

show aa – show asr

- show aaa kerberos, on page 2
- show aaa local user, on page 4
- show aaa login-history, on page 6
- show aaa sdi node-secrets, on page 8
- show aaa-server, on page 9
- show access-list, on page 13
- show activation-key, on page 20
- show ad-groups, on page 31
- show admin-context, on page 34
- show alarm settings, on page 35
- show arp, on page 37
- show arp-inspection, on page 39
- show arp rate-limit, on page 41
- show arp statistics, on page 42
- show arp vtep-mapping, on page 44
- show asdm history, on page 46
- show asdm image, on page 52
- show asdm log_sessions, on page 53
- show asdm sessions, on page 54

show aaa kerberos

To display Kerberos service information, use the **show aaa kerberos** command in privileged EXEC mode.

show aaa kerberos [**username** *user*] | **keytab**]

Syntax Description

keytab	Displays information about the Kerberos keytab file.
username *user*	Displays tickets for the specified user.

Command Default

If you do not specify a keyword, tickets for all users are displayed.

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	—

Usage Guidelines

Use the **show aaa kerberos** command, without keywords, to view all the Kerberos tickets cached on the ASA. Add the **username** keyword to view the Kerberos tickets of a specific user. You must use the **keytab** keyword to see any information about the keytab file.

Examples

The following example shows the usage of the **show aaa kerberos** command:

```
ciscoasa
(config)# show aaa kerberos
Default Principal       Valid Starting     Expires     Service Principalkcduser@example.com
       06/29/10 17:33:00     06/30/10 17:33:00
asa$/mycompany.com@example.comkcduser@example.com       06/29/10 17:33:00     06/30/10
17:33:00    http/owa.mycompany.com@example.com
```

The following example shows how to display information about the Kerberos keytab file.

```
ciscoasa# show aaa kerberos keytab

Principal:   host/asa2@BXB-WIN2016.EXAMPLE.COM
Key version: 10
Key type:    arcfour (23)
```

Related Commands

Command	Description
aaa kerberos import-keytab	Imports a Kerberos keytab file that you exported from the Kerberos Key Distribution Center (KDC).

Command	Description
clear aaa kerberos	Clears the cached Kerberos tickets.
show running-config aaa-server	Displays the AAA server configuration.

show aaa local user

To show the list of usernames that are currently locked, or to show details about the username, use the show **aaa local user** command in global configuration mode.

show aaa local user [**locked**]

Syntax Description

locked	(Optional) Shows the list of usernames that are currently locked.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	We added this command.
9.17(1)	Added **Expired** and **New-User** columns.

Usage Guidelines

If you omit the optional keyword **locked**, the ASA displays the failed-attempts and lockout status details for all AAA local users.

This command affects only the status of users that are locked out.

Users are unlocked after 10 minutes; however, the output of this command will still show a user as locked after 10+ minutes until they successfully log in again.

Examples

The following example shows use of the **show aaa** local user command to display the lockout status of all usernames:

This example shows the use of the **show aaa local user** command to display the number of failed authentication attempts and lockout status details for all AAA local users, after the limit has been set to 5:

```
ciscoasa(config)# aaa local authentication attempts max-fail 5
ciscoasa(config)# show aaa local user
Lock-time  Failed-attempts     Expired     New-User     Locked      User
    -                   6      N            N           Y           cas
    -                   2      N            Y           N           sam
    -                   1      N            Y           N           dean
    -                   4      N            N           N           admin
```

```
ciscoasa(config)#
```

This example shows the use of the **show aaa local user** command with the **lockout** keyword to display the number of failed authentication attempts and lockout status details only for any locked-out AAA local users, after the limit has been set to 5:

```
ciscoasa(config)# aaa local authentication attempts max-fail 5
ciscoasa(config)# show aaa local user
Lock-time  Failed-attempts     Expired     New-User     Locked      User
    -                   6      N            N           Y           cas
ciscoasa(config)#
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Configures the maximum number of times a user can enter a wrong password before being locked out.
clear aaa local user fail-attempts	Resets the number of failed attempts to 0 without modifying the lockout status.
clear aaa local user lockout	Clears th e lockout status of the specified user or all users and sets their failed attempts counters to 0.

show aaa login-history

To view the login history, use the **show aaa login-history** command in privileged EXEC mode.

show aaa login-history [**user** *name*]

Syntax Description

user *name*	(Optional) Specifies the login history for a particular user.

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	—

Usage Guidelines

By default, the ASA saves the login history for usernames in the local database or from a AAA server when you enable local AAA authentication for one or more of the CLI management methods (SSH, Telnet, serial console). Use the **show aaa login-history** command to view the login history. See the **aaa authentication login-history** command to configure the history duration.

ASDM logins are not saved in the history.

The login history is only saved per unit; in failover and clustering environments, each unit maintains its own login history only.

Login history data is not maintained over reloads.

Examples

The following example shows the login history:

```
ciscoasa(config)# show aaa login-history
Login history for user:                              cisco
Logins in last   1 days:                             45
Last successful login:                          14:07:28 UTC Aug 21 2018 from 10.86.190.50
Failures since last login:                           0
Last failed login:                                   None
Privilege level:                                     14
Privilege level changed from 11 to 14 at:            14:07:30 UTC Aug 21 2018
```

Related Commands

Command	Description
aaa authentication login-history	Saves the local **username** login history.
password-history	Stores previous **username** passwords. This command is not user-configurable.

Command	Description
password-policy reuse-interval	Prohibits the reuse of a **username** password.
password-policy username-check	Prohibits a password that matches a **username** name.
show aaa login-history	Shows the local **username** login history.
username	Configures a local user.

show aaa sdi node-secrets

To display information about the SDI node secret files installed on the system, use the **show aaa sdi node-secrets** command in privileged EXEC mode.

show aaa sdi node-secrets

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	—

Usage Guidelines

Use the **show aaa sdi node-secrets** command to view a list of the RSA SecurID servers that have node secret files installed on the system. The node secret files are exported from the RSA Authentication Manager, and uploaded to the system using the **aaa sdi import-node-secret** command. To remove a node secret file, use the **clear aaa sdi node-secret** command.

Examples

The following example shows the SecurID servers that have node secret files installed on the system.

