

# ASDM ( On-Box Management ) による FirePOWER モジュール設定のバックアップと復 元の設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[バックアップ/復元の設定](#)

[ローカル バックアップ/リモート バックアップの設定](#)

[バックアップのスケジュール作成](#)

[バックアップ プロファイルの作成](#)

[バックアップ タスクのスケジュール作成](#)

[バックアップの復元の設定](#)

[設定のインポート/エクスポート](#)

[設定のエクスポート](#)

[設定のインポート](#)

[トラブルシューティング](#)

[確認](#)

[関連情報](#)

## 概要

ADSMFirePOWER //

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- ASA ( 適応型セキュリティ アプライアンス ) ファイアウォール、ASDM ( Adaptive Security Device Manager ) 。
- FirePOWER アプライアンス。
- ASDM 設定で FirePOWER モジュール タブが使用可能であることを確認します。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェア バージョン 5.4.1 以降が稼働する ASA FirePOWER モジュール ( ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X )

- ソフトウェア バージョン 6.0.0 以降が稼働する ASA FirePOWER モジュール ( ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X )

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 背景説明

バックアップ/復元は、主に管理者が定期的に行う有用な作業です。これは、事故後 ( デイザスタリカバリとも呼ばれる ) およびモジュール破損 ( ファイルまたは データ回復 )。

FirePOWER モジュールには、バックアップと復元のための 2 種類のオプションがあります。

1. ASDM では設定バックアップを作成できます。このバックアップは、デイザスタリカバリ / データ破損の場合に同じモデルに復元できます。
2. Firepower Management Center ( FMC ) ではインポート/エクスポート オプションを使用して、設定の各部分のバックアップを実行できます。エクスポートしたポリシーは同じモデルまたは同じバージョンの異なるモデルにインポートできるため、これにはすべてのタイプのポリシーが含まれます。また、モジュール間で設定を移行する場合にもこのオプションを選択できます。

## バックアップ/復元の設定

FirePOWER モジュールは、モジュール自体のハード ドライブまたはリモート デバイスのいずれに対してもバックアップを実行できます。

:Firepower

### ローカル バックアップ/リモート バックアップの設定

FirePOWER モジュールのローカル バックアップを作成するため、[Configuration] > [ASA Firepower Configuration] > [Tools] > [Backup/ Restore] > [Backup Management] に移動し、[Device Backup] をクリックします。

**名前 :** バックアップの名前を指定します。

**[Storage Location] :** ASDM ではローカル ストレージ ( /var/sf/backup ) だけがサポートされています。

**[Email] :** 電子メールでの通知を有効にします。電子メール リレー サーバ設定のシステム ポリシー ( [ASA Firepower Configuration] > [SystemPolicy] ) を設定する必要があります。

**[Copy when Complete] :** リモート バックアップを設定するにはこのチェックボックスをオンにします。FirePOWER はバックアップをバックアップ サーバに送信するときに SCP プロトコル

を使用します。

- **Host** : リモート サーバの IP/ホストを指定します。
- **Path**: リモート ディレクトリ パスを指定します
- **User**: リモート ユーザ名を指定します。
- **パスワード** : リモート ユーザ名のパスワードを指定します

Configuration > ASA FirePOWER Configuration > Tools > Backup Restore

Backup Management | Backup Profiles

**Create Backup**

Name: Production\_backup

Storage Location: /var/sf/backup/

Email: Not available. You must set up your mail relay host.

Copy when complete:

Host: 192.168.1.10

Path: /var/backup

User: admin

Password: .....

