Migrate ASA to Firepower Threat Defense (FTD) Using FMT

Contents

Introduction

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

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:

- Mac OS with Firepower Migration Tool (FMT) v7.0.1
- Adaptive Security Appliance (ASA) v9.16(1)
- Secure Firewall Management Center (FMCv) v7.4.2
- Secure Firewall Threat Defense Virtual (FTDv) v7.4.1

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.

Overview

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
- Cisco Secure Firewall Device Manager (7.2+)
- Check Point (r75-r77)
- Check Point (r80)
- Fortinet (5.0+)

• • Palo Alto Networks (6.1+)

Background Information

Before you migrate your ASA configuration, execute these activities:

Obtain the ASA Configuration File

To migrate an ASA device, use the **show running-config** for single context, or **show tech-support** for multi-context mode to obtain the configuration, save it as a .cfg or .txt file, and transfer it to the computer with the Secure Firewall migration tool.

Export PKI Certificate from ASA and Import into Management Center

Use this command to export the PKI certificate through the CLI from the source ASA config with the keys to a PKCS12 file:
ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
Then, import the PKI certificate into a management center (Object Management PKI Objects). For more information, see PKI Objects in the Firepower Management Center Configuration Guide.

Retrieve AnyConnect Packages and Profiles

AnyConnect profiles are optional and can be uploaded through the management center or Secure Firewall migration tool.

Use this command to copy the required package from the source ASA to an FTP or TFTP server:

Copy <source file location:/source file name> <destination>

ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <----- Example of copying Anyconnect Package.

ASA# copy disk0:/ external-sso- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <----- Example of copying External Browser Package.

ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <----- Example of copying Hostscan Package.

ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <----- Example of copying Dap.xml

ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- Example of copying Data.xml

ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Example of copying Anyconnect Profile.

Import the downloaded packages to management center (**Object Management** > **VPN** > **AnyConnect File**).

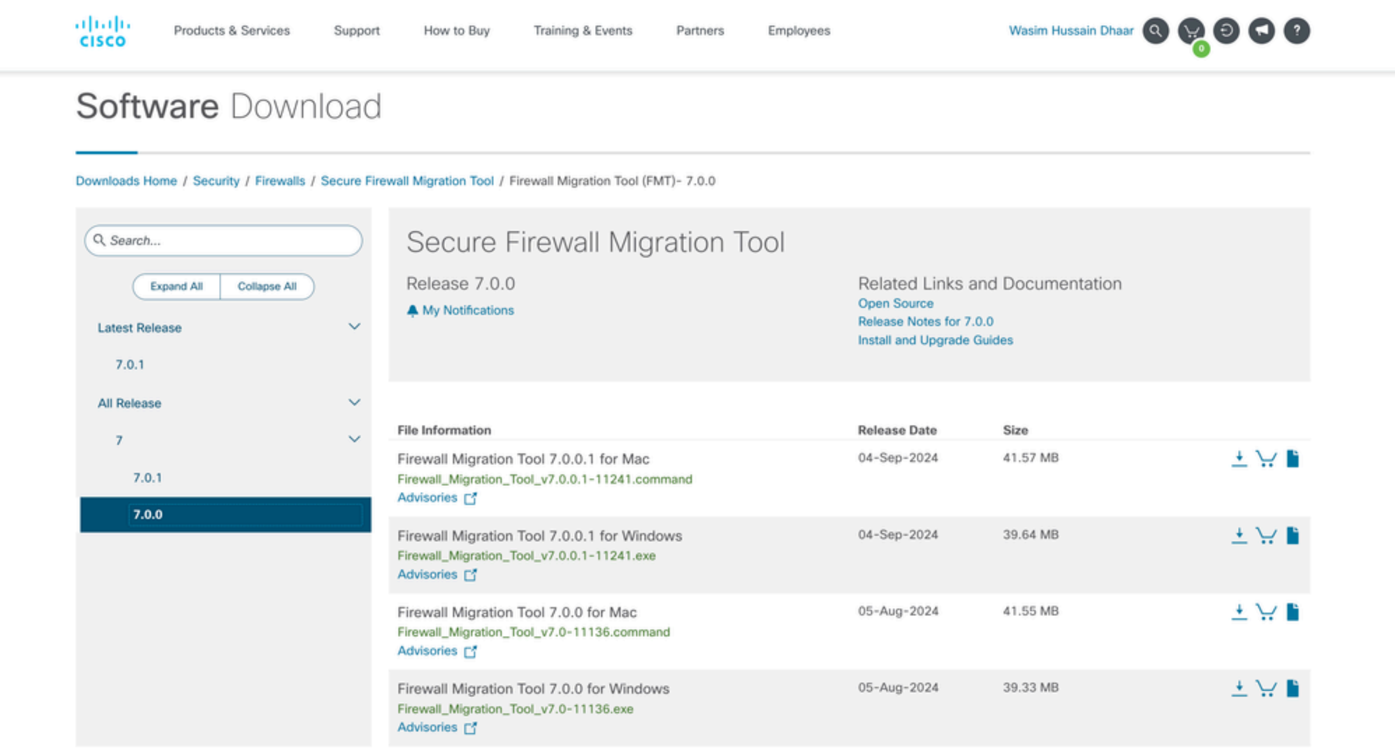
a-Dap.xml and Data.xml must be uploaded to the management center from the Secure Firewall migration tool in the **Review and Validate** > **Remote Access VPN** > **AnyConnect File** section.

b-AnyConnect profiles can be uploaded directly to the management center or through the Secure Firewall migration tool in the **Review and Validate** > **Remote Access VPN** > **AnyConnect File** section.

Configure

Configuration Steps :

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



Software Download

Downloads Home / Security / Firewalls / Secure Firewall Migration Tool / Firewall Migration Tool (FMT)- 7.0.0

Secure Firewall Migration Tool

Release 7.0.0

My Notifications

Related Links and Documentation

Open Source

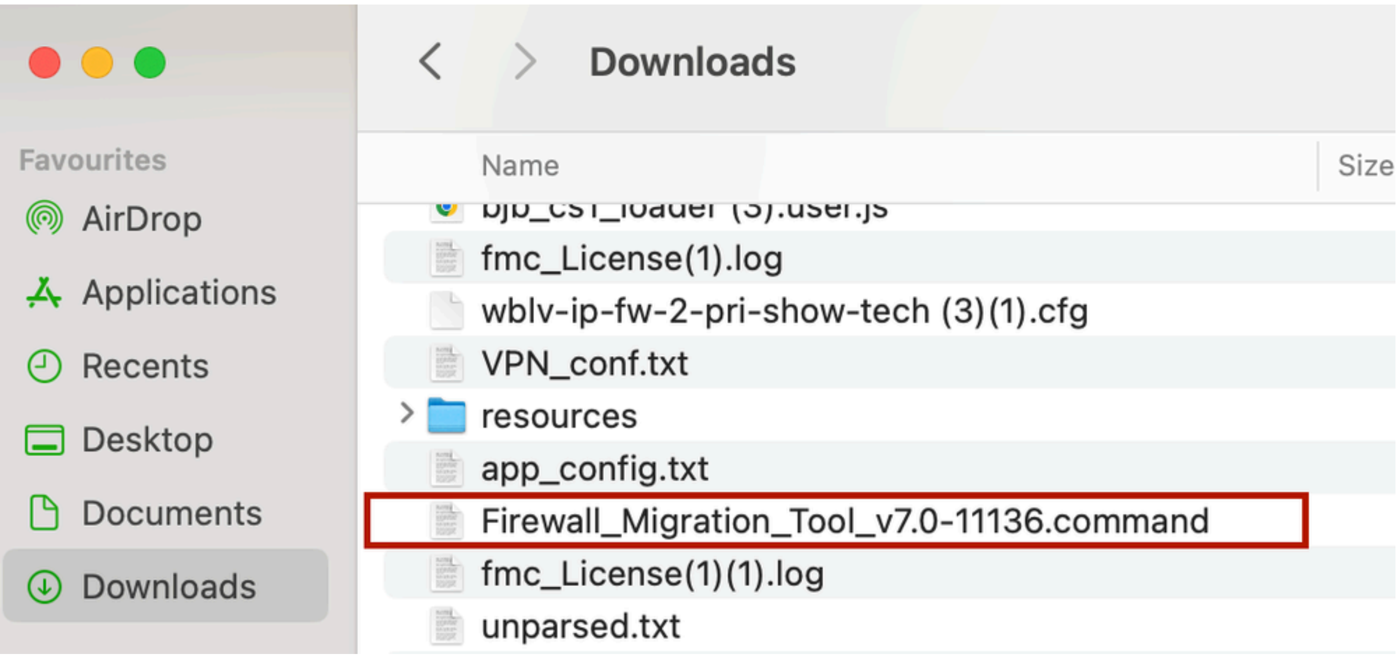
Release Notes for 7.0.0

Install and Upgrade Guides

File Information	Release Date	Size
Firewall Migration Tool 7.0.0.1 for Mac Firewall_Migration_Tool_v7.0.0.1-11241.command Advisories	04-Sep-2024	41.57 MB
Firewall Migration Tool 7.0.0.1 for Windows Firewall_Migration_Tool_v7.0.0.1-11241.exe Advisories	04-Sep-2024	39.64 MB
Firewall Migration Tool 7.0.0 for Mac Firewall_Migration_Tool_v7.0-11136.command Advisories	05-Aug-2024	41.55 MB
Firewall Migration Tool 7.0.0 for Windows Firewall_Migration_Tool_v7.0-11136.exe Advisories	05-Aug-2024	39.33 MB

