



show cr – show cz

- [show crashinfo](#), on page 3
- [show crashinfo console](#), on page 12
- [show crashinfo files](#), on page 13
- [show crypto accelerator load-balance](#), on page 15
- [show crypto accelerator statistics](#), on page 16
- [show crypto ca certificates](#), on page 25
- [show crypto ca srl](#), on page 27
- [show crypto ca server](#), on page 29
- [show crypto ca server cert-db](#), on page 31
- [show crypto ca server certificate](#), on page 34
- [show crypto ca server srl](#), on page 36
- [show crypto ca server user-db](#), on page 38
- [show crypto ca trustpool](#), on page 40
- [show crypto ca trustpool policy](#), on page 42
- [show crypto debug-condition](#), on page 44
- [show crypto ikev1 sa](#), on page 45
- [show crypto ikev2 sa](#), on page 47
- [show crypto ikev2 stats](#), on page 49
- [show crypto ipsec df-bit](#), on page 51
- [show crypto ipsec fragmentation](#), on page 53
- [show crypto ipsec policy](#), on page 55
- [show crypto ipsec sa](#), on page 57
- [show crypto ipsec stats](#), on page 66
- [show crypto isakmp sa](#), on page 69
- [show crypto isakmp stats](#), on page 71
- [show crypto key mypubkey](#), on page 74
- [show crypto protocol statistics](#), on page 75
- [show crypto sockets](#), on page 79
- [show csc node-count](#), on page 81
- [show ctiqbe](#), on page 83
- [show ctl-file](#), on page 85
- [show ctl-provider](#), on page 88
- [show cts environment-data](#), on page 89

- [show cts environment-data sg-table](#), on page 91
- [show cts pac](#), on page 93
- [show cts sgt-map](#), on page 95
- [show cts sxp connections](#), on page 98
- [show cts sxp sgt-map](#), on page 101
- [show curpriv](#), on page 104

show crashinfo

To display the contents of the latest crash information file stored in Flash memory, enter the **show crashinfo** command in privileged EXEC mode.

show crashinfo [**save**]

Syntax Description

save (Optional) Displays if the ASA is configured to save crash information to Flash memory or not.

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(5) The output displays the thread ID (TID) in the **show process** command.

9.4(1) The output displays the most recent 50 lines of generated syslogs. Note that you must enable the **logging buffer** command to enable these results to appear.

9.7(1) The output was updated to display only the latest system generated crash file.

Usage Guidelines

If the crash file is from a test crash (generated from the **crashinfo test** command), the first string of the crash file is “: **Saved_Test_Crash**” and the last string is “: **End_Test_Crash**”. If the crash file is from a real crash, the first string of the crash file is “: **Saved_Crash**” and the last string is “: **End_Crash**”. (This includes crashes from use of the **crashinfo force page-fault** or **crashinfo force watchdog** commands).

If there is no crash data saved in flash, or if the crash data has been cleared by entering the **clear crashinfo** command, the **show crashinfo** command displays an error message.



Note Crash information written to flash memory as a result of using **crashinfo test** command cannot be viewed in this command output. Only the real crash file displays in `crashinfo_YYYYMMDD_HHMMSS 5_UTC` format.

Examples

The following example shows how to display the current crash information configuration:

```
ciscoasa# show crashinfo save
crashinfo save enable
```

The following example shows the output for a crash file test. (However, this test does not actually crash the ASA. It provides a simulated example file.)

```
ciscoasa(config)# crashinfo test
ciscoasa(config)# exit
ciscoasa# show crashinfo
: Saved_Test_Crash
Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)
Traceback:
0: 00323143
1: 0032321b
2: 0010885c
3: 0010763c
4: 001078db
5: 00103585
6: 00000000
   vector 0x000000ff (user defined)
       edi 0x004f20c4
       esi 0x00000000
       ebp 0x00e88c20
       esp 0x00e88bd8
       ebx 0x00000001
       edx 0x00000074
       ecx 0x00322f8b
       eax 0x00322f8b
error code n/a
   eip 0x0010318c
   cs 0x00000008
   eflags 0x00000000
   CR2 0x00000000
F-flags : 0x2
F-flags2 : 0x0
F-flags3 : 0x10000
F-flags4 : 0x0
F-bytes : 0
Stack dump: base:0x00e8511c size:16384, active:1476
0x00e89118: 0x004f1bb4
0x00e89114: 0x001078b4
0x00e89110-0x00e8910c: 0x00000000
0x00e89108-0x00e890ec: 0x12345678
0x00e890e8: 0x004f1bb4
0x00e890e4: 0x00103585
0x00e890e0: 0x00e8910c
0x00e890dc-0x00e890cc: 0x12345678
0x00e890c8: 0x00000000
0x00e890c4-0x00e890bc: 0x12345678
0x00e890b8: 0x004f1bb4
0x00e890b4: 0x001078db
0x00e890b0: 0x00e890e0
0x00e890ac-0x00e890a8: 0x12345678
0x00e890a4: 0x001179b3
0x00e890a0: 0x00e890b0
0x00e8909c-0x00e89064: 0x12345678
0x00e89060: 0x12345600
0x00e8905c: 0x20232970
0x00e89058: 0x616d2d65
0x00e89054: 0x74002023
0x00e89050: 0x29676966
0x00e8904c: 0x6e6f6328
```

```
0x00e89048: 0x31636573
0x00e89044: 0x7069636f
0x00e89040: 0x64786970
0x00e8903c-0x00e88e50: 0x00000000
0x00e88e4c: 0x000a7473
0x00e88e48: 0x6574206f
0x00e88e44: 0x666e6968
0x00e88e40: 0x73617263
0x00e88e3c-0x00e88e38: 0x00000000
0x00e88e34: 0x12345600
0x00e88e30-0x00e88dfc: 0x00000000
0x00e88df8: 0x00316761
0x00e88df4: 0x74706100
0x00e88df0: 0x12345600
0x00e88dec-0x00e88ddc: 0x00000000
0x00e88dd8: 0x00000070
0x00e88dd4: 0x616d2d65
0x00e88dd0: 0x74756f00
0x00e88dcc: 0x00000000
0x00e88dc8: 0x00e88e40
0x00e88dc4: 0x004f20c4
0x00e88dc0: 0x12345600
0x00e88dbc: 0x00000000
0x00e88db8: 0x00000035
0x00e88db4: 0x315f656c
0x00e88db0: 0x62616e65
0x00e88dac: 0x0030fcf0
0x00e88da8: 0x3011111f
0x00e88da4: 0x004df43c
0x00e88da0: 0x0053fef0
0x00e88d9c: 0x004f1bb4
0x00e88d98: 0x12345600
0x00e88d94: 0x00000000
0x00e88d90: 0x00000035
0x00e88d8c: 0x315f656c
0x00e88d88: 0x62616e65
0x00e88d84: 0x00000000
0x00e88d80: 0x004f20c4
0x00e88d7c: 0x00000001
0x00e88d78: 0x01345678
0x00e88d74: 0x00f53854
0x00e88d70: 0x00f7f754
0x00e88d6c: 0x00e88db0
0x00e88d68: 0x00e88d7b
0x00e88d64: 0x00f53874
0x00e88d60: 0x00e89040
0x00e88d5c-0x00e88d54: 0x12345678
0x00e88d50-0x00e88d4c: 0x00000000
0x00e88d48: 0x004f1bb4
0x00e88d44: 0x00e88d7c
0x00e88d40: 0x00e88e40
0x00e88d3c: 0x00f53874
0x00e88d38: 0x004f1bb4
0x00e88d34: 0x0010763c
0x00e88d30: 0x00e890b0
0x00e88d2c: 0x00e88db0
0x00e88d28: 0x00e88d88
0x00e88d24: 0x0010761a
0x00e88d20: 0x00e890b0
0x00e88d1c: 0x00e88e40
0x00e88d18: 0x00f53874
0x00e88d14: 0x0010166d
0x00e88d10: 0x0000000e
0x00e88d0c: 0x00f53874
```

```

0x00e88d08: 0x00f53854
0x00e88d04: 0x0048b301
0x00e88d00: 0x00e88d30
0x00e88cfc: 0x0000000e
0x00e88cf8: 0x00f53854
0x00e88cf4: 0x0048a401
0x00e88cf0: 0x00f53854
0x00e88cec: 0x00f53874
0x00e88ce8: 0x0000000e
0x00e88ce4: 0x0048a64b
0x00e88ce0: 0x0000000e
0x00e88cdc: 0x00f53874
0x00e88cd8: 0x00f7f96c
0x00e88cd4: 0x0048b4f8
0x00e88cd0: 0x00e88d00
0x00e88ccc: 0x0000000f
0x00e88cc8: 0x00f7f96c
0x00e88cc4-0x00e88cc0: 0x0000000e
0x00e88cbc: 0x00e89040
0x00e88cb8: 0x00000000
0x00e88cb4: 0x00f5387e
0x00e88cb0: 0x00f53874
0x00e88cac: 0x00000002
0x00e88ca8: 0x00000001
0x00e88ca4: 0x00000009
0x00e88ca0-0x00e88c9c: 0x00000001
0x00e88c98: 0x00e88cb0
0x00e88c94: 0x004f20c4
0x00e88c90: 0x0000003a
0x00e88c8c: 0x00000000
0x00e88c88: 0x0000000a
0x00e88c84: 0x00489f3a
0x00e88c80: 0x00e88d88
0x00e88c7c: 0x00e88e40
0x00e88c78: 0x00e88d7c
0x00e88c74: 0x001087ed
0x00e88c70: 0x00000001
0x00e88c6c: 0x00e88cb0
0x00e88c68: 0x00000002
0x00e88c64: 0x0010885c
0x00e88c60: 0x00e88d30
0x00e88c5c: 0x00727334
0x00e88c58: 0xa0ffffff
0x00e88c54: 0x00e88cb0
0x00e88c50: 0x00000001
0x00e88c4c: 0x00e88cb0
0x00e88c48: 0x00000002
0x00e88c44: 0x0032321b
0x00e88c40: 0x00e88c60
0x00e88c3c: 0x00e88c7f
0x00e88c38: 0x00e88c5c
0x00e88c34: 0x004b1ad5
0x00e88c30: 0x00e88c60
0x00e88c2c: 0x00e88e40
0x00e88c28: 0xa0ffffff
0x00e88c24: 0x00323143
0x00e88c20: 0x00e88c40
0x00e88c1c: 0x00000000
0x00e88c18: 0x00000008
0x00e88c14: 0x0010318c
0x00e88c10-0x00e88c0c: 0x00322f8b
0x00e88c08: 0x00000074
0x00e88c04: 0x00000001
0x00e88c00: 0x00e88bd8

```

```
0x00e88bfc: 0x00e88c20
0x00e88bf8: 0x00000000
0x00e88bf4: 0x004f20c4
0x00e88bf0: 0x000000ff
0x00e88bec: 0x00322f87
0x00e88be8: 0x00f5387e
0x00e88be4: 0x00323021
0x00e88be0: 0x00e88c10
0x00e88bdc: 0x004f20c4
0x00e88bd8: 0x00000000 *
0x00e88bd4: 0x004eabb0
0x00e88bd0: 0x00000001
0x00e88bcc: 0x00f5387e
0x00e88bc8-0x00e88bc4: 0x00000000
0x00e88bc0: 0x00000008
0x00e88bbc: 0x0010318c
0x00e88bb8-0x00e88bb4: 0x00322f8b
0x00e88bb0: 0x00000074
0x00e88bac: 0x00000001
0x00e88ba8: 0x00e88bd8
0x00e88ba4: 0x00e88c20
0x00e88ba0: 0x00000000
0x00e88b9c: 0x004f20c4
0x00e88b98: 0x000000ff
0x00e88b94: 0x001031f2
0x00e88b90: 0x00e88c20
0x00e88b8c: 0xffffffff
0x00e88b88: 0x00e88cb0
0x00e88b84: 0x00320032
0x00e88b80: 0x37303133
0x00e88b7c: 0x312f6574
0x00e88b78: 0x6972772f
0x00e88b74: 0x342f7665
0x00e88b70: 0x64736666
0x00e88b6c: 0x00020000
0x00e88b68: 0x00000010
0x00e88b64: 0x00000001
0x00e88b60: 0x123456cd
0x00e88b5c: 0x00000000
0x00e88b58: 0x00000008
Cisco XXX Firewall Version X.X
Cisco XXX Device Manager Version X.X
Compiled on Fri 15-Nov-04 14:35 by root
hostname up 10 days 0 hours
Hardware: XXX-XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xffffd8000, 32KB
0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover: Disabled
VPN-DES: Enabled
VPN-3DES-AES: Disabled
Maximum Interfaces: 3
Cut-through Proxy: Enabled
Guards: Enabled
URL-filtering: Enabled
Inside Hosts: Unlimited
Throughput: Unlimited
IKE peers: Unlimited
This XXX has a Restricted (R) license.
Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
```

Configuration last modified by enable_15 at 13:49:42.148 UTC Wed Nov 20 2004

----- show clock -----

15:34:28.129 UTC Sun Nov 24 2004

----- show memory -----

Free memory: 50444824 bytes

Used memory: 16664040 bytes

Total memory: 67108864 bytes

----- show conn count -----

0 in use, 0 most used

----- show xlate count -----

0 in use, 0 most used

----- show vpn-sessiondb summary -----

Active Session Summary

Sessions:

	Active	Cumulative	Peak Concurrent	Inactive
SSL VPN	: 2	: 2	: 2	2
Clientless only	: 0	: 0	: 0	0
With client	: 2	: 2	: 2	2
Email Proxy	: 0	: 0	: 0	0
IPsec LAN-to-LAN	: 1	: 1	: 1	1
IPsec Remote Access	: 0	: 0	: 0	0
VPN Load Balancing	: 0	: 0	: 0	0
Totals	: 3	: 3	: 3	3

License Information:

Shared VPN License Information:

 SSL VPN : 1500

 Allocated to this device : 50

 Allocated in network : 50

 Device limit : 750

IPsec : 750 Configured : 750 Active : 1 Load : 0%

SSL VPN : 52 Configured : 52 Active : 2 Load : 4%

Active : Cumulative : Peak Concurrent

IPsec : 1 : 1 : 1

SSL VPN : 2 : 10 : 2

 AnyConnect Mobile : 0 : 0 : 0

 Linksys Phone : 0 : 0 : 0

Totals : 3 : 11

Tunnels:

Active : Cumulative : Peak Concurrent

IKE : 1 : 1 : 1

IPsec : 1 : 1 : 1

Clientless : 2 : 2 : 2

SSL-Tunnel : 2 : 2 : 2

DTLS-Tunnel : 2 : 2 : 2

Totals : 8 : 8

----- show blocks -----

SIZE	MAX	LOW	CNT
4	1600	1600	1600
80	400	400	400
256	500	499	500
1550	1188	795	927

----- show interface -----

interface ethernet0 "outside" is up, line protocol is up

Hardware is i82559 ethernet, address is 0003.e300.73fd

IP address 172.23.59.232, subnet mask 255.255.0.0

MTU 1500 bytes, BW 10000 Kbit half duplex

6139 packets input, 830375 bytes, 0 no buffer

Received 5990 broadcasts, 0 runts, 0 giants

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

90 packets output, 6160 bytes, 0 underruns

0 output errors, 13 collisions, 0 interface resets

0 babbles, 0 late collisions, 47 deferred

0 lost carrier, 0 no carrier


```

input queue (curr/max blocks): hardware (5/128) software (0/2)
output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
Hardware is i82559 ethernet, address is 0003.e300.73fe
IP address 10.1.1.1, subnet mask 255.255.255.0
MTU 1500 bytes, BW 10000 Kbit half duplex
 0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 1 packets output, 60 bytes, 0 underruns
 0 output errors, 0 collisions, 0 interface resets
 0 babbles, 0 late collisions, 0 deferred
 1 lost carrier, 0 no carrier
input queue (curr/max blocks): hardware (128/128) software (0/0)
output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
Hardware is i82559 ethernet, address is 00d0.b7c8.139e
IP address 127.0.0.1, subnet mask 255.255.255.255
MTU 1500 bytes, BW 10000 Kbit half duplex
 0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 packets output, 0 bytes, 0 underruns
 0 output errors, 0 collisions, 0 interface resets
 0 babbles, 0 late collisions, 0 deferred
 0 lost carrier, 0 no carrier
input queue (curr/max blocks): hardware (128/128) software (0/0)
output queue (curr/max blocks): hardware (0/0) software (0/0)

```

```

----- show cpu usage -----
CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%
----- show process -----

```

PC	SP	STATE	Runtime	SBASE	Stack	Process	TID
Hsi	001e3329	00763e7c	0053e5c8	0	00762ef4	3784/4096 arp_timer	0x0000000000000000a
Lsi	001e80e9	00807074	0053e5c8	0	008060fc	3792/4096 FragDBGC	0x0000000000000006b
Lwe	00117e3a	009dc2e4	00541d18		0 009db46c	3704/4096 dbgtrace	
Lwe	003cee95	009de464	00537718		0 009dc51c	8008/8192 Logger	
Hwe	003d2d18	009e155c	005379c8		0 009df5e4	8008/8192 tcp_fast	
Hwe	003d2c91	009e360c	005379c8		0 009e1694	8008/8192 tcp_slow	
Lsi	002ec97d	00b1a464	0053e5c8		0 00b194dc	3928/4096 xlate clean	
Lsi	002ec88b	00b1b504	0053e5c8		0 00b1a58c	3888/4096 uxlate clean	
Mrd	002e3a17	00c8f8d4	0053e600		0 00c8d93c	7908/8192 tcp_intercept_times	
Lsi	00423dd5	00d3a22c	0053e5c8		0 00d392a4	3900/4096 route_process	
Hsi	002d59fc	00d3b2bc	0053e5c8		0 00d3a354	3780/4096 PIX Garbage Collec	
Hwe	0020e301	00d5957c	0053e5c8		0 00d55614	16048/16384 isakmp_time_keep	
Lsi	002d377c	00d7292c	0053e5c8		0 00d719a4	3928/4096 perfmon	
Hwe	0020bd07	00d9c12c	0050bb90		0 00d9b1c4	3944/4096 IPsec	
Mwe	00205e25	00d9e1ec	0053e5c8		0 00d9c274	7860/8192 IPsec timer handler	
Hwe	003864e3	00db26bc	00557920		0 00db0764	6904/8192 qos_metric_daemon	
Mwe	00255a65	00dc9244	0053e5c8		0 00dc8adc	1436/2048 IP Background	
Lwe	002e450e	00e7bb94	00552c30		0 00e7ad1c	3704/4096 pix/trace	
Lwe	002e471e	00e7cc44	00553368		0 00e7bdcc	3704/4096 pix/tconsole	
Hwe	001e5368	00e7ed44	00730674		0 00e7ce9c	7228/8192 pix/intf0	
Hwe	001e5368	00e80e14	007305d4		0 00e7ef6c	7228/8192 pix/intf1	
Hwe	001e5368	00e82ee4	00730534		2470 00e8103c	4892/8192 pix/intf2	
H*	001a6ff5	0009ff2c	0053e5b0		4820 00e8511c	12860/16384 ci/console	
Csi	002dd8ab	00e8a124	0053e5c8		0 00e891cc	3396/4096 update_cpu_usage	
Hwe	002cb4d1	00f2bfb3	0051e360		0 00f2a134	7692/8192 uauth_in	
Hwe	003d17d1	00f2e0bc	00828cf0		0 00f2c1e4	7896/8192 uauth_thread	
Hwe	003e71d4	00f2f20c	00537d20		0 00f2e294	3960/4096 udp_timer	
Hsi	001db3ca	00f30fc4	0053e5c8		0 00f3004c	3784/4096 557mcfix	
Crđ	001db37f	00f32084	0053ea40	508286220	00f310fc	3688/4096 557poll	
Lsi	001db435	00f33124	0053e5c8		0 00f321ac	3700/4096 557timer	
Hwe	001e5398	00f441dc	008121e0		0 00f43294	3912/4096 fover_ip0	
Cwe	001dcdad	00f4523c	00872b48		120 00f44344	3528/4096 ip/0:0	

```

Hwe 001e5398 00f4633c 008121bc      10 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198      0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174      0 00f475a4 3456/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150      0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850      0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c      0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108      0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4      0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0      0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534      0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c      0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078      0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054      0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8      0 00f77fdc 300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8      0 00f786c4 7640/8192 Crypto CA
----- show failover -----
No license for Failover
----- show traffic -----
outside:
    received (in 865565.090 secs):
        6139 packets    830375 bytes
        0 pkts/sec     0 bytes/sec
    transmitted (in 865565.090 secs):
        90 packets     6160 bytes
        0 pkts/sec     0 bytes/sec
inside:
    received (in 865565.090 secs):
        0 packets     0 bytes
        0 pkts/sec    0 bytes/sec
    transmitted (in 865565.090 secs):
        1 packets     60 bytes
        0 pkts/sec    0 bytes/sec
intf2:
    received (in 865565.090 secs):
        0 packets     0 bytes
        0 pkts/sec    0 bytes/sec
    transmitted (in 865565.090 secs):
        0 packets     0 bytes
        0 pkts/sec    0 bytes/sec
----- show perfmon -----
PERFMON STATS:   Current   Average
Xlates           0/s      0/s
Connections      0/s      0/s
TCP Conns        0/s      0/s
UDP Conns        0/s      0/s
URL Access       0/s      0/s
URL Server Req   0/s      0/s
TCP Fixup        0/s      0/s
TCPIntercept     0/s      0/s
HTTP Fixup       0/s      0/s
FTP Fixup        0/s      0/s
AAA Authen       0/s      0/s
AAA Author       0/s      0/s
AAA Account      0/s      0/s
: End_Test_Crash

```

Related Commands

Command	Description
clear crashinfo	Deletes all the crash information files. the contents of the crash file.
crashinfo force	Forces a crash of the ASA.

Command	Description
crashinfo save disable	Disables crash information from writing to flash memory.
crashinfo test	Tests the ability of the ASA to save crash information to a file in flash memory.
show crashinfo files	Displays the last five crash information files based on the date and timestamp.

show crashinfo console

To display the configuration setting of the **crashinfo console** command, enter the show crashinfo console command.

show crashinfo console

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

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

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

Command History

Release Modification

7.0(4) This command was added.

Usage Guidelines

Compliance with FIPS 140-2 prohibits the distribution of Critical Security Parameters (keys, passwords, etc.) outside of the crypto boundary (chassis). When the device crashes, due to an assert or checkheaps failure, it is possible that the stack or memory regions dumped to the console contain sensitive data. This output must be suppressed in FIPS-mode.

Examples

```
sw8-5520(config)# show crashinfo console
crashinfo console enable
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
crashinfo console disable	Disables the reading, writing and configuration of crash write info to flash.
fips enable	Enables or disablea policy-checking to enforce FIPS compliance on the system or module.
show running-config fips	Displays the FIPS configuration that is running on the ASA.

show crashinfo files

To display the latest system generated crash files in ASA, use the **show crashinfo files** command in privileged EXEC mode. The output displays a maximum of five crash files that are written to flash memory, based on the date and timestamp. The command output does not display any information if there are no crash files.

show crashinfo files

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

9.7(1) This command was added.

Usage Guidelines

Crash information written to flash memory as a result of using **crashinfo test** command cannot be viewed in **show crashinfo files** output. Only the real crash files display in `crashinfo_YYYYMMDD_HHMMSS 5 UTC` format. If there is no crash data saved in flash, or if the crash data has been cleared by entering the **clear crashinfo** command, the **show crashinfo files** command displays an error message.

Examples

The following example displays the actual crash information files:

```
ciscoasa# show crashinfo files
crashinfo_20160725_012315.UTC
crashinfo_20160725_021353.UTC
crashinfo_20160725_022309.UTC
crashinfo_20160725_024205.UTC
```

Related Commands

Command	Description
clear crashinfo	Deletes the contents of all the crash files.
crashinfo force	Forces the ASA to crash.
crashinfo save disable	Disables crash information from writing to flash memory.

Command	Description
show crashinfo	Displays the contents of the latest crash file.
crashinfo test	Tests the ability of the ASA to save crash information to a file in flash memory.

show crypto accelerator load-balance

To display the global and accelerator-specific load-balancing information from the hardware crypto accelerator MIB, use the **show crypto accelerator load-balance** command.

show crypto accelerator load-balance [ipsec | ssl | detail [ipsec | ssl]]

Syntax Description

detail (Optional) Displays detailed information. You can include the ipsec or ssl keyword after this option.

ipsec (Optional) Displays crypto accelerator IPsec load balancing details.

ssl (Optional) Displays crypto accelerator SSL load balancing details.

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	—
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release Modification

7.0(1) This command was added.

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto protocol statistics	Displays the protocol-specific statistics from the crypto accelerator MIB.

show crypto accelerator statistics

To display the global and accelerator-specific statistics from the hardware crypto accelerator MIB, use the **show crypto accelerator statistics** command in global configuration or privileged EXEC mode.

show crypto accelerator statistics

Syntax Description This command has no keywords or variables.

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	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History	Release	Modification
	7.0(1)	This command was added.

Usage Guidelines The output statistics are defined as follows:

Accelerator 0 shows statistics for the software-based crypto engine.

Accelerator 1 shows statistics for the hardware-based crypto engine.

RSA statistics show RSA operations for 2048-bit keys, which are executed in software by default. This means that when you have a 2048-bit key, IKE/SSL VPN performs RSA operations in software during the IPsec/SSL negotiation phase. Actual IPsec/SSL traffic is still processed using hardware. This may cause high CPU if there are many simultaneous sessions starting at the same time, which may result in multiple RSA key operations and high CPU. If you run into a high CPU condition because of this, then you should use a 1024-bit key to process RSA key operations in hardware. To do so, you must reenroll the identity certificate. In releases 8.3(2) or later, you can also use the crypto engine large-mod-accel command on the 5510-5550 platforms to perform these operations in hardware.

If you are using a 2048-bit RSA key and the RSA processing is performed in software, you can use CPU profiling to determine which functions are causing high CPU usage. Generally, the bn_* and BN_* functions are math operations on the large data sets used for RSA, and are the most useful when examining CPU usage during an RSA operation in software. For example:

```

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@ 36.50% : _bn_mul_add_words
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@ 19.75% : _bn_sqr_comba8
    
```


Diffie-Hellman statistics show that any crypto operation with a modulus size greater than 1024 is performed in software (for example, DH5 (Diffie-Hellman group 5 uses 1536)). If so, a 2048-bit key certificate will be processed in software, which can result in high CPU usage when a lot of sessions are running.



Note The ASA 5505 (with a Cavium CN505 processor) only supports Diffie-Hellman Groups 1 and 2 for hardware-accelerated, 768-bit and 1024-bit key generation. Diffie-Hellman Group 5 (1536-bit key generation) is performed in software.

A single crypto engine in the adaptive security appliance performs the IPsec and SSL operations. To display the versions of crypto (Cavium) microcode that are loaded into the hardware crypto accelerator at boot time, enter the **show version** command. For example:

```
ciscoasa(config) show version
Cisco Adaptive Security Appliance Software Version 8.0(4)8
Device Manager Version 6.1(5)
Compiled on Wed 15-Oct-09 17:27 by builders
System image file is "disk0:/interim/asa804-8-k8.bin"
Config file at boot was "startup-config"
asa up 5 days 17 hours
Hardware: ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 512MB
BIOS Flash M50FW080 @ 0xffe00000, 1024KB
Encryption hardware device : Cisco ASA-5505 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-2.05
```

DSA statistics show key generation in two phases. The first phase is a choice of algorithm parameters, which may be shared between different users of the system. The second phase computes private and public keys for a single user.

SSL statistics show records for the processor-intensive public key encryption algorithms involved in SSL transactions to the hardware crypto accelerator.

RNG statistics show records for a sender and receiver, which can generate the same set of random numbers automatically to use as keys.

Examples

The following example, entered in global configuration mode, shows global crypto accelerator statistics:

```
ciscoasa # show crypto accelerator statistics
Crypto Accelerator Status
-----
[Capacity]
  Supports hardware crypto: True
  Supports modular hardware crypto: False
  Max accelerators: 1
  Max crypto throughput: 100 Mbps
  Max crypto connections: 750
[Global Statistics]
  Number of active accelerators: 1
  Number of non-operational accelerators: 0
  Input packets: 700
  Input bytes: 753488
  Output packets: 700
  Output error packets: 0
```

```

Output bytes: 767496
[Accelerator 0]
  Status: Active
  Software crypto engine
  Slot: 0
  Active time: 167 seconds
  Total crypto transforms: 7
  Total dropped packets: 0
  [Input statistics]
    Input packets: 0
    Input bytes: 0
    Input hashed packets: 0
    Input hashed bytes: 0
    Decrypted packets: 0
    Decrypted bytes: 0
  [Output statistics]
    Output packets: 0
    Output bad packets: 0
    Output bytes: 0
    Output hashed packets: 0
    Output hashed bytes: 0
    Encrypted packets: 0
    Encrypted bytes: 0
  [Diffie-Hellman statistics]
    Keys generated: 0
    Secret keys derived: 0
  [RSA statistics]
    Keys generated: 0
    Signatures: 0
    Verifications: 0
    Encrypted packets: 0
    Encrypted bytes: 0
    Decrypted packets: 0
    Decrypted bytes: 0
  [DSA statistics]
    Keys generated: 0
    Signatures: 0
    Verifications: 0
  [SSL statistics]
    Outbound records: 0
    Inbound records: 0
  [RNG statistics]
    Random number requests: 98
    Random number request failures: 0
[Accelerator 1]
  Status: Active
  Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
                                Boot microcode   : CNlite-MC-Boot-Cisco-1.2
                                SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
                                IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.03

Slot: 1
Active time: 170 seconds
Total crypto transforms: 1534
Total dropped packets: 0
[Input statistics]
  Input packets: 700
  Input bytes: 753544
  Input hashed packets: 700
  Input hashed bytes: 736400
  Decrypted packets: 700
  Decrypted bytes: 719944
[Output statistics]
  Output packets: 700

```

