配置用於ASA遷移的安全防火牆遷移工具

目錄

簡介

本檔案介紹將思科調適型安全裝置(ASA)遷移至思科Firepower的過程。

作者：Ricardo Vera，思科TAC工程師。

必要條件

需求

思科建議您瞭解思科防火牆威脅防禦(FTD)和自適應安全裝置(ASA)。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 具備Firepower遷移工具(FMT)v3.0.1的Windows PC
- 自適應安全裝置(ASA)v9.16.1
- 安全防火牆管理中心(FMCv)v7.0.1
- 安全防火牆威脅防御虛擬(FTDv)v7.0.1

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。

本文檔的具體要求包括：

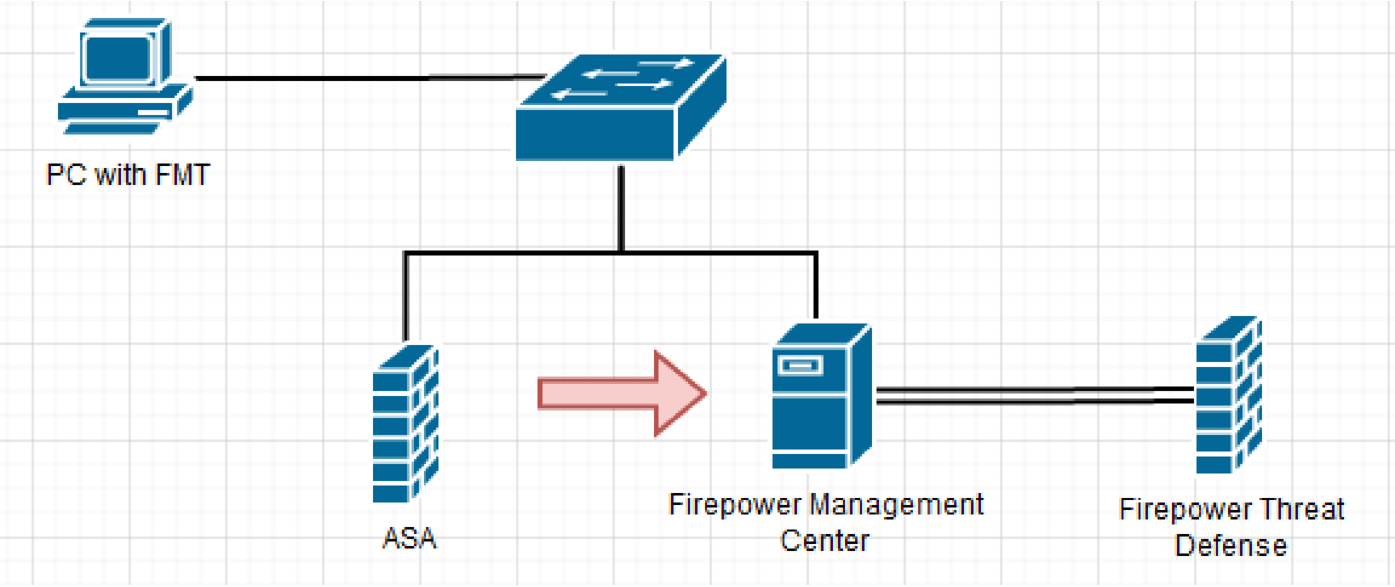
- Cisco Adaptive Security Appliance(ASA)版本8.4或更高版本
- 安全防火牆管理中心(FMCv)版本6.2.3或更高版本

防火牆遷移工具支援以下裝置清單：

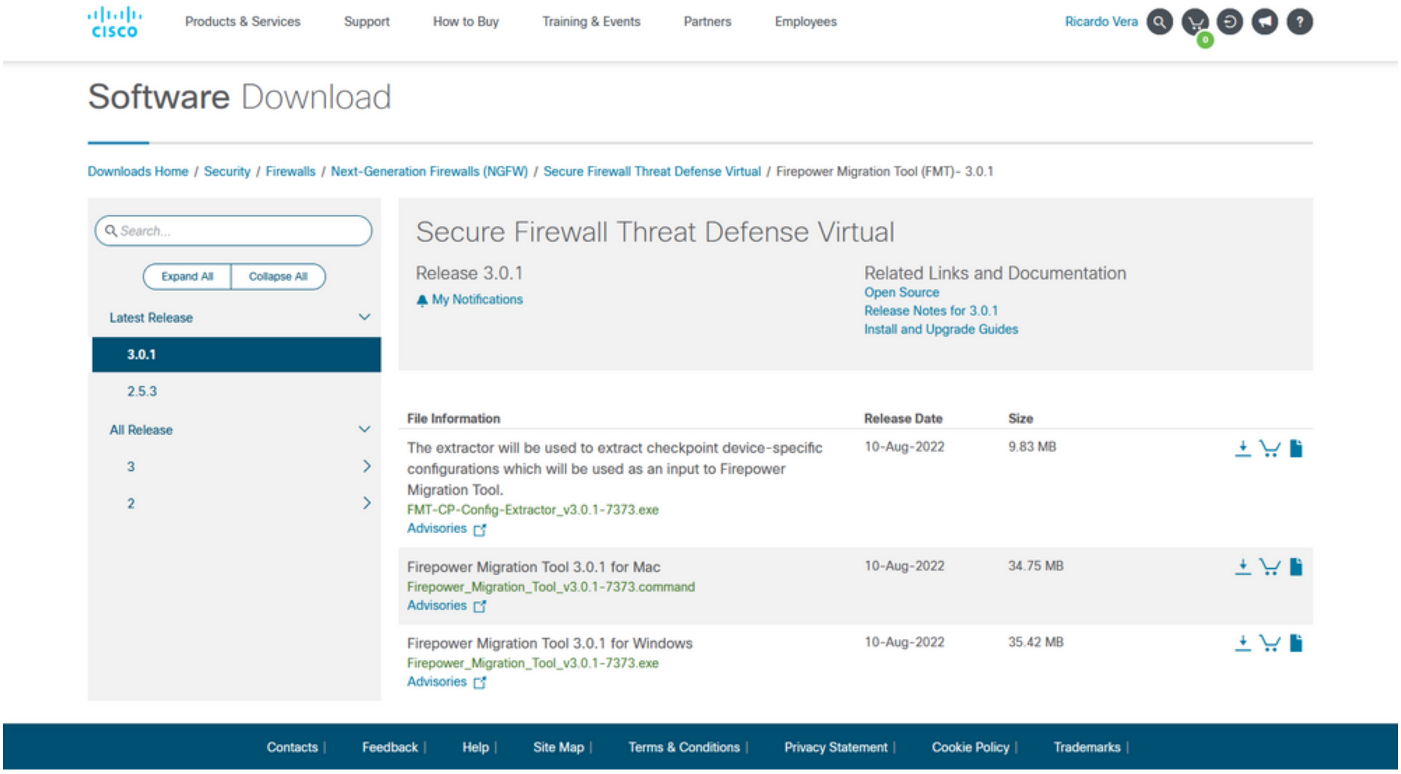
- Cisco ASA(8.4+)
- 具備FPS的Cisco ASA(9.2.2+)
- 檢查點(r75-r77)
- 檢查點(r80)
- Fortinet(5.0+)
- Palo Alto Networks(6.1+)

繼續進行遷移之前，請考慮防火牆遷移工具的准則和限制。

設定



1. **從**思科軟體中心下載最新的Firepower遷移工具：



Software Download

Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / Secure Firewall Threat Defense Virtual / Firepower Migration Tool (FMT)- 3.0.1

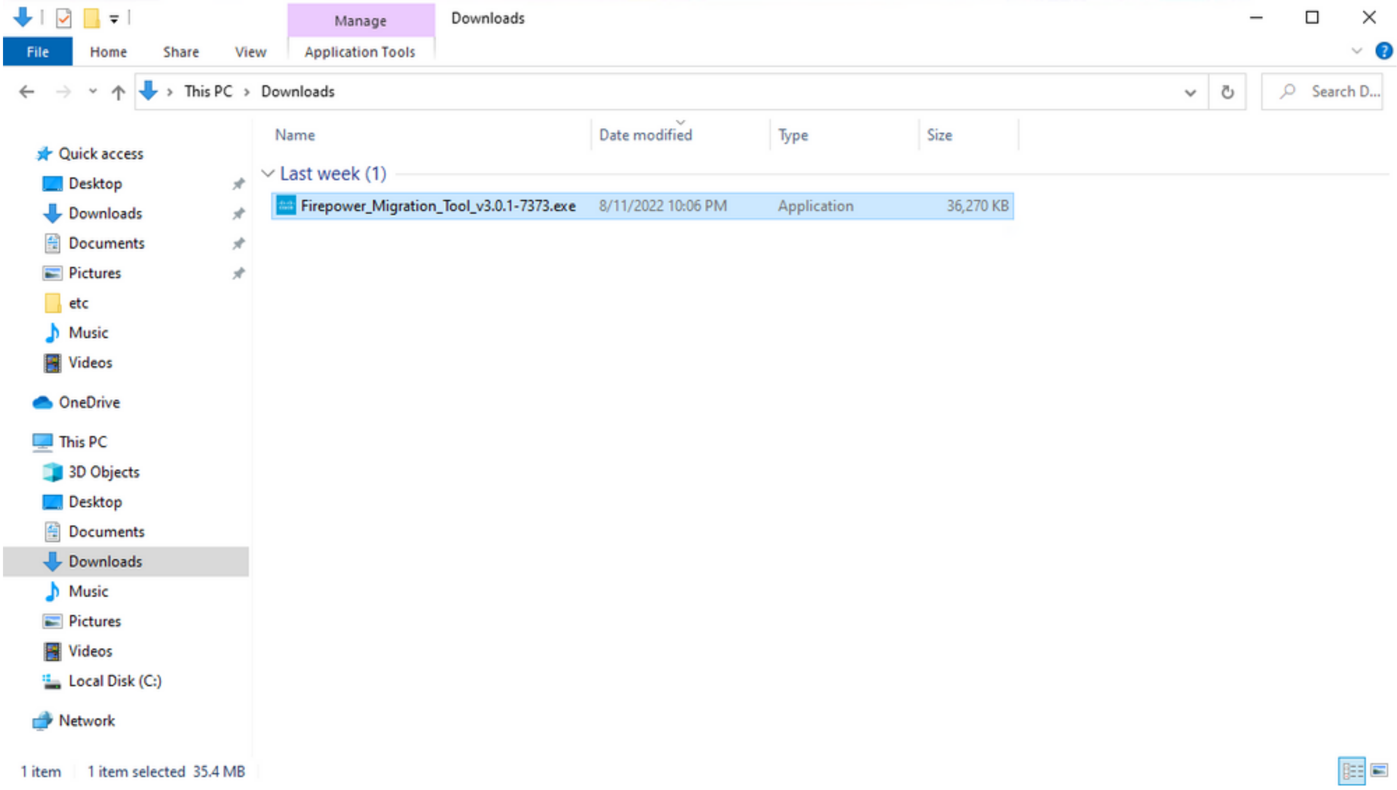
Secure Firewall Threat Defense Virtual

Release 3.0.1

Related Links and Documentation
Open Source
Release Notes for 3.0.1
Install and Upgrade Guides

