



System Administration

- [Changing the Management IP Address, on page 1](#)
- [Changing the Application Management IP, on page 3](#)
- [Changing the Firepower 4100/9300 Chassis Name, on page 5](#)
- [Install a Trusted Identity Certificate, on page 6](#)
- [Auto-Import Certificate Update, on page 12](#)
- [Pre-Login Banner, on page 14](#)
- [Rebooting the Firepower 4100/9300 Chassis, on page 17](#)
- [Powering Off the Firepower 4100/9300 Chassis, on page 18](#)
- [Restoring the Factory Default Configuration, on page 18](#)
- [Securely Erasing System Components, on page 19](#)

Changing the Management IP Address

Before you begin

You can change the management IP address on the Firepower 4100/9300 chassis from the FXOS CLI.



Note After changing the management IP address, you will need to reestablish any connections to Firepower Chassis Manager or the FXOS CLI using the new address.

Procedure

- Step 1** Connect to the FXOS CLI (see [Accessing the FXOS CLI](#)).
- Step 2** To configure an IPv4 management IP address:
- Set the scope for fabric-interconnect a:
Firepower-chassis# **scope fabric-interconnect a**
 - To view the current management IP address, enter the following command:
Firepower-chassis /fabric-interconnect # **show**

c) Enter the following command to configure a new management IP address and gateway:

```
Firepower-chassis /fabric-interconnect # set out-of-band ip ip_address netmask network_mask gw gateway_ip_address
```

d) Commit the transaction to the system configuration:

```
Firepower-chassis /fabric-interconnect* # commit-buffer
```

Step 3 To configure an IPv6 management IP address:

a) Set the scope for fabric-interconnect a:

```
Firepower-chassis# scope fabric-interconnect a
```

b) Set the scope for management IPv6 configuration:

```
Firepower-chassis /fabric-interconnect # scope ipv6-config
```

c) To view the current management IPv6 address, enter the following command:

```
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if
```

d) Enter the following command to configure a new management IP address and gateway:

```
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 ipv6_address ipv6-prefix prefix_length ipv6-gw gateway_address
```

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

e) Commit the transaction to the system configuration:

```
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
```

Example

The following example configures an IPv4 management interface and gateway:

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /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
Firepower-chassis /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
Firepower-chassis /fabric-interconnect* #commit-buffer
Firepower-chassis /fabric-interconnect #
```

The following example configures an IPv6 management interface and gateway:

```

Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if

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

```

Changing the Application Management IP

You can change the management IP address on the application(s) attached to your Firepower 4100/9300 chassis from the FXOS CLI. To do so, you must first change the IP information at the FXOS platform level, then change the IP information at the application level.



Note Changing the application management IP will result in a service interruption.

Procedure

- Step 1** Connect to the FXOS CLI. (See [Accessing the FXOS CLI](#)).
- Step 2** Scope to the logical device:
- ```

scope ssa
scope logical-device logical_device_name

```
- Step 3** Scope to the management bootstrap and configure the new management bootstrap parameters. Note that there are differences between deployments:
- For standalone configuration of an ASA logical device:
- Enter the logical device management bootstrap:
 

```

scope mgmt-bootstrap asa

```
  - Enter the IP mode for the slot:
 

```

scope ipv4_or_6 slot_number default

```
  - (IPv4 only) Set the new IP address:
 

```

set ip ipv4_address mask network_mask

```
  - (IPv6 only) Set the new IP address:
 

```

set ip ipv6_address prefix-length prefix_length_number

```
  - Set the gateway address:
 

