

Firepower Migration Toolを使用したASAコンフィギュレーションファイルからのFTDの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[確認](#)

[Firepower移行ツールに関連する既知のバグ](#)

[関連情報](#)

概要

このドキュメントでは、FPR4145での適応型セキュリティアプライアンス(ASA)からFirepower Threat Defense(FTD)への移行の例について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASAに関する基礎知識
- Firepower Management Center(FMC)およびFTDに関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ASA バージョン 9.12(2)
- FTDバージョン6.7.0
- FMCバージョン6.7.0
- Firepower Migration Toolバージョン2.5.0

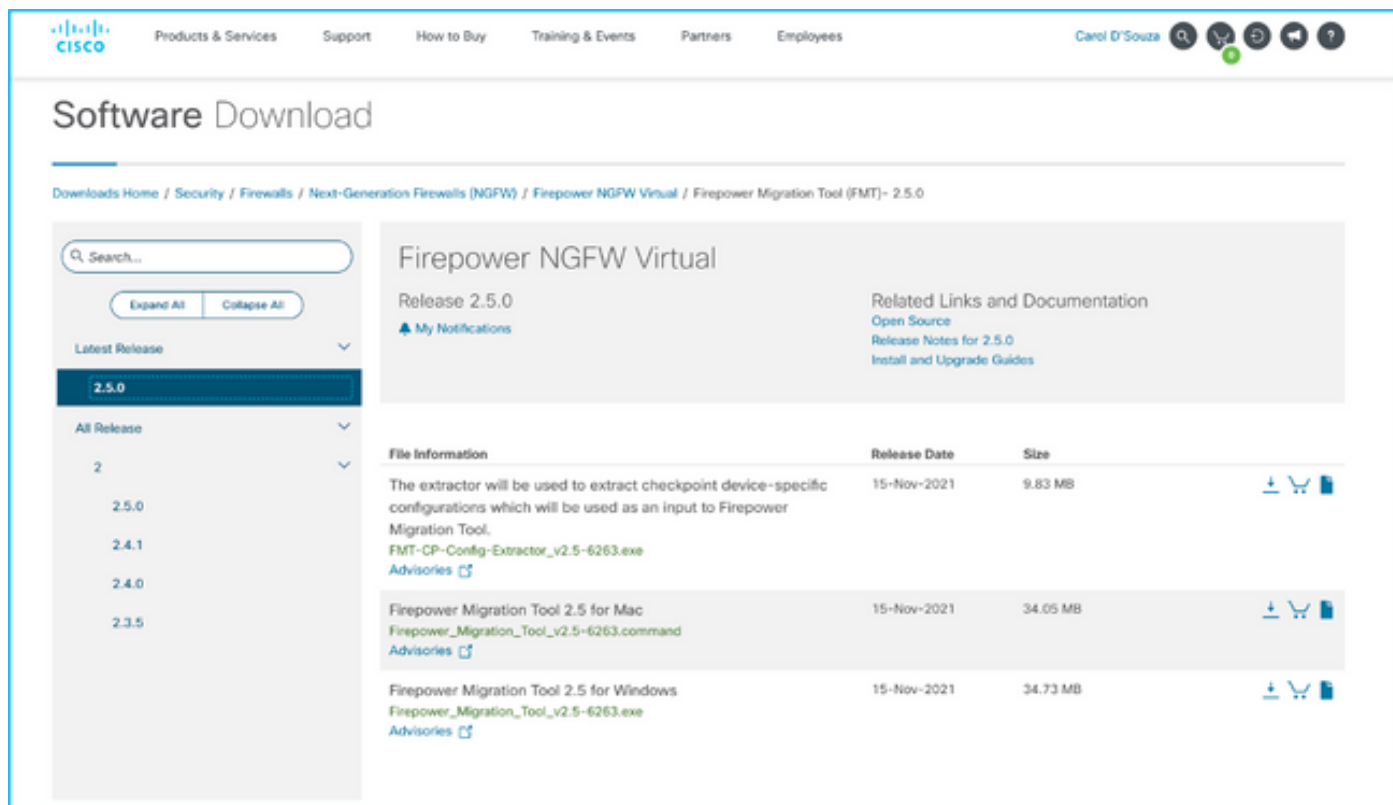
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ASA構成ファイルを.cfgまたは.txt形式でエクスポートします。FMCは、FTDが登録された状態で導入する必要があります。

設定

1.図に示すように、software.cisco.comからFirepower Migration Toolをダウンロードします。



The screenshot shows the Cisco Software Download page for Firepower Migration Tool (FMT) 2.5.0. The page includes a search bar, a navigation menu, and a table of file information. The table lists three files: FMT-CP-Config-Extractor_v2.5-6263.exe (9.83 MB), Firepower Migration Tool 2.5 for Mac (34.05 MB), and Firepower Migration Tool 2.5 for Windows (34.73 MB). All files were released on 15-Nov-2021.

