



システム管理

- [セッション変更により Firepower Chassis Manager セッションが閉じる場合](#) (1 ページ)
- [管理 IP アドレスの変更](#) (2 ページ)
- [アプリケーション管理 IP の変更](#) (4 ページ)
- [Firepower 4100/9300 シャーシ名の変更](#) (6 ページ)
- [トラスト ID 証明書のインストール](#) (7 ページ)
- [証明書の更新の自動インポート](#) (13 ページ)
- [ログイン前バナー](#) (16 ページ)
- [Firepower 4100/9300 シャーシの再起動](#) (19 ページ)
- [Firepower 4100/9300 シャーシの電源オフ](#) (19 ページ)
- [工場出荷時のデフォルト設定の復元](#) (20 ページ)
- [システム コンポーネントの安全な消去](#) (20 ページ)

セッション変更により Firepower Chassis Manager セッションが閉じる場合

次のようにシステムを変更すると、自動的に Firepower Chassis Manager からログアウトする可能性があります。

- 10 分を超えてシステム時刻を変更した場合。
- Firepower Chassis Manager または FXOS CLI を使用してシステムを再起動またはシャットダウンした場合。
- Firepower 4100/9300 シャーシ上の FXOS のバージョンをアップグレードした場合。
- FIPS またはコモンクライテリア モードを有効または無効にした場合。



- (注) 上記の変更に加えて、一定期間にわたって操作がない場合は自動的にシステムからログアウトします。デフォルトでは、10 分間にわたり操作を行わないと自動的にログアウトします。このタイムアウト設定を変更するには、[セッションタイムアウトの設定](#)を参照してください。また、セッションがアクティブな場合でも、一定時間の経過後にユーザをシステムからログオフさせるように絶対タイムアウトを設定することもできます。絶対タイムアウトを設定するには、[絶対セッションタイムアウトの設定](#)を参照してください。

管理 IP アドレスの変更

始める前に

FXOS CLI から Firepower 4100/9300 シャーシの管理 IP アドレスを変更できます。



- (注) 管理 IP アドレスを変更した後、新しいアドレスを使用して Firepower Chassis Manager または FXOS CLI への接続を再確立する必要があります。

手順

ステップ 1 FXOS CLI に接続します ([FXOS CLI へのアクセス](#)を参照)。

ステップ 2 IPv4 管理 IP アドレスを設定するには、次の手順を実行します。

- a) fabric-interconnect a のスコープを設定します。

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

- b) 現在の管理 IP アドレスを表示するには、次のコマンドを入力します。

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

- c) 次のコマンドを入力して、新しい管理 IP アドレスとゲートウェイを設定します。

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

- d) トランザクションをシステム設定にコミットします。

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

ステップ 3 IPv6 管理 IP アドレスを設定するには、次の手順を実行します。

- a) fabric-interconnect a のスコープを設定します。

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

- b) 管理 IPv6 設定の範囲を設定します。

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

- c) 現在の管理 IPv6 アドレスを表示するには、次のコマンドを入力します。

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

- d) 次のコマンドを入力して、新しい管理 IP アドレスとゲートウェイを設定します。

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

(注) シャーシの IPv6 管理アドレスとしてサポートされるのは、IPv6 グローバルユニキャストアドレスのみです。

- e) トランザクションをシステム設定にコミットします。

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

例

次の例では、IPv4 管理インターフェイスとゲートウェイを設定します。

```
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 #
```

次の例では、IPv6 管理インターフェイスとゲートウェイを設定します。

```
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 #
```

アプリケーション管理 IP の変更

FXOS CLI から Firepower 4100/9300 シャーシに接続されたアプリケーションの管理 IP アドレスは変更できます。そのためには、まず FXOS プラットフォーム レベルで IP 情報を変更し、次にアプリケーション レベルで IP 情報を変更する必要があります。



