

# FMC 6.6.1+ — 升級前後的提示

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[FMC升級前要做的幾件事](#)

[選擇FMC目標軟體版本](#)

[驗證當前FMC型號和軟體版本](#)

[規劃升級路徑](#)

[上傳升級包](#)

[建立FMC備份](#)

[驗證NTP同步](#)

[驗證磁碟空間](#)

[部署所有掛起策略更改](#)

[運行Firepower軟體就緒性檢查](#)

[FMC升級後的首要任務](#)

[部署所有掛起策略更改](#)

[驗證是否已安裝最新的漏洞和指紋資料庫](#)

[驗證Snort規則和輕型安全包當前版本](#)

[驗證地理位置更新當前版本](#)

[通過計畫任務自動更新URL過濾資料庫](#)

[配置定期備份](#)

[確保已註冊智慧許可證](#)

[檢視變數集的配置](#)

[驗證雲服務啟用](#)

[URL篩選](#)

[AMP網路版](#)

[思科雲端區域](#)

[思科雲端事件組態](#)

[啟用SecureX整合](#)

[整合SecureX功能區](#)

[將連線事件傳送到SecureX](#)

[整合安全終端 \( 面向終端的AMP \)](#)

[整合安全惡意軟體分析\(Threat Grid\)](#)

## 簡介

本檔案介紹將思科安全防火牆管理中心(FMC)升級到6.6.1+版之前和之後要完成的驗證和組態最佳實踐。

## 必要條件

## 需求

本文件沒有特定需求。

## 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 硬體：Cisco FMC 1000
- 軟體：版本7.0.0 ( 內部版本94 )

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。

## FMC升級前要做的幾件事

### 選擇FMC目標軟體版本

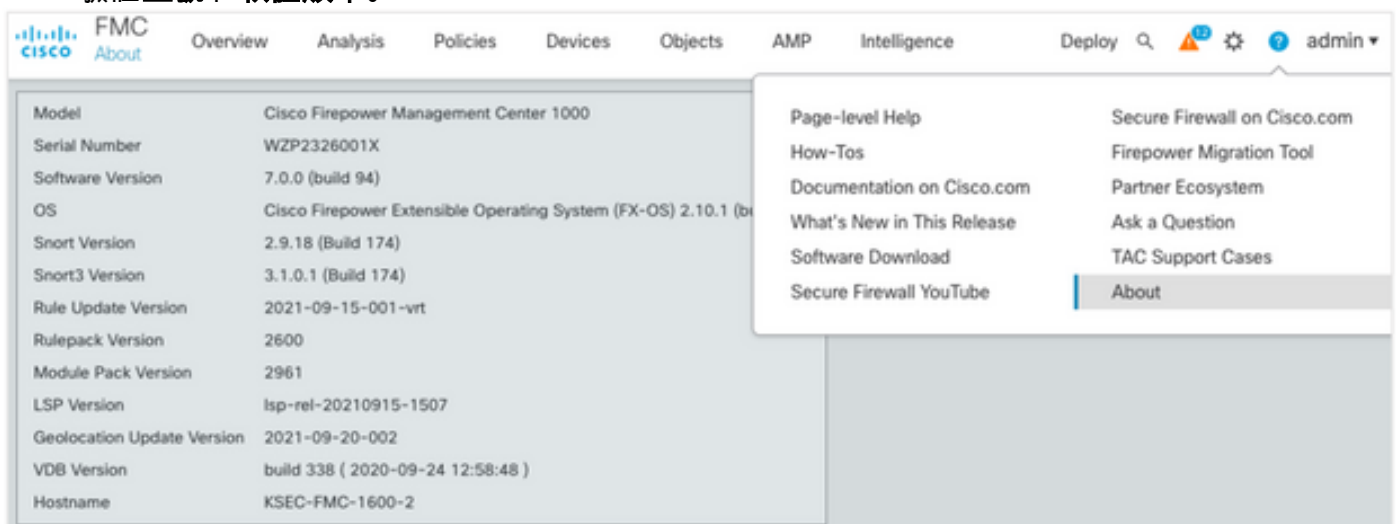
檢視目標版本的[Firepower發行說明](#)，並熟悉：

- 相容性
- 特性和功能
- 已解決的問題
- 已知的問題

### 驗證當前FMC型號和軟體版本

驗證目前的FMC型號和軟體版本：

1. 導航到**幫助>關於**。
2. 驗證**型號和軟體版本**。



The screenshot shows the Cisco FMC 'About' page. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', and 'admin'. The main content area displays system information in a table:

Model	Cisco Firepower Management Center 1000
Serial Number	WZP2326001X
Software Version	7.0.0 (build 94)
OS	Cisco Firepower Extensible Operating System (FX-OS) 2.10.1 (build 174)
Snort Version	2.9.18 (Build 174)
Snort3 Version	3.1.0.1 (Build 174)
Rule Update Version	2021-09-15-001-vrt
Rulepack Version	2600
Module Pack Version	2961
LSP Version	lsp-rel-20210915-1507
Geolocation Update Version	2021-09-20-002
VDB Version	build 338 ( 2020-09-24 12:58:48 )
Hostname	KSEC-FMC-1600-2

