

使用防火牆裝置管理器升級安全防火牆威脅防禦

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[開始之前](#)

[設定](#)

[驗證](#)

簡介

本檔案介紹使用防火牆裝置管理員(FDM)進行思科安全防火牆威脅防禦(FTD)升級的範例。

必要條件

需求

思科建議瞭解以下主題：

- 本指南沒有特定要求

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行FTD版本7.2.3的Cisco Firepower 4125

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文檔的具體要求包括：

- 連線到FTD的管理IP
- 之前從軟體思科入口網站下載的FTD升級套件(.REL.tar)

以下裝置支援此升級過程：

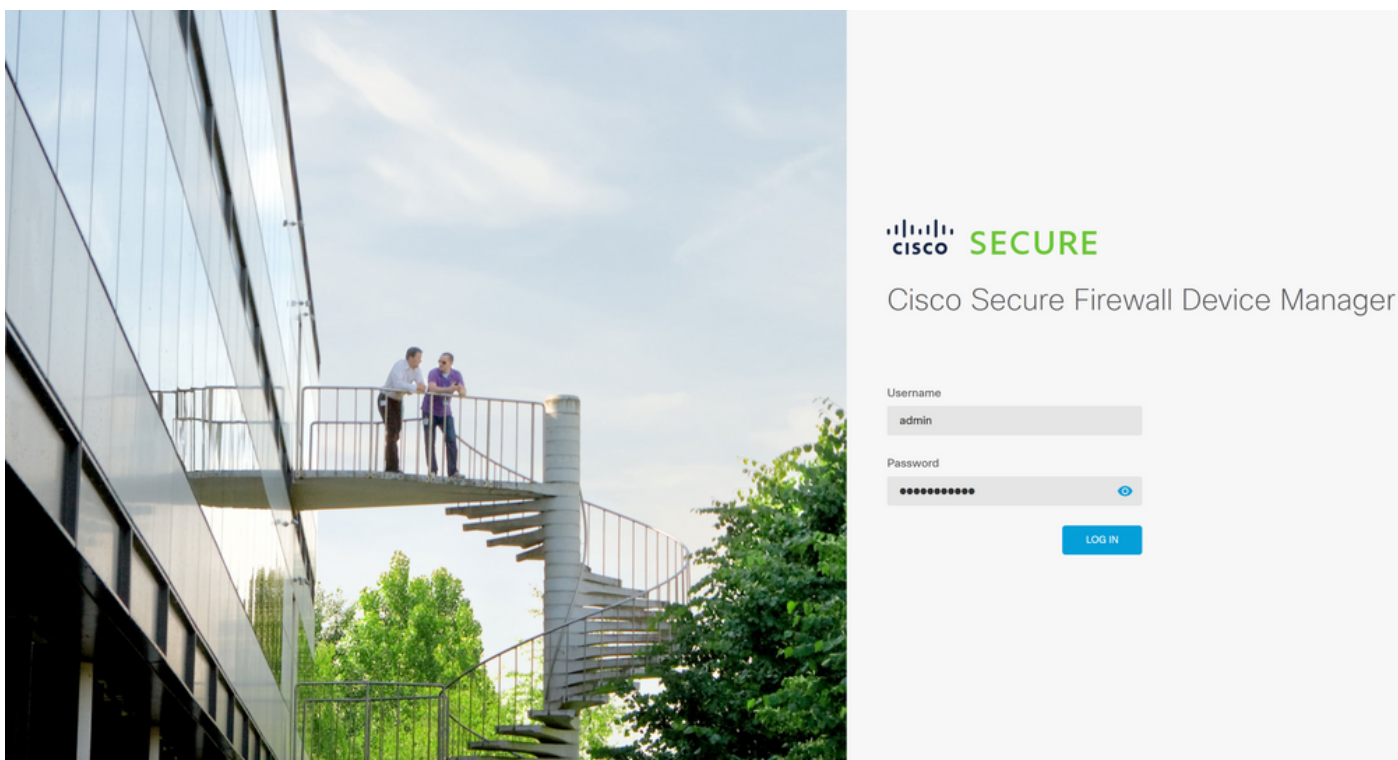
- 任何運行FTD軟體、配置了本地管理的思科Firepower型號。

開始之前

1. 建立並下載FTD組態的備份。
2. 驗證目標版本的升級路徑。
3. 從[思科軟體中心](#)下載升級套件。
4. 請勿重新命名升級檔案。系統認為重新命名的檔案無效。
5. 為升級過程安排維護視窗，因為流量會受到影響。