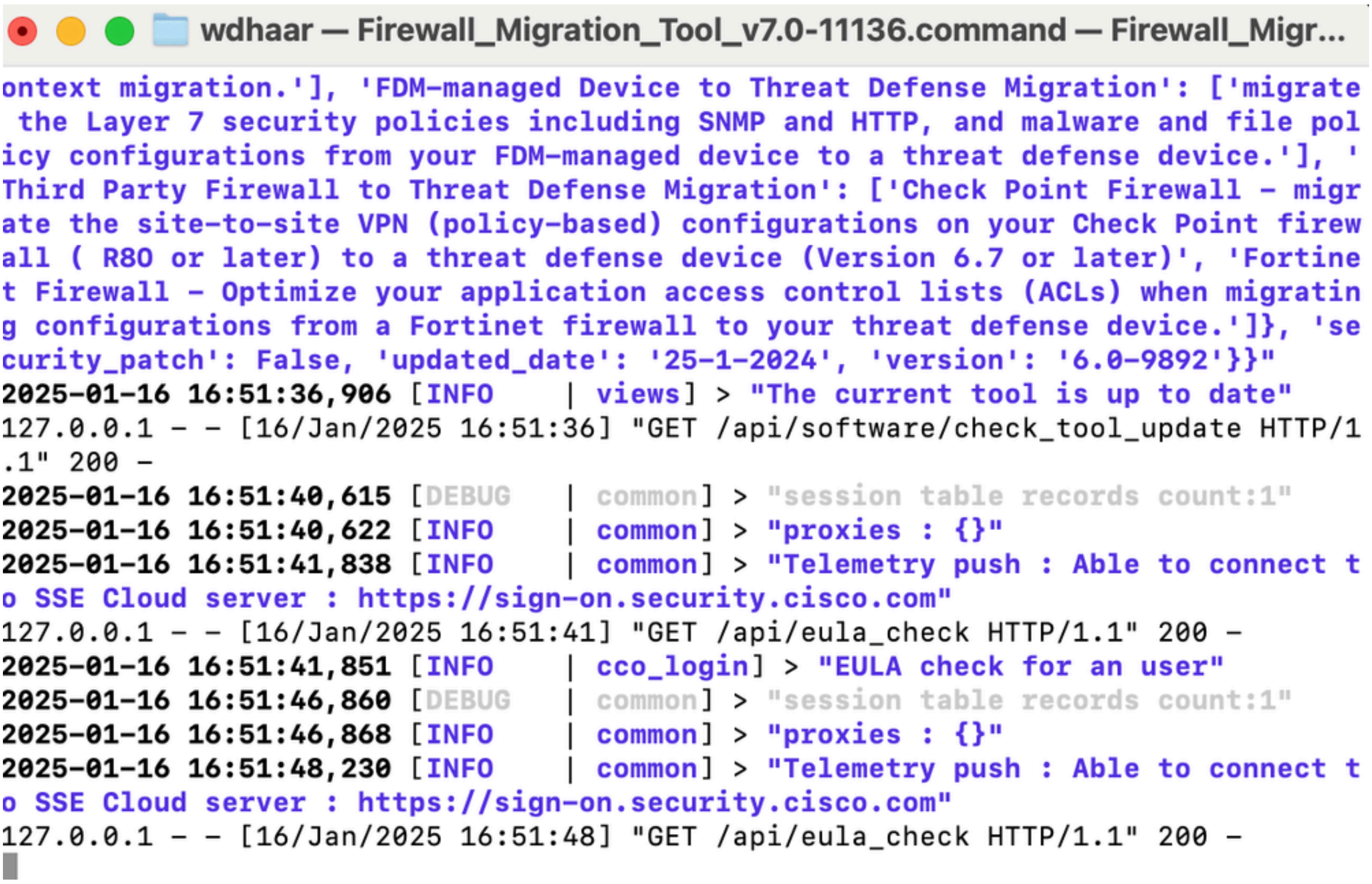
Software Download

2. Click the file you previously downloaded to your computer.



bjb_cs1_loader (3).user.js
fmc_License(1).log
wblv-ip-fw-2-pri-show-tech (3)(1).cfg
VPN_conf.txt
resources
app_config.txt
Firewall_Migration_Tool_v7.0-11136.command
fmc_License(1)(1).log
unparsed.txt

The File

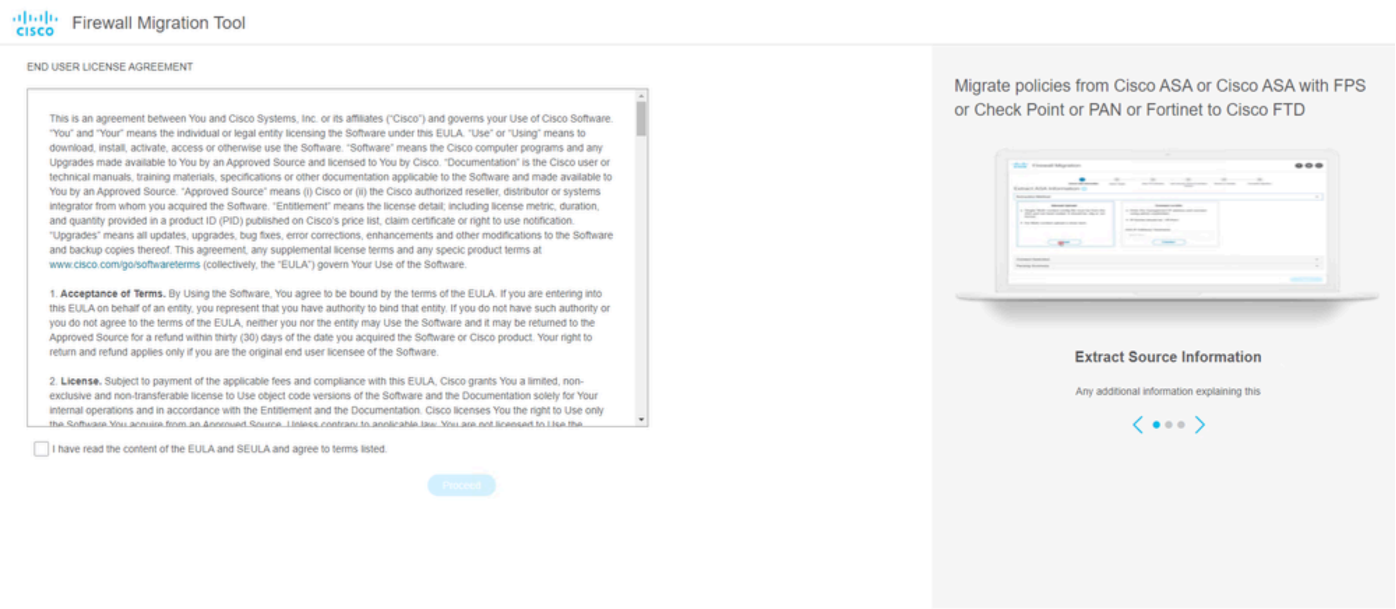

wdhaar — Firewall_Migration_Tool_v7.0-11136.command — Firewall_Migr...

```
ontext migration.'], 'FDM-managed Device to Threat Defense Migration': ['migrate
 the Layer 7 security policies including SNMP and HTTP, and malware and file pol
icy configurations from your FDM-managed device to a threat defense device.'], '
Third Party Firewall to Threat Defense Migration': ['Check Point Firewall - migr
ate the site-to-site VPN (policy-based) configurations on your Check Point firew
all ( R80 or later) to a threat defense device (Version 6.7 or later)', 'Fortine
t Firewall - Optimize your application access control lists (ACLs) when migratin
g configurations from a Fortinet firewall to your threat defense device.']}, 'se
curity_patch': False, 'updated_date': '25-1-2024', 'version': '6.0-9892'}}"
2025-01-16 16:51:36,906 [INFO     | views] > "The current tool is up to date"
127.0.0.1 - - [16/Jan/2025 16:51:36] "GET /api/software/check_tool_update HTTP/1
.1" 200 -
2025-01-16 16:51:40,615 [DEBUG    | common] > "session table records count:1"
2025-01-16 16:51:40,622 [INFO     | common] > "proxies : {}"
2025-01-16 16:51:41,838 [INFO     | common] > "Telemetry push : Able to connect t
o SSE Cloud server : https://sign-on.security.cisco.com"
127.0.0.1 - - [16/Jan/2025 16:51:41] "GET /api/eula_check HTTP/1.1" 200 -
2025-01-16 16:51:41,851 [INFO     | cco_login] > "EULA check for an user"
2025-01-16 16:51:46,860 [DEBUG    | common] > "session table records count:1"
2025-01-16 16:51:46,868 [INFO     | common] > "proxies : {}"
2025-01-16 16:51:48,230 [INFO     | common] > "Telemetry push : Able to connect t
o SSE Cloud server : https://sign-on.security.cisco.com"
127.0.0.1 - - [16/Jan/2025 16:51:48] "GET /api/eula_check HTTP/1.1" 200 -
```

Console Logs

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

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



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.

