



Firewall Threat Defense 3100、4100、4200、9300 のアップグレード

- [Secure Firewall 3100/4200 シャーシのアップグレード \(1 ページ\)](#)
- [Firewall Chassis Manager を使用した Firepower 4100/9300 上の FXOS のアップグレード \(5 ページ\)](#)
- [CLI を使用した Firepower 4100/9300 上の FXOS のアップグレード \(14 ページ\)](#)
- [Firepower 4100/9300 のファームウェアのアップグレード \(26 ページ\)](#)

Secure Firewall 3100/4200 シャーシのアップグレード

アップグレードウィザードを使用してのシャーシをアップグレードするには、次の手順を実行します。

マルチインスタンスモードの Cisco Secure Firewall 3100/4200：すべてのアップグレードでシャーシのアップグレードが必要になる可能性があります。シャーシとファイアウォールは個別にアップグレードしますが、1つのパッケージにシャーシとファイアウォールのアップグレードが含まれており、クラウド提供型 Firewall Management Center から両方のアップグレードを実行します。シャーシのみのアップグレードまたはファイアウォールのみのアップグレードが可能です。

続行すると、選択したシャーシに関する基本情報と、現在のアップグレード関連のステータスが表示されます。表示内容には、アップグレードできない理由が含まれます。

アップグレードウィザードから移動しても進行状況は保持されます。他のユーザーは、すでに選択されているシャーシの新しいアップグレードワークフローを開始できません。（例外：CACでログインしている場合、ログアウトしてから24時間後に進行状況がクリアされます）。ワークフローに戻るには、**[デバイス (Devices)] > [+さらに表示 (+ Show more)] > [アップグレード (Upgrade)] > [シャーシのアップグレード (Chassis Upgrade)]**を選択します。

アップグレードは、ウィザードを完了して**[アップグレードの開始 (Start Upgrade)]**をクリックするまで開始されません。アップグレードパッケージのコピーやアップグレードオプションの選択など、その時点までのすべての手順は、メンテナンスウィンドウ外で実行できます。



注意 アップグレード中は、設定の変更を展開しないでください。シャーシまたはそのデバイスが非アクティブに見えても、手動で再起動またはシャットダウンしないでください。進行中のアップグレードは再開しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。アップグレード中にシャーシが複数回再起動する場合があります。これは想定されている動作です。アップグレードに失敗した、シャーシまたはデバイスが応答しないなど、アップグレードで問題が発生した場合は、Cisco TAC にお問い合わせください。

始める前に

アップグレードの準備が整っていることを確認します。

- ターゲットバージョンを実行できるかどうかを確認します：[互換性](#)
- アップグレードパスを計画します：[アップグレードパス](#)
- アップグレードのガイドラインを確認します：[アップグレードのガイドライン](#)
- インフラストラクチャとネットワークを確認します：[インフラストラクチャとネットワークの確認](#)
- 設定、タスク、および展開全体の正常性を確認します：[設定と展開の確認](#)
- バックアップを実行します：[バックアップ](#)

手順

- ステップ 1** クラウド提供型 Firewall Management Center で、**[管理 (Administration)] > [アップグレードと更新 (Upgrades & updates)] > [製品アップグレード (Product Upgrades)]** を選択します。
- [製品のアップグレード (Product Upgrades)] ページには、アップグレードを中心とした展開の概要（デバイスの数、それらが最後にアップグレードされた日時、進行中のアップグレードの有無など）が表示されます。利用可能なアップグレードが一覧表示されます（推奨リリースには特別なマークが付いています）。
- ステップ 2** （オプション）アップグレードパッケージを取得してクラウド提供型 Firewall Management Center に配置するか、内部サーバーに配置します。
- デバイスがインターネットから直接アップグレードパッケージを取得できる場合は、この手順をスキップします。他のオプションについては、[クラウド提供型 Firewall Management Center によるアップグレードパッケージの管理](#) を参照してください。
- ステップ 3** アップグレードウィザードを起動します。
- ターゲットバージョンの横にある **[アップグレード (Upgrade)]** をクリックします。ドロップダウンメニューが表示されたら、**[シャーシ (Chassis)]** を選択します。
- ステップ 4** アップグレードするシャーシを選択します。