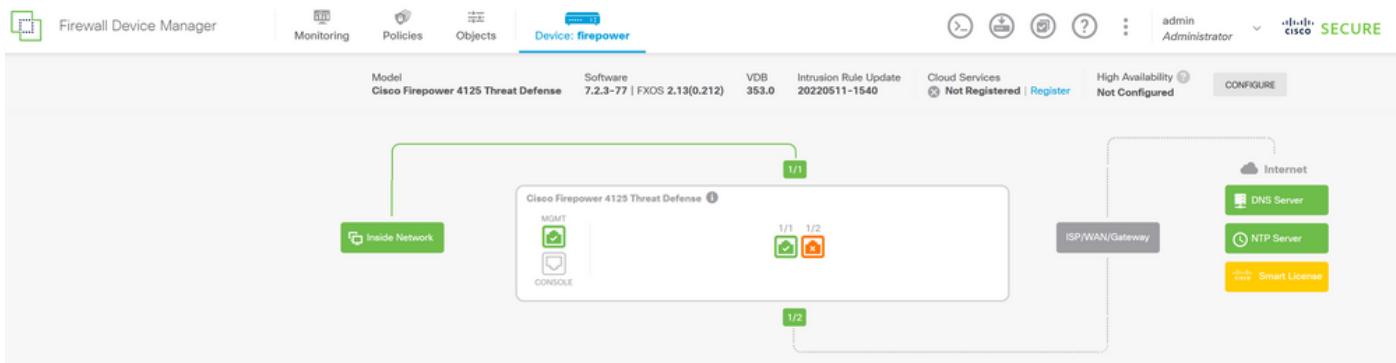
設定

步驟 1. 使用FTD的管理IP登入防火牆裝置管理員：

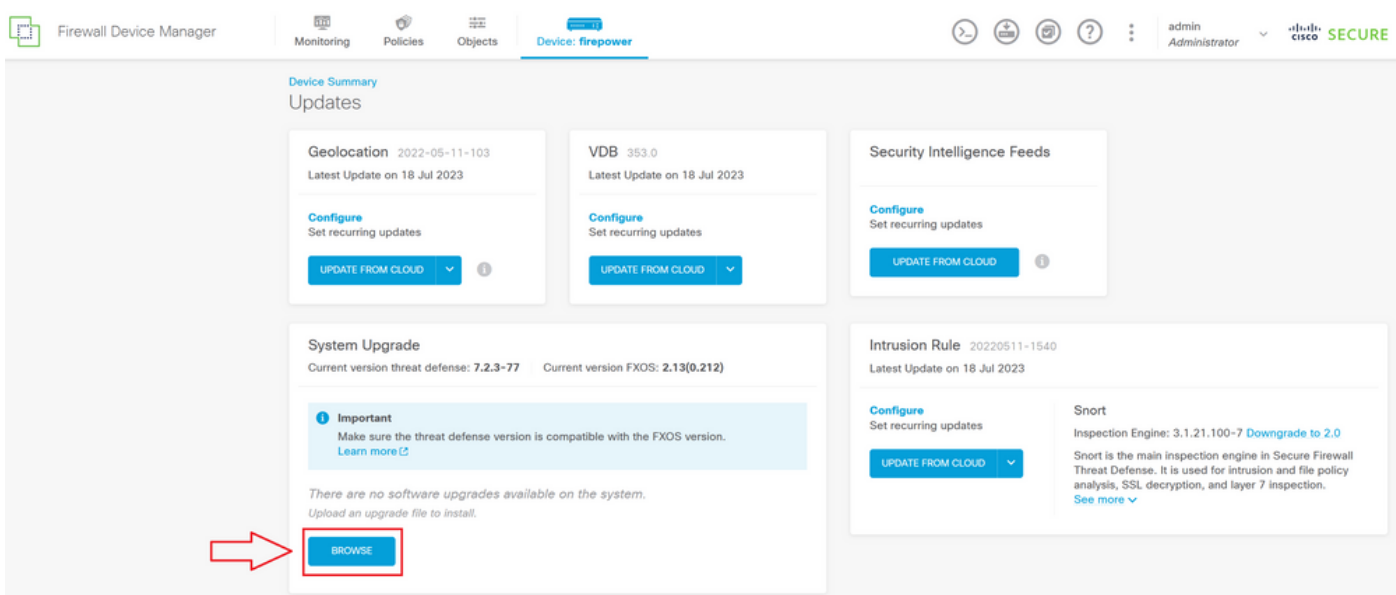


© 2015-2023 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc.
This product contains some software licensed under the "GNU Lesser General Public License, versions: 2, 2.1 and 3" provided with ABSOLUTELY NO WARRANTY under the terms of "GNU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