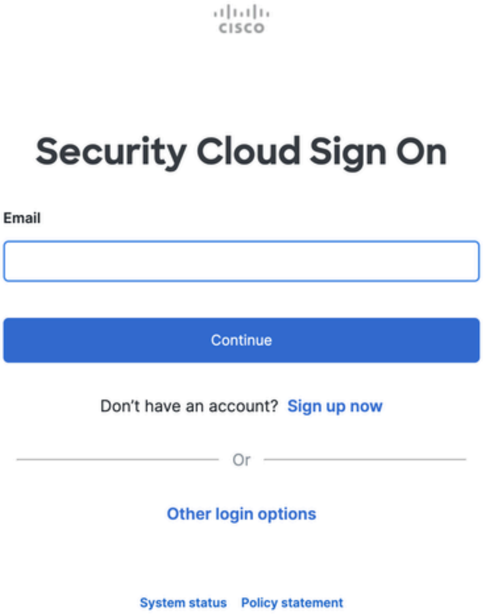
Migrate policies from Cisco ASA or Cisco ASA with FPS or Check Point or PAN or Fortinet to Cisco FTD

Extract Source Information

Any additional information explaining this

EULA

4. Log in using a valid CCO account and the FMT GUI interface appears on the web browser.



Security Cloud Sign On

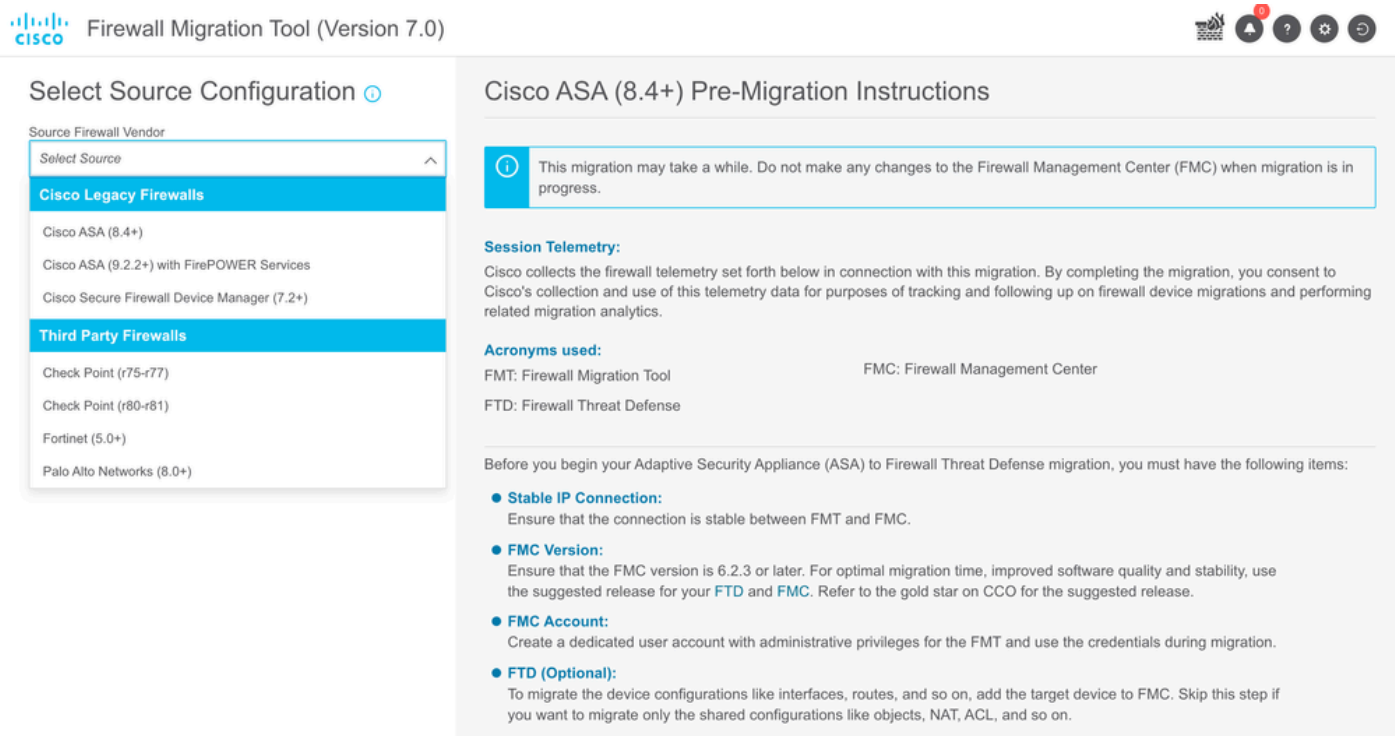
Email

Don't have an account? Sign up now

Or

FMT Login

5. Select the Source Firewall to migrate.



Firewall Migration Tool (Version 7.0)

Select Source Configuration

Source Firewall Vendor

Select Source

Cisco Legacy Firewalls

- Cisco ASA (8.4+)
- Cisco ASA (9.2.2+) with FirePOWER Services
- Cisco Secure Firewall Device Manager (7.2+)

Third Party Firewalls

- Check Point (r75-r77)
- Check Point (r80-r81)
- Fortinet (5.0+)
- Palo Alto Networks (8.0+)

Cisco ASA (8.4+) Pre-Migration Instructions

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

Session Telemetry:

Cisco collects the firewall telemetry set forth below in connection with this migration. By completing the migration, you consent to Cisco's collection and use of this telemetry data for purposes of tracking and following up on firewall device migrations and performing related migration analytics.

Acronyms used:

FMT: Firewall Migration Tool

FMC: Firewall Management Center

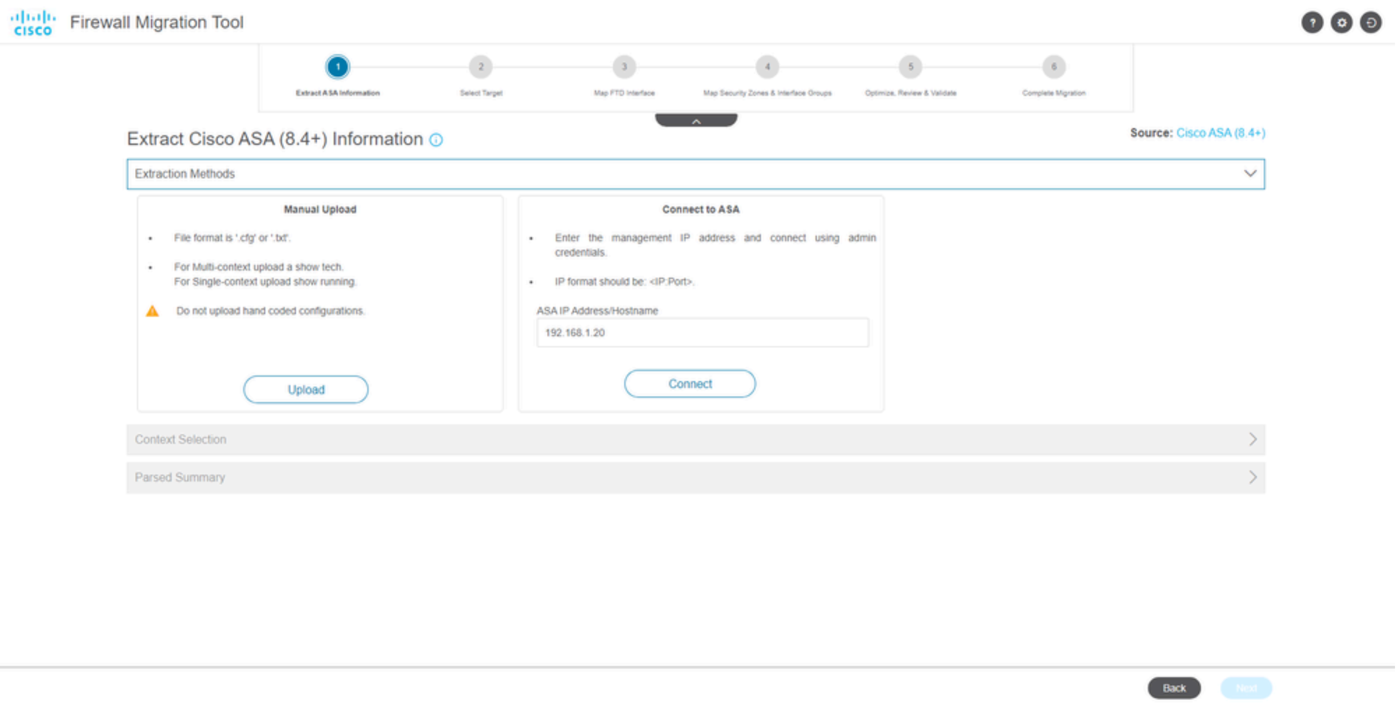
FTD: Firewall Threat Defense

Before you begin your Adaptive Security Appliance (ASA) to Firewall 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.

Source Firewall

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



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
Back
Next

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.