```
ciscoasa
#
show aaa sdi node-secrets

Last update                  SecurID server
---------------------        --------------------
15:16:13 Jun 24 2020         rsaam.cisco.com
15:20:07 Jun 24 2020         10.11.12.13
ciscoasa
#
```

Related Commands

Command	Description
aaa sdi import-node-secret	Imports a node secret file that was exported from an RSA Authentication Manager.
clear aaa sdi node-secret	Removes a node secret file.

show aaa-server

To display AAA server statistics for AAA servers, use the **show aaa-server** command in privileged EXEC mode.

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

Syntax Description

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

Command Default

By default, all AAA server statistics display.

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
7.1(1)	The http-form protocol was added.
8.0(2)	The server status shows if the status was changed manually using the **aaa-server active** command or **fail** command.

Examples

The following is sample output from the **show aaa-server** command:

```
ciscoasa(config)# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE. Last transaction (success) at 11:10:08 UTC  Fri Aug 22
Number of pending requests        20
Average round trip time           4ms
Number of authentication requests 20
Number of authorization requests  0
Number of accounting requests     0
Number of retransmissions         1
Number of accepts                 16
Number of rejects                 4
Number of challenges              5
Number of malformed responses     0
Number of bad authenticators      0
Number of timeouts                0
Number of unrecognized responses  0
```

The following table shows field descriptions for the **show aaa-server** command:

Field	Description
Server Group	The server group name specified by the **aaa-server** command.
Server Protocol	The server protocol for the server group specified by the **aaa-server** command.
Server Address	The IP address of the AAA server.
Server port	The communication port used by the ASA and the AAA server. You can specify the RADIUS authentication port using the **authentication-port** command. You can specify the RADIUS accounting port using the **accounting-port** command. For non-RADIUS servers, the port is set by the **server-port** command.

Field	Description
Server status	The status of the server. One of the following values appears: • ACTIVE—The ASA will communicate with this AAA server. • FAILED—The ASA cannot communicate with the AAA server. Servers that are put into this state remain there for some period of time, depending on the policy configured, and are then reactivated. If the status is followed by "(admin initiated)," then the server was manually failed or reactivated using the **aaa-server active** command or **fail** command. The date and time of the last transaction appear in the following form: **Last transaction (** {**success** | **failure** }**)** **at** *time timezone date* If the ASA has never communicated with the server, the message shows as the following: **Last transaction at Unknown**
Number of pending requests	The number of requests that are still in progress.
Average round trip time	The average time that it takes to complete a transaction with the server.
Number of authentication requests	The number of authentication requests sent by the ASA. This value does not include retransmissions after a timeout.
Number of authorization requests	The number of authorization requests. This value refers to authorization requests due to command authorization, authorization for through-the-box traffic (for TACACS+ servers), or for WebVPN and IPsec authorization functionality enabled for a tunnel group. This value does not include retransmissions after a timeout.
Number of accounting requests	The number of accounting requests. This value does not include retransmissions after a timeout.
Number of retransmissions	The number of times a message was retransmitted after an internal timeout. This value applies only to Kerberos and RADIUS servers (UDP).
Number of accepts	The number of successful authentication requests.
Number of rejects	The number of rejected requests. This value includes error conditions as well as true credential rejections from the AAA server.

Field	Description
Number of challenges	The number of times the AAA server required additional information from the user after receiving the initial username and password information.
Number of malformed responses	N/A. Reserved for future use.
Number of bad authenticators	The number of times that one of the following occurs: • The “authenticator” string in the RADIUS packet is corrupted (rare). • The shared secret key on the ASA does not match the one on the RADIUS server. To fix this problem, enter the correct server key. This value only applies to RADIUS.
Number of timeouts	The number of times the ASA has detected that a AAA server is not responsive or otherwise misbehaving and has declared it offline.
Number of unrecognized responses	The number of times that the ASA received a response from the AAA server that it could not recognize or support. For example, the RADIUS packet code from the server was an unknown type, something other than the known “access-accept,” “access-reject,” “access-challenge,” or “accounting-response” types. Typically, this means that the RADIUS response packet from the server was corrupted, which is rare.

Related Commands

Command	Description
show running-config aaa-server	Displays statistics for all servers in the indicated server group or for a particular server.
clear aaa-server statistics	Clears the AAA server statistics.

show access-list

To display the rules and hit counters for an access list, use the **show access-list** command in privileged EXEC mode.

show access-list [*id* [*ip_address* | **brief** | **numeric**] | **element-count** | **forward-reference** | **internal**]

Syntax Description

brief	(Optional) Displays the access list identifiers, the hit count, and the timestamp of the last rule hit, all in hexadecimal format.
id	(Optional) Shows counters for the ID of an existing access list.
ip_address	(Optional) Shows counters for the source IP address or hostname in the specified access list.
numeric	(Optional.) If you specify an ACL name, displays ports as numbers instead of names. For example, 80 instead of www.
element-count	(Optional.) Displays the total number of access control entries in all access lists defined on the system.
forward-reference	Displays information about ACLs that include objects that are forward referenced. These are objects using in an ACL that are not yet defined.
internal	Displays a summary of the access lists in the system, including counts for various items.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	Support for the **brief** keyword was added.
8.3(1)	The ACE show pattern to display ACL timestamp was modified.
9.14(1)	The **numeric** and **element-count** keywords were added.

Release	Modification
9.17(1)	The command is now supported in the system context, which shows the element count of all access lists configured in all contexts. In addition, the element-count output includes the breakdown of object groups if object-group search is enabled.
9.22(1)	When object group search is enabled, the hexidecimal ID for network objects and the timestanp for the last hit are shown.
9.22(3)	Element count now shows 2 counts: total number of objects, and total number of access control entries.
9.23(1)	The **internal** keyword was added.

Usage Guidelines

You can specify the **brief** keyword to display access list hit count, identifiers, and timestamp information in hexadecimal format. The configuration identifiers displayed in hexadecimal format are presented in three columns, and they are the same identifiers used in syslogs 106023 and 106100.

If an access list has been changed recently, the list is excluded from the output. The following message indicates when this happens. Changes can include: dynamic ACL changes, fully-qualified domain name (FQDN) DNS updates, changes from the device manager (ASDM, CSM, etc.), or a recent CLI change. Wait for the ACL to be fully recompiled, then try again.