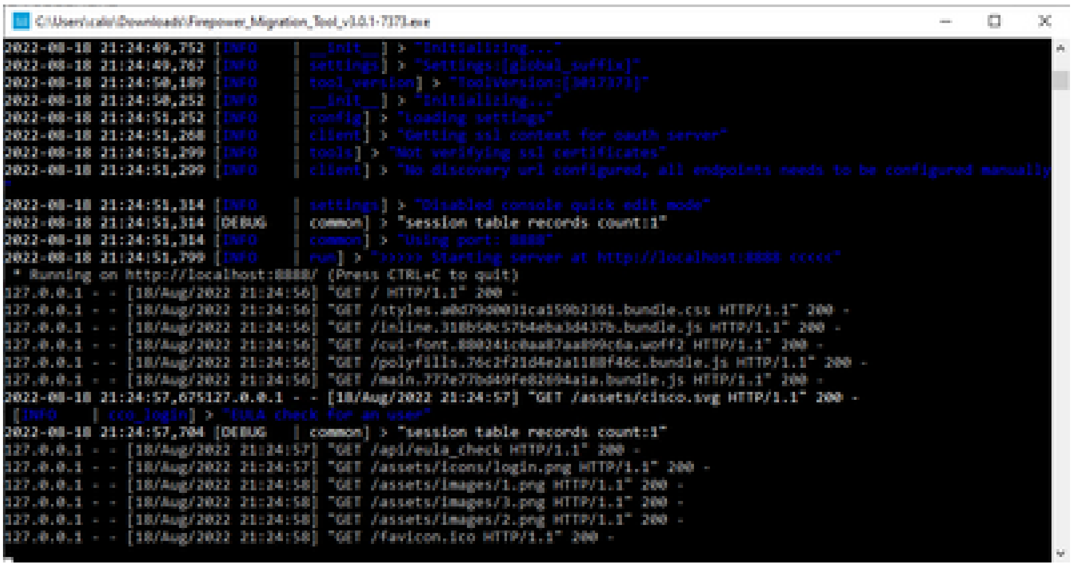
File Information	Release Date	Size
The extractor will be used to extract checkpoint device-specific configurations which will be used as an input to Firepower Migration Tool. FMT-CP-Config-Extractor_v3.0.1-7373.exe Advisories	10-Aug-2022	9.83 MB
Firepower Migration Tool 3.0.1 for Mac Firepower_Migration_Tool_v3.0.1-7373.command Advisories	10-Aug-2022	34.75 MB
Firepower Migration Tool 3.0.1 for Windows Firepower_Migration_Tool_v3.0.1-7373.exe Advisories	10-Aug-2022	35.42 MB

2. 按一下您以前下載到電腦的檔案。

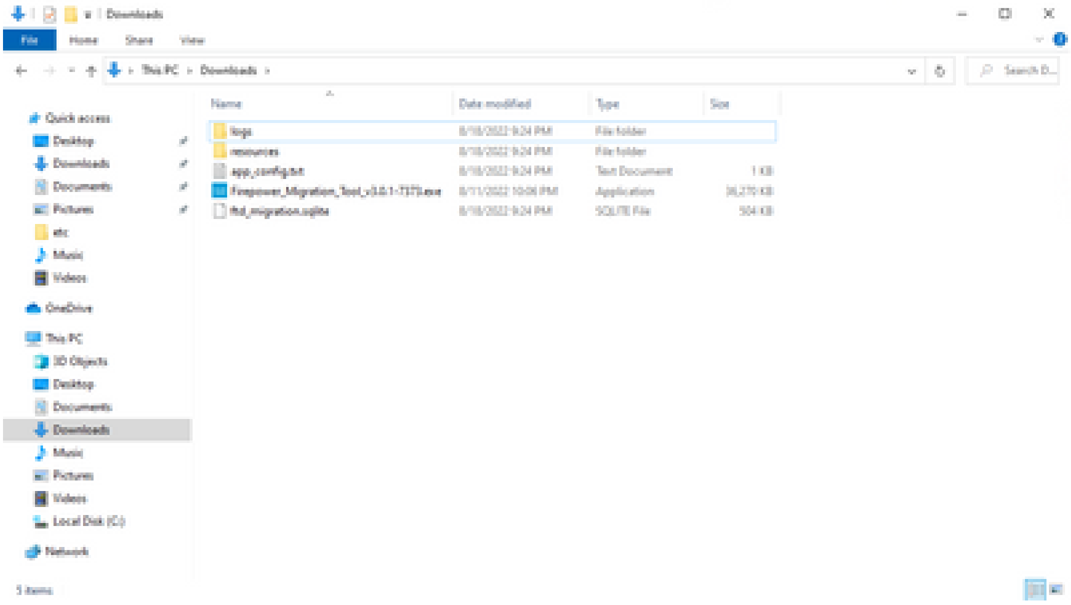


Name	Date modified	Type	Size
Firepower_Migration_Tool_v3.0.1-7373.exe	8/11/2022 10:06 PM	Application	36,270 KB

附註：該程式會自動開啟，控制檯會在您運行檔案的目錄上自動生成內容。

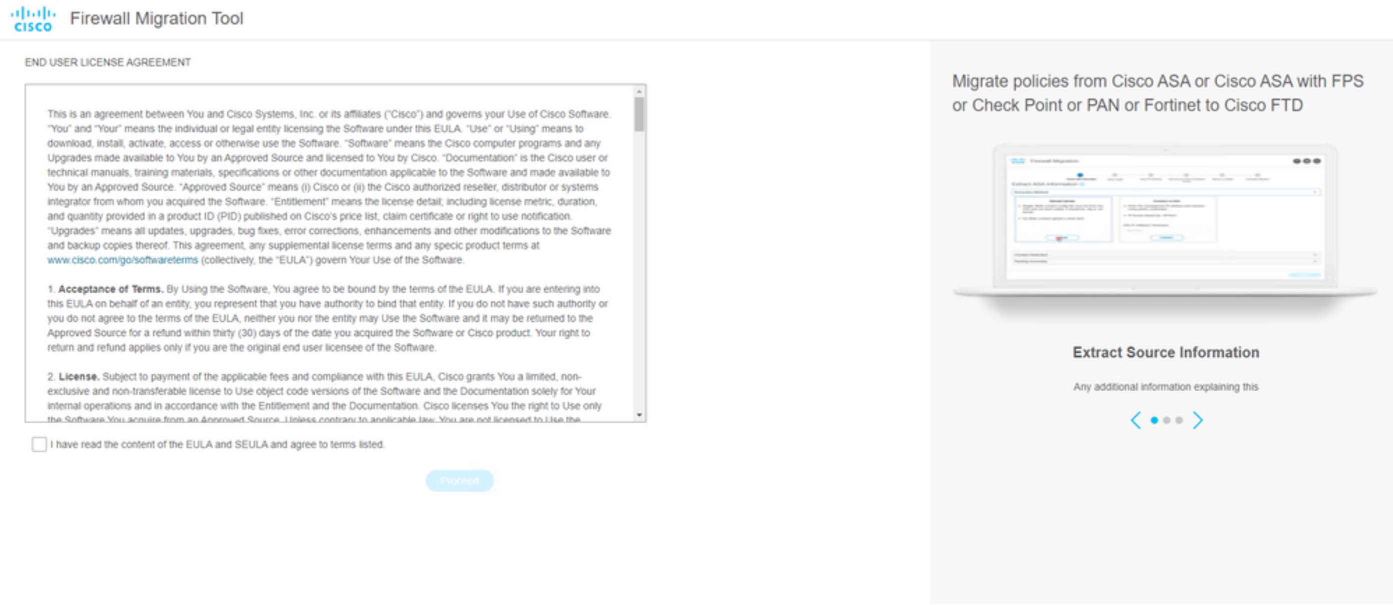

C:\Users\calo\Downloads\Firepower_Migration_Tool_v3.0.1-7373.exe

```
2022-08-18 21:24:49,752 [INFO     | __init__] > "Initializing..."
2022-08-18 21:24:49,767 [INFO     | settings] > "Settings:[global_suffix]"
2022-08-18 21:24:50,189 [INFO     | tool_version] > "ToolVersion:[3017373]"
2022-08-18 21:24:50,252 [INFO     | __init__] > "Initializing..."
2022-08-18 21:24:51,252 [INFO     | config] > "Loading settings"
2022-08-18 21:24:51,268 [INFO     | client] > "Getting ssl context for oauth server"
2022-08-18 21:24:51,299 [INFO     | tools] > "Not verifying ssl certificates"
2022-08-18 21:24:51,299 [INFO     | client] > "No discovery url configured, all endpoints needs to be configured manually
"
2022-08-18 21:24:51,314 [INFO     | settings] > "Disabled console quick edit mode"
2022-08-18 21:24:51,314 [DEBUG    | common] > "session table records count:1"
2022-08-18 21:24:51,314 [INFO     | common] > "Using port: 8888"
2022-08-18 21:24:51,799 [INFO     | run] > ">>>>> Starting server at http://localhost:8888 <<<<<"
 * Running on http://localhost:8888/ (Press CTRL+C to quit)
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /styles.a0d79d0031ca159b2361.bundle.css HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /inline.318b50c57b4eba3d437b.bundle.js HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /cui-font.880241c0aa87aa899c6a.woff2 HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /polyfills.76c2f21d4e2a1188f46c.bundle.js HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /main.777e77bd49fe82094a1a.bundle.js HTTP/1.1" 200 -
2022-08-18 21:24:57,675127.0.0.1 - - [18/Aug/2022 21:24:57] "GET /assets/cisco.svg HTTP/1.1" 200 -
 [INFO     | cco_login] > "EULA check for an user"
2022-08-18 21:24:57,704 [DEBUG    | common] > "session table records count:1"
127.0.0.1 - - [18/Aug/2022 21:24:57] "GET /api/eula_check HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:57] "GET /assets/icons/login.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /assets/images/1.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /assets/images/3.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /assets/images/2.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /favicon.ico HTTP/1.1" 200 -
```



Name	Date modified	Type	Size
logs	8/18/2022 9:24 PM	File folder	
resources	8/18/2022 9:24 PM	File folder	
app_config.txt	8/18/2022 9:24 PM	Text Document	1 KB
Firepower_Migration_Tool_v3.0.1-7373.exe	8/11/2022 10:06 PM	Application	38,270 KB
ftd_migration.sqlite	8/18/2022 9:24 PM	SQLITE File	504 KB

3. 運行該程式後，它會開啟一個顯示「終端使用者許可協定」的Web瀏覽器。 選中此覈取方塊接受條款和條件。按一下**Proceed（繼續）。**



Firewall Migration Tool

END USER LICENSE AGREEMENT

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail; including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof. This agreement, any supplemental license terms and any specic product terms at www.cisco.com/go/softwareterms (collectively, the "EULA") govern Your Use of the Software.

1. **Acceptance of Terms.** By Using the Software, You agree to be bound by the terms of the EULA. If you are entering into this EULA on behalf of an entity, you represent that you have authority to bind that entity. If you do not have such authority or you do not agree to the terms of the EULA, neither you nor the entity may Use the Software and it may be returned to the Approved Source for a refund within thirty (30) days of the date you acquired the Software or Cisco product. Your right to return and refund applies only if you are the original end user licensee of the Software.