Upload

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

Connect

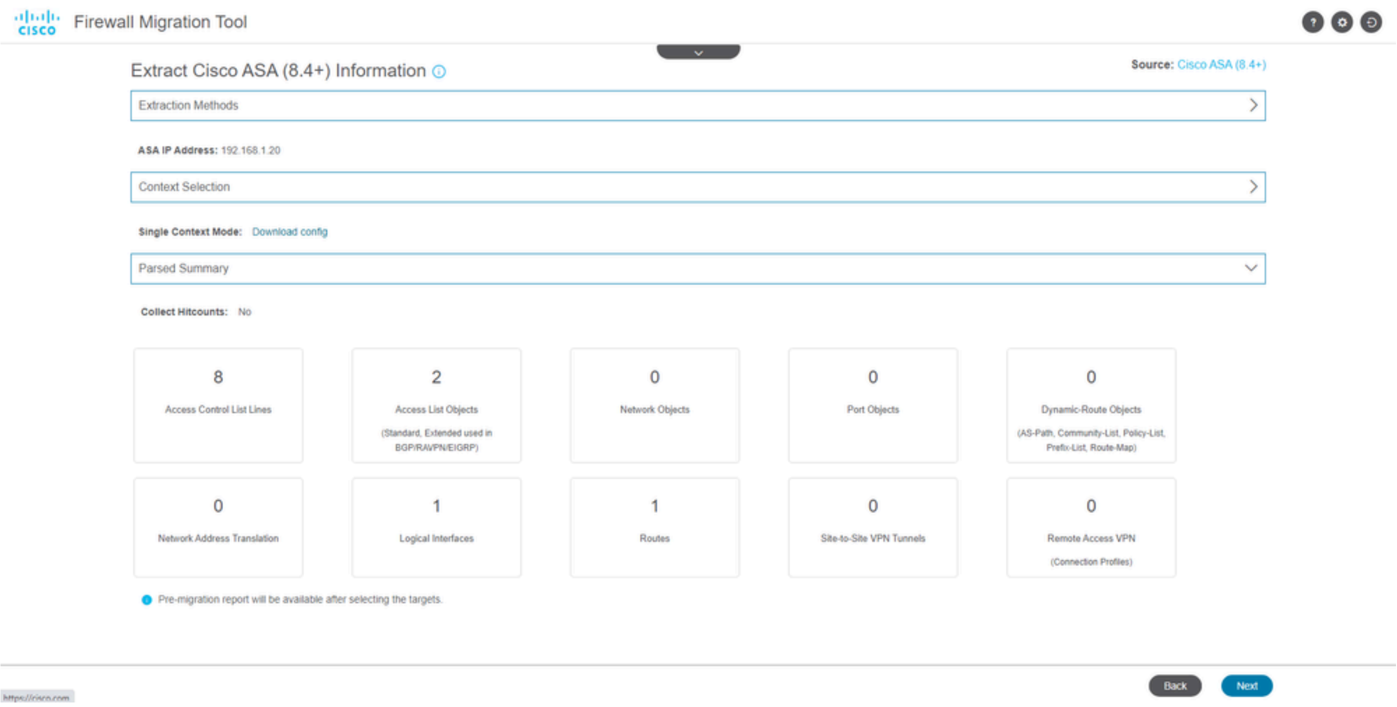
Context Selection

Parsed Summary

Extraction

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**.



Firewall Migration Tool

Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

Extraction Methods

ASA IP Address: 192.168.1.20

Context Selection

Single Context Mode: Download config

Parsed Summary

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)

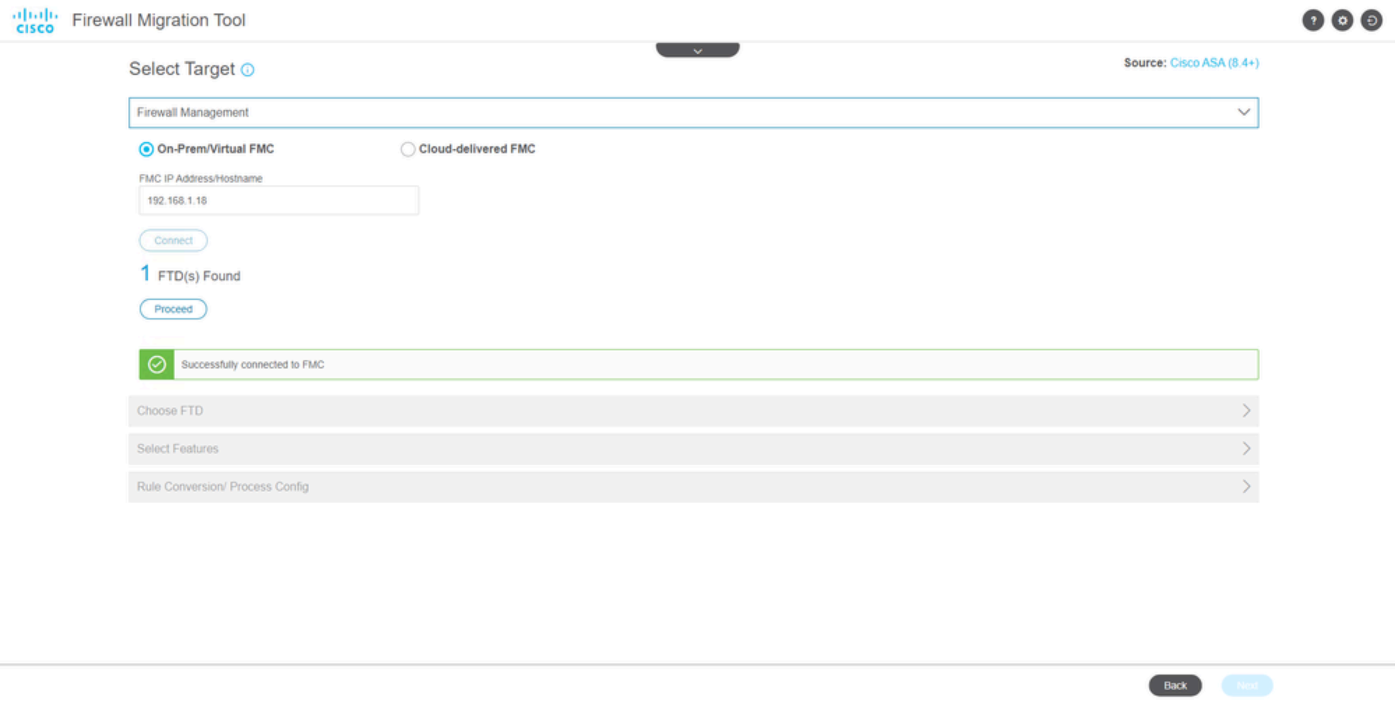
Pre-migration report will be available after selecting the targets.

https://cisco.com

Summary

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

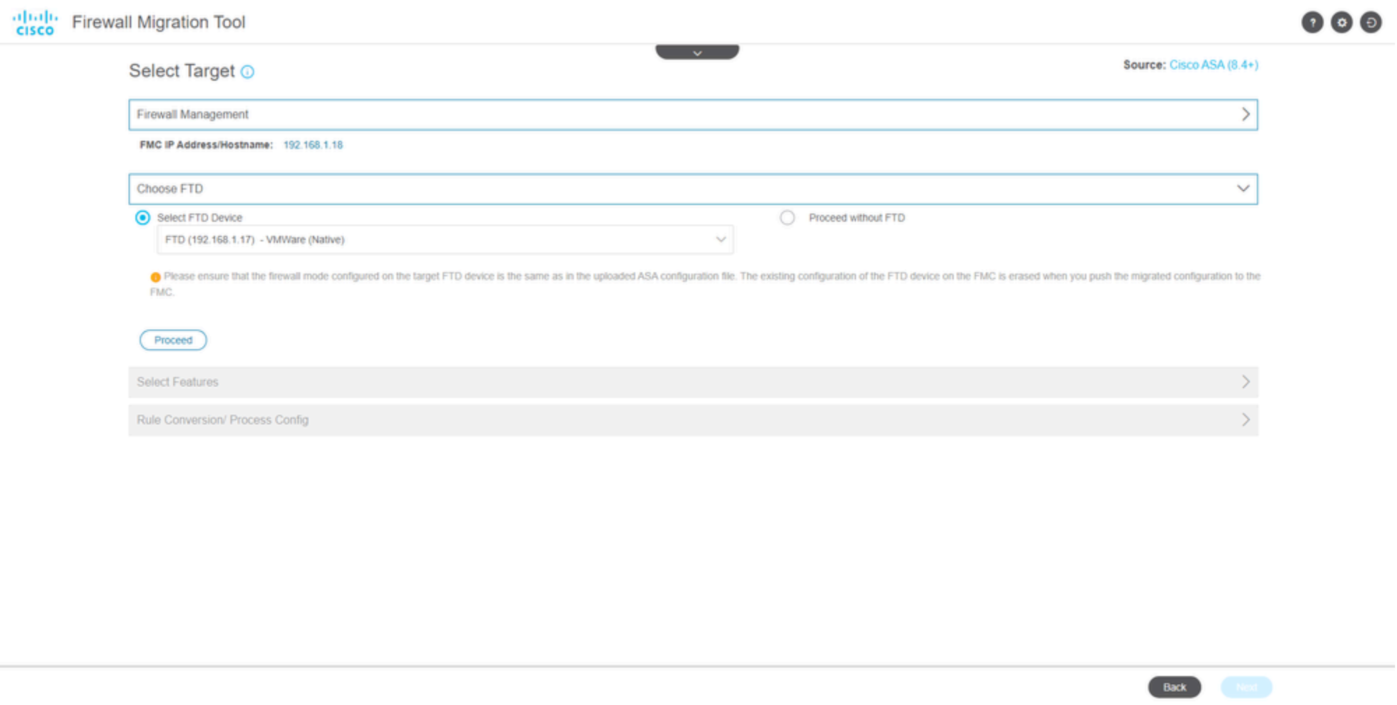
Choose FTD

Select Features

Rule Conversion/ Process Config

FMC IP

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



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.