```

Output bad packets: 0
Output bytes: 767552
Output hashed packets: 700
Output hashed bytes: 744800
Encrypted packets: 700
Encrypted bytes: 728352
[Diffie-Hellman statistics]
  Keys generated: 97
  Secret keys derived: 1
[RSA statistics]
  Keys generated: 0
  Signatures: 0
  Verifications: 0
  Encrypted packets: 0
  Encrypted bytes: 0
  Decrypted packets: 0
  Decrypted bytes: 0
[DSA statistics]
  Keys generated: 0
  Signatures: 0
  Verifications: 0
[SSL statistics]
  Outbound records: 0
  Inbound records: 0
[RNG statistics]
  Random number requests: 1
  Random number request failures: 0

```

The following table describes what the output entries indicates.

Output	Description
Capacity	This section pertains to the crypto acceleration that the ASA can support.
Supports hardware crypto	(True/False) The ASA can support hardware crypto acceleration.
Supports modular hardware crypto	(True/False) Any supported hardware crypto accelerator can be inserted as a separate plug-in card or module.
Max accelerators	The maximum number of hardware crypto accelerators that the ASA supports.
Mac crypto throughput	The maximum rated VPN throughput for the ASA.
Max crypto connections	The maximum number of supported VPN tunnels for the ASA.
Global Statistics	This section pertains to the combined hardware crypto accelerators in the ASA.
Number of active accelerators	The number of active hardware accelerators. An active hardware accelerator has been initialized and is available to process crypto commands.
Number of non-operational accelerators	The number of inactive hardware accelerators. An inactive hardware accelerator has been detected, but either has not completed initialization or has failed and is no longer usable.
Input packets	The number of inbound packets processed by all hardware crypto accelerators.

Output	Description
Input bytes	The number of bytes of data in the processed inbound packets.
Output packets	The number of outbound packets processed by all hardware crypto accelerators.
Output error packets	The number of outbound packets processed by all hardware crypto accelerators in which an error has been detected.
Output bytes	The number of bytes of data in the processed outbound packets.
Accelerator 0	Each of these sections pertains to a crypto accelerator. The first one (Accelerator 0) is always the software crypto engine. Although not a hardware accelerator, the ASA uses it to perform specific crypto tasks, and its statistics appear here. Accelerators 1 and higher are always hardware crypto accelerators.
Status	The status of the accelerator, which indicates whether the accelerator is being initialized, is active, or has failed.
Software crypto engine	The type of accelerator and firmware version (if applicable).
Slot	The slot number of the accelerator (if applicable).
Active time	The length of time that the accelerator has been in the active state.
Total crypto transforms	The total number of crypto commands that were performed by the accelerator.
Total dropped packets	The total number of packets that were dropped by the accelerator because of errors.
Input statistics	This section pertains to input traffic that was processed by the accelerator. Input traffic is considered to be ciphertext that must be decrypted and/or authenticated.
Input packets	The number of input packets that have been processed by the accelerator.
Input bytes	The number of input bytes that have been processed by the accelerator.
Input hashed packets	The number of packets for which the accelerator has performed hash operations.
Input hashed bytes	The number of bytes over which the accelerator has performed hash operations.
Decrypted packets	The number of packets for which the accelerator has performed symmetric decryption operations.
Decrypted bytes	The number of bytes over which the accelerator has performed symmetric decryption operations.

Output	Description
Output statistics	This section pertains to output traffic that has been processed by the accelerator. Input traffic is considered clear text that must be encrypted and/or hashed.
Output packets	The number of output packets that have been processed by the accelerator.
Output bad packets	The number of output packets that have been processed by the accelerator in which an error has been detected.
Output bytes	The number of output bytes that have been processed by the accelerator.
Output hashed packets	The number of packets for which the accelerator has performed outbound hash operations.
Output hashed bytes	The number of bytes over which the accelerator has performed outbound hash operations.
Encrypted packets	The number of packets for which the accelerator has performed symmetric encryption operations.
Encrypted bytes	The number of bytes over which the accelerator has performed symmetric encryption operations.
Diffie-Hellman statistics	This section pertains to Diffie-Hellman key exchange operations.
Keys generated	The number of Diffie-Hellman key sets that have been generated by the accelerator.
Secret keys derived	The number of Diffie-Hellman shared secrets that have been derived by the accelerator.
RSA statistics	This section pertains to RSA crypto operations.
Keys generated	The number of RSA key sets that have been generated by the accelerator.
Signatures	The number of RSA signature operations that have been performed by the accelerator.
Verifications	The number of RSA signature verifications that have been performed by the accelerator.
Encrypted packets	The number of packets for which the accelerator has performed RSA encryption operations.
Decrypted packets	The number of packets for which the accelerator has performed RSA decryption operations.
Decrypted bytes	The number of bytes of data over which the accelerator has performed RSA decryption operations.
DSA statistics	This section pertains to DSA operations. Note that DSA is not supported as of Version 8.2, so these statistics are no longer displayed.

Output	Description
Keys generated	The number of DSA key sets that have been generated by the accelerator.
Signatures	The number of DSA signature operations that have been performed by the accelerator.
Verifications	The number of DSA signature verifications that have been performed by the accelerator.
SSL statistics	This section pertains to SSL record processing operations.
Outbound records	The number of SSL records that have been encrypted and authenticated by the accelerator.
Inbound records	The number of SSL records that have been decrypted and authenticated by the accelerator.
RNG statistics	This section pertains to random number generation.
Random number requests	The number of requests to the accelerator for a random number.
Random number request failures	The number of random number requests to the accelerator that did not succeed.

On platforms that support IPsec flow offload, the output shows the statistics for offloaded flows while the global counters show the total of all offloaded and non-offloaded flows for all accelerator engines on the device.

```
ciscoasa# show crypto accelerator statistics
```

```
Crypto Accelerator Status
-----
[Capability]
  Supports hardware crypto: True
  Supported TLS Offload Mode: HARDWARE
  Supports modular hardware crypto: False
  Max accelerators: 3
  Max crypto throughput: 3000 Mbps
  Max crypto connections: 3000
[Global Statistics]
  Number of active accelerators: 2
  Number of non-operational accelerators: 0
  Input packets: 108
  Input bytes: 138912
  Output packets: 118
  Output error packets: 0
  Output bytes: 142329

[Accelerator 0]
  Status: OK
  Software crypto engine
  Slot: 0
  Active time: 489 seconds
  Total crypto transforms: 2770
  Total dropped packets: 0
  [Input statistics]
    Input packets: 0
```

```
Input bytes: 19232
Input hashed packets: 0
Input hashed bytes: 0
Decrypted packets: 0
Decrypted bytes: 19232
[Output statistics]
Output packets: 0
Output bad packets: 0
Output bytes: 18784
Output hashed packets: 0
Output hashed bytes: 0
Encrypted packets: 0
Encrypted bytes: 18784
[Diffie-Hellman statistics]
Keys generated: 0
Secret keys derived: 0
[RSA statistics]
Keys generated: 1
Signatures: 1
Verifications: 1
Encrypted packets: 1
Encrypted bytes: 28
Decrypted packets: 1
Decrypted bytes: 256
[ECDSA statistics]
Keys generated: 13
Signatures: 12
Verifications: 15
[EDDSA statistics]
Keys generated: 0
Signatures: 0
Verifications: 0
[SSL statistics]
Outbound records: 0
Inbound records: 0
[RNG statistics]
Random number requests: 0
Random number request failures: 0
[HMAC statistics]
HMAC requests: 54

[Accelerator 1]
Status: OK
Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1)
                          AE microcode       : CNN5x-MC-AE-MAIN-0007
                          SE SSL microcode    : CNN5x-MC-SE-SSL-0018

Slot: 1
Active time: 497 seconds
Total crypto transforms: 2910
Total dropped packets: 0
[Input statistics]
Input packets: 4
Input bytes: 13056
Input hashed packets: 0
Input hashed bytes: 0
Decrypted packets: 4
Decrypted bytes: 6528
[Output statistics]
Output packets: 14
Output bad packets: 0
Output bytes: 20786
Output hashed packets: 0
Output hashed bytes: 0
Encrypted packets: 14
```

```

Encrypted bytes: 10393
[Offloaded Input statistics]
Input packets: 106
Input bytes: 115328
Input hashed packets: 0
Input hashed bytes: 0
Decrypted packets: 107
Decrypted bytes: 112992
[Offloaded Output statistics]
Output packets: 107
Output bytes: 116416
Output hashed packets: 0
Output hashed bytes: 0
Encrypted packets: 107
Encrypted bytes: 112992
Total dropped packets: 0
[Diffie-Hellman statistics]
Keys generated: 194
Secret keys derived: 1
[RSA statistics]
Keys generated: 0
Signatures: 2
Verifications: 1
Encrypted packets: 3
Encrypted bytes: 162
Decrypted packets: 2
Decrypted bytes: 512
[ECDSA statistics]
Keys generated: 0
Signatures: 0
Verifications: 0
[EDDSA statistics]
Keys generated: 0
Signatures: 0
Verifications: 0
[SSL statistics]
Outbound records: 14
Inbound records: 4
[RNG statistics]
Random number requests: 34
Random number request failures: 0
[HMAC statistics]
HMAC requests: 26

```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto protocol statistics	Displays the protocol-specific statistics from the crypto accelerator MIB.

show crypto ca certificates

To display the certificates associated with a specific trustpoint or to display all the certificates installed on the system, use the **show crypto ca certificates** command in global configuration or privileged EXEC mode.

show crypto ca certificates [*trustpointname*]

Syntax Description

trustpointname (Optional) The name of a trustpoint. If you do not specify a name, this command displays all certificates installed on the ASA.

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	—
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 crypto ca certificates** command:

```
ciscoasa(config)# show crypto ca certificates test
Certificate
  Subject Name:
    commonName          = test
    unstructuredName     = ciscoasa.cisco.com
    serialNumber         = 9A8N02C5XFU
  Status: Pending terminal enrollment
  Key Usage: General Purpose
  Fingerprint: 7e2bb504 d8e2c4ca e45c76af 5309d2e4
  Associated Trustpoint: test
```

Related Commands

Command	Description
crypto ca authenticate	Obtains a CA certificate for a specified trustpoint.

Command	Description
crypto ca crl request	Requests a CRL based on the configuration parameters of a specified trustpoint.
crypto ca enroll	Initiates the enrollment process with a CA.
crypto ca import	Imports a certificate to a specified trustpoint.
crypto ca trustpoint	Enters trustpoint configuration mode for a specified trustpoint.

show crypto ca crl

To display all cached CRLs or to display all CRLs cached for a specified trustpoint, use the **show crypto ca crl** command in global configuration or privileged EXEC mode.

show crypto ca crl [**trustpool** | **trustpoint** <trustpointname>]

Syntax Description

trustpoint *trustpointname* (Optional) The name of a trustpoint. If you do not specify a name, this command displays all CRLs cached on the ASA.

trustpool The name of the trust pool.

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	—
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 crypto ca crl** command:

```
ciscoasa(config)# show crypto ca crl tp1
CRL Issuer Name:
  cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@example.com
LastUpdate: 19:45:53 UTC Dec 24 2004
NextUpdate: 08:05:53 UTC Jan 1 2005
Retrieved from CRL Distribution Point:
  http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
Associated Trustpoints: tp1
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ca authenticate	Obtains a CA certificate for a specified trustpoint.

Command	Description
crypto ca crl request	Requests a CRL based on the configuration parameters of a specified trustpoint.
crypto ca enroll	Initiates the enrollment process with a CA.
crypto ca import	Imports a certificate to a specified trustpoint.
crypto ca trustpoint	Enters trustpoint configuration mode for a specified trustpoint.

show crypto ca server

To display the status of the local CA configuration on the ASA, use the **show crypto ca server** command in ca server configuration, global configuration, or privileged EXEC mode.

show crypto ca 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
Ca server configuration	• Yes	—	• Yes	—	—
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release Modification

8.0(2) This command was added.

Examples

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

```
ciscoasa# show crypto ca server
#Certificate Server LOCAL-CA-SERVER:
  Status: disabled
  State: disabled
  Server's configuration is unlocked (enter "no shutdown" to lock it)
  Issuer name: CN=asal.cisco.com
  CA cert fingerprint: -Not found-
  Last certificate issued serial number: 0x0
  CA certificate expiration timer: 00:00:00 UTC Jan 1 2009
  CRL not present.
  Current primary storage dir: nvram
ciscoasa#
```

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode CLI command set, which allows you to configure and manage the local CA.
debug crypto ca server	Shows debugging messages when you configure the local CA server.
show crypto ca server certificate	Displays the certificate of the local CA in base64 format.
show crypto ca server crl	Displays the lifetime of the local CA CRL.

show crypto ca server cert-db

To display all or a subset of local CA server certificates, including those issued to a specific user, use the **show crypto ca server cert-db** command in ca server configuration, global configuration, or privileged EXEC mode.

show crypto ca server cert-db [**username** *username* | **allowed** | **enrolled** | **expired** | **on-hold**] [**serial** *certificate-serial-number*]

Syntax Description		
allowed		Specifies that users who are allowed to enroll appear, regardless of the status of their certificate.
enrolled		Specifies that users with valid certificates appear.
expired		Specifies that users holding expired certificates appear.
on-hold		Specifies that users who have not yet enrolled appear.
serial <i>certificate-serial-number</i>		Specifies the serial number of a specific certificate that displays. The serial number must be in hexadecimal format.
username <i>username</i>		Specifies the certificate owner. The username may be a username or an e-mail address. For e-mail addresses, it is the e-mail address used to contact and deliver the one-time password (OTP) to the end user. An e-mail address is required to enable e-mail notifications for the end user.

Command Default By default, if no username or certificate serial number is specified, the entire database of issued certificates appears.

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
Ca server configuration	• Yes	—	• Yes	—	—
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release Modification

8.0(2) This command was added.

Usage Guidelines

The **show crypto ca server cert-db** command displays a list of the user certificates that are issued by the local CA server. You can display a subset of the certificate database by specifying a specific username with one or more of the optional certificate-type keywords, and/or with an optional certificate serial number.

If you specify a username without a keyword or a serial number, all of the certificates issued for that user appear. For each user, the output shows the username, e-mail address, domain name, the time period for which enrollment is allowed, and the number of times that the user has been notified with an enrollment invitation.

In addition, the following information appears in the output:

- The NOTIFIED field is required to support multiple reminders. It tracks when a user needs to be notified of the OTP for enrollment and the reminder notification attempts. This field is set to 0 initially. It is incremented to 1 when the user entry is marked as being allowed to enroll. At this time, the initial OTP notification is generated.
- The NOTIFY field is incremented each time a reminder is sent. Three notifications are sent before the OTP is due to expire. A notification is sent when the user is allowed to enroll, at the mid-point of the expiration, and when $\frac{3}{4}$ of the expiration time has passed. This field is used only for administrator-initiated enrollments. For automatic certificate renewals, the NOTIFY field in the certificate database is used.



