Upgrade of Secure Firewall Threat Defense Using Firewall Device Manager

Contents

Introduction

This document describes an example of a Cisco Secure Firewall Threat Defense (FTD) upgrade using the Firewall Device Manager (FDM).

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- There are no specific requirements for this guide

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Firepower 4125 running 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Specific requirements for this document include:

- Connectivity to the Management IP of the FTD
- The FTD upgrade package (**.REL.tar**) previously downloaded from the Software Cisco Portal

This upgrade procedure is supported on appliances:

- Any Cisco Firepower model running FTD software configured with local management.

Before You Begin

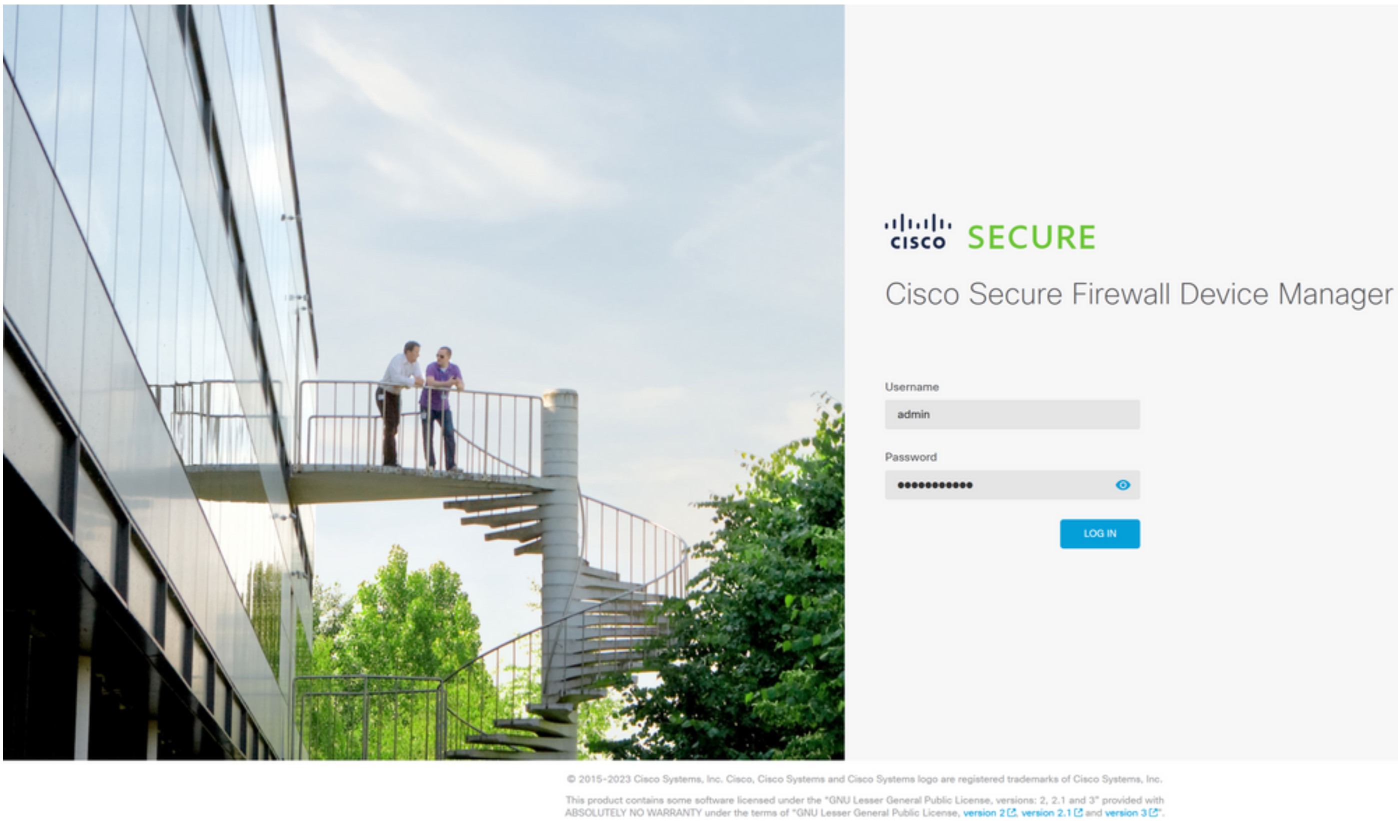
1. Create and download a backup of the FTD Configurations.
2. Validate the upgrade path for the target version.
3. Download the upgrade package from the Cisco Software Central.

4. Do not rename the upgrade file. The system considers renamed files to be invalid.

5. Schedule a maintenance window for the upgrade procedure because traffic is affected.

Configure

Step 1. Log into the Firewall Device Manager using the Management IP of the FTD:



Cisco Secure Firewall Device Manager

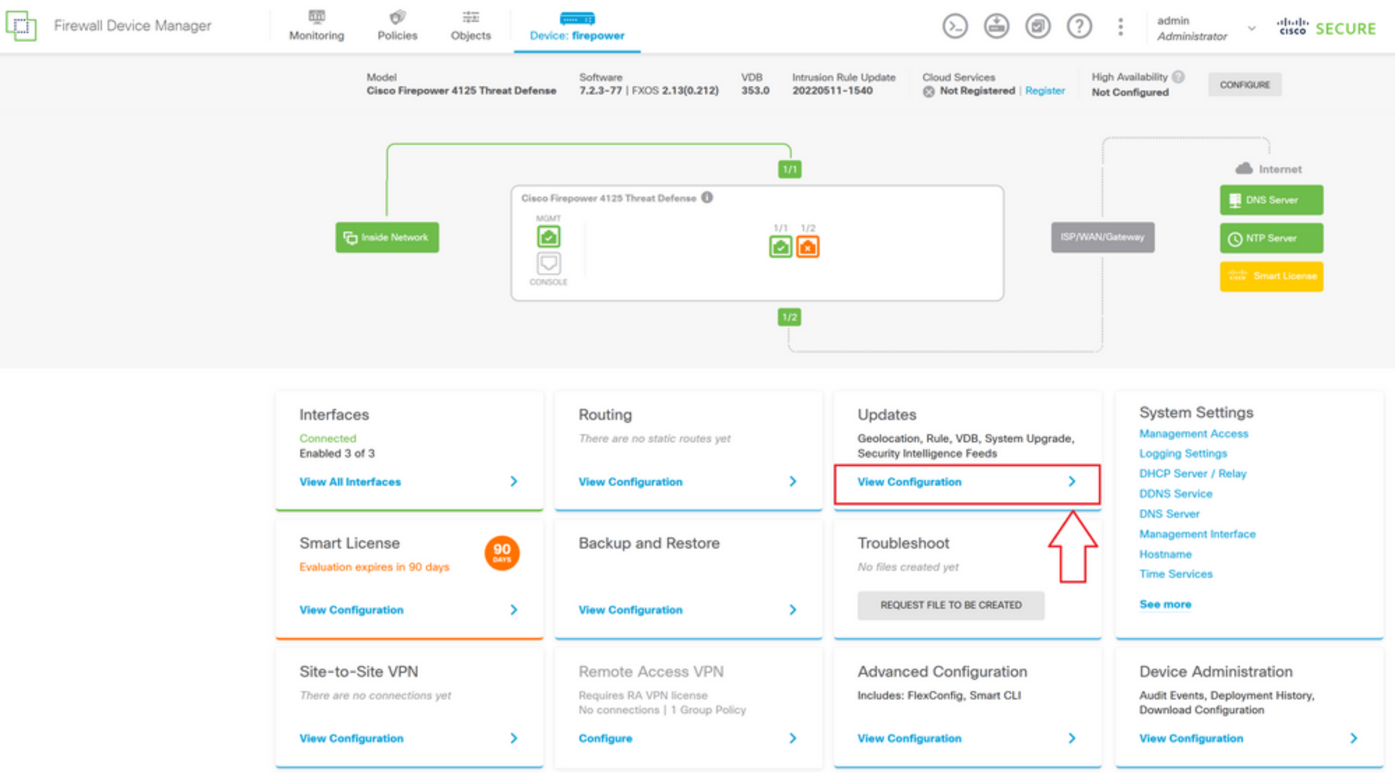
Username: admin

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, 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".

Step 2. Click on **View Configuration** on the Firewall Device Manager Dashboard:



Firewall Device Manager | Monitoring | Policies | Objects | Device: firepower | admin Administrator | cisco SECURE

Model Cisco Firepower 4125 Threat Defense | Software 7.2.3-77 | FXOS 2.13(0.212) | VDB 353.0 | Intrusion Rule Update 20220511-1540 | Cloud Services Not Registered | Register | High Availability Not Configured | CONFIGURE

Interfaces
Connected
Enabled 3 of 3
View All Interfaces

Routing
There are no static routes yet
View Configuration

Updates
Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds
View Configuration

System Settings
Management Access
Logging Settings
DHCP Server / Relay
DDNS Service
DNS Server
Management Interface
Hostname
Time Services
See more

Smart License
90 DAYS
Evaluation expires in 90 days
View Configuration

Backup and Restore
View Configuration

Troubleshoot
No files created yet
REQUEST FILE TO BE CREATED

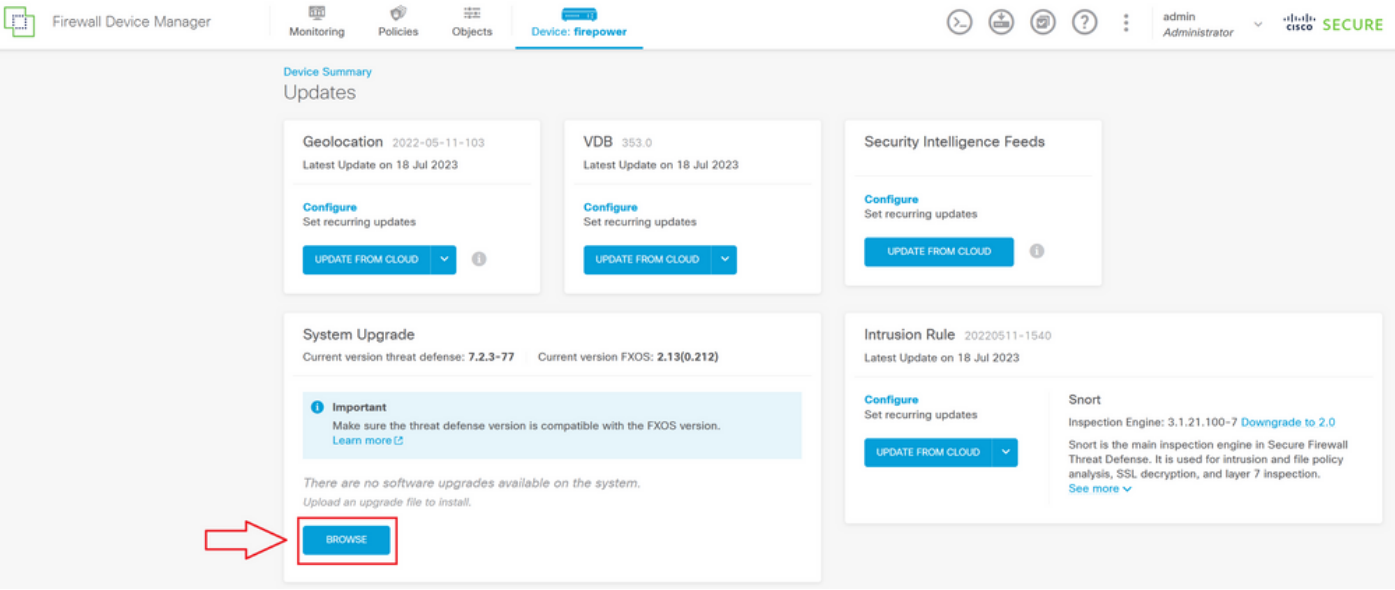
Site-to-Site VPN
There are no connections yet
View Configuration

Remote Access VPN
Requires RA VPN license
No connections | 1 Group Policy
Configure

Advanced Configuration
Includes: FlexConfig, Smart CLI
View Configuration

Device Administration
Audit Events, Deployment History, Download Configuration
View Configuration

Step 3. Click on the **Browse** button under the System Upgrade section to upload the installation package:



Firewall Device Manager | Monitoring | Policies | Objects | Device: firepower | admin Administrator | cisco SECURE