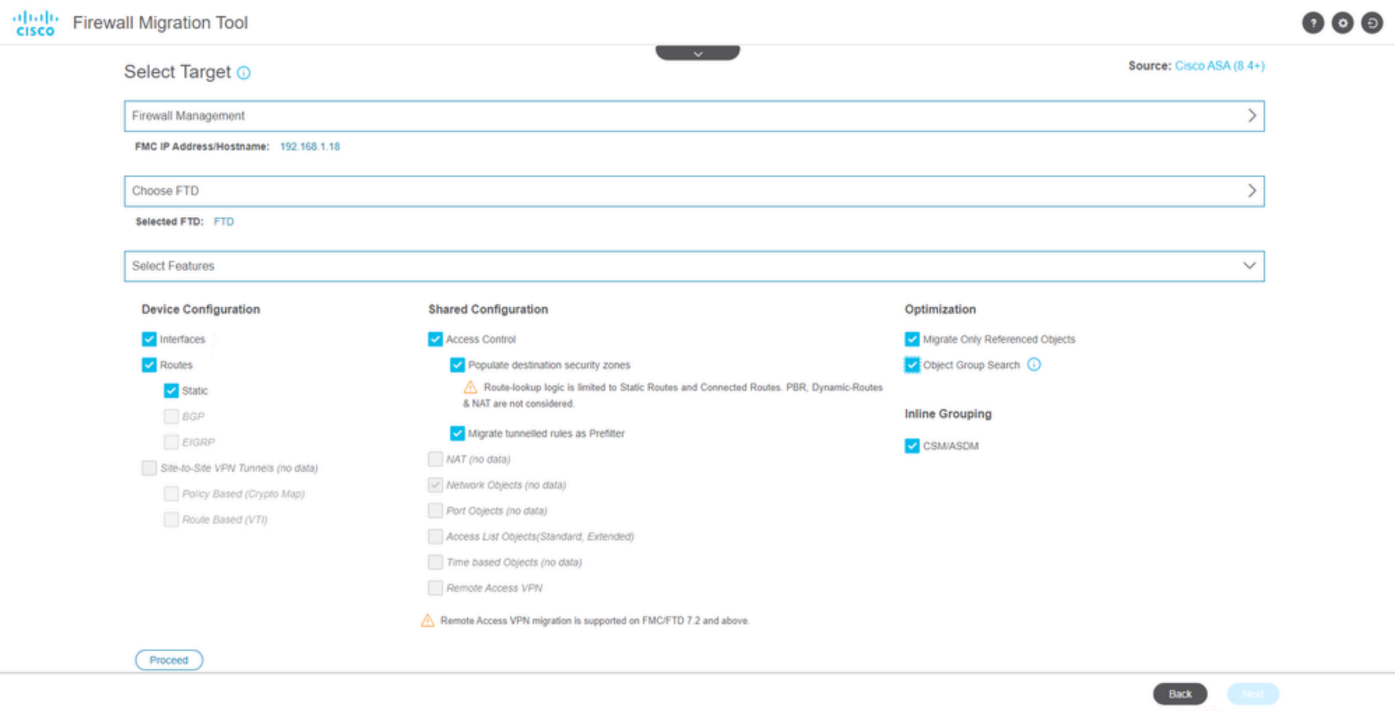
Proceed

Select Features

Rule Conversion/ Process Config

Target FTD

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



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

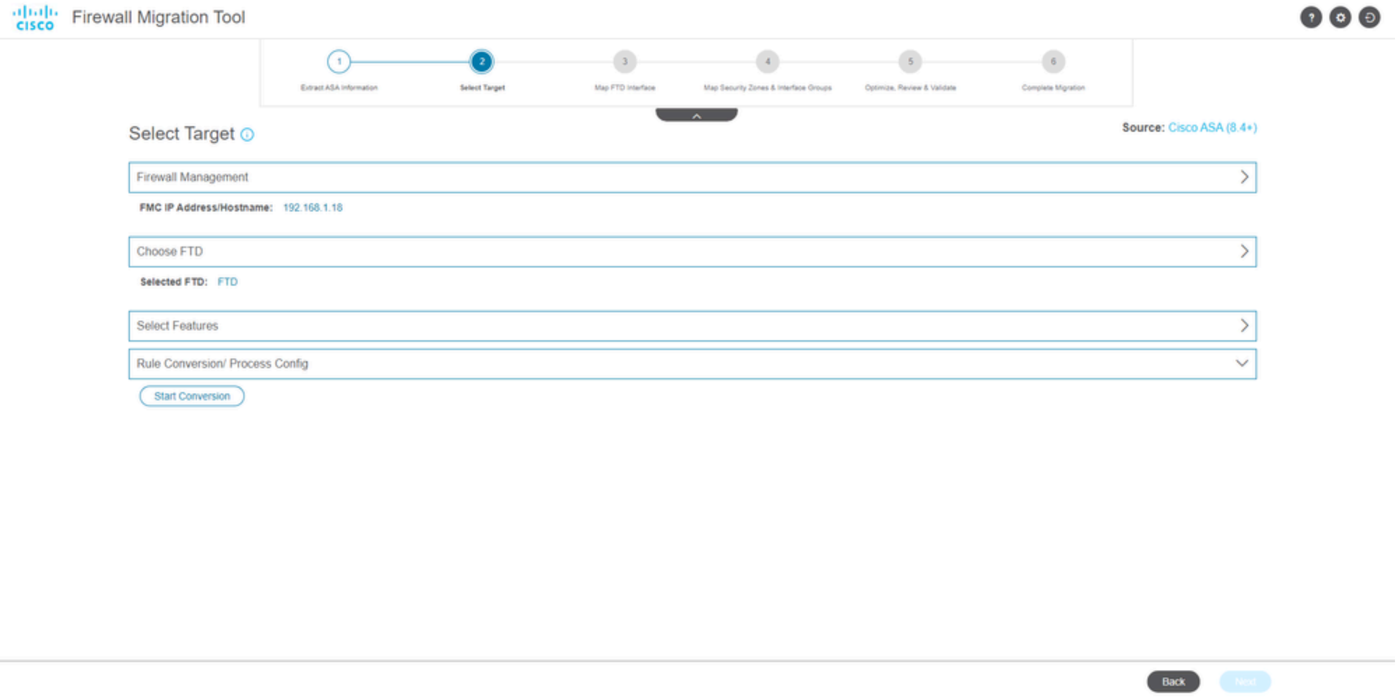
Inline Grouping

☑ CSM/ASDM

Proceed

Configurations

11. Start the conversion of the configurations from ASA to FTD.



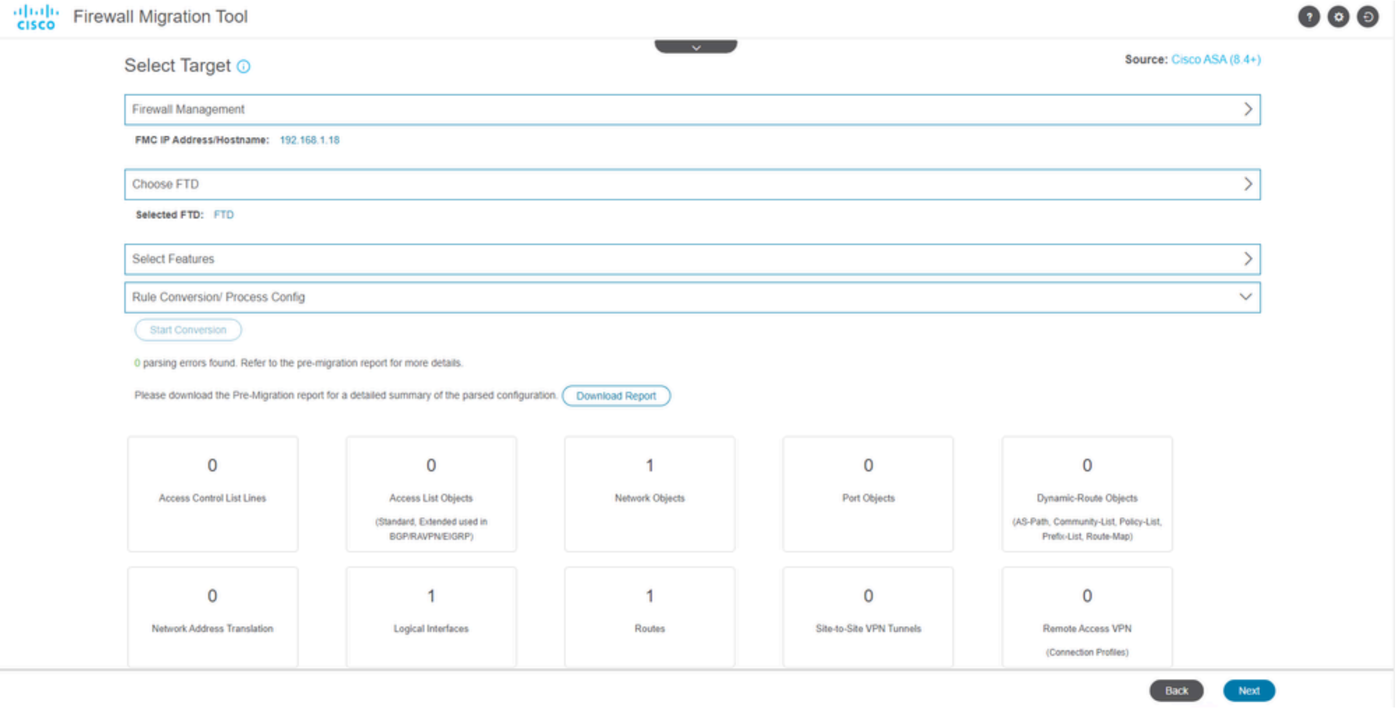
Source: Cisco ASA (8.4+)

FMC IP Address/Hostname: 192.168.1.18

Selected FTD: FTD

Start Conversion

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



Source: Cisco ASA (8.4+)

FMC IP Address/Hostname: 192.168.1.18

Selected FTD: FTD

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.

