

Aggiornamento di Secure Firewall Threat Defense Fusing Firewall Device Manager

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Operazioni preliminari](#)

[Configurazione](#)

[Convalida](#)

Introduzione

Questo documento descrive un esempio di aggiornamento di Cisco Secure Firewall Threat Defense (FTD) con Firewall Device Manager (FDM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Nessun requisito specifico previsto per questa guida

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Firepower 4125 con FTD versione 7.2.3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

I requisiti specifici per questo documento includono:

- Connettività all'IP di gestione dell'FTD
- Il pacchetto di aggiornamento FTD (**.REL.tar**) precedentemente scaricato dal portale Cisco del software

Questa procedura di aggiornamento è supportata sugli accessori:

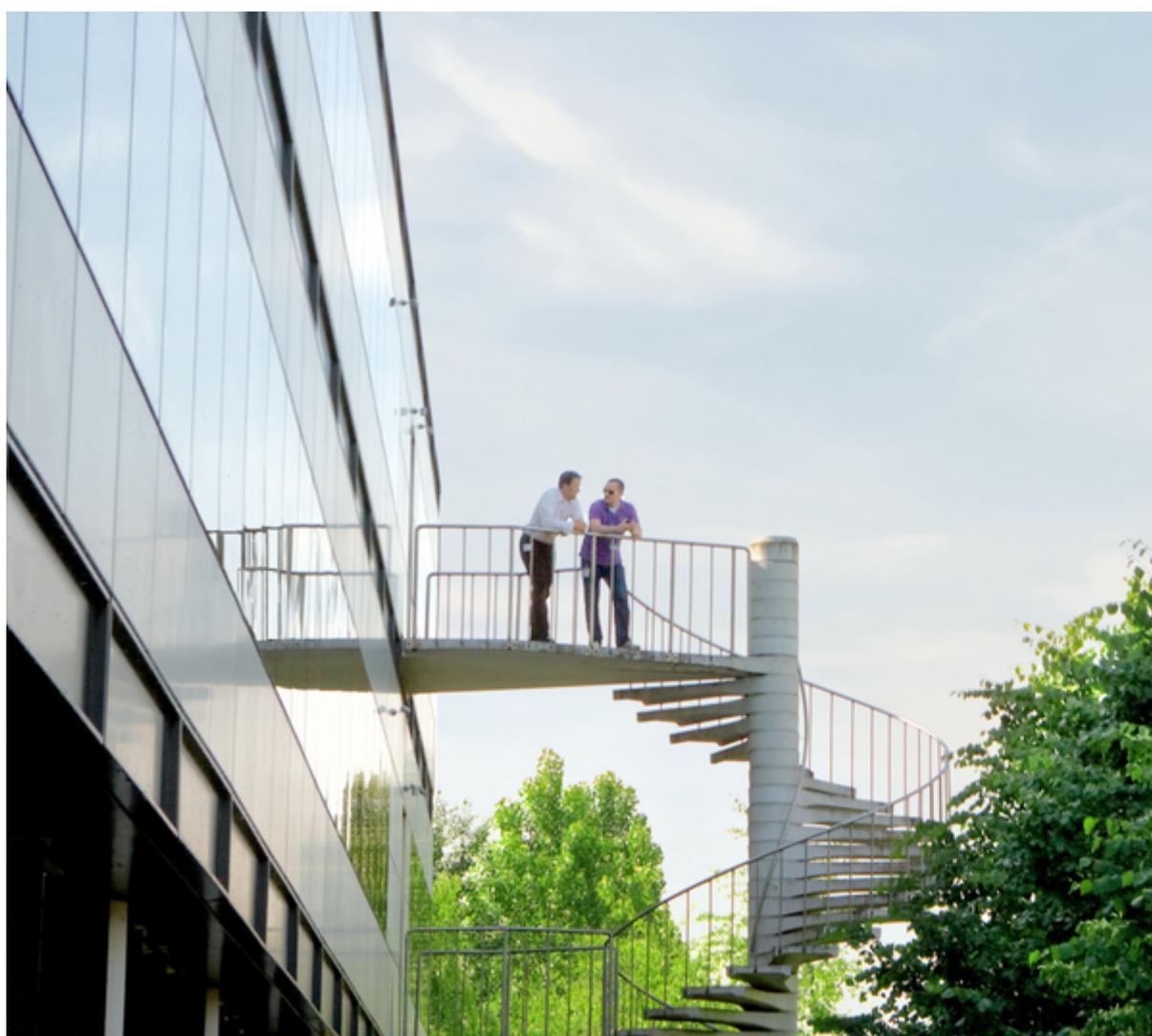
- Qualsiasi modello Cisco Firepower con software FTD configurato con gestione locale.