A help menu is open on the right side of the page, listing various resources:

- Page-level Help
- How-Tos
- Documentation on Cisco.com
- What's New in This Release
- Software Download
- Secure Firewall YouTube
- Secure Firewall on Cisco.com
- Firepower Migration Tool
- Partner Ecosystem
- Ask a Question
- TAC Support Cases
- About

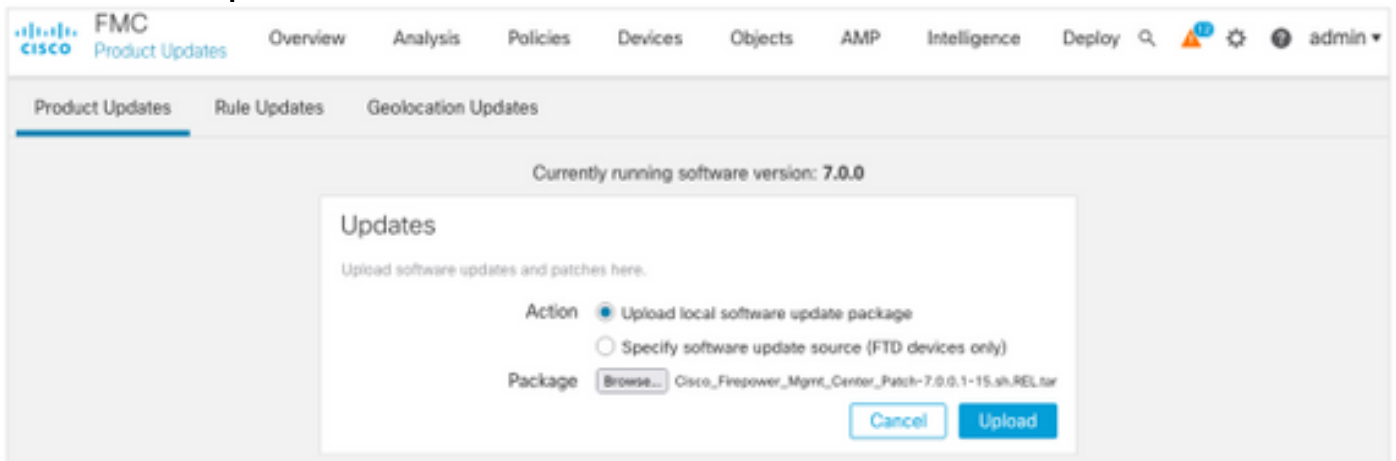
### 規劃升級路徑

根據當前和目標FMC軟體版本，可能需要臨時升級。在[Cisco Firepower Management Center升級指南](#)中，檢視升級路徑：Firepower管理中心部分並規劃升級路徑。

## 上傳升級包

若要將升級套件上傳到裝置，請完成以下步驟：

1. 從[Software](#) Download頁面下載[升級程](#)式包。
2. 在FMC中，導航至**System > Updates**。
3. 選擇**Upload Update**。
4. 按一下**Upload local software update package**單選按鈕。
5. 按一下**Browse**並選擇包。
6. 按一下「**Upload**」。

