

show u – show z

- show uauth, on page 3
- show url-block, on page 5
- show url-cache statistics, on page 7
- show url-server, on page 9
- show usb-port, on page 12
- show user-alert, on page 13
- show user-identity ad-agent, on page 14
- show user-identity ad-group-members, on page 17
- show user-identity ad-groups, on page 19
- show user-identity ad-users, on page 21
- show user-identity group, on page 23
- show user-identity ip-of-user, on page 25
- show user-identity memory, on page 27
- show user-identity statistics, on page 29
- show user-identity statistics top user, on page 31
- show user-identity user active, on page 33
- show user-identity user all, on page 37
- show user-identity user inactive, on page 39
- show user-identity user-not-found, on page 41
- show user-identity user-of-group, on page 42
- show user-identity user-of-ip, on page 44
- show version, on page 46
- show vlan, on page 50
- show vm, on page 52
- show vni vlan-mapping, on page 54
- show vpdn, on page 56
- show vpn cluster stats internal, on page 58
- show vpn load-balancing, on page 59
- show vpn-sessiondb, on page 61
- show vpn-sessiondb ratio, on page 75
- show vpn-sessiondb summary, on page 77
- show wccp, on page 81
- show webvpn anyconnect, on page 83

- show webvpn anyconnect external-browser-pkg, on page 85
- show webvpn csd (Deprecated), on page 86
- show webvpn debug-condition, on page 89
- show webvpn group-alias, on page 90
- show webvpn group-url, on page 91
- show webvpn hostscan, on page 92
- show webvpn hsts, on page 94
- show webvpn kcd, on page 95
- show webvpn mus, on page 97
- show webvpn saml, on page 98
- show webvpn sso-server (Deprecated), on page 99
- show webvpn statistics, on page 102
- show xlate, on page 104
- show zone, on page 108

show uauth

To display one or all currently authenticated users, the host IP to which they are bound, and any cached IP and port authorization information, use the **show uauth** command in privileged EXEC mode.

show uauth [*username*]

Syntax Description

username (Optional) Specifies, by username, the user authentication and authorization information to display.

Command Default

Omitting username displays the authorization information for all users.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	The idle time was added to the output.
7.2(2)	The idle time was removed from the output.

Usage Guidelines

The **show uauth** command displays the AAA authorization and authentication caches for one user or for all users.

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

Each user host IP address has an authorization cache attached to it. The cache allows up to 16 address and service pairs for each user host. If the user attempts to access a service that has been cached from the correct host, the ASA considers it preauthorized and immediately proxies the connection. Once you are authorized to access a website, for example, the authorization server is not contacted for each image as it is loaded (assuming the images come from the same IP address). This process significantly increases performance and reduces the load on the authorization server.

The output from the **show uauth** command displays the username that is provided to the authorization server for authentication and authorization purposes, the IP address to which the username is bound, and if the user is authenticated only or has cached services.

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

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

Examples

This example shows sample output from the **show uauth** command when no users are authenticated and one user authentication is in progress:

```
ciscoasa(config)# show uauth

                        Current    Most Seen
Authenticated Users        1             1
Authen In Progress         0             1
user 'v039294' at 136.131.178.4, authenticated (idle for 0:00:00)
   access-list #ACSACL#-IP-v039294-521b0b8b (*)
   absolute   timeout: 0:00:00
   inactivity timeout: 0:05:00
```

This example shows sample output from the **show uauth** command when three users are authenticated and authorized to use services through the ASA:

```
ciscoasa(config)# show uauth
user 'pat' from 209.165.201.2 authenticated
user 'robin' from 209.165.201.4 authorized to:
                       port 192.168.67.34/telnet                          192.168.67.11/http
                                    192.168.67.33/tcp/8001
                                                      192.168.67.56/tcp/25
                  192.168.67.42/ftp
user 'terry' from 209.165.201.7 authorized to:
                       port 192.168.1.50/http
209.165.201.8/http
```

Related Commands

Command	Description
clear uauth	Removes current user authentication and authorization information.
timeout	Sets the maximum idle time duration.

show url-block

To display the number of packets held in the url-block buffer and the number (if any) dropped due to exceeding the buffer limit or retransmission, use the **show url-block** command in privileged EXEC mode.

show url-block [**block statistics**]

Syntax Description

block **statistics**	(Optional) Displays block buffer usage statistics.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show url-block block statistics** command displays the number of packets held in the url block buffer and the number (if any) dropped due to exceeding the buffer limit or retransmission.

Examples

The following is sample output from the **show url-block** command:

```
ciscoasa# show url-block
 | url-block url-mempool 128 | url-block url-size 4 | url-block block 128
```

This shows the configuration of the URL block buffer.

The following is sample output from the **show url-block block statistics** command:

```
ciscoasa# show url-block block statistics
URL Pending Packet Buffer Stats with max block  128 |
Cumulative number of packets held: | 896
Maximum number of packets held (per URL): | 3
Current number of packets held (global): | 38
Packets dropped due to
 | exceeding url-block buffer limit: | 7546
 | HTTP server retransmission: | 10
Number of packets released back to client: | 0
```

Related Commands

Commands	Description
clear url-block block statistics	Clears the block buffer usage counters.
filter url	Directs traffic to a URL filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

show url-cache statistics

To display information about the url-cache, which is used for URL responses received from an N2H2 or Websense filtering server, use the **show url-cache statistics** command in privileged EXEC mode.

show url-cache statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show url-cache statistics** command displays the following entries:

- Size—The size of the cache in kilobytes, set with the **url-cache** *size* option.
- Entries—The maximum number of cache entries based on the cache size.
- In Use—The current number of entries in the cache.
- Lookups—The number of times the ASA has looked for a cache entry.
- Hits—The number of times the ASA has found an entry in the cache.

You can view additional information about N2H2 Sentian or Websense filtering activity with the **show perfmon** command.

Examples

The following is sample output from the show url-cache statistics command:

```
ciscoasa# show url-cache statistics
URL Filter Cache Stats
----------------------
 |
Size :                                1KB
 Entries :                                    36
            In Use :                                        30
 Lookups :                                    300
```

```
 |
Hits :                                  290
```

Related Commands

Commands	Description
clear url-cache statistics	Removes url-cache command statements from the configuration.
filter url	Directs traffic to a URL filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching for responses received from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

show url-server

To display information about the URL filtering server, use the **show url-server** command in privileged EXEC mode.

show url-server statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show url-server statistics** command displays the URL server vendor; number of URLs total, allowed, and denied; number of HTTPS connections total, allowed, and denied; number of TCP connections total, allowed, and denied; and the URL server status.

The show url-server command displays the following information:

- For N2H2, **url-server (***if_name***)vendor n2h2host** *local_ip* **port** *number* **timeout** *seconds* **protocol** [{**TCP** | **UDP**}{**version 1** | **4**}]
- For Websense, **url-server (***if_name***)vendor websense host** *local_ip* **timeout** *seconds* **protocol** [{**TCP** | **UDP**}]

Examples

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

```
ciscoasa## show url-server statistics
Global Statistics:
------------------
URLs total/allowed/denied         994387/155648/838739
URLs allowed by cache/server      70483/85165
URLs denied by cache/server       801920/36819
HTTPSs total/allowed/denied       994387/155648/838739
HTTPs allowed by cache/server     70483/85165
HTTPs denied by cache/server      801920/36819
FTPs total/allowed/denied         994387/155648/838739
```

```
FTPs allowed by cache/server      70483/85165
FTPs denied by cache/server       801920/36819
Requests dropped                  28715
Server timeouts/retries           567/1350
Processed rate average 60s/300s   1524/1344 requests/second
Denied rate average 60s/300s      35648/33022 requests/second
Dropped rate average 60s/300s     156/189 requests/second
URL Server Statistics:
----------------------
192.168.0.1                       UP
Vendor                           websense
Port                             17035
Requests total/allowed/denied    366519/255495/110457
Server timeouts/retries          567/1350
Responses received               365952
Response time average 60s/300s   2/1 seconds/request
192.168.0.2                        DOWN
Vendor                           websense
Port                             17035
Requests total/allowed/denied    0/0/0
Server timeouts/retries          0/0
Responses received               0
Response time average 60s/300s   0/0 seconds/request
. . .
URL Packets Sent and Received Stats:
------------------------------------
Message                 Sent    Received
STATUS_REQUEST          411     0
LOOKUP_REQUEST          366519  365952
LOG_REQUEST             0       NA
Errors:
-------
RFC noncompliant GET method     0
URL buffer update failure       0
Semantics:
This command allows the operator to display url-server statistics organized on a global and
 per-server basis. The output is reformatted to provide: more-detailed information and
per-server organization.
Supported Modes:
privileged
router || transparent
single || multi/context
Privilege:
ATTR_ES_CHECK_CONTEXT
Debug support:
N/A
Migration Strategy (if any):
N/A
```

Related Commands

Commands	Description
clear url-server	Clears the URL filtering server statistics.
filter url	Directs traffic to a URL filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.

Commands	Description
url-server	Identifies an N2H2 or Websense server for use with the filter command.

show usb-port

To view the current administrative and operational state of the USB port, use the **show usb-port** command.

show usb-port

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.22(1)	This command was added.

Usage Guidelines

The USB port has two states – administrative and operational. The administrative state is the desired state of the USB port and the operational state is the current state of the USB port.

Examples

The following is sample output from the **show usb port** command.

```
ciscoasa(config)# show usb port
USB Port info
---------------
Admin State: disabled
Oper State: disabled
```

Related Commands

Command	Description
usb-port disable	Disables or re-enables the USB port.

show user-alert

To show the currently configured user alert that can be displayed to all active clientless WebVPN sessions use the show user-alert command in privileged EXEC mode.

show user-alert

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	The command was added.

Related Commands

Command	Description
user-alert	Enables broadcast of an urgent message to all clientless SSL VPN users with a currently active session.

show user-identity ad-agent

To display information about the AD Agent for the Identify Firewall, use the **show user-identity ad-agent** command in privileged EXEC mode.

show user-identity ad-agent [**statistics**]

Syntax Description

statistics	(Optional) Displays statistical information about the AD Agent.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

You can monitor the AD Agent component of the Identity Firewall.

Use the **show user-identity ad-agent** command to obtain troubleshooting information for the AD Agent. This command displays the following information about the primary and secondary AD Agents:

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

Table 1: Description of the Command Output

Type	Values	Description
Mode	Configuration mode	Specifies full download or on-demand download.
AD Agent IP Address	IP address	Displays the active AD Agent IP address.
Backup	IP address	Displays the backup AD Agent IP address.

Type	Values	Description
AD Agent Status	• Disabled • Down • Up (registered) • Probing	• The Identity Firewall is disabled. • The AD Agent is down. • The AD Agent is up and running. • The ASA is registered and the AD Agent is up and running. • The ASA is trying to connect to the AD Agent.
Authentication Port	udp/1645	Displays the AD Agent authentication port.
Accounting Port	udp/1646	Displays the AD Agent accounting port.
ASA Listening Port	udp/3799	Displays the ASA listening port.
Interface	Interface	Displays the interface that the ASA uses to contact the AD Agent.
IP Address	IP address	Displays the IP address that the ASA uses to contact the AD Agent.
Uptime	Time	Displays the AD Agent up time.
Average RTT	Milliseconds	Displays the average round trip time the ASA uses to contact the AD Agent.
Domain	Domain nickname Status: up Status: down	Displays the Microsoft Active Directory domain for the AD Agent.

Examples

This example shows how to display information for the AD Agent for the Identify Firewall:

```
ciscoasa# show user-identity ad-agent
Primary AD Agent:
 Status                    up (registered)
 Mode:                     full-download
 IP address:               172.23.62.125
 Authentication port:      udp/1645
 Accounting port:          udp/1646
 ASA Listening port:       udp/3799
 Interface:                mgmt
 Up time:                  15 mins 41 secs
 Average RTT:              57 msec
Secondary AD Agent:
 Status                    up
 Mode:                     full-download
 IP address:               172.23.62.136
 Authentication port:      udp/1645
 Accounting port:          udp/1646
 ASA Listening port:       udp/3799
 Interface:                mgmt
 Up time:                  7 mins 56 secs
 Avg RTT:                  15 msec
```

Related Commands

Command	Description
clear user-identity ad-agent statistics	Clears the statistics data of AD Agents maintained by the ASA for the Identity Firewall.
user-identity enable	Creates the Cisco Identify Firewall instance.
show user-identity ad-group-members	Displays the group members in the domain of the AD Agent for the Identify Firewall.

show user-identity ad-group-members

To display the group members in the domain of the AD Agent for the Identify Firewall, use the **show user-identity ad-group-members** command in privileged EXEC mode.

show user-identity ad-group-members [*domain_nickname* \] *user_group_name* [**timeout seconds** *seconds*]

Syntax Description

domain_nickname	(Optional) Specifies the domain name for the Identity Firewall.
timeout seconds seconds	(Optional) Sets a timer for retrieving group member statistics and specifies the length of time for the timer.
user_group_name	(Optional) Specifies the group name from which to retrieve statistics.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

The **show user-identity ad-group-members** command displays the immediate members (the users and groups) of the specified user group.

Note This command does not display information for locally defined groups on the ASA configured with the **object-group user** command.

The ASA sends an LDAP query for the Active Directory groups configured on the Active Directory server. Running this command is equivalent to running an LDAP browser command that allows you to check members of a specified user group. ASA issues one level of LDAP query to retrieve the immediate members of the specified group in the distinguishedName format. Running this command does not update the ASA internal cache of imported user groups.

When you do not specify *domain_nickname* , the ASA displays information for the group that has *user_group_name* in the default domain. The argument *domain_nickname* can be the real domain nickname or LOCAL.

The group name is the AD group's unique sAMAccountName not the CN name. To display information for a specific group sAMAccountName, use the **show user-identity ad-groups filter** *filter_string* command to retrieve group's sAMAccountName.

