CHAPTER 2

show aaa kerberos through show asdm sessions Commands
show aaa kerberos

To display all the Kerberos tickets cached on the ASA, use the **show aaa kerberos** command in webvpn configuration mode.

```
show aaa kerberos [username user | host ip | hostname]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>host</th>
<th>Specifies the specific host that you want to view.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>hostname</td>
<td>Specifies the hostname.</td>
</tr>
<tr>
<td></td>
<td>ip</td>
<td>Specifies the IP address for the host.</td>
</tr>
<tr>
<td></td>
<td>username</td>
<td>Specifies the specific user that you want to view.</td>
</tr>
</tbody>
</table>

**Defaults**

No defaults exist for this command.

**Command Modes**

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

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System</td>
</tr>
<tr>
<td>Webvpn configuration</td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
</tbody>
</table>

**Command History**

Release Modification
8.4(1) This command was added.

**Usage Guidelines**

Use the **show aaa kerberos** command in webvpn configuration mode to view all the Kerberos tickets cached on the ASA. The **username** and **host** keywords are used to view the Kerberos tickets of a specific user or host.

**Examples**

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

```
ciscoasa(config)# show aaa kerberos
```

```
Default Principal   Valid Starting Expires       Service Principal
kcduser@example.com 06/29/10 17:33:00 06/30/10 17:33:00 asa$/mycompany.com@example.com
kcduser@example.com 06/29/10 17:33:00 06/30/10 17:33:00
http://owa.mycompany.com@example.com
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear aaa kerberos</td>
<td>Clears all the Kerberos tickets cached on the ASA.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>clear configure</code></td>
<td>Removes all AAA command statements from the configuration.</td>
</tr>
<tr>
<td><code>aaa-server</code></td>
<td>Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>locked</th>
<th>(Optional) Shows the list of usernames that are currently locked.</th>
</tr>
</thead>
</table>

Defaults

No default behavior or values.

Command Modes

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

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Transparent</td>
<td>Single</td>
<td>Multiple</td>
</tr>
<tr>
<td>Global configuration</td>
<td>• Yes</td>
<td>• Yes</td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
</tbody>
</table>

Command History

Release   Modification
7.0(1)     This command was added.

Usage Guidelines

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

You can specify a single user by using the username option or all users with the all option.

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

The administrator cannot be locked out of the device.

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  Locked  User
    -          6              Y      test
    -          2              N      mona
    -          1              N      cisco
    -          4              N      newuser
    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:

```plaintext
ciscoasa(config)# aaa local authentication attempts max-fail 5
ciscoasa(config)# show aaa local user
Lock-time Failed-attempts Locked User
- 6 Y test
```

### Related Commands

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

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged EXEC</td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

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

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged EXEC</td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1)</td>
<td>We introduced this command.</td>
</tr>
<tr>
<td>9.12(1)</td>
<td>The output includes the privilege level of the current session and the previous session for the indicated user.</td>
</tr>
</tbody>
</table>

**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
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa authentication login-history</td>
<td>Saves the local <strong>username</strong> login history.</td>
</tr>
<tr>
<td></td>
<td>password-history</td>
<td>Stores previous <strong>username</strong> passwords. This command is not user-configurable.</td>
</tr>
<tr>
<td></td>
<td>password-policy reuse-interval</td>
<td>Prohibits the reuse of a <strong>username</strong> password.</td>
</tr>
<tr>
<td></td>
<td>password-policy username-check</td>
<td>Prohibits a password that matches a <strong>username</strong> name.</td>
</tr>
<tr>
<td></td>
<td>username</td>
<td>Configures a local user.</td>
</tr>
</tbody>
</table>
**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+`

**Defaults**

By default, all AAA server statistics display.

**Command Modes**

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

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged EXEC</td>
<td>Routed: Yes</td>
<td>Single: Yes</td>
</tr>
<tr>
<td></td>
<td>Transparent: Yes</td>
<td>Multiple: Yes</td>
</tr>
</tbody>
</table>