2. **License.** Subject to payment of the applicable fees and compliance with this EULA, Cisco grants You a limited, non-exclusive and non-transferable license to Use object code versions of the Software and the Documentation solely for Your internal operations and in accordance with the Entitlement and the Documentation. Cisco licenses You the right to Use only the Software You acquire from an Approved Source. Unless contrary to applicable law, You are not licensed to Use the

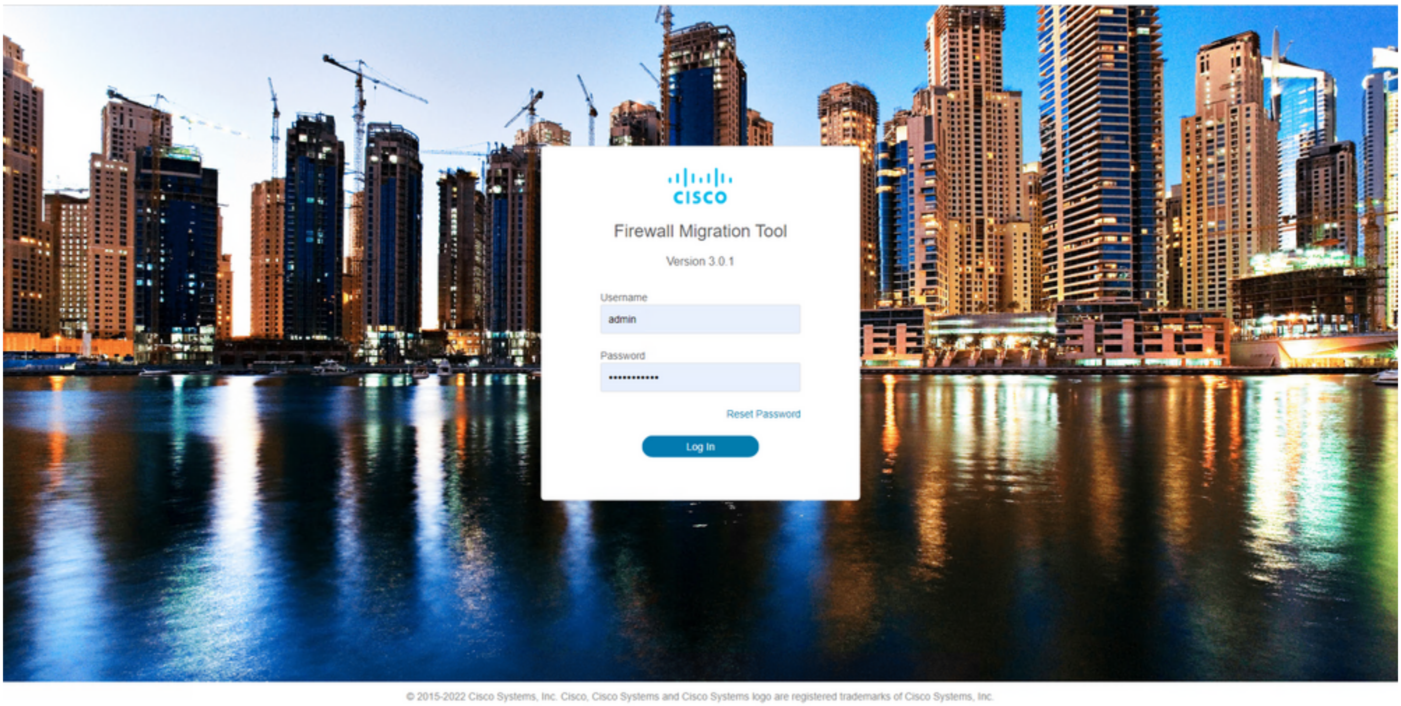
☐ I have read the content of the EULA and SEULA and agree to terms listed.

Migrate policies from Cisco ASA or Cisco ASA with FPS or Check Point or PAN or Fortinet to Cisco FTD

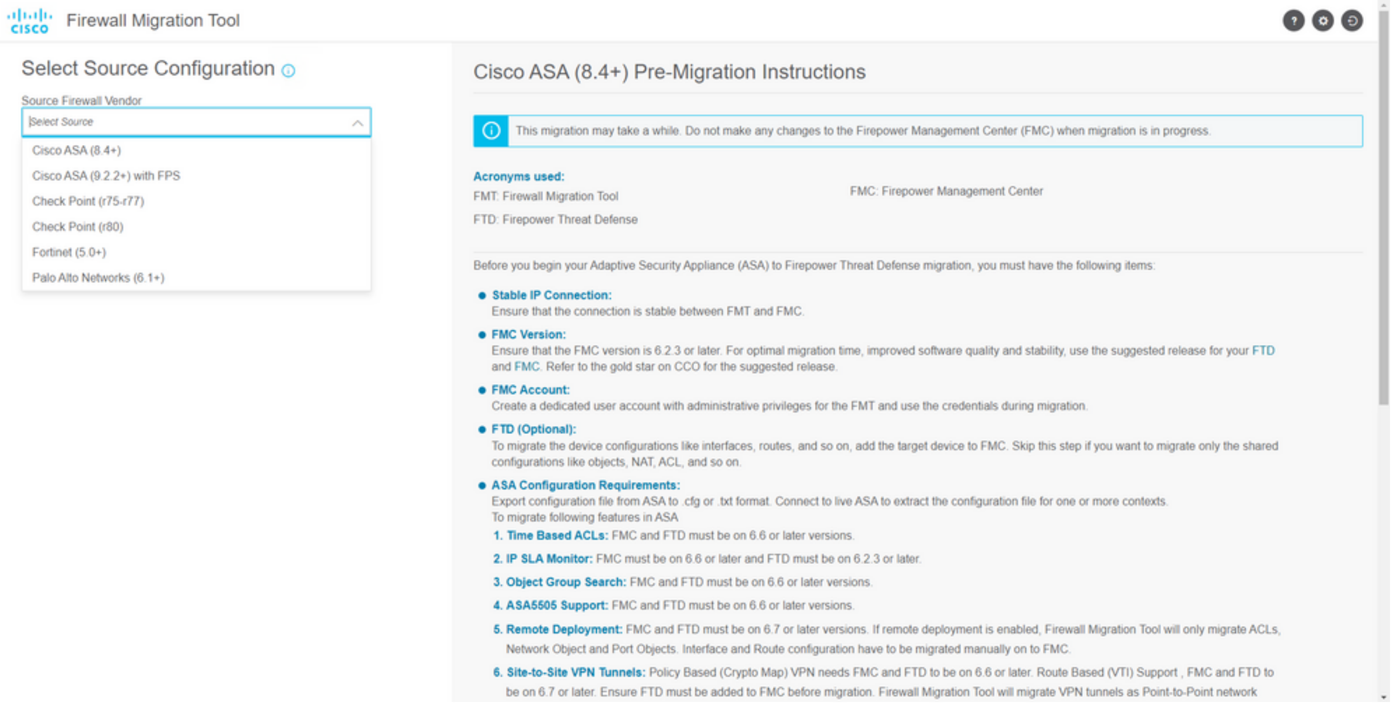
Extract Source Information

Any additional information explaining this

4. 登入到遷移工具。 您可以使用CCO帳戶或本地預設帳戶登入。　本地預設帳戶憑據為：admin/Admin123



5. 選擇要遷移的源防火牆。 在本示例中，使用Cisco ASA(8.4+)作為源。



cisco Firewall Migration Tool
Select Source Configuration
Source Firewall Vendor
Select Source
Cisco ASA (8.4+)
Cisco ASA (9.2.2+) with FPS
Check Point (r75-r77)
Check Point (r80)
Fortinet (5.0+)
Palo Alto Networks (6.1+)

Cisco ASA (8.4+) Pre-Migration Instructions

This migration may take a while. Do not make any changes to the Firepower Management Center (FMC) when migration is in progress.

Acronyms used:

FMT: Firewall Migration Tool

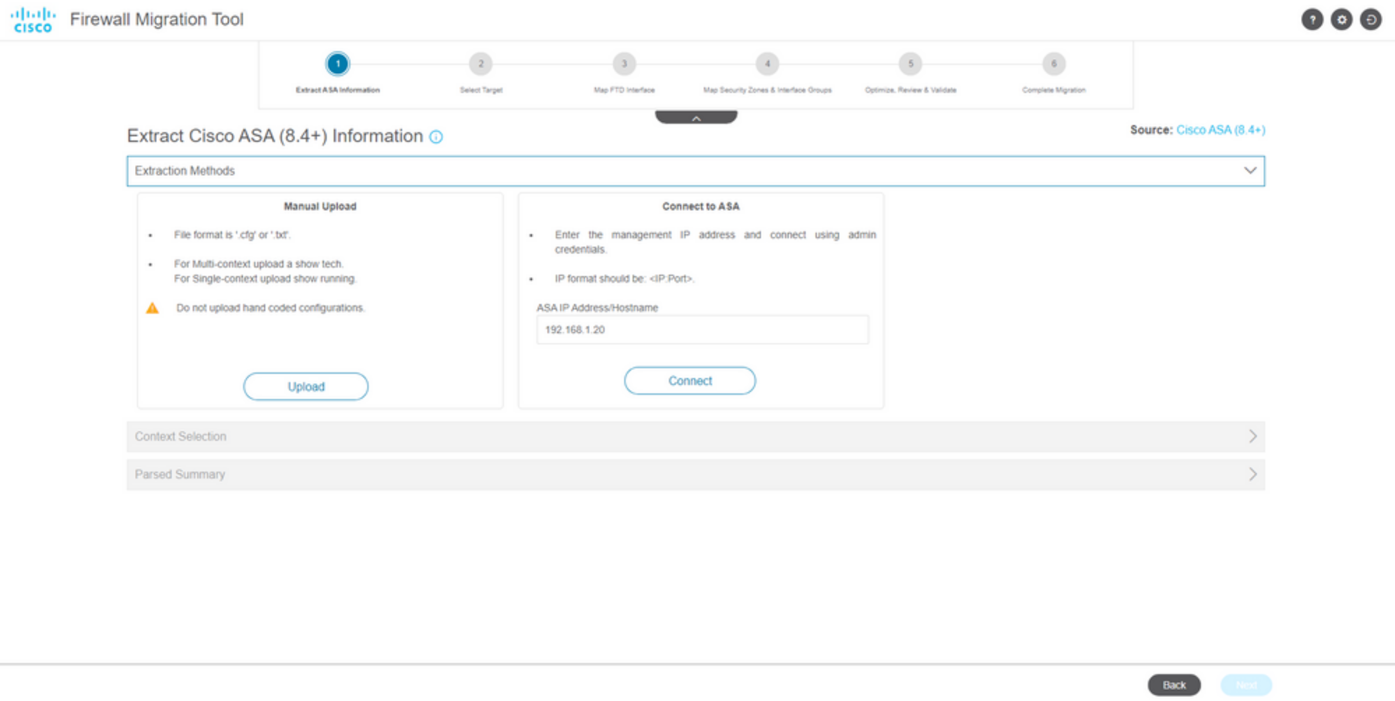
FMC: Firepower Management Center

FTD: Firepower Threat Defense

Before you begin your Adaptive Security Appliance (ASA) to Firepower Threat Defense migration, you must have the following items:

- **Stable IP Connection:**
  Ensure that the connection is stable between FMT and FMC.
- **FMC Version:**
  Ensure that the FMC version is 6.2.3 or later. For optimal migration time, improved software quality and stability, use the suggested release for your FTD and FMC. Refer to the gold star on CCO for the suggested release.
- **FMC Account:**
  Create a dedicated user account with administrative privileges for the FMT and use the credentials during migration.
- **FTD (Optional):**
  To migrate the device configurations like interfaces, routes, and so on, add the target device to FMC. Skip this step if you want to migrate only the shared configurations like objects, NAT, ACL, and so on.
- **ASA Configuration Requirements:**
  Export configuration file from ASA to .cfg or .txt format. Connect to live ASA to extract the configuration file for one or more contexts.
  To migrate following features in ASA
  1. **Time Based ACLs:** FMC and FTD must be on 6.6 or later versions.
  2. **IP SLA Monitor:** FMC must be on 6.6 or later and FTD must be on 6.2.3 or later.
  3. **Object Group Search:** FMC and FTD must be on 6.6 or later versions.
  4. **ASA5505 Support:** FMC and FTD must be on 6.6 or later versions.
  5. **Remote Deployment:** FMC and FTD must be on 6.7 or later versions. If remote deployment is enabled, Firewall Migration Tool will only migrate ACLs, Network Object and Port Objects. Interface and Route configuration have to be migrated manually on to FMC.
  6. **Site-to-Site VPN Tunnels:** Policy Based (Crypto Map) VPN needs FMC and FTD to be on 6.6 or later. Route Based (VTI) Support , FMC and FTD to be on 6.7 or later. Ensure FTD must be added to FMC before migration. Firewall Migration Tool will migrate VPN tunnels as Point-to-Point network

6. 選擇用於獲取配置的提取方法。 手動上傳需要您上傳 **Running Config** ASA檔案，格式為「.cfg」或「.txt」。連線到ASA以直接從防火牆提取配置。



Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

Extraction Methods

Manual Upload

- File format is '.cfg' or '.txt'.
- For Multi-context upload a show tech.
  For Single-context upload show running.

