Configure FTD from ASA Configuration File with Firepower Migration Tool

Contents

Introduction

This document describes an example of Adaptive Security Appliance (ASA) to Firepower Threat Defense (FTD) migration on FPR4145.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of ASA
- Knowledge of Firepower Management Center (FMC) and FTD

Components Used

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

- ASA Version 9.12(2)
- FTD Version 6.7.0
- FMC Version 6.7.0
- Firepower Migration Tool version 2.5.0

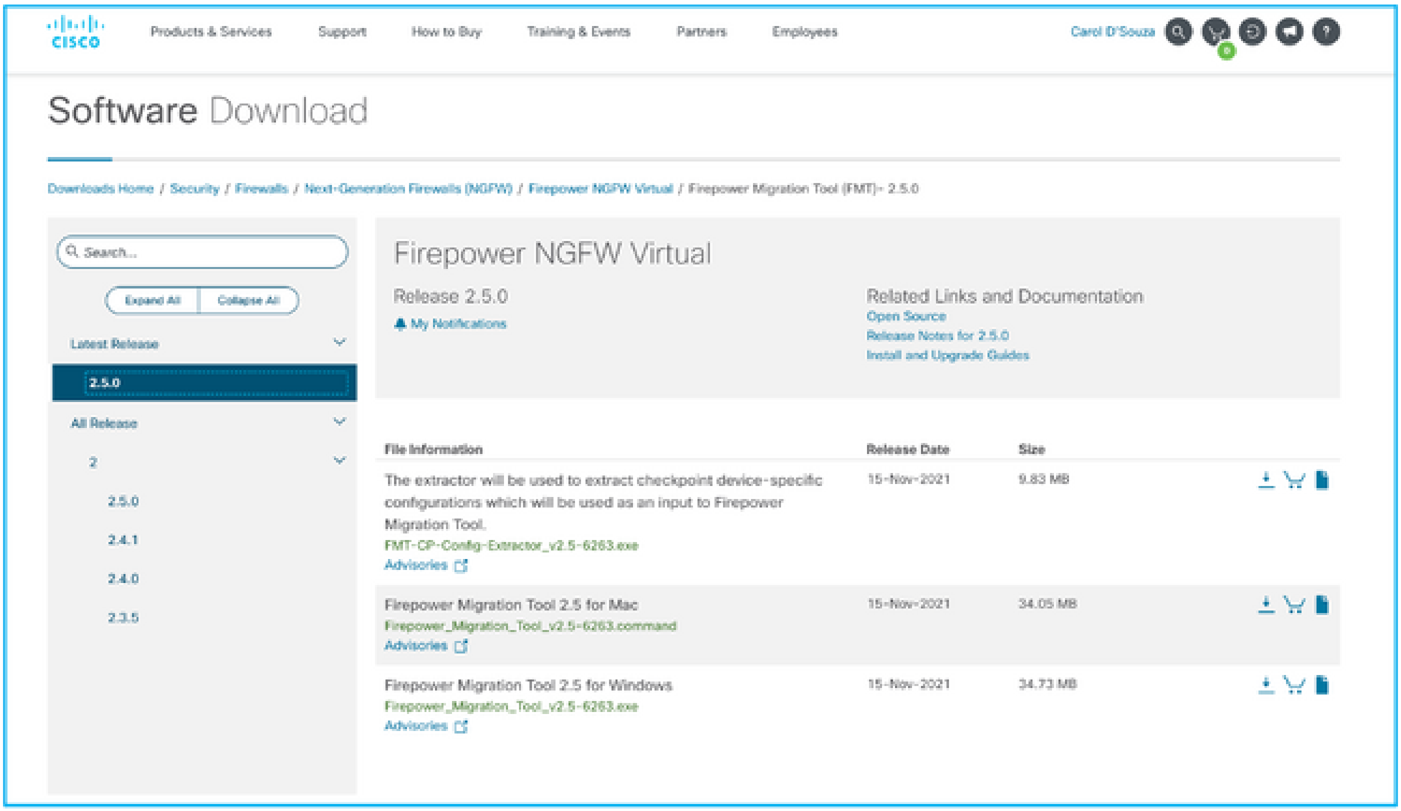
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Export the ASA configuration file in .cfg or .txt format. FMC must be deployed with FTD registered under it.

Configure

1. Download the Firepower Migration Tool from software.cisco.com as shown in the image.



Software Download

Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / Firepower NGFW Virtual / Firepower Migration Tool (FMT)- 2.5.0

Firepower NGFW Virtual

Release 2.5.0

Related Links and Documentation
Open Source
Release Notes for 2.5.0
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_v2.5-6263.exe Advisories	15-Nov-2021	9.83 MB
Firepower Migration Tool 2.5 for Mac Firepower_Migration_Tool_v2.5-6263.command Advisories	15-Nov-2021	34.05 MB
Firepower Migration Tool 2.5 for Windows Firepower_Migration_Tool_v2.5-6263.exe Advisories	15-Nov-2021	34.73 MB

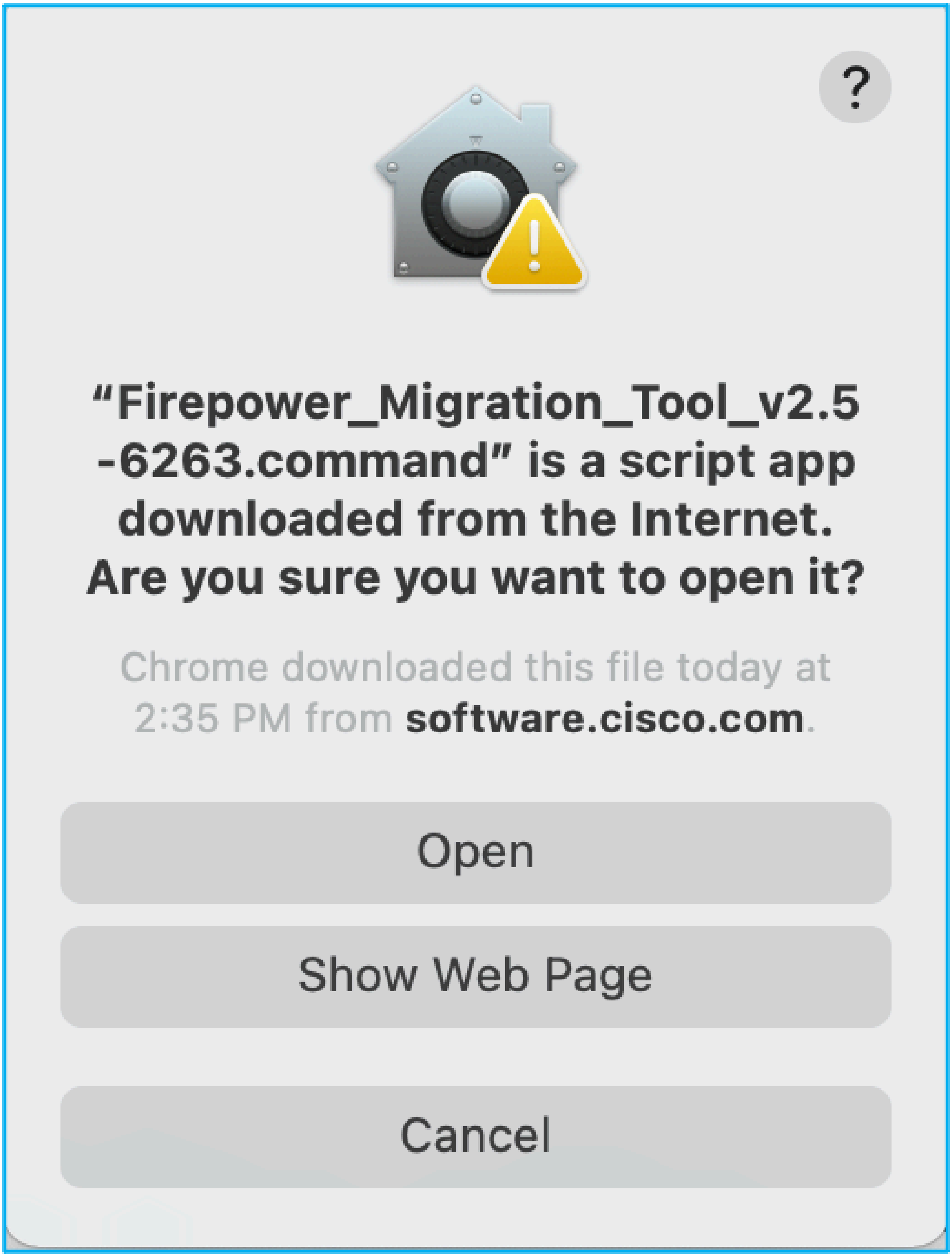
2. Review and verify the requirements for the Firepower Migration Tool section.

3. If you are planning to migrate a large configuration file, configure sleep settings so the system does not go to sleep during a migration push.

3.1. For Windows, navigate to **Power Options** in the **Control Panel**. Click **Change Plan Settings** next to your current power plan and then toggle **Put the computer to sleep** to **Never**. Click **Save Changes**.

3.2. For MAC, navigate to **System Preferences > Energy Saver**. Tick the box next to Prevent the Computer from Sleeping Automatically when the display is off and drag the **Turn Display Off** after slider to **Never**.

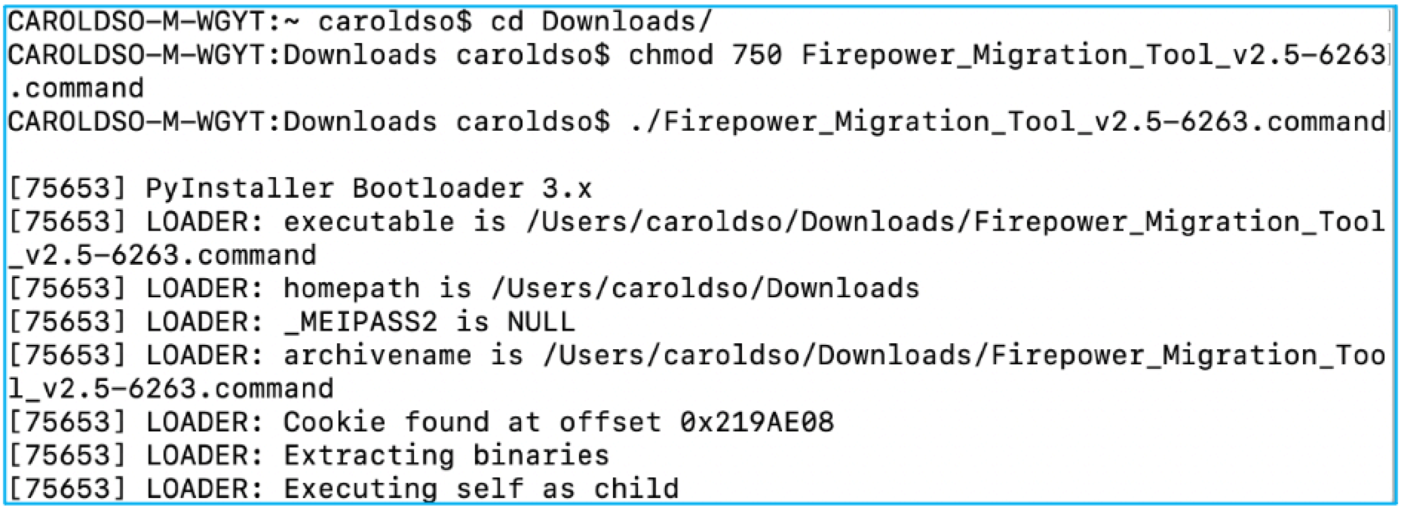
Note: This warning, dialog pops up when MAC users try to open the downloaded file. Ignore this and follow Step 4.1.



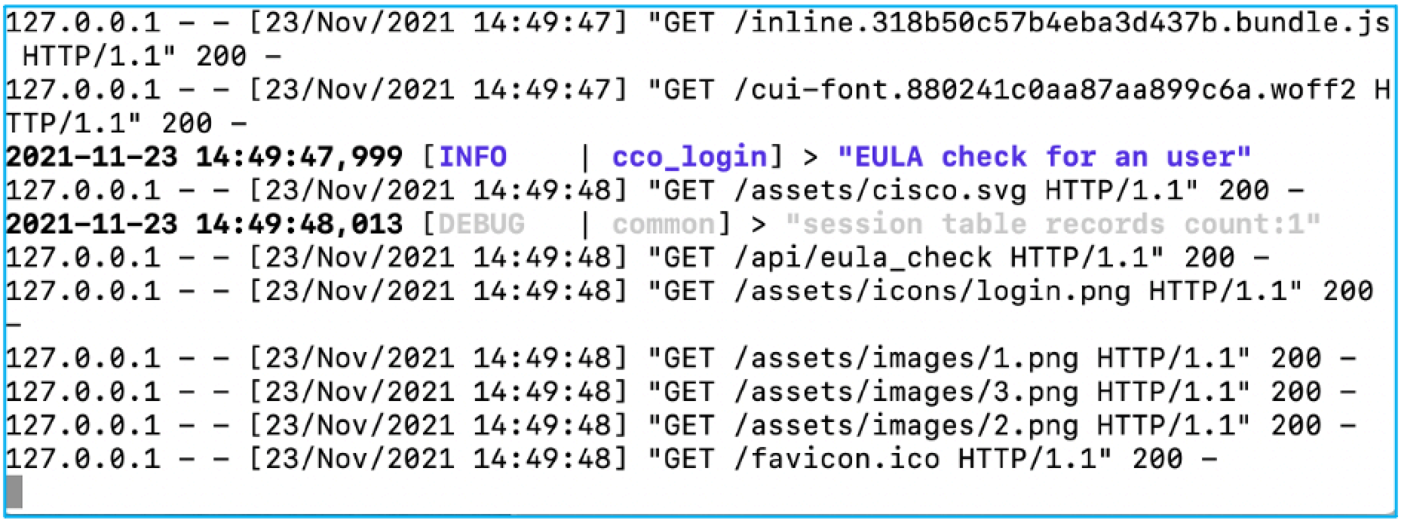
"Firepower_Migration_Tool_v2.5-6263.command" is a script app downloaded from the Internet. Are you sure you want to open it?

Chrome downloaded this file today at 2:35 PM from **software.cisco.com**.

