Configure the Secure Firewall Migration Tool for ASA Migration

Contents

Introduction

This document describes the procedure to migrate Cisco Adaptive Security Appliance (ASA) to Cisco Firepower.

Contributed by Ricardo Vera, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Cisco Firewall Threat Defense (FTD) and Adaptive Security Appliance (ASA).

Components Used

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

- Windows PC with Firepower Migration Tool (FMT) v3.0.1
- Adaptive Security Appliance (ASA) v9.16.1
- Secure Firewall Management Center (FMCv) v7.0.1
- Secure Firewall Threat Defense Virtual (FTDv) v7.0.1

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:

- Cisco Adaptive Security Appliance (ASA) Version 8.4 or later
- Secure Firewall Management Center (FMCv) Version 6.2.3 or later

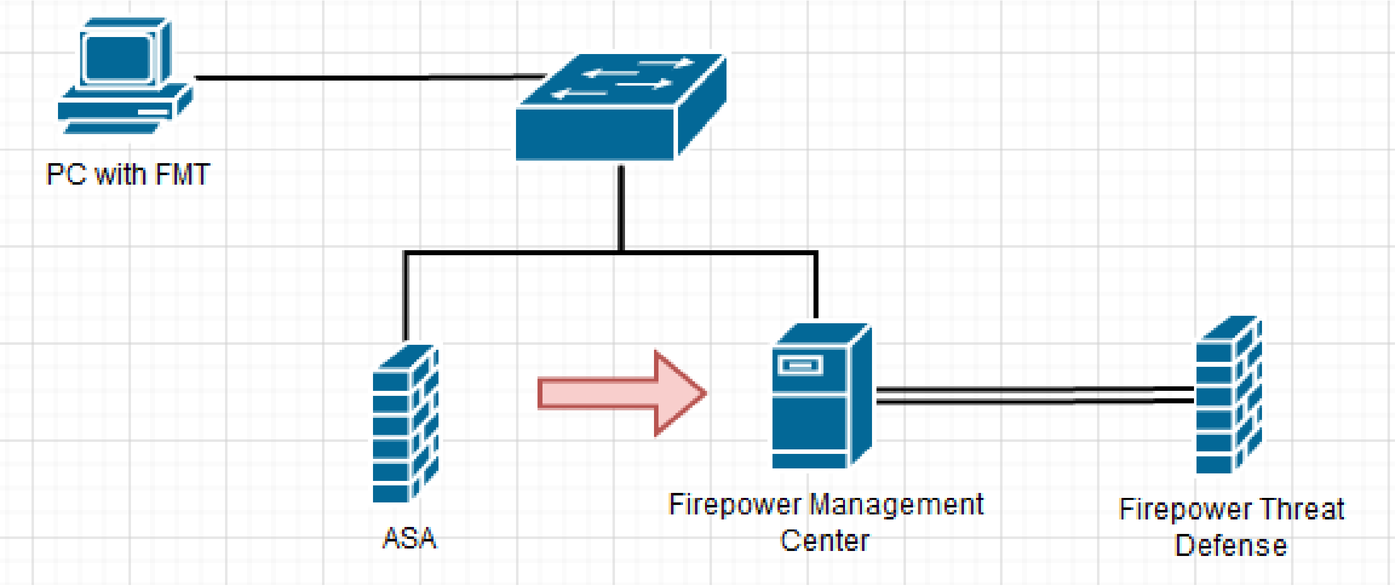
The Firewall Migration Tool supports this list of devices:

- 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+)

Before you proceed with the migration, please consider the Guidelines and Limitations for the Firewall Migration Tool.

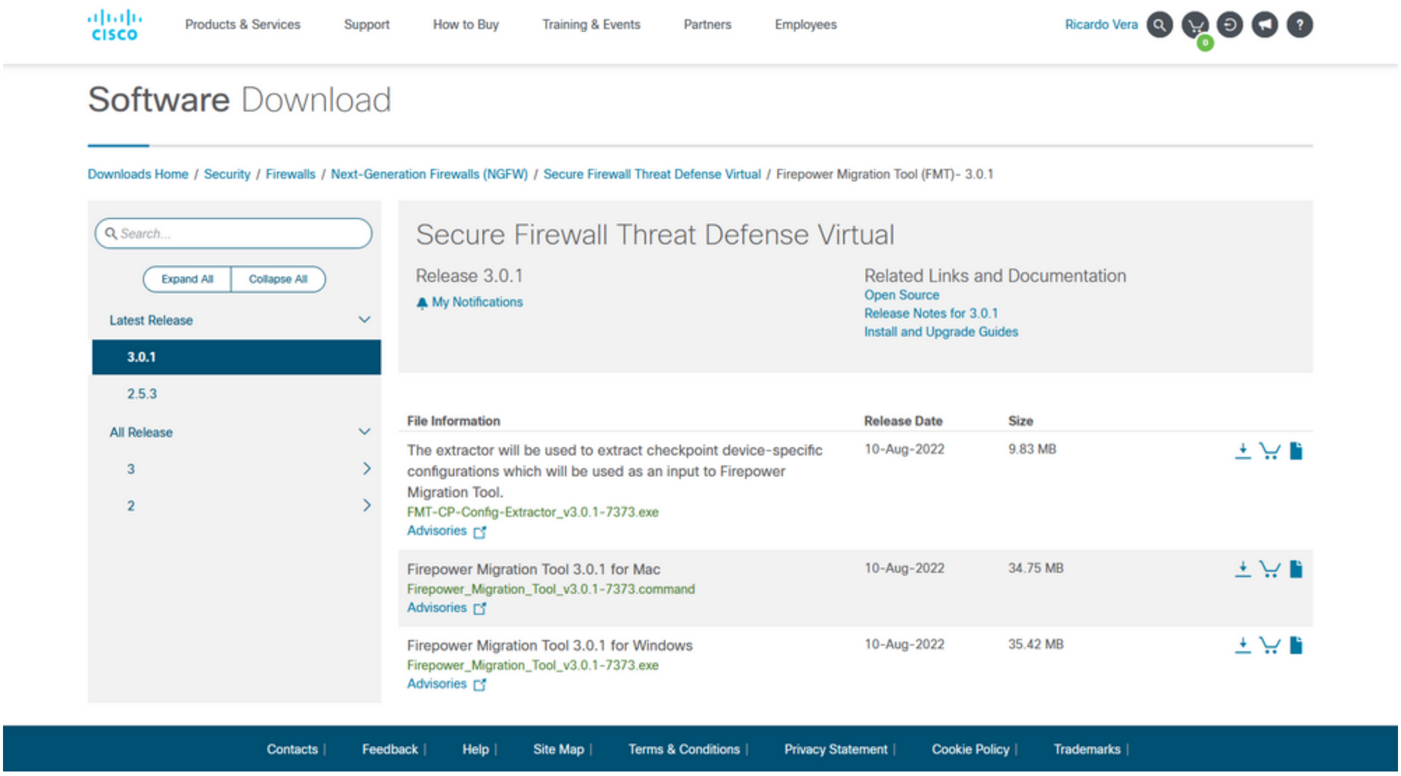
Configure

Network Diagram



Configuration Steps

1. **Download** the most recent Firepower Migration Tool from Cisco Software Central:



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

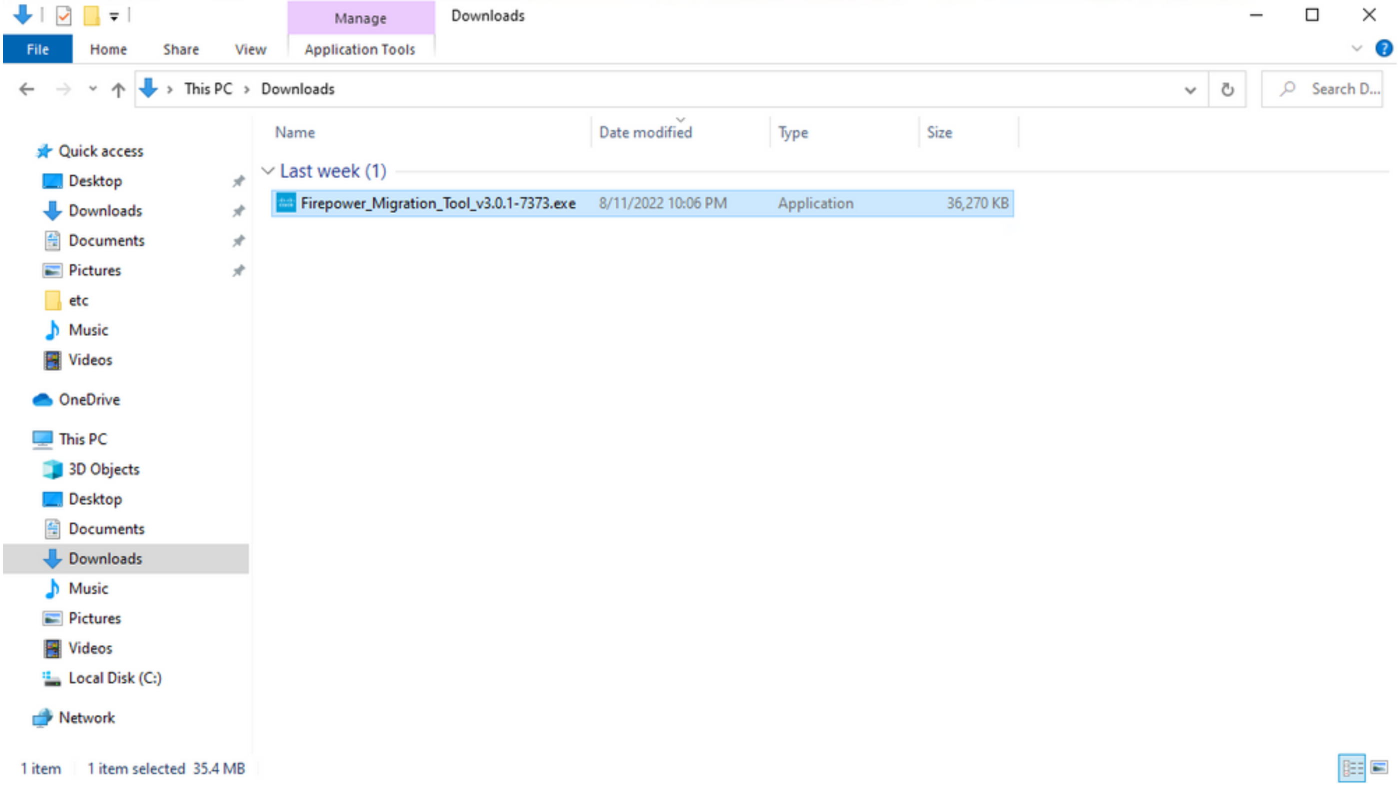
Release 3.0.1

My Notifications

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

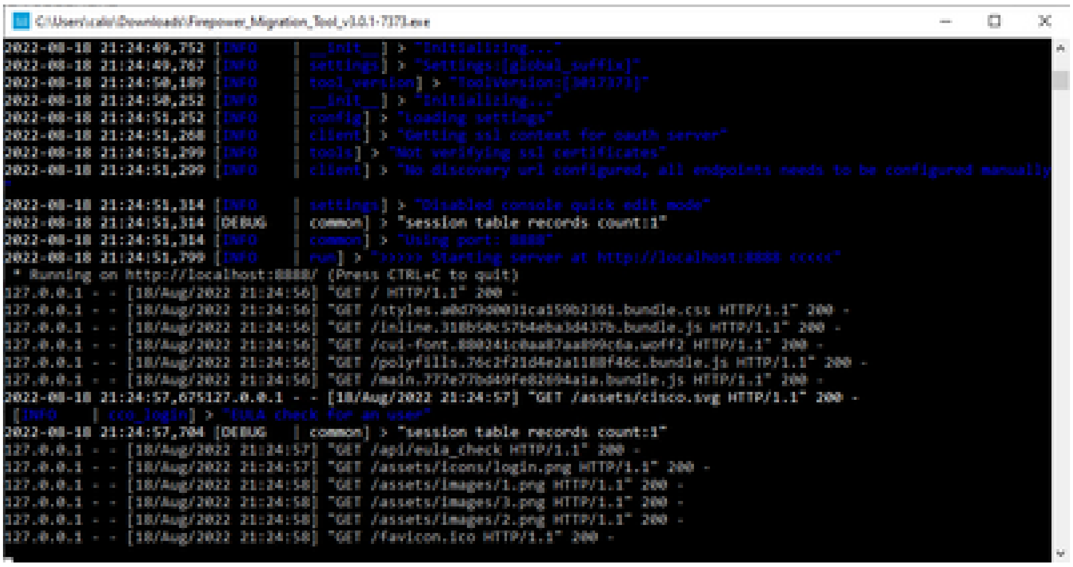
File Information	Release Date	Size
The extractor will be used to extract checkpoint device-specific configurations which will be used as an input to Firepower Migration Tool. FMT-CP-Config-Extractor_v3.0.1-7373.exe Advisories	10-Aug-2022	9.83 MB
Firepower Migration Tool 3.0.1 for Mac Firepower_Migration_Tool_v3.0.1-7373.command 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. Click the file you previously downloaded to your computer.



Name	Date modified	Type	Size
Last week (1)			
Firepower_Migration_Tool_v3.0.1-7373.exe	8/11/2022 10:06 PM	Application	36,270 KB

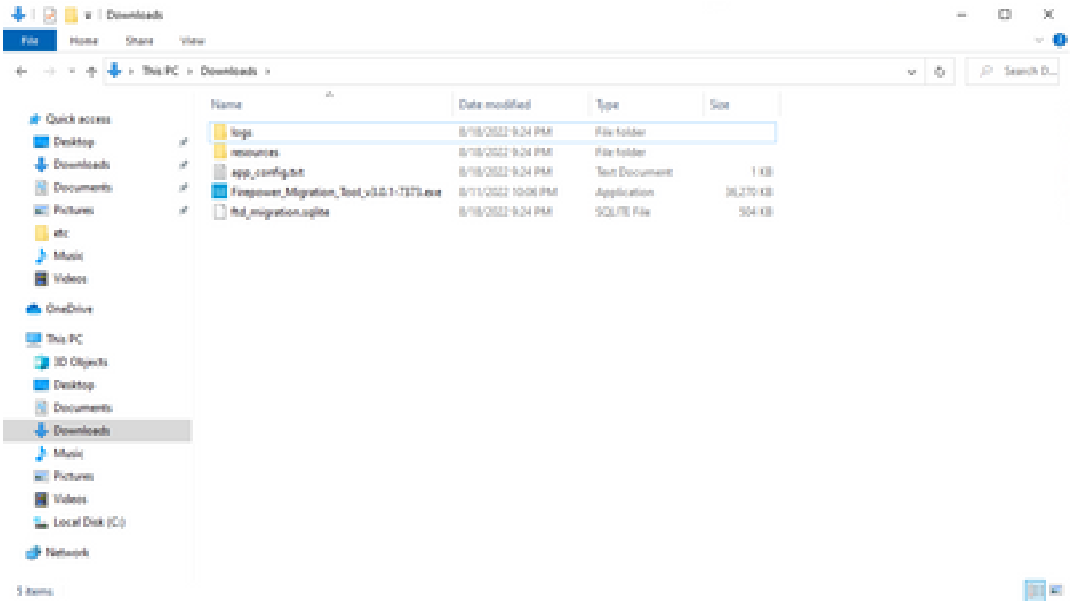
Note: The program opens up automatically and a console auto generates content on the directory where you ran the file.



