

clear a – clear k

- clear aaa kerberos, on page 3
- clear aaa local user, on page 5
- clear aaa sdi node-secret, on page 7
- clear aaa-server statistics, on page 8
- clear access-list, on page 10
- clear arp, on page 12
- clear asp, on page 13
- clear avc, on page 15
- clear bfd counters, on page 16
- clear bgp, on page 18
- clear blocks, on page 21
- clear-button, on page 22
- clear capture, on page 24
- clear clns cache, on page 25
- clear clns is-neighbors, on page 26
- clear clns neighbors, on page 27
- clear clns route, on page 28
- clear cluster info, on page 29
- clear compression, on page 30
- clear configuration session, on page 31
- clear configure, on page 32
- clear conn, on page 34
- clear console-output, on page 37
- clear coredump, on page 38
- clear counters, on page 39
- clear cpu profile, on page 41
- clear crashinfo, on page 42
- clear crypto accelerator statistics, on page 43
- clear crypto ca crls, on page 44
- clear crypto ca trustpool, on page 45
- clear crypto ikev1, on page 46
- clear crypto ikev2, on page 48
- clear crypto ipsec sa, on page 50

- clear crypto ipsec stats, on page 52
- clear crypto isakmp, on page 53
- clear crypto protocol statistics, on page 54
- clear crypto ssl, on page 56
- clear cts, on page 57
- clear dhcpd, on page 59
- clear dhcprelay statistics, on page 60
- clear dns, on page 61
- clear dns-hosts cache, on page 63
- clear dynamic-filter dns-snoop, on page 64
- clear dynamic-filter reports, on page 66
- clear dynamic-filter statistics, on page 69
- clear eigrp events, on page 71
- clear eigrp neighbors, on page 72
- clear eigrp topology, on page 74
- clear facility-alarm output, on page 75
- clear failover statistics, on page 77
- clear flow-export counters, on page 78
- clear flow-offload, on page 79
- clear flow-offload-ipsec, on page 80
- clear fragment, on page 81
- clear gc, on page 83
- clear igmp counters, on page 84
- clear igmp group, on page 85
- clear igmp traffic, on page 86
- clear ikev1, on page 87
- clear ikev2, on page 89
- clear interface, on page 91
- clear ip audit count, on page 93
- clear ipsec sa, on page 94
- clear ipsec stats, on page 96
- clear ipv6 access-list counters (Deprecated), on page 97
- clear ipv6 dhcprelay, on page 98
- clear ipv6 dhcp statistics, on page 99
- clear ipv6 eigrp, on page 102
- clear ipv6 router eigrp, on page 103
- clear ipv6 mld traffic, on page 104
- clear ipv6 neighbors, on page 105
- clear ipv6 ospf, on page 106
- clear ipv6 prefix-list, on page 108
- clear ipv6 route, on page 109
- clear ipv6 traffic, on page 110
- clear ip verify statistics, on page 112
- clear isakmp sa, on page 113
- clear isis, on page 114

clear aaa kerberos

To clear Kerberos information, use the **clear aaa kerberos** command in privileged EXEC mode.

clear aaa kerberos { **tickets** [**username** *user*] | **keytab** }

Syntax Description

keytab	Clears the Kerberos keytab file.
tickets [**username** *user*]	Clears Kerberos ticket information. All tickets are cleared unless you include the username keyword, which specifies the user whose ticket you want to clear.

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.8(4)	The **keytab** keyword was added.

Examples

The following example shows how to clear all Kerberos tickets.

```
ciscoasa# clear aaa kerberos tickets

Proceed with deleting kerberos tickets? [confirm] y
```

The following example shows how to display, and then clear, the Kerberos keytab file.

```
ciscoasa# show aaa kerberos keytab

Principal:   host/asa2@BXB-WIN2016.EXAMPLE.COM
Key version: 10
Key type:    arcfour (23)
ciscoasa# clear aaa kerberos keytab

ciscoasa# show aaa kerberos keytab

No keys found
ciscoasa#
```

Related Commands

Command	Description
show aaa kerberos	Displays all the Kerberos tickets cached on the system, or the keytab file.

clear aaa local user

To unlock a user, or to reset a user's failed authentication attempts to zero, use the **clear aaa local user** command in Privileged EXEC mode.

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

Syntax Description

all	Either unlocks all locked-out users, or resets the failed-attempts counter to 0 for all users.
failed-attempts	Resets the failed attempts counter to 0 for the specified user or all users.
lockout	Unlocks users that are currently locked out and resets to the failed-attempts counter for the users to 0. This option has no impact on users who are not locked out. The administrator cannot be locked out of the device.
username *name*	Specifies a specific username to unlock or reset the failed-attempts counter to 0.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use this command if a user fails to authenticate after a few attempts.

After the configured number of failed authentication attempts, the user is locked out of the system and cannot successfully log in until either a system administrator unlocks the username or the system reboots. The number of failed attempts resets to zero and the lockout status resets to No when the user successfully authenticates, or when the system reboots. In addition, the system resets the counter to zero when the configuration has recently been modified.

Locking or unlocking a username results in a system log message. A system administrator with a privilege level of 15 cannot be locked out.

Examples

The following example shows how to reset the failed-attempts counter to 0 for the username anyuser:

```
ciscoasa# clear aaa local user fail-attempts
            username anyuser
ciscoasa#
```

The following example shows how to reset the failed-attempts counter to 0 for all users:

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

The following example shows to clear the lockout condition and reset the failed-attempts counter to 0 for the username anyuser:

```
ciscoasa# clear aaa local user lockout username anyuser
ciscoasa#
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Configures a limit on the number of failed user authentication attempts allowed.
show aaa local user	Shows the list of usernames with the failed attempts counter and lockout status.

clear aaa sdi node-secret

To delete the node secret file for an RSA SecurID server, use the **clear aaa sdi node-secret** command in privileged EXEC mode.

clear aaa sdi node-secret *rsa_server_address*

Syntax Description

rsa_server_address	The IP address or fully-qualified hostname of the RSA SecurID/Authentication Manager server whose node secret file you want to delete.

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.15(1)	This command was added.

Examples

The following example shows how to view the list of node secret files, then delete one of them. Use the aaa sdi import-node-secret command to import a new node secret file for the server, if necessary.

```
ciscoasa# show aaa sdi node-secrets

Last update                    SecurID server
--------------------           --------------------
15:16:13 Jun 24 2020           rsaam.example.com
15:20:07 Jun 24 2020           10.11.12.13
ciscoasa# clear aaa sdi node-secret rsaam.example.com
```

Related Commands

Command	Description
aaa sdi import-node-secret	Imports an RSA SecurID Authentication Manager node secret file.
show aaa sdi node-secrets	Displays all the SecurID node secret files.

clear aaa-server statistics

To reset the statistics for AAA servers, use the **clear aaa-server statistics** command in privilged EXEC mode.

clear aaa-server statistics [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

Syntax Description

groupname	(Optional) Clears statistics for servers in a group.
host *hostname*	(Optional) Clears statistics for a particular server in the group.
LOCAL	(Optional) Clears statistics for the LOCAL user database.
protocol *protocol*	(Optional) Clears statistics for servers of the specified protocol: • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

Command Default

Remove all AAA server statistics across all groups.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was modified to adhere to CLI guidelines. In the protocol values, **nt** replaces the older **nt-domain**, and **sdi** replaces the older **rsa-ace**.

Examples

The following example shows how to reset the AAA statistics for a specific server in a group:

```
ciscoasa
(config)#

clear aaa-server statistics svrgrp1 host 1.2.3.4
```

The following example shows how to reset the AAA statistics for an entire server group:

```
ciscoasa
(config)#
clear aaa-server statistics svrgrp1
```

The following example shows how to reset the AAA statistics for all server groups:

```
ciscoasa
(config)#
clear aaa-server statistics
```

The following example shows how to reset the AAA statistics for a particular protocol (in this case, TACACS+):

```
ciscoasa
(config)#
clear aaa-server statistics protocol tacacs+
```

Related Commands

Command	Description
aaa-server protocol	Specifies and manages the grouping of AAA server connection data.
clear configure aaa-server	Removes all nondefault AAA server groups or clear the specified group.
show aaa-server	Displays AAA server statistics.
show running-config aaa-server	Displays the current AAA server configuration values.

clear access-list

To clear an access-list counter, use the **clear access-list** command in global configuration mode.

clear access-list *id* **counters**

Syntax Description

counters	Clears access list counters.
id	Name or number of an access list.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When you enter the **clear access-list** command, you must specify the *id* of an access list to clear the counters .

Examples

The following example shows how to clear a specific access list counter:

```
ciscoasa# clear access-list inbound counters
```

Related Commands

Command	Description
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the firewall.
access-list standard	Adds an access list to identify the destination IP addresses of OSPF routes, which can be used in a route map for OSPF redistribution.
clear configure access-list	Clears an access list from the running configuration.
show access-list	Displays the access list entries by number.

Command	Description
show running-config access-list	Displays the access list configuration that is running on the adaptive security appliance.

clear arp

To clear dynamic ARP entries or ARP statistics, use the **clear arp** command in privileged EXEC mode.

clear arp [**statistics**]

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example clears all ARP statistics:

```
ciscoasa# clear arp statistics
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

clear asp

To clear accelerated security path (ASP) statistics, use the **clear asp** command.

clear asp { **cluster counter** | **drop** [**flow** | **frame**] | **event dp-cp** | **queue-exhaustion** [**snapshot** *number*] | **load-balance history** | **overhead** | **table** [**arp** | **classify** | **network-object** | **filter** [**access-list** *acl_name*]] }

Syntax Description

access-list *acl_name*	(Optional) Clears the hit counters only for a specified access list.
arp	(Optional) Clears the hits counters in ASP ARP tables only.
classify	(Optional) Clears the hits counters in ASP classify tables only
cluster counter	Clears cluster counters.
event	Clears data-path to control-plane event statistics.
filter	(Optional) Clears the hits counters in ASP filter tables only
flow	(Optional) Clears the dropped flow statistics.
frame	(Optional) Clears the dropped frame/packet statistics.
load-balance history	Clears the history of ASP load balancing per packet and reset the number of times an automatic switch occurred
network-object	(Optional) Clears the hits counters in ASP network object tables only. These tables are used when object group search is enabled.
overhead	Clears all ASP multiprocessor overhead statistics.
queue-exhaustion	Clears the data-path inspection Snort queue snapshot.
snapshot *number*	(Optional) Clears the queue exhaustion by snapshot ID.
table	Clears the hit counters in the ARP tables. Specify the table type to limit the action.

