set Commands

set absolute-session-timeout

To set the absolute session timeout, use the **set absolute-session-timeout** command.

set absolute-session-timeout *seconds*

Syntax Description

seconds	Absolute session timeout for Web, SSH, and Telnet sessions; value can be 0 to 3600 seconds. To disable this timeout, set the value to 0.

Command Modes

Default authentication (/security/default-auth) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

The absolute session timeout closes user sessions after the specified timeout period has passed, regardless of session use. This absolute timeout is global across all forms of access including serial console, SSH, and HTTPS.

Example

This example shows how to enter default authentication mode and then set the absolute timeout for all sessions to four minutes:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set absolute-session-timeout 240
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set refresh-period	Sets the Web session refresh period.
show detail	Displays the current session and absolute session timeout settings.

set account-status

To specify whether a local user account is active or inactive, use the **set account-status** command.

set account-status {**active** | **inactive**}

Syntax Description

active	Specifies that the local user account is active.
inactive	Specifies that the local user account is disabled.

Command Modes

Local user (/security/local-user) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You must be a user with admin or AAA privileges to use this command.

The admin account is always set to active. It cannot be modified.

Example

This example shows how to enter local user mode and deactivate a local user account:

```
FP9300-A # scope security
FP9300-A /security # scope local-user test_user
FP9300-A /security/local-user # set account-status inactive
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Related Commands

Command	Description
set expiration	Specifies the date on which the user account expires.

set address

To set an email or URL address for a Smart Call Home or Smart Licensing destination, use the **set address** command.

set address *address*

Syntax Description

address	The email address or URL of the Smart Call Home or Smart Licensing destination.

Command Modes

scope monitoring/scope callhome/scope profile/scope destination/

Command History

Release	Modification
1.4(1)	Command added.

Usage Guidelines

Each Firepower 4100/9300 chassis must be registered with the Smart Call Home License Authority or Smart License satellite server. Use this command to set an email or HTTP/HTTPS URL address as the licensing destination.

License Authority example: `https://tools.cisco.com/its/service/oddce/services/DDCEService`

Satellite server example: `https://ip_address/Transportgateway/services/DeviceRequestHandler`

Example

This example shows how to create and enter a Smart Call Home destination:

```
firepower # scope monitoring
firepower /monitoring # scope callhome
firepower /monitoring/callhome # scope profile SLProfile
firepower /monitoring/callhome/profile # scope destination SLDest
firepower /monitoring/callhome/profile/destination # set address
https://tools.cisco.com/its/service/oddce/services/DDCEService
firepower /monitoring/callhome/profile/destination* # commit-buffer
firepower /monitoring/callhome/profile/destination #
```

Related Commands

Command	Description
create destination	Creates a new Smart Call Home destination.
delete destination	Deletes an existing Smart Call Home destination.
set protocol	Sets the transport protocol for a Smart Call Home destination.

set admin-state

To enable or disable the administrative state of a Smart Call Home policy, use the **set admin-state** command.

set admin-state { **disabled** | **enabled** }

Syntax Description

disabled	Sets the policy administrative state to disabled.
enabled	Sets the policy administrative state to enabled.

Command Modes

scope monitoring/scope callhome/policy/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to enable or disable the Call Home policy when a fault or system event matching the associated cause is encountered.

Example

This example shows how to enter and enable a Call Home policy instance for link-down events:

```
firepower /monitoring/callhome # enter policy link-down
firepower /monitoring/callhome/policy* # set admin-state enabled
firepower /monitoring/callhome/policy* # commit-buffer
firepower /monitoring/callhome/policy #
```

Related Commands

Command	Description
enter policy	Enters a Smart Call Home policy.
delete policy	Deletes an existing Smart Call Home policy.
scope policy	Scopes into a Smart Call Home policy.
show	Displays Call Home configuration or policy information.

set auth-server-group

To specify a default authentication server group, use the **set auth-server-group** command.

set auth-server-group *admin*

Syntax Description

admin	The name of the authentication server group.

Command Modes

Default authentication mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to specify the default authentication server group:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set auth-server-group admin_server
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set realm	Specifies the default authentication service.

set authentication

To set the default authentication method for the user during login and when connecting to the FXOS CLI via the console port, use the **set authentication** command.

set authentication

Syntax Description

This command has no arguments or keywords.

Command Modes

scope security

Command History

Release	Modification
2.10(1)	Command added.

Usage Guidelines

You can set the default method by which a user is authenticated during login and when connecting to the FXOS CLI via the console port.

Example

This example shows how to enter security mode and set default authentication method:

```
firepower# scope security
firepower /security # set authentication
  console  Console authentication
  default  Default authentication
```

Related Commands

Command	Description
show authentication	Displays the existing authentication service.

set auto-negotiation

To enable or disable the autonegotiation of an interface, use the **set auto-negotiation** command.

set auto-negotiation {**on** | **off**}

Syntax Description

on	(Optional) Auto-Negotiation is turned on.
off	(Optional) Auto-Negotiation is turned off.

Command Modes

scope eth-uplink/scope fabric a/scope interface/

Command History

Release	Modification
2.1.1	Command added.

Usage Guidelines

This command works only on specific port types.

Example

This example shows how to enable or disable autonegotiation:

```
Firepower-9300 # scope eth-uplink
Firepower-9300 /eth-uplink # scope fabric a
Firepower-9300 /eth-uplink #/fabric # scope interface Ethernet2/1
Firepower-9300 /eth-uplink/fabric/interface* # set auto-negotiation on
Firepower-9300 /eth-uplink/fabric/interface* # commit-buffer
Firepower-9300 /eth-uplink/fabric/interface #
```

Related Commands

Command	Description
scope interface	Displays the Ethernet interface information of the interface.

set cert

To add an RSA certificate to a keyring, use the **set cert** command.

set cert

Syntax Description

This command has no arguments or keywords.

Command Modes

Keyring mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

After entering the command, you are prompted to enter the certificate text, which must end with **ENDOFBUF**.

Example

This example shows how to enter the certificate text for a keyring:

```
FP9300-A /security/keyring # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
>-----BEGIN CERTIFICATE-----
MIIFqDCCA5CgAwIBAgIBBDANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBAcMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxCzAJBgNVBAMMAkNBMRowGAYJKoZIhvcNAQkBFgtzc3BAc3NwLm5l
dDAeFw0xNjEyMTUyMTM0NTRaFw>0yNjEyMTMyMTM0NTRaMHwxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTEPMA0GA1UECgwGbmV3c3RnMRAwDgYDVQQLDAduZXdzdGJ1
MRMwEQYDVQQDDAppbnRlcm0xLWNhMSgwJgYJKoZIhvcNAQkBFhlpbnRlcm0xLWNh
QGludGVybTEtY2EubmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
wLpNnyEx5I4P8uDoW>KWF3IZsegjhLANsodxuAUmhmwKekd0OpZZxHMw1wSO4IBX5
4itJS0xyXFzPmeptG3OXvNqCcsT+4BXl3DoGgPMULccc4NesHeg2z8+q3SPA6uZh
iseWNvKfnUjixbQEBtcrWBiSKnZuOz1cpuBn34gtgeFFoCEXN+EZVpPESiancDVh
8pCPlipc/08ZJ3o9GW2j0eHJN84sguIEDL812ROejQvpmfqGUq11stkIIuh+wB+V
VRhUBVG7p>V57I6DHeeRp6cDMLXaM3iMTelhdShyo5YUaRJMak/t8kCqhtGXfuLlI
E2AkxKXeeveR9n6cpQd5JiNzCT/t9IQL/T/CCqMICRXLFpLCS9o5S5O2B6QFgcTZ
yKR6hsmwe22wpK8QI7/5oWNXlolb96hHJ7RPbG7RXYqmcLiXY/d2j9/RuNoPJawI
hLkfhoIdPA28xlnfIB1azCmMmdPcBO6cbUQfCj5hSmk3StVQKgJCjaujz55TGGd1
G>jnxDMX9twwz7Ee51895Xmtr24qqaCXJoW/dPhcIIXRdJPMsTJ4yPG0BieuRwd0p
i8w/rFwbHzv4C9Fthw1JrRxH1yeHJHrLlZgJ5txSaVUIgrgVCJaf6/jrRRWoRJwt
AzvnzYql2dZPCcEAYgP7JcaQpvdpuDgq++NgBtygiqECAwEAAaNBMD8wDAYDVR0T
BAUwAwEB/zAvBgNVHR8EKDAmMCSgIqAghh5odHRwOi8vMTkyLjE2OC40LjI5>L2lu
dGVybS5jcmwwDQYJKoZIhvcNAQELBQADggIBAG/XujJh5G5UWo+cwTSitAezWbJA
h1dAiXZ/OYWZSxkFRliErKdupLqL0ThjnX/wRFfEXbrBQwm5kWAUUDr97D1Uz+2A
8LC5I8SWKXmyf0jUtsnEQbDZb33oVL7yXJk/A0SF0jihpPheMA+YRazalT9xj9KH
PE7nHCJMbb2ptrHUyvBrKSYrSeEqOpQU2+otnFyV3rS9aelgV>juaWyaWOc3lZ1Oi
CC2tJvY3NnM56j5iesxUCeY/SZ2/ECXN7RRBViLHmA3gFKmWf3xeNiKkxmJCxOaa
UWPC1x2V66I8DG9uUzlWyd79O2dy52aAphAHC6hqlzb6v+gw1Tld7UxaqVd8CD5W
ATjNs+ifkJS1h5ERxHjgcurZXOpR+NWpwF+UDzbMXxx+KAAXCI6ltCd8Pb3wOUC3
PKvwEXaIcCcxGx71eRLpWPZFyEoi4N2NGE9OXRjz0>K/KERZgNhsIW3bQMjcw3aX6
OXskEuKgsayctnWyxVqNnqvpuz06kqyubh4+ZgGKZ5LNEXYmGNz3oED1rUN636Tw
SjGAPHgeROzyTFDixCei6aROlGdP/Hwvb0/+uThIe89g8WZ0djTKFUM8uBO3f+II
/cbuyBO1+JrDMq8NkAjxKlJlp1c3WbfCue/qcwtcfUBYZ4i53a56UNF5Ef0rpy/8
B/+07Me/p2y9Luqa
-----END CERTIFICATE-----
```

```
ENDOFBUF
FP9300-A /security/keyring* #
```

Related Commands

Command	Description
set modulus	Specifies the RSA key modulus (SSL key length) in bits.
set regenerate	Regenerates the RSA keys in the default keyring.
set trustpoint	Specifies whether the keyring certificate can be regenerated.

set certchain

To enter a list (or chain) of certificates for the current trustpoint, use the **set certchain** command.

set certchain [*cert_chain*]

Syntax Description

cert_chain	(Optional) The certificate chain obtained from a Certificate Authority. If this variable is omitted, you are prompted to enter the certificate information manually.

Command Modes

Trustpoint mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

The certificates must be in Base64 encoded X.509 (CER) format.

If you do not specify the certificate chain with the command, you are prompted to enter a certificate or a list of trust points defining a certification path to the root Certificate Authority (CA). Type ENDOFBUF to finish the entry.

See "Certificates, Key Rings, and Trusted Points" in the *Cisco FXOS CLI Configuration Guide* for information about obtaining a trust certificate.

Example

This example shows how to create and enter a new trustpoint, and then paste a certificate chain into the trustpoint :

```
FP9300-A # scope security
FP9300-A /security # enter trustpoint tPoint4
FP9300-A /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
```

```
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
FP9300-A /security/trustpoint* # commit-buffer
FP9300-A /security/trustpoint #
```

Related Commands

Command	Description
enter trustpoint	Enters a trustpoint.
show trustpoint	Shows current trustpoint information.

set (certreq)

To specify parameters for a keyring certificate request, use the **set** command in certificate request mode.

set { *country* | *dns* | *e-mail* | *fi-a-ip* | *fi-a-ipv6* | *fi-b-ip* | *fi-b-ipv6* | *ip* | *ipv6* | *locality* | *org-name* | *org-unit-name* | *password* | *state* | *subject-name* }

Syntax Description

country	(Optional) Specify a two-letter country code for the request; letters must be capitalized.
dns	(Optional) Specify the domain name assigned to the network; common to all host names. This is an alternative to *subject-name*.
e-mail	(Optional) Specify the email address associated with the request.
fi-a-ip	Not used.
fi-a-ipv6	Not used.
fi-b-ip	Not used; there is no fabric interconnect B.
fi-b-ipv6	Not used; there is no fabric interconnect B.
ip	(Optional) Specify the IPv4 address of the device domain.
ipv6	(Optional) Specify the IPv6 address of the device domain.
locality	(Optional) Specify the city or town in which the company requesting the certificate is headquartered. Enter up to 64 characters. You can use any letters, numbers, or spaces, as well as the following special characters: , (comma), . (period), @ (at sign), ^ (carat), ((open parenthesis),) (close parenthesis), - (dash), _ (underscore), + (plus sign), : (colon), / (forward slash).
org-name	(Optional) Specify the name of the organization requesting the certificate. Enter up to 64 characters. You can use any letters, numbers, or spaces, as well as the following special characters: , (comma), . (period), @ (at sign), ^ (carat), ((open parenthesis),) (close parenthesis), - (dash), _ (underscore), + (plus sign), : (colon), / (forward slash).
org-unit-name	(Optional) Specify the name of the unit within the organization. Enter up to 64 characters. You can use any letters, numbers, or spaces, as well as the following special characters: , (comma), . (period), @ (at sign), ^ (carat), ((open parenthesis),) (close parenthesis), - (dash), _ (underscore), + (plus sign), : (colon), / (forward slash).
password	(Optional) You are asked to enter and then confirm a password for the request.

state	(Optional) Specify the state or province in which the company requesting the certificate is headquartered. Enter up to 64 characters. You can use any letters, numbers, or spaces, as well as the following special characters: , (comma), . (period), @ (at sign), ^ (carat), ((open parenthesis),) (close parenthesis), - (dash), _ (underscore), + (plus sign), : (colon), / (forward slash).
subject-name	(Optional) Specify the fully qualified domain name of the local fabric interconnect.

Command Modes

scope security/enter keyring/scope certreq/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

After creating or entering a certificate request, use these options to specify information about the request.

Example

This example shows how to specify information about a certificate request:

```
firepower /security/keyring # enter certreq
firepower /security/keyring/certreq # set subject-name FP9300-1.testnet.com
firepower /security/keyring/certreq* # set password
Certificate request password:
Confirm certificate request password:
firepower /security/keyring/certreq* #
```

Related Commands

Command	Description
create certreq	Creates a new keyring certificate request.
delete certreq	Deletes an existing keyring certificate request.
enter certreq	Enters a keyring certificate request.
set (keyring)	Sets keyring-related information, inluding modulus and trustpoint.

set (cfg-export-policy)

To specify or edit the parameters for an existing configuration-export policy, use the **set** command in configuration-export-policy mode.

set {**adminstate** | **descr** | **hostname** | **password** | **port** | **protocol** | **remote-file** | **schedule** | **user**}

Syntax Description

adminstate {**disable** | **enable**	Enables or disables policy administration. When disabled, configuration back-ups are not exported according to the policy schedule.
descr *description*	(Optional) You can add a description to the configuration object; the description can be between one and 256 characters. Most alphanumeric characters are allowed, as are dashes and underscores; the string can end with punctuation such as semi-colon, period (full stop), and exclamation point, but you cannot embed those characters in the description.
hostname *host_ID*	(Optional) Specify the IP address or host name of the remote server to which the configuration back-up is exported. This host can be a server, storage array, local drive, or any read/write media that is accessible on the network. **Note** To use an actual host name, a configured DNS server must be available.
password	(Optional) Specify the password used to connect to the remote server; you are asked to enter and then confirm the password.
port {*number* | **default**}	(Optional) You can change the port on which communications with the remote server take place; if this option is not specified, the protocol's default port is used. The options are a port-ID number between zero and 4294967295, or **default** for the current protocol's default port.
protocol *name*	(Optional) Specify the file-transfer protocol to use. Available options are: • **ftp** • **scp** • **sftp** • **tftp**
remote-file *name*	(Optional) Specify the full path, including a file name, for the exported configuration; can be between one and 128 characters.
schedule {**bi-weekly** | **daily** | **weekly**}	(Optional) Specify how frequently the configuration is automatically exported: • **bi-weekly** – Export occurs every two weeks. • **daily** – Export occurs every day. • **weekly** – Export occurs once a week.

user *name*	(Optional) Specify the user-account name employed to connect to the remote host; can be between zero and 510 characters.

Command Modes

scope org/scope cfg-export-policy/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

Changing `set adminstate` to `enable` and then issuing a `commit-buffer` command immediately triggers a configuration export.

Example

This example shows how to configure the default configuration-export policy, and then check the policy parameters:

```
firepower # scope org
firepower /org # scope cfg-export-policy default
firepower /org/cfg-export-policy # set protocol scp
firepower /org/cfg-export-policy* # set hostname 192.168.1.2
firepower /org/cfg-export-policy* # set remote-file /export/cfg-backup.xml
firepower /org/cfg-export-policy* # set user user1
firepower /org/cfg-export-policy* # set password
Enter a password:
Confirm the password:
firepower /org/cfg-export-policy* # set schedule weekly
firepower /org/cfg-export-policy* # set adminstate enable
firepower /org/cfg-export-policy* # commit-buffer
firepower /org/cfg-export-policy # show detail
Config Export policy:
    Name: default
    Description: Configuration Export Policy
    Admin State: Enable
    Protocol: Scp
    Hostname: 192.168.1.2
    User: user1
    Remote File: /export/cfg-backup.xml
    Schedule: Weekly
    Port: Default
    Current Task:
firepower /org/cfg-export-policy #
```

Related Commands

Command	Description
export-config	Exports the current system configuration to a remote server as an XML file; creates an export-configuration object.
import-config	Copies a previously exported XML configuration file to this appliance.
set password-encryption-key	Specifies a key used when encrypting sensitive information during configuration export.

set (cfg-export-reminder)

To specify or edit the parameters for the configuration-export reminder object, use the **set** command in configuration-export-reminder mode.

set {**adminstate** | **frequency**}

Syntax Description

adminstate {**disable** | **enable**	Enable or disable the export reminder. When disabled, configuration back-up reminder faults are not generated.
frequency *number_of_days*	Specify the number of days that can pass without a configuration back-up occuring. After this period, the system will generate a reminder fault. This value can be between one and 365 days.

Command Modes

scope org/scope cfg-export-reminder/

Command History

Release	Modification
1.1.3	Command added.

Usage Guidelines

When the reminder is enabled, the system generates a fault when a configuration export hasn't been executed in the specified number of days.

Example

This example shows how to enter the export-reminder object, enable it, specify how often back-ups must occur, and then view the settings:

```
firepower # scope org
firepower /org # scope cfg-export-reminder
firepower /org/cfg-export-reminder # set adminstate enable
firepower /org/cfg-export-reminder* # set frequency 30
firepower /org/cfg-export-policy* # commit-buffer
firepower /org/cfg-export-reminder # show

Config Export Reminder:
    Config Export Reminder (Days): 30
    AdminState: Enable
firepower /org/cfg-export-reminder #
```

Related Commands

Command	Description
scope cfg-export-policy	Enters the configuration export policy.
show	In configuration-export reminder mode, shows the current reminder object set-up.

set cli

To specify whether command output lines wrap or truncate to fit the width of the terminal window, whether table headers are displayed, and whether commas or spaces are used to separate fields in command output tables, use the **set cli** command.

set cli { **suppress-field-spillover** { **off** | **on** } | **suppress-headers** { **off** | **on** } | **table-field-delimiter** { **comma** | **none** } }

Syntax Description

suppress-field-spillover { **off** | **on** }	Use **off** to wrap output lines in the terminal window. Use **on** to truncate output lines at the end of the terminal window.
suppress-headers { **off** | **on** }	Use **off** to display table headers. Use **on** to not display table headers.
table-field-delimiter { **comma** | **none** }	Use **comma** to separate fields in command output tables with commas. Use **none** to separate fields in command output tables with spaces.

Command Default

Command output lines wrap in the terminal window.

Table headers are displayed.

Spaces are used to separate fields in command output tables.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to specify whether command output lines wrap or truncate to fit the width of the terminal window, whether table headers are displayed, and whether commas or spaces are used to separate fields in command output tables.

Example

This example shows how to specify that command output lines truncate, and then how to reset to wrap:

```
FP9300-A# set cli suppress-field-spillover on
FP9300-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Warning   F16520   2010-01-21T18:33:22.065   5785755 [FSM:STAGE:RETRY:]: detect
mezz cards in 1/6(FSM-STAGE:sam:dme:ComputeBladeDiscover:NicPresence)
Condition F77960   2010-01-21T18:32:31.255   1089623 [FSM:STAGE:REMOTE-ERROR]: R
esult: end-point-unavailable Code: unspecified Message: sendSamDmeAdapterInfo: i
dentify failed

FP9300-A# set cli suppress-field-spillover off
FP9300-A# show fault
```

```
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Warning   F16520   2010-01-21T18:33:22.065   5785755 [FSM:STAGE:RETRY:]: detect
Condition F77960   2010-01-21T18:32:31.255   1089623 [FSM:STAGE:REMOTE-ERROR]: R

FP9300-A#
```

Related Commands

Command	Description
show cli	Shows current CLI settings.
terminal	Sets the number of lines, and the width of the lines, displayed in the terminal window.

set clock

To manually set the clock timing in FXOS, use the **set clock** command.

set clock

Syntax Description

set clock	Use **set clock** to maunally set the clock in FXOS.

Command Modes

scope system/scope services

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to set the clock in FXOS:

```
firepower# scope system
firepower /system# scope services
firepower /system/services # set clock aug 23 2021 12 00 00
firepower /system/services* # commit
firepower /system/services # show clock
Tue Aug 24 12:00:02 UTC 2021
```

set cluster-control-link network

To set the cluster control link IP network in the cluster bootstrap configuration for the threat defense and ASA, use the **set cluster-control-link network** command.

set cluster-control-link network *a.b*.**0.0**

Syntax Description

a.b.**0.0**	Specifies any /16 network address, except for loopback (127.0.0.0/8) and multicast (224.0.0.0/4) addresses. If you set the value to 0.0.0.0, then the default network is used: 127.2.0.0.

Command Default

The default network is 127.2.0.0.

Command Modes

scope ssa/create logical-device/create cluster-bootstrap/

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: *a.b.chassis_id.slot_id*.

Bootstrap settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can change most values in the application CLI configuration.

Example

The following example shows how to set the mode to routed mode:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 clustered
Firepower /ssa/logical-device* # create cluster-bootstrap
firepower /ssa/logical-device/cluster-bootstrap* # set cluster-control-link network 10.10.0.0
firepower /ssa/logical-device/cluster-bootstrap* #
```

Related Commands

Command	Description
create logical-device	Creates the logical device.
create cluster-bootstrap	Creates the cluster bootstrap configuration for the application.

set collection-interval

To define how frequently monitored statistics are collected, use the **set collection-interval** command.

set collection-interval *interval*

Syntax Description

interval	Length of time defining the statistics collection interval; available values are: • `1minute` – one-minute intervals • `2minutes` – two-minute intervals • `30seconds` – 30-second intervals • `5minutes` – five-minute intervals

Command Modes

scope monitoring/scope stats-collection-policy/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use the **set collection-interval** command to define how frequently statistics are collected, and use the **set reporting-interval** command to define how frequently the statistics are reported. These intervals define a statistics collection policy.

Reporting intervals are longer than collection intervals so that multiple statistical data points can be collected during the reporting interval, which provides sufficient data to calculate and report minimum, maximum, and average values.

Statistics can be collected and reported for each of the following functional areas of your Firepower system; use the **scope stats-collection-policy** command to access a specific collection policy:

- `Adapter` – statistics related to the adapters.
- `Chassis` – statistics related to the blade chassis.
- `FEX` – statistics related to configured Fabric Extender(s).
- `Host` – this policy is a placeholder for future support.
- `Port` – statistics related to the ports, including server ports, uplink Ethernet ports, and uplink Fibre Channel ports.
- `Server` – statistics related to servers.

Note There is one default statistics collection policy for each of the functional areas. You cannot create additional statistics collection policies and you cannot delete the existing default policies. You can only modify the default policies.

Example

This example shows how to enter the statistics collection policy for ports, set the collection interval to one minute, set the reporting interval to 30 minutes, and then commit the transaction:

```
firepower # scope monitoring
firepower /monitoring # scope stats-collection-policy port
firepower /monitoring/stats-collection-policy # set collection-interval 1minute
firepower /monitoring/stats-collection-policy* # set reporting-interval 30minute
firepower /monitoring/stats-collection-policy* # commit-buffer
firepower /monitoring/stats-collection-policy #
```

Related Commands

Command	Description
scope stats-collection-policy	Enters stats-collection-policy mode, where you manage statistics collection and reporting intervals.
set reporting-interval	Specifies how frequently statistics are reported.

set con-absolute-session-timeout

To set the serial console absolute session timeout, use the **set con-absolute-session-timeout** command.

set con-absolute-session-timeout *seconds*

Syntax Description

seconds	Serial console absolute session timeout; value can be 0 to 3600 seconds. To disable this timeout, set the value to 0.

Command Modes

Default authentication mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can separately configure the absolute session timeout for serial console sessions. This means you can disable the serial console absolute session timeout for debugging while maintaining the absolute timeout for other forms of access.

Example

This example shows how to enter default authentication mode and then set the serial console absolute timeout to four minutes:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set con-absolute-session-timeout 240
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set refresh-period	Sets the Web session refresh period.
show detail	Displays the current session and absolute session timeout settings.

set con-session-timeout

To set the serial console idle session timeout, use the **set con-session-timeout** command.

set con-session-timeout *seconds*

Syntax Description

seconds	Serial console idle session timeout; value can be 0 to 3600 seconds. To disable this timeout, set the value to 0.

Command Modes

Default authentication mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to specify the idle session timeout for serial console sessions.

Example

This example shows how to enter default authentication mode and then set the serial console idle timeout to four minutes:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set con-session-timeout 240
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set refresh-period	Sets the Web session refresh period.
show detail	Displays the current session and absolute session timeout settings.

set cpu-core-count

To set the CPU cores for a resource profile for use with container instances, use the **set cpu-core-count** command.

set cpu-core-count *cores*

Syntax Description

cores	Sets the number of cores for the profile, between 6 and the maximum, depending on your chassis, as an even number. You *cannot* specify 8 cores.

Command Modes

scope ssa/create resource-profile/

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

To specify resource usage per container instance, create one or more resource profiles. When you deploy the logical device/application instance, you specify the resource profile that you want to use. The resource profile sets the number of CPU cores; RAM is dynamically allocated according to the number of cores, and disk space is set to 40 GB per instance.

- The minimum number of cores is 6.
- You cannot specify 8 cores due to internal architecture.
- You can assign cores as an even number (6, 10, 12, 14 etc.) up to the maximum.
- The maximum number of cores available depends on the security module/chassis model.

The chassis includes a default resource profile called "Default-Small," which includes the minimum number of cores. You can change the definition of this profile, and even delete it if it is not in use. Note that this profile is created when the chassis reloads and no other profile exists on the system.

You cannot change the resource profile settings if it is currently in use. You must disable any instances that use it, then change the resource profile, and finally reenable the instance. If you resize instances in an established High Availability pair, then you should make all members the same size as soon as possible.

If you change the resource profile settings after you add the threat defense instance to the management center, update the inventory for each unit on the **Devices** > **Device Management** > **Device** > **System** > **Inventory** dialog box.

Example

The following example adds three resource profiles.

```
firepower# scope ssa
firepower /ssa # enter resource-profile basic
firepower /ssa/resource-profile* # set description "lowest level"
firepower /ssa/resource-profile* # set cpu-core-count 6
firepower /ssa/resource-profile* # exit
firepower /ssa # enter resource-profile standard
firepower /ssa/resource-profile* # set description "middle level"
```

```
firepower /ssa/resource-profile* # set cpu-core-count 10
firepower /ssa/resource-profile* # exit
firepower /ssa # enter resource-profile advanced
firepower /ssa/resource-profile* # set description "highest level"
firepower /ssa/resource-profile* # set cpu-core-count 12
firepower /ssa/resource-profile* # commit-buffer
firepower /ssa/resource-profile #
```

Related Commands

Command	Description
create resource-profile	Adds a resource profile for use with container instances.
set resource-profile-name	Assigned the resource profile to the application instance.
show monitor detail	Shows resource usage for the security module/engine slot.
show resource detail	Shows resource allocation for the application instance.
show resource-profile user-defined	Shows resource profile assignments.

set deploy-type

To set the deployment type for an application instance, either native or container, use the **set deploy-type** command.

set deploy-type {**native** | **container**}

Syntax Description

container	Sets the application instance to the container type.
native	Sets the application instance to the native type.

Command Default

The default type is native.

Command Modes

scope ssa/scope slot/create app-instance/

Command History

Release	Modification
2.4(1)	Command added for threat defense.

Usage Guidelines

Application instances run in the following deployment types:

- Native instance—A native instance uses all of the resources (CPU, RAM, and disk space) of the security module/engine, so you can only install one native instance.
- Container instance—A container instance uses a subset of resources of the security module/engine, so you can install multiple container instances. Multi-instance capability is only supported for the threat defense; it is not supported for the ASA.

Note Multi-instance capability is similar to ASA multiple context mode, although the implementation is different. Multiple context mode partitions a single application instance, while multi-instance capability allows independent container instances. Container instances allow hard resource separation, separate configuration management, separate reloads, separate software updates, and full threat defense feature support. Multiple context mode, due to shared resources, supports more contexts on a given platform. Multiple context mode is not available on the threat defense.

For the Firepower 9300, you can use a native instance on some modules, and container instances on the other module(s).

Example

The following example adds an threat defense application instance, and sets it to the container type:

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
```

```
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

Related Commands

Command	Description
show app-attri	Shows current application attributes.
create resource-profile	Creates a resource profile for use with constainer instances.
show resource-profile-name	Shows available resource profiles.

set descr

To set a description for the port-channel, use the **set descr** command.

set descr *description*

Syntax Description

description	(Optional) Description. Enter up to 256 characters.

Command Modes

scope eth-uplink/scope fabric a/port-channel/

Command History

Release	Modification
2.0.1	Command added.

Usage Guidelines

If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output Ethernet.

Example

This example shows how to set the description:

```
firepower-9300 # scope eth-uplink
firepower-9300 /eth-uplink # scope fabric a
firepower-9300 /eth-uplink/fabric # create port-channel id
firepower-9300 /eth-uplink/fabric/port-channel* # enable
firepower-9300 /eth-uplink/fabric/port-channel* # set descr "link"
firepower-9300 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
show interface	Displays information about the interface, which includes the duplex parameter.

set duplex

To set the duplex for all members of the port-channel, use the **set duplex** command.

set duplex {**fullduplex** | **halfduplex**}

Syntax Description

fullduplex	(Optional) Specifies the duplex mode as full.
halfduplex	(Optional) Specifies the duplex mode as half.

Command Modes

scope eth-uplink/scope fabric a/port-channel/

Command History

Release	Modification
2.0.1	Command added.

Usage Guidelines

You must set the speed before setting the duplex mode. If you specify 10- or 100-Mbps speed, the port is automatically configured to use half-duplex mode, but you can specify full-duplex mode instead. Gigabit Ethernet is full duplex only. You cannot change the duplex mode on Gigabit Ethernet ports or on a 10/100/1000-Mbps port that is set for Gigabit Ethernet.

Example

This example shows how to set the interface duplex mode:

```
firepower-9300# scope eth-uplink
firepower-9300 /eth-uplink # scope fabric a
firepower-9300 /eth-uplink/fabric # create port-channel id
firepower-9300 /eth-uplink/fabric/port-channel* # enable
firepower-9300 /eth-uplink/fabric/port-channel* # set duplex halfduplex
firepower-9300 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
show interface	Displays information about the interface, which includes the duplex parameter.

set email

To set a contact email address for a user account, use the **set email** command.

set email *email_address*

Syntax Description

email_address	An email address for the user account. Specify the email address in the format: *user_name@domain_name*.

Command Modes

Callhome (/monitoring/callhome) mode – to specify a primary contact email address to be included in Call Home messages.

Local user (/security/local-user) mode – to specify a contact email address for the current local user.

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If the email address includes special characters, such as # (hash), spaces, or & (ampersand), the email server may not be able to deliver email messages to that address. Cisco recommends using email addresses which comply with RFC2821 and RFC2822, and include only 7-bit ASCII characters.

In callhome mode, you can use a maximum of 2083 characters for the email address.