```
WARNING: OOB Access-list config change detected. Possible modification from,
    SSH/Telnet sessions, ASDM/CSM or  FQDN resolution.
   Hence, Access- list <ACL_NAME> will not be displayed.
```

Note The output shows how many elements are in the ACL. This number is not necessarily the same as the number of access control entries (ACE) in the ACL. The system might create extra elements when you use network objects with address ranges, for example, and these extra elements are not included in the output.

Clustering Guidelines

When using ASA clustering, if traffic is received by a single unit, the other units may still show a hit count for the ACL due to the clustering director logic. This is an expected behavior. Because the unit that did not receive any packets directly from the client may receive forwarded packets over the cluster control link for an owner request, the unit may check the ACL before sending the packet back to the receiving unit. As a result, the ACL hit count will be increased even though the unit did not pass the traffic.

Examples

The following examples show brief information about the specified access policy in hexadecimal format (ACEs in which the hitcount is not zero). The first two columns display identifiers in hexadecimal format, the third column lists the hit count, and the fourth column displays the timestamp value, also in hexadecimal format. The hit count value represents the number of times the rule has been hit by traffic. The timestamp value reports the time of the last hit. If the hit count is zero, no information is displayed.

The following is sample output from the **show access-list** command and shows the access list name "test," which is applied on an outside interface in the "IN" direction:

```
ciscoasa# show access-list test
access-list test; 3 elements; name hash: 0xcb4257a3
```

```
access-list test line 1 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 2 extended permit object-group TELNET-SSH object-group S1 object-group
 D1 0x44ae5901
  access-list test line 2 extended permit tcp 100.100.100.0 255.255.255.0 10.10.10.0
255.255.255.0 eq telnet (hitcnt=1) 0xca10ca21
  access-list test line 2 extended permit tcp 100.100.100.0 255.255.255.0 10.10.10.0
255.255.255.0 eq ssh(hitcnt=1) 0x5b704158
```

The following is sample output from the **show access-list** command when **object-group-search** is not enabled:

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 9 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN object-group BLK-LAN
 0x724c956b
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0 192.168.4.0
 255.255.255.0 (hitcnt=10) 0x30fe29a6
   access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 192.168.4.0
 255.255.255.0 (hitcnt=4) 0xc6ef2338
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0 14.14.14.0
 255.255.255.0 (hitcnt=2) 0xce8596ec
   access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 14.14.14.0
 255.255.255.0 (hitcnt=0) 0x9a2f1c4d
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
(hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0) 0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
0xa52a0761
```

The following is sample output from the **show access-list** command when **object-group-search** is enabled:

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 6 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN(1) object-group
BLK-LAN(2)(hitcount=16) 0x724c956b
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
(hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0) 0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
0xa52a0761
```

Starting with 9.22(1), with object group search enabled, the information includes the hexadecimal object ID and the timestamp for the last hit (if any).

```
ciscoasa# show access-list
access-list ALPHA line 1 advanced permit ip object-group SOG1 host 5.5.5.5(0xf0050004)
(hitcnt=1) (Last Hit=04:38:46 UTC Feb 6 2024) 0x9ee966bb
access-list ALPHA line 1 advanced permit ip v4-object-group SOG1(0xf0000004) host
5.5.5.5(0xf0050004) (hitcnt=1) (Last Hit=04:38:46 UTC Feb 6 2024) 0x13d72f03
```

The following is sample output from the **show access-list brief** command when Telnet traffic is passed:

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
ca10ca21
 44ae5901 00000001 4a68aa7e
```

The following is sample output from the **show access-list brief** command when SSH traffic is passed:

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
ca10ca21 44ae5901 00000001 4a68aa7e
5b704158
 44ae5901 00000001 4a68aaa9
```

The following is sample output from the **show access-list** command and shows the access list name "test," which is applied on an outside interface in the "IN" direction, with ACL Optimization enabled:

```
ciscoasa# show access-list test
access-list test; 3 elements; name hash: 0xcb4257a3
access-list test line 1 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 2 extended permit object-group TELNET-SSH object-group S1 object-group
 D1 0x44ae5901
  access-list test line 2 extended permit tcp object-group S1(1) object-group D1(2) eq
telnet (hitcnt=1) 0x7b1c1660
  access-list test line 2 extended permit tcp object-group S1(1) object-group D1(2) eq ssh
 (hitcnt=1) 0x3666f922
```

The following is sample output from the **show access-list brief** command when Telnet traffic is passed:

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660
 44ae5901 00000001 4a68ab51
```

The following is sample output from the **show access-list brief** command when SSH traffic is passed:

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
3666f922
 44ae5901 00000001 4a68ab66
```

The following example shows the element count, which is the total number of access control entries for all access lists defined on the system. For access lists that are assigned as access groups, to control access globally or on an interface, you can reduce the element count by enabling object group search using the **object-group-search access-control** command. When object group search is enabled, network objects are used in the access control entries; otherwise, the objects are expanded into the individual IP addresses contained in the objects and separate entries are written for each source/destination address pair. Thus, a single rule that uses a source network object with 5 IP addresses, and a destination object with 6 addresses, would expand into 5 * 6 entries, 30 elements rather than one. The higher the element count, the larger the access lists, which can potentially impact performance.

```
asa(config)# show access-list element-count
```

```
Total number of access-list elements: 33934
```

Starting with 9.17(1), if you enable object-group search, additional information is presented about the number of object groups in the rules (OBJGRP), including the split between source (SRC OBJ) and destination (DST OBJ) objects, and the added and deleted groups.

```
ciscoasa(config)# show access-list element-count
Total number of access-list elements: 892

OBJGRP     SRC OG     DST OG     ADD OG     DEL OG
842        842        842        842        0
```

Starting with 9.22(3), the element count information provides separate counts for total objects (access list elements) and the actual number of access control entries (access-list rules).

```
ciscoasa(config)# show access-list element-count
Total number of access-list elements: 48368
Total number of access-list rules: 34795
```

In multiple context mode, if you use the element-count keyword in the system context, the statistics apply to all contexts, summarizing the count across the systems. If you enable object-group search, the information includes counts for total access control entries (ACE), objects (OBJGRP), and source (SRC) and destination (DST) object groups. If object-group search is disabled, the object counts will always be 0. The following example is for a system context when you have enabled object-group search.

