再イメージ化の手順

ディザスタリカバリの概要

設定のリセット、イメージの再インストール、FXOS パスワードの回復、またはシステムの完全な再イメージ化が必要になる場合があります。次の該当する手順を参照してください。

- 設定の消去と同じイメージでのシステムの再起動：すべての設定が削除され、現在のイメージを使用して Threat Defense が再インストールされます。この手順を実行する場合は、実行後に、管理者パスワードや接続情報などを含めて、システムを再設定する必要があります。ベース インストール ソフトウェア バージョンを使用したシステムの再イメージ化 （2 ページ）を参照してください。

- ROMMON からの工場出荷時設定へのリセットの実行（管理者パスワードの回復）：すべての設定が削除され、現在のイメージを使用して Threat Defense が再インストールされます。この手順を実行する場合は、実行後に、管理者パスワードや接続情報などを含めて、システムを再設定する必要があります。ROMMON からの工場出荷時設定へのリセットの実行（パスワードのリセット） （5 ページ）を参照してください。

- 新しいバージョンでのシステムの再イメージ化：すべての設定が削除され、新しいソフトウェアイメージを使用して Threat Defense が再インストールされます。この手順を実行する場合は、実行後に、管理者パスワードや接続情報などを含めて、システムを再設定する必要があります。新しいソフトウェアバージョンを使用したシステムの再イメージ化 （7 ページ）を参照してください。

（注） この手順を使用して以前のメジャーバージョンにダウングレードすることはできません。代わりに完全な再イメージ化の実行 （18 ページ）を使用する必要があります。

- SSD ファイルシステムの再フォーマット：ディスク破損メッセージが表示された場合に SSD を再フォーマットします。すべての設定が削除されます。この手順を実行する場合は、実行後に、管理者パスワードや接続情報などを含めて、システムを再設定する必要があります。SSD ファイルシステムの再フォーマット（Firepower 2100） （10 ページ）を参照してください。
- ROMMON からの起動：FXOS を起動できない場合に ROMMON から起動します。その後、eMMC を再フォーマットし、ソフトウェアイメージを再インストールできます。この手順では、すべての設定が保持されます。ROMMON からの起動 （10 ページ）を参照してください。
- すべての設定とイメージの消去：システムを工場出荷時のデフォルト設定に戻し、イメージを消去します。この手順では、TFTP 経由でシステムを起動し、Threat Defense ソフトウェアをダウンロードし、システム全体を再設定する必要があります。完全な再イメージ化の実行 （18 ページ） を参照してください。
- 管理者パスワードの変更：Threat Defense CLI から管理者パスワードを変更します。管理者パスワードの変更 （23 ページ） を参照してください。
- Threat Defense がオフラインの場合の管理者パスワードの変更：FXOS から管理者パスワードを変更します。Threat Defense がオフラインの場合の管理者パスワードの変更 （23 ページ） を参照してください。Threat Defense がオンラインの場合は、Threat Defense CLI を使用して管理者パスワードを変更する必要があります。

ベース インストール ソフトウェア バージョンを使用したシステムの再イメージ化

この手順を実行すると、ベース インストール ソフトウェア バージョンの設定を除き、すべての設定が消去されます。設定の消去操作後にシステムが再起動すると、Threat Defense のスタートアップバージョンが実行されます。

現在実行中のバージョンがアップグレード専用イメージの場合は、この手順を実行した後、Threat Defense を再アップグレードする必要があります。たとえば、バージョン 6.2.2.x はアッ

プグレード専用のイメージです。6.2.2.x システムでこの手順を実行すると、ベースインストール パッケージ（バージョン 6.2.1.x）が再インストールされます。その後、Secure Firewall Management Center または Secure Firewall Device Manager を使用してバージョン 6.2.2.x に再アップグレードする必要があります。この場合、FXOS のバージョンが下位バージョンに戻らないことがあります。この不一致により、ハイアベイラビリティ構成で障害が発生する可能性があります。このシナリオでは、システムの完全な再イメージ化を実行することを推奨します（詳細については、完全な再イメージ化の実行 （18 ページ）を参照してください）。

（注） この手順を実行すると、管理者パスワードが **Admin123** にリセットされます。

始める前に

- FXOS CLI コンテキストに接続されていることを確認します。シリアルコンソールを介して Firepower 1000/2100 または Cisco Secure Firewall 3100 デバイスに接続すると、FXOS CLI コンテキストに自動的に接続されます。Threat Defense CLI コンテキストに接続されている場合は、まず **connect fxos** コマンドを使用して FXOS CLI コンテキストに切り替える必要があります。
- アプライアンスの管理IPアドレスの設定をメモし、次のコマンドで示される情報をコピーします。

```
firepower # scope fabric a
firepower /fabric-interconnect # show detail
```

- 次のコマンドを使用して Threat Defense のベース インストール バージョンを確認し、メモしておきます。起動バージョンの列には、ベース インストール バージョンが表示されます。「Running Version」には、ベース インストール バージョンに適用したアップグレードが表示されます。

```
firepower# scope ssa
firepower /ssa # show app-instance
Application Name     Slot ID    Admin State     Operational State    Running Version
 Startup Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
 --------------- ------------------
ftd                  1          Enabled         Online               6.2.2.49
 6.2.1.341       Not Applicable
```

- Smart Licensing からデバイスの関連付けを解除します。
- クラウドテナントからデバイスを登録解除します（該当する場合）。クラウドからの登録解除 （25 ページ） を参照してください。
- Cisco Secure Firewall 3100 デバイスを Threat Defense 7.3.0 バージョンに再イメージ化するには、ROMMON バージョン 1.1.08 以降が必要です。現在の ROMMON バージョンが 1.1.08 未満の場合は、ASA 9.19 以降にアップグレードして ROMMON をアップグレードする必要があります。Management Center または Device Manager を使用して Threat Defense を