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

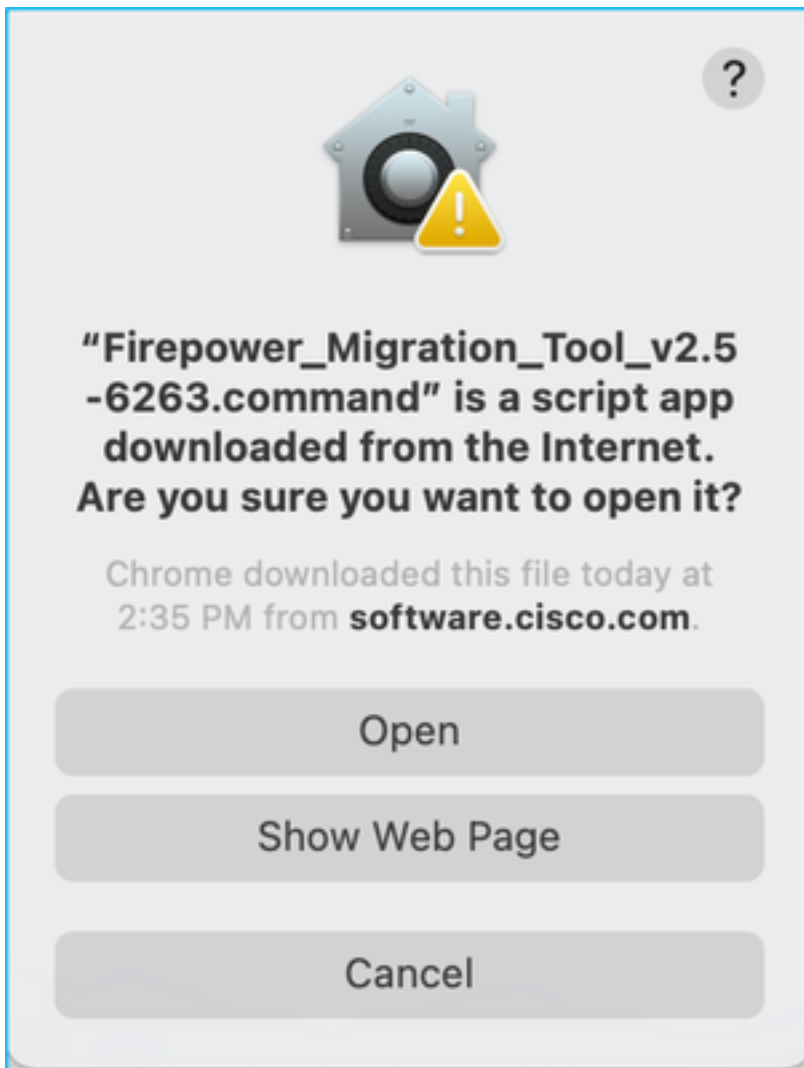
2. Firepower Migration Toolのガイドラインと制限[セクション](#)の要件を確認し、確認します。

3.大規模な構成ファイルを移行する場合は、システムが移行プッシュ中にスリープ状態にならないようにスリープ設定を構成します。

3.1. Windowsの場合は、コントロールパネルの[電源オプション]に移動します。現在の電源プランの横にある[プラン設定の変更]をクリックします。変更コンピュータをスリープ状態に設定してNeverに変更します。[変更の保存]をクリックします。

3.2. MACの場合は、[システム設定] > [省エネルギー]に移動します。ディスプレイがオフのときにコンピュータが自動的にスリープ状態にならないようにボックスをオンにし、[Turn Display Off afterスライダを[Never]にドラッグします。

