

# clear ip access-list counters

To clear IP access list counters, use the **clear ip access-list counters** command in privileged EXEC mode.

**clear ip access-list counters** [*access-list-number* | *access-list-name*]

## Syntax Description

<i>access-list-number</i>   <i>access-list-name</i>	(Optional) Number or name of the IP access list for which to clear the counters. If no name or number is specified, all IP access list counters are cleared.
--	--

## Command Modes

Privileged EXEC

## Command History

Release	Modification
11.0	This command was introduced.

## Usage Guidelines

The counter counts the number of packets that match each **permit** or **deny** statement in an access list. You might clear the counters if you want to start at zero to get a more recent count of the packets that are matching an access list. The **show ip access-lists** command displays the counters as a number of matches.

## Examples

The following example clears the counter for access list 150:

```
Router# clear ip access-list counters 150
```

## Related Commands

Command	Description
<b>show ip access list</b>	Displays the contents of IP access lists.

# clear ip access-template

To clear statistical information on the access list, use the **clear ip access-template** command in privileged EXEC mode.

**clear ip access-template** *access-list*

<b>Syntax Description</b>	<i>access-list</i> Access list number; valid values are from 100 to 199 for an IP extended-access list and from 2000 to 2699 for an expanded-range IP extended-access list.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
	12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

**Examples** This example shows how to clear statistical information on the access list:

```
Router# clear ip access-template 201
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show mls netflow</b>	Displays configuration information about the NetFlow hardware.

# clear ip admission cache

To clear IP admission cache entries from the router, use the **clear ip admission cache** command in privileged EXEC mode.

```
clear ip admission cache {* | host ip address}
```

Syntax Description		
*		Clears all IP admission cache entries and associated dynamic access lists.
host ip address		Clears all IP admission cache entries and associated dynamic access lists for the specified host.

**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** Use this command to clear entries from the admission control cache before they time out.

**Examples** The following example shows that all admission entries are to be deleted:

```
Router# clear ip admission cache *
```

The following example shows that the authentication proxy entry for the host with the IP address 192.168.4.5 is to be deleted:

```
Router# clear ip admission cache 192.168.4.5
```

Related Commands	Command	Description
	show ip admission cache	Displays the admission control entries or the running admission control configuration.

# clear ip audit configuration

To disable Cisco IOS Firewall IDS, remove all intrusion detection configuration entries, and release dynamic resources, use the **clear ip audit configuration** command in EXEC mode.

## clear ip audit configuration

### Syntax Description

This command has no arguments or keywords.

### Command Modes

EXEC

### Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in 12.2S-family releases.
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

Use the **clear ip audit configuration** EXEC command to disable Cisco IOS Firewall IDS, remove all intrusion detection configuration entries, and release dynamic resources.

### Examples

The following example clears the existing IP audit configuration:

```
clear ip audit configuration
```

# clear ip audit statistics

To reset statistics on packets analyzed and alarms sent, use the **clear ip audit statistics** command in EXEC mode.

**clear ip audit statistics**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
	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** Use the **clear ip audit statistics** EXEC command to reset statistics on packets analyzed and alarms sent.

**Examples** The following example clears all IP audit statistics:

```
clear ip audit statistics
```

# clear ip auth-proxy cache

To clear authentication proxy entries from the router, use the **clear ip auth-proxy cache** command in EXEC mode.

```
clear ip auth-proxy cache { * | host-ip-address }
```

## Syntax Description

<b>*</b>	Clears all authentication proxy entries, including user profiles and dynamic access lists.
<i>host-ip-address</i>	Clears the authentication proxy entry, including user profiles and dynamic access lists, for the specified host.

## Command Modes

EXEC

## Command History

Release	Modification
12.0(5)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

Use this command to clear entries from the translation table before they time out.

## Examples

The following example deletes all authentication proxy entries:

```
clear ip auth-proxy cache *
```

The following example deletes the authentication proxy entry for the host with IP address 192.168.4.5:

```
clear ip auth-proxy cache 192.168.4.5
```

## Related Commands

Command	Description
<b>show ip auth-proxy</b>	Displays the authentication proxy entries or the running authentication proxy configuration.

# clear ip auth-proxy watch-list

To delete a single watch-list entry or all watch-list entries in Privileged EXEC configuration command mode, use the **clear ip auth-proxy watch-list** command.

```
clear ip auth-proxy watch-list {ip-addr | *}
```

## Syntax Description

<i>ip-addr</i>	IP address to be deleted from the watch list.
*	All watch-list entries from the watch list.

## Defaults

This command has no default settings.

## Command Modes

Privileged EXEC.

## Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
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

This command is supported on the systems that are configured with a Supervisor Engine 2 only.

If you see entries in the watch list that you suspect are not valid, you can enter the **clear ip auth-proxy watch-list** command to clear them manually instead of waiting for the watch list to expire.

## Examples

This example shows how to delete a single watch-list entry:

```
Router# clear ip auth-proxy watch-list 10.0.0.2
```

```
Router#
```

This example shows how to delete all watch-list entries:

```
Router# clear ip auth-proxy watch-list *
```

```
Router#
```

## Related Commands

Command	Description
<b>ip auth-proxy max-login-attempts</b>	Limits the number of login attempts at a firewall interface and QoS filtering and enter the ARP ACL configuration submode.

Command	Description
<b>ip auth-proxy watch-list</b>	Enables and configures an authentication proxy watch list.
<b>show ip auth-proxy watch-list</b>	Displays the information about the authentication proxy watch list.

# clear ip inspect ha

To delete the Firewall stateful failover sessions information from a router's memory, use the **clear ip inspect ha** command in privileged EXEC mode.

**clear ip inspect ha [sessions all | statistics]**

## Syntax Description

<b>sessions all</b>	(Optional) Clears all the firewall HA sessions.
<b>statistics</b>	(Optional) Clears the HA statistics on the device.

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

If the **clear ip inspect ha sessions all** command is used on the standby device, the standby HA sessions are cleared. This initiates re-synchronization of all HA sessions from the active device to the standby device.

## Examples

The following example shows all sessions being deleted:

```
Router# clear ip inspect ha sessions all
```

The following example shows statistics being deleted.

```
Router# clear ip inspect ha statistics
```

# clear ip inspect session

To delete Context-Based Access Control (CBAC) configuration and session information from a router's memory, use the **clear ip inspect session** command in privileged EXEC mode.

**clear ip inspect session** *session-address*

## Syntax Description

*session-address* Deletes a specific session; the format is 0-FFFFFFF.

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

Sessions consist of control channels and data channels.

Use the **clear ip inspect session** command to delete a control channel or a data channel. If you specify a control channel session, then data channel sessions may also be deleted, depending on the application protocols being used. If you specify a data channel session, then only that specific session is deleted.

If you attempt to delete a session and the **clear ip inspect session** command is not supported for the specified protocol, then an error message is generated.

If you want to delete a specific session, use the **show ip inspect session** command to display all session addresses.



### Note

The **clear ip inspect session** command is recommended for advanced users only because it may disrupt network operations if traffic is still flowing through the session.

## Examples

The following example displays the current session addresses:

```
Router# show ip inspect session

Established Sessions

  Session 25A3318 (10.0.0.1:20)=>(10.1.0.1:46068) ftp-data SIS_OPEN
  Session 25A6E1C (10.1.0.1:46065)=>(10.0.0.1:21) ftp SIS_OPEN
```

The following example shows a specific session being deleted:

```
Router# clear ip inspect session 25A6E1C
```

## Related Commands

Command	Description
<b>show ip inspect</b>	Displays CBAC configuration and session information.

# clear ip ips configuration

To disable Cisco IOS Firewall Intrusion Prevention System (IPS), remove all intrusion detection configuration entries, and release dynamic resources, use the **clear ip ips configuration** command in EXEC mode.

## clear ip ips configuration

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.3(8)T	The command name was changed from the <b>clear ip audit configuration</b> command to the <b>clear ip ips configuration</b> command.
	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 clears the existing IPS configuration:

```
clear ip ips configuration
```

# clear ip ips statistics

To reset statistics on packets analyzed and alarms sent, use the **clear ip ips statistics** command in privileged EXEC mode.

```
clear ip ips statistics [vrf vrf-name]
```

## Syntax Description

<b>vrf</b>	(Optional) Resets statistics on packets analyzed and alarms sent per VRF.
<i>vrf-name</i>	User specific VRF.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the <b>clear ip audit statistics</b> command to the <b>clear ip ips statistics</b> command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	The <b>vrf</b> keyword and argument were added.

## Examples

The following example clears all Intrusion Protection System (IPS) statistics:

```
clear ip ips statistics
```

### Sample Output for the clear ip ips statistics vrf Command

The following example displays the output of the **clear ip ips statistics vrf vrf-name** command:

```
Router# clear ip ips statistics vrf VRF_600
Router# show ip ips statistics vrf VRF_600
Signature statistics [process switch:fast switch]
  signature 5170:1 packets checked: [0:2]
Interfaces configured for ips 3
Session creations since subsystem startup or last reset 0
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [0:0:0]
Last session created 00:02:34
Last statistic reset never
TCP reassembly statistics
  received 8 packets out-of-order; dropped 0
  peak memory usage 12 KB; current usage: 0 KB
  peak queue length 6
```

# clear ip sdee

To clear Security Device Event Exchange (SDEE) events or subscriptions, use the **clear ip sdee** command in privileged EXEC mode.

```
clear ip sdee {events | subscriptions}
```

## Syntax Description

<b>events</b>	Clears SDEE events from the event buffer.
<b>subscriptions</b>	Clears SDEE subscriptions.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.3(8)T	This command was introduced.

## Usage Guidelines

Because subscriptions are properly closed by the Cisco IOS Intrusion Prevention System (IPS) client, this command is typically used only to help with error recovery.

## Examples

The following example shows how to clear all open SDEE subscriptions on the router:

```
Router# clear ip sdee subscriptions
```

## Related Commands

Command	Description
<b>ip ips notify</b>	Specifies the method of event notification.
<b>ip sdee events</b>	Sets the maximum number of SDEE events that can be stored in the event buffer.
<b>ip sdee subscriptions</b>	Sets the maximum number of SDEE subscriptions that can be open simultaneously.

# clear ip trigger-authentication

To clear the list of remote hosts for which automated double authentication has been attempted, use the **clear ip trigger-authentication** command in privileged EXEC mode.

## clear ip trigger-authentication

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC

### 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

Use this command when troubleshooting automated double authentication. This command clears the entries in the list of remote hosts displayed by the **show ip trigger-authentication** command.

### Examples

The following example clears the remote host table:

```
Router# show ip trigger-authentication

Trigger-authentication Host Table:
Remote Host      Time Stamp
172.21.127.114   2940514234
Router# clear ip trigger-authentication
Router# show ip trigger-authentication
```

### Related Commands

Command	Description
<b>show ip trigger-authentication</b>	Displays the list of remote hosts for which automated double authentication has been attempted.

# clear ip urlfilter cache

To clear the cache table, use the **clear ip urlfilter cache** command in user EXEC mode.

```
clear ip urlfilter cache {ip-address | all} [vrf vrf-name]
```

## Syntax Description

<i>ip-address</i>	Clears the cache table of a specified server IP address.
<b>all</b>	Clears the cache table completely.
<b>vrf</b> <i>vrf-name</i>	(Optional) Clears the cache table only for the specified Virtual Routing and Forwarding (VRF) interface.

## Command Modes

User EXEC

## Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The <b>vrf</b> <i>vrf-name</i> keyword/argument pair was 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

The cache table consists of the most recently requested IP addresses and the respective authorization status for each IP address.

## Examples

The following example shows how to clear the cache table of IP address 172.18.139.21:

```
clear ip urlfilter cache 172.18.139.21
```

The following example shows how to clear the cache table of all IP addresses:

```
clear ip urlfilter cache all
```

The following example shows how to clear the cache table of all IP addresses in the vrf named bank.

```
clear ip urlfilter cache all vrf bank
```

## Related Commands

Command	Description
<b>ip urlfilter cache</b>	Configures cache parameters.
<b>show ip urlfilter cache</b>	Displays the destination IP addresses that are cached into the cache table.

# clear kerberos creds

To delete the contents of the credentials cache, use the **clear kerberos creds** command in privileged EXEC mode.

**clear kerberos creds**

**Syntax Description** This command has no arguments or keywords.

**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.
	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** Credentials are deleted when this command is issued.  
Cisco supports Kerberos 5.

**Examples** The following example illustrates the **clear kerberos creds** command:

```
Router# show kerberos creds
Default Principal: chet@cisco.com
Valid Starting      Expires      Service Principal
18-Dec-1995 16:21:07  19-Dec-1995 00:22:24  krbtgt/CISCO.COM@CISCO.COM

Router# clear kerberos creds
Router# show kerberos creds
No Kerberos credentials.
```

Related Commands	Command	Description
	<b>show kerberos creds</b>	Displays the contents of your credentials cache.

# clear logging ip access-list cache

To clear all the entries from the Optimized ACL Logging (OAL) cache and send them to the syslog, use the **clear logging ip access-list cache** command in privileged EXEC mode.

**clear logging ip access-list cache**

**Syntax Description** This command has no arguments or keywords.

**Defaults** This command has no default settings.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

**Usage Guidelines** This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

**Examples** This example shows how to clear all the entries from the OAL cache and send them to the syslog:

```
Router# clear logging ip access-list cache
```

Related Commands	Command	Description
	<b>logging ip access-list cache (global configuration )</b>	Configures the OAL parameters globally.
	<b>logging ip access-list cache (interface configuration )</b>	Enables an OAL-logging cache on an interface that is based on direction.
	<b>show logging ip access-list</b>	Displays information about the logging IP access list.

# clear parameter-map type protocol-info

To clear the Domain Name System (DNS) cache for name resolution of servers within a parameter map, use the **clear parameter-map type protocol-info** command in privileged EXEC mode.

```
clear parameter-map type protocol-info dns-cache dns-name [ip-address ip-address]
```

## Syntax Description

<b>dns-cache</b> <i>dns-name</i>	Cache of the specified DNS server will be cleared.
<b>ip-address</b> <i>ip-address</i>	(Optional) Specified IP address is removed from the cache of the DNS server.  If an IP address is not specified, all IP addresses from the specified DNS server are cleared from the cache.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

## Examples

The following example shows how to clear the cache of the DNS server “sdsc.msg.yahoo.com:

```
Router# clear parameter-map type protocol-info dns-cache sdsc.msg.yahoo.com
```

## Related Commands

Command	Description
<b>parameter-map type</b>	Creates or modifies a parameter map.

# clear port-security

To delete configured secure MAC addresses and sticky MAC addresses from the MAC address table in the Privileged EXEC configuration command mode, use the **clear port-security** command.

**clear port-security dynamic** [**address** *mac-addr* | **interface** *interface-id*] [**vlan** *vlan-id*]

Syntax Description		
<b>address</b> <i>mac-addr</i>	(Optional)	Deletes the specified secure MAC address or sticky MAC address.
<b>interface</b> <i>interface-id</i>	(Optional)	Deletes all secure MAC addresses and sticky MAC addresses on the specified physical port or port channel.
<b>vlan</b> <i>vlan-id</i>	(Optional)	Deletes the specified secure MAC address or sticky MAC address from the specified VLAN.

**Defaults** This command has no default settings.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
	12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
	12.2(18)SXE	The output of this command was changed to support sticky MAC addresses on the Supervisor Engine 720 only.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

**Usage Guidelines** This command is supported on negotiated trunks only.

If you enter the **clear port-security** command without adding any keywords or arguments, the switch removes all the secure MAC addresses and sticky MAC addresses from the MAC address table.

If you enter the **clear port-security dynamic interface** *interface-id* command, all the secure MAC addresses and sticky MAC addresses on an interface are removed from the MAC address table.

You can verify that the information was deleted by entering the **show port-security** command.

---

**Examples**

This example shows how to remove a specific secure address from the MAC address table:

```
Router# clear port-security dynamic address 0008.0070.0007
Router#
```

This example shows how to remove all the secure MAC addresses and sticky MAC addresses learned on a specific interface:

```
Router# clear port-security dynamic interface gigabitethernet0/1
Router#
```

---

**Related Commands**

Command	Description
<code>show port-security</code>	Displays information about the port-security setting.
<code>switchport port-security mac-address</code>	Adds a MAC address to the list of secure MAC addresses.

# clear radius local-server

To clear the display on the local server or to unblock a locked username, use the **clear radius local-server** command in privileged EXEC mode.

```
clear radius local-server {statistics | user username}
```

Syntax Description	Parameter	Description
	<b>statistics</b>	Clears the display of statistical information.
	<b>user</b>	Unblocks the locked username specified.
	<i>username</i>	Locked username.

**Command Modes** Privileged EXEC

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

**Examples** The following example shows how to unblock the locked username “smith”:

```
Router# clear radius local-server user smith
```

Related Commands	Command	Description
	<b>block count</b>	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
	<b>debug radius local-server group</b>	Displays the debug information for the local server.
	<b>group</b>	Enters user group configuration mode and configures shared setting for a user group.
	<b>nas</b>	Adds an access point or router to the list of devices that use the local authentication server.
	<b>radius-server host</b>	Specifies the remote RADIUS server host.
	<b>radius-server local</b>	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
	<b>reauthentication time</b>	Specifies the time after which access points or wireless-aware routers must reauthenticate the members of a group.
	<b>show radius local-server statistics</b>	Displays statistics for a local network access server.
	<b>ssid</b>	Specifies up to 20 SSIDs to be used by a user group.

# clear webvpn nbns

To clear the NetBIOS name service (NBNS) cache on a SSL VPN gateway, use the **clear webvpn nbns** command in privileged EXEC mode.

```
clear webvpn nbns [context {name | all}]
```

Syntax Description	context	(Optional) Clears NBNS statistics for a specific context or all contexts.
	<i>name</i>	Clears NBNS statistics for a specific context.
	<b>all</b>	Clears NBNS statistics for all contexts.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

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

**Usage Guidelines** Entering this command without any keywords or arguments clears all NBNS counters on the network device.

**Examples** The following example clears all NBNS counters:

```
Router# clear webvpn nbns
```

Related Commands	Command	Description
	<b>clear webvpn session</b>	Clears remote users sessions on a SSL VPN gateway.
	<b>clear webvpn stats</b>	Clears application and access counters on a SSL VPN gateway.

# clear webvpn session

To clear SSL VPN remote user sessions, use the **clear webvpn session** command in privileged EXEC mode.

```
clear webvpn session [user name] context {name | all}
```

## Syntax Description

<b>user name</b>	(Optional) Clears session information for a specific user.
<b>context</b> { <i>name</i>   <b>all</b> }	Clears session information for a specific context or all contexts.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

This command is used to clear the session for either the specified remote user or all remote users in the specified context.

## Examples

The following example clears all session information:

```
Router# clear webvpn session context all
```

## Related Commands

Command	Description
<b>clear webvpn nbns</b>	Clears the NBNS cache on a SSL VPN gateway.
<b>clear webvpn stats</b>	Clears application and access counters on a SSL VPN gateway.

# clear webvpn stats

To clear (or reset) SSL VPN application and access counters, use the **clear webvpn stats** command in privileged EXEC mode.

```
clear webvpn stats [[cifs | citrix | mangle | port-forward | sso | tunnel] [context {name | all}]]
```

## Syntax Description

<b>cifs</b>	(Optional) Clears Windows file share (CIFS) statistics.
<b>citrix</b>	(Optional) Clears Citrix application statistics.
<b>mangle</b>	(Optional) Clears URL mangling statistics.
<b>port-forward</b>	(Optional) Clears port forwarding statistics.
<b>sso</b>	(Optional) Clears statistics for Single SignOn (SSO) activities.
<b>tunnel</b>	(Optional) Clears Cisco AnyConnect VPN Client tunnel statistics.
<b>context</b> { <i>name</i>   <b>all</b> }	(Optional) Clears information for either a specific context or all contexts.

## Command Default

If no keywords are entered, all SSL VPN application and access counters are cleared.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	The <b>sso</b> keyword was added.

## Usage Guidelines

This command is used to clear counters for Windows file shares, Citrix applications, URL mangling, application port forwarding, SSO, and Cisco AnyConnect VPN Client tunnels. The counters are cleared for either the specified context or all contexts on the SSL VPN gateway.

## Examples

The following example clears all statistics counters for all SSL VPN processes:

```
Router# clear webvpn stats
```

The following example clears statistics for SSO activities:

```
Router# clear webvpn stats sso
```

## Related Commands

Command	Description
<b>clear webvpn nbns</b>	Clears the NBNS cache on a SSL VPN gateway.
<b>clear webvpn session</b>	Clears remote users sessions on a SSL VPN gateway.

# clear zone-pair

To clear the policy map counters, inspect sessions, or the URL filter cache on a zone-pair, use the **clear zone-pair** command in privileged EXEC mode.

```
clear zone-pair [zone-pair-name] {counter | inspect session | urlfilter cache}
```

## Syntax Description

<i>zone-pair-name</i>	(Optional) Name of the zone-pair on which counters, inspect sessions, or the uRL filter cache are cleared.
<b>counter</b>	Clears the policy-map counters. Resets the statistics of the inspect type policy map on the specified zone-pair.
<b>inspect session</b>	Deletes the inspect sessions on the specified zone-pair.
<b>urlfilter cache</b>	Clears the URL filter cache on the specified zone-pair.

## Command Default

Disabled (it is not necessary to enter this command).

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was implemented on the following platforms: Cisco 881 and Cisco 888.

## Usage Guidelines

If you do not specify a zone-pair name, the policy map counters, sessions, or the URL filter cache are cleared for all the configured zone-pairs.

## Examples

The following example deletes the inspect sessions on the zp zone-pair:

```
Router# clear zone-pair zp inspect session
```

The following example clears the URL filter cache on the zp zone-pair.

```
Router# clear zone-pair zp urlfilter cache
```

# clid

To preauthenticate calls on the basis of the Calling Line IDentification (CLID) number, use the **clid** command in AAA preauthentication configuration mode. To remove the **clid** command from your configuration, use the **no** form of this command.

```
clid [if-avail | required] [accept-stop] [password password]
```

```
no clid [if-avail | required] [accept-stop] [password password]
```

## Syntax Description

<b>if-avail</b>	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
<b>required</b>	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
<b>accept-stop</b>	(Optional) Prevents subsequent preauthentication elements such as <b>ctype</b> or <b>dnis</b> from being tried once preauthentication has succeeded for a call element.
<b>password</b> <i>password</i>	(Optional) Defines the password for the preauthentication element. The default password string is <b>cisco</b> .

## Command Default

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

## Command Modes

AAA preauthentication configuration

## Command History

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

## Usage Guidelines

You may configure more than one of the authentication, authorization and accounting (AAA) preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

---

**Examples**

The following example specifies that incoming calls be preauthenticated on the basis of the CLID number:

```
aaa preauth
  group radius
  clid required
```

---

**Related Commands**

Command	Description
<b>ctype</b>	Preauthenticates calls on the basis of the call type.
<b>dnis (RADIUS)</b>	Preauthenticates calls on the basis of the DNIS number.
<b>dnis bypass (AAA preauthentication configuration)</b>	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
<b>group (RADIUS)</b>	Specifies the AAA RADIUS server group to use for preauthentication.

# client authentication list

To configure Internet Key Exchange (IKE) extended authentication (Xauth) in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **client authentication list** command in ISAKMP profile configuration mode. To restore the default behavior, which is that Xauth is not enabled, use the **no** form of this command.

**client authentication list** *list-name*

**no client authentication list** *list-name*

## Syntax Description

<i>list-name</i>	Character string used to name the list of authentication methods activated when a user logs in. The list name must match the list name that was defined during the authentication, authorization, and accounting (AAA) configuration.
------------------	---

## Defaults

No default behaviors or values

## Command Modes

ISAKMP profile configuration (config-isakmp-profile)

## Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11.5)	Xauth no longer has to be disabled globally for it to be enabled on a profile basis.

## Usage Guidelines

Before configuring Xauth, you must set up an authentication list using AAA commands.

Xauth can be enabled on a profile basis if it has been disabled globally.

Effective with Cisco IOS Release 12.4(11.5), Xauth on either a server or client does not need to be disabled globally to enable it on profile basis.

## Examples

The following example shows that user authentication is configured. User authentication is a list of authentication methods called “xauthlist” in an ISAKMP profile called “vpnprofile.”

```
crypto isakmp profile vpnprofile
 client authentication list xauthlist
```

The following example shows that Xauth has been disabled globally and enabled for the profile “nocerts”:

```
no crypto xauth FastEthernet0/0
!
crypto isakmp policy 1
```

## ■ client authentication list

```

    encr 3des
    group 2
    !
crypto isakmp policy 10
    encr 3des
    authentication pre-share
    group 2
crypto isakmp client configuration group HRZ

crypto isakmp client configuration group vpngroup
    key cisco123
    pool vpnpool
crypto isakmp profile cert_sig
    match identity group HRZ
    isakmp authorization list isakmpauth
    client configuration address respond
    client configuration group HRZ
crypto isakmp profile nocerts
    match identity group vpngroup
    client authentication list vpn-login
    isakmp authorization list isakmpauth
    client configuration address respond

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>aaa authentication login</b>	Sets AAA authentication at login.

# client configuration address

To configure Internet Key Exchange (IKE) configuration mode in the Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **client configuration address** command in ISAKMP profile configuration mode. To disable IKE configuration mode, use the **no** form of this command.

**client configuration address {initiate | respond}**

**no client configuration address {initiate | respond}**

Syntax Description		
	<b>initiate</b>	Router will attempt to set IP addresses for each peer.
	<b>respond</b>	Router will accept requests for IP addresses from any requesting peer.

**Defaults** IKE configuration is not enabled.

**Command Modes** ISAKMP profile configuration

Command History	Release	Modification
	12.2(15)T	This command was introduced.
	12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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

**Examples** The following example shows that IKE mode is configured to either initiate or respond in an ISAKMP profile called "vpnprofile":

```
crypto isakmp profile vpnprofile
client configuration address initiate
client configuration address respond
```

Related Commands	Command	Description
	<b>crypto isakmp profile</b>	Defines an ISAKMP profile.

# client configuration group

To associate a group with the peer that has been assigned an Internet Security Association Key Management Protocol (ISAKMP) profile, use the **client configuration group** command in crypto ISAKMP profile configuration mode. To disable this option, use the **no** form of this command.

**client configuration group** *group-name*

**no client configuration group** *group-name*

## Syntax Description

<i>group-name</i>	Name of the group to be associated with the peer.
-------------------	---

## Defaults

No default behavior or values

## Command Modes

Crypto ISAKMP profile configuration (conf-isa-prof)

## Command History

Release	Modification
12.3(8)T	This command was introduced.
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

The **client configuration group** command is used after the crypto map has been configured and the ISAKMP profiles have been assigned to them.

## Examples

The following example shows that the group “some\_group” is to be associated with the peer:

```
crypto isakmp profile id_profile
  ca trust-point 2315
  match identity host domain cisco.com
  client configuration group some_group
```

## Related Commands

Command	Description
<b>match certificate (ISAKMP)</b>	Assigns an ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate.

# client pki authorization list

To specify the authorization list of AAA servers that will be used to obtain per-user AAA attributes on the basis of the username that is constructed from the certificate, use the **client pki authorization list** command in crypto ISAKMP profile configuration mode. To disable the list name, use the **no** form of this command.

**client pki authorization list** *listname*

**no client pki authorization list** *listname*

Syntax Description	<i>listname</i>	Definition of the argument needed, including syntax-level defaults, if any.
--------------------	-----------------	---

Command Default	User attributes are not pushed to the remote device.
-----------------	--

Command Modes	Crypto ISAKMP profile configuration (config-isakmp-profile)
---------------	---

Command History	Release	Modification
	12.4(4)T	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines	This command is used inside the crypto Internet Security Association and Key Management Protocol (ISAKMP) profile.
------------------	--

Examples	The following example shows that user attributes are to be obtained from the AAA server (list name “usrgrp”) and pushed to the remote device:
----------	---

```
crypto isakmp profile ISA-PROF
 match certificate CERT-MAP
 isakmp authorization list usrgrp
 client pki authorization list usrgrp
 client configuration address respond
 client configuration group pkiuser
 virtual-template 2
```

Related Commands	Command	Description
	<b>crypto isakmp profile</b>	Defines an ISAKMP profile and audits IPsec user sessions.

# client rekey encryption

To set the client acceptable rekey ciphers for the key-encryption-key (KEK), use the **client rekey encryption** command in GDOI group configuration mode. To remove the client acceptable rekey ciphers, use the **no** form of this command.

**client rekey encryption** *cipher* [...*cipher*]

**no client rekey encryption**

## Syntax Description

*cipher*

Any of the following ciphers:

- **3des-cbc**—Specifies triple Data Encryption Standard (3DES) in Cipher-block chaining (CBC) mode.
- **aes 128**—Specifies 128-bit Advanced Encryption Standard (AES).
- **aes 192**—Specifies 192-bit AES.
- **aes 256**—Specifies 256-bit AES.
- **des-cbc**—Specifies DES in CBC mode.

## Command Default

Any cipher assigned by the key-server is accepted.

## Command Modes

GDOI group configuration (config-gdoi-group)

## Command History

Release	Modification
Cisco IOS XE Release 2.4.1	This command was introduced.

## Usage Guidelines

Use the **client rekey encryption** command to specify the acceptable ciphers for KEK. Multiple ciphers can be specified. If a cipher is not set using this command, the cipher assigned by the key server is accepted.

## Examples

The following example shows how to set the acceptable ciphers for KEK:

```
Router# configure terminal
Router(config)# crypto gdoi group GETVPN
Router(config-gdoi-group)# identity number 1111
Router(config-gdoi-group)# server address ipv4 192.10.2.10
Router(config-gdoi-group)# client rekey encryption 3des-cbc aes 192 aes 256
```

## Related Commands

Command	Description
<b>crypto gdoi group</b>	Identifies a GDOI group and enters GDOI group configuration mode.

# client rekey hash

To set acceptable hash algorithms for rekey message signing, use the **client rekey hash** command in GDOI group configuration mode. To remove the acceptable hash algorithms, use the **no** form of this command.

**client rekey hash** *hash*

**no client rekey hash**

## Syntax Description

*hash* Hash for rekey message signing. The supported hash is Secure Hash Standard (sha).

## Command Default

Any hash selected by the key server is accepted.

## Command Modes

GDOI group configuration (config-gdoi-group)

## Command History

Release	Modification
Cisco IOS XE Release 2.4.1	This command was introduced.

## Usage Guidelines

Use the **client rekey hash** command to select the acceptable hash for the rekey message signing. In Cisco IOS XE Release 2.4.1, **sha** is the only supported hash. If a hash is not set using this command, the hash selected by the key server is accepted.

## Examples

The following example shows how to set the acceptable hash for rekey message signing:

```
Router# configure terminal
Router(config)# crypto gdoi group GETVPN
Router(config-gdoi-group)# identity number 1111
Router(config-gdoi-group)# server address ipv4 192.10.2.10
Router(config-gdoi-group)# client rekey hash sha
```

## Related Commands

Command	Description
<b>crypto gdoi group</b>	Identifies a GDOI group and enters GDOI group configuration mode.

# client transform-sets

To specify up to 6 acceptable transform-set tags used by the traffic-encryption-key (TEK) for data encryption or authentication, use the **client transform-sets** command in GDOI group configuration mode. To remove the acceptable transform-set tags, use the **no** form of this command.

```
client transform-sets transform-set-name1 [... [transform-set-name6]]
```

```
no client transform-sets
```

## Syntax Description

<i>transform-set-name</i>	Transform-tags used by the TEK for data encryption or authentication.
---------------------------	---

## Command Default

The transform-set selected by the key server is accepted.

## Command Modes

GDOI group configuration (config-gdoi-group)

## Command History

Release	Modification
Cisco IOS XE Release 2.4.1	This command was introduced.

## Usage Guidelines

Use the **client transform-sets** command to specify up to 6 transform-set tags used by the TEK for data encryption or authentication. If this command is not issued, the transform-set selected by the key server is accepted. The security protocol configured in the transform set must be Encapsulating Security Payload (ESP), which is the only protocol supported by GETVPN in Cisco IOS XE Release 2.4.1.

## Examples

The following example shows how to set the transform-set tags used by TEK for data encryption or authentication:

```
Router# configure terminal
Router(config)# crypto ipsec transform-set g1 esp-aes 192 esp-sha-hmac
Router(cfg-crypto-trans)# exit
Router(config)# crypto gdoi group GETVPN
Router(config-gdoi-group)# client transform-sets g1
```

## Related Commands

Command	Description
<b>crypto gdoi group</b>	Identifies a GDOI group and enters GDOI group configuration mode.
<b>crypto ipsec transform-set</b>	Defines a transform set—an acceptable combination of security protocols and algorithms.

# commands (view)

To add commands or an interface to a command-line interface (CLI) view, use the **commands** command in view configuration mode. To delete a command or an interface from a CLI view, use the **no** form of this command.

## Syntax for Adding and Deleting Commands to a View

```
commands parser-mode {include | include-exclusive | exclude} [all] [command]
```

```
no commands parser-mode {include | include-exclusive | exclude} [all] [command]
```

## Syntax for Adding and Deleting Interfaces to a View

```
commands parser-mode {include | include-exclusive} [all] [interface interface-name] [command]
```

```
no commands parser-mode {include | include-exclusive} [all] [interface interface-name]
[command]
```

### Syntax Description

<i>parser-mode</i>	Mode in which the specified command exists. See <a href="#">Table 20</a> in the “Usage Guidelines” section for a list of available options for this argument.
<b>include</b>	Adds a specified command or a specified interface to the view and allows the same command or interface to be added to an additional view.
<b>include-exclusive</b>	Adds a specified command or a specified interface to the view and excludes the same command or interface from being added to all other views.
<b>exclude</b>	Denies access to commands in the specified parser mode. <b>Note</b> This keyword is available only for command-based views.
<b>all</b>	(Optional) A “wildcard” that allows every command in a specified configuration mode that begins with the same keyword or every subinterface within a specified interface to be part of the view.
<b>interface interface-name</b>	(Optional) Interface that is added to the view.
<i>command</i>	(Optional) Command that is added to the view. <b>Note</b> If no commands are specified, all commands within the specified parser mode are included or excluded, as appropriate.

### Defaults

If this command is not enabled, a view will not have adequate information to deny or allow access to users.

### Command Modes

View configuration

**Command History**

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	The <b>exclude</b> keyword and the <b>interface</b> <i>interface-name</i> option were added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

**Usage Guidelines**

If a network administrator does not enter a specific command (via the *command* argument) or interface (via the **interface** *interface-name* option), users are granted access (via the **include** or **include-exclusive** keywords) or denied access (via the **exclude** keyword) to all commands within the specified parser-mode.

**parser-mode Options**

Table 20 shows some of the keyword options for the *parser-mode* argument in the **commands** command. The available mode keywords vary depending on your hardware and software version. To see a list of available mode options on your system, use the **commands ?** command.

**Table 20** *parser-mode Argument Options*

Command	Description
<b>accept-dialin</b>	VPDN group accept dialin configuration mode
<b>accept-dialout</b>	VPDN group accept dialout configuration mode
<b>address-family</b>	Address Family configuration mode
<b>alps-ascu</b>	ALPS ASCU configuration mode
<b>alps-circuit</b>	ALPS circuit configuration mode
<b>atm-bm-config</b>	ATM bundle member configuration mode
<b>atm-bundle-config</b>	ATM bundle configuration mode
<b>atm-vc-config</b>	ATM virtual circuit configuration mode
<b>atmsig_e164_table_mode</b>	ATMSIG E164 Table
<b>cascustom</b>	Channel-associated signalling (cas) custom configuration mode
<b>config-rtr-http</b>	RTR HTTP raw request Configuration
<b>configure</b>	Global configuration mode
<b>controller</b>	Controller configuration mode
<b>crypto-map</b>	Crypto map config mode
<b>crypto-transform</b>	Crypto transform config modeCrypto transform configuration mode
<b>dhcp</b>	DHCP pool configuration mode
<b>dspfarm</b>	DSP farm configuration mode
<b>exec</b>	EXEC mode
<b>flow-cache</b>	Flow aggregation cache configuration mode
<b>gateway</b>	Gateway configuration mode
<b>interface</b>	Interface configuration mode

Table 20 *parser-mode Argument Options (continued)*

Command	Description
<b>interface-dlci</b>	Frame Relay DLCI configuration mode
<b>ipenacl</b>	IP named extended access-list configuration mode
<b>ipsnacl</b>	IP named simple access-list configuration mode
<b>ip-vrf</b>	Configure IP VRF parameters
<b>lane</b>	ATM Lan Emulation Leacs Configuration Table
<b>line</b>	Line configuration mode
<b>map-class</b>	Map class configuration mode
<b>map-list</b>	Map list configuration mode
<b>mpoa-client</b>	MPOA Client
<b>mpoa-server</b>	MPOA Server
<b>null-interface</b>	Null interface configuration mode
<b>preaut</b>	AAA Preauth definitions
<b>request-dialin</b>	VPDN group request dialin configuration mode
<b>request-dialout</b>	VPDN group request dialout configuration mode
<b>route-map</b>	Route map configuration mode
<b>router</b>	Router configuration mode
<b>rsvp_policy_local</b>	RSVP local policy configuration mode
<b>rtr</b>	RTR Entry Configuration
<b>sg-radius</b>	RADIUS server group definition
<b>sg-tacacs+</b>	TACACS+ server group
<b>sip-ua</b>	SIP UA configuration mode
<b>subscriber-policy</b>	Subscriber policy configuration mode
<b>tcl</b>	Tcl mode
<b>tdm-conn</b>	TDM connection configuration mode
<b>template</b>	Template configuration mode
<b>translation-rule</b>	Translation Rule configuration mode
<b>vc-class</b>	VC class configuration mode
<b>voiceclass</b>	Voice Class configuration mode
<b>voiceport</b>	Voice configuration mode
<b>voipdialpeer</b>	Dial Peer configuration mode
<b>vpdn-group</b>	VPDN group configuration mode

**Examples**

The following example shows how to add the privileged EXEC command **show version** to both CLI views “first” and “second.” Because the **include** keyword was issued, the **show version** command can be added to both views.

```
Router(config)# parser view first
Router(config-view)# secret 5 secret
```

```
Router(config-view)# commands exec include show version
!
Router(config)# parser view second
Router(config-view)# secret 5 myview
Router(config-view)# commands exec include show version
```

The following example shows how to allow users in the view “first” to execute all commands that start with the word “show” except the **show interfaces** command, which is excluded by the view “second”:

```
Router(config)# parser view first
Router(config-view)# secret 5 secret
Router(config-view)# commands exec include all show
!
Router(config)# parser view second
Router(config-view)# secret 5 myview
Router(config-view)# commands exec include-exclusive show interfaces
```

#### Related Commands

Command	Description
<b>parser view</b>	Creates or changes a CLI view and enters view configuration mode.
<b>secret 5</b>	Associates a CLI view or a superview with a password.

# configuration url

To specify on a server the URL that an Easy VPN remote device must use to get a configuration in a Mode Configuration Exchange, use the **configuration url** command in global configuration mode. To delete the URL, use the **no** form of this command.

**configuration url** {*url*}

**no configuration url** {*url*}

## Syntax Description

<i>url</i>	Specifies the URL the Easy VPN remote device must use to get the configuration from the server. <ul style="list-style-type: none"> <li>The URL must be a non-NULL terminated ASCII string that specifies the complete path of the configuration file.</li> </ul>
------------	--

## Command Default

An Easy VPN remote device cannot request a configuration from a server in a Mode Configuration Exchange.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

## Usage Guidelines

After the server “pushes” the URL to a Cisco Easy VPN remote device, the remote device can download the content located at the URL site and apply the configuration content to its running configuration.

Before this command can be configured, the **crypto isakmp client configuration group** command must already have been configured.

## Examples

The file served by the configuration URL should have a Cisco IOS command-line interface (CLI) listing. The listing can have an optional “transient” section. The keyword to begin the transient section is “!*%transient*,” and the keyword should be on a single line. A persistent section can be optionally identified by the keyword “!*%persistent*,” also shown on a single line. An example of a CLI listing follows:

```
ip cef
cdp advertise-v2
!%transient
ip domain-name example.com
ntp server 10.2.3.4
```

```
ntp update-calendar
```

In the above example, the first two lines stay in the configuration even after the tunnel is disconnected (but they are not written into the nonvolatile configuration). The last three lines are effective only as long as the tunnel is “up.”

The following example shows that a server has specified the URL the Easy VPN remote device must use to download the URL:

```
crypto isakmp client configuration group group1  
configuration url http://10.10.8.8/easy.cfg
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>crypto isakmp client configuration group</b>	Specifies to which group a policy profile will be defined.

---

# configuration version

To specify on a server the version that a Cisco Easy VPN remote device must use to get a particular configuration in a Mode Configuration Exchange, use the **configuration version** command in global configuration mode. To delete the version number, use the **no** form of this command.

**configuration version** {*version-number*}

**no configuration version** {*version-number*}

## Syntax Description

<i>version-number</i>	Specifies the version of the configuration. <ul style="list-style-type: none"> <li>The version number will be an unsigned integer in the range 1 through 32767.</li> </ul>
-----------------------	--

## Command Default

A version number is not sent.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

## Usage Guidelines

Before this command can be configured, the **crypto isakmp client configuration group** command must already have been configured.

## Examples

The following example shows that a server has specified the version number a Cisco Easy VPN remote device must use to obtain that particular configuration version:

```
crypto isakmp client configuration group group1
configuration version 10
```

## Related Commands

Command	Description
<b>crypto isakmp client configuration group</b>	Specifies to which group a policy profile will be defined.

# content-length

To permit or deny HTTP traffic through the firewall on the basis of message size, use the **content-length** command in appfw-policy-http configuration mode. To remove message-size limitations from your configuration, use the **no** form of this command.

**content-length** { *min bytes max bytes* | *min bytes* | *max bytes* } **action** { **reset** | **allow** } [**alarm**]

**no content-length** { *min bytes max bytes* | *min bytes* | *max bytes* } **action** { **reset** | **allow** } [**alarm**]

## Syntax Description

<b>min bytes</b>	Minimum content length, in bytes, allowed per message. Number of bytes range: 0 to 65535.
<b>max bytes</b>	Maximum content length, in bytes, allowed per message. Number of bytes range: 0 to 65535.
<b>action</b>	Messages whose size do not meet the minimum or exceed the maximum number of bytes are subject to the specified action ( <b>reset</b> or <b>allow</b> ).
<b>reset</b>	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
<b>allow</b>	Forwards the packet through the firewall.
<b>alarm</b>	(Optional) Generates system logging (syslog) messages for the given action.

## Defaults

If this command is not enabled, message size is not considered when permitting or denying HTTP messages.

## Command Modes

appfw-policy-http configuration

## Command History

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

## Usage Guidelines

All messages exceeding the specified content-length range, will be subjected to the configured action (**reset** or **allow**).

## Examples

The following example, which shows how to define the HTTP application firewall policy “mypolicy,” will not permit HTTP messages longer than 1 byte. This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
  application http
    strict-http action allow alarm
    content-length max 1 action allow alarm
    content-type-verification match-req-resp action allow alarm
```

```
max-header-length request 1 response 1 action allow alarm
max-uri-length 1 action allow alarm
port-misuse default action allow alarm
request-method rfc default action allow alarm
request-method extension default action allow alarm
transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
  ip inspect firewall in
!
!
```

# content-type-verification

To permit or deny HTTP traffic through the firewall on the basis of content message type, use the **content-type-verification** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

```
content-type-verification [match-req-resp] action { reset | allow } [alarm]
```

```
no content-type-verification [match-req-resp] action { reset | allow } [alarm]
```

## Syntax Description

<b>match-req-resp</b>	(Optional) Verifies the content type of the HTTP response against the accept field of the HTTP request.
<b>action</b>	Messages that match the specified content type are subject to the specified action ( <b>reset</b> or <b>allow</b> ).
<b>reset</b>	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
<b>allow</b>	Forwards the packet through the firewall.
<b>alarm</b>	(Optional) Generates system logging (syslog) messages for the given action.

## Defaults

If this command is not issued, all traffic will be allowed.

## Command Modes

appfw-policy-http configuration

## Command History

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

## Usage Guidelines

After the **content-type-verification** command is issued, all HTTP messages are subjected to the following inspections:

- Verify that the content type of the message header is listed as a supported content type. (See [Table 21](#).)
- Verify that the content type of the header matches the content of the message data or entity body portion of the message.

[Table 21](#) contains a list of supported content types.

**Table 21 HTTP Header Supported Content Types**

Supported Content Types
audio/*
audio/basic
audio/midi
audio/mpeg

**Table 21 HTTP Header Supported Content Types (continued)**

<b>Supported Content Types</b>
audio/x-adpcm
audio/x-aiff
audio/x-ogg
audio/x-wav
application/msword
application/octet-stream
application/pdf
application/postscript
application/vnd.ms-excel
application/vnd.ms-powerpoint
application/x-gzip
application/x-java-arching
application/x-java-xm
application/zip
image/*
image/cgf
image/gif
image/jpeg
image/png
image/tiff
image/x-3ds
image/x-bitmap
image/x-niff
image/x-portable-bitmap
image/x-portable-greymap
image/x-xpm
text/*
text/css
text/html
text/plain
text/richtext
text/sgml
text/xmcd
text/xml
video/*
video/-flc

**Table 21 HTTP Header Supported Content Types (continued)**

Supported Content Types
video/mpeg
video/quicktime
video/sgi
video/x-avi
video/x-fli
video/x-mng
video/x-msvideo

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
  application http
  strict-http action allow alarm
  content-length max 1 action allow alarm
  content-type-verification match-req-resp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
  ip inspect firewall in
!
!
```

# copy (consent-parameter-map)

To configure a consent page to be downloaded from a file server, use the **copy** command in parameter-map type consent configuration mode.

```
copy src-file-name dst-file-name
```

Syntax Description	<i>src-file-name</i>	Source file location in which the specified file will be retrieved. The source file location must be TFTP; for example, tftp://10.1.1.1/username/myfile.
	<i>dst-file-name</i>	Destination location in which a copy of the file will be stored. The destination file should be copied to Flash; for example, flash.username.html.

**Command Default** The consent page that is specified via the default parameter-map will be used.

**Command Modes** Parameter-map-type consent (config-profile)

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

**Usage Guidelines** Use the **copy** command to transfer a file (consent web page) from an external server to a local file system on a device. Thus, the file name specified via the **copy** command is retrieved from the destination file location and displayed to the end user as the consent page.

When a consent webpage is displayed to an end user, the filename specified via the **file** command is used. If the file command is not configured, the destination location specified via the **copy** command is used.

**Examples** In the following example, both parameter maps are to use the consent file “tftp://192.168.104.136/consent\_page.html” and store it in “flash:consent\_page.html”:

```
parameter-map type consent consent_parameter_map
copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
authorize accept identity consent_identity_policy
timeout file download 35791
file flash:consent_page.html
logging enabled
exit
!
parameter-map type consent default
copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
authorize accept identity test_identity_policy
timeout file download 35791
file flash:consent_page.html
logging enabled
exit
!
```

■ **copy (consent-parameter-map)****Related Commands**

<b>Command</b>	<b>Description</b>
<b>file (consent-parameter-map)</b>	Specifies a local filename that is to be used as the consent webpage.

# copy idconf

To load a signature package in Cisco IOS Intrusion Prevention System (IPS), use the **copy idconf** command in EXEC mode.

## **copy url idconf**

<b>Syntax Description</b>	<i>url</i>	Specifies the location from which the router loads the signature file. Available URL locations are as follows: <ul style="list-style-type: none"> <li>Local flash, such as flash:sig.xml</li> <li>FTP server, such as ftp://myuser:mypass@ftp_server.sig.xml</li> <li>rcp, such as rcp://myuser@rcp_server/sig.xml</li> <li>TFTP server, such as tftp://tftp_server/sig.xml</li> </ul>
<b>Command Default</b>	None	
<b>Command Modes</b>	EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(11)T	This command was introduced.

## Usage Guidelines

Use the **copy url idconf** command to load a signature package into Cisco IOS IPS. You may wish to load a new signature package into Cisco IOS IPS if a signature (or signatures) with the current signature file is not providing your network with adequate protection from security threats. After the signature package has been loaded into the router, Cisco IOS IPS saves all signature information to the location specified via the **ip ips config location** command.

Signatures are loaded into the scanning table on the basis of importance. Parameters such as signature severity, signature fidelity rating, and time lapsed since signatures were released enable Cisco IOS IPS to compile the most important signatures first, followed by less important signatures, thereby, creating a load order and prioritizing which signatures are loaded first.



### Note

The **copy url idconf** command replaces the **copy ips-sdf** command.

## Examples

The following example shows how to load a signature package into Cisco IOS IPS from the location “flash:IOS-S258-CLI-kd.pkg”:

```
Router# copy flash:IOS-S258-CLI-kd.pkg idconf
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDS_STARTED: 17:19:47 MST Nov 14 2006
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 1 of 13 engines
```

```

*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_READY: multi-string - build time 4 ms - packets
for this engine will be scanned
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDING: service-http - 611 signatures - 2 of 13
engines
*Nov 14 2006 17:20:00 MST: %IPS-6-ENGINE_READY: service-http - build time 12932 ms -
packets for this engine will be scanned
*Nov 14 2006 17:20:00 MST: %IPS-6-ENGINE_BUILDING: string-tcp - 864 signatures - 3 of 13
engines
*Nov 14 2006 17:20:02 MST: %IPS-6-ENGINE_READY: string-tcp - build time 2692 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:02 MST: %IPS-6-ENGINE_BUILDING: string-udp - 74 signatures - 4 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: string-udp - build time 316 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: state - 28 signatures - 5 of 13 engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: state - build time 24 ms - packets for
this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: atomic-ip - 252 signatures - 6 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-4-META_ENGINE_UNSUPPORTED: atomic-ip 2154:0 - this
signature is a component of the unsupported META engine
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: atomic-ip - build time 232 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 e
Router# engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: string-icmp - build time 12 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-ftp - build time 8 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-rpc - 75 signatures - 9 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-rpc - build time 80 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-dns - 38 signatures - 10 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-dns - build time 20 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: normalizer - build time 0 ms - packets for
this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-msrpc - 22 signatures - 12 of
13 engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-msrpc - build time 8 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 16344 ms

```

**Related Commands**

Command	Description
<b>ip ips config-location</b>	Specifies the location in which the router will save signature information.

# copy ips-sdf



## Note

In Cisco IOS Release 12.4(11)T, the **copy ips-sdf** command was replaced with the **copy idconf** command. For more information, see the **copy idconf** command.

To load or save the signature definition file (SDF) in the router, use the **copy ips-sdf** command in EXEC mode.

### Syntax for Loading the SDF

```
copy [/erase] url ips-sdf
```

### Syntax for Saving the SDF

```
copy ips-sdf url
```

## Syntax Description

**/erase** (Optional) Erases the current SDF in the router before loading the new SDF.

**Note** This option is typically available only on platforms with limited memory.

**url**

Description for the *url* argument is one of the following options:

- If you want to load the SDF in the router, the *url* argument specifies the location in which to search for the SDF.
- If you are saving the SDF, the *url* argument represents the location in which the SDF is saved after it has been generated.

Regardless of what option the URL is used for, available URL locations are as follows:

- local flash, such as flash:sig.xml
- FTP server, such as ftp://myuser:mypass@ftp\_server.sig.xml
- rcp, such as rcp://myuser@rcp\_server/sig.xml
- TFTP server, such as tftp://tftp\_server/sig.xml

## Command Modes

EXEC

## Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)T	This command was replaced with the <b>copy idconf</b> command.

**Usage Guidelines****Loading Signatures From the SDF**

Issue the **copy url ips-sdf** command to load the SDF in the router from the location specified via the *url* argument. When the new SDF is loaded, it is merged with the SDF that is already loaded in the router, unless the **/erase** keyword is issued, which overwrites the current SDF with the new SDF.

Cisco IOS Intrusion Prevention System (IPS) will attempt to retrieve the SDF from each specified location in the order in which they were configured in the startup configuration. If Cisco IOS IPS cannot retrieve the signatures from any of the specified locations, the built-in signatures will be used.

If the **no ip ips sdf built-in** command is used, Cisco IOS IPS will fail to load. IPS will then rely on the configuration of the **ip ips fail** command to either fail open or fail closed.

**Note**


---

For Cisco IOS Release 12.3(8)T, the SDF should be loaded directly from Flash.

---

After the signatures are loaded in the router, the signature engines are built. Only after the signature engines are built can Cisco IOS IPS begin scanning traffic.

**Note**


---

Whenever signatures are replaced or merged, the router is suspended while the signature engines for the newly added or merged signatures are being built. The router prompt will be available again after the engines are built.

---

Depending on your platform and how many signatures are being loaded, building the engine can take up to several minutes. It is recommended that you enable logging messages to monitor the engine building status.

---

The **ip sdf ips location** command can also be used to load the SDF. However, unlike the **copy ips-sdf** command, this command does not force and immediately load the signatures. Signatures are not loaded until the router reboots or IPS is initially applied to an interface (via the **ip ips** command).

**Saving a Generated or Merges SDF**

Issue the **copy ips-sdf url** command to save a newly created SDF file to a specified location. The next time the router is reloaded, IPS can refer to the SDF from the saved location by including the **ip ips sdf location** command in the configuration.

**Tip**


---

It is recommended that you save the SDF back out to Flash. Also, you should save the file to a different name than the original attack-drop.sdf file; otherwise, you risk losing the original file.

---

**Examples**

The following example shows how to configure the router to load and merge the attack-drop.sdf file with the default signatures. After you have merged the two files, it is recommended to copy the newly merged signatures to a separate file. The router can then be reloaded (via the **reload** command) or reinitialized to so as to recognize the newly merged file (as shown the following example)

```
!
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
 speed 100
```

```
media-type rj45
no negotiation auto
!
!
! Merge the flash-based SDF (attack-drop.sdf) with the built-in signatures.
copy disk2:attack-drop.sdf ips-sdf
! Save the newly merged signatures to a separate file.
copy ips-sdf disk2:my-signatures.sdf
!
! Configure the router to use the new file, my-signatures.sdf
configure terminal
ip ips sdf location disk2:my-signatures.sdf
! Reinitialize the IPS by removing the IPS rule set and reapplying the rule set.
interface gig 0/1
no ip ips MYIPS in
!
*Apr 8 14:05:38.243:%IPS-2-DISABLED:IPS removed from all interfaces - IPS disabled
!
ip ips MYIPS in
!
exit
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip ips sdf location</b>	Specifies the location in which the router should load the SDF.

---

# crl

To query the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked, use the **crl** command in ca-trustpoint configuration mode. To return to the default behavior in which the router will check the URL that is embedded in the certificate, use the **no** form of this command.

**crl** { *query url* | **optional** | **best-effort** }

**no crl** { *query url* | **optional** | **best-effort** }

## Syntax Description

<b>query url</b>	The Lightweight Directory Access Protocol (LDAP) URL published by the certification authority (CA) server is specified to query the CRL; for example, ldap://another_server.
<b>optional</b>	CRL verification is optional.
<b>best-effort</b>	CRL verification will be attempted, but if the CRL is unavailable, the certificate will be accepted.

## Defaults

If the **query url** option is not enabled, the router will check the CRL distribution point (CDP) that is embedded in the certificate. The **query url** option does not need to be configured if the CDP that is in the certificate is formatted as a URL (for example, http:// url or ldap:// url), including the fully qualified domain name (FQDN) of the host where the CRL is held.

## Command Modes

Ca-trustpoint configuration

## Command History

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

## Usage Guidelines

### The query Keyword

Use the **query url** option if the CDP is in LDAP form, which means that the CDP location in the certificate will indicate only where the CDP is located in the directory; that is, the CDP will not indicate the actual query location for the directory.

### The optional Keyword

If your router does not have the applicable CRL and is unable to obtain one, your router will reject the peer's certificate—unless you include the **optional** keyword in your configuration. If you use the **optional** keyword, your router will check the CRL if it is cached in the router memory, but it will not download the CRL from the CDP. If the **optional** keyword is configured and a CRL is not available, the certificate will always be accepted. If the **crl optional** command is configured, you cannot manually download the CRL via the **crypto ca crl request** command because the manually downloaded CRL may not be deleted after it expires. The expired CRL may cause all certificate verifications to be denied.

### The best-effort Keyword

If you prefer to have the CRL checked and accept certificates if the CRL is not available, use the **best-effort** keyword. This keyword allows the router to attempt to retrieve the CRL from the CDP that is contained in the certificate (or from a different location that is specified via the **crl query url** command). However, if the CRL is not available, the router will accept the certificate if it is presented within its validity period and if the certificate was issued by a trusted CA.



#### Note

The **crypto ca trustpoint** command deprecates the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

### Examples

The following example shows how to configure your router to query the CRL with the LDAP URL that is published by the CA named “bar”:

```
crypto ca trustpoint bar
  enrollment url http://bar.cisco.com
  crl query ldap://bar.cisco.com
```

### Related Commands

Command	Description
<b>crypto ca trustpoint</b>	Declares the CA that your router should use.

# crl best-effort



## Note

Effective with Cisco IOS Release 12.3(2)T, this command was replaced by the **revocation-check** command.

To download the certificate revocation list (CRL) but accept certificates if the CRL is not available, use the **crl best-effort** command in ca-identity configuration mode. To return to the default behavior in which CRL checking is mandatory before your router can accept a certificate, use the **no** form of this command.

## Syntax Description

This command has no arguments or keywords.

## Defaults

If this command is not configured, CRL checking is mandatory before your router can accept a certificate. That is, if CRL downloading is attempted and it fails, the certificate will be considered invalid and will be rejected.

## Command Modes

Ca-identity configuration

## Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(2)T	This command was replaced by the <b>revocation-check</b> command.

## Usage Guidelines

When your router receives a certificate from a peer, it will search its memory for the appropriate CRL. If the appropriate CRL is in the router memory, the CRL will be used. Otherwise, the router will download the CRL from either the certificate authority (CA) or from a CRL distribution point (CDP) as designated in the certificate of the peer. Your router will then check the CRL to ensure that the certificate that the peer sent has not been revoked. (If the certificate appears on the CRL, your router will not accept the certificate and will not authenticate the peer.)

When a CA system uses multiple CRLs, the certificate of the peer will indicate which CRL applies in its CDP extension and should be downloaded by your router.

If your router does not have the applicable CRL in memory and is unable to obtain one, your router will reject the certificate of the peer—unless you include the **crl best-effort** command in your configuration. When the **crl best-effort** command is configured, your router will try to obtain a CRL, but if it cannot obtain a CRL, it will treat the certificate of the peer as not revoked.

When your router receives additional certificates from peers, the router will continue to attempt to download the appropriate CRL if it was previously unsuccessful. The **crl best-effort** command specifies only that when the router cannot obtain the CRL, the router will not be forced to reject the certificate of a peer.

---

**Examples**

The following configuration example declares a CA and permits your router to accept certificates when CRLs are not obtainable:

```
crypto ca identity myid
enrollment url http://mycaserver
crl best-effort
```

---

**Related Commands**

Command	Description
<b>crypto ca identity</b>	Declares the CA your router should use.

---

# crl optional



## Note

Effective with Cisco IOS Release 12.3(2)T, this command was replaced by the **revocation-check** command.

To allow the certificates of other peers to be accepted without trying to obtain the appropriate CRL, use the **crl optional** command in ca-identity configuration mode. To return to the default behavior in which CRL checking is mandatory before your router can accept a certificate, use the **no** form of this command.

**crl optional**

**no crl optional**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The router must have and check the appropriate CRL before accepting the certificate of another IP Security peer.

## Command Modes

Ca-identity configuration

## Command History

Release	Modification
11.3 T	This command was introduced.
12.3(2)T	This command was replaced by the <b>revocation-check</b> command.
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

When your router receives a certificate from a peer, it will search its memory for the appropriate CRL. If the router finds the appropriate CRL, that CRL will be used. Otherwise, the router will download the CRL from either the certificate authority (CA) or from a CRL distribution point (CDP) as designated in the certificate of the peer. Your router will then check the CRL to ensure that the certificate that the peer sent has not been revoked. (If the certificate appears on the CRL, your router will not accept the certificate and will not authenticate the peer.) To instruct the router not to download the CRL and treat the certificate as not revoked, use the **crl optional** command.



## Note

If the CRL already exists in the memory (for example, by using the **crypto ca crl request** command to manually download the CRL), the CRL will still be checked even if the **crl optional** command is configured.

---

**Examples**

The following example declares a CA and permits your router to accept certificates without trying to obtain a CRL. This example also specifies a nonstandard retry period and retry count.

```
crypto ca identity myca
  enrollment url http://ca_server
  enrollment retry-period 20
  enrollment retry-count 100
  crl optional
```

---

**Related Commands**

Command	Description
<code>crypto ca identity</code>	Declares the CA your router should use.

---

# crl query

If you have to query the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked and you have to provide the Lightweight Directory Access Protocol (LDAP) server information, use the **crl query** command in ca-trustpoint configuration mode. To return to the default behavior, assuming that the CRL distribution point (CDP) has a complete LDAP URL, use **no** form of this command.

```
crl query ldap://hostname:[port]
```

```
no crl query ldap://hostname:[port]
```

## Syntax Description

<b>ldap://hostname</b>	Query is made to the hostname of the LDAP server that serves the CRL for the certification authority (CA) server (for example, ldap://myldap.cisco.com).
<b>:port</b>	(Optional) Port number of the LDAP server (for example, ldap://myldap.cisco.com:3899).

## Defaults

Not enabled. If **crl query ldap://hostname:[port]** is not enabled, the router assumes that the CDP that is embedded in the certificate is a complete URL (for example, ldap://myldap.cisco.com/CN=myCA,O=Cisco) and uses it to download the CRL.

If the port number is not configured, the default LDAP server port 389 will be used.

## Command Modes

Ca-trustpoint configuration

## Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(8)T	This command replaced the <b>query url</b> command.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

## Usage Guidelines

When Cisco IOS software tries to verify a peer certificate (for example, during Internet Key Exchange [IKE] or Secure Sockets Layer [SSL] handshake), it queries the CRL to ensure that the certificate has not been revoked. To locate the CRL, it first looks for the CDP extension in the certificate. If the extension exists, it is used to download the CRL. Otherwise, the Simple Certificate Enrollment Protocol (SCEP) GetCRL mechanism is used to query the CRL from the CA server directly (some CA servers do not support this method).

Cisco IOS software supports three types of CDP:

- HTTP URL (Example 1: `http://10.10.10.10:81/myca.crl`)
- LDAP URL (Example 2: `ldap://10.10.10.10:3899/CN=myca, O=cisco` or Example 3: `ldap:///CN=myca, O=cisco`)
- LDAP/X.500 DN (Example 4: `CN=myca, O=cisco`)

To locate the CRL, a complete URL needs to be formed. As a result, Example 3 and Example 4 still require the hostname and the port number. The `ldap://hostname:[port]` keywords and arguments are used to provide this information.



#### Note

The `crypto ca trustpoint` command replaces the `crypto ca identity` and `crypto ca trusted-root` commands and all related subcommands (all `ca-identity` and `trusted-root` configuration mode commands). If you enter a `ca-identity` or `trusted-root` subcommand, the configuration mode and command will be written back as `ca-trustpoint`.

#### Examples

The following example shows how to configure your router to query the CRL with the LDAP URL that is published by the CA named “bar”:

```
crypto ca trustpoint mytp
  enrollment url http://bar.cisco.com
  crl query ldap://bar.cisco.com:3899
```

#### Related Commands

Command	Description
<code>crypto ca trustpoint</code>	Declares the CA that your router should use.
<code>revocation-check</code>	Checks the revocation status of a certificate.

# crl-cache delete-after

To configure the maximum time a router will cache a certificate revocation list (CRL), use the **crl-cache delete-after** command in ca-trustpoint configuration mode. To enable default CRL caching, use the **no** form of this command.

**crl-cache delete-after** *time*

**no crl-cache delete-after** *time*

## Syntax Description

<i>time</i>	The maximum lifetime of a CRL in minutes.
-------------	---

## Command Default

A CRL is deleted from the cache when the CRL default lifetime expires.

## Command Modes

Ca-trustpoint configuration (ca-trustpoint)

## Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

## Usage Guidelines

Use this command to limit the amount of time a router will cache a CRL. You may use the **crl-cache delete-after** command to force a router to download a CRL before the existing CRL expires by configuring a value shorter than the default lifetime of the CRL.

By default, a new CRL will be downloaded after the currently cached CRL expires. The **crl-cache delete-after** command does not effect any currently cached CRLs. The configured lifetime will only effect CRLs downloaded after this command is configured.

When the maximum CRL time expires, the cached CRL will be deleted from the router cache. A new copy of the CRL will be downloaded from the issuing certificate authority (CA) the next time the router has to validate a certificate.



### Note

Only the **crl-cache none** command or the **crl-cache delete-after** command may be specified. If both commands are entered for a trustpoint, the last command executed will take effect and a message will be displayed to the user.

## Examples

The following example shows how to configure a maximum lifetime of 2 minutes for all CRLs associated with the CA1 trustpoint:

```
crypto pki trustpoint CA1
  enrollment url http://CA1:80
  ip-address FastEthernet0/0
  crl query ldap://ldap_CA1
```

```

revocation-check crl
crl-cache delete-after 2

```

The current CRL is still cached immediately after executing the example configuration shown above:

```
Router# show crypto pki crls
```

```

CRL Issuer Name:
  cn=name Cert Manager,ou=pki,o=company.com,c=US
  LastUpdate: 18:57:42 GMT Nov 26 2005
  NextUpdate: 22:57:42 GMT Nov 26 2005
  Retrieved from CRL Distribution Point:
    ldap://ldap.company.com/CN=name Cert Manager,O=company.com

```

When the current CRL expires, a new CRL is then downloaded to the router at the NextUpdate time and the **crl-cache delete-after** command takes effect. This newly cached CRL and all subsequent CRLs will be deleted after a maximum lifetime of 2 minutes.

You can verify that the CRL will be cached for 2 minutes by executing the **show crypto pki crls** command. Note that the NextUpdate time is 2 minutes after the LastUpdate time.

```
Router# show crypto pki crls
```

```

CRL Issuer Name:
  cn=name Cert Manager,ou=pki,o=company.com,c=US
  LastUpdate: 22:57:42 GMT Nov 26 2005
  NextUpdate: 22:59:42 GMT Nov 26 2005
  Retrieved from CRL Distribution Point:
    ldap://ldap.company.com/CN=name Cert Manager,O=company.com

```

#### Related Commands

Command	Description
<b>crl-cache none</b>	Disables CRL caching.

# crl-cache none

To disable certificate revocation list (CRL) caching, use the **crl-cache none** command in ca-trustpoint configuration mode. To enable default CRL caching, use the **no** form of this command.

**crl-cache none**

**no crl-cache none**

**Syntax Description** This command has no arguments or keywords.

**Command Default** CRL caching is enabled.

**Command Modes** Ca-trustpoint configuration (ca-trustpoint)

## Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

## Usage Guidelines

Use this command to disable CRL caching for all CRLs associated with a trustpoint. By default, a new CRL is issued when the currently cached CRL expires.

The **crl-cache none** command does not effect any currently cached CRLs. All CRLs downloaded after this command is configured will not be cached.

This functionality is useful is when a certification authority (CA) issues CRLs with no expiration date or with expiration dates far into the future—days or weeks.



### Note

Only the **crl-cache none** command or the **crl-cache delete-after** command may be specified. If both commands are entered for a trustpoint, the last command executed will take effect and a message will be displayed.

## Examples

The following example shows how to disable CRL caching for all CRLs associated with the CA1 trustpoint:

```
crypto pki trustpoint CA1
  enrollment url http://CA1:80
  ip-address FastEthernet0/0
  crl query ldap://ldap_CA1
  revocation-check crl
  crl-cache none
```

The current CRL is still cached immediately after executing the example configuration shown above:

```
Router# show crypto pki crls
CRL Issuer Name:
  cn=name Cert Manager,ou=pki,o=company.com,c=US
  LastUpdate: 18:57:42 GMT Nov 26 2005
  NextUpdate: 22:57:42 GMT Nov 26 2005
  Retrieved from CRL Distribution Point:
    ldap://ldap.company.com/CN=name Cert Manager,O=company.com
```

When the current CRL expires, a new CRL is then downloaded to the router at the NextUpdate time. The **crl-cache none** command takes effect and all CRLs for the trustpoint are no longer cached; caching is disabled. You can verify that no CRL is cached by executing the **show crypto pki crls** command. No output will be shown because there are no CRLs cached.

---

**Related Commands**

Command	Description
<b>crl-cache delete-after</b>	Configures the maximum lifetime of a CRL.

---