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

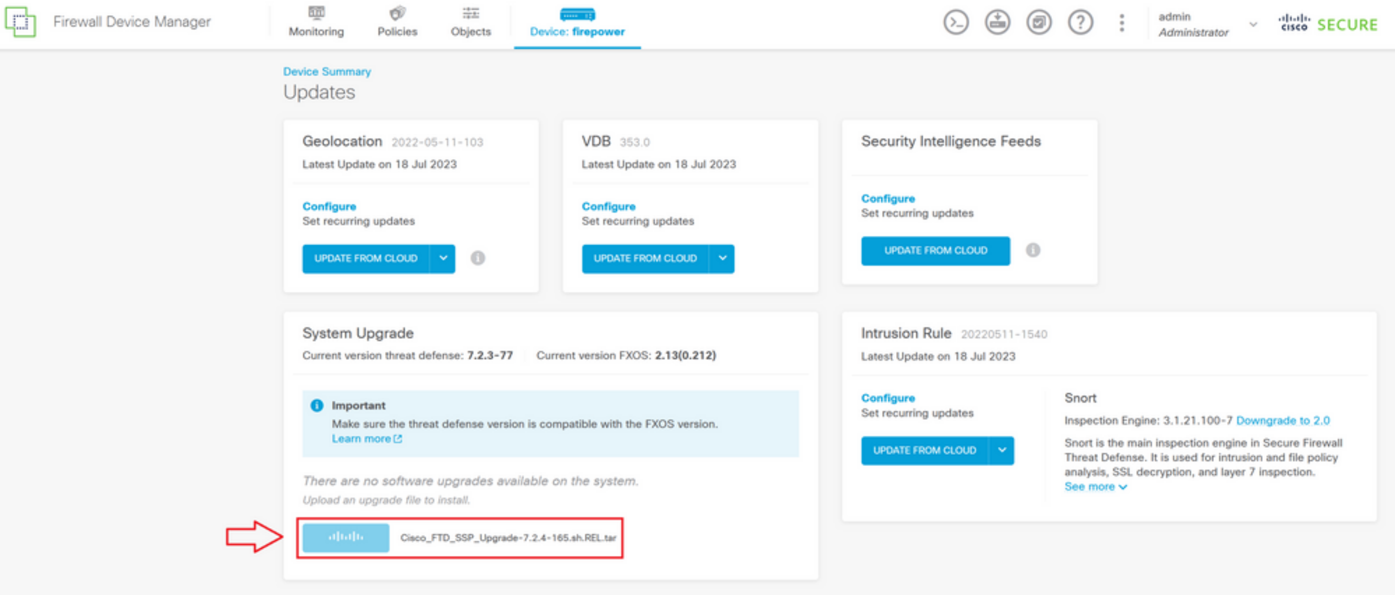
There are no software upgrades available on the system.
Upload an upgrade file to install.
BROWSE

Intrusion Rule 20220511-1540
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

⚠ **Caution**: Once you upload the upgrade package the **BROWSE** is going to display an animation while the file is still getting uploaded. Do not refresh the web page until the upload finishes.

Example of upload progress page:



Device Summary

Updates

Geolocation 2022-05-11-103
Latest Update on 18 Jul 2023
Configure
Set recurring updates

VDB 353.0
Latest Update on 18 Jul 2023
Configure
Set recurring updates

Security Intelligence Feeds
Configure
Set recurring updates

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

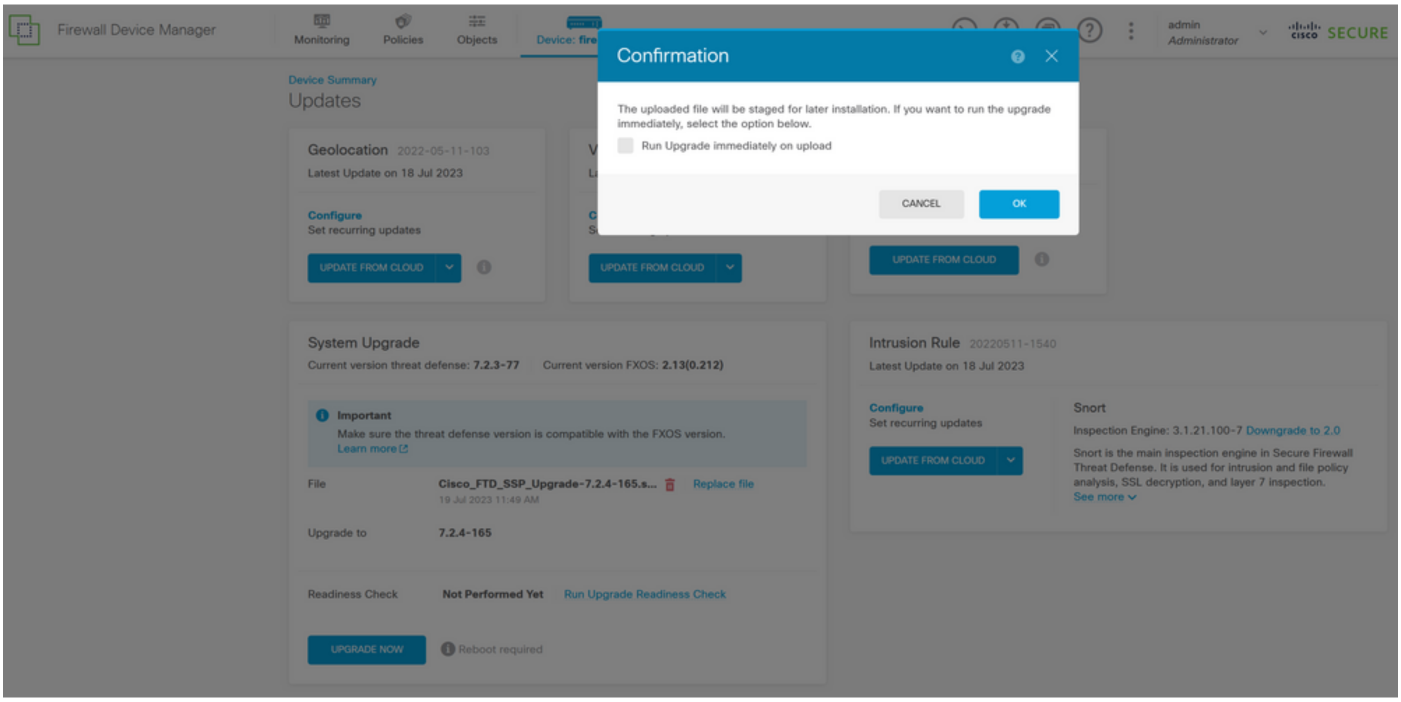
There are no software upgrades available on the system.
Upload an upgrade file to install.