Examples

This example shows how to display members of the group sample1 for the Identity Firewall:

```
ciscoasa# show user-identity ad-group-member group.sample1
Domain:CSCO        AAA Server Group:  CISCO_AD_SERVER
Group Member List Retrieved Successfully
Number of Members in AD Group group.schiang: 12
dn: CN=user1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
dn: CN=user2,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
...
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.
show user-identity ad-groups	Displays information about the AD Agent for the Identify Firewall.

show user-identity ad-groups

To display information for a specific group for the Identify Firewall, use the **show user-identity ad-groups** command in privileged EXEC mode.

show user-identity ad-groups *domain_nickname* { **filter** *filter_string* | **import-user-group** [**count**] }

Syntax Description

count	(Optional) Displays the number of activated groups.
domain_nickname	Specifies the domain name for the Identity Firewall.
filter *filter_string*	Specifies to displays groups that contain the specified filter string in the CN attribute of the domain controller of the Microsoft Active Directory.
import-user-group	Displays only the activated groups for the Identity Firewall.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

When you run the **show user-identity ad-groups** command, the ASA sends an LDAP query to the Microsoft Active Directory to retrieve all user groups that are part of the specified domain nickname. The argument *domain_nickname* can be the real domain nickname or LOCAL. The ASA only retrieves groups that have the group objectclass attribute. The ASA displays the retrieved groups in distinguishedName format.

When you specify the **filter** *filter_string* keyword and argument, the ASA displays groups that contain the specified filter string in the CN attribute of the domain controller. Because the **access-list** and **object-group** commands only take sAMAccountName, you can run the **show user-identity ad-users filter** *filter_string* command to retrieve the sAMAccountName for a group. When you do not specify **filter** *filter_string* , the ASA displays all Active Directory groups.

When you specify the **import-user-group count** keywords, the ASA displays all Active Directory groups that are activated (because they are part an access-group, import-user-group, or service-policy configuration) and stored in the local database. The ASA only displays the sAMAccountName for the groups.

Examples

These examples show how to display user groups that are part of the specified domain nickname for the Identity Firewall:

```
ciscoasa# show user-identity ad-groups CSCO filter sampleuser1
Domain: CSCO        AAA Server Group:       CISCO_AD_SERVER
Group list retrieved successfully
Number of Active Directory Groups       6
dn: CN=group.reg.sampleuser1,OU=Organizational,OU=Cisco Groups,DC=cisco,DC=com
sAMAccountName: group.reg.sampleuser1
dn: CN=group.temp.sampleuser1,OU=Organizational,OU=Cisco Groups,DC=cisco,DC=com
sAMAccountName: group.temp.sampleuser1
...
ciscoasa# show user-identity ad-groups CSCO import-user-group count
Total AD groups in domain CSCO stored in local: 2
ciscoasa# show user-identity ad-groups CSCO import-user-group

Domain: CSCO
Groups:
        group.SampleGroup1
        group.SampleGroup2
...
```

This example shows how to run the command to apply a filter string to the results from an access-list and object-group command. Running the **show user-identity ad-users CSCO filter SampleGroup1** command obtains the sAMAccountName of specified string:

```
ciscoasa# show user-identity ad-users CSCO filter SampleGroup1

Domain:CSCO    AAA Server Group:  CISCO_AD_SERVER
User list retrieved successfully
Number of Active Directory Users: 2
dn: CN=SampleUser1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: SampleUser2
dn: CN=SAMPLEUSER2-WXP05,OU=Workstations,OU=Cisco Computers,DC=cisco,DC=com
sAMAccountName: SAMPLEUSER2-WXP05$
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity ad-users

To display Microsoft Active Directory users for the Identify Firewall, use the **show user-identity ad-users** command in privileged EXEC mode.

show user-identity ad-users *domain_nickname* [**filter** *filter_string*]

Syntax Description

domain_nickname	Specifies the domain name for the Identity Firewall.
filter *filter_string*	(Optional) Specifies to displays users that contain the specified filter string in the CN attribute of the domain controller of the Microsoft Active Directory.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

When you run the **show user-identity ad-users** command, the ASA sends an LDAP query to the Microsoft Active Directory to retrieve all users that are part of the specified domain nickname. The argument *domain_nickname* can be the real domain nickname or LOCAL.

When you specify the **filter** *filter_string* keyword and argument, the ASA displays users that contain the specified filter string in the CN attribute of the domain controller. The ASA sends an LDAP query for the Active Directory groups configured on the Active Directory server.

The ASA only retrieves users that have the user objectclass attribute and the samAccountType attribute 805306368. Other objects, such as machine objects, can be included in the user objectclass; however, the samAccountType 805306368 filters out the non-user objects. When you do not specify a filter string, the ASA displays all Active Directory users.

The ASA displays the retrieved users in distinguishedName format.

Examples

This example shows how to display information about Active Directory users for the Identity Firewall:

```
ciscoasa# show user-identity ad-users CSCO filter user
Domain: CSCO        AAA Server Group:  CISCO_AD_SERVER
User list retrieved successfully
```

```
Number of Active Directory Users: 10
dn: CN=sampleuser1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: sampleuser1
dn: CN=sampleuser2,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: sampleuser2
dn: CN=user3,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: user3
...
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity group

To display the user groups configured for the Identify Firewall, use the **show user-identity group** command in privileged EXEC mode.

show user-identity group

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

Use the **show user-identity group** command to obtain troubleshooting information for the user groups configured for the Identity Firewall. The ASA sends an LDAP query for the Active Directory groups configured on the Active Directory server. This command displays the list of activated user groups in the following format:

domain \group_name

The ASA only displays top groups that are applied to a security policy. The maximum number of activated top groups is 256. Groups are activated when they are part an access-group, import-user-group, or service-policy configuration.

Examples

This example shows how to display the activated groups for the Identity Firewall:

```
ciscoasa# show user-identity group
Group ID        Activated Group Name (Domain\\Group)
--------        ------------------------------------
       1        LOCAL\\og1
       2        LOCAL\\marketing
       3        CISCO\\group.sampleuser1
       4        IDFW\\grp1
...
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity ip-of-user

To display the IP address for a specified user for the Identify Firewall, use the **show user-identity ip-of-user** command in privileged EXEC mode.

show user-identity ip-of-user [*domain_nickname* \] *user-name* [**detail**]

Syntax Description

detail	(Optional) Displays the detailed output about the user and IP address.
domain_nickname	(Optional) Specifies the domain name for the Identity Firewall.
user-name	Specifies the user for which to obtain an IP address.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

This command displays user information and the IP addresses for the specified user. Users can have more than one IP address associated with them.

When you do not specify the *domain_nickname* argument, the ASA displays information for the user with *user_name* in default domain. The argument *domain_nickname* can be the real domain nickname or LOCAL.

When you specify the **detail** keyword, the ASA displays the total number of active connections, the user-statistics period and the drops, and the input packets and output packets during the period over all IP addresses for the specified user. When you do not specify the **detail** option, the ASA displays only the domain nickname and status of each IP address.

Note The ASA displays detailed user statistics, such as received packets, sent packets and drops in the specified time period, only when you enable user-statistics scanning or accounting for the Identity Firewall. See the CLI configuration guide for information about configuring the Identity Firewall.

Examples

These examples show how to display IP addresses of specified users for the Identity Firewall:

```
ciscoasa# show user-identity ip-of-user sampleuser1
CSCO\172.1.1.1 (Login)
CSCO\172.100.3.23 (Login)
CSCO\10.23.51.3 (Inactive)
ciscoasa# show user-identity ip-of-user sampleuser1 detail
CSCO\172.1.1.1 (Login) Login time: 1440 mins;  Idle time: 10 mins; 2 active conns
CSCO\172.100.3.23 (Login) Login time: 20 mins;  Idle time: 10 mins; 10 active conns
CSCO\10.23.51.3 (Inactive) Login time: 3000 mins;  Idle time: 2040 mins; 8 active conns
Total number of active connections: 20
1-hour recv packets: 12560
1-hour sent packets: 32560
20-min drops: 560
ciscoasa# show user-identity ip-of-user sampleuser2
ERROR: no such user
ciscoasa# show user-identity ip-of-user sampleuser3
ERROR: no IP address, user not login now
```

IPv6 support

```
ciscoasa# show user-identity ip-of-user sampleuser4
CSCO\172.1.1.1 (Login)
CSCO\8080:1:3::56 (Login)
CSCO\8080:2:3::34 (Inactive)
ciscoasa# show user-identity ip-of-user sampleuser4 detail
CSCO\172.1.1.1 (Login) Login time: 1440 mins;  Idle time: 10 mins; 8 active conns
CSCO\8080:1:3::56 (Login) Login time: 20 mins;  Idle time: 10 mins; 12 active conns
CSCO\8080:2:3::34 (Inactive) Total number of active connections: 20
1-hour recv packets: 12560
1-hour sent packets: 32560
20-min drops: 560
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.
show user-identity user-of-ip	Displays the user information associated with the specified IP address

show user-identity memory

To display the memory of various modules of the Identify Firewall, use the **show user-identity memory** command in privileged EXEC mode.

show user-identity memory

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

You can monitor the memory usage that the Identity Firewall consumes on the ASA. Running the s**how user-identity memory** command displays the memory for user records, group records, host records, and their associated hash table. The ASA also displays the memory used by the identity-based tmatch table.

The command displays the memory usage in bytes of various modules in the Identity Firewall:

- Users
- Groups
- User Statistics
- LDAP

The ASA sends an LDAP query for the Active Directory groups configured on the Active Directory server. The Active Directory server authenticates users and generates user logon security logs.

- AD Agent
- Miscellaneous
- Total Memory Usage

How you configure the Identity Firewall to retrieve user information from the AD Agent impacts the amount of memory used by the feature. You specify whether the ASA uses on demand retrieval or full download retrieval. Selecting On Demand has the benefit of using less memory as only users of received packets are

queried and stored. See “Configuring Identity Options” in the CLI configuration guide for a description of these options.

Examples

This example shows how to display the memory status of the modules of the Identity Firewall:

```
ciscoasa# show user-identity memory
Users:       22416048 bytes
Groups:           320 bytes
User stats:         0 bytes
LDAP:             300 bytes
AD agent:         500 bytes
Misc:           32428 bytes
Total:       22449596 bytes
Users:       22416048 bytes
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity statistics

To display statistics for a user or user group for the Identify Firewall, use the **show user-identity statistics** command in privileged EXEC mode.

show user-identity statistics [**user** [*domain_nickname* \] *user_name* | **user-group** [*domain_nickname* \] *user_group_name*]

Syntax Description

domain_nickname	(Optional) Specifies the domain name for the Identity Firewall.
user *user_name*	(Optional) Specifies the user name from which to retrieve statistics.
user-group *domain_nickname**user_group_name*	(Optional) Specifies the group name from which to retrieve statistics.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

Run the show **user-identity statistics** command to display the statistics for a user or user group.

When you do not specify the *domain_nickname* argument with the **user** keyword, the ASA displays information for the user with *user_name* in default domain.

When you do not specify *domain_nickname* with the **user-group** keyword, the ASA displays information for the group that has *user_group_name* in the default domain. The argument *domain_nickname* can be the real domain nickname or LOCAL.

Examples

These examples show how to display statistics about users for the Identity Firewall:

```
ciscoasa# show user-identity statistics user

Current monitored users:11  Total not monitored users:0
                         Average(eps)    Current(eps) Trigger      Total events
User: CSCO\user1 tot-ses:4911 act-ses:1213 fw-drop:0 insp-drop:0 null-ses:4861 bad-acc:0
```

```
  20-min Recv attack:                4              10      14              4861
    1-hour Recv pkts:                  1              10        0               4901
User: CSCO\user2 tot-ses:2456 act-ses:607 fw-drop:0 insp-drop:0 null-ses:2431 bad-acc:0
  20-min Sent attack:                4              10        4               4862
  1-hour Sent pkts:                    0               5         0               2451
...
ciscoasa# show user-identity statistics user user1
Current                          Average(eps)    Current(eps) Trigger      Total events
User: -(user1-) tot-ses:4911 act-ses:1213 fw-drop:0 insp-drop:0 null-ses:4861 bad-acc:0
  20-min Recv attack:                4              10       14              4861
  1-hour Recv pkts:                  1              10       0               4901
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity statistics top user

To display statistics for the top 10 users for the Identify Firewall, use the **show user-identity statistics top user** command in privileged EXEC mode.

show user-identity statistics top user

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

The **show user-identity statistics top user** command displays statistics for received EPS packets, sent EPS packets, and sent attacks for the top 10 users. For each user (displayed as *domain \user_name*), the ASA displays the average EPS packet, the current EPS packet, the trigger, and total events for that user.

Examples

This example shows how to display information about the top 10 users for the Identity Firewall:

```
ciscoasa# show user-identity statistics top user
Top          Name   Id    Average(eps)    Current(eps) Trigger      Total events
  1-hour Recv pkts:
01    APAC\sampleuser1
                                  0               0       0               391
  1-hour Sent pkts:
01    APAC\sampleuser2
                                  0               0       0               196
02    CSCO\sampleuser3
                                  0               0       0               195
  10-min Sent attack:
01    CSCO\sampleuser4
                                  0               0       0               352
02    CSCO\sampleuser3
                                  0               0       0               350
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity user active

To display the active users for the Identify Firewall, use the **show user-identity user active** command in privileged EXEC mode.

show user-identity user active [**domain** *domain_nickname* | **user-group** [*domain_nickname* \] *user_group_name* | **user** [*domain_nickname* \] *user_name*] [**list** [**detail**]]

Syntax Description

detail	(Optional) Displays the detailed output of the active user sessions.
domain *domain_nickname*	Displays statistics for the active users in a specified domain.
list	(Optional) Displays a list summarizing the active user statistics.
user *domain_nickname*\ *user_name*	(Optional) Displays statistic for a specified user.
user-group *domain_nickname*\ *user_group_name*	(Optional) Displays statistics for a specified user group.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

You can display information about all users contained in the IP-user mapping database used by the Identity Firewall.

The **show user-identity user active** command displays the following information for users:

- *domain \user_name*
- Active Connections
- Minutes Idle

The default domain name can be the real domain name, a special reserved word, or LOCAL. The Identity Firewall uses the LOCAL domain name for all locally defined user groups or locally defined users (users who

log in and authenticate by using a VPN or web portal). When default domain is not specified, the default domain is LOCAL.

A user's name is appended with the number of minutes idle. The login time and idle time are stored on a per user basis instead of per the IP address of a user.

When the **user-group** keyword is specified, only the activated user-groups are displayed. Groups are activated when they are part an access-group, import-user-group, or service-policy configuration.

When you do not specify *domain_nickname* with the **user-group** keyword, the ASA displays information for the group that has *user_group_name* in the default domain.

Note When the **user-identity action domain-controller-down** is configured with the **disable-user-identity-rule** keyword and the specified domain is down, or when **user-identity action ad-agent-down** command is configured with the **disable-user-identity-rule** keyword and the AD agent is down, all the logged on users are displayed as disabled in the user statistics.

Note The ASA displays detailed user statistics, such as received packets, sent packets and drops in the specified time period, only when you enable user-statistics scanning or accounting for the Identity Firewall. See the CLI configuration guide for information about configuring the Identity Firewall.

