

show running-config through show running-config isakmp Commands

show running-config aaa

To show the AAA configuration in the running configuration, use the **show running-config aaa** command in privileged EXEC mode.

show running-config aaa [**accounting** | **authentication** | **authorization** | **mac-exempt** | **proxy-limit**]

Syntax Description

accounting	(Optional) Show accounting-related AAA configuration.
authentication	(Optional) Show authentication-related AAA configuration.
authorization	(Optional) Show authorization-related AAA configuration.
mac-exempt	(Optional) Show MAC address exemption AAA configuration.
proxy-limit	(Optional) Show the number of concurrent proxy connections allowed per user.

Defaults

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	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

```
hostname# show running-config aaa
aaa authentication match infrastructure_authentication_radiusvrs infrastructure radiusvrs
aaa accounting match infrastructure_authentication_radiusvrs infrastructure radiusvrs
aaa authentication secure-http-client
aaa local authentication attempts max-fail 16
hostname#
```

Related Commands

Command	Description
aaa authentication match	Enables authentication for traffic that is identified by an access list.
aaa authorization match	Enables authorization for traffic that is identified by an access list.

Command	Description
aaa accounting match	Enables accounting for traffic that is identified by an access list.
aaa max-exempt	Specifies the use of a predefined list of MAC addresses to exempt from authentication and authorization.
aaa proxy-limit	Configure the uauth session limit by setting the maximum number of concurrent proxy connections allowed per user.

show running-config aaa-server

To display AAA server configuration, use the **show running-config aaa-server** command in privileged EXEC mode.

show running-config [**all**] **aaa-server** [*server-tag*] [(*interface-name*)] [**host** *hostname*]

Syntax Description

all	(Optional) Shows the running configuration, including default configuration values.
host <i>hostname</i>	(Optional) The symbolic name or IP address of the particular host for which you want to display AAA server statistics.
(interface-name)	(Optional) The network interface where the AAA server resides.
<i>server-tag</i>	(Optional) The symbolic name of the server group.

Defaults

Omitting the *server-tag* value displays the configurations for all AAA servers.

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	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was modified to adhere to CLI guidelines

Usage Guidelines

Use this command to display the settings for a particular server group. Use the **all** parameter to display the default as well as the explicitly configured values.

Examples

To display the running configuration for the default AAA server group, use the following command:

```
hostname(config)# show running-config default aaa-server

aaa-server group1 protocol tacacs+ accounting-mode simultaneous
reactivation-mode depletion deadtime 10
max-failed-attempts 4
hostname(config)#
```

Related Commands

Command	Description
show aaa-server	Displays AAA server statistics.
clear configure aaa-server	Clears the AAA server configuration.

show running-config aaa-server host

To display AAA server statistics for a particular server, use the **show running-config aaa-server** command in global configuration or privileged EXEC mode.

show/clear aaa-server

show running-config [**all**] **aaa-server** *server-tag* [(*interface-name*)] **host** *hostname*

Syntax Description

all	(Optional) Shows the running configuration, including default configuration values.
<i>server-tag</i>	The symbolic name of the server group.

Defaults

Omitting the default keyword displays only the explicitly configured configuration values, not the default 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	•	•	—	—	•
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was modified to adhere to CLI guidelines.

Usage Guidelines

Use this command to display the statistics for a particular server group. Use the default parameter to display the default as well as the explicitly configured values.

Examples

To display the running configuration for the server group svrgrp1, use the following command:

```
hostname(config)# show running-config default aaa-server svrgrp1
hostname(config)#
```

Related Commands

Command	Description
show running-config aaa-server	Displays AAA server settings for the indicated server, group, or protocol.
clear configure aaa	Removes the settings for all AAA servers across all groups.

show running-config access-group

To display the access group information, use the **show running-config access-group** command in privileged EXEC mode.

show running-config access-group

Syntax Description This command has no arguments or keywords.

Defaults 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	•	•	•	•	—

Command History	Release	Modification
	Preexisting	This command was preexisting.

Examples The following is sample output from the **show running-config access-group** command:

```
hostname# show running-config access-group
access-group 100 in interface outside
```

Related Commands	Command	Description
	access-group	Binds an access list to an interface.
	clear configure access-group	Removes access groups from all the interfaces.

show running-config access-list

To display the access-list configuration that is running on the security appliance, use the **show running-config access-list** command in privileged EXEC mode.

show running-config [default] access-list [alert-interval | deny-flow-max]

show running-config [default] access-list id [saddr_ip]

Syntax Description

alert-interval	Shows the alert interval for generating syslog message 106001, which alerts that the system has reached a deny flow maximum.
deny-flow-max	Shows the maximum number of concurrent deny flows that can be created.
<i>id</i>	Identifies the access list that is displayed.
<i>saddr_ip</i>	Shows the access list elements that contain the specified source IP address.

Defaults

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	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Added keyword running-config .

Usage Guidelines

The **show running-config access-list** command allows you to display the current running access list configuration on the security appliance.

Examples

The following is sample output from the **show running-config access-list** command:

```
hostname# show running-config access-list
access-list allow-all extended permit ip any any
```

Related Commands

Command	Description
access-list ethertype	Configures an access list that controls traffic based on its EtherType.
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the firewall.

Command	Description
access-list ethertype	Configures an access list that controls traffic based on its EtherType.
clear access-list	Clears an access list counter.
clear configure access-list	Clears an access list from the running configuration.

show running-config all

To display the entire operating configuration, including defaults, that is running on the security appliance, use the **show running-config all** command in privileged EXEC mode.

show running-config all [*command*]

Syntax Description

command Displays the configuration associated with a specific command.

Defaults

If no arguments or keywords are specified, the entire non-default security appliance configuration displays.

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	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was modified.

Usage Guidelines

The **show running-config all** command displays the current running configuration on the security appliance.



Note

The device manager commands appear in the configuration after you use it to connect to or configure the security appliance.

