

# Firewall Device Managerを使用したセキュアファイアウォール脅威対策のアップグレード

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[はじめる前に](#)

[設定](#)

[検証](#)

---

## はじめに

このドキュメントでは、ファイアウォールデバイスマネージャ(FDM)を使用したCisco Secure Firewall Threat Defense(FTD)のアップグレード例について説明します。

## 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。

- このガイドに関する特別な要件はありません

### 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。

- FTDバージョン7.2.3を実行しているCisco Firepower 4125

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、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

このドキュメントに関する特定の要件は次のとおりです。

- FTDの管理IPへの接続

- 以前にソフトウェアCiscoポータルからダウンロードしたFTDアップグレードパッケージ (.REL.tar)

このアップグレード手順は、アプライアンスでサポートされています。

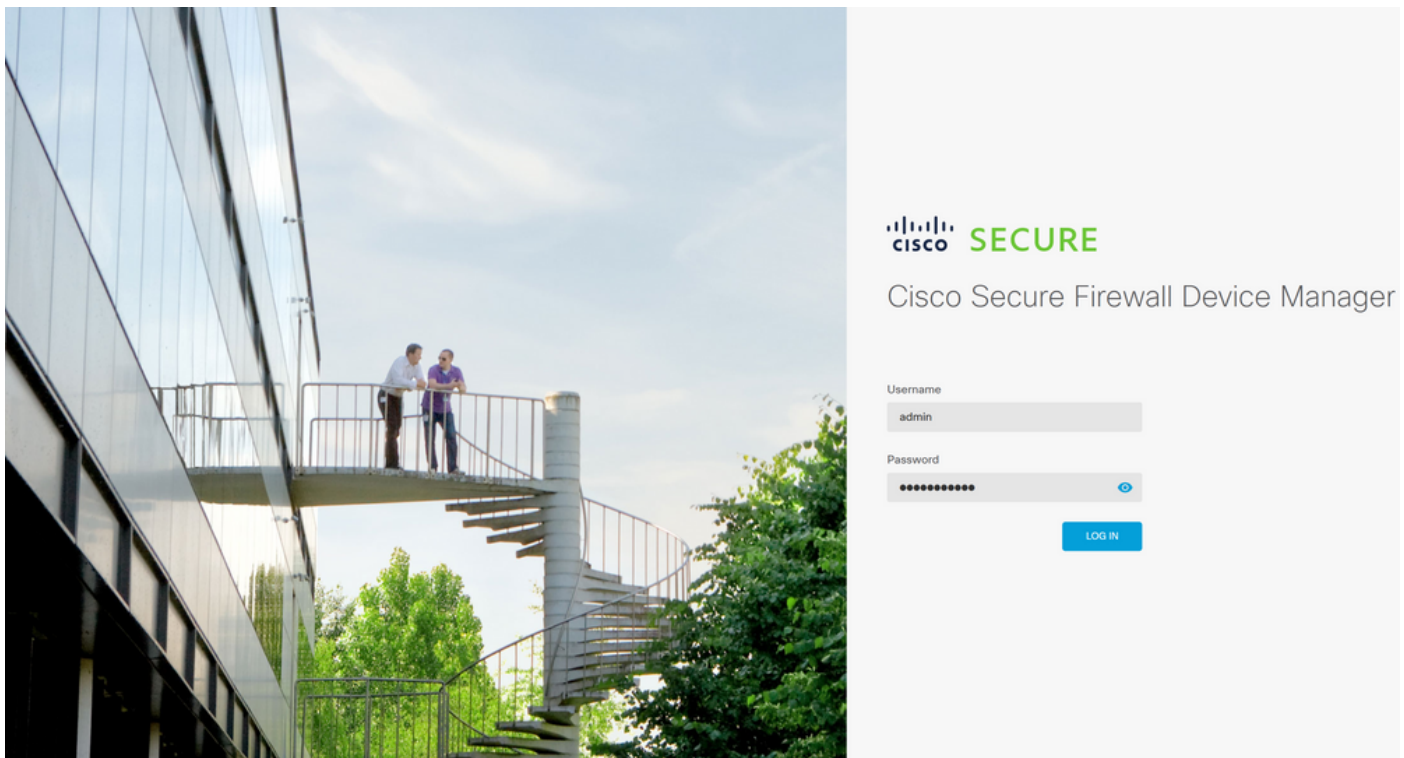
- ローカル管理が設定されたFTDソフトウェアを実行するCisco Firepowerモデル。