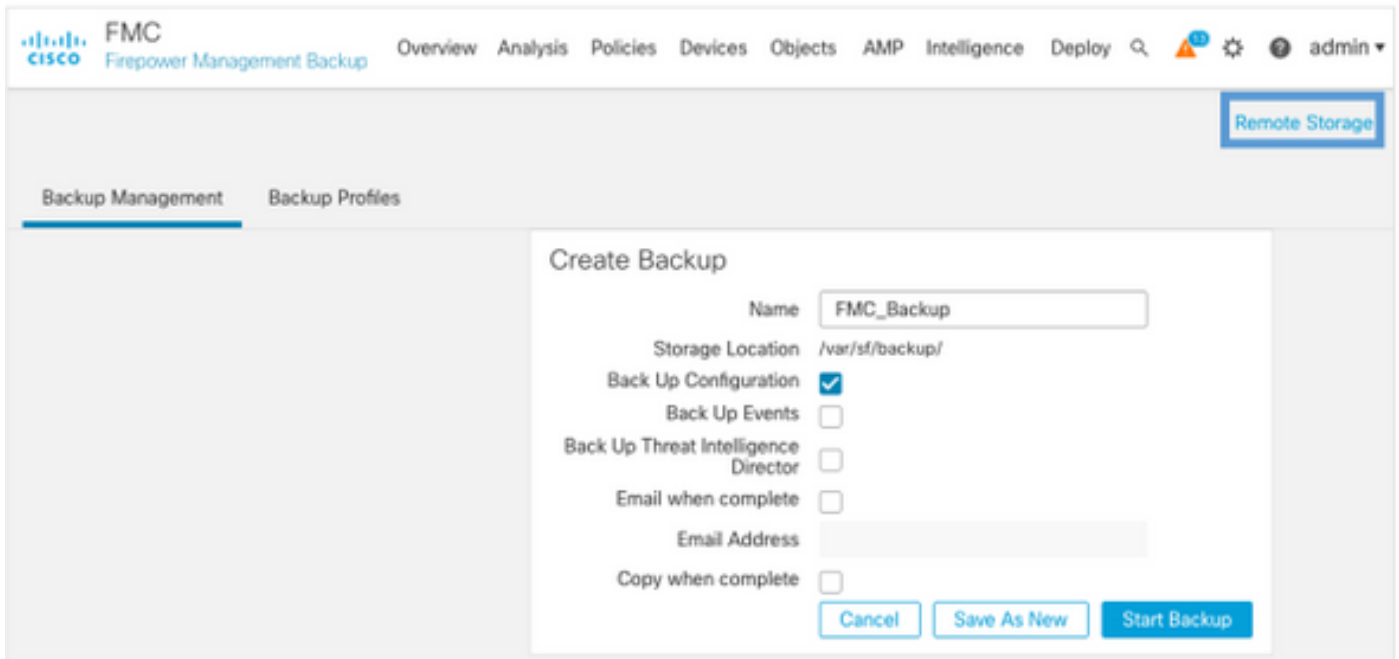


## 建立FMC備份

備份是一個重要的災難恢復步驟，在升級發生災難性故障時可以恢復配置。

1. 導覽至**System > Tools > Backup/Restore**。
2. 選擇**Firepower Management Backup**。
3. 在「**Name**」欄位中，輸入備份名稱。
4. 選擇儲存位置和應包括在備份中的資訊。
5. 按一下**Start Backup**。
6. 在**通知>任務**中，監視備份建立進度。

**提示：**強烈建議備份到安全的遠端位置並驗證傳輸成功。可以從「**備份管理**」頁配置遠端儲存。



有關詳情，請參閱：

- [Firepower管理中心配置指南7.0版 — 章節：備份和還原](#)
- [Firepower管理中心配置指南7.0版 — 遠端儲存管理](#)

## 驗證NTP同步

要成功升級FMC，需要NTP同步。要檢查NTP同步，請完成以下步驟：

1. 導覽至System > Configuration > Time。
2. 驗證NTP狀態。

附註：狀態：「正在使用」表示裝置已與NTP伺服器同步。

Current Setting	Via NTP (based on System Configuration <a href="#">Time Synchronization</a> )			
Current Time	2021-09-21 13:50			
NTP Server	Status	Authentication	Offset	Last Update
173.38.201.115	Being Used	none	+0.011(milliseconds)	126(seconds)
173.38.201.67	Available	none	+0.042(milliseconds)	223(seconds)
127.127.1.1	Unknown	none	+0.000(milliseconds)	12d(seconds)

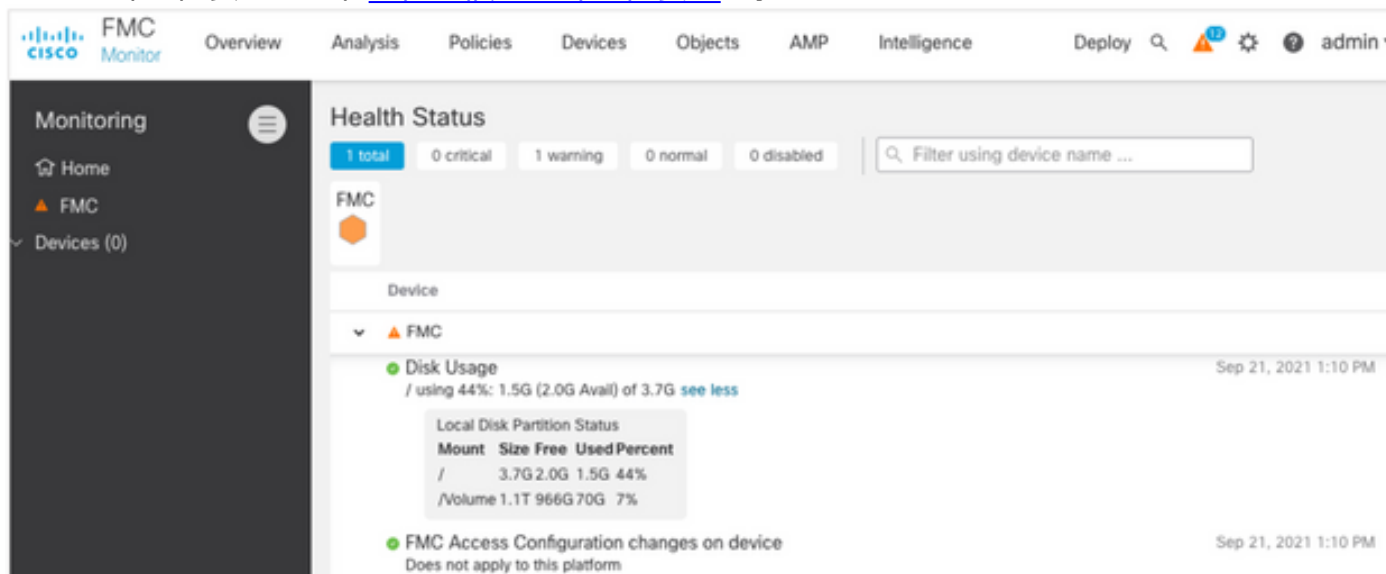
有關詳細資訊，請參閱[Firepower管理中心配置指南7.0版 — 時間和時間同步](#)。