In local user mode, you can use a maximum of 510 characters for the email address.

Example

This example shows how to specify an email address for the current local user:

```
FP9300-A /security/local-user # set email admin@example.com
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Related Commands

Command	Description
create local-user	Creates a new local user account.
set phone-contact	Specifies a telephone contact number for a Smart Call Home account.

set enforce-strong-password

To enable and disable strong password enforcement, use the **set enforce-strong-password** command.

set enforce-strong-password {**no** | **yes**}

Syntax Description

no	Disables strong password enforcement.
yes	Enables strong password enforcement.

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

A password is required for each locally authenticated user account. A user with admin or AAA privileges can configure the system to perform a password strength check on all user passwords. If password strength checking is enabled, each user must have a "strong" password.

We recommend that each user have a strong password. If password strength checking is enabled for locally authenticated users, FXOS rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 80 characters. (The set min-password-length, on page 66 command can be used to specify the minimum number of characters required.)
- Must include at least one uppercase alphabetic character.
- Must include at least one lowercase alphabetic character.
- Must include at least one non-alphanumeric (special) character.
- Must not contain a character that is repeated more than three times consecutively, such as aaabbb.
- Must not contain three consecutive numbers or letters in any order, such as passwordABC or password321.
- Must not be identical to the user name or the reverse of the user name.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign).
- Must not be blank for local user and admin accounts.

Example

This example shows how to enter security mode and enable strong password enforcement:

```
FP9300-A# scope security
FP9300-A /security # set enforce-strong-password yes
FP9300-A /security* # commit-buffer
```

```
FP9300-A /security #
```

Related Commands

Command	Description
set min-password-length	Specifies a minimum password length.

set expiration

To set an expiration date for a local user account, use the **set expiration** command.

set expiration { { **apr** | **aug** | **dec** | **feb** | **jan** | **jul** | **jun** | **mar** | **may** | **nov** | **oct** | **sep** } *day* *year* }

Syntax Description

{ **apr** | **aug** | **dec** | **feb** | **jan** | **jul** | **jun** | **mar** | **may** | **nov** | **oct** | **sep** }	The three-letter month abbreviation.
day	Numeric day of the month; valid values are 1 through 31.
year	Numeric year for expiration; maximum value is 2037.

Command Modes

Local user mode—to specify an expiration date for the current local user.

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can however, reconfigure the account with a different expiration date.

Example

This example shows how to enter security mode, create a new local user account and specify an expiration date for that account:

```
FP9300-A# scope security
FP9300-A /security # create local-user test_user
FP9300-A /security/local-user* # set expiration dec 31 2019
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Related Commands

Command	Description
create local-user	Creates a new local user account.
set password	Specifies a password for a user account.

set (export-config)

To edit the parameters for an existing export-configuration object, use the **set** command in export-configuration mode.

set {**descr** | **password** | **port** | **protocol** | **remote-file** | **user**}

Syntax Description

descr *description*	(Optional) You can add a description to the configuration object; can be between one and 256 characters. Most alphanumeric characters are allowed, as are dashes and underscores; the string can end with punctuation such as semi-colon, period (full stop), and exclamation point, but you cannot embed those characters in the description.
password	(Optional) You can change the password used to connect to the remote server; you are asked to enter and then confirm the password.
port {*number* | **default**}	(Optional) You can change the port on which communications with the remote server take place. The options are a port-ID number between zero and 4294967295, or **default** for the current protocol's default port.
protocol *name*	(Optional) You can change the file-transfer protocol used to transmit the configuration back-up to the remote server. Available options are: • **ftp** • **scp** • **sftp** • **tftp**
remote-file *name*	(Optional) You can change the name of the back-up configuration file; can be between one and 128 characters.
user *name*	(Optional) You can change the user-account name employed to connect to the remote host; can be between zero and 510 characters.

Command Modes

scope system/scope export-config/

Command History

Release	Modification
1.1.3	Command added.

Usage Guidelines

Use these options to change the back-up options for an existing export-configuration object.

An export-configuration object is created when you issue an **export-config** command to back up the current logical device and platform configuration, and **scope export-config** is used to enter the object and edit its parameters.

Please note the following:

- Beginning with FXOS 2.6.1, you must specify a key for use when encrypting sensitive information such as passwords and other secret keys during configuration export, and you must have specified it before you attempt to export the configuration.

  Also, the same key used during export must be set on the target system when you import an exported configuration, unless the file was exported from an FXOS release prior to 2.6.1, in which case the target system will not check the encryption key and will allow the import.

- Do not modify the contents of the configuration file. If a configuration file is modified, configuration import using that file might fail.

- To avoid overwriting existing back-up files, please be sure to change the file name in the export operation, or copy the existing file to another location.

Example

This example shows how to add a description to an existing export-configuration object:

```
firepower # scope system
firepower /system # scope export-config 192.168.1.2
firepower /system/export-config # set descr one-time_back-up_be_sure_to_change_file_name
firepower /system/export-config* # commit-buffer
firepower /system/export-config #
```

Related Commands

Command	Description
cfg-export-policy	Configures a configuration export policy.
export-config	Exports the current system configuration to a remote server as an XML file; creates an export-configuration object.
import-config	Copies a previously exported XML configuration file to this appliance.
set password-encryption-key	Specifies a key used when encrypting sensitive information during configuration export.

set firstname

To specify the first name of a local user, use the **set firstname** command.

set firstname *name*

Syntax Description

name	The user's first name; can be zero to 32 characters.

Command Modes

Local user mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter security mode, create a new local user account and specify a first name and a last name for that user:

```
FP9300-A# scope security
FP9300-A /security # create local-user test_user
FP9300-A /security/local-user* # set firstname john
FP9300-A /security/local-user* # set lastname doe
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Command	Description
create local-user	Creates a new local user account.
set lastname	Specifies the surname for a local user account.

set flow-control-policy

To assign a flow control policy to an interface or a port-channel, use the **set flow-control-policy** command.

set flow-control-policy *name*

Syntax Description

name	The name of the flow control policy; maximum of 16 characters.

Command Modes

scope eth-uplink/scope fabric a/scope interface/

scope eth-uplink/scope fabric a/scope port-channel/

Command History

Release	Modification
2.0.1	Command added.

Usage Guidelines

When you create a new flow control policy, you are automatically entered into flow-control/policy mode (eth-uplink/flow-control/policy) with an asterisk indicating the new policy is not yet committed. You can set policy property values and then commit the new policy. After you create a flow control policy, the policy name cannot be changed. You must delete the policy and create a new one.

Example

This example shows how to assign a flow control policy to an interface:

```
firepower-9300 # scope eth-uplink
firepower-9300 /eth-uplink # scope fabric
firepower-9300 /eth-uplink #/fabric # scope interface Ethernet1/8
firepower-9300 /eth-uplink/fabric/interface* # set flow-control-policy eth1-8flowcontrol
firepower-9300 /eth-uplink/fabric/interface* # commit-buffer
firepower-9300 /eth-uplink/fabric/interface #
```

Related Commands

Command	Description
create policy (flow control)	Creates a new flow control policy.
show interface	Displays the interface status, which includes the speed parameters.
show port-channel	Displays information about a port channel.

set (flow-control policy)

To specify or edit the parameters for an existing flow-control policy, use the **set** command in flow-control/policy mode.

set { **prio** | **receive** | **send** }

Syntax Description

prio { **auto** | **on**	Sets the flow-control priority option: • **auto** – This device and the network will negotiate whether Point-to-Point Protocol (PPP) is used on this fabric. • **on** – PPP is enabled on this fabric.
receive **off**	Specifies that pause requests from the network are ignored and traffic flow continues normally.
send **off** | **on**	Sets the flow-control send parameter: • **off** – Traffic flows normally regardless of packet load. • **on** – This device sends a pause request to the network if the incoming packet buffer becomes full. The pause remains in effect for a few milliseconds while traffic returns to normal levels.

Command Modes

scope eth-uplink/scope flow-control/policy/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

Use this command to specify flow control receive options. When you specify off, pause requests from the network are ignored and traffic flow continues as normal. When you specify on, pause requests are honored and all traffic is halted on that uplink port until the network cancels the pause request.

Use this command to specify flow control send options. When you specify **off**, traffic on the port flows normally regardless of the packet load. When you specify **on**, the FXOS sends a pause request to the network if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is reset to normal levels.

Example

This example shows how to create and enter a named policy for flow control, and then set policy parameters:

```
firepower # scope eth-uplink
firepower /eth-uplink # scope flow-control
firepower /eth-uplink/flow-control # enter policy FCpolicy1
firepower /eth-uplink/flow-control/policy* # set prio auto
firepower /eth-uplink/flow-control/policy* # set send on
firepower /eth-uplink/flow-control/policy* # commit-buffer
```

```
firepower /eth-uplink/flow-control/policy #
```

Related Commands

Command	Description
show policy	In flow-control/policy mode, displays property values for the current flow-control policy. In flow-control mode, displays property values for all currently defined flow-control policies.

set frequency

To generate a fault when a configuration export hasn't been executed in a certain number of days, use the **set frequency** command.

set frequency *days*

Syntax Description

days	Config Export Reminder (Days).

Command Modes

scope org/scope cfg-export-reminder/

Command History

Release	Modification
2.0.1	Command added.

Example

This example shows how to set the configuration frequency days for export reminder:

```
firepower-9300* # scope org
firepower-9300 /org* # scope cfg-export-reminder
firepower-9300 /org/scope cfg-export-reminder* # set frequency 2
firepower-9300 /org/scope cfg-export-reminder* # commit-buffer
firepower-9300 /org/scope cfg-export-reminder* # show detail
Config Export Reminder:
Config Export Reminder (Days): 10
AdminState: Enable
```

Related Commands

Command	Description
set adminstate	Specifies the admin state for the export reminder.

set http-proxy-server-enable

To enable or disable an HTTP/HTTPS proxy for Smart Software Licensing and Smart Call Home, use the **set http-proxy-server-enable** command.

set http-proxy-server-enable {**off** | **on**}

Syntax Description

off	Disables the Smart Call Home HTTP/HTTPS proxy.
on	Enables the Smart Call Home HTTP/HTTPS proxy.

Command Default

The HTTP/HTTPS proxy is disabled by default.

Command Modes

Callhome mode

Usage Guidelines

If your network uses an HTTP proxy for Internet access, you must enable the proxy and configure its address for Smart Software Licensing. This proxy is also used for Smart Call Home in general.

Example

This example shows how to enable an HTTP proxy:

```
FP9300-A# scope monitoring
FP9300-A /monitoring # scope callhome
FP9300-A /monitoring/callhome # set http-proxy-server-enable on
FP9300-A /monitoring/callhome #
```

Related Commands

Command	Description
set http-proxy-server-url	Sets the HTTP or HTTPS address of the proxy server.
set http-proxy-server-port	Sets the communications port for the proxy server.

set http-proxy-server-port

To set the HTTP/HTTPS proxy server port for Smart Software Licensing and Smart Call Home, use the **set http-proxy-server-port** command.

set http-proxy-server-port *port_number*

Syntax Description

port_number	The port for the HTTP or HTTPS proxy server; range is 1 to 65535.

Command Default

The HTTP/HTTPS proxy is disabled by default. The proxy must be enabled before you enter the server address and port number.

Command Modes

Callhome mode

Usage Guidelines

If your network uses an HTTP proxy for Internet access, you must enable the proxy and configure its address for Smart Software Licensing. This proxy is also used for Smart Call Home in general.

Example

This example shows how to enter an HTTP/HTTPS proxy-server port number:

```
FP9300-A# scope monitoring
FP9300-A /monitoring # scope callhome
FP9300-A /monitoring/callhome # set http-proxy-server-port 443
FP9300-A /monitoring/callhome #
```

Related Commands

Command	Description
set http-proxy-server-enable	Enables or disables the HTTP/HTTPS proxy for Smart Software Licensing and Smart Call Home.
set http-proxy-server-url	Sets the HTTP/HTTPS address for the proxy server.

set http-proxy-server-url

To set the HTTP/HTTPS proxy server address for Smart Software Licensing and Smart Call Home, use the **set http-proxy-server-url** command.

set http-proxy-server-url *url*

Syntax Description

url	The HTTP or HTTPS address of the proxy server; can be a maximum of 2083 characters.

Command Default

The HTTP/HTTPS proxy is disabled by default. The proxy must be enabled before you enter the server address.

Command Modes

Callhome mode

Usage Guidelines

If your network uses an HTTP proxy for Internet access, you must enable the proxy and configure its address for Smart Software Licensing. This proxy is also used for Smart Call Home in general.

Example

This example shows how to enter an HTTPS proxy-server address:

```
FP9300-A# scope monitoring
FP9300-A /monitoring # scope callhome
FP9300-A /monitoring/callhome # set http-proxy-server-url https://209.165.201.10
FP9300-A /monitoring/callhome #
```

Related Commands

Command	Description
set http-proxy-server-enable	Enables or disables the HTTP/HTTPS proxy for Smart Software Licensing and Smart Call Home.
set http-proxy-server-port	Sets the communications port for the proxy server.

set https

To specify HTTPS service parameters, use the **set https** command.

set https {**auth-type** {**cert-auth** | **cred-auth**} | **cipher-suite** *cipher_string* | **cipher-suite-mode** {**custom** | **high-strength** | **low-strength** | **medium-strength**} | **crl-mode** {**relaxed** | **strict**} | **keyring** *keyring_name* | **port** *port_number*}

Syntax Description

auth-type {**cert-auth** | **cred-auth**}	(Optional) Specifies the type of authentication to use for HTTPS access: • **cert-auth**—Sets your system to use a client certificate in conjunction with LDAP to authenticate users for HTTPS access. • **cred-auth**—Sets the system to use credential-based user authentication for HTTPS access.
cipher-suite *cipher_string*	(Optional) Specifies the definition string for the cipher suite to be used with the custom **cipher-suite-mode**. The specification string can contain up to 256 characters and must conform to the OpenSSL Cipher Suite specifications. You cannot use any spaces or special characters, except ! (exclamation point), + (plus sign), - (hyphen), and : (colon). See http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite for additional information. **Note** This string is ignored if **cipher-suite-mode** is set to anything other than **custom**.
cipher-suite-mode {**custom** | **high-strength** | **low-strength**	(Optional) Sets the level of Cipher Suite security used: • **custom**—Lets you define a custom Cipher Suite security specification string using the **cipher-suite** option. • **high-strength**—ALL:!EDH-RSA-DES-CBC3-SHA: !EDH-DSS-DES-CBC3-SHA: !DES-CBC3-SHA:!ADH:!3DES: !EXPORT40:!EXPORT56:!LOW:!MEDIUM:!eNULL:!RC4:!MD5: !IDEA:+HIGH:+EXP • **low-strength**—ALL:!EDH-RSA-DES-CBC3-SHA: !EDH-DSS-DES-CBC3-SHA: !DES-CBC3-SHA:!ADH:!3DES: !EXPORT40:!EXPORT56:RC4+RSA: !IDEA:+HIGH:+MEDIUM:+LOW:+EXP:+eNULL • **medium-strength**—ALL:!EDH-RSA-DES-CBC3-SHA: !EDH-DSS-DES-CBC3-SHA: !DES-CBC3-SHA:!ADH:!3DES:!EXPORT40:!EXPORT56: !LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL Generally, cipher strength is roughly based on the bits of security (or symmetric key size), with "low" meaning less than 128 bits of security, "medium" meaning equal to 128 bits, and "high" meaning greater than 128 bits of security.

crl-mode {**relaxed** | **strict**}	(Optional) Defines the level of certificate revocation list (CRL) checking for HTTPS connections: • **relaxed**—Certificates found on a CRL may be used to allow HTTPS authentication, depending on the reason for the certificate's listing; a warning message is logged whenever this occurs. Essentially disables CRL checking. • **strict**—Connection authentication fails for any certificate on a CRL; a warning message is logged whenever this occurs. Also, the CRL must be up to date.
keyring *keyring_name*	(Optional) Specifies the name of the RSA keyring to be used for HTTPS connections.
port *port_number*	(Optional) Specifies the port to be used for HTTPS connections; can be 1 to 65535. Default is 443.

Command Default

The default HTTPS authentication configuration on the Firepower 4100/9300 chassis is credential-based.

The default Cipher Suite security level is medium strength.

Command Modes

Services mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If certificate authentication is enabled, that is the only form of authentication permitted for HTTPS.

The following requirements must be met by the client certificate to use this feature:

- The user name must be included in the X509 attribute Subject Alternative Name email.
- The client certificate must be signed by a root CA which has had its certificate imported into a trustpoint on the supervisor.

Caution When you commit most of these configuration parameters (specifically keyring, port, cipher-suite, and custom cipher-suite-mode), all current HTTP and HTTPS sessions are closed without user warning.

Example

This example shows how to enable certificate-based authentication for HTTPS access:

```
FP9300-A# scope system
FP9300-A /system # scope services
FP9300-A /system/services # set https auth-type cert-auth
FP9300-A /system/services* # commit-buffer
FP9300-A /system/services #
```

Related Commands

Command	Description
enable https	Enables the HTTPS service.
show https	Shows current HTTPS service configuration.

set (interface)

To specify or change the parameters for an interface, use the **set** command in interface mode.

set
{**admin-duplex** | **admin-speed** | **auto-negotiation** | **descr** | **eth-link-profile** | **flow-control-policy** | **nw-ctrl-policy** | **port-type** | **user-label** }

Syntax Description

admin-duplex {**fullduplex** | **halfduplex** }	Defines the duplex mode for the interface: • **fullduplex** – Specifies simultaneous two-way communications. • **halfduplex** – Specifies one-way-at-a-time communications.
admin-speed {**100gbps** | **100mbps** | **10gbps** | **10mbps** | **1gbps** | **40gbps** }	Specify the interface data-transfer speed: • **100gbps** – One hundred Gigabits per second. • **100mbps** – One hundred Megabits per second. • **10gbps** – Ten Gigabits per second. • **10mbps** – Ten Megabits per second. • **1gbps** – One Gigabit per second. • **40gbps** – Forty Gigabits per second.
auto-negotiation {**no** | **yes** }	Enables or disables auto-negotiation of common transmission parameters such as speed, duplex and flow control. • **no** – Disables auto-negotiation. • **yes** – Enables auto-negotiation.
descr *description*	You can add a description to the interface; the description can be between zero and 256 characters. Most alphanumeric characters are allowed, as are dashes and underscores; spaces are not allowed. The string can end with punctuation such as semi-colon, period (full stop), and exclamation point, but you cannot embed those characters in the description.
eth-link-profile *name*	You can assign an Ethernet Link Profile to the interface, automatically configuring the interface according to the profile parameters. Provide the name of the profile; can be up to 16 alphanumeric characters.
flow-control-policy *name*	You can assign a flow-control policy to the interface; provide the policy name, which can be up to 16 alphanumeric characters.
nw-ctrl-policy *name*	You can assign a network-control policy to the interface; provide the policy name, which can be up to 16 alphanumeric characters.

port-type {**cluster** | **data** | **data-sharing** | **firepower-eventing** | **mgmt** }	Specify the interface type or function: • **cluster** – Specify **cluster** only if you want to use this interface as the cluster control link. • **data** – Use for regular data transmission. This is the default type. • **data-sharing** – Use for regular data; only supported with container instances. • **firepower-eventing** – Use this interface as a secondary management interface for threat defense devices. The firepower-eventing interface is used to carry all event traffic (such as Web events). • **mgmt** – Use to manage application instances. You can only assign one management interface per logical device. See set port-type, on page 83 for more information about this command.
user-label *label*	You can apply a descriptive label to this interface. can be beween zero and 16 alphanumeric characters.

Command Modes

scope eth-uplink/scope fabric a/interface/

Command History

Release	Modification
2.4(1)	We added the **data-sharing** type.
1.1(4)	We added the **firepower-eventing** type.
1.1(1)	Command added.

Usage Guidelines

The type `cluster` is a special interface type used for a clustered logical device. This type is automatically assigned to the cluster control link for inter-unit cluster communications. By default, the cluster control link is automatically created on port-channel 48.

Data interfaces cannot be shared between logical devices.

The type `data-sharing` is supported only with container instances, these data interfaces can be shared by one or more logical devices/container instances (threat defense-only). Each container instance can communicate over the backplane with all other instances that share this interface. Shared interfaces can affect the number of container instances you can deploy. Shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode), inline sets, passive interfaces, or failover links.

A `firepower-eventing` interface is a secondary management interface for threat defense devices. To use this interface, you must configure its IP address and other parameters at the threat defense CLI. For example, you can separate management traffic from events (such as Web events). See the “Management Interfaces” section in the *System Configuration* chapter of the Management Center configuration guide. Firepower-eventing interfaces can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface.

Use `mgmt` interfaces to manage application instances. They can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface. You can only assign one management interface per logical device.

The interface speed that you specify can affect the duplex mode used for an interface, so you must set the speed before setting the duplex mode. If you specify 10- or 100-Mbps speed, the port is automatically configured to use half-duplex mode, but you can specify full-duplex mode instead. If you specify a speed of 1000 Mbps (1Gbps) or faster, full duplex is automatically used.

If you edited the default flow control policy, it is already applied to interfaces. If you created a new policy, you can apply it to the interface.

Example

This example shows how to set the interface speed to 10 Gbps and the port type to data:

```
firepower # scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # enter interface Ethernet1/8
firepower /eth-uplink/fabric/interface # enable
firepower /eth-uplink/fabric/interface* # set admin-speed 10gbps
firepower /eth-uplink/fabric/interface* # set port-type data
firepower /eth-uplink/fabric/interface* # commit-buffer
firepower /eth-uplink/fabric/interface
```

Related Commands

Command	Description
enter interface	Enters an interface so you can configure and manage the interface settings.
scope interface	Scopes into an interface so you can configure and manage the interface settings.
show interface	Displays interface configuration and status information.

set ipv6

To enable or disable the IPv6 support on firepower device, use the **set ipv6** command in fabric interconnect mode.

set ipv6 [**enable** | **disable**]

Syntax Description

enable/disable	Enables or disables IPv6 support on the firepower device.

Command Modes

scope fabric-interconnect/scope ipv6-config

Command History

Release	Modification
2.13(1)	Command added.

Usage Guidelines

By default, IPv6 will not be set. Use this command to enable or disable IPv6.

Example

This example shows how to enable IPv6 in a firepower device:

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set ipv6 enable
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

set ipv6-auto eui64

To generate IPv6 address based on eui64 method, use the **set ipv6-auto eui64** command in fabric interconnect mode. The lower 64 bits are derived from the hardware address identifier such as MAC.

set ipv6 auto eui64

Syntax Description

auto eui64	Generates the ipv6 address based on the hardware identifiers.

Command Modes

scope fabric-interconnect/scope ipv6-config

Command History

Release	Modification
2.13(1)	Command added.

Usage Guidelines

You must have a valid global adddress present on the management interface to set ipv6-auto eui64.

Example

This example shows how to set the ipv6-auto eui64:

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set ipv6-auto eui64
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

set ipv6-auto stablesec

To generate ipv6 address based on stable secret seed mechanism, use the **set ipv6-auto stablesec** command in fabric interconnect mode.

set ipv6 auto stablesec

Syntax Description

auto stablesec	Generates the ipv6 address based on the stable secret seed values.

Command Modes

scope fabric-interconnect/scope ipv6-config

Command History

Release	Modification
2.13(1)	Command added.

Example

This example shows how to set the ipv6-auto stablesec:

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set ipv6-auto stablesec
Warning: Setting ipv6readycfg to stablesec will require reboot
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

set ipv6-ready

To set the IPv6 address based on eui64 or stable secret seed method based on the input IPv6 address, use the **set ipv6-ready** command in fabric interconnect mode.

set ipv6-ready [**ipv6-addr** *address* **ipv6-readyconfig-eui64 ipv6-readyprefix** *prefix* | **ipv6-addr** *address* **ipv6-readyconfig stablesec ipv6-readyprefix** *prefix*]

Syntax Description

ipv6-addr <address>	Input IPv6 adress
ipv6-readyconfig eui64	eui64 method to generate the ipv6 address based on the input address
ipv6-readyconfig stablesec	stablesec method to generate the ipv6 address based on the input address
ipv6-readyprefix <prefix>	IPv6 prefix

Command Modes

scope fabric-interconnect/scope ipv6-config

Command History

Release	Modification
2.13(1)	Command added.

Example

This example shows how to set the set the ipv6 address based on eui64 method :

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set ipv6-ready ipv6-addr 2003::12
ipv6-readyconfig eui64 ipv6-readyprefix 64
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

This example shows how to set the set the ipv6 address based on stablesec method :

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set ipv6-ready ipv6-addr
e2ca:83a7:eb48:8f6f:da04:949b:b701:1049 ipv6-readyconfig stablesec ipv6-readyprefix 64
Warning: Setting ipv6readycfg to stablesec will require reboot
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

set keyring-name

To assign a keyring to an IPSec connection, use the **set keyring-name** command.

set keyring-name *name*

Syntax Description

name	The name of a keyring to be assigned to the IPSec connection; maximum of 16 characters.

Command Modes

Connection (/security/ipsec/connection) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to add a keyring to an IPSec connection.

Example

This example shows how to add a keyring to the current IPSec connection:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set keyring-name kr22
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Command	Description
create connection	Creates a new IPSec connection.
set keyring-passwd	Specifies the passphrase for a keyring assigned to an IPSec connection.

set lastname

To specify the last name of a local user, use the **set lastname** command.

set lastname *name*

Syntax Description

name	The user's surname; can be 0 to 32 characters.

Command Modes

Local user mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter security mode, create a new local user account, and then specify a first name and a last name for that user.

```
FP9300-A# scope security
FP9300-A /security # create local-user test_user
FP9300-A /security/local-user* # set firstname john
FP9300-A /security/local-user* # set lastname doe
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Command	Description
create local-user	Creates a new local-user account.
set firstname	Specifies the first name for a local user account.

set link-state-sync

To synchronize the operational link state with the physical link state for data interfaces using a service state, use the **set link-state-sync** command.

set link-state-sync

Syntax Description

This command has no arguments or keywords.

Command Modes

scope ssa

Command History

Release	Modification
2.9(1)	Command added.

Usage Guidelines

Use this command to synchronize the FTD operational link state with the physical link state for data interfaces.

Example

This example shows how to enter scope ssa mode and then set the link-state-sync.

```
firepower# scope ssa
firepower /ssa # scope logical-device <logical device identifier>
firepower /ssa/logical-device # set link-state-sync ?
  disabled  Disabled
  enabled   Enabled
```

set local-address

To specify the local IP address for an IPSec connection, use the **set local-address** command.

set local-address *ip_address*

Syntax Description

ip_address	Provide an IPv4 or IPv6 local gateway address for the IPSec connection; maximum of 510 characters.

Command Modes

Connection mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command and the **set remote-address** command to define the endpoints of an IPSec connection.

Example

This example shows how to set the local address for an IPSec connection:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set local-address 209.165.201.12
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Command	Description
create connection	Creates a new IPSec connection.
set remote-addr	Sets the remote IP address for an IPSec connection.

set log-level

To specify the IPSec logging level, use the **set log-level** command.

set log-level *log_level*

Syntax Description

log_level	Enter a value between 0 and 4 to specify IPSec log verbosity; default is 1. **0** – Basic auditing information; for example, SA up/down. **1** – General control flow information, with errors. **2** – More detailed control flow information; includes debugging information. **3** – Includes raw data dumps (hexadecimal). **4** – Includes sensitive information in the data dumps; for example, SA keys.

Command Modes

IPSec mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use the **show ipsec-log** command to view the logs.

Example

This example shows how to set the IPSec logging level to 2:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # set log-level 2
FP9300-A /security/ipsec* # commit-buffer
FP9300-A /security/ipsec #
```

Related Commands

Command	Description
show ipsec-log	Shows the IPSec log file.

set max-login-attempts

To specify the maximum number of failed login attempts allowed, use the **set max-login-attempts** command.

set max-login-attempts *max_attempts*

Syntax Description

max_attempts	The maximum number of failed login attempts before the user is locked out of the system. The value can range from 0 to 10; the default is 0.

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If any user (including admin users) exceeds this maximum number of login attempts, the user is locked out of the system and must wait a specified amount of time before being allowed to log in again. No notification appears indicating that the user is locked out.

Example

This example shows how to enter security mode and specify a maximum number of login attempts:

```
FP9300-A# scope security
FP9300-A /security # set max-login-attempts 4
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

Related Commands

Command	Description
clear lock-status	Clears a user's locked-out status.
set user-account-unlock-time	Specifies the amount of time a user remains locked out of the system after reaching the maximum number of login attempts.

set message

To add or replace the lines of text presented as the pre-login banner, use the **set message** command.

set message

Syntax Description

This command has no arguments or keywords.

Command Modes

scope security/scope banner/scope pre-login-banner/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

After entering the command, you are prompted to enter the lines of banner text. You must enter `ENDOFBUF` (must be all capital letters) to terminate the banner text.

Note The pre-login banner object must already exist; see create pre-login-banner.

Example

This example shows you how to create and specify a pre-login banner, then commit and view it:

```
firepower # scope security
firepower /security # scope banner
firepower /security/banner # create pre-login-banner
firepower /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Firepower-9300-2
>Western Data Center
>ENDOFBUF
firepower /security/banner/pre-login-banner* # commit
firepower /security/banner/pre-login-banner # show

Pre login banner:
    Message
    -------
    Firepower-9300-2
Western Data Center

firepower /security/banner/pre-login-banner #
```

Related Commands

Command	Description
clear message	Removes the text from an existing pre-login banner; the actual banner object itself is not deleted.

Command	Description
create pre-login-banner	Creates a banner to be presented prior to the log-in screen; the banner object is initially empty.

set min-password-length

To specify a minimum length for user passwords, use the **set min-password-length** command.

set min-password-length *num_chars*

Syntax Description

num_chars	The minimum number of characters required for user passwords; value can range from 8 to 80.

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If enabled, users must create passwords with the specified minimum number of characters or more. For example, if *num_chars* is set to 15, passwords must consist of at least 15 characters.

Example

This example shows how to enter security mode and specify a minimum password length of 15 characters:

```
FP9300-A# scope security
FP9300-A /security # set min-password-length 15
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

Related Commands

Command	Description
set enforce-strong-password	Enables and disables strong password enforcement.

set mode

To specify the IPSec connection mode, use the **set mode** command.

set mode {**transport** | **tunnel**}

Syntax Description

transport	Sets the connection mode to **transport**.
tunnel	Sets the connection mode to **tunnel**.

Command Modes

Connection mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

In transport mode, only the payload of an IP packet is encrypted; in tunnel mode, the entire packet is encrypted. Transport mode is generally used for end-to-end sessions, and tunnel mode is used for all other types of connections (for example, between gateways).

Example

This example shows how to set the IPSec connection mode to tunnel:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set mode tunnel
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Command	Description
create connection	Creates a new IPSec connection.
set local-addr	Sets the local IP address for an IPSec connection.
set remote-addr	Sets the remote IP address for an IPSec connection.

set modulus

To specify the RSA key modulus (SSL key length) in bits, use the **set modulus** command.

set modulus {**mod1536** | **mod2048** | **mod2560** | **mod3072** | **mod3584** | **mod4096**}

Syntax Description

RSA key modulus (SSL key length) in bits	Valid options are: • **mod1536** – Modulus is 1536 bits • **mod2048** – Modulus is 2048 bits • **mod2560** – Modulus is 2560 bits • **mod3072** – Modulus is 3072 bits • **mod3584** – Modulus is 3584 bits • **mod4096** – Modulus is 4096 bits

Command Modes

Keyring mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to specify the key length for a keyring.

Example

This example shows how to specify a key length of 2048 bits for a keyring:

```
FP9300-A# scope security
FP9300-A /security # scope keyring test-ring
FP9300-A /security/keyring # set modulus 2048
FP9300-A /security/keyring* # commit-buffer
switch-A /security/keyring #
```

Related Commands

Command	Description
set cert	Enters an RSA certificate for a keyring.
set regenerate	Regenerates the RSA keys in the default keyring.
set trustpoint	Specifies whether the keyring certificate can be regenerated.

set nd

To enable or disable the IPv6 ND support on the firepower device, use the **set nd** command in fabric interconnect mode.

set nd [**enable** | **disable**]

Syntax Description

enable	Enables the rdnssd (ipv6 recursive dns server discovery daemon) to run, once it is set to enable.
disable	Disables the rdnssd daemon in the firepower device.

Command Modes

scope fabric-interconnect/scope ipv6-config

Command History

Release	Modification
2.13(1)	Command added.

Usage Guidelines

By default, ND will not be set. Use this command to enable or disable IPv6.

Example

This example shows how to enable ND in a firepower device:

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set nd enable
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

set out-of-band

To change the management IP address for the device, use the **set out-of-band** command.

For an IPv4 address:

set out-of-band {**gw** *gateway_address* | **ip** *ip_address* | **netmask** *network_mask*}

For an IPv6 address:

set out-of-band {**ipv6** *ipv6_address* | **ipv6-gw** *ipv6_gateway* | **ipv6-prefix** *ipv6_prefix*}

Syntax Description

gw *gateway_address*	Provide an IPv4 gateway address.
ip *ip_address*	Provide an IPv4 address for device management access.
netmask *network_mask*	Provide a netmask for the IPv4 address.
ipv6 *ipv6_address*	Provide an IPv6 address for device management access.
ipv6-gw *ipv6_gateway*	Provide an IPv6 gateway address.
prefix *ipv6_prefix*	Provide a prefix length for the IPv6 address.

Note Only IPv6 Global Unicast addresses are supported as the chassis's IPv6 management address.

Command Modes

IPv4 address: fabric interconnect mode

IPv6 address: IPv6 configuration (fabric-interconnect/ipv6-config) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

After changing the management IP address, you will need to re-establish any existing connections using the new address.

You can enter the three keywords and variables, for either IP address type, in any order on one command line. See the following examples.

Note Only IPv6 Global Unicast addresses are supported as the chassis's IPv6 management address.

Examples

This example shows how to display the current IPv4 management interface and gateway addresses, and specify new addresses:

```
FP9300-A # scope fabric-interconnect a
FP9300-A /fabric-interconnect # show
```

```
Fabric Interconnect:
ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
Prefix Operability
---- --------------- --------------- --------------- ---------------- ----------------
------ -----------
A    192.0.2.112     192.0.2.1       255.255.255.0   ::               ::               64
    Operable
FP9300-A /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask 255.255.255.0 gw
192.0.2.1
Warning: When committed, this change may disconnect the current CLI session
FP9300-A /fabric-interconnect* # commit-buffer
FP9300-A /fabric-interconnect #
```

This example shows how to display the current IPv6 management interface and gateway addresses, and specify new addresses:

```
FP9300-A # scope fabric-interconnect a
FP9300-A /fabric-interconnect # scope ipv6-config
FP9300-A /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
IPv6 Address                       Prefix     IPv6 Gateway
---------------------------------- ---------- ------------
2001::8998                         64         2001::1
FP9300-A /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999 ipv6-prefix 64
 ipv6-gw 2001::1
FP9300-A /fabric-interconnect/ipv6-config* # commit-buffer
FP9300-A /fabric-interconnect/ipv6-config #
```

Command	Description
show	Shows the current device management IP addresses.
show ipv6-if	Shows the current device management IPv6 address.

set password

To specify the password for a user account, use the **set password** command.

set password

Syntax Description

This command has no arguments or keywords.

Command Modes

`scope security/` – to change the password for the currently logged-in user

`scope security/scope local-user/` – to specify a password for the current local user

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

After entering the **set password** command, you are prompted to enter and confirm the password. For security purposes, the password that you type does not appear in the CLI window.

This password must be a minimum of eight characters and a maximum of 80 characters. Use set min-password-length, on page 66 to define a specific minimum number of characters. Use set enforce-strong-password, on page 35 to require use of "strong" passwords.

Example

This example shows how to enter security mode, create a new local user account and specify a password for that user:

```
firepower# scope security
firepower /security # create local-user test_user
firepower /security/local-user* # set password
Enter a password:
Confirm the password:
firepower /security/local-user* # commit-buffer
firepower /security/local-user #
```

Command	Description
create local-user	Creates a new local-user account.
set expiration	Specifies the date on which the user account expires.

set password-encryption-key

To specify a key for use when encrypting sensitive information during configuration export, use the **set password-encryption-key** command.

set password-encryption-key

Syntax Description

This command has no arguments or keywords. After you enter the command, you are asked to enter and confirm an encryption key.

The key can be between four and 40 characters long; the key you enter is then used to generate a 128-bit MD5 hash value.

Command Modes

scope security/

Command History

Release	Modification
2.6.1	Command added.

Usage Guidelines

You can use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis to a remote server. You can later import that configuration file to quickly apply the configuration settings to your Firepower 4100/9300 chassis to return to a known good configuration or to recover from a system failure.

Beginning with FXOS 2.6.1, you must specify a key for use when encrypting sensitive information such as passwords and other secret keys during configuration export, and you must have specified it before you attempt to export the configuration.

Also, the same key used during export must be set on the target system when you import an exported configuration, unless the file was exported from an FXOS release prior to 2.6.1, in which case the target system will allow the import.

Once a password encryption key is set, it cannot be changed or deleted unless you perform a factory-reset or password-recovery. Factory-reset or password-recovery will clear the key as if it had never been set.

Example

This example shows how to specify a password encryption key prior to exporting the current configuration:

```
firepower # scope security
firepower /security # set password-encryption-key
Enter a key:
Confirm the key:
Warning: Please make note of the encryption key configured. If you change the key, importing
 configurations that were exported with the previous key will fail, because Import and
Export requires the same encryption key on the system.
firepower /security* # commit-buffer
firepower /security #
```

Related Commands

Command	Description
cfg-export-policy	Configures an export policy.
export-config	Exports the current system configuration to a remote server as an XML file.
import-config	Copies a previously exported XML configuration file to this appliance.

set (password-profile)

To specify or change local-user password-profile parameters, use the **set** command in password-profile mode.

set { **change-count** | **change-during-interval** | **change-interval** | **history-count** | **no-change-interval** }

Syntax Description

change-count *count*	The maximum number of times a user can change his or her password (during the time period specified with **set change-interval**); value can be 0 to 10.
change-during-interval { **disable** | **enable** }	Enable or disable restrictions on the number of password changes a locally authenticated user can make: • `disable` – Disables restrictions on the number of password changes. • `enable` – Enables restrictions on the number of password changes. This option must be enabled before you can specify the maximum number of times a locally authenticated user can change his or her password, and the number of hours over which that number of password changes can be made.
change-interval *interval*	The interval over which a user's password changes are tallied to ensure they do not exceed the maximum number specified with the **set change-count** command; the number of hours can be 1 to 745. The **set change-during-interval** option must be enabled before you can specify this interval.
history-count *count*	The number of unique passwords that a locally authenticated user must create before that user can re-use a previously used password; value can be 0 to 15. By default, the *count* value is zero, which disables the password history count, allowing users to re-use previously used passwords at any time.
no-change-interval *hours*	The length of time in hours during which a user cannot change her or his password again; value can be 1 to 745. The **set change-during-interval** option must be disabled before you set this time period, otherwise this value is ignored.

Command Modes

scope security/scope password-profile/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

The **set change-during-interval** option must be enabled before you can specify the maximum number of times a locally authenticated user can change his or her password, and the number of hours over which that number of password changes can be made.

By default, the **set history-count** value is zero, which disables the password history count, allowing users to re-use previously used passwords at any time.

Examples

This example shows how to enter password profile mode, enable password-change restrictions, specify that a user can change his or her password only twice in any 48-hour period, and then view the current settings:

```
firepower # scope security
firepower /security # scope password-profile
firepower /security/password-profile # set change-during-interval enable
firepower /security/password-profile* # set change-count 2
firepower /security/password-profile* # set change-interval 48
firepower /security/password-profile* # commit-buffer
firepower /security/password-profile # show detail

Password profile:
    Password history count: 5
    No password changes allowed (in Hours): 24
    Password change during interval: Enable
    Password change interval (in Hours): 48
    Password change count: 2
firepower /security/password-profile #
```

Related Commands

Command	Description
show detail	Displays the current password-profile settings.

set phone

To set a contact telephone number for a user account, use the **set phone** command.

set phone *tel_number*

Syntax Description

tel_number	A contact telephone number for the user account; maximum of 20 characters.

Command Modes

Local user mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to specify an telephone number for the current local user:

```
FP9300-A /security/local-user # set phone +1-408-555-1212
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Related Commands

Command	Description
create local-user	Creates a new local user account.
set phone-contact	Specifies a contact telephone number for a Smart Call Home account.

set (port-channel)

To specify or edit the parameters for an existing port-channel, use the **set** command in port-channel mode.

set { **auto-negotiation** | **descr** | **duplex** | **flow-control-policy** | **lacp-policy-name** | **nw-ctrl-policy** | **port-channel-mode** | **port-type** | **speed** }

Syntax Description

auto-negotiation { **no** | **yes** }	Enables or disables auto-negotiation of common transmission parameters such as speed, duplex and flow control. • **no** – Disables auto-negotiation. • **yes** – Enables auto-negotiation.
descr *description*	You can add a description to the port-channel; the description can be between zero and 256 characters. Most alphanumeric characters are allowed, as are dashes and underscores; spaces are not allowed. The string can end with punctuation such as semi-colon, period (full stop), and exclamation point, but you cannot embed those characters in the description.
duplex { **fullduplex** | **halfduplex** }	Defines the duplex mode for the port-channel: • **fullduplex** – Specifies simultaneous two-way communications. • **halfduplex** – Specifies one-way-at-a-time communications.
flow-control-policy *name*	You can assign a flow-control policy to the port-channel; provide the policy name, which can be up to 16 alphanumeric characters.
lacp-policy-name *name*	You can assign a LACP policy to the port-channel; provide the policy name, which can be up to 16 alphanumeric characters.
nw-ctrl-policy *name*	You can assign a network-control policy to the port-channel; provide the policy name, which can be up to 16 alphanumeric characters.
port-channel-mode { **active** | **on** }	Define the mode for the port-channel's physical data or data-sharing interfaces: • **active** – Sends and receives LACP updates. An active port-channel can establish connectivity with either an active or a passive port-channel. You should use the active mode unless you need to minimize the amount of LACP traffic. This is the default. • **on** – The port-channel is always on, and LACP is not used. An "on" port-channel can only establish a connection with another "on" port-channel. Non-data interfaces support only active mode.

port-type {**cluster** | **data** | **data-sharing** | **firepower-eventing** | **mgmt**}	Specify the port-channel type or function: • **cluster** – Specify **cluster** only if you want to use this port-channel as the cluster control link. • **data** – Use for regular data transmission. This is the default type. • **data-sharing** – Use for regular data; only supported with container instances. • **firepower-eventing** – Use this port-channel as a secondary management interface for threat defense devices. The firepower-eventing port-channel is used to carry all event traffic (such as Web events). • **mgmt** – Use to manage application instances. You can only assign one management interface per logical device. See set port-type, on page 83 for more information about this command.
speed {**100gbps** | **100mbps** | **10gbps** | **10mbps** | **1gbps** | **40gbps**}	Specify the port data-transfer speed: • **100gbps** – One hundred Gigabits per second. • **100mbps** – One hundred Megabits per second. • **10gbps** – Ten Gigabits per second. • **10mbps** – Ten Megabits per second. • **1gbps** – One Gigabit per second. • **40gbps** – Forty Gigabits per second.

Command Modes

scope eth-uplink/scope fabric a/port-channel/

Command History

Release	Modification
2.4(1)	We added the **data-sharing** type.
1.1(4)	We added the **firepower-eventing** type.
1.1(1)	Command added.

Usage Guidelines

Assign member interfaces to the port-channel before using this command to set parameters.

The LACP port-channel mode applies to data and data-sharing interfaces only. For non-data and non-data-sharing interfaces, the mode is always `active`.

The type `cluster` is a special interface type used for a clustered logical device. This type is automatically assigned to the cluster control link for inter-unit cluster communications. By default, the cluster control link is automatically created on port-channel 48.

Data interfaces cannot be shared between logical devices.

The type `data-sharing` is supported only with container instances, these data interfaces can be shared by one or more logical devices/container instances (threat defense-only). Each container instance can communicate over the backplane with all other instances that share this interface. Shared interfaces can affect the number

of container instances you can deploy. Shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode), inline sets, passive interfaces, or failover links.

A `firepower-eventing` interface is a secondary management interface for threat defense devices. To use this interface, you must configure its IP address and other parameters at the threat defense CLI. For example, you can separate management traffic from events (such as Web events). See the "Management Interfaces" section in the *System Configuration* chapter of the Management Center configuration guide. Firepower-eventing interfaces can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface.

Use `mgmt` interfaces to manage application instances. They can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface. You can only assign one management interface per logical device.

The interface speed that you specify can affect the duplex mode used for an interface, so you must set the speed before setting the duplex mode. If you specify 10- or 100-Mbps speed, the port is automatically configured to use half-duplex mode, but you can specify full-duplex mode instead. If you specify a speed of 1000 Mbps (1Gbps) or faster, full duplex is automatically used.

If you edited the default flow control policy, it is already applied to interfaces. If you created a new policy, you can apply it to the port-channel.

Example

The following example creates Port-Channel 1 with four member interfaces, sets the type to data, and sets the EtherChannel to On mode.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # create port-channel 1
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # set port-type data
firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
firepower /eth-uplink/fabric/port-channel* # commit-buffer
firepower /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
create port-channel	Adds an EtherChannel interface.
scope interface	Enters a physical interface so you can configure and manage the interface settings.

set port-channel-mode

To set the port channel mode for an EtherChannel, use the **set port-channel-mode** command.

set port-channel-mode {**active** | **on**}

Syntax Description

active	Sets the interface in an EtherChannel to be active.
on	Sets the interface in an EtherChannel to be on. Only supported for Data or Data-sharing interfaces.

Command Default

The default mode is active.

Command Modes

scope eth-uplink/scope fabric a/create port-channel/

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

You can configure each physical Data or Data-sharing interface in an EtherChannel to be:

- Active—Sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.
- On—The EtherChannel is always on, and LACP is not used. An “on” EtherChannel can only establish a connection with another “on” EtherChannel.

Non-data interfaces only support active mode.

Example

The following example adds Port-Channel 1 with 4 member interfaces, sets the type to data, and sets the EtherChannel to On mode.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # create port-channel 1
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # set port-type data
firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

Related Commands

Command	Description
create port-channel	Adds an EtherChannel interface.
create member-port	Assigns a member to the EtherChannel.
set port-type	Sets the interface type.

set port-type

To set the port type for an interface, use the **set port-type** command.

set port-type { **cluster** | **data** | **data-sharing** | **firepower-eventing** | **mgmt** }

Syntax Description

cluster	Special interface type used for a clustered logical device. This type is automatically assigned to the cluster control link for inter-unit cluster communications. By default, the cluster control link is automatically created on port-channel 48. For multi-instance clustering, you cannot share a Cluster-type interface across devices. You can add VLAN subinterfaces to the Cluster EtherChannel to provide separate cluster control links per cluster. If you add subinterfaces to a Cluster interface, you cannot use that interface for a native cluster. device manager does not support clustering.
data	Data interfaces cannot be shared between logical devices.
data-sharing	Only supported with container instances, these data interfaces can be shared by one or more logical devices/container instances (threat defense-only). Each container instance can communicate over the backplane with all other instances that share this interface. Shared interfaces can affect the number of container instances you can deploy. Shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode), inline sets, passive interfaces, clusters,or failover links.
firepower-eventing	This interface is a secondary management interface for threat defense devices. To use this interface, you must configure its IP address and other parameters at the threat defense CLI. For example, you can separate management traffic from events (such as web events). See the “Management Interfaces” section in the *System Configuration* chapter of the Management Center configuration guide. Firepower-eventing interfaces can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface.
mgmt	Use management interfaces to manage application instances. They can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface. You can only assign one management interface per logical device.

Command Default

The default type is data.

Command Modes

scope eth-uplink/scope fabric a/scope interface/

scope eth-uplink/scope fabric a/scope interface/create subinterface/

scope eth-uplink/scope fabric a/create port-channel/

scope eth-uplink/scope fabric a/create port-channel/create subinterface/

Command History

Release	Modification
2.8(1)	You can set the **cluster** type on a VLAN subinterface for use with multi-instance clustering.
2.4(1)	We added the **data-sharing** type.
1.1(4)	We added the **firepower-eventing** type.
1.1(1)	Command added.

Usage Guidelines

Container instances can share data-sharing type interfaces. This capability lets you conserve physical interface usage as well as support flexible networking deployments. When you share an interface, the chassis uses unique MAC addresses to forward traffic to the correct instance. However, shared interfaces can cause the forwarding table to grow large due to the need for a full mesh topology within the chassis (every instance must be able to communicate with every other instance that is sharing the same interface). Therefore, there are limits to how many interfaces you can share.

