

# Mise à niveau de Secure Firewall Threat Defense à l'aide de Firewall Device Manager

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Avant de commencer](#)

[Configurer](#)

[Validation](#)

---

## Introduction

Ce document décrit un exemple de mise à niveau de Cisco Secure Firewall Threat Defense (FTD) à l'aide de Firewall Device Manager (FDM).

## Conditions préalables

### Exigences

Cisco recommande de connaître les sujets suivants :

- Il n'existe aucune exigence spécifique pour ce guide

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Firepower 4125 exécutant FTD version 7.2.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Les exigences spécifiques de ce document sont les suivantes :

- Connectivité à l'IP de gestion du FTD

- Le package de mise à niveau FTD (.REL.tar) précédemment téléchargé depuis le portail Cisco Software

Cette procédure de mise à niveau est prise en charge sur les appliances :

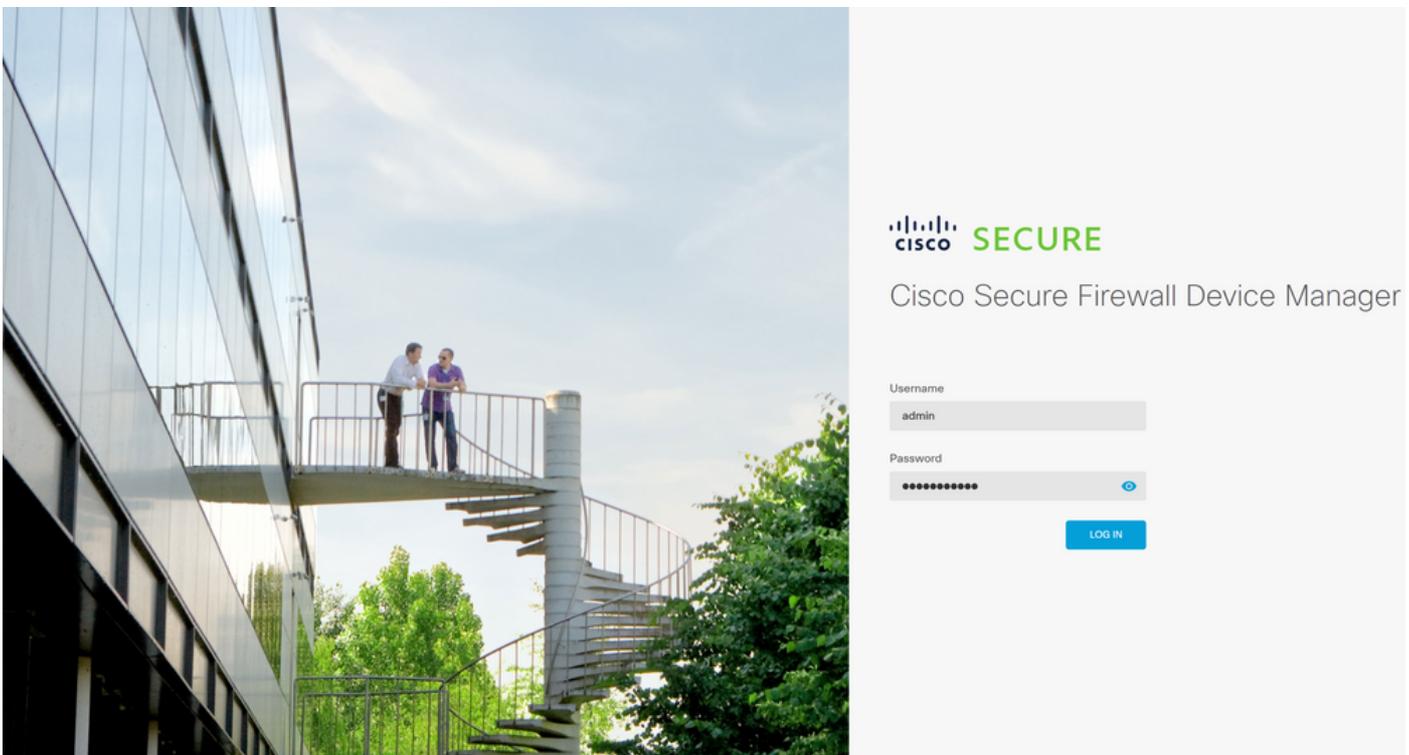
- Tout modèle Cisco Firepower exécutant le logiciel FTD configuré avec la gestion locale.