4.1. For MAC - Use the terminal and run these commands:



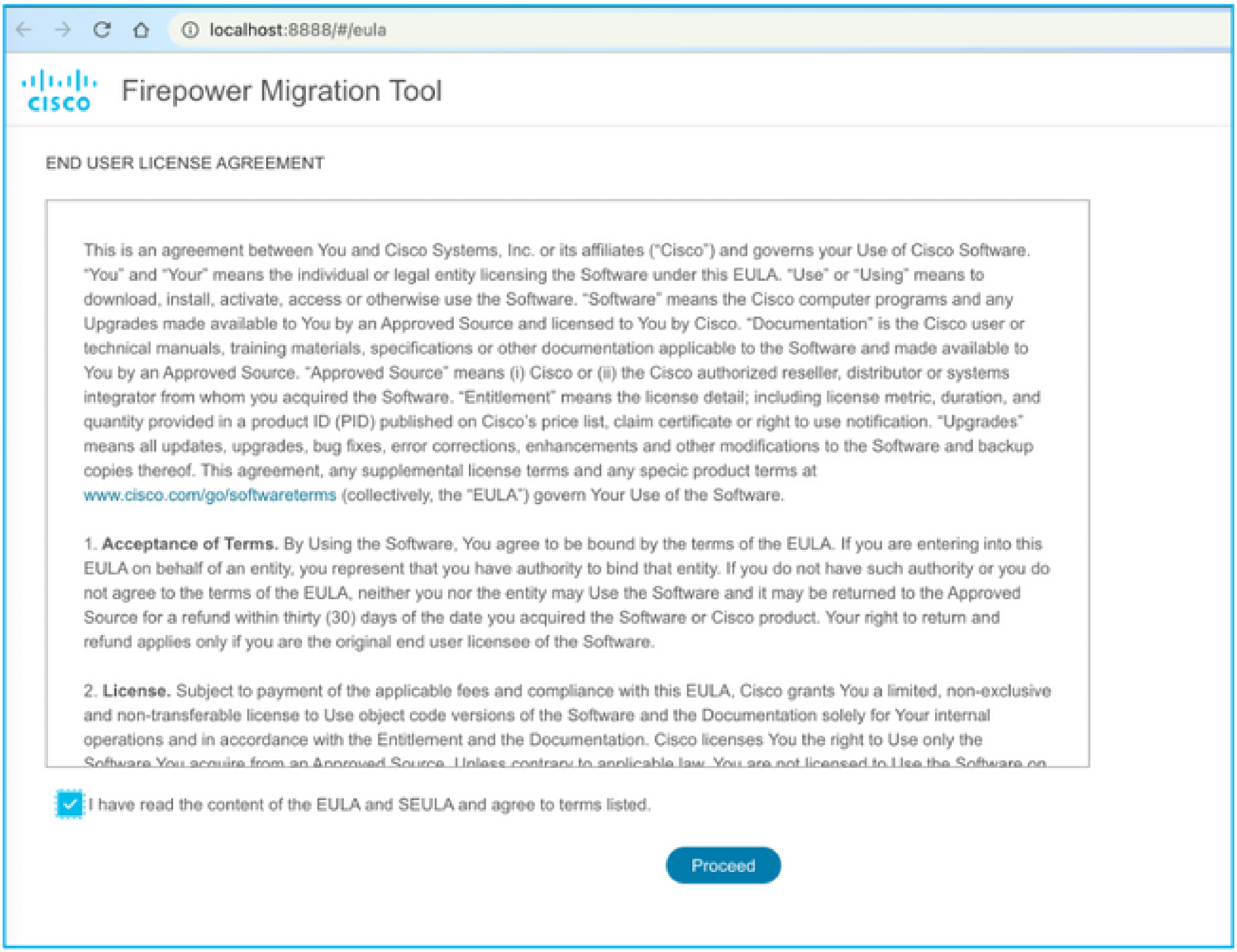
```
CAROLDSO-M-WGYT:~ caroldso$ cd Downloads/
CAROLDSO-M-WGYT:Downloads caroldso$ chmod 750 Firepower_Migration_Tool_v2.5-6263
.command
CAROLDSO-M-WGYT:Downloads caroldso$ ./Firepower_Migration_Tool_v2.5-6263.command

[75653] PyInstaller Bootloader 3.x
[75653] LOADER: executable is /Users/caroldso/Downloads/Firepower_Migration_Tool
_v2.5-6263.command
[75653] LOADER: homepath is /Users/caroldso/Downloads
[75653] LOADER: _MEIPASS2 is NULL
[75653] LOADER: archivename is /Users/caroldso/Downloads/Firepower_Migration_Too
l_v2.5-6263.command
[75653] LOADER: Cookie found at offset 0x219AE08
[75653] LOADER: Extracting binaries
[75653] LOADER: Executing self as child
```



```
127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /inline.318b50c57b4eba3d437b.bundle.js
 HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /cui-font.880241c0aa87aa899c6a.woff2 H
TTP/1.1" 200 -
2021-11-23 14:49:47,999 [INFO    | cco_login] > "EULA check for an user"
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/cisco.svg HTTP/1.1" 200 -
2021-11-23 14:49:48,013 [DEBUG   | common] > "session table records count:1"
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /api/eula_check HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/icons/login.png HTTP/1.1" 200
-
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/1.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/2.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /favicon.ico HTTP/1.1" 200 -
```

4.2. For Windows - double-click the Firepower Migration Tool in order to launch it in a Google Chrome browser.

5. Accept the license as shown in the image:



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.

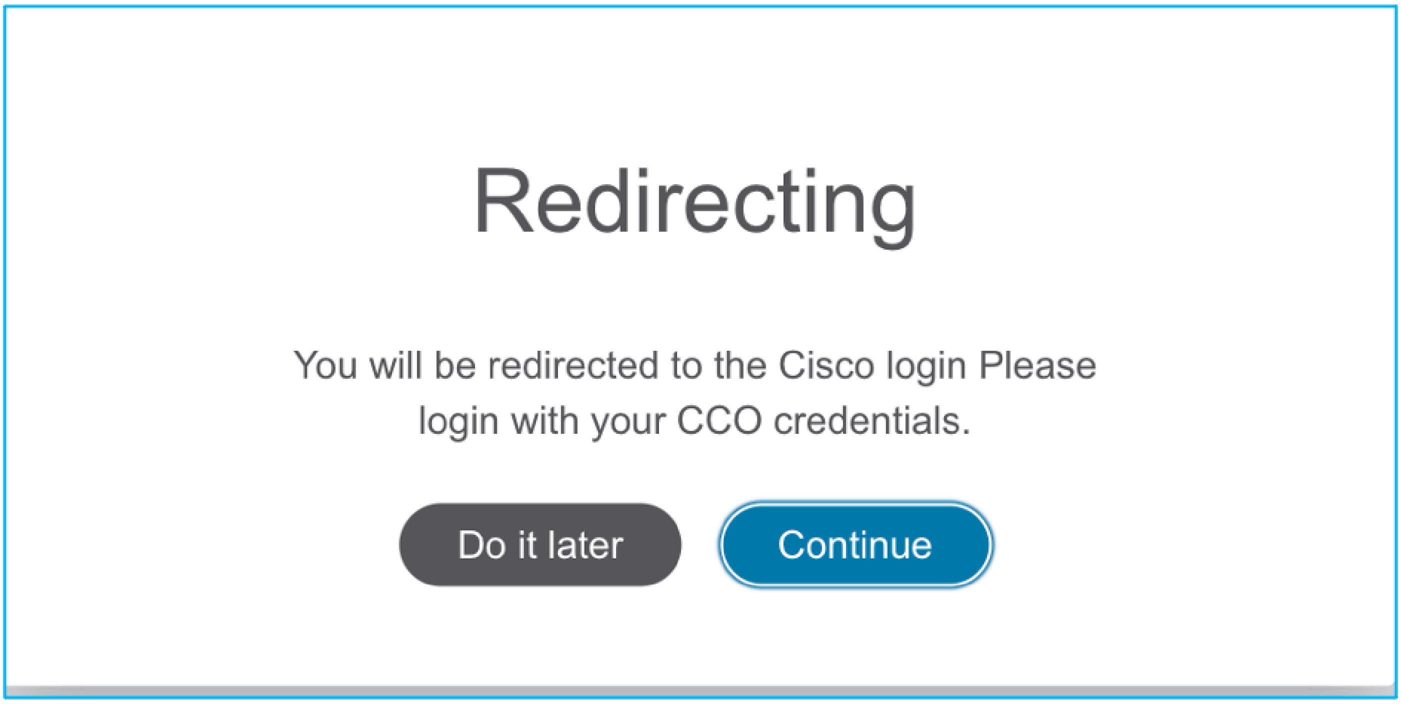
1. **Acceptance of Terms.** By Using the Software, You agree to be bound by the terms of the EULA. If you are entering into this EULA on behalf of an entity, you represent that you have authority to bind that entity. If you do not have such authority or you do not agree to the terms of the EULA, neither 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 Software on

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

6. On the login page of the Firepower Migration Tool, click the login with Cisco Connection Online (CCO) link in order to log in to your **Cisco.com** account with your single-sign-on credentials.

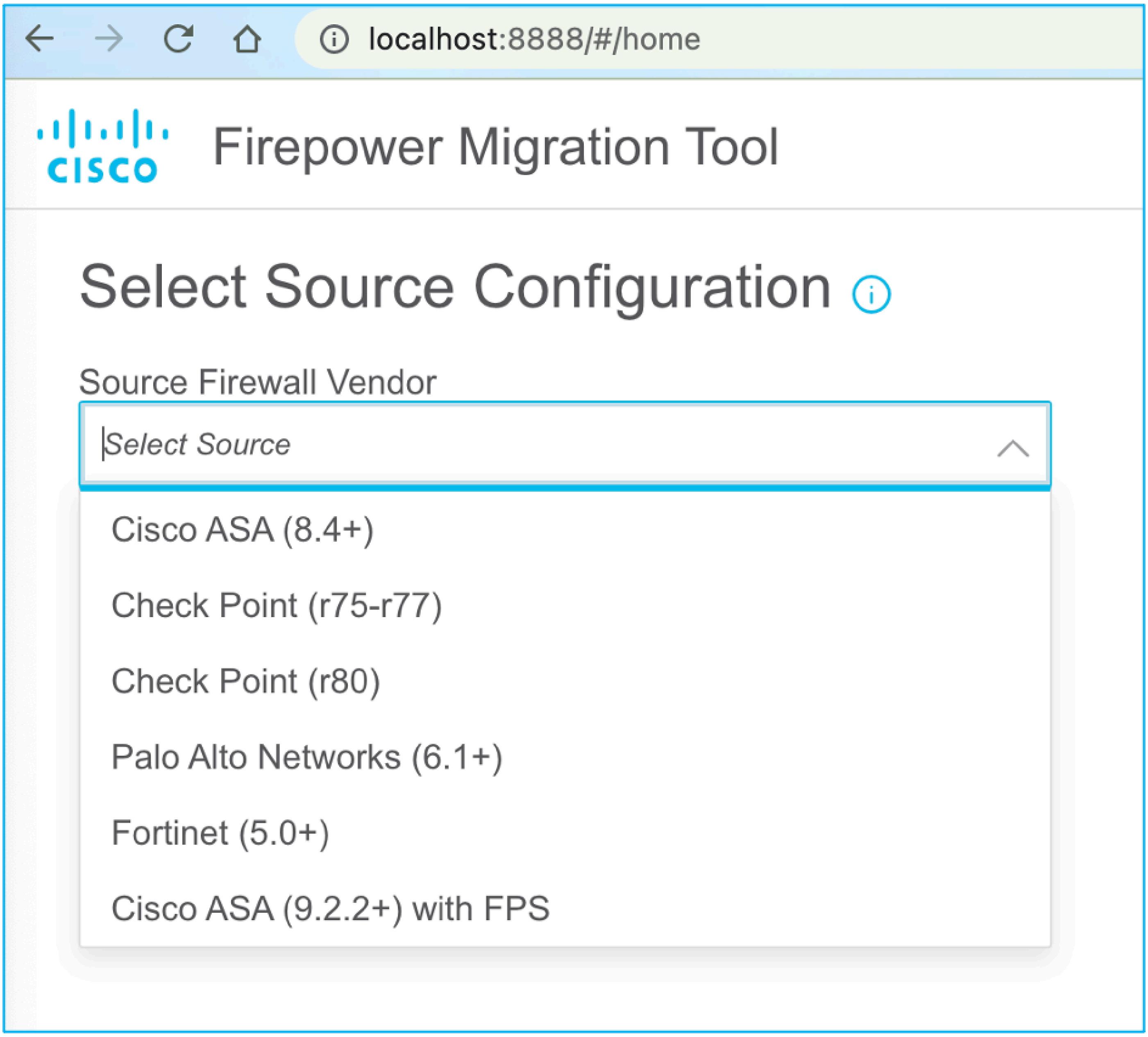
Note: If you do not have a **Cisco.com** account, create it on the **Cisco.com** login page. Log in with these default credentials: Username—admin and Password—Admin123.



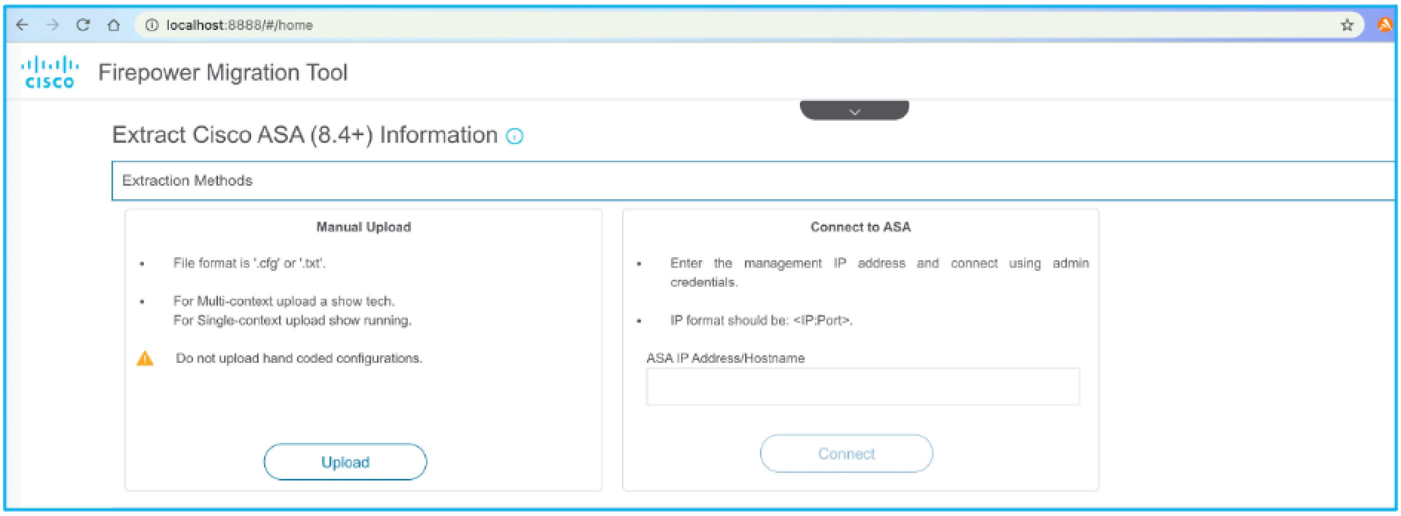
Redirecting

You will be redirected to the Cisco login Please login with your CCO credentials.

7. Choose the source configuration. In this scenario, it is Cisco ASA (8.4+).



8. Choose **Manual Upload** if you do not have connectivity to the ASA. Otherwise, you can retrieve the running configuration from the ASA and enter the management IP and login details. In this scenario, a manual upload was performed.



Manual Upload

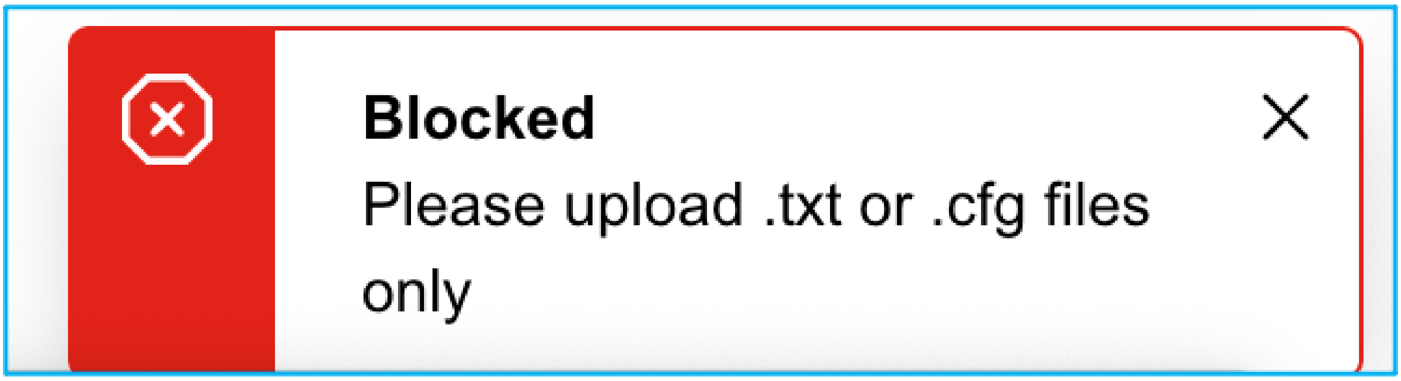
- File format is '.cfg' or '.txt'.
- For Multi-context upload a show tech.
  For Single-context upload show running.

⚠ Do not upload hand coded configurations.