**Command History**

- **Release** 7.1(1) The `http-form` protocol was added.
- **Modification** 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Group</td>
<td>The server group name specified by the <code>aaa-server</code> command.</td>
</tr>
<tr>
<td>Server Protocol</td>
<td>The server protocol for the server group specified by the <code>aaa-server</code> command.</td>
</tr>
<tr>
<td>Server Address</td>
<td>The IP address of the AAA server.</td>
</tr>
<tr>
<td>Server port</td>
<td>The communication port used by the ASA and the AAA server. You can specify the RADIUS authentication port using the <code>authentication-port</code> command.</td>
</tr>
<tr>
<td></td>
<td>You can specify the RADIUS accounting port using the <code>accounting-port</code> command. For non-RADIUS servers, the port is set by the <code>server-port</code> command.</td>
</tr>
<tr>
<td>Server status</td>
<td>The status of the server. One of the following values appears:</td>
</tr>
<tr>
<td></td>
<td>• ACTIVE—The ASA will communicate with this AAA server.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>If the status is followed by “(admin initiated),” then the server was manually failed or reactivated using the <code>aaa-server active</code> command or <code>fail</code> command.</td>
</tr>
<tr>
<td></td>
<td>The date and time of the last transaction appear in the following form:</td>
</tr>
<tr>
<td></td>
<td>`Last transaction (success</td>
</tr>
<tr>
<td></td>
<td>If the ASA has never communicated with the server, the message shows as the following:</td>
</tr>
<tr>
<td></td>
<td><code>Last transaction at Unknown</code></td>
</tr>
<tr>
<td>Number of pending requests</td>
<td>The number of requests that are still in progress.</td>
</tr>
<tr>
<td>Average round trip time</td>
<td>The average time that it takes to complete a transaction with the server.</td>
</tr>
<tr>
<td>Number of authentication requests</td>
<td>The number of authentication requests sent by the ASA. This value does not include retransmissions after a timeout.</td>
</tr>
</tbody>
</table>

**Cisco ASA Series Command Reference, S Commands**
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of authorization requests</td>
<td>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.</td>
</tr>
<tr>
<td>Number of accounting requests</td>
<td>The number of accounting requests. This value does not include retransmissions after a timeout.</td>
</tr>
<tr>
<td>Number of retransmissions</td>
<td>The number of times a message was retransmitted after an internal timeout. This value applies only to Kerberos and RADIUS servers (UDP).</td>
</tr>
<tr>
<td>Number of accepts</td>
<td>The number of successful authentication requests.</td>
</tr>
<tr>
<td>Number of rejects</td>
<td>The number of rejected requests. This value includes error conditions as well as true credential rejections from the AAA server.</td>
</tr>
<tr>
<td>Number of challenges</td>
<td>The number of times the AAA server required additional information from the user after receiving the initial username and password information.</td>
</tr>
<tr>
<td>Number of malformed responses</td>
<td>N/A. Reserved for future use.</td>
</tr>
</tbody>
</table>
| 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show running-config</strong></td>
<td>Displays statistics for all servers in the indicated server group or for a particular server.</td>
</tr>
<tr>
<td><strong>aaa-server</strong></td>
<td>Displays statistics for all servers in the indicated server group or for a particular server.</td>
</tr>
<tr>
<td><strong>clear aaa-server statistics</strong></td>
<td>Clears the AAA server statistics.</td>
</tr>
</tbody>
</table>
show access-list

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

```
show access-list [id [ip_address | brief]]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>brief</code></td>
<td>(Optional) Displays the access list identifiers, the hit count, and the timestamp of the last rule hit, all in hexadecimal format.</td>
</tr>
<tr>
<td><code>id</code></td>
<td>(Optional) Shows counters for the ID of an existing access list.</td>
</tr>
<tr>
<td><code>ip_address</code></td>
<td>(Optional) Shows counters for the source IP address in the specified access list.</td>
</tr>
</tbody>
</table>

### Defaults

No default behavior or values.

### Command Modes

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

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.0(2)</td>
<td>Support for the brief keyword was added.</td>
</tr>
<tr>
<td>8.3(1)</td>
<td>The ACE show pattern to display ACL timestamp was modified.</td>
</tr>
</tbody>
</table>

### 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. A message will indicate when this happens.

### 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:

```plaintext
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) 0xc1a10ca21
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` group is not enabled:

```plaintext
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 192.168.97.0 255.255.255.0 192.168.97.0 255.255.255.0 (hitcnt=10) 0x30fe29a6
access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 13.13.13.0 255.255.255.0 (hitcnt=4) 0xc6e6f2338
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 0xb62d5832
access-list KH-BLK-Tunnel line 2 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` group is enabled:

```plaintext
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

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
cal0ca2l 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
cal0ca2l 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 TELNET-SSH object-group D1 eq telnet (hitcnt=1) 0x7b1c1660
   access-list test line 2 extended permit tcp object-group TELNET-SSH object-group D1 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

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list ethertype</td>
<td>Configures an access list that controls traffic based on its EtherType.</td>
<td></td>
</tr>
<tr>
<td>access-list extended</td>
<td>Adds an access list to the configuration and configures policy for IP traffic through the firewall.</td>
<td></td>
</tr>
<tr>
<td>clear access-list</td>
<td>Clears an access list counter.</td>
<td></td>
</tr>
<tr>
<td>clear configure access-list</td>
<td>Clears an access list from the running configuration.</td>
<td></td>
</tr>
<tr>
<td>show running-config access-list</td>
<td>Displays the current running access-list configuration.</td>
<td></td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Shows inactive time-based licenses.</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values.

