

show running-config

```
: Saved
:
ASA Version 8.4(2)

hostname R3-15-FW-K3
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names

interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 200.3.0.1 255.255.255.0

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

interface Ethernet0/1.10
 vlan 10
 nameif data
 security-level 100
 ip address 10.3.10.1 255.255.255.0

interface Ethernet0/1.20
 vlan 20
 nameif voice
 security-level 100
 ip address 10.3.20.1 255.255.255.0

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
 shutdown
 no nameif
 no security-level
 no ip address

ftp mode passive
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
pager lines 24
mtu outside 1500
mtu data 1500
mtu voice 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
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
user-identity default-domain LOCAL
http server enable
http 10.3.10.0 255.255.255.0 data
http redirect data 80
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 10.3.10.100-10.3.10.250 data
dhcpd enable data

dhcpd address 10.3.20.100-10.3.20.250 voice
dhcpd option 150 ip 10.3.20.254 interface voice
dhcpd enable voice

threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15

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 ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp

service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile CiscoTAC-1
no active
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:b304b13b2a31d4a266def32c058aa746
: 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

```
outside [down/down]
unassigned
Ethernet0/1 [down/down]
unassigned
data [down/down]
unassigned
voice [down/down]
unassigned
Ethernet0/2 [administratively down/down]
unassigned
Ethernet0/3 [administratively down/down]
unassigned
Management0/0 [administratively 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(2)
Device Manager Version 6.4(5)205

Compiled on Wed 15-Jun-11 18:17 by builders
System image file is "disk0:/asa842-k8.bin"
Config file at boot was "startup-config"

R3-15-FW-K3 up 12 days 4 hours

Hardware: ASA5510, 1024 MB RAM, CPU Pentium 4 Celeron 1600 MHz
Internal ATA Compact Flash, 256MB
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 001d.70b2.25f2, irq 9
1: Ext: Ethernet0/1 : address is 001d.70b2.25f3, irq 9
2: Ext: Ethernet0/2 : address is 001d.70b2.25f4, irq 9
3: Ext: Ethernet0/3 : address is 001d.70b2.25f5, irq 9
4: Ext: Management0/0 : address is 001d.70b2.25f1, irq 11
5: Int: Not used : irq 11
6: Int: Not used : irq 5

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs : 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: JMX1229LOWF
Running Permanent Activation Key: 0x732f4f6e 0x98f3c558 0xc8601560 0xb58c684c 0x4a099aa0
Configuration register is 0x1
Configuration last modified by enable_15 at 09:54:25.346 UTC Thu Jan 23 2003