## 驗證磁碟空間

根據FMC型號和目標版本，確保有足夠的可用磁碟空間，否則升級失敗。要檢查可用的FMC磁碟空間，請完成以下步驟：

1. 導航到System > Health > Monitor。

2. 選擇FMC。
3. 展開選單並搜尋磁碟使用情況。
4. 磁碟空間要求可以在[時間測試](#)和[磁碟空間要求](#)中找到。

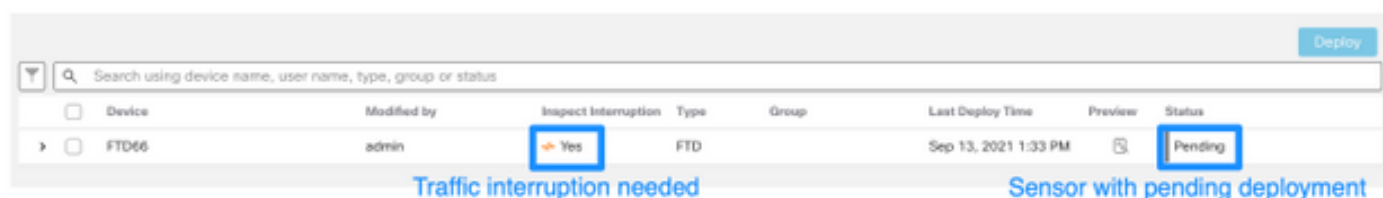


## 部署所有掛起策略更改

在安裝更新或補丁之前，需要將更改部署到感測器中。為了確保部署所有待處理的更改，請完成以下步驟：

1. 導航到**部署>部署**。
2. 選擇清單中的所有裝置並**部署**。

**注意：** Inspect Interruption列指示流量中斷



## 運行Firepower軟體就緒性檢查

就緒性檢查評估Firepower裝置對軟體升級的準備情況。

要執行軟體就緒檢查，請完成以下步驟：

1. 導覽至**System > Updates**。
2. 選擇目標版本旁邊的**安裝**圖示。
3. 選擇FMC並按一下**Check Readiness**。
4. 在彈出視窗中，按一下**OK**。
5. 通過**Notifications > Tasks**監控Readiness Check流程。

有關詳細資訊，請參閱[Cisco Firepower管理中心升級指南 — Firepower軟體就緒性檢查](#)。

## FMC升級後的首要任務

### 部署所有掛起策略更改

每次安裝更新或補丁後，必須立即將更改部署到感測器中。為了確保部署所有待處理的更改，請完成以下步驟：

1. 導航到**部署>部署**。
2. 選擇清單中的所有裝置，然後按一下**Deploy**。

**注意：**Inspect Interruption列指示流量中斷

### 驗證是否已安裝最新的漏洞和指紋資料庫

若要驗證目前的指紋(VDB)版本，請完成以下步驟：

1. 導航到**幫助>關於**。
2. 驗證**VDB**版本。

要直接從cisco.com下載VDB更新，需要從FMC到cisco.com的可訪問性。

1. 導航至**System > Updates > Product Updates**。
2. 選擇**Download updates**。
3. 安裝可用的最新版本。
4. 之後必須重新部署感測器。

**附註：** 如果FMC無法訪問Internet，則可以直接從software.cisco.com下載VDB包。

建議安排執行自動VDB包下載和安裝的任務。

作為一種好的做法，每天檢查VDB更新，並在週末將其安裝在FMC上。

若要從[www.cisco.com](http://www.cisco.com)每天檢查VDB，請完成以下步驟：

1. 導航到**System > Tools > Scheduling**。
2. 按一下**Add Task**。
3. 在「**Job Type**」下拉式清單中選擇「**Download Latest Update**」。
4. 要運行計畫任務，請按一下**Recurring**單選按鈕。
5. 每天重複此任務，並在凌晨3:00或工作時間以外運行它。
6. 對於**更新專案**，請選中**Vulnerability Database**覈取方塊。

New Task

Job Type: Download Latest Update

Schedule task to run:  Once  Recurring

Start On: September 13, 2021 Europe/Warsaw

Repeat Every: 1 Days

Run At: 3:00 Am

Job Name: Downloading Latest VDB

Update Items:  Software  Vulnerability Database

Comment: Daily task to download latest Vulnerability (VDB) database

Email Status To: admin@acme.com

Cancel Save

為了將最新的VDB安裝到FMC中，請設定每週定期任務：

1. 導航到**System > Tools > Scheduling**。
2. 按一下**Add Task**。
3. 在「**Job Type**」下拉選單中，選擇「**Install Latest Update**」。
4. 要運行計畫任務，請按一下**Recurring**單選按鈕。
5. 每1週重複此任務，並在凌晨5:00或工作時間以外運行它。
6. 對於**更新專案**，請選中**Vulnerability Database**覈取方塊。

New Task

Job Type: Install Latest Update

Schedule task to run:  Once  Recurring

Start On: September 13, 2021 (Europe/Warsaw)

Repeat Every: 1 (Weeks)

Run At: 5:00 Am

Repeat On:  Sunday  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday

Job Name: Install VDB in FMC

Update Items:  Software  Vulnerability Database

Device: fmc70

Comment: Install the latest available VDB into FMC

Email Status To: admin@acme.com

Cancel Save

有關詳細資訊，請參閱[Firepower管理中心配置指南7.0版 — 更新漏洞資料庫\(VDB\)](#)

## 驗證Snort規則和輕型安全包當前版本

若要驗證目前的Snort規則(SRU)、輕量型安全套件(LSP)和地理定位版本，請完成以下步驟：

1. 導航到**幫助>關於**。
2. 驗證**規則更新版本**和**LSP版本**。

要直接從[www.cisco.com](http://www.cisco.com)下載SRU和LSP，需要從FMC訪問[www.cisco.com](http://www.cisco.com)。

1. 導航到**System > Updates > Rule Updates**。
2. 在**One-Time Rule Update/Rules Import**頁籤中，選擇**Download new rule update from the Support Site**。
3. 選擇**Import**。
4. 之後將配置部署到感測器。

**附註：**如果FMC無法訪問Internet，則可以從[software.cisco.com](http://software.cisco.com)直接下載SRU和LSP軟體包。

入侵規則更新是累積性的，建議始終匯入最新更新。

若要啟用snort規則更新(SRU/LSP)的每週下載和部署，請完成以下步驟：

1. 導航到**System > Updates > Rule Updates**。
2. 在**Recurring Rule Update Imports**頁籤中，選中**Enable Recurring Rule Update Imports from the Support Site**覆取方塊。



3. 將匯入頻率選擇為每週，選擇每週一天和下午晚些時間進行下載和策略部署。
4. 按一下「Save」。

Recurring Rule Update Imports

The scheduled rule update has not yet run.  
Note: importing will discard all unsaved intrusion policy and network analysis policy edits.

Enable Recurring Rule Update Imports from the Support Site

Import Frequency Weekly on Monc at 10:00 PM Europe/Warsaw

Policy Deploy  Deploy updated policies to targeted devices after rule update completes

Cancel Save

有關詳細資訊，請參閱[Firepower管理中心配置指南7.0版 — 更新入侵規則](#)。

## 驗證地理位置更新當前版本

要驗證當前的地理定位版本，請完成以下步驟：

1. 導航到**幫助>關於**。
2. 驗證地址**更新版本**。

要直接從[www.cisco.com](http://www.cisco.com)下載地理位置更新，需要從FMC訪問[www.cisco.com](http://www.cisco.com)。

1. 導航到**System > Updates > Geolocation Updates**。
2. 在**One-Time Geolocation Update**頁籤中，選擇**Download and install geolocation update from the Support Site**。
3. 按一下「Import」（匯入）。

**附註：**如果FMC無法訪問Internet，則可直接從[software.cisco.com](http://software.cisco.com)下載Geolocation Updates軟體包。

若要啟用自動地理位置更新，請完成以下步驟：

1. 導航到**System > Updates > Geolocation Updates**。
2. 在Recurring Geolocation Updates部分，選中**Enable Recurring Weekly Updates from the Support Site**覈取方塊。
3. 選擇匯入頻率為每週，選擇星期一的午夜。
4. 按一下「Save」。

Recurring Geolocation Updates

Enable Recurring Weekly Updates from the Support Site

Update Start Time Monday 12:00 AM Europe/Warsaw

Cancel Save

有關詳細資訊，請參閱[Firepower管理中心配置指南7.0版 — 更新地理位置資料庫\(GeoDB\)](#)。

## 通過計畫任務自動更新URL過濾資料庫

為了確保URL過濾的威脅資料是最新的，系統必須從思科綜合安全情報(CSI)雲獲取資料更新。要自動執行此過程，請執行以下步驟：

1. 導航到**System > Tools > Scheduling**。
2. 按一下**Add Task**。
3. 在「**Job Type**」下拉選單中，選擇**Update URL Filtering Database**。
4. 要運行計畫任務，請按一下**Recurring**單選按鈕。
5. 每週重複此任務，並在星期日晚上8:00或工作時間以外運行它。
6. 按一下「**Save**」。

New Task

Job Type: Update URL Filtering Database

Schedule task to run:  Once  Recurring

Start On: September 13, 2021 Europe/Warsaw

Repeat Every: 1  Hours  Days  Weeks  Months

Run At: 8:00 Pm

Repeat On:  Sunday  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday

Job Name: Update URL Filtering Database

Comment: This task downloads the latest URL Filtering Database

Email Status To: admin@acme.com

Cancel Save

有關詳細資訊，請參閱[Firepower管理中心配置指南7.0版 — 使用計畫任務自動進行URL過濾更新](#)。

## 配置定期備份

作為災難恢復計畫的一部分，建議執行定期備份。

1. 確保您位於全域性域中。
2. 建立FMC備份配置檔案。有關更多資訊，請參閱**建立FMC備份**部分。
3. 導航到**System > Tools > Scheduling**。
4. 按一下**Add Task**。
5. 在「**Job Type**」下拉式清單中選擇「**Backup**」。
6. 要運行計畫任務，請按一下**Recurring**單選按鈕。  
必須調整備份頻率以適應組織的需要。建議在維護時段或其他使用率較低的時段建立備份。
7. 對於**Backup Type**，請按一下**Management Center**單選按鈕。
8. 在「**Backup Profile**」下拉式清單中選擇「**Backup Profile**」。
9. 按一下「**Save**」。

New Task

Job Type

Schedule task to run  Once  Recurring

Start On    UTC

Repeat Every   Hours  Days  Weeks  Months

Run At

Repeat On  Sunday  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday

Job Name

Backup Type  Management Center  Device

Backup Profile

Comment

Email Status To

有關詳細資訊，請參閱[Firepower管理中心配置指南7.0版 — 章節：備份和還原](#)。

## 確保已註冊智慧許可證

若要使用思科智慧軟體管理器註冊思科防火牆管理中心，請完成以下步驟：

1. 在<https://software.cisco.com>中，導覽至Smart Software Manager > Manage licenses。
2. 導航到Inventory > General頁籤，然後建立New Token。
3. 在FMC UI中，導航至System > Licenses > Smart Licenses。
4. 按一下「Register」。
5. 插入在思科智慧軟體許可門戶中生成的令牌。
6. 確保Cisco Success Network已啟用。
7. 按一下「Apply Changes」。
8. 驗證智慧許可證狀態。

### Smart Licensing Product Registration

Product Instance Registration Token:

```
MGI0ZGJhNTEtOTIxYy00ZGM2LWJjMTctNWE1ZTY5YWUxZGExLTE2NjQwMTUz%0AMDQ0OTZ8bTQxTWJDbmJJWVld3hQMGS4bytHdU4wVzNvRWRZM1pjbk.J4Nkcr%0A!
```

If you do not have your ID token, you may copy it from your Smart Software manager under the assigned virtual account. [Cisco Smart Software Manager](#)

The Management Center establishes a secure connection to the Cisco Cloud so that it can participate in additional service offerings from Cisco. Management Center will establish and maintain this secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network and Cisco Support Diagnostics. Disabling these services will disconnect the device from the cloud.

#### Cisco Success Network

The Cisco Success Network provides usage information and statistics to Cisco. This information allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. Check out the [sample data](#) that will be sent to Cisco.

Enable Cisco Success Network

#### Cisco Support Diagnostics

The Cisco Support Diagnostics capability provides entitled customers with an enhanced support experience by allowing Cisco TAC to collect essential information from your devices during the course of a TAC case. Additionally, Cisco will periodically collect configuration

Internet connection is required.

[Cancel](#) [Apply Changes](#)

有關詳細資訊，請參閱[Firepower管理中心配置指南7.0版 — 註冊智慧許可證](#)。

## 檢視變數集的配置

確保HOME\_NET變數僅包含組織中的內部網路/子網。變數集定義不當會對防火牆的效能產生負面影響。

1. 導航到**對象 > 變數集**。
2. 編輯入侵策略使用的變數集。允許每個具有不同設定的入侵策略設定一個變數。
3. 根據您的環境調整變數，然後按一下**Save**。

其他重要的變數是DNS\_SERVERS或HTTP\_SERVERS。

有關詳細資訊，請參閱[Firepower管理中心配置指南7.0版 — 變數集](#)。

## 驗證雲服務啟用

為了利用不同的雲服務，n導航到**System > Integration > Cloud Services**。

## URL篩選

1. 啟用URL過濾並允許自動更新，開啟Query Cisco Cloud for Unknown URL。  
更頻繁的快取URL過期需要對雲進行更多查詢，這會導致Web載入速度變慢。
2. 保存更改。

提示：對於快取URL過期，請保留預設值**Never**。如果需要更嚴格的網路重新分類，可以相應地修改此設定。

## AMP網路版

1. 確保兩個設定均開啟：**啟用自動本地惡意軟體檢測更新並與思科共用惡意軟體事件的URI**。
2. 在FMC 6.6.X中，停用用於網路的AMP的舊版連線埠32137，因此使用的TCP連線埠為443。
3. 保存更改。

附註：FMC 7.0+中不再提供此設定，並且埠始終為443。

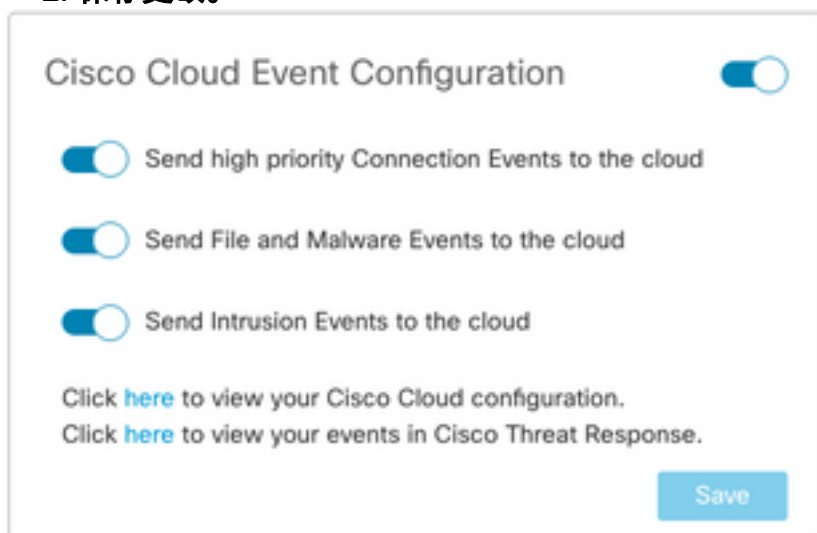
## 思科雲端區域

1. 雲區域需要與SecureX組織區域相匹配。如果未建立SecureX組織，請選擇接近FMC安裝的區域：APJ地區、EU地區或US地區。
2. 保存更改。

## 思科雲端事件組態

### 對於FMC 6.6.x

1. 確保全部三個選項：**選擇向雲傳送高優先順序連線事件、向雲傳送檔案和惡意軟體事件以及向雲傳送入侵事件等。**
2. 保存更改。



Cisco Cloud Event Configuration

Send high priority Connection Events to the cloud

Send File and Malware Events to the cloud

Send Intrusion Events to the cloud

Click [here](#) to view your Cisco Cloud configuration.

Click [here](#) to view your events in Cisco Threat Response.

Save

### 適用於FMC 7.0+

1. 確保同時選擇了兩個選項：**將入侵事件傳送到雲並將檔案及惡意軟體事件傳送到雲。**
2. 對於連線事件的型別，如果正在使用安全分析和日誌記錄解決方案，請選擇**All**。對於SecureX，僅選擇**Security Events**。
3. 保存更改。

Cisco Cloud Event Configuration

Send Intrusion Events to the cloud

Send File and Malware Events to the cloud

Send Connection Events to the cloud:

None  Security Events  All

Save

## 啟用SecureX整合

通過SecureX整合，您可以即時瞭解思科安全產品的威脅形勢。要連線SecureX並啟用功能區，請執行以下步驟：

### 整合SecureX功能區

**附註：**此選項可用於FMC 7.0+版。

1. 登入到SecureX並建立API客戶端：在「**Client Name**」欄位中，輸入FMC的描述性名稱。例如，FMC 7.0 API客戶端。按一下「**Oauth Code Clients**」索引標籤。在「**Client Preset**」下拉選單中，選擇「**Ribbon**」。它選擇範圍：案例手冊，豐富：閱讀，全球英特爾：閱讀，檢查：閱讀，通知，軌道，專用英特爾，配置檔案，響應，遙測：寫入。新增在FMC中顯示的兩個重新導向URL：

**重定向URL:**<FMC\_URL>/securex/oauth/callback

**第二個重定向URL:**<FMC\_URL>/securex/testcallback

1. 在「**Availability**」下拉選單中，選擇「**Organization**」。按一下「**Add New Client**」。

### Add New Client with 10 scopes ✕

Client Name\*

Client Preset  
 ✕ ▾

API Clients    OAuth Code Clients

**Scopes\*** [Select All](#)

🔍

<input checked="" type="checkbox"/> Response	List and execute response actions using configured modules
<input type="checkbox"/> SSE	SSE Integration. Manage your Devices.
<input checked="" type="checkbox"/> Telemetry:write	collect application data for analytics - Write Only
<input type="checkbox"/> Users	Manage users of your organisation
<input type="checkbox"/> Webhook	Manage your Webhooks

**Redirect URL\***

**Redirect URL\*** Delete

Add another Redirect URL

**Availability\***  
 ▾

**Description**


- 2.從FMC導航至System > SecureX。
- 3.開啟右上角的切換按鈕，並確認顯示的區域與SecureX組織匹配。
- 4.複製使用者端ID和使用者端密碼，然後將其貼上到FMC中。
- 5.選擇測試配置。

6. 登入到SecureX以授權API客戶端。
7. 儲存更改並刷新瀏覽器，以檢視底部顯示的功能區。
8. 展開Ribbon並選擇**Get SecureX**。如果出現提示，請輸入SecureX憑據。
9. SecureX功能區現已對您的FMC使用者完全正常工作。

### SecureX Configuration

This feature allows FMC to integrate with other SecureX services via SecureX ribbon.

Follow these steps to configure SecureX

1. Confirm your cloud region  
Currently selected region: `api-sse.cisco.com`  
To change the cloud region, go to [System / Integration / Cloud Services](#).
2. Create a SecureX API client   
Copy and paste the URL below into the "Redirect URL" field:  
[Copy to Clipboard](#)  
`https://10.62.184.21/securex/oauth/callback`  
Then click on "Add another Redirect URL" and copy and paste the URL below:  
[Copied](#)  
`https://10.62.184.21/securex/testcallback`
3. Enter the Client ID and password  
Client ID   
Client Password   
 Show Password

5YVPsGdzrkX8q8q0yYI-tDitezO6p\_17MtH6NATx68fUZ5u9T3qOEq

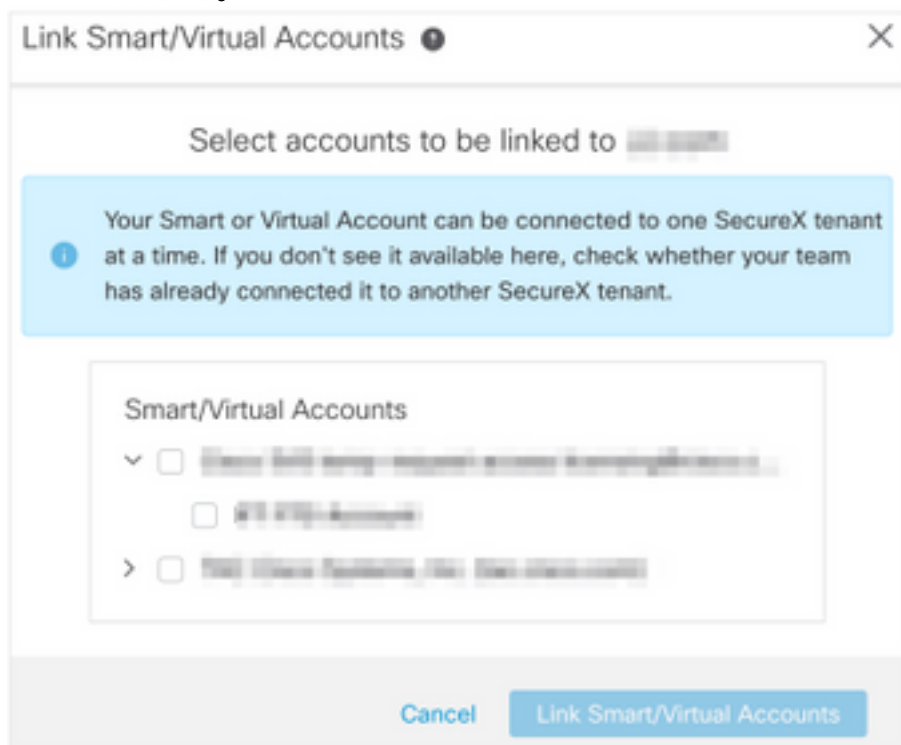
**附註：**如果任何其他FMC使用者需要訪問功能區，則該使用者需要使用SecureX憑據登入功能區。

### 將連線事件傳送到SecureX

1. 在FMC中，導覽至**System > Integration > Cloud Services**，並確保**Cisco Cloud Event Configuration**傳送入侵、檔案和惡意軟體事件，如**啟用雲服務**一節所述。
2. 確保FMC已註冊到智慧許可證，如**註冊智慧許可證**部分所述。



3. 記下System > Licenses > Smart Licenses下的Assigned virtual Account名稱，該名稱顯示在FMC中。
4. 在SecureX中註冊FMC: 在SecureX中，導航到**管理>裝置**。選擇**Manage Devices**。確保瀏覽器中允許彈出視窗。登入到安全服務交換(SSE)。導航到**工具選單>連結智慧/虛擬帳戶**。選擇**Link more accounts**。選擇分配給FMC的虛擬帳戶 ( 步驟3 )。選擇**Link Smart/Virtual Accounts**。



- 確保「Devices ( 裝置 )」中列出了FMC裝置。
  - 導航到**Cloud Services**頁籤，啟用**Cisco SecureX威脅響應**和**Eventing** 功能。
  - 選擇Eventing功能旁邊的**Additional service settings** ( 齒輪圖示 )。
  - 在General頁籤中，選擇**Share event data with Talos**。
  - 在「自動升級事件」頁籤的「按事件型別」部分中，選擇所有可用的事件型別和**儲存**。
- 5.在SecureX主門戶中，導航到**整合模組> Firepower**，然後新增Firepower整合模組。
  - 6.建立新儀表板。
  - 7.新增與Firepower相關的磁貼。

## 整合安全終端 ( 面向終端的AMP )

要啟用與您的Firepower部署的安全終端 ( 面向終端的AMP ) 整合，請執行以下步驟：

1. 導覽至**AMP > AMP Management**。
2. 選擇**Add AMP Cloud Connection**。
3. 選擇雲和註冊。

**附註：** 狀態**Enabled**表示已建立與雲的連線。

## 整合 安全惡意軟體分析(Threat Grid)

預設情況下，Firepower管理中心可以連線到公共Cisco Threat Grid雲以進行檔案提交和報告檢索。

無法刪除此連線。儘管如此，還是建議選擇最接近您的部署雲的位置：

1. 導航到AMP > Dynamic Analysis Connections。
2. 在「操作」部分中按一下編輯 (鉛筆圖示)。
3. 選擇正確的雲名稱。
4. 要將Threat Grid帳戶與詳細報告和高級沙盒功能相關聯，請按一下Associate圖示。

有關詳細資訊，請參閱[Firepower管理中心配置指南7.0版 — 在公共雲中啟用對動態分析結果的訪問](#)。

有關內部部署執行緒網格裝置整合，請參閱[Firepower管理中心配置指南7.0版 — 動態分析內部部署裝置\(Cisco Threat Grid\)](#)。