

Upgrade von Secure Firewall Threat Defense Firewall Device Manager

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Vorbereitungen](#)

[Konfigurieren](#)

[Validierung](#)

Einleitung

Dieses Dokument beschreibt ein Beispiel für ein Cisco Secure Firewall Threat Defense (FTD)-Upgrade mit dem Firewall Device Manager (FDM).

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Für diesen Leitfadens gibt es keine spezifischen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Firepower 4125 mit FTD-Version 7.2.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Spezifische Anforderungen für dieses Dokument:

- Verbindung zur Verwaltungs-IP des FTD
- FTD-Upgrade-Paket (**.REL.tar**), das zuvor vom Software Cisco Portal heruntergeladen wurde

Dieses Upgrade-Verfahren wird auf folgenden Appliances unterstützt:

- Alle Cisco Firepower-Modelle mit FTD-Software, die mit lokaler Verwaltung konfiguriert wurde.

Vorbereitungen

1. Erstellen Sie ein Backup der FTD-Konfigurationen, und laden Sie es herunter.
2. Validieren Sie den [Upgrade-Pfad](#) für die Zielversion.
3. Laden Sie das Upgrade-Paket von [Cisco Software Central herunter](#).
4. Benennen Sie die Upgrade-Datei nicht um. Das System betrachtet umbenannte Dateien als ungültig.
5. Planen Sie ein Wartungsfenster für das Upgrade-Verfahren, da der Datenverkehr betroffen ist.

Konfigurieren

Schritt 1: Melden Sie sich mit der Verwaltungs-IP des FTD beim Firewall-Gerätemanager an:



 **SECURE**

Cisco Secure

Username

admin

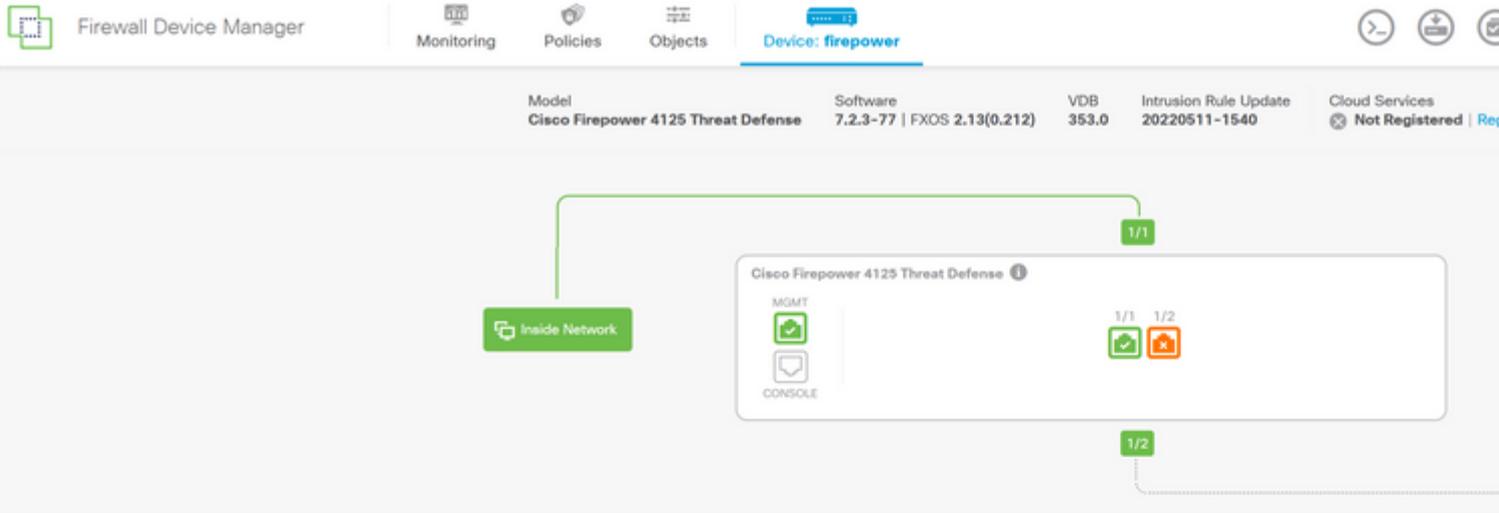
Password

••••••••••

© 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 2.1 or later".
ABSOLUTELY NO WARRANTY under the terms of "GNU Lesser General Public License, version 2.1 or later".