(注) アプリケーション管理 IP を変更すると、サービスの中断が発生します。

手順

ステップ 1 FXOS CLI に接続します。(FXOS CLI へのアクセス を参照)。

ステップ 2 範囲を論理デバイスにします。

scope ssa

scope logical-device *logical_device_name*

ステップ 3 範囲を管理ブートストラップにし、新しい管理ブートストラップパラメータを設定します。導入間で違いがあることに注意してください。

ASA 論理デバイスのスタンドアロンの設定の場合。

a) 論理デバイスのブートストラップに入ります。

scope mgmt-bootstrap *asa*

b) スロットを IP モードにします。

scope ipv4_or_6 *slot_number* default

c) (IPv4 のみ) 新しい IP アドレスを設定します。

set ip *ipv4_address* **mask** *network_mask*

d) (IPv6 のみ) 新しい IP アドレスを設定します。

set ip *ipv6_address* **prefix-length** *prefix_length_number*

e) ゲートウェイアドレスを設定します。

set gateway *gateway_ip_address*

f) 設定をコミットします。

commit-buffer

ASA 論理デバイスのクラスタ設定の場合。

a) クラスタ管理ブートストラップに入ります。

scope cluster-bootstrap *asa*

- b) (IPv4 のみ) 新しい仮想 IP を設定します。
set virtual ipv4 ip_address mask network_mask
- c) (IPv6 のみ) 新しい仮想 IP を設定します。
set virtual ipv6 ipv6_address prefix-length prefix_length_number
- d) 新しい IP プールを設定します。
set ip pool start_ip end_ip
- e) ゲートウェイ アドレスを設定します。
set gateway gateway_ip_address
- f) 設定をコミットします。
commit-buffer

FTD のスタンドアロン設定およびクラスタ設定の場合。

- a) 論理デバイスのブートストラップに入ります。
scope mgmt-bootstrap ftd
- b) スロットを IP モードにします。
scope ipv4_or_6 slot_number firepower
- c) (IPv4 のみ) 新しい IP アドレスを設定します。
set ip ipv4_address mask network_mask
- d) (IPv6 のみ) 新しい IP アドレスを設定します。
set ip ipv6_address prefix-length prefix_length_number
- e) ゲートウェイ アドレスを設定します。
set gateway gateway_ip_address
- f) 設定をコミットします。
commit-buffer

(注) クラスタ設定の場合、Firepower 4100/9300 シャーシに接続されているアプリケーションごとに新しい IP アドレスを設定する必要があります。シャーシ間クラスタまたは HA 設定の場合、両方のシャーシでアプリケーションごとにこれらのステップを繰り返す必要があります。

ステップ 4 アプリケーションごとに管理ブートストラップ情報をクリアします。

- a) 範囲を ssa モードにします。
scope ssa
- b) 範囲をスロットにします。
scope slot slot_number

- c) 範囲をアプリケーションインスタンスにします。

scope app-instance asa_or_ftd

- d) 管理ブートストラップ情報をクリアします。

clear-mgmt-bootstrap

- e) 設定を確定します。

commit-buffer

ステップ 5 アプリケーションを無効にします。

disable

commit-buffer

- (注) クラスタ設定の場合、Firepower 4100/9300 シャーシに接続されているアプリケーションごとに管理ブートストラップ情報をクリアし、無効にする必要があります。シャーシ間クラスタまたはHA設定の場合、両方のシャーシでアプリケーションごとにこれらのステップを繰り返す必要があります。

ステップ 6 アプリケーションがオフラインで、スロットが再度オンラインになったときに、アプリケーションを再度有効にします。

- a) 範囲を ssa モードに戻します。

scope ssa

- b) 範囲をスロットにします。

scope slot slot_number

- c) 範囲をアプリケーションインスタンスにします。

scope app-instance asa_or_ftd

- d) アプリケーションを有効にします。

enable

- e) 設定を確定します。

commit-buffer

- (注) クラスタ設定の場合、これらのステップを繰り返して、Firepower 4100/9300 シャーシに接続されている各アプリケーションを再度有効にします。シャーシ間クラスタまたはHA設定の場合、両方のシャーシでアプリケーションごとにこれらのステップを繰り返す必要があります。

Firepower 4100/9300 シャーシ名の変更

Firepower 4100/9300 シャーシに使用する名前を FXOS CLI から変更することができます。

手順

ステップ 1 FXOS CLI に接続します ([FXOS CLI へのアクセス](#)を参照)。

ステップ 2 システム モードに入ります。

```
Firepower-chassis-A# scope system
```

ステップ 3 現在の名前を表示します。

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

ステップ 4 新しい名前を構成します。

```
Firepower-chassis-A /system # set name device_name
```

ステップ 5 トランザクションをシステム設定にコミットします。

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

例

次の例では、デバイス名を変更します。

```
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 #
```