**Command Modes**

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

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0(1)</td>
<td>This command was added.</td>
</tr>
<tr>
<td>8.0(4)</td>
<td>The <code>detail</code> keyword was added.</td>
</tr>
<tr>
<td>8.2(1)</td>
<td>The output was modified to include additional licensing information.</td>
</tr>
<tr>
<td>8.3(1)</td>
<td>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.</td>
</tr>
<tr>
<td>8.4(1)</td>
<td>Support for No Payload Encryption models was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Some permanent licenses require you to reload the ASA after you activate them. Table 2-1 lists the licenses that require reloading.

**Table 2-1 Permanent License Reloading Requirements**

<table>
<thead>
<tr>
<th>Model</th>
<th>License Action Requiring Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>All models</td>
<td>Downgrading the Encryption license.</td>
</tr>
<tr>
<td>ASA v</td>
<td>Downgrading the vCPU license.</td>
</tr>
</tbody>
</table>

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
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           : 12             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 each installed time-based license (active and inactive):

```
ciscoasa# show activation-key detail
Serial Number: JMX1232L11M
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                 : 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           : 12             62 days
```
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:
<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Physical Interfaces</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Maximum VLANS</td>
<td>150</td>
</tr>
<tr>
<td>Inside Hosts</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Active</td>
</tr>
<tr>
<td>VPN-DES</td>
<td>Enabled</td>
</tr>
<tr>
<td>VPN-3DES-AES</td>
<td>Enabled</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>12</td>
</tr>
<tr>
<td>GTP/GPRS</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect Premium Peers</td>
<td>2</td>
</tr>
<tr>
<td>AnyConnect Essentials</td>
<td>Disabled</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>750</td>
</tr>
<tr>
<td>Total VPN Peers</td>
<td>750</td>
</tr>
<tr>
<td>Shared License</td>
<td>Disabled</td>
</tr>
<tr>
<td>AnyConnect for Mobile</td>
<td>Disabled</td>
</tr>
<tr>
<td>AnyConnect for Cisco VPN Phone</td>
<td>Disabled</td>
</tr>
<tr>
<td>Advanced Endpoint Assessment</td>
<td>Disabled</td>
</tr>
<tr>
<td>UC Phone Proxy Sessions</td>
<td>2</td>
</tr>
<tr>
<td>Total UC Proxy Sessions</td>
<td>2</td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Enabled</td>
</tr>
<tr>
<td>Intercompany Media Engine</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Physical Interfaces</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Maximum VLANS</td>
<td>150</td>
</tr>
<tr>
<td>Inside Hosts</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Active</td>
</tr>
<tr>
<td>VPN-DES</td>
<td>Enabled</td>
</tr>
<tr>
<td>VPN-3DES-AES</td>
<td>Enabled</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>12</td>
</tr>
<tr>
<td>GTP/GPRS</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect Premium Peers</td>
<td>4</td>
</tr>
<tr>
<td>AnyConnect Essentials</td>
<td>Disabled</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>750</td>
</tr>
<tr>
<td>Total VPN Peers</td>
<td>750</td>
</tr>
<tr>
<td>Shared License</td>
<td>Disabled</td>
</tr>
<tr>
<td>AnyConnect for Mobile</td>
<td>Disabled</td>
</tr>
<tr>
<td>AnyConnect for Cisco VPN Phone</td>
<td>Disabled</td>
</tr>
<tr>
<td>Advanced Endpoint Assessment</td>
<td>Disabled</td>
</tr>
<tr>
<td>UC Phone Proxy Sessions</td>
<td>4</td>
</tr>
<tr>
<td>Total UC Proxy Sessions</td>
<td>4</td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

This platform has an ASA 5520 VPN Plus license.
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.

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           : 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.
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 ASAv without a License for show activation-key

The following output for a deployed 1 vCPU ASAv 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 ASAv VPN Premium license.” This message specifies that the ASAv can perform payload encryption; it does not refer to the ASAv Standard vs. Premium licenses.

ciscoasa# show activation-key
Serial Number: 9APM1G61RV41
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 ASAv with a 4 vCPU Standard License for show activation-key

The command output shows, “This platform has an ASAv VPN Premium license.” This message specifies that the ASAv can perform payload encryption; it does not refer to the ASAv 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 ASAv with a 4 vCPU Premium License for show activation-key

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

This platform has an ASAv VPN Premium license.
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

  serial Number:  SAL144705BF
  Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
  Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f88880

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        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 
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.