```
ciscoasa/act(config)# show access-list element-count

Context Name             ACE        OBJGRP     SRC OG     DST OG
system                   0          0          0          0
admin                    0          0          0          0
ciscoasactx001           892        842        842        842
ciscoasactx002           312        298        298        298
ciscoasactx003           398        306        306        306
ciscoasactx004           162        132        132        132
ciscoasactx005           1280       583        583        583
ciscoasactx006           352        345        345        345
ciscoasactx007           353        351        351        351
ciscoasactx008           348        346        346        346
ciscoasactx009           433        420        420        420
ciscoasactx010           342        340        340        340
ciscoasactx011           363        361        361        361
ciscoasactx012           409        406        406        406
ciscoasactx013           381        373        373        373
ciscoasactx014           332        330        330        330
ciscoasactx015           465        374        374        374
ciscoasactx016           444        316        316        316
ciscoasactx017           284        268        268        268
sciscoasactx018          8837       0          0          0
ciscoasactx019           467        412        412        412
ciscoasactx020           934        527        527        527
ciscoasactx021           415        401        401        401
ciscoasactx022           676        562        562        562
ciscoasactx023           1208       1099       1099       1099
ciscoasactx024           350        322        322        322
ciscoasactx025           638        252        252        252
ciscoasactx026           318        304        304        304
ciscoasactx027           359        308        308        308
ciscoasactx028           1249       1087       1087       1087
ciscoasactx029           451        326        326        326
```

```
ciscoasactx030           377        315        315        315
ciscoasactx031           445        418        418        418
ciscoasactx032           347        309        309        309
ciscoasactx033           583        317        317        317
ciscoasactx034           340        311        311        311
ciscoasactx035           350        301        301        301

 Total access-list elements in all Context: 25894
```

The following example shows **show access-list internal** output.

```
ciscoasa(config)# show access-list internal

Id   Type       Count    OG-Cnt   Permit   Trust    Deny     fwd-ref  Mode      OGS
IOO       Name

1    Extended   40682    7086     39632    0        1050     No       Config    Enabled
Enabled   IDC_SUPER-VRF999_access_in
2    Extended   5266     1019     5147     0        119      No       Config    Enabled
Enabled   OSS_BSS_DMZ-SYS00111_access_in
3    Extended   19       4        16       0        3        No       Config    Enabled
Enabled   R4G_UIDAI_ADHAR_access_in
4    Extended   480      72       474      0        6        No       Config    Enabled
Enabled   global_access
5    Extended   2        0        2        0        0        No       Config    Disabled
Disabled  TCP-Conn
6    Extended   8779     12       8778     0        1        No       Config    Disabled
Disabled  LIM_DSS-LIM_DSS-SY00402_access_in
7    Extended   1        0        0        0        1        Yes      Config    Enabled
Enabled   test
-------------------------------------------------------------
     Total      55230    8193     54049    0        1178
```

The **show access-list internal** command provides a table with the following information:

- Id—The index identifier.
- Type—The ACL type: Extended, Ethertype, Standard.
- Count—The total number of elements in the ACL.
- OG-cnt—The number of object groups used in the ACL.
- Permit—The number of Permit rules in the ACL.
- Deny—The number of Deny rules in the ACL.
- AG-fwdref—Yes if the access-group command is configured for an undefined ACL. No if the ACL exists.
- Mode—How the AC was created: Config means it is directly configured, such as access control rules; Dynamic means is it a dynamic ACL (DACL)
- OGS—Whether object-group-search applies for the ACL, Enabled or Disabled. Object-group-search applies for ACL used in access control (access-group) only.
- IOO—Whether interface object optimization applies for the ACL, Enabled or Disabled.
- Name—The name of the ACL.
- Total—Totals for all ACLs for the numeric columns.

Related Commands

Command	Description
access-list ethertype	Configures an access list that controls traffic based on its EtherType.
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the firewall.
clear access-list	Clears an access list counter.
clear configure access-list	Clears an access list from the running configuration.
show running-config access-list	Displays the current running access-list configuration.

show activation-key

To display the permanent license, active time-based licenses, and the running license, which is a combination of the permanent license and active time-based licenses. use the **show activation-key** command in privileged EXEC mode. For failover units, this command also shows the "Failover cluster" license, which is the combined keys of the primary and secondary units.

show activation-key [**detail**]

Syntax Description

detail	Shows inactive time-based licenses.

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.
8.0(4)	The **detail** keyword was added.
8.2(1)	The output was modified to include additional licensing information.
8.3(1)	The output now includes whether a feature uses the permanent or time-based key, as well as the duration of the time-based key in use. It also shows all installed time-based keys, both active and inactive.
8.4(1)	Support for No Payload Encryption models was added.

Usage Guidelines

Some permanent licenses require you to reload the ASA after you activate them. <xref> lists the licenses that require reloading.

Table 1: Permanent License Reloading Requirements

Model	License Action Requiring Reload
All models	Downgrading the Encryption license.
ASA Virtual	Downgrading the vCPU license.

If you need to reload, then the **show activation-key** output reads as follows:

```
The flash activation key is DIFFERENT from the running key.
The flash activation key takes effect after the next reload.
```

If you have a No Payload Encryption model, then when you view the license, VPN and Unified Communications licenses will not be listed.

Examples

Example 2-1 Standalone Unit Output for the show activation-key command

The following is sample output from the **show activation-key** command for a standalone unit that shows the running license (the combined permanent license and time-based licenses), as well as each active time-based license:

```
ciscoasa# show activation-key
Serial Number:  JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual
This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days

0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days
```

Example 2-2 Standalone Unit Output for show activation-key detail

The following is sample output from the **show activation-key detail** command for a standalone unit that shows the running license (the combined permanent license and time-based licenses), as well as the permanent license and each installed time-based license (active and inactive):

```
ciscoasa# show activation-key detail
Serial Number:  88810093382
```

```
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual
This platform has an ASA 5505 Security Plus license.
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.
Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    39 days
Inactive Timebased Activation Key:
0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3
AnyConnect Premium Peers                  : 25     7 days
```

Example 2-3 Primary Unit Output in a Failover Pair for show activation-key detail

The following is sample output from the **show activation-key detail** command for the primary failover unit that shows:

- The primary unit license (the combined permanent license and time-based licenses).
- The “Failover Cluster” license, which is the combined licenses from the primary and secondary units. This is the license that is actually running on the ASA. The values in this license that reflect the combination of the primary and secondary licenses are in bold.

- The primary unit permanent license.
- The primary unit installed time-based licenses (active and inactive).