Cisco_FTD_SSP_Upgrade-7.2.4-165.sh.REL.tar

Intrusion Rule 20220511-1540
Latest Update on 18 Jul 2023
Configure
Set recurring updates

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

Step 4. Once the upload finishes a pop-up window appears asking for confirmation:



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

Device Summary

Updates

Geolocation 2022-05-11-103
Latest Update on 18 Jul 2023
Configure
Set recurring updates

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 **Not Performed Yet** Run Upgrade Readiness Check

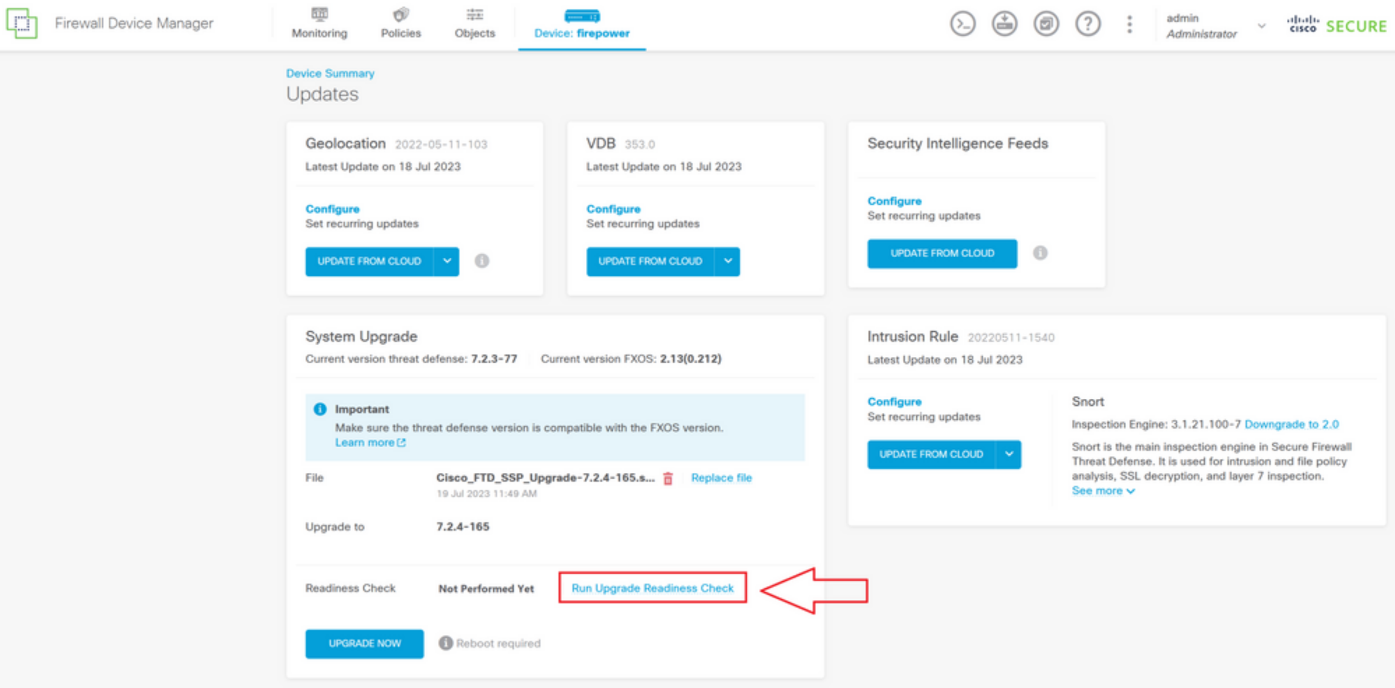
Reboot required

Intrusion Rule 20220511-1540
Latest Update on 18 Jul 2023
Configure
Set recurring updates

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

Note: You can check the **Run Upgrade immediately on upload** option in case you would like to directly proceed with upgrade, however note this is going to skip the **Readiness Check** which can provide insights about conflicts on the upgrade preventing a failure.

Step 5. Click on **Run Upgrade Readiness Check** to perform a pre-validation on the upgrade in order to prevent an upgrade failure:



Device Summary

Updates

Geolocation 2022-05-11-103
Latest Update on 18 Jul 2023
Configure
Set recurring updates

VDB 353.0
Latest Update on 18 Jul 2023
Configure
Set recurring updates

Security Intelligence Feeds
Configure
Set recurring updates

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 Not Performed Yet Run Upgrade Readiness Check

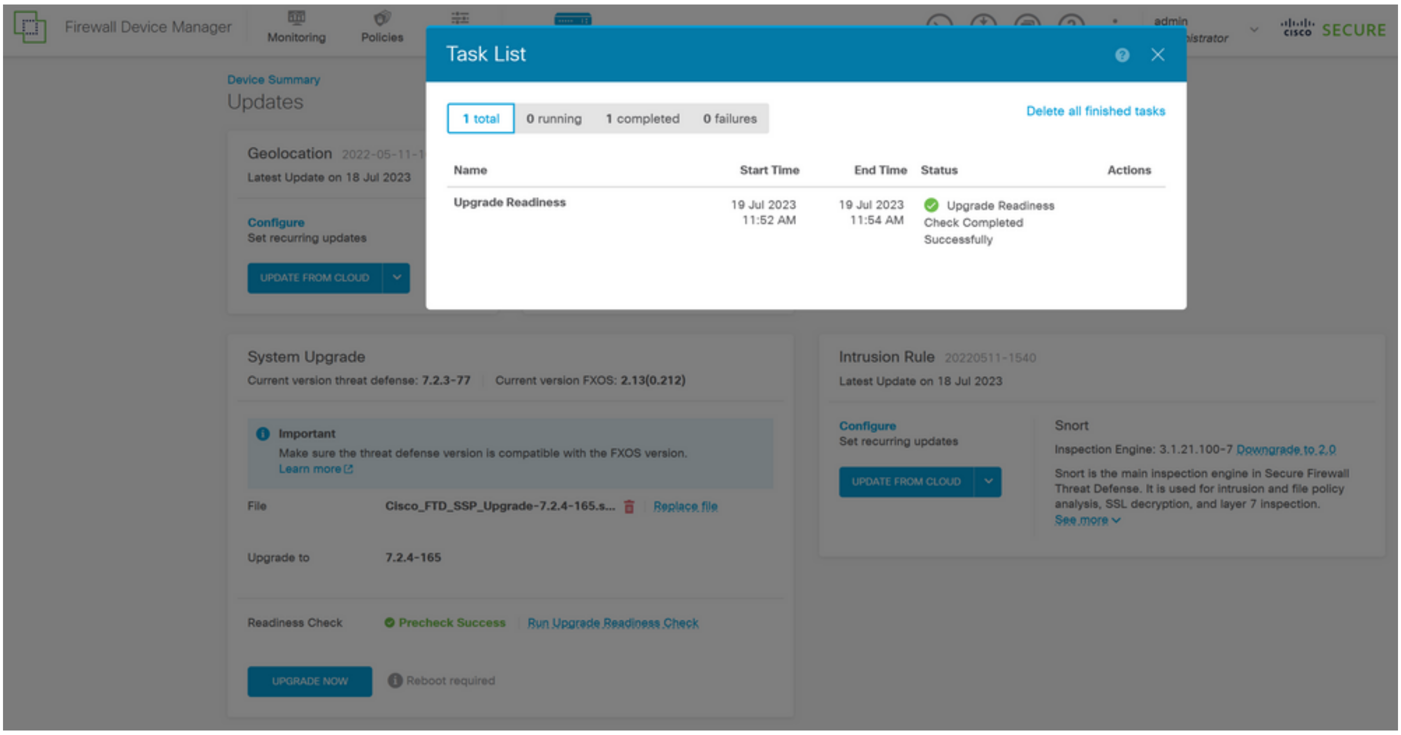
Reboot required

Intrusion Rule 20220511-1540
Latest Update on 18 Jul 2023
Configure
Set recurring updates

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

Note: You can validate that the Readiness Check finished successfully from the Task List.