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

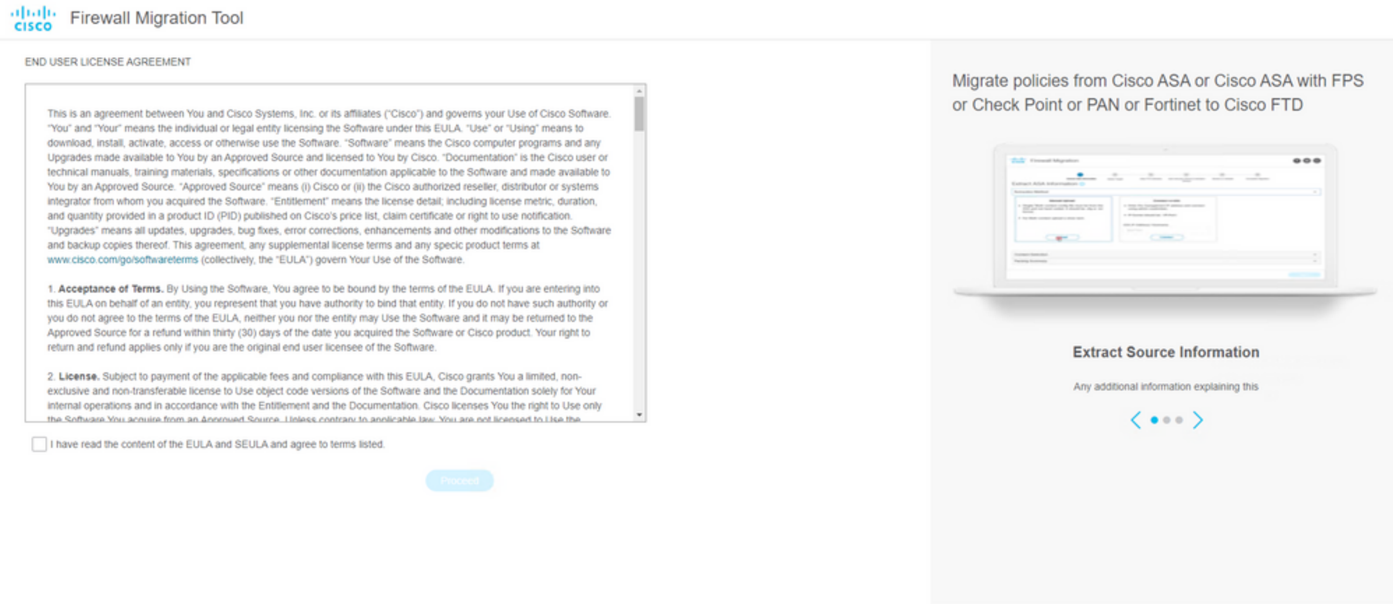
```
2022-08-18 21:24:49,752 [INFO     | __init__] > "Initializing..."
2022-08-18 21:24:49,767 [INFO     | settings] > "Settings:[global_suffix]"
2022-08-18 21:24:50,189 [INFO     | tool_version] > "ToolVersion:[3017373]"
2022-08-18 21:24:50,252 [INFO     | __init__] > "Initializing..."
2022-08-18 21:24:51,252 [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	36,270 KB
ftd_migration.sqlite	8/18/2022 9:24 PM	SQLITE File	504 KB

3. After you run the program, it opens up a web browser that displays the “End User License Agreement”. Mark the check box to accept terms and conditions.Click **Proceed.**



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

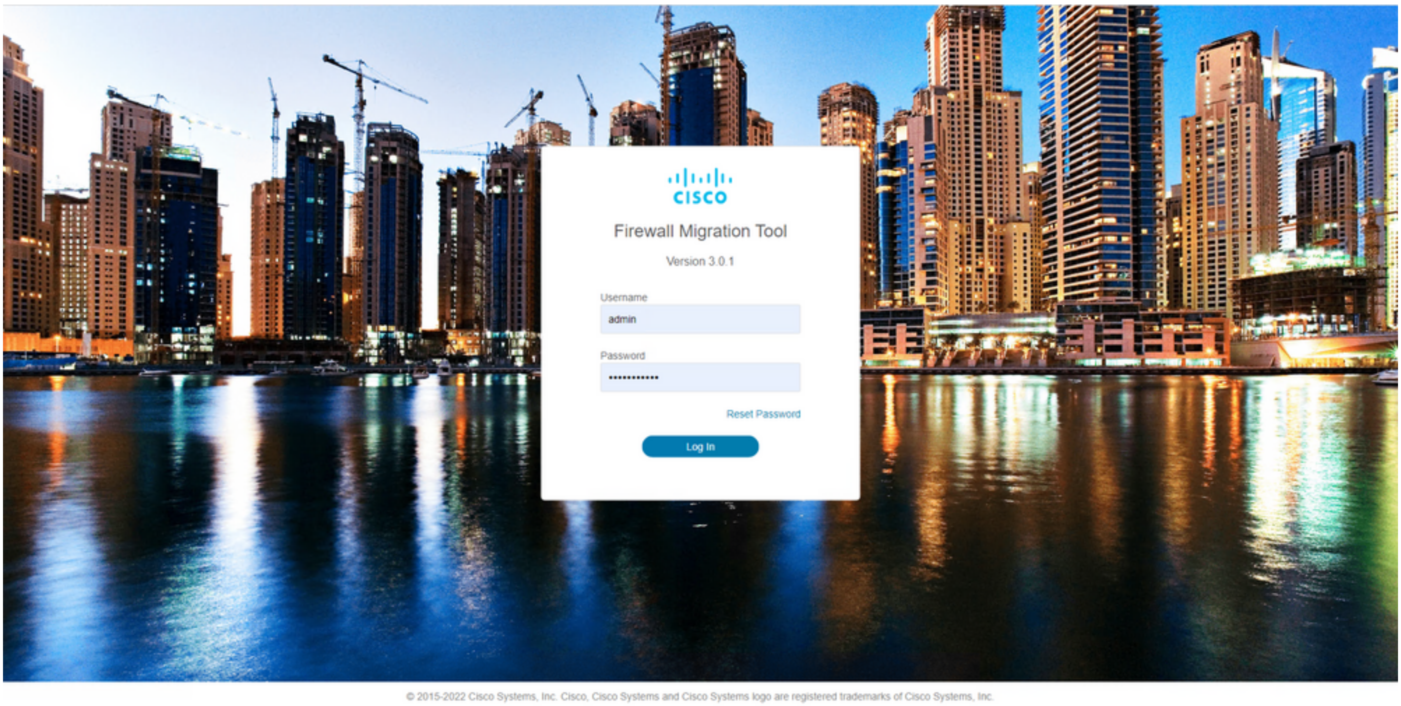
□ I have read the content of the EULA and SEULA and agree to terms listed.

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

Extract Source Information

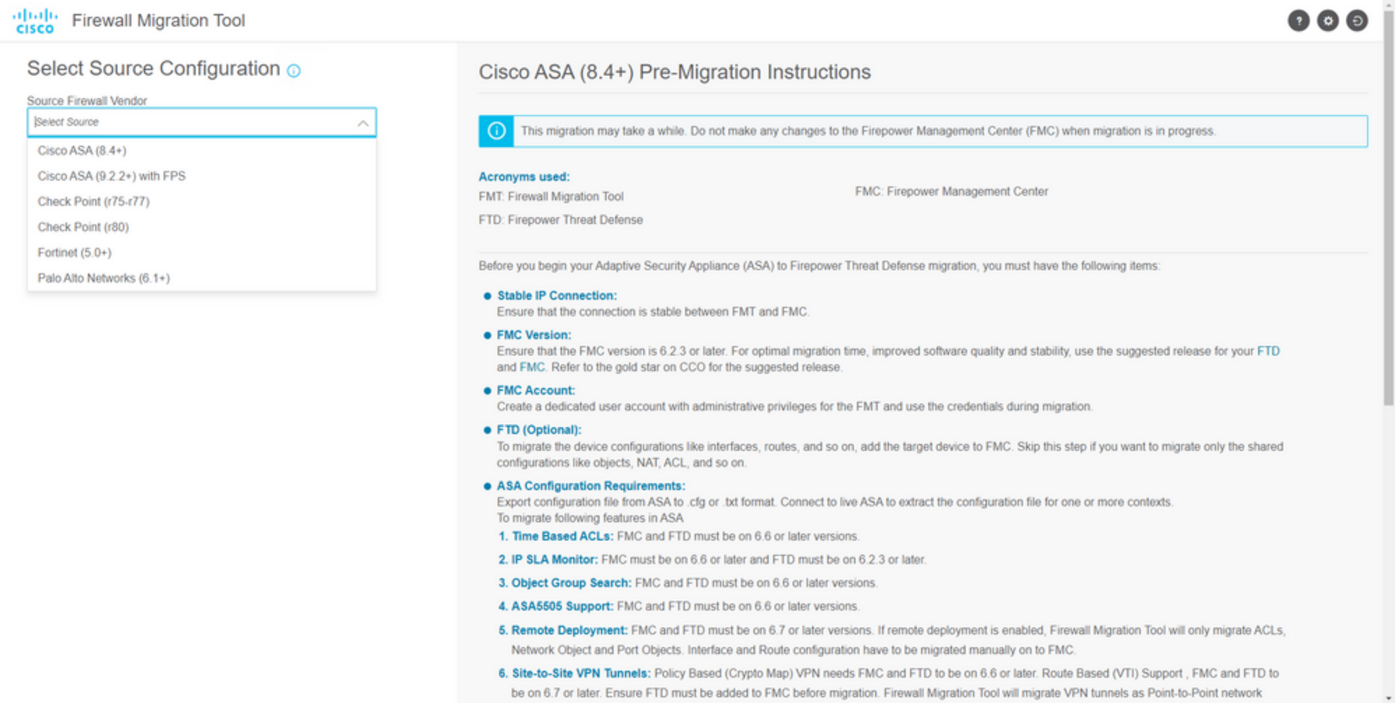
Any additional information explaining this

4. Log in to the migration tool. You can either log in with the CCO account or with the local default account.   Local default account credentials are: admin/Admin123



cisco
Firewall Migration Tool
Version 3.0.1
Username
admin
Password