7.3.0 にアップグレードすることもできます（詳細については、Threat Defense Reimage を参照してください）。

手順

ステップ 1 FXOS CLI でローカル管理に接続します。

firepower # **connect local-mgmt**

ステップ 2 すべての設定を消去します。

firepower(local-mgmt) # **erase configuration**

例：

```
firepower(local-mgmt)# erase configuration
All configurations will be erased and system will reboot. Are you sure? (yes/no):yes
Removing all the configuration. Please wait....
Configurations are cleaned up. Rebooting....
```

ステップ 3 システムが再起動したら、**show app-instance** コマンドを使用してアプリケーションの状態を確認できます。パスワードログインは、デフォルトの **admin/Admin123** にリセットされます。

例：

```
firepower# scope ssa

firepower /ssa # show app-instance
Application Name     Slot ID    Admin State     Operational State    Running Version
Startup Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Disabled        Installing
6.2.1-1314     Not Applicable
```

（注） アプリケーションのインストールが完了するまで 10 分以上かかります。Threat Defense がオンライン状態に戻ると、**show app-instance** コマンドの Operational State に「Online」と表示されます。

例：

```
firepower /ssa # show app-instance
Application Name     Slot ID    Admin State     Operational State    Running Version
Startup Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               6.2.1.10140
```

次のタスク

スタートアップガイドのセットアップタスクを完了し、必要に応じて最新バージョンにアップグレードします。

ROMMONからの工場出荷時設定へのリセットの実行（パスワードのリセット）

FXOS にログインできない場合（パスワードを忘れた場合、または SSD disk1 ファイルシステムが破損している場合）は、ROMMON を使用して FXOS および Threat Defense の設定を工場出荷時のデフォルトに復元できます。管理者パスワードはデフォルトの **Admin123** にリセットされます。パスワードがわかっていて、FXOS 内から工場出荷時のデフォルト設定を復元する場合は、ベース インストール ソフトウェア バージョンを使用したシステムの再イメージ化（2 ページ） を参照してください。

始める前に

- Cisco Secure Firewall 3100 デバイスを Threat Defense 7.3.0 バージョンに再イメージ化するには、ROMMON バージョン 1.1.08 以降が必要です。現在の ROMMON バージョンが 1.1.08 未満の場合は、ASA 9.19 以降にアップグレードして ROMMON をアップグレードする必要があります。Management Center または Device Manager を使用して、Threat Defense のバージョンを 7.3.0 にアップグレードすることもできます（詳細については、Threat Defense Reimage を参照してください）。

手順

ステップ 1 デバイスの電源を入れます。次のようなプロンプトが表示されたら、ESC キーを押してブートを中断します。

```
Example:
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

ステップ 2 ROMMON のバージョンを確認します。

rommon 1 > **show info**

例：

Firepower 1000 および 2100 デバイス

```
rommon 1 > show info

Cisco System ROMMON, Version 1.0.06, RELEASE SOFTWARE
Copyright (c) 1994-2017  by Cisco Systems, Inc.
Compiled Wed 11/01/2017 18:38:59.66 by builder
```

Cisco Secure Firewall 3100 デバイス

```
rommon 1 > show info
Cisco System ROMMON, Version 1.1.08 , RELEASE SOFTWARE
Copyright (c) 1994-2022  by Cisco Systems, Inc.
Compiled Fri 06/10/2022 10:25:43.78 by Administrator
```

ステップ 3 デバイスを工場出荷時設定にリセットします。

ROMMON バージョン1.0.06 以降の場合：

rommon 2 > **factory-reset**

ROMMON バージョン1.0.04 の場合：

rommon 2 > **password_reset**

例：

Firepower 1000 および 2100 デバイス

```
rommon 2 > factory-reset
Warning: All configuration will be permanently lost with this operation
         and application will be initialized to default configuration.
         This operation cannot be undone after booting the application image.

         Are you sure you would like to continue ? yes/no [no]: yes
        Please type 'ERASE' to confirm the operation or any other value to cancel: ERASE


Performing factory reset...
File size is 0x0000001b
Located .boot_string
Image size 27 inode num 16, bks cnt 1 blk size 8*512

Rommon will continue to boot disk0: fxos-k8-fp2k-lfbff.2.3.1.132.SSB
Are you sure you would like to continue ? yes/no [no]: yes
File size is 0x0817a870
Located fxos-k8-fp2k-lfbff.2.3.1.132.SSB
```

例：

Cisco Secure Firewall 3100 デバイス

```
rommon 2 > factory-reset
Warning: All configuration will be permanently lost with this operation
         and application will be initialized to default configuration.
         This operation cannot be undone after booting the application image.

         Are you sure you would like to continue ? yes/no [no]: yes
        Please type 'ERASE' to confirm the operation or any other value to cancel: ERASE


Performing factory reset...
File size is 0x0000001b
Located .boot_string
Image size 27 inode num 16, bks cnt 1 blk size 8*512

Rommon will continue to boot disk0: Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
Are you sure you would like to continue ? yes/no [no]: yes
File size is 0x0817a870
Located Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
```

ステップ 4 システムから起動を求めるプロンプトが表示されない場合は、**boot** コマンドを入力します。

rommon 3 > **boot**

次のタスク

スタートアップガイドのセットアップタスクを実行します。

新しいソフトウェアバージョンを使用したシステムの再イメージ化

この手順では、新しいソフトウェアバージョンでシステムを再イメージ化できます。この手順を実行した後、デバイスの管理 IP アドレスとその他の設定パラメータを再設定する必要があります。設定を消去せずにソフトウェアをアップグレードする場合は、アップグレードガイドを参照してください。

（注） この手順を使用して以前のメジャーバージョンにダウングレードすることはできません。代わりに完全な再イメージ化の実行 （18 ページ）を使用する必要があります。

（注） この手順を実行すると、管理者パスワードが **Admin123** にリセットされます。

始める前に

- FXOS CLI コンテキストに接続されていることを確認します。シリアルコンソールを介して Firepower 1000/2100 または Cisco Secure Firewall 3100 デバイスに接続すると、FXOS CLI コンテキストに自動的に接続されます。Threat Defense CLI コンテキストに接続されている場合は、まず **connect fxos** コマンドを使用して FXOS CLI コンテキストに切り替える必要があります。
- アプライアンスの管理IPアドレスの設定をメモし、次のコマンドで示される情報をコピーします。