Connect to ASA

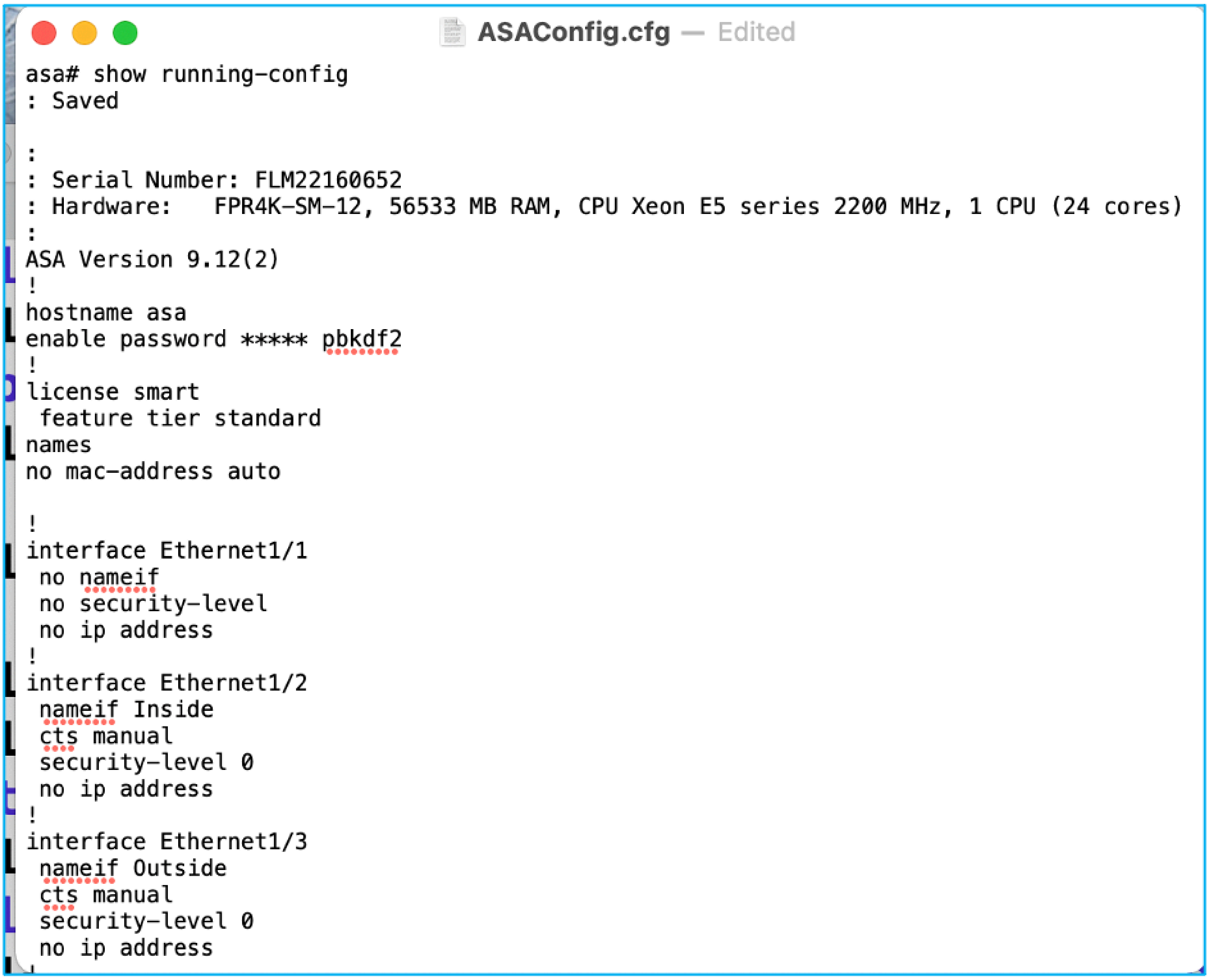
- Enter the management IP address and connect using admin credentials.
- IP format should be: <IP:Port>.

Note: This error is seen if the file is not supported. Ensure to change the format to plain text. (Error is seen despite having extension .cfg.)



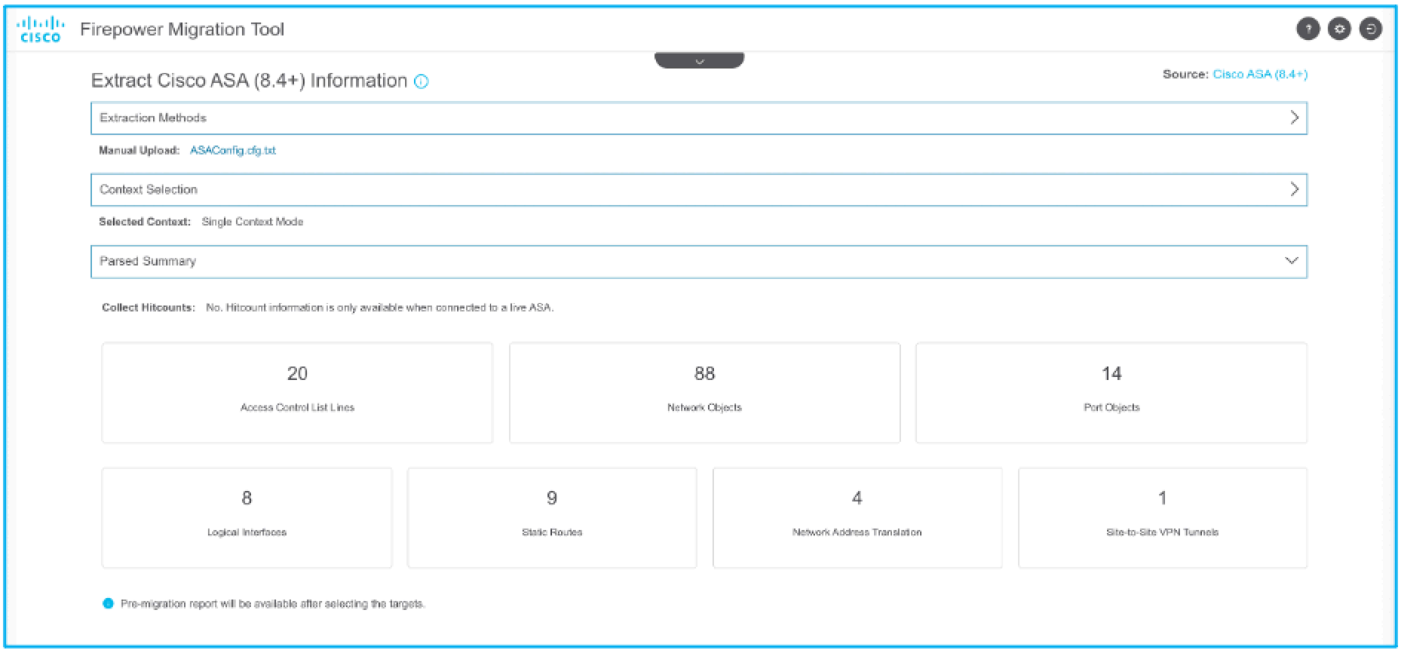
Blocked

Please upload .txt or .cfg files only



```
asa# show running-config
: Saved

:
: Serial Number: FLM22160652
: Hardware:   FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
:
ASA Version 9.12(2)
!
hostname asa
enable password ***** pbkdf2
!
license smart
 feature tier standard
names
no mac-address auto

!
interface Ethernet1/1
 no nameif
 no security-level
 no ip address
!
interface Ethernet1/2
 nameif Inside
 cts manual
 security-level 0
 no ip address
!
interface Ethernet1/3
 nameif Outside
 cts manual
 security-level 0
 no ip address
```

9. After the file is uploaded, the elements are parsed providing a summary as shown in the image:


Firepower Migration Tool

Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

Extraction Methods

Manual Upload: ASAConfig.cfg.txt

Context Selection

Selected Context: Single Context Mode

Parsed Summary

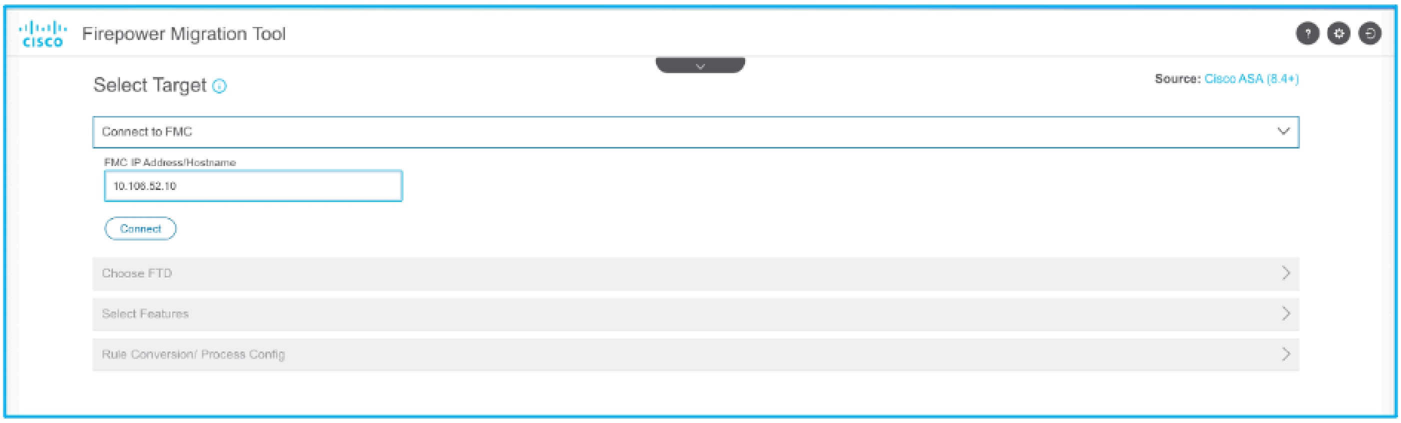
Collect Hitcounts: No. Hitcount information is only available when connected to a live ASA.

20 Access Control List Lines	88 Network Objects	14 Port Objects

8 Logical Interfaces	9 Static Routes	4 Network Address Translation	1 Site-to-Site VPN Tunnels

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

10. Enter the FMC IP and login credentials to which the ASA configuration is to be migrated. Ensure that the FMC IP is reachable from your workstation.

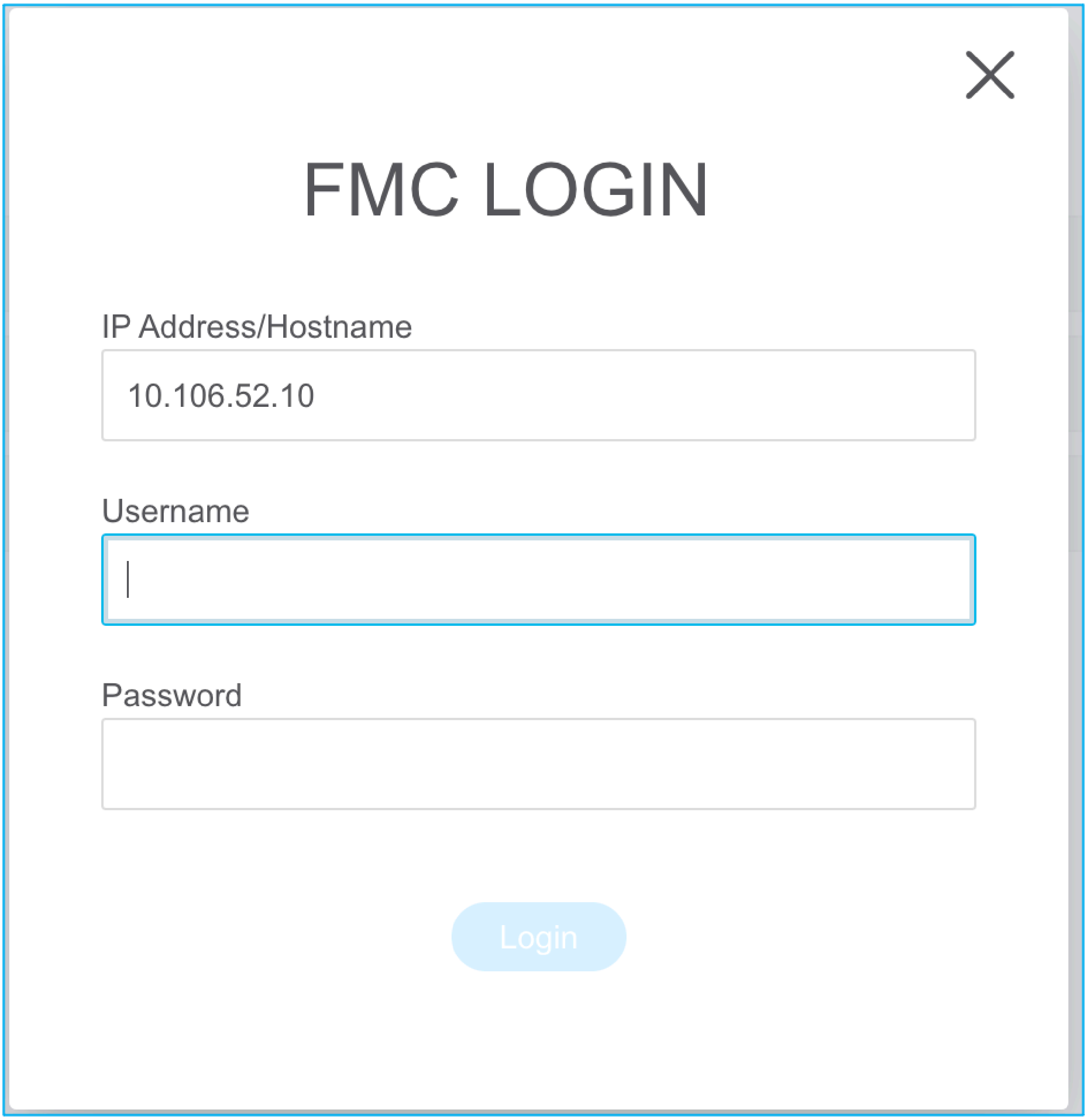

Firepower Migration Tool

Select Target

Source: Cisco ASA (8.4+)

Connect to FMC

FMC IP Address/Hostname: 10.106.52.10



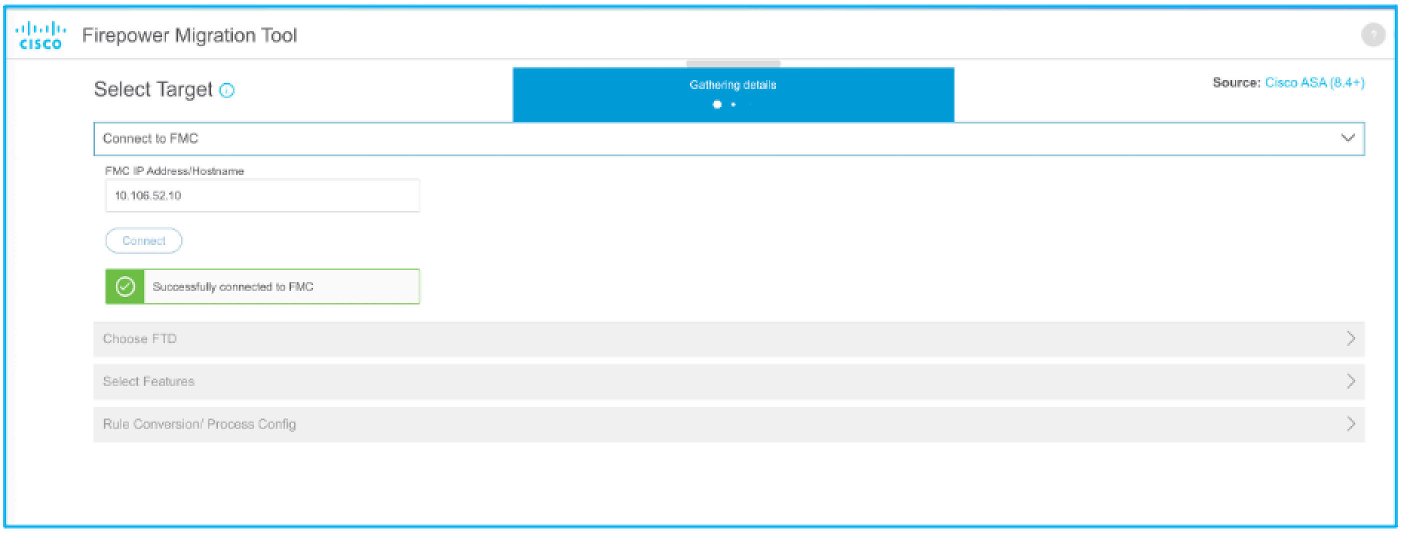
FMC LOGIN

IP Address/Hostname: 10.106.52.10

Username

Password

11. Once the FMC is connected, the managed FTDs under it are displayed.



Select Target

Source: Cisco ASA (8.4+)

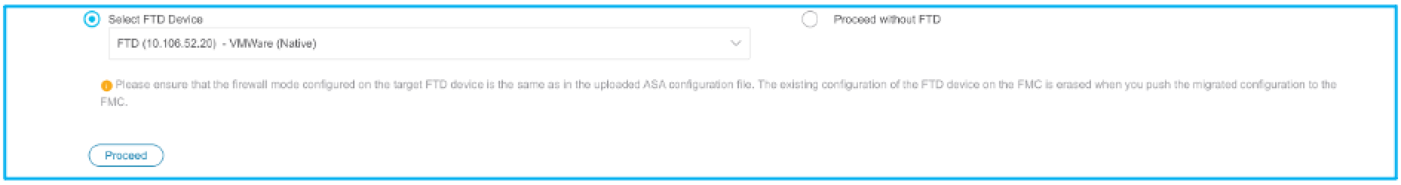
Connect to FMC

FMC IP Address/Hostname: 10.106.52.10

Connect

Successfully connected to FMC

12. Choose the FTD to which you want to perform the migration of the ASA configuration.

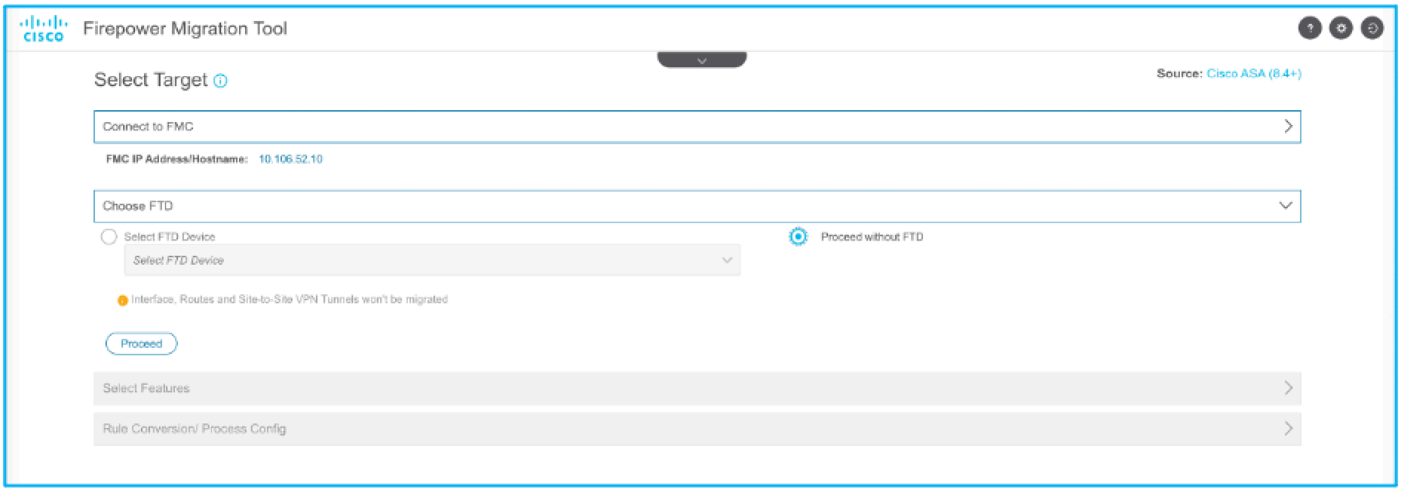


● Select FTD Device: FTD (10.106.52.20) - VMWare (Native)

○ Proceed without FTD

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.

Note: It is recommended to choose the FTD device, else interfaces, routes, and site-to-site VPN configuration must be done manually.



Select Target

Source: Cisco ASA (8.4+)

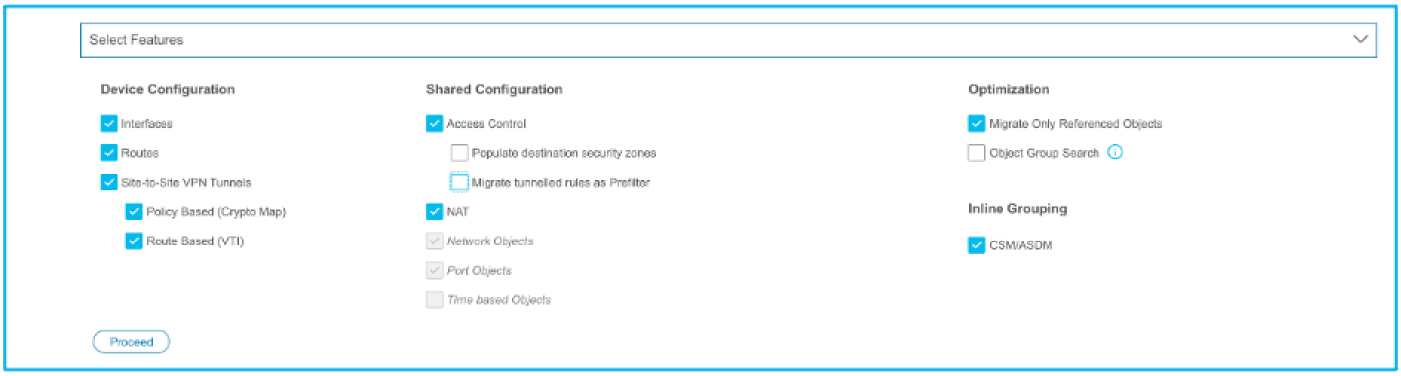
FMC IP Address/Hostname: 10.106.52.10

○ Select FTD Device: Select FTD Device

● Proceed without FTD

Interface, Routes and Site-to-Site VPN Tunnels won't be migrated

13. Choose the features required to be migrated as shown in the image:



Device Configuration

☑ Interfaces
☑ Routes
☑ Site-to-Site VPN Tunnels
☑ Policy Based (Crypto Map)
☑ Route Based (VTI)

Shared Configuration

☑ Access Control
□ Populate destination security zones
□ Migrate tunnelled rules as Prefilter
☑ NAT
☑ *Network Objects*
☑ *Port Objects*
□ *Time based Objects*

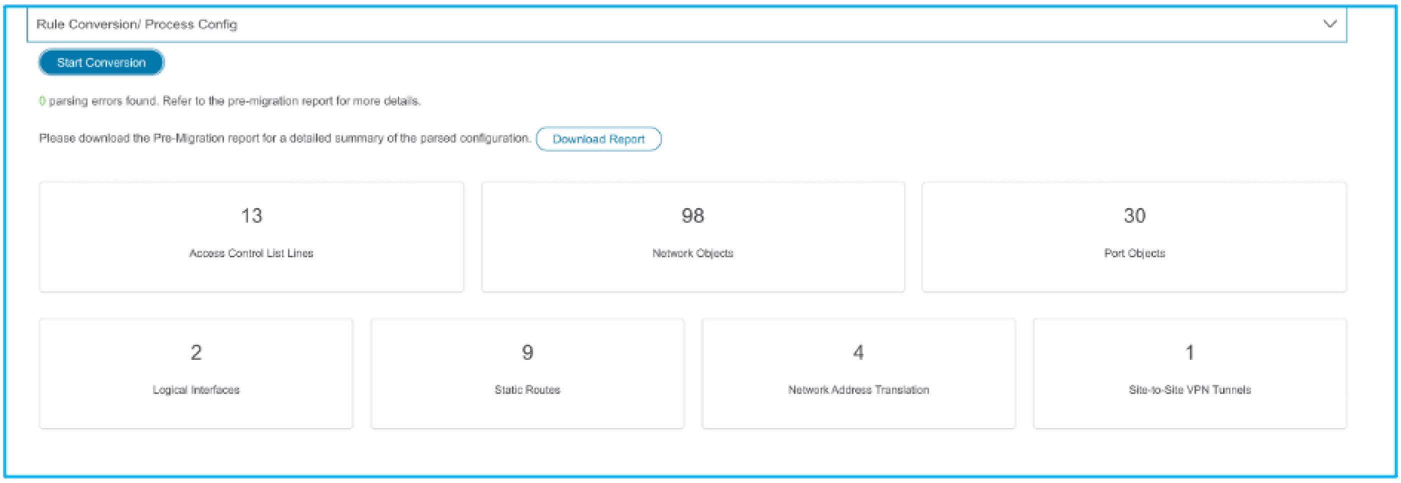
Optimization

☑ Migrate Only Referenced Objects
□ Object Group Search

Inline Grouping

☑ CSM/ASDM

14. Choose **Start Conversion** in order to initiate the pre-migration which populates the elements pertaining to FTD configuration.



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.

13 Access Control List Lines

98 Network Objects

30 Port Objects

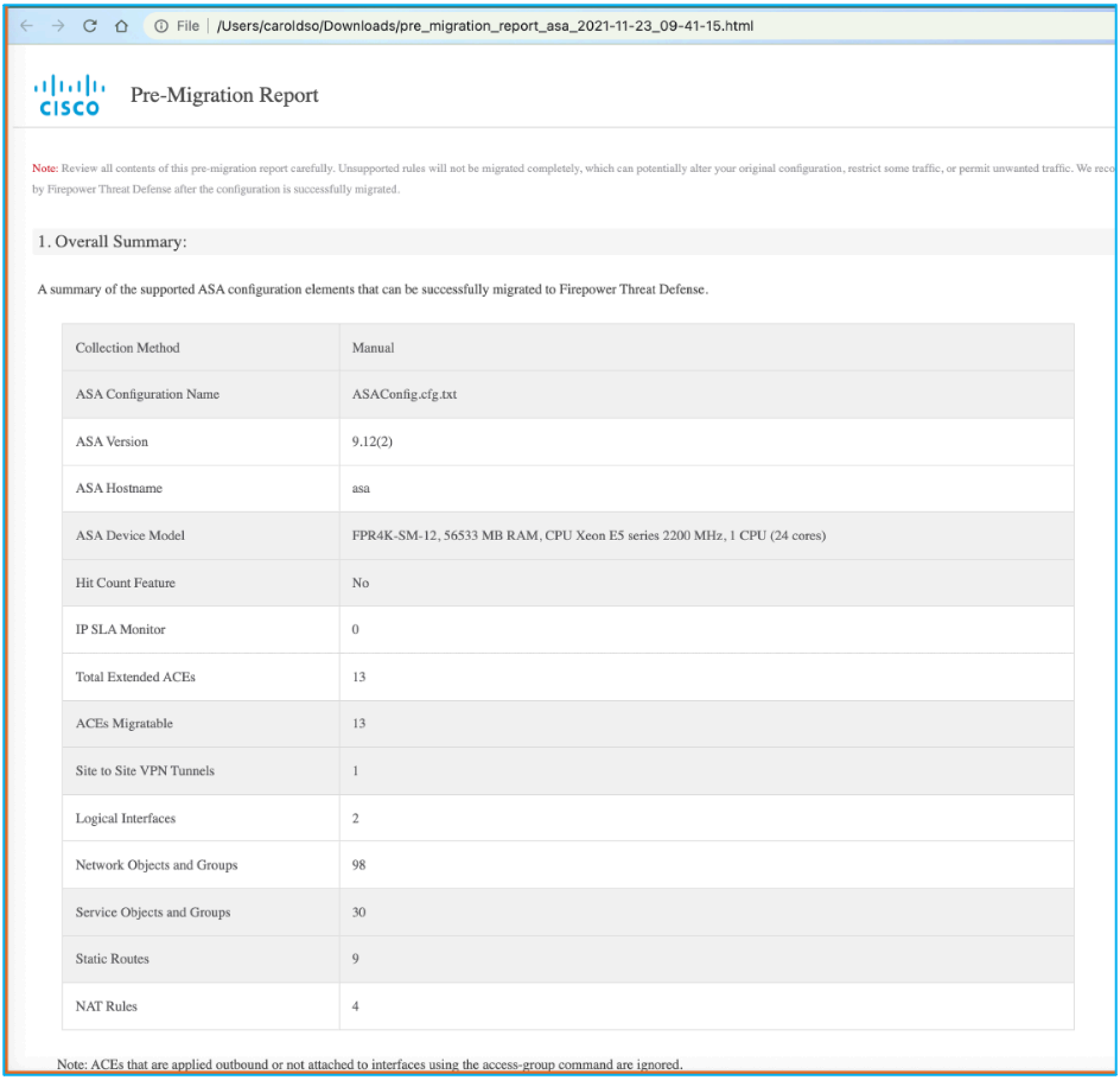
2 Logical Interfaces

9 Static Routes

4 Network Address Translation

1 Site-to-Site VPN Tunnels

15. Click **Download Report** seen previously in order to view the Pre-Migration Report which is as shown in the image:



File | /Users/caroldso/Downloads/pre_migration_report_asa_2021-11-23_09-41-15.html

Pre-Migration Report

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 reco by Firepower Threat Defense after the configuration is successfully migrated.

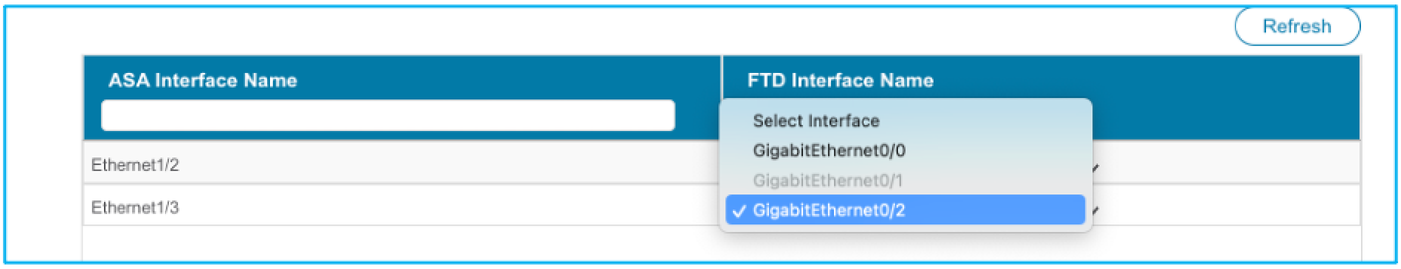
1. Overall Summary:

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

Collection Method	Manual
ASA Configuration Name	ASAConfig.cfg.txt
ASA Version	9.12(2)
ASA Hostname	asa
ASA Device Model	FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
Hit Count Feature	No
IP SLA Monitor	0
Total Extended ACEs	13
ACEs Migratable	13
Site to Site VPN Tunnels	1
Logical Interfaces	2
Network Objects and Groups	98
Service Objects and Groups	30
Static Routes	9
NAT Rules	4

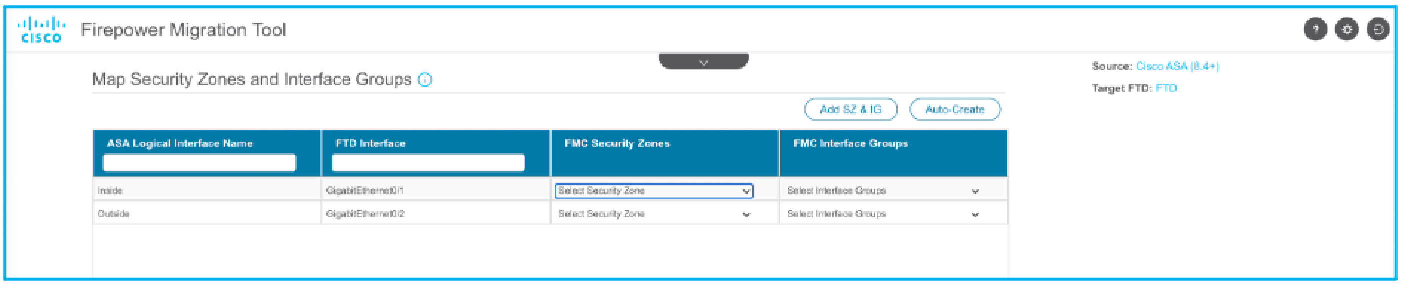
Note: ACEs that are applied outbound or not attached to interfaces using the access-group command are ignored.