⚠ Do not upload hand coded configurations.

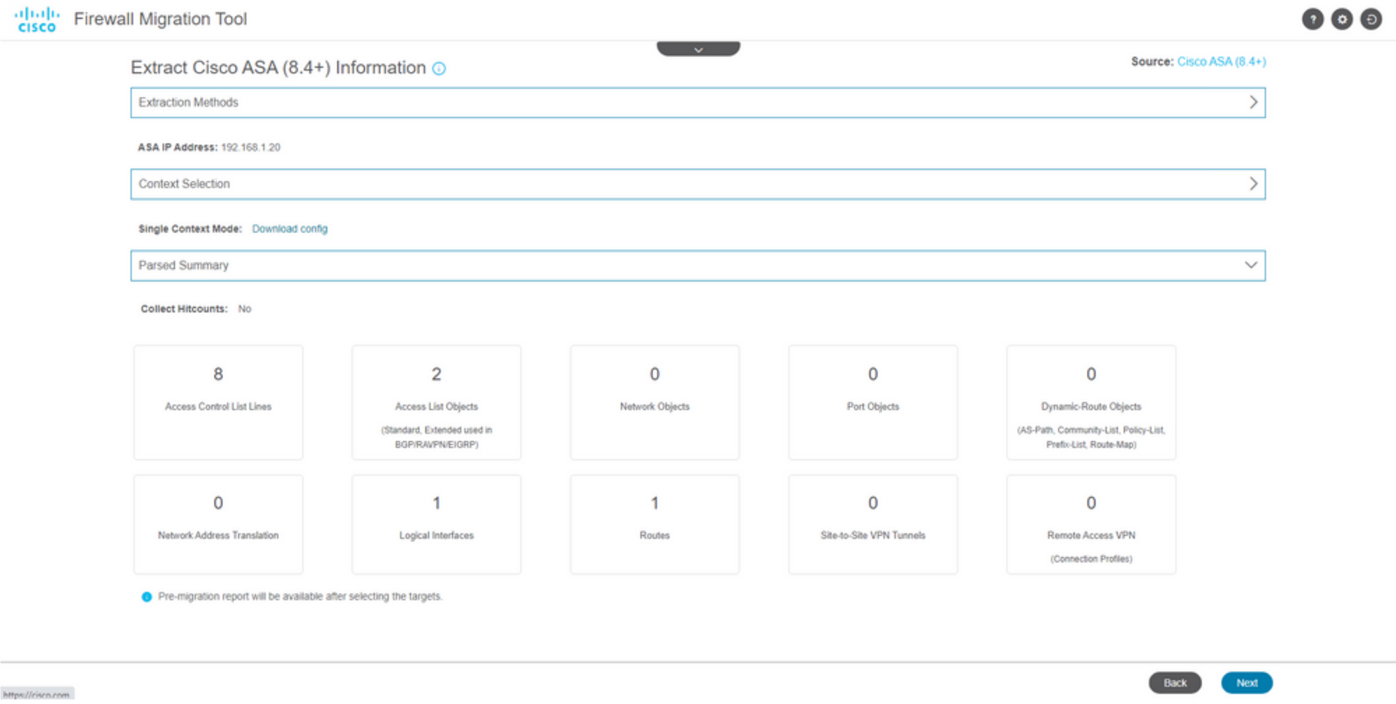
Connect to ASA

- Enter the management IP address and connect using admin credentials.
- IP format should be: <IP:Port>.

ASA IP Address/Hostname: 192.168.1.20

附註：在本示例中，直接連線到ASA。

7. 在防火牆上找到的配置摘要顯示為儀表板，請按一下**下一步**。



Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

ASA IP Address: 192.168.1.20

Single Context Mode: Download config

Collect Hitcounts: No

8 Access Control List Lines

2 Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)

0 Network Objects

0 Port Objects

0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)

0 Network Address Translation

1 Logical Interfaces

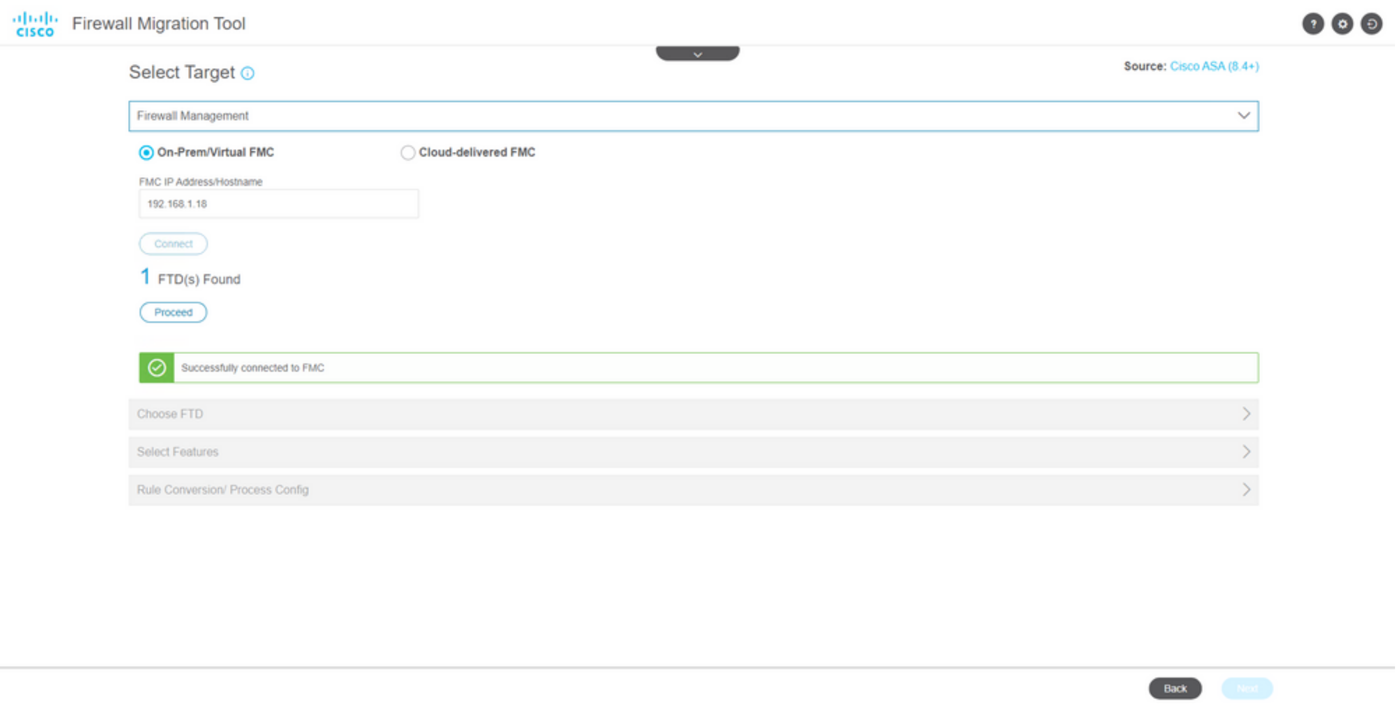
1 Routes

0 Site-to-Site VPN Tunnels

0 Remote Access VPN (Connection Profiles)

Pre-migration report will be available after selecting the targets.

8. 選擇要用於遷移的目標FMC。 提供FMC的IP。　　它會開啟一個彈出視窗，提示您輸入FMC的登入憑證。



Firewall Migration Tool

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

● On-Prem/Virtual FMC ○ Cloud-delivered FMC

FMC IP Address/Hostname: 192.168.1.18

Connect

1 FTD(s) Found

Proceed

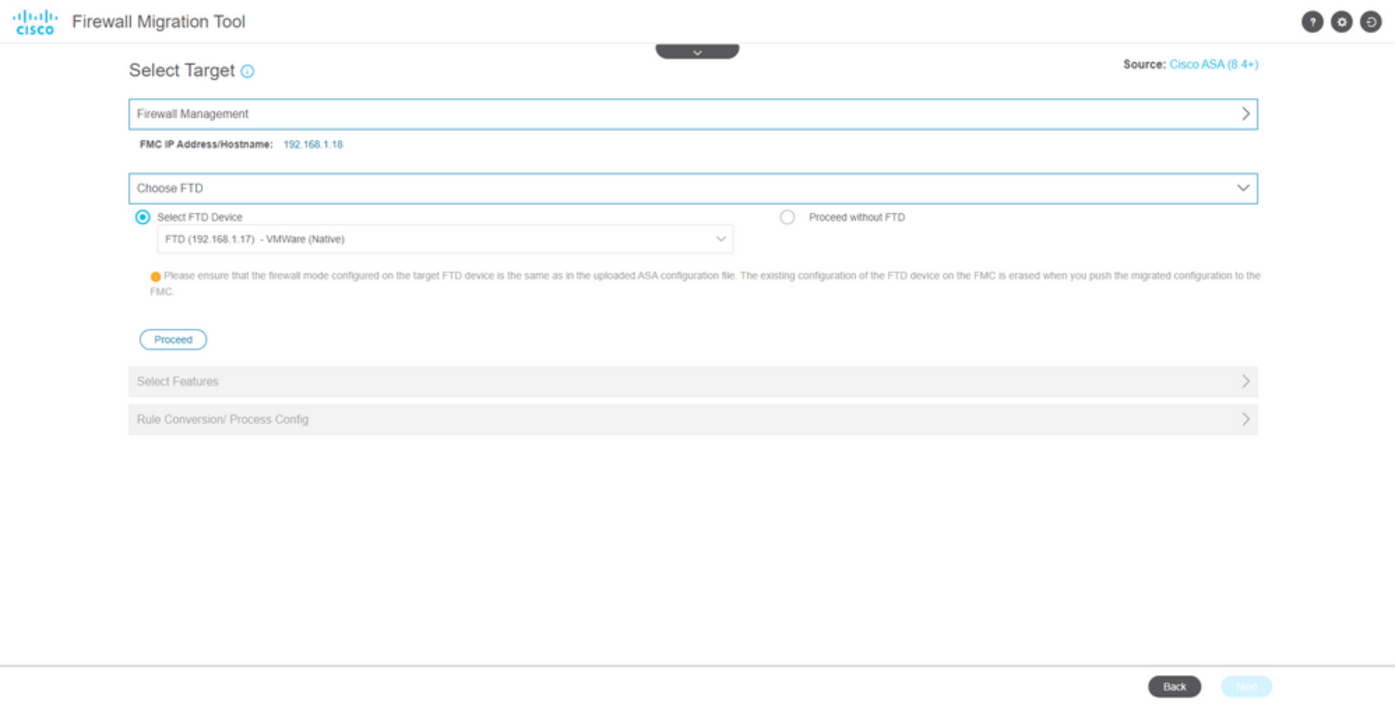
✓ Successfully connected to FMC

Choose FTD

Select Features

Rule Conversion/ Process Config

9. *（可選）*選擇要使用的目標FTD。 如果您選擇移轉到FTD，請選擇要使用的FTD。如果您不想使用FTD，可以填寫此覈取方塊 Proceed without FTD