```
firepower # scope fabric a
firepower /fabric-interconnect # show detail
```

- Smart Licensing からデバイスの関連付けを解除します。
- クラウドテナントからデバイスを登録解除します（該当する場合）。クラウドからの登録解除 （25 ページ） を参照してください。
- Cisco Secure Firewall 3100 デバイスを Threat Defense バージョン 7.3.0 に再イメージ化するには、ROMMONバージョン1.1.08以降が必要です。現在のROMMONバージョンが1.1.08未満の場合は、ASA 9.19 以降にアップグレードして ROMMON をアップグレードする必要があります。Management Center または Device Manager を使用して、Threat Defense のバージョンを7.3.0にアップグレードすることもできます（詳細については、Threat Defense Reimage を参照してください）。

手順

ステップ 1 ソフトウェアバンドルをローカルコンピュータまたは USB フラッシュドライブにダウンロードします。

ステップ 2 USB ドライブを使用する場合は、アプライアンスの USB ポートに USB ドライブを挿入します。

ステップ 3 FXOS で、システムのスコープを入力し、システムで現在実行されているバージョンを確認します。

firepower # **scope system**

firepower /system # **show version detail**

ステップ 4 ファームウェアのスコープを入力します。

firepower # **scope firmware**

ステップ 5 新しいソフトウェアパッケージをダウンロードします。USB ドライブを使用してソフトウェアパッケージをダウンロードする場合は、次の構文を使用します。

firepower # **scope firmware**

firepower /firmware # **download image** usbA:*image_name*

image_name は、ステップ 3（上記）の **show version detail** コマンドの出力です。

次に例を示します。

firepower /firmware # **download image** usbA:cisco-ftd-fp2k.6.2.1-36.SPA

（注） バージョン 7.3+ では、Cisco Secure Firewall 3100 の Threat Defense のインストールおよびアップグレードパッケージを組み合わせたパッケージとなっています。説明されている手順では、`.SPA` ファイルの代わりに`.REL.tar` ファイルを使用できます。

FTP、SCP、SFTP、TFTP を使用して、Threat Defense ソフトウェアパッケージをデバイスにコピーすることもできます。

firepower /firmware # **download image** *tftp/ftp/scp/sftp***://***path to the image, including the server root /image name*

Firepower 1000 および 2100 デバイスの例を示します。

```
firepower /firmware # download image tftp://example.cisco.com/fxos-2k.6.2.1-1314.SPA
```

Cisco Secure Firewall 3100 デバイスの例を示します。

```
firepower /firmware # download image
scp://example.cisco.com/auto/Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar
```

（注） システムはダウンロードイメージ要求で指定されたファイル名の前にスラッシュを付加するので、FTP/TFTP/SCP/SFTP によりファイル転送を実行する場合は、サーバのルートを含むイメージの絶対パスを入力する必要があります。

必要に応じて、IP アドレスの代わりに FQDN を使用できます。

ステップ 6 ダウンロード タスクを表示して、ダウンロードの進行状況をモニタします。

firepower /firmware # **show download-task**

Status 列の出力に「Downloaded」と表示されたら、ダウンロードは完了です。

例：

Cisco Secure Firewall 3100 デバイス

```
firepower 3110 /firmware # show download task
File Name Protocol Server Port Userid State
--------- -------- ------ ---- ------------
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar
          Scp 172.23.205.217 0 <xxxxxx> Downloaded
```

ステップ 7 ダウンロードの完了後、システムにインストールされているソフトウェア パッケージを表示し、出力に示されているバンドル イメージ バージョンをコピーします。

firepower /firmware # **show package**

例：

Firepower 1000 および 2100 デバイス

```
firepower /firmware # show package
Name                                         Package-Vers
-------------------------------------------- ------------
cisco-ftd-fp2k.6.2.1-1314.SPA                6.2.1-1314
```

上記の例では、**6.2.1-1314** はセキュリティパックのバージョンです。

例：

Cisco Secure Firewall 3100 デバイス

```
firepower 3110 /firmware # show package
Name                                           Package Vers
---------------------------------------------  ---------------
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar      7.3.0-14
```

上記の例では、**7.3.0-14** はセキュリティパックのバージョンです。

ステップ 8 自動インストールのスコープを入力します。

firepower /firmware # **scope auto-install**

ステップ 9 新しいアプリケーション ソフトウェア パッケージをインストールします（*version* は上記の show package の出力です）。

firepower /firmware/auto-install # **install security-pack version** *version*

例：

```
firepower 3110 /firmware/auto install # install security pack version 7.3.0-14
…
```