Note While the notification counter in this command is used to track the number of times a user is notified to renew a certificate before expiration, the notification counter in **show crypto ca server user-db** is used to track the number of times a user is notified to enroll for the certificate. Renewal notifications are tracked under **cert-db** and not included in **user-db**.

Each certificate displays the certificate serial number, the issued and expired dates, and the certificate status (Revoked/Not Revoked).

Examples

The following example requests the display of all of the certificates issued for ASA by the CA server:

```
ciscoasa# show crypto ca server cert-db username asa
Username: asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:    0x2
issued:   10:28:04 UTC Tue Sep 24 2013
expired:  10:28:04 UTC Thu Sep 26 2013
status:   Not Revoked
```

The following example requests the display of all the certificates issued by the local CA server with a serial number of 0x2:

```
ciscoasa# show crypto ca server cert-db serial 2
```

```
Username:asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:    0x2
issued:   10:28:04 UTC Tue Sep 24 2013
```



```
expired: 10:28:04 UTC Thu Sep 26 2013
status: Not Revoked
```

The following example requests the display of all of the certificates issued by the local CA server:

```
ciscoasa# show crypto ca server cert-db
Username: asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial: 0x2
issued: 10:28:04 UTC Tue Sep 24 2013
expired: 10:28:04 UTC Thu Sep 26 2013
status: Not Revoked
```

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode CLI command set, which allows you to configure and manage the local CA.
crypto ca server revoke	Marks a certificate issued by the local CA server as revoked in both the certificate database and CRL.
lifetime crl	Specifies the lifetime of the CRL.

show crypto ca server certificate

To display the certificate for the local CA server in base64 format, use the **show crypto ca server certificate** command in ca server configuration, global configuration, or privileged EXEC mode.

show crypto ca server certificate

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
Ca server configuration	• Yes	—	• Yes	—	—
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release Modification

8.0(2) This command was added.

Usage Guidelines

The **show crypto ca server certificate** command displays the local CA server certificate in base64 format. This display allows you to cut and paste a certificate while exporting it to other devices that need to trust the local CA server.

Examples

The following is sample output from the **show crypto ca server certificate** command:

```
ciscoasa# show crypto ca server certificate
The base64 encoded local CA certificate follows:
MIIXlwIBAzCCF1EGCSqGSIB3DQEHAaCCF0IEghc+
MIIXOjCCFzYGCSqGSIB3DQEHBqCCFycwghcjAgEAM
IIXHAYJKoZIhvcNAQcBMBsGCiqGSIB3DQEEMAQMwDQQ
Ijph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphs
UM+IG3SDOiDwZG9n1SvtMieoxd7Hxknxbum06JDruj
WkTHBIqkrm+td34q1NEliGeP2YC94/NQ2z+4ks+uZzw
cRh11KEZTS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CieL
j3h7VVMY6qbx2AC8I+q57+QG5vG515Hi5imwtYfaWwP
EdPQxaWZPrzoG1J8BFqdPa1jBghAzzuSmElm3j/2dQ3
AtrolG9nIsRHgV39fcBgz4fEabHG7/Vanb+fj81d
5n1oiJjDYYbP86tvbZ2yOVZR6aKFVI0b2AfCr6Pbw
```

```

fC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA
5KWScyEcgdqmuBeGDKOncTknfgy0XM+fG5rb3qAXy1
Gk jyFI5Bm9Do6RUROoG1DSrQrKeq/hj . . .

```

```
ciscoasa#
```

Related Commands	Command	Description
	crypto ca server	Provides access to the ca server configuration mode CLI command set, which allows you to configure and manage a local CA.
	issuer-name	Specifies the subject-name DN of the certificate authority certificate.
	keysize	Specifies the size of the public and private keys generated at user certificate enrollment.
	lifetime	Specifies the lifetime of the CA certificate and issued certificates.
	show crypto ca server	Displays the local CA configuration in ASCII text format.

show crypto ca server crl

To display the current CRL of the local CA, use the **show crypto ca server crl** command in ca server configuration, global configuration, or privileged EXEC mode.

show crypto ca server crl

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
Ca server configuration	• Yes	—	• Yes	—	—
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release Modification

8.0(2) This command was added.

Examples

The following is sample output from the **show crypto ca server crl** command:

```
ciscoasa
# show crypto ca server crl
asa5540(config)# sh cry ca ser crl
Certificate Revocation List:
  Issuer: cn=asa5540.frqa.cisco.com
  This Update: 07:32:27 UTC Oct 16 2006
  Next Update: 13:32:27 UTC Oct 16 2006
  Number of CRL entries: 0
  CRL size: 232 bytes
asa5540(config)#
ciscoasa
#
```

Related Commands

Command	Description
cdp-url	Specifies the CRL distribution point (CDP) to be included in the certificates issued by the CA.
crypto ca server	Provides access to the ca server configuration mode CLI command set, which allows you to configure and manage the local CA.
crypto ca server revoke	Marks a certificate issued by the local CA server as revoked in the certificate database and CRL.
lifetime crl	Specifies the lifetime of the CRL.
show crypto ca server	Displays the status of the CA configuration.

show crypto ca server user-db

To display users included in the local CA server user database, use the **show crypto ca server user-db** command in ca server configuration, global configuration, or privileged EXEC mode.

show crypto ca server user-db [**expired** | **allowed** | **on-hold** | **enrolled**]

Syntax Description

allowed (Optional) Specifies that users who are allowed to enroll display, regardless of the status of their certificate.

enrolled (Optional) Specifies that users with valid certificates display.

expired (Optional) Specifies that users holding expired certificates display.

on-hold (Optional) Specifies that users who have not enrolled yet display.

Command Default

By default, all users in the database display if no keywords are entered.

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
Ca server configuration	• Yes	—	• Yes	—	—
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release Modification

8.0(2) This command was added.

Examples

The following example displays currently enrolled users:

```
ciscoasa# show
      crypto ca server user-db enrolled
Username  DN      Certificate issued      Certificate expiration
exampleuser  cn=Example User,o=...  5/31/2009      5/31/2010
ciscoasa#
```

Usage Guidelines

While the notification counter in this command is used to track the number of times a user is notified to enroll for the certificate, the notification counter in `show crypto ca server cert-db` is used to track the number of times a user is notified to renew a certificate before expiration. Renewal notifications are tracked under `cert-db` and not included in `user-db`.

Related Commands

Command	Description
<code>crypto ca server user-db add</code>	Adds a user to the CA server user database.
<code>crypto ca server user-db allow</code>	Allows a specific user or a subset of users in the CA server database to enroll with the local CA.
<code>crypto ca server user-db remove</code>	Removes a user from the CA server user database.
<code>crypto ca server user-db write</code>	Writes user information configured in the local CA database to storage.
<code>show crypto ca server cert-db</code>	Displays all certificates issued by the local CA.

show crypto ca trustpool

To display the certificates that constitute the trustpool, use the **show crypto ca trustpool** command in privileged EXEC mode.

show crypto ca trustpool [**detail**]

Syntax Description

This command has no arguments or keywords.

Command Default

This command shows an abbreviated display of all the trustpool certificates. When the “detail” option is specified, more information is included.

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

9.0(1) This command was added.

Usage Guidelines

The output of the show crypto ca trustpool command includes the fingerprint value of each certificate. These values are required for removal operation.

Examples

```
ciscoasa# show crypto ca trustpool
CA Certificate
Status: Available
Certificate Serial Number: 6c386c409f4ff4944154635da520ed4c
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name: cn=bx2008-root
dc=bdb2008
dc=mycompany
dc=com
Subject Name:
cn=bx2008-root
dc=bx2008
dc=cisco
dc=com
Validity Date:
start date:17:21:06 EST Jan 14 2009
end date:17:31:06 EST Jan 14 2024
CA Certificate
Status: Available
```



```

Certificate Serial Number: 58d1c756000000000059
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
cn=bx2008-root
dc=bx2008
dc=mycompany
dc=com
Subject Name:
cn=BX2008SUB1-CA
dc=bx2008
dc=cisco
dc=com
OCSP AIA:
URL: http://bx2008-1.bx2008.mycompany.com/ocsp
CRL Distribution Points:
(1) http://bx2008-1.bx2008.mycompany.com/CertEnroll/bx2008-root.crl
Validity Date:
start date:11:54:34 EST May 18 2009
end date:12:04:34 EST May 18 2011

```

Related Commands

Command	Description
clear crypto ca trustpool	Removes all certificates from the trustpool.
crypto ca trustpool import	Imports certificates that constitute the PKI trustpool.
crypto ca trustpool remove	Removes a single specified certificate from the trustpool.

show crypto ca trustpool policy

To display the configured trustpool policy and process any applied certificate maps to show how those impact the policy, use the **show crypto ca trustpool policy** command in privileged EXEC mode.

show crypto ca trustpool policy

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

9.0(1) This command was added.

9.5(2) The ability to show status and results of automatic import of trustpool certificates was added.

Examples

```
ciscoasa(config)# sh run cry ca cert map
crypto ca certificate map map1 1
issuer-name eq cn = mycompany manufacturing ca
issuer-name eq cn = mycompany ca
crypto ca certificate map map 2 1
issuer-name eq cn = mycompany manufacturing ca
issuer-name eq cn = mycompany ca2
ciscoasa(config)#
ciscoasa(config)# sh run crypto ca trustpool policy
crypto ca trustpool policy
auto-import url http://www.thawte.com
revocation-check none
match certificate map2 allow expired-certificate
match certificate map1 skip revocation-check
crl cache-time 123
crl enforcenextupdate
auto-import
auto-import url http://www.thawte.com
auto-import time 22:00:00
ciscoasa(config)#
ciscoasa# show crypto ca trustpool policy
800 trustpool certificates installed
Trustpool auto import statistics:
  Last import result: SUCCESS
```

```
Next scheduled import at 22:00:00 Tues Jul 21 2015
Trustpool Policy
Trustpool revocation checking is disabled
CRL cache time: 123 seconds
CRL next update field: required and forced
Automatic import of trustpool certificates is enabled
Automatic import URL: http://www.thawte.com
Download time: 22:00:00
Policy overrides:
map: map1
match: issuer-name eq cn=Mycompany Manufacturing CA
match: issuer-name eq cn=Mycompany CA
action: skip revocation-check
map: map2
match: issuer-name eq cn=mycompany Manufacturing CA
match: issuer-name eq cn=mycompany CA2
action: allowed expired certificates
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ca trustpool policy	Enters a submode that provides the commands that define the trustpool policy.

show crypto debug-condition

To display the currently configured filters, the unmatched states, and the error states for IPsec and ISAKMP debugging messages, use the **show crypto debug-condition** command in global configuration mode.

show crypto debug-condition

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

8.0(2) This command was added.

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

Examples

The following example shows the filtering conditions:

```
ciscoasa(config)# show crypto debug-condition
Crypto conditional debug is turned ON
IKE debug context unmatched flag: OFF
IPsec debug context unmatched flag: ON
IKE peer IP address filters:
1.1.1.0/24 2.2.2.2
IKE user name filters:
my_user
```

Related Commands

Command	Description
debug crypto condition	Sets filtering conditions for IPsec and ISAKMP debugging messages.
debug crypto condition error	Shows debugging messages whether or not filtering conditions have been specified.
debug crypto condition unmatched	Shows debugging messages for IPsec and ISAKMP that do not include sufficient context information for filtering.

show crypto ikev1 sa

To display the IKEv1 runtime SA database, use the **show crypto ikev1 sa** command in global configuration mode or privileged EXEC mode.

show crypto ikev1 sa [**detail**]

Syntax Description **detail** Displays detailed output about the SA database.

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	—
Privileged EXEC	• 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 output from this command includes the following fields:

Detail not specified.

IKE Peer	Type	Dir	Rly	State
209.165.200.225	L2L	Init	No	MM_Active

Detail specified.

IKE Peer	Type	Dir	Rly	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

Examples

The following example, entered in global configuration mode, displays detailed information about the SA database:

```

ciscoasa(config)# show crypto ikev1 sa detail
IKE Peer  Type  Dir  Rky  State  Encrypt Hash  Auth  Lifetime
1 209.165.200.225 User  Resp No  AM_Active 3des  SHA  preshrd 86400
IKE Peer  Type  Dir  Rky  State  Encrypt Hash  Auth  Lifetime
2 209.165.200.226 User  Resp No  AM_ACTIVE 3des  SHA  preshrd 86400
IKE Peer  Type  Dir  Rky  State  Encrypt Hash  Auth  Lifetime
3 209.165.200.227 User  Resp No  AM_ACTIVE 3des  SHA  preshrd 86400
IKE Peer  Type  Dir  Rky  State  Encrypt Hash  Auth  Lifetime
4 209.165.200.228 User  Resp No  AM_ACTIVE 3des  SHA  preshrd 86400
ciscoasa(config)#

```

Related Commands

Command	Description
show crypto ikev2 sa	Displays the IKEv2 runtime SA database.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto ikev2 sa

To display the IKEv2 runtime SA database, use the **show crypto ikev2 sa** command in global configuration mode or privileged EXEC mode.

show crypto ikev2 sa [**detail**]

Syntax Description **detail** Displays detailed output about the SA database.

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	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History	Release	Modification
	8.4(1)	This command was added.
	9.0(1)	Support for multiple context mode was added.
	9.19(1)	Dual-stack support for IKEv2 third-party clients is added. Number of traffic selectors that a child SA can store is extended to 2 traffic selectors.
	9.20(1)	Multiple key exchanges for IKEv2 policy.

Usage Guidelines The output from this command includes the following fields:

Detail not specified.

IKE Peer	Type	Dir	Rly	State
209.165.200.225	L2L	Init	No	MM_Active

Detail specified.

IKE Peer	Type	Dir	Rly	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

Examples

The following example, entered in global configuration mode, displays detailed information about the SA database:

```
ciscoasa(config)# show crypto ikev2 sa detail
IKEv2 SAs:
Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id          Local          Remote        Status        Role
671069399          10.0.0.0/500  10.255.255.255/500  READY        INITIATOR
    Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
    Additional Key Exchange Group: AKE1: 31 AKE2: 21 AKE3: 20 AKE4: 19 AKE5: 16 AKE6: 15
    AKE7: 14
    Life/Active Time: 86400/188 sec
    Session-id: 1
    Status Description: Negotiation done
    Local spi: 80173A0373C2D403      Remote spi: AE8AEFA1B97DBB22
    Local id: asa
    Remote id: asal
    Local req mess id: 8              Remote req mess id: 7
    Local next mess id: 8            Remote next mess id: 7
    Local req queued: 8              Remote req queued: 7
    Local window: 1                 Remote window: 1
    DPD configured for 10 seconds, retry 2
    NAT-T is not detected
    Mobile is enabled
    Assigned host addr: 192.168.0.12
    Assigned host addr IPv6: 2001:db8::2
    IKEv2 Fragmentation Configured MTU:576 bytes, Overhead: 28 bytes, Effective MTU: 548
    bytes
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
                        ::/0- ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:/65535
    remote selector  192.186.0.12/0 - 192.186.0.12/65535
                        2001:db8::2/0- 2001:db8::2/65535
    ESP spi in/out: 0x242a3da5/0xe6262034
    AH spi in/out: 0x0/0x0
    CPI in/out: 0x0/0x0
    Encr: AES-GCM, keysize: 128, esp_hmac: N/A
    ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

Related Commands

Command	Description
show crypto ikev1 sa	Displays the IKEv1 runtime SA database.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto ikev2 stats

To display the IKEv2 runtime statistics use the **show crypto ikev2 stats** command in global configuration mode or privileged EXEC mode.

show crypto ikev2 stats

Syntax Description

This command has no keywords or variables.