Examples

This example show how to display the configuration that is running on the security appliance:

```
hostname# show running-config all
: Saved
:
XXX Version X.X(X)
names
!
interface Ethernet0
 nameif test
 security-level 10
 ip address 10.10.88.50 255.255.255.254
!
interface Ethernet1
 nameif inside
```

```

security-level 100
ip address 10.86.194.176 255.255.254.0
!
interface Ethernet2
shutdown
no nameif
security-level 0
no ip address
!
interface Ethernet3
shutdown
no nameif
security-level 0
no ip address
!
interface Ethernet4
shutdown
no nameif
security-level 0
no ip address
!
interface Ethernet5
shutdown
no nameif
security-level 0
no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname XXX
domain-name XXX.com
boot system flash:/cdisk.bin
ftp mode passive
pager lines 24
mtu test 1500
mtu inside 1500
monitor-interface test
monitor-interface inside
ASDM image flash:ASDM
no ASDM history enable
arp timeout 14400
route inside 0.0.0.0 0.0.0.0 10.86.194.1 1
timeout xlate 3:00:00
timeout conn 2:00:00 half-closed 1:00:00 udp 0:02:00 icmp 1:00:00 rpc 1:00:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
fragment size 200 test
fragment chain 24 test
fragment timeout 5 test
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 1440
ssh timeout 5
console timeout 0
group-policy todd internal
!

```

show running-config all

```

class-map inspection_default
  match default-inspection-traffic
!
!
policy-map xxx_global_fw_policy
  class inspection_default
    inspect dns
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect http
    inspect ils
    inspect mgcp
    inspect netbios
    inspect rpc
    inspect rsh
    inspect rtsp
    inspect sip
    inspect skinny
    inspect sqlnet
    inspect tftp
    inspect xdmcp
    inspect ctiqbe
    inspect cuseeme
    inspect icmp
  !
terminal width 80
service-policy xxx_global_fw_policy global
Cryptochecksum:bfe4cf4b9d1b98b7e8d97434851f57e14
: end

```

Related Commands

Command	Description
configure	Configures the security appliance from the terminal.

show running-config alias

To display the overlapping addresses with dual NAT commands in the configuration, use the **show running-config alias** command in privileged EXEC mode.

show running-config alias {*interface_name*}

Syntax Description

interface_name Internal network interface name that the destination_ip overwrites.

Defaults

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
Global configuration	•	•	—	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

This example shows how to display alias information:

```
hostname# show running-config alias
```

Related Commands

Command	Description
alias	Creates an alias.
clear configure alias	Deletes an alias.

show running-config arp

To show static ARP entries created by the **arp** command in the running configuration, use the **show running-config arp** command in privileged EXEC mode.

show running-config arp

Syntax Description This command has no arguments or keywords.

Defaults 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	•	•	•	•	—

Release	Modification
7.0(1)	This command was introduced.

Examples The following is sample output from the **show running-config arp** command:

```
hostname# show running-config arp
arp inside 10.86.195.11 0008.023b.9893
```

Related Commands	Command	Description
	arp	Adds a static ARP entry.
	arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
	show arp	Shows the ARP table.
	show arp statistics	Shows ARP statistics.

show running-config arp timeout

To view the ARP timeout configuration in the running configuration, use the **show running-config arp timeout** command in privileged EXEC mode.

show running-config arp timeout

Syntax Description This command has no arguments or keywords.

Defaults 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	•	•	•	•	—

Release	Modification
7.0(1)	This command was changed from show arp timeout .

Examples The following is sample output from the **show running-config arp timeout** command:

```
hostname# show running-config arp timeout
arp timeout 20000 seconds
```

Command	Description
arp	Adds a static ARP entry.
arp timeout	Sets the time before the security appliance rebuilds the ARP table.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp statistics	Shows ARP statistics.

show running-config arp-inspection

To view the ARP inspection configuration in the running configuration, use the **show running-config arp-inspection** command in privileged EXEC mode.

show running-config arp-inspection

Syntax Description This command has no arguments or keywords.

Defaults 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	—	•	•	•	—

Release	Modification
7.0(1)	This command was changed from show arp timeout .

Examples The following is sample output from the **show running-config arp-inspection** command:

```
hostname# show running-config arp-inspection

arp-inspection inside1 enable no-flood
```

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
clear configure arp-inspection	Clears the ARP inspection configuration.
firewall transparent	Sets the firewall mode to transparent.
show arp statistics	Shows ARP statistics.

show running-config asdm

To display the **asdm** commands in the running configuration, use the **show running-config asdm** command in privileged EXEC mode.

show running-config asdm [**group** | **location**]

Syntax Description

group	(Optional) Limits the display to the asdm group commands in the running configuration.
location	(Optional) Limits the display to the asdm location commands in the running configuration.

Defaults

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	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed from the show running-config pdm command to the show running-config asdm command.

Usage Guidelines

To remove the **asdm** commands from the configuration, use the **clear configure asdm** command.



Note

On security appliances running in multiple context mode, the **show running-config asdm group** and **show running-config asdm location** commands are only available in the system execution space.

Examples

The following is sample output from the **show running-configuration asdm** command:

```
hostname# show running-config asdm
asdm image flash:/ASDM
asdm history enable
hostname#
```

Related Commands

Command	Description
show asdm image	Displays the current ASDM image file.

show running-config auth-prompt

To displays the current authentication prompt challenge text, use the **show running-config auth-prompt** command in global configuration mode.

show running-config [default] auth-prompt

Syntax Description	default (Optional) Display the default authentication prompt challenge text.
---------------------------	---

Defaults	Display the configured authentication prompt challenge text.
-----------------	--

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	•	•	—	—	•

Command History	Release	Modification
	7.0(1)	This command was modified for this release to conform to CLI guidelines.

Usage Guidelines	After you configure the authentication prompt with the auth-prompt command, use the show running-config auth-prompt command to view the current prompt text.
-------------------------	--

Examples	The following example shows the output of the show running-config auth-prompt command:
-----------------	---

```
hostname(config)# show running-config auth-prompt
auth-prompt prompt Please login:
auth-prompt accept You're in!
auth-prompt reject Try again.
hostname(config)#
```

Related Commands	auth-prompt Set the user authorization prompts.
	clear configure auth-prompt Reset the user authorization prompts to the default value.

show running-config banner

To display the specified banner and all the lines that are configured for it, use the **show running-config banner** command in privileged EXEC mode.

show running-config banner [exec | login | motd]

Syntax Description

exec	(Optional) Displays the banner before the enable prompt.
login	(Optional) Displays the banner before the password login prompt when accessing the security appliance using Telnet.
motd	(Optional) Displays the message-of-the-day banner.

Defaults

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	•	•	•	•	•

Command History

Release	Modification
7.0(1)	The running-config keyword was added.

Usage Guidelines

The **show running-config banner** command displays the specified banner keyword and all the lines configured for it. If a keyword is not specified, then all banners display.