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

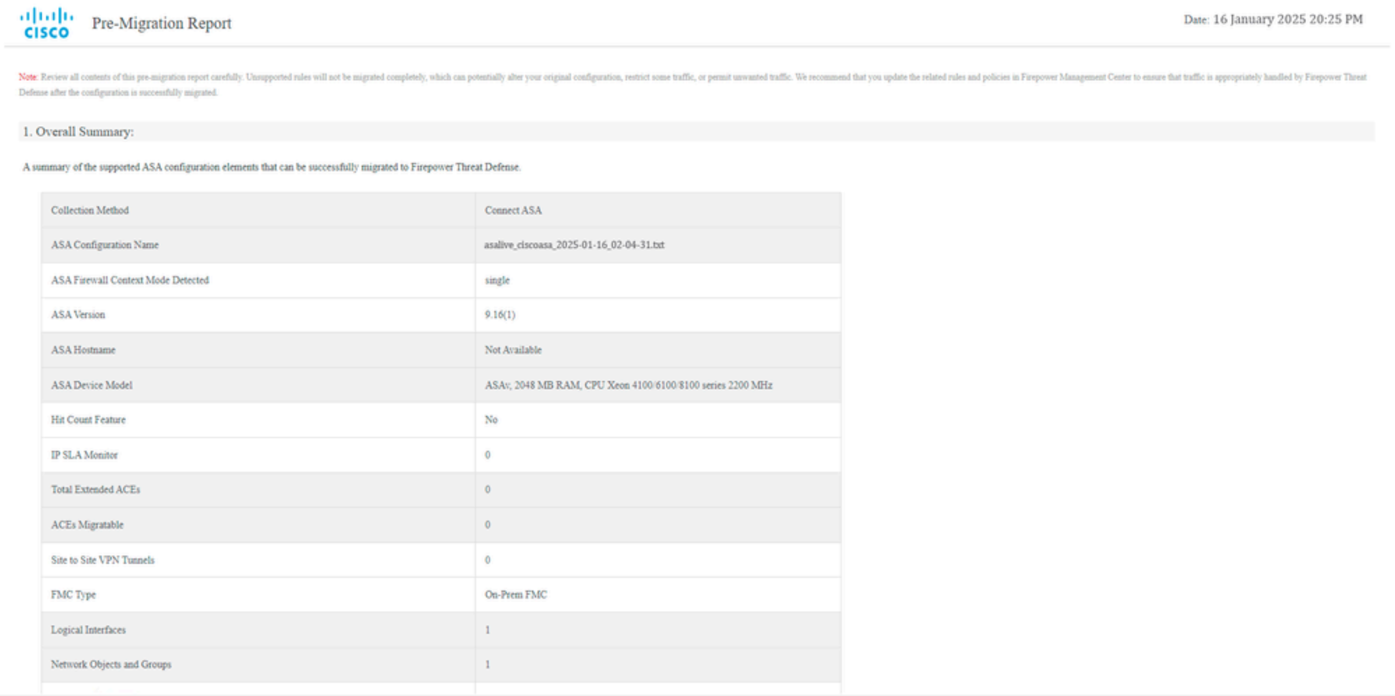
1 Routes

0 Site-to-Site VPN Tunnels

0 Remote Access VPN (Connection Profiles)

Download Report

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



Pre-Migration Report

Date: 16 January 2025 20:25 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.

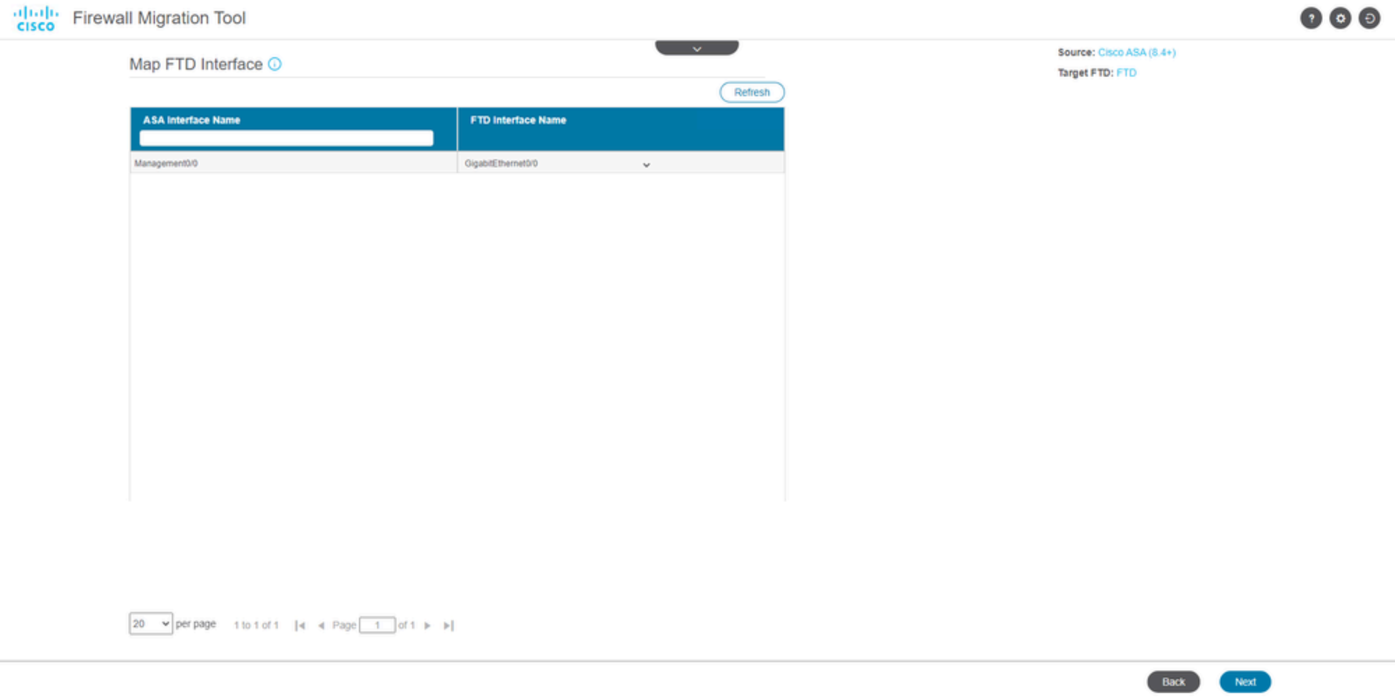
1. Overall Summary:

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_2025-01-16_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