## Avant de commencer

1. Créez et téléchargez une sauvegarde des configurations FTD.
2. Validez le [chemin](#) de [mise à niveau](#) pour la version cible.
3. Téléchargez le package de mise à niveau depuis [Cisco Software Central](#).
4. Ne renommez pas le fichier de mise à niveau. Le système considère que les fichiers renommés ne sont pas valides.
5. Planifiez une fenêtre de maintenance pour la procédure de mise à niveau car le trafic est affecté.

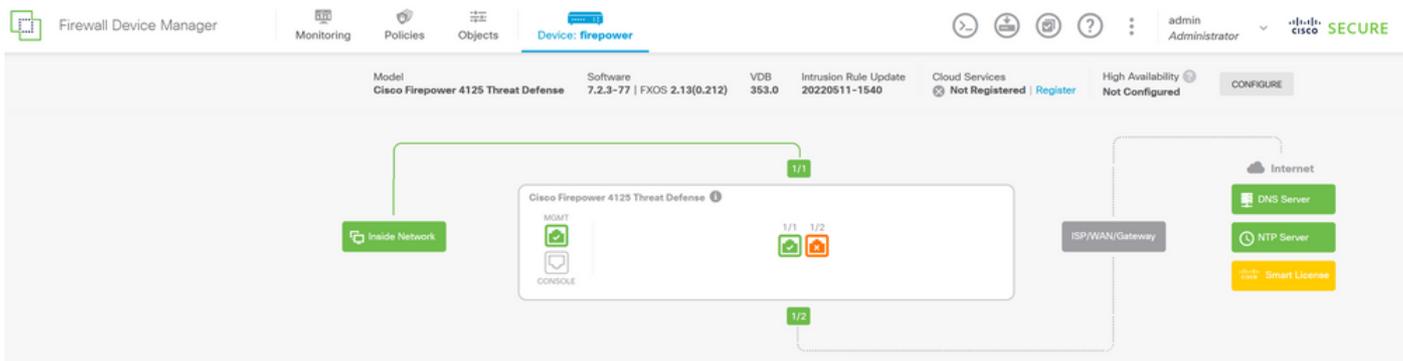
## Configurer

Étape 1. Connectez-vous au Gestionnaire de périphériques du pare-feu à l'aide de l'adresse IP de gestion du FTD :



© 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".

Étape 2. Cliquez sur View Configuration dans le tableau de bord du Gestionnaire de périphériques de pare-feu :



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

Étape 3. Cliquez sur le bouton Browse sous la section System Upgrade pour télécharger le package d'installation :

**⚠ Attention :** une fois que vous avez téléchargé le package de mise à niveau, BROWSE va afficher une animation pendant que le fichier est encore en cours de téléchargement. N'actualisez pas la page Web tant que le téléchargement n'est pas terminé.

Exemple de page de progression du téléchargement :

The screenshot shows the 'Device Summary' page for a 'firepower' device. Under the 'Updates' section, there are several update cards: 'Geolocation', 'VDB', 'Security Intelligence Feeds', 'System Upgrade', and 'Intrusion Rule'. The 'System Upgrade' card is the focus, displaying the current version (7.2.3-77) and the target version (2.13(0.212)). It includes an 'Important' note about compatibility and a message stating that no software upgrades are currently available on the system. A red arrow points to a file upload button in the 'System Upgrade' card, which is labeled 'Cisco\_FTD\_SSP\_Upgrade-7.2.4-165.ah.REL.tar'.

Étape 4. Une fois le téléchargement terminé, une fenêtre contextuelle s'affiche pour demander confirmation :

The screenshot shows the 'System Upgrade' card with a 'Confirmation' dialog box overlaid. The dialog box contains the text: 'The uploaded file will be staged for later installation. If you want to run the upgrade immediately, select the option below.' Below this text is a radio button labeled 'Run Upgrade immediately on upload', which is selected. There are 'CANCEL' and 'OK' buttons at the bottom of the dialog box. In the background, the 'System Upgrade' card shows the file 'Cisco\_FTD\_SSP\_Upgrade-7.2.4-165.s...' and the 'UPGRADE NOW' button.

 Remarque : vous pouvez vérifier l'option Exécuter la mise à niveau immédiatement lors du téléchargement au cas où vous souhaiteriez procéder directement à la mise à niveau, mais notez que cela va ignorer la vérification de préparation qui peut fournir des informations sur les conflits sur la mise à niveau afin d'éviter une défaillance.