••••••••••••
Reset Password
Log In
© 2015-2022 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc.

5. Select the Source Firewall to migrate. In this example, Cisco ASA (8.4+) is used as a source.



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

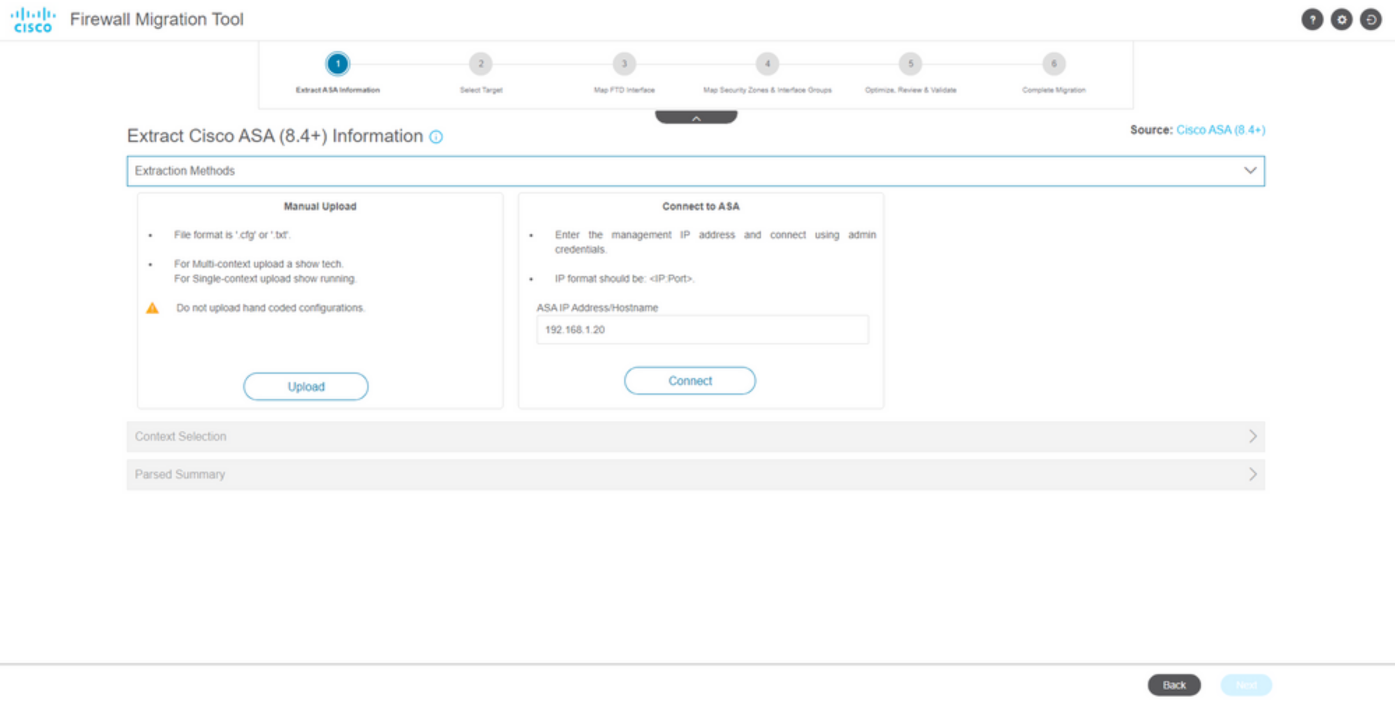
FTD: Firepower Threat Defense

FMC: Firepower Management Center

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. Select the extraction method to be used to get the configuration. Manual Upload requires you to upload the **Running Config** file of the ASA in “.cfg” or “.txt” format.Connect to the ASA to extract configurations directly from the firewall.



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.

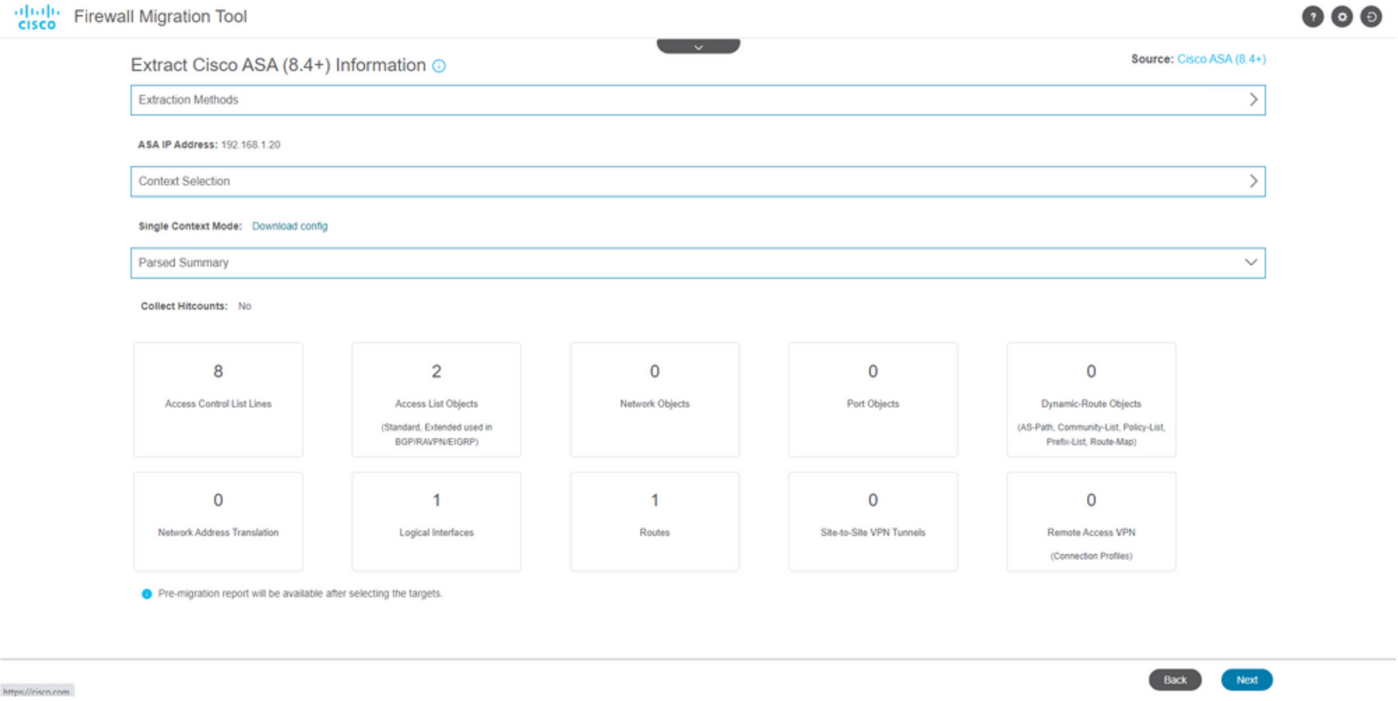
Connect to ASA

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

ASA IP Address/Hostname: 192.168.1.20

Note: For this example, connect directly to the ASA.

7. A summary of the configuration found on the firewall is displayed as a dashboard, please click **Next**.



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

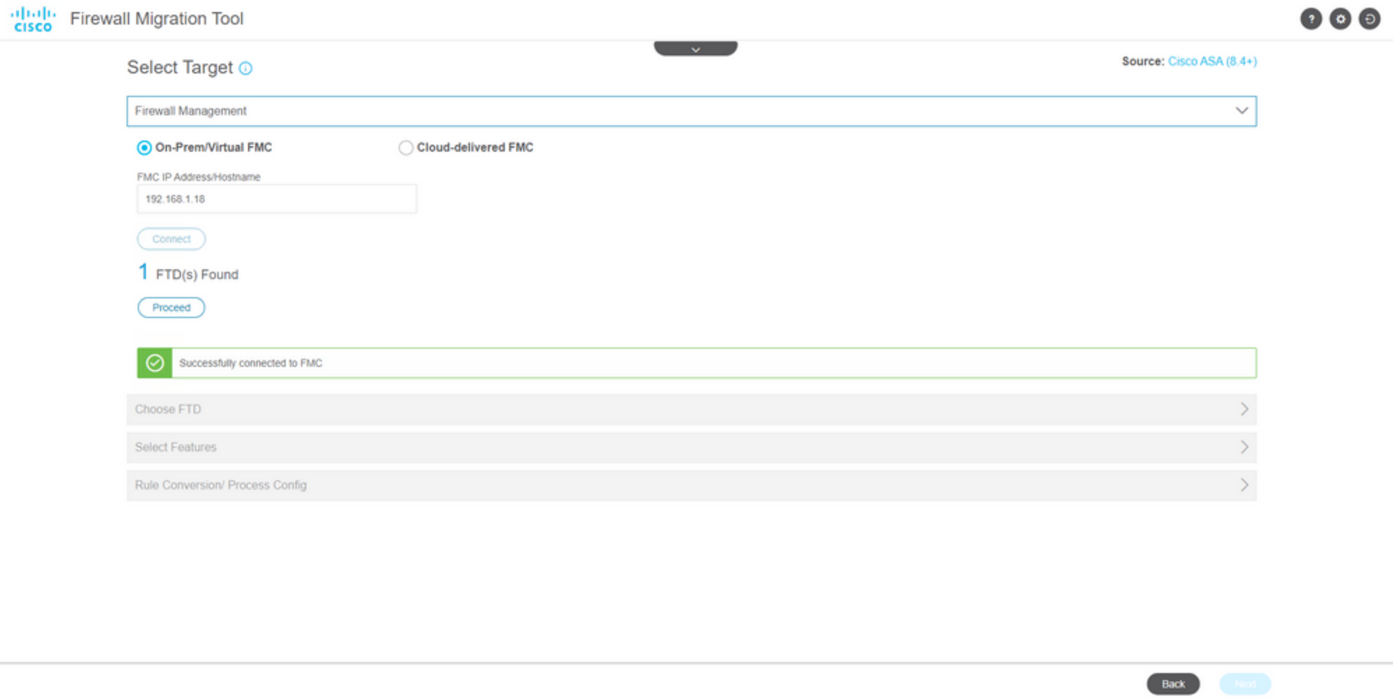
1
Routes

0
Site-to-Site VPN Tunnels

0
Remote Access VPN
(Connection Profiles)

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