アップグレードするシャーシを選択しやすくするために、アップグレードウィザードでは、さまざまな便利な条件に基づいて検索やフィルタ処理を行うことができます。[続行準備完了 (Ready to proceed)] フィルタには、現在アップグレードの対象となっているすべての選択済みシャーシが表示されます。アップグレード手順を続行する前に、選択した番号が続行準備完了番号と一致している必要があります。一致しない場合は、[非候補 (Not candidates)] フィルタを使用して理由を確認します。不適格なシャーシを削除する必要はありません。自動的にアップグレードの対象から除外されます。

ステップ 5 (オプション) 選択したシャーシから不要なアップグレードパッケージを削除します。

シャーシアップグレードパッケージは手動で管理する必要があります。この時点がクリーンアップの最適なタイミングです。[詳細 (Details)] 列には、不要な可能性のあるパッケージを含むシャーシが示されます。該当するシャーシがある場合は、以下を実行します。

- a) 影響を受けるシャーシを表示するには、[警告 (Warning)] フィルタを使用します。
- b) フィルタ処理されたビューで、シャーシの横にある [パッケージの表示とクリーンアップ (View and clean up packages)] をクリックし、削除するパッケージを選択してから、[選択したパッケージの削除 (Delete selected packages)] をクリックします。クリーンアップするシャーシごとにこの手順を繰り返してください。

ステップ 6 [アップグレードの準備 (Prepare for Upgrade)] をクリックすると、シャーシへのアップグレードパッケージのコピーがすぐに開始されます。

アップグレードパッケージの入手先は、展開や以前の構成によって異なります。詳細については、[デバイスへのアップグレードパッケージのコピー](#)を参照してください。

ステップ 7 アップグレードの順序を選択します。

デフォルトでは、シャーシのアップグレードは並行して実行されます。シリアル順序の場合は、適切なシャーシを選択し、[シリアルアップグレードに移行 (Move to Serial Upgrade)] をクリックします。シリアルアップグレード順序を変更するには、[アップグレード順序の変更 (Change Upgrade Order)] をクリックします。



(注) 高可用性インスタンスを含むシャーシの場合、並行アップグレードまたはシリアルアップグレードのいずれかではなく、2つのワークフロー（アップグレードウィザードを2回実行）を推奨します。詳細については、「[アップグレード順序](#)」を参照してください。

ステップ 8 アップグレードの準備が完了していることを再確認します。

以前に実行した設定と展開の正常性チェックを再確認することをお勧めします ([設定と展開の確認](#))。

ステップ 9 [アップグレードの開始 (Start upgrade)] をクリックして、選択を確定します。

アップグレード時のトラフィック処理の詳細については、「[シャーシのアップグレードでのトラフィックフローとインスペクション](#)」を参照してください。

ステップ 10 アップグレードをモニターします。

ウィザードには、全体的なアップグレードの進行状況が表示されます。詳細については、「[Firewall Threat Defense アップグレードのモニタリング](#)」を参照してください。

ステップ 11 成功したことを確認します。

アップグレードが完了したら、**[デバイス (Devices)] > [デバイス管理 (Device Management)]** で成功を確認します。

ステップ 12 (任意) 設定の変更を確認します。

Firewall Threat Defense をアップグレードする前に、シャーシのアップグレードによって行われた変更を確認することをお勧めします。

- ワークフローをクリアしていない場合は、ウィザードに戻ることができます。**[デバイス (Devices)] > [+さらに表示 (+ Show more)] > [アップグレード (Upgrade)] > [シャーシのアップグレード (Chassis Upgrade)]** を選択し、各シャーシの横にある **[構成変更 (Configuration Changes)]** をクリックします。
- ワークフローをクリアした場合、または複数のシャーシの変更レポートをすばやく生成する場合は、**[高度な展開 (Advanced Deploy)]** ページを使用します。**[展開 (Deploy)] > [高度な展開 (Advanced Deploy)]** を選択し、アップグレードしたシャーシを選択して、**[保留中の変更レポート (Pending Changes Reports)]** をクリックします。レポートの生成が完了したら、メッセージセンターの **[タスク (Tasks)]** タブからレポートをダウンロードできます。

ステップ 13 (オプション) 高可用性展開では、デバイスのロールを調べます。

アップグレードの実行方法によっては、高可用性インスタンスのロールが切り替わる場合があります。後続の Firewall Threat Defense のアップグレードでもデバイスロールが切り替わることに注意し、必要な変更を加えてください。

次のタスク

- (オプション) **[アップグレード情報のクリア (Clear Upgrade Information)]** をクリックして、ウィザードをクリアします。これを行うまで、ページには、実行したばかりのアップグレードに関する詳細が引き続き表示されます。ウィザードをクリアしたら、**[デバイス管理 (Device Management)]** ページの **[アップグレード (Upgrade)]** タブを使用して、前回のアップグレード情報を確認します。また、**[高度な展開 (Advanced Deploy)]** 画面で設定の変更を確認します。
- 再度バックアップします：[バックアップ](#)

Firewall Chassis Manager を使用した Firepower 4100/9300 上の FXOS のアップグレード

Firepower Chassis Manager を使用したスタンドアロン FTD 論理デバイスまたは FTD シャーシ内クラスタ用の FXOS のアップグレード

このセクションでは、次のタイプのデバイスのアップグレードプロセスについて説明します。

- FTD 論理デバイスで構成されており、フェールオーバーペアまたはシャーシ間クラスタの一部ではない Firepower 4100 シリーズ シャーシ。
- フェールオーバーペアまたはシャーシ間クラスタの一部ではない 1 つまたは複数のスタンドアロン FTD 論理デバイスで構成されている Firepower 9300 シャーシ。
- シャーシ内クラスタ内の FTD 論理デバイスで構成されている Firepower 9300 シャーシ。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォームバンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。

手順

-
- ステップ 1** Firepower Chassis Manager で、[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 FXOS 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** 新しいプラットフォームバンドルイメージをアップロードします。
- a) [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。
 - b) [ファイルを選択 (ChooseFile)] 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。
 - c) [Upload] をクリックします。
選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。
 - d) 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契約書に同意します。
- ステップ 3** 新しいプラットフォームバンドルイメージが正常にアップロードされたら、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 4 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。

システム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 5 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレードプロセスをモニターできます。

- a) **scope system** を入力します。
- b) **show firmware monitor** を入力します。
- c) すべてのコンポーネント (FPRM、ファブリック インターコネクト、およびシャーシ) で「Upgrade-Status: Ready」と表示されるのを待ちます。



(注) FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例 :

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Fabric Interconnect A:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Chassis 1:
  Server 1:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
  Server 2:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
```

ステップ 6 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

- a) **top** を入力します。
- b) **scope ssa** を入力します。
- c) **show slot** を入力します。
- d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。

- e) **show app-instance** を入力します。
- f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

Firepower Chassis Manager を使用した FTD シャーシ間クラスタの FXOS のアップグレード

シャーシ間クラスタとして構成されている FTD 論理デバイスを備えた FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスがある場合、次の手順を使用して FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスの FXOS プラットフォームバンドルを更新します。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォームバンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。

手順

- ステップ 1** 次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。
- a) シャーシ #2 の FXOS CLI に接続します（これは制御ユニットを持たないシャーシである必要があります）。
 - b) **top** を入力します。
 - c) **scope ssa** を入力します。
 - d) **show slot** を入力します。
 - e) Firepower 4100 シリーズアプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
 - f) **show app-instance** を入力します。
 - g) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」、クラスタの状態が「In Cluster」であることを確認します。また、稼働バージョンとして表示されている FTD ソフトウェアのバージョンが正しいことを確認します。



重要 制御ユニットがこのシャーシ上にないことを確認します。「Master」に設定されているクラスタのロールを持つ Firepower Threat Defense インスタンスがあってはなりません。

- h) Firepower 9300 appliance にインストールされているすべてのセキュリティ モジュール、または Firepower 4100 シリーズ アプライアンス上のセキュリティ エンジンについて、FXOS バージョンが正しいことを確認してください。

scope server 1/slot_id で、Firepower 4100 シリーズ セキュリティ エンジンの場合、**slot_id** は 1 です。

show version を使用して無効にすることができます。

ステップ 2 シャーシ #2 の Firepower Chassis Manager に接続します（これは制御ユニットを持たないシャーシである必要があります）。

ステップ 3 Firepower Chassis Manager で、**[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 FXOS 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 4 新しいプラットフォーム バンドル イメージをアップロードします。

- [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。
- [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。
- [Upload] をクリックします。
選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。
- 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 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契約書に同意します。

ステップ 5 新しいプラットフォーム バンドル イメージが正常にアップロードされたら、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 6 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。

システム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 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレード プロセスをモニターできます。

- scope system** を入力します。
- show firmware monitor** を入力します。
- すべてのコンポーネント (FPRM、ファブリック インターコネクト、およびシャーシ) で「Upgrade-Status: Ready」と表示されるのを待ちます。



(注) FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

- d) **top** を入力します。
- e) **scope ssa** を入力します。
- f) **show slot** を入力します。
- g) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
- h) **show app-instance** を入力します。
- i) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」、クラスタの状態が「In Cluster」、クラスタのロールが「Slave」であることを確認します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready
```

```
Fabric Interconnect A:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready
```

```
Chassis 1:
  Server 1:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
  Server 2:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
```

```
FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot
```

```
Slot:
  Slot ID      Log Level Admin State Oper State
  -----
  1             Info      Ok      Online
  2             Info      Ok      Online
  3             Info      Ok      Not Available
```

```
FP9300-A /ssa #
```

```
FP9300-A /ssa # show app-instance
App Name  Slot ID  Admin State Oper State      Running Version Startup Version Profile Name
Cluster State Cluster Role
-----
ftd       1         Enabled   Online        6.2.2.81      6.2.2.81
In Cluster Slave
ftd       2         Enabled   Online        6.2.2.81      6.2.2.81
In Cluster Slave
ftd       3         Disabled  Not Available  6.2.2.81
Not Applicable None
FP9300-A /ssa #
```

ステップ 8 シャーシ #2 のセキュリティモジュールの 1 つを制御用として設定します。

シャーシ #2 のセキュリティモジュールの 1 つを制御用として設定すると、シャーシ #1 には制御ユニットが含まれなくなり、すぐにアップグレードすることができます。

ステップ 9 クラスタ内の他のすべてのシャーシに対して手順 1 ～ 7 を繰り返します。

ステップ 10 制御ロールをシャーシ #1 に戻すには、シャーシ #1 のセキュリティモジュールの 1 つを制御用として設定します。

Firepower Chassis Manager を使用した FTD ハイアベイラビリティペアの FXOS のアップグレード

ハイアベイラビリティペアとして構成されている FTD 論理デバイスを備えた FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスがある場合、次の手順を使用して FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスの FXOS プラットフォームバンドルを更新します。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。

手順

- ステップ 1** スタンバイの Firepower Threat Defense 論理デバイスを含む Firepower セキュリティアプライアンス上の Firepower Chassis Manager に接続します。
- ステップ 2** Firepower Chassis Manager で、[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 FXOS 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 3** 新しいプラットフォーム バンドル イメージをアップロードします。
- a) [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。
 - b) [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。
 - c) [Upload] をクリックします。
選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。
 - d) 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。

ステップ 4 新しいプラットフォームバンドル イメージが正常にアップロードされたら、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 5 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。

システム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 6 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレード プロセスをモニターできます。

- a) **scope system** を入力します。
- b) **show firmware monitor** を入力します。
- c) すべてのコンポーネント (FPRM、ファブリック インターコネクト、およびシャーシ) で「Upgrade-Status: Ready」と表示されるのを待ちます。



(注) FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例 :

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Fabric Interconnect A:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Chassis 1:
  Server 1:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
  Server 2:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
```

ステップ 7 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

- a) **top** を入力します。
- b) **scope ssa** を入力します。
- c) **show slot** を入力します。

- d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
- e) **show app-instance** を入力します。
- f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

ステップ 8 アップグレードしたユニットをアクティブユニットにして、アップグレード済みのユニットにトラフィックが流れるようにします。

- a) Firepower Management Center に接続します。
- b) **[デバイス (Devices)] > [デバイス管理 (Device Management)]** を選択します。
- c) アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン (🔄) をクリックします。
- d) ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、**[はい (Yes)]** をクリックします。

ステップ 9 新しいスタンバイの Firepower Threat Defense 論理デバイスを含む Firepower セキュリティアプライアンス上の Firepower Chassis Manager に接続します。

ステップ 10 Firepower Chassis Manager で、**[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 FXOS 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 11 新しいプラットフォーム バンドル イメージをアップロードします。

- a) **[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。
- b) **[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。
- c) **[Upload]** をクリックします。
選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。
- d) 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 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契約書に同意します。

ステップ 12 新しいプラットフォーム バンドル イメージが正常にアップロードされたら、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 13 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。

システム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。アップグレードプロセスは、完了までに最大 30 分かかることがあります。

ステップ 14 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレードプロセスをモニターできます。

- a) **scope system** を入力します。
- b) **show firmware monitor** を入力します。
- c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「Upgrade-Status: Ready」と表示されるのを待ちます。



(注) FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Fabric Interconnect A:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Chassis 1:
  Server 1:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
  Server 2:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
```

ステップ 15 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

- a) **top** を入力します。
- b) **scope ssa** を入力します。
- c) **show slot** を入力します。
- d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
- e) **show app-instance** を入力します。
- f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

ステップ 16 アップグレードしたユニットを、アップグレード前のようにアクティブ ユニットにします。

- a) Firepower Management Center に接続します。
- b) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- c) アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン (🔄) をクリックします。

- d) ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい (Yes)] をクリックします。

CLI を使用した Firepower 4100/9300 上の FXOS のアップグレード

FXOS CLI を使用したスタンドアロン FTD 論理デバイスまたは FTD シャーシ内クラスタ用の FXOS のアップグレード

このセクションでは、次のタイプのデバイスの FXOS のアップグレードプロセスについて説明します。

- FTD 論理デバイスで構成されており、フェールオーバーペアまたはシャーシ間クラスタの一部ではない Firepower 4100 シリーズ シャーシ。
- フェールオーバーペアまたはシャーシ間クラスタの一部ではない 1 つまたは複数のスタンドアロン FTD デバイスで構成されている Firepower 9300 シャーシ。
- シャーシ内クラスタ内の FTD 論理デバイスで構成されている Firepower 9300 シャーシ。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。
- Firepower 4100/9300 シャーシにソフトウェアイメージをダウンロードするため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ーの IP アドレスおよび認証クレデンシャル。
 - イメージ ファイルの完全修飾名。

手順

ステップ 1 FXOS CLI に接続します。

ステップ 2 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。

- a) ファームウェア モードに入ります。

Firepower-chassis-a # **scope firmware**

- b) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

Firepower-chassis-a /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**
- **scp://username@hostname/path/image_name**
- **sftp://username@hostname/path/image_name**
- **tftp://hostname:port-num/path/image_name**

- c) ダウンロード プロセスをモニタする場合：

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show 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-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
  File Name: fxos-k9.2.3.1.58.SPA
  Protocol: scp
  Server: 192.168.1.1
  Userid:
  Path:
  Downloaded Image Size (KB): 853688
  State: Downloading
  Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1 (FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

- ステップ 3** 必要に応じて、ファームウェア モードに戻ります。

Firepower-chassis-a /firmware/download-task # **up**

- ステップ 4** auto-install モードにします。

Firepower-chassis-a /firmware # **scope auto-install**

- ステップ 5** 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-a /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、2.3(1.58)）。

- ステップ 6** 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。

yes を入力して、検証に進むことを確認します。

ステップ 7 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。

システム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 8 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 system** を入力します。
- b) **show firmware monitor** を入力します。
- c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「Upgrade-Status: Ready」と表示されるのを待ちます。



(注) FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Fabric Interconnect A:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Chassis 1:
  Server 1:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
  Server 2:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

FP9300-A /system #
```

ステップ 9 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

- a) **top** を入力します。
- b) **scope ssa** を入力します。
- c) **show slot** を入力します。
- d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
- e) **show app-instance** を入力します。

- f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

FXOS CLI を使用した FTD シャーシ間クラスタの FXOS のアップグレード

シャーシ間クラスタとして構成されている FTD 論理デバイスを備えた FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスがある場合、次の手順を使用して FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスの FXOS プラットフォームバンドルを更新します。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。
- Firepower4100/9300 シャーシにソフトウェアイメージをダウンロードするため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ーの IP アドレスおよび認証クレデンシャル。
 - イメージ ファイルの完全修飾名。

手順

- ステップ 1** シャーシ #2 の FXOS CLI に接続します（これは制御ユニットを持たないシャーシである必要があります）。
- ステップ 2** 次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。
- a) **top** を入力します。
 - b) **scope ssa** を入力します。
 - c) **show slot** を入力します。
 - d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
 - e) **show app-instance** を入力します。

- f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」、クラスターの状態が「In Cluster」であることを確認します。また、稼働バージョンとして表示されている FTD ソフトウェアのバージョンが正しいことを確認します。



重要 制御ユニットがこのシャーシ上にないことを確認します。「Master」に設定されているクラスターのロールを持つ Firepower Threat Defense インスタンスがあってははいけません。

- g) Firepower 9300 appliance にインストールされているすべてのセキュリティ モジュール、または Firepower 4100 シリーズ アプライアンス上のセキュリティ エンジンについて、FXOS バージョンが正しいことを確認してください。

scope server 1/slot_id で、Firepower 4100 シリーズ セキュリティ エンジンの場合、**slot_id** は 1 です。

show version を使用して無効にすることができます。

ステップ 3 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。

- a) **top** を入力します。
b) ファームウェア モードに入ります。

Firepower-chassis-a # **scope firmware**

- c) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

Firepower-chassis-a /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**
- **scp://username@hostname/path/image_name**
- **sftp://username@hostname/path/image_name**
- **tftp://hostname:port-num/path/image_name**

- d) ダウンロード プロセスをモニタする場合：

Firepower-chassis-a /firmware # **scope download-task image_name**

Firepower-chassis-a /firmware/download-task # **show 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-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
  File Name: fxos-k9.2.3.1.58.SPA
  Protocol: scp
  Server: 192.168.1.1
  Userid:
  Path:
```

```
Downloaded Image Size (KB): 853688
State: Downloading
Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1 (FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 4 必要に応じて、ファームウェア モードに戻ります。

Firepower-chassis-a /firmware/download-task # **up**

ステップ 5 auto-install モードにします。

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

ステップ 6 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、2.3(1.58))。

ステップ 7 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。

yes を入力して、検証に進むことを確認します。

ステップ 8 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。

システム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 9 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 system** を入力します。
- b) **show firmware monitor** を入力します。
- c) すべてのコンポーネント (FPRM、ファブリック インターコネクト、およびシャーシ) で「Upgrade-Status: Ready」と表示されるのを待ちます。



(注) FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

- d) **top** を入力します。
- e) **scope ssa** を入力します。
- f) **show slot** を入力します。
- g) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
- h) **show app-instance** を入力します。

- i) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」、クラスタの状態が「In Cluster」、クラスタのロールが「Slave」であることを確認します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready
```

```
Fabric Interconnect A:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready
```

```
Chassis 1:
  Server 1:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
  Server 2:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
```

```
FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot
```

```
Slot:
  Slot ID      Log Level Admin State Oper State
  -----
  1             Info       Ok         Online
  2             Info       Ok         Online
  3             Info       Ok         Not Available
```

```
FP9300-A /ssa #
```

```
FP9300-A /ssa # show app-instance
App Name      Slot ID      Admin State Oper State      Running Version Startup Version Profile Name
Cluster State Cluster Role
-----
ftd           1           Enabled    Online          6.2.2.81        6.2.2.81
In Cluster    Slave
ftd           2           Enabled    Online          6.2.2.81        6.2.2.81
In Cluster    Slave
ftd           3           Disabled   Not Available   6.2.2.81
Not Applicable None
FP9300-A /ssa #
```

ステップ 10 シャーシ #2 のセキュリティモジュールの 1 つを制御用として設定します。

シャーシ #2 のセキュリティモジュールの 1 つを制御用として設定すると、シャーシ #1 には制御ユニットが含まれなくなり、すぐにアップグレードすることができます。

ステップ 11 クラスタ内の他のすべてのシャーシに対して手順 1 ～ 9 を繰り返します。

ステップ 12 制御ロールをシャーシ #1 に戻すには、シャーシ #1 のセキュリティモジュールの 1 つを制御用として設定します。

FXOS CLI を使用した FTD ハイアベイラビリティペアの FXOS のアップグレード

ハイアベイラビリティペアとして構成されている FTD 論理デバイスを備えた FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスがある場合、次の手順を使用して FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスの FXOS プラットフォームバンドルを更新します。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。
- Firepower4100/9300 シャーシにソフトウェアイメージをダウンロードするため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ーの IP アドレスおよび認証クレデンシャル。
 - イメージ ファイルの完全修飾名。

手順

ステップ 1 スタンバイの Firepower Threat Defense 論理デバイスを含む Firepower セキュリティ アプライアンス上の FXOS CLI に接続します。

ステップ 2 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。

a) ファームウェア モードに入ります。

Firepower-chassis-a # **scope firmware**

b) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

Firepower-chassis-a /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**
- **scp://username@hostname/path/image_name**
- **sftp://username@hostname/path/image_name**
- **tftp://hostname:port-num/path/image_name**

c) ダウンロードプロセスをモニタする場合：

Firepower-chassis-a /firmware # **scope download-task image_name**

```
Firepower-chassis-a /firmware/download-task # show 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-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
  File Name: fxos-k9.2.3.1.58.SPA
  Protocol: scp
  Server: 192.168.1.1
  Userid:
  Path:
  Downloaded Image Size (KB): 853688
  State: Downloading
  Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1 (FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 3 必要に応じて、ファームウェア モードに戻ります。

```
Firepower-chassis-a /firmware/download-task # up
```

ステップ 4 auto-install モードにします。

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

ステップ 5 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-a /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、2.3(1.58)）。

ステップ 6 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。

yes を入力して、検証に進むことを確認します。

ステップ 7 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。

システム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 8 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 system** を入力します。
- b) **show firmware monitor** を入力します。
- c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「Upgrade-Status: Ready」と表示されるのを待ちます。



(注) FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Fabric Interconnect A:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Chassis 1:
  Server 1:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
  Server 2:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

FP9300-A /system #
```

- ステップ 9** すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。
- top** を入力します。
 - scope ssa** を入力します。
 - show slot** を入力します。
 - Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
 - show app-instance** を入力します。
 - シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。
- ステップ 10** アップグレードしたユニットをアクティブユニットにして、アップグレード済みのユニットにトラフィックが流れるようにします。
- Firepower Management Center に接続します。
 - [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
 - アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン (🔄) をクリックします。
 - ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい (Yes)] をクリックします。
- ステップ 11** 新しいスタンバイの Firepower Threat Defense 論理デバイスを含む Firepower セキュリティ アプライアンス上の FXOS CLI に接続します。

ステップ 12 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。

a) ファームウェア モードに入ります。

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

b) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

```
Firepower-chassis-a /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
- **scp**://username@hostname/path/image_name
- **sftp**://username@hostname/path/image_name
- **tftp**://hostname:port-num/path/image_name

c) ダウンロード プロセスをモニタする場合 :

```
Firepower-chassis-a /firmware # scope download-task image_name
```

```
Firepower-chassis-a /firmware/download-task # show 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-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
  File Name: fxos-k9.2.3.1.58.SPA
  Protocol: scp
  Server: 192.168.1.1
  Userid:
  Path:
  Downloaded Image Size (KB): 853688
  State: Downloading
  Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1 (FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 13 必要に応じて、ファームウェア モードに戻ります。

```
Firepower-chassis-a /firmware/download-task # up
```

ステップ 14 auto-install モードにします。

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

ステップ 15 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-a /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、2.3(1.58))。

ステップ 16 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。

yes を入力して、検証に進むことを確認します。

ステップ 17 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。システム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 18 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 system** を入力します。
- b) **show firmware monitor** を入力します。
- c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「Upgrade-Status: Ready」と表示されるのを待ちます。



(注) FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Fabric Interconnect A:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Chassis 1:
  Server 1:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
  Server 2:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

FP9300-A /system #
```

ステップ 19 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

- a) **top** を入力します。
- b) **scope ssa** を入力します。
- c) **show slot** を入力します。
- d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。

- e) **show app-instance** を入力します。
- f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

ステップ 20 アップグレードしたユニットを、アップグレード前のようにアクティブ ユニットにします。

- a) Firepower Management Center に接続します。
- b) **[デバイス (Devices)] > [デバイス管理 (Device Management)]** を選択します。
- c) アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン (🔄) をクリックします。
- d) ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、**[はい (Yes)]** をクリックします。

Firepower 4100/9300 のファームウェアのアップグレード

シャーシの FXOS 2.14.1 以降へのアップグレード (Firewall Threat Defense 7.4 の関連リリース) にはファームウェアが含まれます。古いデバイスをアップグレードする場合は、「[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。

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。