clear l – clear z

clear lisp eid

To clear the ASA EID table, use the **clear lisp eid** command in privileged EXEC mode.

clear lisp eid [*ip_address*]

Syntax Description

ip_address	Removes the specified IP address from the EID table.

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)	We introduced this command.

Usage Guidelines

The ASA maintains an EID table that correlates the EID and the site ID. The **clear lisp eid** command clears EID entries in the table.

About LISP Inspection for Cluster Flow Mobility

The ASA inspects LISP traffic for location changes and then uses this information for seamless clustering operation. With LISP integration, the ASA cluster members can inspect LISP traffic passing between the first hop router and the ETR or ITR, and can then change the flow owner to be at the new site.

Cluster flow mobility includes several inter-related configurations:

1. (Optional) Limit inspected EIDs based on the host or server IP address—The first hop router might send EID-notify messages for hosts or networks the ASA cluster is not involved with, so you can limit the EIDs to only those servers or networks relevant to your cluster. For example, if the cluster is only involved with 2 sites, but LISP is running on 3 sites, you should only include EIDs for the 2 sites involved with the cluster. See the **policy-map type inspect lisp**, **allowed-eid,** and **validate-key** commands.
2. LISP traffic inspection—The ASA inspects LISP traffic for the EID-notify message sent between the first hop router and the ITR or ETR. The ASA maintains an EID table that correlates the EID and the site ID. For example, you should inspect LISP traffic with a source IP address of the first hop router and a destination address of the ITR or ETR. See the **inspect lisp** command.
3. Service Policy to enable flow mobility on specified traffic—You should enable flow mobility on business-critical traffic. For example, you can limit flow mobility to only HTTPS traffic, and/or to traffic to specific servers. See the **cluster flow-mobility lisp** command.

4. Site IDs—The ASA uses the site ID for each cluster unit to determine the new owner. See the **site-id** command.
5. Cluster-level configuration to enable flow mobility—You must also enable flow mobility at the cluster level. This on/off toggle lets you easily enable or disable flow mobility for a particular class of traffic or applications. See the **flow-mobility lisp** command.

Related Commands

Command	Description
allowed-eids	Limits inspected EIDs based on IP address.
clear cluster info flow-mobility counters	Clears the flow mobility counters.
clear lisp eid	Removes EIDs from the ASA EID table.
cluster flow-mobility lisp	Enables flow mobility for the service policy.
flow-mobility lisp	Enables flow mobility for the cluster.
inspect lisp	Inspects LISP traffic.
policy-map type inspect lisp	Customizes the LISP inspection.
site-id	Sets the site ID for a cluster chassis.
show asp table classify domain inspect-lisp	Shows the ASP table for LISP inspection.
show cluster info flow-mobility counters	Shows flow mobility counters.
show conn	Shows traffic subject to LISP flow-mobility.
show lisp eid	Shows the ASA EID table.
show service-policy	Shows the service policy.
validate-key	Enters the pre-shared key to validate LISP messages.

clear local-host (Deprecated)

To reinitialize per-client run-time states such as connection limits and embryonic limits, use the **clear local-host** command in privileged EXEC mode.

clear local-host [*ip_address*] [**all**] [**zone** [*zone_name*]]

Syntax Description

all	(Optional) Clears all connections, including to-the-box traffic. Without the **all** keyword, only through-the-box traffic is cleared.
ip_address	(Optional) Specifies the local host IP address.
zone [*zone_name*]	(Optional) Specifies zone connections.

Command Default

Clears all through-the-box run-time states.

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.
9.3(2)	The **zone** keyword was added.
9.16(1)	This command was deprecated. Use the **clear conn address** command to clear connections to local addresses.

Usage Guidelines

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 local-host** command. You can alternatively use the **clear conn** command for more granular connection clearing, or the **clear xlate** command for connections that use dynamic NAT.

The **clear local-host** command releases the hosts from the host license limit. You can see the number of hosts that are counted toward the license limit by entering the **show local-host** command.

Examples

The following example clears the run-time state and assocaited connections for the host 10.1.1.15:

```
ciscoasa# clear local-host 10.1.1.15
```

Related Commands

Command	Description
clear conn	Terminates connections in any state.
clear xlate	Clears a dynamic NAT session, and any connections using NAT.
show local-host	Displays the network states of local hosts.

clear logging asdm

To clear the ASDM logging buffer, use the **clear logging asdm** command in privileged EXEC mode.

clear logging asdm

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 changed from the **clear pdm logging** command to the **clear asdm log** command.

Usage Guidelines

ASDM system log messages are stored in a separate buffer from the ASA system log messages. Clearing the ASDM logging buffer only clears the ASDM system log messages; it does not clear the ASA system log messages. To view the ASDM system log messages, use the **show asdm log** command.

Examples

The following example clears the ASDM logging buffer:

```
ciscoasa(config)# clear logging asdm
ciscoasa(config)#
```

Related Commands

Command	Description
show asdm log_sessions	Displays the contents of the ASDM logging buffer.

clear logging buffer

To clear the log buffer, use the **clear logging buffer** command in privileged EXEC mode.

clear logging buffer

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

This example shows how to clear the contents of the log buffer:

```
ciscoasa
#
clear logging buffer
```

Related Commands

Command	Description
logging buffered	Configures the log buffer.
show logging	Displays logging information.

clear logging counter

To clear the logged counters and statistics, use the **clear logging counter** command in privileged EXEC mode.

clear logging counter { **all** | **console** | **monitor** | **buffer** | **trap** | **asdm** | **mail** }

Syntax Description

counter	Clears the counters and statistics for the specified logging destination. Specify **all** to clear statistics for all logging destinations. Optionally, you can specify the destination that you want to clear the statistics for—**console**, **monitor**, **buffer**, **trap**, **asdm**, **mail**.

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
9.14(1)	This command was added.

Usage Guidelines

The **show logging** command provides statistics of messages logged for each logging category configured on the ASA. In order to clear these statistics/counters, use the **clear logging counter** command.

Examples

This example shows how to clear the counters of the logged messages:

```
ciscoasa
#
clear logging counter all
```

Related Commands

Command	Description
show logging	Displays logging information.

clear logging queue bufferwrap

To clear the saved log buffers (ASDM, internal, FTP, and flash), use the **clear logging queue bufferwrap** command in privileged EXEC mode.

clear logging queue bufferwrap

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 shows how to clear the contents of the saved log buffers:

```
ciscoasa
#
clear logging queue bufferwrap
```

Related Commands

Command	Description
logging buffered	Configures the log buffer.
show logging	Displays logging information.

clear mac-address-table

To clear dynamic MAC address table entries, use the **clear mac-address-table** command in privileged EXEC mode.

clear mac-address-table [*interface_name*]

Syntax Description

interface_name	(Optional) Clears the MAC address table entries for the selected 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	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example clears the dynamic MAC address table entries:

```
ciscoasa# clear mac-address-table
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
firewall transparent	Sets the firewall mode to transparent.
mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.
mac-learn	Disables MAC address learning.
show mac-address-table	Shows MAC address table entries.

clear memory appcache-threshold

To clear the hit count of memory appcache-threshold, use the **clear memory appcache-threshold** command in privileged EXEC mode.

clear memory appcache-threshold

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
9.10(1)	This command was introduced.

Usage Guidelines

Whenever the application cache threshold is hit, the counter increments by 1. The **clear memory appcache-threshold** command clears the hit count of memory application cache threshold and resets to 0.

Examples

The following example clears the hit count of memory appcache-threshold:

```
ciscoasa# clear memory appcache-threshold
```

Related Commands

Command	Description
memory appcache-threshold enable	Enable memory appcache-threshold to restrict application cache allocations after reaching certain memory threshold
show memory appcache-threshold	Show the status and hit count of memory appcache-threshold

clear memory delayed-free-poisoner

To clear the delayed free-memory poisoner tool queue and statistics, use the **clear memory delayed-free-poisoner** command in privileged EXEC mode.

clear memory delayed-free-poisoner

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.

Usage Guidelines

The **clear memory delayed-free-poisoner** command returns all memory held in the delayed free-memory poisoner tool queue to the system without validation and clears the related statistical counters.

Examples

The following example clears the delayed free-memory poisoner tool queue and statistics:

```
ciscoasa# clear memory delayed-free-poisoner
```

Related Commands

Command	Description
memory delayed-free-poisoner enable	Enables the delayed free-memory poisoner tool.
memory delayed-free-poisoner validate	Forces validation of the delayed free-memory poisoner tool queue.
show memory delayed-free-poisoner	Displays a summary of the delayed free-memory poisoner tool queue usage.

clear memory profile

To clear the memory buffers held by the memory profiling function, use the **clear memory profile** command in privileged EXEC mode.

clear memory profile [**peak**]

Syntax Description

peak	(Optional) Clears the contents of the peak memory buffer.

Command Default

Clears the current "in use" profile buffer by 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
Privileged EXEC	• Yes	• Yes	—	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **clear memory profile** command releases the memory buffers held by the profiling function, and therefore requires that profiling stop before it is cleared.

Examples

The following example clears the memory buffers held by the profiling function:

```
ciscoasa# clear memory profile
```

Related Commands

Command	Description
memory profile enable	Enables the monitoring of memory usage (memory profiling).
memory profile text	Configures a text range of memory to profile.
show memory profile	Displays information about the memory usage (profiling) of the ASA.

clear mfib counters

To clear MFIB router packet counters, use the **clear mfib counters** command in privileged EXEC mode.

clear mfib counters [*group* [*source*]]

Syntax Description

group	(Optional) IP address of the multicast group.
source	(Optional) IP address of the multicast route source. This is a unicast IP address in four-part dotted-decimal notation.

Command Default

When this command is used with no arguments, route counters for all routes 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	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example clears all MFIB router packet counters:

```
ciscoasa# clear mfib counters
```

Related Commands

Command	Description
show mfib count	Displays MFIB route and packet count data.

clear module

To clear information about the SSM on the ASAs, information about the SSC on the ASA 5505, information about the SSP installed on the ASA 5585-X, information about the IPS SSP installed on the ASA 5585-X, information about the ASA Services Module, and system information, use the **clear module** command in privileged EXEC mode.

clear module [*mod_id* | *slot*] [**all** | [**details** | **recover** | **log** [**console**]]]

Syntax Description

all	(Default) Clears all SSM information.
console	(Optional) Clears console log information for the module.
details	(Optional) Clears additional information, including remote management configuration for SSMs (for example, ASA-SSM-*x* 0).
log	(Optional) Clears log information for the module.
mod_id	Clears the module name used for software modules, such as IPS.
recover	(Optional) For SSMs, clears the settings for the **hw-module module recover** command. **Note** The **recover** keyword is valid only when you have created a recovery configuration for the SSM by using the **configure** keyword with the **hw-module module recover** command. (Optional) For an IPS module installed on the ASA 5512-X, 5515-X, 5525-X, 5545-X, or 5555-X, clears the settings for the **sw-module module** *mod_id* **recover configure image** *image_location* command.
slot	Clears the module slot number, which can be 0 or 1.

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.
8.2(1)	Support for the SSC was added.

Release	Modification
8.2(5)	Support for the ASA 5585-X and the IPS SSP on the ASA 5585-X was added.
8.4(2)	Support for a dual SSP installation was added.
8.5(1)	Support for the ASASM was added.
8.6(1)	Support for the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X was added.

Usage Guidelines

This command clears information about the SSC, SSM, ASASM, IPS SSP, and device and built-in interfaces.

Examples

The following example clears the recovery settings for an SSM:

```
ciscoasa# clear module 1 recover
```

Related Commands

Command	Description
hw-module module recover	Recovers an SSM by loading a recovery image from a TFTP server.
hw-module module reset	Shuts down an SSM and performs a hardware reset.
hw-module module reload	Reloads the SSM software.
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

clear nac-policy

To reset NAC policy usage statistics, use the **clear nac-policy** command in global configuration mode.

clear nac-policy [*nac-policy-name*]

Syntax Description

nac-policy-name	(Optional) Name of the NAC policy for which to reset usage statistics.

Command Default

If you do not specify a name, the CLI resets the usage statistics for all NAC policies.

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
8.0(2)	This command was added.

Examples

The following example resets the usage statistics for the NAC policy named framework1:

```
ciscoasa
(config)#

clear nac-policy framework1
```

The following example resets all NAC policy usage statistics:

```
ciscoasa
(config)#

clear nac-policy
```

Related Commands

Command	Description
show nac-policy	Displays NAC policy usage statistics on the ASA.
show vpn-session_summary.db	Displays the number of IPsec, WebVPN, and NAC sessions.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

clear nat counters

To clear NAT policy counters, use the **clear nat counters** command in global configuration mode.

clear nat counters [*src_ifc* [*src_ip* [*src_mask*]] [*dst_ifc* [*dst_ip* [*dst_mask*]]]]

Syntax Description

dst_ifc	(Optional) Specifies destination interface to filter.
dst_ip	(Optional) Specifies destination IP address to filter.
dst_mask	(Optional) Specifies mask for destination IP address.
src_ifc	(Optional) Specifies source interface to filter.
src_ip	(Optional) Specifies source IP address to filter.
src_mask	(Optional) Specifies mask for source IP address.

Command Default

This command has no default settings.

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(4)	This command was added.

Examples

This example shows how to clear the NAT policy counters:

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

Related Commands

Command	Description
nat	Identifies addresses on one interface that are translated to mapped addresses on another interface.
nat-control	Enables or disables NAT configuration requirements.
show nat counters	Displays the protocol stack counters.

clear nve

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

clear nve 1

Syntax Description

1	Specifies the NVE instance, which is always 1.

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
9.4(1)	This command was added.

Usage Guidelines

This command clears the parameters, status and statistics of a NVE interface, status of its carrier interface, IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.

Examples

The following example clears the NVE interface statistics:

```
ciscoasa# clear nve 1
```

Related Commands

Command	Description
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.

clear object

To clear the hit counts of network-service objects, use the **clear object** command in privileged EXEC mode..

clear object [**id** *object_name* | **network-service**]

Syntax Description

id *name*	(Optional) Clear the counter of the specified network-service object. Capitalization matters. For example “object-name” does not match “Object-Name.”
network-service	(Optional.) Clear the counters of all network-service objects. This action is the same as you would get by specifying no parameters on the command.

Command Default

Without parameters, all objects hit counts 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
9.17(1)	This command was added.

Example

The following example clears the hit counts of all objects.