Pre-Migration Report

13. Map the ASA interfaces with the FTD interfaces on the Migration Tool.

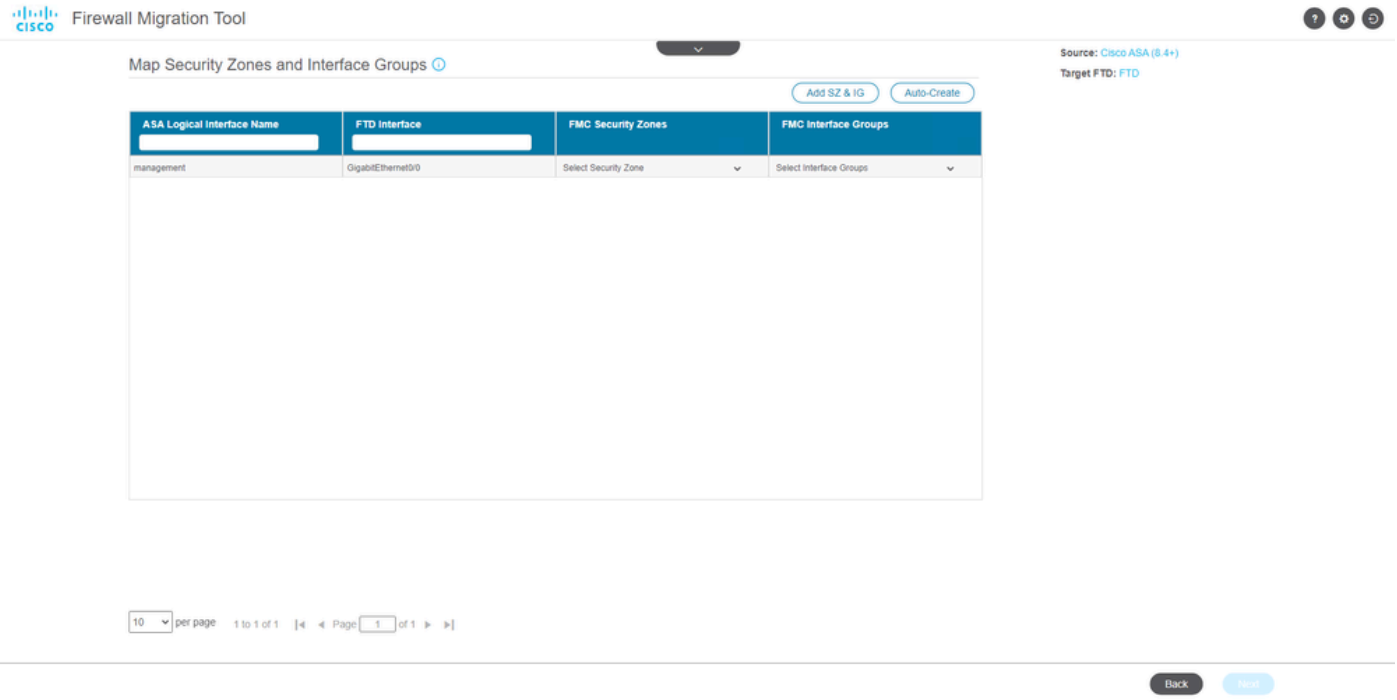


Map FTD Interface

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

Map interfaces

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



Firewall Migration Tool

Map Security Zones and Interface Groups

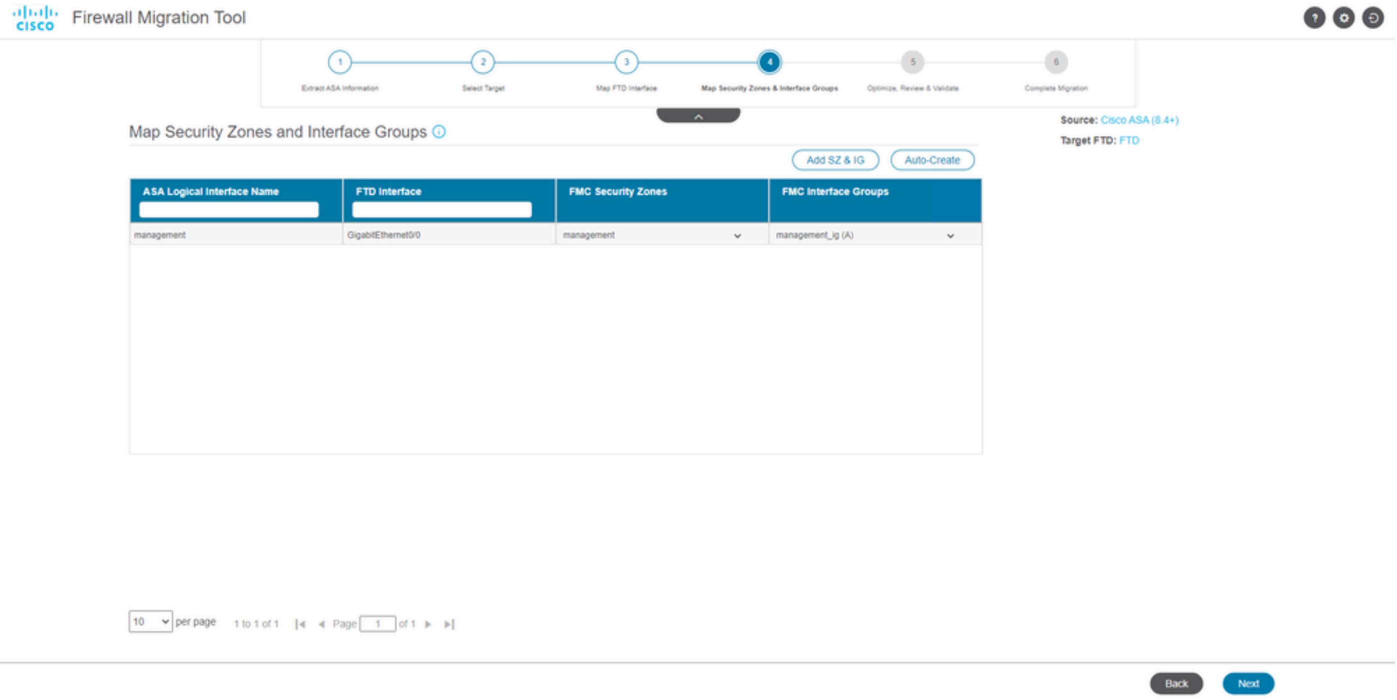
Source: Cisco ASA (8.4+)

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 & 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

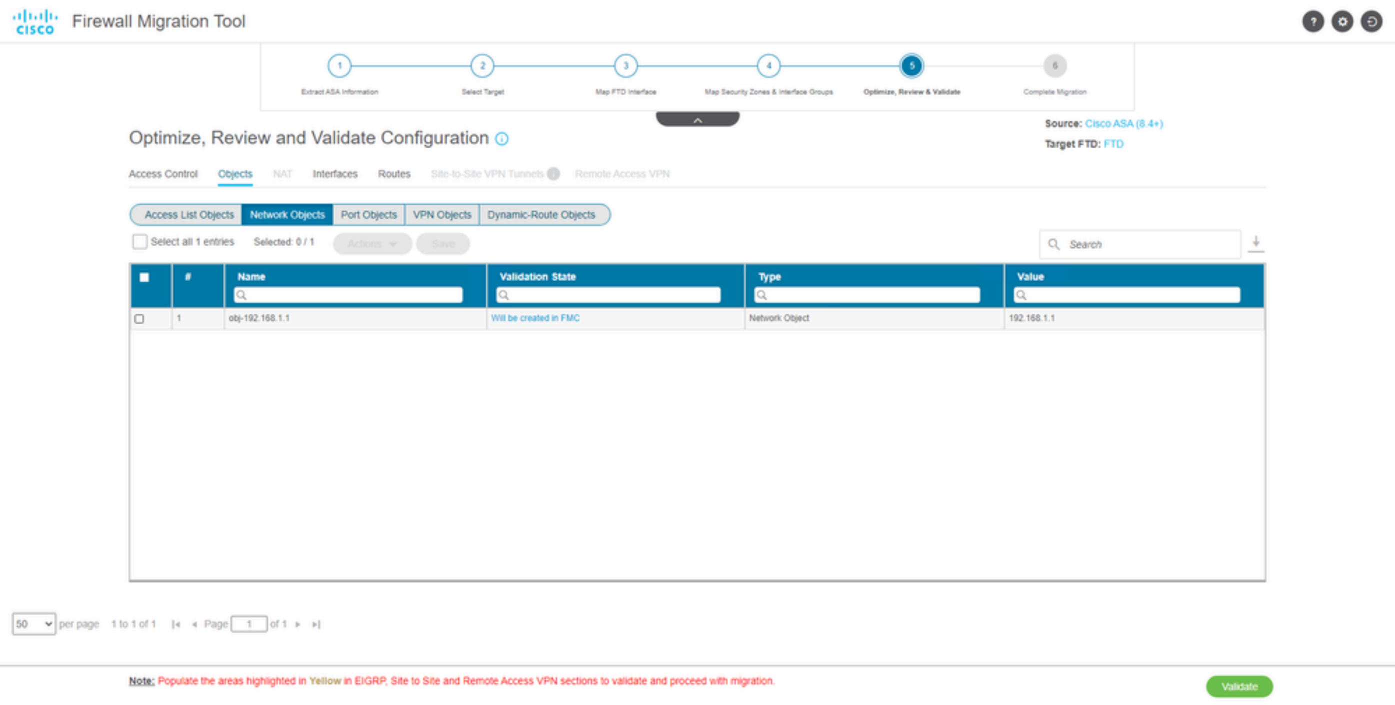
Source: Cisco ASA (8.4+)

Target FTD: FTD

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

Auto-Create tool

15. Review and validate the configurations to be migrated on the Migration Tool.
    1. 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

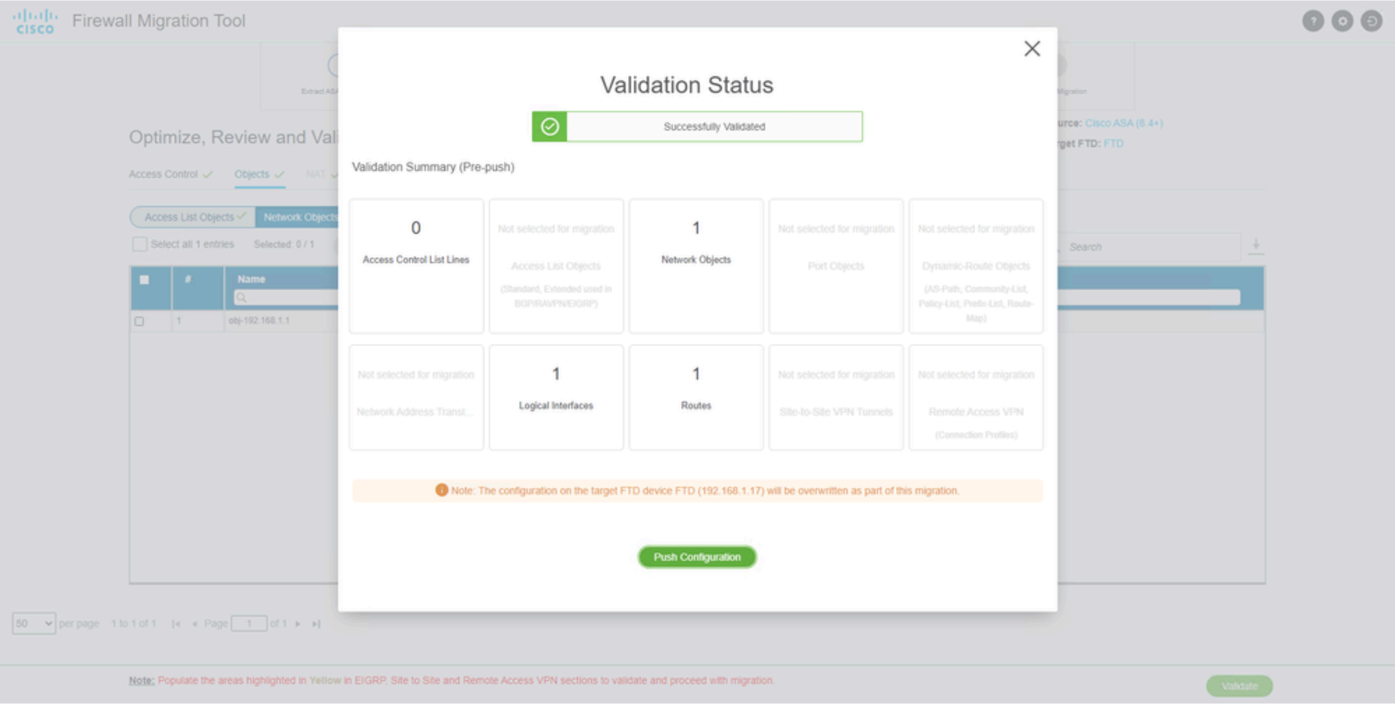
	#	Name	Validation State	Type	Value
☐	1	obj-192.168.1.1	Will be created in FMC	Network Object	192.168.1.1

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.