8. Select the target FMC to use on the migration. Provide the IP of the FMC.   It opens a pop-up window where it prompts you for the log in credentials of the FMC.


Firewall Migration Tool

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

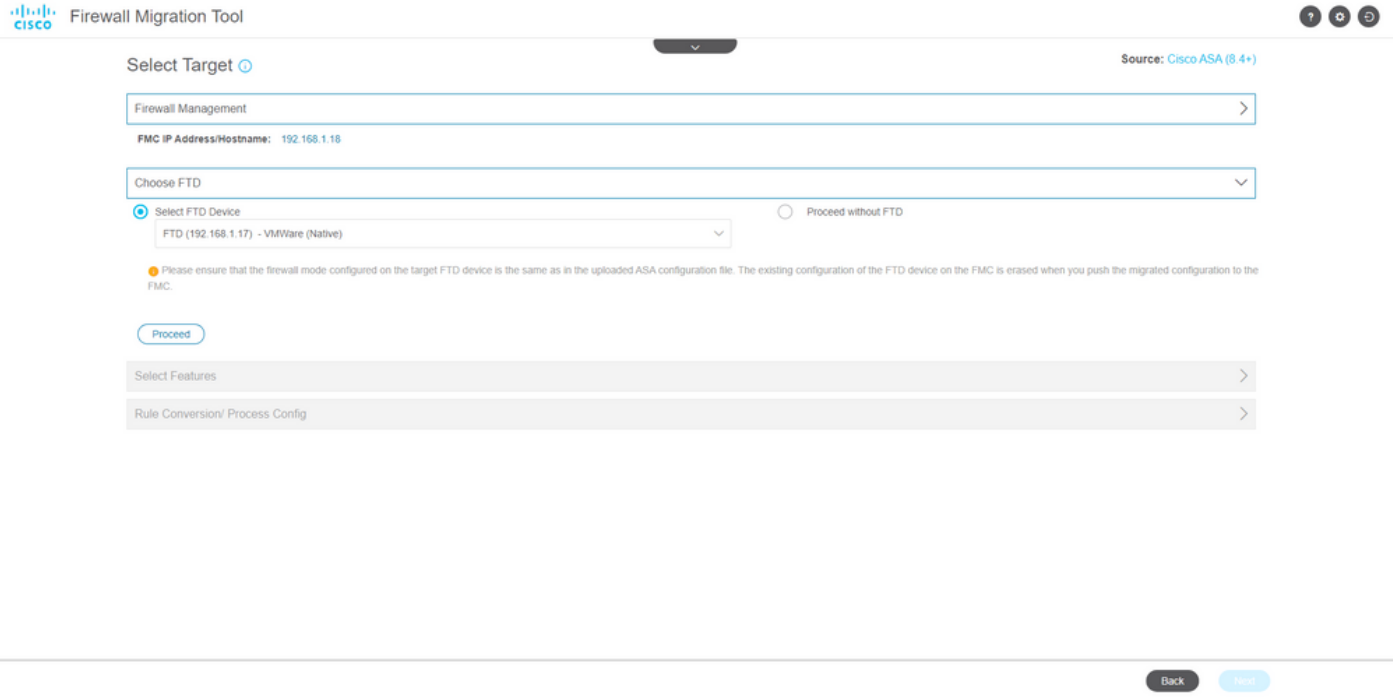
● On-Prem/Virtual FMC ○ Cloud-delivered FMC

FMC IP Address/Hostname: 192.168.1.18

1 FTD(s) Found

Successfully connected to FMC

9. *(Optional)* Select the Target FTD you want to use. If you choose to migrate to an FTD, select the FTD you want to use.If you do not want to use an FTD you can fill the check box Proceed without FTD


Firewall Migration Tool

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

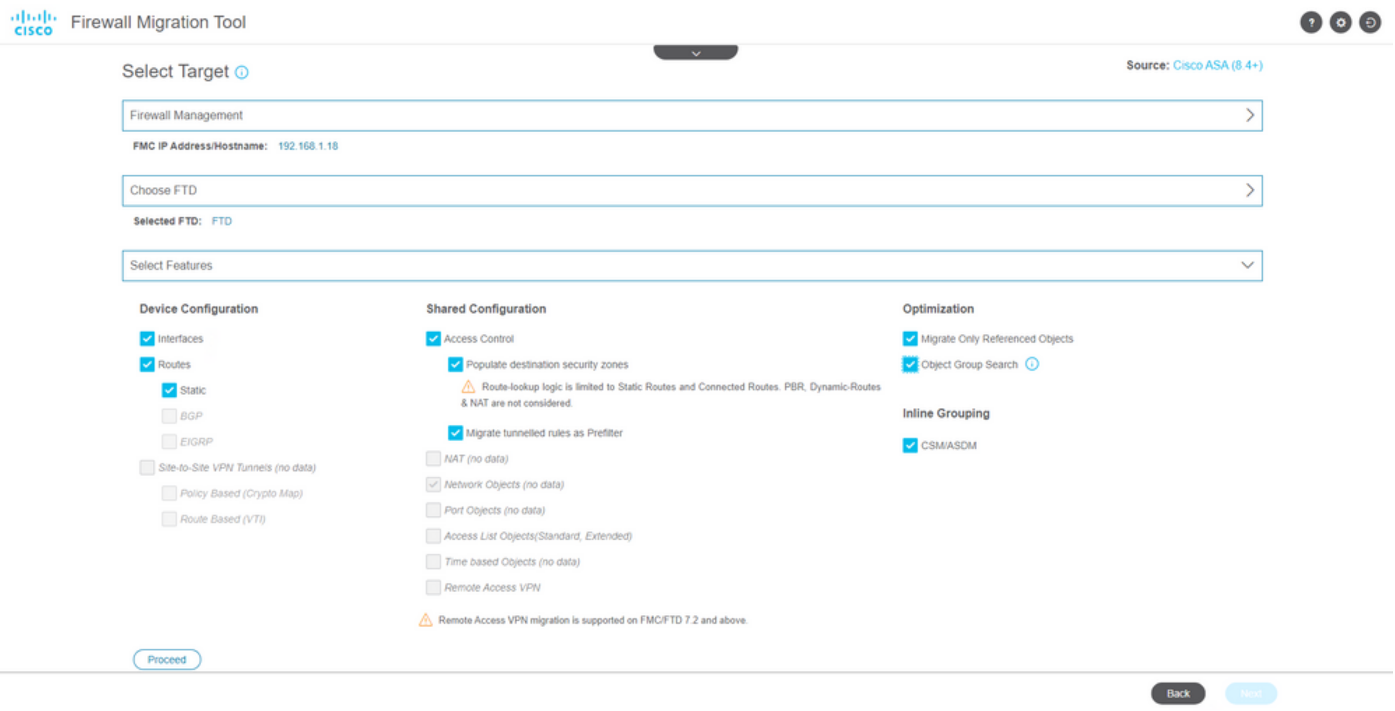
Choose FTD

● 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.

10. Select the configurations you want to migrate, options are displayed on the screenshots.



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

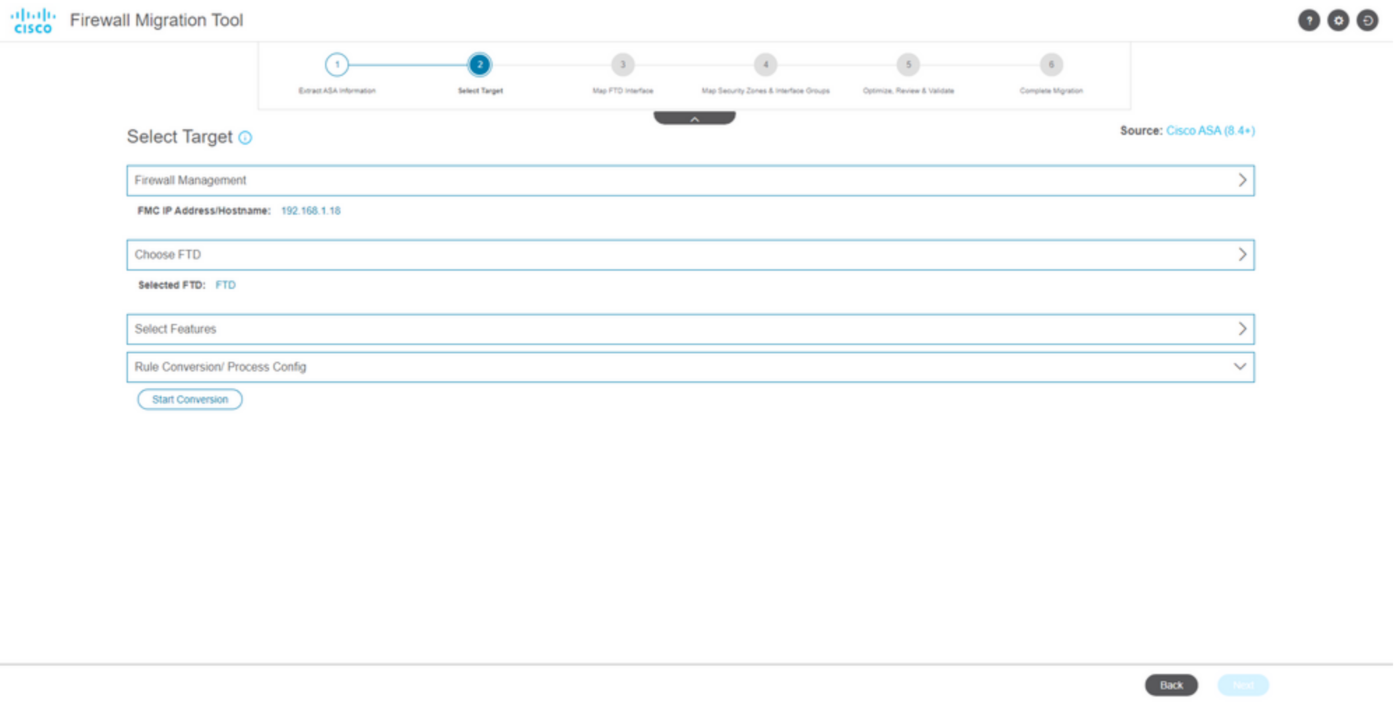
Inline Grouping

☑ CSM/ASDM

Proceed

Back Next

11. Start the conversion of the configurations from ASA to 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

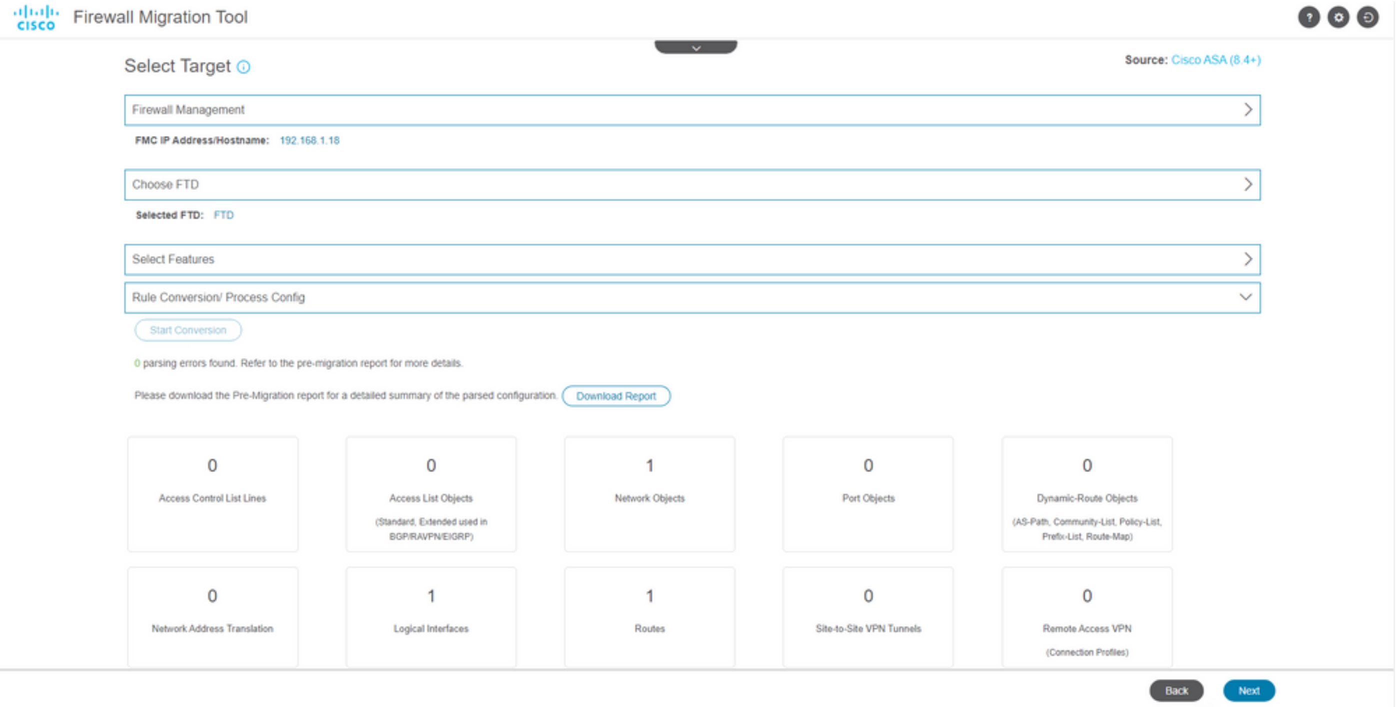
Select Features

Rule Conversion/ Process Config

Start Conversion

Back Next