In addition to the forwarding table, the chassis maintains a VLAN group table for VLAN subinterface forwarding. Depending on the number of parent interfaces and other deployment decisions, you can create up to 500 VLAN subinterfaces.

See the following limits for shared interface allocation:

- Maximum 14 instances per shared interface. For example, you can allocate Ethernet1/1 to Instance1 through Instance14.
- Maximum 10 shared interfaces per instance. For example, you can allocate Ethernet1/1.1 through Ethernet1/1.10 to Instance1.

See the following table for interface type support for FTD and ASA applications in standalone and cluster deployments.

Table 1: Interface Type Support

Application		Data	Data: Subinterface	Data-Sharing	Data-Sharing: Subinterface	Mgmt	Firepower-Eventing	Cluster (EtherChannel only)	Cluster: Subinterface
FTD	Standalone Native Instance	**Yes**	—	—	—	**Yes**	**Yes**	—	—
	Standalone Container Instance	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	—	—
	Cluster Native Instance	**Yes** (EtherChannel only for inter-chassis cluster)	—	—	—	**Yes**	**Yes**	**Yes**	—
	Cluster Container Instance	**Yes** (EtherChannel only for inter-chassis cluster)	—	—	—	**Yes**	**Yes**	**Yes**	**Yes**
ASA	Standalone Native Instance	**Yes**	—	—	—	**Yes**	—	**Yes**	—
	Cluster Native Instance	**Yes** (EtherChannel only for inter-chassis cluster)	—	—	—	**Yes**	—	**Yes**	—

Examples

The following example adds Port-Channel 1 with 4 member interfaces, sets the type to data, and sets the EtherChannel to On mode.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # create port-channel 1
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
```

```
firepower /eth-uplink/fabric/port-channel* # set port-type data
firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

The following example adds three subinterfaces and sets the port type to data-sharing.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # enter interface Ethernet1/1
firepower /eth-uplink/fabric/interface # enter subinterface 10
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 10
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # enter subinterface 11
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 11
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # enter subinterface 12
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 12
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
firepower /eth-uplink/fabric/interface/subinterface #
```

Related Commands

Command	Description
create port-channel	Adds an EtherChannel interface.
scope interface	Enters a physical interface so you can configure and manage the interface settings.

set port-type (aggr-interface)

To configure the port type for the interface, use the **set port-type** command.

set port-type { *data* | *data-sharing* | *mgmt* | *firepower-eventing* | *cluster* }

Syntax Description

data	(Optional) Data interfaces cannot be shared between logical devices.
data-sharing	(Optional) Only supported with container instances, these data interfaces can be shared by one or more logical devices/container instances (FTD-only). Each container instance can communicate over the backplane with all other instances that share this interface. Shared interfaces can affect the number of container instances you can deploy. Shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode), inline sets, passive interfaces, or failover links.
mgmt	(Optional) Use management interfaces to manage application instances. They can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface. You can only assign one management interface per logical device.
firepower-eventing	(Optional) This interface is a secondary management interface for FTD devices. To use this interface, you must configure its IP address and other parameters at the FTD CLI. For example, you can separate management traffic from events (such as web events). See the "Management Interfaces" section in the Management Center configuration guide System Configuration chapter. Firepower-eventing interfaces can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface.
cluster	(Optional) Special interface type used for a clustered logical device. This type is automatically assigned to the cluster control link for inter-unit cluster communications. By default, the cluster control link is automatically created on Port-channel 48.

Command Modes

scope cabling/scope fabric a/

Command History

Release	Modification
2.4(1)	Added the **data-sharing** type.
1.1(4)	Added the **firepower-eventing** type.
1.1(1)	Command added.

Usage Guidelines

Container instances can share data-sharing type interfaces. This capability lets you conserve physical interface usage as well as support flexible networking deployments. When you share an interface, the chassis uses unique MAC addresses to forward traffic to the correct instance. However, shared interfaces can cause the forwarding table to grow large due to the need for a full mesh topology within the chassis (every instance

must be able to communicate with every other instance that is sharing the same interface). Therefore, there are limits to how many interfaces you can share.

Example

The following example shows to configure the interface port-type and then list the available commands:

```
firepower-9300* # scope cabling
firepower-9300 /cabling* # scope fabric a
firepower-9300 /cabling/fabric* # create breakout port breakout 2 1
firepower-9300 /cabling/fabric* # show config
 scope fabric a
+    enter breakout 2 3
+    exit
 exit
firepower-9300 /cabling/fabric* # exit
firepower-9300 /cabling* # exit
```

The system reboots after you use the `commit-buffer` command.

```
firepower-9300* # scope eth-uplink
firepower-9300 /eth-uplink* # scope fabric a
firepower-9300 /eth-uplink/fabric* # show

Fabric:
    Fabric ID
    ---------
    Afirepower-9300 /eth-uplink/fabric* # show
  <CR>
  >               Redirect it to a file
  >>              Redirect it to a file in append mode
  aggr-interface  Aggregate Interface
  detail          Detail
  event           Event Management
  expand          Expand
  fault           Fault
  fsm             Fsm
  interface       Interface
  port-channel    Port Channel
  stats           statistics
  |               Pipe command output to filter

firepower-9300 /eth-uplink/fabric* # show aggr-interface expand
firepower-9300 /eth-uplink/fabric* # show aggr-interface
  1-4     Slot
  <CR>
  >       Redirect it to a file
  >>      Redirect it to a file in append mode
  detail  Detail
  expand  Expand
  n/n     Ethernet<Slot Id>/<Aggregate Port Id>
  |       Pipe command output to filter
firepower-9300 /eth-uplink/fabric* # show aggr-interface expand
firepower-9300 /eth-uplink/fabric* #
  acknowledge  Acknowledge
  create       Create managed objects
  delete       Delete managed objects
  enter        Enters a managed object
  scope        Changes the current mode
  show         Show system information
```

```
firepower-9300 /eth-uplink/fabric* # scope aggr-interface
  1-4  Slot
  n/n  Ethernet<Slot Id>/<Aggregate Port Id>

firepower-9300 /eth-uplink/fabric* # scope port-channel 2
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface* # create member-port
Ethernet2/1/1
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* # show config
+enter member-port 2 1
+exit
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* #
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* # exit
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface* # exit
firepower-9300 /eth-uplink/fabric/port-channel* # show config
 enter port-channel 2
     enable
+    enter aggr-interface 2 1
+        enter member-port 2 1
+        exit
+    exit
     enter member-port 1 6
         enable
     exit
     set auto-negotiation no
     set descr ""
     set duplex fullduplex
     set flow-control-policy default
     set lacp-policy-name default
     set nw-ctrl-policy default
     set port-channel-mode active
     set port-type data
     set speed 1gbps
 exit

firepower-9300 /eth-uplink/fabric/port-channel* # set port-type
  cluster             Cluster
  data                Data
  data-sharing        Data Sharing
  firepower-eventing  Firepower Eventing
  mgmt                Mgmt

firepower-9300 /eth-uplink/fabric/port-channel* # set port-type cluster
firepower-9300 /eth-uplink/fabric/port-channel* commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
create port-channel	Adds an EtherChannel interface
scope interface	Edits a physical interface.

set prefix

To set the MAC address prefix to use when autogenerating MAC addresses for container instance interfaces, use the **set prefix** command.

set prefix *prefix*

Syntax Description

prefix	Specifies a decimal value between 1 and 65535. This prefix is converted to a four-digit hexadecimal number, and used as part of the MAC address.

Command Modes

scope ssa/scope auto-macpool/

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

The FXOS chassis automatically generates MAC addresses for container instance interfaces, and guarantees that a shared interface in each instance uses a unique MAC address.

If you manually assign a MAC address to a shared interface within the application, then the manually-assigned MAC address is used. If you later remove the manual MAC address, the autogenerated address is used. In the rare circumstance that the generated MAC address conflicts with another private MAC address in your network, we suggest that you manually set the MAC address for the interface within the application.

Because autogenerated addresses start with A2, you should not start manual MAC addresses with A2 due to the risk of overlapping addresses.

Note Even if you are not sharing a subinterface, if you manually configure MAC addresses, make sure you use unique MAC addresses for all subinterfaces on the same parent interface to ensure proper classification.

The FXOS chassis generates the MAC address using the following format:

A2*xx*.*yyzz*.*zzzz*

Where *xx*.*yy* is a user-defined prefix or a system-defined prefix, and *zz*.*zzzz* is an internal counter generated by the chassis. The system-defined prefix matches the lower 2 bytes of the first MAC address in the burned-in MAC address pool that is programmed into the IDPROM. Use **connect fxos**, then **show module** to view the MAC address pool. For example, if the range of MAC addresses shown for module 1 is b0aa.772f.f0b0 to b0aa.772f.f0bf, then the system prefix will be f0b0.

The user-defined prefix is an integer that is converted into hexadecimal. For an example of how the user-defined prefix is used, if you set a prefix of 77, then the chassis converts 77 into the hexadecimal value 004D (*yyxx*). When used in the MAC address, the prefix is reversed (*xxyy*) to match the chassis native form:

A2**4D**.**00***zz*.*zzzz*

For a prefix of 1009 (03F1), the MAC address is:

A2**F1**.**03***zz*.*zzzz*

Example

The following example sets the MAC prefix to 33.

```
firepower# scope ssa
firepower /ssa # scope auto-macpool
firepower /ssa/auto-macpool # set prefix 33
firepower /ssa/auto-macpool* # commit-buffer
firepower /ssa/auto-macpool
```

Related Commands

Command	Description
scope ssa	Enters ssa mode.
scope auto-macpool	Enter auto-macpool mode.
show mac-address	Shows the assigned MAC addresses.

set protocol

To specify the protocol to use when communicating with the remote server for the export policy, use the **set protocol** command.

set protocol { **ftp** | **scp** | **sftp** | **tfp** }

Syntax Description

ftp	Specifies the File Transfer Protocol (FTP) for file transfer.
scp	Specifies the Secure Copy Protocol (SCP) for file transfer.
sftp	Specifies the Secure File Transfer Protocol (SFTP) for file transfer.
tfp	Specifies the Trivial File Transfer Protocol (TFTP) for file transfer.

Command Modes

Configuration export policy (/org/cfg-export-policy)

Command History

Release	Modification
2.0.1	Command added.

Usage Guidelines

Use this command to specify a file transfer protocol.

Example

This example shows how to set the port number for the export policy:

```
firepower-9300* # scope org
firepower-9300 /org* # scope cfg-export-policy default
firepower-9300 /org/cfg-export-policy* # set protocol scp
firepower-9300 /org/cfg-export-policy* # commit-buffer
firepower-9300 /org/cfg-export-policy #
```

Related Commands

Command	Description
set adminstate (/org)	Enables the export policy.
set hostname (/org)	Specifies the hostname location where the backup file must be stored.
set password (/org)	Specifies the password for the remote server username.
set port (/org)	Specifies the port number.
set protocol (/org)	Specifies the protocol to use when communicating with the remote server.
set remote-file (/org)	Specifies the full path to where you want the configuration file exported including the filename.
set schedule (/org)	Specifies the schedule on which you would like to have the configuration automatically exported.

Command	Description
set user (/org)	Specifies the username the system should use to log in to the remote server.

set realm

To specify the default authentication service, use the **set realm** command.

set realm {**ldap** | **local** | **none** | **radius** | **tacacs**}

Syntax Description

ldap	Specifies LDAP authentication.
local	Specifies local authentication.
none	Allows local users to log on without specifying a password.
radius	Specifies RADIUS authentication.
tacacs	Specifies TACACS+ authentication.

Command Modes

Default authentication mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter security/default-auth mode and set the default authentication service to Radius:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set realm radius
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set auth-server-group	Specifies an associated authentication provider group.
set use-2-factor	Sets the authentication method to two-factor authentication for a Radius or TACACS+ realm.

set refresh-period

To set the Web session refresh period—the maximum time allowed between refresh requests for a user in this domain—use the **set refresh-period** command.

set refresh-period *seconds*

Syntax Description

seconds	Number of seconds after which a Web session is considered inactive. Value can be 0 to 3600 seconds; default is 600 seconds.

Command Modes

Default authentication mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If this time limit is exceeded, FXOS considers the Web session to be inactive, but it does not terminate the session.

Example

This example shows how to enter default authentication mode and set the session refresh interval:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set refresh-period 800
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set timeout values	The **set absolute-session-timeout**, **set con-absolute-session-timeout**, **set con-session-timeout**, and **set session-timeout** commands are used to set various timeout values.

set regenerate

To regenerate the keys in the default keyring, use the **set regenerate** command.

set regenerate {**no** | **yes**}

Syntax Description

no	Do not regenerate the keys.
yes	Regenerate the keys.

Command Modes

Keyring mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to regenerate the RSA keys in the default keyring. This command is accepted only in the default keyring.

Example

This example shows how to regenerate the keys in the default keyring:

```
FP9300-A# scope security
FP9300-A /security # scope keyring default
FP9300-A /security/keyring # set regenerate yes
FP9300-A /security/keyring* # commit-buffer
switch-A /security/keyring #
```

Related Commands

Command	Description
set cert	Enters an RSA certificate for a keyring.
set modulus	Specifies the RSA key modulus (SSL key length) in bits.
set trustpoint	Specifies whether the keyring certificate can be regenerated.

set remote-address

To specify the remote IP address for an IPSec connection, use the **set remote-address** command.

set remote-address *ip_address*

Syntax Description

ip_address	Provide an IPv4 or IPv6 remote gateway address for the IPSec connection; maximum of 510 characters.

Command Modes

Connection (/security/ipsec/connection) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command and the **set local-address** command to define the endpoints of an IPSec connection.

Example

This example shows how to set the remote address for an IPSec connection:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set local-address 209.165.202.129
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Command	Description
create connection	Creates a new IPSec connection.
set local-addr	Sets the local IP address for an IPSec connection.

set remote-ike-ident

To specify the remote peer IKE identity for an IPSec tunnel connection, use the **set remote-ike-ident** command.

set remote-ike-ident *remote_ID*

Syntax Description

remote_ID	The IKE identification of the remote peer; maximum of 510 characters.

Command Modes

Connection (/security/ipsec/connection) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to specify the remote peer's IKE ID for an IPSec connection. This identification is used for peer validation during IKE negotiations.

Example

This example shows how to specify the remote IKE ID for an IPSec connection:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set remote-ike-ident 203.0.113.12
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Command	Description
create connection	Creates a new IPSec connection.
set remote-addr	Sets the remote IP address for an IPSec connection.

set remote-subnet

To specify the remote subnet for an IPSec tunnel connection, use the **set remote-subnet** command.

set remote-subnet *ip_address/mask_bits*

Syntax Description

ip_address/mask_bits	Provide an IPv4 or IPv6 remote subnet address/mask for the IPSec connection; maximum of 510 characters.

Command Modes

Connection (/security/ipsec/connection) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to specify the IP address/mask of an IPSec connection's remote subnet.

Example

This example shows how to set the remote subnet for an IPSec connection:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set remote-subnet 209.165.202.128/27
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Command	Description
create connection	Creates a new IPSec connection.
set remote-addr	Sets the remote IP address for an IPSec connection.

set remote-user

To restrict access to those users matching an established user role, use the **set remote-user** command.

set remote-user default-role { **assign-default-role** | **no-login** }

Syntax Description

assign-default-role	When a user attempts to log in and the remote authentication provider does not supply a user role with the user's authentication information, the user is allowed to log in with a read-only user role.
no-login	When a user attempts to log in and the remote authentication provider does not supply a user role with the user's authentication information, access is denied.

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

assign-default-role is the default behavior.