```
firepower /firmware # connect ftd
> show version
-----------------[ firepower 3100 ]-----------------
Model : Cisco Secure Firewall 3110 Threat Defense (80) Version 7.3.0 (Build
```

ステップ 10 入力を求められたら、**yes** と入力します。

システムが再起動し、最新のソフトウェアバンドルがインストールされます。

次のタスク

スタートアップガイドのセットアップタスクを実行します。

SSD ファイルシステムの再フォーマット（Firepower 2100）

FXOS に正常にログインしたが、ディスク破損エラーメッセージが表示された場合は、FXOS および Threat Defense 設定が保存されている SSD1 を再フォーマットできます。この手順により、FXOS 設定が工場出荷時のデフォルトに復元されます。管理者パスワードはデフォルトの **Admin123** にリセットされます。この手順では、Threat Defense の設定もリセットされます。

この手順は Firepower 1000 および Cisco Secure Firewall 3100 に適用されません。このため、スタートアップイメージを維持しながら SSD を消去することはできません。

手順

ステップ 1 コンソールポートから FXOS CLI に接続します。

ステップ 2 SSD1 を再フォーマットします。

connect local-mgmt

format ssd1

ステップ 3 スタートアップガイドのセットアップタスクを実行します。

ROMMON からの起動

デバイスを起動できない場合は、USB または TFTP イメージから FXOS を起動できる ROMMON が起動します。FXOS を起動した後、eMMC（ソフトウェアイメージを保持する内部フラッシュデバイス）を再フォーマットできます。再フォーマットした後、イメージを eMMC に再ダウンロードする必要があります。この手順では、個別の ssd1 に保存されているすべての設定が保持されます。

電力障害やその他のまれな状態が原因で、eMMC ファイルシステムが破損している可能性があります。

始める前に

- この手順を実行するには、コンソールにアクセスできる必要があります。
- Cisco Secure Firewall 3100 デバイスを Threat Defense バージョン 7.3.0 に再イメージ化するには、ROMMON バージョン 1.1.08 以降が必要です。現在の ROMMON バージョンが 1.1.08 未満の場合は、ASA 9.19 以降にアップグレードして ROMMON をアップグレードする必要があります。Management Center または Device Manager を使用して、Threat Defense のバージョンを 7.3.0 にアップグレードすることもできます（詳細については、Threat Defense Reimage を参照してください）。

手順

ステップ 1 起動できない場合、システムは ROMMON を起動します。ROMMON が自動的に起動されない場合、ブートアップ中に ROMMON プロンプトを表示するよう要求されたら、**Esc** を押します。モニタを注視します。

例：

```
********************************************************************************
Cisco System ROMMON, Version 1.0.06, RELEASE SOFTWARE
Copyright (c) 1994-2018  by Cisco Systems, Inc.
Compiled Thu 04/06/2018 12:16:16.21 by builder
********************************************************************************

Current image running: Boot ROM0
Last reset cause: ResetRequest
DIMM_1/1 : Present
DIMM_2/1 : Present

Platform FPR-2130 with 32768 MBytes of main memory
BIOS has been successfully locked !!
MAC Address: 0c:75:bd:08:c9:80

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

この時点で、Esc を押します。

ステップ 2 USB ドライブ上のイメージからブートするか、または TFTP を使用してネットワークを介してブートします。

（注） 6.4 以前の場合、ROMMON から FXOS を起動し、現在インストールされているイメージもブート可能である場合は、現在インストールされているイメージと同じバージョンを起動していることを確認してください。それ以外の場合、FXOS/Threat Defense バージョンが一致しないと、Threat Defense がクラッシュします。6.5 以降では、ROMMON から FXOS を起動すると、Threat Defense が自動的にロードされなくなります。

Firepower 1000/2100 USB から起動する場合：

boot disk1:*/path/filename*

デバイスは FXOS CLI に起動します。ディスクの内容を表示するには、**dir disk1:** コマンドを使用します。

例：

```
rommon 1 > dir disk1:
rommon 2 > boot disk1:/cisco-ftd-fp2k.6.4.0.SPA
```

Cisco Secure Firewall 3100 USB から起動する場合：

boot usb:/*path*/*filename*

デバイスは FXOS CLI に起動します。ディスクの内容を表示するには、**dir usb:** コマンドを使用します。

例：

```
rommon 1 > dir usb:
rommon 2 > boot usb:/cisco-ftd-fp3k.7.1.0.SPA
```

TFTP から起動する場合は、次のようにします。

管理 1/1 のネットワーク設定を指定し、次の ROMMON コマンドを使用して Threat Defense パッケージをロードします。

address *management_ip_address*

netmask *subnet_mask*

server *tftp_ip_address*

gateway *gateway_ip_address*

file*path*/*filename*

set

sync

tftp -b

FXOS イメージがダウンロードされ、CLI にブートアップされます。

次の情報を参照してください。

- **set**：ネットワーク設定を表示します。**ping** コマンドを使用してサーバへの接続を確認することもできます。
- **sync**：ネットワーク設定を保存します。
- **tftp -b**：FXOS をロードします。

例：

Firepower 1000 および 2100 デバイス

```
rommon 1 > address 10.86.118.4
rommon 2 > netmask 255.255.252.0
rommon 3 > server 10.86.118.21
```

```
rommon 4 > gateway 10.86.118.1
rommon 5 > file cisco-ftd-fp2k.6.4.0.SPA
rommon 6 > set
ROMMON Variable Settings:
  ADDRESS=10.86.118.4
  NETMASK=255.255.252.0
  GATEWAY=10.86.118.21
  SERVER=10.86.118.21
  IMAGE=cisco-ftd-fp2k.6.4.0.SPA
  CONFIG=
  PS1="rommon ! > "

rommon 7 > sync
rommon 8 > tftp -b
Enable boot bundle: tftp_reqsize = 268435456

             ADDRESS: 10.86.118.4
             NETMASK: 255.255.252.0
             GATEWAY: 10.86.118.21
              SERVER: 10.86.118.1
               IMAGE: cisco-ftd-fp2k.6.4.0.SPA
             MACADDR: d4:2c:44:0c:26:00
           VERBOSITY: Progress
               RETRY: 40
          PKTTIMEOUT: 7200
             BLKSIZE: 1460
            CHECKSUM: Yes
                PORT: GbE/1
             PHYMODE: Auto Detect

link up
Receiving cisco-ftd-fp2k.6.4.0.SPA from 10.86.118.21!!!!!!!!
[…]
```