12. Once the conversion finishes, it displays a dashboard with the summary of the objects to be migrated (restricted to compatibility). You can optionally click on **Download Report** to receive a summary of the configurations to be migrated.



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

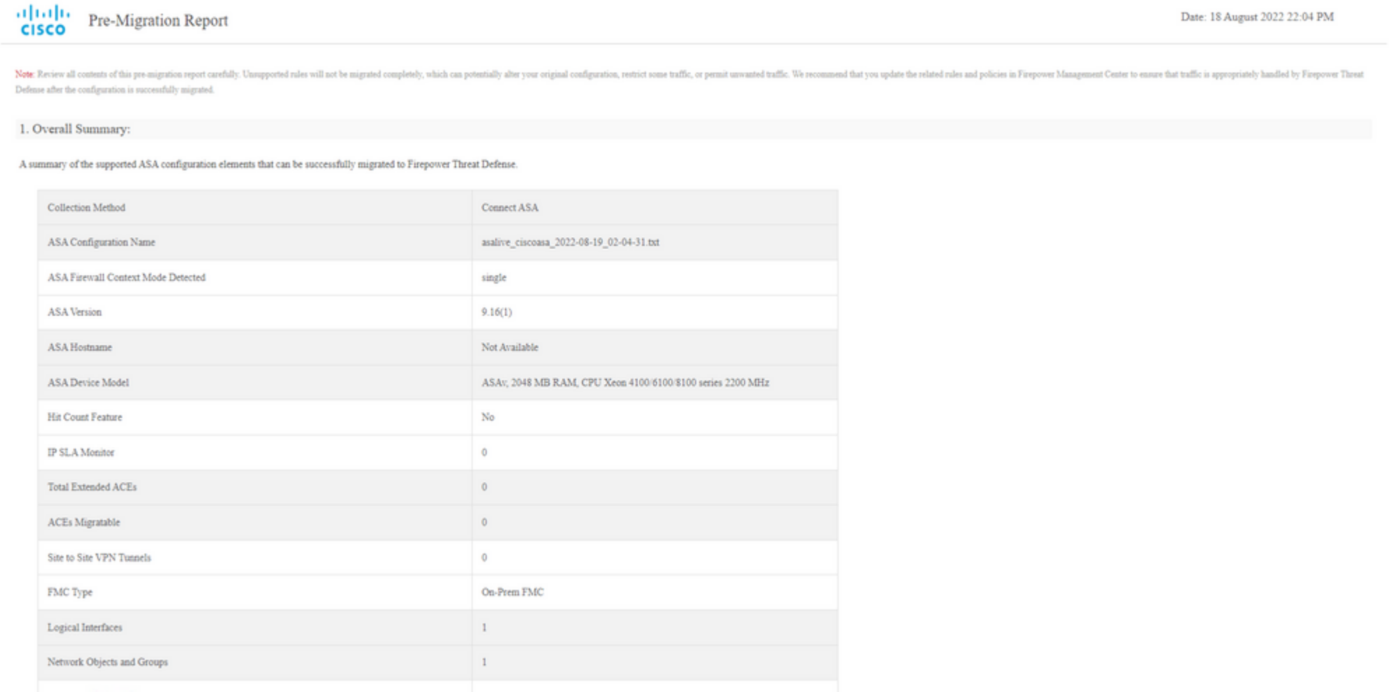
Start Conversion

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)

Pre-Migration report example, as shown in the image:



Pre-Migration Report

Date: 18 August 2022 22:04 PM

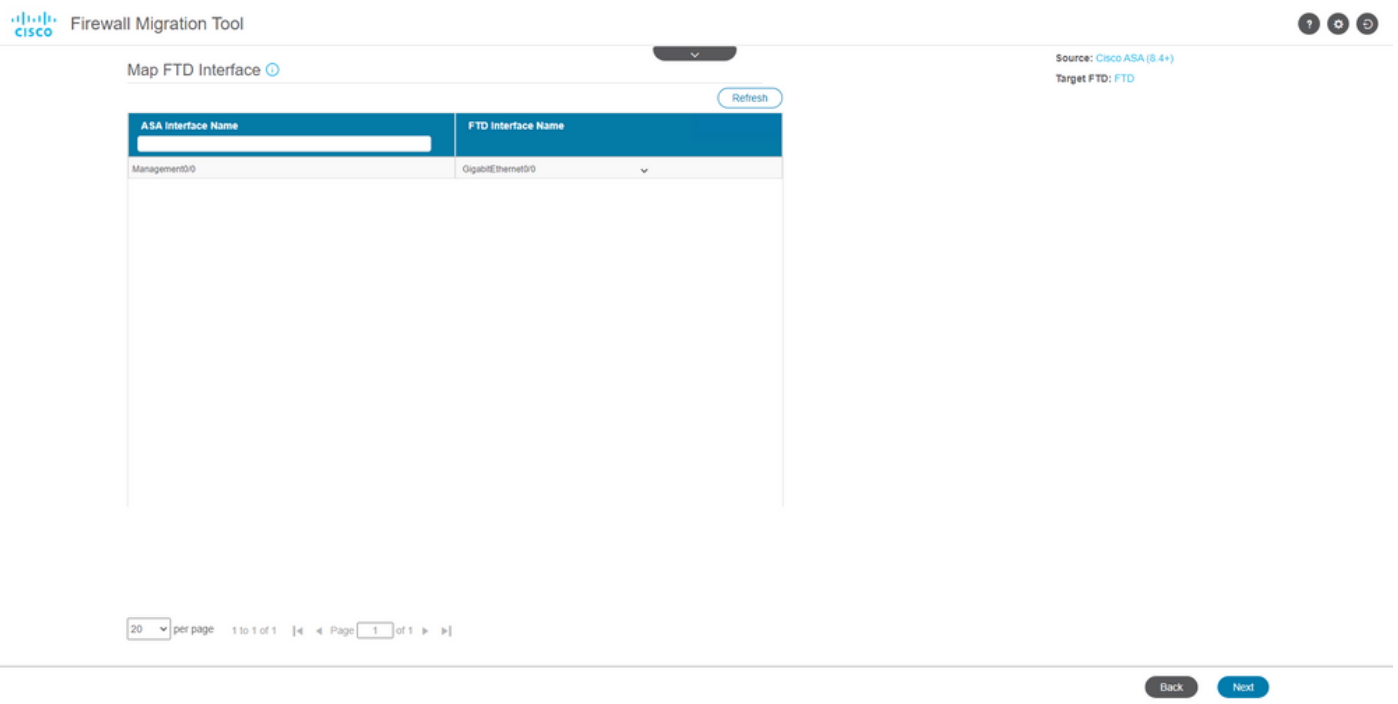
Note: Review all contents of this pre-migration report carefully. Unsupported rules will not be migrated completely, which can potentially alter your original configuration, restrict some traffic, or permit unwanted traffic. We recommend that you update the related rules and policies in Firepower Management 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. Map the ASA interfaces with the FTD interfaces on the Migration Tool.



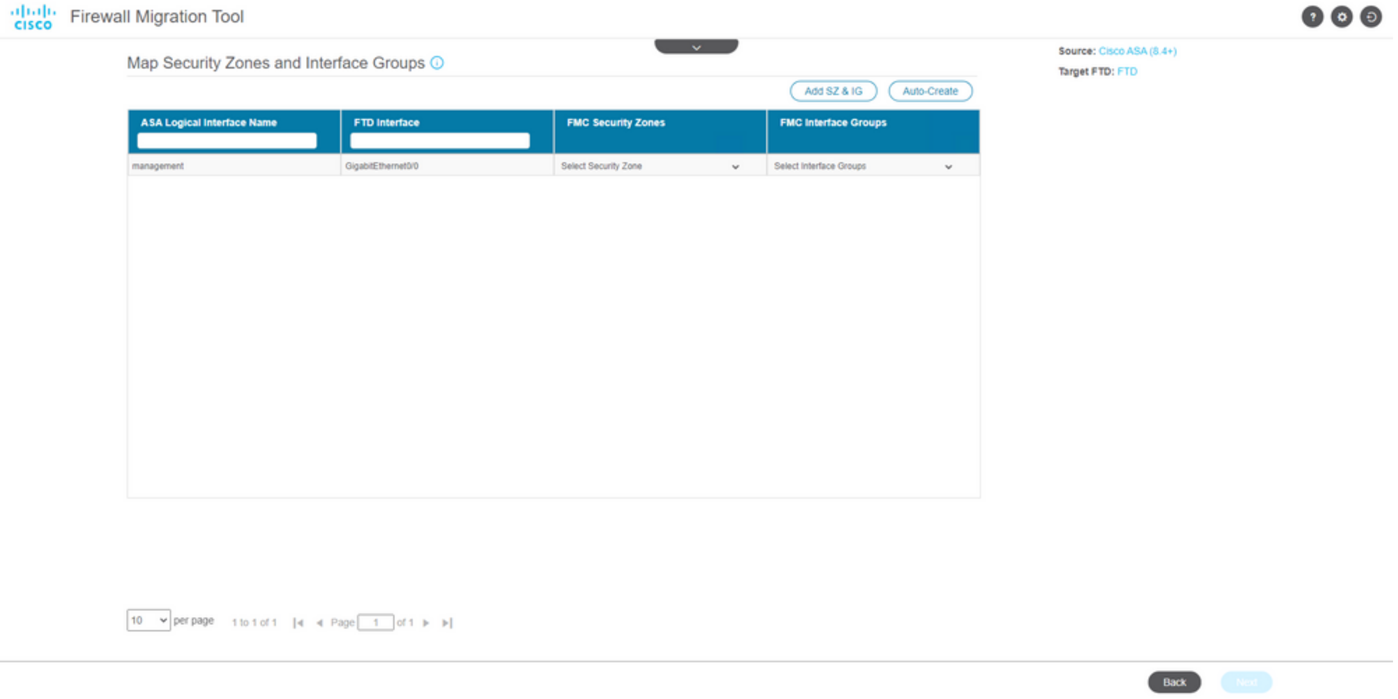
Map FTD Interface

Source: Cisco ASA (8.4+)

Target FTD: FTD

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

14. Create the Security Zones and Interface Groups for the interfaces on the FTD



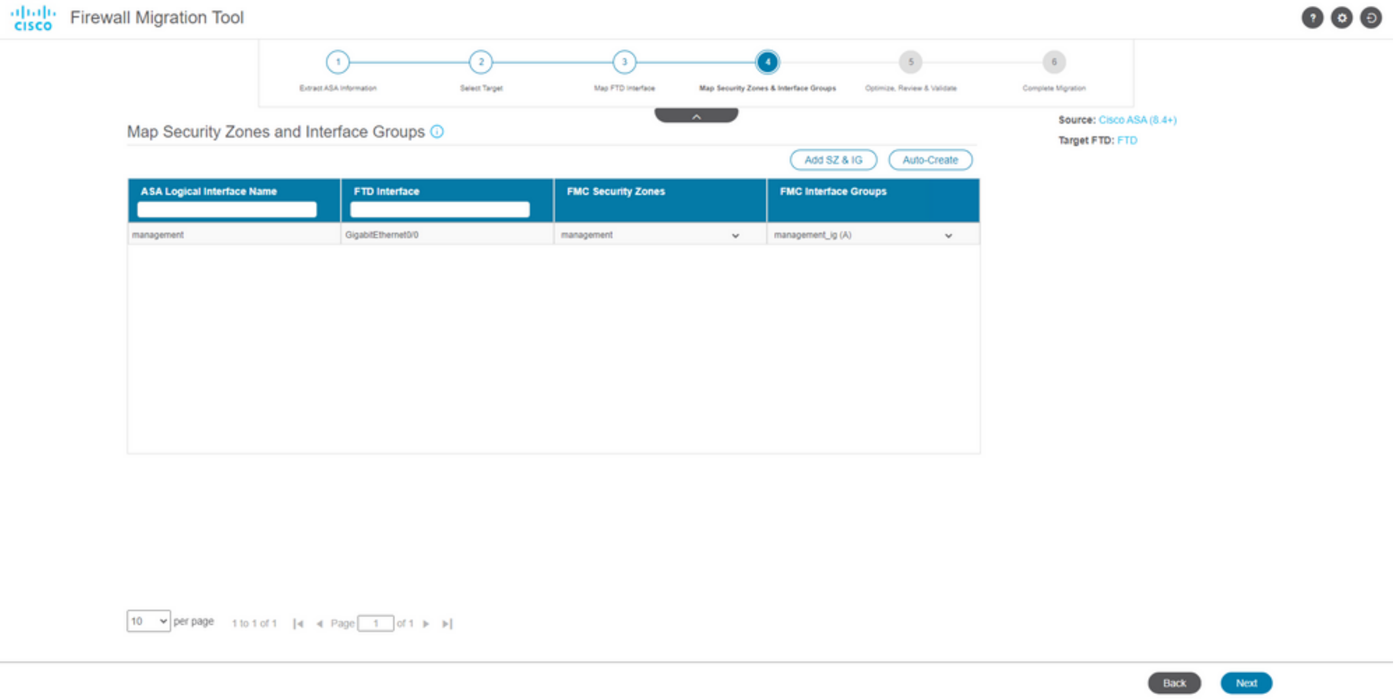