Command Default

No default behavior or values.

Command History

Release	Modification
7.0(1)	This command was added.
7.2(4)	We added the **table** keyword.
8.2(2)	We added the **filter** keyword.
9.3(1)	We added the **load-balance history** keywords.
9.22(1)	The **table network-object** option was added.

Examples

The following example clears all ASP table statistics:

```
ciscoasa# clear asp table
Warning: hits counters in asp arp and classify tables are cleared, which might impact the
hits statistic of other modules and output of other "show" commands! ciscoasa#clear asp
table arp
Warning: hits counters in asp arp table are cleared, which might impact the hits statistic
 of other modules and output of other "show" commands! ciscoasa#clear asp table classify
Warning: hits counters in classify tables are cleared, which might impact the hits statistic
 of other modules and output of other "show" commands! ciscoasa(config)# clear asp table
Warning: hits counters in asp tables are cleared, which might impact the hits statistics
of other modules and output of other "show" commands! ciscoasa# sh asp table arp
Context: single_vf, Interface: inside 10.1.1.11 Active 00e0.8146.5212 hits 0
Context: single_vf, Interface: identity :: Active 0000.0000.0000 hits 0 0.0.0.0 Active
0000.0000.0000 hits 0
```

Related Commands

Command	Description
asp load-balance per-packet	Changes the load balancing behavior.
show asp load-balance	Displays a histogram of the load balancer queue sizes.
show asp load-balance per-packet	Displays current status, high and low watermarks, and the global threshold.
show asp load-balance per-packet history	Displays current status, high and low watermarks, the global threshold, the times of switching ASP load balancing per packet on and off since the last reset, the history of ASP load balancing per packet with time stamps, and the reasons for switching it on and off.
show asp	Shows ASP statistics.

clear avc

To clear statistics and hit counts for the Application Visibility and Control (AVC) feature, use the clear avc command in Privileged EXEC mode.

clear avc

Command Default

No defaults

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.24(1)	This command was added.

Example

The following example clears AVC counters.

```
ciscoasa# clear avc
```

Related Commands

Command	Description
avc	Enable Application Visibility and Control (AVC).
show avc	Display AVC information.

clear bfd counters

To clear the BFD counters, use the **clear bfd counters** command in privileged EXEC mode.

clear bfd counters [**ld** *local_discr* | *interface_name* | **ipv4** *ip-address* | **ipv6** *ipv6-address*]

Syntax Description

ld *local_discr*	(Optional) Clears BFD counters for the specified local discriminator, 1 - 4294967295.
interface_name	(Optional) Clears BFD counters for the specified interface.
ipv4 *ip_address*	(Optional) Clears BFD counters for the specified neighbor IP address.
ipv6 *ip_address*	(Optional) Clears BFD counters for the specified neighbor IPv6 address.

Command Default

This command clears all BFD counters.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Examples

The following example clears all BFD counters.

```
ciscoasa# clear bfd counters
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd slow-timers	Configures the BFD slow timers value.

Command	Description
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

clear bgp

Note ASA platforms do not support the legacy neighbor soft-reconfiguration inbound CLI or memory caching of inbound BGP updates. Instead, ASA relies exclusively on BGP Dynamic Route Refresh (RFC 2918) for inbound policy changes. The **clear bgp <neighbor> in** command triggers a route refresh using this mechanism.

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration, use the **clear bgp** command in privileged EXEC mode.

clear bgp { [***** | **external**] [**ipv4 unicast** [*as_number* | *neighbor_address* | **table-map**] | **ipv6 unicast** [*as_number* | *neighbor_address*]] [**soft**] [**in** | **out**] | *as_number* [**soft**] [**in** | **out**] | *neighbor_address* [**soft**] [**in** | **out**] | **table-map** }

Syntax Description

*	Specifies that all current BGP sessions will be reset.
as_number	(Optional) Number of the autonomous system in which all BGP peer sessions will be reset.
external	Specifies that all external BGP sessions will be reset.
in	(Optional) Initiates inbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
ipv4 unicast	Resets BGP connections using hard or soft econfiguration for IPv4 address family sessions.
ipv6 unicast	Resets BGP connections using hard or soft econfiguration for IPv6 address family sessions.
neighbor_address	(Optional) Specifies that only the identified BGP neighbor will be reset. The value for this argument can be an IPv4 or IPv6 address.
out	(Optional) Initiates inbound or outbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
soft	(Optional) Triggers a soft reconfiguration. For inbound sessions, this utilizes BGP Dynamic Route Refresh (RFC 2918) to request updates from the peer without tearing down the BGP session.
table-map	Clears table-map configuration information in BGP routing tables. This command can be used to clear traffic-index information configured with the BGP Policy Accounting feature.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was introduced.

Usage Guidelines

The **clear bgp** command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration triggers the BGP Dynamic Route Refresh (RFC 2918) process to reconfigure and activate BGP routing tables without tearing down existing peering sessions. This allows you to apply a new BGP policy without disrupting the network and does not require additional memory for storing inbound routing updates.

Only the **clear bgp *** command is available in the system execution space in multiple context mode.

Examples

In the following example, all the BGP sessions in all contexts are reset when the **clear bgp** command is given in the system execution space. A warning is issued to confirm the action as this command will reset all the BGP sessions:

```
ciscoasa# clear bgp *
This command will reset BGP in ALL contexts.
Are you sure you want to continue? [no]:
```

In the following example, all the BGP sessions are reset in single mode or in a multiple context mode context:

```
ciscoasa# clear bgp *
```

In the following example, a soft reconfiguration is initiated for the inbound session with the neighbor 10.100.0.1, and the outbound session is unaffected:

```
ciscoasa# clear bgp 10.100.0.1 soft in
```

In the following example, the route refresh capability is enabled on the BGP neighbor routers, a soft reconfiguration is initiated for the inbound session with the neighbor 172.16.10.2, and the outbound session is unaffected:

```
ciscoasa# clear bgp 172.16.10.2 in
```

In the following example, a hard reset is initiated for sessions with all routers in the autonomous system numbered 35700:

```
ciscoasa# clear bgp 35700
```

In the following example, a soft reconfiguration is configured for all inbound eBGP peering sessions:

```
ciscoasa# clear bgp external soft in
```

In the following example, all outbound address family IPv4 multicast eBGP peering sessions are cleared:

```
ciscoasa# clear bgp external ipv4 multicast out
```

In the following example, a soft reconfiguration is initiated for the inbound sessions for BGP neighbors in IPv4 unicast address family sessions in autonomous system 65400, and the outbound session is unaffected:

```
ciscoasa# clear bgp ipv4 unicast 65400 soft in
```

In the following example, a hard reset is initiated for BGP neighbors in IPv4 unicast address family sessions in the 4-byte autonomous system numbered 65538 in asplain notation:

```
ciscoasa# clear bgp ipv4 unicast 65538
```

In the following example, a hard reset is initiated for BGP neighbors in IPv4 unicast address family sessions in the 4-byte autonomous system numbered 1.2 in asdot notation:

```
ciscoasa# clear bgp ipv4 unicast 1.2
```

The following example clears the table map for IPv4 unicast peering sessions:

```
ciscoasa# clear bgp ipv4 unicast table-map
```

clear blocks

To reset the packet buffer counters such as the exhaustion condition and history information, use the **clear blocks** command in privileged EXEC mode.

clear blocks [**exhaustion** { **history** | **snapshot** } | **export-failed** | **queue** [**history** [**core-local** [*number*]]]]

Syntax Description

core-local [*number*]	(Optional) Clears system buffers queued by application for all cores, or if you specify the core number, a specific core.
exhaustion	(Optional) Clears the exhaustion condition.
export-failed	(Optional) Clears the export failed counters.
history	(Optional) Clears the history.
queue	(Optional) Clears queued blocks.
snapshot	(Optional) Clears the snapshot information.

Command Default

No default behavior or values.

Command History

Release	Modification
7.0(1)	This command was added.
9.1(5)	The **history** and **snapshot** options were added.

Usage Guidelines

Resets the low watermark counters to the current available blocks in each pool. Additionally, this command clears the history information stored during the last buffer allocation failure.

Examples

The following example clears the blocks:

```
ciscoasa# clear blocks
```

Related Commands

Command	Description
blocks	Increases the memory assigned to block diagnostics.
show blocks	Shows the system buffer utilization.

clear-button

To customize the Clear button of the WebVPN page login field that is displayed to WebVPN users when they connect to the ASA, use the **clear-button** command in customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

clear-button { **text** | **style** } *value*
no clear-button [{ **text** | **style** }] *value*

Syntax Description

style	Specifies you are changing the style.
text	Specifies you are changing the text.
value	The actual text to display or Cascading Style Sheet (CSS) parameters, each with a maximum of 256 characters allowed.

Command Default

The default text is “Clear”.

The default style is border:1px solid black;background-color:white;font-weight:bold;font-size:80%.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example changes the default background color of the Clear button from black to blue:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# clear-button style background-color:blue
```

Related Commands

Command	Description
group-prompt	Customizes the group prompt of the WebVPN page Login field.
login-button	Customizes the login button of the WebVPN page Login field.
login-title	Customizes the title of the WebVPN page Login field.
password-prompt	Customizes the password prompt of the WebVPN page Login field.
username-prompt	Customizes the username prompt of the WebVPN page Login field.

clear capture

To clear the capture buffer, use the **clear capture** command in privileged EXEC configuration mode.

clear capture { **/all** | *capture_name* }

Syntax Description

/all	Clears packets on all interfaces.
capture_name	Specifies the name of the packet capture.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The shortened form of the **clear capture** (for example, **cl cap** or **clear cap**) is n ot supported to prevent accidental destruction of all the packet captures.