Examples

This example shows how to display the message-of-the-day (motd) banner:

```
hostname# show running-config banner motd
```

Related Commands

Command	Description
banner	Creates a banner.
clear configure banner	Deletes a banner.

show running-config class

To show the resource class configuration, use the **show running-config class** command in privileged EXEC mode.

show running-config class

Syntax Description This command has no arguments or keywords.

Defaults 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	•	•	—	—	•

Release	Modification
7.2(1)	This command was introduced.

Examples The following is sample output from the **show running-config class** command:

```
hostname# show running-config class

class default
  limit-resource All 0
  limit-resource Mac-addresses 65535
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
```

Related Commands	Command	Description
	class	Configures a resource class.
	clear configure class	Clears the class configuration.
	context	Configures a security context.
	limit-resource	Sets the resource limit for a class.
	member	Assigns a context to a resource class.

show running-config class-map

To display the information about the class map configuration, use the **show running-config class-map** command in privileged EXEC mode.

```
show running-config [all] class-map [class_map_name] type {management | regex |
inspect [protocol]}
```

Syntax Description

all	(Optional) Shows all commands, including the commands you have not changed from the default.
<i>class_map_name</i>	(Optional) Shows the running configuration for a class map name.
inspect	(Optional) Shows inspection class maps.
management	(Optional) Shows management class maps.
<i>protocol</i>	(Optional) Specifies the type of application map you want to show. Available types include: • dns • ftp • h323 • http • im • p2p-donkey • sip
regex	(Optional) Shows regular expression class maps.
type	(Optional) Specifies the type of class map you want to show. To show Layer 3/4 class maps, to not specify the type.

Defaults

The **class-map class-default** command, which contains a single **match any** command is the default class map.

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	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Added keyword running-config .

Examples

The following is sample output from the **show running-config class-map** command:

```
hostname# show running-config class-map
class-map tcp-port
  match port tcp eq ftp
hostname#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.

show running-config client-update

To display global client-update configuration information, use the **show running-config client-update** command in global configuration mode or in tunnel-group ipsec-attributes configuration mode.

show running-config client-update

Syntax Description This command has no arguments or keywords.

Defaults 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	•	•	—	—	•
Tunnel-group ipsec-attributes configuration	•	—	•	—	—

Command History	Release	Modification
	7.0(1)	This command was introduced.
	7.1(1)	Added tunnel-group ipsec-attributes configuration mode.

Usage Guidelines Use this command to display global client-update configuration information.

Examples This example shows a **show running-config client-update** command in global configuration mode and its output for a configuration with client-update enabled:

```
hostname(config)# show running-config client-update
hostname(config)# client-update enable
```

Related Commands	Command	Description
	clear configure client-update	Clears the entire client-update configuration.
	client-update	Configures client-update.

show running-config clock

To show the clock configuration in the running configuration, use the **show running-config clock** command in privileged EXEC mode.

show running-config [all] clock

Syntax Description	all	(Optional) Shows all clock commands, including the commands you have not changed from the default.
---------------------------	------------	---

Defaults	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	•	•	•	—	•

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

Usage Guidelines	The all keyword also displays the exact day and time for the clock summer-time command, as well as the default setting for the offset, if you did not originally set it.
-------------------------	--

Examples	The following is sample output from the show running-config clock command. Only the clock summer-time command was set.
-----------------	--

```
hostname# show running-config clock
clock summer-time EDT recurring
```

The following is sample output from the **show running-config all clock** command. The default setting for the unconfigured **clock timezone** command displays, and the detailed information for the **clock summer-time** command displays.

```
hostname# show running-config all clock
clock timezone UTC 0
clock summer-time EDT recurring 1 Sun Apr 2:00 last Sun Oct 2:00 60
```

Related Commands

Command	Description
clock set	Manually sets the clock on the security appliance.
clock summer-time	Sets the date range to show daylight saving time.
clock timezone	Sets the time zone.

show running-config command-alias

To display the command aliases that are configured, use the **show running-config command-alias** command in privileged EXEC mode.

show running-config [all] command-alias

Syntax Description	all (Optional) Displays all command aliases configured, including defaults.
---------------------------	--

Defaults	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	•	•	•	•	•

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

Usage Guidelines	If you do not enter the all keyword, only non-default command aliases display.
-------------------------	---

Examples	The following example displays all command aliases that are configured on the security appliance, <i>including</i> defaults:
-----------------	--

```
hostname# show running-config all command-alias
command-alias exec h help
command-alias exec lo logout
command-alias exec p ping
command-alias exec s show
command-alias exec save copy running-config startup-config
```

The following example displays all command aliases that are configured on the security appliance, *excluding* defaults:

```
hostname# show running-config command-alias
command-alias exec save copy running-config startup-config
hostname#
```

Related Commands

Command	Description
command-alias	Creates a command alias.
clear configure command-alias	Deletes all non-default command aliases.

show running-config compression

To display the compression configuration in the running configuration, use the **show running-config compression** command from privileged EXEC mode:

show running-config compression

Defaults

There is no default behavior for this command.

Command Modes

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

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

Command History

Release	Modification
7.1.1	This command was introduced.

Examples

The following example shows the compression configuration within the running configuration:

```
hostname# show running-config compression
compression svc http-comp
```

Related Commands

Command	Description
compression	Enables compression for all SVC, WebVPN, and Port Forwarding connections.

show running-config console timeout

To display the console connection timeout value, use the **show running-config console timeout** command in privileged EXEC mode.

show running-config console timeout

Syntax Description This command has no arguments or keywords.

Defaults 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	•	•	•	•	•

Release	Modification
7.0(1)	This command was introduced.

Examples The following example shows how to display the console connection timeout setting:

```
hostname# show running-config console timeout
console timeout 0
```

Command	Description
console timeout	Sets the idle timeout for a console connection to the security appliance.
clear configure console	Resets the console connection settings to defaults.

show running-config context

To show the context configuration in the system execution space, use the **show running-config context** command in privileged EXEC mode.

show running-config context

Syntax Description This command has no arguments or keywords.

Defaults 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	•	•	—	—	•

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

Examples The following is sample output from the **show running-config context** command:

```
hostname# show running-config context

admin-context admin
context admin
  allocate-interface GigabitEthernet0/0
  config-url flash:/admin.cfg
!