```

set gateway gateway_ip_address

```

- f) Commit the configuration:

**commit-buffer**

For a clustered configuration of ASA logical devices:

- a) Enter the cluster management bootstrap:

**scope cluster-bootstrap asa**

- b) (IPv4 only) Set the new virtual IP:

**set virtual ipv4 ip\_address mask network\_mask**

- c) (IPv6 only) Set the new virtual IP:

**set virtual ipv6 ipv6\_address prefix-length prefix\_length\_number**

- d) Set the new IP pool:

**set ip pool start\_ip end\_ip**

- e) Set the gateway address:

**set gateway gateway\_ip\_address**

- f) Commit the configuration:

**commit-buffer**

For standalone and clustered configurations of FTD:

- a) Enter the logical device management bootstrap:

**scope mgmt-bootstrap ftd**

- b) Enter the IP mode for the slot:

**scope ipv4\_or\_6 slot\_number firepower**

- c) (IPv4 only) Set the new IP address:

**set ip ipv4\_address mask network\_mask**

- d) (IPv6 only) Set the new IP address:

**set ip ipv6\_address prefix-length prefix\_length\_number**

- e) Set the gateway address:

**set gateway gateway\_ip\_address**

- f) Commit the configuration:

**commit-buffer**

**Note** For a clustered configuration, you must set the new IP address for each application attached to the Firepower 4100/9300 chassis. If you have an inter-chassis cluster or a HA configuration, you must repeat these steps for each application on both chassis.

**Step 4** Clear the management bootstrap information for each application:

- a) Scope to ssa mode:

**scope ssa**

- b) Scope to the slot:  
**scope slot** *slot\_number*
- c) Scope to the application instance:  
**scope app-instance** *asa\_or\_ftd*
- d) Clear the management bootstrap information:  
**clear-mgmt-bootstrap**
- e) Commit the configuration:  
**commit-buffer**

**Step 5** Disable the application:

**disable**  
**commit-buffer**

**Note** For a clustered configuration, you must clear and disable the management bootstrap information for each application attached to the Firepower 4100/9300 chassis. If you have an inter-chassis cluster or a HA configuration, you must repeat these steps for each application on both chassis.

**Step 6** When the application is offline and the slot comes online again, re-enable the application.

- a) Scope back to ssa mode:  
**scope ssa**
- b) Scope to the slot:  
**scope slot** *slot\_number*
- c) Scope to the application instance:  
**scope app-instance** *asa\_or\_ftd*
- d) Enable the application:  
**enable**
- e) Commit the configuration:  
**commit-buffer**

**Note** For a clustered configuration, you must repeat these steps to re-enable each application attached to the Firepower 4100/9300 chassis. If you have an inter-chassis cluster or a HA configuration, you must repeat these steps for each application on both chassis.

---

## Changing the Firepower 4100/9300 Chassis Name

You can change the name used for your Firepower 4100/9300 chassis from the FXOS CLI.

## Procedure

---

- Step 1** Connect to the FXOS CLI (see [Accessing the FXOS CLI](#)).
- Step 2** Enter the system mode:  
Firepower-chassis-A# **scope system**
- Step 3** To view the current name:  
Firepower-chassis-A /system # **show**
- Step 4** To configure a new name:  
Firepower-chassis-A /system # **set name** *device\_name*
- Step 5** Commit the transaction to the system configuration:  
Firepower-chassis-A /fabric-interconnect\* # **commit-buffer**
- 

## Example

The following example changes the devices name:

```
Firepower-chassis-A# scope system
Firepower-chassis-A /system # set name New-name
Warning: System name modification changes FC zone name and redeploys them non-disruptively
Firepower-chassis-A /system* # commit-buffer
Firepower-chassis-A /system # show

Systems:
 Name Mode System IP Address System IPv6 Address

 New-name Stand Alone 192.168.100.10 ::
New-name-A /system #
```

# Install a Trusted Identity Certificate

After initial configuration, a self-signed SSL certificate is generated for use with the Firepower 4100/9300 chassis web application. Because that certificate is self-signed, client browsers do not automatically trust it. The first time a new client browser accesses the Firepower 4100/9300 chassis web interface, the browser will throw an SSL warning, requiring the user to accept the certificate before accessing the Firepower 4100/9300 chassis. You can use the following procedure to generate a Certificate Signing Request (CSR) using the FXOS CLI and install the resulting identity certificate for use with the Firepower 4100/9300 chassis. This identity certificate allows a client browser to trust the connection, and bring up the web interface with no warnings.

## Procedure

---

- Step 1** Connect to the FXOS CLI. (See [Accessing the FXOS CLI](#)).

- Step 2** Enter the security module:  
**scope security**
- Step 3** Create a keyring:  
**create keyring** *keyring\_name*
- Step 4** Set a modulus size for the private key:  
**set modulus** *size*
- Step 5** Commit the configuration:  
**commit-buffer**
- Step 6** Configure the CSR fields. The certificate can be generated with basic options (for example, a subject-name), and optionally more advanced options that allow information like locale and organization to be embedded in the certificate. Note that when you configure the CSR fields, the system prompts for a certificate password.
- create certreq** **subject-name** *subject\_name*  
*password*  
**set country** *country*  
**set state** *state*  
**set locality** *locality*  
**set org-name** *organization\_name*  
**set org-unit-name** *organization\_unit\_name*  
**set subject-name** *subject\_name*
- Step 7** Commit the configuration:  
**commit-buffer**
- Step 8** Export the CSR to provide to your certificate authority. The certificate authority uses the CSR to create your identity certificate.
- Show the full CSR:  
**show certreq**
  - Copy the output starting with (and including) "**-----BEGIN CERTIFICATE REQUEST-----**", ending with (and including) "**-----END CERTIFICATE REQUEST-----**":  
**Example:**  
-----BEGIN CERTIFICATE REQUEST-----  
MIIC6zCCAdMCAQAwdzELMAkGA1UEBhMCVVMxEzARBgNVBAGMCkNhbG1mb3JuaWEyETAPBgNVBACMFNhb1Bkb3NlMRYwFAyDVQQKDA1DaXNjbyBTeXN0ZW1zMQwwCgYDVQQLDANUQUxGjAYBgNVBAMMEWZwNDEyMC50ZXN0LmxxvY2FsMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0ON5gagkfZ2fi4JVEANG+7YGgcHbnUt7LpVymChnKOPJjBwkUMNQA1mQsRQDcbJ232/sK0fMSnyqOL8JzC7itxeVEZRyz7/ax7WGNveg/XP+zd03nt4GXM63FsrPcPmA7EwgqDSLoShtBEV10hhf4+Nw4pKCZ+eSSkSJKtB1ZHakV9bttYg3kf/UEUUGk/EyrVq3B+u2DsooPVq76mTm8BwYMqHbJEv4PmuRjWE88yEvVwH7JTEij90vxbatjDjVSJHZBURtCanvyBvGuLP/Q/Nmv3Lo3G9ITbLl5gIYZVatTxp6HTUezH2MIiZoavU6d1tB9rnyxgGth5dPV0dhQIDAQABoC8wLQYJKoZIhvcNAQkOMSAwHjAcBgNVHREEFtATghFmcDQxMjAudGVzdC5sb2NhbnDANBgkqhkiG9w0BAQsFAAOCAQEAZUfCbwx9vt5aVdCL+tAtu5xFE3LA310ck6Gj1Nv6W/6rjBNLxusYi1rZZcW+CgnvNs4ArqYGyNVBySOavJO/VvQ1KfyxxJ1OikyX3RzEjgK0