SSH Public Key: ssh-rsa AAAAB3NzaC1yc2EAAAADAQ  
*To use ssh keys place this public key in your authorized\_keys file.*

Start Backup | Save As New | Cancel

[バックアップの開始]オプションをクリックしてバックアッププロセスを開始します。[新しい名前]で保存]オプションは、バックアッププロファイルで使用できるバックアッププロファイルを作成します。

## バックアップのスケジュール作成

デバイスの設定の適切な時点でのバックアップをスケジュールできます。バックアップスケジュールでは、デバイスのバックアップ処理を時間単位/日単位/週単位/月単位で自動化できます。バックアップをスケジュールするには、次の2つの手順を実行します。

**ステップ 1: バックアッププロファイルの作成。**

**ステップ 2: バックアップタスクのスケジュール作成。**

### バックアッププロファイルの作成

バックアッププロファイルを作成するには、[Configuration] > [ASA Firepower Configuration] > [Tools] > [Backup/ Restore] > [Backup Management] に移動し、[Backup profile] をクリックします。

バックアッププロファイル作成オプションは、直前の項 ( 「ローカルバックアップ/リモートバックアップの設定」 ) で説明したオプションに似ています。

### バックアップタスクのスケジュール作成

バックアップ タスクをスケジュールするには、[Configuration] > [ASA Firepower Configuration] > [Tools] > [Scheduling] に移動し、[Add Task] をクリックします。

[ジョブタイプ] : ドロップダウンリストでジョブタイプとして[バックアップ]を選択します。

実行するタスクのスケジュール : ラジオボタンを選択して、スケジュールするタスクの頻度を定義します。

[開始日] : ドロップダウンリストから[日付]を選択して、バックアップの開始日を定義します。

繰り返し間隔 : バックアップ・ スケジュール・ タスクの繰り返し頻度を時間/日/週/月単位で指定します。

[実行時刻]:ドロップダウンリストからバックアップの開始時刻を選択します。

[繰り返し日] : バックアップを繰り返す日のチェックボックスをオンにします。

ジョブ名 : スケジュールされたジョブの名前を指定します。

[バックアッププロファイル]:ドロップダウンリストから、前の手順で作成したバックアッププロファイルを選択します。

コメント : 作成したジョブに関する説明を記述できます。

電子メールのステータス : 電子メール中継ホストを設定して、スケジュールされたジョブバックアップのステータスを送信できます。

Configuration > ASA FirePOWER Configuration > Tools > Scheduling

Add Task Today

### New Task

Job Type: Backup

Schedule task to run:  Once  Recurring

Start On: April 24, 2016 America/New York

Repeat Every: 1  Hours  Days  Weeks  Months

Run At: 12:00 Pm

Repeat On:  Sunday  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday

Job Name: Production Backup Weekly

Backup Profile: Production\_backup

Comment: Firepower Backup of Datacenter ABC

Email Status To: Not available. You must set up your mail relay host by editing the System Policy using the Remote Manager.

Save Cancel

[Save] ボタンをクリックして、スケジュール バックアップの設定を保存します。

## バックアップの復元の設定

デバイス設定が破損しているか、アプライアンスをリイメージした場合には、バックアップを復元する必要があります。新しくリイメージしたアプライアンスに古い設定を復元できます。

バックアップ タスクを復元するには、[Configuration] > [ASA Firepower Configuration] > [Tools] > [Backup/ Restore] に移動します。リモート ストレージを設定している場合は、リモート ストレージからバックアップ ファイルを取得し、[Upload Backup] オプションを選択してバックアップ ファイルをアップロードします。

アップロードされたファイルまたは既に作成されたバックアップファイルは、バックアップ管理 ページで使用できます。復元するバックアップファイルを選択して、[復元]オプションをクリックして復元バックアップを開始します。

Configuration > ASA FirePOWER Configuration > Tools > Backup Restore

Backup Management | Backup Profiles

Device Backup | Upload Backup

### Device Backups

<input type="checkbox"/>	System Information	Date Created	File Name	VDB Version	Location	Size (MB)
<input checked="" type="checkbox"/>	<b>firepower</b> ASA5506 v6.0.0	2016-04-24 23:13:10	Test_backup-2016-04-25T03-10-32.tgz	build 252	Local	50

Restore | Download | Delete

Storage Location: /var/sf/backup/ (Disk Usage: 16%)