注：MACユーザーがダウンロードしたファイルを開こうとすると、この警告ダイアログが表示されます。これを無視して、ステップ4 Aに従います。



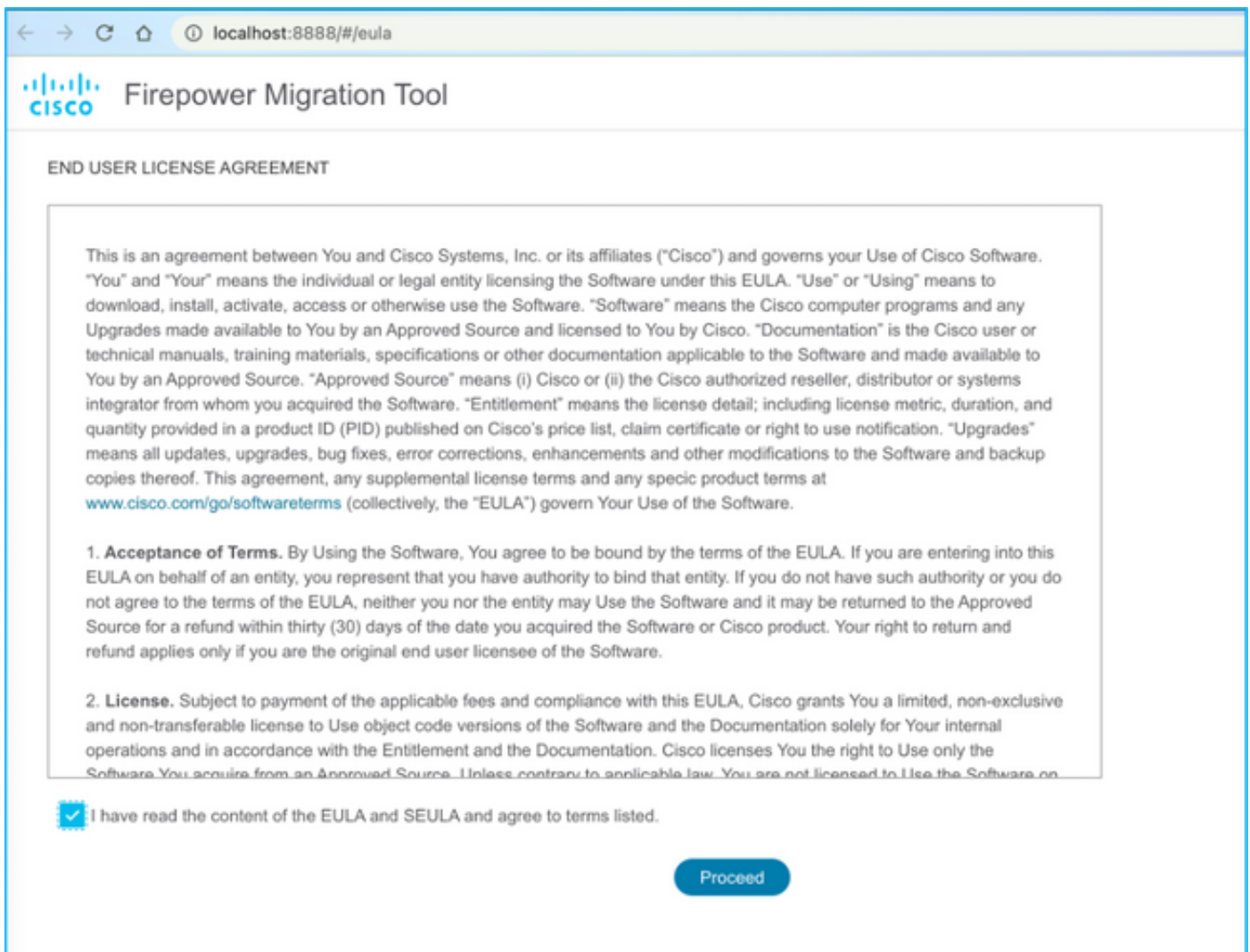
4. A. MACの場合 – ターミナルを使用して、次のコマンドを実行します。

```
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: hompath 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. B. Windowsの場合 – Firepower Migration Toolをダブルクリックして、Google Chromeブラウザで起動します。

5.図に示すように、ライセンスを受け入れます。



← → ↻ 🏠 ⓘ localhost:8888/#/eula

