



## 系统管理

---

- [导致 Firepower 机箱管理器会话关闭的系统更改](#)，第 1 页
- [更改管理 IP 地址](#)，第 2 页
- [更改应用管理 IP](#)，第 3 页
- [更改 Firepower 4100/9300 机箱名称](#)，第 6 页
- [安装受信任身份证书](#)，第 7 页
- [自动导入证书更新](#)，第 13 页
- [登录前横幅](#)，第 15 页
- [重新启动 Firepower 4100/9300 机箱](#)，第 18 页
- [关闭 Firepower 4100/9300 机箱电源](#)，第 18 页
- [恢复出厂默认配置](#)，第 18 页
- [安全地擦除系统组件](#)，第 19 页

## 导致 Firepower 机箱管理器会话关闭的系统更改

以下系统更改可能会导致您自动从 Firepower 机箱管理器系统中注销：

- 对系统时间的改动超过 10 分钟
- 使用 Firepower 机箱管理器或 FXOS CLI 重新启动或关闭系统
- 在 Firepower 4100/9300 机箱上升级 FXOS 版本
- 启用或禁用 FIPS 或通用标准模式



注释

除上述更改外，如果在特定时间段内没有任何活动，您也会自动从系统中注销。默认情况下，此自动注销超时时间为 10 分钟。要配置此超时设置，请参阅[配置会话超时](#)。另外，您还可以配置一个绝对超时设置，使系统在经过特定时间后强制注销登录用户（即使用户会话处于活动状态）。要配置绝对超时设置，请参阅[配置绝对会话超时](#)。

## 更改管理 IP 地址

### 开始之前

您可以从 FXOS CLI 更改 Firepower 4100/9300 机箱上的管理 IP 地址。



**注释** 更改管理 IP 地址后，您需要使用新地址重新建立到 Firepower 机箱管理器或 FXOS CLI 的任何连接。

### 过程

**步骤 1** 连接到 FXOS CLI（请参阅[访问 FXOS CLI](#)）。

**步骤 2** 要配置 IPv4 管理 IP 地址，请执行以下操作：

- a) 设置交换矩阵互联 a 的范围：

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

- b) 要查看当前管理 IP 地址，请输入以下命令：

```
Firepower-chassis /fabric-interconnect # show
```

- c) 输入以下命令，配置新的管理 IP 地址和网关：

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

- d) 将任务提交到系统配置：

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

**步骤 3** 要配置 IPv6 管理 IP 地址，请执行以下操作：

- a) 设置交换矩阵互联 a 的范围：

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

- b) 设置管理 IPv6 配置的范围：

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

- c) 要查看当前管理 IPv6 地址，请输入以下命令：

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

- d) 输入以下命令，配置新的管理 IP 地址和网关：

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

**注释** 仅支持 IPv6 全局单播地址作为机箱的 IPv6 管理地址。

e) 将任务提交到系统配置:

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

## 示例

以下示例配置 IPv4 管理接口和网关:

```
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 #
```

以下示例配置 IPv6 管理接口和网关:

```
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 #
```

## 更改应用管理 IP

您可以从 FXOS CLI 更改连接到 Firepower 4100/9300 机箱的应用上的管理 IP 地址。为此，您必须首先在 FXOS 平台级别更改 IP 信息，然后在应用级别更改 IP 信息。



注释 更改应用程序管理 IP 会导致服务中断。

## 过程

---

**步骤 1** 连接到 FXOS CLI。（请参阅[访问 FXOS CLI](#)）。

**步骤 2** 将范围设置为逻辑设备：

```
scope ssa
```

```
scope logical-device logical_device_name
```

**步骤 3** 将范围设置为管理引导程序，并配置新的管理引导程序参数。请注意，配置之间存在差异：

对于 ASA 逻辑设备的独立配置：

a) 输入逻辑设备管理引导程序：

```
scope mgmt-bootstrap asa
```

b) 输入插槽的 IP 模式：

```
scope ipv4_or_6 slot_number default
```

c) （仅限 IPv4）设置新的 IP 地址：

```
set ip ipv4_address mask network_mask
```

d) （仅限 IPv6）设置新的 IP 地址：

```
set ip ipv6_address prefix-length prefix_length_number
```