Example

This example shows how to enter security mode and deny access to users without a user role:

```
FP9300-A# scope security
FP9300-A /security # set remote-user default-role no-login
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

Related Commands

Command	Description
set authentication	Specifies the default authentication service.

set reporting-interval

To define how frequently monitored statistics are reported, use the **set reporting-interval** command.

set reporting-interval *interval*

Syntax Description

interval	Length of time defining the statistics reporting interval; available values are: • `15minutes` – 15-minute intervals • `2hours` – two-hour (120-minute) intervals • `2minutes` – two-minute intervals • `30minutes` – 30-minute intervals • `4hours` – four-hour (240-minute) intervals • `60minutes` – 60-minute (one-hour) intervals • `8hours` – eight-hour (480-minute) intervals

Command Modes

scope monitoring/scope stats-collection-policy/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use the **set collection-interval** command to define how frequently statistics are collected, and use the **set reporting-interval** command to define how frequently the statistics are reported. These intervals define a statistics collection policy.

Reporting intervals are longer than collection intervals so that multiple statistical data points can be collected during the reporting interval, which provides sufficient data to calculate and report minimum, maximum, and average values.

Statistics can be collected and reported for each of the following functional areas of your Firepower system; use the **scope stats-collection-policy** command to access a specific collection policy:

- `Adapter` – statistics related to the adapters.
- `Chassis` – statistics related to the blade chassis.
- `FEX` – statistics related to configured Fabric Extender(s).
- `Host` – this policy is a placeholder for future support.
- `Port` – statistics related to the ports, including server ports, uplink Ethernet ports, and uplink Fibre Channel ports.
- `Server` – statistics related to servers.

Note There is one default statistics collection policy for each of the functional areas. You cannot create additional statistics collection policies and you cannot delete the existing default policies. You can only modify the default policies.

Example

This example shows how to enter the statistics collection policy for ports, set the collection interval to one minute, set the reporting interval to 30 minutes, and then commit the transaction:

```
firepower # scope monitoring
firepower /monitoring # scope stats-collection-policy port
firepower /monitoring/stats-collection-policy # set collection-interval 1minute
firepower /monitoring/stats-collection-policy* # set reporting-interval 30minute
firepower /monitoring/stats-collection-policy* # commit-buffer
firepower /monitoring/stats-collection-policy #
```

Related Commands

Command	Description
scope stats-collection-policy	Enters stats-collection-policy mode, where you manage statistics collection and reporting intervals.
set collection-interval	Specifies how frequently statistics are collected.

set resource-profile-name

To set the resource profile for an application instance, use the **set resource-profile-name** command.

set resource-profile-name *profile_name*

Syntax Description

profile_name	Sets the resource profile name for this application instance.

Command Modes

scope ssa/scope slot/create app-instance/

Command History

Release	Modification
2.4(1)	Can now be used for container instances.
1.1(1)	Command added for use with vDP.

Usage Guidelines

For vDP, resource profiles are pre-created in the FXOS configuration when you download the vDP image. For container instances, create resource profiles using the **create resource-profile**command. Use the **show resource-profile system** command to view available profiles.

If you change the resource profile for an application instance that is running, then the instance reboots.

Example

The following example shows how to set the the resource profile for a vDP application instance:

```
firepower# scope ssa
firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default App

    ---------- --------------- ---------- ---------------------- ----------- --------------

    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
    vdp        8.13.01.09-2    radware    Vm                     Application Yes

firepower /ssa # show resource-profile system
Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core Count
 RAM Size (MB)  Default Profile Profile Type Description
----------------- ---------- ------------ ---------- --------------- ----------------------
 -------------- --------------- ------------ -----------
DEFAULT-4110-RESOURCE
                   vdp        8.13.01.09-2 No         FPR4K-SM-12
 4          16384 Yes             System
DEFAULT-RESOURCE   vdp        8.13.01.09-2 No        FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

 6          24576 Yes             System
VDP-10-CORES       vdp        8.13.01.09-2 No        FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

10          40960 No              System
VDP-2-CORES        vdp        8.13.01.09-2 No         all
 2           8192 No              System
```

```
VDP-4-CORES         vdp         8.13.01.09-2 No          all
 4          16384 No              System
VDP-8-CORES         vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

 8          32768 No              System
firepower /ssa/app # exit
firepower /ssa # scope slot 1
firepower /ssa/slot # create app-instance vdp VDP1
firepower /ssa/slot/app-instance* # set resource-profile-name VDP-10-CORES
firepower /ssa/slot/app-instance* #
```

Example

The following example shows how to set the the resource profile for a threat defense container instance:

```
firepower# scope ssa
firepower /ssa # show resource-profile

Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core Count
 RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- --------------- ----------------------
 -------------- --------------- ------------ -----------
bronze              N/A        N/A          No          all
 6            N/A No              Custom       low end device
silver              N/A        N/A          No          all
 8            N/A No              Custom       mid-level

firepower /ssa # scope slot 1
firepower /ssa/slot # create app-instance ftd FTD1
firepower /ssa/slot/app-instance* # set resource-profile-name silver
firepower /ssa/slot/app-instance* #
```

Related Commands

Command	Description
show app-attri	Shows current application attributes.
create resource-profile	Creates a resource profile for use with constainer instances.
show resource-profile-name	Shows available resource profiles.

set session-timeout

To set the idle session timeout for Web, SSH, and Telnet sessions, use the **set session-timeout** command.

set session-timeout *seconds*

Syntax Description

seconds	Idle session timeout for Web, SSH, and Telnet sessions; value can be 0 to 3600 seconds.

Command Modes

Default authentication mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to specify the idle session timeout for Web, SSH, and Telnet sessions.

Example

This example shows how to enter default authentication mode and then set the idle session timeout to four minutes:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set session-timeout 240
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set refresh-period	Sets the Web session refresh period.
show detail	Displays the current session and absolute session timeout settings.

set snmp-adminappinstance

To set Simple Network Management Protocol (SNMP) admin app-instance configuration parameters, use the **set snmp adminappinstance** command.

set snmp adminappinstance { **slot | appname | id | enable | yes/no** }

Syntax Description

slot	Slot selection between 1-3
appname	Displays appname
id	Displays Identifier name
enable	Select **yes/no** to enable/disable

Command Modes

scope monitoring

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

Cisco recommends that you enable only communication services needed to interact with other network applications. So, you must enable the SNMP agent (**enable snmp**).

This is a subcommand of the **show** command in scope monitoring.

Example

This example shows how to display information of snmp:

```
Firepower /monitoring # set snmp adminappinstance
  slot  Slot
Firepower /monitoring # set snmp adminappinstance slot
  1-3  Admin App Slot
Firepower /monitoring # set snmp adminappinstance slot 1
  appname  AppName
Firepower /monitoring # set snmp adminappinstance slot 1 appname
  WORD  Admin App Name (Min size 0, Max size 510)
Firepower /monitoring # set snmp adminappinstance slot 1 appname ftd
  id  Id
Firepower /monitoring # set snmp adminappinstance slot 1 appname ftd id
  WORD  Admin App Id (Min size 0, Max size 510)
Firepower /monitoring # set snmp adminappinstance slot 1 appname ftd id FTD
  enable  Enable
Firepower /monitoring # set snmp adminappinstance slot 1 appname ftd id FTD enable
  no   No
  yes  Yes
Firepower /monitoring # set snmp adminappinstance slot 1 appname ftd id FTD enable yes
Firepower /monitoring* # commit-buffer

Firepower /monitoring #
Firepower /monitoring # show snmp
Name: snmp
    Admin State: Enabled
```

```
Port: 161
Is Community Set: No
Sys Contact:
Sys Location:
Admin App Enable: Yes
    Admin App Slot: 1
    Admin App Name: ftd
    Admin App Id: FTD
```

set snmp

To set Simple Network Management Protocol (SNMP) configuration parameters, use the **set snmp** command.

set snmp {**community** | **syscontact** | **syslocation**}

Syntax Description

community	After you enter this command, you are asked to enter a SNMP community name, which can be between 1 and 32 alphanumeric characters. The community name is not displayed as you type; however after you press **Enter**, the system prompt is displayed with an asterisk indicating you need to commit the buffer.
syscontact *name*	Enter the name of the person to contact regarding SNMP on this system; can be 0 to 255 alphanumeric characters.
syslocation *location*	Enter a location for this system; can be 0 to 510 alphanumeric characters.

Command Modes

scope monitoring/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

Cisco recommends that you enable only the communication services needed to interact with other network applications.

You must enable the SNMP agent (**enable snmp**) before configuring SNMP on this system.

Use **set snmp community** to specify the community access string used to permit access to the SNMP trap destination. If SNMPv1 or v2c is set as the SNMP version, the community argument is used as the community string. If SNMPv3 is configured, it is used as the SNMP user name for sending trap messages.

When you specify an SNMP community name, you are also automatically enabling SNMP versions 1 and 2c for polling requests from the SNMP remote manager.

Note Be aware that SNMP versions 1 and 2c have serious known security issues: they transmit all information without encryption, including the community string, which serves as the only form of authentication in these versions.

There can be only one community name; however, you can use **set snmp community** to overwrite the existing name. To delete an existing community name, enter **set snmp community** but do not type a community string; that is, simply press **Enter** again. After you commit the buffer, **show snmp** output will include the line `Is Community Set: No`.

Example

The following example shows you how to scope into monitoring mode, enable SNMP processing, set the SNMP community string and a system contact, commit your changes, and use the **show snmp** command to confirm the changes:

```
firepower # scope monitoring
firepower /monitoring # enable snmp
firepower /monitoring* # set snmp community
Enter a snmp community:
firepower /monitoring* # set snmp syscontact R_Admin
firepower /monitoring* # commit-buffer
firepower /monitoring # show snmp
Name: snmp
    Admin State: Enabled
    Port: 161
    Is Community Set: Yes
    Sys Contact: R_Admin
    Sys Location:
firepower /monitoring #
```

Related Commands

Command	Description
disable snmp	Disables SNMP.
enable snmp	Enables SNMP.
show snmp	Shows the current SNMP configuration.

set (snmp-trap)

To specify Simple Network Management Protocol (SNMP) trap parameters, use the **set** command in snmp-trap mode.

set { **community** | **notificationtype** | **port** | **v3privilege** | **version** }

Syntax Description

community	Specifies the SNMPv1/v2c community string, or the SNMPv3 user name, to permit access to the trap destination. You are queried for the community name after you enter this command. The name can be up to 32 characters with no spaces; the name is not displayed as you type.
notificationtype { **informs** | **traps** }	Specifies the type of SNMP notification produced by this agent: • **informs** – These are unsolicited notifications sent to notify the manager of significant local events. These messages are acknowledged. This option can be used only if **version** is set to **vc2**. • **traps** – These are unsolicited notifications sent to notify the manager of significant local events. These messages are not acknowledged.
port *port_num*	Use this command to change the port on which the agent receives SNMP requests; the default port is 161.
v3privilege { **auth** | **noauth** | **priv** }	Use this command to specify the Simple Network Management Protocol version 3 (SNMPv3) security level for the transmitted SNMP traps. • **auth** – Specifies keyed-hash authentication but no encryption. • **noauth** – Specifies no authentication or encryption. Note that while you can specify it, FXOS does not support this security level with SNMPv3. • **priv** – Specifies keyed-hash authentication and data encryption (privacy).
version { **v1** | **v2c** | **v3** }	Use this command to specify the SNMP security model used when sending trap notifications: • **v1** – Specifies SNMP version 1. • **v2c** – Specifies SNMP version 2c. • **v3** – Specifies SNMP version 3. **Note** Be aware that SNMP versions 1 and 2c have serious known security issues: they transmit all information without encryption, including the community string, which serves as the only form of authentication in these versions.

Command Modes

scope monitoring/snmp-trap

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

You must enable SNMP (**enable snmp**), and create an SNMP community (**set snmp community**), before you create an SNMP trap and set these parameters.

When you create a new SNMP trap, you are automatically entered into monitoring/snmp-trap mode with an asterisk indicating the new trap is not yet committed.

Note You can create up to eight SNMP traps.

If SNMPv1 or v2c is configured with **set version**, the **set community** argument is used as the community string. If SNMPv3 is configured, it is used as the user name for transmitting the notifications.

With SNMPv3, the trap's **v3privilege** setting must be compatible with the associated SNMPv3 user's security level; that is, the associated user's security configuration must be at least as secure as the trap's. For example, if authentication is enabled for the SNMPv3 user (perform authentication but not privacy encryption), then the user's priv-password would not be set. But to send notifications with privacy enabled (that is, authenticate and do privacy encryption) the user's priv-password would be set. The password associated with the SNMPv3 user is used to authenticate the user when a trap/inform is sent.

Example

The following example enables SNMP, creates an SNMP trap using an IPv4 address, sets the version to v3, sets the v3 privilege level to privacy, and commits the transaction:

```
firepower # scope monitoring
firepower /monitoring/ # enable snmp
firepower /monitoring/ # create snmp-trap 192.168.100.112
firepower /monitoring/snmp-trap* # set notificationtype traps
firepower /monitoring/snmp-trap* # set version v3
firepower /monitoring/snmp-trap* # set v3privilege priv
firepower /monitoring/snmp-trap* # commit-buffer
firepower /monitoring/snmp-trap #
```

Related Commands

Command	Description
create snmp-trap	Creates a new SNMP trap destination.
enable snmp	Enables SNMP.

set (snmp-user)

To specify parameters for an existing Simple Network Management Protocol (SNMP) v3 user, use the **set** command in `snmp-user` mode.

set {**aes-128** | **auth** | **password** | **priv-password**}

Syntax Description

aes-128 {**no** | **yes**}	Disable or enable the use of Advanced Encryption Standard (AES)-128 encryption: enter `no` or `yes`. By default, AES-128 encryption is disabled.
auth sha	Enables authentication for SNMPv3 users based on the HMAC Secure Hash Algorithm (SHA).
password	Specify a password for this user; you are asked to enter the password, and confirm it, after you enter this command.
priv-password	Specify a user privacy password; you are asked to enter the password, and confirm it, after you enter this command. The AES privacy password must be a minimum of eight characters.

Command Modes

scope monitoring/snmp-user

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

You must enable SNMP (**enable snmp** before you create an SNMP user and set these parameters.

When you create a new SNMP user, you are automatically entered into monitoring/snmp-user mode with an asterisk indicating the new user is not yet committed.

The privacy password, or priv option, offers a choice of DES or 128-bit AES encryption for SNMP security encryption. If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, the Firepower chassis uses the privacy password to generate a 128-bit AES key.

Example

The following example creates an SNMPv3 user named `snmp-user14`, enables AES-128 encryption, sets a privacy password, and commits the transaction:

```
firepower # scope monitoring
firepower /monitoring/ # enable snmp
firepower /monitoring/ # create snmp-user snmp-user14
Password:
firepower /monitoring/snmp-user* # set aes-128 yes
firepower /monitoring/snmp-user* # set priv-password
Enter a password:
Confirm the password:
firepower /monitoring/snmp-user* # commit-buffer
firepower /monitoring/snmp-user #
```

Related Commands

Command	Description
create snmp-user	Creates a new SNMPv3 user.
enable snmp	Enables SNMP.

set speed

To set the interface speed., use the **set speed** command.

Note This command is available in port-channel scope only.

set speed { **10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps** }

Syntax Description

10mbps	(Optional) Sets the speed at 10 Mbps.
100mbps	(Optional) Sets the speed at 100 Mbps.
1gbps	(Optional) Sets the speed at 1 Gbps.
10gbps	(Optional) Sets the speed at 10 Gbps.
40gbps	(Optional) Sets the speed at 40 Gbps.
100gbps	(Optional) Sets the speed at 100 Gbps.

Command Modes

scope eth-uplink/scope fabric a/port-channel/

Command History

Release	Modification
2.4.1(1)	Command added.

Usage Guidelines

The interface speed that you specify can affect the duplex mode used for an interface, so you must set the speed before setting the duplex mode. If you specify 10- or 100-Mbps speed, the port is automatically configured to use half-duplex mode, but you can specify full-duplex mode instead. If you specify a speed of 1000 Mbps (1Gbps) or faster, full duplex is automatically used.

Example

This example shows how to set the interface speed:

```
firepower-9300 # scope eth-uplink
firepower-9300 /eth-uplink # scope fabric a
firepower-9300 /eth-uplink/fabric # create port-channel id
firepower-9300 /eth-uplink/fabric/port-channel* # enable
firepower-9300 /eth-uplink/fabric/port-channel* # set speed
firepower-9300 /eth-uplink/fabric/port-channel* # set speed 1gbps
firepower-9300 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
duplex	Specifies the duplex mode as full or half.

Command	Description
show interface	Displays the interface status, which includes the speed parameters.

set speed (aggr-interface)

To set the speed of the interface, use the **set speed** command.

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

Syntax Description

10mbps	(Optional) Sets the speed at 10 Mbps.
100mbps	(Optional) Sets the speed at 100 Mbps.
1gbps	(Optional) Sets the speed at 1 Gbps.
10gbps	(Optional) Sets the speed at 10 Gbps.
40gbps	(Optional) Sets the speed at 40 Gbps.
100gbps	(Optional) Sets the speed at 100 Gbps.