```

zzyoyrG+EZXCS5ShiraS8HuWvE2wFM2wwWntHWtvcQy55+/hDPD2Bv8pQOC2Zng3I
kLfG1dxWf1xAxLzf5J+AuIQ0CM5HzM9Zm8zREoWT+xHtLSqAgg/aCuomN9/vEwyU
OYfoJMvAqC6AZyUnMfUfCoyuLpLwgkxB0gyaRdnea5RhiGjYQ21DXyDjEXp7rCx9
+6bvD1ln70JCegHdCWtP75SaNyaBEPk00365rTckbw==
-----END CERTIFICATE REQUEST-----

```

**Step 9** Exit the certreq mode:

```
exit
```

**Step 10** Exit the keyring mode:

```
exit
```

**Step 11** Provide the CSR output to the Certificate Authority in accordance with the Certificate Authority's enrollment process. If the request is successful, the Certificate Authority sends back an identity certificate that has been digitally signed using the CA's private key.

**Step 12** **Note** All identity certificates must be in Base64 format to be imported into FXOS. If the identity certificate chain received from the Certificate Authority is in a different format, you must first convert it with an SSL tool such as OpenSSL.

Create a new trustpoint to hold the identity certificate chain.

```
create trustpoint trustpoint_name
```

**Step 13** Enter the identity certificate chain you received from the Certificate Authority in step 11, following the instructions on screen.

**Note** For a Certificate Authority that uses intermediate certificates, the root and intermediate certificates must be combined. In a text file, paste the root certificate at the top, followed by each intermediate certificate in the chain, including all BEGIN CERTIFICATE and END CERTIFICATE flags. Copy and paste that entire text block into the trustpoint.

```
set certchain
```

**Example:**

```

firepower /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
>-----BEGIN CERTIFICATE-----
>MIICDTCCAbOgAwIBAgIQYIutxPDPw6BOP3uKNgJHZDAKBggqhkjOPQQDAjBTMRUw
>EwYKcZImiZPyLQBGryFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>MB4GA1UEAxMXbmfhdXN0aW4tTtkFBVVNUSU4tUEMtQ0EwHhcNMtUwNzI4MTc1NjU2
>WhcNMjAwNzI4MTgwNjU2WjBTMRUwEwYKcZImiZPyLQBGryFbG9jYWwxGDAWBgoJ
>kiaJk/IsZAEZFghuYWF1c3RpbjEgMB4GA1UEAxMXbmfhdXN0aW4tTtkFBVVNUSU4t
>UEMtQ0EwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASvEA27V1Enq1gMtLkvJ6rx
>GXRpXWIEyuiBM4eQRoqZKnkeJUKmlxmqlubaDHPJ5TMGfJQYszLBRJPq+mdrKcDl
>o2kwZzATBgkrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0T
>AQH/BAUwAwEB/zAdBgnVH04EFgQUyInbdHPrFwEEBcbxGSgQW7pOVIkwEAYJKwYB
>BAGCNxUBBAMCAQAwCgYIKoZIzj0EAwIDSAAwRQIhAP++QJTUmnIB/AxPDDN63Lqy
>18odMDofTKg4p3Tb/2yMAiAtMYh1sv1gCxsQV0w0xZVRugSdoOak6n7wCjTFX9jr
>RA==
>-----END CERTIFICATE-----
>ENDOFBUF

```

**Step 14** Commit the configuration:

```
commit-buffer
```



- Step 15** Exit the trustpoint mode:  
**exit**
- Step 16** Enter the keyring mode:  
**scope keyring** *keyring\_name*
- Step 17** Associate the trustpoint created in step 13 with the keyring that was created for the CSR:  
**set trustpoint** *trustpoint\_name*
- Step 18** Import the signed identity certificate for the server.  
**set cert**
- Step 19** Paste the contents of the identity certificate provided by the Certificate authority:

**Example:**

Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.  
Keyring certificate:

```
>-----BEGIN CERTIFICATE-----
>MIIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkJOPQODAjbT
>MRUwEwYKcZImiZPyLGQBGryFbG9jYwWxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
>bJEGMB4GA1UEAxMxYmFhZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3
>OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQGEwJVUzETMBEGA1UECBMKQ2F5
>aWZvcmluZS5pYTERMA8GA1UEBxMIU2FuIEpvc2UxYjFjYUJGNVBAoTDUNpc2NvIFN5c3Rl
>bXN5bWVudDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3
>MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQczQ43mBqCR9nZ+Lg1UQA0b7tga
>BwdudS3sulXIwKGco48mMHCRCQw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
>RlHLPv9rHtYY296D9c/7N3Tee3gZcZrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
>ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
>yodskS/g+a5GNyTzzIS9XAfsLMSKP06/Ftq2MONVIkdKFRG0Jqe/IG8a4s/9D82a
>/cujcb0hNssvmAhh1Vq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2H109XR2FAGMB
>AAGjggJYMIICVDAcBgNVHREEFtATghFmcDQxMjAudGVzdC5sb2NhbdAdBgNVHQ4E
>FgQU/1WpstiEYExs8D1ZWcuHZwPtU5QwHwYDVR0jBBgwFoAUyInbDHPPrFwEEBcbx
>GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBY6CByIaBxWxkYXA6Ly8vQ049bmFh
>dXN0aW4tTkFBVVNUSU4tUEMTOE049bmFhZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3
>YmXpYyUyMEtleSUyMFBVbn1cnZpY2VzLENOPVN1cnZpY2VzLENOPUNvbmZpZ3V5YXRp
>b24sREM9bmFhZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3ZDQ3
>dD9iYXN1P29iamVjdENsYXNzPWNSTERpc3RyaWJldGlvb1BvaW50MIHMBggrBgEF
>BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
>QVVTVELOLVBDELUNBLENOPUFJQSxDTj1QdWJsaWMLMjBLZXk1MjBTZXJ2aWN1cyxD
>Tj1TZXJ2aWN1cyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPwvY2Fs
>P2NBQ2VydG1maWwNhdGU/YmFzZT9vYmplY3RDbGFzZj1jZXJ0aWZpY2F0aW9uQXV0
>aG9yaXR5MCEGCSsGAQQBgjcUAQQUHhIAVwBLAGIAUwBIAHIAHgBIAHIAwDgYDVR0P
>AQH/BAQDAgWgMBMGA1UdJQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0GAMEUC
>IFew7NcJirEtFRvYxjkQ4/dVo2oI6CRB308WQbYHNuU/AiEA7UdObiSJBG/PBZjm
>sgoIK60akbjoTtVtUdUd9b6K1Uw=
>-----END CERTIFICATE-----
>ENDOFBUF
```

- Step 20** Exit the keyring mode:  
**exit**
- Step 21** Exit the security mode:  
**exit**
- Step 22** Enter the system mode:

**scope system**

**Step 23** Enter the services mode:

**scope services**

**Step 24** Configure the FXOS web service to use the new certificate:

```
set https keyring keyring_name
```

**Step 25** Commit the configuration:

**commit-buffer**

**Step 26** Display the keyring associated with the HTTPS server. It should reflect the keyring name created in step 3 of this procedure. If the screen output displays the default keyring name, the HTTPS server has not yet been updated to use the new certificate:

**show https****Example:**

```
fp4120 /system/services # show https
Name: https
 Admin State: Enabled
 Port: 443
 Operational port: 443
 Key Ring: firepower_cert
 Cipher suite mode: Medium Strength
 Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL
```

**Step 27** Display the contents of the imported certificate, and verify that the **Certificate Status** value displays as **Valid**:

**scope security****show keyring *keyring\_name* detail****Example:**