步驟 2. 在Firewall Device Manager Dashboard上按一下View Configuration:



步驟 3.按一下「System Upgrade (系統升級)」部分下的「Browse」按鈕上傳安裝軟體包：



⚠ 注意：上傳升級軟體包後，BROWSE將在檔案仍被上傳時顯示動畫。上傳完成之前請勿刷新網頁。

上載進度頁示例：

Firewall Device Manager

Monitoring Policies Objects Device: firepower

admin Administrator

SECURE

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. [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.ah.REL.tar

Intrusion Rule 20220511-1540 Latest Update on 18 Jul 2023

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](#)

步驟 4.上傳完成後，系統會顯示一個彈出視窗，要求確認：

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

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

19 Jul 2023 11:49 AM

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

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](#)

註：如果您想直接繼續升級，可以選中upload 選項以立即運行升級，但是請注意，這將跳過 Readiness Check，該檢查可提供有關升級衝突的資訊，從而防止失敗。

步驟5.按一下Run Upgrade Readiness Check，對升級執行預驗證，以防止升級失敗：

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](#)

註：您可以驗證是否已成功從任務清單完成就緒性檢查。

成功準備情況檢查示例：

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	

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

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](#)

步驟 6. 按一下「UPGRADE NOW」按鈕以繼續軟體升級：

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... 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](#)

步驟 7.在彈出視窗中選擇CONTINUE以繼續升級：

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... 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

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

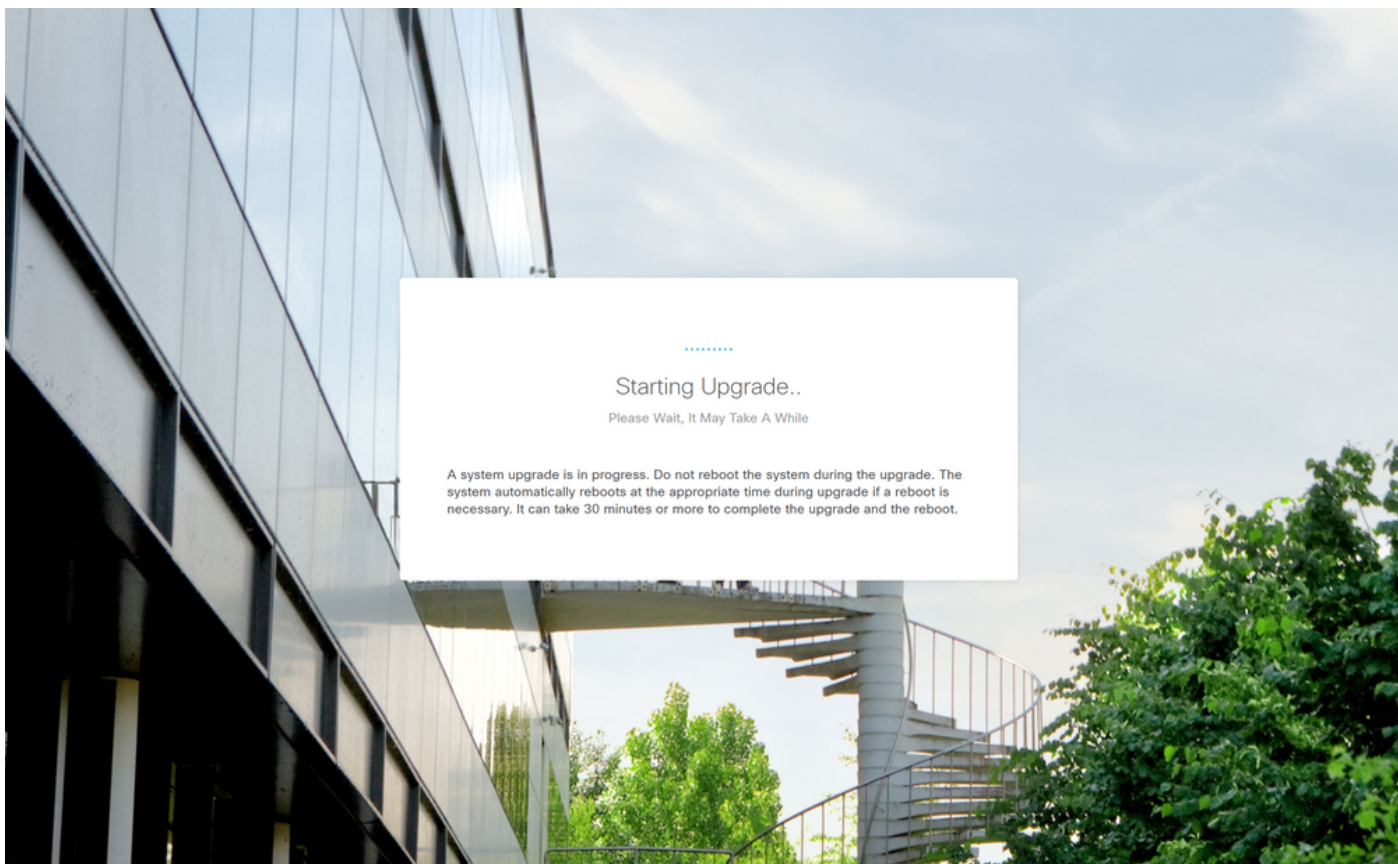
Configure Set recurring updates

UPDATE FROM CLOUD

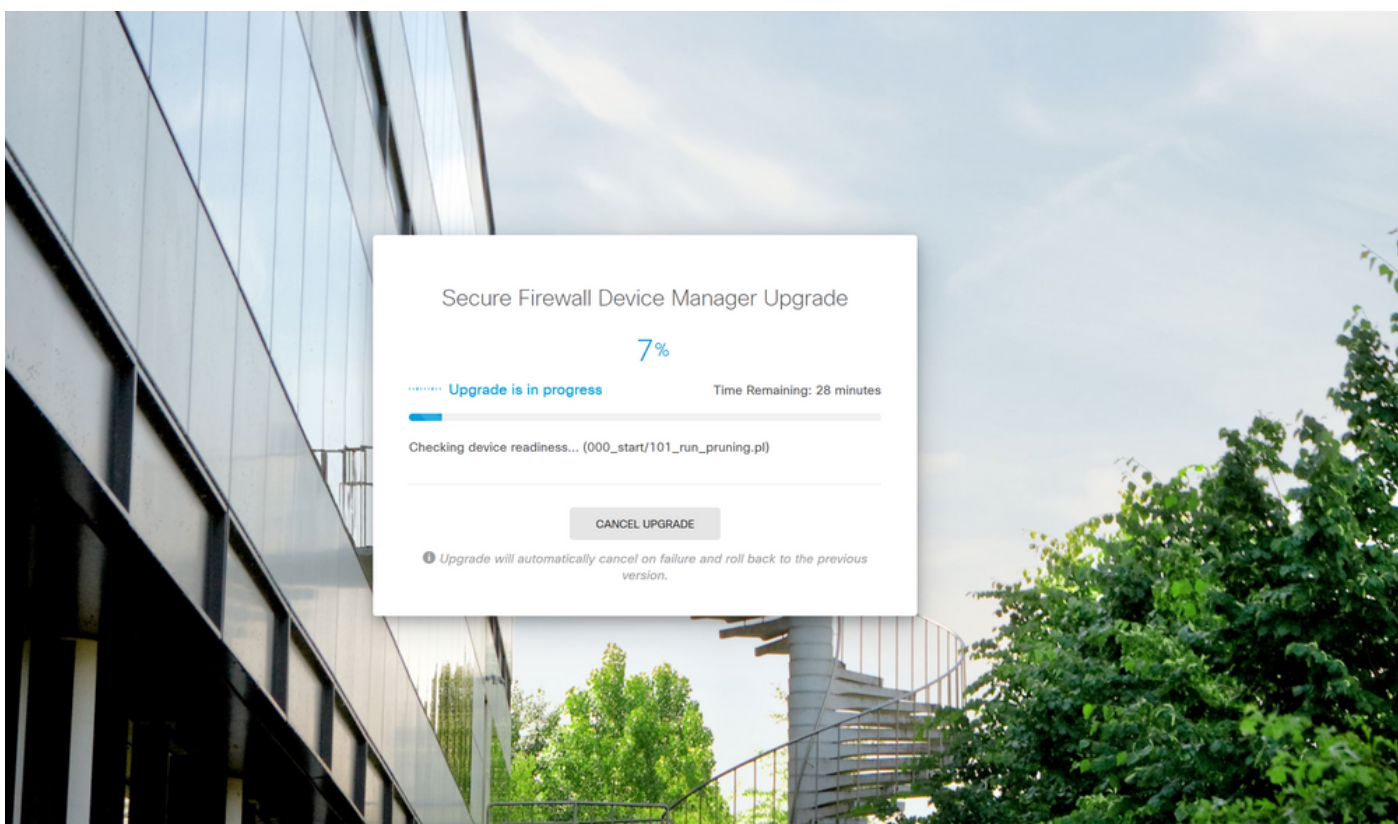
Snort
Inspection Engine: 3.1.21.100-7 Downgrade to 2.0
Snort is the main inspection engine in Secure Firewall Threat Defense. It is used for intrusion and file policy analysis, SSL decryption, and layer 7 inspection.
[See more](#)