Example of a successful Readiness Check:



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	

Device Summary

Updates

Geolocation 2022-05-11-1
Latest Update on 18 Jul 2023
Configure
Set recurring updates

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

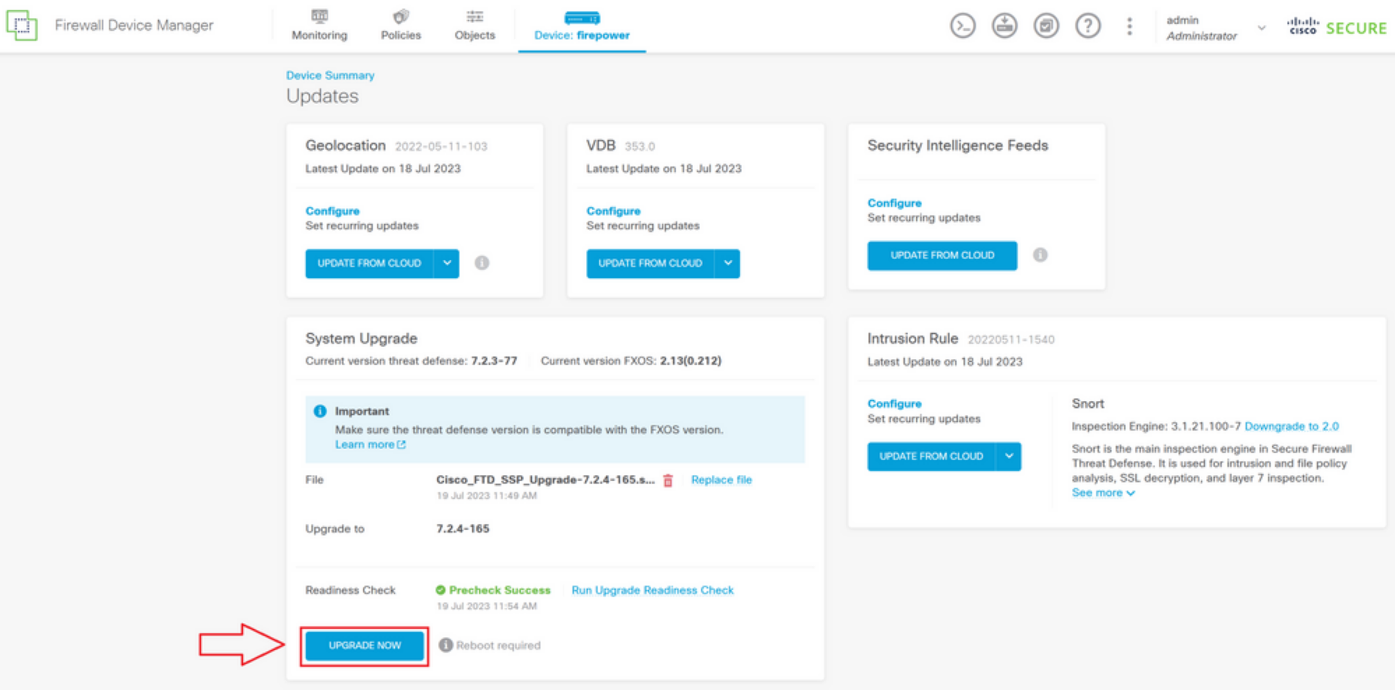
Readiness Check ✓ Precheck Success Run Upgrade Readiness Check

Reboot required

Intrusion Rule 20220511-1540
Latest Update on 18 Jul 2023
Configure
Set recurring updates

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

Step 6. Click on the **UPGRADE NOW** button to proceed with the software upgrade:



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...** Replace file
19 Jul 2023 11:49 AM

Upgrade to **7.2.4-165**

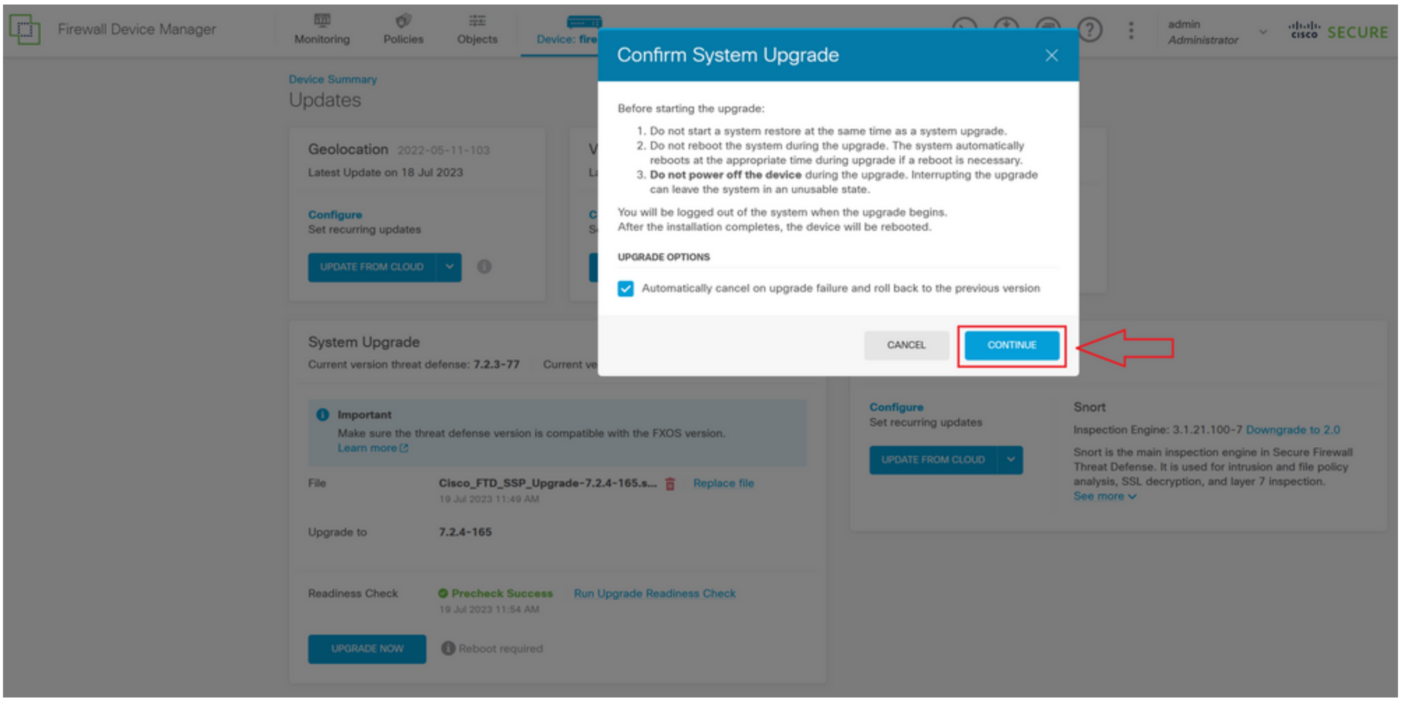
Readiness Check **Precheck Success** Run Upgrade Readiness Check
19 Jul 2023 11:54 AM

UPGRADE NOW
Reboot required

Intrusion Rule 20220511-1540
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

Step 7. On the pop-up window select **CONTINUE** to proceed with the upgrade:



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.

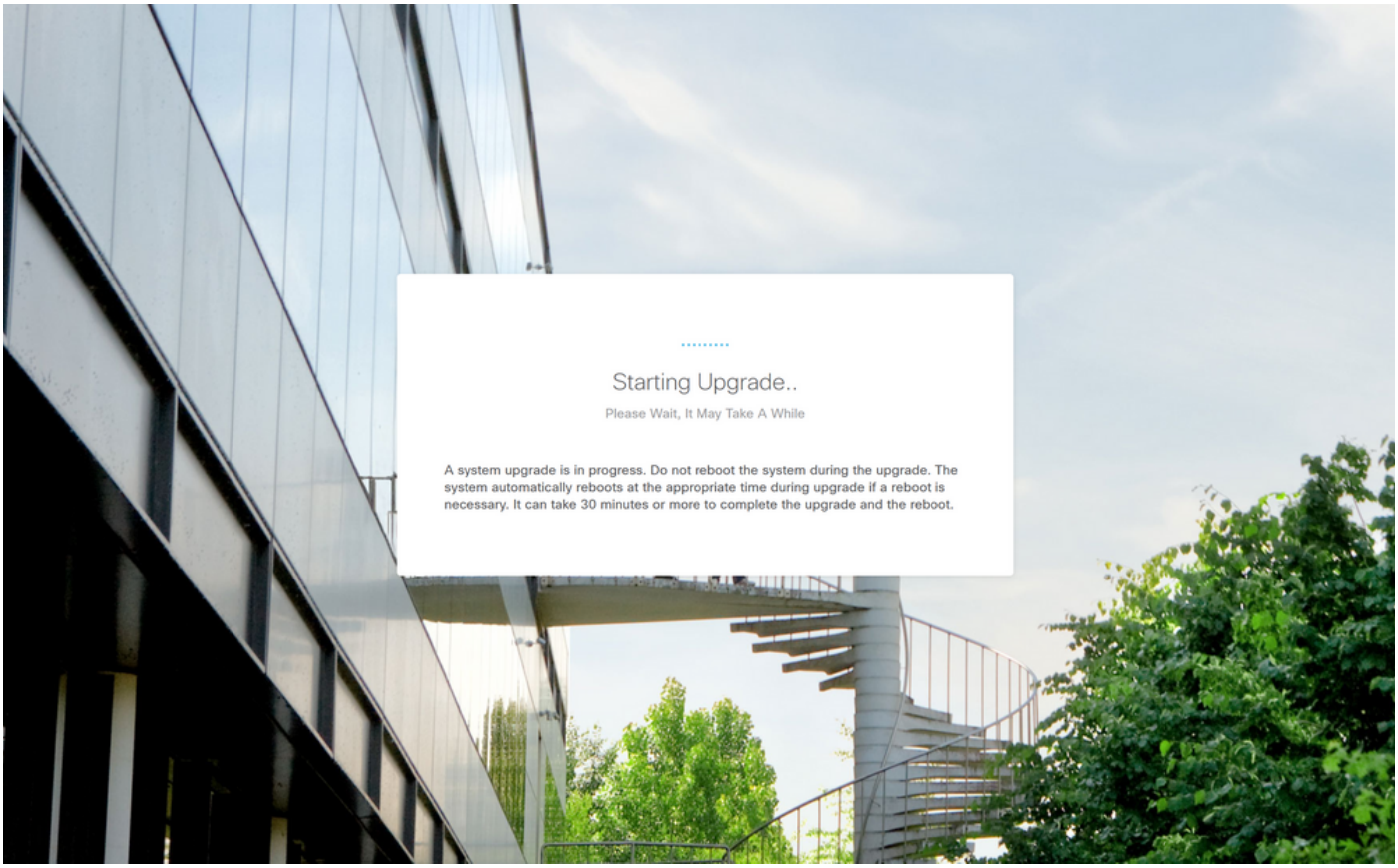
UPGRADE OPTIONS

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

CANCEL CONTINUE

Note: The rollback option is enabled by default, it is suggested you keep this option in order to revert any upgrade configuration in case of an issue on the upgrade.

Step 8. You are redirected to a page where the upgrade progress is going to be displayed:

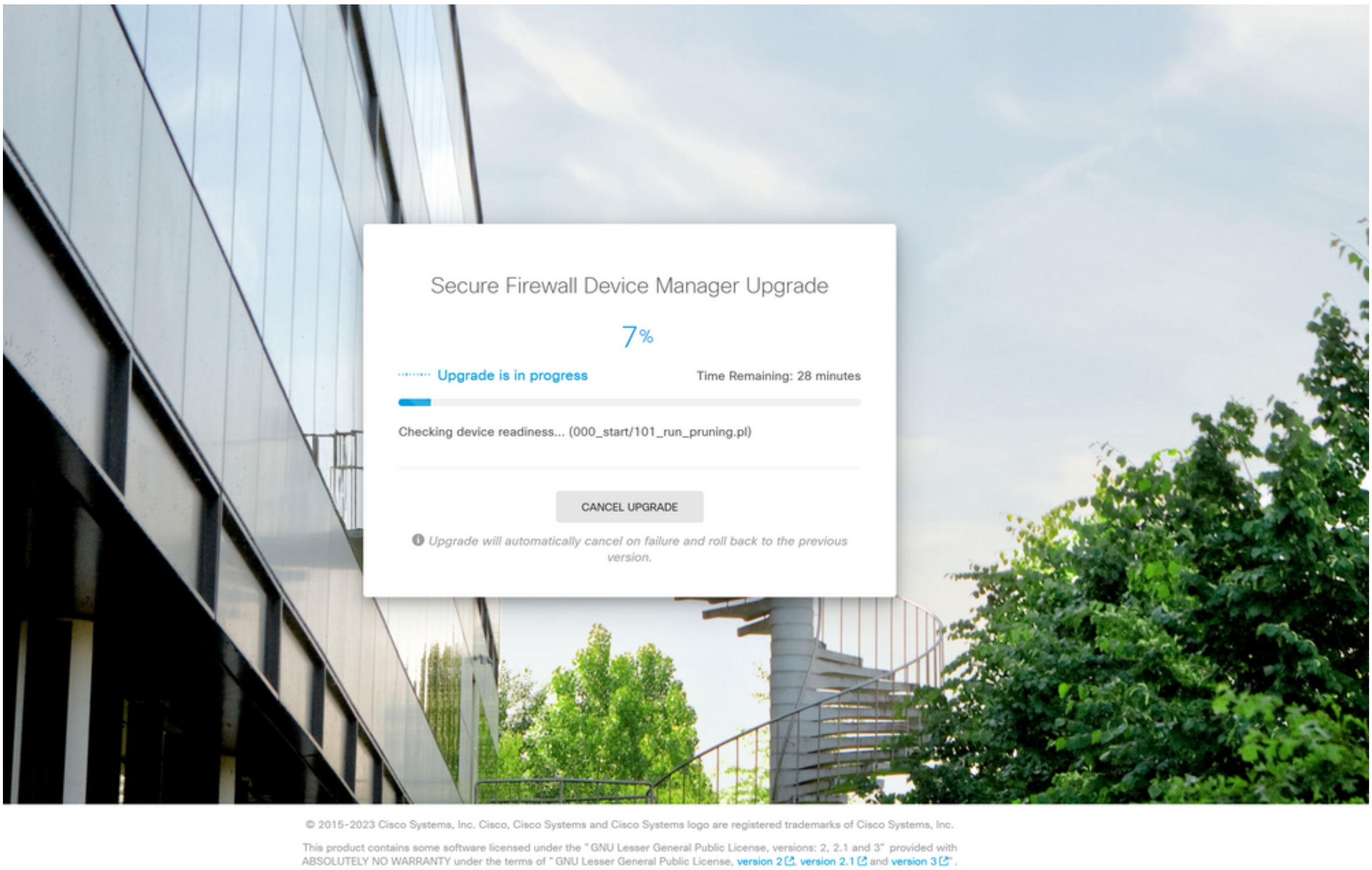


Starting Upgrade..

Please Wait, It May Take A While

A system upgrade is in progress. Do not reboot the system during the upgrade. The system automatically reboots at the appropriate time during upgrade if a reboot is necessary. It can take 30 minutes or more to complete the upgrade and the reboot.

Example of the progress page:



Secure Firewall Device Manager Upgrade

7%

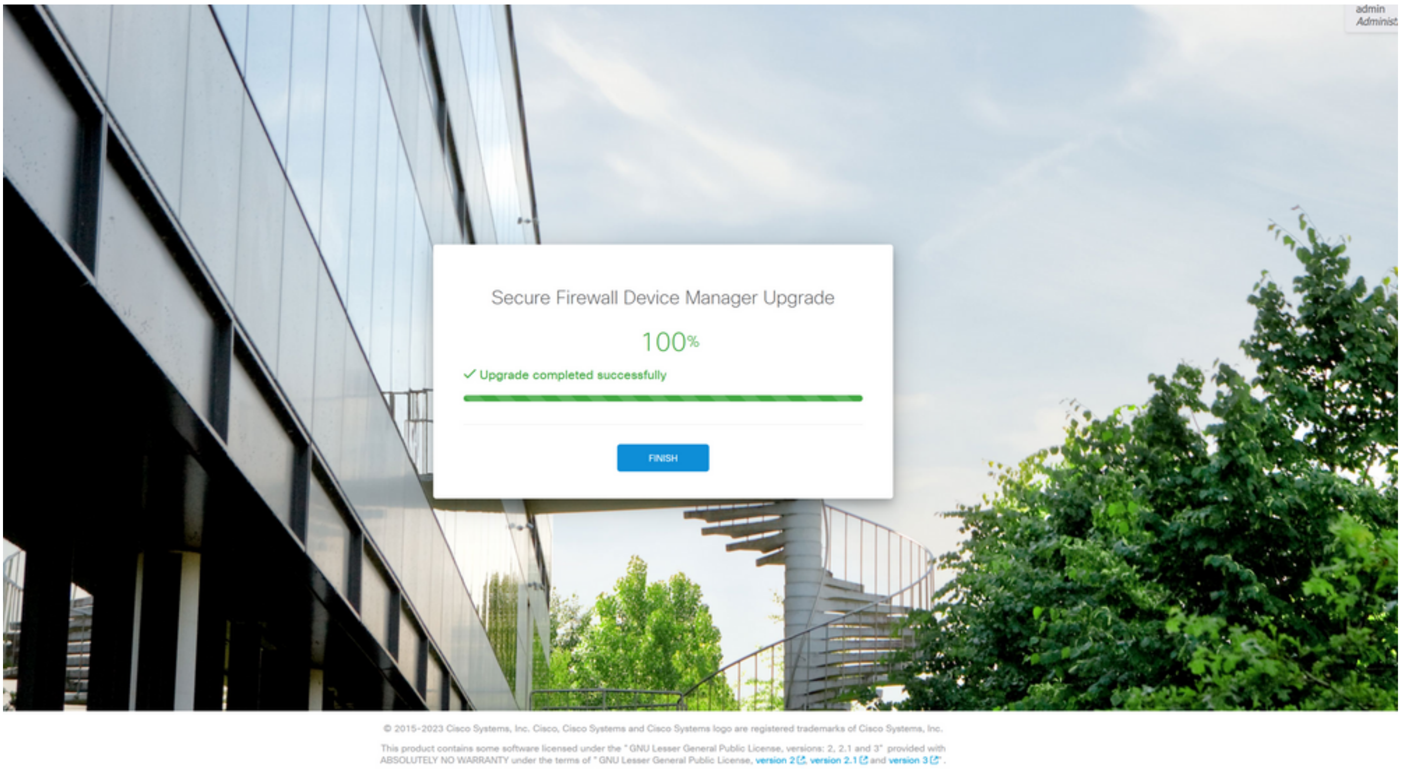
Upgrade is in progress

Time Remaining: 28 minutes

Checking device readiness... (000_start/101_run_pruning.pl)

Upgrade will automatically cancel on failure and roll back to the previous version.

Step 9. Click on the **FINISH** button after the upgrade completes successfully to return to the login screen:



Secure Firewall Device Manager Upgrade

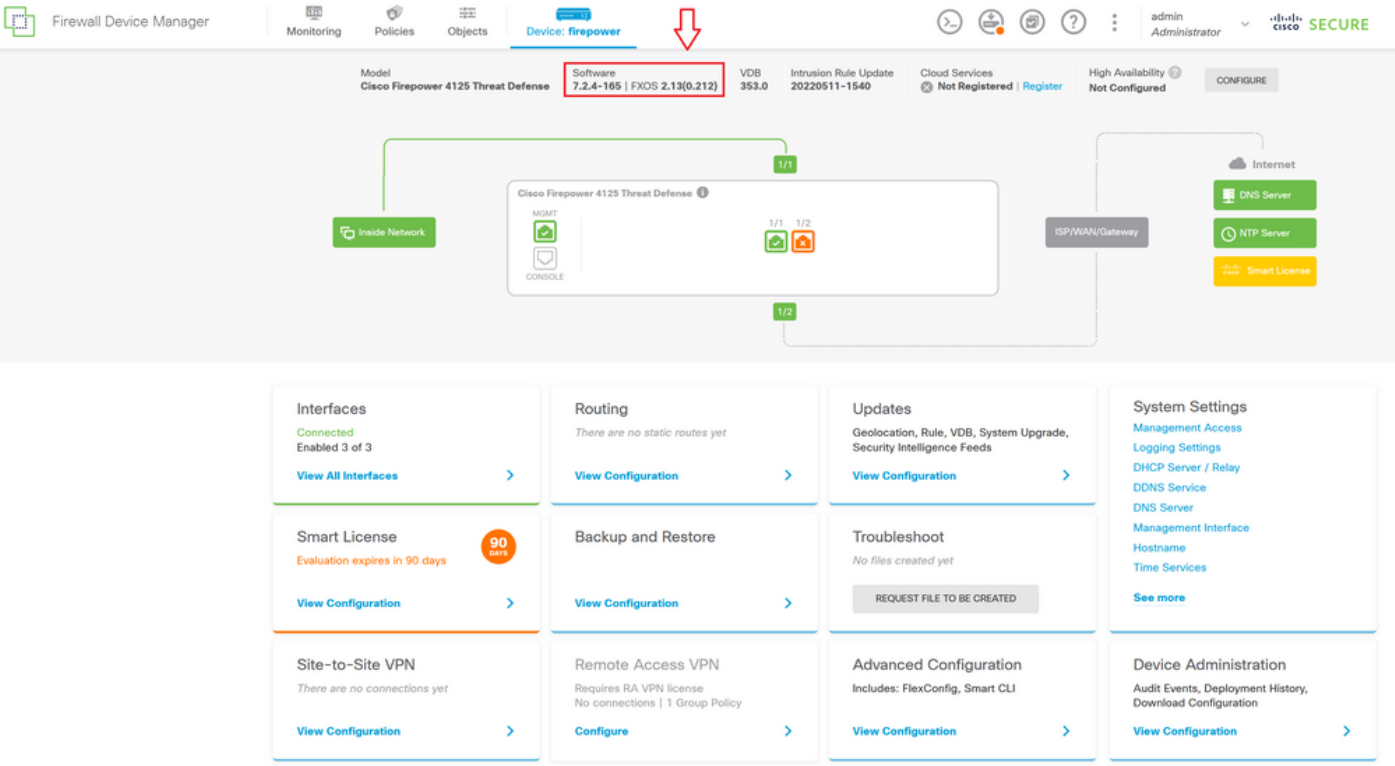
100%

✓ Upgrade completed successfully

FINISH

Validation

Once the upgrade finishes you can log into the Firepower Device Manager to validate the current version, this is displayed on the Overview dashboard:



Model
Cisco Firepower 4125 Threat Defense

Software
7.2.4-165 | FXOS 2.13(0.212)

VDB
353.0

Intrusion Rule Update
20220511-1540

Cloud Services
Not Registered | Register

High Availability
Not Configured

CONFIGURE

Interfaces
Connected
Enabled 3 of 3
View All Interfaces

Routing
There are no static routes yet
View Configuration

Updates
Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds
View Configuration

System Settings
Management Access
Logging Settings
DHCP Server / Relay
DDNS Service
DNS Server
Management Interface
Hostname
Time Services
See more

Smart License
Evaluation expires in 90 days
90 DAYS
View Configuration

Backup and Restore
View Configuration

Troubleshoot
No files created yet
REQUEST FILE TO BE CREATED

Site-to-Site VPN
There are no connections yet
View Configuration

Remote Access VPN
Requires RA VPN license
No connections | 1 Group Policy
Configure

Advanced Configuration
Includes: FlexConfig, Smart CLI
View Configuration

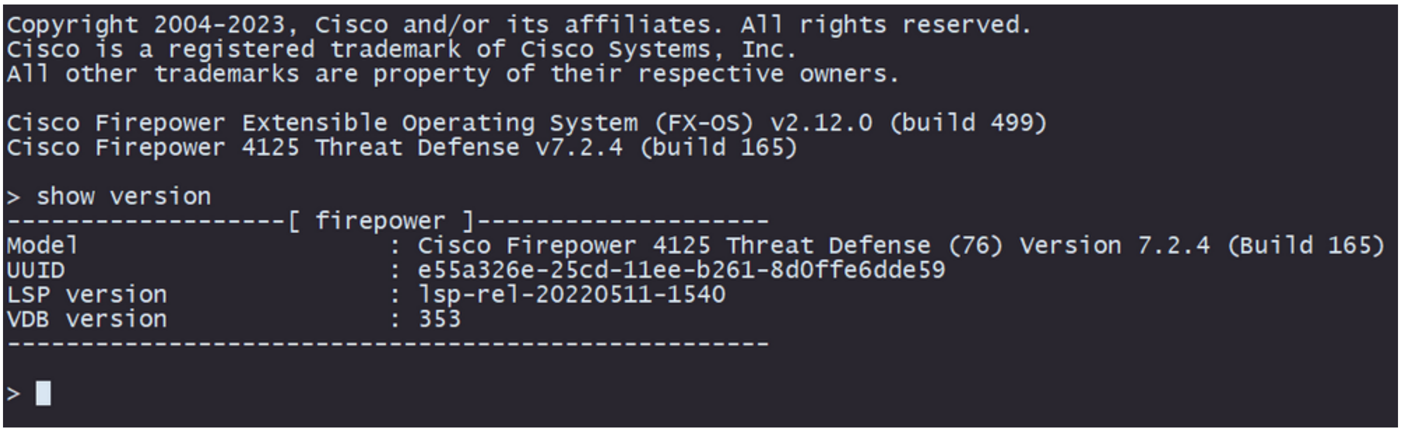
Device Administration
Audit Events, Deployment History, Download Configuration
View Configuration

To perform an upgrade validation via CLI you can use these steps:

I. Create an SSH Session using the Management IP of the FTD.

II. Use the **show version** command to validate the current version on your chassis.

Example of the suggested procedure:



```
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
----------------------------------------------------

>
```