トラスト ID 証明書のインストール

初期設定後に、自己署名 SSL 証明書が Firepower 4100/9300 シャーシ Web アプリケーションで使用するために生成されます。その証明書は自己署名であるため、クライアントブラウザが自動的に信頼することはありません。新しいクライアントブラウザで Firepower 4100/9300 シャーシ Web インターフェイスに初めてアクセスするときに、ブラウザは SSL 警告をスローして、ユーザが Firepower 4100/9300 シャーシにアクセスする前に証明書を受け入れることを要求します。FXOS CLI を使用して証明書署名要求 (CSR) を生成し、Firepower 4100/9300 シャーシで使用する結果の ID 証明書をインストールするには、以下の手順を使用できます。この ID 証明書により、クライアントブラウザは接続を信頼し、警告なしで Web インターフェイスを起動できるようになります。

手順

- ステップ 1** FXOS CLI に接続します。（[FXOS CLIへのアクセス](#) を参照）。
- ステップ 2** セキュリティ モジュールを入力します。
- scope security**
- ステップ 3** キーリングを作成します。
- create keyring *keyring_name***
- ステップ 4** 秘密キーのモジュラス サイズを設定します。
- set modulus *size***
- ステップ 5** 設定をコミットします。
- commit-buffer**
- ステップ 6** CSR フィールドを設定します。証明書は、基本オプション（*subject-name* など）を指定して生成できます。さらに任意で、ロケールや組織などの情報を証明書に組み込むことができる詳細オプションを指定できます。CSR フィールドを設定する場合、システムにより証明書パスワードの入力が求められることに注意してください。
- 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***
- ステップ 7** 設定をコミットします。
- commit-buffer**
- ステップ 8** 認証局に提供する CSR をエクスポートします。認証局は CSR を使用して ID 証明書を作成します。
- a) 完全な CSR を表示します。
- show certreq**
- b) 「-----BEGIN CERTIFICATE REQUEST-----」から「-----END CERTIFICATE REQUEST-----」までの出力をコピーします。

例：

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC6zCCAQMCAQAwdzELMAkGA1UEBhMCVVMxEzARBgNVBAGMCkNhbG1mb3JuaWEw
ETAPBgNVBACMFNhb3N1MRYwFAYDVQQKDA1DaXNjb3R5BTeXN0ZW1zMQwwCgYD
```



```
>-----END CERTIFICATE-----  
>ENDOFBUF
```

ステップ 20 キーリング モードを終了します。

```
exit
```

ステップ 21 セキュリティ モードを終了します。

```
exit
```

ステップ 22 システム モードに入ります。

```
scope system
```

ステップ 23 サービス モードに入ります。

```
scope services
```

ステップ 24 新しい証明書を使用するように FXOS Web サービスを設定します。

```
set https keyring keyring_name
```

ステップ 25 設定をコミットします。

```
commit-buffer
```

ステップ 26 HTTPS サーバに関連付けられているキーリングを表示します。これにはこの手順の手順 3 で作成したキーリングの名前が反映されることとなります。画面出力にデフォルトのキーリング名が表示される場合には、HTTPS サーバはまだ、新しい証明書を使用するように更新されていません。

```
show https
```

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
```

ステップ 27 インポートされた証明書の内容を表示し、**Certificate Status**値が**Valid**と表示されることを確認します。

```
scope security
```

```
show keyring keyring_name detail
```