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

Serial Number: JMX1232L11M  
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 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:
Oxyadayad1 Oxyadayad1 Oxyadayad1 Oxyadayad1 Oxyadayad1
Botnet Traffic Filter : Enabled 646 days
Oxyadayad2 Oxyadayad2 Oxyadayad2 Oxyadayad2 Oxyadayad2
Total UC Proxy Sessions : 10 62 days

Inactive Timebased Activation Key:
Oxyadayad3 Oxyadayad3 Oxyadayad3 Oxyadayad3 Oxyadayad3
SSL VPN Peers : 100 108 days

---

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>activation-key</strong></td>
<td>Changes the activation key.</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name of the Active Directory server group to query.</td>
</tr>
<tr>
<td>string</td>
<td>A string within quotes specifying all or part of the group name to search for.</td>
</tr>
</tbody>
</table>

### Defaults

No default behavior or values.

### Command Modes

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

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Trans pare nt</td>
</tr>
<tr>
<td></td>
<td>Single</td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td>Context</td>
<td>System</td>
</tr>
<tr>
<td>Privileged EXEC mode</td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.0(4)</td>
<td>This command was added.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap-group-base-dn</td>
<td>Specifies a level in the Active Directory hierarchy where the server begins searching for groups that are used by dynamic group policies.</td>
</tr>
<tr>
<td>group-search-timeout</td>
<td>Adjusts the time the ASA waits for a response from an Active Directory server for a list of groups.</td>
</tr>
</tbody>
</table>
**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
```

**Defaults**

No default behavior or values.

**Command Modes**

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

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Transpareent</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin-context</td>
<td>Sets the admin context.</td>
</tr>
<tr>
<td>changeto</td>
<td>Changes between contexts or the system execution space.</td>
</tr>
<tr>
<td>clear configure context</td>
<td>Removes all contexts.</td>
</tr>
<tr>
<td>mode</td>
<td>Sets the context mode to single or multiple.</td>
</tr>
<tr>
<td>show context</td>
<td>Shows a list of contexts (system execution space) or information about the current context.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td>Global configuration</td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.7(1)</td>
<td>We introduced this command.</td>
</tr>
</tbody>
</table>

**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               Disabled
   Relay                   Disabled
   Notifies                Disabled
   Syslog                  Disabled
Input-Alarm 1
   Alarm                   Enabled
   Relay                   Disabled
   Notifies                Disabled
   Syslog                  Enabled
Input-Alarm 2
   Alarm                   Enabled
```
### Chapter

<table>
<thead>
<tr>
<th>Relay</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notifies</td>
<td>Disabled</td>
</tr>
<tr>
<td>Syslog</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

#### Related Commands

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

**Defaults**

No default behavior or values.

**Command Modes**

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

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0(8)/7.2(4)/8.0(4)</td>
<td>Dynamic ARP age was added to the display.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp</td>
<td>Adds a static ARP entry.</td>
</tr>
<tr>
<td>arp-inspection</td>
<td>Inspects ARP packets to prevent ARP spoofing.</td>
</tr>
<tr>
<td>clear arp statistics</td>
<td>Clears ARP statistics.</td>
</tr>
<tr>
<td>show arp statistics</td>
<td>Shows ARP statistics.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Shows the current configuration of the ARP timeout.</td>
</tr>
<tr>
<td>show running-config</td>
<td></td>
</tr>
<tr>
<td>show running-config</td>
<td></td>
</tr>
</tbody>
</table>
**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.

**Defaults**
No default behavior or values.

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

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Transient</td>
<td>Single</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0(1)</td>
<td>This command was added.</td>
</tr>
<tr>
<td>9.7(1)</td>
<td>Support for routed mode was added.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp</td>
<td>Adds a static ARP entry.</td>
</tr>
<tr>
<td>arp-inspection</td>
<td>Inspects ARP packets to prevent ARP spoofing.</td>
</tr>
<tr>
<td>clear arp statistics</td>
<td>Clears ARP statistics.</td>
</tr>
<tr>
<td>show arp statistics</td>
<td>Shows ARP statistics.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Shows the current configuration of the ARP timeout.</td>
</tr>
<tr>
<td>arp</td>
<td></td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
<tr>
<td></td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.6(2)</td>
<td>We introduced this command.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp rate-limit</td>
<td>Sets the ARP rate limit.</td>
</tr>
</tbody>
</table>
### 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.

**Defaults**

No default behavior or values.