```
fp4120 /security # scope security
fp4120 /security # show keyring firepower_cert detail
Keyring firepower_cert:
 RSA key modulus: Mod2048
 Trustpoint CA: firepower_chain
 Certificate status: Valid
Certificate:
Data:
 Version: 3 (0x2)
 Serial Number:
 45:00:00:00:0a:de:86:55:16:82:24:f3:be:00:00:00:00:00:0a
 Signature Algorithm: ecdsa-with-SHA256
 Issuer: DC=local, DC=naaustin, CN=naaustin-NAAUSTIN-PC-CA
 Validity
 Not Before: Apr 28 13:09:54 2016 GMT
 Not After : Apr 28 13:09:54 2018 GMT
 Subject: C=US, ST=California, L=San Jose, O=Cisco Systems, OU=TAC,
 CN=fp4120.test.local
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (2048 bit)
 Modulus:
 00:b3:43:8d:e6:06:a0:91:f6:76:7e:2e:09:54:40:
```

```

0d:1b:ee:d8:1a:07:07:6e:75:2d:ec:ba:55:c8:c0:
a1:9c:a3:8f:26:30:70:91:43:0d:40:0d:66:42:c4:
50:0d:c6:c9:db:7d:bf:b0:ad:1f:31:29:f2:a8:e2:
fc:27:30:bb:8a:dc:5e:54:46:51:cb:3e:ff:6b:1e:
d6:18:db:de:83:f5:cf:fb:37:74:de:7b:78:19:73:
3a:dc:5b:2b:3d:c3:e6:03:b1:30:82:a0:d2:2e:84:
a1:b4:11:15:d7:48:61:7f:8f:8d:c3:8a:4a:09:9f:
9e:49:29:12:26:44:c1:d5:91:da:29:5f:5b:b6:d6:
20:de:47:ff:50:45:14:82:4f:c4:ca:b5:6a:dc:1f:
ae:d8:3b:28:a0:f5:6a:ef:a9:93:9b:c0:70:60:ca:
87:6c:91:2f:e0:f9:ae:46:35:84:f3:cc:84:bd:5c:
07:ec:94:c4:8a:3f:4e:bf:16:da:b6:30:e3:55:22:
47:64:15:11:b4:26:a7:bf:20:6f:1a:e2:cf:fd:0f:
cd:9a:fd:cb:a3:71:bd:21:36:cb:2f:98:08:61:95:
5a:b5:3c:69:e8:74:d4:7b:31:f6:30:82:33:39:ab:
d4:e9:dd:6d:07:da:e7:cb:18:06:b6:1e:5d:3d:5d:
1d:85
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Alternative Name:
 DNS:fp4120.test.local
X509v3 Subject Key Identifier:
 FF:55:A9:B2:D8:84:60:4C:6C:F0:39:59:59:CB:87:67:03:ED:BB:94
X509v3 Authority Key Identifier:
 keyid:C8:89:DB:0C:73:EB:17:01:04:05:C6:F1:19:28:10:5B:BA:4E:54:89
X509v3 CRL Distribution Points:
 Full Name:
 URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=naaustin-pc,CN=CDP,
 CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
 DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint

Authority Information Access:
 CA Issuers - URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=AIA,
 CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
 DC=local?cACertificate?base?objectClass=certificationAuthority
 1.3.6.1.4.1.311.20.2:
 ...W.e.b.s.e.r.v.e.r
X509v3 Key Usage: critical
 Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
 TLS Web Server Authentication
Signature Algorithm: ecdsa-with-SHA256
 30:45:02:20:57:b0:ec:d7:09:8a:b1:2d:15:1b:f2:c6:39:10:
 e3:f7:55:a3:6a:08:e8:24:41:df:4f:16:41:b6:07:35:4b:bf:
 02:21:00:ed:47:4e:6e:24:89:04:6f:cf:05:98:e6:b2:0a:08:
 2b:ad:1a:91:b8:e8:b4:e4:ef:51:d5:1d:f5:be:8a:d5:4c
-----BEGIN CERTIFICATE-----
MIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkJOPQQDAjBT
MRUwEwYKCZImiZPyLGBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
OTU0WWhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
aWZvcn5pYTERMA8GA1UEBxMIU2FuIEpvc2UxU2FjAUBGNVBAoTDUNpc2NvIFN5c3Rl
bXMxDDAKBgNVBAsTA1RBQzEaMBGGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
BwdudS3sulXIwKGCco48mMHCQRw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopXlu21iDeR/9QRRSCT8TKtWrch67YOyig9WrvqZ0bwhBg
yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
/cujcb0hNssvmAhh1Vq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2H109XR2FAgMB
AAGjggJYMIICVDAcBgNVHREFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
FgQU/1WpstieYExs8DlZwcuHZwPtU5QwHwYDVR0jBBGwFoAUyInbDHPFwEEBcbx
GSgQW7pOVIkwgdwGALUdHwSB1DCB0TCBzqCBY6CBYIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVVNUSU4tUEMtQ0E049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
YmxpYyUyMETleSUyMFN1cnZpY2VzLENOPVN1cnZpY2VzLENOPUNvbmZpZ3VyYXRp

```

