



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 セキュリティ アプライアンスへのイメージのアップロード](#) (2 ページ)
- [イメージの整合性の確認](#) (3 ページ)
- [Firepower eXtensible Operating System プラットフォーム バンドルのアップグレード](#) (3 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](#) (4 ページ)
- [論理デバイスのイメージバージョンの更新](#) (7 ページ)
- [ファームウェア アップグレード](#) (8 ページ)
- [バージョン 2.0.1 以下への手動ダウングレード](#) (8 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** : Firepower プラットフォームバンドルは、Firepower Supervisor および Firepower 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、Firepower eXtensible Operating System 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 Firepower Supervisor 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。

Cisco.com からのイメージのダウンロード

Cisco.com から FXOS およびアプリケーションイメージをダウンロードし、Firepower シャーシにアップロードすることができます。

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 セキュリティ アプライアンスへのイメージのアップロード

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ます。

始める前に

アップロードするイメージがローカル コンピュータで使用可能であることを確認してください。

手順

- ステップ 1** [システム (System)] > [更新 (Updates)] を選択します。
[使用可能な更新 (Available Updates)] ページに、シャーシで使用可能な Firepower eXtensible Operating System プラットフォーム バンドルのイメージやアプリケーションのイメージのリストが表示されます。
- ステップ 2** [イメージのアップロード (Upload Image)] をクリックして、[イメージのアップロード (Upload Image)] ダイアログ ボックスを開きます。

- ステップ3** [ファイルを選択 (Choose File)] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
- ステップ4** [Upload] をクリックします。
選択したイメージが Firepower4100/9300 シャーシにアップロードされます。イメージがアップロードされている間、システムは経過表示バーを表示して、完了したアップロードの割合を示します。
- ステップ5** 特定のソフトウェア イメージについては、イメージをアップロードした後にエンドユーザーライセンス契約書が表示されます。システムのプロンプトに従ってエンドユーザー契約書に同意します。

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 Firepower4100/9300 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** [システム (System)] > [更新 (Updates)] を選択します。
[使用可能な更新 (Available Updates)] ページに、シャーシで使用可能な Firepower eXtensible Operating System プラットフォーム バンドルのイメージやアプリケーションのイメージのリストが表示されます。
- ステップ2** 確認するイメージの [確認 (Verify)] (チェックマーク アイコン) をクリックします。
システムはイメージの整合性を確認し、[イメージの整合性 (Image Integrity)] フィールドにステータスを表示します。

Firepower eXtensible Operating System 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 シャーシにアップロードします ([Firepower セキュリティ アプライアンスへのイメージのアップロード \(2 ページ\)](#) 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 Firepower 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しません。

シャーシ間クラスタに属する Firepower 9300 または Firepower 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 [システム (System)] > [更新 (Updates)] を選択します。

[使用可能な更新 (Available Updates)] ページに、シャーシで使用可能な Firepower eXtensible Operating System プラットフォームバンドルのイメージやアプリケーションのイメージのリストが表示されます。

ステップ 2 アップグレードする FXOS プラットフォームバンドルの [アップグレード (Upgrade)] をクリックします。

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ブートする必要があることが警告されます。

ステップ 3 インストールの続行を確定するには [はい (Yes)] を、インストールをキャンセルするには [いいえ (No)] をクリックします。

Firepower eXtensible Operating System 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。

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

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

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ヤル
- ソフトウェア イメージ ファイルの完全修飾名

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

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                               Native    Application No
  asa       9.4.1.65  N/A                               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、Firepower Threat Defense 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。

Firepower Chassis Manager または FXOS CLI を使用して Firepower Threat Defense 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、Firepower Threat Defense 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。FTD 論理デバイスの初期作成後には、FTD 論理デバイスを、Firepower Chassis Manager 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。FTD 論理デバイスをアップグレードするには、Firepower 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 FirePOWER システムのリリース 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、FTD 論理デバイスへの更新は、Firepower Chassis Manager 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、FTD 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。

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。

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 シャーシにアップロードします ([Firepower セキュリティ アプライアンスへのイメージのアップロード \(2 ページ\)](#) 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** [論理デバイス (Logical Devices)] を選択して、[論理デバイス (Logical Devices)] ページを開きます。
[論理デバイス (Logical Devices)] ページに、シャーシに設定されている論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが代わりに表示されます。
- ステップ2** 更新する論理デバイスの [Update Version] をクリックして、[Update Image Version] ダイアログボックスを開きます。
- ステップ3** [New Version] では、ソフトウェアバージョンを選択します。
- ステップ4** [OK] をクリックします。
-

ファームウェアアップグレード

Firepower 4100/9300 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 \(4 ページ\)](#)」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。