Command Modes

scope eth-uplink/scope fabric a/port-channel/

Command History

Release	Modification
2.4.1(1)	Command added.

Usage Guidelines

The interface speed that you specify can affect the duplex mode used for an interface, so you must set the speed before setting the duplex mode. If you specify 10- or 100-Mbps speed, the port is automatically configured to use half-duplex mode, but you can specify full-duplex mode instead. If you specify a speed of 1000 Mbps (1Gbps) or faster, full duplex is automatically used.

This example shows how to set the interface speed:

```
firepower-9300* # scope cabling
firepower-9300 /cabling* # scope fabric a
firepower-9300 /cabling/fabric* # create breakout port breakout 2 1
firepower-9300 /cabling/fabric* # show config
 scope fabric a
+    enter breakout 2 3
+    exit
 exit
firepower-9300 /cabling/fabric* # exit
firepower-9300 /cabling* # exit
firepower-9300* # scope eth-uplink
firepower-9300 /eth-uplink* # scope fabric a
firepower-9300 /eth-uplink/fabric* # show

Fabric:
    Fabric ID
    ---------
    A
firepower-9300 /eth-uplink/fabric* # show
  <CR>
  >               Redirect it to a file
  >>              Redirect it to a file in append mode
  aggr-interface  Aggregate Interface
```

```
  detail          Detail
  event           Event Management
  expand          Expand
  fault           Fault
  fsm             Fsm
  interface       Interface
  port-channel    Port Channel
  stats           statistics
  |               Pipe command output to filter

firepower-9300 /eth-uplink/fabric* # show aggr-interface expand
firepower-9300 /eth-uplink/fabric* # show aggr-interface
  1-4     Slot
  <CR>
  >       Redirect it to a file
  >>      Redirect it to a file in append mode
  detail  Detail
  expand  Expand
  n/n     Ethernet<Slot Id>/<Aggregate Port Id>
  |       Pipe command output to filter
firepower-9300 /eth-uplink/fabric* # show aggr-interface expand
firepower-9300 /eth-uplink/fabric* #
  acknowledge  Acknowledge
  create       Create managed objects
  delete       Delete managed objects
  enter        Enters a managed object
  scope        Changes the current mode
  show         Show system information

firepower-9300 /eth-uplink/fabric* # scope aggr-interface
  1-4  Slot
  n/n  Ethernet<Slot Id>/<Aggregate Port Id>

firepower-9300 /eth-uplink/fabric* # scope port-channel 2
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface* # create member-port
Ethernet2/1/1
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* # show config
+enter member-port 2 1
+exit
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* # exit
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface* # exit
firepower-9300 /eth-uplink/fabric/port-channel* # show config
 enter port-channel 2
     enable
+    enter aggr-interface 2 1
+        enter member-port 2 1
+        exit
+    exit
     enter member-port 1 6
         enable
     exit
     set auto-negotiation no
     set descr ""
     set duplex fullduplex
     set flow-control-policy default
     set lacp-policy-name default
     set nw-ctrl-policy default
     set port-channel-mode active
     set port-type data
     set speed 1gbps
 exit
firepower-9300 /eth-uplink/fabric/port-channel* # set speed
  100gbps  100 Gbps
  100mbps  100 Mbps
```

```
  10gbps   10 Gbps
  10mbps   10 Mbps
  1gbps    1 Gbps
  40gbps   40 Gbps

firepower-9300 /eth-uplink/fabric/port-channel* # set speed 1gbps
firepower-9300 /eth-uplink/fabric/port-channel* commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
duplex	Specifies the duplex mode as full or half.
show interface	Displays the interface status, which includes the speed parameters.

set ssh-server

To set the SSH host key size, use the **set ssh-server** command.

set ssh-server host-key rsa *key_size*

Syntax Description

rsa	Specifies the host key type.
key-size	The size of the host key.

Command Modes

Services mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to set the SSH host key size.

Example

This example shows how to set the SSH host key size to 2048 bits:

```
FP9300-A # scope system
FP9300-A /system # scope services
FP9300-A /system/services # set ssh-server host-key rsa 2048
FP9300-A /system/services* # commit-buffer
FP9300-A /system/services #
```

Related Commands

Command	Description
create ssh-server	Creates a new SSH server host key.
delete ssh-server	Deletes the existing SSH host key.
show ssh-server	Shows the host key size.

set sshkey

To specify an SSH key that allows access without a password, use the **set sshkey** command.

set sshkey [**none** | *user_ssh_key*]

Syntax Description

none	(Optional) Enter the **none** keyword to clear the user's SSH public key.
user_ssh_key	(Optional) Enter or paste the user's public SSH key.

Command Modes

Local user mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If you press **Enter** after entering **set sshkey**, you are prompted to provide the SSH key, one line at a time. Enter ENDOFBUF to finish. Press Ctrl-C to abort.

Example

This example shows how to specify a public SSH key for the current local user:

```
FP9300-A /security/local-user # set sshkey
"ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw85lkdQqap+NFuNmHcb4K
iaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VOIEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpD
 m8HPh2LOgyH7Ei1MI8="
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Related Commands

Command	Description
create local-user	Creates a new local-user account.
set password	Specifies a password for a user account.

set startup-version

To specify the startup version of an application, use the **set startup-version** command.

set startup-version

Syntax Description

startup-version	The startup software version of an application instance

Command Modes

scope ssa

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If you press **Enter** after **scope app-instance ftd ftd1** , you are prompted to set the startup version.

Example

This example shows how to set the startup version for an ftd application:

```
FPR# scope ssa
FPR /ssa # scope slot 1
FPR /ssa/slot # scope app-instance ftd ftd1
FPR /ssa/slot/app-instance # set startup-version 6.6.1.91
Warning: Upgrade of ftd through FXOS is not supported. The specified version of ftd will
be installed. Please reinitialize or reinstall ftd.
```

set timezone

To set the timezone in FXOS, use the **set timezone** command.

set timezone

Syntax Description		
	set timezone	Use the command set timezone to set the timezone in FXOS

Command Modes

scope system/scope services

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to set the timezone in FXOS.

Example

This example shows how to set the timezone in FXOS:

```
firepower# scope system
firepower /system# scope services
firepower /system/services # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean


#? 8 <====== Europe


Please select a country.
 1) Aaland Islands        18) Greece               35) Norway
 2) Albania               19) Guernsey             36) Poland
 3) Andorra               20) Hungary              37) Portugal
 4) Austria               21) Ireland              38) Romania
 5) Belarus               22) Isle of Man          39) Russia
 6) Belgium               23) Italy                40) San Marino
 7) Bosnia & Herzegovina  24) Jersey               41) Serbia
 8) Britain (UK)          25) Latvia               42) Slovakia
 9) Bulgaria              26) Liechtenstein        43) Slovenia
10) Croatia               27) Lithuania            44) Spain
11) Czech Republic        28) Luxembourg           45) Sweden
12) Denmark               29) Macedonia            46) Switzerland
13) Estonia               30) Malta                47) Turkey
14) Finland               31) Moldova              48) Ukraine
15) France                32) Monaco               49) Vatican City
16) Germany               33) Montenegro
17) Gibraltar             34) Netherlands

#? 36 <======Poland

The following information has been given:
```

```
        Poland

Therefore timezone 'Europe/Warsaw' will be set.
Local time is now:      Sun Oct 24 08:51:04 CEST 2021.
Universal Time is now:  Sun Oct 24 06:51:04 UTC 2021.
Is the above information OK?
1) Yes
2) No


#? 1 <======== Yes

firepower /system/services* # commit
firepower /system/services # show timezone
Timezone: Europe/Warsaw <======= Timezone is set

To set the timezone to UTC:

firepower /system/services* # set timezone UTC
firepower /system/services* # commit
```

set trustpoint

To set the certificate trustpoint for a keyring, use the **set trustpoint** command.

set trustpoint *trustpoint_name*

Syntax Description

trustpoint_name	Name of a defined trustpoint. This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

Command Modes

scope security/scope keyring/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to specify the trusted point that signed this keyring's certificate.

Example

This example shows how to regenerate the keys in the default keyring:

```
firepower# scope security
firepower /security # scope keyring test-ring
firepower /security/keyring # set trustpoint CiscoCA5
firepower /security/keyring* # commit-buffer
firepower /security/keyring #
```

Command	Description
set cert	Enters an RSA certificate for a keyring.
set modulus	Specifies the RSA key modulus (SSL key length) in bits.
set regenerate	Regenerates the RSA keys in the default keyring.

set use-2-factor

To enable and disable two-factor authentication for the authentication realm, use the **set use-2-factor** command.

Note Two-factor authentication applies only to RADIUS and TACACS+ realms.

set use-2-factor {**no** | **yes**}

Syntax Description

no	Disables two-factor authentication for the realm.
yes	Enables two-factor authentication for the realm.

Command Modes

Default authentication mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If you set two-factor authentication for a RADIUS or TACACS+ realm, consider increasing the session-refresh and session-timeout periods so that remote users do not have to re-authenticate too frequently.

Example

This example shows how to enter default authentication mode and enable two-factor authentication:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set use-2-factor yes
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set authentication	Specifies the default authentication service.
set timeout values	The **set absolute-session-timeout**, **set con-absolute-session-timeout**, **set con-session-timeout**, and **set session-timeout** commands are used to set various timeout values.

set user-account-unlock-time

To specify the amount of time a user remains locked out of the system after reaching the maximum number of login attempts, use the **set user-account-unlock-time** command.

set user-account-unlock-time *unlock_time*

Syntax Description

unlock_time	The amount of time in seconds a user remains locked out of the system. The value can range from 600 to 36000; the default is 1800 seconds (30 minutes).

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If any user (including admin users) exceeds the specified maximum number of login attempts, the user is locked out of the system and must wait this amount of time before being allowed to log in again. No notification appears indicating that the user is locked out.

Example

This example shows how to enter security mode and specify the amount of time that must pass before a locked-out user can log in again:

```
FP9300-A # scope security
FP9300-A /security # set user-account-unlock-time 900
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

Related Commands

Command	Description
clear lock-status	Clears a user's locked-out status.
set max-login-attempts	Specifies the maximum number of failed login attempts before the user is locked out of the system.

set user-label

To assign a user-defined identifier to the appliance chassis, use the **set user-label** command in `chassis/` mode.

To assign a user-defined identifier to one of the installed servers, use the **set user-label** command in `server/` mode.

set user-label *user_label*

Syntax Description

user_label	The label you want assigned to the appliance or server; maximum of 32 characters.

Command Modes

scope chassis/

scope chassis/scope server

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can use the **show detail** command in `chassis/` mode to view the user label currently assigned to the chassis.

You can use the **show detail** command in `chassis/server/` mode to view the user label currently assigned to the connected server.

Example

This example shows how to assign a user-defined label to the appliance chassis:

```
firepower # scope chassis 1
firepower /chassis # set user-label FP9300-4
firepower /chassis* # commit-buffer
firepower /chassis # show detail

Chassis:
    Chassis: 1
    User Label: FP9300-4
    Overall Status: Operable
    Oper qualifier: N/A
    Operability: Operable
    Conf State: Ok
    Admin State: Acknowledged
    Conn Path: A
    Conn Status: A
    Managing Instance: A
    Product Name: Cisco Firepower 9300 Security Appliance AC
    PID: FPR-C9300-AC
    VID: V02
    Part Number: 68-100280-04
    Vendor: Cisco Systems Inc
    Model: FPR-C9300-AC
    Serial (SN): JMX1950196H
    HW Revision: 0
```

```
    Mfg Date: 2015-12-16T00:00:00.000
    Power State: Ok
    Thermal Status: Ok
    SEEPROM operability status: Operable
    Dynamic Reallocation: Chassis
    Reserved Power Budget (W): 600
    PSU Capacity (W): 0
    PSU Line Mode: High Line
    PSU State: Ok
    Current Task:
firepower /chassis #
```

Related Commands

Command	Description
show detail	In `chassis/` mode, shows detailed chassis information including the chassis' current user label. In `chassis/server/` mode, shows detailed server information including the connected server's user label.

set value (create bootstrap-key FIREWALL_MODE)

To specify the firewall mode, routed or transparent, in the bootstrap configuration for the threat defense and ASA, use the **set value** command.

set value {**routed** | **transparent**}

Syntax Description

routed	Sets the firewall mode to routed firewall mode.
transparent	Sets the firewall mode to transparent firewall.

Command Modes

scope ssa/create logical-device/create mgmt-bootstrap/create bootstrap-key FIREWALL_MODE/

Command Default

The default mode is routed.

Command History

Release	Modification
2.4(1)	Added support for the ASA.
1.1(4)	Command added for FTD.

Usage Guidelines

Bootstrap settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can change most values in the application CLI configuration.

Example

The following example shows how to set the mode to routed mode:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

Related Commands

Command	Description
create bootstrap-key FIREWALL_MODE	Sets the firewall mode for the application.
create logical-device	Creates the logical device.
create mgmt-bootstrap	Creates the bootstrap configuration for the application.

set value (create bootstrap-key MANAGEMENT_TYPE)

To specify the manager, FMC or FDM, in the bootstrap configuration for the threat defense, use the **set value** command.

set value {**FMC** | **LOCALLY_MANAGED**}

Syntax Description

FMC	Sets the manager to FDM.
LOCALLY_MANAGED	Sets the manager to FMC.

Command Modes

scope ssa/create logical-device/create mgmt-bootstrap/create bootstrap-key LOCALLY_MANAGED/

Command Default

The default manager is FMC.

Command History

Release	Modification
2.7(1)	Command added for FTD.

Usage Guidelines

Bootstrap settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can change most values in the application CLI configuration.

Example

The following example shows how to set the manager to FDM:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key MANAGEMENT_TYPE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value LOCALLY_MANAGED
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

Related Commands

Command	Description
create bootstrap-key FIREWALL_MODE	Sets the firewall mode for the application.
create logical-device	Creates the logical device.
create mgmt-bootstrap	Creates the bootstrap configuration for the application.

set value (create bootstrap-key PERMIT_EXPERT_MODE)

To permit Expert Mode from FTD SSH sessions for the threat defense, use the **set value** command.

set value {**yes** | **no**}

Syntax Description

no	Disallows Expert Mode from an SSH session to the threat defense.
yes	Allows an Expert Mode from an SSH session to the threat defense.

Command Modes

scope ssa/create logical-device/create mgmt-bootstrap/create bootstrap-key PERMIT_EXPERT_MODE/

Command Default

The default is no.

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

Expert Mode provides FTD shell access for advanced troubleshooting. By default for container instances, Expert Mode is only available to users who access the FTD CLI from the FXOS CLI. This limitation is only applied to container instances to increase isolation between instances. Use Expert Mode only if a documented procedure tells you it is required, or if the Cisco Technical Assistance Center asks you to use it. To enter this mode, use the expert command in the FTD CLI.

Example

The following example shows how to enable Expert Mode from SSH:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key PERMIT_EXPERT_MODE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value yes
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

Related Commands

Command	Description
create bootstrap-key FIREWALL_MODE	Sets the firewall mode for the application.
create logical-device	Creates the logical device.
create mgmt-bootstrap	Creates the bootstrap configuration for the application.

set vlan

To set the VLAN ID for a subinterface for use with container instances, use the **set vlan** command.

set vlan *id*

Syntax Description

id	Sets the VLAN ID between 1 and 4095.

Command Modes

scope eth-uplink/scope fabric a/scope interface/create subinterface/

scope eth-uplink/scope fabric a/create port-channel/create subinterface/

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

You can add between 250 and 500 VLAN subinterfaces to the chassis, depending on your network deployment.

VLAN IDs per interface must be unique, and within a container instance, VLAN IDs must be unique across all assigned interfaces. You can reuse VLAN IDs on *separate* interfaces as long as they are assigned to different container instances. However, each subinterface still counts towards the limit even though it uses the same ID.

Example

The following example creates 3 subinterfaces on Ethernet 1/1, and sets them to be data-sharing interfaces.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # scope interface Ethernet1/1
firepower /eth-uplink/fabric/interface # create subinterface 10
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 10
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # create subinterface 11
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 11
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # create subinterface 12
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 12
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
firepower /eth-uplink/fabric/interface/subinterface #
```

Related Commands

Command	Description
create port-channel	Creates an EtherChannel (port channel).
create subinterface	Adds a subinterface.

Command	Description
scope interface	Enters the physical interface object.
set port-type	Sets the interface type.