e) 设置网关地址：

```
set gateway gateway_ip_address
```

f) 提交配置：

```
commit-buffer
```

对于 ASA 逻辑设备的群集配置：

a) 输入群集管理引导程序：

```
scope cluster-bootstrap asa
```

b) （仅限 IPv4）设置新的虚拟 IP：

```
set virtual ipv4 ip_address mask network_mask
```

c) （仅限 IPv6）设置新的虚拟 IP：

```
set virtual ipv6 ipv6_address prefix-length prefix_length_number
```

d) 设置新的 IP 池：

```
set ip pool start_ip end_ip
```

e) 设置网关地址：

```
set gateway gateway_ip_address
```

f) 提交配置：

**commit-buffer**

对于 FTD 的独立和群集配置：

- a) 输入逻辑设备管理引导程序：

```
scope mgmt-bootstrap ftd
```

- b) 输入插槽的 IP 模式：

```
scope ipv4_or_6 slot_number firepower
```

- c) （仅限 IPv4）设置新的 IP 地址：

```
set ip ipv4_address mask network_mask
```

- d) （仅限 IPv6）设置新的 IP 地址：

```
set ip ipv6_address prefix-length prefix_length_number
```

- e) 设置网关地址：

```
set gateway gateway_ip_address
```

- f) 提交配置：

```
commit-buffer
```

**注释** 对于群集配置，您必须为连接到 Firepower 4100/9300 机箱的每个应用设置新的 IP 地址。如果您有机箱间群集或 HA 配置，则必须对两个机箱上的每个应用重复这些步骤。

**步骤 4** 为每个应用清除管理引导程序信息：

- a) 将范围设置为 ssa 模式：

```
scope ssa
```

- b) 将范围设置为插槽：

```
scope slot slot_number
```

- c) 将范围设置为应用实例：

```
scope app-instance asa_or_ftd
```

- d) 清除管理引导程序信息：

```
clear-mgmt-bootstrap
```

- e) 提交配置：

```
commit-buffer
```

**步骤 5** 禁用应用：

```
disable
```

```
commit-buffer
```

**注释** 对于群集配置，您必须清除并禁用连接到 Firepower 4100/9300 机箱的每个应用的管理引导程序信息。如果您有机箱间群集或 HA 配置，则必须对两个机箱上的每个应用重复这些步骤。

**步骤 6** 当应用离线且插槽恢复在线时，重新启用应用。

a) 将范围重置为 ssa 模式：

**scope ssa**

b) 将范围设置为插槽：

**scope slot slot\_number**

c) 将范围设置为应用实例：

**scope app-instance asa\_or\_fid**

d) 启用应用：

**enable**

e) 提交配置：

**commit-buffer**

**注释** 对于群集配置，您必须重复执行这些步骤以重新启用连接到 Firepower 4100/9300 机箱的每个应用。如果您有机箱间群集或 HA 配置，则必须对两个机箱上的每个应用重复这些步骤。

## 更改 Firepower 4100/9300 机箱名称

您可以在 FXOS CLI 中更改用于 Firepower 4100/9300 机箱的名称。

### 过程

**步骤 1** 连接到 FXOS CLI（请参阅[访问 FXOS CLI](#)）。

**步骤 2** 进入系统模式：

Firepower-chassis-A# **scope system**

**步骤 3** 查看当前名称：

Firepower-chassis-A /system # **show**

**步骤 4** 配置新名称：

Firepower-chassis-A /system # **set name device\_name**

**步骤 5** 将任务提交到系统配置：

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

## 示例

以下示例将更改设备名称：

```
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 #
```

# 安装受信任身份证书

在完成初始配置后，系统将生成自签名 SSL 证书以供 Firepower 4100/9300 机箱 Web 应用使用。由于该证书是自签名证书，客户端浏览器不会自动信任它。新的客户端浏览器首次访问 Firepower 4100/9300 机箱 Web 界面时，浏览器会抛出 SSL 警告，要求用户在访问 Firepower 4100/9300 机箱之前接受证书。您可以使用以下程序，使用 FXOS CLI 生成证书签名请求 (CSR)，并安装得到的身份证书以供 Firepower 4100/9300 机箱使用。此身份证书允许客户端浏览器信任连接，并直接启动 Web 界面而无警告。