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-----
MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkJOPQDAjBT
MRUwEwYKcZImiZPyLGGQBGryFbG9jYWwxGDAWBgOJkiaJk/IsZAEZFghuYWF1c3Rp
bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMmTYwNDI4MTMw
OTU0WhcNMmTYwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2F5
aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxXjAUBGNVBAOTDUNpc2NvIFN5c3Rl
bXMxMmYyTERMA8GA1UEBxMIU2FuIEpvc2UxXjAUBGNVBAOTDUNpc2NvIFN5c3Rl
bXMxMmYyTERMA8GA1UEBxMIU2FuIEpvc2UxXjAUBGNVBAOTDUNpc2NvIFN5c3Rl
MA0GCgsqGSIB3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+Lg1UQA0b7tga
BwdudS3sulXIwKGC048mMHCRQw1ADWZCxFANxsnbfb+wrR8xKfKo4vvnMLuK3F5U
R1HLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67Y0yig9WrvqZObwHBg
yodskS/g+a5GNYTzzIS9XAfs1MSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
/cujcb0hNssvmAhh1Vq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAA2H109XR2FAGMB
AAGjggJYMIICVDAcBgNVHREEFtATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
FgQU/1WpstIEYExs8DlZWcuHwZwPtU5QwHwYDVR0jBBgwFoAUyInbDHPPrFwEEBcbx
GsgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBY6CBYIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVVNUSU4tUEMtQ0EwEsQ049bmFhdXN0aW4tccGMsQ049Q0RQLENOFVB1
YmXpYyUyMEtleSUyMFN1cnZpY2VzLENOPVN1cnZpY2VzLENOPUNvbmZpZ3VyYXRp
b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmawNhdGVsZXZvY2F0aW9uTG1z
dD9iYXN1P29iamVjdENsYXNzPWNSTERpc3RyaWJ1dG1vb1BvaW50MIHMBGgrBgEF
BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
QVVVTE1OLVBDLUNBLENOFUFJQSxDTj1QdWJsaWM1MjBLZXklMjBTZXJ2aWN1cyxD
Tj1TZXXJ2aWN1cyxDTj1Db25maWdlcmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
P2NBQ2VydGlmawNhdGU/YmFzZT9vYmplY3RDbGFzZz1jZXJ0aWZpY2F0aW9uQXV0
aG9yaXR5MCEGCSsGAQQBgjcUAQQUHhIAVwBlAGIAUwBlAHIAAdgBlAHIAWdYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
IFew7NcJirEtFRvxyjkQ4/dVo2oI6CRB308WQbYHNUU/AIEA7UdObiSJBG/PBZjm
sgoIK60akbjotOtvUdUd9b6K1Uw=
-----END CERTIFICATE-----

```

Zeroized: No

次のタスク

新しい信頼できる証明書が存在していることを確認するには、Web ブラウザのアドレス バーに `https://<FQDN_or_IP>/` と入力して、Firepower Chassis Manager に移動します。



- (注) ブラウザはさらに、アドレス バーの入力内容に照らして証明書のサブジェクト名を確認します。証明書が完全修飾ドメイン名に対して発行されている場合、ブラウザでもそのようにアクセスする必要があります。IP アドレスを使用してアクセスすると、信頼できる証明書が使用されているとしても、別の SSL エラー（共通名が無効）がスローされます。

証明書の更新の自動インポート

Cisco 証明書サーバーが別のルート CA を利用するようにアイデンティティ証明書を変更すると、ASA デバイスを実行している 4100 または 9300 のスマートライセンスの接続が切断されます。ライセンス接続はアプリケーションの Lina ではなくスーパーバイザによって処理される

ため、スマートライセンス機能は失敗します。FXOS ベースのデバイスの場合、FXOS ソフトウェアにアップグレードしなくても、自動インポート機能を使用して問題を解決できます。

デフォルトでは、自動インポート機能はディセーブルです。次の手順を使用して、FXOS CLI を使用して自動インポート機能を有効にすることができます。

始める前に

DNS サーバーは、Cisco 証明書サーバーに到達するように設定する必要があります。

http://www.cisco.com/security/pki/trs/ios_core.p7b

手順

ステップ 1 FXOS CLI に接続します。

ステップ 2 セキュリティ モジュールを入力します。

scope security

ステップ 3 自動インポート機能を有効にします。

enter tp-auto-import

例 :

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

ステップ 4 設定をコミットします。

commit-buffer

ステップ 5 自動インポートステータスの検証

show detail

例 :

自動インポートの成功 :

```
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 #
```

自動インポートの失敗 :