```
b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydG1maWNhdGVsZXZvY2F0aW9uTG1z
dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJldG1vb1BvaW50MIHMBggrBgEF
BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vLONOPW5hYXVzdGluLU5B
QVVTVE1OLVBDDLUNBLENOPUFJQSxDTj1QdWJsaWMLMjBLZXklMjBTZXJ2aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
P2NBQ2VydG1maWNhdGU/YmFzZT9vYmp1Y3RDdGFzc1jZlZlJ0aWZpY2F0aW9uQXV0
aG9yaXR5MCEGCSSGAQQBgjcUAQQUHhIAVwBLAGIAUwBIAHIAAgBlAHIAwDgYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
sgoIK60akbjotOTvUdUd9b6K1Uw=
-----END CERTIFICATE-----
```

Zeroized: No

### What to do next

To verify that the new trusted certificate is presented, navigate to the Firepower Chassis Manager by entering `https://<FQDN_or_IP>/` in the address bar of a web browser.



**Note** Browsers also verify the subject-name of a certificate against the input in the address bar. If the certificate is issued to the fully qualified domain name, it must be accessed that way in the browser. If it is accessed via IP address, a different SSL error is thrown (Common Name Invalid) even if the trusted certificate is used.

## Auto-Import Certificate Update

When the Cisco certificate server changes its identity certificate to leverage a different root CA, the connectivity for the Smart Licensing on 4100 or 9300s running the ASA devices gets broken. Because the licensing connectivity is handled by the supervisor instead of Lina on the application, the Smart Licensing function fails. For FXOS-based devices, the issue can be resolved using the auto-import feature without an upgrade to the FXOS software.

By default, the auto-import feature is disabled. You can use the following procedure to enable the auto-import feature using the FXOS CLI.

### Before you begin

DNS server should be configured to reach the [cisco certificate server](#).

### Procedure

- 
- Step 1** Connect to the FXOS CLI.
- Step 2** Enter the security module:
- scope security**
- Step 3** Enable the auto-import feature.
- enter tp-auto-import**

**Example:**

```
FXOS# scope security
FXOS /security # enter tp-auto-import
FXOS /security #
```

**Step 4** Commit the configuration.

```
commit-buffer
```

**Step 5** Verify the auto-import status

```
show detail
```

**Example:**

Successful auto-import:

```
FXOS /security/tp-auto-import #
FXOS /security/tp-auto-import # show detail
Trustpoints auto import source URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
TrustPoints auto import scheduled time : 22:00
Last Importing Status : Success, Imported with 23 TrustPoint(s)
TrustPoints auto Import function : Enabled
FXOS /security/tp-auto-import #
```

Auto-import failure:

```
FXOS /security/tp-auto-import #
FXOS /security/tp-auto-import # show detail
Trustpoints auto import source URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
TrustPoints auto import scheduled time : 22:00
Last Importing Status : Failure
TrustPoints auto Import function : Enabled
FXOS /security/tp-auto-import #
```

**Step 6** Configure the tp-auto-import feature. Set the import-time-hour.

```
set import-time-hour hour import-time-min minutes
```

**Example:**

```
FXOS /security/tp-auto-import # set
import-time-hour Trustpoints auto import hour time
FXOS /security/tp-auto-import # set import-time-hour
0-23 Import Time Hour
FXOS /security/tp-auto-import # set import-time-hour 7 import-time-min
0-59 Import Time Min
FXOS /security/tp-auto-import # set import-time-hour 7 import-time-min 20
<CR>
FXOS /security/tp-auto-import # set import-time-hour 7 import-time-min 20
FXOS /security/tp-auto-import* # commit-buffer
FXOS /security/tp-auto-import #
```

**Note** The auto-import source URL is fixed and you must change the import time detail to minute per day. Import occurs everyday on the scheduled time of the day. If hours and minutes are not set then the certificate import occurs only once while enabling it. Certificates get downloaded as a bundle into the box under the path /opt/certstore which can only be accessed through secure-login option. Along with the bundle (ios\_core.p7b), individual certificates (AutoTP1 to AutoTPn) get extracted automatically.

**Step 7** After the auto-import configuration completion, enter show detail command.