## はじめる前に

1. FTD設定のバックアップを作成してダウンロードします。
2. ターゲットバージョンの[アップグレードパス](#)を検証します。
3. [Cisco Software Central](#)からアップグレードパッケージをダウンロードします。
4. アップグレードファイルの名前は変更しないでください。システムは、名前が変更されたファイルを無効と見なします。
5. トラフィックが影響を受けるため、アップグレード手順のメンテナンスウィンドウをスケジュールします。

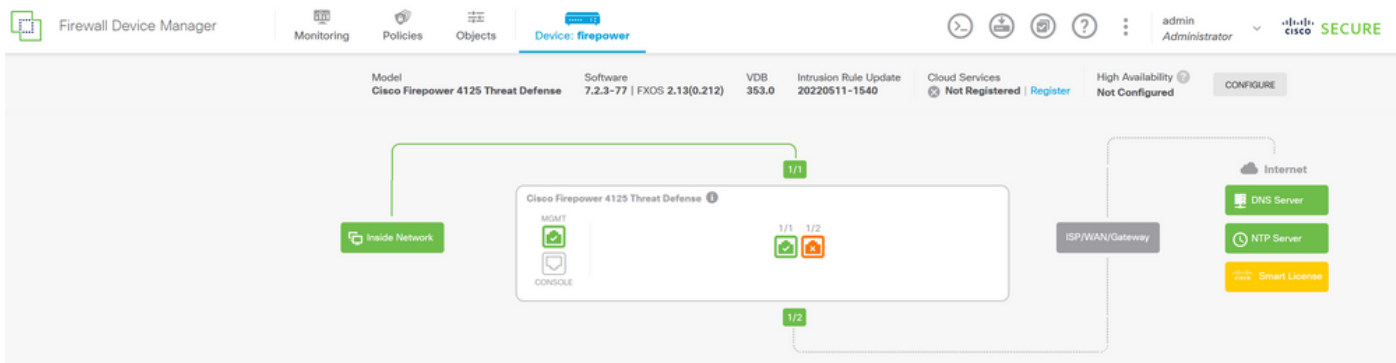
## 設定

ステップ 1 : FTDの管理IPを使用して、ファイアウォールデバイスマネージャにログインします。



© 2015-2023 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. This product contains some software licensed under the "GNU Lesser General Public License, versions: 2, 2.1 and 3" provided with ABSOLUTELY NO WARRANTY under the terms of "GNU Lesser General Public License, version 2.0, version 2.1 and version 3.0".