Firewall Migration Tool

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

● Select FTD Device ○ Proceed without FTD

FTD (192.168.1.17) - VMWare (Native)

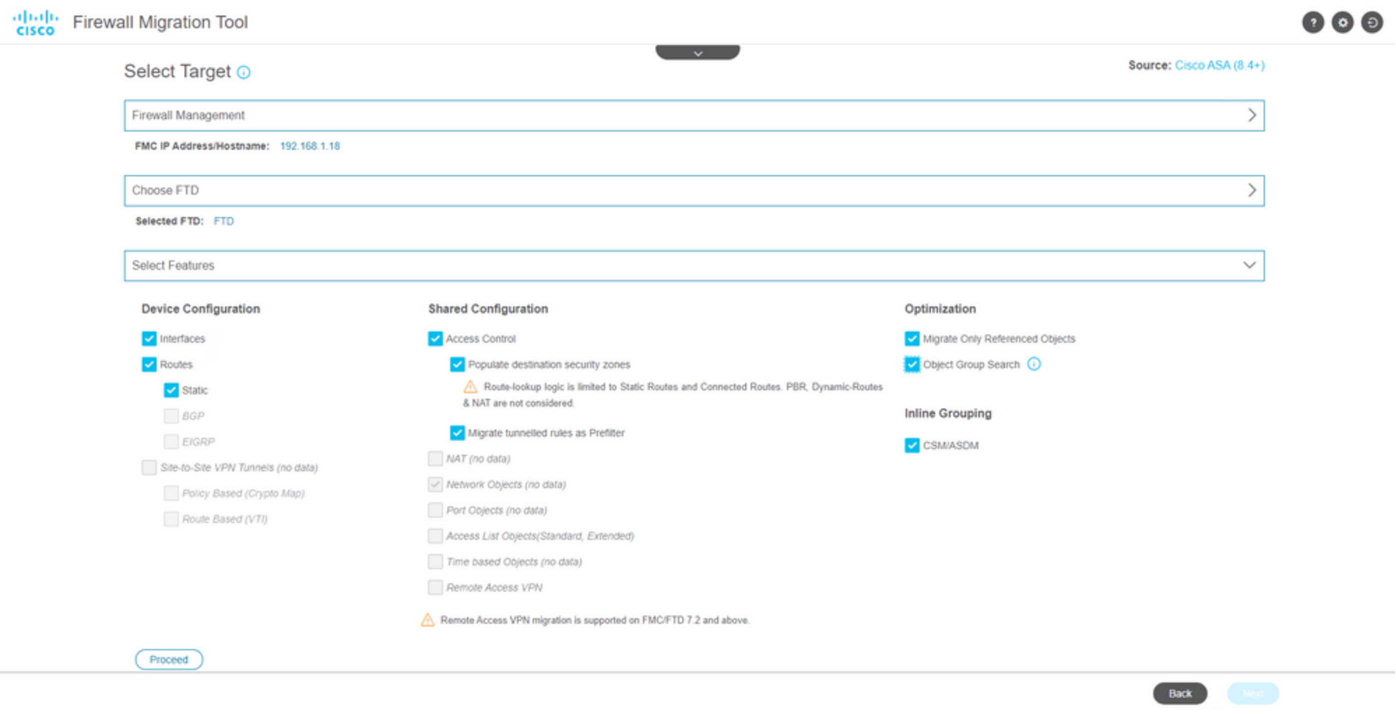
Please ensure that the firewall mode configured on the target FTD device is the same as in the uploaded ASA configuration file. The existing configuration of the FTD device on the FMC is erased when you push the migrated configuration to the FMC.

Proceed

Select Features

Rule Conversion/ Process Config

10. 選擇要遷移的配置，螢幕截圖上顯示選項。



Firewall Migration Tool

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

Device Configuration

- ☑ Interfaces
- ☑ Routes
  - ☑ Static
  - □ BGP
  - □ EIGRP
- □ Site-to-Site VPN Tunnels (no data)
  - □ Policy Based (Crypto Map)
  - □ Route Based (VTI)

Shared Configuration

- ☑ Access Control
  - ☑ Populate destination security zones
    - ⚠ Route-lookup logic is limited to Static Routes and Connected Routes. PBR, Dynamic-Routes & NAT are not considered.
  - ☑ Migrate tunnelled rules as Prefilter
- □ NAT (no data)
- ☑ Network Objects (no data)
- □ Port Objects (no data)
- □ Access List Objects(Standard, Extended)
- □ Time based Objects (no data)
- □ Remote Access VPN

⚠ Remote Access VPN migration is supported on FMC/FTD 7.2 and above.

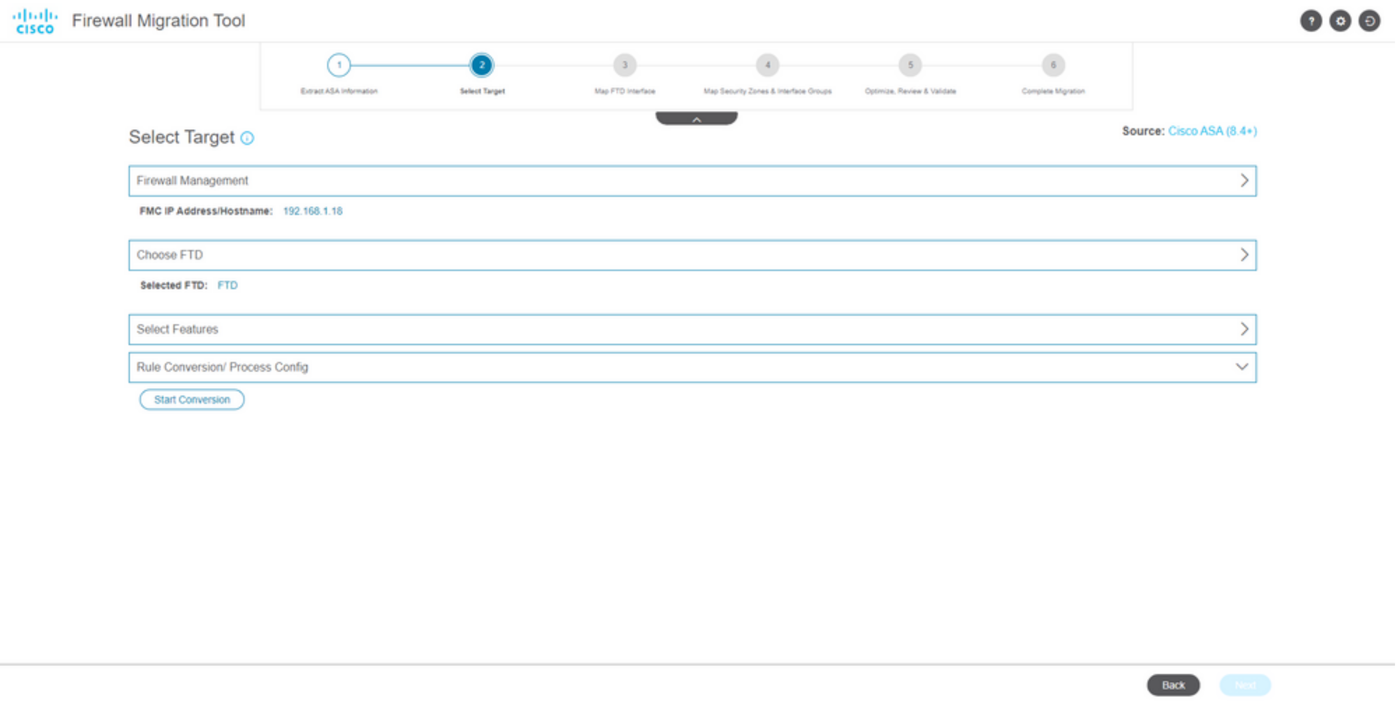
Optimization

- ☑ Migrate Only Referenced Objects
- ☑ Object Group Search

Inline Grouping

- ☑ CSM/ASDM

11. 開始將配置從ASA轉換為FTD。



Firewall Migration Tool

1 Extract ASA Information
2 Select Target
3 Map FTD Interface
4 Map Security Zones & Interface Groups
5 Optimize, Review & Validate
6 Complete Migration

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

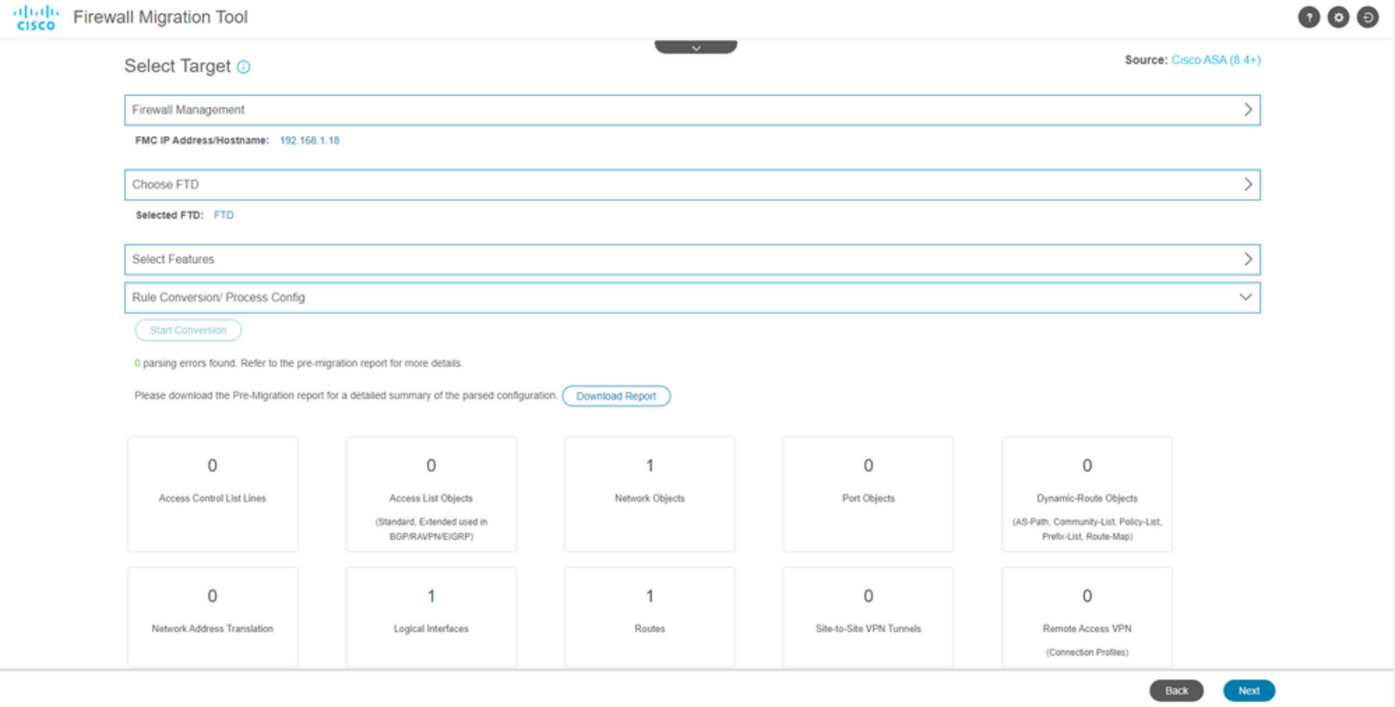
Selected FTD: FTD

Select Features

Rule Conversion/ Process Config

Start Conversion
Back
Next

12. 轉換完成後，它會顯示一個儀表板，其中包含要遷移的對象（僅限於相容性）的摘要。 您也可以按一下 **Download Report** 接收要遷移的配置摘要。