Operazioni preliminari

1. Creare e scaricare un backup delle configurazioni FTD.
2. Convalidare il [percorso di aggiornamento](#) per la versione di destinazione.
3. Scaricare il pacchetto di aggiornamento da [Cisco Software Central](#).
4. Non rinominare il file di aggiornamento. Il sistema considera i file rinominati non validi.
5. Pianificare una finestra di manutenzione per la procedura di aggiornamento in quanto il traffico è interessato.

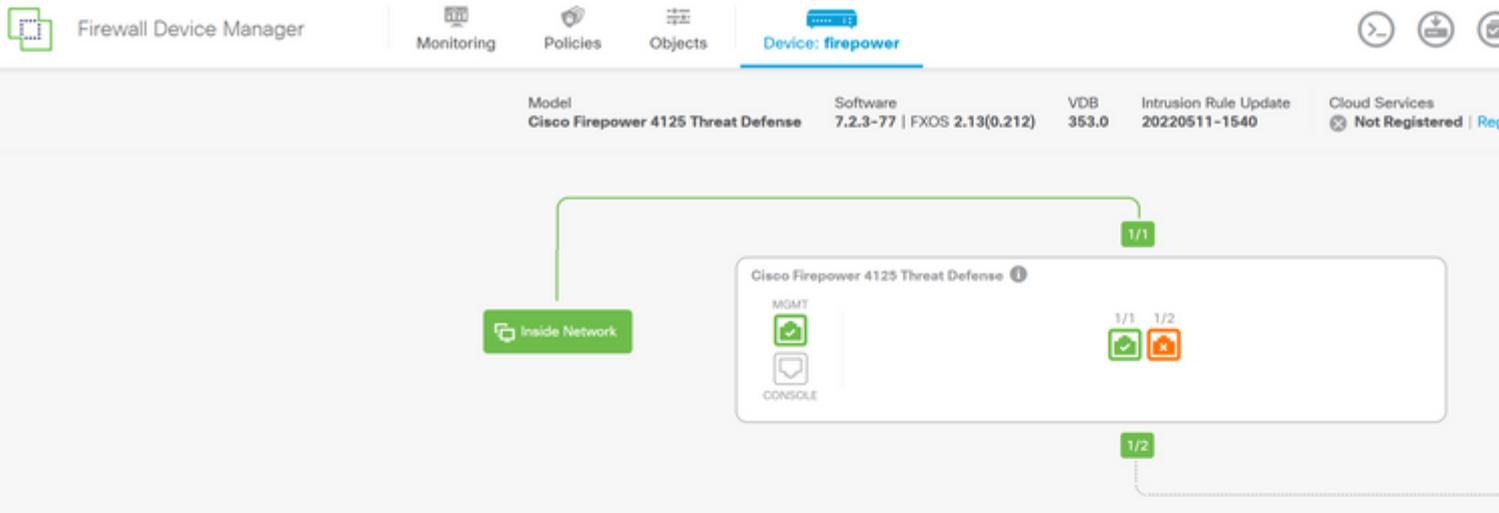
Configurazione

Passaggio 1. Accedere a Gestione periferiche firewall utilizzando l'IP di gestione dell'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, version 2.0 or later" (LGPLv2). ABSOLUTELY NO WARRANTY under the terms of "GNU Lesser General Public License, version 2.0 or later" (LGPLv2).