cisco Firepower 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 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

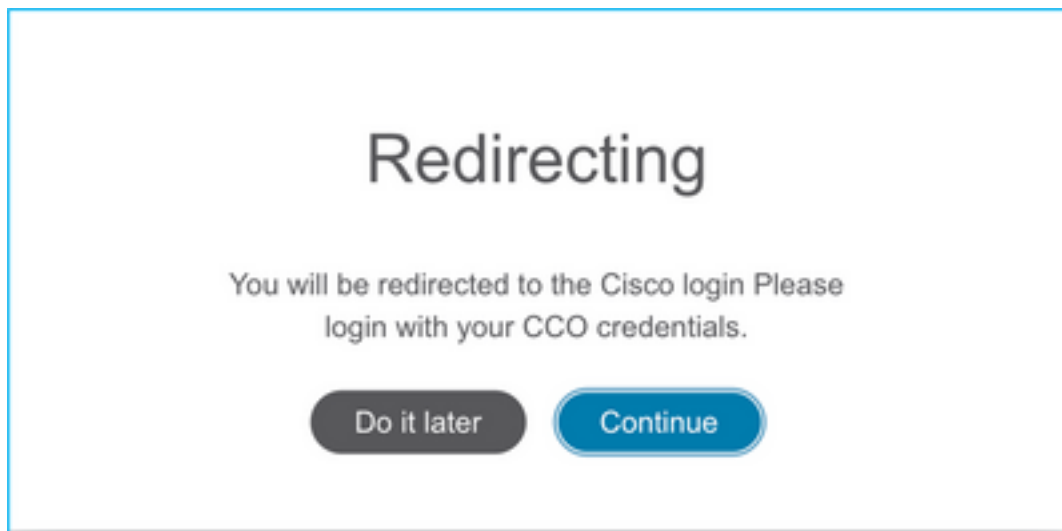
I have read the content of the EULA and SEULA and agree to terms listed.

Proceed

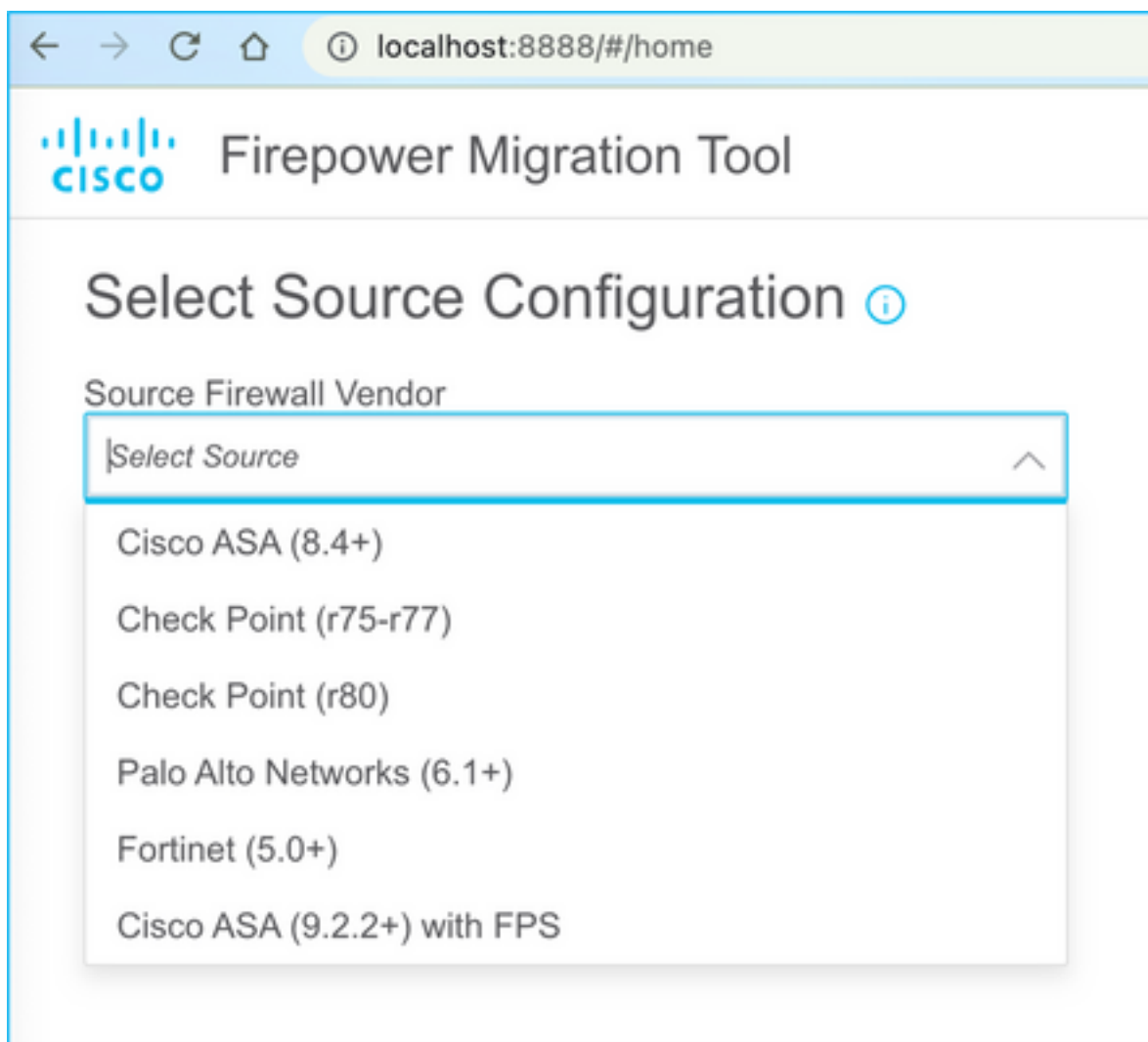
6. Firepower Migration Toolのログインページで、[Login with CCO]リンクをクリックして、シングルサインオンのクレデンシャルでCisco.comアカウントにログインします。

注：Cisco.comアカウントがない場合は、Cisco.comのログインページで作成します。次の

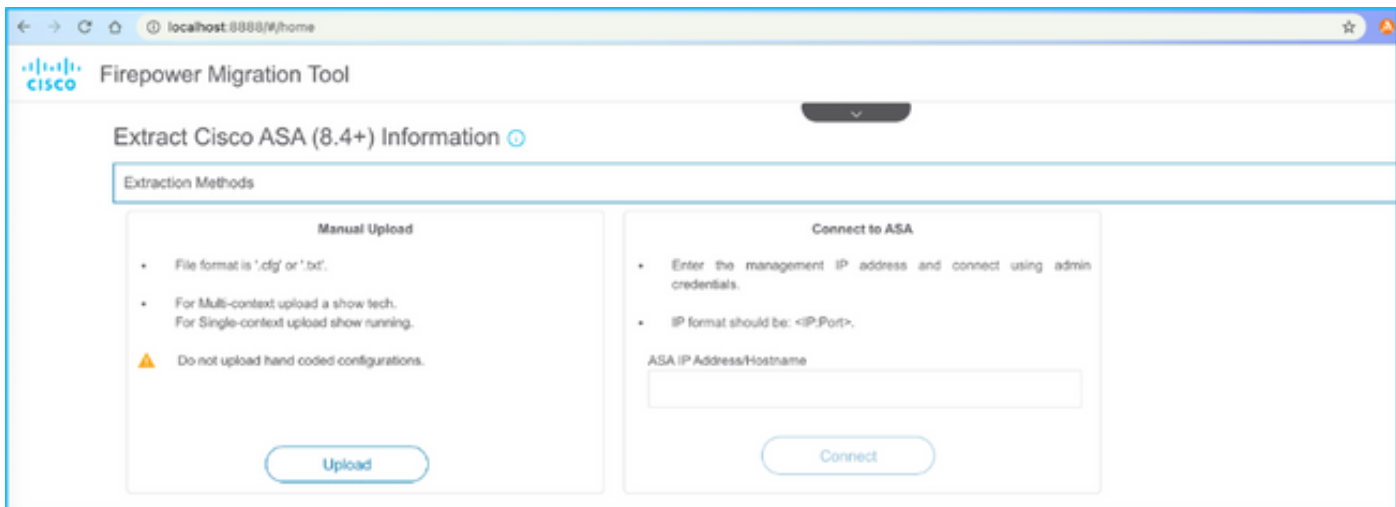