ステップ 2 : ファイアウォールデバイスマネージャダッシュボードでView Configurationをクリックします。

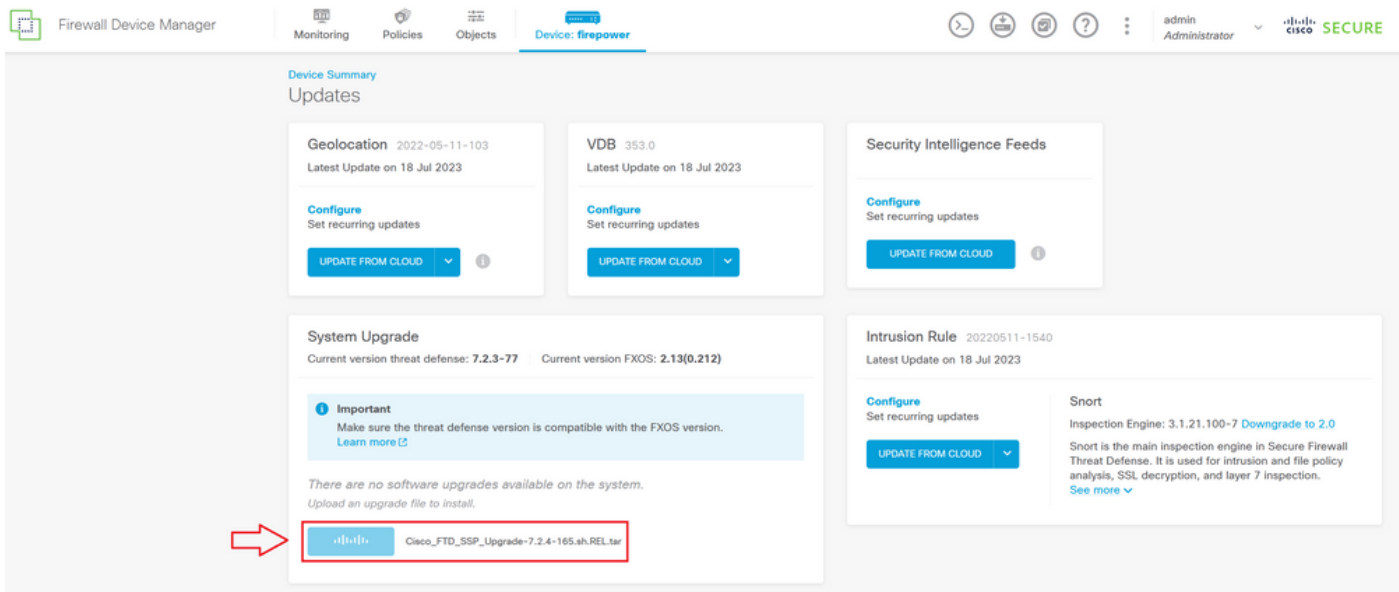


<b>Interfaces</b> Connected Enabled 3 of 3 <a href="#">View All Interfaces</a>	<b>Routing</b> There are no static routes yet <a href="#">View Configuration</a>	<b>Updates</b> Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds <a href="#">View Configuration</a>	<b>System Settings</b> <a href="#">Management Access</a> <a href="#">Logging Settings</a> <a href="#">DHCP Server / Relay</a> <a href="#">DDNS Service</a> <a href="#">DNS Server</a> <a href="#">Management Interface</a> <a href="#">Hostname</a> <a href="#">Time Services</a> <a href="#">See more</a>
<b>Smart License</b> Evaluation expires in 90 days <a href="#">View Configuration</a>	<b>Backup and Restore</b> <a href="#">View Configuration</a>	<b>Troubleshoot</b> No files created yet REQUEST FILE TO BE CREATED	
<b>Site-to-Site VPN</b> There are no connections yet <a href="#">View Configuration</a>	<b>Remote Access VPN</b> Requires RA VPN license No connections   1 Group Policy <a href="#">Configure</a>	<b>Advanced Configuration</b> Includes: FlexConfig, Smart CLI <a href="#">View Configuration</a>	<b>Device Administration</b> <a href="#">Audit Events</a> , <a href="#">Deployment History</a> , <a href="#">Download Configuration</a> <a href="#">View Configuration</a>

ステップ 3 : System Upgradeセクションの下にあるBrowseボタンをクリックして、インストールパッケージをアップロードします。

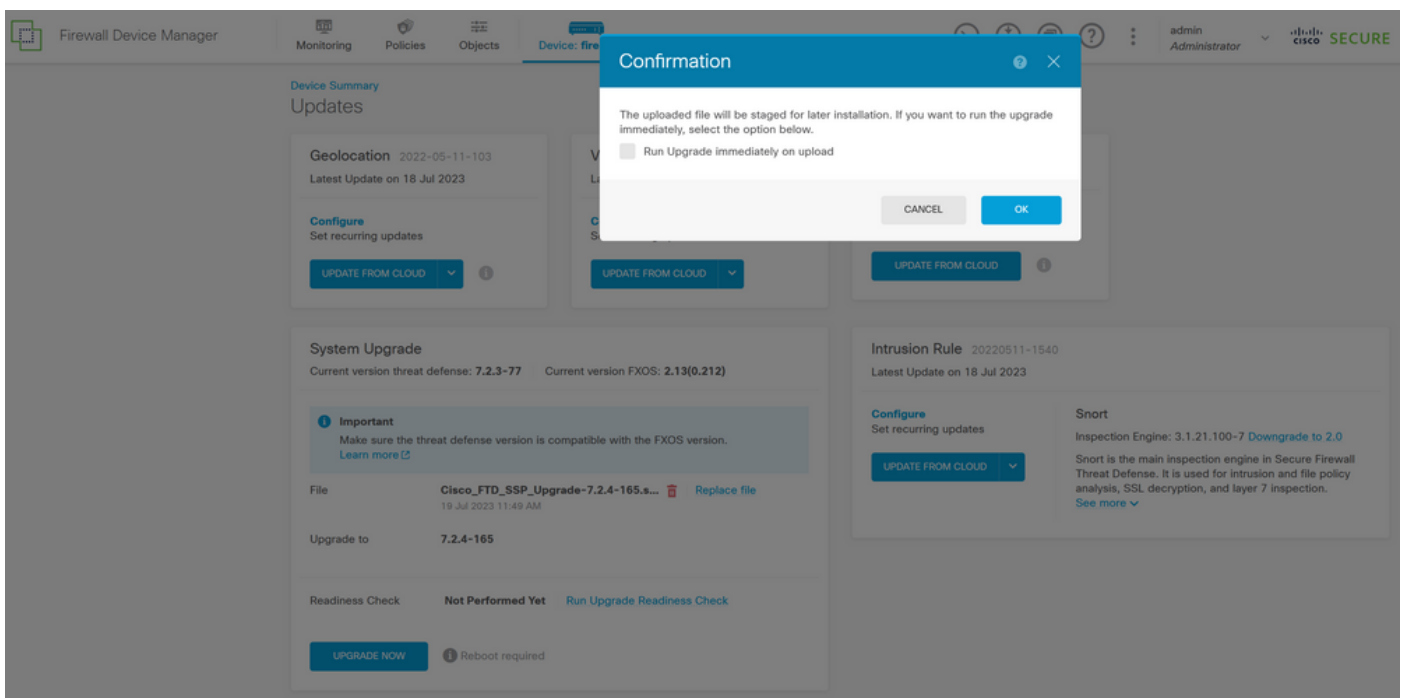
**⚠ 注意 :** アップグレードパッケージをアップロードすると、ファイルのアップロード中に BROWSEによってアニメーションが表示されます。アップロードが完了するまでWebページを更新しないでください。