16. Map ASA interfaces to FTD interfaces as required as shown in the image:



ASA Interface Name	FTD Interface Name
Ethernet1/2	
Ethernet1/3	GigabitEthernet0/2

17. Assign security zones and interface groups to the FTD interfaces.



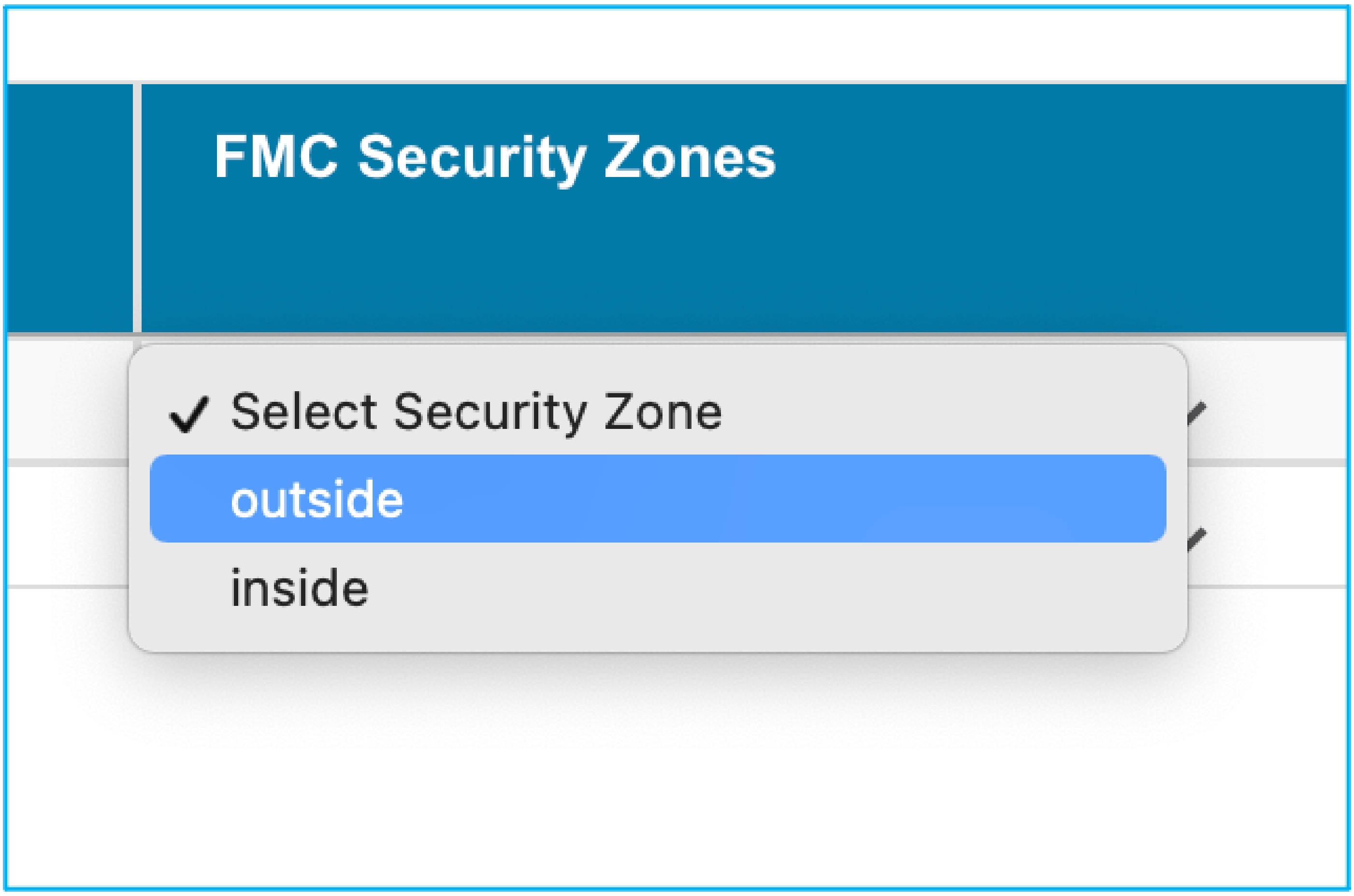
Map Security Zones and Interface Groups

Source: Cisco ASA (8.4+)

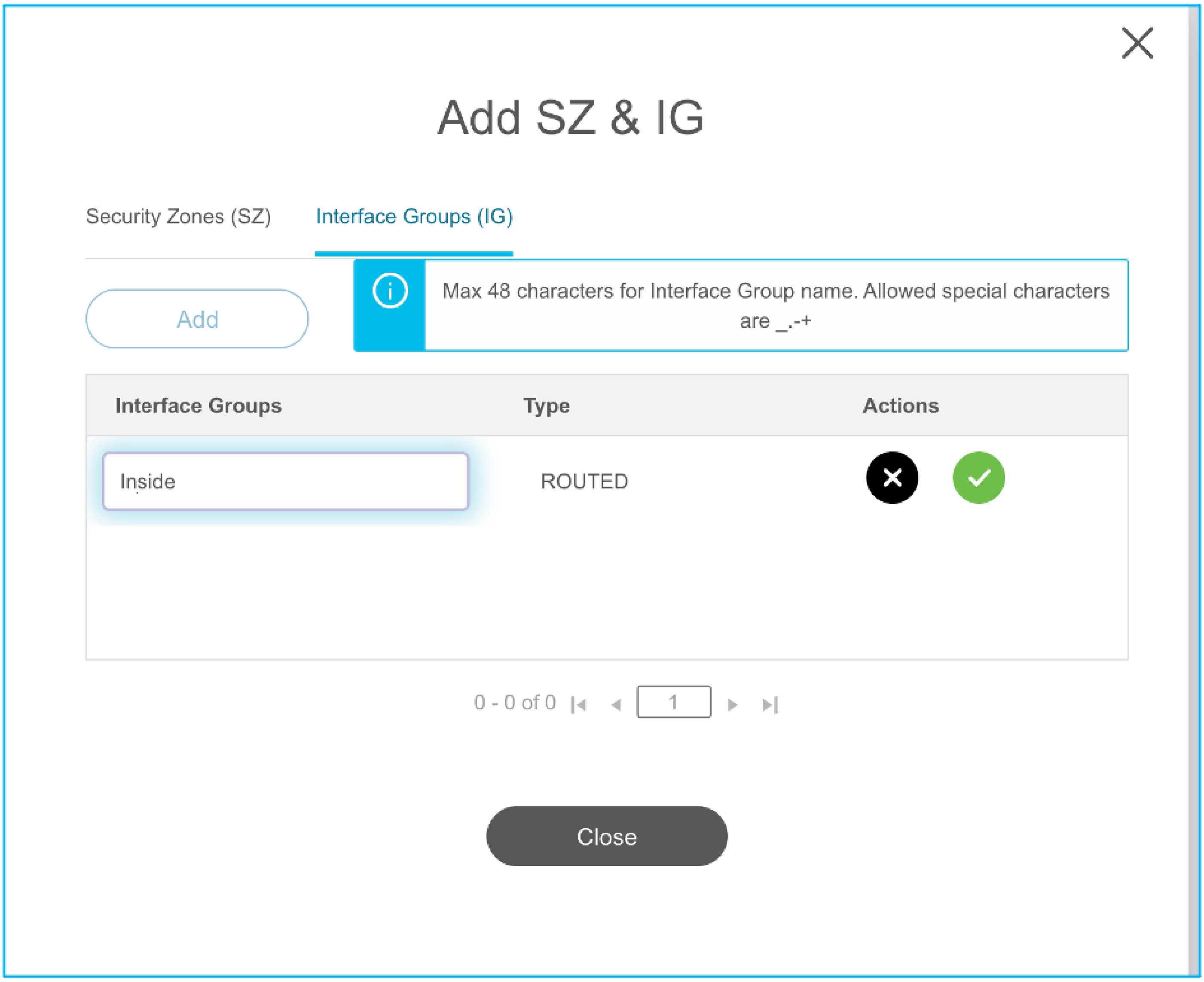
Target FTD: FTD

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
Inside	GigabitEthernet0/1	Select Security Zone	Select Interface Groups
Outside	GigabitEthernet0/2	Select Security Zone	Select Interface Groups

17.1. If the FMC has security zones and interface groups already created, you can choose them as needed:



17.2. If there is a need to create security zones and an Interface group, click **Add SZ & IG** as shown in the image:

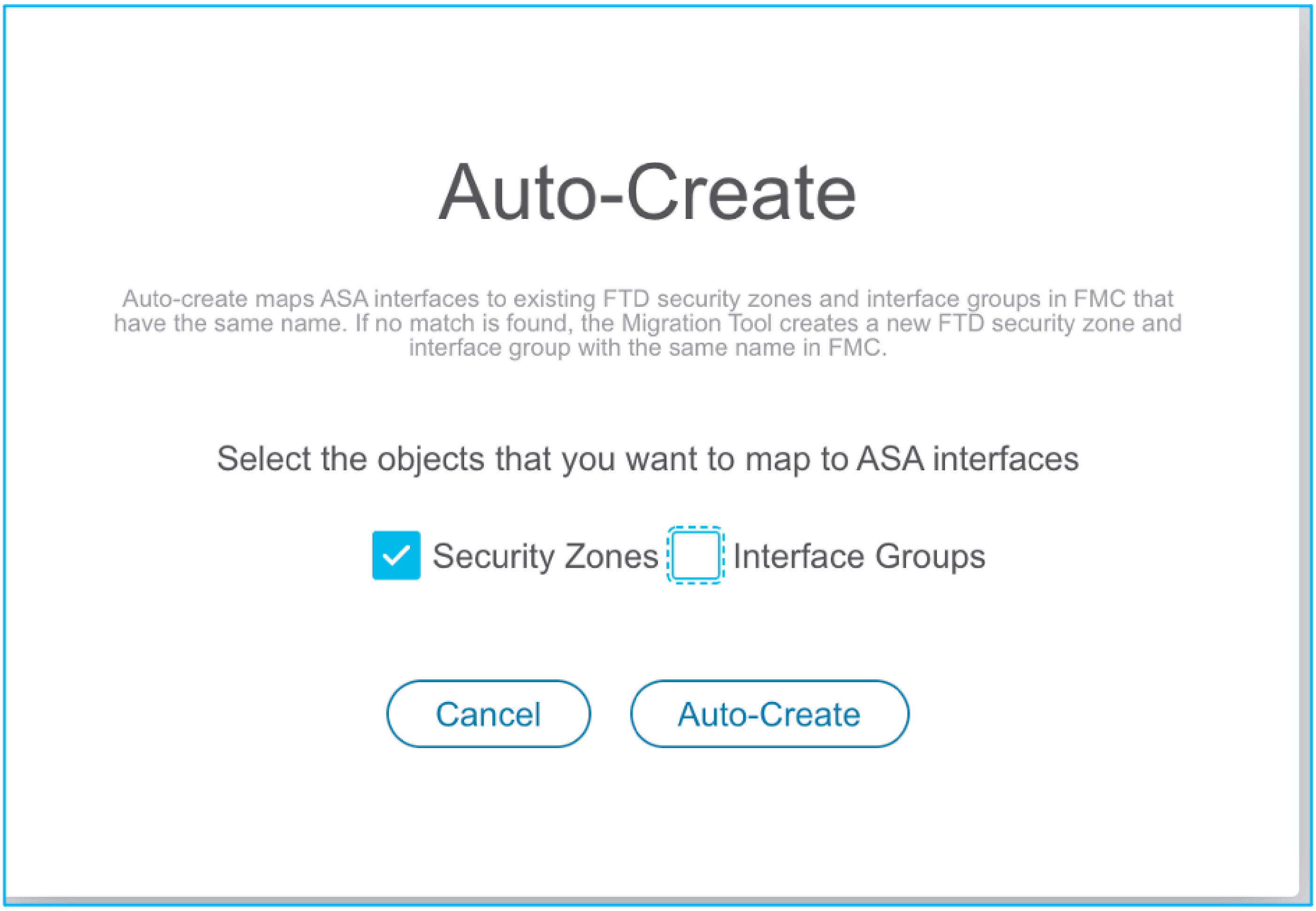


Max 48 characters for Interface Group name. Allowed special characters are _.-+

Interface Groups	Type	Actions
Inside	ROUTED	✕ ✓

0 - 0 of 0 1

17.3. Otherwise, you can proceed with the option **Auto-Create** which creates security zones and interface groups with the name **ASA logical interface_sz** and **ASA logical interface_ig** respectively.

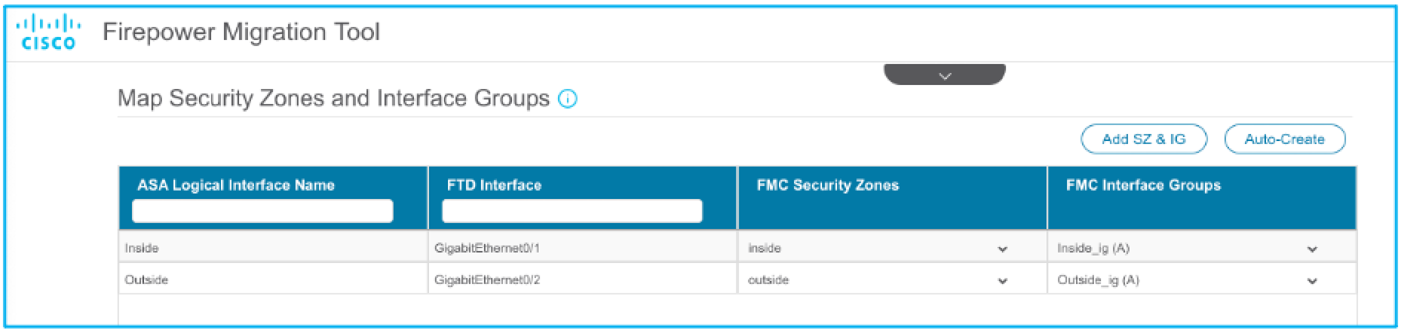


Auto-Create

Auto-create maps ASA interfaces to existing FTD security zones and interface groups in FMC that have the same name. If no match is found, the Migration Tool creates a new FTD security zone and interface group with the same name in FMC.

Select the objects that you want to map to ASA interfaces

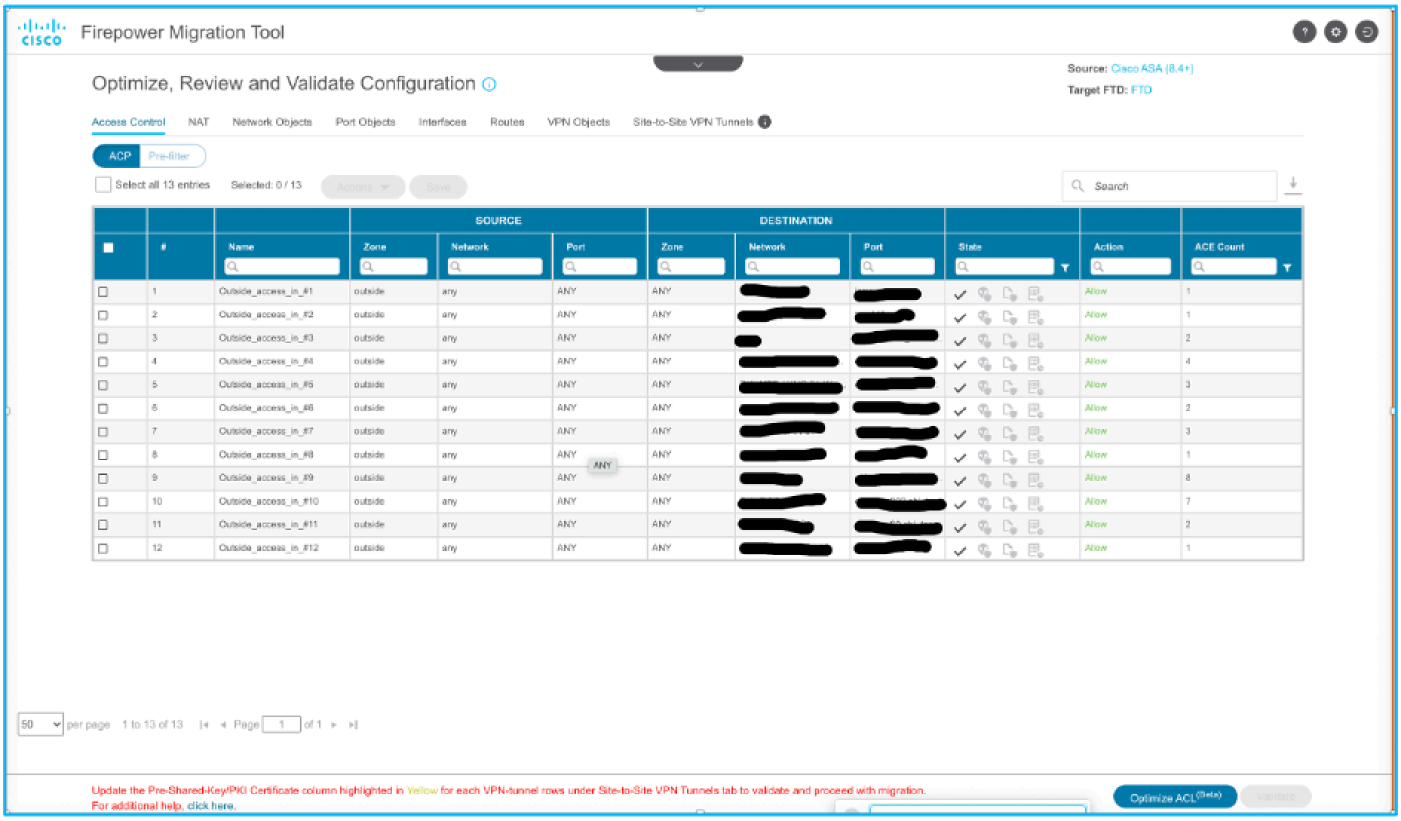
☑ Security Zones □ Interface Groups



Map Security Zones and Interface Groups

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
Inside	GigabitEthernet0/1	inside	Inside_ig (A)
Outside	GigabitEthernet0/2	outside	Outside_ig (A)

18. Review and validate each of the FTD elements created. Alerts are seen in red as shown in the image:



Optimize, Review and Validate Configuration

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

□ Select all 13 entries   Selected: 0 / 13

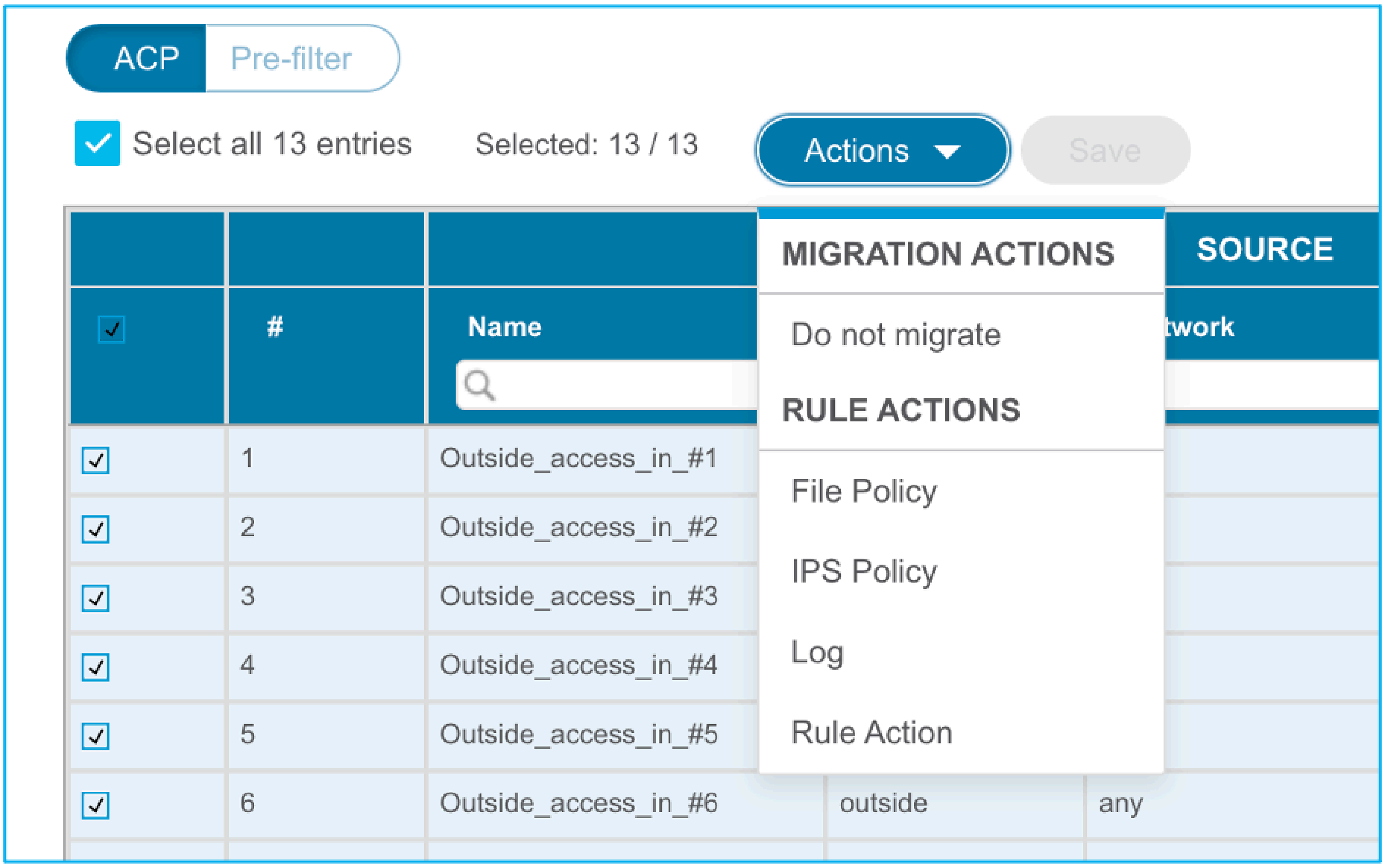
			SOURCE			DESTINATION					
□	#	Name	Zone	Network	Port	Zone	Network	Port	State	Action	ACE Count
□	1	Outside_access_in_#1	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	1
□	2	Outside_access_in_#2	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	1
□	3	Outside_access_in_#3	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	2
□	4	Outside_access_in_#4	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	4
□	5	Outside_access_in_#5	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	3
□	6	Outside_access_in_#6	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	2
□	7	Outside_access_in_#7	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	3
□	8	Outside_access_in_#8	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	1
□	9	Outside_access_in_#9	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	8
□	10	Outside_access_in_#10	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	7
□	11	Outside_access_in_#11	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	2
□	12	Outside_access_in_#12	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	1

ANY

50 per page 1 to 13 of 13 Page 1 of 1

Update the Pre-Shared-Key/PKI Certificate column highlighted in Yellow for each VPN-tunnel rows under Site-to-Site VPN Tunnels tab to validate and proceed with migration.
For additional help, click here.

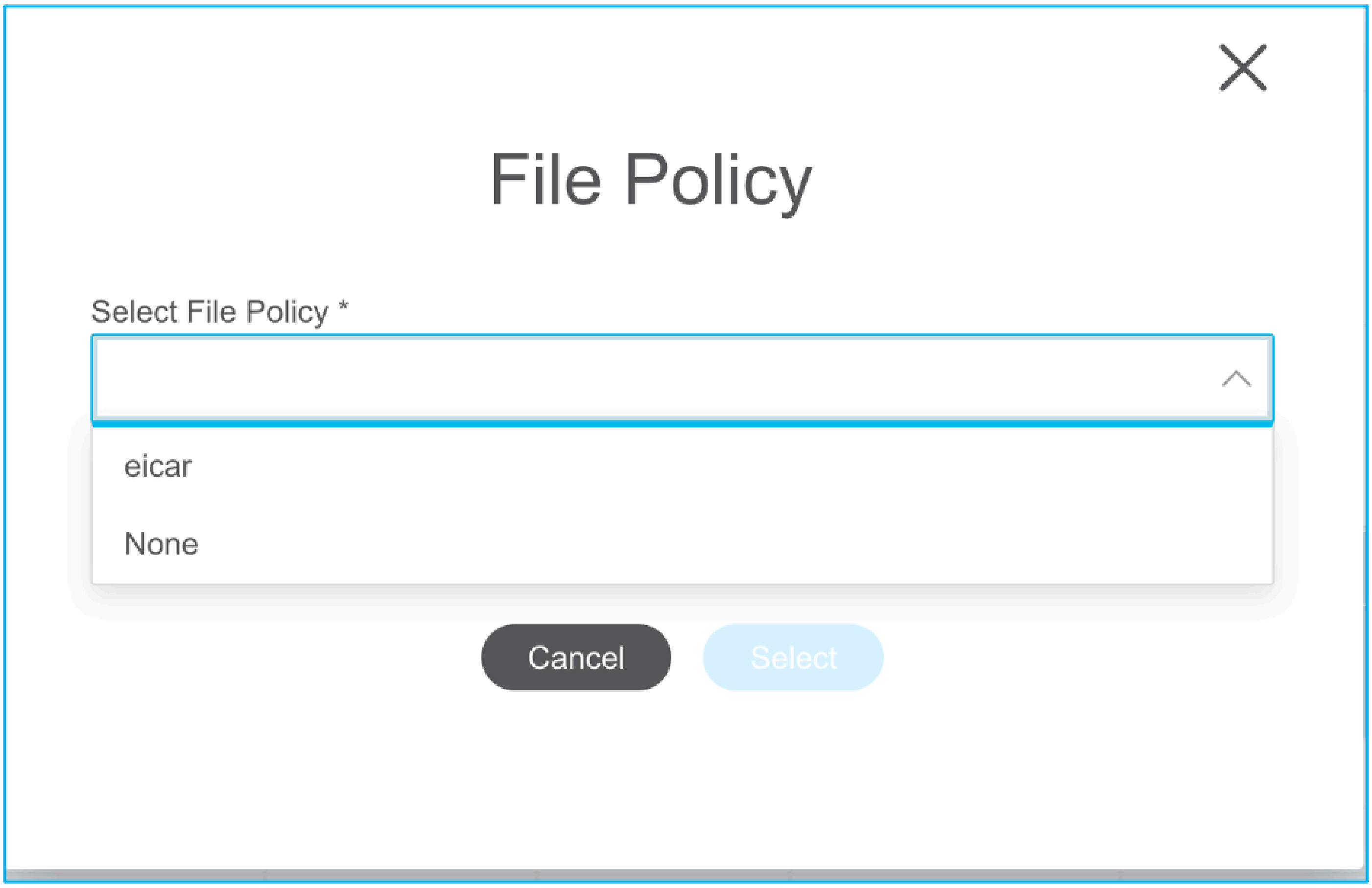
19. The migration actions can be chosen as shown in the image if you want to edit any rule. FTD features of adding files and IPS policy can be done at this step.



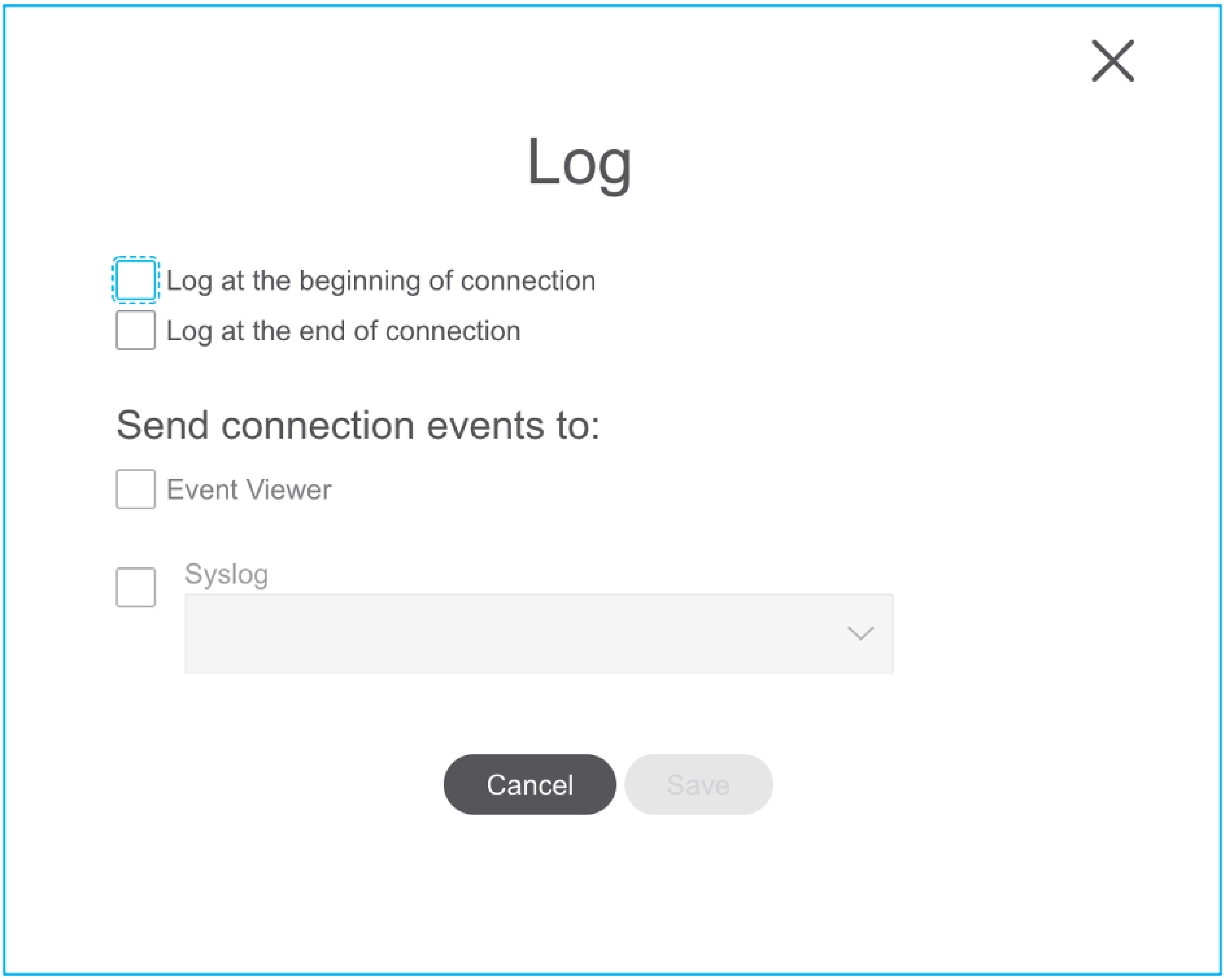
☑ Select all 13 entries   Selected: 13 / 13

			SOURCE	
☑	#	Name		twork
☑	1	Outside_access_in_#1		
☑	2	Outside_access_in_#2		
☑	3	Outside_access_in_#3		
☑	4	Outside_access_in_#4		
☑	5	Outside_access_in_#5		
☑	6	Outside_access_in_#6	outside	any

Note: If File Policies already exist in the FMC, they are populated as shown in the image. The same holds true for IPS policies along with the default policies.



Log configuration can be done for the required rules. Syslog server configuration existing on the FMC can be chosen at this stage.



Log

□ Log at the beginning of connection

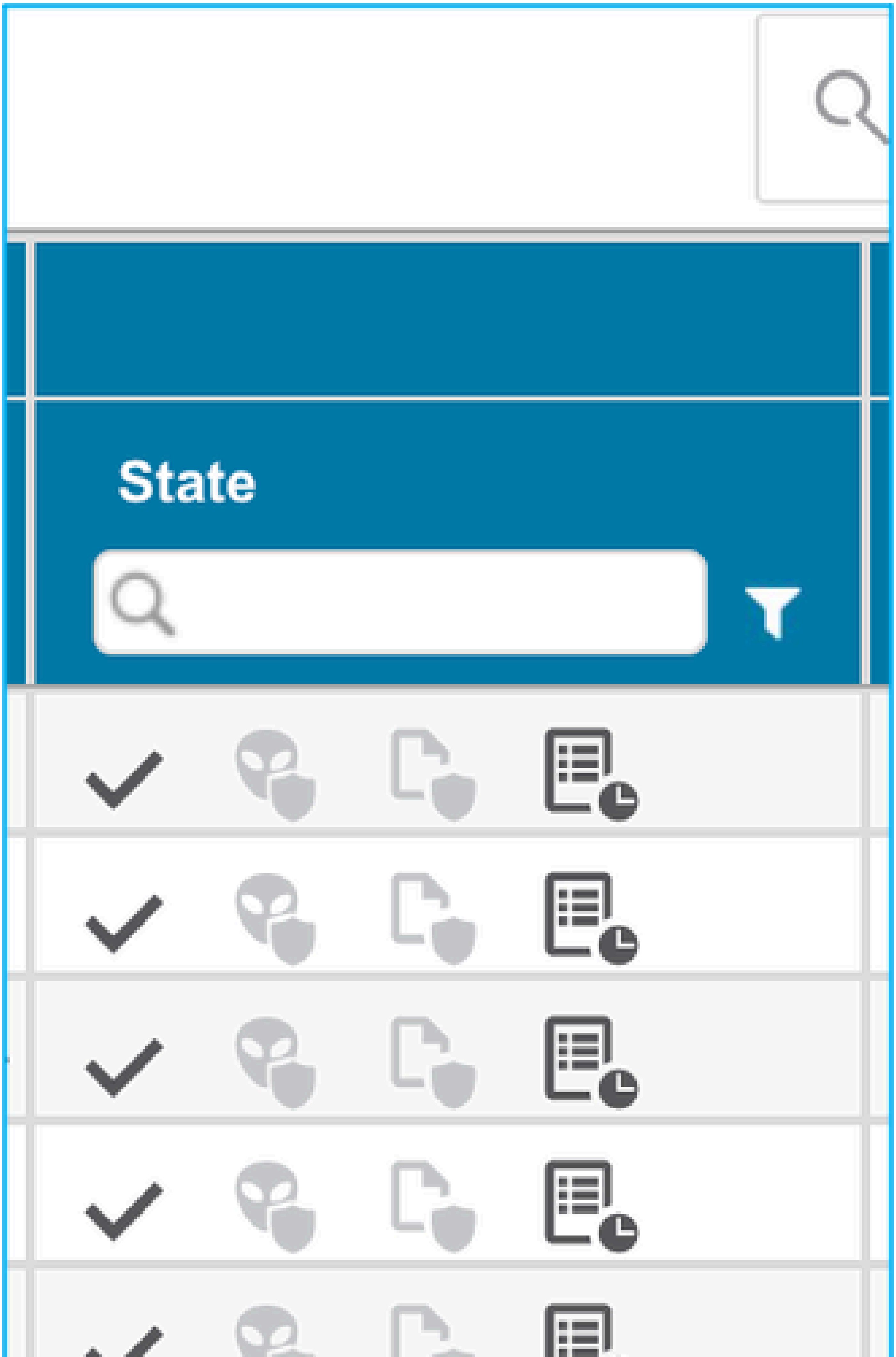
□ Log at the end of connection

Send connection events to:

□ Event Viewer

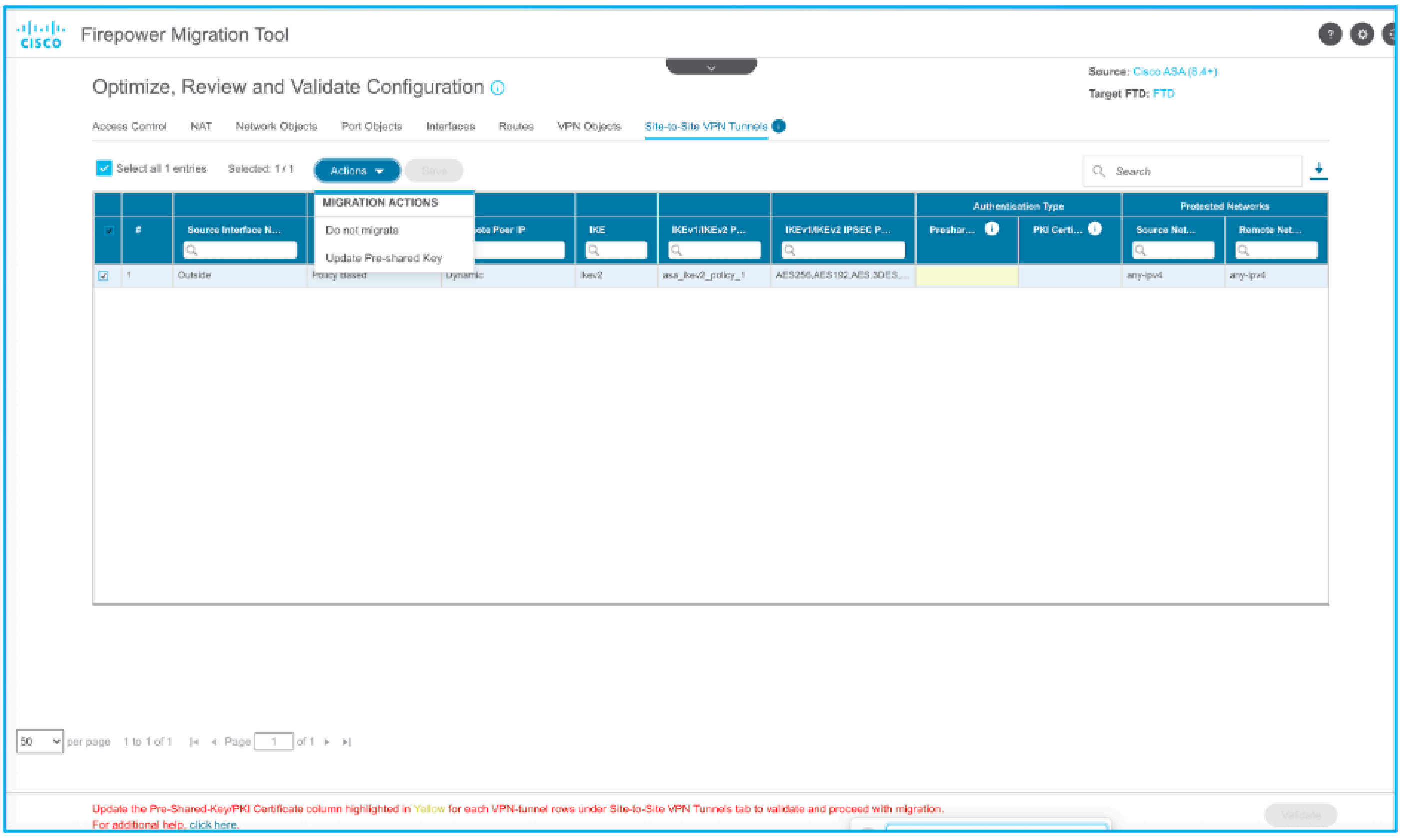
□ Syslog

The rule actions chosen are highlighted accordingly for each rule.



State

: Alert is notified as shown in the image in order to update the pre-shared key since it does not get copied in the ASA configuration file. Navigate to **Actions > Update Pre-Shared Key** in order to enter the value.



Firepower Migration Tool

Optimize, Review and Validate Configuration

Source: Cisco ASA (8.4+)

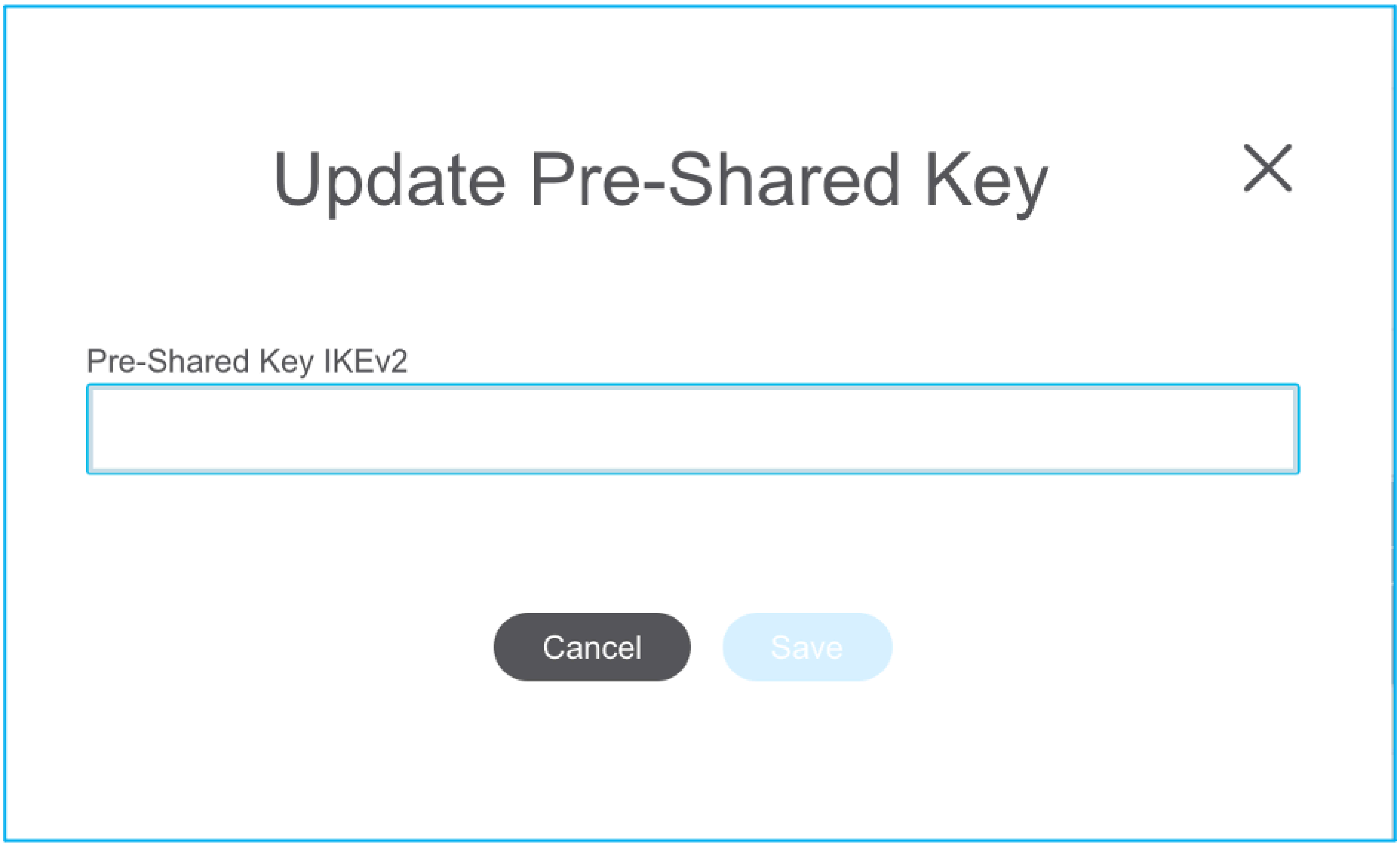
Target FTD: FTD

☑ Select all 1 entries   Selected: 1 / 1

								Authentication Type		Protected Networks	
☑	#	Source Interface N...		ote Peer IP	IKE	IKEv1/IKEv2 P...	IKEv1/IKEv2 IPSEC P...	Preshar...	PKI Certi...	Source Net...	Remote Net...
☑	1	Outside	Policy based	Dynamic	ikev2	asa_ikev2_policy_1	AES256,AES192,AES,3DES...			any-ipv4	any-ipv4

50 per page 1 to 1 of 1 Page 1 of 1

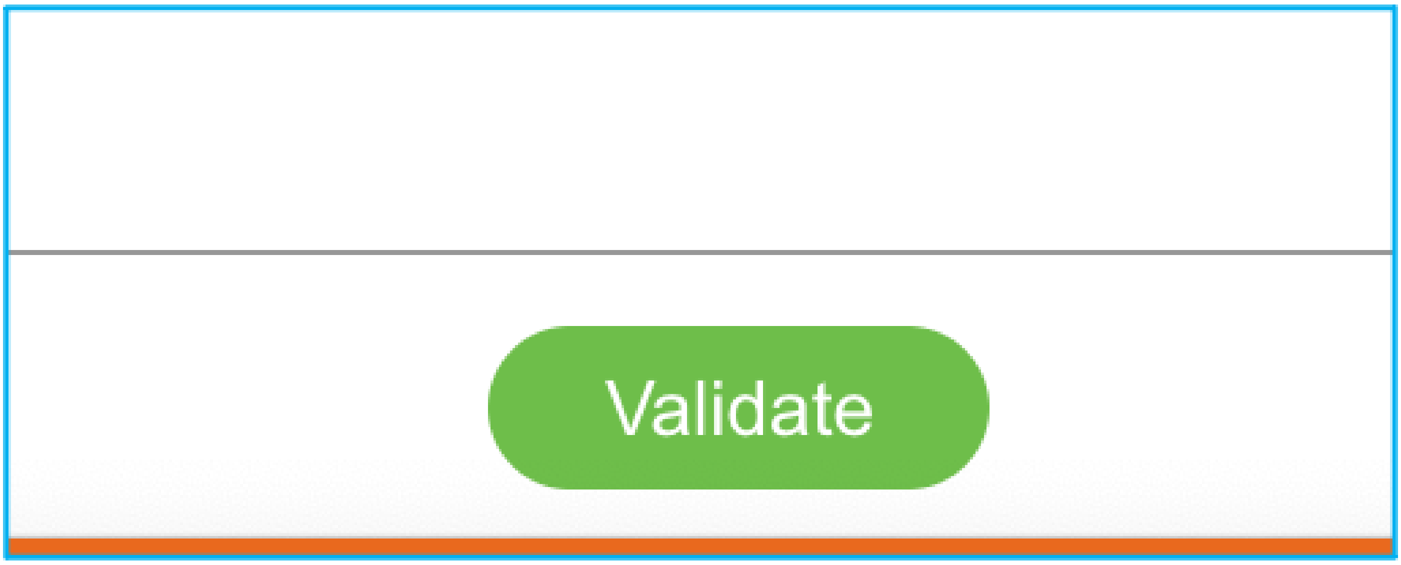
Update the Pre-Shared-Key/PKI Certificate column highlighted in Yellow for each VPN-tunnel rows under Site-to-Site VPN Tunnels tab to validate and proceed with migration.
For additional help, click here.



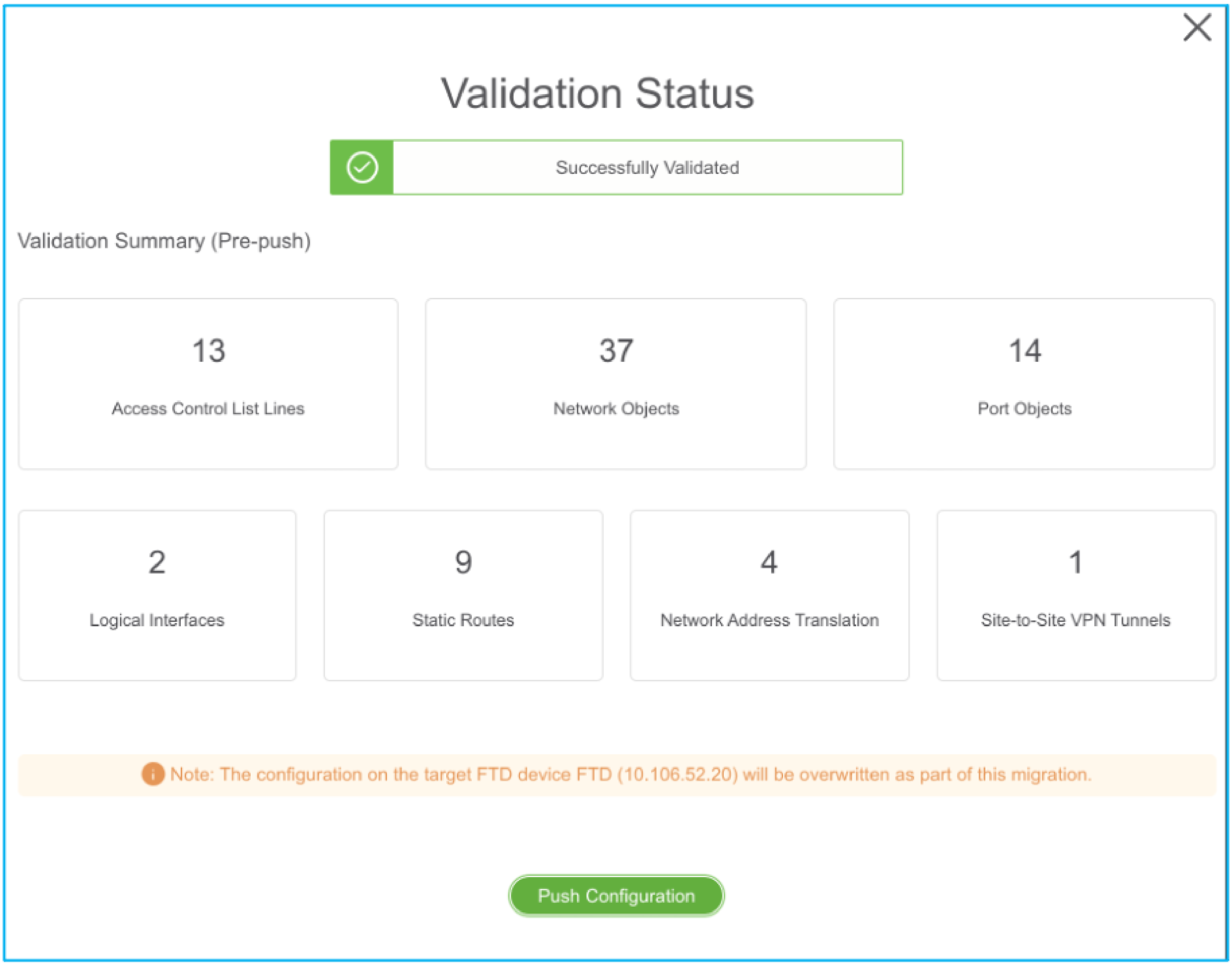
Update Pre-Shared Key

Pre-Shared Key IKEv2

21. Finally, click the **Validate** icon at the bottom right of the screen as shown in the image:



22. Once the validation is successful, click **Push Configuration** as shown in the image:



Validation Status

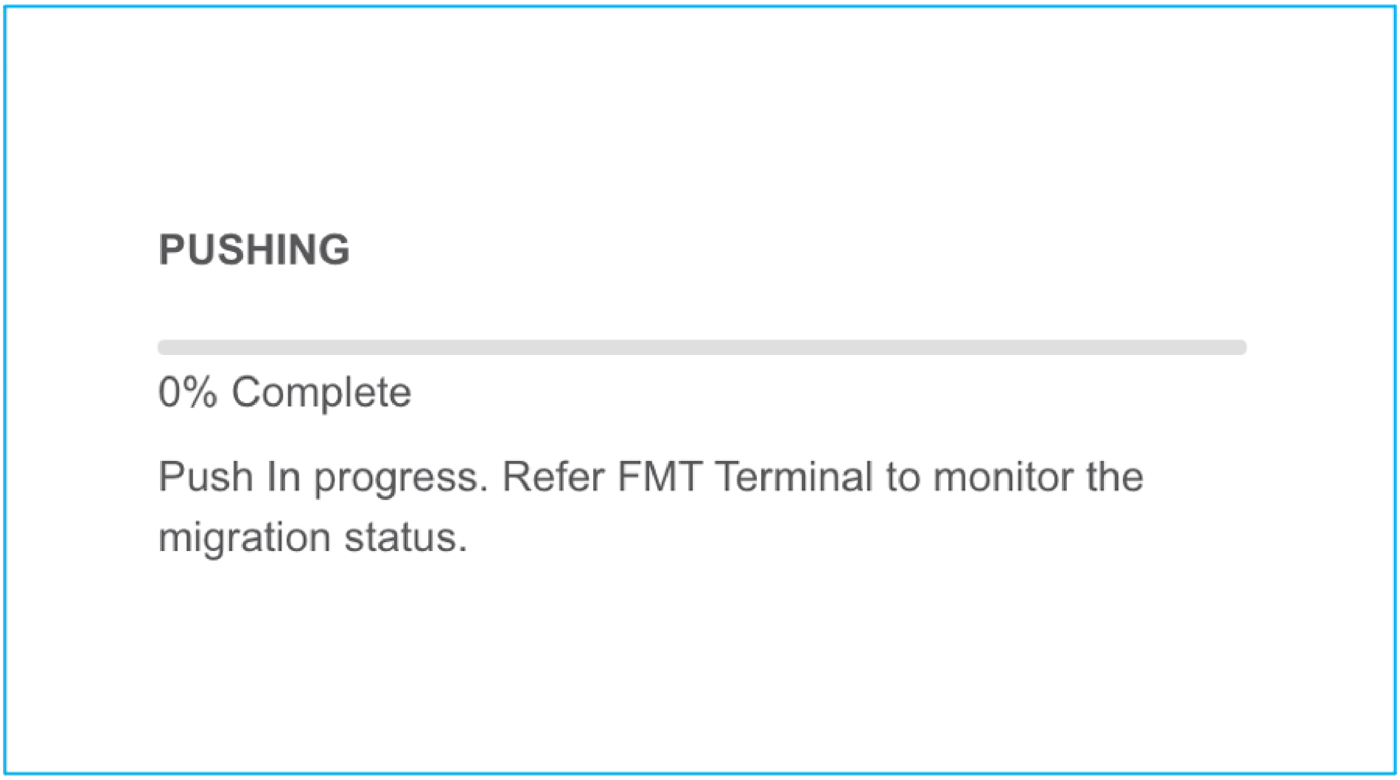
Successfully Validated

Validation Summary (Pre-push)