デフォルトのクレデンシャルでログインします。ユーザ名 : adminパスワード : Admin123。



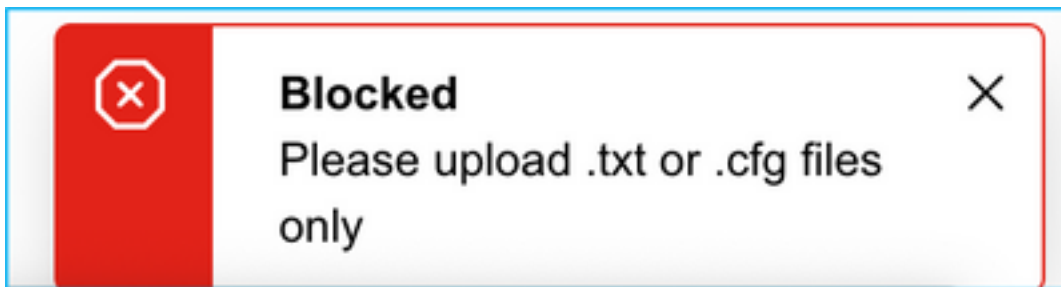
7.ソース構成を選択します。このシナリオでは、Cisco ASA(8.4+)です。



8. ASAに接続できない場合は、[Manual Upload]を選択します。または、ASAから実行コンフィギュレーションを取得し、管理IPとログインの詳細を入力できます。このシナリオでは、手動アップロードが実行されました。

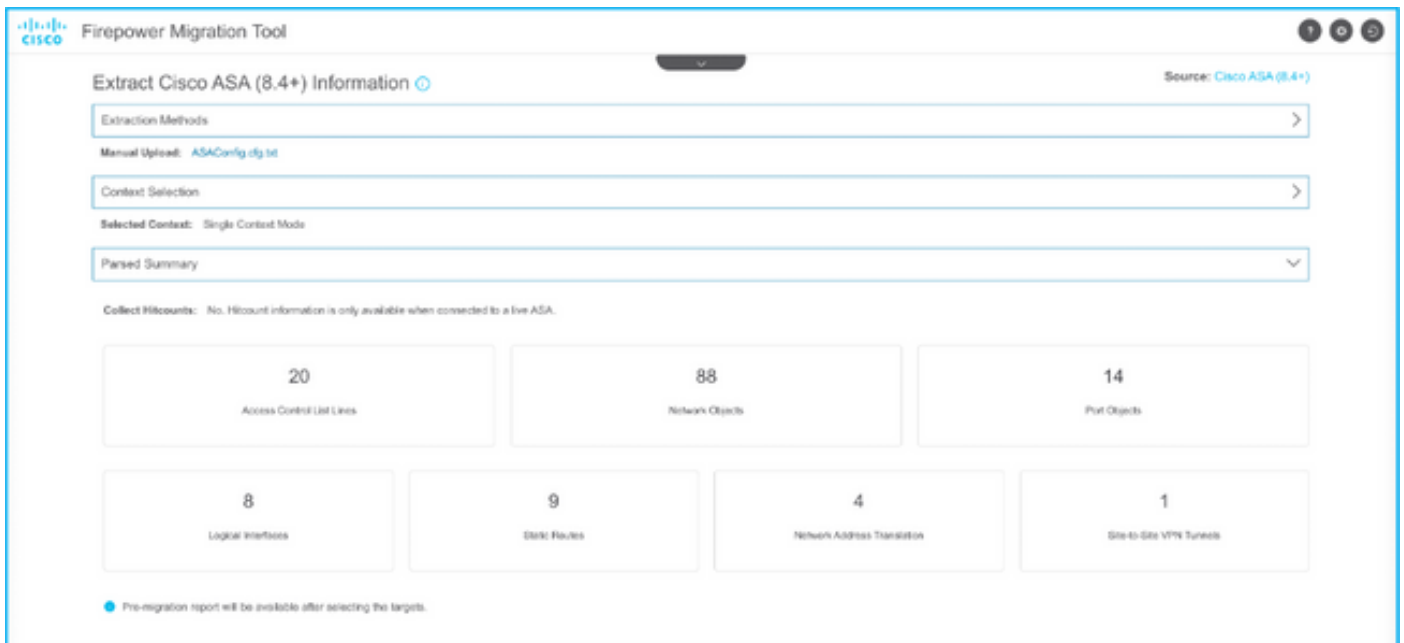


注：このエラーは、ファイルがサポートされていない場合に表示されます。形式をプレーンテキストに変更してください。（拡張子に.cfgが含まれているにもかかわらずエラーが発生します）。

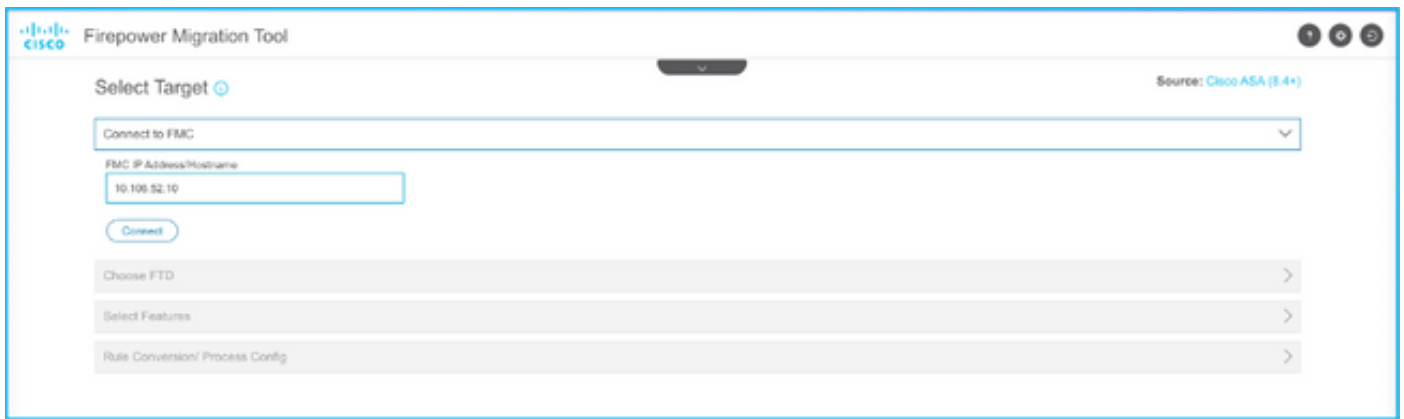


```
ASAConfig.cfg — Edited
asa# show running-config
: Saved
:
: Serial Number: FLM22160652
: Hardware: FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
:
ASA Version 9.12(2)
:
hostname asa
enable password ***** pbkdf2
:
license smart
feature tier standard
names
no mac-address 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
```

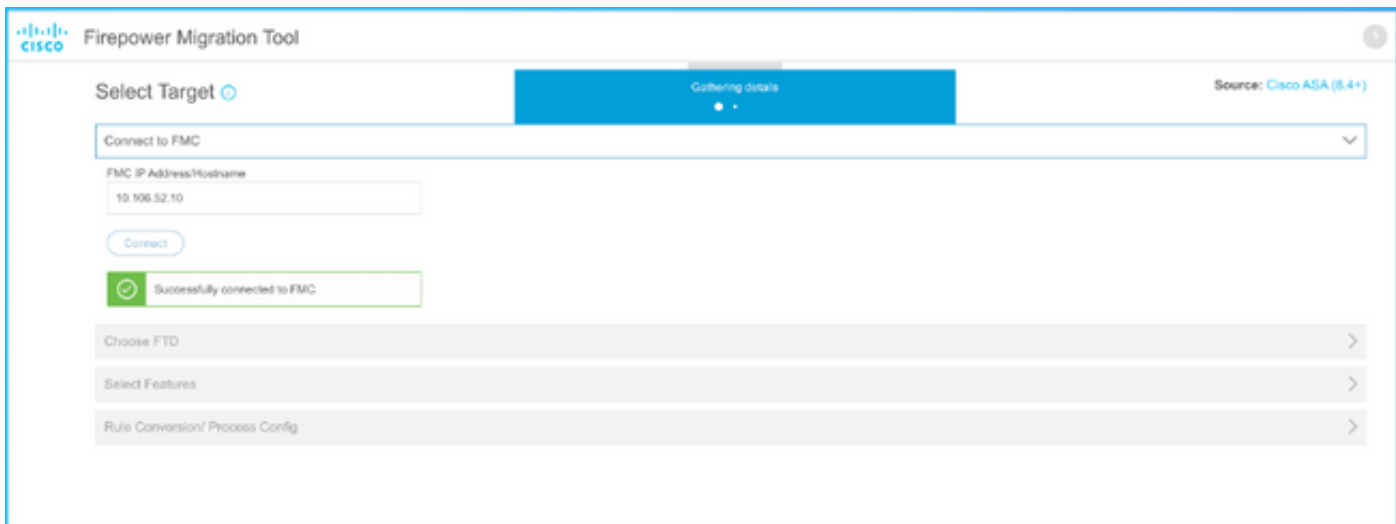
9.ファイルがアップロードされると、図に示すように、要素が解析され、要約が提供されます。



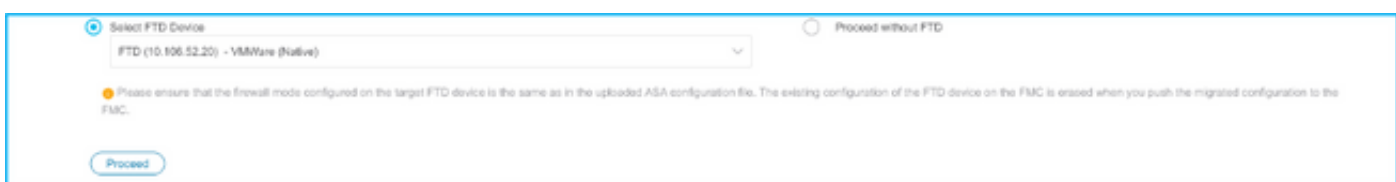
10. ASA設定の移行先となるFMC IPおよびログインクレデンシャルを入力します。ワークステーションからFMC IPに到達できることを確認します。



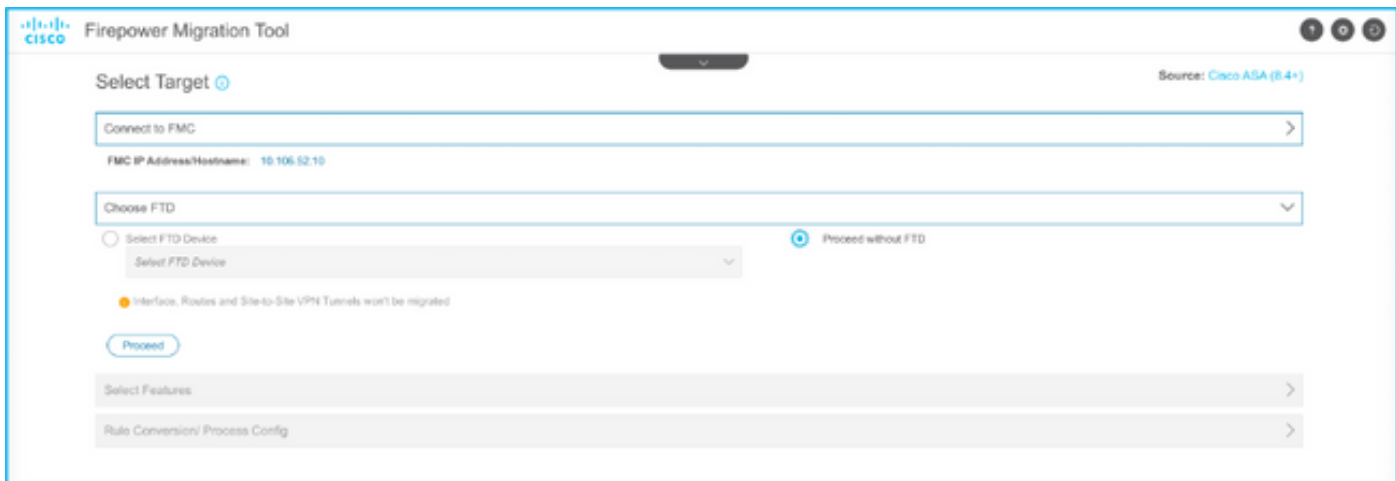
11. FMCが接続されると、その下の管理対象FTDが表示されます。



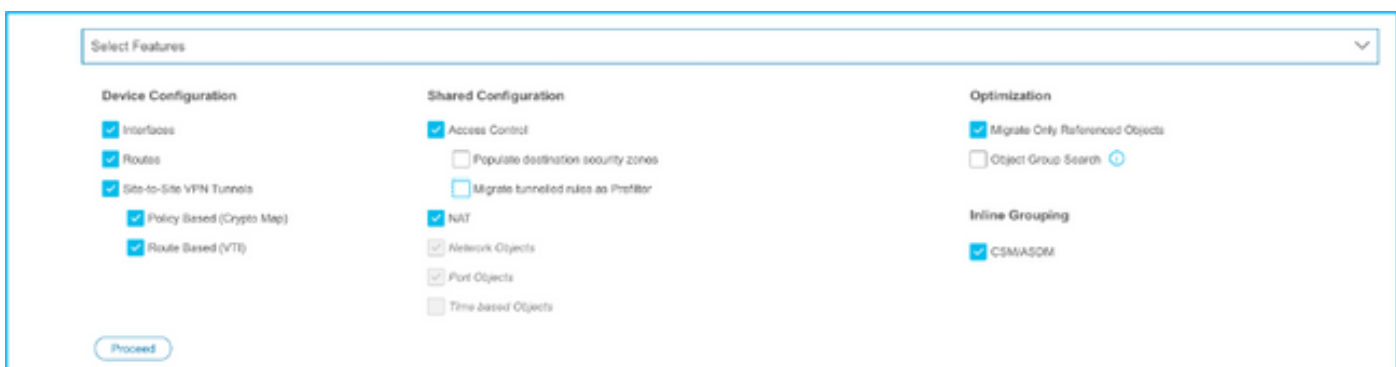
12. ASA設定の移行を実行するFTDを選択します。



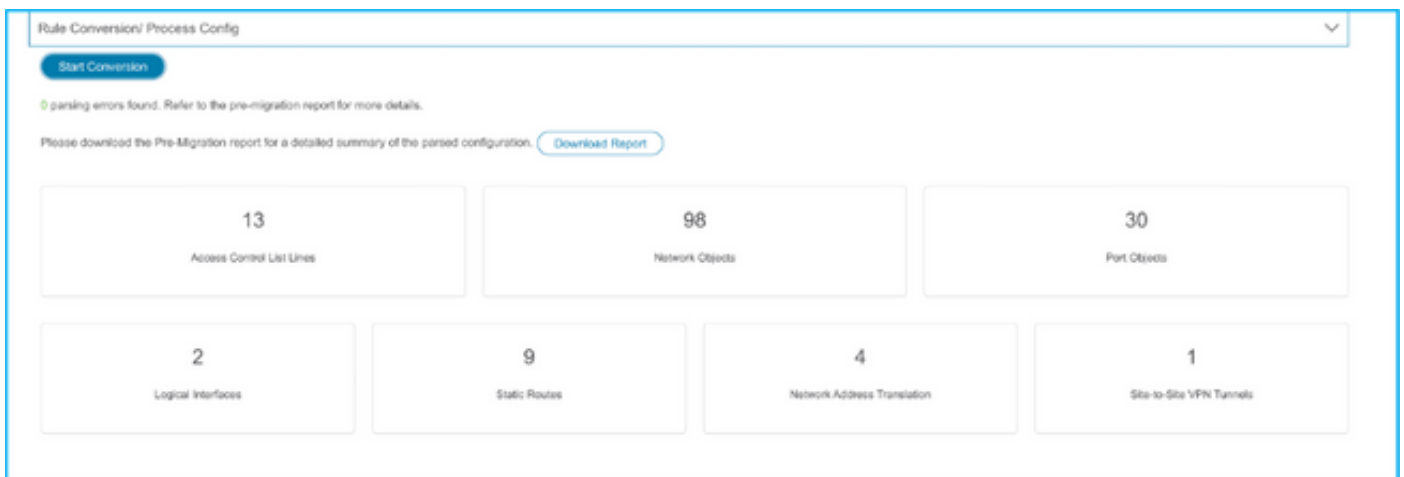
注：FTDデバイスを選択することをお勧めします。選択しない場合、インターフェイス、ルート、サイト間VPN設定は手動で行う必要があります。



13.図に示すように、移行に必要な機能を選択します。




14. 「変換の開始」を選択し、FTD構成に関連する要素を入力する事前移行を開始します。



15.前に表示した[Download Report]をクリックすると、図に示すように、移行前レポートが表示されます。

← → 🏠 📄 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 recommend reviewing the configuration 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

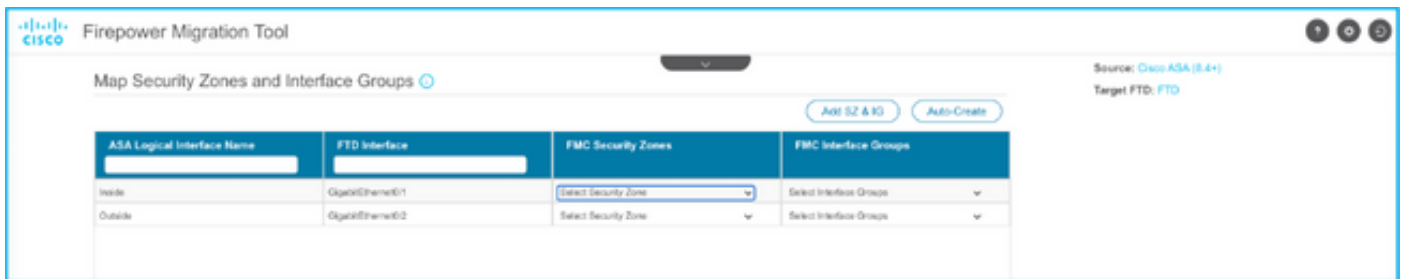
Note: ACEs that are applied outbound or not attached to interfaces using the access-group command are ignored.

16.図に示すように、必要に応じてASAインターフェイスをFTDインターフェイスにマッピングします。

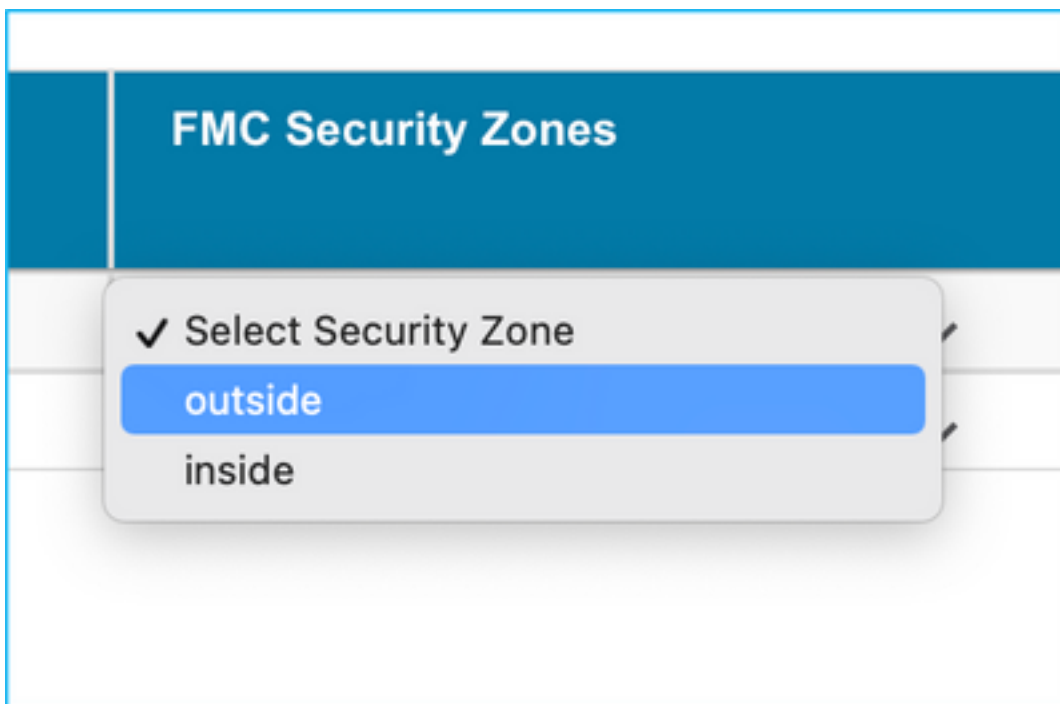
Refresh

ASA Interface Name	FTD Interface Name
<input type="text"/>	<div style="border: 1px solid gray; padding: 5px;"> Select Interface GigabitEthernet0/0 GigabitEthernet0/1 <input checked="" type="checkbox"/> GigabitEthernet0/2 </div>
Ethernet1/2	
Ethernet1/3	

17. FTDインターフェイスにセキュリティゾーンとインターフェイスグループを割り当てます。



A. FMCにセキュリティゾーンとインターフェイスグループがすでに作成されている場合は、必要に応じて選択できます。



B. セキュリティゾーンとインターフェイスグループを作成する必要がある場合は、図に示すように[Add SZ & IG]をクリックします。



Add SZ & IG

Security Zones (SZ)

Interface Groups (IG)

Add



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

Interface Groups	Type	Actions
<input type="text" value="Inside"/>	ROUTED	

0 - 0 of 0 |< < 1 > >|

Close

C. それ以外の場合は、ASA logical interface_szとASA logical interface_igという名前のセキュリティゾーンとインターフェイスグループをそれぞれ作成するAuto-Createオプションを選択できます。

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

Cancel

Auto-Create

Firepower Migration Tool

Map Security Zones and Interface Groups ⓘ

Add SZ & IG Auto-Create

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. 作成された各FTD要素を確認および検証します。図に示すように、アラートは赤で表示されます。

Firepower Migration Tool

Optimize, Review and Validate Configuration ⓘ

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

Access Control NAT Network Objects Port Objects Interfaces Routes VPN Objects Site-to-Site VPN Tunnels ⓘ

ADP Pre-Filter