Étape 5. Cliquez sur Run Upgrade Readiness Check pour effectuer une pré-validation de la mise à niveau afin d'éviter un échec de la mise à niveau :

Firewall Device Manager

Monitoring Policies Objects **Device: firepower**

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

UPGRADE 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](#)

Remarque : vous pouvez vérifier que le test de préparation s'est terminé correctement à partir de la liste des tâches.

Exemple d'une vérification de préparation réussie :

Firewall Device Manager

Monitoring Policies Objects **Device: firepower**

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 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** [Run Upgrade Readiness Check](#)

UPGRADE 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](#)

**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 |         |

Étape 6. Cliquez sur le bouton UPGRADE NOW pour procéder à la mise à niveau logicielle :

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

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.

File Cisco\_FTD\_SSP\_Upgrade-7.2.4-165.s...  
19 Jul 2023 11:49 AM

Upgrade to 7.2.4-165

Readiness Check **Precheck Success** Run Upgrade Readiness Check  
19 Jul 2023 11:54 AM

**UPDATE NOW** Reboot required

Étape 7. Dans la fenêtre contextuelle, sélectionnez CONTINUE pour poursuivre la mise à niveau :

Firewall Device Manager

Monitoring Policies Objects **Device: fire**

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 ve

**Confirm System Upgrade**

Before starting the upgrade:

- Do not start a system restore at the same time as a system upgrade.
- Do not reboot the system during the upgrade. The system automatically reboots at the appropriate time during upgrade if a reboot is necessary.
- 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.