[Restore] をクリックすると、設定データを本当に置き換えるか確認を求められます。[Restore] をもう一度クリックして、復元プロセスに進みます。

## 設定のインポート/エクスポート

FirePOWER モジュールでは、さまざまなタイプの設定をコピーするときに使用するインポート/エクスポート機能がサポートされています。これには、同一タイプ/異なるタイプのモジュール間でのポリシーのインポート/エクスポートも含まれます。

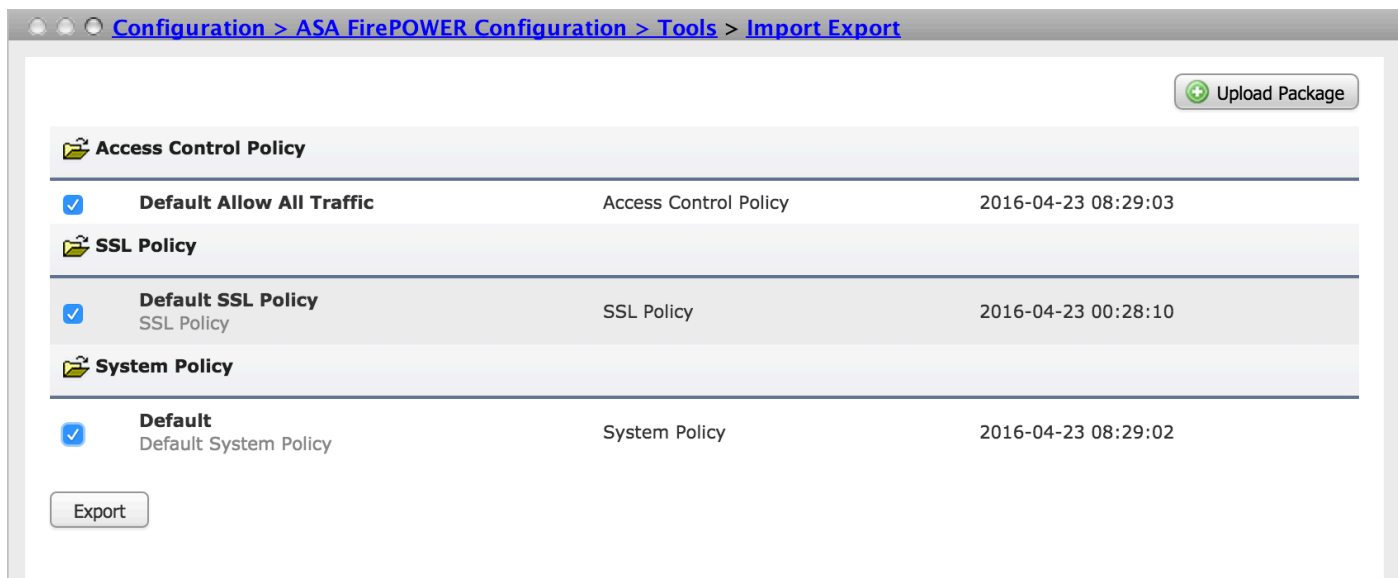
エクスポートおよびインポートできるポリシーのタイプを次に示します。

- アクセスコントロール ポリシー ( ネットワーク分析とファイル ポリシーを含む )
- 侵入ポリシー
- システム ポリシー
- アラート応答

## 設定のエクスポート

設定をエクスポートするには、[Configuration] > [ASA Firepower Configuration] > [Tools] > [Import/Export] に移動します。

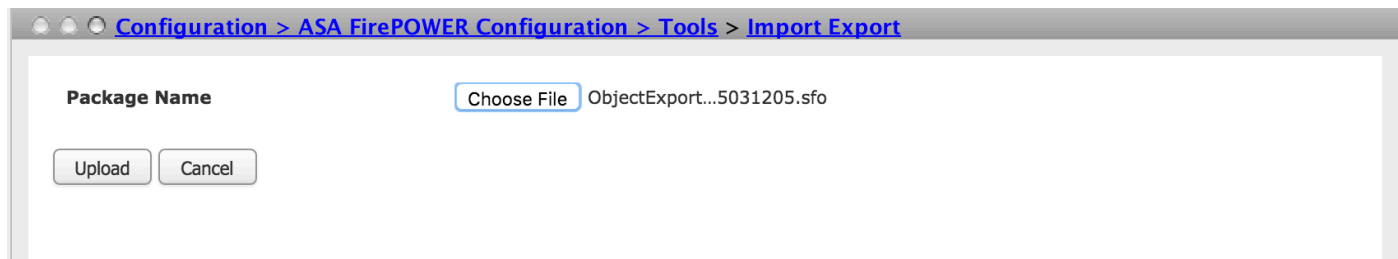
FirePOWER モジュールでは、1つのポリシー、または同一タイプ/異なるタイプのポリシーのセットを、その設定のリビジョン番号と共に一括でエクスポートできます。