```
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 #
```

ステップ6 tp-auto-import 機能を設定します。import-time-hour を設定します。

set import-time-hour *hour* **import-time-min** *minutes*

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) 自動インポートのソース URL は固定されており、インポート時間の詳細を 1 日あたりの分に変更する必要があります。インポートは、スケジュールされた時刻に毎日行われます。時間と分が設定されていない場合、証明書のインポートはその有効化時に 1 回だけ行われます。証明書は、/opt/certstore パスの下のボックスにバンドルとしてダウンロードされ、セキュアログインオプションを介してのみアクセスできます。バンドル (ios_core.p7b) とともに、個々の証明書 (AutoTP1 から AutoTPn) が自動的に抽出されます。

ステップ7 自動インポート設定が完了したら、show detail コマンドを入力します。

show detail

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) インポートできる証明書の最大数は 30 です。Cisco 証明書サーバーへの接続に問題がある場合、各インポートは 6 回繰り返され、show コマンドで最後のインポートステータスが更新されます。

ステップ8 (オプション) 自動インポート機能を無効にするには、delete auto-import コマンドを入力します。

delete tp-auto-import

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) 自動インポート機能を無効にすると、インポートされた証明書は、ビルドの変更がなくなるまで持続します。自動インポート機能を無効にしてからビルドをダウングレード/アップグレードすると、証明書が削除されます。

ログイン前バナー

ログイン前バナーでは、ユーザが Firepower Chassis Manager にログインするとシステムにバナーテキストが表示されます。ユーザ名とパスワードのシステムプロンプトの前に、メッセージの画面で [OK] をクリックする必要があります。ログイン前バナーを設定しないと、システムはユーザ名とパスワードのプロンプトにすぐに進みます。

ユーザが FXOS CLI にログインすると、設定されている場合はシステムがパスワードのプロンプトの前にログインバナーテキストを表示します。

ログイン前バナーの作成

手順

ステップ 1 FXOS CLI に接続します ([FXOS CLI へのアクセス](#)を参照)。

ステップ 2 セキュリティ モードを開始します。

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

ステップ 3 バナー セキュリティ モードに入ります。

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

ステップ 4 次のコマンドを入力して、ログイン前バナーを作成します。

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

ステップ 5 Firepower Chassis Manager または FXOS CLI へのログイン前のユーザに FXOS が表示するメッセージを指定します。

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

ログイン前バナー メッセージのテキストを入力するためのダイアログを開始します。

ステップ 6 プロンプトで、ログイン前バナー メッセージを入力します。このフィールドには、標準の ASCII 文字を入力できます。複数行のテキストを入力できますが、各行の最大文字数は 192 文字です。行の区切りで Enter キーを押します。

入力内容の次の行に **ENDOFBUF** と入力し、**Enter** キーを押して終了します。

[メッセージの設定 (set message)] ダイアログをキャンセルするには、**Ctrl+C** キーを押します。

ステップ 7 トランザクションをシステム設定にコミットします。

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

例

次の例は、ログイン前バナーを作成します。

```
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 #
```

ログイン前バナーの変更

手順

ステップ 1 FXOS CLI に接続します ([FXOS CLIへのアクセス](#)を参照)。

ステップ 2 セキュリティ モードを開始します。

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

ステップ 3 バナー セキュリティ モードに入ります。

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

ステップ 4 ログイン前バナーのバナー セキュリティ モードに入ります。

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

ステップ 5 Firepower Chassis Manager または FXOS CLI へのログイン前のユーザに FXOS が表示するメッセージを指定します。

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

ログイン前バナー メッセージのテキストを入力するためのダイアログを開始します。

ステップ6 プロンプトで、ログイン前バナーメッセージを入力します。このフィールドには、標準のASCII文字を入力できます。複数行のテキストを入力できますが、各行の最大文字数は192文字です。行の区切りでEnterキーを押します。

入力内容の次の行に **ENDOFBUF** と入力し、**Enter** キーを押して終了します。

[メッセージの設定 (set message)]ダイアログをキャンセルするには、**Ctrl+C** キーを押します。

ステップ7 トランザクションをシステム設定にコミットします。

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

例

次に、ログイン前バナーを変更する例を示します。

```
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 #
```

ログイン前バナーの削除

手順

ステップ1 FXOS CLI に接続します ([FXOS CLIへのアクセス](#)を参照)。

ステップ2 セキュリティ モードを開始します。

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

ステップ3 バナー セキュリティ モードに入ります。

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

ステップ4 システムからログイン前バナーを削除します。

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

ステップ5 トランザクションをシステム設定にコミットします。

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

例

次に、ログイン前バナーを削除する例を示します。