Passaggio 2. Fare clic su **View Configuration** (Visualizza configurazione) nel dashboard di Gestione periferiche firewall:



Interfaces Connected Enabled 3 of 3 View All Interfaces	Routing <i>There are no static routes yet</i> View Configuration	Updates Geolocation, Rule, VDB, System Up Security Intelligence Feeds View Configuration
Smart License Evaluation expires in 90 days View Configuration	Backup and Restore View Configuration	Troubleshoot <i>No files created yet</i> REQUEST FILE TO BE CREATED
Site-to-Site VPN <i>There are no connections yet</i> View Configuration	Remote Access VPN Requires RA VPN license No connections 1 Group Policy Configure	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration

Passaggio 3. Fare clic sul pulsante Browse (Sfoglia) nella sezione System Upgrade (Aggiornamento del sistema) per caricare il pacchetto di installazione:

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)

ImportantMake sure the threat defense version is compatible with the FXOS version.
[Learn more](#)*There are no software upgrades available on the system.**Upload an upgrade file to install.*

BROWSE



Intrusion Rule 20220511-15

Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD

Attenzione: una volta caricato il pacchetto di aggiornamento, **BROWSE** visualizzerà un'animazione mentre il file è ancora in fase di caricamento. Non aggiornare la pagina Web fino al termine del caricamento.

Esempio di pagina di avanzamento del caricamento:

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](#)

There are no software upgrades available on the system.
Upload an upgrade file to install.

Cisco_FTD_SSP_Upgrade-7.2.4-165.REL.tar

Intrusion Rule 20220511-154
Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD

Passaggio 4. Al termine del caricamento, viene visualizzata una finestra popup che richiede di confermare:

Firewall Device Manager

Monitoring Policies Objects Device: fire

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	Uploaded	Action
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 20220511-154
Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD

Confirmation

The uploaded file will be staged for later installation. If you want to run the upgrade immediately, select the option below.

Run Upgrade immediately on upload

CANCEL OK

Nota: è possibile selezionare l'opzione **Esegui aggiornamento immediatamente al caricamento** se si desidera procedere direttamente con l'aggiornamento. Tuttavia, questa opzione salterà il **Controllo preparazione** che può fornire informazioni dettagliate sui conflitti nell'aggiornamento che impediscono un errore.

Passaggio 5. Fare clic su Esegui controllo preparazione aggiornamento per eseguire una preconvalida dell'aggiornamento per evitare errori:

The screenshot shows the 'Firewall Device Manager' interface for a device named 'firepower'. The 'Updates' section is active, displaying several update cards: 'Geolocation', 'VDB', 'Security Intelligence Feed', and 'Intrusion Rule'. The 'System Upgrade' section is the primary focus, showing the current version (7.2.3-77) and the target version (7.2.4-165). An 'Important' message states: 'Make sure the threat defense version is compatible with the FXOS version.' Below this, a table lists the upgrade file: 'Cisco_FTD_SSP_Upgrade-7.2.4-165.s...' with a 'Replace file' option. The 'Readiness Check' status is 'Not Performed Yet', and a red box highlights the 'Run Upgrade Readiness Check' button, which is pointed to by a red arrow. Other buttons include 'UPDATE FROM CLOUD' and 'UPGRADE NOW'.

Nota: è possibile verificare che il controllo di idoneità sia stato completato correttamente dall'Elenco task.

Esempio di verifica di fattibilità completata:

The screenshot displays the Firewall Device Manager interface. A 'Task List' modal window is open, showing a summary of tasks: 1 total, 0 running, 1 completed, and 0 failures. The task list contains one entry: 'Upgrade Readiness' with a start time of 19 Jul 2023 11:52 AM and an end time of 19 Jul 2023 11:54 AM. The status is 'Upgrade Readiness Check Completed Successfully'.

In the background, the 'System Upgrade' section is visible. It shows the current version of threat defense (7.2.3-77) and FXOS (2.13(0.212)). An important message states: 'Make sure the threat defense version is compatible with the FXOS version.' A file 'Cisco_FTD_SSP_Upgrade-7.2.4-165.s...' is listed with a 'Replace file' link. The upgrade target is '7.2.4-165'. A 'Readiness Check' shows 'Precheck Success' with a 'Run Upgrade Readiness Check' link. At the bottom, there is an 'UPGRADE NOW' button and a note 'Reboot required'.

