

show running-config

```
: Saved
:
ASA Version 8.4(3)

hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names

interface Ethernet0/0
nameif OUT
security-level 0
ip address 200.1.0.254 255.255.255.0

interface Ethernet0/1
no nameif
no security-level
no ip address

interface Ethernet0/1.10
vlan 10
nameif IN_DATA
security-level 100
ip address 10.1.0.125 255.255.255.128

interface Ethernet0/1.20
vlan 20
nameif IN_VOICE
security-level 100
ip address 10.1.0.253 255.255.255.128

interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address

interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address

interface Management0/0
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
management-only

ftp mode passive
object network cme
host 10.1.0.254
object network cme_inside_global
host 200.1.0.253
object network data_pat
subnet 10.1.0.0 255.255.255.128
access-list OUT_access_in extended permit icmp any any
access-list OUT_access_in extended deny ip any any
pager lines 24
logging enable
logging asdm informational
mtu management 1500
mtu IN_DATA 1500
mtu OUT 1500
mtu IN_VOICE 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
nat (IN_VOICE,OUT) source static cme cme_inside_global

object network data_pat
nat (any,OUT) dynamic interface
access-group OUT_access_in in interface OUT
route OUT 0.0.0.0 0.0.0.0 200.1.0.1 1
```

```
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management

threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn

class-map inspection_default
match default-inspection-traffic

policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options

service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
Cryptochecksum:ldc43ee35434a84b64192f42d9cc1468
: end
```

show ip route

```
^  
ERROR: % Invalid input detected at '^' marker.
```

show ipv6 route

IPv6 Routing Table - 0 entries
Codes: C - Connected, L - Local, S - Static

show ip int brief

^
ERROR: % Invalid input detected at '^' marker.

show ipv6 int brief

```
OUT [down/down]
unassigned
Ethernet0/1 [down/down]
unassigned
IN_DATA [down/down]
unassigned
IN_VOICE [down/down]
unassigned
Ethernet0/2 [administratively down/down]
unassigned
Ethernet0/3 [administratively down/down]
unassigned
management [down/down]
unassigned
```

show cdp neighbors

```
^  
ERROR: % Invalid input detected at '^' marker.
```

show ipv6 ospf 10

^
ERROR: % Invalid input detected at '^' marker.

show ipv6 ospf 10 neighbor

^

ERROR: % Invalid input detected at '^' marker.

show ip bgp summary

```
^  
ERROR: % Invalid input detected at '^' marker.
```

show access-lists

^
ERROR: % Invalid input detected at '^' marker.

show version

Cisco Adaptive Security Appliance Software Version 8.4(3)
Device Manager Version 6.4(7)

Compiled on Fri 06-Jan-12 10:24 by builders
System image file is "disk0:/asa843-k8.bin"
Config file at boot was "startup-config"

ciscoasa up 22 days 9 hours

Hardware: ASA5510, 1024 MB RAM, CPU Pentium 4 Celeron 1600 MHz
Internal ATA Compact Flash, 64MB
Slot 1: ATA Compact Flash, 64MB
BIOS Flash M50FW080 @ 0xffff00000, 1024KB

Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
Boot microcode : CN1000-MC-BOOT-2.00
SSL/IKE microcode : CNLite-MC-SSLm-PLUS-2.03
IPSec microcode : CNlite-MC-IPSECm-MAIN-2.06
Number of accelerators: 1

0: Ext: Ethernet0/0 : address is 0016.c789.d540, irq 9
1: Ext: Ethernet0/1 : address is 0016.c789.d541, irq 9
2: Ext: Ethernet0/2 : address is 0016.c789.d542, irq 9
3: Ext: Ethernet0/3 : address is 0016.c789.d543, irq 9
4: Ext: Management0/0 : address is 0016.c789.d53f, irq 11
5: Int: Internal-Data0/0 : address is 0000.0001.0002, irq 11
6: Int: Internal-Control0/0 : address is 0000.0001.0001, irq 5

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs : 50 perpetual
Inside Hosts : Unlimited perpetual
Failover : Disabled perpetual
VPN-DES : Enabled perpetual
VPN-3DES-AES : Enabled perpetual
Security Contexts : 0 perpetual
GTP/GPRS : Disabled perpetual
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 250 perpetual
Total VPN Peers : 250 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 2 perpetual
Total UC Proxy Sessions : 2 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual

This platform has a Base license.

Serial Number: JMX1016K0R8
Running Permanent Activation Key: 0xcal32d74 0x8480aa25 0x741049a8 0x95384890 0x0910f2ae
Configuration register is 0x1
Configuration last modified by enable_15 at 17:51:18.876 UTC Tue Mar 7 2017