```
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 #
```

Firepower 4100/9300 シャーシの再起動

手順

-
- ステップ 1** [概要 (Overview)] を選択して、[概要 (Overview)] ページを開きます。
 - ステップ 2** [概要 (Overview)] ページの右上隅の [シャーシ稼働時間 (Chassis Uptime)] の横にある [リブート (Reboot)] をクリックします。
 - ステップ 3** [はい (Yes)] をクリックして、Firepower 4100/9300 シャーシを電源オフにすることを確認します。
システムはそのシステム上で構成されているすべての論理デバイスをグレースフルにシャットダウンし、最終的に Firepower 4100/9300 シャーシの電源をオフにして再起動する前に、セキュリティ モジュール/エンジンの電源を個別にオフにします。このプロセスには約 15 ～ 20 分かかります。
-

Firepower 4100/9300 シャーシの電源オフ

手順

-
- ステップ 1** [Overview] を選択して、[Overview] ページを開きます。
 - ステップ 2** [概要 (Overview)] ページの右上隅の [シャーシ稼働時間 (Chassis Uptime)] の横にある [シャットダウン (Shutdown)] をクリックします。
 - ステップ 3** [はい (Yes)] をクリックして、Firepower 4100/9300 シャーシを電源オフにすることを確認します。
システムはそのシステム上で構成されているすべての論理デバイスをグレースフルにシャットダウンし、最終的に Firepower 4100/9300 シャーシの電源をオフにする前に、セキュリティ モジュール/エンジンの電源を個別にオフにします。
-

工場出荷時のデフォルト設定の復元

FXOS CLI を使用して Firepower 4100/9300 シャーシを工場出荷時のデフォルト設定に戻すことができます。



(注) このプロセスによって、論理デバイス設定を含むすべてのユーザ設定がシャーシから消去されます。この手順が完了したら、システムを再設定する必要があります ([初期設定](#) を参照してください)。

手順

ステップ 1 (任意) **erase configuration** コマンドはシャーシからスマート ライセンス設定を削除しません。スマート ライセンス設定も削除する場合は、次の手順を実行します。

scope license

deregister

Firepower 4100/9300 シャーシの登録を解除すると、アカウントからデバイスが削除されます。さらに、デバイス上のすべてのライセンス資格と証明書が削除されます。

ステップ 2 ローカル管理シェルに接続します。

connect local-mgmt

ステップ 3 Firepower 4100/9300 シャーシからすべてのユーザ設定を消去し、最初の工場出荷時のデフォルト設定にシャーシを復元するには、次のコマンドを入力します。

erase configuration

すべてのユーザ設定を消去するかどうかを確認するように求められます。

ステップ 4 設定の消去を確認するには、コマンドプロンプトに **yes** と入力します。

すべてのユーザ設定が Firepower 4100/9300 シャーシから消去された後、システムがリブートします。

システム コンポーネントの安全な消去

FXOS CLI を使用して、アプライアンスのコンポーネントを安全に消去することができます。

「[工場出荷時のデフォルト設定の復元 \(20 ページ\)](#)」で説明されているように、**erase configuration** コマンドを実行すると、シャーシのすべてのユーザ設定情報が削除され、工場出荷時のデフォルト設定に戻ります。

secure erase コマンドにより、指定したアプライアンス コンポーネントが安全に消去されます。つまり、単にデータが削除されるだけでなく、物理ストレージが「ワイプ」（完全に消去）されます。これは、ハードウェア ストレージ コンポーネントが残存データやスタブを保持しない状態で、アプライアンスを転送または返却する際に重要です。



- (注) 完全消去中にデバイスが再起動します。これは、SSH接続が終了したことを意味します。したがって、シリアルコンソールポート接続を介して完全消去を実行することをお勧めします。

手順

ステップ 1 ローカル管理シェルに接続します。

```
connect local-mgmt
```

ステップ 2 指定したアプライアンス コンポーネントを安全に消去するには、次の **erase configuration** コマンドのいずれかを入力します。

a) **erase configuration chassis**

すべてのデータとイメージが失われ、回復できないことを警告するメッセージが表示され、続行するかどうかの確認が求められます。**y**を入力すると、シャーシ全体が安全に消去されます。セキュリティモジュールが最初に消去され、その後にスーパーバイザが消去されます。

デバイス上のすべてのデータとソフトウェアが消去されるため、デバイスリカバリはROM モニタ (ROMMON) からのみ実行できます。

b) **erase configuration security_module module_id**

モジュール上のすべてのデータとイメージが失われ、回復できないことを警告するメッセージが表示され、続行するかどうかの確認が求められます。**y**を入力すると、モジュールが消去されます。

- (注) **decommission-secure** コマンドの実行結果は、基本的にこのコマンドを実行した場合と同じです。

セキュリティモジュールが消去されると、確認応答されるまでダウンした状態になります (デコミッションされたモジュールと同様)。

c) **erase configuration supervisor**

すべてのデータとイメージが失われ、回復できないことを警告するメッセージが表示され、続行するかどうかの確認が求められます。**y**を入力すると、スーパーバイザが安全に消去されます。

スーパーバイザ上のすべてのデータとソフトウェアが消去されるため、デバイスリカバリは ROM モニタ (ROMMON) からのみ実行できます。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。