Map Security Zones and Interface Groups

Source: Cisco ASA (8.4+)

Target FTD: FTD

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

Security Zones (SZ) and Interface Groups (IG) are auto-created by the tool, as shown in the image:


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

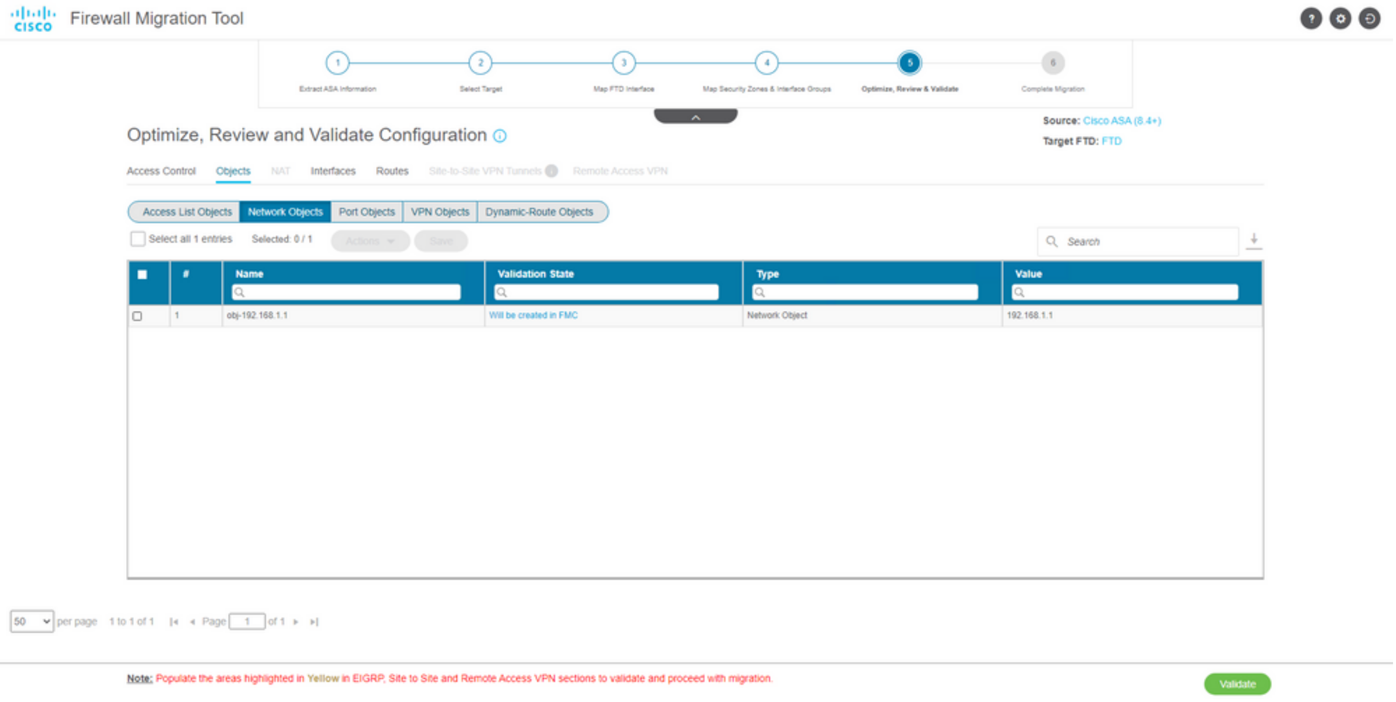
Map Security Zones and Interface Groups

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)

10 per page 1 to 1 of 1 Page 1 of 1

15. Review and validate the configurations to be migrated on the Migration Tool. If you have already finished the review and optimization of the configurations, click Validate.


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

Optimize, Review and Validate Configuration

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

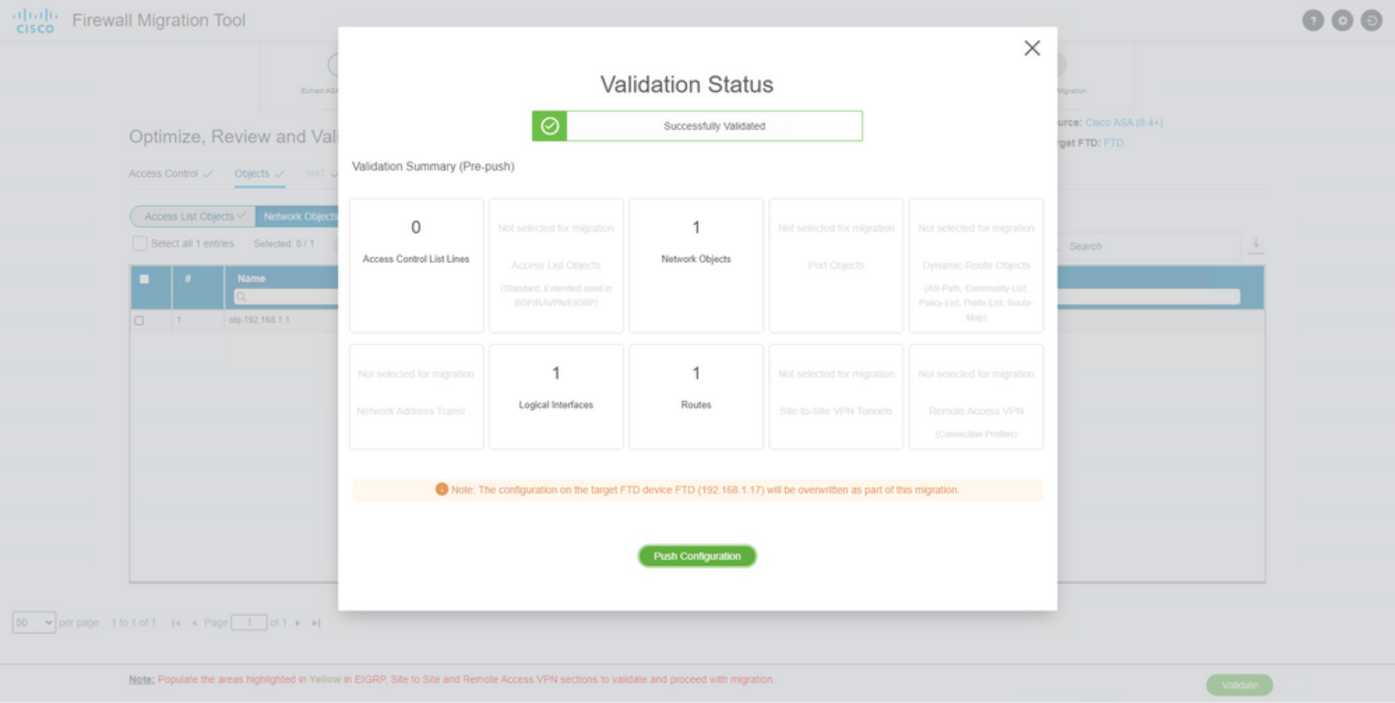
□ Select all 1 entries Selected: 0 / 1

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

50 per page 1 to 1 of 1 Page 1 of 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. If the validation status is successful, push the configurations to the target devices.



Validation Status

Successfully Validated

Validation Summary (Pre-push)

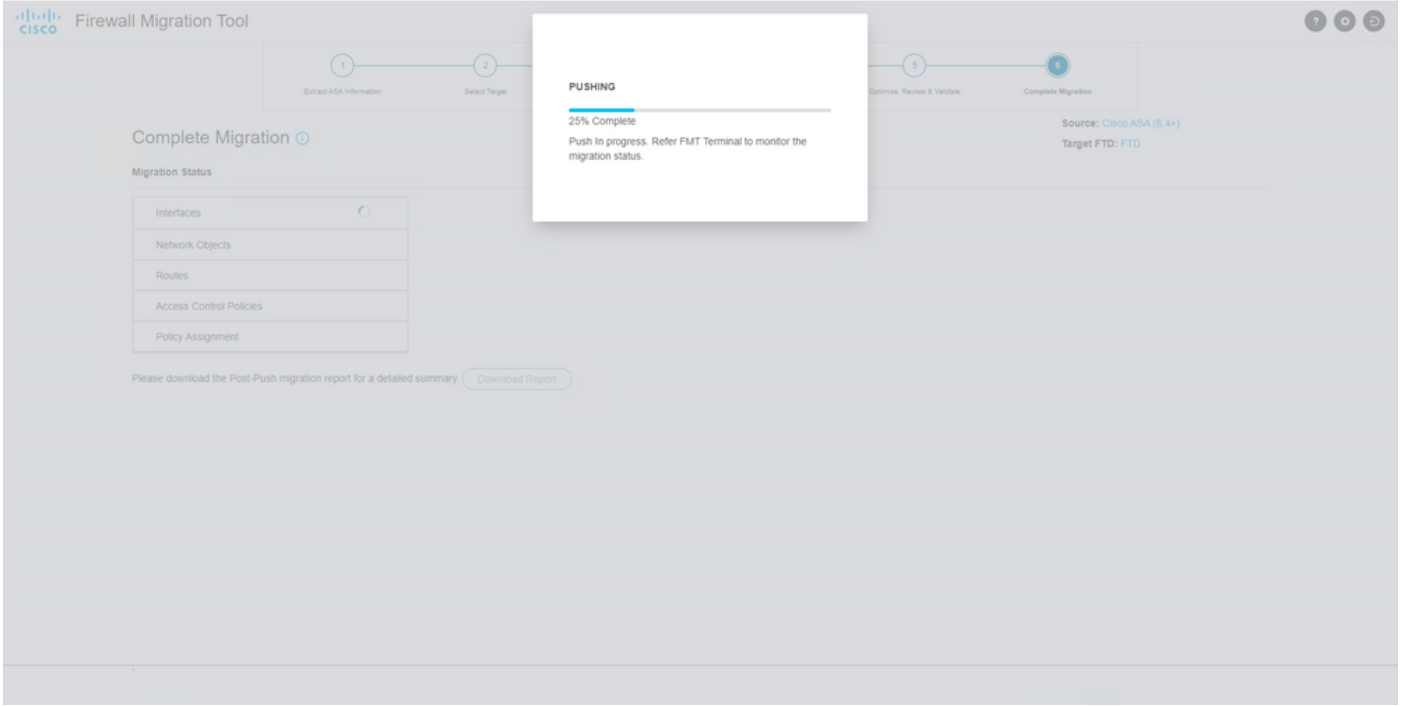