13	37	14
Access Control List Lines	Network Objects	Port Objects

2	9	4	1
Logical Interfaces	Static Routes	Network Address Translation	Site-to-Site VPN Tunnels

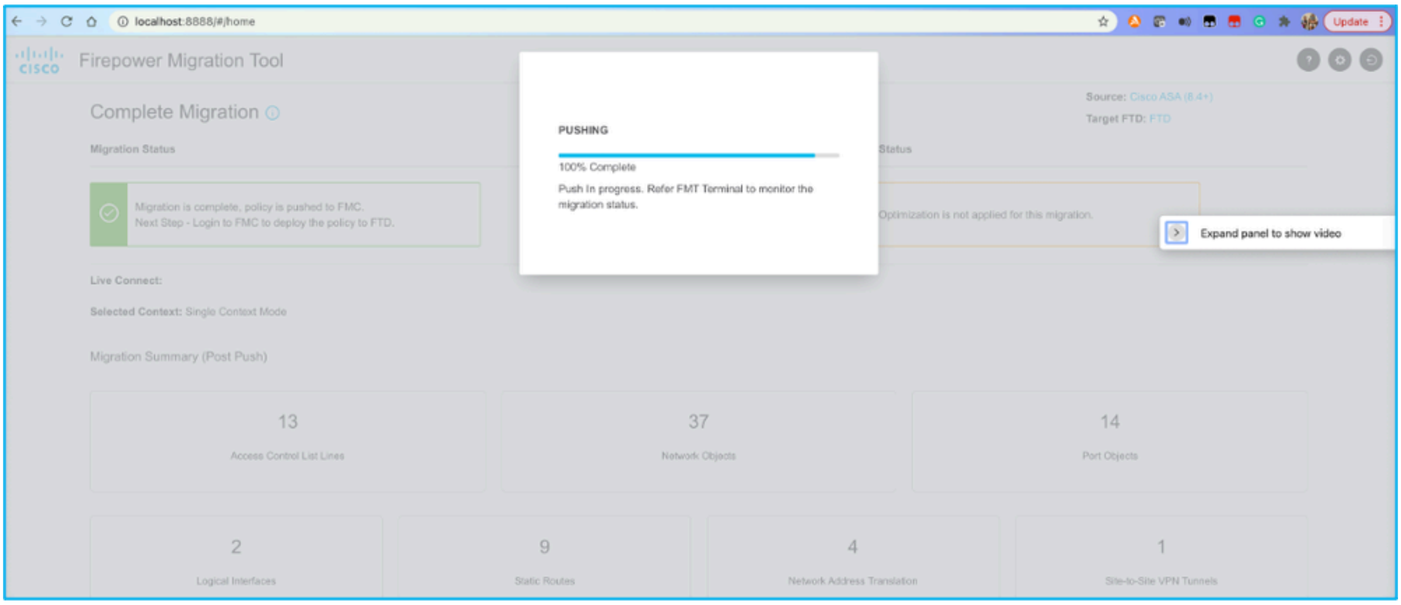
Note: The configuration on the target FTD device FTD (10.106.52.20) will be overwritten as part of this migration.



PUSHING

0% Complete

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



localhost:8888/#/home

Firepower Migration Tool

Complete Migration

Migration Status

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

Status

Optimization is not applied for this migration.

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

Live Connect:

Selected Context: Single Context Mode

Migration Summary (Post Push)

13 Access Control List Lines	37 Network Objects	14 Port Objects

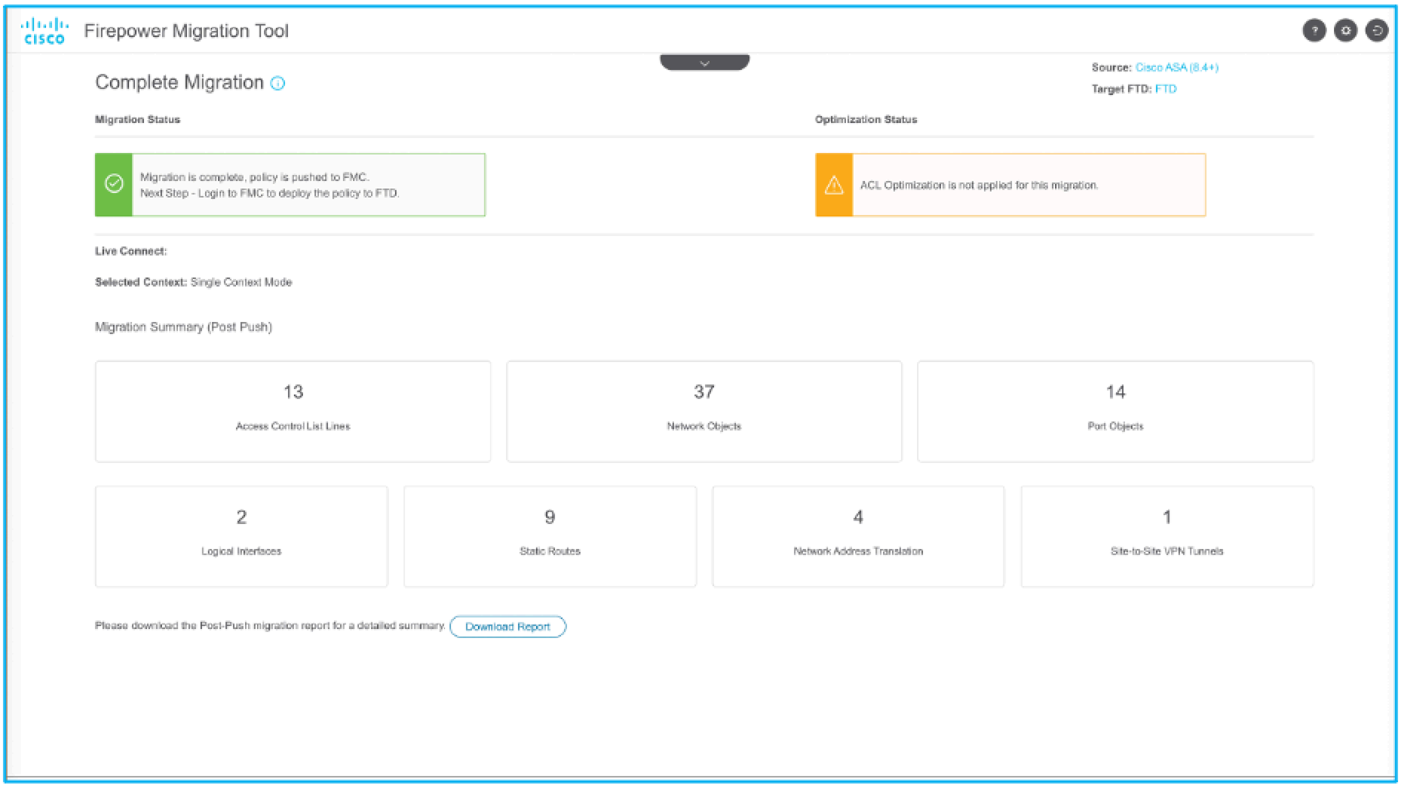
2 Logical Interfaces	9 Static Routes	4 Network Address Translation	1 Site-to-Site VPN Tunnels

PUSHING

100% Complete

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

23. Once the migration is successful, the message that is displayed is shown in the image.



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:

Selected Context: Single Context Mode

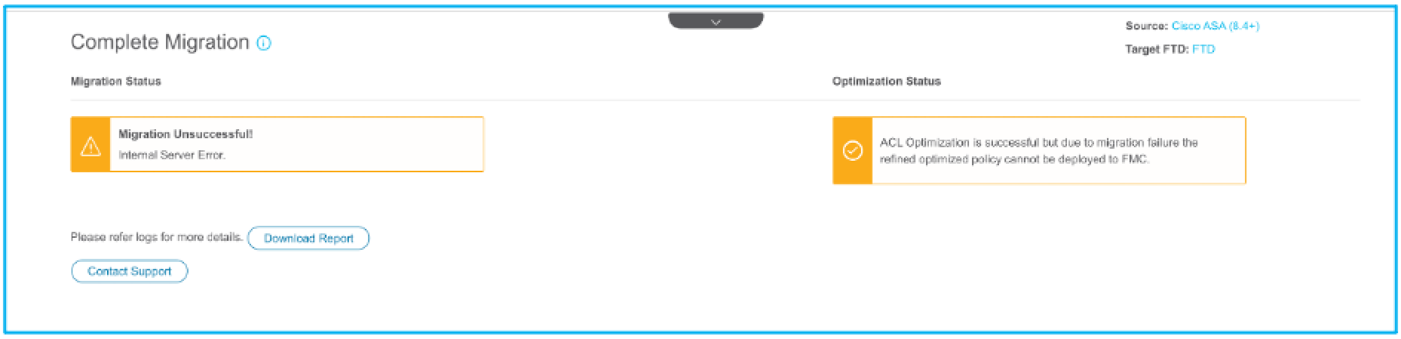
Migration Summary (Post Push)

13 Access Control List Lines	37 Network Objects	14 Port Objects

2 Logical Interfaces	9 Static Routes	4 Network Address Translation	1 Site-to-Site VPN Tunnels

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

Note: If the migration is unsuccessful, click **Download Report** in order to view the Post-migration report.



Complete Migration

Source: Cisco ASA (8.4+)

Target FTD: FTD

Migration Status

Migration Unsuccessful!
Internal Server Error.

Optimization Status

ACL Optimization is successful but due to migration failure the refined optimized policy cannot be deployed to FMC.

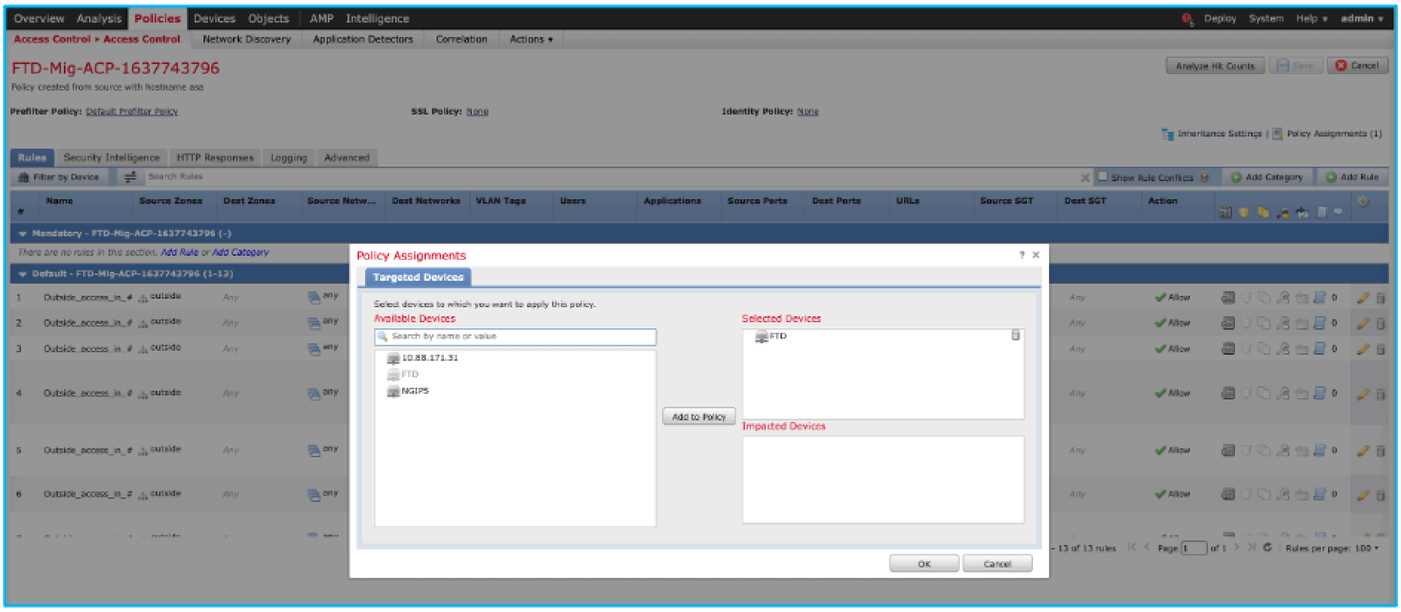
Please refer logs for more details.

Verify

Use this section in order to confirm that your configuration works properly.

Validation on the FMC:

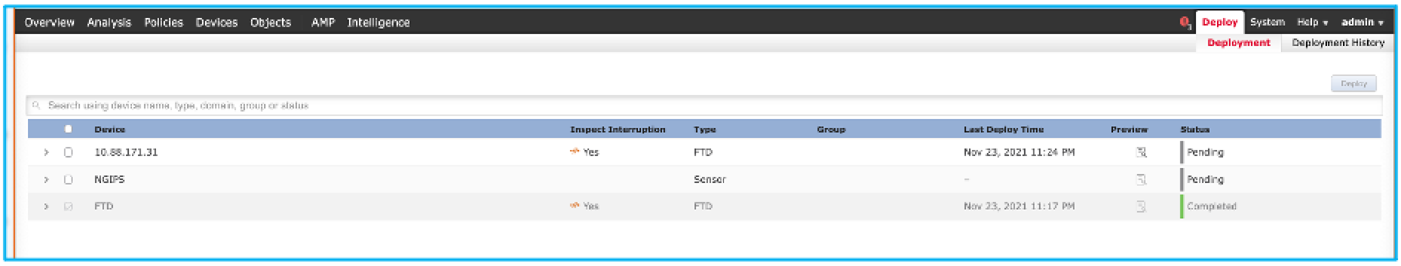
1. Navigate to Policies > Access Control > Access Control Policy > Policy Assignment in order to confirm that the selected FTD is populated.



Note: The migration access control policy has a name with the prefix FTD-Mig-ACP. If no FTD was selected earlier, the FTD must be selected on the FMC.

---

2. Push the policy to the FTD. Navigate to Deploy > Deployment > FTD Name > Deploy as shown in the image:


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help admin
Deployment
Deployment History
Deploy
Search using device name, type, domain, group or status

Device	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
10.88.171.31	Yes	FTD		Nov 23, 2021 11:24 PM		Pending
NGIPS		Sensor		-		Pending
FTD	Yes	FTD		Nov 23, 2021 11:17 PM		Completed

Known Bugs Related to the Firepower Migration Tool

- Cisco bug ID CSCwa56374 - FMT tool hangs on zone mapping page with error with high memory utilization
- Cisco bug ID CSCvz88730 - Interface push failure for FTD Port-channel Management interface type
- Cisco bug ID CSCvx21986 - Port-Channel migration to Target Platform - Virtual FTD is not supported
- Cisco bug ID CSCvy63003 - Migration Tool must disable the interface feature if FTD is already part of the Cluster
- Cisco bug ID CSCvx08199 - ACL needs to split when the application reference is more than 50

Related Information

- Migrating ASA Firewall to Threat Defense with the Firewall Migration Tool
- Technical Support & Documentation - Cisco Systems