サーバーへの接続をトラブルシューティングするには、**Ping** を実行します。

```
rommon 1 > ping 10.86.118.21
Sending 10, 32-byte ICMP Echoes to 10.86.118.21 timeout is 4 seconds
!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 2 >
```

例：

Cisco Secure Firewall 3100 デバイス

```
rommon 1 > show info

Cisco System ROMMON, Version 1.1.08, RELEASE SOFTWARE
Copyright (c) 1994-2022  by Cisco Systems, Inc.
Compiled Fri 06/10/2022 10:25:43.78 by Administrator
********************************************************************************

rommon 2 > ADDRESS=172.16.0.50
rommon 3 > NETMASK=255.255.255.0
rommon 4 > GATEWAY=172.16.0.254
rommon 5 > SERVER=172.23.37.186
rommon 6 > IMAGE=image_dir/Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
rommon 7 > set
    ADDRESS=172.16.0.50
    NETMASK=255.255.255.0
    GATEWAY=172.16.0.254
```

```
    SPEED=10000
    SERVER=172.23.37.186
    IMAGE= image_dir/Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
    CONFIG=
    PS1="rommon ! > "
    FIRMWARE_VERSION=1.3.5

rommon 8 > sync
rommon 9 > tftp -b
Enable boot bundle: tftp_reqsize = 402653184

             ADDRESS: 172.16.0.50
             NETMASK: 255.255.255.0
             GATEWAY: 172.16.0.254
              SERVER: 172.23.37.186
               IMAGE: image_dir/Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
           VERBOSITY: Progress
               RETRY: 40
          PKTTIMEOUT: 7200
             BLKSIZE: 1460
            CHECKSUM: Yes
                PORT: 10G/1
             PHYMODE: Auto Detect
.=====…
+------------------------------------------------------------------------+
+------------------------- SUCCESS --------------------------------------+
+------------------------------------------------------------------------+
|                                                                        |
|             LFBFF signature authentication passed !!!                  |
|                                                                        |
+------------------------------------------------------------------------+
LFBFF signature verified.
```

ステップ 3 現在の管理者パスワードを使用して FXOS にログインします。

（注） ログイン情報がわからない場合、またはディスクの破損が原因でログインできない場合は、ROMMON **factory-reset** コマンドを使用して工場出荷時設定へのリセットを実行する必要があります（ROMMON からの工場出荷時設定へのリセットの実行（パスワードのリセット） （5 ページ） を参照）。初期設定へのリセットを実行したら、この手順を再開して FXOS を起動し、デフォルトのログイン情報（**admin/Admin123**）でログインします。

ステップ 4 EMMC を再フォーマットします。

connect local-mgmt

format emmc

yes と入力します。

例：

```
firepower-2110# connect local-mgmt
firepower-2110(local-mgmt)# format emmc
All bootable images will be lost.
Do you still want to format? (yes/no):yes


firepower-3110# connect local-mgmt
firepower-3110(local-mgmt)# format emmc
```

```
All bootable images will be lost.
Do you still want to format? (yes/no):yes
```

ステップ 5 Threat Defense パッケージを再ダウンロードして起動します。

（注） ログインできなかったために工場出荷時設定へのリセットを実行した場合は、設定が工場出荷時のデフォルト設定に復元されます。このリセットは、ネットワーク設定がデフォルトに変更されたことを意味します。ネットワーク設定を復元するには、スタートアップガイドに従って初期設定を実行します。ネットワーク接続を再確立した後、この手順を続行します。

a) パッケージをダウンロードします。USB または TFTP から一時的に起動したので、引き続きローカルディスクにイメージをダウンロードする必要があります。

scope firmware

download image *url*

show download-task

次のいずれかを使用してインポートするファイルの URL を指定します。

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*
- **usbA:**/*path*/*filename*

例：

Firepower 1000 および 2100 デバイス

```
firepower-2110# scope firmware
firepower-2110 /firmware # download image tftp://10.86.118.21/cisco-asa-fp2k.9.8.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
 download progress.
firepower-2110 /firmware # show download-task
Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.21             0                 Downloaded
```

例：

Cisco Secure Firewall 3100 デバイス

```
firepower-3110# scope firmware
firepower-3110 /firmware # download image
scp://172.23.205.217/auto/Cisco_FTD_SSP_FP3K_Upgrade 7.3.0-14.sh.REL.tar
Please use the command 'show download-task' or 'show download-task detail' to check
 download progress.
firepower-3110 /firmware # show download-task
Download task:
```

```
File Name     Protocol     Server           Port     Userid     State
---------     --------     ---------------  ----     ------     -----
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar 7.3.0-14.sh.REL.tar
              Scp          172.23.205.217     0                Downloaded
```

b) パッケージのダウンロードが完了（[ダウンロード済み（Downloaded）] の状態）したら、パッケージを起動します。

show package

scope auto-install

install security-pack version *version*

show package の出力で、**security-pack version** 番号の **Package-Vers** 値をコピーします。シャーシが ASA イメージをインストールして再起動します。

例：

Firepower 1000 および 2100 デバイス

```
firepower 2110 /firmware # show package
Name                                         Package-Vers
-------------------------------------------- ------------
cisco-asa-fp2k.9.8.2.SPA                     9.8.2
firepower 2110 /firmware # scope auto-install
firepower 2110 /firmware/auto-install # install security-pack version 9.8.2
The system is currently installed with security software package not set, which has:

   - The platform version: not set
If you proceed with the upgrade 9.8.2, it will do the following:
   - upgrade to the new platform version 2.2.2.52
   - install with CSP asa version 9.8.2
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   If you proceed the system will be re-imaged. All existing configuration will be
lost,
   and the default configuration applied.
Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.2
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
```

例：

Cisco Secure Firewall 3100 デバイス

```
firepower 3110 /firmware # show package
Name                                          Package-Vers
--------------------------------------------- -------------
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar 7.3.0-14
firepower 3110 /firmware # scope auto-install
firepower 3110 /firmware/auto-install # install security-pack version 9.19.0
```

```
The system is currently installed with security software package not set, which has:

   - The platform version: not set
If you proceed with the upgrade 9.19.2, it will do the following:
   - upgrade to the new platform version 7.0.3-14
   - install with CSP asa version 9.19.2
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   If you proceed the system will be re-imaged. All existing configuration will be
lost,
   and the default configuration applied.
Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.19.0
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
```

ステップ 6 シャーシのリブートが完了するのを待ちます（5 ～ 10 分）。

FXOS が起動しても、ASA が稼働するまで（5 分）待機する必要があります。次のメッセージが表示されるまで待機します。

Firepower 1000 および 2100 デバイス

```
firepower-2110#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
...
```

Cisco Secure Firewall 3100 デバイス

```
firepower-3110#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.19.0.0__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.19.0.0 ...
Verifying signature for cisco-asa.9.19.0.0 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.19.0.0__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
...
```

完全な再イメージ化の実行

この手順では、システム全体を再フォーマットし、イメージを消去して、工場出荷時のデフォルト設定に戻します。この手順を実行する場合は、実行後に新しいソフトウェアイメージをダウンロードして、システムを再設定する必要があります。

（注） この手順を実行すると、管理者パスワードが **Admin123** にリセットされます。

（注） FXOS イメージのダウングレードはサポートされていません。シスコがサポートする唯一の FXOS のイメージバージョンのダウングレード方法は、デバイスの完全な再イメージ化を実行することです。デバイスの再イメージ化の影響は次のとおりです。

- 既存のデバイスの構成が失われます。
- 新しいバージョンですべての ASA ソフトウェア利用資格を設定する必要があります。
- Backup and Restore はサポートされていません。

始める前に

- クラウドテナントからデバイスを登録解除します（該当する場合）。クラウドからの登録解除 （25 ページ） を参照してください。
- FXOS CLI コンテキストに接続されていることを確認します。シリアルコンソールを介して Firepower 1000/2100 または Cisco Secure Firewall 3100 デバイスに接続すると、FXOS CLI コンテキストに自動的に接続されます。Threat Defense CLI コンテキストに接続されている場合は、まず **connect fxos** コマンドを使用して FXOS CLI コンテキストに切り替える必要があります。
- Cisco Secure Firewall 3100 デバイスを Threat Defense バージョン 7.3.0 に再イメージ化するには、ROMMON バージョン 1.1.08 以降が必要です。現在の ROMMON バージョンが 1.1.08 未満の場合は、ASA 9.19 以降にアップグレードして ROMMON をアップグレードする必要があります。Management Center または Device Manager を使用して、Threat Defense のバージョンを 7.3.0 にアップグレードすることもできます（詳細については、Threat Defense を参照してください）。
- Threat Defense ソフトウェアを入手します。

（注） Cisco.com のログインおよびシスコ サービス契約が必要です。

表 *1 : Threat Defense* のソフトウェア

Threat Defense モデル	ダウンロードの場所	パッケージ
Firepower 1000 シリーズ	参照先：https://www.cisco.com/go/ftd-software	
	Threat Defense package 使用しているモデル > [Firepower Threat Defense Software] > バージョンの順に選択します。	パッケージには、次のようなファイル名が付けられています：cisco-ftd-fp1k.6.4.0.**SPA**。
Firepower 2100 シリーズ	参照先：https://www.cisco.com/go/ftd-software	
	Threat Defense package 使用しているモデル > [Firepower Threat Defense Software] > バージョンの順に選択します。	パッケージには、次のようなファイル名が付けられています：cisco-ftd-fp2k.6.2.2.**SPA**。
Secure Firewall 3100 シリーズ	参照先：https://www.cisco.com/go/ftd-software	
	Threat Defense package 使用しているモデル > [Firepower Threat Defense Software] > バージョンの順に選択します。	• 7.3 以降：パッケージには Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-01.sh.REL.**tar** のようなファイル名が付いています。 • 7.2：パッケージには cisco-ftd-fp3k.7.1.0 のようなファイル名が付いています。**SPA**。
Threat Defense package 使用しているモデル > [Firepower Threat Defense Software] > バージョンの順に選択します。	パッケージには、Cisco_Secure_FW_TD_4200-7.4.0-01.sh.REL.**tar** のようなファイル名がついています。	

手順

ステップ 1 FXOS CLI でローカル管理に接続します。

firepower # **connect local-mgmt admin**

ステップ 2 システムをフォーマットします。

firepower(local-mgmt) # **format everything**

例：

```
firepower(local-mgmt)# format
  emmc        eMMC Flash Device
  everything  Format All storage devices
  ssd1        Primary SSD Disk
  ssd2        Secondary SSD Disk
```

```
firepower(local-mgmt)# format everything
All configuration and bootable images will be lost.
Do you still want to format? (yes/no):yes
```

ステップ 3 次のようなプロンプトが表示されたら、ESC キーを押してブートを中断します。

例：

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

ステップ 4 システムが再起動し、ROMMON プロンプトで停止します。

（注） 最初にゲートウェイの IP で ARP が試行されます。デバイスを TFTP サーバーに直接接続する場合は、ゲートウェイの IP とサーバーの IP を同じ IP に設定する必要があります。