```
ciscoasa# show activation-key detail
Serial Number:  P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual
This platform has an ASA 5520 VPN Plus license.
Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers       : 4           perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
            Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual
This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
```

```
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.
Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    33 days
Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts               : 2          7 days
AnyConnect Premium Peers                   : 100        7 days
0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4
Total UC Proxy Sessions         : 100        14 days
```

Example 2-4 Secondary Unit Output in a Failover Pair for show activation-key detail

The following is sample output from the **show activation-key detail** command for the secondary failover unit that shows:

- The secondary unit license (the combined permanent license and time-based licenses).
- The "Failover Cluster" license, which is the combined licenses from the primary and secondary units. This is the license that is actually running on the ASA. The values in this license that reflect the combination of the primary and secondary licenses are in bold.
- The secondary unit permanent license.
- The secondary installed time-based licenses (active and inactive). This unit does not have any time-based licenses, so none display in this sample output.

```
ciscoasa# show activation-key detail
Serial Number:  P3000000011
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1
Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
```

```
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual
This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
            Security Contexts              : 10             perpetual
            GTP/GPRS                       : Enabled        perpetual
            AnyConnect Premium Peers          : 4              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
            Total UC Proxy Sessions        : 4              perpetual
            Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual
This platform has an ASA 5520 VPN Plus license.
Running Permanent Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1
Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual
The flash permanent activation key is the SAME as the running permanent key.
```

Example 2-5 Standalone Unit Output for the ASA Virtual without a License for show activation-key

The following output for a deployed 1 vCPU ASA Virtual shows a blank activation key, an Unlicensed status, and a message to install a 1 vCPU license.

Note The command output shows, “This platform has an ASA Virtual VPN Premium license.” This message specifies that the ASA Virtual can perform payload encryption; it does not refer to the ASA Virtual Standard vs. Premium licenses.

```
ciscoasa# show activation-key
Serial Number:  9APM1G4RV41
Running Permanent Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
ASAv Platform License State: Unlicensed
*Install 1 vCPU ASAv platform license for full functionality.
The Running Activation Key is not valid, using default settings:
Licensed features for this platform:
Virtual CPUs                      : 0              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual
This platform has an ASAv VPN Premium license.
Failed to retrieve flash permanent activation key.
The flash permanent activation key is the SAME as the running permanent key.
```

Example 2-6 Standalone Unit Output for the ASA Virtual with a 4 vCPU Standard License for show activation-key



Note The command output shows, “This platform has an ASA Virtual VPN Premium license.” This message specifies that the ASA Virtual can perform payload encryption; it does not refer to the ASA Virtual Standard vs. Premium licenses.

```
ciscoasa# show activation-key

Serial Number:  9ALQ8W1XCJ7
Running Permanent Activation Key: 0x0013e945 0x685a232c 0x1153fdac 0xeae8b068 0x4413f4ae
ASAv Platform License State: Compliant
Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
```

```
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual
This platform has an ASAv VPN Premium license.
The flash permanent activation key is the SAME as the running permanent key.
```

Example 2-7 Standalone Unit Output for the ASA Virtual with a 4 vCPU Premium License for show activation-key

Note The command output shows, “This platform has an ASA Virtual VPN Premium license.” This message specifies that the ASA Virtual can perform payload encryption; it does not refer to the ASA Virtual Standard vs. Premium licenses.

```
ciscoasa# show activation-key
Serial Number:  9ALQ8W1XCJ7
Running Permanent Activation Key: 0x8224dd7d 0x943ed77c 0x9d71cdd0 0xd90474d0 0xcb04df82
ASAv Platform License State: Compliant
Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 750            perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Enabled        perpetual
AnyConnect for Cisco VPN Phone    : Enabled        perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
UC Phone Proxy Sessions           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual
This platform has an ASAv VPN Premium license.
The flash permanent activation key is the SAME as the running permanent key.
ciscoasa#
```

Example 2-8 Primary Unit Output for the ASA Services Module in a Failover Pair for show activation-key

The following is sample output from the **show activation-key** command for the primary failover unit that shows:

- The primary unit license (the combined permanent license and time-based licenses).

- The “Failover Cluster” license, which is the combined licenses from the primary and secondary units. This is the license that is actually running on the ASA. The values in this license that reflect the combination of the primary and secondary licenses are in bold.
- The primary unit installed time-based licenses (active and inactive).

```
ciscoasa# show activation-key
erial Number:  SAL144705BF
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.
Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.
The flash permanent activation key is the SAME as the running permanent key.
Active Timebased Activation Key:
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Botnet Traffic Filter           : Enabled    330 days
```

Example 2-9 Secondary Unit Output for the ASA Services Module in a Failover Pair for show activation-key

The following is sample output from the **show activation-key** command for the secondary failover unit that shows:

- The secondary unit license (the combined permanent license and time-based licenses).
- The “Failover Cluster” license, which is the combined licenses from the primary and secondary units. This is the license that is actually running on the ASA. The values in this license that reflect the combination of the primary and secondary licenses are in bold.
- The secondary installed time-based licenses (active and inactive). This unit does not have any time-based licenses, so none display in this sample output.

```
ciscoasa# show activation-key detail
Serial Number:  SAD143502E3
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683
Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
```

```
GTP/GPRS                          : Disabled       perpetual
Botnet Traffic Filter             : Disabled       perpetual
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.
Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.
The flash permanent activation key is the SAME as the running permanent key.
```

Example 2-10 Output in a Cluster for show activation-key

```
ciscoasa# show activation-key
 Serial Number: JMX1504L2TD
 Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4143a90c 0xe5849088 0x4412d4a9
 Licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 2 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 2 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 2 perpetual
 Total UC Proxy Sessions : 2 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual
 This platform has an ASA 5585-X base license.
 Failover cluster licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 4 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 4 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 4 perpetual
 Total UC Proxy Sessions : 4 perpetual
 Botnet Traffic Filter : Disabled perpetual
```

```
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual
 This platform has an ASA 5585-X base license.
 The flash permanent activation key is the SAME as the running permanent key.
Serial Number:  JMX1232L11M
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1
Running Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited  perpetual
Maximum VLANs                : 50         perpetual
Inside Hosts                 : Unlimited  perpetual
Failover                     : Disabled   perpetual
VPN-DES                      : Enabled    perpetual
VPN-3DES-AES                 : Enabled    perpetual
Security Contexts            : 0          perpetual
GTP/GPRS                     : Disabled   perpetual
SSL VPN Peers                : 2          perpetual
Total VPN Peers              : 250        perpetual
Shared License               : Disabled   perpetual
AnyConnect for Mobile        : Disabled   perpetual
AnyConnect for Linksys phone : Disabled   perpetual
AnyConnect Essentials        : Enabled    perpetual
Advanced Endpoint Assessment : Disabled   perpetual
UC Phone Proxy Sessions      : 12         62 days
Total UC Proxy Sessions      : 12         62 days
Botnet Traffic Filter        : Enabled    646 days

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1
Botnet Traffic Filter        : Enabled    646 days
0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
SSL VPN Peers           : 100         108 days
```

Related Commands

Command	Description
activation-key	Changes the activation key.

show ad-groups

To display groups that are listed on an Active Directory server, use the **show ad-groups** command in privileged EXEC mode:

show ad-groups *name* [**filter** *string*]

Syntax Description

name	The name of the Active Directory server group to query.
string	A string within quotes specifying all or part of the group name to search for.

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 mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	This command was added.

Usage Guidelines

The show ad-groups command applies only to Active Directory servers that use the LDAP protocol to retrieve groups. Use this command to display AD groups that you can use for dynamic access policy AAA selection criteria.

When the LDAP attribute type = LDAP, the default time that the ASA waits for a response from the server is 10 seconds. You can adjust this time using the **group-search-timeout** command in aaa-server host configuration mode.

Note If the Active Directory server has a large number of groups, the output of the **show ad-groups command** may be truncated based on limitations of the amount of data the server can fit into a response packet. To avoid this problem, use the **filter** option to reduce the number of groups reported by the server.

Examples

```
ciscoasa# show ad-groups LDAP-AD17
            Server Group    LDAP-AD17

            Group list retrieved successfully
```

```
Number of Active Directory Groups       46

Account Operators

Administrators

APP-SSL-VPN CIO Users

Backup Operators

Cert Publishers

CERTSVC_DCOM_ACCESS

Cisco-Eng

DHCP Administrators

DHCP Users

Distributed COM Users

DnsAdmins

DnsUpdateProxy

Doctors

Domain Admins

Domain Computers

Domain Controllers

Domain Guests

Domain Users

Employees

Engineering

Engineering1

Engineering2

Enterprise Admins

Group Policy Creator Owners

Guests

HelpServicesGroup
```

The next example shows the same command with the **filter** option:

```
ciscoasa(config)# show ad-groups LDAP-AD17 filter “Eng”
.

Server Group    LDAP-AD17
```

```
Group list retrieved successfully

Number of Active Directory Groups       4

Cisco-Eng

Engineering

Engineering1

Engineering2
```

Related Commands

Command	Description
ldap-group-base-dn	Specifies a level in the Active Directory hierarchy where the server begins searching for groups that are used by dynamic group policies.
group-search-timeout	Adjusts the time the ASA waits for a response from an Active Directory server for a list of groups.

show admin-context

To display the context name currently assigned as the admin context, use the **show admin-context** command in privileged EXEC mode.

show admin-context

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 mode	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show admin-context** command. The following example shows the admin context called “admin” and stored in the root directory of flash:

```
ciscoasa# show admin-context
Admin: admin flash:/admin.cfg
```

Related Commands

Command	Description
admin-context	Sets the admin context.
changeto	Changes between contexts or the system execution space.
clear configure context	Removes all contexts.
mode	Sets the context mode to single or multiple.
show context	Shows a list of contexts (system execution space) or information about the current context.

show alarm settings

To display the configuration for each type of alarm in the ISA 3000, use the **show alarm settings** command in user EXEC mode.

show alarm settings

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.7(1)	We introduced this command.

Examples

The following is a sample output from the **show alarm settings** command:

```
ciscoasa> show alarm settings

Power Supply
         Alarm                   Disabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Disabled
Temperature-Primary
         Alarm                   Enabled
         Thresholds              MAX: 92C                MIN: -40C
         Relay                   Enabled
         Notifies                Enabled
         Syslog                  Enabled
Temperature-Secondary
         Alarm                   Disabled
         Threshold
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Disabled
Input-Alarm 1
         Alarm                   Enabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Enabled
```

```
Input-Alarm 2
         Alarm                   Enabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Enabled
```

Related Commands

Command	Description
alarm contact description	Specifies the description for the alarm inputs.
alarm contact severity	Specifies the severity of alarms.
alarm contact trigger	Specifies a trigger for one or all alarm inputs.
alarm facility input-alarm	Specifies the logging and notification options for alarm inputs.
alarm facility power-supply rps	Configures the power supply alarms.
alarm facility temperature	Configures the temperature alarms.
alarm facility temperature (high and low thresholds)	Configures the low or high temperature threshold value.
show environment alarm-contact	Displays all external alarm settings.
show facility-alarm relay	Displays relay in activated state.
show facility-alarm status	Displays all triggered alarms, or alarms based on severity specified.
clear facility-alarm output	De-energizes the output relay and clears the alarm state of the LED.

show arp

To view the ARP table, use the **show arp** command in privileged EXEC mode.

show arp

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(8)/7.2(4)/8.0(4)	Dynamic ARP age was added to the display.

Usage Guidelines

The display output shows dynamic, static, and proxy ARP entries. Dynamic ARP entries include the age of the ARP entry in seconds. Static ARP entries include a dash (-) instead of the age, and proxy ARP entries state “alias.”

Examples

The following is sample output from the **show arp** command. The first entry is a dynamic entry aged 2 seconds. The second entry is a static entry, and the third entry is from proxy ARP.

```
ciscoasa# show arp
        outside 10.86.194.61 0011.2094.1d2b 2
        outside 10.86.194.1 001a.300c.8000 -
        outside 10.86.195.2 00d0.02a8.440a alias
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	Inspects ARP packets to prevent ARP spoofing.
clear arp statistics	Clears ARP statistics.
show arp statistics	Shows ARP statistics.

Command	Description
show running-config arp	Shows the current configuration of the ARP timeout.

show arp-inspection

To view the ARP inspection setting for each interface, use the **show arp-inspection** command in privileged EXEC mode.

show arp-inspection

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.
9.7(1)	Support for routed mode was added.

Examples

The following is sample output from the **show arp-inspection** command:

```
ciscoasa# show arp-inspection
interface               arp-inspection         miss
-------------------------------------------------------
inside1                 enabled                flood
outside                 disabled                -
```

The **miss** column shows the default action to take for non-matching packets when ARP inspection is enabled, either “flood” or “no-flood.”

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	Inspects ARP packets to prevent ARP spoofing.
clear arp statistics	Clears ARP statistics.
show arp statistics	Shows ARP statistics.

Command	Description
show running-config arp	Shows the current configuration of the ARP timeout.

show arp rate-limit

To show the ARP rate limit setting, use the **show arp rate-limit** command in privileged EXEC mode.

show arp rate-limit

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
9.6(2)	We introduced this command.

Usage Guidelines

Use this command to view the **arp rate-limit** setting.

Examples

The following example shows the ARP rate as 10000 per second:

```
ciscoasa# show arp rate-limit
arp rate-limit 10000
```

Related Commands

Command	Description
arp rate-limit	Sets the ARP rate limit.

show arp statistics

To view ARP statistics, use the show arp statistics command in privileged EXEC mode.

show arp statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show arp statistics** command:

```
ciscoasa# show arp statistics
        Number of ARP entries:
        ASA : 6
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

Table 2 shows each field description.

Table 2: show arp statistics Fields

Field	Description
Number of ARP entries	The total number of ARP table entries.
Dropped blocks in ARP	The number of blocks that were dropped while IP addresses were being resolved to their corresponding hardware addresses.

Field	Description
Maximum queued blocks	The maximum number of blocks that were ever queued in the ARP module, while waiting for the IP address to be resolved.
Queued blocks	The number of blocks currently queued in the ARP module.
Interface collision ARPs received	The number of ARP packets received at all ASA interfaces that were from the same IP address as that of an ASA interface.
ARP-defense gratuitous ARPs sent	The number of gratuitous ARPs sent by the ASA as part of the ARP-Defense mechanism.
Total ARP retries	The total number of ARP requests sent by the ARP module when the address was not resolved in response to first ARP request.
Unresolved hosts	The number of unresolved hosts for which ARP requests are still being sent out by the ARP module.
Maximum unresolved hosts	The maximum number of unresolved hosts that ever were in the ARP module since it was last cleared or the ASA booted up.

Related Commands

Command	Description
arp-inspection	Inspects ARP packets to prevent ARP spoofing.
clear arp statistics	Clears ARP statistics and resets the values to zero.
show arp	Shows the ARP table.
show running-config arp	Shows the current configuration of the ARP timeout.

show arp vtep-mapping

To display MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses, use the **show arp vtep-mapping** command in privileged EXEC mode.

show arp vtep-mapping

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
9.4(1)	This command was added.

Usage Guidelines

When the ASA sends a packet to a device behind a peer VTEP, the ASA needs two important pieces of information:

- The destination MAC address of the remote device
- The destination IP address of the peer VTEP

There are two ways in which the ASA can find this information:

- A single peer VTEP IP address can be statically configured on the ASA.

You cannot manually define multiple peers.

The ASA then sends a VXLAN-encapsulated ARP broadcast to the VTEP to learn the end node MAC address.

- A multicast group can be configured on each VNI interface (or on the VTEP as a whole).

The ASA sends a VXLAN-encapsulated ARP broadcast packet within an IP multicast packet through the VTEP source interface. The response to this ARP request enables the ASA to learn both the remote VTEP IP address along with the destination MAC address of the remote end node.

The ASA maintains a mapping of destination MAC addresses to remote VTEP IP addresses for the VNI interfaces.

Examples

See the following output for the **show arp vtep-mapping** command:

```
ciscoasa# show arp vtep-mapping
vni-outside 192.168.1.4 0012.0100.0003 577 15.1.2.3
vni-inside 192.168.0.4 0014.0100.0003 577 15.1.2.3
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
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.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

show asdm history

To display the contents of the ASDM history buffer, use the **show asdm history** command in privileged EXEC mode.

show asdm history [**view** *timeframe*] [**snapshot**] [**feature** *feature*] [**asdmclient**]

Syntax Description

asdmclient	(Optional) Displays the ASDM history data formatted for the ASDM client.
feature *feature*	(Optional) Limits the history display to the specified feature. The following are valid values for the *feature* argument: • **all** —Displays the history for all features (default). • **blocks** —Displays the history for the system buffers. • **cpu** —Displays the history for CPU usage. • **failover** —Displays the history for failover. • **ids** —Displays the history for IDS. • **interface** *if_name* —Displays the history for the specified interface. The *if_name* argument is the name of the interface as specified by the **nameif** command. • **memory** —Displays memory usage history. • **perfmon** —Displays performance history. • **sas** —Displays the history for Security Associations. • **tunnels** —Displays the history for tunnels. • **xlates** —Displays translation slot history.
snapshot	(Optional) Displays only the last ASDM history data point.
view *timeframe*	(Optional) Limits the history display to the specified time period. Valid values for the *timeframe* argument are: • **all** —all contents in the history buffer (default). • **12h** —12 hours • **5d** —5 days • **60m** —60 minutes • **10m** —10 minutes

Command Default

If no arguments or keywords are specified, all history information for all features is displayed.

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 **show pdm history** command to the **show asdm history** command.

Usage Guidelines

The **show asdm history** command displays the contents of the ASDM history buffer. Before you can view ASDM history information, you must enable ASDM history tracking using the **asdm history enable** command.

Examples

The following is sample output from the **show asdm history** command. It limits the output to data for the outside interface collected during the last 10 minutes.

```
ciscoasa# show asdm history view 10m feature interface outside
Input KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 62640 62636 62633 62628 62622 62616 62609
Output KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 25178 25169 25165 25161 25157 25151 25147
Input KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]   752   752   751   751   751   751   751
Output KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]    55    55    55    55    55    55    55
Input Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  3397  2843  3764  4515  4932  5728  4186
Output Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  7316  3292  3349  3298  5212  3349  3301
Input Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     5     4     6     7     6     8     6
Output Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     1     0     0     0     0     0     0
Input Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
No Buffer:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Received Broadcasts:
        [  10s:12:46:41 Mar 1 2005  ] 375974 375954 375935 375902 375863 375833 375794
Runts:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Giants:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
CRC:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Frames:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Overruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Underruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Output Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
```

```
Collisions:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
LCOLL:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Reset:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Deferred:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Lost Carrier:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]   128   128   128   128   128   128   128
Software Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Software Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Drop KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
ciscoasa#
```

The following is sample output from the **show asdm history** command. Like the previous example, it limits the output to data for the outside interface collected during the last 10 minutes. However, in this example the output is formatted for the ASDM client.

```
ciscoasa# show asdm history view 10m feature interface outside asdmclient
MH|IBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|62439|62445|62453|62457|62464|
62469|62474|62486|62489|62496|62501|62506|62511|62518|62522|62530|62534|62539|62542|62547|
62553|62556|62562|62568|62574|62581|62585|62593|62598|62604|62609|62616|62622|62628|62633|
62636|62640|62653|62657|62665|62672|62678|62681|62686|62691|62695|62700|62704|62711|62718|
62723|62728|62733|62738|62742|62747|62751|62761|62770|62775|
...
```

The following is sample output from the **show asdm history** command using the **snapshot** keyword:

```
ciscoasa# show asdm history view 10m snapshot
Available 4 byte Blocks:  [  10s] : 100
Used 4 byte Blocks:  [  10s] : 0
Available 80 byte Blocks:  [  10s] : 100
Used 80 byte Blocks:  [  10s] : 0
Available 256 byte Blocks:  [  10s] : 2100
Used 256 byte Blocks:  [  10s] : 0
Available 1550 byte Blocks:  [  10s] : 7425
Used 1550 byte Blocks:  [  10s] : 1279
Available 2560 byte Blocks:  [  10s] : 40
Used 2560 byte Blocks:  [  10s] : 0
Available 4096 byte Blocks:  [  10s] : 30
Used 4096 byte Blocks:  [  10s] : 0
Available 8192 byte Blocks:  [  10s] : 60
Used 8192 byte Blocks:  [  10s] : 0
Available 16384 byte Blocks:  [  10s] : 100
Used 16384 byte Blocks:  [  10s] : 0
Available 65536 byte Blocks:  [  10s] : 10
Used 65536 byte Blocks:  [  10s] : 0
CPU Utilization:  [  10s] : 31
Input KByte Count:  [  10s] : 62930
Output KByte Count:  [  10s] : 26620
Input KPacket Count:  [  10s] : 755
Output KPacket Count:  [  10s] : 58
Input Bit Rate:  [  10s] : 24561
Output Bit Rate:  [  10s] : 518897
Input Packet Rate:  [  10s] : 48
```

```
Output Packet Rate:  [  10s] : 114
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 377331
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 3672
Output KByte Count:  [  10s] : 4051
Input KPacket Count:  [  10s] : 19
Output KPacket Count:  [  10s] : 20
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 1458
Runts:  [  10s] : 1
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 63
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 15
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
```

```
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Available Memory:  [  10s] : 205149944
Used Memory:  [  10s] : 63285512
Xlate Count:  [  10s] : 0
Connection Count:  [  10s] : 0
TCP Connection Count:  [  10s] : 0
UDP Connection Count:  [  10s] : 0
URL Filtering Count:  [  10s] : 0
URL Server Filtering Count:  [  10s] : 0
TCP Fixup Count:  [  10s] : 0
TCP Intercept Count:  [  10s] : 0
HTTP Fixup Count:  [  10s] : 0
FTP Fixup Count:  [  10s] : 0
AAA Authentication Count:  [  10s] : 0
AAA Authorzation Count:  [  10s] : 0
AAA Accounting Count:  [  10s] : 0
Current Xlates:  [  10s] : 0
Max Xlates:  [  10s] : 0
ISAKMP SAs:  [  10s] : 0
IPsec SAs:  [  10s] : 0
L2TP Sessions:  [  10s] : 0
L2TP Tunnels:  [  10s] : 0
ciscoasa#
```

Related Commands

Command	Description
asdm history enable	Enables ASDM history tracking.

show asdm image

To the current ASDM software image file, use the show **asdm image** command in privileged EXEC mode.

show asdm image

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 changed from the **show pdm image** command to the **show asdm image** command.

Examples

The following is sample output from the **show asdm image** command:

```
ciscoasa# show asdm image
Device Manager image file, flash:/ASDM
```

Related Commands

Command	Description
asdm image	Specifies the current ASDM image file.

show asdm log_sessions

To display a list of active ASDM logging sessions and their associated session IDs, use the **show asdm log_sessions** command in privileged EXEC mode.

show asdm log_sessions

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

Each active ASDM session has one or more associated ASDM logging sessions. ASDM uses the logging session to retrieve syslog messages from the ASA. Each ASDM logging session is assigned a unique session ID. You can use this session ID with the **asdm disconnect log_session** command to terminate the specified session.

Note Because each ASDM session has at least one ASDM logging session, the output for the **show asdm sessions** and **show asdm log_sessions** may appear to be the same.

Examples

The following is sample output from the **show asdm log_sessions** command:

```
ciscoasa# show asdm log_sessions
0 192.168.1.1
1 192.168.1.2
```

Related Commands

Command	Description
asdm disconnect log_session	Terminates an active ASDM logging session.

show asdm sessions

To display a list of active ASDM sessions and their associated session IDs, use the **show asdm sessions** command in privileged EXEC mode.

show asdm sessions

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 changed from the **show pdm sessions** command to the **show asdm sessions** command.

Usage Guidelines

Each active ASDM session is assigned a unique session ID. You can use this session ID with the **asdm disconnect** command to terminate the specified session.

Examples

The following is sample output from the **show asdm sessions** command:

```
ciscoasa# show asdm sessions
0 192.168.1.1
1 192.168.1.2
```

Related Commands

Command	Description
asdm disconnect	Terminates an active ASDM session.