## 过程

**步骤 1** 连接到 FXOS CLI。（请参阅[访问 FXOS CLI](#)）。

**步骤 2** 输入安全模块：

```
scope security
```

**步骤 3** 创建密钥环：

```
create keyring keyring_name
```

**步骤 4** 设置私钥的模数大小：

```
set modulus size
```

**步骤 5** 提交配置：

```
commit-buffer
```

- 步骤 6** 配置 CSR 字段。可以使用基本选项（例如，主题名称）生成证书，也可以选择允许将信息（例如，区域和组织）嵌入证书的更高级选项。请注意，在您配置 CSR 字段时，系统会提示输入证书密码。

```
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
```

- 步骤 7** 提交配置：

```
commit-buffer
```

- 步骤 8** 导出 CSR，将其提供给您的证书颁发机构。证书颁发机构使用 CSR 来创建您的身份证书。

- a) 显示完整 CSR：

```
show certreq
```

- b) 复制从（并包含）“-----BEGIN CERTIFICATE REQUEST-----”到（并包含）“-----END CERTIFICATE REQUEST-----”的输出：

示例：

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC6zCCAdMCAQAwZELMAkGA1UEBhMCVVMxEzARBgNVBAGMCkNhbG1mb3JuaWEw
ETAPBgNVBACMFNhb3N1MRYwFAYDVQQKDA1DaXNjbyBTeXN0ZW1zMQwwCgYD
VQQLDANUQUxGjAYBgNVBAMMEWZwNDEyMC50ZXN0LmxxY2F5MIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0ON5gagkfZ2fi4JVEANG+7YGgcHbnUt7LpV
yMChnKOPJjBwkUMNQA1mQsRQDcbJ232/sK0fMSnyqOL8JzC7itxeVEZRyz7/ax7W
GNveg/XP+zd03nt4GXM63FsrPcPmA7EwgqDSLoShtBEV10hhf4+Nw4pKCZ+eSSkS
JkTBlZHaKV9bttYg3kf/UEUgk/EyrVq3B+u2DsooPVq76mTm8BwYmQhBjEv4Pmu
RjWE88yEvVwH7JTEij9OvxbatjDjVSJHZBURtCanvyBvGuLP/Q/Nmv3Lo3G9ITbL
L5gIYZVatTxp6HTUezH2MIIzOavU6d1tB9rnyxgGth5dPV0dhQIDAQABoC8wLQYJ
KoZIHvcNAQkOMSAwHjAcBgNVHREEFtATghFmcdQxMjAudGVzdC5sb2NhbdANBgkq
hkiG9w0BAQsFAAOCAQEAZUfCbwx9vt5aVdCltAtTu5xFE3LA310ck6Gj1Nv6W/6r
jBNLxusYilrZZcW+CgnvNs4ArqYGyNVBySOavJO/VvQ1KfyxxJ10Ikyx3RzEjgK0
zzyoyrG+EZXC5ShiraS8HuWvE2wFM2wwWNtHWtvcQy55+/hDPD2Bv8pQOC2Zng3I
kLfgldxWflxAxLz5J+AuIQ0CM5HzM9Zm8zREoWT+xHtLSqAqg/aCuomN9/vEwyU
OYfoJMvAqC6AZyUnMfUfCoyuLpLwgkxBOgyaRdnea5RhiGjYQ2lDXYDjEXp7rCx9
+6bvD11n70JCegHdCwTP75SaNyaBEPk00365rTckbw==
-----END CERTIFICATE REQUEST-----
```

- 步骤 9** 退出证书请求模式：