```
ciscoasa# clear object
```

Related Commands

Command	Description
show object	Shows network-service objects and their hit counts.

clear object-group

To clear the hit counts of objects in a network object group, use the **clear object-group** command in privileged EXEC mode.

clear object-group [*object_group_name*]

Syntax Description

object_group_name	The name of the object group whose counters should be cleared. If you do not specify a name, counters for all object groups are 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	• Yes	• Yes	—

Command History

Release	Modification
8.3(1)	This command was added.
9.17(1)	This command was extended to work with network-service objects.

Examples

The following example shows how to clear the network object hit count for the network object group named “Anet”:

```
ciscoasa# clear object-group Anet
```

Related Commands

Command	Description
show object-group	Shows object group information and hit counts.

clear ospf

To clear OSPF process information, use the **clear ospf** command in privileged EXEC mode.

clear ospf [*pid*] { **process counters** }

Syntax Description

counters	Clears the OSPF counters.
pid	(Optional) Internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535.
process	Restarts the OSPF routing process.

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

This command does not remove any part of the configuration. Use the **no** form of the configuration commands to clear specific commands from the configuration or use the **clear configure router ospf** command to remove all global OSPF commands from the configuration.

Note The **clear configure router ospf** command does not clear OSPF commands entered in interface configuration mode.

Examples

The following example shows how to clear the OSPF neighbor counters:

```
ciscoasa# clear ospf counters
```

Related Commands

Command	Description
clear configure router	Clears all global router commands from the running configuration.

clear path-monitoring

To clear path monitoring settings on the interface, use the **clear path-monitoring** command.

clear path-monitoring [**interface** *name*]

Syntax Description

Interface *name*	Removes the path-monitoring settings configured on the specified interface.

Command History

Release	Modification
9.18(1)	This command was introduced.

Examples

The following example clears the path monitoring settings on the *outside1* interface:

```
> clear path-montoring outside1
```

Related Commands

Command	Description
show path-monitoring	Shows path-monitoring metric information.

clear pclu

To clear PC logical update statistics, use the **clear pclu** command in privileged EXEC mode.

clear pclu

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 PC information:

```
ciscoasa# clear pclu
```

clear phone-proxy secure-phones

To clear the secure phone entries in the phone proxy database, use the **clear phone-proxy secure-phones** command in privileged EXEC mode.

clear phone-proxy secure-phones [*mac_address* | **noconfirm**]

Syntax Description

mac_address	Removes the IP phone from the phone proxy database with the specified MAC address.
noconfirm	Removes all the secure phone entries in the phone proxy database without prompting for confirmation. If you do not specify the **noconfirm** keyword, you are prompted to confirm whether to remove all the secure phone entries.

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
8.2(1)	This command was added.

Usage Guidelines

Because secure phones always request a CTL file upon bootup, the phone proxy creates a database that marks the phone as secure. The entries in the secure phone database are removed after a specified configured timeout (via the **timeout secure-phones** command). Alternatively, you can use the **clear phone-proxy secure-phones** command to clear the phone proxy database without waiting for the configured timeout.

Examples

The following example clears secure entries in the phone proxy database:

```
ciscoasa# clear phone-proxy secure-phones 001c.587a.4000
```

Related Commands

Command	Description
timeout secure-phones	Configures the idle timeout after which the secure phone entry is removed from the phone proxy database.

clear pim counters

To clear the PIM traffic counters, use the **clear pim counters** command in privileged EXEC mode.

clear pim 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	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command only clears the traffic counters. To clear the PIM topology table, use the **clear pim topology** command.

Examples

The following example clears the PIM traffic counters:

```
ciscoasa# clear pim counters
```

Related Commands

Command	Description
clear pim reset	Forces MRIB synchronization through reset.
clear pim topology	Clears the PIM topology table.
show pim traffic	Displays the PIM traffic counters.

clear pim group-map

To delete group-to-rendezvous point (RP) mapping entries from the RP mapping cache, use the clear pim group-map command.

clear pim group-map [*rp-address*]

Syntax Description

rp-address	Rendezvous point mapping address.

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
9.5(2)	This command was introduced.

Examples

The following example deletes group-RP mapping entries at the 23.23.23.2 RP address:

```
ciscoasa(config)# sh pim group-map
Group Range         Proto Client Groups RP address      Info

224.0.1.39/32*      DM    static 0      0.0.0.0
224.0.1.40/32*      DM    static 0      0.0.0.0
224.0.0.0/24*       L-Localstatic 1      0.0.0.0
232.0.0.0/8*        SSM   config 0      0.0.0.0
224.0.0.0/4*        SM    config 0      9.9.9.9         RPF: ,0.0.0.0
224.0.0.0/4         SM    BSR    0      23.23.23.2      RPF: Gi0/3,23.23.23.2
ciscoasa(config)# clear pim group-map 23.23.23.2
ciscoasa(config)# sh pim group-map
Group Range         Proto Client Groups RP address      Info

224.0.1.39/32*      DM    static 0      0.0.0.0
224.0.1.40/32*      DM    static 0      0.0.0.0
224.0.0.0/24*       L-Localstatic 1      0.0.0.0
232.0.0.0/8*        SSM   config 0      0.0.0.0
224.0.0.0/4*        SM    config 0      9.9.9.9         RPF: ,0.0.0.0
224.0.0.0/4         SM    static 0      0.0.0.0         RPF: ,0.0.0.0
```

Related Commands

Command	Description
clear pim counters	Clears PIM counters and statistics.
clear pim topology	Clears the PIM topology table.
clear pim counters	Clears PIM traffic counters.

clear pim reset

To force MRIB synchronization through reset, use the **clear pim reset** command in privileged EXEC mode.

clear pim reset

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.

Usage Guidelines

All information from the topology table is cleared, and the MRIB connection is reset. This command can be used to synchronize states between the PIM topology table and the MRIB database.

Examples

The following example clears the topology table and resets the MRIB connection:

```
ciscoasa# clear pim reset
```

Related Commands

Command	Description
clear pim counters	Clears PIM counters and statistics.
clear pim topology	Clears the PIM topology table.
clear pim counters	Clears PIM traffic counters.

clear pim topology

To clear the PIM topology table, use the **clear pim topology** command in privileged EXEC mode.

clear pim topology [*group*]

Syntax Description

group	(Optional) Specifies the multicast group address or name to be deleted from the topology table.

Command Default

Without the optional *group* argument, all entries are cleared from the topology 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	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command clears existing PIM routes from the PIM topology table. Information obtained from the MRIB table, such as IGMP local membership, is retained. If a multicast group is specified, only those group entries are cleared.

Examples

The following example clears the PIM topology table:

```
ciscoasa# clear pim topology
```

Related Commands

Command	Description
clear pim counters	Clears PIM counters and statistics.
clear pim reset	Forces MRIB synchronization through reset.
clear pim counters	Clears PIM traffic counters.

clear priority-queue statistics

To clear the priority-queue statistics counters for an interface or for all configured interfaces, use the **clear priority-queue statistics** command in either global configuration or privileged EXEC mode.

clear priority-queue statistics [*interface-name*]

Syntax Description

interface-name	(Optional) Specifies the name of the interface for which you want to show the best-effort and low-latency queue details.

Command Default

If you omit the interface name, this command clears the priority-queue statistics for all configured 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	—
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows the use of the **clear priority-queue statistics** command in privileged EXEC mode to remove the priority queue statistics for the interface named “test”:

```
ciscoasa# clear priority-queue statistics test
ciscoasa#
```

Related Commands

Command	Description
clear configure priority queue	Removes the priority-queue configuration from the named interface.
priority-queue	Configures priority queueing on an interface.
show priority-queue statistics	Shows the priority queue statistics for a specified interface or for all interfaces.
show running-config priority-queue	Shows the current priority-queue configuration on the named interface.

clear process

To clear statistics for specified processes running on the ASA, use the **clear process** command in privileged EXEC mode.

clear process [**cpu-hog** | **internals**]

Syntax Description

cpu-hog	Clears CPU hogging statistics.
internals	Clears process internal 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	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to clear CPU hogging statistics:

```
ciscoasa# clear process cpu-hog
ciscoasa#
```

Related Commands

Command	Description
cpu hog granular-detection	Triggers real-time CPU hog detection information.
show processes	Displays a list of the processes that are running on the ASA.

clear resource usage

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

clear resource usage [**context** *context_name* | **all** | **summary** | **system**] [**resource** { [**rate**] *resource_name* | **all** }]

Syntax Description

context *context_name*	(Multiple mode only) Specifies the context name for which you want to clear statistics. Specify **all** (the default) for all contexts.
resource [**rate**] *resource_name*	Clears the usage of a specific resource. Specify **all** (the default) for all resources. Specify **rate** to clear the rate of usage of a resource. Resources that are measured by rate include **conns**, **inspects**, and **syslogs**. You must specify the **rate** keyword with these resource types. The conns resource is also measured as concurrent connections; only use the **rate** keyword to view the connections per second. Resources include the following types: • **asdm**—ASDM management sessions. • **conns**—TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. • **inspects**—Application inspections. • **hosts**—Hosts that can connect through the ASA. • **mac-addresses**—For transparent firewall mode, the number of MAC addresses allowed in the MAC address table. • **ssh**—SSH sessions. • **syslogs**—Syslog messages. • **telnet**—Telnet sessions. • (Multiple mode only) **VPN Other**—Site-to-site VPN sessions. • (Multiple mode only) **VPN Burst Other**—Site-to-site VPN burst sessions. • **xlates**—NAT translations.
summary	(Multiple mode only) Clears the combined context statistics.
system	(Multiple mode only) Clears the system-wide (global) usage statistics.

Command Default

For multiple context mode, the default context is **all**, which clears resource usage for every context. For single mode, the context name is ignored and all resource statistics are cleared.

The default resource name is **all**, which clears all resource types.

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
7.2(1)	This command was added.

Examples

The following example clears all resource usage statistics for all contexts, but not the system-wide usage statistics:

```
ciscoasa# clear resource usage
```

The following example clears the system-wide usage statistics:

```
ciscoasa# clear resource usage system
```

Related Commands

Command	Description
context	Adds a security context.
show resource types	Shows a list of resource types.
show resource usage	Shows the resource usage of the ASA.

clear route

To remove dynamically learned routes from the routing table, use the **clear route** command in privileged EXEC mode.

clear route [**management-only**] [*ip_address* [*ip_mask*]]

Syntax Description

ip_address [*ip_mask*]	Specifies the destination IP address and, optionally, subnet mask of the route to be removed. If you omit this keyword, all dynamic routes are deleted.
management-only	Clears the IPv4 management routing table. If you omit this keyword, the route is removed from the data interface routing table.

Command Default

All dynamically learned routes are removed from the data interface routing 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	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.5(1)	The **management-only** keyword was added.
9.17(1)	Starting with version 9.17, for units that are part of a high availability group or cluster, this command is available on the active or control unit only. The command clears routes from all units in the HA group or cluster. In previous releases, the command clears routes on the unit on which it is run only.

Usage Guidelines

Use the **clear route** command to recover any missing routes. Whenever this command is executed, all routes from global RIB are deleted. All routes (dynamic or static) are pushed to global RIB by the respective modules (protocols).

On the other hand, when the best route is installed on the global RIB, the same is redistributed to peers and NP table. This process runs sequentially on multiple threads. The time taken to complete a cycle depends on the number of routes on the global RIB.

Thus, if you are using the **clear route** command consecutively, ensure to follow a minimum time interval of 30 seconds and a maximum time interval of 120 seconds. If this command is executed multiple times without following the recommended time interval, there is a chance of the distributed routes getting deleted, resulting in losing the routes from the RIB.

Examples

The following example shows how to remove all dynamically learned routes:

```
ciscoasa# clear route
```

The following example shows how to remove dynamically learned routes for a specific address.

```
ciscoasa# clear route 10.118.86.3
```

Related Commands

Command	Description
show route	Displays route information.
show running-config route	Displays configured routes.

clear service-policy

To clear operational data or statistics (if any) for enabled policies, use the **clear service-policy** command in privileged EXEC mode.

clear service-policy [**global** | **interface** *intf*] [**user-statistics**]

Syntax Description

global	(Optional) Clears the statistics of the global service policy.
interface *intf*	(Optional) Clears the service policy statistics of a specific interface.
user-statistics	(Optional) Clears the global counters for user statistics but does not clear the per-user statistics. Per-user or per-user-group statistics can still be seen using **show user-identity statistics** command. When the **accounting** keyword for the **user-statistics** command is specified, all global counters for sent packets, received packets, and sent dropped packets are cleared. When the **scanning** keyword **user-statistics** command is specified, the global counter for sent dropped packets is cleared. For the ASA to collect these user statistics, you must configure a policy map to collect user statistics. See the **user-statistics** command in this guide.

Command Default

By default, this command clears all the statistics for all enabled service policies.

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

Some inspection engines let you selectively clear statistics. See the **clear service-policy inspect** commands.

Examples

The following example shows how to clear service policy statistics for the outside interface.

```
ciscoasa# clear service-policy interface outside
```

Related Commands

Command	Description
clear service-policy inspect gtp	Clears service policy statistics for the GTP inspection engine.
clear service-policy inspect radius-accounting	Clears service policy statistics for the RADIUS accounting inspection engine.
show service-policy	Displays the service policy.
show running-config service-policy	Displays the service policies configured in the running configuration.
clear configure service-policy	Clears service policy configurations.
service-policy	Configures service policies.

clear service-policy inspect gtp

To clear GTP inspection statistics, use the **clear service-policy inspect gtp** command in privileged EXEC mode.

clear service-policy inspect gtp { **pdp-context** { **all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num* } | **requests** [*name* | **map** *name* | **version** *version_num*] | **statistics** [**gsn** *IP_address* | *IP_address*] }

Syntax Description

pdp-context { **all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num* }	Clears Packet Data Protocol (PDP) or bearer context information. You can specify the contexts to clear using the following keywords: • **all** —Clear all contexts. • **apn** *ap_name* —Clear contexts for the specified access point name. • **imsi** *IMSI_value* —Clear contexts for the specified IMSI hexadecimal number. • **ms-addr** *IP_address* —Clear contexts for the specified mobile subscriber (MS) IP address. • **tid** *tunnel_ID* —Clear contexts for the specified GTP tunnel ID, a hexadecimal number. • **version** *version_num* —Clear contexts for the specified GTP version (0-255).
requests [*name* | **map** *name* | **version** *version_num*	Clears GTP requests. You can optionally limit the requests to clear using the following parameters: • *name* —Clears requests associated with the specified GTP inspection policy map. This option is not available starting with 9.5(1). • **map** *name* —(9.5(1)+.) Clears requests associated with the specified GTP inspection policy map. • **version** *version_num* —(9.5(1)+.) Clears requests for the specified GTP version (0-255).
statistics [**gsn** *IP_address* | *IP_address*]	Clears GTP statistics for the **inspect gtp** command. You can clear the statistics for a specific endpoint by specifying the endpoint's address on the **gsn** keyword. Starting with 9.5(1), specify the address only, do not include the **gsn** keyword.

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.
9.5(1)	The following changes were made: • The **gsn** keyword on the **statistics** option was removed. To clear statistics for an endpoint, simply specify the endpoint IP address. • The **version** keyword was added to the **requests** option. The **map** keyword was added for the policy map name, replacing the ability to enter the map name directly after the **requests** option. • Support for IPv6 addresses.

Usage Guidelines

Use this command to clear statistics from GTP inspection. Use the **show** version of this command to view the statistics.

Examples

The following example clears GTP statistics:

```
ciscoasa# clear service-policy inspect gtp statistics
```

Related Commands

Commands	Description
inspect gtp	Enables GTP inspection.
show service-policy inspect gtp	Displays GTP statistics.

clear service-policy inspect m3ua

To clear M3UA inspection statistics, use the **clear service-policy inspect m3ua** command in privileged EXEC mode.

clear service-policy inspect m3ua { **drops** | **endpoint** [*ip_address*] | **session** [[**assocID** *hex_number*] }

Syntax Description

drops	Clears M3UA drop statistics.
endpoint [*ip_address*]	Clears M3UA endpoint statistics. You can optionally include the IP address of an endpoint to clear only the statistics for that endpoint.
session [**assocID** *hex_number*]	Clears all M3UA sessions, which are tracked if you enable strict application server process (ASP) state validation. If you want to clear a specific section, add the **assocID** keyword with the hexadecimal session number. Use the **show service-policy inspect m3ua session** command to see the current sessions and their association IDs.

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
9.6(2)	This command was added.
9.7(1)	The **session** keyword was added.

Usage Guidelines

Use this command to clear statistics or sessions from M3UA inspection. Use the **show** version of this command to view the statistics and sessions.

Examples

The following example clears M3UA endpoint statistics:

```
ciscoasa# clear service-policy inspect m3ua endpoint
```

The following example clears a specific M3UA session:

```
ciscoasa(config)# show service-policy inspect m3ua session

1 in use, 1 most used
Flags: d - double exchange      , s - single exchange
AssocID: c0bbe629 in Down state, idle:0:00:06, timeout:0:30:00, s
ciscoasa(config)# clear service-policy inspect m3ua session assocID c0bbe629
```

Related Commands

Commands	Description
inspect m3ua	Enables M3UA inspection.
show service-policy inspect m3ua	Displays the M3UA statistics.
strict-asp-state	Enables strict M3UA ASP state validation.

clear service-policy inspect radius-accounting

To clear RADIUS accounting users, use the **clear service-policy inspect radius-accounting** command in privileged EXEC mode.

clear service-policy inspect radius-accounting users { **all** | *ip_address* | *policy_map* }

Syntax Description

all	Clears all users.
ip_address	Clears a user with this IP address.
policy_map	Clears users associated with this policy map.

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
7.2(1)	This command was added.

Examples

The following example clears all RADIUS accounting users:

```
ciscoasa# clear service-policy inspect radius-accounting users all
```

clear session

To delete the contents of a configuration session or to reset its access flag, use the **clear session** command in global configuration mode.

clear session *session_name* { **access** | **configuration** }

Syntax Description

session_name	The name of an existing configuration session. Use the **show configuration session** command for a list of current sessions.
access	Clears the access flag. The flag indicates that a session is being edited. Clear this flag only if you know the edit session was abandoned and you need to get into the session to complete the changes.
configuration	Clears the configuration changes made within the session without deleting the session.

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.

The primary use of this command is to reset the access flag. When you open a session, the flag marks it as being edited. If you then break your connection to the ASA without cleanly exiting the session, the flag stays set, and this can prevent you from opening the session again. If you are certain no one is actually editing the session, you can reset the flag to regain access.

You can also use this command to empty the session of changes without deleting the session. 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 the **clear configuration session** command to delete the session and the changes it contains.

Examples

The following example resets the access flag on my-session:

```
ciscoasa(config)# clear session my-session access
```

Related Commands

Command	Description
clear configuration session	Deletes a configuration session and its contents.
configure session	Creates or opens a session.
show configuration session	Shows the changes made in each current session.

clear shared license

To reset shared license statistics, shared license client statistics, and shared license backup server statistics to zero, use the **clear shared license** command in privileged EXEC mode.

clear shared license [**all** | **backup** | **client** [*hostname*]]

Syntax Description

all	(Optional) Clears all statistics. This is the default setting.
backup	(Optional) Clears statistics for the backup server.
client	(Optional) Clears statistics for all participants.
hostname	(Optional) Clears statistics for a particular participant.

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
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The shared license counters include statistical data as well as error data.

Examples

The following example shows how to reset all shared license counters:

```
ciscoasa# clear shared license all
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.

Command	Description
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

clear shun

To disable all the shuns that are currently enabled and clear the shun statistics, use the **clear shun** command in privileged EXEC mode.

clear shun [*statistics*]

Syntax Description

statistics	(Optional) Clears the interface counters only.

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 shows how to disable all the shuns that are currently enabled and clear the shun statistics:

```
ciscoasa(config)# clear shun
```

Related Commands

Command	Description
shun	Enables a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection.
show shun	Displays the shun information.

clear snmp-server statistics

To clear SNMP server statistics (SNMP packet input and output counters), use the **clear snmp-server statistics** command in privileged EXEC mode.

clear snmp-server 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 shows how to clear SNMP server statistics:

```
ciscoasa
#
clear snmp-server statistics
```

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP server configuration.
show snmp-server statistics	Displays SNMP server configuration information.

clear ssl

To clear SSL information for debugging purposes, use the **clear ssl** command in privileged EXEC mode.

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

Syntax Description

all	Clears all sessions and statistics in SSL session cache.
cache	Clears expired sessions in 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 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(1)	This command was added.
9.5(2)	Support for multiple context mode was added.

Usage Guidelines

DTLS cache is never cleared because it would impact Secure Client functionality.

Examples

The following example shows clearing ssl cache and clearing all sessions and statistics in SSL session cache.

```
ciscoasa# clear ssl cache
SSL session cache cleared: 2
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared
ciscoasa# clear ssl cache all
Clearing all sessions and statistics
SSL session cache cleared: 5
No SSL VPNLB session cache
```

```
No SSLDEV session cache
DLTS caches are not cleared
```

clear startup-config errors

To clear configuration error messages from memory, use the **clear startup-config errors** command in privileged EXEC mode.

clear startup-config errors

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.

Usage Guidelines

To view configuration errors generated when the ASA loaded the startup configuration, use the **show startup-config errors** command.

Examples

The following example clears all configuration errors from memory:

```
ciscoasa# clear startup-config errors
```

Related Commands

Command	Description
show startup-config errors	Shows configuration errors generated when the ASA loaded the startup configuration.

clear sunrpc-server active

To clear the pinholes opened by Sun RPC application inspection, use the **clear sunrpc-server active** command in privileged EXEC mode.

clear sunrpc-server active

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 the **clear sunrpc-server active** command to clear the pinholes opened by Sun RPC application inspection that allow service traffic, such as NFS or NIS, to pass through the ASA.

Examples

The following example shows how to clear the SunRPC services table:

```
ciscoasa# clear
 sunrpc-server
```

Related Commands

Command	Description
clear configure sunrpc-server	Clears the Sun remote processor call services from the ASA.
inspect sunrpc	Enables or disables Sun RPC application inspection and configures the port used.
show running-config sunrpc-server	Displays information about the SunRPC services configuration.
show sunrpc-server active	Displays information about active Sun RPC services.

clear terminal

To clear the terminal settings for the current CLI session and use the defaults, use the **clear terminal** command in privileged EXEC mode.

clear terminal { **interactive** | **pager** [[**lines**] *number*] }

Syntax Description

interactive	Clears the interactive help setting (when you enter **?** at the CLI). The default is enabled.
pager [[**lines**] *number*]]	Clears the setting for the number of lines in a page before the ---more--- prompt appears. The default is 24.

Command Default

The default terminal behavior is:

- **interactive**—Enabled
- **pager**—24 lines

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 clear the pager setting:

```
ciscoasa# clear
 terminal pager
```

Related Commands

Command	Description
terminal pager	Sets the number of lines on a page before the “---More---” prompt appears.
terminal interactive	Enables or disables help when you enter ? at the CLI.

clear threat-detection rate

To clear statistics when you enable basic threat detection using the **threat-detection basic-threat** command, use the **clear threat detection rate** command in privileged EXEC mode.

clear threat-detection rate

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
8.0(2)	This command was added.

Examples

The following example clears the rate statistics:

```
ciscoasa# clear threat-detection rate
```

Related Commands

Command	Description
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
show threat-detection rate	Shows basic threat detection statistics.
threat-detection basic-threat	Enables basic threat detection.
threat-detection rate	Sets the threat detection rate limits per event type.
threat-detection scanning-threat	Enables scanning threat detection.

clear threat-detection scanning-threat

To clear the attackers and targets after you enable scanning threat detection with the **threat-detection scanning-threat** command, use the **clear threat-detection scanning-threat** command in privileged EXEC mode.

clear threat-detection scanning-threat [**attacker** [*ip_address* [*mask*]] | **target** [*ip_address* [*mask*]]

Syntax Description

attacker	(Optional) Clears only attackers.
ip_address	(Optional) Clears a specific IP address.
mask	(Optional) Sets the subnet mask.
target	(Optional) Clears only targets.

Command Default

If you do not specify an IP address, all hosts are released.

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.

Usage Guidelines

To view current attackers and targets, use the **show threat-detection scanning-threat** command.

Examples

The following example shows targets and attackers with the **show threat-detection scanning-threat** command, and then clears all targets:

```
ciscoasa# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0
    192.168.1.249
   Latest Attacker Host & Subnet List:
    192.168.10.234
    192.168.10.0
    192.168.10.2
    192.168.10.3
    192.168.10.4
```

```
    192.168.10.5
    192.168.10.6
    192.168.10.7
    192.168.10.8
    192.168.10.9
ciscoasa# clear threat-detection scanning-threat target
```

Related Commands

Command	Description
show threat-detection shun	Shows currently shunned hosts.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection scanning-threat	Enables scanning threat detection.

clear threat-detection shun

To release the currently shunned hosts after you enable scanning threat detection with the **threat-detection scanning-threat** command and automatically shunning attacking hosts, use the **clear threat-detection shun** command in privileged EXEC mode.

clear threat-detection shun [*ip_address* [*mask*]]

Syntax Description

ip_address	(Optional) Releases a specific IP address from being shunned. The address can be IPv4 or IPv6 (with optional prefix length).
mask	(Optional) Sets the subnet mask for the shunned host IP address.

Command Default

If you do not specify an IP address, all hosts are released.

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.
9.20(1)	Support for IPv6 addresses was added.

Usage Guidelines

To view currently shunned hosts, use the **show threat-detection shun** command.

Examples

The following example views currently shunned hosts with the **show threat-detection shun** command, and then releases host 10.1.1.6 from being shunned:

```
ciscoasa# show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
ciscoasa# clear threat-detection shun 10.1.1.6 255.255.255.255
```

Related Commands

Command	Description
show threat-detection shun	Shows currently shunned hosts.

Command	Description
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection scanning-threat	Enables scanning threat detection.

clear threat-detection statistics

To clear the statistics after you enable TCP Intercept statistics with the **threat-detection statistics tcp-intercept** command, use the **clear threat-detection scanning-threat** command in privileged EXEC mode.

clear threat-detection statistics [**tcp-intercept**]

Syntax Description

tcp-intercept	(Optional) Clears TCP Intercept statistics.

Command Default

Clears TCP Intercept 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	—	—

Command History

Release	Modification
8.0(4)	This command was added.

Usage Guidelines

To view TCP Intercept statistics, enter the **show threat-detection statistics top** command.

Examples

The following example shows TCP Intercept statistics with the **show threat-detection statistics top tcp-intercept** command, and then clears all statistics:

```
ciscoasa# show threat-detection statistics top tcp-intercept
Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
ciscoasa# clear threat-detection statistics
```

Related Commands

Command	Description
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection statistics	Enables threat detection statistics.

clear traffic

To reset the counters for transmit and receive activity, use the **clear traffic** command in privileged EXEC mode.

clear 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	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The clear traffic command resets the counters for transmit and receive activity that is displayed with the **show traffic** command. The counters indicate the number of packets and bytes moving through each interface since the last clear traffic command was entered or since the ASA came online. And the number of seconds indicate the duration the ASA has been online since the last reboot.

Examples

The following example shows the **clear traffic** command:

```
ciscoasa# clear
 traffic
```

Related Commands

Command	Description
show traffic	Displays the counters for transmit and receive activity.

clear uauth

To delete all the cached authentication and authorization information for a user or for all users, use the **clear uauth** command in privileged EXEC mode.

clear uauth [*username*]

Syntax Description

username	(Optional) Specifies the user authentication information to remove by username.

Command Default

Omitting the *username* argument deletes the authentication and authorization information for all users.

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 uauth** command deletes the AAA authorization and authentication caches for one user or for all users, which forces the user or users to reauthenticate the next time that they create a connection.

This command is used with the **timeout** command.

Each user host IP address has an authorization cache attached to it. If the user attempts to access a service that has been cached from the correct host, the ASA considers it preauthorized and immediately proxies the connection. Once you are authorized to access a website, for example, the authorization server is not contacted for each image as it is loaded (assuming the images come from the same IP address). This process significantly increases performance and reduces the load on the authorization server.

The cache allows up to 16 address and service pairs for each user host.

Note When you enable Xauth, an entry is added to the uauth table (as shown by the **show uauth** command) for the IP address that is assigned to the client. However, when using Xauth with the Easy VPN Remote feature in Network Extension Mode, the IPsec tunnel is created from network to network, so that the users behind the firewall cannot be associated with a single IP address. For this reason, a uauth entry cannot be created upon completion of Xauth. If AAA authorization or accounting services are required, you can enable the AAA authentication proxy to authenticate users behind the firewall. For more information on AAA authentication proxies, see the AAA commands.

Use the **timeout uauth** command to specify how long the cache should be kept after the user connections become idle. Use the **clear uauth** command to delete all the authorization caches for all the users, which will cause them to have to reauthenticate the next time that they create a connection.

Examples

The following example shows how to cause the user to reauthenticate:

```
ciscoasa(config)# clear uauth user
```

Related Commands

Command	Description
aaa authentication	Enables, disables, or views LOCAL, TACACS+ or RADIUS user authentication (on a server designated by the aaa-server command).
aaa authorization	Enables, disables, or views TACACS+ or RADIUS user authorization (on a server designated by the aaa-server command).
show uauth	Displays current user authentication and authorization information.
timeout	Sets the maximum idle time duration.

clear uc-ime

To clear the counters used to display statistics about the Cisco Intercompany Media Engine proxy, use the **clear uc-ime** command in privileged EXEC mode.

clear uc-ime [[**mapping-service-sessions** | **signaling-sessions** | **fallback-notification**] **statistics**]

Syntax Description

fallback-notification	(Optional) Clears the counters for fallback notification statistics.
mapping-service-sessions	(Optional) Clears the counters for mapping-service-session statistics.
signaling-sessions	(Optional) Clears the counters for signaling-session statistics.
statistics	(Optional) The keyword to configure which counters to clear for the Cisco Intercompany Media Engine proxy.

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
8.3(1)	This command was added.

Examples

The following example clears the counters which are used to display signaling-sessions statistics:

```
ciscoasa# clear configure signaling-sessions statistics
```

Related Commands

Command	Description
clear configure uc-ime	Clears the running configuration for the Cisco Intercompany Media Engine proxy on the ASA.
show running-config uc-ime	Shows the running configuration of the Cisco Intercompany Media Engine proxy.
show uc-ime	Displays statistical or detailed information about fallback notifications, mapping-service sessions, and signaling sessions.

Command	Description
uc-imc	Creates the Cisco Intercompany Media Engine proxy instance on the ASA.

clear url-block block statistics

To clear the block buffer usage counters, use the clear **url-block block statistics** command in privileged EXEC mode.

clear url-block block 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.

Usage Guidelines

The **clear url-block block statistics** command clears the block buffer usage counters, except for the Current number of packets held (global) counter.

Examples

The following example clears the URL block statistics and displays the status of the counters after they have been cleared:

```
ciscoasa# clear url-block block statistics
ciscoasa# show url-block block statistics
URL Pending Packet Buffer Stats with max block  0
-----------------------------------------------------
Cumulative number of packets held: | 0
Maximum number of packets held (per URL): | 0
Current number of packets held (global): | 38
Packets dropped due to
 | exceeding url-block buffer limit: | 0
 | HTTP server retransmission: | 0
Number of packets released back to client: | 0
```

Related Commands

Commands	Description
filter url	Directs traffic to a URL filtering server.

Commands	Description
show url-block	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manages the URL buffers used for web server responses.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

clear url-cache statistics

To remove **url-cache** command statements from the configuration, use the clear **url-cache** command in privileged EXEC mode.

clear url-cache 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.

Usage Guidelines

The **clear url-cache** command removes URL cache statistics from the configuration.

Using the URL cache does not update the Websense accounting logs for Websense protocol Version 1. If you are using Websense protocol Version 1, let Websense run to accumulate logs so you can view the Websense accounting information. After you get a usage profile that meets your security needs, enter the **url-cache** command to increase throughput. Accounting logs are updated for Websense protocol Version 4 and for N2H2 URL filtering while using the **url-cache** command.

Examples

The following example clears the URL cache statistics:

```
ciscoasa# clear url-cache statistics
```

Related Commands

Commands	Description
filter url	Directs traffic to a URL filtering server.
show url-cache statistics	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.

Commands	Description
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

clear url-server

To clear URL filtering server statistics, use the clear **url-server** command in privileged EXEC mode.

clear url-server 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.

Usage Guidelines

The **clear url-server** command removes URL filtering server statistics from the configuration.

Examples

The following example clears the URL server statistics:

```
ciscoasa# clear url-server statistics
```

Related Commands

Commands	Description
filter url	Directs traffic to a URL filtering server.
show url-server	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

clear user-identity active-user-database

To set the status of specified users to logged out for the Identity Firewall, use the **clear user-identity active-user-database** command in privileged EXEC mode.

clear user-identity active-user-database [**user** [*domain_nickname*\ ] *use_rname*] | **user-group** [*domain_nickname*\\ ] *user_group_name*]

Syntax Description

*domain_nickname**user_group_name*	Specifies a user group for which to clear statistics. The *group_name* can contain any character including [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.]. If *domain _NetBIOS_name \group _name* contains a space, you must enclose the domain name and user name in quotation marks.
domain_nickname \use_rname	Specifies a user for which to clear statistics. The *user_name* can contain any character including [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.]. If *domain_NetBIOS_name\user _name* contains a space, you must enclose the domain name and user name in quotation marks.
user	Specifies to clear statistics for users.
user-group	Specifies to clear statistics for user groups.

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
8.4(2)	This command was added.

Usage Guidelines

This command sets the status of the specified user, all users belong to the specified user group, or all users to logged out.

When you specify the **user-group** keyword, the status of all users belong to the specified user group are set to logged out. When you do not specify the *domain_nickname* argument with the **user-group** keyword, users in the groups with *user_group_name* in default domain are given the logged out status.

When you specify the **user** keyword, the status of the specified user is set to logged out. When you do not specify the *domain_nickname* argument with the **user** keyword, the user with *user_name* in default domain receives a logged out status.

When you do not specify either the **user** or **user-group** keywords, all users have their status set to logged out.

Examples

The following example sets the status of all users in user group users1 in the SAMPLE domain to logged out:

```
ciscoasa# clear user-identity active-user-database user-group SAMPLE\users1
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.
show user-identity user active	Displays the active users for the Identify Firewall.

clear user-identity ad-agent statistics

To clear the AD Agent statistics for the Identity Firewall, use the **clear user-identity ad-agent statistics** command in privileged EXEC mode.

clear user-identity ad-agent 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	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

The ASA maintains the following information about the primary and secondary AD Agents:

- Status of the AD Agents
- Status of the domains
- Statistics for the AD Agents

Use the **clear user-identity ad-agent statistics** command to clear the statistics data of AD Agents.

Examples

The following example clears the AD Agent statistics for the Identity Firewall:

```
ciscoasa# clear user-identity ad-agent statistics
ciscoasa# show user-identity ad-agent statistics
 Primary AD Agent               Total  Last Activity
 -------------------------  ----------  ------------------------
 Input packets:                     0  N/A
 Output packets:                    0  N/A
 Send updates:                      0  N/A
 Recv updates:                      0  N/A
 Keepalive failed:                  0  N/A
 Send update failed:                0  N/A
 Query failed:                      0  N/A
 Secondary AD Agent             Total  Last Activity
 -------------------------  ----------  ------------------------
```

```
Input packets:                  0  N/A
Output packets:                 0  N/A
Send updates:                   0  N/A
Recv updates:                   0  N/A
Keepalive failed:               0  N/A
Send update failed:             0  N/A
Query failed:                   0  N/A
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.
show user-identity ad-agent [**statistics**]	Displays statistical information about the AD Agent for the Identity Firewall.

clear user-identity statistics

To clear the counters used to display statistics about the Identity Firewall, use the **clear user-identity statistics** command in privileged EXEC mode.

clear user-identity statistics [**user** [*domain_nickname*\ ] *use_rname*] | **user-group** [*domain_nickname*\\ ] *user_group-name*]

Syntax Description

*domain_nickname**user_group_name*	Specifies a user group for which to clear statistics. The *group_name* can contain any character including [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.]. If *domain _NetBIOS_name \group _name* contains a space, you must enclose the domain name and user name in quotation marks.
domain_nickname \use_rname	Specifies a user for which to clear statistics. The *user_name* can contain any character including [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.]. If *domain_NetBIOS_name\user _name* contains a space, you must enclose the domain name and user name in quotation marks.
user	Specifies to clear statistics for users.
user-group	Specifies to clear statistics for user groups.

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
8.4(2)	This command was added.

Usage Guidelines

When *domain_nickname* is not specified before *user_group_name*, the ASA removes the Identity Firewall statistics for the group with *user_group_name* in the default domain.

When *domain_nickname* is not specified before *user_name*, the ASA removes the Identity Firewall statistics for the user with *user_name* in the default domain.

Examples

The following example clears the counters which are used to display statistics for a user group:

```
ciscoasa# clear user-identity statistics user-group SAMPLE\users1
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.
show user-identity statistics	Displays statistics for a user or user group for the Identify Firewall.

clear user-identity user-not-found

To clear the ASA local user-not-found database for the Identity Firewall, use the **clear user-identity user-not-found** command in privileged EXEC mode.

clear user-identity user-not-found

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
8.4(2)	This command was added.

Usage Guidelines

The ASA maintains a local user-not-found database of the IP addresses not found in Microsoft Active Directory. The ASA keeps only the last 1024 packets (contiguous packets from the same source IP address are treated as one packet) of the user-not-found list and not the entire list in the database.

User the **clear user-identity user-not-found** command to clear the local database on the ASA.

Tip Use the **show user-identity user-not-found** command to display the IP addresses of the users who are not found in Microsoft Active Directory.

Examples

The following example clears the local user-not-found database for the Identity Firewall:

```
ciscoasa# show user-identity user-not-found
172.13.1.2
171.1.45.5
169.1.1.2
172.13.12
ciscoasa# clear user-identity user-not-found
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.
show user-identity user-not-found	Displays the IP addresses of the Active Directory users not found in the ASA user-not-found database.

clear user-identity user no-policy-activated

To clear the local records on the ASA of users who are not activated for the Identity Firewall, use the **clear user-identity user no-policy-activated** command in privileged EXEC mode.

clear user-identity user no-policy-activated

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
8.4(2)	This command was added.

Usage Guidelines

Use the **clear user-identity user no-policy-activated** to clear the local records of users not activated by any security policy, meaning the user is not part of an activated user group or not referenced in an access list or service policy configuration.

The **clear user-identity user no-policy-activated** command also clears the IP addresses of users who are active but not activated.

When you create a user group for the Identity Firewall, it must be activated, meaning the group is an import user group (defined as a user group in an access list or service policy configuration) or a local user group (defined in an object-group user).

Examples

The following example clears the local records on the ASA for users who are not activated:

```
ciscoasa# clear user-identity user no-policy-activated
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.
show user-identity group	Displays the list of activated user groups for the Identity Firewall.

clear vpn cluster stats internal

To clear the internal counters for VPN clustering, use this command in global configuration or privileged EXEC mode.

clear vpn cluster stats internal

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	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.9(1)	Command added.

Related Commands

Command	Description
show vpn cluster stats internal	Clear all VPN cluster counters.

clear vpn-sessiondb statistics

To clear information about VPN sessions, including all statistics or specific sessions or protocols, use the clear **vpn-sessiondb statistics** command in privileged EXEC mode.

clear vpn-sessiondb { **all** | **anyconnect** | **failover** | **email-proxy** | **global** | **index** *index_number* | **ipaddress** *IPaddr* | **l2l** | **name** *username* | **protocol** *protocol* | **ra-ikev1-ipsec** | **ra-ikev2-ipsec** | **tunnel-group** *name* | **vpn-lb** | **webvpn** }

Syntax Description

all	Clears statistics for all sessions.
anyconnect	**Clears statistics for AnyConnect VPN client sessions.**
failover	Clears statistics for failover IPsec sessions.
email-proxy	(Deprecated) Clears **statistics for** e-mail proxy sessions.
global	Clears **statistics for** global session data.
index *indexnumber*	Clears statistics of a single session by index number. The output of the show vpn-sessiondb detail command displays index numbers for each session.
ipaddress *IPaddr*	Clears statistics for sessions of the IP address that you specify.
l2l	Clears stastistics for VPN LAN-to-LAN sessions.

protocol protocol	Clears **statistics for the following protocols:** • ikev1—Sessions using the IKEv1 protocol. • ikev2—Sessions using theIKEv2 protocol. • ipsec—IPsec sessions using either IKEv1 or IKEv2. • ipseclan2lan—IPsec LAN-to-LAN sessions. • ipseclan2lanovernatt—IPsec LAN-to-LAN over NAT-T sessions. • ipsecovernatt—IPsec over NAT-T sessions. • ipsecovertcp—IPsec over TCP sessions. • ipsecoverudp—IPsec over UDP sessions. • l2tpOverIpSec—L2TP over IPsec sessions. • l2tpOverIpsecOverNatT—L2TP over IPsec over NAT-T sessions. • ospfv3—OSPFv3 over IPsec sessions. • webvpn—Clientless SSL VPN sessions. • imap4s—IMAP4 sessions. • pop3s—POP3 sessions. • smtps—SMTP sessions. • anyconnectParent—Secure Client sessions, regardless of the protocol used for the session (terminates AnyConnect IPsec IKEv2 and SSL sessions). • ssltunnel—SSL VPN sessions, including Secure Client sessions using SSL and clientless SSL VPN sessions. • dtlstunnel—Secure Client sessions with DTLS enabled.
ra-ikev1-ipsec	Clears statistics for IPsec IKEv1 and L2TP sessions.
ra-ikev2-ipsec	Clears statistics for IPsec IKEv2 sessions.
tunnel-group *groupname*	Clears statistics for sessions for the tunnel group (connection profile) that you specify.
vpn-lb	Clears statistics for VPN load balancing management sessions.
webvpn	Clears statistics for clientless SSL VPN sessions.

Command Default

There is 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.
9.3(2)	The **ra-ikev2-ipsec** keyword was added.
9.8(1)	The email-proxy option was deprecated.
9.0(1)	The OSPFv3 session type and multiple context mode was added.

clear wccp

To reset WCCP information, use the **clear wccp** command in privileged EXEC mode.

clear wccp [**web-cache** | *service_number*]

Syntax Description

web-cache	Specifies the web-cache service.
service-number	A dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 255. There is a maximum allowable number of 256 that includes the web-cache service specified with the **web-cache** keyword.

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
7.2(1)	This command was added.

Examples

The following example shows how to reset the WCCP information for the web-cache service:

```
ciscoasa# clear wccp web-cache
```

Related Commands

Command	Description
show wccp	Displays the WCCP configuration.
wccp redirect	Enables support of WCCP redirection.

clear webvpn sso-server statistics

To reset the statistics from the WebVPN Single Sign-On (SSO) server, use the **clear webvpn sso-server statistics** command in privileged EXEC mode.

clear webvpn sso-server statistics *servername*

Syntax Description

servername	Specifies the name of the SSO server to be reset.

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	—	—

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 does not reset the "pending requests" statistic.

Examples

The following example displays crypto accelerator statistics:

```
ciscoasa # clear webvpn sso-server statistics
ciscoasa #
```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
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 xlate

To clear current dynamic translation and connection information, use the **clear xlate** command in privileged EXEC mode.

clear xlate [**global** *ip1* [- *ip2*] [**netmask** *mask*]] [**local** *ip1* [- *ip2*] [**netmask** *mask*]] [**gport** *port1* [- *port2*]] [**interface** *if_name*] [**state** *state*]

Syntax Description

global *ip1* [- *ip2*]	(Optional) Clears the active translations by global IP address or range of addresses.
gport *port1* [-*port2*]	(Optional) Clears the active translations by the global port or range of ports.
interface *if_name*	(Optional) Displays the active translations by interface.
local *ip1* [- *ip2*]	(Optional) Clears the active translations by local IP address or range of addresses.
lport *port1* [-*port2*]	(Optional) Clears the active translations by local port or range of ports.
netmask *mask*	(Optional) Specifies the network mask to qualify the global or local IP addresses.
state *state*	(Optional) Clears the active translations by state. You can enter one or more of the following states: • **static** —Specifies **static** translations. • **portmap** —Specifies PAT global translations. • **norandomseq** —Specifies a **nat** or **static** translation with the **norondomseq** setting. • **identity** —Specifies **nat 0** identity address translations. When specifying more than one state, separate the states with a space.

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.

Usage Guidelines

The **clear xlate** command clears the contents of the translation slots ("xlate" refers to the translation slot). Translation slots can persist after key changes have been made. Always use the clear xlate command after adding, changing, or removing the global or nat commands in your configuration.

An xlate describes a NAT or PAT session. These sessions can be viewed with the **show xlate** command with the **detail** option. There are two types of xlates: static and dynamic.

A static xlate is a persistent xlate that is created using the **static** command. The **clear xlate** command does not clear for a host in a static entry. Static xlates can only be removed by removing the **static** command from the configuration; the **clear xlate** command does not remove the static translation rule. If you remove a static command from the configuration, preexisting connections that use the static rule can still forward traffic. Use the **clear local-host** or **clear conn** command to deactivate these connections.

A dynamic xlate is an xlate that is created on demand with traffic processing (through the **nat** or **global** command). The **clear xlate** command removes dynamic xlates and their associated connections. You can also use the **clear local-host** or **clear conn** command to clear the xlate and associated connections. If you remove a **nat** or a **global** command from the configuration, the dynamic xlate and associated connections may remain active. Use the **clear xlate** command to remove these connections.

Examples

The following example shows how to clear the current translation and connection slot information:

```
ciscoasa# clear xlate global
```

Related Commands

Command	Description
clear local-host	Clears local host network information.
clear uauth	Clears cached user authentication and authorization information.
show conn	Displays all active connections.
show local-host	Displays the local host network information.
show xlate	Displays the current translation information.