0 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	1 Network Objects	Not selected for migration Port Objects	Not selected for migration Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
Not selected 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.

Example of configuration pushed through the migration tool, as shown in the image:



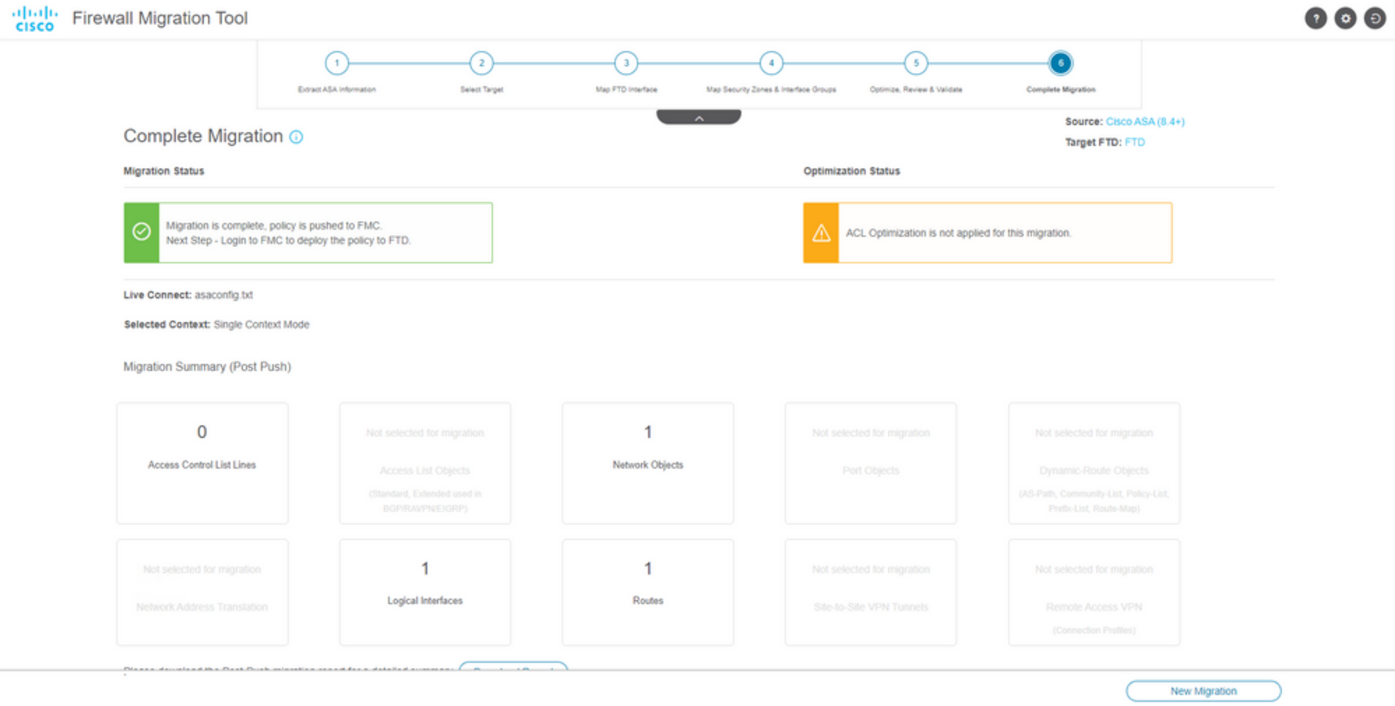
PUSHING

25% Complete

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

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

Example of a successful migration, as shown in the image:


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.

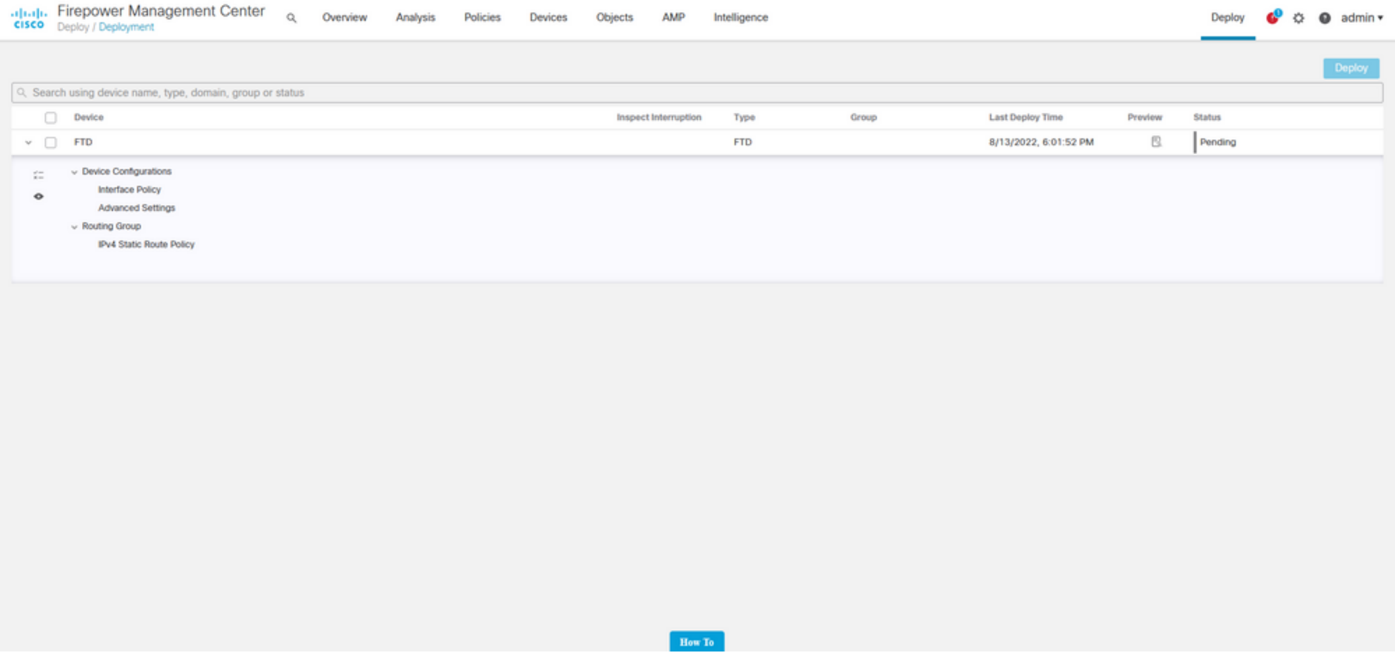
Live Connect: asaconfig.txt

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. *(Optional)* If you selected to migrate the configuration to an FTD, it requires a deployment to push the available configuration from the FMC to the firewall, in order to deploy the configuration: Log in to the FMC GUI.Navigate to the Deploy tab.Select the deployment to push configuration to the firewall.Click 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

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Verify the logs in the directory where the Firepower Migration Tool File was placed, for example:

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