Passaggio 6. Fare clic sul pulsante UPGRADE NOW per procedere con l'aggiornamento del software:

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 Feed

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... 🗑️ Replace file 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

UPGRADE NOW ⓘ Reboot required

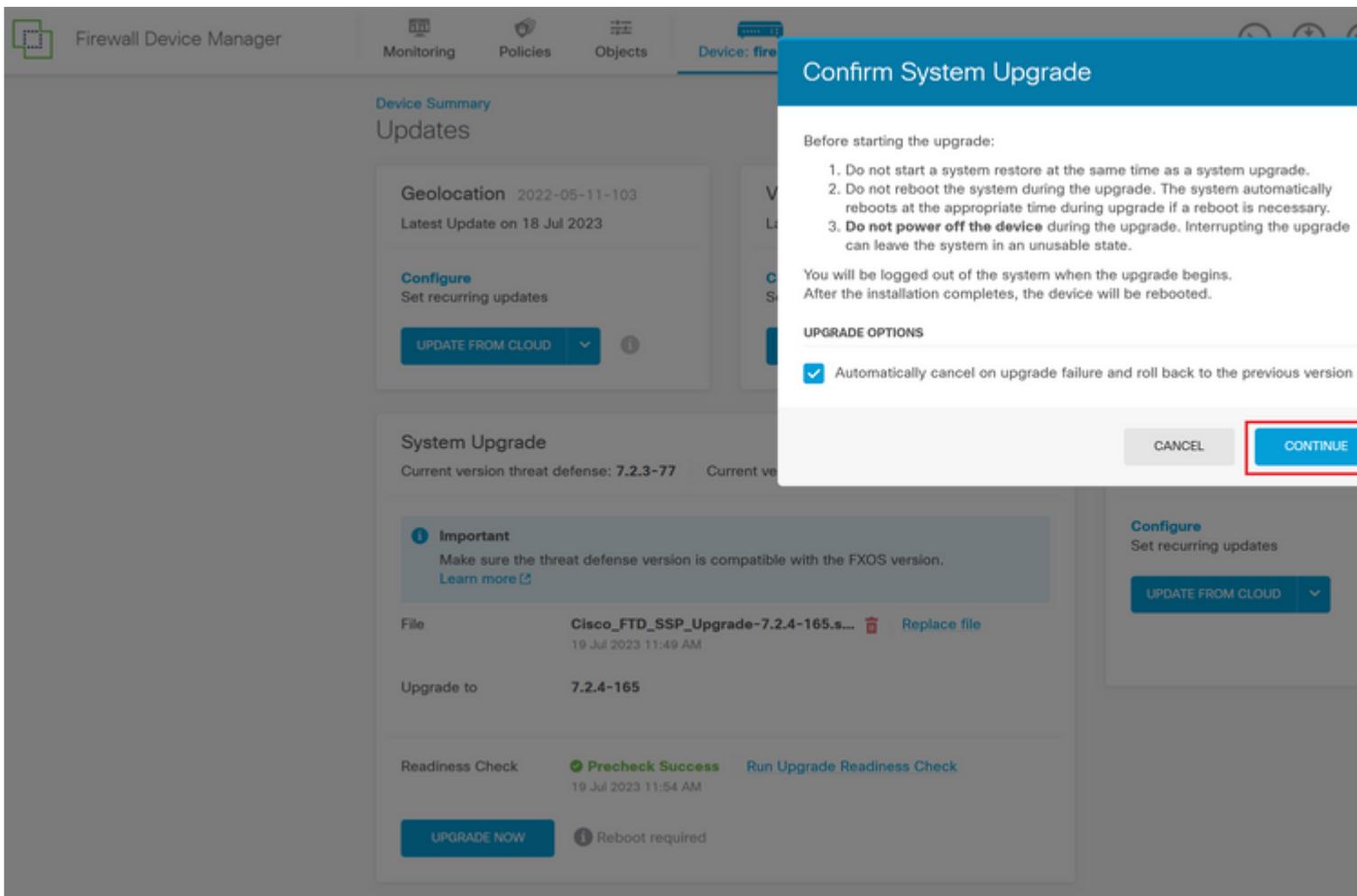
Intrusion Rule 20220511-15
Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD ⌵