```
exit
```

- 步骤 10** 退出密钥环模式：

```
exit
```



**步骤 11** 根据证书颁发机构的注册流程，向证书颁发机构提供 CSR 输出。如果请求成功，证书颁发机构将发回一份已使用 CA 的私钥进行数字签名的身份证书。

**步骤 12** **注释** 所有身份证书必须采用 Base64 格式才能导入到 FXOS。如果从证书颁发机构接收到的身份证书链采用的是其他格式，您必须先使用 SSL 工具（例如，OpenSSL）进行转换。

创建新的信任点以保存身份证书链。

**create trustpoint** *trustpoint\_name*

**步骤 13** 按照屏幕上的说明，输入您在第 11 步中从证书颁发机构接收到的身份证书链。

**注释** 对于使用中间证书的证书颁发机构，必须对根证书和中间证书进行组合。在文本文件中，将根证书粘贴在顶部，然后是链中的每一个中间证书，包括所有 BEGIN CERTIFICATE 和 END CERTIFICATE 标记。将整个文本块复制并粘贴到信任点。

**set certchain**

**示例：**

```
firepower /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
>-----BEGIN CERTIFICATE-----
>MIICDTCCAbOgAwIBAgIQYIutxPDPw6BOP3uKNgJHZDAKBggqhkJOPQDAjBTMRUw
>EwYKcZImiZPyLQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>MB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTC1NjU2
>WhcNMjAwNzI4MTgwNjU2WjBTMRUwEwYKcZImiZPyLQBGRYFbG9jYWwxGDAWBgoJ
>kiaJk/IsZAEZFghuYWF1c3RpbjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4t
>UEMtQ0EwWTATBgcqhkJOPQIBBggqhkJOPQMBBwNCAASvEA27V1Enq1gMtLkvJ6rx
>GXRpXWIEyuiBM4eQRoqZKnkeJUKmlxmqlubaDHPJ5TMGfJQYszLBRJPq+mdrKcDl
>o2kwZzATBgkrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8EBAMCAYwDwYDVR0T
>AQH/BAUwAwEB/zAdBgNVHQ4EFgQUyInbDHPPrFwEEBcbxGSgQW7pOVIkwEAYJKwYB
>BAGCNxUBBAMCAQAwCgYIKoZIzj0EAwIDSAAwRQIhAP++QJTUmniB/AxPDDN63Lqy
>18odMDoFTkG4p3Tb/2yMAiAtMYh1sv1gCxsQVOW0xZVRugSdoOak6n7wCjTFX9jr
>RA==
>-----END CERTIFICATE-----
>ENDOFBUF
```

**步骤 14** 提交配置：

**commit-buffer**

**步骤 15** 退出信任点模式：

**exit**

**步骤 16** 进入密钥环模式：

**scope keyring** *keyring\_name*

**步骤 17** 将在第 13 步中创建的信任点与为 CSR 创建的密钥环关联：

**set trustpoint** *trustpoint\_name*

**步骤 18** 导入服务器的签名身份证书。

**set cert**

**步骤 19** 粘贴证书颁发机构提供的身份证书的内容：

**示例:**