Examples

This example shows how to clear the capture buffer for the capture buffer “example”:

```
ciscoasa
(config)#
clear capture example
```

Related Commands

Command	Description
capture	Enables packet capture capabilities for packet sniffing and network fault isolation.
show capture	Displays the capture configuration when no options are specified.

clear clns cache

To clear and reinitialize the Connectionless Network Service (CLNS) routing cache, use the clear clns cache EXEC command.

clear clns cache

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

To clear routing cache information, use the **clear clns cache** command.

Examples

The following example clears CLNS routing cache:

```
ciscoasa# clear clns cache
```

Related Commands

Command	Description
show clns cache	Shows clns routing cache.

clear clns is-neighbors

To remove IS neighbor information from the adjacency database, use the clear clns is-neighbors EXEC command.

clear clns is-neighbors

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

To clear IS neighbor information from the adjacency database, use the **clear clns is-neighbors** command.

Examples

The following example clears CLNS es-neighbor:

```
ciscoasa# clear clns is-neighbors
```

Related Commands

Command	Description
clear clns neighbors	Removes clns neighbor information.
show clns is-neighbors	Shows clns is neighbor information.

clear clns neighbors

To remove CLNS neighbor information from the adjacency database, use the clear clns neighbors EXEC command.

clear clns neighbors

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

To clear neighbor information from the adjacency database, use the **clear clns neighbors** command.

Examples

The following example removes the CLNS neighbor information from the adjacency database:

```
ciscoasa# clear clns neighbors
```

Related Commands

Command	Description
clear clns is-neighbors	Removes clns is-neighbor information.
show clns neighbors	Shows clns neighbor information.

clear clns route

To remove all of the dynamically derived CLNS routing information, use the clear clns route EXEC command.

clear clns route

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

To clear routing information, use the **clear clns is-neighbors** command.

Examples

The following example removes all of the dynamically derived CLNS routing information:

```
ciscoasa# clear clns route
```

Related Commands

Command	Description
show clns route	Shows clns route information.

clear cluster info

To clear cluster statistics, use the **clear cluster info** command in privileged EXEC mode.

clear cluster info { **flow-mobility counters** | **health details** | **trace** | **transport** }

Syntax Description

flow-mobility counters	Clears the cluster flow-mobility counters.
health details	Clears cluster health information.
trace	Clears cluster event trace information.
transport	Clears cluster transport statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.5(2)	We introduced the **flow-mobility counters** keywords.
9.0(1)	This command was added.

Usage Guidelines

To view cluster statistics, use the **show cluster info** command.

Examples

The following example clears cluster event trace information:

```
ciscoasa# clear cluster info trace
```

Related Commands

Command	Description
show cluster info	Shows cluster statistics.

clear compression

To clear compression statistics for all SVC and WebVPN connections, use the **clear compression** command in privileged EXEC mode.

clear compression { **all** | **anyconnect-ssl** | **http-comp** }

Syntax Description

all	Clears all compressions statistics.
http-comp	Clears HTTP-COMP statistics.
anyconnect-ssl	Clears anyconnect-ssl compression statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.
8.4(1)	anyconnect-ssl replaced svc.
9.5(2)	Support for multiple context mode was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example, clears the compression configuration for the user:

```
hostname# clear configure compression
```

Related Commands

Command	Description
compression	Enables compression for all SVC and WebVPN connections.
svc compression	Enables compression of data over an SVC connection for a specific group or user.

clear configuration session

To delete a configuration session, use the **clear configuration session** command in global configuration mode.

clear configuration session [*session_name*]

Syntax Description

session_name	The name of an existing configuration session. Use the **show configuration session** command for a list of current sessions. If you omit this parameter, all existing sessions are deleted.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

Use this command in conjunction with the **configure session** command, which creates isolated sessions for editing ACLs and their objects. If you decide you no longer need a session you created, and you do not want to commit the changes defined in the session, use this command to remove the session and the changes it contains.

If you want to simply clear the changes made within a session without deleting the session, use the **clear session** command instead of this one.

Examples

The following example deletes the session named old-session:

```
ciscoasa(config)# clear configuration session old-session
```

Related Commands

Command	Description
clear session	Clears the contents of a configuration session or resets its access flag.
configure session	Creates or opens a session.
show configuration session	Shows the changes made in each current session.

clear configure

To clear the running configuration, use the **clear configure** command in global configuration mode.

clear configure { **primary** | **secondary** | **all** | *command* }

Syntax Description

all	Clears the entire running configuration.
command	Clears the configuration for a specified command. For available commands, use the **clear configure ?** command for CLI help.
primary	For a failover pair, clears the primary unit configuration.
secondary	For a failover pair, clears the secondary unit configuration.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When you enter this command in a security context, you clear only the context configuration. If you enter this command in the system execution space, you clear the system running configuration as well as all context running configurations. Because you cleared all context entries in the system configuration (see the **context** command), the contexts are no longer running, and you cannot change to a context execution space.

Before clearing the configuration, make sure you save any changes to the **boot config** command (which specifies the startup configuration location) to the startup configuration; if you changed the startup configuration location only in the running configuration, then when you restart, the configuration loads from the default location.

If you clear an object that is being used in another command, such as an access list, the object is emptied but not removed. After you remove the object from all commands that refer to it, you can use the no form of the object or object-group commands to delete the object.

Note When you enter the **clear configure all** command, the master pass phrase used in password encryption is not removed. For more information about the master pass phrase, see the **config key password-encryption** command.

Examples

The following example clears the entire running configuration:

```
ciscoasa(config)# clear configure all
```

The following example clears the AAA configuration:

```
ciscoasa(config)# clear configure aaa
```

Related Commands

Command	Description
show running-config	Shows the running configuration.

clear conn

To clear a specific connection or multiple connections, use the clear **conn** command in privileged EXEC mode.

clear conn [**all**] [**tcp | udp** | **sctp** }] [**address** *src_ip*] [- *src_ip*] [**netmask** *mask*]] [**port** *src_port* [- *src_port*]] [**address** *dest_ip* [- *dest_ip*] [**netmask** *mask*]] [**port** *dest_port* [- *dest_port*] [**user** [*domain_nickname*\ ] *user_name* | **user-group** [*domain_nickname*\\ ] *user_group_name*] | **zone** [*zone_name*]] [**data-rate**]

Syntax Description

address	(Optional) Clears connections with the specified source or destination IP address.
all	(Optional) Clears all connections, including to-the-box connections. Without the **all** keyword, only through-the-box connections are cleared.
dest_ip	(Optional) Specifies the destination IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-). For example: `10.1.1.1-10.1.1.5`
dest_port	(Optional) Specifies the destination port number. To specify a range, separate the port numbers with a dash (-). For example: `1000-2000`
netmask *mask*	(Optional) Specifies a subnet mask for use with the given IP address.
port	(Optional) Clears connections with the specified source or destination port.
protocol {tcp | udp | **sctp}**	(Optional) Clears connections with the specified protocol.
src_ip	(Optional) Specifies the source IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-). For example: `10.1.1.1-10.1.1.5`
src_port	(Optional) Specifies the source port number. To specify a range, separate the port numbers with a dash (-). For example: `1000-2000`
user [*domain_nickname* \ ] *user_name*	(Optional) Clears connections that belong to the specified user. When you do not include the *domain_nickname* argument, the ASA clears connections for the user in the default domain.
user-group [*domain_nickname* \\ ] *user_group_name*	(Optional) Clears connections that belong to the specified user group. When you do not include the *domain_nickname* argument, the ASA clears connections for the user group in the default domain.
zone [*zone_name*]	Clears connections that belong to a traffic zone.

data-rate	(Optional) Clears the current maximum data-rate stored.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(8)/7.2(4)/8.0(4)	This command was added.
8.4(2)	Added the **user** and **user-group** keywords to support the Identity Firewall.
9.3(2)	The **zone** keyword was added.
9.5(2)	The **protocol sctp** keyword was added.
9.14(1)	The **data-rate** keyword was added.

Usage Guidelines

This command supports IPv4 and IPv6 addresses.

When you make security policy changes to the configuration, all *new* connections use the new security policy. Existing connections continue to use the policy that was configured at the time of the connection establishment. To ensure that all connections use the new policy, you need to disconnect the current connections so they can reconnect using the new policy using the **clear conn** command. You can alternatively use the **clear local-host** command to clear connections per host, or the **clear xlate** command for connections that use dynamic NAT.

When the ASA creates a pinhole to allow secondary connections, this is shown as an incomplete connection in the **show conn** command output. To clear this incomplete connection, use the **clear conn** command.