Examples

The following examples show how to display information about active users for the Identity Firewall:

```
ciscoasa# show user-identity user active

Total active users: 30  Total IP addresses: 35
  LOCAL: 0 users, 0 IP addresses
  cisco.com: 0 users, 0 IP addresses
  d1: 0 users, 0 IP addresses
  IDFW: 0 users, 0 IP addresses
  idfw.com: 0 users, 0 IP addresses
  IDFWTEST: 30 users, 35 IP addresses
ciscoasa# show user-identity user active domain CSCO

Total active users: 48020 Total IP addresses:10000
  CSCO: 48020 users, 10000 IP addresses
ciscoasa# show user-identity user active domain CSCO list

Total active users: 48020 Total IP addresses: 10000
  CSCO: 48020 users, 10000 IP addresses
   CSCO\sampleuser1: 20 active conns; idle 0 mins
   CSCO\member-1: 20 active conns; idle 5 mins
   CSCO\member-2: 20 active conns; idle 20 mins
   CSCO\member-3: 3 active conns; idle 101 mins
   ...
ciscoasa# show user-identity user active list

Total active users: 48032  Total IP addresses: 10000
   CSCO\sampleuser1: 20 active conns; idle 0 mins
   CSCO\member-1: 20 active conns; idle 6 mins
   APAC\sampleuser2: 20 active conns; idle 0 mins
   CSCO\member-2: 20 active conns; idle 1 mins
   CSCO\member-3: 20 active conns; idle 0 mins
```

```
   APAC\member-2: 20 active conns; idle 22 mins
   CSCO\member-4: 3 active conns; idle 101 mins
   ...
ciscoasa# show user-identity user active list detail

Total active users: 48032 Total IP addresses: 10010
  CSCO: 48020 users, 10000 IP addresses
  APAC: 12 users, 10 IP addresses
   CSCO\sampleuser1: 20 active conns; idle 0 mins
     172.1.1.1: login 360 mins, idle 0 mins, 15 active conns
     172.100.3.23: login 200 min, idle 15 mins , 5 active conns
     10.23.51.3: inactive
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560
   CSCO\member-1: 4 active connections;  idle 350 mins
   ...
  APAC\sampleuser12: 3 active conns; idle 101 mins
     172.1.1.1: login 360 mins, idle 101 mins, 1 active conns
     172.100.3.23: login 200 min, idle 150 mins, 2 active conns
     10.23.51.3: inactive
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560
ciscoasa# show user-identity user active list detail
Total users: 25  Total IP addresses: 5
   LOCAL\idfw: 0 active conns
    6.1.1.1: inactive
  cisco.com\sampleuser1: 0 active conns
  cisco.com\sampleuser2: 0 active conns
  cisco.com\sampleuser3: 0 active conns
    20.0.0.3: login 0 mins, idle 0 mins, 0 active conns (disabled)
  cisco.com\sampleuser4: 0 active conns; idle 0 mins
    20.0.0.2: login 0 mins, idle 0 mins, 0 active conns (disabled)
  cisco.com\sampleuser5: 0 active conns
  ...
ciscoasa# show user-identity user active user sampleuser1 list detail

CSCO\sampleuser1: 20 active conns; idle 3 mins
     172.1.1.1: login 360 mins, idle 20 mins, 15 active conns
     172.100.3.23: login 200 mins, idle 3 mins, 5 active conns
     10.23.51.3: inactive
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560
ciscoasa# show user-identity user active user APAC\sampleuser2

APAC\sampleuser2: 20 active conns; idle 2 mins
ciscoasa# show user-identity user active user-group APAC\\marketing list

   APAC\sampleuser1: 20 active conns; idle 2 mins
   APAC\member-1: 20 active conns; idle 0 mins
   APAC\member-2: 20 active conns; idle 0 mins
   APAC\member-3: 20 active conns; idle 6 mins
...
ciscoasa# show user-identity user active user-group APAC\\inactive list
ERROR: group is not activated
```

Related Commands

Command	Description
clear user-identity active-user-database	Sets the status of a specified user, all users belong to a specified user group, or all users to logged out for the Identity Firewall.

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity user all

To display statistics about users for the Identify Firewall, use the **show user-identity user all** command in privileged EXEC mode.

show user-identity user all [**list**] [**detail**]

Syntax Description

detail	(Optional) Displays the detailed output about all users for the Identity Firewall.
list	(Optional) Displays a list summarizing the statistics for all users for the Identity Firewall.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

Use the show user-identity all command to display information for all users contained in the IP-user mapping database used by the Identity Firewall.

When you include the detail keyword with this command and the command output shows an IP address is inactive, the IP address is not associated with the user. Searching for the user associated with that IP address will return an error.

Note When the **user-identity action domain-controller-down** is configured with the **disable-user-identity-rule** keyword and the specified domain is down, or when **user-identity action ad-agent-down** command is configured with the **disable-user-identity-rule** keyword and the AD agent is down, all the logged on users are displayed as disabled in the user statistics.

Note The ASA displays detailed user statistics, such as received packets, sent packets and drops in the specified time period, only when you enable user-statistics scanning or accounting for the Identity Firewall. See the CLI configuration guide for information about configuring the Identity Firewall.

Examples

The following examples show how to display statistics about all users for the Identity Firewall:

```
ciscoasa# show user-identity user all list
Total inactive users: 1201  Total IP addresses: 100
ciscoasa# show user-identity user all list
Total users: 7
  LOCAL\idfw: 0 active conns
  cisco.com\sampleuser1: 0 active conns
  cisco.com\sampleuser2: 0 active conns
  cisco.com\sampleuser3: 0 active conns
  cisco.com\sampleuser4: 0 active conns; idle 300 mins
  cisco.com\sampleuser5: 0 active conns
  cisco.com\sampleuser6: 0 active conns
  cisco.com\sampleuser7: 0 active conns
ciscoasa# show user-identity user all list detail
Total users: 7 Total IP addresses: 3
  LOCAL\idfw: 0 active conns
    10.1.1.1: inactive
  cisco.com\sampleuser1: 0 active conns
  cisco.com\sampleuser2: 0 active conns
  cisco.com\sampleuser3: 0 active conns; idle 300 mins
    171.69.42.8: inactive
    10.0.0.2: login 300 mins, idle 300 mins, 5 active conns
  cisco.com\sampleuser4: 0 active conns
  cisco.com\sampleuser5: 0 active conns
  cisco.com\sampleuser6: 0 active conns
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity user inactive

To display information about the inactive users for the Identify Firewall, use the **show user-identity user inactive** command in privileged EXEC mode.

show user-identity user inactive [**domain** *domain_nickname* | **user-group** [*domain_nickname* \] *user_group_name*]

Syntax Description

domain *domain_nickname*	(Optional) Displays statistics for the inactive users in the specified domain name for the Identity Firewall.
user-group *domain_nickname\user_group_name*	(Optional) Displays statistics for the inactive users in the specified user group.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

Use the **show user-identity user inactive** command to display information about users who have no active traffic for longer than the value configured with the **user-identity inactive-user-timer** command.

When the **user-group** keyword is specified, only the activated user-groups are displayed. Groups are activated when they are part an access-group, import-user-group, or service-policy configuration.

When you do not specify *domain_nickname* with the **user-group** keyword, the ASA displays information for the group that has *user_group_name* in the default domain. The argument *domain_nickname* can be the real domain nickname or LOCAL.

Examples

These examples show how to display the status of inactive users for the Identity Firewall:

```
ciscoasa# show user-identity user inactive
Total inactive users: 1201
   APAC\sampleuser1
   CSCO\sampleuser2
172.1.1.1: inactive     ...
...
```

```
ciscoasa# show user-identity user inactive domain CSCO
Total inactive users: 1101
    CSCO: 1101
   CSCO\sampleuser1
   CSCO\sampleuser2
   CSCO\sampleuser3
...
ciscoasa# show user-identity user inactive user-group CSCO\\marketing
Total inactive users: 21
   CSCO\sampleuser1
   CSCO\sampleuser2
...
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.
user-identity inactive-user-timer	Specifies the amount of time before a user is considered idle for the Cisco Identify Firewall instance.

show user-identity user-not-found

To display the IP addresses of the Active Directory users not found for the Identify Firewall, use the **show user-identity user-not-found** command in privileged EXEC mode.

show user-identity user-not-found

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

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

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

Examples

This example shows how to display information about not-found users for the Identity Firewall:

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

Related Commands

Command	Description
clear user-identity user-not-found	Clears the ASA local user-not-found database for the Identity Firewall.
user-identity enable	Creates the Cisco Identify Firewall instance.
user-identity user-not-found	Enables user-not-found tracking for the Identify Firewall.

show user-identity user-of-group

To display the users of a specified user group for the Identify Firewall, use the **show user-identity user-of-group** command in privileged EXEC mode.

show user-identity user-of-group [*domain_nickname* \] *user_group_name*

Syntax Description

domain_nickname	Specifies the domain name for the Identity Firewall.
user_group_name	Specifies the user group for which to display statistics.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

Use the **show user-identity user-of-group** command to display users whose group ID matches the specified user group. (The ASA scans the IP-user hash list for this information and rather than sending an LDAP query to Active Directory. The AD Agent maintains a cache of user ID and IP address mappings and notifies the ASA of changes.)

The user group name you specify must be activated, meaning the group is an import user group (defined as a user group in an access list or service policy configuration) or a local user group (defined in an object-group user).

The group can have more than one user member. The members of the user group are all immediate members (including users and groups) of the specified group.

When you do not specify *domain_nickname* with the *user_group_name* argument, the ASA displays information for the group that has *user_group_name* in the default domain. The argument *domain_nickname* can be the real domain nickname or LOCAL.

When the command out put indicates a user's status is inactive, the user can be logged out or has never logged in.

Examples

These examples show how to display users of a specified user group for the Identity Firewall:

```
ciscoasa# show user-identity user-of-group group.samplegroup1
Group: CSCO\\group.user1 Total users: 13
CSCO\user2 10.0.0.10(Login) 20.0.0.10(Inactive) ...
CSCO\user3 10.0.0.11(Inactive)
CSCO\user4 10.0.0.12 (Login)
CSCO\user5 10.0.0.13 (Login)
CSCO\user6 10.0.0.14 (Inactive)
....
ciscoasa# show user-identity user-of-group group.local1
Group: LOCAL\\group.local1    Total users: 2
CSCO\user1 10.0.4.12 (Login)
LOCAL\user2 10.0.3.13 (Login)
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity user-of-ip

To display information about a user with a specific IP address for the Identify Firewall, use the **show user-identity user-of-ip** command in privileged EXEC mode.

show user-identity user-of-ip *ip_address* [**detail**]

Syntax Description

detail	(Optional) Displays the detailed output about user with the specified IP address.
ip_address	Indicates the IP address of the user for which to display information.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

Use the **show user-identity user-of-ip** command to display the user information associated with the specified IP address.

When you specify the **detail** keyword, the ASA displays user login time, idle time, the number of active connections, the user-statistics period and the drops, and the input packets and output packets during the period. When you do not specify the **detail** keyword, the ASA only displays the domain nickname, user name, and status.

When user status is inactive, the user can be logged out or has never logged in.

When you include the **detail** keyword with this command and the command output for an IP address displays an error, the IP address is inactive, meaning that the IP address is not associated with a user.



Note The ASA displays detailed user statistics, such as received packets, sent packets and drops in the specified time period, only when you enable user-statistics scanning or accounting for the Identity Firewall. See the CLI configuration guide for information about configuring the Identity Firewall.

Examples

These examples show how to display the status of the active users for the Identity Firewall:

```
ciscoasa# show user-identity user-of-ip 172.1.1.1
CSCO\sampleuser1 (Login)
ciscoasa# show user-identity user-of-ip 172.1.1.1 detail
CSCO\sampleuser1 (Login) Login time: 240 mins;  Idle time: 10 mins
Number of active connections: 20
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60
ciscoasa# show user-identity user-of-ip 172.1.2.2 detail
CSCO\sampleuser2 (Login) Login time: 1440 mins; Idle time: 100 mins
Number of active connections: 0
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60
ciscoasa# show user-identity user-of-ip 172.1.7.7
ERROR: no user with this IP address
```

IPv6 Support

```
ciscoasa# show user-identity user-of-ip 8080:1:1::4

CSCO\sampleuser1 (Login)
ciscoasa# show user-identity user-of-ip 8080:1:1::4 detail
CSCO\sampleuser1 (Login) Login time: 240 mins;  Idle time: 10 mins
Number of active connections: 20
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60
ciscoasa# show user-identity user-of-ip 8080:1:1::6 detail
CSCO\sampleuser2 (Login) Login time: 1440 mins; Idle time: 100 mins
Number of active connections: 0
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60
ciscoasa# show user-identity user-of-ip 8080:1:1::100
ERROR: no user with this IP address
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show version

To display the software version, hardware configuration, license key, and related uptime data, use the **show version** command in user EXEC mode.

show version

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	In stateful failover mode, an additional line showing cluster uptime is displayed.
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.
8.4(1)	Support for No Payload Encryption models (NPE) was added.
9.3(2)	If REST API Agent is enabled, its version number is displayed.
9.17(1)	Information on how long it took to start (boot) up the system was added to the output.

Usage Guidelines

The show version command allows you to display the software version, operating time since the last reboot, processor type, Flash partition type, interface boards, serial number (BIOS ID), activation key value, license type, and time stamp for when the configuration was last modified.

If the REST API Agent is installed and enabled, its version number is also displayed.

The serial number listed with the show version command is for the flash partition BIOS. This number is different from the serial number on the chassis. When you get a software upgrade, you will need the serial number that appears in the show version command, not the chassis number.

The failover cluster uptime value indicates how long a failover set has been running. If one unit stops running, the uptime value continues to increase as long as the active unit continues to operate. Therefore, it is possible for the failover cluster uptime to be greater than the individual unit uptime. If you temporarily disable failover, and then reenable it, the failover cluster uptime reports the time the unit was up before failover was disabled plus the time the unit was up while failover was disabled.

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

For the Total VPN Peers on the ASA 5505, the total combined number of VPN sessions of all types depends on your licenses. If you enable AnyConnect Essentials, then the total is the model maximum of 25. If you enable AnyConnect Premium, then the total is the AnyConnect Premium value plus the Other VPN value, not to exceed 25 sessions. Unlike other models, where the Other VPN value equals the model limit for all VPN sessions, the ASA 5505 has a lower Other VPN value than the model limit, so the total value can vary depending on the AnyConnect Premium license.

Examples

The following is sample output from the **show version** command, and shows the software version, hardware configuration, license key, and related uptime information. Note that in an environment where stateful failover is configured an additional line showing the failover cluster uptime is displayed. If failover is not configured, the line is not displayed. This display shows a warning message about minimum memory requirements.

```
**************************************************************************
**                                                                      **
**   *** WARNING *** WARNING *** WARNING *** WARNING *** WARNING ***    **
**                                                                      **
**          ----> Minimum Memory Requirements NOT Met! <----            **
**                                                                      **
**  Installed RAM:  512 MB                                              **
**  Required  RAM: 2048 MB                                              **
**  Upgrade part#: ASA5520-MEM-2GB=                                     **
**                                                                      **
**  This ASA does not meet the minimum memory requirements needed to    **
**  run this image. Please install additional memory (part number       **
**  listed above) or downgrade to ASA version 8.2 or earlier.           **
**  Continuing to run without a memory upgrade is unsupported, and      **
**  critical system features will not function properly.                **
**                                                                      **
**************************************************************************
Cisco Adaptive Security Appliance Software Version 8.4(1)
Device Manager Version 6.4(1)
Compiled on Thu 20-Jan-12 04:05 by builders
System image file is "disk0:/cdisk.bin"
Config file at boot was "disk0:/tomm_backup.cfg"

asa3 up 3 days 3 hours
Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 64MB
Slot 1: ATA Compact Flash, 128MB
BIOS Flash AT49LW080 @ 0xfff00000, 1024KB
Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
                             Boot microcode   : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.03
                             IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.06
 0: Ext: GigabitEthernet0/0  : address is 0013.c480.82ce, irq 9
 1: Ext: GigabitEthernet0/1  : address is 0013.c480.82cf, irq 9
 2: Ext: GigabitEthernet0/2  : address is 0013.c480.82d0, irq 9
 3: Ext: GigabitEthernet0/3  : address is 0013.c480.82d1, irq 9
 4: Ext: Management0/0       : address is 0013.c480.82cd, irq 11
 5: Int: Not used            : irq 11
 6: Int: Not used            : irq 5
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
Serial Number: JMX0938K0C0
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Configuration register is 0x1
Configuration last modified by docs at 15:23:22.339 EDT Fri Oct 30 2012
```

The following message appears if you enter the **show version** command after the **eject** command has been executed, but the device has not been physically removed:

```
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
```

Starting with version 9.17(1), you can see how long it took to boot up the system. The information is after status of how long the system has been running.

```
FP2130-2# show version
Cisco Adaptive Security Appliance Software Version 99.17(1)144
SSP Operating System Version 82.11(1.288i)
Device Manager Version 88.31(0)45

Compiled on Tue 06-Apr-21 05:41 GMT by builders
System image file is "disk0:/mnt/boot/installables/switch/fxos-k8-fp2k-npu.82.11.1.288i.SSB"
Config file at boot was "startup-config"

FP2130-2 up 1 day 23 hours
Start-up time 2 mins 40 secs

Hardware:   FPR-2130, 13703 MB RAM, CPU MIPS 1200 MHz, 1 CPU (12 cores)


 1: Int: Internal-Data0/1    : address is 000f.b748.4800, irq 0
 3: Int: Not licensed        : irq 0
 4: Ext: Management1/1       : address is 2cf8.9b36.0759, irq 0
 5: Int: Internal-Data1/1    : address is 0000.0100.0001, irq 0

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
```

```
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Disabled
Security Contexts                 : 2
Carrier                           : Disabled
AnyConnect Premium Peers          : 7500
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 7500
Total VPN Peers                   : 7500
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 8000
Cluster                           : Disabled

Serial Number: JAD232913UX
Configuration register is 0x1
Configuration has not been modified since last system restart.
```

The following example shows the **show version** output for Secure Firewall 6100 that includes crypto details including crypto hardware revisions:

```
firepower# show version detail
<snip>
Fpga-Crypto-Vers: 0.14.00
Fpga-Crypto2-Vers:
<snip>
```

Related Commands

Command	Description
eject	Allows shutdown of external compact flash device before physical removal from the ASA.
show hardware	Displays detail hardware information.
show serial	Displays the hardware serial information.
show uptime	Displays how long the ASA has been up.

show vlan

To display all VLANs configured on the ASA, use the show vlan command in privileged EXEC mode.

show vlan [**mapping** [*primary_id*]]

Syntax Description

mapping	(Optional) Shows the secondary VLANs mapped to the primary VLAN.
primary_id	(Optional) Shows secondary VLANs for a specific primary VLAN.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
9.5(2)	The **mapping** keyword was added.

Examples

The following example displays the configured VLANs:

```
ciscoasa# show vlan
10-11,30,40,300
```

The following example displays the secondary VLANs that are mapped to each primary VLAN:

```
ciscoasa# show vlan mapping
Interface                       Secondary VLAN ID                       Mapped VLAN ID
0/1.100                         200                                             300
0/1.100                         201                                             300
0/2.500                         400                                             200
```

Related Commands

Command	Description
clear interface	Clears counters for the **show interface** command.
interface	Configures an interface and enters interface configuration mode.

Command	Description
show interface	Displays the runtime status and statistics of interfaces.

show vm

To display virtual platform information on the ASA Virtual, use the show vm command in privileged EXEC mode.

show vm

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

For the ASA Virtual, note the following licensing guidelines:

- The number of allowed vCPUs is determined by the vCPU platform license installed.
  - If the number of licensed vCPUs matches the number of provisioned vCPUs, the state is Compliant.
  - If the number of licensed vCPUs is less than the number of provisioned vCPUs, the state is Noncompliant: Over-provisioned.
  - If the number of licensed vCPUs is more than the number of provisioned vCPUs, the state is Compliant: Under-provisioned.
- The memory limit is determined by the number of vCPUs provisioned.
  - If the provisioned memory is at the allowed limit, the state is Compliant.
  - If the provisioned memory is above the allowed limit, the state is Noncompliant: Over-provisioned.
  - If the provisioned memory is below the allowed limit, the state is Compliant: Under-provisioned.
- The Frequency Reservation limit is determined by the number of vCPUs provisioned.
  - If the frequency reservation memory is at or above the required minimum (1000 MHz), the state is Compliant.

- If the frequency reservation memory is below the required minimum (1000 MHz), the state is Compliant: Under-provisioned.

Examples

The following example displays the virtual platform information for an unlicensed ASAv10:

```
ciscoasa# show vm
Virtual Platform Resource Limits
--------------------------------
Number of vCPUs              :     0
Processor Memory             :     0 MB
Virtual Platform Resource Status
--------------------------------
Number of vCPUs                :     1     (Noncompliant: Over-provisioned)
Processor Memory               :  2048 MB  (Noncompliant: Over-provisioned)
Hypervisor                     :   VMware
Model Id                       :   ASAv10
```

The following example displays the virtual platform information for a licensed ASAv10:

```
ciscoasa# show vm
Virtual Platform Resource Limits
--------------------------------
Number of vCPUs              :     1
Processor Memory             :  2048 MB
Virtual Platform Resource Status
--------------------------------
Number of vCPUs                :     1     (Compliant)
Processor Memory               :  2048 MB  (Compliant)
Hypervisor                     :   VMware
Model Id                       :   ASAv10
```

Related Commands

Command	Description
show cpu detail	Shows vCPU information on a per-vCPU basis.

show vni vlan-mapping

To show the mapping between VNI segment IDs and VLAN interfaces or physical interfaces, use the **show vni vlan-mapping** command in privileged EXEC mode.

show vni vlan-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	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

This command is only valid in transparent firewall mode because in routed mode, the mapping between VXLANs and VLANs can include too many values to show.

Examples

See the following output for the **show vni vlan-mapping** command:

```
ciscoasa# show vni vlan-mapping
vni1: segment-id: 6000, interface: 'g0110', vlan 10, interface: 'g0111', vlan 11
vni2: segment_id: 5000, interface: 'g01100', vlan 1, interface: 'g111', vlan 3, interface:
 'g112', vlan 4
```

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.

Command	Description
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 vpdn

To show the status of virtual private dial-up network (VPDN) connections such as PPPoE or L2TP, use the **show vpdn** command in privileged EXEC mode.

show vpdn { **group** *name* | **pppinterface** [**id** *number*] | **session** [| **l2tp** | **pppoe**] [**id** *number*] { **packets** | **state** | **window** } | **tunnel** [**l2tp** | **pppoe**] [**id** *number*] { **packets** | **state** | **summary** | **transport** } | **username** *name* }

Syntax Description

group *name*	Shows the VPDN group configuration.
id *number*	(Optional) Shows information about the VPDN session with the specified ID.
l2tp	(Optional) Shows session or tunnel information about L2TP.
packets	Shows session or tunnel packet information.
pppinterface	Shows PPP interface information.
pppoe	(Optional) Show session or tunnel information about PPPoE.
session	Shows session information.
state	Shows session or tunnel state information.
summary	Shows the tunnel summary.
transport	Shows tunnel transport information.
tunnel	Shows tunnel information.
username *name*	Shows user information.
window	Shows session window information.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	We introduced this command.

Usage Guidelines

Use this command to troubleshoot the VPDN PPPoE or L2TP connections.

Examples

The following is sample output from the **show vpdn session** command:

```
ciscoasa# show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
```

The following is sample output from the **show vpdn tunnel** command:

```
ciscoasa# show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
   6 packets sent, 6 received, 84 bytes sent, 0 received
```

Related Commands

Command	Description
vpdn group	Configures VPDN client settings

show vpn cluster stats internal

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

show vpn cluster stats internal

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.9(1)	Command added.

Related Commands

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

show vpn load-balancing

To display the runtime statistics for the VPN load-balancing virtual cluster configuration, use the **show vpn-load-balancing** command in global configuration, privileged EXEC, or VPN load-balancing mode.

show vpn load-balancing

Syntax Description

This command has no variables or arguments.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—
Vpn load-balancing	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	Added separate IPsec and SSL columns for both Load (%) display and Session display in the output example.
8.4(2)	New information was added to the displayed output.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **show vpn load-balancing** command displays statistical information for the virtual VPN load-balancing cluster. If the local device is not participating in the VPN load-balancing cluster, this command indicates that VPN load balancing has not been configured for this device.

The asterisk (*) in the output indicates the IP address of the ASA to which you are connected.

Examples

This example displays **show vpn load-balancing** command and its output for a situation in which the local device is participating in the VPN load-balancing cluster:

```
ciscoasa# sh vpn load-balancing
```

```
------------------------------------------------------------------------------
    Status     Role   Failover   Encryption        Cluster IP   Peers
------------------------------------------------------------------------------
   Enabled   Master        n/a     Disabled  192.0.2.255       0
Peers:
------------------------------------------------------------------------------
       Public IP     Role  Pri             Model  Load-Balancing Version
------------------------------------------------------------------------------
  192.0.2.255      Master    5          ASA-5520               3
Total License Load:
------------------------------------------------------------------------------
       Public IP    AnyConnect Premium/Essentials          Other VPN
                    -------------------------------   ---------------------
                         Limit    Used   Load          Limit    Used   Load
------------------------------------------------------------------------------
     192.0.2.255       750       0     0%            750       1     0%
Licenses Used By Inactive Sessions :
------------------------------------------------------------------------------
       Public IP    AnyConnect Premium/Essentials     Inactive Load
------------------------------------------------------------------------------
     192.0.2.255           0                0%
```

On the primary device, the Total License Load output includes information about the primary and backup device; however, the backup device only shows information about itself and not the primary device. Thus, the primary device knows about all licensed members, but the licensed members themselves only know about their own licenses.

The output also contains a License Used by Inactive Session section. When an Secure Client session goes inactive, the ASA keeps that session as long as the session has not terminated by normal means. That way, Secure Client sessions can reconnect using the same webvpn cookie and not have to re-authenticate. The inactive sessions will remain in that state until either the Secure Client resumes the session or an idle timeout occurs. The licenses for those sessions are maintained for these inactive sessions and are represented in this License Used by Inactive Session section.

If the local device is not participating in the VPN load-balancing cluster, the **show vpn load-balancing** command shows a different result:

```
ciscoasa(config)# show vpn load-balancing
VPN Load Balancing has not been configured.
```

Related Commands

Command	Description
clear configure vpn load-balancing	Removes **vpn load-balancing** command statements from the configuration.
show running-config vpn load-balancing	Displays the the current VPN load-balancing virtual cluster configuration.
vpn load-balancing	Enters vpn load-balancing mode.

show vpn-sessiondb

To display information about VPN sessions, use the **show vpn-sessiondb** command in privileged EXEC mode. The command includes options for displaying information in full or in detail, lets you specify type of sessions to display, and provides options to filter and sort the information. The syntax table and usage notes organize the choices accordingly

show vpn-sessiondb [**all**] [**backup** { **index | l2l** }] [**detail**] [**ospfv3**] [**failover**] [**full**] [**summary**] [**ratio** { **encryption | protocol** }] [**license-summary**] { **anyconnect | email-proxy | index** *indexnumber* **| l2l | ra-ikev1-ipsec | ra-ikev2-ipsec | vpn-lb | webvpn** } [**filter** { **name** *username* **| ipaddress** *IPaddr* **| a-ipaddress** *IPaddr* **| p-ipaddress** *IPaddr* **| tunnel-group** *groupname* **| protocol** *protocol-name* **| encryption** *encryption-algo* **| inactive** }] [**sort** { **name | ipaddress | a-ipaddress | p-ip address | tunnel-group | protocol | encryption | inactivity** }]

Syntax Description

all	Displays all clustered sessions, active and backup.
anyconnect	**Displays AnyConnect VPN client sessions, including OSPFv3 session information.**
backup {index | l2l}	Display backup sessions only.
detail	(Optional) Displays extended details about a session. For example, using the detail option for an IPsec session displays additional details such as the IKE hashing algorithm, authentication mode, and rekey interval. If you choose detail, and the full option, the ASA displays the detailed output in a machine-readable format.
email-proxy	(Deprecated) Displays email-proxy sessions.
encryption	Displays the ratio of encryption types as a ratio of the total number of sessions.
failover	Displays the session information for the failover IPsec tunnels.
filter *filter_criteria*	(Optional) Filters the output to display only the information you specify by using one or more of the filter options. For a list of *filter_criteria* options, see the "Usage Guidelines" section.
full	(Optional) Displays streamed, untruncated output. Output is delineated by | characters and a || string between records.
index *indexnumber*	Displays a single session by index number. Specifies the index number for the session, which ranges from 1 - 750.
l2l	Displays VPN LAN-to-LAN session information. When you choose detail, cluster information is also provided.
license-summary	Displays VPN license summary information.
ospfv3	Displays OSPFv3 session information.
protocol	Displays the ratio of protocol types as a ratio of the total number of sessions.

ra-ikev1-ipsec	Displays IPsec IKEv1 sessions.
ra-ikev2-ipsec	Displays details for IKEv2 remote access client connections.
sort *sort_criteria*	(Optional) Sorts the output according to the sort option you specify. For a list of *sort_criteria* options, see the "Usage Guidelines" section.
summary	Displays VPN session summary information.
vpn-lb	Displays VPN load balancing management sessions.
webvpn	Displays clientless SSL VPN sessions, including OSPFv3 session information.

Command Default

There is no default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	The VLAN field description was added.
8.0(5)	**inactive** as a **filter** option and **inactivity** as a **sort** option were added.
8.2(1)	License information was added to the output.
8.4(1)	The svc keyword was changed to anyconnect. The remote keyword was changed to ra-ikev1-ipsec. The **ratio keyword was added.**
9.0(1)	The **ospfv3** keyword was added, and the OSPFv3 session information is now included in the VPN session summary. The **filter a-ipversion** and **filter p-ipversion** options were added to allow filtering on all Secure Client, LAN-to-LAN, and Clientless SSL VPN sessions assigned IPv4 or IPv6 addresses. Support for multiple context mode was added.
9.1(2)	The failover tunnel type and **failover** keyword to support failover IPsec tunnels was added. See the **failover ipsec pre-shared-key** command.
9.1(4)	Output when using the **detail anyconnect** options and show crypto ipsec sa has been updated to reflect the assigned IPv6 address and to indicate the GRE Transport Mode security association when doing IKEv2 dual traffic.

Release	Modification
9.3(2)	The ra-ikev2-ipsec keyword to display details for IKEv2 remote access client connections was added. The VPN session summary output was updated to include IKEv2 remote access client connections and IKEv2 and IPsec tunnel counts. The VPN licenses usage summary output was updated to add IKEv2 remote access client connections.
9.4(1)	Cert Auth Int and Cert Auth Left were added to the output of this command.
9.8(1)	The email-proxy option was deprecated.
9.9(1)	The all and backup options added.
9.19(1)	The ra-ikev2-ipsec keyword to display both IPv4 and IPv6 addresses assigned to IKEv2 remote access client VPN session.

Usage Guidelines

You can use the following options to filter and to sort the session display:

Filter/Sort Option	Description
filter a-ipaddress *IPaddr*	Filters the output to display information for the specified assigned IP address or addresses only.
sort a-ipaddress	Sorts the display by assigned IP addresses.
filter a-ipversion {v4 | v6}	Filters the output to display information about all Secure Client sessions assigned IPv4 or IPv6 addresses.
filter encryption *encryption-algo*	Filters the output to display information for sessions using the specified encryption algorithm(s) only.
sort encryption	Sorts the display by encryption algorithm. Encryption algorithms include: aes128, aes192, aes256, des, 3des, rc4
filter inactive	Filters inactive sessions which have gone idle and have possibly lost connectivity (due to hibernation, mobile device disconnection, and so on). The number of inactive sessions increases when TCP keepalives are sent from the ASA without a response from the Secure Client. Each session is time stamped with the SSL tunnel drop time. If the session is actively passing traffic over the SSL tunnel, 00:00m:00s is displayed. **Note** The ASA does not send TCP keepalives to some devices (such as the iPhone, iPad, and iPod) to save battery life, so the failure detection cannot distinguish between a disconnect and a sleep. For this reason, the inactivity counter remains as 00:00:00 by design.
sort inactivity	Sorts inactive sessions.
filter ipaddress *IPaddr*	Filters the output to display information for the specified inside IP address or addresses only.
sort ipaddress	Sorts the display by inside IP addresses.

Filter/Sort Option	Description
filter name *username* **sort name**	Filters the output to display sessions for the specified username(s). Sorts the display by usernames in alphabetical order.
filter p-address *IPaddr*	Filters the output to display information for the specified outside IP address only.
sort p-address	Sorts the display by the specified outside IP address or addresses.
filter p-ipversion {v4 | v6}	Filters the output to display information about all Secure Client sessions originating from endpoints with IPv4 or IPv6 addresses.
filter protocol *protocol-name*	Filters the output to display information for sessions using the specified protocol(s) only.
sort protocol	Sorts the display by protocol. Protocols include: IKE, IMAP4S, IPsec, IPsecLAN2LAN, IPsecLAN2LANOverNatT, IPsecOverNatT, IPsecoverTCP, IPsecOverUDP, SMTPS, userHTTPS, vcaLAN2LAN
filter tunnel-group *groupname*	Filters the output to display information for the specified tunnel group(s) only.
sort tunnel-group	Sorts the display by tunnel group.
|	Modifies the output, using the following arguments: {begin | include | exclude | grep | [-v]} {reg_exp}

Note: The command output shows the username only up to 120 characters. If the length exceeds 120, the remaining characters are truncated and displayed in the command output.

Examples

The following is sample output from the **show vpn-sessiondb** command:

```
ciscoasa
#
 show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ------------------------------------------------
AnyConnect Client           :      1 :         78 :           2 :        0
  SSL/TLS/DTLS              :      1 :         72 :           2 :        0
  IKEv2 IPsec               :      0 :          6 :           1 :        0
IKEv2 Generic IPsec Client  :      0 :          0 :           0
Clientless VPN              :      0 :          8 :           2
  Browser                   :      0 :          8 :           2
--------------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :     86
Device Total VPN Capacity   :    750
Device Load                 :     0%
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concurrent
```

```
                            ---------------------------------------------
IKEv2                       :      0 :          6 :               1
IPsecOverNatT               :      0 :          6 :               1
Clientless                  :      0 :         17 :               2
AnyConnect-Parent           :      1 :         69 :               2
SSL-Tunnel                  :      1 :         75 :               2
DTLS-Tunnel                 :      1 :         56 :               2
-------------------------------------------------------------------------------
Totals                      :      3 :        229
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
IPv6 Usage Summary
-------------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                            ---------------------------------------------
AnyConnect SSL/TLS/DTLS     :        :            :
  IPv6 Peer                 :      1 :         41 :           2
  Tunneled IPv6             :      1 :         70 :           2
AnyConnect IKEv2            :        :            :
  IPv6 Peer                 :      0 :          4 :           1
Clientless                  :        :            :
  IPv6 Peer                 :      0 :          1 :           1
-------------------------------------------------------------------------------
```

The following is sample output from the **show vpn-sessiondb detail l2l** command, showing detailed information about LAN-to-LAN sessions:

```
ciscoasa
#
 show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed
Connection   : 172.16.0.0
Index        : 1
IP Addr      : 172.16.0.0
Protocol     : IKEv2 IPsec
Encryption   : IKEv2: (1)AES256  IPsec: (1)AES256
Hashing      : IKEv2: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 240                   Bytes Rx     : 160
Login Time   : 14:50:35 UTC Tue May 1 2012
Duration     : 0h:00m:11s
IKEv2 Tunnels: 1
IPsec Tunnels: 1
IKEv2:
  Tunnel ID    : 1.1
  UDP Src Port : 500                   UDP Dst Port : 500
  Rem Auth Mode: preSharedKeys
  Loc Auth Mode: preSharedKeys
  Encryption   : AES256                Hashing      : SHA1
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 86389 Seconds
  PRF          : SHA1                  D/H Group    : 5
  Filter Name  :
  IPv6 Filter  :
IPsec:
  Tunnel ID    : 1.2
  Local Addr   : 10.0.0.0/255.255.255.0
  Remote Addr  : 209.165.201.30/255.255.255.0
  Encryption   : AES256                Hashing      : SHA1
  Encapsulation: Tunnel                PFS Group    : 5
  Rekey Int (T): 120 Seconds           Rekey Left(T): 107 Seconds
  Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
  Bytes Tx     : 240                   Bytes Rx     : 160
  Pkts Tx      : 3                     Pkts Rx      : 2
```

```
NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 13 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

The following is sample output from the **show vpn-sessiondb detail index 1** command:

```
AsaNacDev# show vpn-sessiondb detail index 1
Session Type: Remote Detailed
Username     : user1
Index        : 1
Assigned IP  : 192.168.2.70           Public IP    : 10.86.5.114
Protocol     : IPsec                  Encryption   : AES128
Hashing      : SHA1
Bytes Tx     : 0                      Bytes Rx     : 604533
Client Type  : WinNT                  Client Ver   : 4.6.00.0049
Tunnel Group : bxbvpnlab
Login Time   : 15:22:46 EDT Tue May 10 2005
Duration     : 7h:02m:03s
Filter Name  :
NAC Result   : Accepted
Posture Token: Healthy
VM Result    : Static
VLAN         : 10
IKE Sessions: 1 IPsec Sessions: 1 NAC Sessions: 1
IKE:
  Session ID   : 1
  UDP Src Port : 500                    UDP Dst Port : 500
  IKE Neg Mode : Aggressive             Auth Mode    : preSharedKeysXauth
  Encryption   : 3DES                   Hashing      : MD5
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 61078 Seconds
  D/H Group    : 2
IPsec:
  Session ID   : 2
  Local Addr   : 0.0.0.0
  Remote Addr  : 192.168.2.70
  Encryption   : AES128                 Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 26531 Seconds
  Bytes Tx     : 0                      Bytes Rx     : 604533
  Pkts Tx      : 0                      Pkts Rx      : 8126
NAC:
  Reval Int (T): 3000 Seconds           Reval Left(T): 286 Seconds
  SQ Int (T)   : 600 Seconds            EoU Age (T)  : 2714 Seconds
  Hold Left (T): 0 Seconds              Posture Token: Healthy
  Redirect URL : www.cisco.com
```

The following is sample output from the **show vpn-sessiondb ospfv3** command:

```
asa# show vpn-sessiondb ospfv3

Session Type: OSPFv3 IPsec
Connection   :
Index        : 1                      IP Addr      : 0.0.0.0
Protocol     : IPsec
Encryption   : IPsec: (1)none         Hashing      : IPsec: (1)SHA1
Bytes Tx     : 0                      Bytes Rx     : 0
Login Time   : 15:06:41 EST Wed Feb 1 2012
Duration     : 1d 5h:13m:11s
```

The following is sample output from the **show vpn-sessiondb detail ospfv3** command:

```
asa# show vpn-sessiondb detail ospfv3
```

```
Session Type: OSPFv3 IPsec Detailed
Connection   :
Index        : 1                       IP Addr      : 0.0.0.0
Protocol     : IPsec
Encryption   : IPsec: (1)none          Hashing      : IPsec: (1)SHA1
Bytes Tx     : 0                       Bytes Rx     : 0
Login Time   : 15:06:41 EST Wed Feb 1 2012
Duration     : 1d 5h:14m:28s
IPsec Tunnels: 1
IPsec:
  Tunnel ID    : 1.1
  Local Addr   : ::/0/89/0
  Remote Addr  : ::/0/89/0
  Encryption   : none                    Hashing      : SHA1
  Encapsulation: Transport
  Idle Time Out: 0 Minutes               Idle TO Left : 0 Minutes
  Bytes Tx     : 0                       Bytes Rx     : 0
  Pkts Tx      : 0                       Pkts Rx      : 0

NAC:
  Reval Int (T): 0 Seconds               Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds               EoU Age(T)   : 105268 Seconds
  Hold Left (T): 0 Seconds               Posture Token:
  Redirect URL :
```

The following is sample output from the **show vpn-sessiondb summary** command:

```
ciscoasa# show vpn-sessiondb summary

-------------------------------------------------------------------------------
VPN Session Summary
-------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ------------------------------------------------
OSPFv3 IPsec               :      1 :          1 :           1
-------------------------------------------------------------------------------
Total Active and Inactive    :      1             Total Cumulative :      1
Device Total VPN Capacity    :  10000
Device Load                  :     0%
-------------------------------------------------------------------------
```

The following is sample output from the **show vpn-sessiondb summary** command for generic IKEv2 IPsec remote access sessions:

```
ciscoasa# show vpn-sessiondb summary
-------------------------------------------------------------------------------
VPN Session Summary
-------------------------------------------------------------------------------
                              Active : Cumulative : Peak Concur : Inactive
                             ------------------------------------------------
Generic IKEv2 Remote Access  :      1 :          1 :           1
-------------------------------------------------------------------------------
Total Active and Inactive    :      1             Total Cumulative :      1
Device Total VPN Capacity    :    250
Device Load                  :     0%
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Tunnels Summary
-------------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ------------------------------------------------
IKEv2                        :      1 :          1 :               1
```

```
IPsec                        :      1 :          1 :               1
-------------------------------------------------------------------------------
Totals                       :      2 :          2
-------------------------------------------------------------------------------
```

The following is sample output from the **show vpn-sessiondb det anyconnect** command:

```
ciscoasa# show vpn-sessiondb det anyconnect
Session Type: AnyConnect Detailed
Username     : userab                 Index        : 2
Assigned IP  : 65.2.1.100             Public IP    : 75.2.1.60
Assigned IPv6: 2001:1000::10
Protocol     : IKEv2 IPsecOverNatT AnyConnect-Parent
License      : AnyConnect Premium
Encryption   : IKEv2: (1)3DES  IPsecOverNatT: (1)3DES  AnyConnect-Parent: (1)none
Hashing      : IKEv2: (1)SHA1  IPsecOverNatT: (1)SHA1  AnyConnect-Parent: (1)none
Bytes Tx     : 0                      Bytes Rx     : 21248
Pkts Tx      : 0                      Pkts Rx      : 238
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy          Tunnel Group : test1
Login Time   : 22:44:59 EST Tue Aug 13 2013
Duration     : 0h:02m:42s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1
AnyConnect-Parent:
  Tunnel ID    : 2.1
  Public IP    : 75.2.1.60
  Encryption   : none                   Hashing      : none
  Auth Mode    : userPassword
  Idle Time Out: 400 Minutes            Idle TO Left : 397 Minutes
  Conn Time Out: 500 Minutes            Conn TO Left : 497 Minutes
  Client OS    : Windows
  Client Type  : AnyConnect
  Client Ver   : 3.1.05050
IKEv2:
  Tunnel ID    : 2.2
  UDP Src Port : 64251                  UDP Dst Port : 4500
  Rem Auth Mode: userPassword
  Loc Auth Mode: rsaCertificate
  Encryption   : 3DES                   Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86241 Seconds
  PRF          : SHA1                   D/H Group    : 2
  Filter Name  : mixed1
  Client OS    : Windows
IPsecOverNatT:
  Tunnel ID    : 2.3
  Local Addr   : 75.2.1.23/255.255.255.255/47/0
  Remote Addr  : 75.2.1.60/255.255.255.255/47/0
  Encryption   : 3DES                   Hashing      : SHA1
  Encapsulation: Transport, GRE
  Rekey Int (T): 28400 Seconds          Rekey Left(T): 28241 Seconds
  Idle Time Out: 400 Minutes            Idle TO Left : 400 Minutes
  Conn Time Out: 500 Minutes            Conn TO Left : 497 Minutes
  Bytes Tx     : 0                      Bytes Rx     : 21326
  Pkts Tx      : 0                      Pkts Rx      : 239
NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 165 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

```
Output from show vpn-sessiondb detail anyconnect showing a DTLS tunnel.
...
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 10280                 Bytes Rx     : 3819
Pkts Tx      : 8                     Pkts Rx      : 45
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy         Tunnel Group : DefaultWEBVPNGroup
Login Time   : 09:42:39 UTC Tue Dec 5 2017
Duration     : 0h:00m:07s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                   VLAN         : none
Audt Sess ID : 00000000000010005a266a0f
Security Grp : none
...
DTLS-Tunnel:
  Tunnel ID    : 1.3
  Assigned IP  : 95.0.225.240          Public IP    : 85.0.224.13
  Encryption   : AES256                Hashing      : SHA1
  Ciphersuite  : AES256-SHA
  Encapsulation: DTLSv1.2              UDP Src Port : 51008
  UDP Dst Port : 443                   Auth Mode    : userPassword
  Idle Time Out: 30 Minutes            Idle TO Left : 30 Minutes
  Client OS    : Windows
  Client Type  : DTLS VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.x
```

The following example is sample output from the **show vpn-sessiondb ra-ikev2-ipsec** command:

```
ciscoasa(config)# show vpn-sessiondb detail ra-ikev2-ipsec
Session Type: Generic Remote-Access IKEv2 IPsec Detailed
Username     : IKEV2TG               Index        : 1
Assigned IP  : 95.0.225.200          Public IP    : 85.0.224.12
Assigned IPv6: 2001:db8::1
Protocol     : IKEv2 IPsec
License      : AnyConnect Essentials
Encryption   : IKEv2: (1)3DES  IPsec: (1)AES256
Hashing      : IKEv2: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 0                     Bytes Rx     : 17844
Pkts Tx      : 0                     Pkts Rx      : 230
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : GroupPolicy_IKEV2TG   Tunnel Group : IKEV2TG
Login Time   : 11:39:54 UTC Tue May 6 2014
Duration     : 0h:03m:17s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                   VLAN         : none
Audt Sess ID : 5f00e105000010005368ca0a
Security Grp : none
IKEv2 Tunnels: 1
IPsec Tunnels: 1
```

The following is sample output from the **show vpn-sessiondb license-summary** command:

```
----------------------------------------------------------------------------
VPN Licenses and Configured Limits Summary
----------------------------------------------------------------------------
                                    Status : Capacity : Installed :  Limit
                                   ----------------------------------------
AnyConnect Premium                : DISABLED :      250 :        10 :   NONE
AnyConnect Essentials             :  ENABLED :      250 :       250 :   NONE
Other VPN (Available by Default) :  ENABLED :      250 :       250 :   NONE
```

```
Shared License Server            : DISABLED
Shared License Participant       : DISABLED
AnyConnect for Mobile            : DISABLED(Requires Premium or Essentials)
Advanced Endpoint Assessment     : DISABLED(Requires Premium)
AnyConnect for Cisco VPN Phone   : DISABLED
VPN-3DES-AES                     :  ENABLED
VPN-DES                          :  ENABLED
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
VPN Licenses Usage Summary
-----------------------------------------------------------------------------
                         Local : Shared :   All  :   Peak :  Eff.  :
                        In Use : In Use : In Use : In Use :  Limit : Usage
                       ---------------------------------------------------
AnyConnect Essentials  :      1 :      0 :      1 :      1 :    250 :    0%
  AnyConnect Client    :                :      0 :      0          :    0%
    AnyConnect Mobile  :                :      0 :      0          :    0%
  Generic IKEv2 Client :                :      1 :      1          :    0%
Other VPN              :                :      0 :      0 :    250 :    0%
  Cisco VPN Client     :                :      0 :      0          :    0%
-----------------------------------------------------------------------------
Shared License Network Summary
-----------------------------------------------------------------------------
AnyConnect Premium
  Total shared licenses in network                                : 500
  Shared licenses held by this participant                        :  0
  Shared licenses held by all participants in the network         :  0
-----------------------------------------------------------------------------
```

As shown in the examples, the fields displayed in response to the **show vpn-sessiondb** command vary, depending on the keywords you enter. Table 14-2 describes these fields.

Table 2: show vpn-sessiondb Command Fields

Field	Description
Auth Mode	Protocol or mode used to authenticate this session.
Assigned IP	Private IP address assigned to the remote client for current session.
Assigned IPv6	Private IPv6 address assigned to the remote client for current session.
Bytes Rx	Total number of bytes received from the remote peer or client by the ASA.
Bytes Tx	Number of bytes transmitted to the remote peer or client by the ASA.
Client Type	Client software running on the remote peer, if available.
Client Ver	Version of the client software running on the remote peer.
Connection	Name of the connection or the private IP address.
D/H Group	Diffie-Hellman Group. The algorithm and key size used to generate IPsec SA encryption keys.
Duration	Elapsed time (HH:MM:SS) between the session login time and the last screen refresh.
EAPoUDP Session Age	Number of seconds since the last successful posture validation.

Field	Description
Encapsulation	Mode used to apply IPsec ESP (Encapsulation Security Payload protocol) encryption and authentication (that is, the part of the original IP packet that has ESP applied).
Encryption	Data encryption algorithm this session is using, if any.
EoU Age (T)	EAPoUDP Session Age. Number of seconds since the last successful posture validation.
Filter Name	Username specified to restrict the display of session information.
Hashing	Algorithm used to create a hash of the packet, which is used for IPsec data authentication.
Hold Left (T)	Hold-Off Time Remaining. 0 seconds if the last posture validation was successful. Otherwise, the number of seconds remaining before the next posture validation attempt.
Hold-Off Time Remaining	0 seconds if the last posture validation was successful. Otherwise, the number of seconds remaining before the next posture validation attempt.
IKE Neg Mode	IKE (IPsec Phase 1) mode for exchanging key information and setting up SAs: Aggressive or Main.
IKE Sessions	Number of IKE (IPsec Phase 1) sessions; usually 1. These sessions establish the tunnel for IPsec traffic.
Index	Unique identifier for this record.
IP Addr	Private IP address assigned to the remote client for this session. This is also known as the “inner” or “virtual” IP address. It lets the client appear to be a host on the private network.
IPsec Sessions	Number of IPsec (Phase 2) sessions, which are data traffic sessions through the tunnel. Each IPsec remote-access session can have two IPsec sessions: one consisting of the tunnel endpoints, and one consisting of the private networks reachable through the tunnel.
License Information	Shows information about the shared SSL VPN license.
Local IP Addr	IP address assigned to the local endpoint of the tunnel (that is the interface on the ASA).
Login Time	Date and time (MMM DD HH:MM:SS) that the session logged in. Time is displayed in 24-hour notation.

Field	Description
NAC Result	State of Network Admission Control Posture Validation. It can be one of the following: • Accepted—The ACS successfully validated the posture of the remote host. • Rejected—The ACS could not successfully validate the posture of the remote host. • Exempted—The remote host is exempt from posture validation according to the Posture Validation Exception list configured on the ASA. • Non-Responsive—The remote host did not respond to the EAPoUDP Hello message. • Hold-off—The ASA lost EAPoUDP communication with the remote host after successful posture validation. • N/A—NAC is disabled for the remote host according to the VPN NAC group policy. • Unknown—Posture validation is in progress.
NAC Sessions	Number of Network Admission Control (EAPoUDP) sessions.
Packets Rx	Number of packets received from the remote peer by the ASA.
Packets Tx	Number of packets transmitted to the remote peer by the ASA.
PFS Group	Perfect Forward Secrecy group number.
Posture Token	Informational text string configurable on the Access Control Server. The ACS downloads the posture token to the ASA for informational purposes to aid in system monitoring, reporting, debugging, and logging. A typical posture token is Healthy, Checkup, Quarantine, Infected, or Unknown.
Protocol	Protocol the session is using.
Public IP	Publicly routable IP address assigned to the client.
Redirect URL	Following posture validation or clientless authentication, the ACS downloads the access policy for the session to the ASA. The Redirect URL is an optional part of the access policy payload. The ASA redirects all HTTP (port 80) and HTTPS (port 443) requests for the remote host to the Redirect URL if it is present. If the access policy does not contain a Redirect URL, the ASA does not redirect HTTP and HTTPS requests from the remote host. Redirect URLs remain in force until either the IPsec session ends or until posture revalidation, for which the ACS downloads a new access policy that can contain a different redirect URL or no redirect URL.
Rekey Int (T or D)	Lifetime of the IPsec (IKE) SA encryption keys. The T value is the lifetime in duration, the D value is in data transmitted. Only the T value is shown for remote access VPN.

Field	Description
Rekey Left (T or D)	Lifetime remaining of the IPsec (IKE) SA encryption keys. The T value is the lifetime in duration, the D value is in data transmitted. Only the T value is shown for remote access VPN.
Rekey Time Interval	Lifetime of the IPsec (IKE) SA encryption keys.
Remote IP Addr	IP address assigned to the remote endpoint of the tunnel (that is the interface on the remote peer).
Reval Int (T)	Revalidation Time Interval. Interval in seconds required between each successful posture validation.
Reval Left (T)	Time Until Next Revalidation. 0 if the last posture validation attempt was unsuccessful. Otherwise, the difference between the Revalidation Time Interval and the number of seconds since the last successful posture validation.
Revalidation Time Interval	Interval in seconds required between each successful posture validation.
Session ID	Identifier for the session component (subsession). Each SA has its own identifier.
Session Type	Type of session: LAN-to-LAN or Remote
SQ Int (T)	Status Query Time Interval. Time in seconds allowed between each successful posture validation or status query response and the next status query response. A status query is a request made by the ASA to the remote host to indicate whether the host has experienced any changes in posture since the last posture validation.
Status Query Time Interval	Time in seconds allowed between each successful posture validation or status query response and the next status query response. A status query is a request made by the ASA to the remote host to indicate whether the host has experienced any changes in posture since the last posture validation.
Time Until Next Revalidation	0 if the last posture validation attempt was unsuccessful. Otherwise, the difference between the Revalidation Time Interval and the number of seconds since the last successful posture validation.
Tunnel Group	Name of the tunnel group referenced by this tunnel for attribute values.
UDP Dst Port or UDP Destination Port	Port number used by the remote peer for UDP.
UDP Src Port or UDP Source Port	Port number used by the ASA for UDP.
Username	User login name with which the session is established.
VLAN	Egress VLAN interface assigned to this session. The ASA forwards all traffic to that VLAN. One of the following elements specifies the value: • Group policy • Inherited group policy

Related Commands

Command	Description
show running-configuration vpn-sessiondb	Displays the VPN session database running configuration (max-other-vpn-limit, max-anyconnect-premium-or-essentials-limit).
show vpn-sessiondb ratio	Displays VPN session encryption or protocol ratios.

show vpn-sessiondb ratio

To display the ratio of current sessions as a percentage by protocol or encryption algorithm, use the **show vpn-sessiondb ratio** command in privileged EXEC mode.

show vpn-sessiondb ratio { **protocol | encryption** } [**filter** *groupname*]

Syntax Description

encryption	Identifies the encryption protocols you want to display. Refers to phase 2 encryption. Encryption algorithms include:	
	aes128	des
	aes192	3des
	aes256	rc4
filter *groupname*	Filters the output to include session ratios only for the tunnel group you specify.	
protocol	Identifies the protocols you want to display. Protocols include:	
	IKEv1	L2TPOverIPsecOverNatT
	IKEv2	Clientless
	IPsec	Port-Forwarding
	IPsecLAN2LAN	IMAP4S
	IPsecLAN2LANOverNatT	POP3S
	IPsecOverNatT	SMTPS
	IPsecOverTCP	AnyConnect-Parent
	IPsecOverUDP	SSL-Tunnel
	L2TPOverIPsec	DTLS-Tunnel

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
8.4(1)	The output was enhanced to include IKEv2.
9.0(1)	Support for multiple context mode was added.

Examples

The following is sample output for the **show vpn-sessiondb ratio** command, with **encryption** as the argument:

```
ciscoasa# show vpn-sessiondb ratio encryption
Filter Group         : All
Total Active Sessions: 5
Cumulative Sessions  : 9
Encryption               Sessions       Percent
none                     0               0%
DES                      1              20%
3DES                     0               0%
AES128                   4          80%
AES192                   0               0%
AES256                   0               0%
```

The following is sample output for the **show vpn-sessiondb ratio** command with **protocol** as the argument:

```
ciscoasa# show vpn-sessiondb ratio protocol
Filter Group         : All
Total Active Sessions: 6
Cumulative Sessions  : 10
Protocol                 Sessions       Percent
IKE                      0               0%
IPsec                    1              20%
IPsecLAN2LAN             0               0%
IPsecLAN2LANOverNatT     0               0%
IPsecOverNatT            0               0%
IPsecOverTCP             1        20%
IPsecOverUDP             0               0%
L2TP                     0               0%
L2TPOverIPsec            0               0%
L2TPOverIPsecOverNatT    0               0%
PPPoE                    0               0%
vpnLoadBalanceMgmt       0               0%
userHTTPS                0               0%
IMAP4S                   3      30%
POP3S                    0               0%
SMTPS                    3        30%
```

Related Commands

Command	Description
show vpn-sessiondb	Displays sessions with or without extended details, optionally filtered and sorted by criteria you specify.
show vpn-sessiondb summary	Displays a session summary, including total current session, current sessions of each type, peak and total cumulative, maximum concurrent sessions

show vpn-sessiondb summary

To display the number of IPsec, Cisco Secure Client, and NAC sessions, use the **show vpn-sessiondb summary** command in privileged EXEC mode.

show vpn-sessiondb summary

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(7)	This command was added.
8.0(2)	The VLAN Mapping Sessions table was added.
8.0(5)	New output for active, cumulative, peak concurrent, and inactive was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following is sample output for the **show vpn-sessiondb summary** command with one IPsec IKEv1 and one clientless session:

Note A device in standby does not differentiate active from inactive sessions.

```
ciscoasa# show vpn-sessiondb summary
VPN Session Summary
Sessions:
       Active : Cumulative : Peak Concurrent : Inactive :
 Clientless VPN        :  1:   2:    1  Browser       :  1:   2:    1 IKEv1 IPsec/L2TP IPsec
     0  :  1:   1:    1
Total Active and Inactive: 2          Total Cumulative: 3
Device Total VPN Capacity: 10000
Device Load      : 0%
License Information:
 Shared VPN License Information:
  SSL VPN        : 12000
   Allocated to this device       :  0
```

```
   Allocated to network       :  0
   Device limit       : 750
IPsec  : 750   Configured : 750    Active :  0   Load :  0%
SSL VPN  : 750  Configured : 750    Active :   0  Load :  0%
      Active : Cumulative : Peak Concurrent
SSL VPN     :   0 :   1 :    1
Totals    :   0 :   1 :
Active NAC Sessions:
  Accepted               : 0
  Rejected               : 0
  Exempted               : 0
  Non-responsive         : 0
Hold-off               : 0
  N/A                    : 0
Active VLAN Mapping Sessions:
  Static                 : 0
  Auth                   : 0
  Access                 : 0
  Guest                  : 0
  Quarantine             : 0
  N/A                    : 0
ciscoasa#
```

You can use the SSL output to determine the physical device resources in respect to the number of licenses. A single user session may occupy a license but could use multiple tunnels. For example, an Secure Client user with DTLS often has the parent session, SSL tunnel, and DTLS tunnels associated with it.

Note The parent session represents when the client is not actively connected. It does not represent an encrypted tunnel. If the client shuts down, or sleeps, IPsec, IKE, TLS, and DLTLS tunnels are closed, but the parent session remains until the idle time or maximum connect time limit is reached. This enables the user to reconnect without reauthenticating.

With this example, you would see three tunnels allocated on the device, even if only one user is logged in. An IPsec LAN-to-LAN tunnel counts as one session, and it allows many host-to-host connections through the tunnel. An IPsec remote access session is one remote access tunnel that supports one user connection.

From the output you can see which sessions are active. If a session has no underlying tunnels associated to it, the status is *waiting to resume* mode (displayed as clientless in the session output). This mode means that dead peer detection from the head-end device has started, and the head-end device can no longer communicate with the client. When you encounter this condition, you can hold the session to allow the user to roam networks, go to sleep, recover the session, and so on. These sessions count towards the actively connected sessions (from a license standpoint) and are cleared with a user idle timeout, a user logging out, or a resumption of the original session.

The Active SSL VPN With Client column shows the number of active connections passing data. The Cumulative SSL VPN With Client column shows the number of active sessions that have been established. It includes those that are inactive and increments only when a new session is added. The Peak Concurrent SSL VPN With Client column shows the peak number of concurrently active sessions that are passing data. The Inactive SSL VPN With Client column shows how long the Secure Client was disconnected. You can use this Inactivity timeout value to determine when licenses are expired. The ASA can then determine whether reconnection is possible. These are Secure Client sessions without an active SSL tunnel associated with them.

Table 14-3 explains the fields in the Active Sessions and Session Information tables.

Table 3: show vpn-sessiondb summary Command: Active Sessions and Session Information Fields

Field	Description
Concurrent Limit	Maximum number of concurrently active sessions permitted on this ASA.
Cumulative Sessions	Number of sessions of all types since the ASA was last booted or reset.
LAN-to-LAN	Number of IPsec LAN-to-LAN sessions that are currently active.
Peak Concurrent	Highest number of sessions of all types that were concurrently valid sessions (active + inactive) since the ASA was last booted or reset.
Percent Session Load	Percentage of the vpn session allocation in use. This value equals the Total Active Sessions divided by the maximum number of sessions available, displayed as a percentage. The maximum number of sessions available can be either of the following: • Maximum number of IPsec and SSL VPN sessions licensed • **vpn-sessiondb ?** (maximum number of sessions configured) • **max-anyconnect-premium-or-essentials-limit** (maximum AnyConnect Premium or Essentials session limit) • **max-other-vpn-limit** (maximum other VPN session limit)
Remote Access	ra-ikev1-ipsec—Number of IKEv1 IPsec remote-access user, L2TP over IPsec, and IPsec through NAT sessions that are currently active.
Total Active Sessions	Number of sessions of all types that are currently active.

Examples

The Active NAC Sessions table shows general statistics about remote peers that are subject to posture validation.

The Cumulative NAC Sessions table shows general statistics about remote peers that are or have been subject to posture validation.

Table 14-2 explains the fields in the Active NAC Sessions and Total Cumulative NAC Sessions tables.

Table 4: show vpn-sessiondb summary Command: Active NAC Sessions and Total Cumulative NAC Sessions Fields

Field	Description
Accepted	Number of peers that passed posture validation and have been granted an access policy by an Access Control Server.
Exempted	Number of peers that are not subject to posture validation because they match an entry in the Posture Validation Exception list configured on the ASA.
Hold-off	Number of peers for which the ASA lost EAPoUDP communications after a successful posture validation. The NAC Hold Timer attribute (Configuration > VPN > NAC) determines the delay between this type of event and the next posture validation attempt for each peer.
N/A	Number of peers for which NAC is disabled according to the VPN NAC group policy.

Field	Description
Non-responsive	Number of peers not responsive to Extensible Authentication Protocol (EAP) over UDP requests for posture validation. Peers on which no CTA is running do not respond to these requests. If the ASA configuration supports clientless hosts, the Access Control Server downloads the access policy associated with clientless hosts to the ASA for these peers. Otherwise, the ASA assigns the NAC default policy.
Rejected	Number of peers that failed posture validation or were not granted an access policy by an Access Control Server.

The Active VLAN Mapping Sessions table shows general statistics about remote peers that are subject to posture validation.

The Cumulative VLAN Mapping Sessions table shows general statistics about remote peers that are or have been subject to posture validation.

Table 14-5 explains the fields in the Active VLAN Mapping Sessions and Cumulative VLAN Mapping Sessions tables.

Table 5: show vpn-sessiondb summary Command: Active VLAN Mapping Sessions and Cumulative Active VLAN Mapping Sessions Fields

Field	Description
Access	Reserved for future use.
Auth	Reserved for future use.
Guest	Reserved for future use.
N/A	Reserved for future use.
Quarantine	Reserved for future use.
Static	This field shows the number of VPN sessions assigned to a pre-configured VLAN.

Related Commands

Command	Description
show vpn-sessiondb	Displays sessions with or without extended details, optionally filtered and sorted by criteria you specify.
show vpn-sessiondb ratio	Displays VPN session encryption or protocol ratios.

show wccp

To display global statistics related to Web Cache Communication Protocol (WCCP), use the **show wccp** command in privileged EXEC mode.

show wccp { **web-cache** | *service-number* } [*detail* | *view*]

Syntax Description

detail	(Optional) Displays information about the router and all web caches.
service-number	(Optional) Identification number of the web-cache service group being controlled by the cache. The number can be from 0 to 256. For web caches using Cisco Cache Engines, the reverse proxy service is indicated by a value of 99.
view	(Optional) Displays other members of a particular service group have or have not been detected.
web-cache	Specifies statistics for the web-cache service.

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to display WCCP information:

```
ciscoasa(config)# show wccp
Global WCCP information:
    Router information:
        Router Identifier:                  -not yet determined-
        Protocol Version:                   2.0
    Service Identifier: web-cache
        Number of Cache Engines:            0
        Number of routers:                  0
        Total Packets Redirected:           0
        Redirect access-list:               foo
        Total Connections Denied Redirect:  0
        Total Packets Unassigned:           0
        Group access-list:                  foobar
```

```
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total Bypassed Packets Received:     0
ciscoasa(config)#
```

Related Commands

Commands	Description
wccp	Enables support of WCCP with service groups.
wccp redirect	Enables support of WCCP redirection.

show webvpn anyconnect

To view information about SSL VPN client images installed on the ASA and loaded in cache memory, or to test a file to see if it is a valid client image, use the show webvpn anyconnect command from privileged EXEC mode.

show webvpn anyconnect [**image** *filename*]

Syntax Description

image *filename*	Specifies the name of a file to test as an SSL VPN client image file.

Command Default

This command has no default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was added.
8.4(1)	The **show webvpn** anyconnect form of the command replaced show webvpn svc.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use the **show webvpn anyconnect** command to view information about SSL VPN client images that are loaded in cache memory and available for download to remote PCs. Use the **image** *filename* keyword and argument to test a file to see if it is a valid image. If the file is not a valid image, the following message appears:

```
ERROR: This is not a valid SSL VPN Client image file.
```

Examples

The following example shows the output of the show webvpn anyconnect command for currently installed images:

```
ciscoasa# show webvpn anyconnect
1. windows.pkg 1
SSL VPN Client
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
2. window2.pkg 2
```

```
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
```

The following example shows the output of the **show webvpn anyconnect image** *filename* command for a valid image:

```
ciscoasa(config-webvpn)# show webvpn anyconnect image sslclient-win-1.0.2.127.pkg
This is a valid SSL VPN Client image:
  CISCO STC win2k+ 1.0.0
  1,0,2,127
  Fri 07/22/2005 12:14:45.43
```

Related Commands

Command	Description
anyconnect enable	Enables the ASA to download the SSL VPN client to remote PCs.
anyconnect image	Causes the security appliance to load SSL VPN client files from flash memory to cache memory, and specifies the order in which the security appliance downloads portions of the client image to the remote PC as it attempts to match the client image with the operating system.
vpn-tunnel-protocol	Enables specific VPN tunnel protocols for remote VPN users, including SSL used by an SSL VPN client.

show webvpn anyconnect external-browser-pkg

To view information about the single sing-on external browser package file, use the show webvpn anyconnect external-browser-pkg command from privileged EXEC mode.

show webvpn anyconnect external-browser-pkg [*package-path*]

Syntax Description

package-path	Specifies the path where the AnyConnect external browser package is installed.

Command Default

This command has no default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.17(1)	This command was added.

Usage Guidelines

Use the **show webvpn anyconnectexternal-browser-pkg** command to view information about the AnyConnect external browser package. Use the *package-path* keyword and argument to specify the path where the package is installed.

Examples

The following example shows the output of the show webvpn anyconnect external-browser-pkg command:

```
ciscoasa# show webvpn anyconnect external-browser-pkg
disk0:/external-sso-98.161.00015-webdeploy-k9.pkg
Cisco AnyConnect External Browser Headend Package
  98.161.00015
  Wed 07/15/21 15:49:27.81738
```

Related Commands

Command	Description
anyconnect image	Causes the security appliance to load SSL VPN client files from flash memory to cache memory, and specifies the order in which the security appliance downloads portions of the client image to the remote PC as it attempts to match the client image with the operating system.
external-browser	Configures the default operating system for single sign-on authentication.

show webvpn csd (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To determine whether CSD is enabled, display the CSD version in the running configuration, determine what image is providing the Host Scan package, and to test a file to see if it is a valid CSD distribution package, use the show webvpn csd command in privileged EXEC mode.

show webvpn csd [**image** *filename*]

Syntax Description

filename	Specifies the name of a file to test for validity as a CSD distribution package. It must take the form **csd_n.n.n-k9.pkg**.

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
7.1(1)	This command was added.
9.5(2)	This command was deprecated. It is replaced by **show webvpn hostscan**.
9.0(1)	Support for multiple context mode was added.

Examples

Use the **show webvpn csd** command to check the operational status of CSD. The CLI responds with a message indicating if CSD is installed and if it is enabled, if Host Scan is installed and if it is enabled, and which image is supplying the Host Scan package if there is both a CSD package and a Host Scan package installed.

```
ciscoasa# show webvpn csd
```

These are the messages you could receive:

- Secure Desktop is not installed

Hostscan is not installed

- Secure Desktop version n.n.n.n is currently installed but not enabled

Standalone Hostscan package is not installed (Hostscan is currently installed via the CSD package but not enabled)

- Secure Desktop version n.n.n.n is currently installed and enabled

```
Standalone Hostscan package is not installed (Hostscan is currently installed and enabled
via the CSD package)
```

The message, " Secure Desktop version n.n.n.n is currently installed ... " means that the image is loaded on the ASA and in the running configuration. The image can be either enabled or not enabled. You can go to webvpn configuration mode and enter the **csd enable** command to enable CSD.

The messaage, " (Hostscan is currently installed and enabled via the CSD package) " means that the Host Scan package delivered with the CSD package is the Host Scan package in use.

- Secure Desktop version n.n.n.n is currently installed and enabled

Hostscan version n.n.n.n is currently installed and enabled

The message, " Secure Desktop version n.n.n.n is currently installed and enabled Hostscan version n.n.n.n is currently installed and enabled " means that both CSD and a Host Scan package, delivered either as a standalone package or as part of an Secure Client image, are installed. If Host Scan is enabled and both CSD and an Secure Client image with Host Scan, or a standalone Host Scan package, are installed and enabled, the Host Scan package delivered as a standalone package or as part of an Secure Client image takes precedence over the one provided with a CSD package.

- Secure Desktop version n.n.n.n is currently installed but not enabled

Hostscan version n.n.n.n is currently installed but not enabled

Use the **show webvpn csd image** *filename* command to test a file to determine if a CSD distribution package is valid.

ciscoasa# **show webvpn csd image csd_n.n.n-k9.pkg**

The CLI responds with one of the following messages when you enter this command:

- ERROR: This is not a valid Secure Desktop image file.

Make sure the filename is in the form the form **csd_n.n.n_k9.pkg**. If the csd package does not have this naming convention, replace the file with one obtained from the following website:

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

Then reenter the **show webvpn csd image** command. If the image is valid, use the **csd image** and **csd enable** commands in webvpn configuration mode to install and enable CSD.

- This is a valid Cisco Secure Desktop image:

Version : 3.6.172.0

Hostscan Version : 3.6.172.0

Built on : Wed Feb 23 15:46:44 MST 2011

Note that the CLI provides both the version and date stamp if the file is valid.

Related Commands

Command	Description
csd enable	Enables CSD for management and remote user access.
csd image	Copies the CSD image named in the command, from the flash drive specified in the path to the running configuration.

show webvpn debug-condition

To view information about the WebVPN debug filters, use the **show webvpn debug-condition** command from privileged EXEC mode.

show webvpn debug-condition

Syntax Description

This command has no arguments or keywords.

Command Default

This command has 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
9.14	The command was added.

Usage Guidelines

WebVPN must be running when you enter the **show webvpn debug-condition** command.

Example

The following example displays information about the webvpn debug filters:

```
ciscoasa#show webvpn debug-condition
INFO: Webvpn conditional debug is turned OFF
```

show webvpn group-alias

To display the aliases for a specific tunnel-group or for all tunnel groups, use the **group-alias** command in privileged EXEC mode.

show webvpn group-alias [*tunnel-group*]

Syntax Description

tunnel-group	(Optional) Specifies a particular tunnel group for which to show the group aliases.

Command Default

If you do not enter a tunnel-group name, this command displays all the aliases for all the tunnel groups.

Command Modes

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

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

Command History

Release	Modification
7.1	This command was added.
9.0	Support for multiple context mode was added.

Usage Guidelines

WebVPN must be running when you enter the **show webvpn group-alias** command.

Each tunnel group can have multiple aliases or no alias.

Examples

The following example shows the **show webvpn group-alias** command that displays the aliases for the tunnel group “devtest” and the output of that command:

```
ciscoasa# show webvpn group-alias devtest
QA
Fra-QA
```

Related Commands

Command	Description
group-alias	Specifies one or more URLs for the group.
tunnel-group webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

show webvpn group-url

To display the URLs for a specific tunnel-group or for all tunnel groups, use the **group-url** command in privileged EXEC mode.

show webvpn group-url [*tunnel-group*]

Syntax Description

tunnel-group	(Optional) Specifies a particular tunnel group for which to show the URLs.

Command Default

If you do not enter a tunnel-group name, this command displays all the URLs for all the tunnel groups.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

WebVPN must be running when you enter the **show webvpn group-url** command. Each group can have multiple URLs or no URL.

Examples

The following example shows the **show webvpn group-url** command that displays the URLs for the tunnel group “frn-eng1” and the output of that command:

```
ciscoasa# show webvpn group-url
http://www.cisco.com
https://fra1.example.com
https://fra2.example.com
```

Related Commands

Command	Description
group-url	Specifies one or more URLs for the group.
tunnel-group webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

show webvpn hostscan

To determine whether Hostscan is enabled, display the Hostscan version in the running configuration, determine which image is providing the Host Scan package, and to test a file to see if it is a valid Hostscan distribution package, use the show webvpn hostscan command in privileged EXEC mode.

show webvpn hostscan [**image** *filename*]

Syntax Description

filename	Specifies the name of a file to test for validity as a Hostscan distribution package. It must take the form **hostscan_4.1.04011-k9.pkg**.

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
9.5(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

Use the **show webvpn hostscan** command to check the operational status of Hostscan. The CLI responds with a message indicating if Hostscan is installed and if it is enabled, if Host Scan is installed and if it is enabled, and which image is supplying the Host Scan package.

```
ciscoasa# show webvpn hostscan
```

These are the messages you could receive:

- Hostscan is not installed
- Hostscan n.n.n is currently installed and enabled

The message, " Hostscan version n.n.n is currently installed ... " means that the image is loaded on the ASA and in the running configuration. The image can be either enabled or not enabled. You can go to webvpn configuration mode and enter the **hostscan enable** command to enable CSD.

- Hostscan version n.n.n is currently installed but not enabled

Use the **show webvpn hostscan image** *filename* command to test a file to determine if a Hostscan distribution package is valid.

ciscoasa# **show webvpn hostscan image hostscan_4.1.04011-k9.pkg**

The CLI responds with one of the following messages when you enter this command:

- ERROR: This is not a valid Hostscan image file.

Make sure the filename is in the form the form **hostscan_n.n.n-k9.pkg**. If the Hostscan package does not have this naming convention, replace the file with one obtained from the Cisco download site for the version of Secure Client that you are using.

Then reenter the **show webvpn hostscan image** command. If the image is valid, use the **hostscan image** and **hostscan enable** commands in webvpn configuration mode to install and enable Hostscan.

- This is a valid Hostscan image:

Version : 4.1.4011

Built on : Mon July 27 15:46:44 MST 2015

Note that the CLI provides both the version and date stamp if the file is valid.

Related Commands

Command	Description
hostscan enable	Enables Hostscan for management and remote user access.
hostscan image	Copies the Hostscan image named in the command, from the flash drive specified in the path to the running configuration.

show webvpn hsts

To view information about HTTP Strict-Transport-Security (HSTS) on ASA, use the **show webvpn hsts** command from privileged EXEC mode.

show webvpn hsts host { **all** | **name** *hsts_hostname* }

Syntax Description

all	Displays information about all HSTS hosts.
name	Displays information about a specific HSTS host.
hsts_hostname	Specifies a particular HSTS host.

Command Default

This command has 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
9.14	The command was added.

Usage Guidelines

WebVPN must be running when you enter the **show webvpn hsts** command.

Example

The following example displays information about all the HSTS hosts:

```
ciscoasa#show webvpn hsts all
```

show webvpn kcd

Use the **show** webvpn kcd command in webvpn configuration mode to display the Domain Controller information and Domain join status on the ASA.

show webvpn kcd

Syntax Description

None.

Command Default

There are no defaults for this command.

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
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

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

Usage Guidelines

The **show** webvpn kcd command in webvpn configuration mode displays the Domain Controller information and Domain join status on the ASA.

Examples

The following example shows important details to note from the **show webvpn kcd** command and the interpretation of the status message.

This example shows that the registration is under way and not finished:

ciscoasa # **show webvpn kcd**Kerberos Realm: CORP.TEST.INTERNALDomain Join: In-Progress

This example shows that a registration was successful and that the ASA has joined the domain:

```
ciscoasa# show webvpn kcd
Kerberos Realm: CORP.TEST.INTERNALDomain Join: Complete
```

Related Commands

Command	Description
clear aaa kerberos	Clears all the Kerberos tickets cached on the ASA.
kcd-server	Allows the ASA to join an Active Directory domain.

Command	Description
show aaa kerberos	Displays all the Kerberos tickets cached on the ASA.

show webvpn mus

To view information about Mobile User Security (MUS), use the **show webvpn mus** command in privileged EXEC mode.

show webvpn mus

Syntax Description

This command has no arguments or keywords.

Command Default

This command has 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
9.14	The command was added.

Usage Guidelines

WebVPN must be running when you enter the **show webvpn mus** command.

Example

The following example displays information about Mobile User Security:

```
ciscoasa#show webvpn mus
No active WSA connections
```

show webvpn saml

To view information about the SAML identity provider, use the **show webvpn saml idp** command from privileged EXEC mode.

show webvpn saml idp

Syntax Description

This command has no arguments or keywords.

Command Default

This command has 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
9.14	The command was added.

Usage Guidelines

WebVPN must be running when you enter the **show webvpn saml idp** command.

Example

The following example displays information about the SAML identity provider:

```
ciscoasa#show webvpn saml idp
```

show webvpn sso-server (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To display the operating statistics for Webvpn single sign-on servers, use the **show webvpn sso-server** command in privileged EXEC mode.

show webvpn sso-server [*name*]

Syntax Description

name Optionally specifies the name of the SSO server. The server name must be between four and 31 characters in length.

Command Default

No default values or behavior.

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
Config-webvpn-sso-saml	• Yes	—	• Yes	—	—
Config-webvpn-sso-siteminder	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.5(2)	This command was deprecated, due to support for SAML 2.0.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The **show webvpn sso-server** command displays operating statistics for any and all SSO servers configured on the security device.

If no SSO server name argument is entered, statistics for all SSO servers display.

Examples

The following example, entered in privileged EXEC mode, displays statistics for a SiteMinder-type SSO server named example:

```
ciscoasa# show webvpn sso-server example
Name: example
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL: http://www.example.com/webvpn
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
ciscoasa#
The following example of the command issued without a specific SSO server name, displays
statistics for all configured SSO servers on the ASA:
ciscoasa#(config-webvpn)# show webvpn sso-server
Name: high-security-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
Name: my-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
Name: server
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the ASA retries a failed SSO authentication attempt.
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder-type SSO server.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.

Command	Description
sso-server	Creates a single sign-on server.
web-agent-url	Specifies the SSO server URL to which the ASA makes SiteMinder SSO authentication requests.

show webvpn statistics

To view the WebVPN event statistics, use the **show webvpn statistics** command from privileged EXEC mode.

show webvpn statistics

Syntax Description

This command has no arguments or keywords.

Command Default

This command has 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
9.14	The command was added.

Usage Guidelines

WebVPN must be running when you enter the **show webvpn statistics** command.

Example

The following example displays information about the WebVPN event statistics:

```
ciscoasa#show webvpn statistics
Total number of objects served          0
html                            0
js                              0
css                             0
vb                              0
java archive                    0
java class                      0
image                           0
undetermined                    0
Server compression statistics
Decompression success from server                 0
Unsolicited compression from server               0
Unsupported compression algorithm used by server  0
Decompression failure for server responses        0
IOBuf failure statistics
uib_create_with_channel                           0
uib_create_with_string                            0
uib_create_with_string_and_channel                0
uib_transfer                                      0
uib_add_filter                                    0
```

```
uib_yyread                                      0
uib_read                                        0
uib_set_buffer_max                              0
uib_set_eof_symbol                              0
        uib_get_capture_handle                          0
        uib_set_capture_handle                          0
        uib_buflen                                      0
        uib_bufptr                                      0
        uib_buf_endptr                                  0
        uib_get_buf_offset                              0
        uib_get_buf_offset_addr                         0
        uib_get_nth_char                                0
        uib_consume                                     0
        uib_advance_bufptr                              0
```

show xlate

To display information about NAT sessions (xlates), use the **show xlate** command in privileged EXEC mode.

show xlate [**global** *ip1* [*-ip2*] [**netmask** *mask*]] [**local** *ip1* [*-ip2*] [**netmask** *mask*]] [**gport** *port1* [*-port2*]] [**lport** *port1* [*-port2*]] [**interface** *if_name*] [**type** *type*]

show xlate type deterministic external | **subscriber** *ip address* [*port*]

Syntax Description

count	Displays the translation count.
global *ip1*[**-***ip2*]	(Optional) Displays the active translations by mapped IP address or range of addresses.
gport *port1*[*-port2*]	Displays the active translations by the mapped port or range of ports.
interface *if_name*	(Optional) Displays the active translations by interface.
local*ip1*[**-***ip2*]	(Optional) Displays the active translations by real IP address or range of addresses.
lport *port1*[*-port2*]	Displays the active translations by real port or range of ports.
netmask *mask*	(Optional) Specifies the network mask to qualify the mapped or real IP addresses.
type *type*	(Optional) Displays the active translations by type. You can enter one or more of the following types: • **static** • **portmap** • **dynamic** • **twice-nat** • **deterministic** When specifying more than one type, separate the types with a space.
deterministic	Displays active translations for deterministic Carrier-Grade NAT entries. Deterministic entries are explicitly marked with the **deterministic** xlate type for easier troubleshooting and filtering.
external*ip address* [*port*]	(Optional) Displays deterministic Carrier-Grade NAT mappings for the specified public IPv4 address. If you also specify a port, the ASA retrieves the subscriber mapping for that public IPv4 address and port.
subscriber*ip address*	(Optional) Displays deterministic Carrier-Grade NAT mappings for the specified subscriber private IPv4 address.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.3(1)	This command was modified to support the new NAT implementation.
8.4(3)	The **e** flag was added to show use of extended PAT. In addition, the destination address to which the xlate is extended is shown.
9.0(1)	This command was modified to support IPv6.
9.24.10	The **deterministic** xlate type and the **external** and **subscriber** display forms were added for deterministic Carrier-Grade NAT mappings.

Usage Guidelines

The **show xlate** command displays the contents of the network address translation slots.

When the **vpnclient** configuration is enabled and the inside host is sending out DNS requests, the **show xlate** command may list multiple xlates for a static translation.

In an ASA clustering environment, up to three xlates may be duplicated to different nodes in the cluster to handle a PAT session. One xlate is created on the unit that owns the connection. One xlate is created on a different unit to backup the PAT address. Finally, one xlate exists on the director that replicates the flow. In the case where the backup and director is the same unit, two instead of three xlates may be created.

If you create twice NAT rules without specifying a destination translation, the system interprets it as a static translation for any address. Thus, the NAT table includes a translation for 0.0.0.0/0 to 0.0.0.0/0. This rule is implied from your twice NAT rule.

Usage Guidelines

When deterministic Carrier-Grade NAT is configured, the ASA marks the translation entry with the type **deterministic**. You can use the deterministic type to display deterministic translations separately from static, dynamic, portmap, and twice-NAT entries. Use these forms to retrieve mappings:

- `show xlate type deterministic` — displays all deterministic translations
- `show xlate type deterministic external <public_ip>` — displays mappings for a public IPv4 address
- `show xlate type deterministic external <public_ip> <port>` — identifies the subscriber mapping for a public IPv4 address and port
- `show xlate type deterministic subscriber <subscriber_ip>` — displays the public IPv4 address and port block for a subscriber

Usage Guidelines

If the idle time seems excessively long, use **show conn** to see if there is a connection that is up and keeping the xlate open (based on initiator and responder). If there is a connection that is up, the idle time is not abnormal and should represent the total lifetime of the connection. However, if there is not a related "up" connection, the xlate is stale and can be cleared using the **clear xlate** command.

Examples

The following is sample output from the **show xlate** command.

```
ciscoasa# show xlate
5 in use, 5 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
       e - extended
NAT from any:10.90.67.2 to any:10.9.1.0/24
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.1.1.0/24 to any:172.16.1.0/24
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.90.67.2 to any:10.86.94.0
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.9.0.9, 10.9.0.10/31, 10.9.0.12/30,
    10.9.0.16/28, 10.9.0.32/29, 10.9.0.40/30,
    10.9.0.44/31 to any:0.0.0.0
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.1.1.0/24 to any:172.16.1.0/24
    flags idle 277:05:14 timeout 0:00:00
```

The following is sample output from the **show xlate** command showing use of the **e - extended** flag and the destination address to which the xlate is extended.

```
ciscoasa# show xlate
1 in use, 1 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
       e - extended
ICMP PAT from inside:10.2.1.100/6000 to outside:172.16.2.200/6000(172.16.2.99)
 flags idle 0:00:06 timeout 0:00:30
TCP PAT from inside:10.2.1.99/5 to outside:172.16.2.200/5(172.16.2.90)
 flags idle 0:00:03 timeout 0:00:30
UDP PAT from inside:10.2.1.101/1025 to outside:172.16.2.200/1025(172.16.2.100)
 flags idle 0:00:10 timeout 0:00:30
```

The following is sample output from the **show xlate** command showing a translation from IPv4 to IPv6.

```
ciscoasa# show xlate
1 in use, 2 most used
NAT from outside:0.0.0.0/0 to in:2001::/96
flags sT idle 0:16:16 timeout 0:00:00
```

This example shows how to retrieve mappings by external IPv4 address. This command displays deterministic mappings associated with public IPv4 address **198.51.100.0**.

```
ciscoasa# show xlate type deterministic external 198.51.100.0
```

Related Commands

Command	Description
clear xlate	Clears current translation and connection information.
show conn	Displays all active connections.

Command	Description
show local-host	Displays the local host network information.
show uauth	Displays the currently authenticated users.

show zone

To shows zone ID, context, security level, and members, use the **show zone** command in privileged EXEC mode.

show zone [*name*]

Syntax Description

name	(Optional) Identifies the zone name set by the **zone** command.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

To view the zone configuration, use the **show running-config zone** command.

Examples

See the following output for the **show zone** command:

```
ciscoasa# show zone outside-zone
Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
 Zone Member(s) : 2
  outside1       GigabitEthernet0/0
  outside2       GigabitEthernet0/1
```

Related Commands

Command	Description
clear configure zone	Clears the zone configuration.
clear conn zone	Clears zone connections.
clear local-host zone	Clears zone hosts.
show asp table routing	Shows the accelerated security path tables for debugging purposes, and shows the zone associated with each route.

Command	Description
show asp table zone	Shows the accelerated security path tables for debugging purposes.
show conn long	Shows connections information for zones.
show local-host zone	Shows the network states of local hosts within a zone.
show nameif zone	Shows the interface names and zone names.
show route zone	Shows the routes for zone interfaces.
show running-config zone	Shows the zone configuration.
show zone	Shows zone ID, context, security level, and members.
zone	Configures a traffic zone.
zone-member	Assigns an interface to a traffic zone.