context A
  allocate-interface GigabitEthernet0/1
  config-url flash:/A.cfg
!
```

Related Commands	Command	Description
	admin-context	Sets the admin context.
	allocate-interface	Assigns interfaces to a context.
	changeto	Changes between contexts or the system execution space.
	config-url	Specifies the location of the context configuration.
	context	Creates a security context in the system configuration and enters context configuration mode.

show running-config crypto

To display the entire crypto configuration including IPSec, crypto maps, dynamic crypto maps, and ISAKMP, use the **show running-config crypto** command in global configuration or privileged EXEC mode.

show running-config crypto

Syntax Description This command has no keywords or arguments.

Defaults 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	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Release	Modification
7.0(1)	This command was introduced.

Examples The following example entered in privileged EXEC mode, displays all crypto configuration information:

```
hostname# show running-config crypto map
crypto map abc 1 match address xyz
crypto map abc 1 set peer 209.165.200.225
crypto map abc 1 set transform-set ttt
crypto map abc interface test
isakmp enable inside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
hostname#
```

Related Commands	Command	Description
	clear configure isakmp	Clears all the ISAKMP configuration.
	clear configure isakmp policy	Clears all ISAKMP policy configuration.
	clear isakmp sa	Clears the IKE runtime SA database.

Command	Description
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp sa	Displays IKE runtime SA database with additional information.

show running-config crypto dynamic-map

To view a dynamic crypto map, use the **show running-config crypto dynamic-map** command in global configuration or privileged EXEC mode.

show running-config crypto dynamic-map

Syntax Description This command has no keywords or arguments.

Defaults 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	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

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

Examples The following example entered in global configuration mode, displays all configuration information about crypto dynamic maps:

```
hostname(config)# show running-config crypto dynamic-map
```

```
Crypto Map Template "dyn1" 10
```

```
access-list 152 permit ip host 172.21.114.67 any
Current peer: 0.0.0.0
Security association lifetime: 4608000 kilobytes/120 seconds
PFS (Y/N): N
Transform sets={ tauth, t1, }
```

```
hostname(config)#
```

Related Commands	Command	Description
	clear configure isakmp	Clears all the ISAKMP configuration.
	clear configure isakmp policy	Clears all ISAKMP policy configuration.
	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 security appliance.
	show isakmp sa	Displays IKE runtime SA database with additional information.

show running-config crypto ipsec

To display the complete IPSec configuration, use the **show running-config crypto ipsec** command in global configuration or privileged EXEC mode.

show running-config crypto ipsec

Syntax Description This command has no default behavior or values.

Defaults 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	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples The following example issued in global configuration mode, displays information about the IPSec configuration:

```
hostname(config)# show running-config crypto ipsec
crypto ipsec transform-set ttt esp-3des esp-md5-hmac
hostname(config)#
```

Related Commands	Command	Description
	clear configure isakmp	Clears all the ISAKMP configuration.
	clear configure isakmp policy	Clears all ISAKMP policy configuration.
	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 security appliance.
	show isakmp sa	Displays IKE runtime SA database with additional information.

show running-config crypto isakmp

To display the complete ISAKMP configuration, use the **show running-config crypto isakmp** command in global configuration or privileged EXEC mode.

show running-config crypto isakmp

Syntax Description

This command has no default behavior or values.

Defaults

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	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The show running-config isakmp command was introduced.
7.2(1)	This command was deprecated. The show running-config crypto isakmp command replaces it.

Examples

The following example issued in global configuration mode, displays information about the ISKAKMP configuration:

```
hostname<config># show running-config crypto isakmp
crypto isakmp enable inside
crypto isakmp policy 1 authentication pre-share
crypto isakmp policy 1 encryption 3des
crypto isakmp policy 1 hash md5
crypto isakmp policy 1 group 2
crypto isakmp policy 1 lifetime 86400
hostname<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.

Command	Description
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show crypto isakmp sa	Displays IKE runtime SA database with additional information.

show running-config crypto map

To display all configuration for all crypto maps, use the **show running-config crypto map** command in global configuration or privileged EXEC mode.

show running-config crypto map

Syntax Description This command has no keywords or arguments.

Defaults 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	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Release	Modification
7.0(1)	This command was introduced.

Command History

Examples The following example entered in privileged EXEC mode, displays all configuration information for all crypto maps:

```
hostname# show running-config crypto map
crypto map abc 1 match address xyz
crypto map abc 1 set peer 209.165.200.225
crypto map abc 1 set transform-set ttt
crypto map abc interface test
hostname#
```

Related Commands	Command	Description
	clear configure isakmp	Clears all the ISAKMP configuration.
	clear configure isakmp policy	Clears all ISAKMP policy configuration.
	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 security appliance.
	show isakmp sa	Displays IKE runtime SA database with additional information.

show running-config ddns

To display the DDNS update methods of the running configuration, use the **show running-config ddns** command in privileged EXEC mode.

show running-config [all] ddns [update]

Syntax Description	all	(Optional) Shows the running configuration, including default configuration values.
	update	(Optional) Specifies that DDNS update method information be displayed.

Defaults 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	•	—	•	•	—

Command History	Release	Modification
	7.2(1)	This command was introduced.

Examples The following example displays the DDNS methods in the running configuration with test in the name:

```
hostname# show running-config all ddns | grep test
ddns update method test
hostname#
```

Related Commands	Command	Description
	ddns (DDNS-update-method mode)	Specifies a DDNS update method type for a created DDNS method.
	ddns update (interface config mode)	Associates a security appliance interface with a DDNS update method or a DDNS update hostname.
	ddns update method (global config mode)	Creates a method for dynamically updating DNS resource records.
	show ddns update interface	Displays the interfaces associated with each configured DDNS method.
	show ddns update method	Displays the type and interval for each configured DDNS method. a DHCP server to perform DDNS updates.

show running-config dhcp-client

To display the DHCP client update parameters in the running configuration, use the **show running-config dhcp-client** command in privileged EXEC mode.

show running-config [all] dhcp-client

Syntax Description	all	(Optional) Shows the running configuration including default configuration values.
---------------------------	------------	--

Defaults	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	•	—	•	•	—

Command History	Release	Modification
	7.2(1)	This command was introduced.

Examples	The following example displays DHCP client update parameters in the running configuration that specify updates for both A and PTR records:
-----------------	--

```
hostname# show running-config all dhcp-client | grep both
dhcp-client update dns server both
hostname#
```

Related Commands	Command	Description
	dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
	dhcpd update dns	Enables a DHCP server to perform DDNS updates.
	clear configure dhcp-client	Clears the DHCP client configuration.

show running-config dhcpd

To show the DHCP configuration, use the **show running-config dhcpd** command in privileged EXEC or global configuration mode.

show running-config dhcpd

Syntax Description This command has no arguments or keywords.