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	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release Modification

8.4(1) This command was added.

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

9.9(1) Local IKEv2 statistics are now provided

Usage Guidelines

The local output from this command is:

```
Global IKEv2 Statistics
Active Tunnels:                0
Previous Tunnels:              0
In Octets:                     0
In Packets:                    0
In Drop Packets:               0
In Drop Fragments:            0
In Notifys:                    0
In P2 Exchange:               0
In P2 Exchange Invalids:      0
In P2 Exchange Rejects:       0
In IPSEC Delete:              0
In IKE Delete:                 0
Out Octets:                    0
Out Packets:                   0
Out Drop Packets:              0
Out Drop Fragments:           0
```

show crypto ikev2 stats

```

Out Notifys: 0
Out P2 Exchange: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out IPSEC Delete: 0
Out IKE Delete: 0
SAs Locally Initiated: 0
SAs Locally Initiated Failed: 0
SAs Remotely Initiated: 0
SAs Remotely Initiated Failed: 0
System Capacity Failures: 0
Authentication Failures: 0
Decrypt Failures: 0
Hash Failures: 0
Invalid SPI: 0
In Configs: 0
Out Configs: 0
In Configs Rejects: 0
Out Configs Rejects: 0
Previous Tunnels: 0
Previous Tunnels Wraps: 0
In DPD Messages: 0
Out DPD Messages: 0
Out NAT Keepalives: 0
IKE Rekey Locally Initiated: 0
IKE Rekey Remotely Initiated: 0
Locally Initiated IKE Rekey Rejected: 0
Remotely Initiated IKE Rekey Rejected: 0
CHILD Rekey Locally Initiated: 0
CHILD Rekey Remotely Initiated: 0

IKEV2 Call Admission Statistics
Max Active SAs: No Limit
Max In-Negotiation SAs: 15000
Cookie Challenge Threshold: Never
Active SAs: 0
In-Negotiation SAs: 0
Incoming Requests: 0
Incoming Requests Accepted: 0
Incoming Requests Rejected: 0
Outgoing Requests: 0
Outgoing Requests Accepted: 0
Outgoing Requests Rejected: 0
Rejected Requests: 0
Rejected Over Max SA limit: 0
Rejected Low Resources: 0
Rejected Reboot In Progress: 0
Cookie Challenges: 0
Cookie Challenges Passed: 0
Cookie Challenges Failed: 0

```

Related Commands

Command	Description
show crypto ikev2 sa	Displays the IKEv1 runtime SA database.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto ipsec df-bit

To display the IPsec do-not-fragment (DF-bit) policy for IPsec packets for a specified interface, use the **show crypto ipsec df-bit** command in global configuration mode and privileged EXEC mode. You can also use the command synonym **show ipsec df-bit**.

show crypto ipsec df-bit *interface*

Syntax Description *interface* Specifies an interface name.

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
Global configuration	• Yes	• Yes	• Yes	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History **Release Modification**

7.0(1) This command was added.

Usage Guidelines The df-bit setting determines how the system handles the do-not-fragment (DF) bit in the encapsulated header. The DF bit within the IP header determines whether or not a device is allowed to fragment a packet. Based on this setting, the system either clears, sets, or copies the DF-bit setting of the clear-text packet to the outer IPsec header when applying encryption.

Examples The following example displays the IPsec DF-bit policy for interface named inside:

```
ciscoasa(config)# show
crypto
ipsec df-bit inside
df-bit inside copy
ciscoasa(config)#
```

Related Commands	Command	Description
	crypto ipsec df-bit	Configures the IPsec DF-bit policy for IPsec packets.

Command	Description
crypto ipsec fragmentation	Configures the fragmentation policy for IPsec packets.
show crypto ipsec fragmentation	Displays the fragmentation policy for IPsec packets.

show crypto ipsec fragmentation

To display the fragmentation policy for IPsec packets, use the **show crypto ipsec fragmentation** command in global configuration or privileged EXEC mode. You can also use the command synonym **show ipsec fragmentation**.

show crypto ipsec fragmentation *interface*

Syntax Description

interface Specifies an interface name.

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	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release Modification

7.0(1) This command was added.

Usage Guidelines

When encrypting packets for a VPN, the system compares the packet length with the MTU of the outbound interface. If encrypting the packet will exceed the MTU, the packet must be fragmented. This command shows whether the system will fragment the packet after encrypting it (after-encryption), or before encrypting it (before-encryption). Fragmenting the packet before encryption is also called prefragmentation, and is the default system behavior because it improves overall encryption performance.

Examples

The following example, entered in global configuration mode, displays the IPsec fragmentation policy for an interface named inside:

```
ciscoasa(config)# show crypto ipsec fragmentation inside
fragmentation inside before-encryption
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ipsec fragmentation	Configures the fragmentation policy for IPsec packets.
crypto ipsec df-bit	Configures the DF-bit policy for IPsec packets.

Command	Description
show crypto ipsec df-bit	Displays the DF-bit policy for a specified interface.

show crypto ipsec policy

To display IPsec secure socket API (SS API) security policy configured for OSPFv3, use the **show crypto ipsec policy** command in global configuration or privileged EXEC mode. You can also use the alternate form of this command: **show ipsec policy**.

show crypto ipsec policy

Syntax Description

This command has no keywords or variables.

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	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release Modification

9.0(1) This command was added.

Examples

The following example shows the OSPFv3 authentication and encryption policy.

```
ciscoasa# show crypto ipsec policy

Crypto IPsec client security policy data
Policy name:      OSPFv3-1-256
Policy refcount:  1
Policy flags:     0x00000000
SA handles:      sess 268382208 (0xffff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound  ESP SPI:      256 (0x100)
Outbound ESP SPI:     256 (0x100)
Inbound  ESP Auth Key: 12345678901234567890123456789012345678901234567890
Outbound ESP Auth Key: 12345678901234567890123456789012345678901234567890
Inbound  ESP Cipher Key: 123456789012345678901234567890123456789012
Outbound ESP Cipher Key: 123456789012345678901234567890123456789012
Transform set:     esp-aes esp-sha-hmac
```

Related Commands

Command	Description
ipv6 ospf encryption	Configures the authentication and encryption policy for OSPFv3.
show crypto sockets	Displays secure socket information.

Command	Description
show ipv6 ospf interface	Displays information about OSPFv3 interfaces.

show crypto ipsec sa

To display a list of IPsec SAs, use the **show crypto ipsec sa** command in global configuration mode or privileged EXEC mode. You can also use the alternate form of this command: **show ipsec sa** .

show crypto ipsec sa [**entry** | **identity** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

Syntax Description	detail	(Optional) Displays detailed error information on what is displayed.
	entry	(Optional) Displays IPsec SAs sorted by peer address
	identity	(Optional) Displays IPsec SAs for sorted by identity, not including ESPs. This is a condensed form.
	map <i>map-name</i>	(Optional) Displays IPsec SAs for the specified crypto map.
	peer <i>peer-addr</i>	(Optional) Displays IPsec SAs for specified peer IP addresses.

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	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release Modification

7.0(1) This command was added.

9.0(1) Support for OSPFv3, multiple context mode, Suite B algorithm in the transform and IV size portion, and ESPV3 IPsec output were added.

9.13(1) The following new counters was added for troubleshooting errors in *show crypto ipsec sa detail* :

- **#pkts invalid ip version (send)**
- **#pkts invalid length (send)**
- **#pkts invalid ctx (send) and #pkts invalid ctx (rcv)**
- **#pkts invalid ifc (send) and #pkts invalid ifc (rcv)**
- **#pkts failed (send) and #pkts failed (rcv)**

Release Modification

9.19(1) Dual-stack support for IKEv2 third-party clients is added. Number of traffic selectors that inbound and outbound IPsec SA can support is extended to 2 traffic selectors.

Examples

The following example, entered in global configuration mode, displays IPsec SAs that include a tunnel identified as OSPFv3.

```
ciscoasa(config)# show crypto ipsec sa
interface: outside2
  Crypto map tag: def, local addr: 10.132.0.17
    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
    local ident (addr/mask/prot/port): (::/0/0/0)
    remote ident (addr/mask/prot/port): (3000::1/128/0/0)
    current_peer: 172.20.0.21
    dynamic allocated peer ip: 10.135.1.5
    dynamic allocated peer ip(ipv6): 3000::1
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
    #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
    #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
    #send errors: 0, #recv errors: 0
    local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21
    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: DC15BF68
  inbound esp sas:
    spi: 0x1E8246FC (511854332)
      transform: esp-3des esp-md5-hmac
      in use settings ={L2L, Transport, Manual key, (OSPFv3), }
      slot: 0, conn_id: 3, crypto-map: def
      sa timing: remaining key lifetime (sec): 548
      IV size: 8 bytes
      replay detection support: Y
  outbound esp sas:
    spi: 0xDC15BF68 (3692412776)
      transform: esp-3des esp-md5-hmac
      in use settings ={L2L, Transport, Manual key, (OSPFv3), }
      slot: 0, conn_id: 3, crypto-map: def
      sa timing: remaining key lifetime (sec): 548
      IV size: 8 bytes
      replay detection support: Y
  Crypto map tag: def, local addr: 10.132.0.17
    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
ciscoasa(config)#
```



Note Fragmentation statistics are pre-fragmentation statistics if the IPsec SA policy states that fragmentation occurs before IPsec processing. Post-fragmentation statistics appear if the SA policy states that fragmentation occurs after IPsec processing.

The following example, entered in global configuration mode, shows IPsec SAs for the keyword detail with the newly added counters to troubleshoot the errors in the traffic.

```
(config)# sh ipsec sa det
interface: outside
```

```

Crypto map tag: outside_map, seq num: 10, local addr: 10.86.94.103
  access-list toASA-5525 extended permit ip host 10.86.94.103 host 10.86.95.135
  local ident (addr/mask/prot/port): (10.86.94.103/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (10.86.95.135/255.255.255.255/0/0)
  local ident (addr/mask/prot/port): (::/0/0/0)
  remote ident (addr/mask/prot/port): (3000::1/128/0/0)
  current_peer: 10.86.95.135
  dynamic allocated peer ip: 10.86.95.135
  dynamic allocated peer ip(ipv6): 3000::1
  #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
  #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
  #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
  #pkts invalid prot (rcv): 0, #pkts verify failed: 0
  #pkts invalid identity (rcv): 0
  #pkts invalid pad (rcv): 0
  #pkts invalid ip version (send): 0, #pkts invalid ip version (rcv): 0
  #pkts invalid len (send): 0, #pkts invalid len (rcv): 0
  #pkts invalid ctx (send): 0, #pkts invalid ctx (rcv): 0
  #pkts invalid ifc (send): 0, #pkts invalid ifc (rcv): 0
  #pkts failed (send): 0, #pkts failed (rcv): 0
  #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
  #pkts replay failed (rcv): 0
  #pkts min mtu frag failed (send): 0, #pkts bad frag offset (rcv): 0
  #pkts internal err (send): 0, #pkts internal err (rcv): 0

local crypto endpt.: 10.86.94.103/500, remote crypto endpt.: 10.86.95.135/500
path mtu 1500, ipsec overhead 94(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 25356578
current inbound spi : A1029CE2
inbound esp sas:
  spi: 0xA1029CE2 (2701303010)
    SA State: active
    transform: esp-aes esp-sha-512-hmac no compression
    in use settings ={L2L, Tunnel, IKEv2, }
    slot: 0, conn_id: 195272704, crypto-map: outside_map
    sa timing: remaining key lifetime (kB/sec): (3962879/28782)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
      0x00000000 0x0000001F
outbound esp sas:
  spi: 0x25356578 (624256376)
    SA State: active
    transform: esp-aes esp-sha-512-hmac no compression
    in use settings ={L2L, Tunnel, IKEv2, }
    slot: 0, conn_id: 195272704, crypto-map: outside_map
    sa timing: remaining key lifetime (kB/sec): (4193279/28772)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
      0x00000000 0x00000001

```

The following example, entered in global configuration mode, displays IPsec SAs for a crypto map named def.

```

ciscoasa(config)# show crypto ipsec sa map def
cryptomap: def
  Crypto map tag: def, local addr: 172.20.0.17
    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
    local ident (addr/mask/prot/port): (::/0/0/0)
    remote ident (addr/mask/prot/port): (3000::1/128/0/0)
    current_peer: 10.132.0.21
    dynamic allocated peer ip: 90.135.1.5
    dynamic allocated peer ip(ipv6): 3000::1
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
    #send errors: 0, #recv errors: 0
    local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: DC15BF68
  inbound esp sas:
    spi: 0x1E8246FC (511854332)
      transform: esp-3des esp-md5-hmac
      in use settings =(RA, Tunnel, )
      slot: 0, conn_id: 3, crypto-map: def
      sa timing: remaining key lifetime (sec): 480
      IV size: 8 bytes
      replay detection support: Y
  outbound esp sas:
    spi: 0xDC15BF68 (3692412776)
      transform: esp-3des esp-md5-hmac
      in use settings =(RA, Tunnel, )
      slot: 0, conn_id: 3, crypto-map: def
      sa timing: remaining key lifetime (sec): 480
      IV size: 8 bytes
      replay detection support: Y
  Crypto map tag: def, local addr: 172.20.0.17
    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
    local ident (addr/mask/prot/port): (::/0/0/0)
    remote ident (addr/mask/prot/port): (3001:db8::1/128/0/0)
    current_peer: 10.135.1.8
    dynamic allocated peer ip: 0.0.0.0
    dynamic allocated peer ip(ipv6): 3001:db8::1
    #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
    #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
    #send errors: 0, #recv errors: 0
    local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: 3B6F6A35
  inbound esp sas:
    spi: 0xB32CF0BD (3006066877)
      transform: esp-3des esp-md5-hmac
      in use settings =(RA, Tunnel, )
      slot: 0, conn_id: 4, crypto-map: def
      sa timing: remaining key lifetime (sec): 263
      IV size: 8 bytes
      replay detection support: Y
  outbound esp sas:
    spi: 0x3B6F6A35 (997157429)
      transform: esp-3des esp-md5-hmac
      in use settings =(RA, Tunnel, )
      slot: 0, conn_id: 4, crypto-map: def

```

```

sa timing: remaining key lifetime (sec): 263
IV size: 8 bytes
replay detection support: Y
ciscoasa(config)#

```

The following example, entered in global configuration mode, shows IPsec SAs for the keyword entry .