アップロードプログレスページの例 :



ステップ 4 : アップロードが完了すると、確認を求めるポップアップウィンドウが表示されます

。



 注 : アップグレードを直接進める場合は、「アップロード時に直ちにアップグレードを実行」オプションをオンにできます。ただし、ここでは「レディネスチェック」をスキップするため、アップグレード上の競合に関する洞察を提供し、障害を回避できることに注意してください。

ステップ5:アップグレードの失敗を防ぐために、アップグレードの事前検証を実行するには、Run Upgrade Readiness Checkをクリックします。

Firewall Device Manager

Monitoring Policies Objects **Device: firepower**

admin Administrator

Device Summary

Updates

Geolocation 2022-05-11-103  
Latest Update on 18 Jul 2023

VDB 353.0  
Latest Update on 18 Jul 2023

Security Intelligence Feeds

Intrusion Rule 20220511-1540  
Latest Update on 18 Jul 2023

System Upgrade  
Current version threat defense: 7.2.3-77 Current version FXOS: 2.13(0.212)

**Important**  
Make sure the threat defense version is compatible with the FXOS version.  
Learn more

File Cisco\_FTD\_SSP\_Upgrade-7.2.4-165.s...  
19 Jul 2023 11:49 AM [Replace file](#)

Upgrade to 7.2.4-165

Readiness Check **Not Performed Yet** [Run Upgrade Readiness Check](#)

**UPGRADE NOW** Reboot required

注：準備状況の確認が正常に終了したことをタスクリストから検証できます。

正常な準備状況チェックの例：

Firewall Device Manager

Monitoring Policies Objects **Device: firepower**

admin Administrator

Device Summary

Updates

Geolocation 2022-05-11-103  
Latest Update on 18 Jul 2023

System Upgrade  
Current version threat defense: 7.2.3-77 Current version FXOS: 2.13(0.212)

**Important**  
Make sure the threat defense version is compatible with the FXOS version.  
Learn more

File Cisco\_FTD\_SSP\_Upgrade-7.2.4-165.s... [Replace file](#)

Upgrade to 7.2.4-165

Readiness Check **Precheck Success** [Run Upgrade Readiness Check](#)

**UPGRADE NOW** Reboot required

Intrusion Rule 20220511-1540  
Latest Update on 18 Jul 2023

**Task List**

1 total 0 running 1 completed 0 failures [Delete all finished tasks](#)

Name	Start Time	End Time	Status	Actions
Upgrade Readiness	19 Jul 2023 11:52 AM	19 Jul 2023 11:54 AM	Upgrade Readiness Check Completed Successfully	

手順 6：UPGRADE NOWボタンをクリックして、ソフトウェアアップグレードを続行します。

Firewall Device Manager

Monitoring Policies Objects Device: **firepower**

admin Administrator

Device Summary

Updates

Geolocation 2022-05-11-103  
Latest Update on 18 Jul 2023

Configure  
Set recurring updates

UPDATE FROM CLOUD

VDB 353.0  
Latest Update on 18 Jul 2023

Configure  
Set recurring updates

UPDATE FROM CLOUD

Security Intelligence Feeds

Configure  
Set recurring updates

UPDATE FROM CLOUD

System Upgrade  
Current version threat defense: 7.2.3-77 Current version FXOS: 2.13(0.212)

**Important**  
Make sure the threat defense version is compatible with the FXOS version.  
[Learn more](#)

File  
Cisco\_FTD\_SSP\_Upgrade-7.2.4-165.s...  
19 Jul 2023 11:49 AM [Replace file](#)

Upgrade to  
7.2.4-165

Readiness Check  
**Precheck Success** 19 Jul 2023 11:54 AM [Run Upgrade Readiness Check](#)