ポリシーをエクスポートするには、[Export] ボタンをクリックします。FirePOWER モジュールから、エクスポート ファイル ( \*.sfo ) を保存するよう求められます。

## 設定のインポート

ASDM で保存されているエクスポート ファイルをインポートするには、[Configuration] > [ASA Firepower Configuration] > [Tools] > [Import/Export] に移動し、[Upload Package] をクリックします。インポートするファイルを選択して [Upload] をクリックするよう求められます。

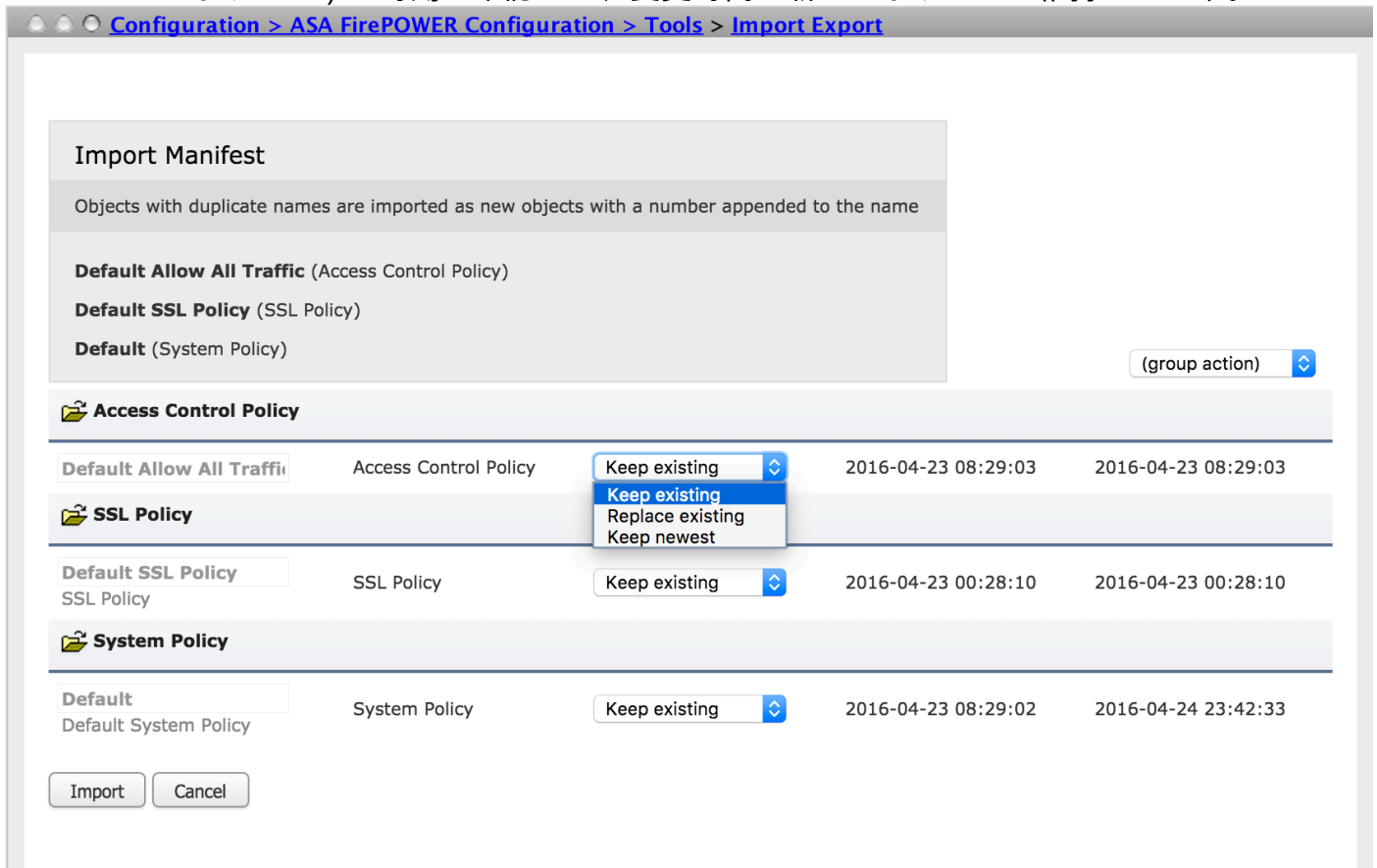


次のページに、インポートしたファイル ( \*.sfo ) に含まれているポリシーが表示されます。FirePOWER モジュールにインポートするポリシーを選択します。



ポリシーをインポートするには、[Import] ボタンをクリックします。エクスポートされたポリシーの名前が FirePOWER モジュールに存在するポリシーと競合する場合、FirePOWER モジュールには次のオプションがあります。

- **[Keep Existing]** : このオプションを選択すると、既存のポリシーが維持され、新しいポリシーのインポートは許可されません。
- **[Replace Existing]** : このオプションを選択すると、既存のポリシーを置き換えることができます。
- **[Keep Newest]** : このオプションを選択すると、両方のポリシー ( 既存のポリシーとインポートされるポリシー ) の時刻が確認され、変更時間が新しいポリシーが維持されます。



エクスポートしたポリシーをインポートするには、[Import] ボタンをクリックします。

## トラブルシューティング

**ステップ 1 :** モジュールのコマンドライン インターフェイス ( CLI ) にログインし、Telnet および Ping コマンドを使用してリモート サーバへのネットワーク接続を確認します。

**ステップ 2 :** バックアップが保存されているリモート ディレクトリでの Secure Copy ( SCP ) ユーザの権限を確認します。

**ステップ 3 :** ASA FirePOWER モジュールはその情報を使用して、その設定を別のアプライアンスにインポートできるかどうかを判断します。アプライアンスにすでに存在する設定リビジョンをインポートすることはできません。

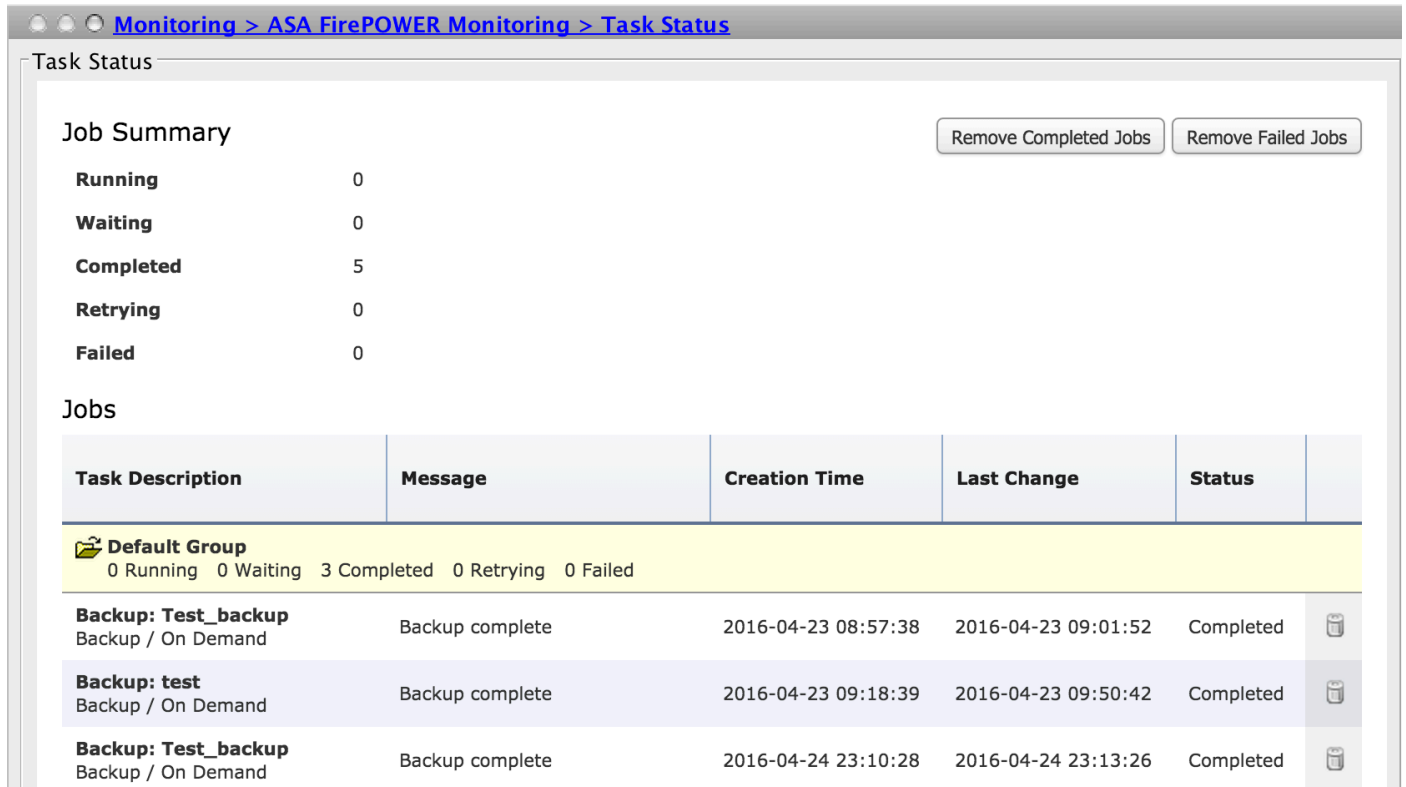
**ステップ 4 :** バックアップの復元では、ソフトウェアバージョン、ルール更新バージョン、VDBバージョン、およびハードウェアモデルが同じであることを確認する必要があります。

**ステップ 5 :** エクスポートされたポリシーのインポートでは、同じソフトウェアバージョン、ルールアップデートバージョン、およびVDBバージョンを使用していることを確認する必要があります。



# 確認

ステップ 1 : バックアップ/復元タスクが正常に完了していることを確認するため、[Monitoring] > [ASA Firepower Monitoring] > [Task Status] に移動して確認します。



Monitoring > ASA FirePOWER Monitoring > Task Status

Task Status

Job Summary Remove Completed Jobs Remove Failed Jobs

<b>Running</b>	0
<b>Waiting</b>	0
<b>Completed</b>	5
<b>Retrying</b>	0
<b>Failed</b>	0

Jobs

Task Description	Message	Creation Time	Last Change	Status	
<b>Default Group</b> 0 Running 0 Waiting 3 Completed 0 Retrying 0 Failed					
<b>Backup: Test_backup</b> Backup / On Demand	Backup complete	2016-04-23 08:57:38	2016-04-23 09:01:52	Completed	
<b>Backup: test</b> Backup / On Demand	Backup complete	2016-04-23 09:18:39	2016-04-23 09:50:42	Completed	
<b>Backup: Test_backup</b> Backup / On Demand	Backup complete	2016-04-24 23:10:28	2016-04-24 23:13:26	Completed	

ステップ 2 : [Configuration] > [ASA Firepower Configuration] > [Tools] > [Backup/ Restore] > [Backup Management] に移動し、バックアップ ファイルが作成されているかどうかを確認します。

- [Cisco ASA FirePOWER](#)
- [– Cisco Systems](#)