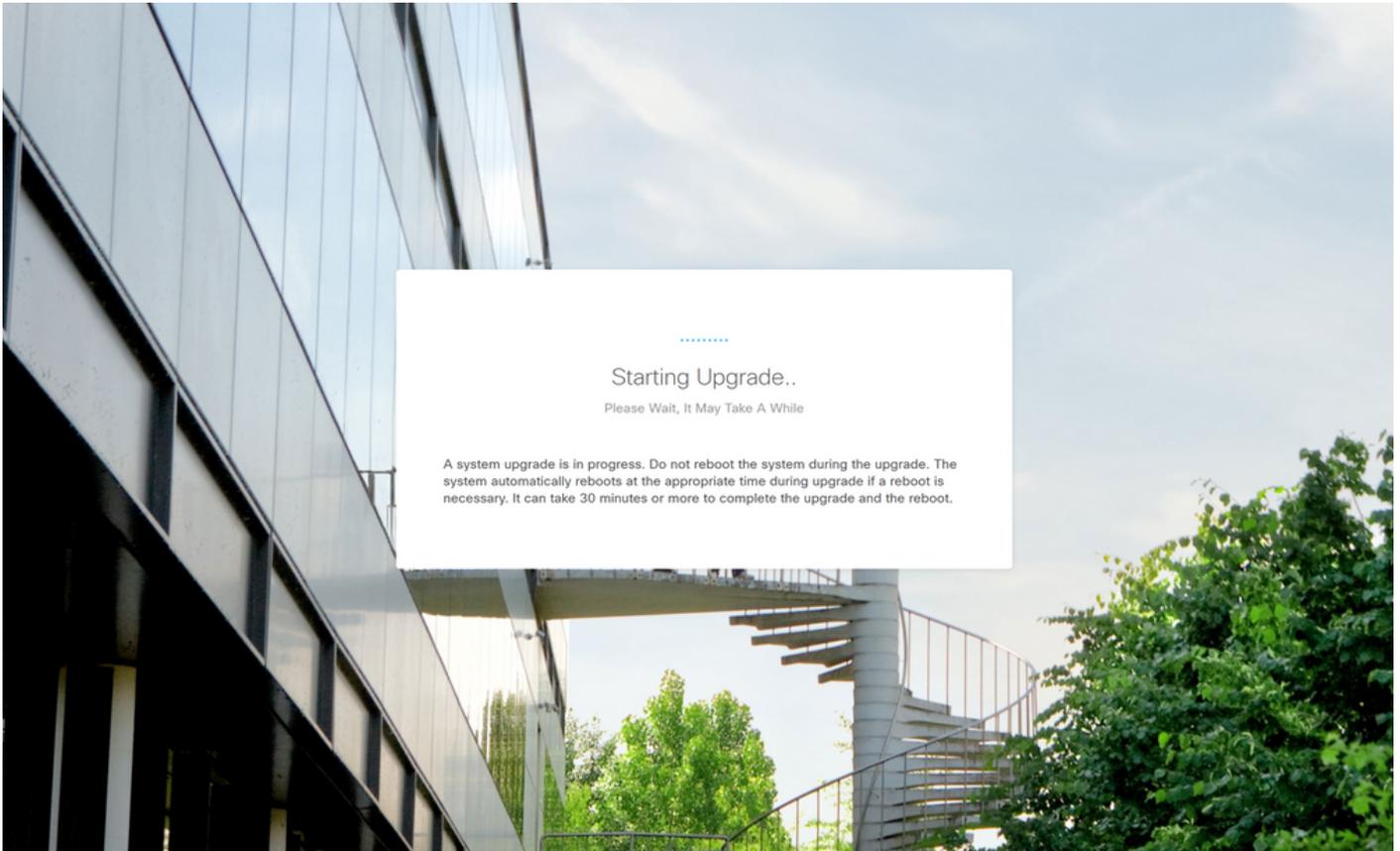
UPGRADE OPTIONS

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

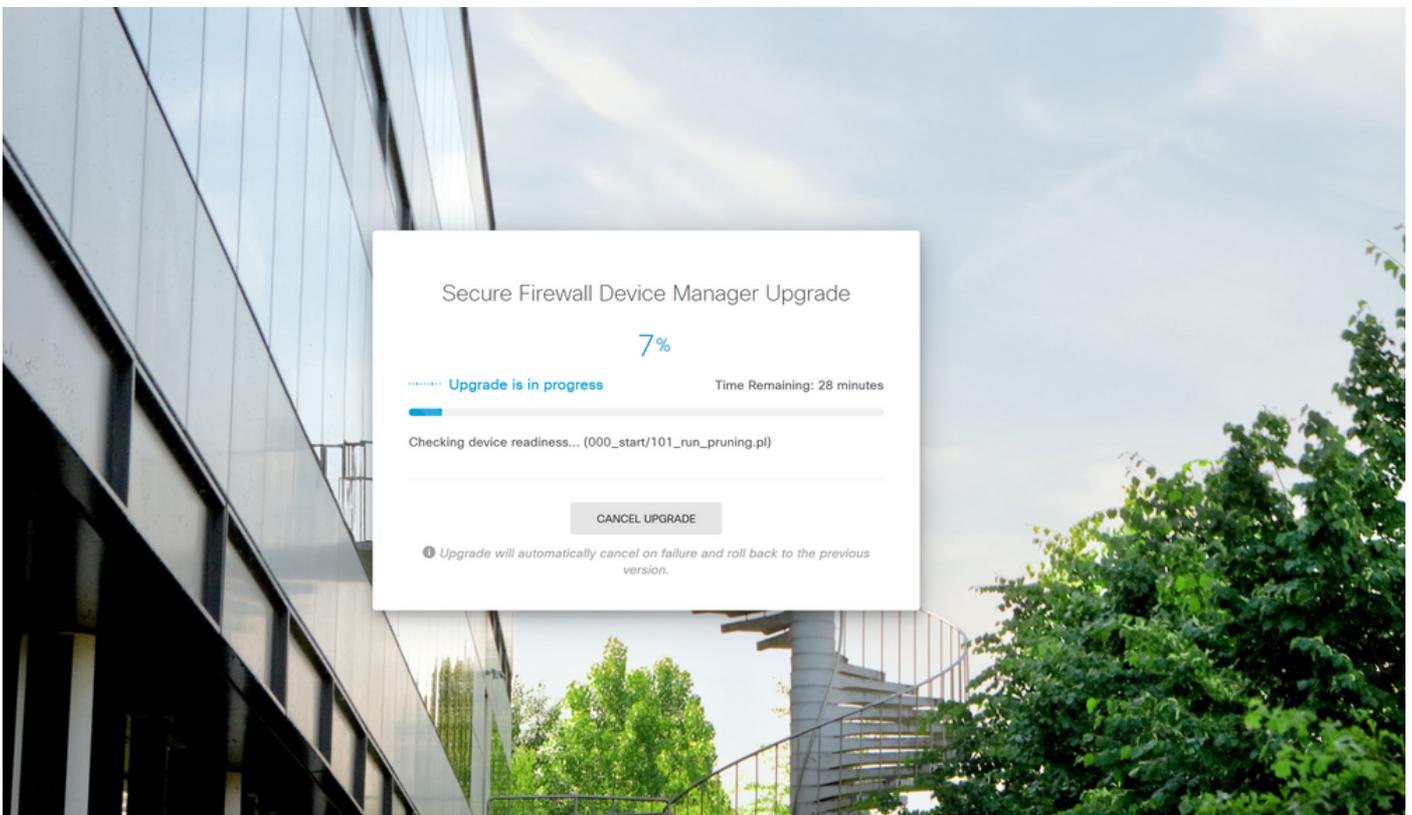
CANCEL **CONTINUE**

 Remarque : l'option de restauration est activée par défaut. Il est conseillé de conserver cette option afin de rétablir toute configuration de mise à niveau en cas de problème lors de la mise à niveau.

Étape 8. Vous êtes redirigé vers une page où la progression de la mise à niveau va s'afficher :



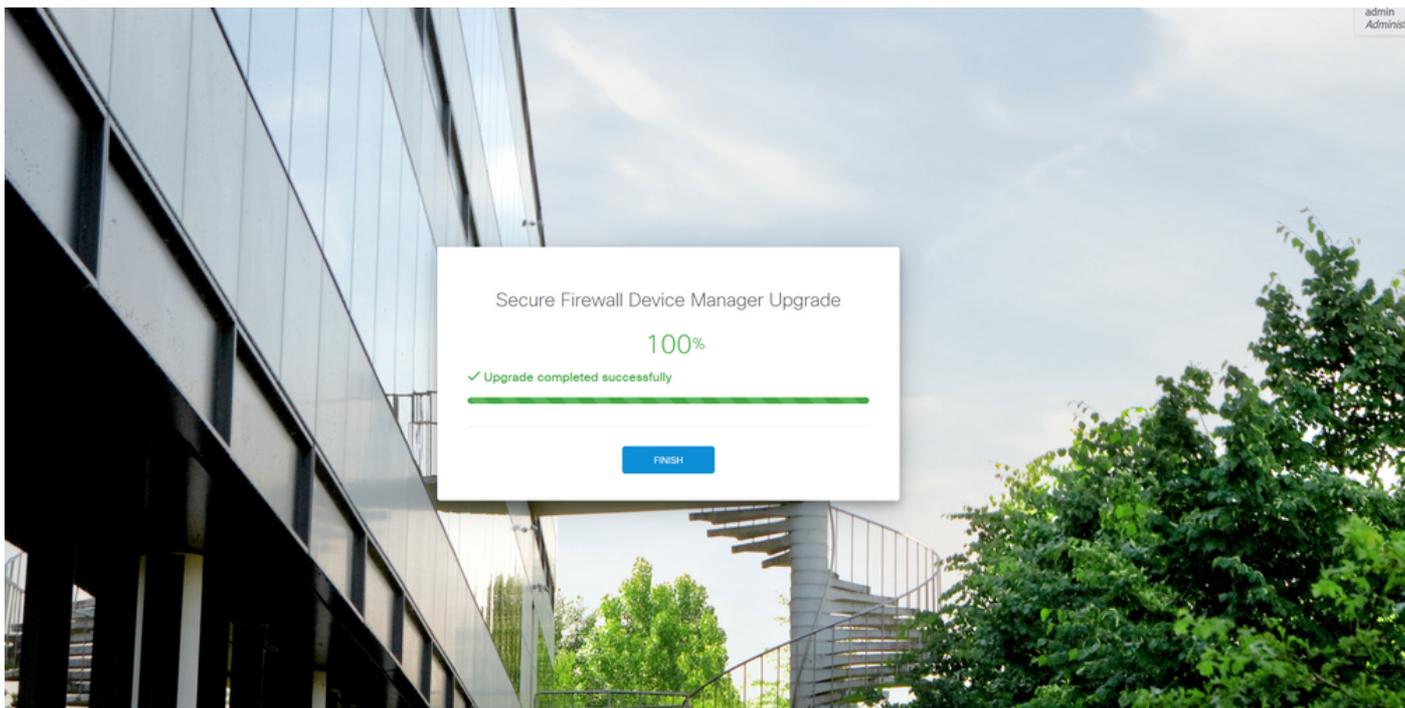
Exemple de la page de progression :



© 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](#)".

Étape 9. Cliquez sur le bouton FINISH une fois la mise à niveau terminée avec succès pour

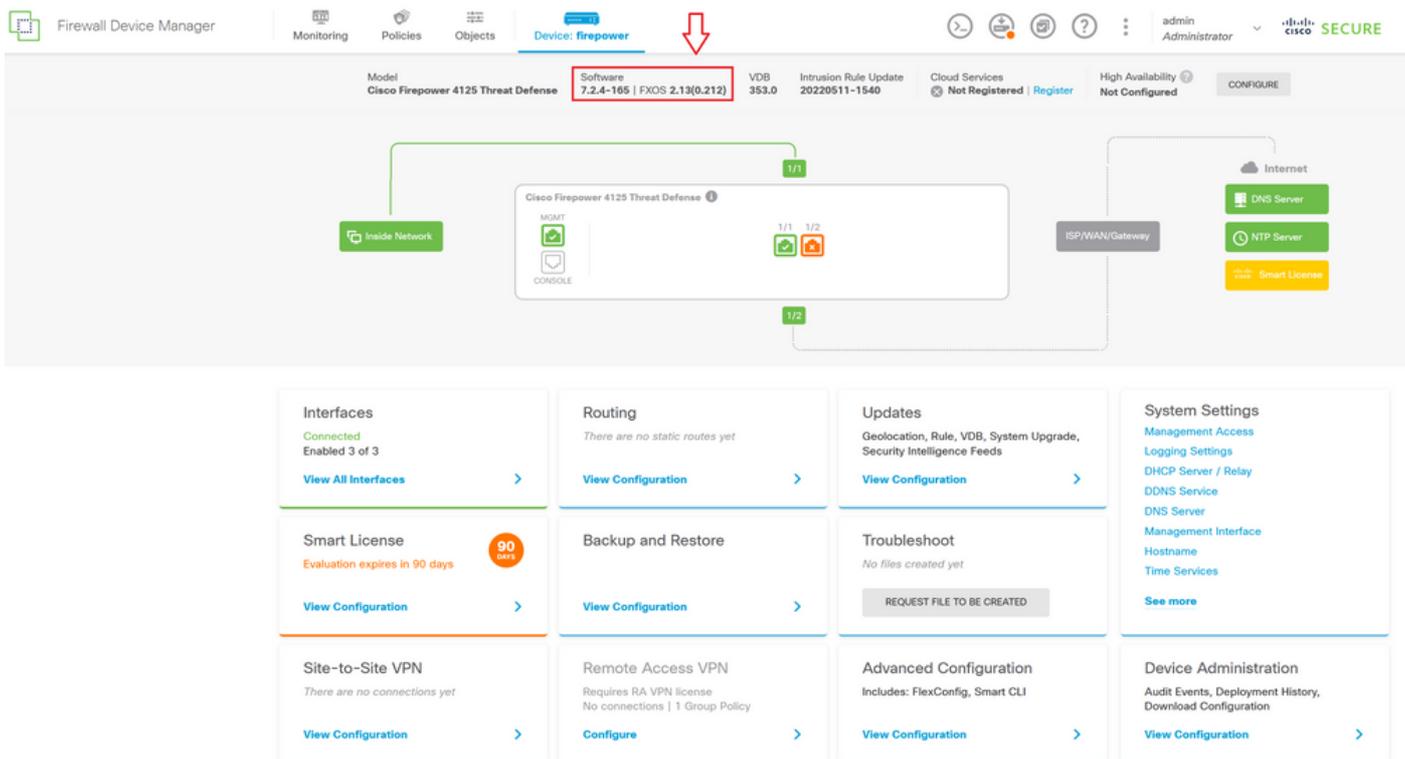
revenir à l'écran de connexion :



© 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 [L], version 2.1 [L] and version 3 [L]".

## Validation

Une fois la mise à niveau terminée, vous pouvez vous connecter au Gestionnaire de périphériques Firepower pour valider la version actuelle. Celle-ci s'affiche dans le tableau de bord Présentation :



Pour effectuer une validation de mise à niveau via l'interface de ligne de commande, procédez comme suit :

I. Créez une session SSH à l'aide de l'adresse IP de gestion du FTD.

II. Utilisez la commande show version pour valider la version actuelle sur votre châssis.

Exemple de la procédure proposée :

```
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
-----
> █
```

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.