```
show detail
```

**Example:**

```
FXOS /security/tp-auto-import # show detail
Trustpoints auto import source URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
TrustPoints auto import scheduled time : 07:20
Last Importing Status : Success, Imported with 23 TrustPoint(s)
TrustPoints auto Import function : Enabled
```

**Note** The maximum certificates that can be imported is 30. Each import re-iterates for 6 times if there is any connectivity issue to Cisco Certificate Server and then updates the last importing status in the show command.

**Step 8** (Optional) To disable the auto-import feature, enter the delete auto-import command.

**delete tp-auto-import****Example:**

```
FXOS /security #
FXOS /security # delete tp-auto-import
FXOS /security* # commit-buffer
FXOS /security # show detail
security mode:
 Password Strength Check: No
 Minimum Password Length: 8
 Is configuration export key set: No
 Current Task:
FXOS /security # scope tp-auto-import
Error: Managed object does not exist
FXOS /security #
FXOS /security # enter tp-auto-import
FXOS /security/tp-auto-import* # show detail
FXOS /security/tp-auto-import* #
```

**Note** If you disable the auto-import feature, certificates that are imported remain persistent till the time there is no change in the build. Certificates get removed if you disable the auto-import feature and then downgrade/upgrade the build.

---

## Pre-Login Banner

With a pre-login banner, when a user logs into Firepower Chassis Manager, the system displays the banner text and the user must click **OK** on the message screen before the system prompts for the username and password. If a pre-login banner is not configured, the system goes directly to the username and password prompt.

When a user logs into the FXOS CLI, the system displays the banner text, if configured, before it prompts for the password.

## Creating the Pre-Login Banner

### Procedure

- 
- Step 1** Connect to the FXOS CLI (see [Accessing the FXOS CLI](#)).
- Step 2** Enter security mode:  
Firepower-chassis# **scope security**
- Step 3** Enter banner security mode:  
Firepower-chassis /security # **scope banner**
- Step 4** Enter the following command to create a pre-login banner:  
Firepower-chassis /security/banner # **create pre-login-banner**
- Step 5** Specify the message that FXOS should display to the user before they log into Firepower Chassis Manager or the FXOS CLI:  
Firepower-chassis /security/banner/pre-login-banner\* # **set message**  
Launches a dialog for entering the pre-login banner message text.
- Step 6** At the prompt, type a pre-login banner message. You can enter any standard ASCII character in this field. You can enter multiple lines of text with each line having up to 192 characters. Press **Enter** between lines. On the line following your input, type **ENDOFBUF** and press **Enter** to finish. Press **Ctrl** and **C** to cancel out of the set message dialog.
- Step 7** Commit the transaction to the system configuration:  
Firepower-chassis /security/banner/pre-login-banner\* # **commit-buffer**
- 

### Example

The following example creates the pre-login banner:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # create pre-login-banner
Firepower-chassis /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

## Modifying the Pre-Login Banner

### Procedure

---

- Step 1** Connect to the FXOS CLI (see [Accessing the FXOS CLI](#)).
- Step 2** Enter security mode:  
Firepower-chassis# **scope security**
- Step 3** Enter banner security mode:  
Firepower-chassis /security # **scope banner**
- Step 4** Enter pre-login-banner banner security mode:  
Firepower-chassis /security/banner # **scope pre-login-banner**
- Step 5** Specify the message that FXOS should display to the user before they log into Firepower Chassis Manager or the FXOS CLI:  
Firepower-chassis /security/banner/pre-login-banner # **set message**  
Launches a dialog for entering the pre-login banner message text.
- Step 6** At the prompt, type a pre-login banner message. You can enter any standard ASCII character in this field. You can enter multiple lines of text with each line having up to 192 characters. Press **Enter** between lines.  
On the line following your input, type **ENDOFBUF** and press **Enter** to finish.  
Press **Ctrl** and **C** to cancel out of the set message dialog.
- Step 7** Commit the transaction to the system configuration:  
Firepower-chassis /security/banner/pre-login-banner\* # **commit-buffer**
- 

### Example

The following example modifies the pre-login banner:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # scope pre-login-banner
Firepower-chassis /security/banner/pre-login-banner # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```



## Deleting the Pre-Login Banner

### Procedure

---

- Step 1** Connect to the FXOS CLI (see [Accessing the FXOS CLI](#)).
- Step 2** Enter security mode:  
Firepower-chassis# **scope security**
- Step 3** Enter banner security mode:  
Firepower-chassis /security # **scope banner**
- Step 4** Delete the pre-login banner from the system:  
Firepower-chassis /security/banner # **delete pre-login-banner**
- Step 5** Commit the transaction to the system configuration:  
Firepower-chassis /security/banner\* # **commit-buffer**
- 

### Example

The following example deletes the pre-login banner:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # delete pre-login-banner
Firepower-chassis /security/banner* # commit-buffer
Firepower-chassis /security/banner #
```