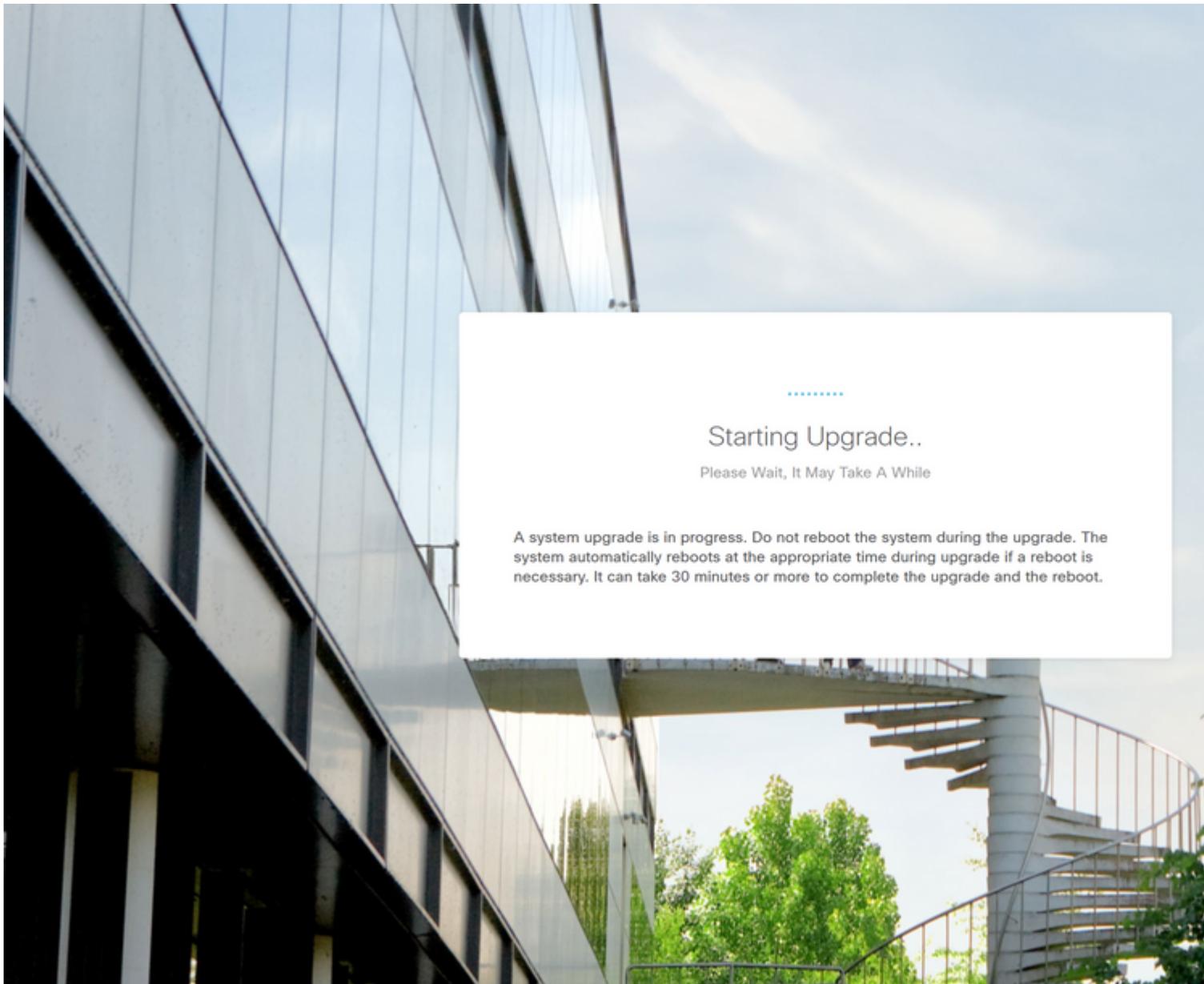


Passaggio 7. Nella finestra popup selezionare CONTINUE (CONTINUA) per procedere con l'aggiornamento:

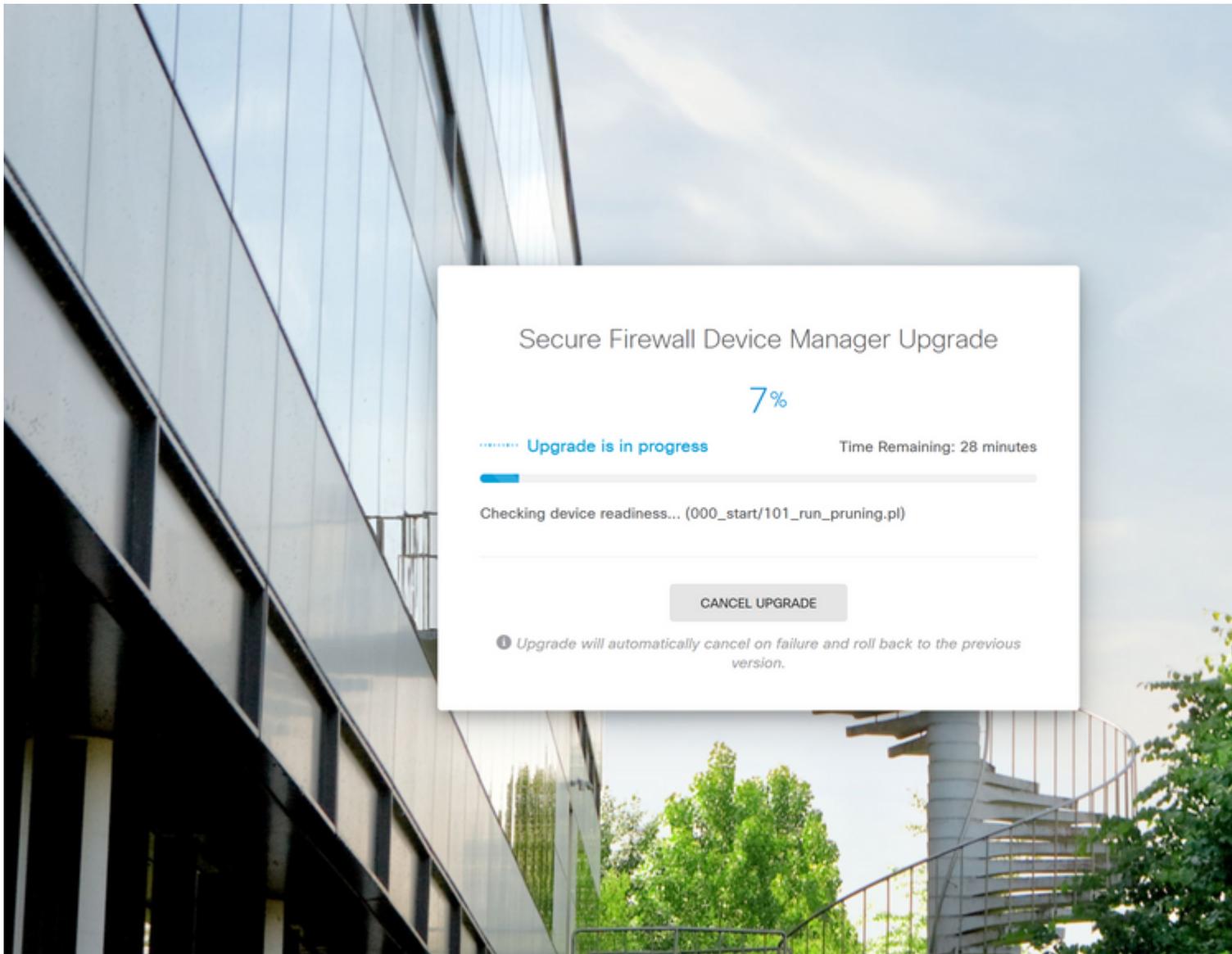


Nota: l'opzione di rollback è abilitata per impostazione predefinita. Si consiglia di mantenere questa opzione per ripristinare qualsiasi configurazione di aggiornamento in caso di problemi durante l'aggiornamento.

Passaggio 8. Viene visualizzata una pagina in cui verrà visualizzato lo stato dell'aggiornamento:

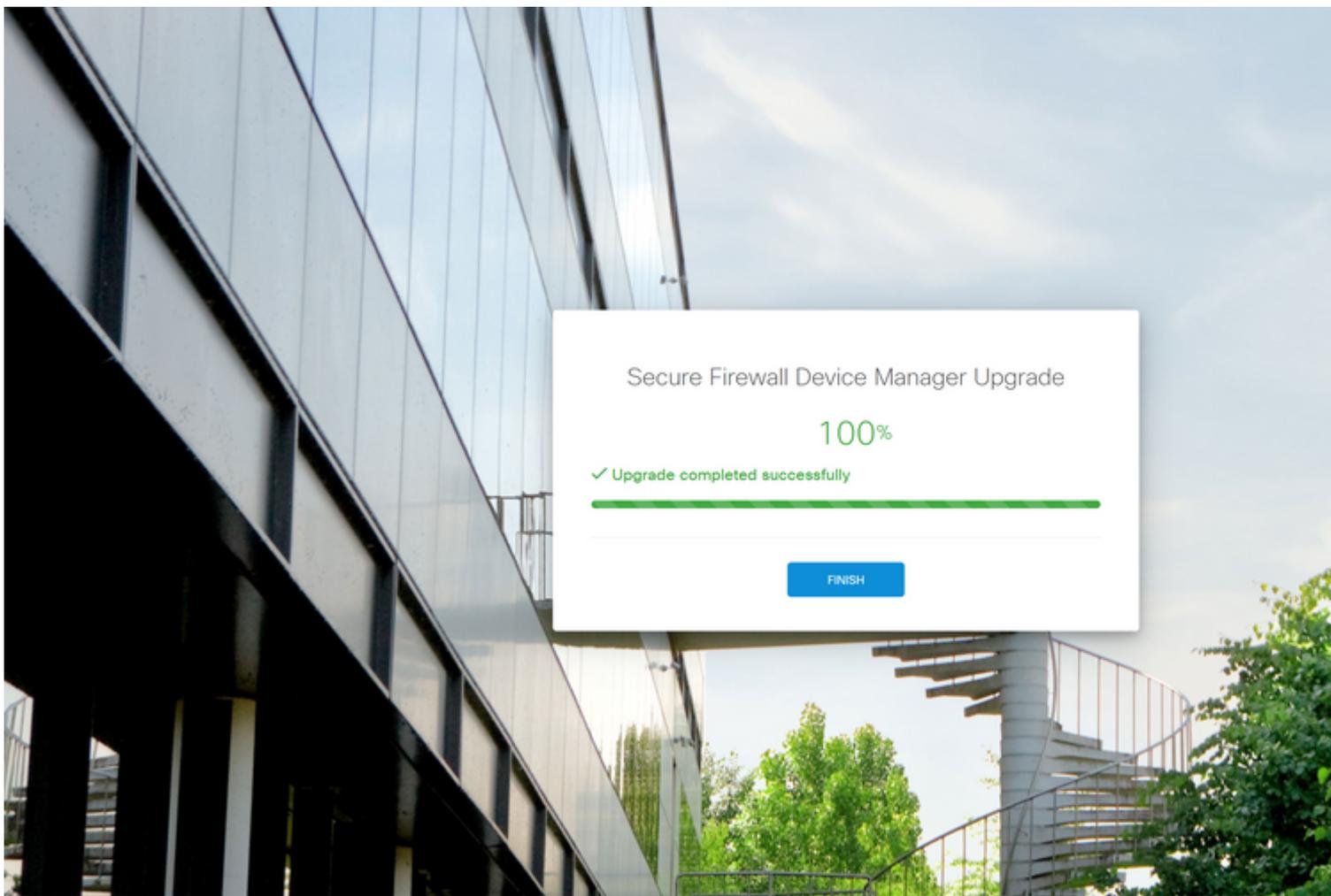


Esempio di pagina di avanzamento:



© 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](#)".

Passaggio 9. Fare clic sul pulsante FINISH al termine dell'aggiornamento per tornare alla schermata di accesso:



© 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](#)".

Convalida

Al termine dell'aggiornamento, è possibile accedere a Gestione periferiche di Firepower per convalidare la versione corrente, che viene visualizzata nel dashboard Panoramica:

Per eseguire una convalida di aggiornamento tramite CLI, è possibile utilizzare i seguenti passaggi:

- I. Creare una sessione SSH usando l'IP di gestione dell'FTD.
- II. Usare il comando **show version** per convalidare la versione corrente sullo chassis.

Esempio della procedura suggerita:

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) Ve  
UUID                 : e55a326e-25cd-11ee-b261-8d0ffe6dde59  
LSP version          : lsp-rel-20220511-1540  
VDB version          : 353  
-----
```

> █

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).