Schritt 2: Klicken Sie auf **View Configuration** im Firewall Device Manager Dashboard:



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

Schritt 3: Klicken Sie auf die Schaltfläche **Durchsuchen im Abschnitt System Upgrade, um das Installationspaket hochzuladen:**

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.*

BROWSE

Intrusion Rule 20220511-15

Latest Update on 18 Jul 2023

Configure

Set recurring updates

UPDATE FROM CLOUD ▾ ⓘ



Achtung: Nachdem Sie das Upgrade-Paket hochgeladen haben, zeigt **BROWSE** eine Animation an, während die Datei noch hochgeladen wird. Aktualisieren Sie die Webseite erst, wenn der Upload beendet ist.

Beispiel für die Fortschrittseite beim Hochladen:

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.sh.REL.tar

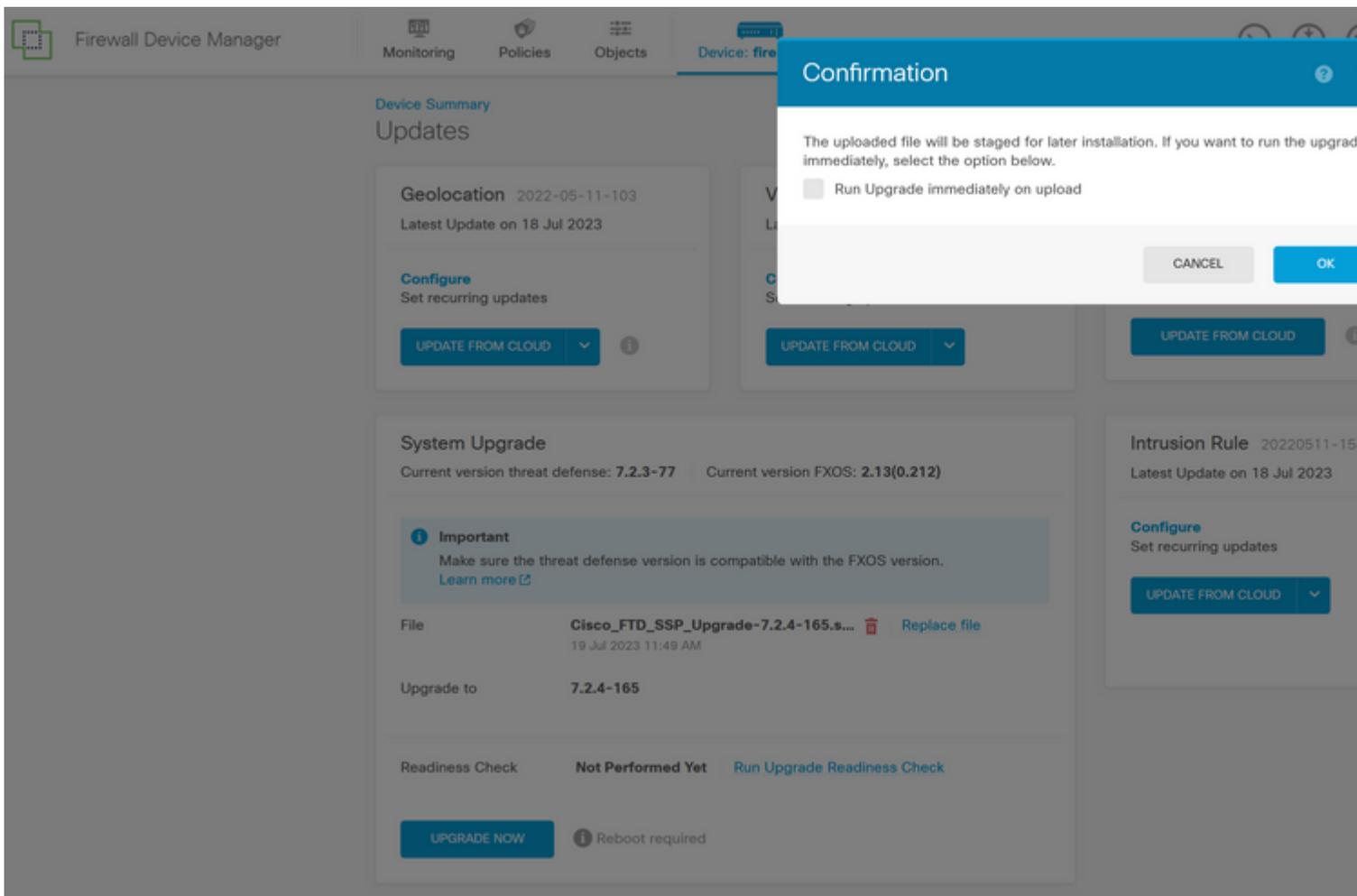
Intrusion Rule 20220511-154

Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD

Schritt 4: Wenn der Upload abgeschlossen ist, wird ein Popup-Fenster angezeigt, in dem Sie zur Bestätigung aufgefordert werden:



Hinweis: Sie können die Option **Upgrade sofort beim Upload ausführen** aktivieren, falls Sie das Upgrade direkt fortsetzen möchten. Beachten Sie jedoch, dass dadurch die **Bereitschaftsprüfung** übersprungen wird, die Einblicke in Konflikte bezüglich des Upgrades liefern kann, das einen Fehler verhindert.

Schritt 5: Klicken Sie auf **Run Upgrade Readiness Check (Upgrade-Bereitschaftsprüfung ausführen)**, um eine Vorabvalidierung des Upgrades durchzuführen, um einen Upgrade-Fehler zu vermeiden:

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... 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 20220511-15
Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD

Hinweis: Sie können in der Aufgabenliste überprüfen, ob die Bereitschaftsprüfung erfolgreich abgeschlossen wurde.

Beispiel für eine erfolgreiche Bereitschaftsprüfung:

The screenshot displays the Firewall Device Manager interface. A 'Task List' modal is open, showing a summary of tasks: 1 total, 0 running, 1 completed, and 0 failures. The task list table contains one entry:

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

In the background, the 'System Upgrade' section is visible, 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.' A file 'Cisco_FTD_SSP_Upgrade-7.2.4-165.s...' is listed for replacement. The 'Readiness Check' shows a 'Precheck Success' status. A prominent 'UPGRADE NOW' button is present at the bottom of the upgrade section, with a note that a 'Reboot required'.

Schritt 6: Klicken Sie auf die Schaltfläche **JETZT AKTUALISIEREN**, um mit dem Software-Upgrade fortzufahren:

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

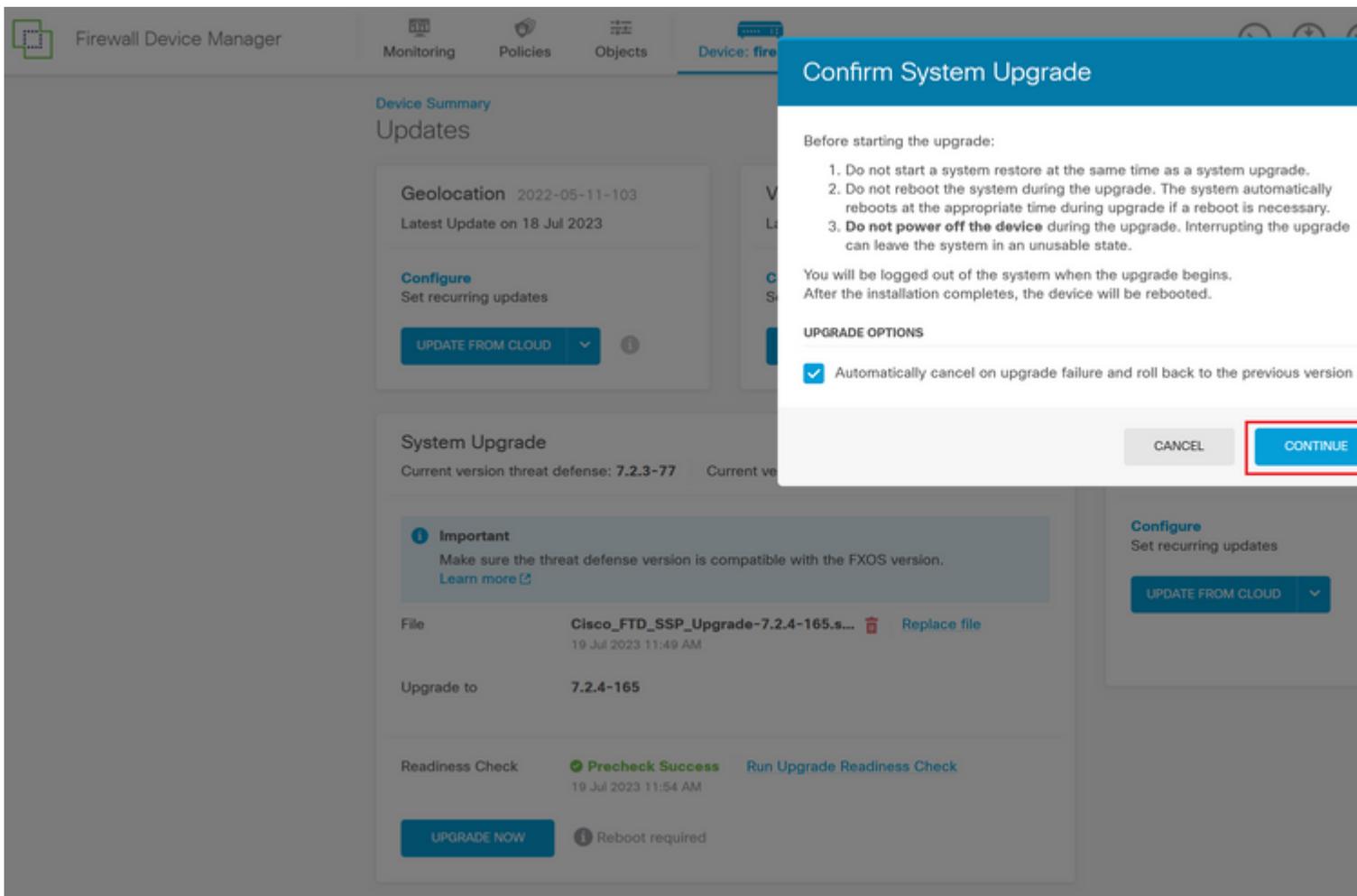
Intrusion Rule 20220511-15

Latest Update on 18 Jul 2023

Configure
