



イメージ管理

- [イメージ管理について \(1 ページ\)](#)
- [Cisco.com からのイメージのダウンロード \(2 ページ\)](#)
- [Firepower 4100/9300 シャーシへの FXOS のソフトウェア イメージのダウンロード \(2 ページ\)](#)
- [イメージの整合性の確認 \(4 ページ\)](#)
- [FXOS プラットフォーム バンドルのアップグレード \(5 ページ\)](#)
- [Firepower 4100/9300 シャーシへの論理デバイスのソフトウェア イメージのダウンロード \(6 ページ\)](#)
- [論理デバイスのイメージバージョンの更新 \(9 ページ\)](#)
- [ファームウェア アップグレード \(11 ページ\)](#)
- [バージョン 2.0.1 以下への手動ダウングレード \(11 ページ\)](#)

イメージ管理について

Firepower 4100/9300 シャーシ では 2 つの基本タイプのイメージを使用します。



(注) すべてのイメージにデジタル署名が行われ、セキュアブートによって検証されます。どのような場合も、イメージを変更しないでください。変更すると、検証エラーになります。

- **プラットフォームバンドル**：プラットフォームバンドルは、**Supervisor** およびセキュリティ モジュール/エンジン で動作する、複数の独立したイメージの集まりです。プラットフォームバンドルは、FXOS のソフトウェア パッケージです。
- **アプリケーション**：アプリケーションイメージは、Firepower 4100/9300 シャーシのセキュリティ モジュール/エンジンに導入するソフトウェア イメージです。アプリケーションイメージは、Cisco Secure Package ファイル (CSP) として提供されます。これは、論理デバイス作成時にセキュリティ モジュール/エンジンに展開されるまで（または以降の論理デバイス作成に備えて）スーパーバイザに保存されます。同じアプリケーション イメージタイプの複数の異なるバージョンをスーパーバイザに保存できます。



(注) プラットフォームバンドルイメージと1つ以上のアプリケーションイメージの両方をアップグレードする場合、まずプラットフォームバンドルをアップグレードする必要があります。



(注) デバイスに ASA アプリケーションをインストールする場合は、既存のアプリケーション脅威に対する防御のイメージを削除できます。その逆も同様です。すべての脅威に対する防御イメージを削除しようとする、少なくとも1つのイメージの削除が拒否され、「Invalid operation as no default 脅威に対する防御 /ASA APP will be left. Please select a new default 脅威に対する防御 app」というエラーメッセージが表示されます。すべての脅威に対する防御イメージを削除するには、デフォルトイメージだけを残して、その他のイメージを削除し、最後にデフォルトイメージを削除する必要があります。

Cisco.com からのイメージのダウンロード

FXOS およびアプリケーションイメージをシャーシにアップロードできるように Cisco.com からダウンロードします。

始める前に

Cisco.com アカウントが必要です。

手順

- ステップ1 Web ブラウザを使用して、<http://www.cisco.com/go/firepower9300-software> または <http://www.cisco.com/go/firepower4100-software> にアクセスします。Firepower 4100/9300 シャーシのソフトウェアダウンロードページがブラウザに表示されます。
- ステップ2 該当するソフトウェアイメージを見つけて、ローカルコンピュータにダウンロードします。

Firepower 4100/9300 シャーシへの FXOS のソフトウェアイメージのダウンロード

FTP、HTTP/HTTPS、SCP、SFTP、または TFTP を使用して、FXOS のソフトウェアイメージを Firepower 4100/9300 シャーシにコピーできます。

始める前に

コンフィギュレーションファイルのインポートに必要な次の情報を収集します。

- イメージのコピー元のサーバの IP アドレスおよび認証クレデンシャル
- FXOS イメージ ファイルの完全修飾名



(注) FXOS 2.8.1 以降では、ファームウェアおよびアプリケーションイメージのダウンロード用に HTTP/HTTPS がサポートされています。

手順

ステップ 1 ファームウェア モードを開始します。

```
Firepower-chassis # scope firmware
```

ステップ 2 FXOS ソフトウェア イメージをダウンロードします。

```
Firepower-chassis /firmware # download image URL
```

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp://username@hostname/path/image_name**
- **http://username@hostname/path/image_name**
- **https://username@hostname/path/image_name**
- **scp://username@hostname/path/image_name**
- **sftp://username@hostname/path/image_name**
- **ftpt://hostname:port-num/path/image_name**
- **usbA://hostname:port-num/path/image_name**

ステップ 3 ダウンロード プロセスをモニタする場合 :

```
Firepower-chassis /firmware # show package image_name detail
```

例

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.1.1.1.119.SPA
Firepower-chassis /firmware # show package fxos-k9.1.1.1.119.SPA detail
Download task:
  File Name: fxos-k9.1.1.1.119.SPA
  Protocol: scp
  Server: 192.168.1.1
  Userid:
  Path:
```

```
Downloaded Image Size (KB): 5120
State: Downloading
Current Task: downloading image fxos-k9.1.1.1.119.SPA from
192.168.1.1 (FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

次の例では、HTTP/HTTPS プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
https://user@192.168.1.1/images/fxos-k9.1.1.1.119.SPA
Firepower-chassis /firmware # show download task
```

```
Download task:
File Name      Protocol  Server  Port  Userid State
-----
fxos-k9.1.1.1.119.SPA
      Hhttps 192.168.1.1 0    Downloaded
fxos-k9.1.1.1.119.SPA
      Hhttp  sjc-ssp-artifac      0    Downloaded
```

```
-----
Firepower-chassis /firmware # show package fxos-k9.1.1.1.119.SPA detail
Download task:
File Name: fxos-k9.1.1.1.119.SPA
Protocol: https
Server: 192.168.1.1
Userid:
Path:
Downloaded Image Size (KB): 5120
State: Downloading
Current Task: downloading image fxos-k9.1.1.1.119.SPA from
192.168.1.1 (FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

イメージの整合性の確認

イメージの整合性は、新しいイメージが Firepower 4100/9300 シャーシに追加されると自動的に確認されます。必要な場合に、手動でイメージの整合性を確認するには、次の手順を実行できます。

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 ファームウェア モードを開始します。

```
Firepower-chassis# scope firmware
```

ステップ 3 イメージをリストします。

```
Firepower-chassis /firmware # show package
```

ステップ 4 イメージを確認します。

```
Firepower-chassis /firmware # verify platform-pack version version_number
```

`version_number` は、確認する FXOS プラットフォームバンドルのバージョン番号です（たとえば、1.1(2.51)）。

ステップ 5 確認には数分かかる可能性があることがシステムにより警告されます。

`yes` を入力して、検証に進むことを確認します。

ステップ 6 イメージ確認のステータスを確認するには、次の手順を実行します。

```
Firepower-chassis /firmware # show validate-task
```

FXOS プラットフォームバンドルのアップグレード

始める前に

プラットフォームバンドルのソフトウェアイメージを [Cisco.com](#) からダウンロードして（[Cisco.com](#) からのイメージのダウンロード（2 ページ）を参照）、そのイメージを Firepower 4100/9300 シャーシにダウンロードします（[Firepower 4100/9300 シャーシへの論理デバイスのソフトウェアイメージのダウンロード（6 ページ）](#)を参照）。



(注) アップグレードプロセスには通常 20 ～ 30 分かかります。

スタンドアロン論理デバイスを実行中の Firepower 9300 または 4100 シリーズセキュリティアプライアンスをアップグレードしている場合、またはシャーシ内クラスタを実行中の Firepower 9300 セキュリティアプライアンスをアップグレードしている場合、アップグレード中にはトラフィックがデバイスを通りません。

シャーシ間クラスタに属する Firepower 9300 または 4100 シリーズセキュリティアプライアンスをアップグレードしている場合、アップグレード中には、アップグレード対象のデバイスをトラフィックが通過しません。ただし、クラスタ内の他のデバイスではトラフィックは通過し続けます。

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 ファームウェア モードを開始します。

```
Firepower-chassis# scope firmware
```

ステップ 3 auto-install モードにします。

```
Firepower-chassis /firmware # scope auto-install
```

ステップ 4 FXOS プラットフォームバンドルをインストールします。

Firepower-chassis /firmware/auto-install # **install platform platform-vers version_number**

version_number は、インストールする FXOS プラットフォームバンドルのバージョン番号です (たとえば、1.1(2.51))。

ステップ 5 システムは、まずインストールするソフトウェアパッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォームソフトウェアパッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリポートする必要があることが警告されます。

yes を入力して、検証に進むことを確認します。

ステップ 6 インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

FXOS がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 7 アップグレードプロセスをモニタするには、次の手順を実行します。

- a) **scope firmware** を入力します。
- b) **scope auto-install** を入力します。
- c) **show fsm status expand** を入力します。

Firepower 4100/9300 シャーシへの論理デバイスのソフトウェアイメージのダウンロード

FTP、HTTP/HTTPS、SCP、SFTP、または TFTP を使用して、論理デバイスのソフトウェアイメージを Firepower 4100/9300 シャーシにコピーできます。

始める前に

コンフィギュレーションファイルのインポートに必要な次の情報を収集します。

- イメージのコピー元のサーバの IP アドレスおよび認証クレデンシャル
- ソフトウェアイメージファイルの完全修飾名



(注) FXOS 2.8.1 以降のバージョンでは、ファームウェアおよびアプリケーションイメージのダウンロード用に HTTP/HTTPS プロトコルがサポートされています。

手順

ステップ 1 セキュリティ サービス モードを開始します。

```
Firepower-chassis # scope ssa
```

ステップ 2 アプリケーション ソフトウェア モードに入ります。

```
Firepower-chassis /ssa # scope app-software
```

ステップ 3 論理デバイスのソフトウェア イメージをダウンロードします。

```
Firepower-chassis /ssa/app-software # download image URL
```

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- `ftp://username@hostname/path`
- `http://username@hostname/path`
- `https://username@hostname/path`
- `scp://username@hostname/path`
- `sftp://username@hostname/path`
- `tftp://hostname:port-num/path`

(注) イメージのインストールに `tftpdnld` を使用しないでください。エラーがスローされます。

ステップ 4 ダウンロードプロセスをモニタする場合：

```
Firepower-chassis /ssa/app-software # show download-task
```

ステップ 5 ダウンロードアプリケーションを表示するには、次のコマンドを使用します。

```
Firepower-chassis /ssa/app-software # up
```

```
Firepower-chassis /ssa # show app
```

ステップ 6 特定のアプリケーションの詳細情報を表示するには、次のコマンドを使用します。

```
Firepower-chassis /ssa # scope app application_type image_version
```

```
Firepower-chassis /ssa/app # show expand
```

例

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task
```

Downloads for Application Software:

File Name	Protocol	Server	Userid	State
-----------	----------	--------	--------	-------

```

-----
cisco-asa.9.4.1.65.csp      Scp      192.168.1.1      user
Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
Name          Version      Description Author      Deploy Type CSP Type      Is Default App
-----
asa           9.4.1.41     N/A
asa           9.4.1.65     N/A
Native        Application No
Native        Application Yes

Firepower-chassis /ssa # scope app asa 9.4.1.65
Firepower-chassis /ssa/app # show expand

Application:
Name: asa
Version: 9.4.1.65
Description: N/A
Author:
Deploy Type: Native
CSP Type: Application
Is Default App: Yes

App Attribute Key for the Application:
App Attribute Key Description
-----
cluster-role      This is the role of the blade in the cluster
mgmt-ip           This is the IP for the management interface
mgmt-url          This is the management URL for this application

Net Mgmt Bootstrap Key for the Application:
Bootstrap Key Key Data Type Is the Key Secret Description
-----
PASSWORD         String          Yes              The admin user password.

Port Requirement for the Application:
Port Type: Data
Max Ports: 120
Min Ports: 1

Port Type: Mgmt
Max Ports: 1
Min Ports: 1

Mgmt Port Sub Type for the Application:
Management Sub Type
-----
Default

Port Type: Cluster
Max Ports: 1
Min Ports: 0
Firepower-chassis /ssa/app #

```

論理デバイスのイメージバージョンの更新

この手順を使用して、新しいバージョンに ASA アプリケーションイメージをアップグレードするか、脅威に対する防御 アプリケーションイメージをディザスタリカバリ シナリオで使用される新しいスタートアップバージョンに設定します。

シャーシマネージャまたは FXOS CLI を使用して 脅威に対する防御 論理デバイスでスタートアップバージョンを変更しても、アプリケーションはすぐに新しいバージョンにアップグレードされません。論理デバイス スタートアップバージョンは、脅威に対する防御 がディザスタリカバリ シナリオで再インストールされるバージョンです。脅威に対する防御 論理デバイスの初期作成後には、脅威に対する防御 論理デバイスを、シャーシマネージャまたは FXOS CLI を使用してアップグレードすることはありません。脅威に対する防御 論理デバイスをアップグレードするには、Management Center を使用する必要があります。詳細については、次のサイトにあるシステムリリースノートを参照してください。 <http://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html>

さらに、脅威に対する防御 論理デバイスへの更新は、シャーシマネージャの [論理デバイス (Logical Devices)] > [編集 (Edit)] ページおよび [システム (System)] > [更新 (Updates)] ページには反映されないことに注意してください。これらのページで、表示されるバージョンは、脅威に対する防御 論理デバイスを作成するために使用されたソフトウェアバージョン (CSP イメージ) を示します。



- (注) 脅威に対する防御 のスタートアップバージョンを設定すると、アプリケーションのスタートアップバージョンが更新されます。したがって、アプリケーションを手動で再インストールするか、ブレードを再初期化して、選択したバージョンを適用する必要があります。この手順は、脅威に対する防御 ソフトウェアのアップグレードまたはダウングレードとは異なり、完全な再インストール (再イメージ化) です。そのため、アプリケーションが削除され、既存の設定が失われます。

ASA 論理デバイスでスタートアップバージョンを変更すると、ASA はこのバージョンにアップグレードされ、すべての設定が復元されます。設定に応じて ASA スタートアップバージョンを変更するには、次のワークフローを使用します。



- (注) ASA のスタートアップバージョンを設定すると、アプリケーションが自動的に再起動されます。この手順は、ASA ソフトウェアのアップグレードまたはダウングレードと同様です (既存の設定は保持されます)。

ASA ハイ アベイラビリティ :

1. スタンバイ ユニットで論理デバイス イメージバージョンを変更します。
2. スタンバイ ユニートをアクティブにします。
3. 他のユニットでアプリケーションバージョンを変更します。

ASA シャーシ間クラスタ :

1. データユニットでスタートアップバージョンを変更します。
2. データユニットを制御ユニットにします。
3. 元の制御ユニット（ここではデータユニット）でスタートアップバージョンを変更します。

始める前に

論理デバイスに使用するアプリケーション イメージを [Cisco.com](#) からダウンロードして ([Cisco.com からのイメージのダウンロード \(2 ページ\)](#) を参照)、そのイメージを Firepower 4100/9300 シャーシにダウンロードします ([Firepower 4100/9300 シャーシ への論理デバイスのソフトウェア イメージのダウンロード \(6 ページ\)](#) を参照)。

プラットフォーム バンドル イメージと 1 つ以上のアプリケーション イメージの両方をアップグレードする場合、まずプラットフォーム バンドルをアップグレードする必要があります。

手順

ステップ 1 セキュリティ サービス モードを開始します。

```
Firepower-chassis # scope ssa
```

ステップ 2 スコープを更新するセキュリティ モジュールに設定します。

```
Firepower-chassis /ssa # scope slot slot_number
```

ステップ 3 スコープを更新するアプリケーションに設定します。

```
Firepower-chassis /ssa/slot # scope app-instance app_template
```

ステップ 4 スタートアップ バージョンを設定します。

```
Firepower-chassis /ssa/slot/app-instance # set startup-version version_number
```

脅威に対する防御 論理デバイスでアプリケーション スタートアップ バージョンを設定すると、次の警告メッセージが表示されます。

```
13254 : 警告 : 脅威に対する防御 ではFXOSアップグレードはサポートされていません。指定されたバージョンは、脅威に対する防御 の再インストールが必要な場合にのみ使用されます。
```

例 :

```
firepower /ssa/slot/app-instance # set startup-version 6.2.2.81
13254: Warning: FXOS upgrades are not supported for ftd. The specified version will be used only if ftd needs to be reinstalled.
```

ステップ 5 設定を確定します。

```
commit-buffer
```

トランザクションをシステム設定にコミットします。アプリケーションイメージが更新され、アプリケーションが再起動します。

例

次に、セキュリティモジュール1で実行しているASAのソフトウェアイメージを更新する例を示します。**show**コマンドを使用すると、更新ステータスを表示できます。

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # scope slot 1
Firepower-chassis /ssa/slot # scope app-instance asa
Firepower-chassis /ssa/slot/app-instance # set startup-version 9.4.1.65
Firepower-chassis /ssa/slot/app-instance* # show configuration pending
  enter app-instance asa
+   set startup-version 9.4.1.65
  exit
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance # show
```

Application Instance:

Application Name	Admin State	Operational State	Running Version	Startup Version
asa	Enabled	Updating	9.4.1.41	9.4.1.65

```
Firepower-chassis /ssa/slot/app-instance #
Firepower-chassis /ssa/slot/app-instance # show
```

Application Instance:

Application Name	Admin State	Operational State	Running Version	Startup Version
asa	Enabled	Online	9.4.1.65	9.4.1.65

```
Firepower-chassis /ssa/slot/app-instance #
```

ファームウェアアップグレード

Firepower4100/9300 シャーシでファームウェアをアップグレードする方法については、『[Cisco Firepower 4100/9300 FXOS ファームウェアアップグレードガイド](#)』を参照してください。

バージョン 2.0.1 以下への手動ダウングレード

セキュリティモジュールにCIMCイメージを手動でダウングレードするには、次のCLI手順に従います。



- (注) この手順は、バージョン 2.1.1 以降からバージョン 2.0.1 以前にダウングレードする際に使用します。

始める前に

ダウングレード対象のアプリケーションイメージが Firepower 4100/9300 シャーシにダウンロードされていることを確認します（「[Cisco.com からのイメージのダウンロード \(2 ページ\)](#)」および「[Firepower 4100/9300 シャーシへの論理デバイスのソフトウェアイメージのダウンロード \(6 ページ\)](#)」を参照）。

手順

ステップ 1 CIMC イメージをダウングレードする前に、イメージバージョンの比較を無効にします。

デフォルトのプラットフォーム イメージバージョンを消去するには、次の例の手順に従います。

例：

```
firepower# scope org
firepower /org # scope fw-platform-pack default
firepower /org/fw-platform-pack # set platform-bundle-version ""
Warning: Set platform version to empty will result software/firmware incompatibility issue.
firepower /org/fw-platform-pack* # commit-buffer
firepower /org/fw-platform-pack #
```

ステップ 2 モジュールイメージをダウングレードします。

CIMC イメージを変更するには、次の例の手順に従います。

例：

```
firepower# scope server 1/1
firepower /chassis/server # scope cimc
firepower /chassis/server/cimc # update firmware <version_num>
firepower /chassis/server/cimc* # activate firmware <version_num>
firepower /chassis/server/cimc* # commit-buffer
firepower /chassis/server/cimc #
```

他のモジュールを更新するには、必要に応じてこの手順を繰り返します。

ステップ 3 新しいファームウェアバンドルをインストールします。

ダウングレードイメージをインストールするには、次の例の手順に従います。

例：

```
firepower# scope firmware
firepower /firmware # scope auto-install
firepower /firmware/auto-install # install platform platform-vers <version_num>
The currently installed FXOS platform software package is <version_num>

WARNING: If you proceed with the upgrade, the system will reboot.

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
```

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

次のタスク

firmware/auto-install モードで **show fsm status expand** コマンドを使用すると、インストールプロセスをモニタできます。

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。