Examples

The following example shows how to view all connections and then clear the management connection between 10.10.10.108:4168 and 10.0.8.112:22:

```
ciscoasa# show conn all
TCP mgmt 10.10.10.108:4168 NP Identity Ifc 10.0.8.112:22, idle 0:00:00, bytes 3084, flags
UOB
ciscoasa# clear conn address 10.10.10.108 port 4168 address 10.0.8.112 port 22
```

The following example shows how to clear connection maximum data-rate stored in the extension memory:

```
ciscoasa# clear conn data-rate
Released conn extension memory for 10 connection(s)
```

Related Commands

Commands	Description
clear local-host	Clears all connections by a specific local host or all local hosts.
clear xlate	Clears a dynamic NAT session, and any connections using NAT.
show conn	Shows connection information.
show local-host	Displays the network states of local hosts.
show xlate	Shows NAT sessions.

clear console-output

To remove the currently captured console output, use the **clear console-output** command in privileged EXEC mode.

clear console-output

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to remove the currently captured console output:

```
ciscoasa# clear console-output
```

Related Commands

Command	Description
console timeout	Sets the idle timeout for a console connection to the ASA.
show console-output	Displays the captured console output.
show running-config console timeout	Displays the idle timeout for a console connection to the ASA.

clear coredump

To clear the coredump log, use the clear coredump command in global configuration mode.

clear coredump

Syntax Description

This command has no arguments or keywords.

Command Default

By default, coredumps are not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Note For ASAs that are operating on 4100/9300 platforms, use the bootstrap CLI mode for working with coredumps.

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

This command removes the coredump file system contents and the coredump log. The coredump file system remains intact. The current coredump configuration remains unchanged.

Examples

The following example removes the coredump file system contents and the coredump log:

```
ciscoasa(config)# clear coredump
Proceed with removing the contents of the coredump filesystem on 'disk0:' [confirm]
```

Related Commands

Command	Description
coredump enable	Enables the coredump feature.
clear configure coredump	Removes the coredump file system and its contents from your system.
show coredump filesystem	Displays files on the coredump filesystem.
show coredump log	Shows the coredump log.

clear counters

To clear the protocol stack counters, use the **clear counters** command in global configuration mode.

clear counters [**all** | **context** *context-name* | **summary** | **top** *n*] [**detail**] [**protocol** *protocol_name* | *counter_name*]] [**threshold** *n*]

Syntax Description

all	(Optional) Clears all filter details.
context *context-name*	(Optional) Specifies the context name.
counter_name	(Optional) Specifies a counter by name. Use the **show counters protocol** command to see which counters are available.
detail	(Optional) Clears detailed counters information.
protocol *protocol_name*	(Optional) Clears the counters for the specified protocol.
summary	(Optional) Clears the counter summary.
threshold *n*	(Optional) Clears the counters at or above the specified threshold. The range is 1 through 4294967295.
top *n*	(Optional) Clears the counters at or above the specified threshold. The range is 1 through 4294967295.

Command Default

The **clear counters summary detail** command is the default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to clear the protocol stack counters:

```
ciscoasa(config)# clear counters
```

Related Commands

Command	Description
show counters	Displays the protocol stack counters.

clear cpu profile

To clear the CPU profiling statistics, use the **clear cpu profile** command in privileged EXEC mode.

clear cpu profile

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to delete the crash file:

```
ciscoasa# clear cpu profile
```

Related Commands

show cpu	Displays information about the CPU.
show cpu profile	Displays CPU profiling data.

clear crashinfo

To delete all the crash information files stored in flash memory, use the **clear crashinfo** command in privileged EXEC mode.

clear crashinfo [**module** { **0** | **1** }]

Syntax Description

module {**0** | **1**}	(Optional) Clears the crash file for a module in slot 0 or 1.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	The output was updated to delete all the crashinfo files that are written to flash memory.

Examples

The following example shows how to delete the crash file:

```
ciscoasa# clear crashinfo
```

Related Commands

crashinfo force	Forces a crash of the ASA.
crashinfo save disable	Disables crash information from writing to flash memory.
crashinfo test	Tests the ability of the ASA to save crash information to a file in flash memory.
show crashinfo	Displays the contents of the latest crash information file stored in flash memory.
show crashinfo files	Displays the last five crash information files based on the date and timestamp.

clear crypto accelerator statistics

To clear the the global and accelerator-specific statistics from the crypto accelerator MIB, use the **clear crypto accelerator statistics** command in privileged EXEC mode.

clear crypto accelerator statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the mode in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example entered in global configuration mode, displays crypto accelerator statistics:

```
ciscoasa(config)# clear crypto accelerator statistics
ciscoasa(config)#
```

Related Commands

Command	Description
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto accelerator statistics	Displays the global and accelerator-specific statistics in the crypto accelerator MIB.
show crypto protocol statistics	Displays the protocol-specific statistics from the crypto accelerator MIB.

clear crypto ca crls

To empty the CRL cache of all CRLs associated with a specified trustpoint, all CRLs associated with the trustpool from the cache, or the CRL cache of all CRLs, use the **clear crypto ca crls** command in privileged EXEC mode.

clear crypto ca crls [**trustpoool** | **trustpoint** *trust_point_name*]

Syntax Description

trustpoint *trust_point_name*	The name of a trustpoint. If you do not specify a name, this command clears all CRLs cached on the system. If you give the trustpoint keyword without a *trust_point_name* , the command fails.
trustpool	Indicates that the action should be applied only to the CRLs that are associated with certificates in the trustpool.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Examples

The following independent examples issued in privileged EXEC configuration mode clear all of the trustpool CRLs, clears all of the CRLs associated with trustpoint123, and removes all of the cached CRLs from the ASA:

```
ciscoasa# clear crypto ca crl trustpool
ciscoasa# clear crypto ca crl trustpoint trustpoint123
ciscoasa# clear crypto ca crl
```

Related Commands

Command	Description
crypto ca crl request	Downloads the CRL based on the CRL configuration of the trustpoint.
show crypto ca crl	Displays all cached CRLs or CRLs cached for a specified trustpoint.

clear crypto ca trustpool

To remove all certificates from the trustpool, use the **clear crypto ca trustpool** command in privileged EXEC mode.

clear crypto ca trustpool [**noconfirm**]

Syntax Description

noconfirm	(Optional) Suppresses user confirmation prompts, and the command will be processes as requested.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes		—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The user is asked to confirm this action before carrying it out.

Examples

The following example clears all certificates:

```
ciscoasa# clear crypto ca trustpool
You are about to clear the trusted certificate pool. Do you want to continue? (y/n) y
ciscoasa#
```

Related Commands

Command	Description
crypto ca trustpool export	Exports the certificates that constitute the PKI trustpool.
crypto ca trustpool import	Imports the certificates that constitute the PKI trustpool.
crypto ca trustpool remove	Removes a single specified certificate from the trustpool.

clear crypto ikev1

To remove the IPsec IKEv1 SAs or statistics, use the **clear crypto ikev1** command in privileged EXEC mode. To clear all IKEv1 SAs, use this command without arguments.

clear crypto ikev1 { **sa** *ip_address* | **stats** }

Syntax Description

sa **ip_address**	Clears the SA.
stats	Clears the IKEv1 statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

To clear all IPsec IKEv1 SAs, use this command without arguments.

Examples

The following example removes all of the IPsec IKEv1 statistics from the ASA:

```
ciscoasa# clear crypto ikev1 stats
ciscoasa#
```

The following example deletes SAs with a peer IP address of 10.86.1.1:

```
ciscoasa# clear crypto ikev1 sa peer 10.86.1.1
ciscoasa#
```

Related Commands

Command	Description
clear configure crypto map	Clears all or specified crypto maps from the configuration.

Command	Description
clear configure isakmp	Clears all ISAKMP policy configuration.
show ipsec sa	Displays information about IPSec SAs, including counters, entry, map name, peer IP address and hostname.
show running-config crypto	Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.

clear crypto ikev2

To remove the IPsec IKEv2 SAs or statistics, use the **clear crypto ikev2** command in privileged EXEC mode. To clear all IKEv2 SAs, use this command without arguments.

clear crypto ikev2 { **sa** *ip_address* | **stats** }

Syntax Description

sa **ip_address**	Clears the SA.
stats	Clears the IKEv2 statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

To clear all IPsec IKEv2 SAs, use this command without arguments.

Examples

The following example removes all of the IPsec IKEv2 statistics from the ASA:

```
ciscoasa# clear crypto ikev2 stats
ciscoasa#
```

The following example deletes SAs with a peer IP address of 10.86.1.1:

```
ciscoasa# clear crypto ikev2 sa peer 10.86.1.1
ciscoasa#
```

Related Commands

Command	Description
clear configure crypto map	Clears all or specified crypto maps from the configuration.

Command	Description
clear configure isakmp	Clears all ISAKMP policy configuration.
show ipsec sa	Displays information about IPsec SAs, including counters, entry, map name, peer IP address and hostname.
show running-config crypto	Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.

clear crypto ipsec sa

To remove the IPsec SA counters, entries, crypto maps or peer connections, use the **clear crypto ipsec sa** command in privileged EXEC mode. To clear all IPsec SAs, use this command without arguments.

clear crypto ipsec sa [**counters** | **entry** *ip_address* { **esp** | **ah** } *spi* | **map** *map name* | **peer** *ip_address*]

Syntax Description

ah	Authentication header.
counters	Clears all IPsec per SA statistics.
entry *ip_address*	Deletes the tunnel that matches the specified IP address/hostname, protocol, and SPI value.
esp	Encryption security protocol.
map *map name*	Deletes all tunnels associated with the specified crypto map as identified by map name.
peer *ip_address*	Deletes all IPsec SAs to a peer as identified by the specified hostname or IP address.
spi	Identifies the Security Parameters Index (a hexidecimal number). This must be the inbound SPI. We do not support this command for the outbound SPI.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

To clear all IPsec SAs, use this command without arguments.

