

show s

- show saml metadata, on page 2
- show scansafe server, on page 3
- show scansafe statistics, on page 5
- show sctp, on page 7
- show service-policy, on page 9
- show shared license, on page 17
- show shun, on page 21
- show sip, on page 22
- show skinny, on page 24
- show sla monitor configuration, on page 26
- show sla monitor operational-state, on page 28
- show snmp-server engineid, on page 30
- show snmp-server group, on page 31
- show snmp-server host, on page 33
- show snmp-server statistics, on page 35
- show snmp-server user, on page 37
- show software authenticity development, on page 39
- show software authenticity file, on page 41
- show software authenticity keys, on page 43
- show software authenticity running, on page 45
- show ssd, on page 47
- show ssh sessions, on page 48
- show ssl, on page 50
- show startup-config, on page 56
- show sunrpc-server active, on page 58
- show switch mac-address-table, on page 59
- show switch vlan, on page 61
- show sw-reset-button, on page 63

show saml metadata

Show the SAML metadata tunnel-group-name.

show saml metadata tunnel-group-name

Syntax Description

Enter the name of the tunnel group to display SAML metadata for.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

Show SAML SP's metadata for a particular tunnel group.

Examples

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

```
ciscoasa# show saml metadata saml_sso_tunnel_group
```

Related Commands

Command	Description
saml idp	Creates an inspection class map for whitelisted users and groups.

show scansafe server

To show the status of the Cloud Web Security proxy servers, use the **show scansafe server** command in privileged EXEC mode.

show scansafe server

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command shows the status of the server, whether it is the current active server, the backup server, or unreachable.

In multiple context mode, the output of this command depends on the admin-contexts ability to reach the Scansafe servers. The admin context makes regular poll attempts to verify whether the Scansafe server is up when no traffic is going through the ASA. The polling attempt interval is unconfigurable and is fixed at 15 minutes. The admin-context also sends keepalives to the Scansafe tower.

Examples

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

```
ciscoasa# show scansafe server
ciscoasa# Primary: proxy197.scansafe.net (72.37.244.115) (REACHABLE)*
ciscoasa# Backup: proxy137.scansafe.net (80.254.152.99)
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.

Command	Description
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe statistics	Shows total and current http connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

show scansafe statistics

To show information about Cloud Web Security activity, use the **show scansafe statistics** command in privileged EXEC mode.

show scansafe 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
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **show scansafe statistics** command shows information about Cloud Web Security activity, such as the number of connections redirected to the proxy server, the number of current connections being redirected, and the number of whitelisted connections.

Examples

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

```
ciscoasa# show scansafe statistics
Current HTTP sessions : 0
Current HTTPS sessions : 0
Total HTTP Sessions : 0
Total HTTPS Sessions : 0
Total Fail HTTP sessions : 0
Total Fail HTTPS sessions : 0
Total Bytes In : 0 Bytes
Total Bytes Out : 0 Bytes
HTTP session Connect Latency in ms(min/max/avg) : 0/0/0
HTTPS session Connect Latency in ms(min/max/avg) : 0/0/0
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.

Command	Description
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it's the current active server, the backup server, or unreachable.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

show sctp

To display current Stream Control Transmission Protocol (SCTP) cookies and associations, use the **show sctp** command in privileged EXEC mode.

show sctp [**detail**]

Syntax Description

detail	Displays detailed information about SCTP associations.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.5(2)	This command was added.
9.7(1)	Detailed output now includes information about multi-homing, multiple streams, and frame reassembly.

Usage Guidelines

The **show sctp** command displays information about SCTP cookies and associations.

Examples

The following is sample output from the **show sctp** command:

```
ciscoasa# show sctp

AssocID: 2279da7a
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40174 (ESTABLISHED)
AssocID: 4924f520
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40200 (ESTABLISHED)
```

The following is sample output from the **show sctp detail** command:

```
ciscoasa(config)# show sctp detail


AssocID: 8b7e3ffb
Local:  192.168.100.56/3868 (ESTABLISHED)
    Receiver Window: 48000
    Cumulative TSN: 5cb6cd9b
```

```
    Next TSN: 5cb6cd9c
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
Remote: 192.168.200.78/3868 (ESTABLISHED)
    Receiver Window: 114688
    Cumulative TSN: 5cb6cd98
    Next TSN: 0
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
```

Starting with 9.7(1), detailed output includes information about multi-homing, multiple streams, and frame reassembly.

```
asa2005# show sctp detail

AssocID: 2e590263
Local:  10.0.103.250/50000 (ESTABLISHED)
    Multi-homing IP's: 10.0.103.251(10.0.103.251)
    Receiver Window: 106496
    Cumulative TSN: bf0a3180
    Next TSN: 0
    Earliest Outstanding TSN: 0
    Re-ordering queue:
    Stream ID 3: next SN 10, first/last queued SN 11/16, hole SN:
    Stream ID 4: next SN 10, first/last queued SN 11/16, hole SN:
Remote: 10.0.102.250/3868 (CLOSED)
    Multi-homing IP's: 10.0.102.251(10.0.102.251)
    Receiver Window: 106496
    Cumulative TSN: 915d5916
    Next TSN: 0
    Earliest Outstanding TSN: 0
    Re-ordering queue:
Secondary Conn List:
    10.0.102.251(10.0.102.251):3868 to 10.0.103.251(10.0.103.251):50000
    10.0.103.251(10.0.103.251):50000 to 10.0.102.251(10.0.102.251):3868
    10.0.102.250(10.0.102.250):3868 to 10.0.103.251(10.0.103.251):50000
    10.0.103.251(10.0.103.251):50000 to 10.0.102.250(10.0.102.250):3868
    10.0.102.251(10.0.102.251):3868 to 10.0.103.250(10.0.103.250):50000
    10.0.103.250(10.0.103.250):50000 to 10.0.102.251(10.0.102.251):3868
```

Related Commands

Command	Description
show local-host	Shows information on hosts making connections through the ASA, per interface.
show service-policy inspect sctp	Shows SCTP inspection statistics.
show traffic	Shows connection and inspection statistics per interface

show service-policy

To display the service policy statistics, use the **show service-policy** command in privileged EXEC mode.

show service-policy [**global | interface** *intf*] [**csc | cxsc | inspect** *inspection* [*arguments*]] **| ips | police | priority | set connection** [**details**] **| sfr | shape | user-statistics**]
show service-policy [**global | interface** *intf*] [**flow** *protocol* { **host** *src_host* | *src_ip src_mask* } [**eq** *src_port*] { **host** *dest_host* | *dest_ip dest_mask* } [**eq** *dest_port*] [*icmp_number* | *icmp_control_message*]]

Syntax Description

csc	(Optional) Shows detailed information about policies that include the **csc** command.
cxsc	(Optional) Shows detailed information about policies that include the **cxsc** command.
dest_ip dest_mask	For the **flow** keyword, the destination IP address and netmask of the traffic flow.
details	(Optional) For the **set connection** keyword, displays per-client connection information, if a per-client connection limit is enabled.
eq *dest_port*	(Optional) For the **flow** keyword, equals the destination port for the flow.
eq *src_port*	(Optional) For the **flow** keyword, equals the source port for the flow.
flow *protocol*	(Optional) Shows policies that match a particular flow identified by the 5-tuple (protocol, source IP address, source port, destination IP address, destination port). You can use this command to check that your service policy configuration will provide the services you want for specific connections. Because the flow is described as a 5-tuple, not all policies are supported. See the following supported policy matches: • **match access-list** • **match port** • **match rtp** • **match default-inspection-traffic**
global	(Optional) Limits output to the global policy.
host *dest_host*	For the **flow** keyword, the host destination IP address of the traffic flow.
host *src_host*	For the **flow** keyword, the host source IP address of the traffic flow.
icmp_control_message	(Optional) For the **flow** keyword when you specify ICMP as the protocol, specifies an ICMP control message of the traffic flow.
icmp_number	(Optional) For the **flow** keyword when you specify ICMP as the protocol, specifies the ICMP protocol number of the traffic flow.

inspect *inspection* [*arguments*]	(Optional) Shows detailed information about policies that include an **inspect** command. Not all **inspect** commands are supported for detailed output. To see all inspections, use the **show service-policy** command without any arguments. The arguments available for each inspection vary; see the CLI help for more information.
interface *intf*	(Optional) Displays policies applied to the interface specified by the *intf* argument, where *intf* is the interface name given by the **nameif** command.
ips	(Optional) Shows detailed information about policies that include the **ips** command.
police	(Optional) Shows detailed information about policies that include the **police** command.
priority	(Optional) Shows detailed information about policies that include the **priority** command.
set connection	(Optional) Shows detailed information about policies that include the **set connection** command.
sfr	(Optional) Shows detailed information about policies that include the **sfr** command.
shape	(Optional) Shows detailed information about policies that include the **shape** command.
src_ip src_mask	For the **flow** keyword, the source IP address and netmask used in the traffic flow.
user-statistics	(Optional) Shows detailed information about policies that include the **user-statistics** command. This command displays user statistics for the Identify Firewall, including sent packet count, sent drop count, received packet count, and send drop count for selected users.

Command Default

If you do not specify any arguments, this command shows all global and interface policies.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	The **csc** keyword was added.

Release	Modification
7.2(4)/8.0(4)	The **shape** keyword was added.
8.4(2)	Support for the **user-statistics** keyword for the Identity Firewall was added.
8.4(4.1)	Support for the **cxsc** keyword for the ASA CX module was added.
9.2(1)	Support for the **sfr** keyword for the ASA FirePOWER module was added.
9.5(2)	The **inspect sctp** and **inspect diameter** keywords were added.
9.6(2)	The **inspect stun** and **inspect m3ua** { **drops** | **endpoint** *ip_address* } keywords were added.
9.7(1)	The **inspect m3ua session** and **inspect gtp pdpmcb teid** *teid* keywords were added. In addition, the limitation for showing rules was increased from 64 per class map to 128.
9.10(1)	The **detail** keyword was added to inspect dns. The detailed information provides more information about Cisco Umbrella.

Usage Guidelines

The number of embryonic connections displayed in the **show service-policy** command output indicates the current number of embryonic connections to an interface for traffic matching that defined by the **class-map** command. The "embryonic-conn-max" field shows the maximum embryonic limit configured for the traffic class using the Modular Policy Framework. If the current embryonic connections displayed equals or exceeds the maximum, TCP intercept is applied to new TCP connections that match the traffic type defined by the **class-map** command.

When you make service policy changes to the configuration, all *new* connections use the new service policy. Existing connections continue to use the policy that was configured at the time of the connection establishment. **show** command output will not include data about the old connections. For example, if you remove a QoS service policy from an interface, then re-add a modified version, then the **show service-policy** command only displays QoS counters associated with new connections that match the new service policy; existing connections on the old policy no longer show in the command output. To ensure that all connections use the new policy, you need to disconnect the current connections so they can reconnect using the new policy. See the **clear conn** or **clear local-host** commands.



Note For an **inspect icmp** and **inspect icmp error** policies, the packet counts only include the echo request and reply packets.

Examples

The following is sample output from the **show service-policy global** command:

```
ciscoasa# show service-policy global
Global policy:
  Service-policy: inbound_policy
    Class-map: ftp-port
      Inspect: ftp strict inbound_ftp, packet 0, drop 0, reset-drop 0
```

The following is sample output from the **show service-policy priority** command:

```
ciscoasa# show service-policy priority
Interface outside:
Global policy:
  Service-policy: sa_global_fw_policy
Interface outside:
  Service-policy: ramap
    Class-map: clientmap
      Priority:
        Interface outside: aggregate drop 0, aggregate transmit 5207048
    Class-map: udpmap
      Priority:
        Interface outside: aggregate drop 0,  aggregate transmit 5207048
    Class-map: cmap
```

The following is sample output from the **show service-policy flow** command:

```
ciscoasa# show service-policy flow udp host 209.165.200.229 host 209.165.202.158 eq 5060
Global policy:
  Service-policy: f1_global_fw_policy
    Class-map: inspection_default
      Match: default-inspection-traffic
      Action:
        Input flow:  inspect sip
Interface outside:
  Service-policy: test
    Class-map: test
      Match: access-list test
       Access rule: permit ip 209.165.200.229 255.255.255.224 209.165.202.158 255.255.255.224

      Action:
        Input flow:  ids inline
        Input flow:  set connection conn-max 10 embryonic-conn-max 20
```

The following is sample output from the **show service-policy inspect http** command. This example shows the statistics of each match command in a match-any class map.

```
ciscoasa# show service-policy inspect http
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: http http, packet 1916, drop 0, reset-drop 0
        protocol violations
          packet 0
        class http_any (match-any)
          Match: request method get, 638 packets
          Match: request method put, 10 packets
          Match: request method post, 0 packets
          Match: request method connect, 0 packets
          log, packet 648
```

For devices that have multiple CPU cores, there is a counter for lock failure. The locking mechanism is used to protect shared data structures and variables, because they can be used by multiple cores.When the core fails to acquire a lock, it tries to get the lock again. The lock fail counter increments for each failed attempt.

```
ciscoasa# show service-policy
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      ...
      Inspect: esmtp _default_esmtp_map, packet 96716502, lock fail 7, drop 25,
```

```
reset-drop 0
      Inspect: sqlnet, packet 2526511491, lock fail 21, drop 2362, reset-drop 0
```

The following is sample output from the **show service-policy inspect waas** command. This example shows the waas statistics.

```
ciscoasa# show service-policy inspect waas
Global policy:
  Service-policy: global_policy
    Class-map: WAAS
      Inspect: waas, packet 12, drop 0, reset-drop 0
  SYN with WAAS option 4
  SYN-ACK with WAAS option 4
  Confirmed WAAS connections 4
  Invalid ACKs seen on WAAS connections 0
  Data exceeding window size on WAAS connections 0
```

The following command shows the statistics for GTP inspection. The output is explained in Table 12-1.

```
firewall(config)# show service-policy inspect gtp statistics

GPRS GTP Statistics:
  version_not_support               0     msg_too_short             0
  unknown_msg                       0     unexpected_sig_msg        0
  unexpected_data_msg               0     ie_duplicated             0
  mandatory_ie_missing              0     mandatory_ie_incorrect    0
  optional_ie_incorrect             0     ie_unknown                0
  ie_out_of_order                   0     ie_unexpected             0
  total_forwarded                  67     total_dropped             1
  signalling_msg_dropped            1     data_msg_dropped          0
  signalling_msg_forwarded         67     data_msg_forwarded        0
  total created_pdp                33     total deleted_pdp         32
  total created_pdpmcb             31     total deleted_pdpmcb      30
  total dup_sig_mcbinfo             0     total dup_data_mcbinfo    0
  no_new_sgw_sig_mcbinfo            0     no_new_sgw_data_mcbinfo   0
  pdp_non_existent                  1
```

Table 1: GPRS GTP Statistics

Column Heading	Description
version_not_support	Displays packets with an unsupported GTP version field.
msg_too_short	Displays packets less than 8 bytes in length.
unknown_msg	Displays unknown type messages.
unexpected_sig_msg	Displays unexpected signaling messages.
unexpected_data_msg	Displays unexpected data messages.
mandatory_ie_missing	Displays messages missing a mandatory Information Element (IE).
mandatory_ie_incorrect	Displays messages with an incorrectly formatted mandatory Information Element (IE).
optional_ie_incorrect	Displays messages with an invalid optional Information Element (IE).

Column Heading	Description
ie_unknown	Displays messages with an unknown Information Element (IE).
ie_out_of_order	Displays messages with out-of-sequence Information Elements (IEs).
ie_unexpected	Displays messages with an unexpected Information Element (IE).
ie_duplicated	Displays messages with a duplicated Information Element (IE).
optional_ie_incorrect	Displays messages with an incorrectly formatted optional Information Element (IE).
total_dropped	Displays the total messages dropped.
signalling_msg_dropped	Displays the signaling messages dropped.
data_msg_dropped	Displays the data messages dropped.
total_forwarded	Displays the total messages forwarded.
signalling_msg_forwarded	Displays the signaling messages forwarded.
data_msg_forwarded	Displays the data messages forwarded.
total created_pdp	Displays the total Packet Data Protocol (PDP) or bearer contexts created.
total deleted_pdp	Displays the total Packet Data Protocol (PDP) or bearer contexts deleted.
total created_pdpmcb total deleted_pdpmcb total dup_sig_mcbinfo total dup_data_mcbinfo no_new_sgw_sig_mcbinfo no_new_sgw_data_mcbinfo	These fields relate to the use of PDP master control blocks, which is an implementation feature. These counters are used by Cisco Technical Support for troubleshooting and are not of direct interest to end users.
pdp_non_existent	Displays the messages received for a non-existent PDP context.

The following command displays information about the PDP contexts:

```
ciscoasa# show service-policy inspect gtp pdp-context
1 in use, 32 most used
Version TID                 MS Addr        SGSN Addr    Idle     Timeout   APN
v2      2692026893437055 10.0.0.1       10.0.0.11      0:00:11  0:04:00  gprs.example.com
```

Starting with ASA 9.6.2, GTP PDP context information is shown one per line instead of in a table. This makes it easier to read when using IPv6 addresses.

```
ciscoasa# show service-policy inspect gtp pdp-context
4 in use, 5 most used
Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:52:01,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517056,  MS Addr 100.100.100.102,
SGW Addr 10.0.203.24,      Idle 0:00:05,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517057,  MS Addr 100.100.100.103,
SGW Addr 10.0.203.25,      Idle 0:00:04,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517055,  MS Addr 100.100.100.101,
SGW Addr 10.0.203.23,      Idle 0:00:06,   Timeout 3:00:00,   APN ssenoauth146
```

Table 12-2 describes the output from the **show service-policy inspect gtp pdp-context** command.

Table 2: PDP Contexts

Column Heading	Description
Version	Displays the version of GTP.
TID	Displays the tunnel identifier.
MS Addr	Displays the mobile station address.
SGSN Addr SGW Addr	Displays the serving gateway service node (SGSN) or serving gateway (SGW).
Idle	Displays the time for which the PDP or bearer context has not been in use.
APN	Displays the access point name.

If you are using Application Visibilty and Control, and you are using AVC-based network-service groups in an ACL used for service policy traffic matching, the output includes AVC application statistics. The following example shows policing output that includes AVC application statistics.

```
ciscoasa# show service-policy police

Interface inside:
  Service-policy: throttle_map
    Class-map: app_throttled
      match access-list app_throttled
        network service object group/category _mobile_application_
          WeChat (hitcnt=4) WhatsApp (hitcnt=2)
      Input police Interface inside:
        cir 8000 bps, bc 1500 bytes
        conformed 59 packets, 5781 bytes; actions:  transmit
        exceeded 150 packets, 14700 bytes; actions:  drop
        conformed 0 bps, exceed 16 bps
    Class-map: custom_app_throttled
      match access-list custom_app_throttled
        network service object group/category custom_app_throttled
          Twitter/X (hitcnt=2)
      Input police Interface inside:
        cir 16000 bps, bc 1500 bytes
        conformed 70 packets, 6860 bytes; actions:  transmit
        exceeded 29 packets, 2842 bytes; actions:  drop
        conformed 8 bps, exceed 0 bps
```

Related Commands

Command	Description
clear configure service-policy	Clears service policy configurations.
clear service-policy	Clears all service policy configurations.
service-policy	Configures the service policy.
show running-config service-policy	Displays the service policies configured in the running configuration.

show shared license

To show shared license statistics, use the **show shared license** command in privileged EXEC mode. Optional keywords are available only for the licensing server.

show shared license [**detail | client** [*hostname*] | **backup**]

Syntax Description

backup	(Optional) Shows information about the backup server.
client	(Optional) Limits the display to participants.
detail	(Optional) Shows all statistics, including per participant.
hostname	(Optional) Limits the display to a particular participant.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

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

Usage Guidelines

To clear the statistics, enter the **clear shared license** command.

Examples

The following is sample output from the **show shared license** command on the license participant:

```
ciscoasa# show shared license
Primary License Server : 10.3.32.20
  Version              : 1
  Status               : Inactive
Shared license utilization:
  SSLVPN:
    Total for network :     5000
    Available         :     5000
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
```

```
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
Client ID           Usage   Hostname
  ASA0926K04D         0       5510-B
```

Table 12-3 describes the output from the **show shared license** command.

Table 3: show shared license Description

Field	Description
Primary License Server	The IP address of the primary server.
Version	The shared license version.
Status	If the command is issued on the backup server, “Active” means that this device has taken on the role as a Primary Shared Licensing server. “Inactive” means that the device is ready in standby mode, and the device is communicating with the primary server. If failover is configured on the primary licensing server, the backup server may become “Active” for a brief moment during a failover but should return to “Inactive” after communications have synced up again.
Shared license utilization	
SSLVPN	
Total for network	Displays the total number of shared sessions available.
Available	Displays the remaining shared sessions available.
Utilized	Displays the shared sessions obtained for the active license server.
This device	
Platform limit	Displays the total number of SSL VPN sessions for this device according to the installed license.
Current usage	Displays the number of shared SSL VPN session currently owned by this device from the shared pool.
High usage	Displays the highest number of shared SSL VPN sessions ever owned by this device.
Messages Tx/Rx/Error	
RegistrationGetReleaseTransfer	Shows the Transmit, Received, and Error packets of each type of connection.
Client ID	A unique client ID.
Usage	Displays the number of sessions in use.
Hostname	Displays the hostname for this device.

Examples

The following is sample output from the **show shared license detail** command on the license server:

```
ciscoasa# show shared license detail
Backup License Server Info:
Device ID           : ABCD
Address             : 10.1.1.2
Registered          : NO
HA peer ID          : EFGH
Registered          : NO
  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0
Shared license utilization:
  SSLVPN:
    Total for network :      500
    Available         :      500
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
Client Info:
  Hostname          : 5540-A
  Device ID         : XXXXXXXXXXX
  SSLVPN:
    Current usage   : 0
    High            : 0
  Messages Tx/Rx/Error:
    Registration    : 1 / 1 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
...
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.

Command	Description
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show vpn-sessiondb	Shows license information about VPN sessions.

show shun

To display shun information, use the **show shun** command in privileged EXEC mode.

show shun [*src_ip* | **statistics**]

Syntax Description

src_ip	(Optional) Displays the information for that address.
statistics	(Optional) Displays the interface counters only.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
8.2(2)	For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.

Examples

The following is sample output from the **show shun** command:

```
ciscoasa# show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

Related Commands

Command	Description
clear shun	Disables all the shuns that are currently enabled and clears the shun statistics.
shun	Enables a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection.

show sip

To display SIP sessions, use the show **sip** command in privileged EXEC mode.

show sip

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 sip** command displays information for SIP sessions established across the ASA.

Note We recommend that you configure the **pager** command before using the **show sip** command. If there are a lot of SIP session records and the **pager** command is not configured, it will take a while for the **show sip** command output to reach its end.

Examples

The following is sample output from the **show sip** command:

```
ciscoasa# show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
 | state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
 | state Active, idle 0:00:06
```

This sample shows two active SIP sessions on the ASA (as shown in the Total field). Each call-id represents a call.

The first session, with the call-id c3943000-960ca-2e43-228f@10.130.56.44, is in the state Call Init , which means the session is still in call setup. Call setup is complete only when the ACK is seen. This session has been idle for 1 second.

The second session is in the state Active , in which call setup is complete and the endpoints are exchanging media. This session has been idle for 6 seconds.

Related Commands

Commands	Description
inspect sip	Enables SIP application inspection.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

show skinny

To troubleshoot SCCP (Skinny) inspection engine issues, use the show skinny command in privileged EXEC mode.

show skinny

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show skinny** command displays information for SCCP (Skinny) sessions.

Examples

The following is sample output from the **show skinny** command under the following conditions. There are two active Skinny sessions set up across the ASA. The first one is established between an internal Cisco IP Phone at local address 10.0.0.11 and an external Cisco CallManager at 172.18.1.33. TCP port 2000 is the CallManager. The second one is established between another internal Cisco IP Phone at local address 10.0.0.22 and the same Cisco CallManager.

```
ciscoasa# show skinny
MEDIA 10.0.0.22/20798         172.18.1.11/22948
LOCAL                  FOREIGN                 STATE
-----------------------------------------------------------------
1       10.0.0.11/52238         172.18.1.33/2000               1
  MEDIA 10.0.0.11/22948         172.18.1.22/20798
2       10.0.0.22/52232         172.18.1.33/2000               1
  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

The output indicates a call has been established between both internal Cisco IP Phones. The RTP listening ports of the first and second phones are UDP 22948 and 20798 respectively.

Related Commands

Commands	Description
inspect skinny	Enables SCCP application inspection.

Commands	Description
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

show sla monitor configuration

To display the configuration values, including the defaults, for SLA operations, use the **show sla monitor configuration** command in user EXEC mode.

show sla monitor configuration [*sla-id*]

Syntax Description

sla-id (Optional) The ID number of the SLA operation. Valid values are from 1 to 2147483647.

Command Default

If the *sla-id* is not specified, the configuration values for all SLA operations are shown.

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	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Use the **show running config sla monitor** command to see the SLA operation commands in the running configuration.

Examples

The following is sample output from the **show sla monitor** command. It displays the configuration values for SLA operation 123. Following the output of the **show sla monitor** command is the output of the **show running-config sla monitor** command for the same SLA operation.

```
ciscoasa> show sla monitor 124
SA Agent, Infrastructure Engine-II
Entry number: 124
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.1.1.1
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
```

```
Status of entry (SNMP RowStatus): Active
Enhanced History:
ciscoasa# show running-config sla monitor 124
sla monitor 124
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

Related Commands

Command	Description
show running-config sla monitor	Displays the SLA operation configuration commands in the running configuration.
sla monitor	Defines an SLA monitoring operation.

show sla monitor operational-state

To display the operational state of SLA operations, use the **show sla monitor operational-state** command in user EXEC mode.

show sla monitor operational-state [*sla-id*]

Syntax Description

sla-id (Optional) The ID number of the SLA operation. Valid values are from 1 to 2147483647.

Command Default

If the *sla-id* is not specified, statistics for all SLA operations are displayed.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Use the **show running-config sla monitor** command to display the SLA operation commands in the running configuration.

Examples

The following is sample output from the **show sla monitor operational-state** command:

```
ciscoasa> show sla monitor operationl-state
Entry number: 124
Modification time: 14:42:23.607 EST Wed Mar 22 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 4043
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 18:04:26.609 EST Wed Mar 22 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

Related Commands

Command	Description
show running-config sla monitor	Displays the SLA operation configuration commands in the running configuration.
sla monitor	Defines an SLA monitoring operation.

show snmp-server engineid

To display the identification of the SNMP engine that has been configured on the ASA, use the **show snmp-server engineid** command in privileged EXEC mode.

show snmp-server engineid

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was added.

Examples

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

```
ciscoasa
#
show snmp-server engineid
Local SNMP engineID: 80000009fe85f8fd882920834a3af7e4ca79a0a1220fe10685
```

Usage Guidelines

An SNMP engine is a copy of SNMP that can reside on a local device. The engine ID is a unique value that is assigned for each SNMP agent for each ASA context. The engine ID is not configurable on the ASA. The engine ID is 25 bytes long, and is used to generate encrypted passwords. The encrypted passwords are then stored in flash memory. The engine ID can be cached. In a failover pair, the engine ID is synchronized with the peer.

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP server configuration.
show running-config snmp-server	Displays the SNMP server configuration.
snmp-server	Configures the SNMP server.

show snmp-server group

To display the names of configured SNMP groups, the security model being used, the status of different views, and the storage type of each group, use the **show snmp-server group** command in privileged EXEC mode.

show snmp-server 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
8.2(1)	This command was added.

Examples

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

```
ciscoasa
#
show snmp-server group
groupname: public                              security model:v1
readview : <no readview specified>             writeview: <no writeview specified>
notifyview: <no readview specified>
row status: active
groupname: public                              security model:v2c
readview : <no readview specified>             writeview: <no writeview specified>
notifyview: *<no readview specified>
row status: active
groupname: privgroup                       security model:v3 priv
readview : def_read_view                   writeview: <no writeview specified>
notifyview: def_notify_view
row status: active
```

Usage Guidelines

SNMP users and groups are used according to the View-based Access Control Model (VACM) for SNMP. The SNMP group determines the security model to be used. The SNMP user should match the security model of the SNMP group. Each SNMP group name and security level pair must be unique.

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP server configuration.

Command	Description
show running-config snmp-server	Displays the SNMP server configuration.
snmp-server	Configures the SNMP server.

show snmp-server host

To display the names of configured SNMP hosts that belong to a host group, the interface being used, and the version of SNMP being used, use the **show snmp-server host** command in privileged EXEC mode.

show snmp-server host

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was added.
9.4(1)	The output was updated to show only active hosts that are polling the ASA, as well as the statically configured hosts.

Examples

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

```
ciscoasa
#
show snmp-server host
host ip = 10.10.10.1, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.10, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.2, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.3, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.4, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.5, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.6, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.7, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.8, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.9, interface = mgmt  poll community ***** version 2c
```

The following is sample output from the **show snmp-server host** command as of Version 9.4(1), which shows only the active hosts polling the ASA:

```
ciscoasa
#
show snmp-server host
```

```
host ip = 10.10.10.3, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.6, interface = mgmt  poll community ***** version 2c
```

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP server configuration.
show running-config snmp-server	Displays the SNMP server configuration.
snmp-server	Configures the SNMP server.

show snmp-server statistics

To display SNMP server statistics, use the **show snmp-server statistics** command in privileged EXEC mode.

show snmp-server statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

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

```
ciscoasa# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP server configuration.
clear snmp-server statistics	Clears the SNMP packet input and output counters.

Command	Description
show running-config snmp-server	Displays the SNMP server configuration.
snmp-server	Configures the SNMP server.

show snmp-server user

To display information about the configured characteristics of SNMP users, use the **show snmp-server user** command in privileged EXEC mode.

show snmp-server user [*username*]

Syntax Description

username (Optional) Identifies a specific user or users about which to display SNMP 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
8.2(1)	This command was added.

Examples

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

```
ciscoasa
#
show snmp-server user authuser
User name: authuser
Engine ID: 000000090200000000C025808
storage-type: nonvolatile       active access-list: N/A
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: DES
Group name: VacmGroupName
```

The output provides the following information:

- The username, which is a string that identifies the name of the SNMP user.
- The engine ID, which is a string that identifies the copy of SNMP on the ASA.
- The storage-type, which indicates whether or not the settings have been set in volatile or temporary memory on the ASA, or in nonvolatile or persistent memory, in which settings remain after the ASA has been turned off and on again.
- The active access list, which is the standard IP access list associated with the SNMP user.
- The Rowstatus, which indicates whether or not it is active or inactive.

- The authentication protocol, which identifies which authentication protocol is being used. Options are MD5, SHA, or none. If authentication is not supported in your software image, this field does not appear.
- The privacy protocol, which indicates whether or not DES packet encryption is enabled. If privacy is not supported in your software image, this field does not appear.
- The group name, which indicates to which SNMP group the user belongs. SNMP groups are defined according to the View-based Access Control Model (VACM).

Usage Guidelines

An SNMP user must be part of an SNMP group. If you do not enter the *username* argument, the **show snmp-server user** command displays information about all configured users. If you enter the *username* argument and the user exists, the information about that user appears.

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP server configuration.
show running-config snmp-server	Displays the SNMP server configuration.
snmp-server	Configures the SNMP server.

show software authenticity development

To verify that the loading of development key signed images is enabled or disabled, use the **show software authenticity development** command in privileged EXEC mode.

show software authenticity development

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.3(2)	This command was added.

Examples

The following is sample output from the **show software authenticity file** command:

```
ciscoasa(config)# show software authenticity development
Loading of development images is disabled
ciscoasa(config)#
```

Related Commands

Command	Description
show version	Displays the software version, hardware configuration, license key, and related uptime data.
software authenticity key add special	Adds a new development key to SPI flash.
software authenticity key revoke special	Deletes older development keys from SPI flash.
show software authenticity keys	Displays the development keys in SPI flash.
show software authenticity file disk0:asa932-1fbff.SSA	Displays the contents of the development keys file.
show software authenticity running	Displays the digital signature information related to the current running file.

Command	Description
show software authenticity	Displays digital signature information related to software authentication for a specific image file.

show software authenticity file

To display digital signature information related to software authentication for a specific image file, use the **show software authenticity file** command in privileged EXEC mode.

show software authenticity [*filename*]

Syntax Description

filename	(Optional) Identifies a specific image file.

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
9.3(2)	This command was added.

Examples

The following is sample output from the **show software authenticity file** command:

```
ciscoasa
#
show software authenticity file asa913.SSA
File Name                     : disk0:/asa913.SSA
Image type                    : Development
    Signer Information
        Common Name           : Cisco
        Organization Unit     : ASA5585-X
        Organization Name     : Engineering
    Certificate Serial Number : abcd1234efgh5678
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
```

The output provides the following information:

- The filename, which is the name of the filename in memory.
- The image type, which is the type of image being shown.
- The signer information specifies the signature information, which includes the following:
- The common name, which is the name of the software manufacturer.
- The organization unit, which indicates the hardware that the software image is deployed on.

- The organization name, which is the owner of the software image.
- The certificate serial number, which is the certificate serial number for the digital signature.
- The hash algorithm, which indicates the type of hash algorithm used in digital signature verification.
- The signature algorithm, which identifies the type of signature algorithm used in digital signature verification.
- The key version, which indicates the key version used for verification.

Related Commands

Command	Description
show version	Displays the software version, hardware configuration, license key, and related uptime data.

show software authenticity keys

To display information about development keys and release keys that are stored in SPI flash, use the **show software authenticity keys** command in privileged EXEC mode.

show software authenticity keys

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.3(2)	This command was added.

Examples

The following is sample output from the **show software authenticity keys** command:

```
ciscoasa# show software authenticity keys
Public Key #1 Information
-------------------------
Key Type              : Development (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
Exponent              : 65537
Key Version           : A
Public Key #2 Information
-------------------------
```

```
Key Type              : Release (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        96:A2:E6:E4:51:4D:4A:B0:F0:EF:DB:41:82:A6:AC:D0:
        FC:11:40:C2:F0:76:10:19:CE:D0:16:7D:26:73:B1:55:
        FE:42:FE:5D:5F:4D:A5:D5:29:7F:91:EC:91:4D:9B:33:
        54:4B:B8:4D:85:E9:11:2D:79:19:AA:C5:E7:2C:22:5E:
        F6:66:27:98:1C:5A:84:5E:25:E7:B9:09:80:C7:CD:F4:
        13:FB:32:6B:25:B5:22:DE:CD:DC:BE:65:D5:6A:99:02:
        95:89:78:8D:1A:39:A3:14:C9:32:EE:02:4C:AB:25:D0:
        38:AD:E4:C9:C6:6B:28:FE:93:C3:0A:FE:90:D4:22:CC:
        FF:99:62:25:57:FB:A7:C6:E4:A5:B2:22:C7:35:91:F8:
        BB:2A:19:42:85:8F:5E:2E:BF:A0:9D:57:94:DF:29:45:
        AA:31:56:6B:7C:C4:5B:54:FE:DE:30:31:B4:FC:4E:0C:
        9D:D8:16:DB:1D:3D:8A:98:6A:BB:C2:34:8B:B4:AA:D1:
        53:66:FF:89:FB:C2:13:12:7D:5B:60:16:CA:D8:17:54:
        7B:41:1D:31:EF:54:DB:49:40:1F:99:FB:18:38:03:EE:
        2D:E8:E1:9F:E6:B2:C3:1C:55:70:F4:F3:B2:E7:4A:5A:
        F5:AA:1D:03:BD:A1:C3:9F:97:80:E6:63:05:27:F2:1F
Exponent              : 65537
Key Version           : A
Public Key #3 Information
-------------------------
Key Type              : Development (Backup)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
Exponent              : 65537
Key Version           : A
```

Related Commands

Command	Description
show software authenticity file disk0:asa932-1fbff.SSA	Displays the contents of the Development Key file.
show software authenticity keys	Displays the Development Keys.
show software authenticity running	Displays the digital signature information related to the current running file.
software authenticity key add special	Adds a new Development Key to SPR flash.
software authenticity key revoke special	Deletes older Development Keys from SPR flash.

show software authenticity running

To display digital signature information related to software authentication for a specific image file, use the **show software authenticity running** command in privileged EXEC mode. This command is the same as **show software authenticity file** except that it displays the digital signature information related to the current running file.

show software authenticity running

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.3(2)	This command was added.

Examples

The following is sample output from the **show software authenticity running** command:

```
ciscoasa# show software authenticity running
Image type                    : Development
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 5448091A
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
    Verifier Information
        Verifier Name         : ROMMON
        Verifier Version      : Cisco Systems ROMMON,1.0.16
```

The output provides the following information:

- The filename, which is the name of the filename in memory.
- The image type, which is the type of image being shown.
- The signer information specifies the signature information, which includes the following:
- The common name, which is the name of the software manufacturer.

- The organization unit, which indicates the hardware that the software image is deployed on.
- The organization name, which is the owner of the software image.
- The certificate serial number, which is the certificate serial number for the digital signature.
- The hash algorithm, which indicates the type of hash algorithm used in digital signature verification.
- The signature algorithm, which identifies the type of signature algorithm used in digital signature verification.
- The key version, which indicates the key version used for verification.

Related Commands

Command	Description
show software authenticity file disk0:asa932-1fbff.SSA	Displays the contents of the Development Key file.
software authenticity key add special	Adds a new Development Key to SPR flash.
software authenticity key revoke special	Deletes older Development Keys from SPR flash.

show ssd

To view the status of the SSDs, use the **show ssd** command.

Note This command is only supported on the Secure Firewall 3100.

show ssd

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

Command History

Release	Modification
9.17(1)	This command was introduced.

Examples

The following sample display shows information about the SSDs:

```
> show ssd
Local Disk: 1
Name: nvme0n1
Size(MB): 858306
Operability:
operable
Presence:
equipped
Model: Micron_7300_MTFDHBE960TDF
Serial: MSA244302N0
Drive State: online
SED Support:
yes
SED State:
unlocked
SED Auth Status: ok
RAID action: none
```

Related Commands

Command	Description
raid	Adds or removes an SSD from the RAID.
show raid	Shows the RAID status.

show ssh sessions

To display information about the active SSH sessions on the ASA, use the **show ssh sessions** command in privileged EXEC mode.

show ssh sessions [**hostname** *or* **A.B.C.D**] [**hostname** *or* **X:X:X:X::X**] [**detail**]

Syntax Description

hostname or **A.B.C.D**	(Optional) Displays SSH session information for only the specified SSH client IPv4 address.
hostname or **X:X:X:X::X**	(Optional) Displays SSH session information for only the specified SSH client IPv6 address.
detail	Displays detailed SSH session 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
7.0(1)	This command was added.
9.1(2)	The **detail** option was added.

Usage Guidelines

The SID is a unique number that identifies the SSH session. The Client IP is the IP address of the system running an SSH client. The Version is the protocol version number that the SSH client supports. If the SSH only supports SSH version 1, then the Version column displays 1.5. If the SSH client supports both SSH version 1 and SSH version 2, then the Version column displays 1.99. If the SSH client only supports SSH version 2, then the Version column displays 2.0. The Encryption column shows the type of encryption that the SSH client is using. The State column shows the progress that the client is making as it interacts with the ASA. The Username column lists the login username that has been authenticated for the session. The Mode column describes the direction of the SSH data streams.

For SSH version 2, which can use the same or different encryption algorithms, the Mode field displays in and out. For SSH version 1, which uses the same encryption in both directions, the Mode field displays nil (‘-’) and allows only one entry per connection.

Examples

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

```
ciscoasa# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
```

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

```
ciscoasa# show ssh sessions detail
SSH Session ID             : 0
>   Client IP              : 161.44.66.200
>   Username               : root
>   SSH Version            : 2.0
>   State                  : SessionStarted
>   Inbound Statistics
>    Encryption            : aes256-cbc
>    HMAC                  : sha1
>    Bytes Received        : 2224
>   Outbound Statistics
>    Encryption            : aes256-cbc
>    HMAC                  : sha1
>    Bytes Transmitted     : 2856
>   Rekey Information
>    Time Remaining (sec)  : 3297
>    Data Remaining (bytes): 996145356
>    Last Rekey            : 16:17:19.732 EST Wed Jan 2 2013
>    Data-Based Rekeys     : 0
>    Time-Based Rekeys     : 0
```

Related Commands

Command	Description
ssh disconnect	Disconnects an active SSH session.
ssh timeout	Sets the timeout value for idle SSH sessions.

show ssl

To display information about the SSL configuration and active SSL sessions on the ASA, use the **show ssl** command in privileged EXEC mode.

show ssl [**cache | ciphers** [*level*] | **errors | information | mib | objects**]

Syntax Description

cache	(Optional) Displays SSL session cache statistics.
ciphers [*level*]	(Optional) Displays which ciphers are configured for use, based on the levels that are configured using the **ssl cipher** command. You can specify one of the following levels to see just the ciphers at that level. If you do not specify a level, the medium level for each SSL/TLS/DTLS version are shown. • **all** —Includes all ciphers. • **low** —Includes all ciphers except NULL-SHA. • **medium** —Includes all ciphers except the null, DES, and RC4 ciphers. • **fips** —Includes all FIPS-compliant ciphers. • **high** —Applies only to TLSv1.2, and includes only the strongest ciphers.
errors	(Optional) Displays SSL errors.
information	(Optional) Displays SSL supported configuration either with or without 3DES license and all ciphers that can be supported on the device.
mib	(Optional) Displays SSL MIB statistics.
objects	(Optional) Displays SSL object statistics.

Command Default

For show ssl information, the following default settings are applied with or without 3DES:

- Default setting without 3DES (or higher cipher support):

```
ssl server-version tlsv1 dtlsv1
ssl client-version tlsv1
ssl cipher default low
ssl cipher tlsv1 low
ssl cipher tlsv1.1 low
ssl cipher tlsv1.2 low
ssl cipher dtlsv1 low
ssl cipher dtlsv1.2 low
ssl dh-group group2
ssl ecdh-group group19
ssl certificate-authentication fca-timeout 2
```

- Default setting with 3DES (or higher cipher support):

```
ssl server-version tlsv1 dtlsv1
ssl client-version tlsv1 dtlsv1
ssl cipher default medium
```

```
 ssl cipher tlsv1 medium
 ssl cipher tlsv1.1 medium
 ssl cipher tlsv1.2 medium
 ssl cipher dtlsv1 medium
 ssl cipher dtlsv1.2 medium
 ssl dh-group group2
 ssl ecdh-group group19
 ssl certificate-authentication fca-timeout 2
```

The following output is for the show ssl cache command

```
SSL session cache statistics:
  Maximum cache size:          750    Current cache size:           5
  Cache hits:                    0    Cache misses:                 0
  Cache timeouts:                0    Cache full:                   0
  Accept attempts:               5    Accepts successful:           5
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:          0
  Connect renegotiates:          0
SSL VPNLB session cache statistics:
  Maximum cache size:           10    Current cache size:           0
  Cache hits:                    0    Cache misses:                 0
  Cache timeouts:                0    Cache full:                   0
  Accept attempts:               0    Accepts successful:           0
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:          0
  Connect renegotiates:          0
DTLS session cache statistics:
  Maximum cache size:          750    Current cache size:           1
  Cache hits:                    1    Cache misses:                 0
  Cache timeouts:                0    Cache full:                   0
  Accept attempts:               2    Accepts successful:           1
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:          0
  Connect renegotiates:          0
```

Command Modes

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

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

Command History

Release	Modification
9.16(1)	Output of the `show ssl cache` command has been updated to remove SSLDEV session cache statistics.
9.12(1)	The show ssl cipher all command was removed and deprecated, and the show ssl cipher information command was added.
9.3(2)	Support for TLSv1.1 and TLSv1.2 was added. The **ciphers** keyword was added.
9.1(2)	The **detail** option was added.

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

Usage Guidelines

This command shows information about the current SSLv2 and SSLv3 sessions, including the enabled cipher order, which ciphers are disabled, SSL trustpoints being used, and whether or not certificate authentication is enabled.

Examples

The following is sample output from the **show ssl** command:

```
ciscoasa# show ssl
Accept connections using SSLv2 or greater and negotiate to TLSv1.2 or greater
Start connections using SSLv3 and negotiate to SSLv3 or greater
SSL DH Group: group2
SSL trust-points:
  Self-signed RSA certificate available
  Default: certsha256
  Interface inside: certsha256
Certificate authentication is not enabled
```

The following is sample output from the **show ssl ciphers fips** command:

```
ciscoasa# show ssl ciphers fips

  ECDHE-ECDSA-AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  DHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-ECDSA-AES256-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-SHA384 (tlsv1.2)
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  DHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
```

The following is output from the **show ssl ciphers** command.

```
ciscoasa# show ssl ciphers all

These are the ciphers for the given cipher level; not all ciphers
are supported by all versions of SSL/TLS.
These names can be used to create a custom cipher list
  ECDHE-ECDSA-AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  DHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-ECDSA-AES256-SHA384 (tlsv1.2)
```

```
  ECDHE-RSA-AES256-SHA384 (tlsv1.2)
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  DHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DES-CBC3-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  RC4-SHA (tlsv1)
  RC4-MD5 (tlsv1)
  DES-CBC-SHA (tlsv1)
  NULL-SHA (tlsv1)
asa3(config-tlsp)# show ssl ciphers medium
  ECDHE-ECDSA-AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  DHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-ECDSA-AES256-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-SHA384 (tlsv1.2)
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  DHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
asa3(config-tlsp)# show ssl ciphers fips
  ECDHE-ECDSA-AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  DHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-ECDSA-AES256-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-SHA384 (tlsv1.2)
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  DHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
asa3(config-tlsp)# show ssl ciphers
Current cipher configuration:
```

```
default (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
tlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
tlsv1.1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
tlsv1.2 (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
dtlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
```

Related Commands

Command	Description
license-server port	Sets the port on which the server listens for SSL connections from participants.

Command	Description
ssl ciphers	Specifies the encryption algorithms for the SSL, DTLS, and TLS protocols.

show startup-config

To show the startup configuration or to show any errors when the startup configuration loaded, use the **show startup-config** command in privileged EXEC mode.

show startup-config [**errors**]

Syntax Description

errors	(Optional) Shows any errors that were generated when the ASA loaded the startup configuration.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System[1]
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

[1]The errors keyword is only available in single mode and the system execution space.

Command History

Release	Modification
7.0(1)	The **errors** keyword was added.
8.3(1)	Encrypted passwords were added to the output.

Usage Guidelines

In multiple context mode, the **show startup-config** command shows the startup configuration for your current execution space: the system configuration or the security context.

The **show startup-config** command output displays encrypted, masked, or clear text passwords when password encryption is either enabled or disabled.

To clear the startup errors from memory, use the **clear startup-config errors** command.

Examples

The following is sample output from the **show startup-config** command:

```
ciscoasa# show startup-config
: Saved
: Written by enable_15 at 01:44:55.598 UTC Thu Apr 17 2003
Version 7.X(X)
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 209.165.200.224
 webvpn enable
!
interface GigabitEthernet0/1
```

```
 shutdown
 nameif test
 security-level 0
 ip address 209.165.200.225
!
...
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname firewall1
domain-name example.com
boot system disk0:/cdisk.bin
ftp mode passive
names
name 10.10.4.200 outside
access-list xyz extended permit ip host 192.168.0.4 host 209.165.200.226
!
ftp-map ftp_map
!
ftp-map inbound_ftp
 deny-request-cmd appe stor stou
!
...
Cryptochecksum:4edf97923899e712ed0da8c338e07e63
```

The following is sample output from the **show startup-config errors** command:

```
ciscoasa# show startup-config errors
ERROR: 'Mac-addresses': invalid resource name
*** Output from config line 18, "limit-resource Mac-add..."
INFO: Admin context is required to get the interfaces
*** Output from config line 30, "arp timeout 14400"
Creating context 'admin'... WARNING: Invoked the stub function ibm_4gs3_context_
set_max_mgmt_sess
WARNING: Invoked the stub function ibm_4gs3_context_set_max_mgmt_sess
Done. (1)
*** Output from config line 33, "admin-context admin"
WARNING: VLAN *24* is not configured.
*** Output from config line 12, context 'admin', "nameif inside"
.....
*** Output from config line 37, "config-url disk:/admin..."
```

Related Commands

Command	Description
clear startup-config errors	Clears the startup errors from memory.
show running-config	Shows the running configuration.

show sunrpc-server active

To display the pinholes open for Sun RPC services, use the **show sunrpc-server active** command in privileged EXEC mode.

show sunrpc-server active

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **show sunrpc-server active** command to display the pinholes open for Sun RPC services, such as NFS and NIS.

Examples

To display the pinholes open for Sun RPC services, enter the **show sunrpc-server active** command. The following is sample output from the **show sunrpc-server active** command:

```
ciscoasa# show sunrpc-server active
        LOCAL           FOREIGN                 SERVICE TIMEOUT
        -----------------------------------------------
        192.168.100.2/0 209.165.200.5/32780     100005 00:10:00
```

The entry in the LOCAL column shows the IP address of the client or server on the inside interface, while the value in the FOREIGN column shows the IP address of the client or server on the outside interface.

Related Commands

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

show switch mac-address-table

To view the switch MAC address table, use the **show switch mac-address-table** command in privileged EXEC mode.

show switch mac-address-table

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
9.13(1)	Support for the Firepower 1010 was added.

Usage Guidelines

This command is for models with built-in switches only.

The switch MAC address table maintains the MAC address-to-switch port mapping for traffic within each VLAN in the switch hardware. If you are in transparent firewall mode, use the **show mac-address-table** command to view the bridge MAC address table in the ASA software. The bridge MAC address table maintains the MAC address-to-VLAN interface mapping for traffic that passes between VLANs.

MAC address entries age out in 5 minutes.

Examples

The following is sample output from the **show switch mac-address-table** command.

```
ciscoasa# show switch mac-address-table
Legend: Age - entry expiration time in seconds
   Mac Address  | VLAN |       Type       | Age | Port
-----------------------------------------------------
 000e.0c4e.2aa4 | 0001 |     dynamic      | 287 | Et0/0
 0012.d927.fb03 | 0001 |     dynamic      | 287 | Et0/0
 0013.c4ca.8a8c | 0001 |     dynamic      | 287 | Et0/0
 00b0.6486.0c14 | 0001 |     dynamic      | 287 | Et0/0
 00d0.2bff.449f | 0001 |     static       |  -  | In0/1
 0100.5e00.000d | 0001 | static multicast |  -  | In0/1,Et0/0-7
Total Entries: 6
```

The following table explains each field.

Table 4: show switch mac-address-table Fields

Field	Description
Mac Address	Shows the MAC address.
VLAN	Shows the VLAN associated with the MAC address.
Type	Shows if the MAC address was learned dynamically, as a static multicast address, or statically. The only static entry is for the internal backplane interface.
Age	Shows the age of a dynamic entry in the MAC address table.
Port	Shows the switch port through which the host with the MAC address can be reached.

Related Commands

Command	Description
show mac-address-table	Shows the MAC address table for models that do not have a built-in switch.
show switch vlan	Shows the VLAN and physical MAC address association.

show switch vlan

To view the VLANs and the associated switch ports, use the **show switch vlan** command in privileged EXEC mode.

show switch vlan

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
9.13(1)	Support for the Firepower 1010 was added.

Usage Guidelines

This command is for models with built-in switches only. For other models, use the **show vlan** command.

Examples

The following is sample output from the **show switch vlan** command.

```
ciscoasa# show switch vlan
VLAN Name                            Status    Ports
---- --------------------------------- --------- -------------
100  inside                          up        Et0/0, Et0/1
200  outside                         up        Et0/7
300  -                               down      Et0/1, Et0/2
400  backup                          down      Et0/3
```

The following table explains each field.

Table 5: show switch vlan Fields

Field	Description
VLAN	Shows the VLAN number.
Name	Shows the name of the VLAN interface. If no name is set using the **nameif** command, or if there is no **interface vlan** command, the display shows a dash (-).

Field	Description
Status	Shows the status, up or down, to receive and send traffic to and from the VLAN in the switch. At least one switch port in the VLAN needs to be in an up state for the VLAN state to be up.
Ports	Shows the switch ports assigned to each VLAN. If a switch port is listed for multiple VLANs, it is a trunk port. The above sample output shows Ethernet 0/1 is a trunk port that carries VLAN 100 and 300.

Related Commands

Command	Description
clear interface	Clears counters for the **show interface** command.
interface vlan	Creates a VLAN interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show vlan	Shows the VLANs for models that do not have built-in switches.
switchport mode	Sets the mode of the switch port to access or trunk mode.

show sw-reset-button

To show whether the ASA 5506-X, 5508-X, or 5516-X software reset button is enabled, use the **show sw-reset-button** command in privileged EXEC mode.

show sw-reset-button

Syntax Description

This command has no arguments or keywords.

Command Default

The software reset button is enabled 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
9.3(2))	Command added.

Usage Guidelines

Enable or disable the software reset button using the **service sw-reset-button** command. The reset button is a small recessed button on the rear panel that if pressed for longer than three seconds resets the ASA to its default "as-shipped" state following the next reboot. Configuration variables are reset to factory default. However, the flash is not erased, and no files are removed.

Examples

The following example enables the software reset button:

```
ciscoasa(config)# service sw-reset-button
ciscoasa(config)# show sw-reset-button
Software Reset Button is configured.
```

The following example disables the software reset button:

```
ciscoasa(config)# no service sw-reset-button
ciscoasa(config)# show sw-reset-button
Software Reset Button is not configured.
```

Related Commands

Command	Description
service sw-reset-button	Enables or disables the software reset button.