UPDATE NOW **Reboot required**

Intrusion Rule 20220511-1540  
Latest Update on 18 Jul 2023

Configure  
Set recurring updates

UPDATE FROM CLOUD

Snort  
Inspection Engine: 3.1.21.100-7 [Downgrade to 2.0](#)  
Snort is the main inspection engine in Secure Firewall Threat Defense. It is used for intrusion and file policy analysis, SSL decryption, and layer 7 inspection.  
[See more](#)

手順 7 : ポップアップウィンドウでCONTINUEを選択し、アップグレードを続行します。

Firewall Device Manager

Monitoring Policies Objects Device: fire

admin Administrator

Device Summary

Updates

Geolocation 2022-05-11-103  
Latest Update on 18 Jul 2023

Configure  
Set recurring updates

UPDATE FROM CLOUD

System Upgrade  
Current version threat defense: 7.2.3-77 Current ve

**Important**  
Make sure the threat defense version is compatible with the FXOS version.  
[Learn more](#)

File  
Cisco\_FTD\_SSP\_Upgrade-7.2.4-165.s...  
19 Jul 2023 11:49 AM [Replace file](#)

Upgrade to  
7.2.4-165

Readiness Check  
**Precheck Success** 19 Jul 2023 11:54 AM [Run Upgrade Readiness Check](#)

UPDATE NOW **Reboot required**

Intrusion Rule 20220511-1540  
Latest Update on 18 Jul 2023

Configure  
Set recurring updates

UPDATE FROM CLOUD

Snort  
Inspection Engine: 3.1.21.100-7 [Downgrade to 2.0](#)  
Snort is the main inspection engine in Secure Firewall Threat Defense. It is used for intrusion and file policy analysis, SSL decryption, and layer 7 inspection.  
[See more](#)

**Confirm System Upgrade**

Before starting the upgrade:


1. Do not start a system restore at the same time as a system upgrade.
2. Do not reboot the system during the upgrade. The system automatically reboots at the appropriate time during upgrade if a reboot is necessary.
3. **Do not power off the device** during the upgrade. Interrupting the upgrade can leave the system in an unusable state.

You will be logged out of the system when the upgrade begins.  
After the installation completes, the device will be rebooted.