**Command Modes**

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

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Multiple Context</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0(1)</td>
<td>This command was added.</td>
</tr>
</tbody>
</table>

**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 2-2  show arp statistics Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of ARP entries</td>
<td>The total number of ARP table entries.</td>
</tr>
<tr>
<td>Dropped blocks in ARP</td>
<td>The number of blocks that were dropped while IP addresses were being resolved to their corresponding hardware addresses.</td>
</tr>
<tr>
<td>Maximum queued blocks</td>
<td>The maximum number of blocks that were ever queued in the ARP module, while waiting for the IP address to be resolved.</td>
</tr>
</tbody>
</table>
### Table 2-2  
**show arp statistics Fields (continued)**

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp-inspection</td>
<td>Inspects ARP packets to prevent ARP spoofing.</td>
</tr>
<tr>
<td>clear arp statistics</td>
<td>Clears ARP statistics and resets the values to zero.</td>
</tr>
<tr>
<td>show arp</td>
<td>Shows the ARP table.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Shows the current configuration of the ARP timeout.</td>
</tr>
<tr>
<td>arp</td>
<td></td>
</tr>
</tbody>
</table>
**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:

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Transpare</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.4(1)</td>
<td>This command was added.</td>
</tr>
</tbody>
</table>

**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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>asdmclient (Optional) Displays the ASDM history data formatted for the ASDM client.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>feature feature (Optional) Limits the history display to the specified feature. The following are valid values for the feature argument:</td>
</tr>
<tr>
<td></td>
<td>• all—Displays the history for all features (default).</td>
</tr>
<tr>
<td></td>
<td>• blocks—Displays the history for the system buffers.</td>
</tr>
<tr>
<td></td>
<td>• cpu—Displays the history for CPU usage.</td>
</tr>
<tr>
<td></td>
<td>• failover—Displays the history for failover.</td>
</tr>
<tr>
<td></td>
<td>• ids—Displays the history for IDS.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• memory—Displays memory usage history.</td>
</tr>
<tr>
<td></td>
<td>• perfmon—Displays performance history.</td>
</tr>
<tr>
<td></td>
<td>• sas—Displays the history for Security Associations.</td>
</tr>
<tr>
<td></td>
<td>• tunnels—Displays the history for tunnels.</td>
</tr>
<tr>
<td></td>
<td>• xlates—Displays translation slot history.</td>
</tr>
<tr>
<td></td>
<td>snapshot (Optional) Displays only the last ASDM history data point.</td>
</tr>
<tr>
<td></td>
<td>view timeframe (Optional) Limits the history display to the specified time period. Valid values for the timeframe argument are:</td>
</tr>
<tr>
<td></td>
<td>• all—all contents in the history buffer (default).</td>
</tr>
<tr>
<td></td>
<td>• 12h—12 hours</td>
</tr>
<tr>
<td></td>
<td>• 5d—5 days</td>
</tr>
<tr>
<td></td>
<td>• 60m—60 minutes</td>
</tr>
<tr>
<td></td>
<td>• 10m—10 minutes</td>
</tr>
</tbody>
</table>

Defaults

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:

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0(1)</td>
<td>This command was changed from the <code>show pdm history</code> command to the <code>show asdm history</code> command.</td>
</tr>
</tbody>
</table>

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:
Output KByte Count:
Input KPacket Count:
Output KPacket Count:
Input Bit Rate:
  [ 10s:12:46:41 Mar 1 2005 ] 3397 2843 3764 4515 4932 5728 4186
Output Bit Rate:
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:
```
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|10c|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
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
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 Authorization 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#

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>asdm history enable</td>
<td>Enables ASDM history tracking.</td>
</tr>
</tbody>
</table>
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.

**Defaults**
No default behavior or values.

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

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0(1)</td>
<td>This command was changed from the show pdm image command to the show asdm image command.</td>
</tr>
</tbody>
</table>

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>asdm image</td>
<td>Specifies the current ASDM image file.</td>
</tr>
</tbody>
</table>
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.

**Defaults**
No default behavior or values.

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

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Single</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0(1)</td>
<td>This command was added.</td>
</tr>
</tbody>
</table>

**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:

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>asdm disconnect</td>
<td>Terminates an active ASDM logging session.</td>
</tr>
<tr>
<td>log_session</td>
<td></td>
</tr>
</tbody>
</table>
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.

**Defaults**
No default behavior or values.

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

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0(1)</td>
<td>This command was changed from the <code>show pdm sessions</code> command to the <code>show asdm sessions</code> command.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>asdm disconnect</td>
<td>Terminates an active ASDM session.</td>
</tr>
</tbody>
</table>