次のようにパラメータを入力します。

rommon 2 > **ADDRESS=** *address*

rommon 3 > **NETMASK=** *netmask*

rommon 4 > **GATEWAY=** *gateway*

rommon 5 > **SERVER=** *server*

rommon 6 > **IMAGE=** *image*

（注） Threat Defense または ASA バンドルをインストールするには、tftpdnld -b コマンドを使用します。

ステップ 5 次のように設定します。

rommon 7 > **set**

ステップ 6 新しい設定を同期させます。

rommon 8 > **sync**

ステップ 7 ROMMON から TFTP/FTP/SCP サーバの IP への ICMP 接続をテストします。

rommon 9 > **ping** *server IP*

（注） TFTP/FTP/SCP サーバの IP から管理 IP への ping は失敗します。これは想定されている動作です。

ステップ 8 Threat Defense ソフトウェアイメージを起動します。

tftp -b

（注） システムが再起動すると、次のエラーが表示されることがあります。

```
firepower-2110 : <<%%FPRM-2-DEFAULT_INFRA_VERSION_MISSING>>
[F1309][critical][default-infra-version-missing][org-root/fw-infra-pack-default]
Bundle version in firmware package is empty, need to re-install

firepower-3105 FPRM: <<%FPRM-2-DEFAULT_INFRA_VERSION_MISSING>>
[F1309][critical][default-infra-version-missing][org-root/fw-infra-pack-default]

Bundle version in firmware package is empty, need to re-install
```

このエラー状態は、この手順で後述するように、新しい Threat Defense ソフトウェアパッケージバージョンをインストールするとすぐに解消されます。

ステップ 9 システムが起動したら、admin/Admin123 としてログインし、管理 IP アドレスを再設定します。

a) ファブリック インターコネクトのスコープを入力します。

firepower#/ **scope fabric-interconnect a**

b) 新しい管理 IP 情報を設定します。

firepower /fabric-interconnect # **set out-of-band static ip** *ip* **netmask** *netmask* **gw** *gateway*

c) 設定をコミットします。

commit-buffer

（注） 次のエラーが発生する場合は、変更をコミットする前に DHCP を無効にする必要があります。DHCP を無効にするには、次の手順に従います。

```
firepower /fabric-interconnect* # commit-buffer
Error: Update failed: [Management ipv4 address (IP <ip> / net mask <netmask> ) is not
in the same network of current DHCP server IP range <ip - ip>. Either disable DHCP server
 first or config with a different ipv4 address.]
```

a) firepower /fabric-interconnect # **exit**
b) firepower # **scope system**
c) firepower #/system **scope services**
d) firepower #/system/services **disable dhcp-server**
e) firepower #/system/services **commit-buffer**
f) DHCP サーバが無効になったら、戻って新しい管理 IP を設定できます。

ステップ 10 新しい Threat Defense アプリケーション ソフトウェア パッケージをダウンロードします。USB ドライブを使用してソフトウェアパッケージをダウンロードする場合は、次の構文を使用します。

firepower # **scope firmware**

firepower /firmware # **download image** usbA:*image_name*

次に例を示します。

firepower /firmware # **download image** usbA:cisco-ftd-fp2k.6.2.1-36.SPA

FTP、SCP、SFTP、TFTP を使用して、Threat Defense ソフトウェアパッケージをデバイスにコピーすることもできます。

firepower /firmware # **download image** *tftp/ftp/scp/sftp***://***path to the image, including the server root /image name*

Firepower 1000 および 2100 デバイスの例を示します。

```
firepower /firmware # download image tftp://example.cisco.com/fxos-2k.6.2.1-36.SPA
```

Cisco Secure Firewall 3100 デバイスの例を示します。

```
firepower /firmware # download image scp://172.23.205.217/auto/Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar
```

（注） システムはダウンロードイメージ要求で指定されたファイル名の前にスラッシュを付加するので、FTP/TFTP/SCP/SFTP によりファイル転送を実行する場合は、サーバのルートを含むイメージの絶対パスを入力する必要があります。

必要に応じて、IP アドレスの代わりに FQDN を使用できます。

ステップ 11 コマンド出力に自動的に表示されるダウンロードの進行状況あるいは、**download-task** コマンドを入力して、状態がダウンロード済みであることを確認します。

firepower /firmware # **show download-task**

例：

```
firepower-3110 /firmware # show download task
File Name     Protocol     Server         Port     Userid     State
---------     --------     ------         ----     ------     -----
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar
              Scp         172.23.205.217     0               Downloaded
```

ステップ 12 ダウンロードしたパッケージのバージョンを表示します。

firepower /firmware # **show package**

例：

```
firepower /firmware # show package
Name                                          Package-Vers
--------------------------------------------- ------------
cisco-ftd-fp2k.6.2.1-1314.SPA                 6.2.1-1314
```

```
firepower-3110 /firmware # show package
Name                                              Package-Vers
------------------------------------------------  ---------------
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar     7.3.0-14
```

ステップ 13 自動インストールのスコープを入力します。

firepower /firmware # **scope auto-install**

ステップ 14 新しいソフトウェアアプリケーションパッケージをインストールします（バージョンは、**show package** コマンドのバージョン出力です）。

firepower /firmware/auto-install # **install security-pack version** *version* **force**

ステップ 15 ソフトウェアパッケージをインストールしたら、ハードウェア プラットフォームのスタートアップガイドにある設定手順を続行します。

管理者パスワードの変更

デバイスを再イメージ化すると、管理者パスワードが Admin123 にリセットされます。初回ログイン時にパスワードを変更するように求められます。パスワードを後で変更する場合、この Threat Defense CLI の手順を使用して管理者パスワードを新しい文字列に変更します。

手順

ステップ 1 Threat Defense アプリケーションの CLI に接続します。

firepower-chassis # **connect ftd**

ステップ 2 **users** テーブルに admin ユーザアカウントがあることを確認します。

> **show user**

例：

```
> show user
Login UID Auth Access Enabled Reset Exp Warn Str Lock Max
admin 100 Local Config Enabled No Never N/A Dis No 0
```

ステップ 3 admin ユーザアカウントの新しいパスワードを設定します。

firepower-chassis # **configure user password admin**

例：

```
> configure user password admin
Enter current password:
Enter new password for user admin:
Confirm new password for user admin:
```

Threat Defense がオフラインの場合の管理者パスワードの変更

デバイスを再イメージ化すると、管理者パスワードが Admin123 にリセットされます。初回ログイン時にパスワードを変更するように求められます。パスワードを後で変更する場合、Threat Defense がオフラインなどの理由で使用できないときは、この手順を使用して管理者パスワードを新しい文字列に変更します。Threat Defense がオンラインの場合は、Threat Defense CLI を使用して管理者パスワードを変更する必要があります（管理者パスワードの変更 （23 ページ）を参照）。

（注） FXOS CLI を使用して管理者パスワードを変更する手順は、現在実行している Threat Defense のバージョンによって異なります。

始める前に

- FXOS CLI コンテキストに接続されていることを確認します。シリアルコンソールを介して Firepower 1000/2100 または Cisco Secure Firewall 3100 デバイスに接続すると、FXOS CLI コンテキストに自動的に接続されます。Threat Defense CLI コンテキストに接続されている場合は、まず **connect fxos** コマンドを使用して FXOS CLI コンテキストに切り替える必要があります。

手順

ステップ 1 FXOS CLI で、セキュリテのスコープを入力します。

firepower # **scope security**

ステップ 2 （Firepowerバージョン6.4以降）新しいパスワードを設定するには、古い管理者パスワードを再認証する必要があります。

firepower /security* # **set password**

例：

```
FPR-2120# scope security
FPR-2120# /security # set password
Enter old password:
Enter new password:
Confirm new password:
firepower-2120 /security* # commit-buffer
```

（Firepowerバージョン6.3以前）現在のローカルユーザのリストを表示します。デバイスを再イメージ化したばかりの場合は、このリストに表示されるユーザは admin のみになります。

firepower /security # **show local-user**

例：

```
FPR-2120# scope security
FPR-2120 /security # show local-user
User Name       First Name      Last name
--------------- --------------- ---------
admin
```

a) （Firepower バージョン 6.3 以前）admin ローカルユーザのスコープを入力します。

firepower /security # **enter local-user admin**

b) （Firepower バージョン 6.3 以前）ユーザ admin の新しいパスワードを設定します。

firepower /security/local-user # **set password**

例：

```
FPR-2100 /security # enter local-user admin
FPR-2100 /security/local-user # set password
Enter a password: cisco
Confirm the password: cisco
```

ステップ 3 設定をコミットします。

firepower /security/local-user* # **commit-buffer**

クラウドからの登録解除

Firepower 1000/2100 または Cisco Secure Firewall 3100 デバイスを新しい目的（社内の新しいグループに転送する場合、またはサードパーティベンダーからデバイスを購入した場合など）のために、再イメージ化または工場出荷時の状態にリセットする際は、クラウドのテナントからデバイスの登録解除が必要になることがあります。

デバイスが登録されたクラウド（CDO）アカウントにアクセスできる場合は、そのアカウントにログインして Firepower 1000/2100 または Cisco Secure Firewall 3100 デバイスを削除します。

クラウドアカウントにアクセスできない場合は、次の手順で FXOS CLI を使用してクラウドテナントから Firepower 1000/2100 または Cisco Secure Firewall 3100 デバイスの登録を解除します。

始める前に

- FXOS CLI コンテキストに接続されていることを確認します。シリアルコンソールを介して Firepower 1000/2100 または Cisco Secure Firewall 3100 デバイスに接続すると、FXOS CLI コンテキストに自動的に接続されます。Threat Defense CLI コンテキストに接続されている場合は、まず **connect fxos** コマンドを使用して FXOS CLI コンテキストに切り替える必要があります。
- デバイスがクラウドにアクセスできるかどうかを確認します。

```
firepower # scope fabric a
firepower /fabric-interconnect # show detail
```

`show detail` の出力に管理 IP アドレスが表示されない場合は、まずデバイスの管理 IP を設定する必要があります

1. ファブリック インターコネクト スコープを開始します。

   firepower # **scope fabric-interconnect**

2. 新しい管理 IP 情報を設定します。

   firepower /fabric-interconnect # **set out-of-band static ip** *ip* **netmask** *netmask* **gateway** *gateway*

3. 設定をコミットします。

   firepower /fabric-interconnect # **commit buffer**

手順

ステップ 1 ローカル管理コマンドシェルに接続します。

firepower # **connect local**

ステップ 2 クラウドからデバイスを登録解除します。

firepower(local-mgmt)# **cloud deregister**

例

```
firepower # connect local
firepower(local-mgmt) # cloud deregister
```

Firepower 1000/2100 および Cisco Secure Firewall 3100 FXOS トラブルシューティングの履歴

機能名	プラットフォームリリース	説明
スイッチパケットパス	Firepower 7.1	`portmanager` FXOS CLI コマンドを使用して、スイッチパケットパスの問題について Cisco Secure Firewall 3100 デバイスをトラブルシューティングできるようになりました。
クラウドの登録解除	Firepower 6.7	`cloud deregister` FXOS CLI コマンドを使用して、クラウドテナントから Firepower 1000/2100 デバイスの登録を解除できるようになりました。
管理者パスワードの変更	Firepower 6.4	Firepower バージョン 6.4 以降の Firepower 1000/2100 デバイスでは、新しい管理者パスワードを設定する前に古い管理者パスワードを再認証する必要があります。

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。