Firewall Migration Tool

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

Rule Conversion/ Process Config

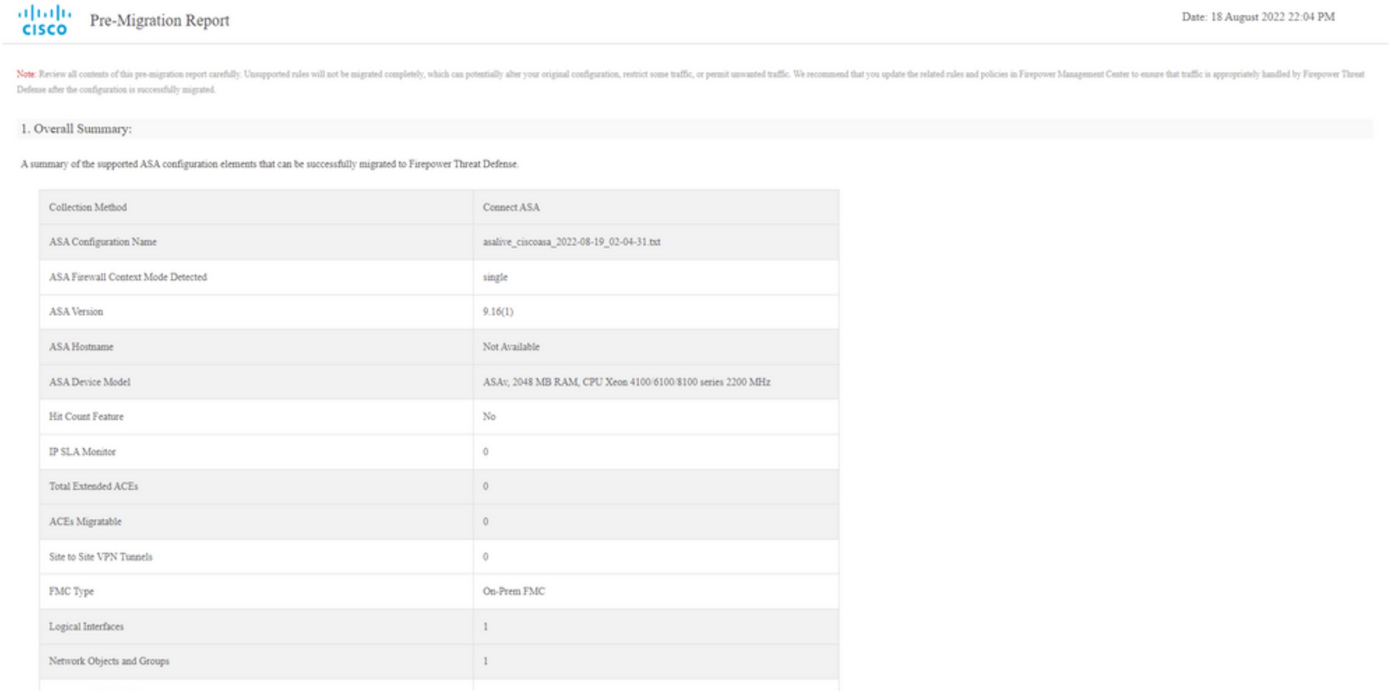
Start Conversion

0 parsing errors found. Refer to the pre-migration report for more details.

Please download the Pre-Migration report for a detailed summary of the parsed configuration. Download Report

0 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	1 Network Objects	0 Port Objects	0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
0 Network Address Translation	1 Logical Interfaces	1 Routes	0 Site-to-Site VPN Tunnels	0 Remote Access VPN (Connection Profiles)

遷移前報告示例，如下圖所示：



Pre-Migration Report

Date: 18 August 2022 22:04 PM

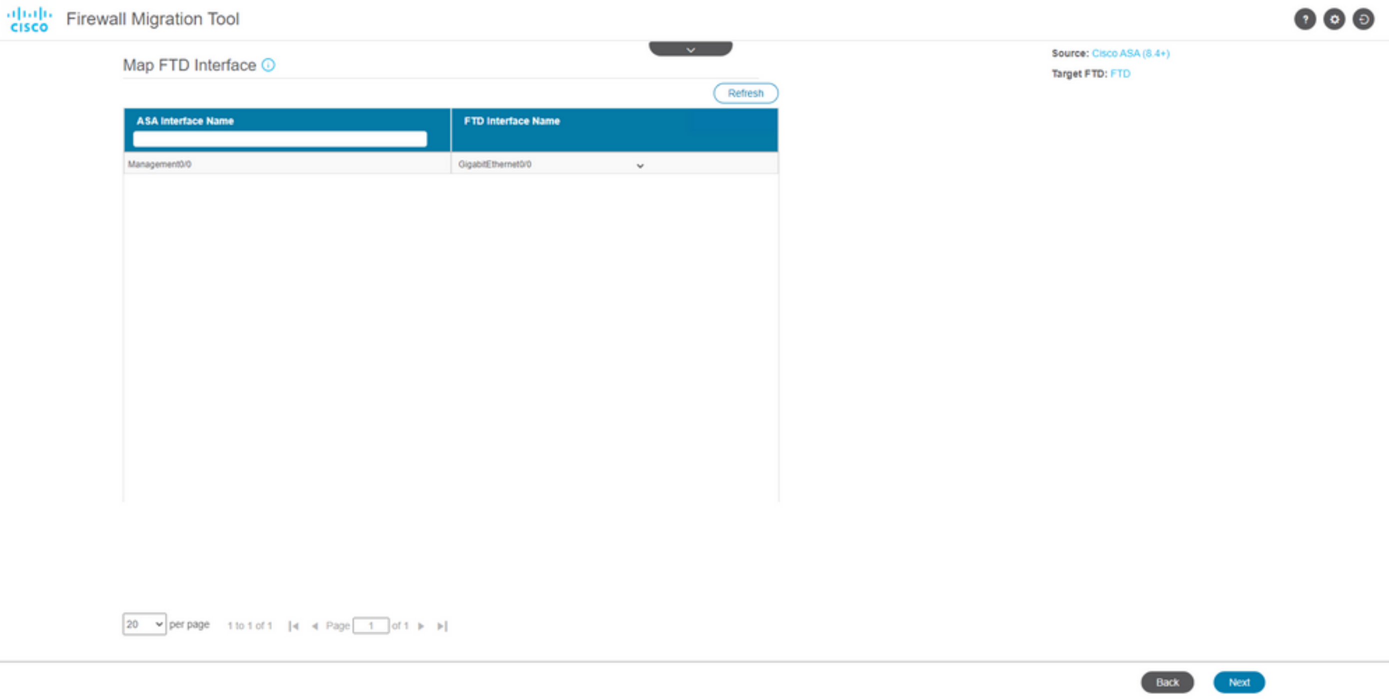
Note: Review all contents of this pre-migration report carefully. Unsupported rules will not be migrated completely, which can potentially alter your original configuration, restrict some traffic, or permit unwanted traffic. We recommend that you update the related rules and policies in Firepower Management Center to ensure that traffic is appropriately handled by Firepower Threat Defense after the configuration is successfully migrated.

1. Overall Summary:

A summary of the supported ASA configuration elements that can be successfully migrated to Firepower Threat Defense.

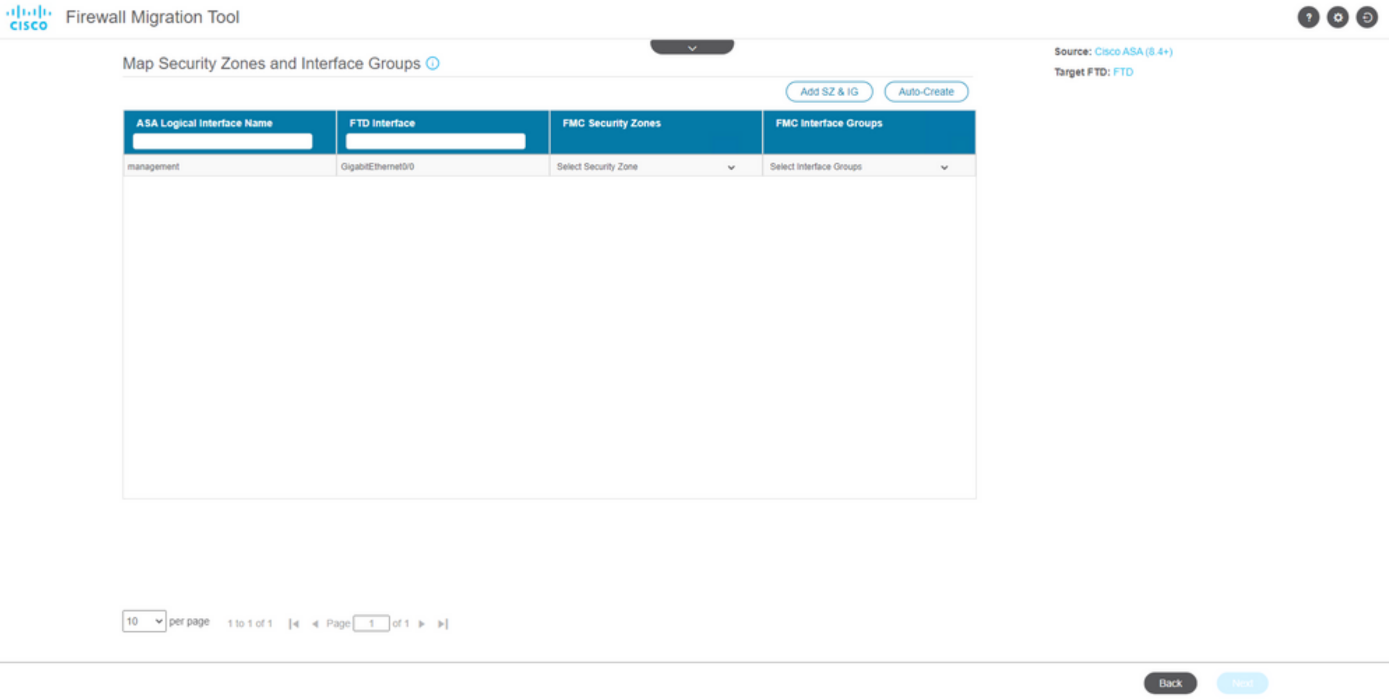
Collection Method	Connect ASA
ASA Configuration Name	asalive_ciscoasa_2022-08-19_02-04-31.txt
ASA Firewall Context Mode Detected	single
ASA Version	9.16(1)
ASA Hostname	Not Available
ASA Device Model	ASAv, 2048 MB RAM, CPU Xeon 4100/6100/8100 series 2200 MHz
Hit Count Feature	No
IP SLA Monitor	0
Total Extended ACEs	0
ACEs Migratable	0
Site to Site VPN Tunnels	0
FMC Type	On-Prem FMC
Logical Interfaces	1
Network Objects and Groups	1