```

ciscoasa(config)# show crypto ipsec sa entry
peer address: 10.132.0.21
Crypto map tag: def, local addr: 172.20.0.17
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
local ident (addr/mask/prot/port): (::/0/0/0)
remote ident (addr/mask/prot/port): (3000::1/128/0/0)
current_peer: 10.132.0.21
dynamic allocated peer ip: 90.135.1.5
dynamic allocated peer ip(ipv6): 3000::1
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0
local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: DC15BF68
inbound esp sas:
spi: 0x1E8246FC (511854332)
transform: esp-3des esp-md5-hmac
in use settings =(RA, Tunnel, )
slot: 0, conn_id: 3, crypto-map: def
sa timing: remaining key lifetime (sec): 429
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0xDC15BF68 (3692412776)
transform: esp-3des esp-md5-hmac
in use settings =(RA, Tunnel, )
slot: 0, conn_id: 3, crypto-map: def
sa timing: remaining key lifetime (sec): 429
IV size: 8 bytes
replay detection support: Y
peer address: 10.135.1.8
Crypto map tag: def, local addr: 172.20.0.17
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
local ident (addr/mask/prot/port): (::/0/0/0)
remote ident (addr/mask/prot/port): (3001:db8::1/128/0/0)
current_peer: 10.135.1.8
dynamic allocated peer ip: 0.0.0.0
dynamic allocated peer ip(ipv6): 3001:db8::1
#pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
#pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0
local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 3B6F6A35
inbound esp sas:
spi: 0xB32CF0BD (3006066877)
transform: esp-3des esp-md5-hmac
in use settings =(RA, Tunnel, )

```

```

    slot: 0, conn_id: 4, crypto-map: def
    sa timing: remaining key lifetime (sec): 212
    IV size: 8 bytes
    replay detection support: Y
  outbound esp sas:
    spi: 0x3B6F6A35 (997157429)
    transform: esp-3des esp-md5-hmac
    in use settings =(RA, Tunnel, )
    slot: 0, conn_id: 4, crypto-map: def
    sa timing: remaining key lifetime (sec): 212
    IV size: 8 bytes
    replay detection support: Y
ciscoasa(config)#

```

The following example, entered in global configuration mode, shows IPsec SAs with the keywords **entry detail**.

```

ciscoasa(config)# show crypto ipsec sa entry detail
peer address: 10.132.0.21
  Crypto map tag: def, local addr: 172.20.0.17
    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
    local ident (addr/mask/prot/port): (::/0/0/0)
    remote ident (addr/mask/prot/port): (3000::1/128/0/0)
    current_peer: 10.132.0.21
    dynamic allocated peer ip: 90.135.1.5
    dynamic allocated peer ip(ipv6): 3000::1
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
    #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
    #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
    #pkts invalid prot (rcv): 0, #pkts verify failed: 0
    #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
    #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
    #pkts replay failed (rcv): 0
    #pkts internal err (send): 0, #pkts internal err (rcv): 0
    local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: DC15BF68
  inbound esp sas:
    spi: 0x1E8246FC (511854332)
    transform: esp-3des esp-md5-hmac
    in use settings =(RA, Tunnel, )
    slot: 0, conn_id: 3, crypto-map: def
    sa timing: remaining key lifetime (sec): 322
    IV size: 8 bytes
    replay detection support: Y
  outbound esp sas:
    spi: 0xDC15BF68 (3692412776)
    transform: esp-3des esp-md5-hmac
    in use settings =(RA, Tunnel, )
    slot: 0, conn_id: 3, crypto-map: def
    sa timing: remaining key lifetime (sec): 322
    IV size: 8 bytes
    replay detection support: Y
peer address: 10.135.1.8
  Crypto map tag: def, local addr: 172.20.0.17
    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
    local ident (addr/mask/prot/port): (::/0/0/0)
    remote ident (addr/mask/prot/port): (3001:db8::1/128/0/0)

```

```

current_peer: 10.135.1.8
dynamic allocated peer ip: 0.0.0.0
dynamic allocated peer ip(ipv6): 3001:db8::1
#pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
#pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
#pkts no sa (send): 0, #pkts invalid sa (rcv): 0
#pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
#pkts invalid prot (rcv): 0, #pkts verify failed: 0
#pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
#pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv): 0
local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 3B6F6A35
inbound esp sas:
spi: 0xB32CF0BD (3006066877)
  transform: esp-3des esp-md5-hmac
  in use settings ={RA, Tunnel, }
  slot: 0, conn_id: 4, crypto-map: def
  sa timing: remaining key lifetime (sec): 104
  IV size: 8 bytes
  replay detection support: Y
outbound esp sas:
spi: 0x3B6F6A35 (997157429)
  transform: esp-3des esp-md5-hmac
  in use settings ={RA, Tunnel, }
  slot: 0, conn_id: 4, crypto-map: def
  sa timing: remaining key lifetime (sec): 104
  IV size: 8 bytes
  replay detection support: Y
ciscoasa(config)#

```

The following example shows IPsec SAs with the keyword **identity** .

```

ciscoasa(config)# show crypto ipsec sa identity
interface: outside2
Crypto map tag: def, local addr: 172.20.0.17
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
local ident (addr/mask/prot/port): (::/0/0/0)
remote ident (addr/mask/prot/port): (3000::1/128/0/0)
current_peer: 10.132.0.21
dynamic allocated peer ip: 90.135.1.5
dynamic allocated peer ip(ipv6): 3000::1
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0
local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: DC15BF68
Crypto map tag: def, local addr: 172.20.0.17
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
local ident (addr/mask/prot/port): (::/0/0/0)
remote ident (addr/mask/prot/port): (3001:db8::1/128/0/0)
current_peer: 10.135.1.8
dynamic allocated peer ip: 0.0.0.0
dynamic allocated peer ip(ipv6): 3001:db8::1
#pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756

```

```

#pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #rcv errors: 0
local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 3B6F6A35

```

The following example shows IPsec SAs with the keywords **identity** and **detail**.

```

ciscoasa(config)# show crypto ipsec sa identity detail
interface: outside2
  Crypto map tag: def, local addr: 172.20.0.17
    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
    local ident (addr/mask/prot/port): (::/0/0/0)
    remote ident (addr/mask/prot/port): (3000::1/128/0/0)
    current_peer: 10.132.0.21
    dynamic allocated peer ip: 90.135.1.5
    dynamic allocated peer ip(ipv6): 3000::1
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
    #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
    #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
    #pkts invalid prot (rcv): 0, #pkts verify failed: 0
    #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
    #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
    #pkts replay failed (rcv): 0
    #pkts internal err (send): 0, #pkts internal err (rcv): 0
    local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: DC15BF68
  Crypto map tag: def, local addr: 172.20.0.17
    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
    local ident (addr/mask/prot/port): (::/0/0/0)
    remote ident (addr/mask/prot/port): (3001:db8::1/128/0/0)
    current_peer: 10.135.1.8
    dynamic allocated peer ip: 0.0.0.0
    dynamic allocated peer ip(ipv6): 3001:db8:1
    #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
    #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
    #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
    #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
    #pkts invalid prot (rcv): 0, #pkts verify failed: 0
    #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
    #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
    #pkts replay failed (rcv): 0
    #pkts internal err (send): 0, #pkts internal err (rcv): 0
    local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: 3B6F6A35

```

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.

Command	Description
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA.
show running-config isakmp	Displays all the active ISAKMP configuration.

show crypto ipsec stats

To display a list of IPsec statistics, use the **show crypto ipsec stats** command in global configuration mode or privileged EXEC mode.

show crypto ipsec stats

Syntax Description

This command has no keywords or variables.

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	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release Modification

7.0(1) This command was added.

Examples

The following example, entered in global configuration mode, displays IPsec statistics:

```
ciscoasa(config)# show crypto ipsec stats
IPsec Global Statistics
-----
Active tunnels: 2
Previous tunnels: 9
Inbound
  Bytes: 4933013
  Decompressed bytes: 4933013
  Packets: 80348
  Dropped packets: 0
  Replay failures: 0
  Authentications: 80348
  Authentication failures: 0
  Decryptions: 80348
  Decryption failures: 0
  Decapsulated fragments needing reassembly: 0
Outbound
  Bytes: 4441740
  Uncompressed bytes: 4441740
  Packets: 74029
  Dropped packets: 0
```

```

Authentications: 74029
Authentication failures: 0
Encryptions: 74029
Encryption failures: 0
Fragmentation successes: 3
  Pre-fragmentation successes:2
  Post-fragmentation successes: 1
Fragmentation failures: 2
  Pre-fragmentation failures:1
  Post-fragmentation failures: 1
Fragments created: 10
PMTUs sent: 1
PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
ciscoasa(config)#

```

Related Commands

Command	Description
clear ipsec sa	Clears IPsec SAs or counters based on specified parameters.
crypto ipsec transform-set	Defines a transform set.
show ipsec sa	Displays IPsec SAs based on specified parameters.
show ipsec sa summary	Displays a summary of IPsec SAs.

Examples

The following example, issued in global configuration mode, displays ISAKMP statistics:

```

ciscoasa(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0

```

```
No Sa Fails: 0  
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto isakmp sa

To display the IKE runtime SA database, use the **show crypto isakmp sa** command in global configuration mode or privileged EXEC mode.

show crypto isakmp sa [detail]

Syntax Description **detail** Displays detailed output about the SA database.

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
	7.0(1)	The show isakmp sa command was added.
	7.2(1)	This show isakmp sa command was deprecated. The show crypto isakmp sa command replaced it.
	9.0(1)	Support for multiple context mode was added.

Usage Guidelines The output from this command includes the following fields:

Detail not specified

IKE Peer 209.165.200.225

Type—L2L or User

Dir—Init

Rky—No or Yes. If yes, a rekey is occurring, and a second matching SA will be in a different state until the rekey completes.

Role—Initiator or Responder State. Tells the current state of the state machine for the SA.

State—A tunnel up and passing data has a value of either MM_ACTIVE or AM_ACTIVE. Other active states include MM_BLD_MSG4, MM_BLD_MSG6, MM_FREE, MM_SND_MSG6_H, MM_START,

MM_TM_INIT_MODECFG_H, MM_TM_PEND_QM, MM_WAIT_DELETE, MM_WAIT_MSG3, MM_WAIT_MSG5, and so on.

Detail specified

IKE Peer 209.165.200.225

Type—L2L or User

Dir—Init

Rky—No or Yes. If yes, a rekey is occurring, and a second matching SA will be in a different state until the rekey completes.

Role—Initiator or Responder State. Tells the current state of the state machine for the SA. A tunnel up and passing data has a value of either MM_ACTIVE or AM_ACTIVE.

State—Other than MM_ACTIVE or AM_ACTIVE, other active states include MM_BLD_MSG4, MM_BLD_MSG6, MM_FREE, MM_SND_MSG6_H, MM_START, MM_TM_INIT_MODECFG_H, MM_TM_PEND_QM, MM_WAIT_DELETE, MM_WAIT_MSG3, MM_WAIT_MSG5, and so on.

Encrypt—3des

Hash—md5

Auth—preshrd

Lifetime—86400

Examples

The following example, entered in global configuration mode, displays detailed information about the SA database:

```
ciscoasa(config)# show crypto isakmp sa detail
IKE Peer  Type Dir  Rky State      Encrypt Hash  Auth  Lifetime
1 209.165.200.225 User Resp No  AM_Active 3des  SHA  preshrd 86400
IKE Peer  Type Dir  Rky State      Encrypt Hash  Auth  Lifetime
2 209.165.200.226 User Resp No  AM_ACTIVE 3des  SHA  preshrd 86400
IKE Peer  Type Dir  Rky State      Encrypt Hash  Auth  Lifetime
3 209.165.200.227 User Resp No  AM_ACTIVE 3des  SHA  preshrd 86400
IKE Peer  Type Dir  Rky State      Encrypt Hash  Auth  Lifetime
4 209.165.200.228 User Resp No  AM_ACTIVE 3des  SHA  preshrd 86400
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto isakmp stats

To display runtime statistics, use the **show crypto isakmp stats** command in global configuration mode or privileged EXEC mode.

show crypto isakmp stats

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

7.0(1) The **show isakmp stats** command was added.

7.2(1) The **show isakmp stats** command was deprecated. The **show crypto isakmp stats** command replaced it.

Usage Guidelines

The output from this command includes the following fields:

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests

- Out Octets
- Out Packets
- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

Examples

The following example, issued in global configuration mode, displays ISAKMP statistics:

```
ciscoasa(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
```



```
No Sa Fails: 0  
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto key mypubkey

To display the default keys (called "mypubkey") and information about the keys, use the **show crypto key mypubkey** command in privileged EXEC mode.

```
show crypto key mypubkey { ecdsa | eddsa | rsa }
```

Syntax Description

ecdsa Specifies the key type as ECDSA.

eddsa Specifies the key type as EDDSA.

rsa Specifies the key type as RSA.

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.

9.0(1) Support for ECDSA keys was added.

9.16(1) Support for EDDSA keys was added.

Related Commands

Command	Description
crypto key generate	Creates key pairs.
crypto key zeroize	Removes key pairs.

show crypto protocol statistics

To display the protocol-specific statistics in the crypto accelerator MIB, use the **show crypto protocol statistics** command in global configuration or privileged EXEC mode.

show crypto protocol statistics *protocol*

Syntax Description

protocol Specifies the name of the protocol for which to display statistics. Protocol choices are as follows:

ikev1—Internet Key Exchange version 1.

ipsec—IP Security Phase-2 protocols.

ssl—Secure Sockets Layer.

other—Reserved for new protocols.

all—All protocols currently supported.

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	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release Modification

7.0(1) This command was added.

Examples

The following examples entered in global configuration mode, display crypto accelerator statistics for specified protocols:

```
ciscoasa
#
show crypto protocol statistics ikev1
[IKEv1 statistics]
  Encrypt packet requests: 39
  Encapsulate packet requests: 39
  Decrypt packet requests: 35
  Decapsulate packet requests: 35
  HMAC calculation requests: 84
```

```

    SA creation requests: 1
    SA rekey requests: 3

SA deletion requests: 2
    Next phase key allocation requests: 2
    Random number generation requests: 0

Failed requests: 0
ciscoasa
#
show crypto protocol statistics ipsec
[IPsec statistics]
    Encrypt packet requests: 700
    Encapsulate packet requests: 700
    Decrypt packet requests: 700
    Decapsulate packet requests: 700
    HMAC calculation requests: 1400
    SA creation requests: 2
    SA rekey requests: 0
    SA deletion requests: 0
    Next phase key allocation requests: 0
    Random number generation requests: 0
    Failed requests: 0
ciscoasa
#
show crypto protocol statistics ssl
[SSL statistics]
    Encrypt packet requests: 0
    Encapsulate packet requests: 0
    Decrypt packet requests: 0
    Decapsulate packet requests: 0
    HMAC calculation requests: 0
    SA creation requests: 0
    SA rekey requests: 0
    SA deletion requests: 0
    Next phase key allocation requests: 0
    Random number generation requests: 0
    Failed requests: 0
ciscoasa
#
show crypto protocol statistics other
[Other statistics]
    Encrypt packet requests: 0
    Encapsulate packet requests: 0
    Decrypt packet requests: 0
    Decapsulate packet requests: 0
    HMAC calculation requests: 0
    SA creation requests: 0
    SA rekey requests: 0
    SA deletion requests: 0
    Next phase key allocation requests: 0
    Random number generation requests: 99
    Failed requests: 0
ciscoasa
#
show crypto protocol statistics all
[IKEv1 statistics]
    Encrypt packet requests: 46
    Encapsulate packet requests: 46
    Decrypt packet requests: 40
    Decapsulate packet requests: 40
    HMAC calculation requests: 91

```

```
SA creation requests: 1
SA rekey requests: 3
SA deletion requests: 3
Next phase key allocation requests: 2
Random number generation requests: 0
Failed requests: 0
[IKEv2 statistics]
  Encrypt packet requests: 0
  Encapsulate packet requests: 0

Decrypt packet requests: 0
  Decapsulate packet requests: 0
  HMAC calculation requests: 0
  SA creation requests: 0
  SA rekey requests: 0
  SA deletion requests: 0
  Next phase key allocation requests: 0
  Random number generation requests: 0
  Failed requests: 0
[IPsec statistics]
  Encrypt packet requests: 700
  Encapsulate packet requests: 700

Decrypt packet requests: 700
  Decapsulate packet requests: 700
  HMAC calculation requests: 1400
  SA creation requests: 2
  SA rekey requests: 0
  SA deletion requests: 0
  Next phase key allocation requests: 0
  Random number generation requests: 0
  Failed requests: 0
[SSL statistics]
  Encrypt packet requests: 0
  Encapsulate packet requests: 0
  Decrypt packet requests: 0
  Decapsulate packet requests: 0
  HMAC calculation requests: 0
  SA creation requests: 0
  SA rekey requests: 0
  SA deletion requests: 0
  Next phase key allocation requests: 0
  Random number generation requests: 0
  Failed requests: 0
[SSH statistics are not supported]
[SRTP statistics are not supported]
[Other statistics]
  Encrypt packet requests: 0
  Encapsulate packet requests: 0
  Decrypt packet requests: 0
  Decapsulate packet requests: 0

HMAC calculation requests: 0
SA creation requests: 0
SA rekey requests: 0
SA deletion requests: 0
Next phase key allocation requests: 0
Random number generation requests: 99
Failed requests: 0
ciscoasa #
```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto accelerator statistics	Displays the global and accelerator-specific statistics from the crypto accelerator MIB.

show crypto sockets

To display crypto secure socket information, use the **show crypto sockets** command in global configuration mode or privileged EXEC mode.

show crypto sockets

Syntax Description

This command has no keywords or variables.

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	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release Modification

7.0(1) This command was added.

Examples

The following example, entered in global configuration mode, displays crypto secure socket information:

```
ciscoasa(config)# show crypto sockets
Number of Crypto Socket connections 1
  Gi0/1 Peers: (local): 2001:1::1
           (remote): ::
           Local Ident (addr/plen/port/prot): (2001:1::1/64/0/89)
           Remote Ident (addr/plen/port/prot): (::/0/0/89)
           IPsec Profile: "CSSU-UTF"
           Socket State: Open
           Client: "CSSU_App(UTF)" (Client State: Active)
Crypto Sockets in Listen state:
```

The following table describes the fields in the **show crypto sockets** command output.

Field	Description
Number of Crypto Socket connections	Number of crypto sockets in the system.

Field	Description
Socket State	This state can be Open, which means that active IPsec security associations (SAs) exist, or it can be Closed, which means that no active IPsec SAs exist.
Client	Application name and its state.
Flags	If this field says “shared,” the socket is shared with more than one tunnel interface.
Crypto Sockets in Listen state	Name of the crypto IPsec profile.

Related Commands

Command	Description
show crypto ipsec policy	Displays the crypto secure socket API installed policy information.

show csc node-count

To display the number of nodes for which the CSC SSM scanned traffic, use the **show csc node-count** command in privileged EXEC mode:

```
show csc node-count [ yesterday ]
```

Syntax Description

yesterday (Optional) Shows the number of nodes for which the CSC SSM scanned traffic in the preceding 24-hour period, from midnight to midnight.

Command Default

By default, the node count displayed is the number of nodes scanned since midnight.

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

A node is any distinct source IP address or the address of a device that is on a network protected by the ASA. The ASA keeps track of a daily node count and communicates this to the CSC SSM for user license enforcement.

Examples

The following is sample output of the **show csc node-count** command, which displays the number of nodes for which the CSC SSM has scanned traffic since midnight:

```
ciscoasa# show csc node-count
Current node count is 1
```

The following is sample output of the **show csc node-count** command, which displays the number of nodes for which the CSC SSM scanned traffic in the preceding 24-hour period, from midnight to midnight:

```
ciscoasa(config)# show csc node-count yesterday
Yesterday's node count is 2
```

Related Commands

csc	Sends network traffic to the CSC SSM for scanning of FTP, HTTP, POP3, and SMTP, as configured on the CSC SSM.
show running-config class-map	Shows current class map configuration.
show running-config policy-map	Shows the current policy map configuration.

show running-config service-policy	Shows the current service policy configuration.
------------------------------------	---

show ctiqbe

To display information about CTIQBE sessions established across the ASA, use the **show ctiqbe** command in privileged EXEC mode.

show ctiqbe

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 ctiqbe** command displays information of CTIQBE sessions established across the ASA. Along with **debug ctiqbe** and **show local-host**, this command is used for troubleshooting CTIQBE inspection engine issues.



Note We recommend that you have the **pager** command configured before using the **show ctiqbe** command. If there are a lot of CTIQBE sessions and the **pager** command is not configured, it can take a while for the **show ctiqbe** command output to reach the end.

Examples

The following is sample output from the **show ctiqbe** command under the following conditions. There is only one active CTIQBE session setup across the ASA. It is established between an internal CTI device (for example, a Cisco IP SoftPhone) at local address 10.0.0.99 and an external Cisco Call Manager at 172.29.1.77, where TCP port 2748 is the Cisco CallManager. The heartbeat interval for the session is 120 seconds.

```
ciscoasa# | show ctiqbe
Total: 1
-----
LOCAL          FOREIGN          STATE  HEARTBEAT
-----
1             10.0.0.99/1117  172.29.1.77/2748  1      120
-----
```

```

RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 - 1029)
-----
MEDIA: Device ID 27      Call ID 0
      Foreign 172.29.1.99  (1028 - 1029)
      Local   172.29.1.88  (26822 - 26823)
-----

```

The CTI device has already registered with the CallManager. The device internal address and RTP listening port is PATed to 172.29.1.99 UDP port 1028. Its RTCP listening port is PATed to UDP 1029.

The line beginning with RTP/RTCP: PAT xlates: appears only if an internal CTI device has registered with an external CallManager and the CTI device address and ports are PATed to that external interface. This line does not appear if the CallManager is located on an internal interface, or if the internal CTI device address and ports are NATed to the same external interface that is used by the CallManager.

The output indicates a call has been established between this CTI device and another phone at 172.29.1.88. The RTP and RTCP listening ports of the other phone are UDP 26822 and 26823. The other phone locates on the same interface as the CallManager because the ASA does not maintain a CTIQBE session record associated with the second phone and CallManager. The active call leg on the CTI device side can be identified with Device ID 27 and Call ID 0.

Related Commands

Commands	Description
inspect ctiqbe	Enables CTIQBE application inspection.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

show ctl-file

To show the contents of the CTL file used by the phone proxy, use the **show ctl-file** command in global configuration mode.

show ctl-file *filename* [**parsed**]

Syntax Description	<i>filename</i> Displays the phones capable of secure mode stored in the database.
	parsed (Optional) Displays detailed information from the CTL file specified.

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	—	—

Command History	Release Modification
	8.2(1) The command was added.

Usage Guidelines When specifying the filename of the CTL file stored in Flash memory, specify the disk number, filename, and extension; for example: `disk0:/testctl.tlv` . Using the **show ctl-file** command is useful for debugging when configuring the phone proxy instance.

Examples The following example shows the use of the **show ctl-file** command to show general information about the CTL file:

```
ciscoasa# show ctl-file
disk0:/ctlfile.tlv

Total Number of Records: 1
CTL Record Number 1
  Subject Name:
    serialNumber=JMX1215L2TX+hostname=ciscoasa
  Issuer Name:
    serialNumber=JMX1215L2TX+hostname=ciscoasa
  Function:
    cucm
  IP Address:
    192.168.52.102
  Associated Trustpoint:
    cucm_primary
```

The following example shows the use of the **show ctl-file** command to show detailed information about the CTL file:

```
ciscoasa# show ctl-file
disk0:/ctlfile.tlv
  parsed
TAG 0x01: Version: Maj 1, Min 2
TAG 0x02: Header Len: Len 288
TAG 0x03: Signer ID: Len 103
TAG 0x04: Signer Name: Len 45 Name: <cn=_internal_myctl_SAST_0,ou=STG,o=Cisco Inc>
TAG 0x05: Cert SN: Len 4 SN: c43c9048
TAG 0x06: CA Name: Len 45 Name: <cn=_internal_myctl_SAST_0,ou=STG,o=Cisco Inc>
TAG 0x07: Signature: Len 15
TAG 0x08: Digest Alg: Len 1 Name: SHA-1
TAG 0x09: Sig Alg Info: Len 8
TAG 0x0A: Sig Alg: Len 1 Name: RSA
TAG 0x0B: Modulus: Len 1 Name: 1024
TAG 0x0C: Sig Block: Len 128 Signature:
521debcbf b7a77ea8 94eba5f7 f3c8b0d8 3337a9fa 267cela7 202b2c8b 2ac980d3
9608f64d e7cd82df e205e5bf 74ald9c4 fae20f90 f3d2746a e90f439e ef93fca7
d4925551 72daa414 2c55f249 ef7e6dc2 bcb9f9b5 39be8238 5011eeeb ce37e4d1
866e6550 6779c3fd 25c8bab0 6e9be32c 7f79fe34 5575e3af ea039145 45ce3158

TAG 0x0E: File Name: Len 12 Name: <CTLFile.tlv>
TAG 0x0F: Timestamp: Len 4 Timestamp: 48903cc6

### CTL RECORD No. 1 ###
TAG 0x01: Rcd Len: Len 731
TAG 0x03: Sub Name: Len 43 Sub Name: <serialNumber=JMX1215L2TX+hostname=ciscoasa>
TAG 0x04: Function: Len 2 Func: CCM
TAG 0x05: Cert Issuer: Len 43 Issuer Name: <serialNumber=JMX1215L2TX+hostname=ciscoasa>
TAG 0x06: Cert SN: Len 4 Cert SN: 15379048
TAG 0x07: Pub Key: Len 140 Pub Key:
30818902 818100ad a752b4e6 89769a49 13115e52 1209b3ef 96a179af 728c29d7
af7fed4e c759d0ea cebd7587 dd4f7c4c 322da86b 3a677c08 ce39ce60 2525f6d2
50fe87cf 2aea60a5 690ec985 10706e5a 30ad26db e6fdb243 159758ed bb487525
f901ef4a 658445de 29981546 3867d2d1 ce519ee4 62c7be32 51037c3c 751c0ad6
040bedbb 3e984502 03010001
TAG 0x09: Cert: Len 469 X.509v3 Cert:
308201d1 3082013a a0030201 02020415 37904830 0d06092a 864886f7 0d010104
0500302d 312b3012 06035504 05130b4a 4d583132 31354c32 54583015 06092a86
4886f70d 01090216 08636973 636f6173 61301e17 0d303830 37333030 39343033
375a170d 31383037 32383039 34303337 5a302d31 2b301206 03550405 130b4a4d
58313231 354c3254 58301506 092a8648 86f70d01 09021608 63697363 6f617361
30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00ada752
b4e68976 9a491311 5e521209 b3ef96a1 79af728c 29d7af7f ed4ec759 d0eacebd
7587dd4f 7c4c322d a86b3a67 7c08ce39 ce602525 f6d250fe 87cf2aea 60a5690e
c9851070 6e5a30ad 26dbe6fd b2431597 58edbb48 7525f901 ef4a6584 45de2998
15463867 d2d1ce51 9ee462c7 be325103 7c3c751c 0ad6040b edbb3e98 45020301
0001300d 06092a86 4886f70d 01010405 00038181 005d82b7 ac45dbf8 bd911d4d
a330454a a2784a4b 5ef898b1 482e0bbf 4a86ed86 9019820b 00e80361 fd7b2518
9efa746c b98b1e23 fcc0793c de48de6d 6b1a4998 cd6f4e66 ba661d3a d200739a
ae679c7c 94f550fb a6381b94 1eae389e a9ec4b11 30ba31f3 33cd184e 25647174
ce00231d 102d5db3 c9c111a6 df37eb43 66f3d2d5 46
TAG 0x0A: IP Addr: Len 4 IP Addr: 192.168.52.102
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL instance to create for the phone proxy or parses the CTL file stored in Flash memory.
ctl-file (phone-proxy)	Specifies the CTL instance to use when configuring the phone proxy.

Command	Description
phone proxy	Configures the Phone Proxy instance.

show ctl-provider

To display the configuration of CTL providers used in unified communications, use the **show ctl-provider** command in privileged EXEC mode.

show ctl-provider [*name*]

Syntax Description

name (Optional) Shows information for this CTL provider only.

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

This example shows how to display the configuration of the CTL providers.

```
ciscoasa# show ctl-provider

!
ctl-provider my-ctl
 client interface inside address 192.168.1.55
 client interface inside address 192.168.1.56
 client username admin password gWe.oMSKmeGtelxS encrypted
 export certificate ccm-proxy
!
```

Related Commands

Command	Description
ctl-provider	Configures CTL providers.

show cts environment-data

To show the health and status of the environment data refresh operation on the ASA for Cisco TrustSec, use the **show cts environment-data** command in privileged EXEC mode.

show cts environment-data

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

9.0(1) This command was added.

Usage Guidelines

This command is not supported on a standby device in a failover configuration. If you enter this command on a standby device, the following error message appears:

```
ERROR: This command is only permitted on the active device.
```

This command is only supported on the master unit in a clustering configuration. If you enter this command on a slave unit, the following error message appears:

```
This command is only permitted on the master device.
```

Examples

The following is sample output from the **show cts environment-data** command

```
ciscoasa# show cts environment-data
CTS Environment Data
=====
Status:                Active
Last download attempt: Successful
Environment Data Lifetime: 1200 secs
Last update time:      18:12:07 EST Feb 27 2012
Env-data expires in:   0:00:12:24 (dd:hr:mm:sec)
Env-data refreshes in: 0:00:02:24 (dd:hr:mm:sec)
```

Related Commands

Commands	Description
show running-config cts	Shows the SXP connections for the running configuration.
show cts pac	Shows the components on the PAC.

show cts environment-data sg-table

To show the resident security group table on the ASA for Cisco TrustSec, use the **show cts environment-data sg-table** command in privileged EXEC mode.

show cts environment-data sg-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	• Yes	—

Command History

Release Modification

9.0(1) This command was added.

Usage Guidelines

This command is not supported on a standby device in a failover configuration. If you enter this command on a standby device, the following error message appears:

```
ERROR: This command is only permitted on the active device.
```

This command is only supported on the master unit in a clustering configuration. If you enter this command on a slave unit, the following error message appears:

```
This command is only permitted on the master device.
```

Examples

The following is sample output from the **show cts environment-data sg-table** command

```
ciscoasa# show cts environment-data sg-table
Security Group Table:
Valid until: 18:32:07 EST Feb 27 2012
Showing 9 of 9 entries
SG Name                SG Tag  Type
-----
ANY                    65535  unicast
ExampleSG1             2      unicast
ExampleSG13           14     unicast
ExampleSG14           15     unicast
ExampleSG15           16     unicast
ExampleSG16           17     unicast
```

```

ExampleSG17          18    unicast
ExampleSG18          19    unicast
Unknown              0     unicast

```

Related Commands

Commands	Description
show running-config cts	Shows the SXP connections for the running configuration.
show cts pac	Shows the components on the PAC.

show cts pac

To show the components of the Protected Access Credential (PAC) on the ASA for Cisco TrustSec, use the **show cts pac** command in privileged EXEC mode.

show cts pac

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
9.0(1)	This command was added.

Usage Guidelines The **show cts pac** command displays PAC information, including the expiration time. The expiration time is important because the ASA cannot retrieve security group table updates after the PAC lifetime lapses. The administrator must request and install a new PAC before the old one expires to maintain synchronization with the security group table on the Identity Services Engine.

This command is not supported on a standby device in a failover configuration. If you enter this command on a standby device, the following error message appears:

```
ERROR: This command is only permitted on the active device.
```

This command is only supported on the master unit in a clustering configuration. If you enter this command on a slave unit, the following error message appears:

```
This command is only permitted on the master device.
```

Examples

The following is sample output from the **show cts pac** command

```
ciscoasa# show cts pac
PAC-Info:
  Valid until: Jul 28 2012 08:03:23
  AID:        6499578bc0240a3d8bd6591127ab270c
  I-ID:       BrianASA36
  A-ID-Info:  Identity Services Engine
  PAC-type:   Cisco Trustsec
```

PAC-Opaque :

```
000200b000030001000400106499578bc0240a3d8bd6591127ab270c00060094000301
00d75a3f2293ff3b1310803b9967540ff7000000134e2d2deb00093a803d227383e2b9
7db59ed2eeac4e469fcb1eeb0ac2dd84e76e13342a4c2f1081c06d493e192616d43611
8ff93d2af9b9135bb95127e8b9989db36cf1667b4fe6c284e220c11e1f7dbab91721d1
00e9f47231078288dab83a342ce176ed2410f1249780882a147cc087942f52238fc9b4
09100e1758
```

Related Commands

Commands	Description
show running-config cts	Shows the SXP connections for the running configuration.
show cts environment	Shows the health and status of the environment data refresh operation.

show cts sgt-map

To show the IP address-security group table manager entries in the control path, use the **show cts sgt-map** command in privileged EXEC mode.

```
show cts sgt-map [ sgt sgt ] [ address ip4 [/ mask ] | address ipv6 [/ prefix ] | ipv4 | ipv6 ] [ name ] [ brief | detail ]
```

Syntax Description		
address { <i>ipv4</i> [/mask] / <i>ipv6</i> [/prefix]}		Shows only IP address-security group table mapping for the specific IPv4 or IPv6 address. Include an IPv4 subnet mask or IPv6 prefix to see the mapping for a network.
brief		Shows the IP address-security group table mapping summary.
detail		Shows the IP address-security group table mapping.
ipv4		Shows the IPv4 address-security group table mapping. By default, only the IPv4 address-security group table mapping is displayed.
ipv6		Shows the IPv6 address-security group table mapping.
name		Shows IP address-security group table mapping with the matched security group name.
sgt <i>sgt</i>		Shows only IP address-security group table mapping with the matched security group table.

Command Default No default behavior or values.

Command Modes

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

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

Command History

Release Modification

- 9.0(1) The command was added.
- 9.3(1) The output was updated to include IP-SGT binding information from the “CLI-HI” source, which is populated by the **cts role-based sgt-map** command.
- 9.6(1) The ability to show network mappings was added.

Usage Guidelines

This command displays the IP address-security group table manager entries in the control path.

Examples

The following is sample output from the **show cts sgt-map** command:

```
ciscoasa# show cts sgt-map
Active IP-SGT Bindings Information
IP Address      SGT Source
=====
1.1.1.1         7 CLI-HI
10.10.10.1      7 CLI-HI
10.10.10.10     3 LOCAL
10.10.100.1     7 CLI-HI
198.26.208.31  7 SXP
IP-SGT Active Bindings Summary
=====
Total number of LOCAL   bindings = 1
Total number of CLI-HI  bindings = 3
Total number of SXP     bindings = 1
Total number of active  bindings = 5
```

The following is sample output from the **show cts sgt-map** command with some network bindings.

```
ciscoasa# show cts sgt-map
Active IP-SGT Bindings Information
IP Address      SGT Source
=====
10.1.1.1        7 CLI-HI
10.252.10.0/24  7 CLI-HI
10.252.10.10    3 LOCAL
10.252.100.1    7 CLI-HI
172.26.0.0/16   7 SXP
IP-SGT Active Bindings Summary
=====
Total number of LOCAL   bindings = 1
Total number of CLI-HI  bindings = 3
Total number of SXP     bindings = 1
Total number of active  bindings = 5
```

The following is sample output from the **show cts sgt-map ipv6** command:

```
ciscoasa# show cts sgt-map ipv6
Active IP-SGT Bindings Information
IP Address      SGT      Source
=====
3330::1         17       SXP
FE80::A8BB:CCFF:FE00:110  17       SXP
IP-SGT Active Bindings Summary
=====
Total number of SXP     bindings = 2
Total number of active  bindings = 2
```

The following is sample output from the **show cts sgt-map ipv6 detail** command:

```
ciscoasa# show cts sgt-map ipv6 detail
Active IP-SGT Bindings Information
IP Address      Security Group      Source
=====
3330::1         2345                SXP
1280::A8BB:CCFF:FE00:110  Security Tech Business Unit(12345)  SXP
IP-SGT Active Bindings Summary
```



```

=====
Total number of SXP bindings    = 2
Total number of active bindings = 2

```

The following is sample output from the **show cts sgt-map ipv6 brief** command:

```

ciscoasa# show cts sgt-map ipv6 brief
Active IP-SGT Bindings Information
IP-SGT Active Bindings Summary
=====
Total number of SXP bindings    = 2
Total number of active bindings = 2

```

The following is sample output from the **show cts sgt-map address** command:

```

ciscoasa# show cts sgt-map address 10.10.10.5
Active IP-SGT Bindings Information
IP Address      SGT      Source
=====
10.10.10.5     1234     SXP
IP-SGT Active Bindings Summary
=====
Total number of SXP bindings = 1
Total number of active bindings = 1

```

Related Commands

Command	Description
show running-config cts	Shows the SXP connections for the running configuration.
show cts environment	Shows the health and status of the environment data refresh operation.

show cts sxp connections

To show the Security eXchange Protocol (SXP) connections on the ASA, use the **show cts sxp connections** command in privileged EXEC mode.

show cts sxp connections [*peer peer addr*] [**local** *local addr*] [**ipv4** | **ipv6**] [**status** { **on** | **off** | **delete-hold-down** | **pending-on** }] [**mode** { **speaker** | **listener** }] [**brief**]

Syntax Description

brief	(Optional) Shows the SXP connection summary.
delete-hold-down	(Optional) The TCP connection was terminated (TCP is down) when it was in the ON state. Only an ASA configured in listener mode can be in this state.
ipv4	(Optional) Shows SXP connections with IPv4 addresses.
ipv6	(Optional) Shows SXP connections with IPv6 addresses.
listener	(Optional) Shows the ASA configured in listener mode.
local <i>local addr</i>	(Optional) Shows SXP connections with the matched local IP addresses.
mode	(Optional) Shows SXP connections with the matched mode.
off	(Optional) The TCP connection has not been initiated. The ASA retries the TCP connection only in this state.
on	(Optional) An SXP OPEN or SXP OPEN RESP message has been received. The SXP connection has been successfully established. The ASA only exchanges SXP messages in this state.
peer <i>peer addr</i>	(Optional) Shows SXP connections with the matched peer IP addresses.
pending-on	(Optional) An SXP OPEN message has been sent to the peer; the response from the peer is being awaited.
speaker	(Optional) Shows the ASA configured in speaker mode.
status	(Optional) Shows SXP connections with the matched status.

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
	9.0(1) The command was added.

Usage Guidelines

The SXP states change under the following conditions:

- If the SXP listener drops its SXP connection because its peer unconfigures SXP or disables SXP, then the SXP listener moves to the OFF state.
- If the SXP listener drops its SXP connection because its peer crashes or has the interface shut down, then the SXP listener moves to the DELETE_HOLD_DOWN state.
- The SXP speaker moves to the OFF state when either of the first two conditions occurs.

This command is supported on the active device only in failover mode, and the master unit only in a cluster.

Examples

The following is sample output from the **show cts sxp connections** command:

```
ciscoasa# show cts sxp connections
SXP                : Enabled
Highest version    : 2
Default password   : Set
Default local IP   : Not Set
Delete hold down period : 120 secs
Reconcile period   : 120 secs
Retry open period  : 10 secs
Retry open timer   : Not Running
Total number of SXP connections : 3
Total number of SXP connection shown : 3
-----
Peer IP           : 2.2.2.1
Local IP          : 2.2.2.2
Conn status       : On
Local mode        : Listener
Ins number        : 1
TCP conn password : Default
Delete hold down timer : Not Running
Reconciliation timer : Not Running
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
-----
Peer IP           : 3.3.3.1
Local IP          : 3.3.3.2
Conn status       : On
Local mode        : Listener
Ins number        : 2
TCP conn password : None
Delete hold down timer : Not Running
Reconciliation timer : Not Running
Duration since last state change: 0:01:02:20 (dd:hr:mm:sec)
-----
Peer IP           : 4.4.4.1
Local IP          : 4.4.4.2
Conn status       : On
Local mode        : Speaker
Ins number        : 1
TCP conn password : Set
Delete hold down timer : Not Running
Reconciliation timer : Not Running
Duration since last state change: 0:03:01:20 (dd:hr:mm:sec)
```

Related Commands

Command	Description
show running-config cts	Shows the SXP connections for the running configuration.
show cts environment	Shows the health and status of the environment data refresh operation.

show cts sxp sgt-map

To show the current IP address-security group table mapping database entries in the Security eXchange Protocol (SXP) module on the ASA for Cisco TrustSec, use the **show cts sxp sgt-map** command in privileged EXEC mode.

```
show cts sxp sgt-map [ peer peer_addr ] [ sgt sgt ] [ address ipv4 [ / mask ] | address ipv6 [ / prefix ]
| ipv4 | ipv6 ] [ name ] [ brief | detail ] [ status ]
```

Syntax Description

address { <i>ipv4</i> [/ <i>mask</i>] <i>ipv6</i> [/ <i>prefix</i>] }	Shows only IP address-security group table mapping for the specific IPv4 or IPv6 address. Include an IPv4 subnet mask or IPv6 prefix to see the mapping for a network.
brief	Shows the IP address-security group table mapping summary.
detail	Shows the security group table information. If a security group name is not available, only the security group table value is displayed without the bracket.
ipv4	Shows the IP address-security group table mapping with IPv4 addresses. By default, only the IP address-security group table mapping with IPv4 addresses is displayed.
ipv6	Shows the IP address-security group table mapping with IPv6 addresses.
name	Shows IP address-security group table mapping with the matched security group name.
peer <i>peer_addr</i>	Shows only IP address-security group table mapping with the matched peer IP address.
sgt <i>sgt</i>	Shows only IP address-security group table mapping with the matched security group table.
status	Shows active or inactive mapped entries.

Command Default

No default behavior or values.

Command Modes

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

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

Command History**Release Modification**

 9.01) The command was added.

 9.6(1) The ability to show network mappings was added.

Usage Guidelines

This command displays the active IP address-security group table mapped entries consolidated from SXP.

This command is not supported on a standby device in a failover configuration. In a cluster, enter the command on the master unit.

Examples

The following is sample output from the **show cts sxp sgt-map** command:

```
ciscoasa# show cts sxp sgt-map
Total number of IP-SGT mappings : 3
SGT          : 7
IPv4         : 2.2.2.1
Peer IP      : 2.2.2.1
Ins Num      : 1
SGT          : 7
IPv4         : 2.2.2.0
Peer IP      : 3.3.3.1
Ins Num      : 1
SGT          : 7
IPv6         : FE80::A8BB:CCFF:FE00:110
Peer IP      : 2.2.2.1
Ins Num      : 1
```

The following is sample output from the **show cts sxp sgt-map detail** command:

```
ciscoasa# show cts sxp sgt-map detail
Total number of IP-SGT mappings : 3
SGT          : STBU(7)
IPv4         : 2.2.2.1
Peer IP      : 2.2.2.1
Ins Num      : 1
Status       : Active
SGT          : STBU(7)
IPv4         : 2.2.2.0
Peer IP      : 3.3.3.1
Ins Num      : 1
Status       : Inactive
SGT          : 6
IPv6         : 1234::A8BB:CCFF:FE00:110
Peer IP      : 2.2.2.1
Ins Num      : 1
Status       : Active
```

The following is sample output from the **show cts sxp sgt-map brief** command. Some mappings are to networks.

```
ciscoasa# show cts sxp sgt-map brief
Total number of IP-SGT mappings : 3
SGT, IPv4: 7, 2.2.2.0/24
SGT, IPv4: 7, 3.3.3.3
SGT, IPv6: 7, FE80::0/64
```

Related Commands

Command	Description
show running-config cts	Shows the SXP connections for the running configuration.
show cts environment	Shows the health and status of the environment data refresh operation.

show curpriv

To display the current user privileges, use the **show curpriv** command:

show curpriv

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release Modification

7.0(1) Modified to conform to CLI guidelines.

Usage Guidelines

The **show curpriv** command displays the current privilege level. Lower privilege level numbers indicate lower privilege levels.

Examples

These examples show output from the **show curpriv** command when a user named enable_15 is at different privilege levels. The username indicates the name that the user entered when the user logged in. P_PRIV indicates that the user has entered the **enable** command. P_CONF indicates that the user has entered the **config terminal** command.

```
ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
ciscoasa(config)# exit
ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
ciscoasa(config)# exit
ciscoasa(config)# show curpriv
Username : enable_1
```



```
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa(config)#
```

The following example shows a known behavior. When you are in enable mode, then enter disable mode, the initial logged-in username is replaced with enable_1:

```
ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
ciscoasa(config)# exit
ciscoasa# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
ciscoasa# exit
Logoff
Type help or '?' for a list of available commands.
ciscoasa# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa#
```

Related Commands

Command	Description
clear configure privilege	Remove privilege command statements from the configuration.
show running-config privilege	Display privilege levels for commands.