 注意：預設情況下啟用回滾選項，建議您保留該選項，以便在升級出現問題時恢復任何升級配置。

步驟 8.系統會將您重新導向至顯示升級進度的頁面：

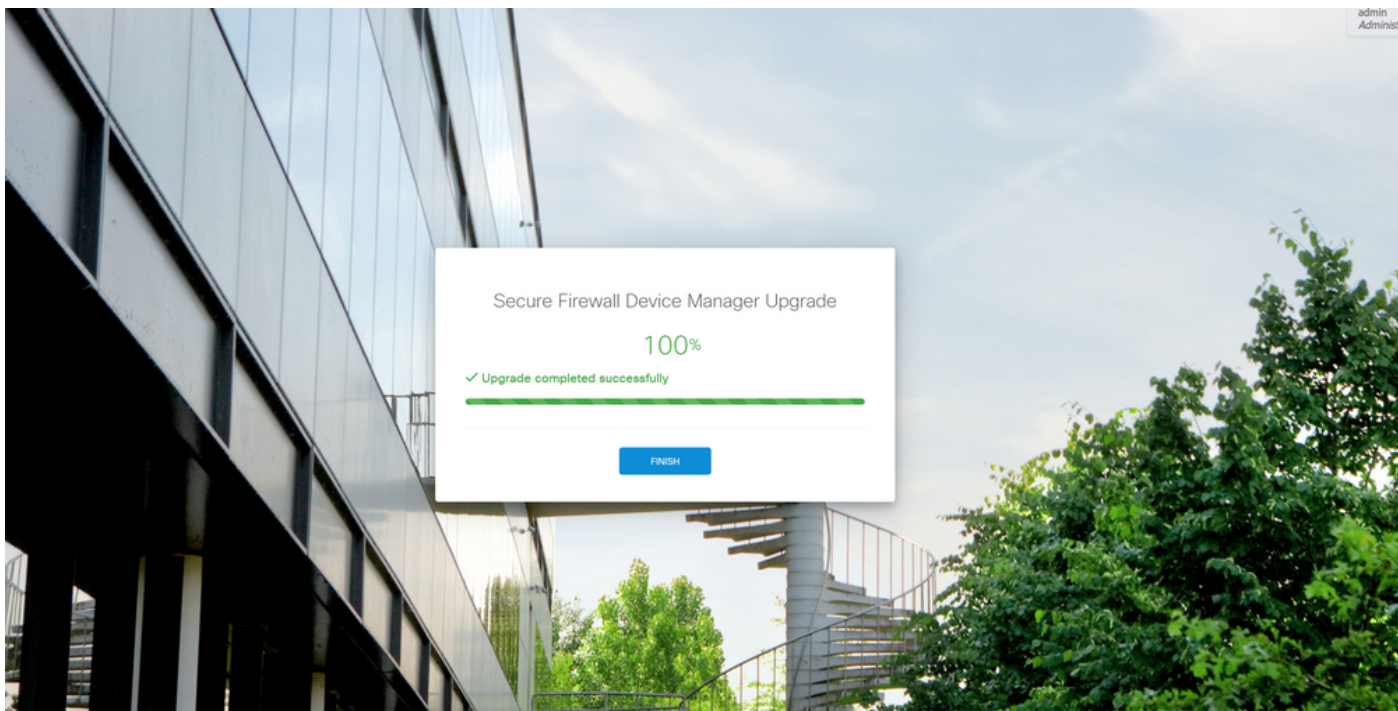


進度頁示例：



© 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](#)".

步驟 9. 升級成功完成後，按一下FINISH按鈕返回登入螢幕：



© 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".

驗證

升級完成後，您可以登入到Firepower裝置管理器以驗證當前版本，這將在概述控制面板上顯示：

要通過CLI執行升級驗證，您可以使用以下步驟：

I.使用FTD的管理IP建立SSH作業階段。

II.使用show version命令驗證機箱上的當前版本。

建議過程的示例：

```
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  
-----  
> █
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。