Set recurring updates

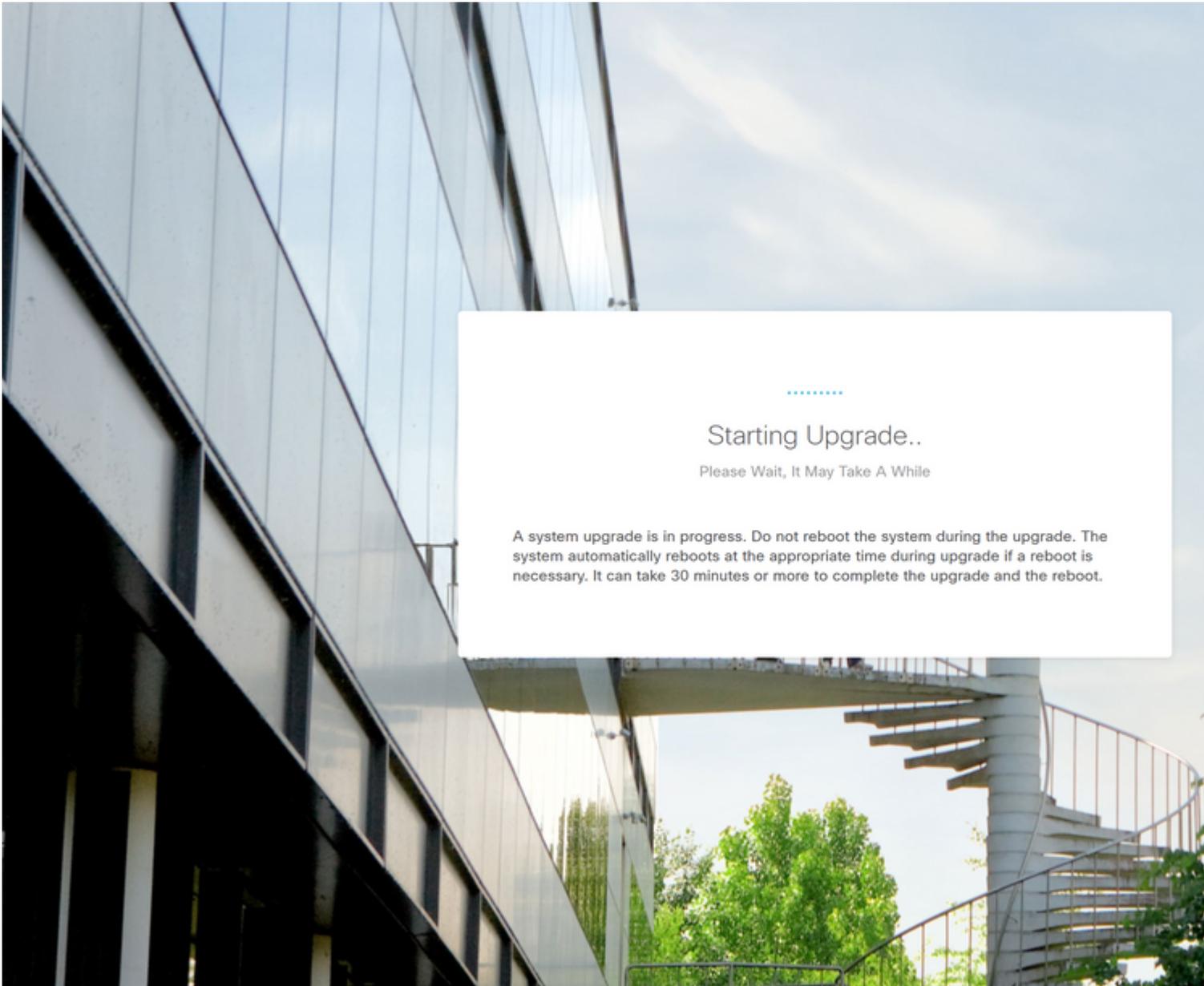
UPDATE FROM CLOUD

Schritt 7. Wählen Sie im Popup-Fenster die Option **WEITER**, um mit der Aktualisierung fortzufahren:

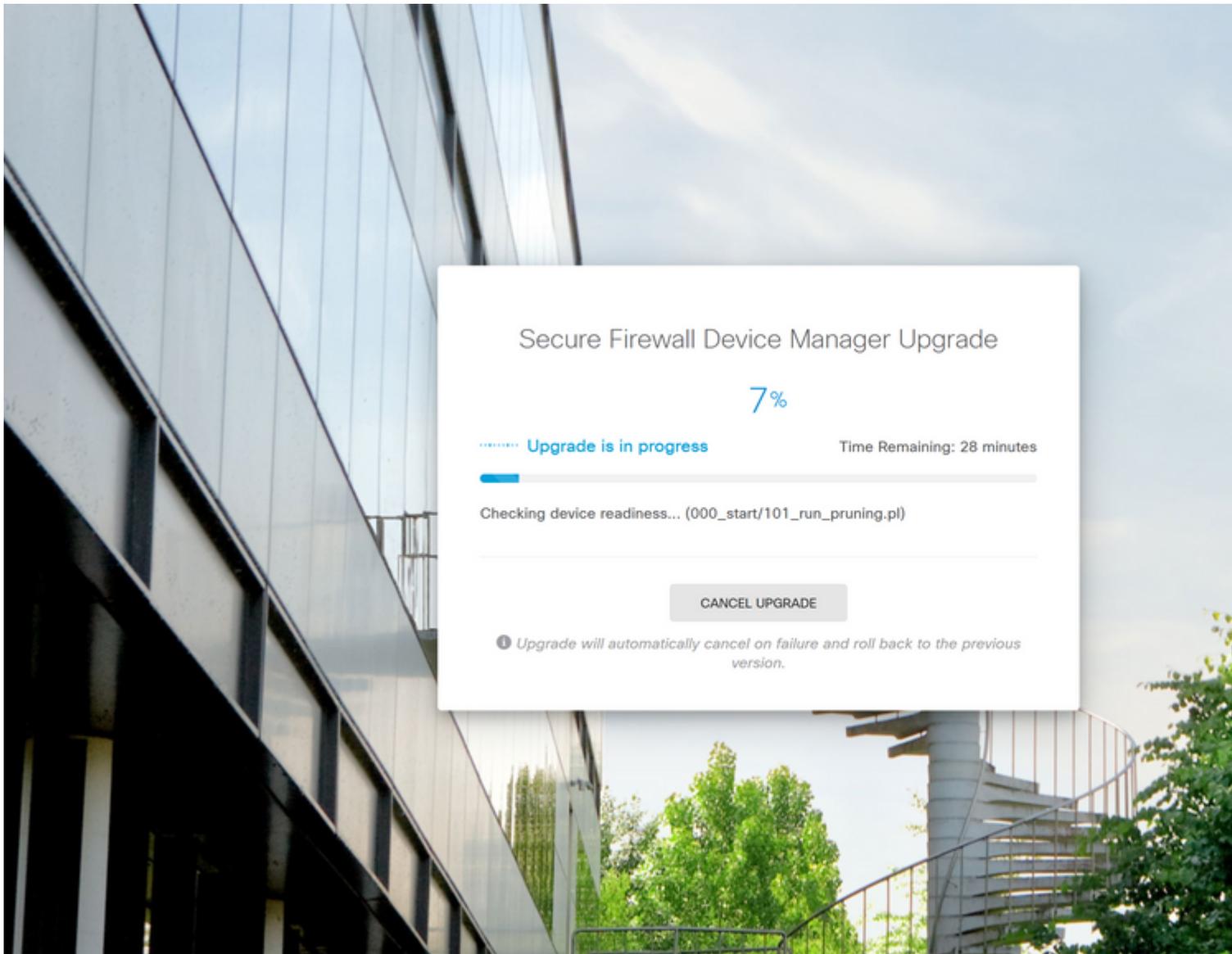


Hinweis: Die Option "Rollback" ist standardmäßig aktiviert. Es wird empfohlen, diese Option beizubehalten, um alle Upgrade-Konfigurationen zurückzusetzen, falls bei der Aktualisierung ein Problem auftritt.

Schritt 8: Sie werden auf eine Seite umgeleitet, auf der der Fortschritt der Aktualisierung angezeigt wird:

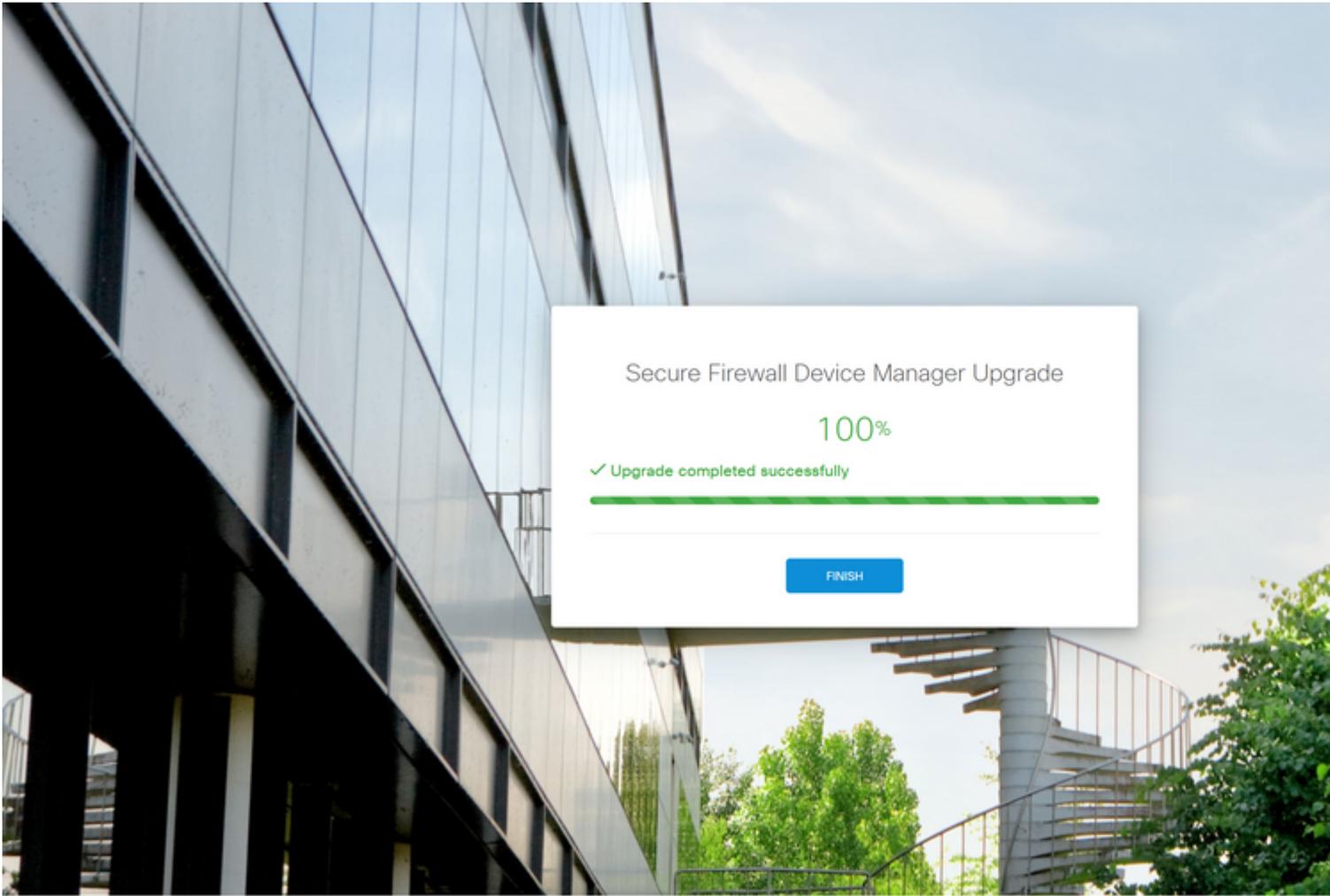


Beispiel der Fortschrittseite:



© 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](#)".

Schritt 9. Klicken Sie auf die Schaltfläche **FERTIG, nachdem das Upgrade erfolgreich abgeschlossen wurde, um zum Anmeldebildschirm zurückzukehren:**



© 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](#)".

Validierung

Wenn das Upgrade abgeschlossen ist, können Sie sich beim Firepower Geräte-Manager anmelden, um die aktuelle Version zu überprüfen. Dies wird im Übersichts-Dashboard angezeigt:

The screenshot shows the Firewall Device Manager interface for a Cisco Firepower 4125 Threat Defense device. The top navigation bar includes Monitoring, Policies, Objects, and Device: firepower. The device details section shows the Model as Cisco Firepower 4125 Threat Defense, Software as 7.2.4-165 | FXOS 2.13(0.212), VDB as 353.0, and Intrusion Rule Update as 20220511-1540. A red box highlights the software version. Below the device details, there is a network diagram showing the device connected to an Inside Network. The main content area displays several configuration sections: Interfaces (Connected, Enabled 3 of 3), Routing (No static routes yet), Updates (Geolocation, Rule, VDB, System Upd, Security Intelligence Feeds), Smart License (Evaluation expires in 90 days), Backup and Restore (No files created yet), Site-to-Site VPN (No connections yet), Remote Access VPN (Requires RA VPN license, No connections | 1 Group Policy), and Advanced Configuration (Includes: FlexConfig, Smart CLI).

Um eine Upgrade-Validierung über die CLI durchzuführen, gehen Sie wie folgt vor:

- I. Erstellen Sie eine SSH-Sitzung mit der Management-IP-Adresse des FTD.
- II. Verwenden Sie den Befehl **show version**, um die aktuelle Version auf Ihrem Chassis zu überprüfen.

Beispiel für das vorgeschlagene Verfahren:

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  
-----
```

> █

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.