13. 在遷移工具上將ASA介面與FTD介面對映。



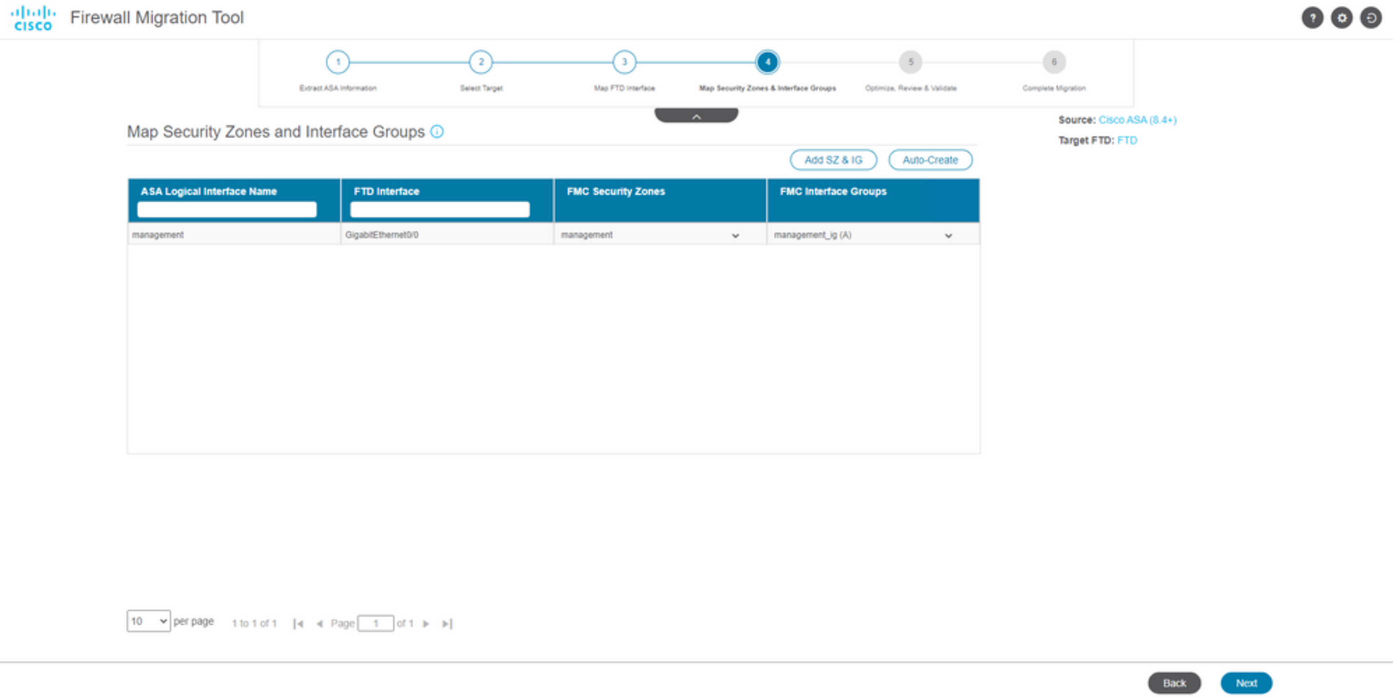
ASA Interface Name	FTD Interface Name
Management0/0	GigabitEthernet0/0

14. 為FTD上的介面建立安全區和介面組



ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	Select Security Zone	Select Interface Groups

安全區域(SZ)和介面組(IG)由工具自動建立，如下圖所示：

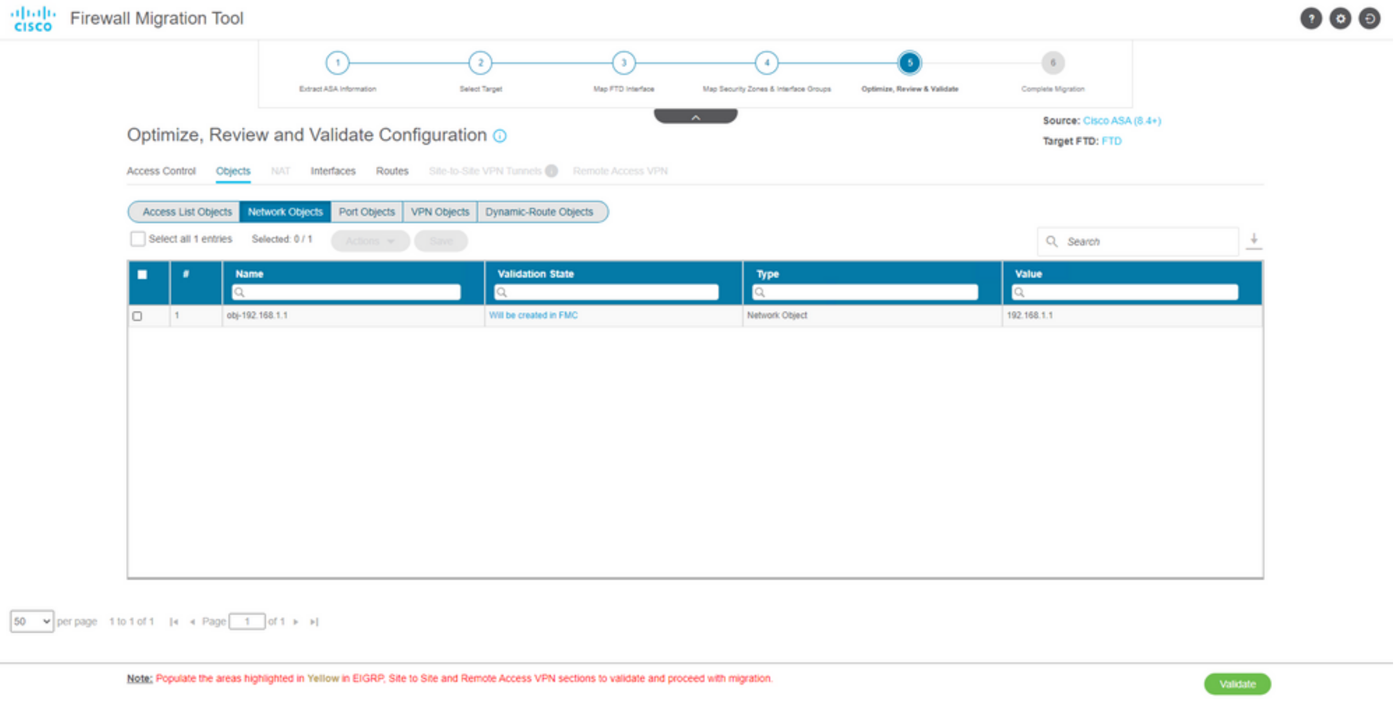


Map Security Zones and Interface Groups

Source: Cisco ASA (8.4+)
Target FTD: FTD

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	management	management_ig (A)

15. 檢視並驗證要在遷移工具上遷移的配置。
    如果您已完成配置的複查和最佳化，請按一下 Validate.



Optimize, Review and Validate Configuration

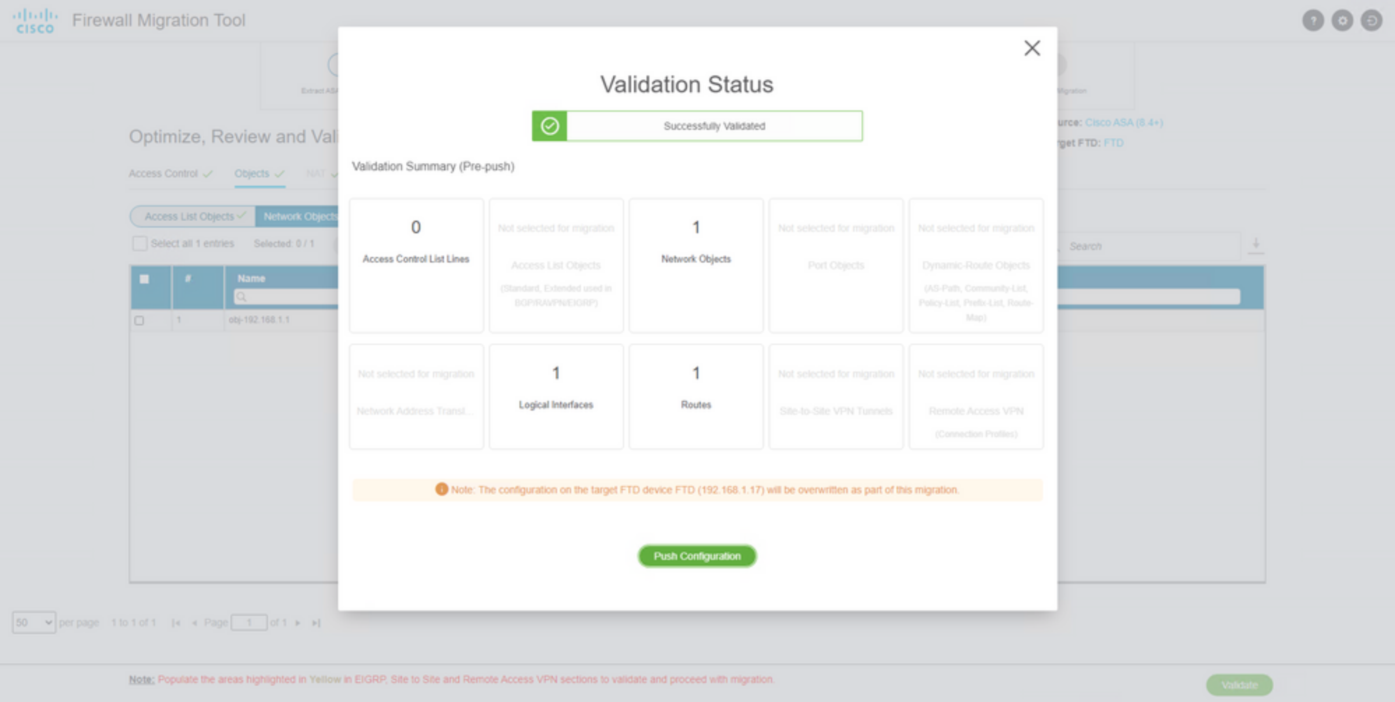
Source: Cisco ASA (8.4+)
Target FTD: FTD

□ Select all 1 entries   Selected: 0 / 1

■	#	Name	Validation State	Type	Value
□	1	obj-192.168.1.1	Will be created in FMC	Network Object	192.168.1.1

Note: Populate the areas highlighted in Yellow in EIGRP, Site to Site and Remote Access VPN sections to validate and proceed with migration.

16. 如果驗證狀態成功，將配置推送到目標裝置。



Firewall Migration Tool

Optimize, Review and Validate

Validation Status

Successfully Validated

Validation Summary (Pre-push)

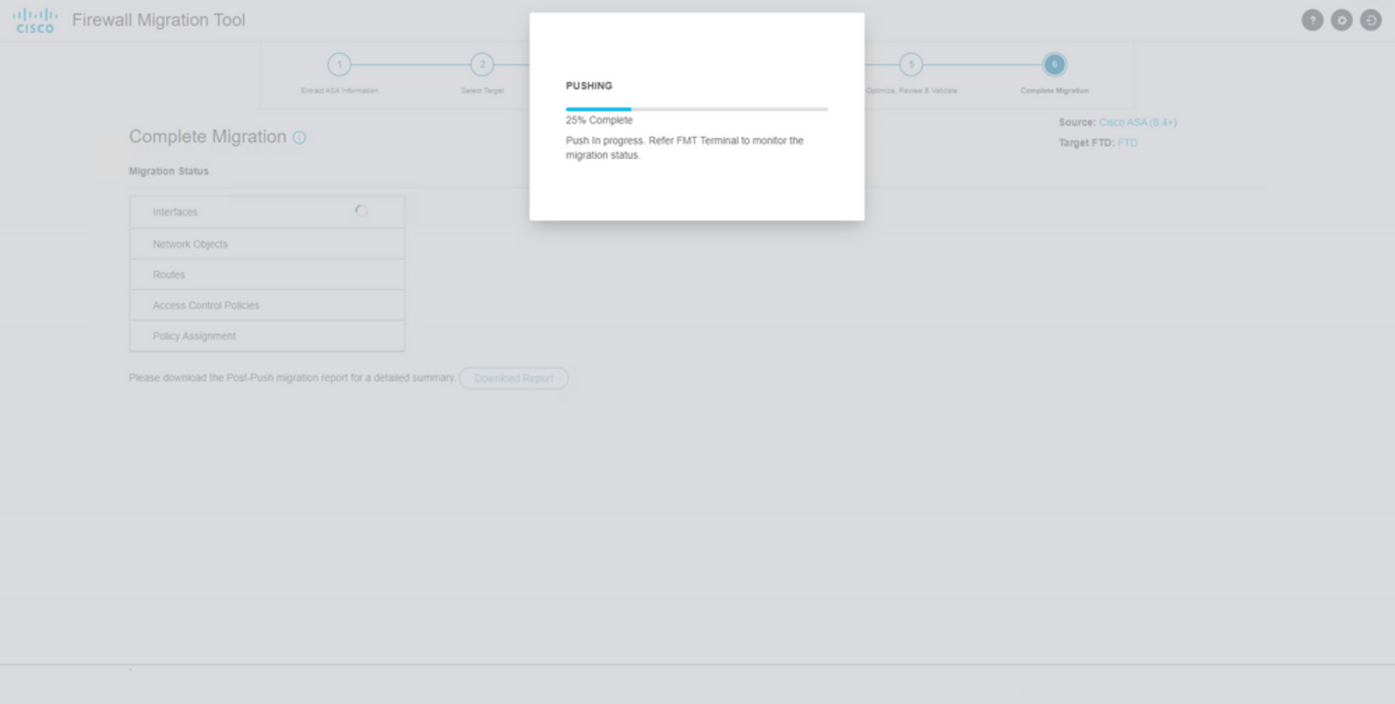
0 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	1 Network Objects	Not selected for migration Port Objects	Not selected for migration Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
Not selected for migration Network Address Transl...	1 Logical Interfaces	1 Routes	Not selected for migration Site-to-Site VPN Tunnels	Not selected for migration Remote Access VPN (Connection Profiles)

Note: The configuration on the target FTD device FTD (192.168.1.17) will be overwritten as part of this migration.

Push Configuration

Note: Populate the areas highlighted in Yellow in EIGRP, Site to Site and Remote Access VPN sections to validate and proceed with migration.

通過遷移工具推送的配置示例，如下圖所示：



Firewall Migration Tool

Complete Migration

Source: Cisco ASA (8.4+)
Target FTD: FTD

PUSHING

25% Complete

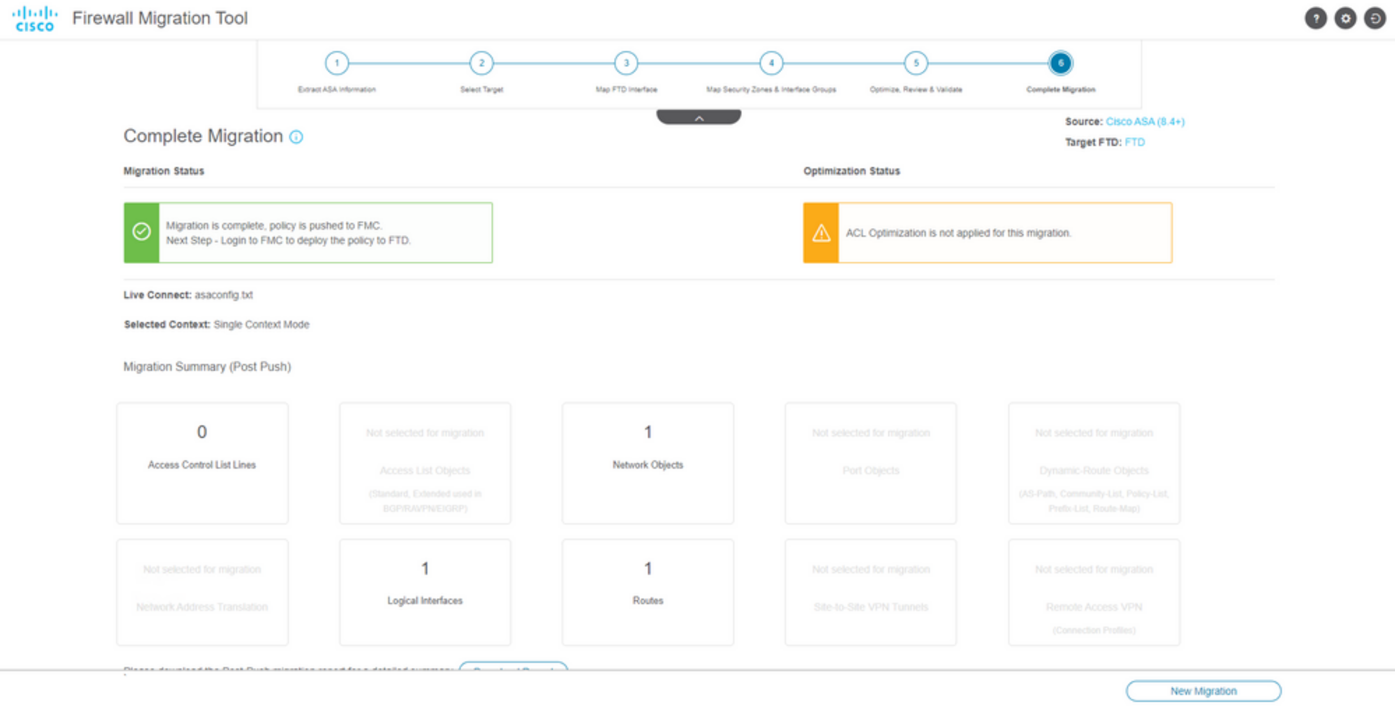
Push In progress. Refer FMT Terminal to monitor the migration status.

Migration Status

- Interfaces
- Network Objects
- Routes
- Access Control Policies
- Policy Assignment

Please download the Post-Push migration report for a detailed summary. Download Report

成功遷移的示例，如下圖所示：


Firewall Migration Tool
1 Extract ASA Information
2 Select Target
3 Map FTD Interface
4 Map Security Zones & Interface Groups
5 Optimize, Review & Validate
6 Complete Migration
New Migration

Complete Migration

Source: Cisco ASA (8.4+)
Target FTD: FTD

Migration Status

Migration is complete, policy is pushed to FMC.
Next Step - Login to FMC to deploy the policy to FTD.

Optimization Status

ACL Optimization is not applied for this migration.

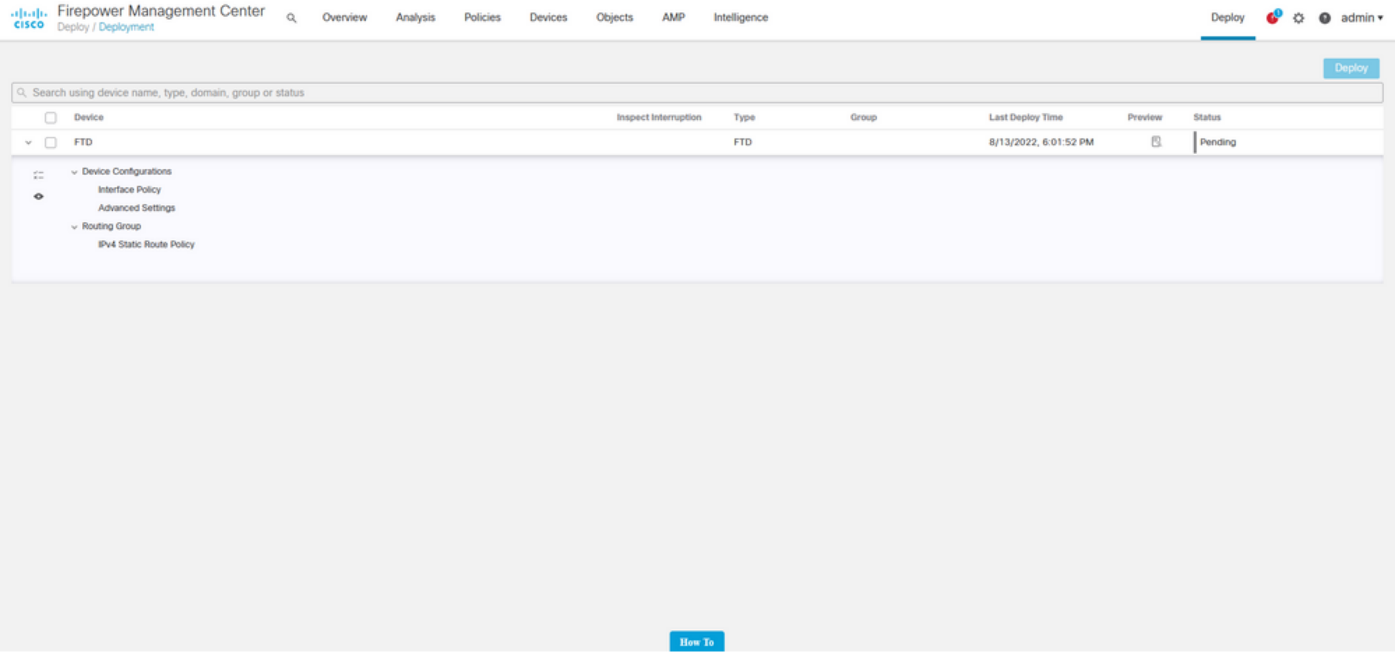
Live Connect: asaconfig.txt

Selected Context: Single Context Mode

Migration Summary (Post Push)

0 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	1 Network Objects	Not selected for migration Port Objects	Not selected for migration Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
Not selected for migration Network Address Translation	1 Logical Interfaces	1 Routes	Not selected for migration Site-to-Site VPN Tunnels	Not selected for migration Remote Access VPN (Connection Profiles)

17. *(可*選)如果選擇將組態移轉到FTD，則需要部署將可用組態從FMC推送到防火牆，才能部署組態： 登入到FMC GUI。導航至 Deploy 頁籤。選擇要將配置推送到防火牆的部署。按一下 Deploy.



	Device	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
⌄ □	FTD		FTD		8/13/2022, 6:01:52 PM		Pending

- Device Configurations
  - Interface Policy
  - Advanced Settings
- Routing Group
  - IPv4 Static Route Policy

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

驗證放置Firepower遷移工具檔案的目錄中的日誌，例如：

Firepower_Migration_Tool_v3.0.1-7373.exe/logs/log_2022-08-18-21-24-46.log

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）。