## Rebooting the Firepower 4100/9300 Chassis

### Procedure

---

- Step 1** Enter chassis mode:  
**scope chassis 1**
- Step 2** Enter the following command to reboot the chassis:  
**reboot** [*reason*] [**no-prompt**]

**Note** If you use the [**no-prompt**] keyword, the chassis will reboot immediately after entering the command. If you do not use the [**no-prompt**] keyword, the system will not reboot until you enter the **commit-buffer** command.

The system will gracefully shut down any logical devices configured on the system and then power down each security module/engine before finally powering down and then restarting the Firepower 4100/9300 chassis. This process takes approximately 15-20 minutes.

**Step 3** To monitor the reboot process:

```
scope chassis 1
```

```
show fsm status
```

---

## Powering Off the Firepower 4100/9300 Chassis

### Procedure

---

**Step 1** Enter chassis mode:

```
scope chassis 1
```

**Step 2** Enter the following command to power down the chassis:

```
shutdown [reason] [no-prompt]
```

**Note** If you use the **[no-prompt]** keyword, the chassis will shut down immediately after entering the command. If you do not use the **[no-prompt]** keyword, the system will not shut down until you enter the **commit-buffer** command.

The system will gracefully shut down any logical devices configured on the system and then power down each security module/engine before finally powering down the Firepower 4100/9300 chassis. This process takes approximately 15-20 minutes. After the chassis has successfully shut down, you can then physically unplug the power on the chassis.

**Step 3** To monitor the shutdown process:

```
scope chassis 1
```

```
show fsm status
```

---

## Restoring the Factory Default Configuration

You can use the FXOS CLI to restore your Firepower 4100/9300 chassis to factory default configuration.



**Note** This process erases all user configuration from the chassis including any logical device configuration. After completing this procedure, you will need to reconfigure the system (see [Initial Configuration](#)).

---

### Procedure

---

- Step 1** (Optional) The **erase configuration** command does not remove the Smart License configuration from the chassis. If you also want to remove the Smart License configuration, perform the following steps:
- scope license**
- deregister**
- Deregistering the Firepower 4100/9300 chassis removes the device from your account. All license entitlements and certificates on the device are removed.
- Step 2** Connect to the local-management shell:
- connect local-mgmt**
- Step 3** Enter the following command to erase all user configuration from your Firepower 4100/9300 chassis and restore the chassis to its original factory default configuration:
- erase configuration**
- The system prompts you to verify that you are sure you want to erase all user configuration.
- Step 4** Confirm that you want to erase the configuration by entering **yes** at the command prompt. The system will erase all user configuration from your Firepower 4100/9300 chassis and then reboot the system.
- 

## Securely Erasing System Components

You can use the FXOS CLI to erase and securely erase components of your appliance.

The **erase configuration** command removes all user-configuration information on the chassis, restoring it to its original factory-default configuration, as described in [Restoring the Factory Default Configuration, on page 18](#).

The **secure erase** command securely erases the specified appliance component. That is, data is not just deleted—the physical storage is “wiped” (completely erased). This is important when transferring or returning the appliance as hardware storage components do not retain residual data or stubs.



---

**Note** The device reboots during secure erase, which means SSH connections are terminated. Therefore, we recommend performing secure erase over a serial console-port connection.

---

### Procedure

---

- Step 1** Connect to the local-management shell:
- connect local-mgmt**
- Step 2** Enter one of the following **erase configuration** commands to securely erase the specified appliance component:

a) **erase configuration chassis**

The system warns you that all data and images will be lost and cannot be recovered, and asks you to confirm that you want to proceed. If you enter **y**, the entire chassis is securely erased; security modules are erased first, followed by the Supervisor.

Since all data and software on the device are erased, device recovery can be accomplished only from the ROM Monitor (ROMMON).

b) **erase configuration security\_module** *module\_id*

The system warns you that all data and images on the module will be lost and cannot be recovered, and asks you to confirm that you want to proceed. If you enter **y**, the module is erased.

**Note** The **decommission-secure** command produces essentially the same result as this command.

After a security module is erased, it remains down until acknowledged (similar to a module that is decommissioned).

c) **erase configuration supervisor**

The system warns you that all data and images will be lost and cannot be recovered, and asks you to confirm that you want to proceed. If you enter **y**, the Supervisor is securely erased.

Since all data and software on the Supervisor are erased, device recovery can be accomplished only from the ROM Monitor (ROMMON).

---