Defaults 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	•	•	•	•	—

Command History	Release	Modification
	7.0(1)	This command was changed from the show dhcpd command to the show running-config dhcpd command.

Usage Guidelines The **show running-config dhcpd** command displays the DHCP commands entered in the running configuration. To see DHCP binding, state, and statistical information, use the **show dhcpd** command.

Examples The following is sample output from the **show running-config dhcpd** command:

```
hostname# show running-config dhcpd

dhcpd address 10.0.1.100-10.0.1.108 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd dns 209.165.201.2 209.165.202.129
dhcpd enable inside
```

Related Commands	Command	Description
	clear configure dhcpd	Removes all DHCP server settings.
	debug dhcpd	Displays debug information for the DHCP server.
	show dhcpd	Displays DHCP binding, statistic, or state information.

show running-config dhcprelay

To view the current DHCP relay agent configuration, use the **show running-config dhcprelay** command in privileged EXEC mode.

show running-config dhcprelay

Syntax Description This command has no arguments or keywords.

Defaults 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	•	—	•	•	—

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines The **show running-config dhcprelay** command displays the current DHCP relay agent configuration. To show DHCP relay agent packet statistics, use the **show dhcprelay statistics** command.

Examples The following example shows output from the **show running-config dhcprelay** command:

```
hostname(config)# show running-config dhcprelay
```

```
dhcprelay server 10.1.1.1
dhcprelay enable inside
dhcprelay timeout 90
```

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
clear dhcprelay statistics	Clears the DHCP relay agent statistic counters.
debug dhcprelay	Displays debug information for the DHCP relay agent.
show dhcprelay statistics	Displays DHCP relay agent statistic information.

show running-config dns

To show the DNS configuration in the running configuration, use the **show running-config dns** command in privileged EXEC mode.

show running-config dns

Syntax Description This command has no arguments or keywords.

Defaults 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	•	•	•	•	—

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

Examples The following is sample output from the **show running-config dns** command:

```
hostname# show running-config dns
dns domain-lookup inside
dns name-server
dns retries 2
dns timeout 15
dns name-server 10.1.1.1
```

Related Commands	Command	Description
	dns domain-lookup	Enables the security appliance to perform a name lookup.
	dns name-server	Configures a DNS server address.
	dns retries	Specifies the number of times to retry the list of DNS servers when the security appliance does not receive a response.
	dns timeout	Specifies the amount of time to wait before trying the next DNS server.
	show dns-hosts	Shows the DNS cache.

show running-config dns server-group

To show the DNS configuration in the running configuration, use the **show running-config dns** command in privileged EXEC mode.

show [**all**] **running-config dns server-group** [*name*]

Syntax	Description
all	Displays the default and explicitly configured configuration information for one or all dns-server-groups.
<i>name</i>	Specifies the name of the dns server group for which you want to show the configuration information.

Defaults If you omit the dns-server-group name, this command displays all the existing dns-server-group configurations.

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	•	•	•	•	—

Command History	Release	Modification
	7.1	This command was introduced.

Examples The following is sample output from the **show running-config dns server-group** command:

```
hostname# show running-config dns server-group
dns domain-lookup inside
dns server-group DefaultDNS
  name-server 90.1.1.22
  domain-name frqa.cisco.com
dns server-group writers1
  retries 10
  timeout 3
  name-server 10.86.194.61
  domain-name doc-group
hostname#
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters DNS server group mode, in which you can configure a DNS server group.

show running-config domain-name

To show the domain name configuration in the running configuration, use the **show running-config domain-name** command in privileged EXEC mode.

show running-config domain-name

Syntax Description This command has no arguments or keywords.

Defaults 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	•	•	•	•	•

Release	Modification
7.0(1)	This command was changed from show domain-name .

Examples The following is sample output from the **show running-config domain-name** command:

```
hostname# show running-config domain-name
example.com
```

Command	Description
domain-name	Sets the default domain name.
hostname	Sets the security appliance hostname.

show running-config enable

To show the encrypted enable passwords, use the **show running-config enable** command in privileged EXEC mode.

show running-config enable

Syntax Description This command has no arguments or keywords.

Defaults 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	•	•	•	•	•

Command History	Release	Modification
	7.0(1)	This command was changed from the show enable command.

Usage Guidelines The password is saved to the configuration in encrypted form, so you cannot view the original password after you enter it. The password displays with the **encrypted** keyword to indicate that the password is encrypted.

Examples The following is sample output from the **show running-config enable** command:

```
hostname# show running-config enable
enable password 2AfK9Kjr3BE2/J2r level 10 encrypted
enable password 8Ry2YjIyt7RRXU24 encrypted
```

Related Commands	Command	Description
	disable	Exits privileged EXEC mode.
	enable	Enters privileged EXEC mode.
	enable password	Sets the enable password.

show running-config established

To display the allowed inbound connections that are based on established connections, use the **show running-config established** command in privileged EXEC mode.

show running-config established

Syntax Description This command has no arguments or keywords.

Defaults 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	•	•	•	•	—

Release	Modification
7.0(1)	The keyword running-config was added.

Usage Guidelines This command has no usage guidelines.

Examples This example shows how to display inbound connections that are based on established connections:

```
hostname# show running-config established
```

Command	Description
established	Permits return connections on ports that are based on an established connection.
clear configure established	Removes all established commands.

show running-config failover

To display the **failover** commands in the configuration, use the **show running-config failover** command in privileged EXEC mode.

show running-config [all] failover

Syntax Description	all	(Optional) Shows all failover commands, including the commands you have not changed from the default.
---------------------------	------------	---

Defaults	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	•	•	•	—	•

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

Usage Guidelines	The show running-config failover command displays the failover commands in the running configuration. It does not display the monitor-interface or join-failover-group commands.
-------------------------	--

Examples	The following example shows the default failover configuration before failover has been configured:
-----------------	---

```
hostname# show running-config all failover
no failover
failover lan unit secondary
failover polltime unit 15 holdtime 45
failover polltime interface 15
failover interface policy 1
hostname#
```

Related Commands	Command	Description
	show failover	Displays failover state and statistics.

show running-config filter

To show the filtering configuration, use the **show running-config filter** command in privileged EXEC mode.

show running-config filter

Defaults

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	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show running-config filter** command displays the filtering configuration for the security appliance.

Examples

The following is sample output from the **show running-config filter** command, and shows the filtering configuration for the security appliance:

```
hostname# show running-config filter
!
filter activex 80 10.86.194.170 255.255.255.255 10.1.1.0 255.255.255.224
!
```

This example shows ActiveX filtering is enabled on port80 for the address 10.86.194.170.

Related Commands

Commands	Description
filter activex	Removes ActiveX objects from HTTP traffic passing through the security appliance.
filter ftp	Identifies the FTP traffic to be filtered by a URL filtering server.
filter https	Identifies the HTTPS traffic to be filtered by a Websense server.
filter java	Removes Java applets from HTTP traffic passing through the security appliance.
filter url	Directs traffic to a URL filtering server.

show running-config fips

To display the FIPS configuration that is running on the security appliance, use the **show running-config fips** command.

show running-config fips

Syntax Description

fips	FIPS-2 compliance information
-------------	-------------------------------

Defaults

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
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

The **show running-config fips** command allows you to display the current running fips configuration. You use the **running-config** keyword only in the **show running-config fips** command. You cannot use this keyword with **no** or **clear**, or as a standalone command as it is not supported. When you enter the **?**, **no ?**, or **clear ?** keywords, a **running-config** keyword is not listed in the command list.

Examples

```
sw8-ASA(config)# show running-config fips
```

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 disables a policy-checking to enforce FIPS compliance on the system or module.
fips self-test poweron	Executes power-on self-tests.
show crashinfo console	Reads, writes, and configures crash write to flash.

show running-config fragment

To display the current configuration of the fragment databases, use the **show running-config fragment** command in privileged EXEC mode.

show running-config fragment [*interface*]

Syntax Description

interface (Optional) Specifies the security appliance interface.

Defaults

If an interface is not specified, the command applies to all interfaces.

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	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show running-config fragment** command displays the current configuration of the fragment databases. If you specify an interface name, only information for the database residing at the specified interface displays. If you do not specify an interface name, the command applies to all interfaces.

Use the **show running-config fragment** command to display this information:

- **Size**—Maximum number of packets set by the **size** keyword. This value is the maximum number of fragments that are allowed on the interface.
- **Chain**—Maximum number of fragments for a single packet set by the **chain** keyword.
- **Timeout**—Maximum number of seconds set by the **timeout** keyword. This is the maximum number of seconds to wait for an entire fragmented packet to arrive. The timer starts after the first fragment of a packet arrives. If all fragments of the packet do not arrive by the number of seconds specified, all fragments of the packet that were already received will be discarded.

Examples

The following example shows how to display the states of the fragment databases on all interfaces:

```
hostname# show running-config fragment
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
```

```
fragment size 200 outside2
fragment chain 24 outside2
fragment timeout 5 outside2
fragment size 200 outside3
fragment chain 24 outside3
fragment timeout 5 outside3
```

The following example shows how to display the states of the fragment databases on interfaces that start with the name “outside”:

**Note**

In this example, the interfaces named “outside1”, “outside2”, and “outside3” display.

```
hostname# show running-config fragment outside
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
fragment size 200 outside2
fragment chain 24 outside2
fragment timeout 5 outside2
fragment size 200 outside3
fragment chain 24 outside3
fragment timeout 5 outside3
```

The following example shows how to display the states of the fragment databases on the interfaces named “outside1” only:

```
hostname# show running-config fragment outside1
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
```

Related Commands

Command	Description
clear configure fragment	Resets all the IP fragment reassembly configurations to defaults.
clear fragment	Clears the operational data of the IP fragment reassembly module.
fragment	Provides additional management of packet fragmentation and improves compatibility with NFS.
show fragment	Displays the operational data of the IP fragment reassembly module.

show running-config ftp mode

To show the client mode configured for FTP, use the **show running-config ftp mode** command in privileged EXEC mode.

show running-config ftp mode

Defaults

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	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show running-config ftp mode** command displays the client mode that is used by the security appliance when accessing an FTP server.

Examples

The following is sample output from the **show running-config ftp-mode** command:

```
hostname# show running-config ftp-mode
!
ftp-mode passive
!
```

Related Commands

Commands	Description
copy	Uploads or downloads image files or configuration files to or from an FTP server.
debug ftp client	Displays detailed information about FTP client activity.
ftp mode passive	Sets the FTP client mode used by the security appliance when accessing an FTP server.

show running-config global

To display the **global** commands in the configuration, use the **show running-config global** command in privileged EXEC mode.

show running-config global

Syntax Description This command has no arguments or keywords.

Defaults 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	•	—	•	•	—

Command History	Release	Modification
	7.0(1)	Added keyword running-config .

Examples The following is sample output from the **show running-config global** command:

```
hostname# show running-config global
global (outside1) 10 interface
```

Related Commands	Command	Description
	clear configure global	Removes global commands from the configuration.
	global	Creates entries from a pool of global addresses.

show running-config group-delimiter

To display the current delimiter to be used when parsing group names from the user names that are received when tunnels are being negotiated, use the **show running-config group-delimiter** command in global configuration mode or in tunnel-group ipsec-attributes configuration mode.

show running-config group-delimiter

Syntax Description

This command has no arguments or keywords.

Defaults

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	•	•	—	—	•
Tunnel-group ipsec-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Added tunnel-group ipsec-attributes configuration mode.

Usage Guidelines

Use this command to display the currently configured group-delimiter.

Examples

This example shows a **show running-config group-delimiter** command and its output:

```
hostname(config)# show running-config group-delimiter
group-delimiter @
```

Related Commands

Command	Description
group-delimiter	Enables group-name parsing and specifies the delimiter to be used when parsing group names from the user names that are received when tunnels are being negotiated.

show running-config group-policy

To display the running configuration for a particular group policy, use the **show running-config group-policy** command in privileged EXEC mode and append the name of the group policy. To display the running configuration for all group policies, use this command without naming a specific group policy. To have either display include the default configuration, use the **all** keyword.

show running-config [all] group-policy [name]

Syntax Description

all	(Optional) Displays the running configuration including default values.
<i>name</i>	(Optional) Specifies the name of the group policy.

Defaults

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	•	—	•	—	—
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to display the running configuration, including default values, for the group policy named FirstGroup:

```
hostname# show running-config all group-policy FirstGroup
```

Related Commands

Command	Description
group-policy	Creates, edits, or removes a group policy.
group-policy attributes	Enters group-policy attributes mode, which lets you configure AVPs for a specified group policy.
clear config group-policy	Removes the configuration for a particular group policy or for all group policies.

show running-config http

To display the current set of configured http commands, use the **show running-config http** command in privileged EXEC mode.

show running-config http

Defaults

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	•	—	•	—	—
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Examples

The following sample output shows how to use the **show running-config http** command:

```
hostname# show running-config http
http server enabled
0.0.0.0 0.0.0.0 inside
```

Related Commands

Command	Description
clear http	Remove the HTTP configuration: disable the HTTP server and remove hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the security appliance interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the security appliance.
http redirect	Specifies that the security appliance redirect HTTP connections to HTTPS.
http server enable	Enables the HTTP server.

show running-config icmp

To show the access rules configured for ICMP traffic, use the **show running-config icmp** command in privileged EXEC mode.

show running-config icmp *map_name*

Defaults

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	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show running-config icmp** command displays the access rules configured for ICMP traffic.

Examples

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

```
hostname# show running-config icmp
!
icmp permit host 172.16.2.15 echo-reply outside
icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
icmp permit any unreachable outside
!
```

Related Commands

Commands	Description
clear configure icmp	Clears the ICMP configuration.
debug icmp	Enables the display of debug information for ICMP.
show icmp	Displays ICMP configuration.
timeout icmp	Configures the idle timeout for ICMP.

show running-config imap4s

To display the running configuration for IMAP4S, use the **show running-config imap4s** command in privileged EXEC mode.

show running-config [all] imap4s

Syntax Description	all (Optional) Displays the running configuration including default values.
---------------------------	--

Defaults	No default behavior or values.
-----------------	--------------------------------

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

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	•	—	•	—	—
Global configuration	•	—	•	—	—
Webvpn	•	—	•	—	—

Examples	The following is sample output from the show running-config imap4s command:
-----------------	--

```
hostname# show running-config imap4s

imap4s
 server 10.160.105.2
 authentication-server-group KerbSvr
 authentication aaa

hostname# show running-config all imap4s

imap4s
 port 993
 server 10.160.105.2
 outstanding 20
 name-separator :
 server-separator @
 authentication-server-group KerbSvr
 no authorization-server-group
 no accounting-server-group
 no default-group-policy
 authentication aaa
```

Related Commands

Command	Description
clear configure imap4s	Removes the IMAP4S configuration.
imap4s	Creates or edits an IMAP4S e-mail proxy configuration.

show running-config interface

To show the interface configuration in the running configuration, use the **show running-config interface** command in privileged EXEC mode.

```
show running-config [all] interface [physical_interface [.subinterface] | mapped_name | interface_name]
```

Syntax Description

all	(Optional) Shows all interface commands, including the commands you have not changed from the default.
<i>interface_name</i>	(Optional) Identifies the interface name set with the nameif command.
<i>mapped_name</i>	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the allocate-interface command.
<i>physical_interface</i>	(Optional) Identifies the interface ID, such as gigabitethernet0/1 . See the interface command for accepted values.
<i>subinterface</i>	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not specify an interface, this command shows the configuration for all interfaces.

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	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You cannot use the interface name in the system execution space, because the **nameif** command is only available within a context. Similarly, if you mapped the interface ID to a mapped name using the **allocate-interface** command, you can only use the mapped name in a context.

Examples

The following is sample output from the **show running-config interface** command. The following example shows the running configuration for all interfaces. The GigabitEthernet0/2 and 0/3 interfaces have not been configured yet, and show the default configuration. The Management0/0 interface also shows the default settings.

```
hostname# show running-config interface
!
interface GigabitEthernet0/0
```

```

no shutdown
nameif inside
security-level 100
ip address 10.86.194.60 255.255.254.0
webvpn enable
!
interface GigabitEthernet0/1
no shutdown
nameif test
security-level 0
ip address 10.10.4.200 255.255.0.0
!
interface GigabitEthernet0/1.1
vlan 101
no shutdown
nameif dmz
security-level 50
ip address 10.50.1.1 255.255.255.0
mac-address 000C.F142.4CDE standby 020C.F142.4CDE
!
interface GigabitEthernet0/2
shutdown
no nameif
security-level 0
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
security-level 0
no ip address
!
interface Management0/0
shutdown
no nameif
security-level 0
no ip address

```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear configure interface	Clears the interface configuration.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
show interface	Displays the runtime status and statistics of interfaces.

show running-config ip address

To show the IP address configuration in the running configuration, use the **show running-config ip address** command in privileged EXEC mode.

show running-config ip address [*physical_interface* [*.subinterface*] | *mapped_name* | *interface_name*]

Syntax Description

<i>interface_name</i>	(Optional) Identifies the interface name set with the nameif command.
<i>mapped_name</i>	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the allocate-interface command.
<i>physical_interface</i>	(Optional) Identifies the interface ID, such as gigabitethernet0/1 . See the interface command for accepted values.
<i>subinterface</i>	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not specify an interface, this command shows the IP address configuration for all interfaces.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

In multiple context mode, if you mapped the interface ID in the **allocate-interface** command, you can only specify the mapped name or the interface name in a context.

In transparent firewall mode, do not specify an interface because this command shows only the management IP address; the transparent firewall does not have IP addresses associated with interfaces.

This display also shows the **nameif** command and **security-level** command configuration.

Examples

The following is sample output from the **show running-config ip address** command:

```
hostname# show running-config ip address
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
```

```
ip address 10.86.194.60 255.255.254.0
!
interface GigabitEthernet0/1
 nameif test
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!
```

Related Commands

Command	Description
clear configure interface	Clears the interface configuration.
interface	Configures an interface and enters interface configuration mode.
ip address	Sets the IP address for the interface or sets the management IP address for a transparent firewall.
nameif	Sets the interface name.
security-level	Sets the security level for the interface.

show running-config ip audit attack

To show the **ip audit attack** configuration in the running configuration, use the **show running-config ip audit attack** command in privileged EXEC mode.

show running-config ip audit attack

Syntax Description This command has no arguments or keywords.

Defaults 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	•	•	•	•	—

Release	Modification
7.0(1)	This command was changed from show ip audit attack .

Examples The following is sample output from the **show running-config ip audit attack** command:

```
hostname# show running-config ip audit attack
ip audit attack action drop
```

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.

show running-config ip audit info

To show the **ip audit info** configuration in the running configuration, use the **show running-config ip audit info** command in privileged EXEC mode.

show running-config ip audit info

Syntax Description This command has no arguments or keywords.

Defaults 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	•	•	•	•	—

Command History	Release	Modification
	7.0(1)	This command was changed from show ip audit info .

Examples The following is sample output from the **show running-config ip audit info** command:

```
hostname# show running-config ip audit info
ip audit info action drop
```

Related Commands	Command	Description
	ip audit attack	Sets the default actions for packets that match an attack signature.
	ip audit info	Sets the default actions for packets that match an informational signature.
	ip audit interface	Assigns an audit policy to an interface.
	ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
	ip audit signature	Disables a signature.

show running-config ip audit interface

To show the **ip audit interface** configuration in the running configuration, use the **show running-config ip audit interface** command in privileged EXEC mode.

show running-config ip audit interface [*interface_name*]

Syntax Description

interface_name (Optional) Specifies the interface name.

Defaults

If you do not specify an interface name, this command shows the configuration for all interfaces.

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	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from show ip audit interface .

Examples

The following is sample output from the **show running-config ip audit interface** command:

```
hostname# show running-config ip audit interface
ip audit interface inside insidepolicy
ip audit interface outside outsidepolicy
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.

show running-config ip audit name

To show the **ip audit name** configuration in the running configuration, use the **show running-config ip audit name** command in privileged EXEC mode.

show running-config ip audit name [*name* [**info** | **attack**]]

Syntax Description

attack	(Optional) Shows the named audit policy configuration for attack signatures.
info	(Optional) Shows the named audit policy configuration for informational signatures.
<i>name</i>	(Optional) Shows the configuration for the audit policy name created using the ip audit name command.

Defaults

If you do not specify a name, this command shows the configuration for all audit policies.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was changed from show ip audit name .

Examples

The following is sample output from the **show running-config ip audit name** command:

```
hostname# show running-config ip audit name
ip audit name insidepolicy1 attack action alarm
ip audit name insidepolicy2 info action alarm
ip audit name outsidepolicy1 attack action reset
ip audit name outsidepolicy2 info action alarm
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.

show running-config ip audit signature

To show the **ip audit signature** configuration in the running configuration, use the **show running-config ip audit signature** command in privileged EXEC mode.

show running-config ip audit signature [*signature_number*]

Syntax Description

signature_number (Optional) Shows the configuration for the signature number, if present. See the **ip audit signature** command for a list of supported signatures.

Defaults

If you do not specify a number, this command shows the configuration for all signatures.

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	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from show ip audit signature .

Examples

The following is sample output from the **show running-config ip audit signature** command:

```
hostname# show running-config ip audit signature
ip audit signature 1000 disable
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.

show running-config ip local pool

To display IP address pools, use the **show running-config ip local pool** command in privileged EXEC mode.

show running-config ip local pool [*poolname*]

Syntax Description

poolname (Optional) Specifies the name of the IP address pool.

Defaults

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
EXEC	•	—	•	—	—
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show running-config ip local pool** command:

```
hostname(config)# show running-config ip local pool firstpool
```

```
Pool          Begin          End          Mask          Free          In use
firstpool          10.20.30.40    10.20.30.50    255.255.255.0    11
0
```

Available Addresses:

```
10.20.30.40
10.20.30.41
10.20.30.42
10.20.30.43
10.20.30.44
10.20.30.45
10.20.30.46
10.20.30.47
10.20.30.48
10.20.30.49
10.20.30.50
```

```
hostname(config)#
```

 show running-config ip local pool**Related Commands**

Command	Description
clear configure ip local pool	Removes all ip local pools
ip local pool	Configures an IP address pool.

show running-config ip verify reverse-path

To show the **ip verify reverse-path** configuration in the running configuration, use the **show running-config ip verify reverse-path** command in privileged EXEC mode.

show running-config ip verify reverse-path [**interface** *interface_name*]

Syntax Description	interface (Optional) Shows the configuration for the specified interface. <i>interface_name</i>
---------------------------	---

Defaults	This command shows the configuration for all interfaces.
-----------------	--

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	•	—	•	•	—

Command History	Release	Modification
	7.0(1)	This command was changed from show ip verify reverse-path .

Examples	The following is sample output from the show ip verify statistics command: <pre>hostname# show running-config ip verify reverse-path ip verify reverse-path interface inside ip verify reverse-path interface outside ip verify reverse-path interface dmz</pre>
-----------------	--

Related Commands	Command	Description
	clear configure ip verify reverse-path	Clears the ip verify reverse-path configuration.
	clear ip verify statistics	Clears the Unicast RPF statistics.
	ip verify reverse-path	Enables the Unicast Reverse Path Forwarding feature to prevent IP spoofing.
	show ip verify statistics	Shows the Unicast RPF statistics.

show running-config ipv6

To display the IPv6 commands in the running configuration, use the **show running-config ipv6** command in privileged EXEC mode.

show running-config [all] ipv6

Syntax Description

all (Optional) Shows all **ipv6** commands, including the commands you have not changed from the default, in the running configuration.

Defaults

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	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show running-config ipv6** command:

```
hostname# show running-config ipv6
ipv6 unicast-routing
ipv6 route vlan101 ::/0 fec0::65:0:0:a0a:6575
ipv6 access-list outside_inbound_ipv6 permit ip any any
ipv6 access-list vlan101_inbound_ipv6 permit ip any any
hostname#
```

Related Commands

Command	Description
debug ipv6	Displays IPv6 debug messages.
show ipv6 access-list	Displays the IPv6 access list.
show ipv6 interface	Displays the status of the IPv6 interfaces.
show ipv6 route	Displays the contents of the IPv6 routing table.
show ipv6 traffic	Displays IPv6 traffic statistics.

show running-config isakmp

To display the complete ISAKMP configuration, use the **show running-config isakmp** command in global configuration or privileged EXEC mode.

show running-config isakmp

Syntax Description This command has no default behavior or values.

Defaults 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	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History	Release	Modification
	7.0(1)	The show running-config isakmp command was introduced.
	7.2(1)	This command was deprecated. The show running-config crypto isakmp command replaces it.

Examples The following example issued in global configuration mode, displays information about the ISKAKMP configuration:

```
hostname(config)# show running-config isakmp
isakmp enable inside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
hostname(config)#
```

Related Commands	Command	Description
	clear configure isakmp	Clears all the ISAKMP configuration.
	clear configure isakmp policy	Clears all ISAKMP policy configuration.
	clear isakmp sa	Clears the IKE runtime SA database.

Command	Description
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp sa	Displays IKE runtime SA database with additional information.