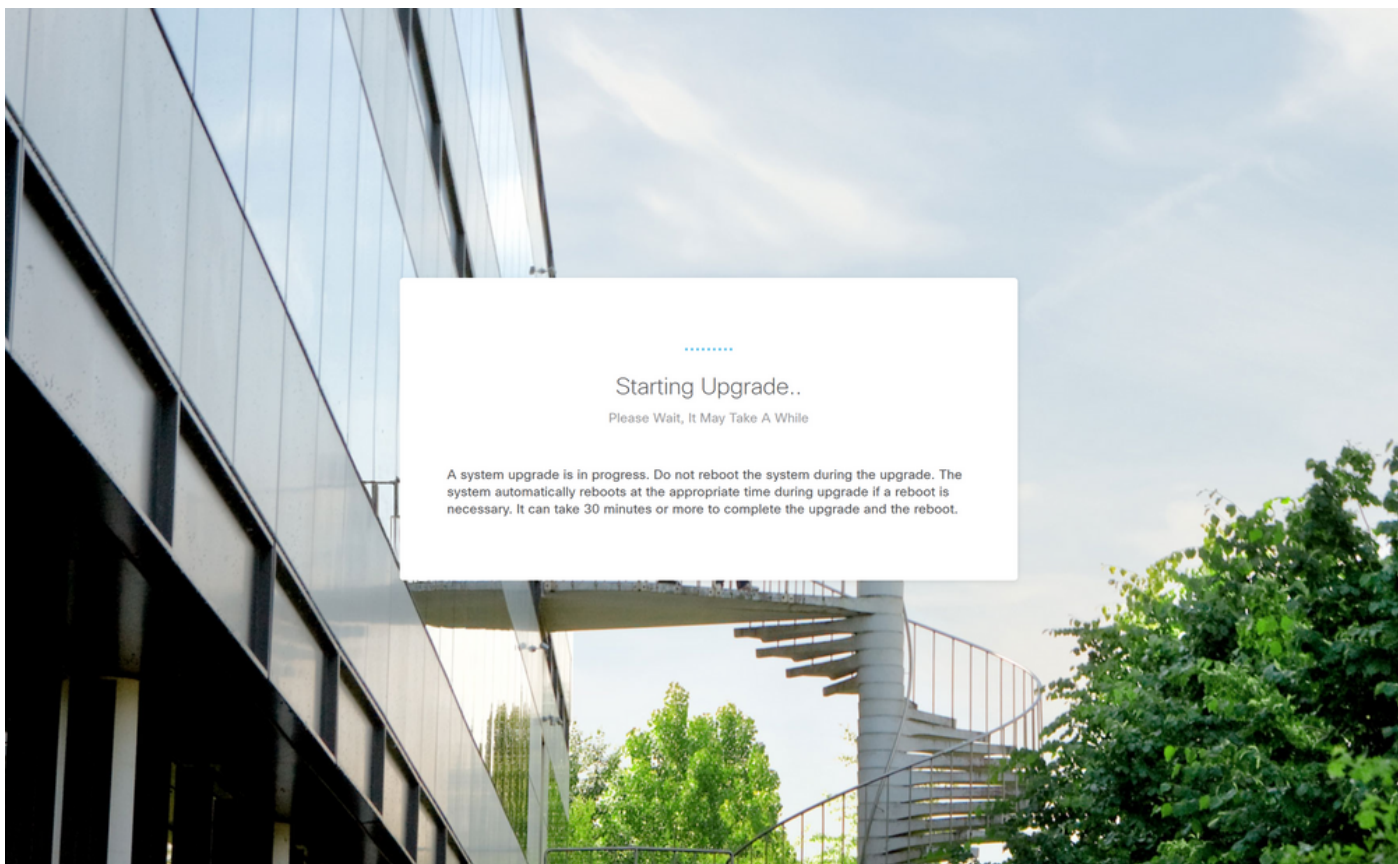
UPGRADE OPTIONS

Automatically cancel on upgrade failure and roll back to the previous version

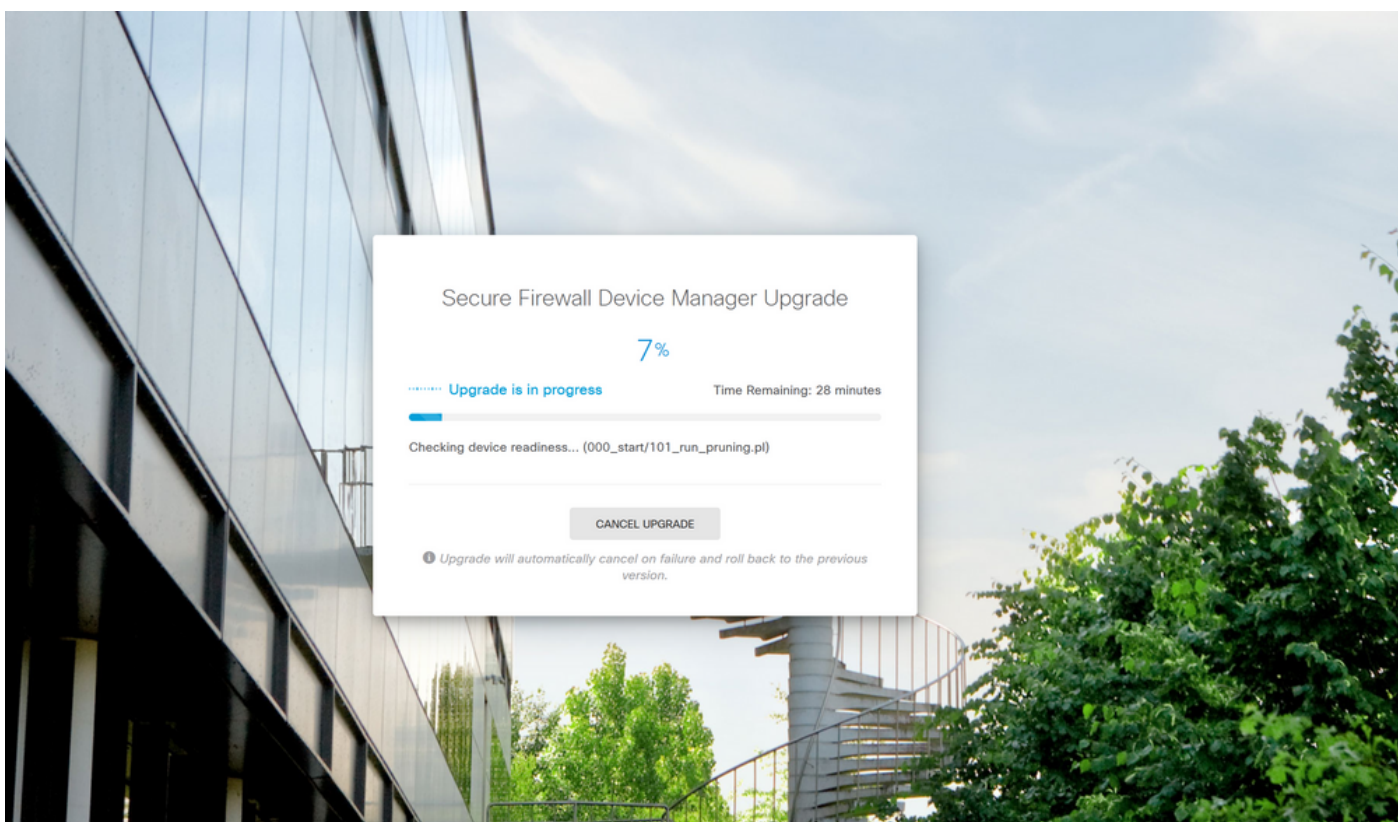
CANCEL CONTINUE

 注 : ロールバックオプションはデフォルトで有効になっています。アップグレードで問題が発生した場合にアップグレード設定を元に戻すには、このオプションを保持することをお勧めします。

ステップ 8 : アップグレードの進行状況が表示されるページにリダイレクトされます。



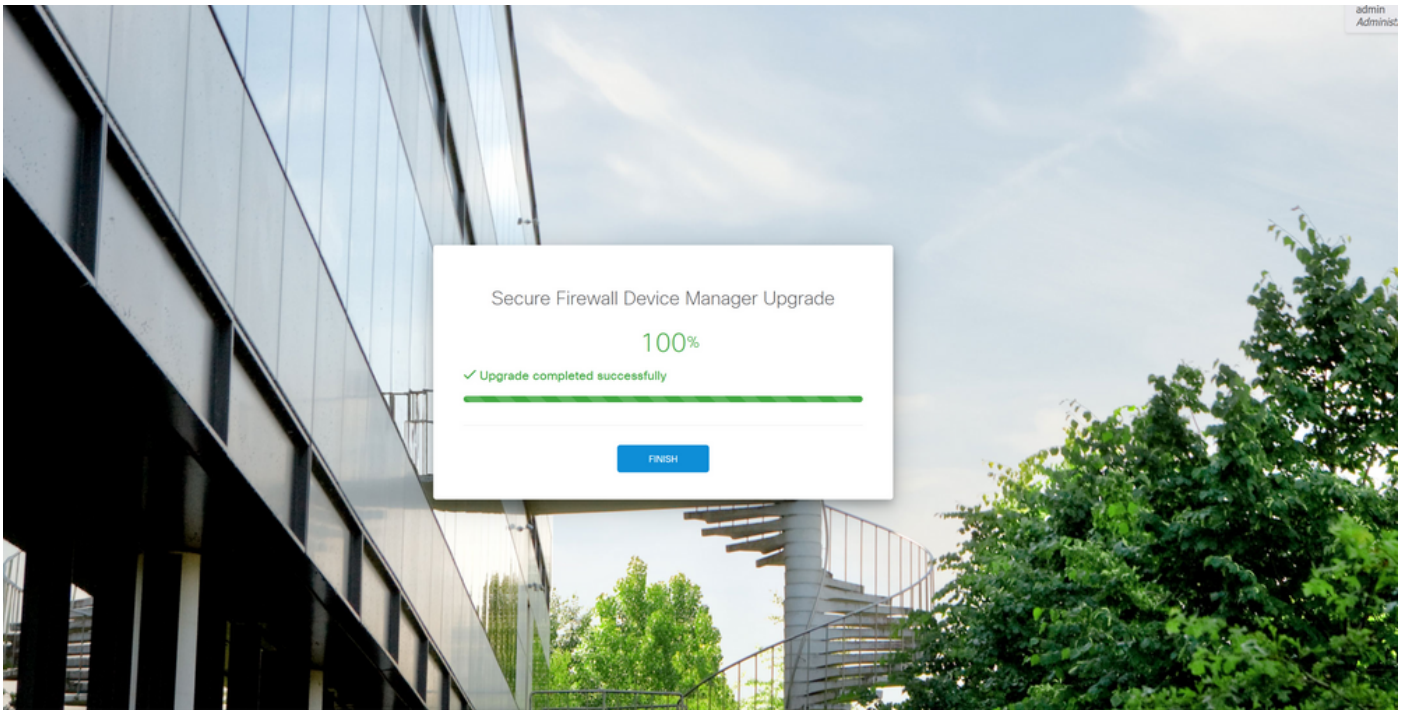
進行状況ページの例：



© 2015-2023 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc.  
This product contains some software licensed under the "GNU Lesser General Public License, versions: 2, 2.1 and 3" provided with ABSOLUTELY NO WARRANTY under the terms of "GNU Lesser General Public License, [version 2](#), [version 2.1](#) and [version 3](#)".

ステップ 9 : アップグレードが正常に完了したら、FINISHボタンをクリックしてログイン画面に

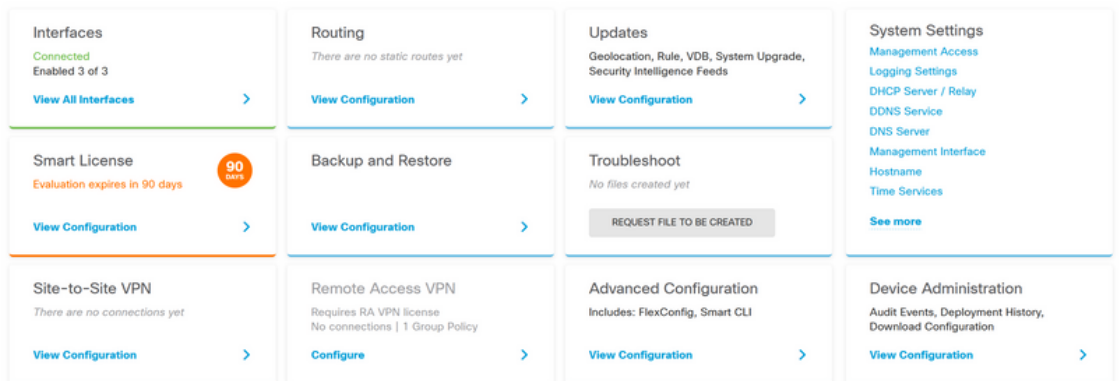
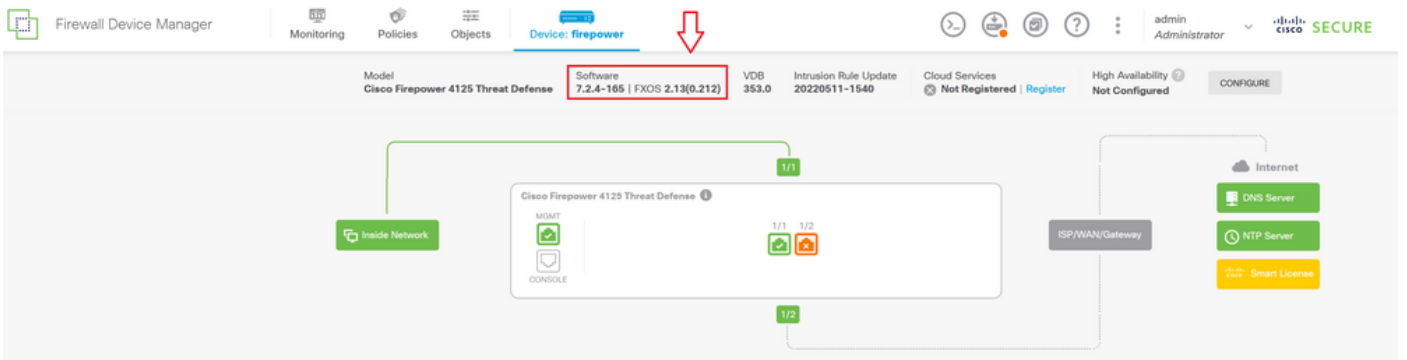
戻ります。



© 2015-2023 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc.  
This product contains some software licensed under the "GNU Lesser General Public License, versions: 2, 2.1 and 3" provided with ABSOLUTELY NO WARRANTY under the terms of "GNU Lesser General Public License, version 2.0, version 2.1.0 and version 3.0".

## 検証

アップグレードが完了したら、Firepower Device Manager(FDM)にログインして現在のバージョンを検証できます。次の情報が概要ダッシュボードに表示されます。



CLIを使用してアップグレードの検証を実行するには、次の手順を使用できます。



I. FTDの管理IPを使用してSSHセッションを作成します。

II. シャーシの現在のバージョンを確認するには、show versionコマンドを使用します。

推奨される手順の例：

```
Copyright 2004-2023, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.12.0 (build 499)
Cisco Firepower 4125 Threat Defense v7.2.4 (build 165)

> show version
-----[ firepower ]-----
Model          : Cisco Firepower 4125 Threat Defense (76) Version 7.2.4 (Build 165)
UUID           : e55a326e-25cd-11ee-b261-8d0ffe6dde59
LSP version    : lsp-rel-20220511-1540
VDB version    : 353
-----

> █
```

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。