Review and validate

16. If the validation status is successful, push the configurations to the target devices.



Validation Status

Successfully Validated

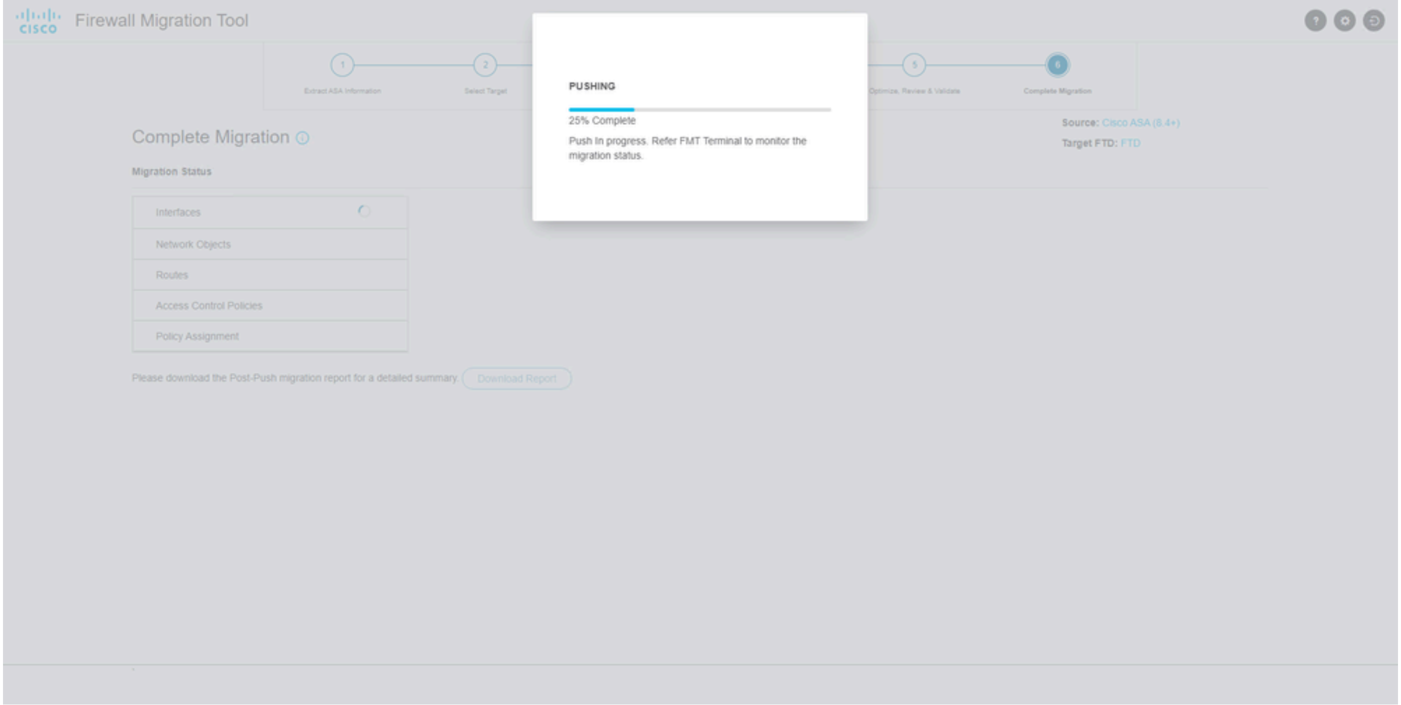
Validation Summary (Pre-push)

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.

Validation

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.

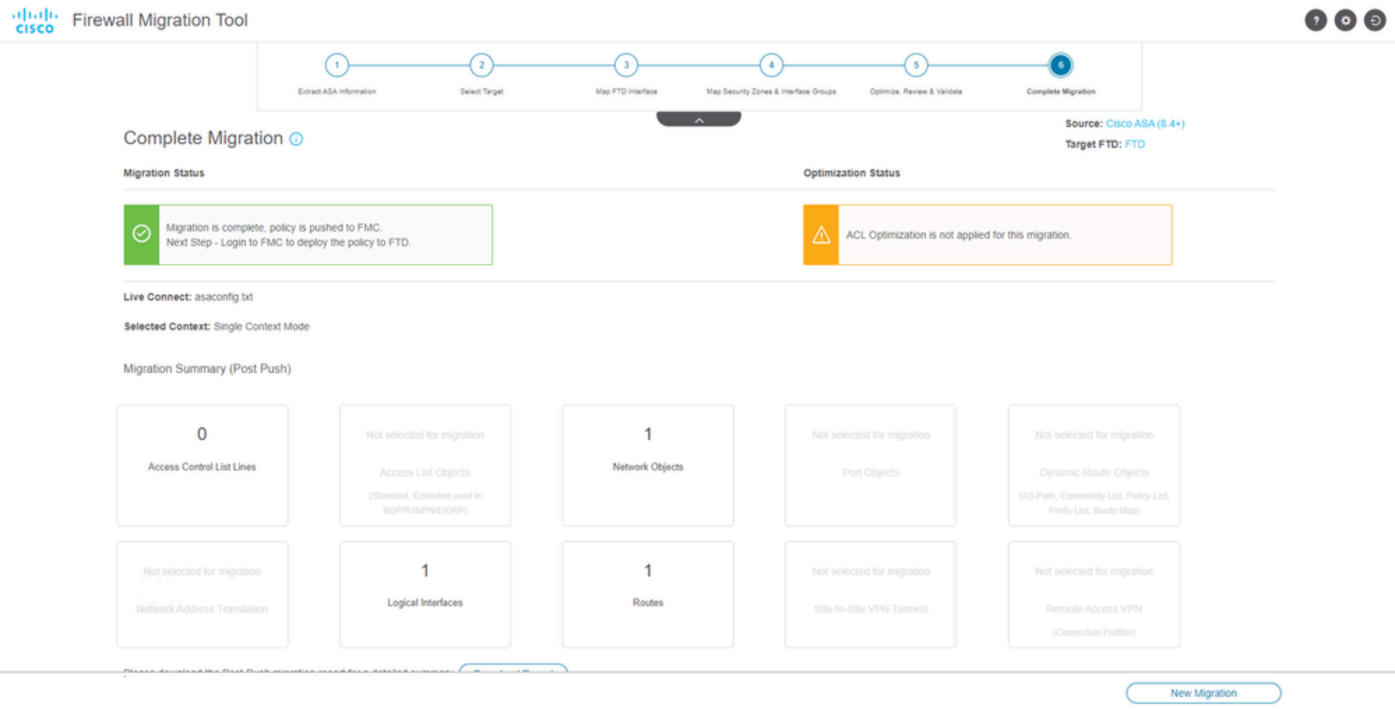
Source: Cisco ASA (8.4+)

Target FTD: FTD

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

Push

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



Source: Cisco ASA (8.4+)

Target FTD: FTD

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

ACL Optimization is not applied for this migration.

Live Connect: asaconfig.txt

Selected Context: Single Context Mode

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)

Successful migration

(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:

1. Log in to the FMC GUI.
2. Navigate to the Deploy tab.
3. Select the deployment to push configuration to the firewall.

4. Click Deploy.

Troubleshoot

Troubleshooting Secure Firewall Migration Tool

- **Common migration failures**:
    - Unknown or invalid characters in the ASA config file.
    - Missing or incomplete configuration elements.
    - Network connectivity issues or latency.
    - Issues during ASA config file upload or pushing config to the management center.
    - Common problems include:
- **Using the Support Bundle for troubleshooting**:
    - On the "Complete Migration" screen, click the **Support** button.
    - Select **Support Bundle** and choose the configuration files to download.
    - **Log and DB files** are selected by default.
    - Click **Download** to get a .zip file.
    - Extract the .zip to view logs, DB, and config files.
    - Click **Email us** to send failure details to the technical team.
    - Attach the support bundle in your email.
    - Click **Visit TAC page** to create a Cisco TAC case for assistance.
    - The tool allows you to download a support bundle for log files, database, and configuration files.
    - Steps to download:
    - For further support: