspect, on page 35
- class type urlfilter, on page 38
- class-map type inspect, on page 40
- class-map type urlfilter, on page 44
- clear aaa cache filterserver acl, on page 47
- clear aaa cache filterserver group, on page 48
- clear aaa cache group, on page 49
- clear aaa counters servers, on page 50
- clear aaa local user fail-attempts, on page 51
- clear aaa local user lockout, on page 52
- clear access-list counters, on page 53

- clear access-template, on page 54
- clear appfw dns cache, on page 56
- clear ase signatures, on page 57
- clear authentication sessions, on page 59
- clear content-scan, on page 61
- clear crypto call admission statistics, on page 62
- clear crypto ctcp, on page 63
- clear crypto datapath, on page 64
- clear crypto engine accelerator counter, on page 65
- clear crypto gdoi, on page 68
- clear crypto gdoi ks cooperative role, on page 70
- clear crypto ikev2 cluster dead-slaves, on page 71
- clear crypto ikev2 cluster stats, on page 72
- clear crypto ikev2 sa, on page 73
- clear crypto ikev2 stats, on page 74
- clear crypto ipsec client ezvpn, on page 75
- clear crypto isakmp, on page 77
- clear crypto sa, on page 79
- clear crypto session, on page 82
- clear crypto pki benchmarks, on page 84
- clear crypto pki crls, on page 85
- clear cws, on page 86
- clear dmvpn session, on page 87
- clear dmvpn statistics, on page 89
- clear dot1x, on page 90
- clear eap, on page 91
- clear eou, on page 92

ca trust-point

To identify the trustpoints that is used to validate a certificate during Internet Key Exchange (IKE) authentication, use the **ca trust-point**command in ISAKMP profile configuration mode. To remove the trustpoint, use the **no** form of this command.

ca trust-point *trustpoint-name*
no ca trust-point *trustpoint-name*

Syntax Description

trustpoint-name	The trustpoint name as defined in the global configuration.

Command Default

If there is no trustpoint defined in the Internet Security Association and Key Management Protocol (ISAKMP) profile configuration, the default is to validate the certificate using all the trustpoints that are defined in the global configuration.

Command Modes

ISAKMP profile configuration (conf-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **ca trust-point** command can be used multiple times to define more than one trustpoint.

This command is useful when you want to restrict validation of certificates to a list of trustpoints. For example, the router global configuration has two trustpoints, A and B, which are trusted by VPN1 and VPN2, respectively. Each Virtual Private Network (VPN) wants to restrict validation only to its trustpoint.

Before you can use this command, you must enter the **crypto isakmp profile** command.



Note A router initiating IKE and a router responding to the IKE request should have symmetrical trustpoint configurations. For example, a responding router (in IKE Main Mode) performing RSA signature encryption and authentication might use trustpoints that were defined in the global configuration when sending the CERT-REQ payloads. However, the router might use a restricted list of trustpoints that were defined in the ISAKMP profile for the certificate verification. If the peer (the IKE initiator) is configured to use a certificate whose trustpoint is in the global list of the responding router but not in ISAKMP profile of the responding router, the certificate is rejected. (However, if the initiating router does not know about the trustpoints in the global configuration of the responding router, the certificate can still be authenticated.)

To validate a certificate chain sent by the initiator, it is recommended that you configure the required trustpoints of the certificate chain in the ISAKMP profile of the responder. For example, the following configuration on the responder will fail when the initiator sends a certificate chain for myroot trustpoint.

```
crypto pki trustpoint mysub
 chain-validation continue myroot
 revocation-check crl
 rsakeypair mysub
!
```

```
crypto pki trustpoint myroot
 enrollment terminal
 revocation-check crl

crypto isakmp identity dn
crypto isakmp profile mypeer
   ca trust-point mysub
   match certificate cisco
```

This is because the responder builds the CERT_REQ based on trustpoints in the reverse order in which they are defined globally. IKE responder sends the CERT_REQ for myroot to the initiator and IKE initiator sends myroot certificate chain to validate this certificate chain. This can be avoided by the following configuration on the responder ISAKMP profile.

```
crypto pki trustpoint mysub
chain-validation continue myroot
revocation-check crl
rsakeypair mysub
!
crypto pki trustpoint myroot
enrollment terminal
revocation-check crl
!
crypto isakmp identity dn
crypto isakmp profile mypeer
ca trust-point myroot
ca trust-point mysub
match certificate cisco
```

Examples

The following example specifies two trustpoints, A and B. The ISAKMP profile configuration restricts each VPN to one trustpoint.

```
crypto ca trustpoint A
enrollment url http://kahului:80
crypto ca trustpoint B
enrollment url http://arjun:80
!
crypto isakmp profile vpn1
 trustpoint A
!
crypto isakmp profile vpn2
 ca trust-point B
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile.

cabundle url

To configure the URL from which the public key infrastructure (PKI) trustpool certificate authority (CA) bundle is downloaded, use the **cabundle url** command in ca-trustpool configuration mode. To remove the URL, use the **no** form of this command.

cabundle url {*url* | **none**}
no cabundle url {*url* | **none**}

Syntax Description

url	The URL of the CA certificate bundle.
none	Specifies that autoupdates of the PKI trustpool CA are not permitted.

Command Default

The PKI trustpool CA bundle download URL is not configured.

Command Modes

Ca-trustpool configuration (ca-trustpool)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

Multiple bundle commands can be issued so that the bundle update process is not connected to a single application.

Examples

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# cabundle url http://www.cisco.com/security/pki/crl/crca2048.crl
```

Related Commands

Command	Description
chain-validation	Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool.
crl	Specifes the CRL query and cache options for the PKI trustpool.
crypto pki trustpool import	Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA certificate bundle.
crypto pki trustpool policy	Configures PKI trustpool policy parameters.

Command	Description
default	Resets the value of a ca-trustpool configuration command to its default.
match	Enables the use of certificate maps for the PKI trustpool.
ocsp	Specifies OCSP settings for the PKI trustpool.
revocation-check	Disables revocation checking when the PKI trustpool policy is being used.
show	Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.
show crypto pki trustpool	Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy.
source interface	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
storage	Specifies a file system location where PKI trustpool certificates are stored on the router.
vrf	Specifies the VRF instance to be used for CRL retrieval.

cache authentication profile (server group configuration)

To specify a cache authentication profile to use in a named RADIUS or TACACS+ server group, use the **cache authentication profile**command in server group configuration mode. To disable an authentication cache profile, use the **no** form of this command.

cache authentication profile *name*
no cache authentication profile *name*

Syntax Description

name	Name of an authentication cache profile.

Command Default

No authentication cache profile is enabled.

Command Modes

Server group configuration (config-sg-radius)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use this command to specify a cache authentication profile for a RADIUS or TACACS+ server group.

Configure the authentication profile prior to applying it to a RADIUS or TACACS+ server group to avoid an error message.

Examples

The following example caches authentication responses from a RADIUS server according to the rules configured in the authentication profile authen-profile:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa group server radius networkauthentications
Router(config-sg-radius)# cache authentication profile authen-profile
```

Related Commands

Command	Description
cache authorization profile	Specifies an authorization cache profile to use in a named RADIUS or TACACS+ server group.

cache authorization profile (server group configuration)

To specify a cache authorization profile to use in a named RADIUS or TACACS+ server group, use the **cache authorization profile**command in server group configuration mode. To disable an authorization cache profile, use the **no** form of this command.

cache authorization profile *name*
no cache authorization profile *name*

Syntax Description

name	Name of a cache authorization profile to apply to either a RADIUS or TACACS+ server group.

Command Default

No authorization cache profile is enabled.

Command Modes

Server group configuration (config-sg-radius)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use this command to specify an authorization profile for a RADIUS or TACACS+ server group.

Examples

The following example caches authorization responses from a RADIUS server according to the rules configured in the authorization profile author-profile:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa group server radius authorizations
Router(config-sg-radius)# cache authorization profile author-profile
The authorization profile author-profile must be configured prior to applying it to a RADIUS
 or TACACS+ server group or an error message is generated.
```

Related Commands

Command	Description
cache authentication profile	Specifies an authentication cache profile to use in a named RADIUS or TACACS+ server group.

cache clear age

To specify when, in minutes, cache entries expire and the cache is cleared, use the **cache clear age** command in AAA filter configuration mode. To return to the default value, use the **no** form of this command.

cache clear age *minutes*
no cache clear age

Syntax Description

minutes	Any value from 0 to 4294967295; the default value is 1440 minutes.

Command Default

1440 minutes (1 day)

Command Modes

AAA filter configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

After enabling the **aaa cache filter**command, which allows you to configure cache filter parameters, you can use the **cache clear age** command to specify when cache entries should expire. If this command is not specified, the default value (1440 minutes) will be enabled.

Examples

The following example shows how to configure the cache entries to expire every 60 minutes:

```
aaa cache filter
 cache clear age 60
```

Related Commands

Command	Description
aaa cache filter	Enables filter cache configuration.

cache disable

To disable the cache, use the **cache disable** command in AAA filter configuration mode. To return to the default, use the **no** form of this command.

cache disable
no cache disable

Syntax Description

This command has no arguments or keywords.

Command Default

Caching is enabled.

Command Modes

AAA filter configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

After enabling the **aaa cache filter**command, which allows you to configure cache filter parameters, you can use the **cache disable** command to disable filter caching. This command can be used to verify that the access control lists (ACLs) are being downloaded.

Examples

The following example shows how to disable filter caching:

```
aaa cache filter
 cache disable
```

Related Commands

Command	Description
aaa cache filter	Enables filter cache configuration.

cache expiry (server group configuration)

To configure how long cached database profile entries in RADIUS or TACACS+ server groups are stored before they expire, use the **cache expiry**command in server group configuration mode. To reset the expiration time to the default value, use the **no** form of this command.

cache expiry *hours* [**enforce** | **failover**]
no cache expiry

Syntax Description

hours	Length of time, in hours, for a cache database profile entry to expire. Range is from 0 to 2147483647. Default is 24 hours.
enforce	(Optional) Specifies to not use expired entries.
failover	(Optional) Specifies to use an expired entry if all other methods fail.

Command Default

Cache entries expire in 24 hours.

Command Modes

Server group configuration (config-sg-radius)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use this command to set the amount of time before a cache entry expires (becomes stale). A stale entry is still usable, but the entry will, by default, revise its record with more updated information.

Examples

The following example sets the expiry time for cache profile entries to 10 days such that the expired entries cannot be used:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa group server radius networkusers
Router(config-sg-radius)# cache expiry 240 enforce
```

Related Commands

Command	Description
cache authentication profile	Specifies an authentication cache profile to use in a named RADIUS or TACACS+ server group.
cache authorization profile	Specifies an authorization cache profile to use in a named RADIUS or TACACS+ server group.

cache max

To limit the absolute number of entries that a cache can maintain for a particular server, use the **cache max** command in AAA filter configuration mode. To return to the default value, use the **no** form of this command.

cache max *number*
no cache max

Syntax Description

number	Maximum number of entries the cache can maintain. Any value from 0 to 4294967295; the default value is 100 entries.

Command Default

100 entries

Command Modes

AAA filter configuration

Command History

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

Usage Guidelines

After enabling the **aaa cache filter**command, which allows you to configure cache filter parameters, you can use the **cache max** command to specify the maximum number of entries the cache can have at any given time. If this command is not specified, the default value (100 entries) will be enabled.

Examples

The following example shows how to configure the cache to maintain a maximum of 150 entries:

```
aaa cache filter
 password mycisco
 cache max 150
```

Related Commands

Command	Description
aaa cache filter	Enables filter cache configuration.

cache refresh

To refresh a cache entry after a new session begins, use the **cache refresh** command in AAA filter configuration mode. To disable this functionality, use the **no** form of this command.

cache refresh
no cache refresh

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

AAA filter configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **cache refresh** command is used in an attempt to keep cache entries from the filter server, that are being referred to by new sessions, within the cache. This command resets the idle timer for these entries when they are referenced by new calls.

Examples

The following example shows how to disable the **cache refresh** command:

```
aaa cache filter
 password mycisco
 no cache refresh
 cache max 100
```

Related Commands

Command	Description
aaa cache filter	Enables filter cache configuration.

call admission limit

To instruct Internet Key Exchange (IKE) to drop security association (SA) requests (that is, calls for Call Admission Control [CAC]) when a specified level of system resources is being consumed, use the **call admission limit** command in global configuration mode. To disable this feature, use the **no** form of this command.

call admission limit *charge*
no call admission limit *charge*

Syntax Description

charge	Level of the system resources that, when used, causes IKE to stop accepting new SA requests. Valid values are 1 to 100000.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

To prevent IKE processes from using excessive CPU resources, you can set a limit value depending on the network topology, the capabilities of the router, and the traffic patterns.

Examples

The following example causes IKE to drop calls when a given level of system resources are being used:

```
Router(config)# call admission limit 90000
```

Related Commands

Command	Description
call admission load	Configures a CAC metric for scaling WAN protocol session load.
crypto call admission limit	Specifies the maximum number of IKE SAs that the router can establish before IKE begins rejecting new SA requests.
show call admission statistics	Monitors the global CAC configuration parameters and the behavior of CAC.

call guard-timer

To set a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request, use the **call guard-timer** command in controller configuration mode. To remove the **call guard-timer** command from your configuration file, use the **no** form of this command.

call guard-timer *milliseconds* [**on-expiry** {**accept** | **reject**}]
no call guard-timer *milliseconds* [**on-expiry** {**accept** | **reject**}]

Syntax Description

milliseconds	Specifies the number of milliseconds to wait for a response from the RADIUS server.
on-expiry accept	(Optional) Accepts the call if a response is not received from the RADIUS server within the specified time.
on-expiry reject	(Optional) Rejects the call if a response is not received from the RADIUS server within the specified time.

Command Default

No default behavior or values.

Command Modes

Controller configuration

Command History

Release	Modification
12.1(3)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 Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows a guard timer that is set at 20000 milliseconds. A call will be accepted if the RADIUS server has not responded to a preauthentication request when the timer expires.

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
  call guard-timer 20000 on-expiry accept
aaa preauth
group radius
  dnis required
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication configuration mode.

category (ips)

To specify a signature category that is to be used for multiple signature actions or conditions, use the **category** command in IPS-category configuration mode.

category *category* [*sub-category*]

Syntax Description

category	Category name. For a list of supported top-level categories, use the router CLI help (**?**).
sub-category	(Optional) Category submode. Submode categories are dependent on the category type; that is, submode categories vary from category to category. For a list of supported submode categories, use the router CLI help (**?**).

Command Default

None

Command Modes

IPS-category configuration (config-ips-category)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Cisco IOS Intrusion Prevention System (IPS) 5.x uses signatures and signature categories. All signatures are pregrouped into categories; the categories are hierarchical. An individual signature can belong to more than one category. Top-level categories help to define general types of signatures. Subcategories exist beneath each top-level signature category.

Examples

The following example shows how to tune event-action parameters for the signature category "adware/spyware." All tuning information will be applied to all signatures that belong to the adware/spyware category.

```
Router(config)# ip ips signature-categor
y
Router(config-ips-category)# category attack adware/spyware
Router(config-ips-category-action)# event-action produce-alert
Router(config-ips-category-action)# event-action deny-packet-inline
Router(config-ips-category-action)# event-action reset-tcp-connection
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# ^Z
Do you want to accept these changes? [confirm]y
```

Related Commands

Command	Description
ip ips signature-category	Enters IPS category (config-ips-category) configuration mode, which allows you to tune Cisco IOS IPS signature parameters on the basis of a signature category.

cdp-url

To specify a certificate revocation list (CRL) distribution point (CDP) to be used in certificates that are issued by the certificate server, use the **cdp-url** command in certificate server configuration mode. To remove a CDP from your configuration, use the **no** form of this command.

cdp-url *url*
no cdp-url *url*

Syntax Description

url	HTTP URL where CRLs are published.

Command Default

When verifying a certificate that does not have a specified CDP, Cisco IOS public key infrastructure (PKI) clients use the Simple Certificate Enrollment Protocol (SCEP) to retrieve the CRL directly from their configured certificate server.

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.

CRLs can be distributed through SCEP, which is the default method, or a CDP, if configured and available. If you set up a CDP, use the **cdp-url**command to specify the CDP location. The CDP URL may be changed after the certificate server is running, but existing certificates are not reissued with the new CDP that is specified through the **cdp-url** command.

You may specify the CDP location by a simple HTTP URL string for example,

cdp-url http://server.company.com/ca1.crl

The certificate server supports only one CDP; thus, all certificates that are issued include the same CDP.

If you have PKI clients that are not running Cisco IOS software and that do not support a SCEP GetCRL request, you can specify a non-SCEP request for the retrieval of the CRL from the certificate server by specifying **cdp-url** command with the URL in the following format where *cs-addr* is the location of the certificate server:

cdp-url http://*cs-addr*/cgi-bin/pkiclient.exe?operation=GetCRL



Note If your Cisco IOS certificate authority (CA) is also configured as your HTTP CDP server, specify your CDP with the **cdp-url** http://*cs-addr*/cgi-bin/pkiclient.exe?operation=GetCRL command syntax.

It is the responsibility of the network administrator to ensure that the CRL is available from the location that is specified through the **cdp-url** command.

In order to force the parser to retain the embedded question mark within the specified location, enter Ctrl-v prior to the question mark. If this action is not taken, CRL retrieval through HTTP returns an error message.

Examples

The following example shows how to configure a CDP location where the PKI clients do not support SCEP GetCRL requests:

```
Router(config)# crypto pki server aaa
Router(cs-server)# database level minimum
Router(cs-server)# database url tftp://10.1.1.1/username1/
Router(cs-server)# issuer-name CN=aaa
Router(cs-server)# cdp-url http://server.company.com/certEnroll/aaa.crl
```

The following example shows how to configure a CDP location where the PKI clients support SCEP GetCRL requests:

```
Router(config)# crypto pki server aaa
Router(cs-server)# database level minimum
Router(cs-server)# database url tftp://10.1.1.1/username1 /
Router(cs-server)# issuer-name CN=aaa
Router(cs-server)# cdp-url http://aaa/cgi-bin/pkiclient.exe?operation=GetCRL
```

Verifying a CDP Configuration

The following example is sample output from the **show crypto ca certificates** command, which allows you to verify the specified CDP. In this example, the CDP is "http://msca-root.cisco.com/certEnroll/aaa.crl."

```
Router# show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 03
  Certificate Usage: General Purpose
  Issuer:
    CN = aaa
  Subject:
    Name: Router.cisco.com
    OID.1.2.840.113549.1.9.2 = Router.cisco.com
  CRL Distribution Point:
    http://msca-root.cisco.com/certEnroll/aaa.crl
  Validity Date:
    start date: 18:44:49 GMT Jun 6 2003
    end   date: 18:44:49 GMT Jun 5 2004
    renew date: 00:00:00 GMT Jan 1 1970
  Associated Trustpoints: bbb
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
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 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.

certificate

To manually add certificates, use the **certificate** command in certificate chain configuration mode. To delete your router's certificate or any registration authority certificates stored on your router, use the **no** form of this command.

certificate *certificate-serial-number*
no certificate *certificate-serial-number*

Syntax Description

certificate-serial-number	Serial number of the certificate to add or delete.

Command Default

No default behavior or values.

Command Modes

Certificate chain configuration

Command History

Release	Modification
11.3 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 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 could use this command to manually specify a certificate. However, this command is rarely used in this manner. Instead, this command is usually used only to add or delete certificates.

Examples

The following example deletes the router's certificate. In this example, the router had a general purpose RSA key pair with one corresponding certificate. The **show** command is used in this example to determine the serial number of the certificate to be deleted.

```
myrouter# show crypto ca certificates
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 0123456789ABCDEF0123456789ABCDEF
  Key Usage: General Purpose

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
myrouter# configure terminal
myrouter(config)# crypto ca certificate chain myca
myrouter(config-cert-chain)# no certificate 0123456789ABCDEF0123456789ABCDEF
% Are you sure you want to remove the certificate [yes/no]? yes
% Be sure to ask the CA administrator to revoke this certificate.
myrouter(config-cert-chain)# exit
```

Related Commands

Command	Description
crypto ca certificate chain	Enters the certificate chain configuration mode.

chain-validation (ca-trustpool)

To enable chain validation from the peer's certificate to the root certificate authority (CA) certificate in the public key infrastructure (PKI) trustpool, use the **chain-validation** command in ca-trustpool configuration mode. To revert to the command default, use the **no** form of this command.

chain-validation
no chain-validation

Syntax Description

This command has no arguments or keywords.

Command Default

Chain validation is disabled.

Command Modes

Ca-trustpool configuration (ca-trustpool)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

If the **chain-validation** command is not configured, then the validation stops at the peer certificate's issuer.

Examples

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# chain-validation
```

Related Commands

Command	Description
cabundle url	Configures the URL from which the PKI trustpool CA bundle is downloaded.
crl	Specifes the CRL query and cache options for the PKI trustpool.
crypto pki trustpool import	Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle.
crypto pki trustpool policy	Configures PKI trustpool policy parameters.
default	Resets the value of a ca-trustpool configuration command to its default.

Command	Description
match	Enables the use of certificate maps for the PKI trustpool.
ocsp	Specifies OCSP settings for the PKI trustpool.
revocation-check	Disables revocation checking when the PKI trustpool policy is being used.
show	Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.
show crypto pki trustpool	Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy.
source interface	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
storage	Specifies a file system location where PKI trustpool certificates are stored on the router.
vrf	Specifies the VRF instance to be used for CRL retrieval.

chain-validation

To configure the level to which a certificate chain is processed on all certificates, including subordinate certificate authority (CA) certificates, use the **chain-validation** command in ca-trustpoint configuration mode. To revert to the command default, use the **no** form of this command.

chain-validation [{**stop** | **continue**} [*parent-trustpoint*]]
no chain-validation [{**stop** | **continue**} [*parent-trustpoint*]]

Syntax Description

stop	(Optional) Specifies that the certificate is already trusted. This is the default setting.
continue	(Optional) Specifies that the subordinate CA certificate associated with the trustpoint must be validated.
parent-trustpoint	(Optional) The name of the CA parent trustpoint.

Command Default

Certificate chain path processing continues until the first trusted certificate, or trustpoint, is reached.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

Configuring the level to which a certificate chain is processed allows for the reauthentication of trusted certificates, the extension of a trusted certificate chain, or the completion of a certificate chain that contains a gap. Devices must be enrolled in your PKI hierarchy and the appropriate key pair associated with the certificate.

If there is more than one parent trustpoint configured, Cisco IOS will select a parent trustpoint based upon configured settings to validate the certificate chain. If you want a specific parent trustpoint to validate certificates, then that trustpoint must be configured with the *parent-trustpoint* argument specified. All certificates, peer and subordinate CA certificates, are validated in the same manner. All trustpoint settings--ACLs, AAA authorization lists, CDP or OCSP overrides--will apply, as will trustpoint policies for trusted and untrusted certificates.

A trustpoint associated with the root CA cannot be configured to be validated to the next level. If **chain-validation continue** is configured for the trustpoint associated with the root CA, an error message will be displayed and the chain validation will revert to the default **chain-validation stop**.

Examples

In the following configuration example, all of the certificates will be validated--the peer, SubCA11, SubCA1, and RootCA certificates.

```
crypto pki trustpoint RootCA
 enrollment terminal
```

```
 chain-validation stop
 revocation-check none
 rsakeypair RootCA
crypto pki trustpoint SubCA1
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsakeypair SubCA1
crypto pki trustpoint SubCA11
 enrollment terminal
 chain-validation continue SubCA1
 revocation-check none
 rsakeypair SubCA11
```

In the following configuration example, the following certificates will be validated--the peer and SubCA1 certificates.

```
crypto pki trustpoint RootCA
 enrollment terminal
 chain-validation stop
 revocation-check none
 rsakeypair RootCA
crypto pki trustpoint SubCA1
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsakeypair SubCA1
crypto pki trustpoint SubCA11
 enrollment terminal
 chain-validation continue SubCA1
 revocation-check none
 rsakeypair SubCA11
```

In the following configuration example, SubCA1 is not in the configured Cisco IOS hierarchy but is expected to have been supplied in the certificate chain presented by the peer.

If the peer sends SubCA1, SubCA11, and the peer certificates in the certificate chain, the following certificates will be validated--the peer, SubCA11, and SubCA1 certificates.

If the peer does not supply the SubCA1 certificate in the presented certificate chain, the chain validation will fail.

```
crypto pki trustpoint RootCA
 enrollment terminal
 chain-validation stop
 revocation-check none
 rsakeypair RootCA
crypto pki trustpoint SubCA11
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsakeypair SubCA11
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.
revocation-check	Checks the revocation status of a certificate.

cifs-url-list

To enter webvpn URL list configuration mode to configure a list of Common Internet File System (CIFS) server URLs to which a user has access on the portal page of a Secure Sockets Layer Virtual Private Network (SSL VPN) and to attach the URL list to a policy group, use the **cifs-url-list** command in webvpn context configuration and webvpn group policy configuration mode, respectively. To remove the CIFS server URL list from the SSL VPN context configuration and from the policy group, use the **no** form of this command.

cifs-url-list *name*
no cifs-url-list *name*

Syntax Description

name	Name of the URL list. The list name can up to 64 characters in length.

Command Default

Webvpn URL list configuration mode is not entered, and a list of URLs to which a user has access on the portal page of an SSL VPN website is not configured. If the command is not used to attach a CIFS server URL list to a policy group, then a URL list is not attached to a group policy.

Command Modes

Webvpn context configuration (config-webvpn-context)
Webvpn group policy configuration (config-webvpn-group)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Entering this command places the router in webvpn URL list configuration mode. In this mode, the list of CIFS server URLs is configured. A URL list can be configured under the SSL VPN context configuration and then separately for each individual policy group configuration. Individual CIFS server URL list configurations must have unique names.

Examples

The following example shows that CIFS URL lists have been added under the webvpn context and for a policy group:

```
webvpn context context1
 ssl authenticate verify all
 !
 acl "acl1"
   error-msg "warning!!!..."
   permit url "http://www.exampleurl1.com"
   deny url "http://www.exampleurl2.com"
   permit http any any
 !
 nbns-list l1
   nbns-server 10.1.1.20
 !
 cifs-url-list "c1"
   heading "cifs-url"
   url-text "SSLVPN-SERVER2" url-value "\\SSLVPN-SERVER2"
   url-text "SSL-SERVER2" url-value "\\SSL-SERVER2"
 !
 policy group default
```

```
  acl "acl1"
  cifs-url-list "c1"
  nbns-list "l1"
  functions file-access
  functions file-browse
  functions file-entry
default-group-policy default
gateway public
inservice
```

Related Commands

Command	Description
heading	Configures the heading that is displayed above URLs listed on the portal page of a SSL VPN website.
policy group	Attaches a URL list to policy group configuration.
url-text	Adds an entry to a URL list.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

cipherkey

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

To specify the symmetric keyname that is used to decrypt the filter, use the **cipherkey** command in FPM match encryption filter configuration mode.

cipherkey *keyname*

Syntax Description

keyname	String that is used to decrypt the filter. The value that can be used is realm-etcdf-01.sym.

Command Default

No symmetric keyname 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 **cipherkey** command to specify the the symmetric keyname that is used to decrypt the filter.

Examples

The following example shows how to configure the cipherkey for filter decryption:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# cipherkey realm-abc.sym
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.

ciphervalue

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

To specify the encrypted filter contents, use the **ciphervalue** command in FPM match encryption filter configuration mode.

ciphervalue *contents*

Syntax Description

contents	The encrypted filter contents in the format c encrypted-filter-contents c, where c is any delimiting character except + (plus sign), = (equals sign), and / (forward slash).

Command Default

No filter content 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 **ciphervalue** command to specify the encrypted filter contents. You can enter up to 200 characters at a time in a multiline input mode for the encrypted filter contents. The new line character (\n) and line feed character (\r) entered in the multiline input mode are ignored in the final cipher value contents.

Examples

The following example shows how to specify the encrypted filter contents:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# ciphervalue #2bcXhFL8Ld1v+DqU+dnxgmONCxl4JrYfcLl95xg
ET0b2B1z0sjoCkozE8YxiH/SXL+eG2wf3ogaA7/Fh
awIH7OF3tUcS5Jwim/u95Xlzh2RLNw819tuIBCdorV
Cu0ZzWCF3vqwpGQzaxtSE4sFgPAvSE2LxZc/VT22
F7EQKBhRo=#
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.

cisco (ips-auto-update)

To enable automatic Cisco IOS Intrusion Prevention System (IPS) signature updates from Cisco.com, use the **cisco** command in IPS-auto-update configuration mode. To disable automatic IPS signature updates from Cisco.com, use the **no** form of this command.

cisco
no cisco

Syntax Description

This command has no arguments or keywords.

Command Default

Automatic IPS signature updates from Cisco.com are not enabled.

Command Modes

IPS-auto-update configuration (config-ips-auto-update)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

The **cisco**command cannot be used in conjunction with the **url**command.

Examples

The following example shows how to configure automatic signature updates from Cisco.com that occur at the third hour of the 5 day of the month, at the 56th minute of this hour.



Note Adjustments are made for months without 31 days and daylight savings time.

```
Router(config)# ip ips auto-update
Router(config-ips-auto-update)# cisco
Router(config-ips-auto-update)# occur-at monthly 5 56 3
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.
occur-at	Defines a preset time for which the Cisco IOS Intrusion Prevention System (IPS) automatically obtains updated signature information.

cisp enable

To enable Client Information Signalling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch, use the **cisp enable** command in global configuration mode. To disable CISP, use the **no** form of this command.

cisp enable
no cisp enable

Syntax Description

This command has no arguments or keywords.

Command Default

CISP is disabled on the switch.

Command Modes

Global configuration.

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use CISP on a switch so that it acts as an authenticator to a supplicant switch. The link between the authenticator and supplicant switch is a trunk. When you enable VLAN Trunk Protocol (VTP) on both switches, the VTP domain name must be the same, and the VTP mode must be *server*.

When you configure VTP mode, to avoid the MD5 checksum mismatch error, verify that:

- VLANs are not configured on two different switches, which can be caused by two VTP servers in the same domain.
- Both switches have the different configuration revision numbers.

Examples

The following example shows how to enable CISP on a switch so that it acts as an authenticator to a supplicant switch:

```
Switch(config)# cisp enable
```

Related Commands

Command	Description
dot1x credentials	Configures a profile on a supplicant switch.

citrix enabled

To enable Citrix application support for end users in a policy group, use the **citrix enabled** command in webvpn group policy configuration mode. To remove Citrix support from the policy group configuration, use the **no** form of this command.

citrix enabled
no citrix enabled

Syntax Description

This command has no arguments or keywords.

Command Default

Citrix application support is not enabled.

Command Modes

Webvpn group policy configuration

Command History

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

Usage Guidelines

Citrix support allows a citrix client to use applications running on a remote server as if they were running locally. Entering the **citrix-enabled** command configures Citrix support for the policy group.

Examples

The following example configures Citrix support under the policy group:

```
Router(config)# webvpn context context1

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

Router(config-webvpn-group)# citrix enabled

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

Related Commands

Command	Description
filter citrix	Configures a Citrix application access filter.
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.

class type inspect

To specify the traffic (class) on which an action is to be performed, use the **class type inspect** command in policy-map configuration mode. To delete a class, use the **no** form of this command.

class type inspect *class-map-name*
no class type inspect *class-map-name*

Layer 7 (Application-Specific) Traffic Class Syntax
class type inspect *protocol-name class-map-name*
no class type inspect *protocol-name class-map-name*

Syntax Description

class-map-name	Name of the class on which an action is to be performed. • The *class-map-name* must match the appropriate class name specified with the **class-map type inspect** command.
protocol-name	Layer 7 application-specific traffic class. The supported protocols are as follows: • **aol** - America Online Instant Messenger (IM) • **edonkey** - eDonkey peer-to-peer (P2P) • **fasttrack** - FastTrack traffic P2P • **gnutella** - Gnutella Version 2 traffic P2P • **gtpv0** - General Packet Radio Service (GPRS) Tunnel Protocol Version 0 (GTPv0) • **gtpv1** - GTP Version 1 (GTPv1) • **h323** - H.323 protocol Version 4 • **http** - HTTP • **icq** - I Seek You (ICQ) IM protocol • **imap** - Internet Message Access Protocol (IMAP) • **kazaa2** - Kazaa Version 2 P2P protocol • **msnmsgr** - MSN Messenger IM protocol • **pop3** - Post Office Protocol Version 3 (POP3) • **sip** - Session Initiation Protocol (SIP) • **smtp** - Simple Mail Transfer Protocol (SMTP) • **sunrpc** - SUN Remote Procedure Call (SUNRPC) • **winmsgr** - Windows Messenger IM protocol • **ymsgr** - Yahoo IM

Command Default

None

Command Modes

Policy-map configuration (config-pmap)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	This command was modified. Support for the IM protocol and the following keywords was added: **aol**, **msnmsgr**, **ymsgr**. Support for the P2P protocol and the following keywords was added: **edonkey**, **fasttrack**, **gnutella**, **kazaa2**.
12.4(20)T	This command was modified. Support for the ICQ and Windows Messenger IM protocols and the following keywords was added: **icq**, **winmsgr**. Support for the H.323 protocol and the following keyword was added: **h323**. Support for SIP and the following keyword was added: **sip**.
Cisco IOS XE Release 3.4S	This command was modified. The following GTP keywords were added: **gtpv0**, **gtpv1**.

Usage Guidelines

Use the **class type inspect** command to specify the class and protocol (if applicable) on which an action is to be performed.

Thereafter, you can specify any of the following actions: drop, inspect, pass, reset, urlfilter, or attach a Layer 7 (application-specific) policy map to a “top-level” (Layer 3 or Layer 4) policy map (with the **service-policy (policy-map)** command).

Note A Layer 7 policy is considered to be a nested policy of the top-level policy, and it is called a child policy.

Note To attach a Layer 7 policy-map, it is mandatory to configure the **inspect** action under class type inspect .

The following protocols are supported for Cisco IOS XE Release 3.4S.

- GTPv0
- GTPv1
- HTTP
- IMAP
- Match-all Logical-AND all matching statements under this classmap
- Match-any Logical-OR all matching statements under this classmap
- POP3

- SMTP
- Sun RPC

Examples

The following example shows how to configure the “my-im-pmap” policy map with two IM classes (AOL and Yahoo Messenger) and only allow text-chat messages to pass through. When any packet with a service other than “text-chat” is seen, the connection will be reset.

```
class-map type inspect aol match-any my-aol-cmap
 match service text-chat
!
class-map type inspect ymsgr match-any my-ysmgr-cmap
 match service any
!
policy-map type inspect im my-im-pmap
 class type inspect aol my-aol-cmap
 allow
 log
!
 class type inspect ymsgr my-ysmgr-cmap
 rest
 log
!
class-map type inspect gtpv1
 match-any gtp_policy_gtpv1
 match message-id 18

policy-map type inspect gtpv1 gtp_policy_gtpv1
class type inspect gtpv1 gtp_policy_gtpv1
 log
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect-type class map.
policy-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect-type policy map.
service-policy (policy-map)	Attaches a Layer 7 policy map to a top-level Layer 3 or Layer 4 policy map.

class type urlfilter

To associate a URL filter class with a URL filtering policy map, use the **class type urlfilter** command in policy-map configuration mode. To disassociate the class, use the **no** form of this command.

class type urlfilter [**trend** | **n2h2** | **websense**] *class-map-name*
no class type urlfilter [**trend** | **n2h2** | **websense**] *class-map-name*

Syntax Description

trend	(Optional) Specifies that the class map applies to a Trend Micro filtering URL filtering policy. If a keyword is not specified, the class map applies to a local filtering policy.
n2h2	(Optional) Specifies that the class map applies to a SmartFilter URL filtering policy. If a keyword is not specified, the class map applies to a local filtering policy.
websense	(Optional) Specifies that the class map applies to a Websense URL filtering policy. If a keyword is not specified, the class map applies to a local filtering policy.
class-map-name	Name of the URL filter class map.

Command Default

No class is associated with a policy map.

Command Modes

Policy-map configuration (config-pmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **class type urlfilter** command to associate a class with a URL filtering policy map. You can associate one or more classes with the URL filtering policy map. You must create the class map for the class before you can associate the class with the policy map. In addition, you must use the **parameter type urlfpolicy** command to associate URL filtering parameters with the policy before you canassociate a class with the URL filtering policy map.

Examples

The following example shows how the **class type urlfilter**command is used to create the URL filtering policy map trend-policy and associate three classes with the policy map--trusted-domain-class, untrusted-domain-class, and drop-category.

```
policy-map type inspect urlfilter trend-policy
 parameter type urlfpolicy trend trend-param-map
 class type urlfilter trusted-domain-class
  log
  allow
 class type urlfilter untrusted-domain-class
  log
  reset
 class type urlfilter trend drop-category
```

```
log
reset
```

Related Commands

Command	Description
policy-map type inspect urlfilter	Creates or modifies a URL filter type inspect policy map.

class-map type inspect

To create a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map, use the **class-map type inspect** command in global configuration mode. To remove a class map from the router configuration file, use the **no** form of this command.

Layer 3 and Layer 4 (Top Level) Class Map Syntax
class-map type inspect {**match-any** | **match-all**} *class-map-name*
no class-map type inspect {**match-any** | **match-all**} *class-map-name*

Layer 7 (Application-Specific) Class Map Syntax
class-map type inspect *protocol-name* {**match-any** | **match-all**} *class-map-name*
no class-map type inspect *protocol-name* {**match-any** | **match-all**} *class-map-name*

Syntax Description

match-any	Determines how packets are evaluated when multiple match criteria exist. Packets must meet one of the match criteria to be considered a member of the class.
match-all	Determines how packets are evaluated when multiple match criteria exist. Packets must meet all of the match criteria to be considered a member of the class. **Note** The **match-all** keyword is available only with Layer 3, Layer 4, SMTP, and HTTP type class maps.
class-map-name	Name of the class map. The name can have a maximum of 40 alphanumeric characters. The class map name is used to configure the policy for the class in the policy map.

protocol-name	Layer 7 application-specific class map. The supported protocols are as follows: • **aol** - America Online Instant Messenger (IM) • **edonkey** - eDonkey peer-to-peer (P2P) • **fasttrack** - FastTrack traffic P2P • **gnutella** - Gnutella Version 2 traffic P2P • **gtpv0** - General Packet Radio Service (GPRS) Tunnel Protocol Version 0 (GTPv0) • **gtpv1**- GTP Version 1 (GTPv1) • **gtpv2**gtpv2 - GTP Version 2 (GTPv2) • **h323** - h323 Protocol, Version 4 • **http** - HTTP • **icq** - I Seek You (ICQ) IM • **imap** - Internet Message Access Protocol (IMAP) • **kazaa2** - Kazaa Version 2 P2P • **msnmsgr** - MSN Messenger IM protocol • **pop3** - Post Office Protocol, Version 3 (POP 3) • **sip** - Session Initiation Protocol (SIP) • **smtp** - Simple Mail Transfer Protocol (SMTP) • **sunrpc** - SUN Remote Procedure Call (SUNRPC) • **winmsgr** - Windows IM • **ymsgr** - Yahoo IM

Command Default

The behavior of the **match-any** keyword is the default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	This command was modified. The following P2P protocol keywords were added: **edonkey**, **fasttrack**, **gnutella**, **kazaa2**. The following IM protocol keywords were added: **aol**, **msnmsgr**, **ymsgr**.
12.4(15)XZ	This command was modified. Support for the Session Initiation Protocol (SIP) was added.

Release	Modification
12.4(20)T	This command was modified. The following IM protocol keywords were added: **icq, winmsgr**. The following VoIP protocol keyword was added: **h323 (Version 4)**.
15.1(2)T	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.2S	This command was modified. The following keywords were added: **smtp**, **imap**, **pop3**, and **sunrpc**.
Cisco IOS XE Release 3.4S	This command was modified. The following GTP keywords were added: **gtpv0**, **gtpv1**.
Cisco IOS XE Release 3.9S	This command was modified. The **gtpv2** keyword was added.

Usage Guidelines

Use the **class-map type inspect** command to specify the name and protocol (if applicable) of a Layer 3, Layer 4, or Layer 7 class map.

Layer 3 and Layer 4 (Top-Level) Class Maps

You can configure a top-level (Layer 3 or Layer 4) class map, which allows you to identify the traffic stream at a high level, by issuing the **match access-group** and **match protocol** commands. These class maps cannot be used to classify traffic at the application level (the Layer 7 level).

Layer 7 (Application-Specific) Class Maps

Application-specific class maps allow you to identify traffic based on the attributes of a given protocol. Match conditions in these class maps are specific to an application (for example, HTTP or SMTP). In addition to the type inspect, you must specify a protocol name (*protocol-name* argument) to create an application-specific class map.



Note Configuring the **match access-group** 101 filter enables Layer-4 inspection. As a result, Layer-7 inspection is skipped unless the class-map is of type **match-all**.

Examples

The following example shows how to configure class map c1 with the match criterion of ACL 101 based on the HTTP protocol:

```
class-map type inspect match-all c1
 match access-group 101
 match protocol http
```

The following example shows how to configure the class map winmsgr-textchat with the match criterion of text-chat based on the Windows IM protocol:

```
class-map type inspect match-any winmsgr winmsgr-textchat
 match service text-chat
```

The following example shows how to configure the class map gtpv2_l4c with the match criterion of Layer7 based on the GTPv1 protocol:

```
class-map type inspect match-all gtpv2_l4c
 match protocol gtpv1
```

Related Commands

Command	Description
match access-group	Configures the match criteria for a class map based on the specified ACL number or name.
match class-map	Uses a traffic class as a classification policy.
match protocol	Configures the match criteria for a class map based on the specified protocol.
match service	Configures the match criteria for a class map based on the specified IM protocol.

class-map type urlfilter

To create or modify a URL filter class map, use the **class-map type urlfilter** command in global configuration mode. To remove the class map, use the **no** form of this command.

Releases Prior to Cisco IOS 15.4(3)M

class-map type urlfilter [**trend** | **n2h2** | **websense**] [**match-any**] *class-map-name*
no class-map type urlfilter [**trend** | **n2h2** | **websense**] [**match-any**] *class-map-name*

Cisco IOS Release 15.4(3)M and Later Releases

class-map type urlfilter [**match-any**] *class-map-name*
no class-map type urlfilter [**match-any**] *class-map-name*

Syntax Description

trend	(Optional) Specifies that the class map applies to a Trend Micro URL filtering policy. If a keyword is not specified, the class map applies to a local URL filtering policy.
n2h2	(Optional) Specifies that the class map applies to a SmartFilter URL filtering policy. If a keyword is not specified, the class map applies to a local URL filtering policy.
websense	(Optional) Specifies that the class map applies to a Websense URL filtering policy. If a keyword is not specified, the class map applies to a local URL filtering policy.
match-any	(Optional) Specifies how URL requests are evaluated when multiple match criteria exist in a class map.
class-map-name	Name of the URL filter class map.

Command Default

No class maps are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
15.4(3)M	This command was modified. The following keywords are removed: **trend**, **n2h2**, **websense**.

Usage Guidelines

Use the **class-map type urlfilter** command to enter class-map configuration mode and create or modify a URL filter class map. The class map is used as a traffic filter to segregate HTTP traffic for which a URL filtering policy applies. If you specify multiple match criteria and want to segregate the traffic when there is at least one match, use the **match-any** keyword. If you do not specify a type of filtering policy with the **trend**, **n2h2**, or **websense** keyword, then the class map applies to a local URL filtering policy.

Local Class Maps

Use the **class-map type urlfilter match-any** *class-m ap-name* to create or modify a local class map. filtering mode. Typically, you create three local class maps: one to specify trusted domains, one to specify untrusted domains, and one to specify keywords to block.

To specify the match criteria for the trusted and untrusted domain classes, use the following command:

- **match server-domain urlf-glob** *parameter-map-name*

Before you use this command, you must configure the **urlf-glob** parameter with the **parameter-map type urlf-glob** command.

To specify the match criteria for the keyword class map use the following command:

- **match url-keyword urlf-glob** *parameter-map-name*

Before you use this command, you must configure the **urlf-glob** keyword with the **parameter-map type urlf-glob** command.

Trend Micro Class Maps

Use the **class-map type urlfilter trend match-any** *class-m ap-name* command to create or modify a URL class map for the Trend Router Provisioning Server (TRPS). Typically, you create two Trend Micro class maps: one to specify URL categories and one to specify URL reputations.

To specify the Trend Micro URL categories for which filtering takes place, use the following command:

- **match url category** *category-name*

To specify the Trend Micro URL reputations for which filtering takes place, use the following command:

- **match url reputation** *reputation-name*

SmartFilter Class Maps

Use the **class-map type urlfilter n2h2** *class-map-name* command to create or modify a URL filter class map for a SmartFilter filtering service. Use the following command to specify the match condition for the class map:

- **match server-response any**

Websense Class Maps

Use the **class-map type urlfilter websense** *class-map-name* command to create or modify a URL filter class map for a Websense filtering server. Use the following command to specify the match condition for the class map:

- **match server-response any**

Examples

The following example configures the parameters for local filtering, and then specifies three class maps for local URL filtering: trusted-domain-class, untrusted-domain-class, and keyword-class:

```
parameter-map type urlf-glob trusted-domains-param
 pattern www.example.com
 pattern *.example1.com
parameter-map type urlf-glob untrusted-domain-param
 pattern www.example2.com
 pattern www.example3.org
parameter-map type urlf-glob keyword-param
```

```
 pattern games
 pattern adult
class-map type urlfilter match-any trusted-domain-class
 match server-domain urlf-glob trusted-domain-param
class-map type urlfilter match-any untrusted-domain-class
 match server-domain urlf-glob untrusted-domain-param
class-map type urlfilter match-any keyword-class
 match url-keyword urlf-glob keyword-param
```

The following example configures two class maps for Trend Micro filtering: drop-category and drop-reputation:

```
class-map type urlfilter trend match-any drop-category
 match url category Gambling
 match url category Personals-Dating
class-map type urlfilter trend match-any drop-reputation
 match url reputation PHISHING
 match url reputation ADWARE
```

The following example specifies a class map for SmartFilter filtering called n2h2-class and configures the match criteria as any response from the SmartFilter server:

```
class-map type urlfilter n2h2 match-any n2h2-class
 match server-response any
```

Related Commands

Command	Description
match server-domain urlf-glob	Specifies the server domain match criteria for a URL filtering class map.
match server-response any	Specifies the match criterion for SmartFilter and Websense class maps.
match url category	Specifies the URL category match criteria for a URL filtering class map.
match url-keyword urlf-glob	Specifies the URL keyword match criteria for a URL filtering class map.
match url reputation	Specifies the URL reputation match criteria for a URL filtering class map.
parameter-map type urlf-glob	Specifies the filtering parameters for trusted domains, untrusted domains, and blocked keywords.

clear aaa cache filterserver acl

To clear the cache status for a particular filter or all filters, use the **clear aaa cache filterserver acl**command in EXEC mode.

clear aaa cache filterserver acl [*filter-name*]

Syntax Description

filter-name	(Optional) Cache status of a specified filter is cleared.

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
122(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

After you clear the cache status for a particular filter or all filters, it is recommended that you enable the **show aaa cache filterserver** command to verify that the cache status.

Examples

The following example shows how to clear the cache for all filters:

```
clear aaa cache filterserver acl
```

Related Commands

Command	Description
show aaa cache filterserver	Displays the cache status.

clear aaa cache filterserver group

To clear contents of the server group cache, use the **clear aaa cache filterserver group** command in privileged EXEC mode.

clear aaa cache filterserver group *name* {**all** | **profile** *name*}

Syntax Description

name	Name of the server group being cleared.
all	Clears all profiles.
profile *name*	Clears an individual profile.

Command Default

All profiles are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows how to clear all RADIUS server IDs:

```
Router# clear aaa cache filterserver group group1
```

Related Commands

Command	Description
aaa cache filterserver	Enables AAA filter server definitions.

clear aaa cache group

To clear an individual entry or all entries in the cache, use the **clear aaa cache group**command in privileged EXEC mode.

clear aaa cache group *name* {**profile** *name* | **all**}

Syntax Description

name	Text string representing the name of a cache server group.
profile *name*	Specifies the name of an individual profile entry to clear.
all	Specifies that all profiles in the named cache group are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use this command to clear cache entries.

Note To update an old record with profile cache settings and to remove an old record from the cache, clear the cache for the profile.

Examples

The following example clears all cache entries in the localusers group:

```
Router# clear aaa cache group localusers all
```

Related Commands

Command	Description
show aaa cache group	Displays all of the cache entries stored by the AAA cache.

clear aaa counters servers

To clear the authentication, authorization, and accounting (AAA) server information, use the **clear aaa counters servers**command in privileged EXEC mode.

clear aaa counters servers {**all** | **radius** {*server-id* | **all**} | **sg** *name*}

Syntax Description

all	Clears all AAA server information.
radius	Clears RADIUS server information.
server-id	Clears all server IDs displayed by **show aaa servers**command. The range is from 0 to 2147483647.
all	Clears all server IDs.
sg	Clear all servers in a server group.
name	Server group name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2 .1	This command was integrated into Cisco IOS XE Release 2.1.
15.2(4)S1	This command was modified. The **all** keyword was modified to clear all AAA counter server information except for the estimated outstanding and throttled (access and accounting) transactions.

Examples

The following example shows how to clear AAA counter server information:

```
Device# clear aaa counters servers all
```

Related Commands

Command	Description
aaa cache filterserver	Enables AAA filter server definitions.
show aaa servers	Displays the status and number of packets that are sent to and received from all public and private AAA RADIUS servers as interpreted by the AAA Server MIB.

clear aaa local user fail-attempts

To clear the unsuccessful login attempts of a user, use the **clear aaa local user fail-attempts**command in privileged EXEC mode.

clear aaa local user fail-attempts {**username** *username* | **all**}

Syntax Description

username *username*	Specifies the name of the user.
all	Clears unsuccessful login attempts for all users.

Command Default

Unsuccessful login attempts are not cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

This command is available only to users having the root privilege.

Examples

The following example shows that the unsuccessful login attempts for all users will be cleared:

```
Router#
clear aaa local user fail-attempts all
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Specifies the maximum number of unsuccessful authentication attempts before a user is locked out.
clear aaa local user lockout	Unlocks the locked-out users.
show aaa local user locked	Displays a list of all locked-out users.

clear aaa local user lockout

To unlock the locked-out users, use the **clear aaa local user lockout** command in privileged EXEC mode.

clear aaa local user lockout {**username** *username* | **all**}

Syntax Description

username *username*	Specifies the name of the user to be unlocked.
all	Specifies that all users are to be unlocked.

Command Default

Locked-out users remain locked out.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Only a user having the root privilege can use this command.

Examples

The following example shows that all locked-out users will be unlocked:

```
Router#
clear aaa local user lockout all
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Specifies the maximum number of unsuccessful authentication attempts before a user is locked out.
clear aaa local user fail-attempts	Clears the unsuccessful login attempts of a user.
show aaa local user loced	Displays a list of all locked-out users.

clear access-list counters

To clear the counters of an access list, use the **clear access-list counters**commandin privilegedEXEC mode.

clear access-list counters {*access-list-numberaccess-list-name*}

Syntax Description

access-list-number	Access list number of the access list for which to clear the counters.
access-list-name	Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	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.

Usage Guidelines

Some access lists keep counters that count the number of packets that pass each line of an access list. The **show access-lists** command displays the counters as a number of matches. Use the **clear access-list counters** command to restart the counters for a particular access list to 0.

Examples

The following example clears the counters for access list 101:

```
Router# clear access-list counters 101
```

Related Commands

Command	Description
show access-lists	Displays the contents of current IP and rate-limit access lists.

clear access-template

To manually clear a temporary access list entry from a dynamic access list, use the **clear access-template** command in privileged EXEC mode.

clear access-template {*access-list-numbername*} *template-name* {*source-address source-wildcard-bit* | **any** | **host** {*hostnamesource-address*}} {*destination-address dest-wildcard-bit* | **any** | **host** {*hostnamedestination-address*}} [**timeout** *minutes*]

Syntax Description

access-list-number	Number of the dynamic access list. The ranges are from 100 to 199 and from 2000 to 2699.
name	Name of an IP access list. • The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.
template-name	Name of a dynamic access list.
source-address	Source address in a dynamic access list. • All other attributes are inherited from the original access-list entry.
source-wildcard-bit	Source wildcard bits.
any	Specifies any source hostname.
host	Specifies a specific source host.
hostname	Name of the host.
destination-address	Destination address in a dynamic access list. • All other attributes are inherited from the original access-list entry.
dest-wildcard-bit	Destination wildcard bits.
timeout *minutes*	(Optional) Specifies a maximum time limit, in minutes, for each entry within this dynamic list. The range is from 1 to 9999. • This is an absolute time, from creation, that an entry can reside in the list. The default is an infinite time limit and allows an entry to remain permanently.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **any**, **host** *hostname*, and **timeout** *minutes* keywords and arguments were added.

Usage Guidelines

The **clear access-template** command is related to the lock-and-key access feature. It clears any temporary access list entries that match the parameters you define.

Examples

The following example shows how to clear any temporary access list entries with a source of 172.20.1.12 from the dynamic access list named vendor:

```
Router> enable
Router# clear access-template vendor 172.20.1.12 any host 172.20.1.13
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-template	Places a temporary access list entry on a router to which you are connected manually.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

clear appfw dns cache

To clear at least one IP address from the Domain Name System (DNS) cache, use the **clear appfw dns cache**command in privileged EXEC mode.

clear appfw dns cache name *dns-name* [**address** *address*]

Syntax Description

name *dns-name*	DNS name of the IM server as entered in the **server name** command in application firewall policy.
address *address*	(Optional) Deletes a specific IP address from the DNS server cache. If an IP address is not specified, all IP addresses for the *dns-name* are deleted from the DNS server cache.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Resolved IP addresses are never "timed out" and not automatically removed from the DNS cache. Thus, if you find an obsolete IP address in the instant messenger database (DNS cache), you can issue the **clear appfw dns cache** command to remove the IP address and prevent the address from being interpreted by the router as an IM server.

Only one IP address can be deleted at a time. If the deleted IP address appears in the subsequent DNS resolution, the IP address is added to the DNS cache again.

Examples

The following example shows how to clear the IP address "172.16.0.0" from the cache of the DNS server "logon.cat.aol.com":

```
Router# clear appfw dns cache name logon.cat.aol.com address 172.16.0.0
```

Related Commands

Command	Description
server	Configures a set of DNS servers for which the specified instant messenger application will be interacting.

clear ase signatures

Note Effective with Cisco IOS Release 12.4(24), the **clear ase signatures** command is not available in Cisco IOS software.

To remove all Automatic Extraction Signatures (ASEs), use the **clear ase signatures** command in privileged EXEC configuration mode.

clear ase signatures

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(24)	This command was removed.

Usage Guidelines

This command is used to remove all the generated signatures that are displayed in the **show ase signatures** command output.

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example output demonstrates the result of removing generated signatures:

```
Router# show ase signatures
Automatic Signature Extraction Detected Signatures
==================================================
Signature Hash: 0x1E4A2076AAEA19B1, Offset: 54, Dest Port: TCP 135,
Signature: 05 00 00 03 10 00 00 00 F0 00 10 00 01 00 00 00 B8 00 00 00 00 00 03 00 01 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
Signature Hash: 0x24EC60FB1CF9A800, Offset: 72, Dest Port: TCP 445,
Signature: 00 00 00 00 00 00 00 00 00 00 00 00 FF FE 00 00 00 00 00 62 00 02 50 43 20 4E
45 54 57 4F 52 4B 20 50 52 4F 47 52 41 4D
Signature Hash: 0x0B0275535FFF480C, Offset: 54, Dest Port: TCP 445,
Signature: 00 00 00 85 FF 53 4D 42 72 00 00 00 00 18 53 C8 00 00 00 00 00 00 00 00 00 00
00 00 00 00 FF FE 00 00 00 00 00 62 00 02
Router# clear ase signatures
Router# show ase signatures
Automatic Signature Extraction Detected Signatures
==================================================
```

The table below describes the significant fields shown in the display.

Table 1: clear ase signatures Field Descriptions

Field	Description
Signature Hash	Hash (total) value of the 40-byte pattern, used as a check number for error control
Offset	Offset within the packet where the pattern begins
Dest Port	Layer 4 destination port for packets that contain this pattern
Signature	40 bytes of packet data used to potentially identify a piece of malware

Related Commands

Command	Description
ase collector	Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector.
ase group	Identifies the TIDP group number for the ASE feature.
ase enable	Enables the ASE feature on a specified interface.
ase signature extraction	Enables the ASE feature globally on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.
show ase	Shows the ASE run-time status, which includes the TIDP group number.

clear authentication sessions

To clear information about current Auth Manager sessions and force 802.1X clients on all 802.1X-enabled interfaces to initialize or reauthenticate, use the **clear authentication sessions**command in privileged EXEC mode.



Note Effective with Cisco IOS Release 12.2(33)SXI, the **clear authentication session** command replaces the **dot1x intitialize** and **dot1x re-authenticate** commands.

clear authentication sessions [**handle** *handle-id*] [**interface** *type number*] [**mac** *mac-address*] [**method** *method-name*] [**session-id** *session-name*]

Syntax Description

handle *handle-id*	(Optional) Specifies the particular handle for which Auth Manager information is to be displayed.
interface *type number*	(Optional) Specifies a particular interface type and number for which Auth Manager information is to be displayed.
mac *mac-address*	(Optional) Specifies the particular MAC address for which you want to display information.
method *method-name*	(Optional) Specifies the particular authentication method for which Auth Manager information is to be displayed.
session-id *session-name*	(Optional) Clears a particular authentication session by reference to its session ID.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to use the **clear authentication sessions** command to clear information for all Auth Manager sessions:

```
Switch# clear authentication sessions
```

The following example shows how to use the **clear authentication sessions** command to clear information for the Auth Manager session on a particular interface:

```
Switch# clear authentication sessions interface GigabitEthernet/0/23
```

The following example shows how to use the **clear authentication sessions** command to clear information for the Auth Manager session on a particular MAC address:

```
Switch# clear authentication sessions mac 000e.84af.59bd
```

Related Commands

Command	Description
show authentication sessions	Displays information about current Auth Manager sessions.

clear content-scan



Note Effective with Cisco IOS Release 15.4(2)T, the **clear content-scan** command is replaced by the **clear cws** command. See the **clear cws** command for more information.

To clear the content scan configuration information, use the **clear content-scan** command in privileged EXEC mode.

clear content-scan {**session** {***** | *ip-address* [**failures**]} | **statistics** [**failures**]}

Syntax Description

session	Clears content scan session information.
*****	Clears all content scan sessions.
ip-address	IP address of the client.
failures	(Optional) Clears content scan failure statistics.
statistics	Clears content scan statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)T1	This command was introduced.
15.2(4)M	This command was modified. The *ip-address* argument and the **session**, *****, and **failures** keywords were added.
15.4(2)T	This command was replaced by the **clear cws** command.

Usage Guidelines

Cisco ScanSafe web security provides content scanning of HTTP and secure HTTP (HTTPS) traffic and malware protection service to web traffic. The content scanning process redirects client web traffic to the ScanSafe web servers. ScanSafe web servers scan the web traffic content and either allow or block traffic based on the compliance with configured policies and thus protect clients from malware. Content scanning is enabled on an Internet-facing WAN interface to protect web traffic that goes out. Use the **clear content-scan** command to clear content scan configuration information.

Examples

The following example shows how to clear the content scan statistics:

```
Device# clear content-scan statistics
```

Related Commands

Command	Description
content-scan out	Enables content scanning on an egress interface.

clear crypto call admission statistics

To clear the counters that track the number of accepted and rejected Internet Key Exchange (IKE) requests, use the **call admission limit** command in global configuration mode.

clear crypto call admission statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example sets to zero the number of accepted and rejected IKE requests:

```
Router(config)# clear crypto call admission statistics
```

Related Commands

Command	Description
show crypto call admission statistics	Monitors Crypto CAC statistics.

clear crypto ctcp

To clear all Cisco Tunnel Control Protocol (cTCP) sessions and all Internet Key Exchange (IKE) and IPsec security associations (SAs) that are created on those sessions, use the **clear crypto ctcp**command in privileged EXEC mode.

clear crypto ctcp [**peer** *ip-address*]
no clear crypto ctcp [**peer** *ip-address*]

Syntax Description

peer	(Optional) Clears a specific cTCP peer.
ip-address	(Optional) IP address of the peer to be cleared.

Command Default

cTCP sessions are not cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Examples

The following example shows that all cTCP sessions and all IKE and IPsec SAs that are created on those sessions are to be cleared:

```
Router# clear crypto ctcp
```

The following example shows that only cTCP sessions for peer 10.76.235.21 and all IKE and IPsec SAs that are created on those sessions are to be cleared.

```
Router# clear crypto ctcp peer 10.76.235.21
```

Related Commands

Command	Description
crypto ctcp	Configures cTCP encapsulation for Easy VPN.

clear crypto datapath

To clear the counters or error history buffers in an encrypted network, use the **clear crypto datapath**command in privileged EXEC mode.

clear crypto datapath {**ipv4** | **ipv6**} [**error** | **internal** | **punt** | **success**]

Syntax Description

ipv4	Clears all counters in a network using IPv4.
ipv6	Clears all counters in a network using IPv6.
error	(Optional) Clears the error history buffer.
internal	(Optional) Clears the internal event counter.
punt	(Optional) Clears the punt event counter.
success	(Optional) Clears the success event counter.

Command Default

All counters are cleared, unless a keyword is entered to specify one counter.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use the **clear crypto datapath command to clear the history buffers or counters associated with an encrypted data path. You must specify the IP version for the network. If you only use the IP version keyword, all counters will be cleared. To clear only a specific counter, enter the keyword for that counter.**

Examples

The following example shows how to clear **all the counters in a network using IP version 4**:

```
Router# clear crypto datapath ipv4
```

This example shows how to clear the success counter only:

```
Router# clear crypto datapath ipv4 success
```

Related Commands

Command	Description
show crypto datapath	Displays the counters associated with an encrypted data path.

clear crypto engine accelerator counter

To reset the statistical and error counters of the hardware accelerator of the router or the IPsec Virtual Private Network (VPN) Shared Port Adapter (SPA) to zero, use the **clear crypto engine accelerator counter** command in privileged EXEC mode.

clear crypto engine accelerator counter

IPsec VPN SPA
clear crypto engine accelerator statistic [**slot** *slot*/*subslot* | **all**] [**detail**]

Syntax Description

slot *slot* / *subslot*	(IPsec VPN SPA only--Optional) Chassis slot number and secondary slot number on the SPA Interface Processor (SIP) where the SPA is installed. Refer to the appropriate hardware manual for slot information. For SIPs, 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. Resets platform statistics for the corresponding IPsec VPN SPA to zero. This output will not include network interface controller statistics.
all	(IPsec VPN SPA only--Optional) Resets platform statistics for all IPsec VPN SPAs on the router to zero. This reset will not include network interface controller statistics.
detail	(IPsec VPN SPA only--Optional) Resets platform statistics for the IPsec VPN SPA and network interface controller statistics to zero.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(3)XL	This command was introduced for the Cisco uBR905 cable access router.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII and AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	The AIM-VPN/BPII was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA to support the IPsec VPN SPA on Cisco 7600 series routers and Catalyst 6500 series switches.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

No specific usage guidelines apply to the hardware accelerators.

IPsec VPN SPA

Enter the **slot** keyword to reset platform statistics for the corresponding IPsec VPN SPA to zero. This reset will not include network interface controller statistics.

Enter the **all** keyword to reset platform statistics for all IPsec VPN SPAs on the router to zero. This reset will not include network interface controller statistics.

Enter the **detail** keyword to reset both the platform statistics for the IPsec VPN SPA and network interface controller statistics to zero.

Examples

Hardware VPN Module

The following example shows the statistical and error counters of the hardware accelerator being cleared to zero:

```
Router# clear crypto engine accelerator counter
```

IPsec VPN SPA

The following example shows the platform statistics for the IPsec VPN SPA in slot 2, subslot 1 being cleared to zero:

```
Router# clear crypto engine accelerator counter slot 2/1
```

The following example shows the platform statistics for all IPsec VPN SPAs on the router being cleared to zero:

```
Router# clear crypto engine accelerator counter all
```

Related Commands

Command	Description
crypto ca	Defines the parameters for the certification authority used for a session.
crypto cisco	Defines the encryption algorithms and other parameters for a session.
crypto dynamic map	Creates a dynamic map crypto configuration for a session.
crypto engine accelerator	Enables the use of the onboard hardware accelerator for IPsec encryption.
crypto ipsec	Defines the IPSec security associations and transformation sets.
crypto isakmp	Enables and defines the IKE protocol and its parameters.
crypto key	Generates and exchanges keys for a cryptographic session.
crypto map	Creates and modifies a crypto map for a session.
debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.

Command	Description
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator ring	Displays the contents of command and transmits rings for the crypto engine.
show crypto engine accelerator sa database	Displays the active (in-use) entries in the crypto engine SA database.
show crypto engine accelerator statistic	Displays the current run-time statistics and error counters for the crypto engine.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

clear crypto gdoi

To clear the state of the current session of a Group Domain of Interpretation (GDOI) group member (GM) with the key server, use the **clear crypto gdoi** command in privileged EXEC mode.

clear crypto gdoi [**group** *group-name*] [**ks coop** {**counter** | **role**} | **ks members** [**counters** | **now**] | **replay counter**]

Syntax Description

group *group-name*	(Optional) Name of the group.
ks coop	(Optional) Specifies that data will be cleared for the cooperative key server (KS).
counter	(Optional) Clears the counters for the cooperative KS.
role	(Optional) Clears the role of the cooperative KS.
ks members	(Optional) Specifies that the data will be cleared for GMs on the current KS.
counters	(Optional) Clears the counters for all GMs on the current KS.
now	(Optional) Forces GMs to delete old TEKs and KEKs immediately and re-register.
replay counter	(Optional) Clears the anti-replay counters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	This command was modified. The **group** and **replay** keywords and the *group-name* argument were added.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.
15.1(3)T	This command was modified. The **ks members counters** keyword combination was added.
15.2(1)T	This command was modified. The **now** keyword was added.
Cisco IOS XE Release 3.8S	This command was modified. The **now** keyword was added.

Usage Guidelines

If this command is issued on the group member, the policy of the group member is deleted, and the group member re-registers with the key server.

If this command is issued on the key server, the state on the key server is deleted. If redundancy is configured and this command is issued on the key server, the key server goes back into election mode to elect a new primary key server.

Examples

If the following command is issued on the key server, the state on the key server is cleared. If the command is issued on a group member, the state is cleared for the entire group, and a re-registration to the key server is forced:

```
Device# clear crypto gdoi
```

If the following command is issued on the key server, the state of the group that is specified is cleared on the key server. If the command is issued on a group member, the state of the group that is specified is cleared on the group member, and re-registration to the key server is forced:

```
Device# clear crypto gdoi group group1
```

The following command clears the anti-replay counters for the GDOI groups:

```
Device# clear crypto gdoi replay counter
```

The following command clears the counters for the cooperative key server:

```
Device# clear crypto gdoi ks coop counter
```

The following command clears all counters for all GMs on the current key server:

```
Device# clear crypto gdoi ks members counters
```

The following command forces GMs to delete old TEKs and KEKs immediately and re-register:

```
Device# clear crypto gdoi ks members now
```

Related Commands

Command	Description
show crypto gdoi feature	Displays the version of the GET VPN software running on each KS and GM in the GET VPN network and displays whether each device is running a version that supports GM removal, rekey triggering with policy replacement, or the GDOI MIB.

clear crypto gdoi ks cooperative role

To reset the cooperative role of the key server and to initiate the election process on the key server, use the **clear crypto gdoi ks cooperative role** command in privileged EXEC mode.

clear crypto gdoi ks cooperative role

Syntax Description

This command has no arguments or keywords.

Command Default

Cooperative role is not reset.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

If the **clear crypto gdoi ks cooperative role** command is executed on a secondary key server, the election is triggered on that secondary key server although that server would most likely remain a secondary key server because there has been an elected primary key server. However, if the **clear crypto gdoi ks cooperative role** command is executed on the primary key server, the primary key server is reassigned to a secondary role, and as a result, a new election that involves all the key servers is triggered. If the previous primary server has the highest priority (of all the key servers), it again becomes the primary server. If the previous primary server does not have the highest priority, the server having the highest priority is elected as the new primary server.

Examples

The following example shows that the cooperative role of the key server has been reset and that the election process is to be initiated:

```
clear crypto gdoi ks cooperative role
```

Related Commands

Command	Description
clear crypto gdoi	Clears the state of the current session of a group member with the key server.

clear crypto ikev2 cluster dead-slaves

To clear dead secondary gateways from the Internet Key Exchange Version 2 (IKEv2) cluster, use the **clear crypto ikev2 cluster dead-slaves** command in privileged EXEC mode.

clear crypto ikev2 cluster dead-slaves

Note Keywords such as **master** and **slave** in the context of cluster roles will be replaced with **primary** and **secondary** to align with inclusive language best practices. Users are advised to update their configurations accordingly.

Syntax Description

This command has no keywords or arguments.

Command Default

Dead secondary gateways are not cleared by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOSE XE 17.14.1a	This command was introduced.

Examples

The following is a sample output from the **show crypto ikev2 cluster dead-slaves** command:

```
Device#clear crypto ikev2 cluster dead-secondary

Role           : CLB Primary
Status         : Up
CLB Secondary  : 1
Cluster IP     : 1:1:1::100
Hold time      : 15000 msec
Overload limit : 80%
Codes          : '*' Least loaded, '-' Overloaded

Load statistics:
  Gateway           Role   Last-seen  Prio   Load     IKE  FQDN
  ------------------------------------------------------------
  1:1:1::2           Dead  00:53.867   100   21.6%      0
```

clear crypto ikev2 cluster stats

To reset the statistics for Internet Key Exchange Version 2 (IKEv2) cluster load balancing, use the **clear crypto ikev2 cluster stats** command in privileged EXEC mode.

clear crypto ikev2 cluster stats

Syntax Description

This command has no keywords or arguments.

Command Default

The IKEv2 cluster load-balancing statistics are not reset.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOSE XE 17.14.1a	This command was introduced.

Usage Guidelines

Use this command to clear the statistics related to IKEv2 cluster load balancing. This can help you troubleshoot or maintain the cluster by resetting the counters to their initial state.

Examples

The following example shows how to clear IKEv2 cluster load-balancing statistics:

```
Device# clear crypto ikev2 cluster stats

  Gateway           Last-update   redirects
  ------------------------------------------------------------------------
  1:1:1::2           00:00.492       0
  ------------------------------------------------------------------------
Total IKE SAs : 0

Device#
```

Related Commands

Command	Description
clear crypto ikev2 stats	Clears IKEv2 security associations statistics.

clear crypto ikev2 sa

To clear the Internet Key Exchange Version 2 (IKEv2) security associations (SA), use the **clear crypto ikev2 sa** command in privileged EXEC mode.

clear crypto ikev2 sa [**local** {*ipv4-addressipv6-address*} | **remote** {*ipv4-addressipv6-address*} | **fvrf** *vrf-name* | **psh** *number* | **reconnect**]

Syntax Description

local {*ipv4-address* | *ipv6-address*}	(Optional) Clears the IKEv2 security associations matching the local address.
remote {*ipv4-address* | *ipv6-address*}	(Optional) Clears the IKEv2 security associations matching the remote address.
fvrf *vrf-name*	(Optional) Clears the IKEv2 security associations matching the specified front door virtual routing and forwarding (FVRF) instance.
psh *number*	(Optional) Clears the IKEv2 platform service handler matching the specified connection ID.
reconnect	(Optional) Clears the IKEv2 reconnect security associations.

Command Default

The security associations are not cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.4(1)T	This command was modified. The **reconnect** keyword was added.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use this command to clear an IKEv2 security association and the child security associations.

Examples

The following example shows how to clear the IKEv2 security associations:

```
Device# clear crypto ikev2 sa
```

clear crypto ikev2 stats

To clear Internet Key Exchange Version 2 (IKEv2) security associations (SAs) statistics, use the **clear crypto ikev2 stats** command in privileged EXEC mode.

clear crypto ikev2 stats [**exchange** [**detailed**] | **ext-service** | **priority-queue** | **timeout**]

Syntax Description

exchange	(Optional) Clears information about IKEv2 exchange and notification statistics.
detailed	(Optional) Provides detailed information about IKEv2 exchange and notification statistics.
ext-service	(Optional) Clears information about pass and fail counters for IKEv2 external services.
priority-queue	(Optional) Clears information about the priority queue.
timeout	(Optional) Clears information about IKEv2 internal timers.

Command Default

The IKEv2 SAs statistics are not cleared.

Command Modes

Privileged EXEC (#)

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.
15.3(2)T	This command was modified. The keywords **exchange**, **detailed**, **ext-service**, **priority-queue**, and **timeout** were added.

Usage Guidelines

Use this command to clear IKEv2 SA statistics.

Examples

The following example shows how to clear IKEv2 SA statistics:

```
Device# clear crypto ikev2 stats
Cleared crypto ikev2 statistics
```

Related Commands

Command	Description
show crypto ikev2 stats	Displays IKEv2 SA statistics.

clear crypto ipsec client ezvpn

To reset the Cisco Easy VPN remote state machine and bring down the Cisco Easy VPN remote connection on all interfaces or on a given interface (tunnel), use the **clear crypto ipsec client ezvpn** command in privileged EXEC mode. If a tunnel name is specified, only the specified tunnel is cleared.

clear crypto ipsec client ezvpn [*name*]

Syntax Description

name	(Optional) Identifies the IPSec virtual private network (VPN) tunnel to be disconnected or cleared with a unique, arbitrary name. If no name is specified, all existing tunnels are disconnected or cleared.

Command Default

If no tunnel name is specified, all active tunnels on the machine are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)YA	This command was introduced for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(8)YJ	This command was enhanced to specify an IPSec VPN tunnel to be cleared or disconnected for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
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 **clear crypto ipsec client ezvpn** command resets the Cisco Easy VPN remote state machine, bringing down the current Cisco Easy VPN remote connection and bringing it back up on the interface. If you specify a tunnel name, only that tunnel is cleared. If no tunnel name is specified, all active tunnels on the machine are cleared.

If the Cisco Easy VPN remote connection for a particular interface is configured for autoconnect, this command also initiates a new Cisco Easy VPN remote connection.

Examples

The following example shows the Cisco Easy VPN remote state machine being reset:

```
Router# clear crypto ipsec client ezvpn
```

Related Commands

Command	Description
crypto ipsec client ezvpn (global)	Creates a Cisco Easy VPN remote configuration.
crypto ipsec client ezvpn (interface)	Assigns a Cisco Easy VPN remote configuration to an interface.

clear crypto isakmp

To clear active Internet Key Exchange (IKE) connections, use the **clear crypto isakmp** command in privileged EXEC mode.

clear crypto isakmp [*connection-id*] [**active** | **standby**]

Syntax Description

connection-id	(Optional) ID of the connection that is to be cleared. If this argument is not used, all existing connections will be cleared.
active	(Optional) Clears only IKE security associations (SAs) in the active state. For each active SA that is cleared, the standby router will be notified to clear the corresponding standby SA.
standby	(Optional) Clears only IKE SAs in the standby (secondary) state. **Note** If the router is in standby mode, the router will immediately resynchronize the standby SAs; thus, it may appear as though the standby SAs were not cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(11)T	The **active** and **standby** keywords were added.
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.

Usage Guidelines



Caution If the *connection-id*argument is not used, all existing IKE connections will be cleared when this command is issued.

Examples

The following example clears an IKE connection between two peers connected by interfaces 172.21.114.123 and 172.21.114.67:

```
Router# show crypto isakmp sa
    dst            src          state        conn-id   slot
172.21.114.123 172.21.114.67  QM_IDLE           1       0
209.165.201.1  209.165.201.2  QM_IDLE           8       0
Router
#
```

```
clear crypto isakmp 1
Router# show crypto isakmp sa
    dst           src          state        conn-id   slot
209.165.201.1  209.165.201.2  QM_IDLE           8       0
Router#
```

Related Commands

Command	Description
show crypto isakmp sa	Displays current IKE SAs.

clear crypto sa

To delete IP Security (IPSec) security associations (SAs), use the **clear crypto sa** command in privileged EXEC mode.

clear crypto sa [**active** | **standby**]

Virtual Routing and Forwarding (VRF) Syntax
clear crypto sa peer [**vrf** *fvrf-name*] *address*
clear crypto sa [**vrf ivrf-name**]

Crypto Map Syntax
clear crypto sa map *map-name*

IP Address, Security Protocol Standard, and SPI Syntax
clear crypto sa entry *destination-address protocol spi*

Traffic Counters Syntax
clear crypto sa counters

Syntax Description

active	(Optional) Clears only IPSec SAs that are in the active state.
standby	(Optional) Clears only IPSec SAs that are in the standby state. **Note** If the router is in standby mode, the router will immediately resynchronize the standby SAs; thus, it may appear as though the standby SAs were not cleared.
peer vrf fvrf-name] address	Deletes any IPSec SAs for the specified peer. The *fvrf-name* argument specifies the front door VRF (FVRF) of the peer address.
vrf *ivrf-name*	(Optional) Clears all IPSec SAs whose inside virtual routing and forwarding (IVRF) is the same as the *ivrf-name*.
map	Deletes any IPSec SAs for the named crypto map set.
map-name	Specifies the name of a crypto map set.
entry	Deletes the IPSec SA with the specified address, protocol, and security parameter index (SPI).
destination-address	Specifies the IP address of the remote peer.
protocol	Specifies either the Encapsulation Security Protocol (ESP) or Authentication Header (AH).
spi	Specifies an SPI (found by displaying the SA database).
counters	Clears the traffic counters maintained for each SA; the **counters** keyword does not clear the SAs themselves.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(15)T	The **vrf**keywordand *fvrf-name*argument for **clear crypto sa peer** were added. The **vrf** keyword and *ivrf-name*argument for **clear crypto sa** were added.
12.3(11)T	The **active** and **standby** keywords were added.
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.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

This command clears (deletes) IPSec SAs.

If the SAs were established via Internet Key Exchange (IKE), they are deleted and future IPSec traffic will require new SAs to be negotiated. (When IKE is used, the IPSec SAs are established only when needed.)

If the SAs are manually established, the SAs are deleted and reinstalled. (When IKE is not used, the IPSec SAs are created as soon as the configuration is completed.)



Note If the **peer**, **map**, **entry**, **counters, active**, or **standby**keywords are not used, all IPSec SAs will be deleted.

- The **peer** keyword deletes any IPSec SAs for the specified peer.
- The **map** keyword deletes any IPSec SAs for the named crypto map set.
- The **entry** keyword deletes the IPSec SA with the specified address, protocol, and SPI.
- The **active** and **standby** keywords delete the IPSec SAs in the active or standby state, respectively.

If any of the above commands cause a particular SA to be deleted, all the "sibling" SAs--that were established during the same IKE negotiation--are deleted as well.

The **counters** keyword simply clears the traffic counters maintained for each SA; it does not clear the SAs themselves.

If you make configuration changes that affect SAs, these changes will not apply to existing SAs but to negotiations for subsequent SAs. You can use the **clear crypto sa** command to restart all SAs so that they will use the most current configuration settings. In the case of manually established SAs, if you make changes that affect SAs you must use the **clear crypto sa** command before the changes take effect.

If the router is processing active IPSec traffic, it is suggested that you clear only the portion of the SA database that is affected by the changes, to avoid causing active IPSec traffic to temporarily fail.

Note that this command clears only IPSec SAs; to clear IKE state, use the **clear crypto isakmp** command.

Examples

The following example clears (and reinitializes if appropriate) all IPSec SAs at the router:

```
clear crypto sa
```

The following example clears (and reinitializes if appropriate) the inbound and outbound IPSec SAs established, along with the SA established for address 10.0.0.1 using the AH protocol with the SPI of 256:

```
clear crypto sa entry 10.0.0.1 AH 256
```

The following example clears all the SAs for VRF VPN1:

```
clear crypto sa vrf vpn1
```

Related Commands

Command	Description
clear crypto isakmp	Clears active IKE connections.

clear crypto session

To delete crypto sessions (IP security [IPsec] and Internet Key Exchange [IKE] security associations [SAs]), use the **clear crypto session** command in privileged EXEC mode.

clear crypto session [**local** {*ipv4-addressipv6-address*} [**port** *local-port*]] [**remote** {*ipv4-addressipv6-address*} [**port** *remote-port*]]
[**fvrf** *vrf-name*] [**ivrf** *vrf-name*]
isakmp group *group-name*
username *user-name*

IPsec and IKE Stateful Failover Syntax
clear crypto session [**active** | **standby**]

Syntax Description

local {*ipv4-address*| *ipv6-address*	(Optional) Clears crypto sessions for a local crypto endpoint. • TheIP address is the IP address of the local crypto endpoint.
port *local-port*	(Optional) IKE port of the local endpoint. The *local-port* value can be 1 through 65535. The default value is 500.
remote {*ipv4-address*| *ipv6-address*	(Optional) Clears crypto sessions for a remote IKE peer. • The IP address is the IP address of the remote IKE peer.
port *remote-port*	(Optional) IKE port of the remote endpoint to be deleted. The *remote-port* value can be from 1 through 65535. The default value is 500.
fvrf *vrf-name*	(Optional) Specifies the front door virtual routing and forwarding (FVRF) session that is to be cleared.
ivrf *vrf-name*	(Optional) Specifies the inside VRF (IVRF) session that is to be cleared.
isakmp group **group-** *name*	(Optional) Clears the specified crypto session using the isakmp group.
username user- *name*	(Optional) Clears the crypto session for the specified xauth or pki-aaa username.
active	(Optional) Clears only IPsec and IKE SAs in the active state.
standby	(Optional) Clears only IPsec and IKE SAs in the standby state. **Note** If the router is in standby mode, the router will immediately resynchronize the standby SAs with the active router.

Command Default

All existing sessions will be deleted. The IPsec SAs will be deleted first. Then the IKE SAs are deleted.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.3(11)T	The **active** and **standby** keywords were added.
12.4(11)T	The isakmp group **group-** *name* and **username user-** *name* keywords and associated arguments were added.

Usage Guidelines

To clear a specific crypto session or a subset of all the sessions, you need to provide session-specific parameters, such as a local or remote IP address, a local or remote port, an FVRF name, or an IVRF name.

If a local IP address is provided as a parameter when you use the **clear crypto session** command, all the sessions (and their IKE SAs and IPsec SAs) that share the IP address as a local crypto endpoint (IKE local address) will be deleted.

Examples

The following example shows that all crypto sessions will be deleted:

```
Router# clear crypto session
```

The following example shows that the crypto session of the FVRF named “blue” will be deleted:

```
Router# clear crypto session fvrf blue
```

The following example shows that the crypto sessions of the FVRF “blue” and the IVRF session “green” will be deleted:

```
Router# clear crypto session fvrf blue ivrf green
```

The following example shows that the crypto sessions of the local endpoint 10.1.1.1 and remote endpoint 10.2.2.2 will be deleted. The local endpoint port is 5, and the remote endpoint port is 10.

```
Router# clear crypto session local 10.1.1.1 port 5 remote 10.2.2.2 port 10
```

Related Commands

Command	Description
show crypto isakmp peer	Displays peer descriptions.
show crypto session	Displays status information for active crypto sessions in a router.

clear crypto pki benchmarks

To clear Public Key Infrastructure (PKI) benchmarking data and release all memory associated with this data, use the **clear crypto pki benchmarks**command in privileged EXEC mode.

clear crypto pki benchmarks

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **clear crypto pki benchmarks**command to clear all PKI benchmarking data and release all memory associated with this data. PKI benchmarking data is used for IOS PKI performance monitoring and optimization. PKI performance monitoring and optimization is turned on or off by using the **crypto pki benchmark** command.

Examples

The following example shows how to clear PKI benchmarking data:

```
Router# clear crypto pki benchmarks
```

Related Commands

Command	Description
crypto pki benchmark	Starts or stops benchmarking data for PKI performance monitoring and optimization.
show crypto pki benchmarks	Displays benchmarking data for PKI performance monitoring and optimization that was collected.

clear crypto pki crls

To remove the certificate revocation list (CRL) database that determines the validity status of digital certificates presented by encryption peers in a PKI, use the **clear crypto pki crls**command in privileged EXEC mode.

clear crypto pki crls

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

The the **clear crypto pki crls**command removes the CRL database that was configured with the **crypto pki certificate chain** command, which is used to configure a certificate authority (CA).

Related Commands

Command	Description
crypto pki certificate chain	Enters certificate chain configuration mode for a specified CA.

clear cws

To clear the Cloud Web Security configuration information, use the **clear cws** command in privileged EXEC mode.

clear cws {**session** {***** | *ip-address* [**failures**]} | **statistics** [**failures**]}

Syntax Description

session	Clears Cloud Web Security session information.
*****	Clears all Cloud Web Security sessions.
ip-address	IP address of the client.
failures	(Optional) Clears Cloud Web Security failure statistics.
statistics	Clears Cloud Web Security statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.4(2)T	This command was introduced. This command replaces the **clear content-scan** command.

Usage Guidelines

Cisco Cloud Web Security provides content scanning of HTTP and secure HTTP (HTTPS) traffic and malware protection service to web traffic. The content scanning process redirects client web traffic to the Cloud Web Security web servers. Cloud Web Security web servers scan the web traffic content and either allow or block traffic based on the compliance with configured policies and thus protect clients from malware. Content scanning is enabled on an Internet-facing WAN interface to protect web traffic that goes out. Use the **clear cws** command to clear Cloud Web Security configuration information.

Examples

The following example shows how to clear the Cloud Web Security statistics:

```
Device# clear cws statistics
```

Related Commands

Command	Description
cws out	Enables Cloud Web Security content-scanning on an egress interface.

clear dmvpn session

To clear Dynamic Multipoint VPN (DMVPN) sessions, use the **clear dmvpn session** command in privileged EXEC mode.

clear dmvpn session [**interface tunnel** *number* | **peer** {*ipv4-addressFQDN-stringipv6-address*} | **vrf** *vrf-name*] [**static**]

Syntax Description

interface	(Optional) Displays DMVPN information based on a specific interface.
tunnel *number*	(Optional) Specifies the tunnel address for the DMVPN peer. The range is from 0 to 2147483647.
peer	(Optional) Specifies a DMVPN peer.
ipv4-address	(Optional) The IPv4 address for the DMVPN peer.
FQDN-string	(Optional) Next hop server (NHS) fully qualified domain name (FQDN) string.
ipv6-address	(Optional) The IPv6 address for the DMVPN peer.
vrf *vrf-name*	(Optional) Clears all Next Hop Resolution Protocol (NHRP) sessions related to the specified virtual routing and forwarding (VRF) configuration.
static	(Optional) Clears all static and dynamic NHRP entries. • You must use the **static**keyword for all NHS FQDN configurations. **Note** If the **static** keyword is not specified, only dynamic NHRP entries are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(20)T	This command was modified. The *ipv6-address* argument was added.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
15.1(2)T	This command was modified. The *FQDN-string* argument was added.
15.2(1)T	This command was modified. The *ipv6-address* argument was added for the **peer** keyword.

Usage Guidelines

This command clears existing DMVPN sessions based on input parameters.

Examples

The following example shows how to clear all DMVPN sessions, both static and dynamic, for the specified peer nonbroadcast multiple access (NBMA) address:

```
Router# clear dmvpn session peer nbma static
```

The following example shows how to clear all DMVPN sessions, both static and dynamic, for the specified peer FQDN string:

```
Router# clear dmvpn session peer examplehub.example1.com static
```

Related Commands

Command	Description
clear ip nhrp	Clears all dynamic entries from the IPv4 NHRP cache.
clear ipv6 nhrp	Clears all dynamic entries from the IPv6 NHRP cache.

clear dmvpn statistics

To clear Dynamic Multipoint VPN (DMVPN)-related counters, use the **clear dmvpn statistics**command in privileged EXEC mode.

clear dmvpn statistics [**peer** {**nbma** | **tunnel**} *ip-address*] [**interface tunnel** *number*] [**vrf** *vrf-name*]

Syntax Description

peer	(Optional) Specifies a DMVPN peer.
nbma	(Optional) Specifies nonbroadcast mapping access (NBMA).
tunnel	(Optional) Specifies a tunnel.
ip-address	(Optional) Specifies the IP address for the DMVPN peer.
interface	(Optional) Displays DMVPN information based on a specific interface.
tunnel *number*	(Optional) Specifies the tunnel address for the DMVPN peer.
vrf *vrf-name*	(Optional) Clears all DMVPN counters related to the specified virtual routing forwarding (VRF) configuration.

Command Default

DMVPN-related counters will not be cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Based on input parameters, DMVPN-related session counters will be cleared.

Examples

The following example shows how to clear DMVPN related session counters for the specified tunnel interface:

```
Router# clear dmvpn statistics peer tunnel 192.0.2.3
```

Related Commands

Command	Description
clear dmvpn session	Clears DMVPN sessions.

clear dot1x

To clear 802.1X interface information, use the **clear dot1x** command in privileged EXEC mode.

clear dot1x {**all** | **interface interface-name**}

Syntax Description

all	Clears 802.1X information for all interfaces.
interface interface-name	Clears 802.1X information for the specified interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)SEE	This command was integrated into Cisco IOS Release 12.2(25)SEE.
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.

Examples

The following configuration shows that 802.1X information will be cleared for all interfaces:

```
Router# clear dot1x all
```

The following configuration shows that 802.1X information will be cleared for the Ethernet 0 interface:

```
Router# clear dot1x interface ethernet 0
```

You can verify that the information was deleted by entering the **show dot1x** command.

Related Commands

Command	Description
debug dot1x	Displays 802.1X debugging information.
identity profile default	Creates an identity profile and enters identity profile configuration mode.
show dot1x	Displays details for an identity profile.

clear eap

To clear Extensible Authentication Protocol (EAP) information on a switch or for a specified port, use the **clear eap** command in privileged EXEC mode.

clear eap [**sessions** [**credentials** *credentials-name* | **interface** *interface-name* | **method** *method-name* | **transport** *transport-name*]]

Syntax Description

sessions	(Optional) Clears EAP sessions on a switch or a specified port.
credentials *credentials-name*	(Optional) Clears EAP credential information for only the specified profile.
interface *interface-name*	(Optional) Clears EAP credential information for only the specified interface.
method *method-name*	(Optional) Clears EAP credential information for only the specified method.
transport *transport-name*	(Optional) Clears EAP credential information for only the specified lower layer.

Command Default

All active EAP sessions are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEE	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines

You can clear all counters by using the **clear eap** command with the **sessions** keyword, or you can clear only the specified information by using the **credentials**, **interface**, **method**, or **transport** keywords.

Examples

The following example shows how to clear all EAP information:

```
Router# clear eap sessions
```

The following example shows how to clear EAP session information for the specified profile:

```
Router# clear eap sessions credentials type1
```

Related Commands

Command	Description
show eap registrations	Displays EAP registration information.
show eap sessions	Displays active EAP session information.

clear eou

To clear all client device entries that are associated with a particular interface or that are on the network access device (NAD), use the **clear eou** command in privileged EXEC mode.

clear eou {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface** *interface-type* | **ip** *ip-address* | **mac** *mac-address* | **posturetoken** *name*}

Syntax Description

all	Clears all client device entries.
authentication	Authentication type.
clientless	Authentication type is clientless.
eap	Authentication type is Extensible Authentication Procotol (EAP).
static	Authentication type is static.
interface	Provides information about the interface.
interface-type	Type of interface (see the table below for a list of interface types).
ip	Specifies an IP address.
ip-address	IP address of the client device.
mac	Specifies a MAC address.
mac-address	The 48-bit address of the client device.
posturetoken	Posture token name.
name	Name of the posture token.

Command Modes

Privileged EXEC#

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The table below lists the interface types that may be used for the *interface-type* **argument**.

Table 2: Description of Interface Types

Interface Type	Description
Async	Asynchronous interface

Interface Type	Description
BVI	Bridge-Group Virtual Interface
CDMA-Ix	Code division multiple access Internet exchange (CDMA Ix) interface
CTunnel	Connectionless Network Protocol (CLNS) tunnel (Ctunnel) interface
Dialer	Dialer interface
Ethernet	IEEE 802.3 standard interface
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle interface
Multilink	Multilink-group interface
Null	Null interface
Serial	Serial interface
Tunnel	Tunnel interface
Vif	Pragmatic General Multicast (PGM) Multicase Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual template interface
Virtual-TokenRing	Virtual TokenRing interface

Examples

The following example shows that all client device entries are to be cleared:

```
Router# clear eou all
```

Related Commands

Command	Description
eou	Displays information about EAPoUDP.