Examples

The following example removes all of the IPsec SAs from the ASA:

```
ciscoasa# clear crypto ipsec sa
ciscoasa#
```

The following example deletes SAs with a peer IP address of 10.86.1.1:

```
ciscoasa# clear crypto ipsec peer 10.86.1.1
```

ciscoasa#

Related Commands

Command	Description
clear configure crypto map	Clears all or specified crypto maps from the configuration.
clear configure isakmp	Clears all ISAKMP policy configuration.
show ipsec sa	Displays information about IPsec SAs, including counters, entry, map name, peer IP address and hostname.
show running-config crypto	Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.

clear crypto ipsec stats

To remove the global IPsec statistics and reset the statistics, use the **clear crypto ipsec stats** command in privileged EXEC mode.

clear crypto ipsec stats

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.16(1)	This command was added.

Usage Guidelines

To clear all the global IPsec statistics, use this command without arguments.

Examples

The following example removes and resets the the IPsec statistics in the ASA:

```
ciscoasa# clear crypto ipsec stats
ciscoasa#
```

Related Commands

Command	Description
clear configure crypto map	Clears all or specified crypto maps from the configuration.
show ipsec stats	Displays information about IPsec SAs, including counters, entry, map name, peer IP address and hostname.
show running-config crypto	Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.

clear crypto isakmp

To clear ISAKMP SAs or statistics, use the **clear crypto isakmp** command in privileged EXEC mode.

clear crypto isakmp [**sa** | **stats**]

Syntax Description

sa	Clears IKEv1 and IKEv2 SAs.
stats	Clears IKEv1 and IKEv2 statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

To clear all ISAKMP operational data, use this command without arguments.

Examples

The following example removes all of the ISAKMP SAs:

```
ciscoasa# clear crypto isakmp sa
ciscoasa#
```

Related Commands

Command	Description
clear configure crypto map	Clears all or specified crypto maps from the configuration.
clear configure isakmp	Clears all ISAKMP policy configuration.
show isakmp	Displays information about ISAKMP operational data.
show running-config crypto	Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.

clear crypto protocol statistics

To clear the protocol-specific statistics in the crypto accelerator MIB, use the **clear crypto protocol statistics** command in privileged EXEC mode.

clear crypto protocol statistics *protocol*

Syntax Description

protocol Specifies the name of the protocol for which you want to clear statistics. Protocol choices are as follows:

- **all**—All protocols currently supported.
- **ikev1**—Internet Key Exchange (IKE) version 1.
- **ikev2**—Internet Key Exchange (IKE) version 2.
- **ipsec-client**—IP Security (IPsec) Phase-2 protocols.
- **other**—Reserved for new protocols.
- srtp—Secure RTP (SRTP) protocol
- ssh—Secure Shell (SSH) protocol
- ssl-client— Secure Socket Layer (SSL) protocol.

Command Default

No default behavior or values.

Command Modes

The following table shows the mode in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.4(1)	The **ikev1** and ikev2 keywords were added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example clears all crypto accelerator statistics:

```
ciscoasa# clear crypto protocol statistics all
ciscoasa#
```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
show crypto accelerator statistics	Displays the global and accelerator-specific statistics from the crypto accelerator MIB.
show crypto protocol statistics	Displays the protocol-specific statistics in the crypto accelerator MIB.

clear crypto ssl

To clear SSL information, use the **clear crypto ssl** command in privileged EXEC mode.

clear crypto ssl { **cache** [**all**] | **errors** | **mib** | **objects** }

Syntax Description

cache	Clears expired sessions in the SSL session cache.
all	(Optional) Clears all sessions and statistics in the SSL session cache.
errors	Clears SSL errors.
mib	Clears SSL MIB statistics.
objects	Clears SSL object statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the mode in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example clears all SSL cache sessions and statistics:

```
ciscoasa# clear crypto ssl cache all
ciscoasa#
```

Related Commands

Command	Description
show crypto ssl	Displays the SSL information.

clear cts

To clear data used by the ASA when integrated with Cisco TrustSec, use the **clear cts** command in global configuration mode:

clear cts { **environment-data** | **pac** } [**noconfirm**]

Syntax Description

noconfirm	Clears the data without asking for confirmation.
environment-data	Clears all CTS environment data downloaded from Cisco ISE.
pac	Clears the CTS PAC information stored in NVRAM.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

If you clear the environment data, you can trigger the next environment data refresh manually or the system will refresh the data when the refresh timer expires. Clearing environment data does not remove the Cisco TrustSec PAC from the system, but it does impact traffic policy.

Before clearing the stored PAC, please understand that without a PAC, the system cannot download Cisco TrustSec environment data. However, environment data that is already on the system remains in use. Running the **clear cts pac** command renders the system unable to retrieve environment data updates.

In a cluster, you can use this command on the master unit only. In active/standby high-availability (failover), you can use it on the active unit only.

Examples

The following examples show how to clear CTS data from the system.

```
ciscoasa# clear cts pac
Are you sure you want to delete the cts PAC? (y/n) y

ciscoasa# clear cts environment-data
Are you sure you want to delete the cts environment data? (y/n) y
```

Related Commands

Command	Description
clear configure cts	Clears the configuration for integrating the ASA with Cisco TrustSec.
cts sxp enable	Enables the SXP protocol on the ASA.
show cts	Displays Cisco Trustsec (CTS) information.

clear dhcpd

To clear the DHCP server bindings and statistics, use the **clear dhcp** command in privileged EXEC mode.

clear dhcpd { **binding** [**all** | *ip_address*] | **statistics** }

Syntax Description

all	(Optional) Clears all dhcpd bindings.
binding	Clears all the client address bindings.
ip_address	(Optional) Clears the binding for the specified IP address.
statistics	Clears statistical information counters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you include the optional IP address in the **clear dhcpd binding** command, only the binding for that IP address is cleared.

To clear all of the DHCP server commands, use the **clear configure dhcpd** command.

Examples

The following example shows how to clear the **dhcpd** statistics:

```
ciscoasa# clear dhcpd statistics
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show dhcpd	Displays DHCP binding, statistic, or state information.

clear dhcprelay statistics

To clear the DHCP relay statistic counters, use the **clear dhcprelay statistics** command in privileged EXEC mode.

clear dhcprelay statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **clear dhcprelay statistics** command only clears the DHCP relay statistic counters. To clear the entire DHCP relay configuration, use the **clear configure dhcprelay** command.

Examples

The following example shows how to clear the DHCP relay statistics:

```
ciscoasa# clear dhcprelay statistics
ciscoasa#
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
debug dhcprelay	Displays debugging information for the DHCP relay agent.
show dhcprelay statistics	Displays DHCP relay agent statistic information.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

clear dns

To clear IP addresses associated with fully qualified domain name (FQDN) hosts, use the **clear dns** command in privileged EXEC mode.

clear dns [**host** *fqdn_name* | **ip-cache** [**counters**]]

Syntax Description

host *fqdn_name*	(Optional) Specifies the fully qualified domain name of the host whose addresses should be cleared.
ip-cache [**counters**]	Clear the IP cache that is used to hold domain name resolutions for network-service objects. Once removed, domains in network-service objects will not be matched until client DNS resolution requests are resolved and snooped to rebuild the cache. Include the **counters** keyword to simply reset the hit counts for the domains and leave the IP cache in place.

Command Default

Without parameters, all DNS resolutions are cleared for hosts used in access control rules. For domain names used in network-service objects, the counters are cleared, but the IP cache is not removed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.
9.17(1)	The **ip-cache** keyword was added.

Examples

The following example clears the IP address associated with the specified FQDN host used in an FQDN network object:

```
ciscoasa# clear dns host www.example.com
```

Note The setting of the **dns expire-entry** keyword is ignored when resolutions are cleared. New DNS queries are sent for each activated FQDN host specified in an FQDN network object.

The following example clears hit counts for domains used in network-service objects.

```
ciscoasa# clear dns ip-cache counters
```

Related Commands

Command	Description
dns domain-lookup	Enables the ASA to perform a name lookup.
dns name-server	Configures a DNS server address.
show dns ip-cache	Shows the DNS resolution IP cache used for network-service objects.
show dns-hosts	Shows the DNS cache.

clear dns-hosts cache

To clear the DNS cache, use the **clear dns-hosts cache** command in privileged EXEC mode.

clear dns-hosts cache

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command does not clear static entries that you added with the name command.

Examples

The following example clears the DNS cache:

```
ciscoasa# clear dns-hosts cache
```

Related Commands

Command	Description
dns domain-lookup	Enables the ASA to perform a name lookup.
dns name-server	Configures a DNS server address.
dns retries	Specifies the number of times to retry the list of DNS servers when the ASA does not receive a response.
dns timeout	Specifies the amount of time to wait before trying the next DNS server.
show dns-hosts	Shows the DNS cache.

clear dynamic-filter dns-snoop

To clear Botnet Traffic Filter DNS snooping data, use the **clear dynamic-filter dns-snoop** command in in privileged EXEC mode.

clear dynamic-filter dns-snoop

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Examples

The following example clears all Botnet Traffic Filter DNS snooping data:

```
ciscoasa# clear dynamic-filter
 dns-snoop
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.

Command	Description
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

clear dynamic-filter reports

To clear report data for the Botnet Traffic Filter, use the **clear dynamic-filter reports** command in privileged EXEC mode.

clear dynamic-filter reports { **top** [**malware-sites** | **malware-ports** | **infected-hosts**] | **infected-hosts** }

Syntax Description

malware-ports	(Optional) Clears report data for the top 10 malware ports.
malware-sites	(Optional) Clears report data for the top 10 malware sites.
infected-hosts (**top**)	(Optional) Clears report data for the top 10 infected hosts.
top	Clears report data for the top 10 malware sites, ports, and infected hosts.
infected-hosts	Clears report data for infected hosts.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.2(1)	This command was added.
8.2(2)	The **botnet-sites** and **botnet-ports** keywords were changed to **malware-sites** and **malware-ports**. The **top** keyword was added to differentiate clearing the top 10 reports and the new infected-hosts reports. The **infected-hosts** keyword was added (without **top**).

Examples

The following example clears all Botnet Traffic Filter top 10 report data:

```
ciscoasa# clear dynamic-filter
 reports top
```

The following example clears only the top 10 malware sites report data:

```
ciscoasa# clear dynamic-filter
 reports top malware-sites
```

The following example clears all infected hosts report data:

```
ciscoasa# clear dynamic-filter
 reports infected-hosts
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.

Command	Description
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports infected-hosts	Generates reports of infected hosts.
show dynamic-filter reports top	Generates reports of the top 10 malware sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

clear dynamic-filter statistics

To clear Botnet Traffic Filter statistics, use the **clear dynamic-filter statistics** command in in privileged EXEC mode.

clear dynamic-filter statistics [**interface** *name*]

Syntax Description

interface *name*	(Optional) Clears statistics for a particular interface.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Examples

The following example clears all Botnet Traffic Filter DNS statistics:

```
ciscoasa# clear dynamic-filter
 statistics
```

Related Commands

Command	Description
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.

Command	Description
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports infected-hosts	Generates reports of infected hosts.
show dynamic-filter reports top	Generates reports of the top 10 malware sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

clear eigrp events

To clear the EIGRP event log, use the **clear eigrp events** command in privileged EXEC mode.

clear eigrp [*as-number*] **events**

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are clearing the event log. Because the ASA only supports one EIGRP routing process, you do not need to specify the autonomous system number (process ID).

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

You can use the **show eigrp events** command to view the EIGRP event log.

Examples

The following example clears the EIGRP event log:

```
ciscoasa# clear eigrp events
```

Related Commands

Command	Description
show eigrp events	Displays the EIGRP event log.

clear eigrp neighbors

To delete entries from the EIGRP neighbor table, use the **clear eigrp neighbors** command in privileged EXEC mode.

clear eigrp [*as-number*] **neighbors** [*ip-addr* | *if-name*] [**soft**]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are deleting neighbor entries. Because the ASA only supports one EIGRP routing process, you do not need to specify the autonomous system number (AS), which is the process ID.
if-name	(Optional) The name of an interface as specified by the **nameif** command. Specifying an interface name removes all neighbor table entries that were learned through this interface.
ip-addr	(Optional) The IP address of the neighbor you want to remove from the neighbor table.
soft	Causes the ASA to resynchronize with the neighbor without resetting the adjacency.

Command Default

If you do not specify a neighbor IP address or an interface name, all dynamic entries are removed from the neighbor table.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **clear eigrp neighbors** command does not remove neighbors defined using the **neighbor** command from the neighbor table. Only dynamically discovered neighbors are removed.

You can use the **show eigrp neighbors** command to view the EIGRP neighbor table.

Examples

The following example removes all entries from the EIGRP neighbor table:

```
ciscoasa# clear eigrp neighbors
```

The following example removes all entries learned through the interface named “outside” from the EIGRP neighbor table:

```
ciscoasa# clear eigrp neighbors outside
```

Related Commands

Command	Description
debug eigrp neighbors	Displays debugging information for EIGRP neighbors.
debug ip eigrp	Displays debugging information for EIGRP protocol packets.
show eigrp neighbors	Displays the EIGRP neighbor table.

clear eigrp topology

To delete entries from the EIGRP topology table, use the **clear eigrp topology** command in privileged EXEC mode.

clear eigrp [*as-number*] **topology** *ip-addr* [*mask*]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process. Because the ASA only supports one EIGRP routing process, you do not need to specify the autonomous system number (AS), which is the process ID.
ip-addr	The IP address to clear from the topology table.
mask	(Optional) The network mask to apply to the *ip-addr* argument.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command clears existing EIGRP entries from the EIGRP topology table. You can use the **show eigrp topology** command to view the topology table entries.

Examples

The following example removes entries in the 192.168.1.0 network from EIGRP topology table:

```
ciscoasa# clear eigrp topology 192.168.1.0 255.255.255.0
```

Related Commands

Command	Description
show eigrp topology	Displays the EIGRP topology table.

clear facility-alarm output

To de-energize the output relay and clear the alarm state of the LED in the ISA 3000, use the **clear facility-alarm output** command in privileged EXEC mode.

clear facility-alarm output

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

This command de-energizes the output relay and clears the alarm state of the output LED. This turns off the external alarm. However, this command does not fix the alarm condition that triggered the external alarm: you still must resolve the problem. Use the **show facility-alarm status** command to determine the current alarm conditions.

Examples

The following example de-energizes the output relay and clears the alarm state of the output LED:

```
ciscoasa(config)# clear facility-alarm output
```

Related Commands

Command	Description
alarm contact description	Specifies the description for the alarm inputs.
alarm contact severity	Specifies the severity of alarms.
alarm contact trigger	Specifies a trigger for one or all alarm inputs.
alarm facility input-alarm	Specifies the logging and notification options for alarm inputs.
alarm facility power-supply rps	Configures the power supply alarms.

Command	Description
alarm facility temperature	Configures the temperature alarms.
alarm facility temperature (high and low thresholds)	Configures the low or high temperature threshold value.
show alarm settings	Displays all global alarm settings.
show environment alarm-contact	Displays all external alarm settings.
show facility-alarm relay	Displays relay in activated state.
show facility-alarm status	Displays all triggered alarms, or alarms based on severity specified.

clear failover statistics

To clear the failover statistic counters, use the **clear failover statistics** command in privileged EXEC mode.

clear failover statistics [**np-clients** | **cp-clients**]

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.20(2)	The **np-clients** and **cp-clients** keywords were added.

Usage Guidelines

This command clears the statistics displayed with the **show failover statistics** command and the counters in the Stateful Failover Logical Update Statistics section of the **show failover** command output. The **np-clients** and **cp-clients** keywords clears the data plane and control plane statistics of HA clients displayed in the **show failover statistics bulk-sync** commnad.

To remove the failover configuration, use the **clear configure failover** command.

Examples

The following example shows how to clear the failover statistic counters:

```
ciscoasa# clear failover statistics
ciscoasa#
```

Related Commands

Command	Description
debug fover	Displays failover debugging information.
show failover	Displays information about the failover configuration and operational statistics.

clear flow-export counters

To reset runtime counters for NetFlow statistical and error data to zero, use the **clear flow-export counters** command in privileged EXEC mode.

clear flow-export counters

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.1(1)	This command was added.

Examples

The following example shows how to reset NetFlow runtime counters:

```
ciscoasa# clear flow-export counters
```

Related Commands

Commands	Description
flow-export destination	Specifies the IP address or hostname of the NetFlow collector, and the UDP port on which the NetFlow collector is listening.
flow-export template timeout-rate	Controls the interval at which the template information is sent to the NetFlow collector.
logging flow-export-syslogs enable	Enables syslog messages after you have entered the **logging flow-export-syslogs disable** command, and the syslog messages that are associated with NetFlow data.
show flow-export counters	Displays all NetFlow runtime counters.

clear flow-offload

To clear off-loaded flow statistics or off-loaded flows, use the **clear flow-offload** command in privileged EXEC mode.

clear flow-offload { **statistics** | **flow all** }

Syntax Description

statistics	Clear statistics for off-loaded flows.
flow all	Clear all off-loaded flows.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was introduced.

Usage Guidelines

The **clear flow-offload statistics** command resets statistics for off-loaded flows to zero.

If you use **clear flow-offload flow all** to remove off-loaded flows, subsequent packets for these flows would go to the ASA. The ASA would then off-load the flows again. Overall statistics for the flows that you cleared would not be correct. This command is meant for debugging purposes only.

Examples

The following example clears statistics:

```
ciscoasa# clear flow-offload statistics
```

Related Commands

Commands	Description
flow-offload	Enables flow off-load.
set-connection advanced-options flow-offload	Identifies traffic flows as eligible for off-load.
show flow-offload	Displays information about flow off-loading.

clear flow-offload-ipsec

To clear information related to IPsec flow offload, use the **clear flow-offload-ipsec** command in privileged EXEC mode.

clear flow-offload-ipsec statistics

Syntax Description

statistics	Clear statistics related to IPsec flow offload.

Command Default

All statistics are cleared.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.18(1)	This command was introduced.

Example

The following example clears all IPsec flow offload statistics.

```
ciscoasa# clear flow-offload-ipsec statistics
```

Related Commands

Command	Description
flow-offload-ipsec	Configures IPsec flow offload.
show flow-offload-ipsec	Displays IPsec flow offload statistics and information.

clear fragment

To clear the operational data of the IP fragment reassembly module, enter the **clear fragment** command in privileged EXEC mode.

clear fragment { **queue** | **statistics** [*interface_name*] }

Syntax Description

interface_name	(Optional) Specifies the ASA interface.
queue	Clears the IP fragment reassembly queue.
statistics	Clears the IP fragment reassembly statistics.

Command Default

If an *interface_name* is not specified, the command applies to all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	The command was separated into two commands, **clear fragment** and **clear configure fragment**, to separate clearing of the configuration data from the operational data.

Usage Guidelines

This command clears either the currently queued fragments that are waiting for reassembly (if the **queue** keyword is entered) or clears all IP fragment reassembly statistics (if the **statistics** keyword is entered). The statistics are the counters, which tell how many fragments chains were successfully reassembled, how many chains failed to be reassembled, and how many times the maximum size was crossed resulting in overflow of the buffer.

Examples

The following example shows how to clear the operational data of the IP fragment reassembly module:

```
ciscoasa# clear fragment queue
```

Related Commands

Command	Description
clear configure fragment	Clears the IP fragment reassembly configuration and resets the defaults.
fragment	Provides additional management of packet fragmentation and improves compatibility with the NFS.

Command	Description
show fragment	Displays the operational data of the IP fragment reassembly module.
show running-config fragment	Displays the IP fragment reassembly configuration.

clear gc

To remove the garbage collection (GC) process statistics, use the **clear** gc command in privileged EXEC mode.

clear gc

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to remove the GC process statistics:

```
ciscoasa# clear gc
```

Related Commands

Command	Description
show gc	Displays the GC process statistics.

clear igmp counters

To clear all IGMP counters, use the **clear igmp counters** command in privileged EXEC mode.

clear igmp counters [*if_name*]

Syntax Description

if_name	The interface name, as specified by the **nameif** command. Including an interface name with this command causes only the counters for the specified interface to be cleared.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example clears the IGMP statistical counters:

```
ciscoasa# clear igmp counters
```

Related Commands

Command	Description
clear igmp group	Clears discovered groups from the IGMP group cache.
clear igmp traffic	Clears the IGMP traffic counters.

clear igmp group

To clear discovered groups from the IGMP group cache, use the **clear igmp** command in privileged EXEC mode.

clear igmp group [*group* | **interface** *name*]

Syntax Description

group	IGMP group address. Specifying a particular group removes the specified group from the cache.
interface *name*	Interface name, as specified by the **namif** command. When specified, all groups associated with the interface are removed.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you do not specify a group or an interface, all groups are cleared from all interfaces. If you specify a group, only the entries for that group are cleared. If you specify an interface, then all groups on that interface are cleared. If you specify both a group and an interface, only the specified groups on the specified interface are cleared.

This command does not clear statically configured groups.

Examples

The following example shows how to clear all discovered IGMP groups from the IGMP group cache:

```
ciscoasa# clear igmp group
```

Related Commands

Command	Description
clear igmp counters	Clears all IGMP counters.
clear igmp traffic	Clears the IGMP traffic counters.

clear igmp traffic

To clear the IGMP traffic counters, use the **clear igmp traffic** command in privileged EXEC mode.

clear igmp traffic

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example clears the IGMP statistical traffic counters:

```
ciscoasa# clear igmp traffic
```

Related Commands

Command	Description
clear igmp group	Clears discovered groups from the IGMP group cache.
clear igmp counters	Clears all IGMP counters.

clear ikev1

To remove the IPsec IKEv1 SAs or statistics, use the **clear ikev1** command in privileged EXEC mode. To clear all IKEv1 SAs, use this command without arguments.

clear ikev1 { **sa** *ip_address* | **stats** }

Syntax Description

sa **ip_address**	Clears the SA.
stats	Clears the IKEv1 statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

To clear all IPsec IKEv1 SAs, use this command without arguments.

Examples

The following example removes all of the IPsec IKEv1 statistics from the ASA:

```
ciscoasa# clear ikev1 stats
ciscoasa#
```

The following example deletes SAs with a peer IP address of 10.86.1.1:

```
ciscoasa# clear ikev1 sa peer 10.86.1.1
```

ciscoasa#

Related Commands

Command	Description
clear configure crypto map	Clears all or specified crypto maps from the configuration.

Command	Description
clear configure isakmp	Clears all ISAKMP policy configuration.
show ipsec sa	Displays information about IPSec SAs, including counters, entry, map name, peer IP address and hostname.
show running-config crypto	Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.

clear ikev2

To remove the IPsec IKEv2 SAs or statistics, use the **clear ikev2** command in privileged EXEC mode. To clear all IKEv2 SAs, use this command without arguments.

clear ikev2 { **sa** *ip_address* | **stats** }

Syntax Description

sa **ip_address**	Clears the SA.
stats	Clears the IKEv2 statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

To clear all IPsec IKEv2 SAs, use this command without arguments.

Examples

The following example removes all of the IPsec IKEv2 statistics from the ASA:

```
ciscoasa# clear ikev2 stats
ciscoasa#
```

The following example deletes SAs with a peer IP address of 10.86.1.1:

```
ciscoasa# clear ikev2 sa peer 10.86.1.1
```

ciscoasa#

Related Commands

Command	Description
clear configure crypto map	Clears all or specified crypto maps from the configuration.

Command	Description
clear configure isakmp	Clears all ISAKMP policy configuration.
show ipsec sa	Displays information about IPsec SAs, including counters, entry, map name, peer IP address and hostname.
show running-config crypto	Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.

clear interface

To clear interface statistics, use the **clear interface** command in privileged EXEC mode.

clear interface [*physical_interface* [**.** *subinterface*] | *mapped_name* | *interface_name*]

Syntax Description

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Command Default

By default, this command clears all interface statistics.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If an interface is shared among contexts, and you enter this command within a context, the ASA clears only statistics for the current context. If you enter this command in the system execution space, the ASA clears the combined statistics.

You cannot use the interface name in the system execution space, because the **nameif** command is only available within a context. Similarly, if you mapped the interface ID to a mapped name using the **allocate-interface** command, you can only use the mapped name in a context.

Examples

The following example clears all interface statistics:

```
ciscoasa# clear interface
```

Related Commands

Command	Description
clear configure interface	Clears the interface configuration.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show running-config interface	Displays the interface configuration.

clear ip audit count

To clear the count of signature matches for an audit policy, use the **clear ip audit count** command in privileged EXEC mode.

clear ip audit count [**global** | **interface** *interface_name*]

Syntax Description

global	(Default) Clears the number of matches for all interfaces.
interface *interface_name*	(Optional) Clears the number of matches for the specified interface.

Command Default

If you do not specify a keyword, this command clears the matches for all interfaces (**global**).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example clears the count for all interfaces:

```
ciscoasa# clear ip audit count
```

Related Commands

Command	Description
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
show ip audit count	Shows the count of signature matches for an audit policy.
show running-config ip audit attack	Shows the configuration for the **ip audit attack** command.

clear ipsec sa

To clear IPsec SAs entirely or based on specified parameters, use the **clear ipsec sa** command in privileged EXEC mode.

clear ipsec sa [**counters** | **entry** *peer-addr protocol spi* | **peer** *peer-addr* | **map** *map-name*]

Syntax Description

counters	(Optional) Clears all counters.
entry	(Optional) Clears IPsec SAs for a specified IPsec peer, protocol and SPI.
inactive	(Optional) Clears IPsec SAs that are unable to pass traffic.
map*map-name*	(Optional) Clears IPsec SAs for the specified crypto map.
peer	(Optional) Clears IPsec SAs for a specified peer.
peer-addr	Specifies the IP address of an IPsec peer.
protocol	Specifies an IPsec protocol: **esp** or **ah**
spi	Specifies an IPsec SPI.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

You can also use an alternate form of this command to perform the same function: **clear crypto ipsec sa**.

Examples

The following example, entered in global configuration mode, clears all IPsec SA counters:

```
ciscoasa# clear ipsec sa counters
ciscoasa#
```

Related Commands

Command	Description
show ipsec sa	Displays IPsec SAs based on specified parameters.
show ipsec stats	Displays global IPsec statistics from the IPsec flow MIB.

clear ipsec stats

To clear IPsec statistics and reset the statstics, use the **clear ipsec stats** command in privileged EXEC mode.

clear ipsec stats

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.16(1)	This command was added.

Usage Guidelines

You can also use an alternate form of this command to perform the same function: **clear crypto ipsec stats**.

Examples

The following example, entered in global configuration mode, clears all IPsec statistics:

```
ciscoasa# clear ipsec stats
ciscoasa#
```

Related Commands

Command	Description
show ipsec sa	Displays IPsec SAs based on specified parameters.
show ipsec stats	Displays global IPsec statistics from the IPsec flow MIB.

clear ipv6 access-list counters (Deprecated)

To clear the IPv6 access list statistical counters, use the **clear ipv6 access-list counters** command in privileged EXEC mode.

clear ipv6 access-list *id* **counters**

Syntax Description

id	The IPv6 access list identifier.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	This command was deprecated.

Examples

The following example shows how to clear the statistical data for the IPv6 access list 2:

```
ciscoasa# clear ipv6 access-list 2 counters
ciscoasa#
```

Related Commands

Command	Description
clear configure ipv6	Clears the **ipv6 access-list** commands from the current configuration.
ipv6 access-list	Configures an IPv6 access list.
show ipv6 access-list	Displays the **ipv6 access-list** commands in the current configuration.

clear ipv6 dhcprelay

To clear the IPv6 DHCP relay binding entries and statistics, use the **clear ipv6 dhcprelay** command in privileged EXEC mode.

clear ipv6 dhcprelay { **binding** [*ip_address*] | **statistics** }

Syntax Description

binding	Clears the IPv6 DHCP relay binding entries.
ip_address	(Optional) Specifies the IPv6 address for the DHCP relay binding. If the IP address is specified, only the relay binding entries associated with that IP address are cleared.
statistics	Clears the IPv6 DHCP relay agent statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Examples

The following example shows how to clear the statistical data for the IPv6 DHCP relay binding:

```
ciscoasa# clear ipv6 dhcprelay binding
ciscoasa#
```

Related Commands

Command	Description
show ipv6 dhcprelay binding	Shows the relay binding entries created by the relay agent.
show ipv6 dhcprelay statistics	Shows the IPv6 DHCP relay agent information.

clear ipv6 dhcp statistics

To clear DHCPv6 client and Prefix Delegation client statistics, use the **clear ipv6 dhcp client statistics** command in privileged EXEC mode.

clear ipv6 dhcp { **client** [**pd**] | **interface** *interface_name* | **server** } **statistics**

Syntax Description

client	Clears the DHCPv6 client statistics.
interface *interface_name*	Clears the DHCPv6 statistics for the specified interface.
pd	Clears the Prefix Delegation client statistics.
server	Clears the DHCPv6 server statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

This command clears DHCPv6 client statistics.

Examples

The following example clears the DHCPv6 client statistics:

```
ciscoasa# clear ipv6 dhcp client statistics
```

The following example clears the DHCPv6 Prefix Delegation client statistics:

```
ciscoasa# clear ipv6 dhcp client pd statistics
```

The following example clears statistics on the outside interface:

```
ciscoasa# clear ipv6 dhcp interface outside statistics
```

The following example clears DHCPv6 server statistics:

```
ciscoasa# clear ipv6 dhcp server statistics
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.

Command	Description
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

clear ipv6 eigrp

To remove IPv6 router configuration, use the **clear ipv6 eigrp** command

clear ipv6 eigrp

Syntax Description

ipv6_address	Neighbor address.
interface_name	Interface name.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• —	• Yes	• Yes	• —

Command History

Release	Modification
9.20(1)	This command was added.

Examples

```
ciscoasa# clear ipv6 eigrp
```

Related Commands

Command	Description
ipv6 eigrp	Enables EIGRP for IPv6 on an interface.
show ipv6 eigrp	Displays the EIGRP router configuration mode commands in the running configuration. Displays information about interfaces configured with IPv6 EIGRP.

clear ipv6 router eigrp

To remove IPv6 router configuration as well clear the routing process, use the **clear ipv6 router eigrp** command. This command will remove all the IPv6 route as well interface commands.

clear ipv6 router eigrp *as_number*

Syntax Description

as_number	The autonomous system number. This must be the same as the autonomous system number of your EIGRP routing process.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• —	• Yes	• Yes	• —

Command History

Release	Modification
9.20(1)	This command was added.

Examples

```
ciscoasa# clear ipv6 route eigrp 1
```

Related Commands

Command	Description
ipv6 eigrp	Enables EIGRP for IPv6 on an interface.
show ipv6 eigrp	Displays information about interfaces configured with IPv6 EIGRP.

clear ipv6 mld traffic

To clear the IPv6 Multicast Listener Discovery (MLD) traffic counters, use the **clear ipv6 mld traffic** command in privileged EXEC mode.

clear ipv6 mld traffic

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(4)	This command was added.

Usage Guidelines

The **clear ipv6 mld traffic** command allows you to reset all the MLD traffic counters.

Examples

The following example shows how to clear the traffic counters for IPv6 MLD:

```
ciscoasa# clear ipv6 mld traffic
ciscoasa#
```

Related Commands

Command	Description
debug ipv6 mld	Displays all debugging messages for MLD.
show debug ipv6 mld	Displays the MLD commands for IPv6 in the current configuration.

clear ipv6 neighbors

To clear the IPv6 neighbor discovery cache, use the **clear ipv6 neighbors** command in privileged EXEC mode.

clear ipv6 neighbors

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command deletes all discovered IPv6 neighbor from the cache; it does not remove static entries.

Examples

The following example deletes all entries, except static entries, in the IPv6 neighbor discovery cache:

```
ciscoasa# clear ipv6 neighbors
ciscoasa#
```

Related Commands

Command	Description
ipv6 neighbor	Configures a static entry in the IPv6 neighbor discovery cache.
show ipv6 neighbor	Displays IPv6 neighbor cache information.

clear ipv6 ospf

To clear OSPFv3 routing parameters, use the **clear ipv6 ospf** command in privileged EXEC mode.

clear ipv6 [*process_id*] [**counters**] [**events**] [**force-spf**] [**process**] [**redistribution**] [**traffic**]

Syntax Description

counters	Resets the OSPF process counters.
events	Clears the OSPF event log.
force-ospf	Clears the SPF for OSPF processes.
process	Resets the OSPFv3 process.
process_id	Clears the process ID number. Valid values range from 1 to 65535.
redistribution	Clears OSPFv3 route redistribution.
traffic	Clears traffic-related statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command removes all OSPFv3 routing parameters.

Examples

The following example shows how to clear all OSPFv3 route redistribution:

```
ciscoasa# clear ipv6 ospf
            redistribution
ciscoasa#
```

Related Commands

Command	Description
show running-config ipv6 router	Shows the running configuration of OSPFv3 processes.
clear configure ipv6 router	Clears OSPFv3 routing processes.

clear ipv6 prefix-list

To clear routing prefix-lists, use the **clear ipv6 prefix-list** command in privileged EXEC mode.

clear ipv6 prefix-list [*name*]

Syntax Description

name	Clears the named prefix-list created by the **ipv6 prefix-list** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

This command removes IPv6 prefix-lists.

Examples

The following example shows how to clear the list1 IPv6 prefix-list:

```
ciscoasa# clear ipv6 prefix-list list1
ciscoasa#
```

Related Commands

Command	Description
show running-config ipv6 prefix-list	Shows the running configuration of IPv6 prefix-lists.
clear configure ipv6 prefix-list	Clears the IPv6 prefix-lost configuration.

clear ipv6 route

To delete routes from the IPv6 routing table, use the clear ipv6 route command in privileged EXEC mode.

clear ipv6 route [**management-only**] { **all** | *ipv6-prefix / prefix-length* }

Syntax Description

management-only	Clears only the IPv6 management routing table.
ipv6-prefix/prefix-length	Clears routed for the IPv6 prefix.
all	Clears all IPv6 routes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

The **clear ipv6 route** command is similar to the **clear ip route** command, except that it is IPv6-specific. The per-destination maximum transmission unit (MTU) cache is also cleared.

Examples

The following example deletes the IPv6 route for 2001:0DB8::/35:

```
ciscoasa# clear ipv6 route 2001:0DB8::/35
```

Related Commands

Command	Description
show ipv6 route	Displays IPv6 routes.

clear ipv6 traffic

To reset the IPv6 traffic counters, use the **clear ipv6 traffic** command in privileged EXEC mode.

clear ipv6 traffic

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Using this command resets the counters in the output from the **show ipv6 traffic** command.

Examples

The following example resets the IPv6 traffic counters. The output from the **ipv6 traffic** command shows that the counters have been reset:

```
ciscoasa# clear ipv6 traffic
ciscoasa# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  1 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent
ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
```

```
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
  Sent: 1 output
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output
TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

Related Commands

Command	Description
show ipv6 traffic	Displays IPv6 traffic statistics.

clear ip verify statistics

To clear the unicast RPF statistics, use the **clear ip verify statistics** command in privileged EXEC mode.

clear ip verify statistics [**interface** *interface_name*]

Syntax Description

interface *interface_name*	Sets the interface on which you want to clear unicast RPF statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

See the ip verify reverse-path command to enable unicast RPF.

Examples

The following example clears the unicast RPF statistics:

```
ciscoasa# clear ip verify statistics
```

Related Commands

Command	Description
clear configure ip verify reverse-path	Clears the ip verify reverse-path configuration.
ip verify reverse-path	Enables the unicast RPF feature to prevent IP spoofing.
show ip verify statistics	Shows the unicast RPF statistics.
show running-config ip verify reverse-path	Shows the ip verify reverse-path configuration.

clear isakmp sa

To remove all of the IKEv1 and IKEv2 runtime SA database, use the **clear isakmp sa** command in privileged EXEC mode.

clear isakmp sa

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	The **clear isakmp sa** command was changed to **clear crypto isakmp sa**.
9.0(1)	Support for multiple context mode was added.

Examples

The following example removes the IKE runtime SA database from the configuration:

```
ciscoasa# clear isakmp sa
ciscoasa#
```

Related Commands

Command	Description
clear isakmp	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA.
show isakmp stats	Displays runtime statistics.
show isakmp sa	Displays IKE runtime SA database with additional information.
show running-config isakmp	Displays all the active ISAKMP configuration.

clear isis

To clear the IS-IS data structures, use the **clear isis** command.

clear isis { ***** | **lspfull** | **rib redistribution** [**level-1** | **level-2**] [*network_prefix*] [*network_mask*] }

Syntax Description

*****	Clears all IS-IS data structures.
level-1	(Optional) Clears Level 1 IS-IS redistributed prefixes from the redistribution cache.
level-2	(Optional) Clears Level 2 IS-IS redistributed prefixes from the redistribution cache.
lspfull	Clears the IS-IS LSPFULL state.
network_mask	(Optional) The network ID in the A.B.C.D format for the network mask for the specific network prefix you want to clear from the RIB. If you do not provide a network mask for the prefix, the major net of the prefix will be used for the network mask.
network_prefix	(Optional) The network ID in the A.B.C.D format for the specific network prefix you want to clear from the redistribution Routing Information Base (RIB). If you do not provide a network mask for the prefix, the major net of the prefix will be used for the network mask.
rib redistribution	Clears prefixes in the IS-IS redistribution cache.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

If the link-state PDU (LSP) becomes full because too many routes are redistributed, use the **clear isis lspfull** command to clear the state after the problem has been resolved.

We recommend that you use the **clear isis rib** command in a troubleshooting situation only when a Cisco Technical Assistance Center representative requests you to do so following a software error.

Examples

The following example clears the LSPFULL state:

```
ciscoasa# clear isis lspfull
```

The following example clears the network prefix 10.1.0.0 from the IP local redistribution cache:

```
ciscoasa# clear isis rib redistribution 10.1.0.0 255.255.0.0
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.

Command	Description
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).

Command	Description
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.