```

Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
>-----BEGIN CERTIFICATE-----
>MIE8DCBjAgAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkJOPQDAjBT
>MRUwEwYKcZImiZPyLgQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
>bJgEMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
>OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQGEwJVUzETMBEGAlUECBMKQ2Fs
>aWZvcn5pYTERMA8GA1UEBxMIU2FuIEpvc2UxXjAUBGNVBAoTDUNpc2NvIFN5c3Rl
>bXMxDDAKBgNVBAsTA1RBQzEaMBGGA1UEAxMRZna0MTIwLnRlc3QubG9jYVwwggEi
>MAOGCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+Lg1UQA0b7tga
>BwdudS3sulXIwKGo48mMHCQRw1ADWZCxFANxsnfb+wrR8xKfKo4vvnMLuK3F5U
>R1HLPv9rHtYY296D9c/7N3Tee3gzczrcWys9w+YdsTCCoNIuhKG0ERXXSGF/j43D
>ikoJn55JKRlMRMHVkdopXlu21iDeR/9QRRSCT8TKtWrcH67YQyig9WrvqZObwHBg
>yodsks/g+a5GNYTzzIS9XAfs1MSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
>/cujcb0hNssvmAhh1Vq1PGnodNR7mfYwgjM5q9Tp3W0H2ufLGaa2H109XR2FAGMB
>AAGjggJYMIICVDAcBgNVHREEFtAtghFmcDQxMjAudGVzdC5sb2NhbdAdBgNVHQ4E
>FgQU/1WpstiEYExs8D1ZwcuHwPtu5QwHwYDVR0jBBgwFoAUyInbDHPFwEEBcbx
>GSGQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBY6CBYIaBxWxkYXA6Ly8vQ049bmFh
>dXN0aW4tTkFBVVNUSU4tUEMtQ0E049bmFhdXN0aW4tcGMsQ049Q0RQLENOFVB1
>YmXpYyUyMEtleSUyMFN1cnZpY2VzLENOPVN1cnZpY2VzLENOPUNvbmZpZ3VyYXRp
>b24sREM9bmFhdXN0aW4sREM9bG9jYVww/Y2VydG1maWNhdGVSZXZvY2F0aW9uTG1z
>dD9iYXN1P29iamVjDENsYXNzPWNSTERpc3RyaWJldG1vb1BvaW50MIHMBGgrBgEF
>BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
>QVVTVE1OLVBDLUNBLENOFUFJQSxDTj1QdWJsaWMLMjBLZXklMjBTZXJ2aWN1cyxD
>Tj1TZXJ2aWN1cyxDj1Db25maWdlcmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
>P2NBQ2VydG1maWNhdGU/YmFzZT9vYmplY3RDbGFzYXZ1jZl0aWZpY2F0aW9uQXV0
>aG9yaXR5MCEGCSsGAQQBggjCUAgQUHhIAVwBlAGIAUwBlAHIAIAdgBlAHlwDgYDVR0P
>AQH/BAQDAgWgMBMGA1UdJQOMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
>IFew7NcJirEtFRvxyjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
>sgoIK60akbjotOtvUdUd9b6K1Uw=
>-----END CERTIFICATE-----
>ENDOFBUF

```

**步骤 20** 退出密钥环模式:

```
exit
```

**步骤 21** 退出安全模式:

```
exit
```

**步骤 22** 进入系统模式:

```
scope system
```

**步骤 23** 进入服务模式:

```
scope services
```

**步骤 24** 配置 FXOS Web 服务以使用新证书:

```
set https keyring keyring_name
```

**步骤 25** 提交配置:

```
commit-buffer
```

**步骤 26** 显示与 HTTPS 服务器关联的密钥环。它应显示在本程序的第 3 步中创建的密钥环名称。如果屏幕输出显示默认的密钥环名称，则 HTTPS 服务器尚未更新，不能使用新证书：

### show https

#### 示例：

```
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
```

**步骤 27** 显示导入的证书的内容，确认 **Certificate Status** 值显示为 **Valid**：

### scope security

### show keyring keyring\_name detail

#### 示例：

```
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-----
MIIE8DCBjAgAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkJOPQDAjBT
MRUwEwYKZImiZPyLGQBGryFbG9jYWwxGDAWbgoJkiaJk/IsZAEZFghuYWF1c3Rp
bjEgMB4GA1UEAxMXbmfhdXN0aW4tTkFBVVNUSU4tUEMTOEwHhcNMjYwNDI4MTMw
OTU0WhcNMjYwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2F5
aWZvcmlkLWUyMC93aW50LWUyMC93aW50LWUyMC93aW50LWUyMC93aW50LWUyMC93
aW50LWUyMC93aW50LWUyMC93aW50LWUyMC93aW50LWUyMC93aW50LWUyMC93aW50
LWUyMC93aW50LWUyMC93aW50LWUyMC93aW50LWUyMC93aW50LWUyMC93aW50LWUy
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
BwdudS3sulXlWkGco48mMHCQRwlADWZCxFANxsnbf+wrR8xKfKo4vvnMLuK3F5U
RlHLPv9rHtYY296D9c/7N3Tee3gZcZrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopXlU21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZOwbHBg
yodskS/g+a5GNyTzzIS9XAfslMSKPO6/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
/cujcb0hNssvmAhhlVq1PGnodNR7mfYwgjM5q9Tp3W0H2ufLGAa2H109XR2FAGmB
AAGjggJYMIICVDAcBgNVHREFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
FgQU/1WpstiEYExs8D1ZWcuHZwPtU5QwHwYDVR0jBBGwFoAUYInbDHPPrFwEEBcbx
GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzQCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVVNUSU4tUEMTOEwHhcNMjYwNDI4MTMwOTU0WjB3MQswCQYDVQQGEw
YWF1c3RpbmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmYWVhbnhdGVSZXZvY2F0aW9uTG1z
dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJldG1vb1BvaW50MIHhBggrBgEF
BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0N0Pw5hYXVzdGluLU5B
QVVTVE10LVBDBLUNBLENOPUFJQSxDtj1QdWJsaWMLmJBLZXklmJBTZXJ2aWNlcyxDTj
1TZxJ2aWNlcyxDTj1Db25maWdlcmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2F5P2Ns
P2NBQ2VydGlmYWVhbnhdGU/YmFzZT9vYmplY3RDbGFzcj1jZXJ0aWZvY2F0aW9uQXV0
aG9yaXR5MCEGCSSGAQOQBgjcuAQUHhIAVwBlAGIAUwBlAHIAIAdgBlAHIAIAdgYDVR0P
AQH/BAQDAgWgMBMGAlUdJQMMMAoGCCsGAQUFBwMBAoGCCqGSM49BAMCA0gAMEUC
IFew7NcJirEtFrVyxkq4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBzjm
sgoIK60akbjotOTvUdUd9b6K1Uw=
-----END CERTIFICATE-----

```

Zeroized: No

### 下一步做什么

要验证显示的证书是新的受信任证书，请通过在 Web 浏览器的地址栏输入 `https://<FQDN_or_IP>/` 转至 Firepower 机箱管理器。



**注释** 浏览器还根据地址栏中的输入验证证书的主题名称。如果证书颁发给完全限定域名，则必须在浏览器中以相应方式访问它。如果通过 IP 地址访问，将引发其他 SSL 错误（公用名无效 [Common Name Invalid]），即使使用的是受信任证书。

## 自动导入证书更新

当 Cisco 证书服务器更改其身份证书以利用不同的根 CA 时，运行 ASA 设备的 4100 或 9300 上的智能许可连接会中断。由于许可连接由主管而不是应用程序上的 Lina 处理，因此智能许可功能将失败。对于 FXOS 设备，可以使用自动导入功能解决此问题，而无需升级到 FXOS 软件。

默认情况下，已禁用自动导入功能。您可以通过以下程序使用 FXOS CLI 启用自动导入功能。

### 开始之前

应配置 DNS 服务器以访问 [Cisco 证书服务器](#)。

### 过程

**步骤 1** 连接到 FXOS CLI。

**步骤 2** 输入安全模块：

```
scope security
```

**步骤 3** 启用自动导入功能。

```
enter tp-auto-import
```

示例：

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

**步骤 4** 提交配置。

```
commit-buffer
```

**步骤 5** 验证自动导入状态

**show detail**

示例:

自动导入成功:

```
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 #
```

自动导入失败:

```
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 #
```

**步骤 6** 配置 tp-auto-import 功能。设置 import-time-hour。

**set import-time-hour** 小时 **import-time-min** 分钟

示例:

```
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 #
```

**注释** 自动导入源 URL 是固定的，您必须将导入时间详细信息更改为每天的分钟数。导入每天在计划的时间进行。如果未设置小时数和分钟数，则证书导入仅在启用时进行一次。证书作为捆绑包下载到路径 /opt/certstore 下的框中，只能通过安全登录选项进行访问。与捆绑包 (ios\_core.p7b) 一起，系统会自动提取各个证书 (AutoTP1 到 AutoTPn)。

**步骤 7** 自动导入配置完成后，输入 show detail 命令。

**show detail**

示例:

```
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
```

**注释** 可导入的最大证书数为 30。如果 Cisco 证书服务器存在任何连接问题，则每次导入都会重复 6 次，然后在 show 命令中更新上次导入状态。

**步骤 8**（可选）要禁用自动导入功能，请输入 `delete auto-import` 命令。

### **delete tp-auto-import**

示例:

```
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* #
```

**注释** 如果禁用自动导入功能，导入的证书将保持不变，直到内部版本中没有更改为止。如果您禁用自动导入功能，然后降级/升级内部版本，则会删除证书。

## 登录前横幅

如果配置了登录前横幅，当用户登录到 Firepower 机箱管理器时，系统将显示横幅文本，用户必须在消息屏幕上单击**确定**，然后系统才会提示输入用户名和密码。如果未配置登录前横幅，系统会直接进入用户名和密码输入提示屏幕。

当用户登录到 FXOS CLI 时，系统显示横幅文本（如已配置），然后提示输入密码。

## 创建登录前横幅

过程

**步骤 1** 连接到 FXOS CLI（请参阅[访问 FXOS CLI](#)）。

**步骤 2** 进入安全模式:

```
Firepower-chassis# scope security
```

**步骤 3** 进入横幅安全模式:

```
Firepower-chassis /security # scope banner
```

**步骤 4** 输入以下命令创建登录前横幅:

```
Firepower-chassis /security/banner # create pre-login-banner
```

**步骤 5** 指定在用户登录 Firepower 机箱管理器或 FXOS CLI 前 FXOS 应向用户显示的消息：

```
Firepower-chassis /security/banner/pre-login-banner* # set message
```

启动一个对话框，用于输入登录前横幅消息文本。

**步骤 6** 在提示符处，键入登录前横幅消息。您可以在此字段中输入任何标准 ASCII 字符。您可以输入多行文本，每行最多 192 个字符。按 **Enter** 键换行。

在您输入信息的下一行，键入 **ENDOFBUF** 并按 **Enter** 键以完成操作。

按 **Ctrl** 和 **C** 键取消设置消息对话框。

**步骤 7** 将任务提交到系统配置：

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

## 示例

以下示例创建登录前横幅：

```
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 #
```

## 修改登录前横幅

### 过程

**步骤 1** 连接到 FXOS CLI（请参阅[访问 FXOS CLI](#)）。

**步骤 2** 进入安全模式：

```
Firepower-chassis# scope security
```

**步骤 3** 进入横幅安全模式：

```
Firepower-chassis /security # scope banner
```

**步骤 4** 进入登录前横幅安全模式：

```
Firepower-chassis /security/banner # scope pre-login-banner
```

**步骤 5** 指定在用户登录 Firepower 机箱管理器或 FXOS CLI 前 FXOS 应向用户显示的消息：



```
Firepower-chassis /security/banner/pre-login-banner # set message
```

启动一个对话框，用于输入登录前横幅消息文本。

**步骤 6** 在提示符处，键入登录前横幅消息。您可以在此字段中输入任何标准 ASCII 字符。您可以输入多行文本，每行最多 192 个字符。按 **Enter** 键换行。

在您输入信息的下一行，键入 **ENDOFBUF** 并按 **Enter** 键以完成操作。

按 **Ctrl** 和 **C** 键取消设置消息对话框。

**步骤 7** 将任务提交到系统配置：

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

## 示例

以下示例修改登录前横幅：

```
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 #
```

# 删除登录前横幅

## 过程

**步骤 1** 连接到 FXOS CLI（请参阅[访问 FXOS CLI](#)）。

**步骤 2** 进入安全模式：

```
Firepower-chassis# scope security
```

**步骤 3** 进入横幅安全模式：

```
Firepower-chassis /security # scope banner
```

**步骤 4** 从系统中删除登录前横幅：

```
Firepower-chassis /security/banner # delete pre-login-banner
```

**步骤 5** 将任务提交到系统配置：

```
Firepower-chassis /security/banner* # commit-buffer
```

---

### 示例

以下示例删除登录前横幅：

```
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 #
```

## 重新启动 Firepower 4100/9300 机箱

### 过程

---

- 步骤 1** 选择概览 (**Overview**) 打开“概览 (Overview)”页面。
  - 步骤 2** 单击“概览 (Overview)”页面右上角“机箱运行时间 (Chassis Uptime)”旁边的**重新启动 (Reboot)**。
  - 步骤 3** 单击**是 (Yes)**确认您要关闭 Firepower 4100/9300 机箱。  
系统将正常关闭系统上配置的任何逻辑设备，然后关闭每个安全模块/引擎，最后关闭并重新启动 Firepower 4100/9300 机箱。此过程大约需要 15-20 分钟。
- 

## 关闭 Firepower 4100/9300 机箱电源

### 过程

---

- 步骤 1** 选择概览 (**Overview**) 打开“概览 (Overview)”页面。
  - 步骤 2** 单击“概览 (Overview)”页面右上角“机箱运行时间 (Chassis Uptime)”旁边的**关闭 (Shutdown)**。
  - 步骤 3** 单击**是**确认您要关闭 Firepower 4100/9300 机箱。  
系统将正常关闭系统上配置的任何逻辑设备，然后关闭每个安全模块/引擎，最后关闭 Firepower 4100/9300 机箱。
- 

## 恢复出厂默认配置

您可以使用 FXOS CLI 将您的 Firepower 4100/9300 机箱恢复至出厂默认配置。



**注释** 此过程将从机箱中清除所有用户配置，包括所有逻辑设备配置。完成此程序后，您需要重新配置系统（请参阅[初始配置](#)）。

### 过程

**步骤 1** （可选） **erase configuration** 命令不会从机箱中删除智能许可证配置。如果您还想要删除智能许可证配置，请执行以下步骤：

**scope license**

**deregister**

取消注册 Firepower 4100/9300 机箱会从账户中删除设备。系统会删除设备上的所有许可证授权和证书。

**步骤 2** 连接到本地管理外壳：

**connect local-mgmt**

**步骤 3** 输入以下命令，从您的 Firepower 4100/9300 机箱中清除所有用户配置，并将机箱恢复到其原始出厂默认配置：

**erase configuration**

系统将提示您确认，是否确定想要清除所有用户配置。

**步骤 4** 通过在命令提示符后输入 **yes**，确认您想要清除配置。

系统将从您的 Firepower 4100/9300 机箱中清除所有用户配置，然后重启系统。

## 安全地擦除系统组件

您可以使用 FXOS CLI 清除并安全地擦除设备的组件。

如[恢复出厂默认配置](#)，第 18 页中所述，**erase configuration** 命令可删除机箱上的所有用户配置信息，将其恢复为原始出厂默认配置。

**secure erase** 命令会安全地擦除指定的设备组件。也就是说，并非仅删除数据，物理存储也会被“擦除”（完全清除）。这在运输或退回设备时非常重要，因为硬件存储组件不会保留残留数据或存根。



**注释** 设备会在安全清除期间重新引导，这意味着 SSH 连接会终止。因此，我们建议通过串行控制台端口连接执行安全擦除。

## 过程

---

**步骤 1** 连接到本地管理外壳：

**connect local-mgmt**

**步骤 2** 输入以下 **erase configuration** 命令之一，以安全地擦除指定的设备组件：

a) **erase configuration chassis**

系统会警告您，所有数据和映像都将丢失且无法恢复，并要求您确认是否要继续。如果您输入 **y**，整个机箱会被安全地擦除；首先清除安全模块，然后再清除管理引擎。

由于设备上的所有数据和软件都会被清除，因此只能从 ROM 监控器 (ROMMON) 恢复设备。

b) **erase configuration security\_module module-ID**

系统会警告您，模块上的所有数据和映像都将丢失且无法恢复，并要求您确认是否要继续。如果输入 **y**，模块将被清除。

注释 **decommission-secure** 命令产生的结果与此命令基本相同。

清除安全模块后，它将保持关闭状态，直到被确认（类似于已停用的模块）。

c) **erase configuration supervisor**

系统会警告您，所有数据和映像都将丢失且无法恢复，并要求您确认是否要继续。如果您输入 **y**，管理引擎会被安全地清除。

由于管理引擎上的所有数据和软件都会被清除，因此只能从 ROM 监控器 (ROMMON) 恢复设备。

---