Select all 13 entries Selected 0 / 13

#	Name	SOURCE				DESTINATION				State	Action	ACE Count
		Zone	Network	Port	Zone	Network	Port					
1	Outside_access_in_01	outside	any	ANY	ANY			✓	Allow	1		
2	Outside_access_in_02	outside	any	ANY	ANY			✓	Allow	1		
3	Outside_access_in_03	outside	any	ANY	ANY			✓	Allow	2		
4	Outside_access_in_04	outside	any	ANY	ANY			✓	Allow	4		
5	Outside_access_in_05	outside	any	ANY	ANY			✓	Allow	3		
6	Outside_access_in_06	outside	any	ANY	ANY			✓	Allow	2		
7	Outside_access_in_07	outside	any	ANY	ANY			✓	Allow	3		
8	Outside_access_in_08	outside	any	ANY	ANY			✓	Allow	1		
9	Outside_access_in_09	outside	any	ANY	ANY			✓	Allow	8		
10	Outside_access_in_010	outside	any	ANY	ANY			✓	Allow	7		
11	Outside_access_in_011	outside	any	ANY	ANY			✓	Allow	2		
12	Outside_access_in_012	outside	any	ANY	ANY			✓	Allow	1		

50 /page 1 to 13 of 13 | Page 1 of 1

Update the Pre-Shared Key (PSK) 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.

Optimize ACL (RMH)

19.ルールを編集する場合は、図に示すように移行アクションを選択できます。ファイルとIPSポリシーを追加するFTD機能は、この手順で実行できます。

The screenshot shows a configuration interface with a table of rules. At the top, there are tabs for 'ACP' and 'Pre-filter', and a 'Select all 13 entries' checkbox. Below the table, there is an 'Actions' dropdown menu that is open, showing options for 'MIGRATION ACTIONS' and 'RULE ACTIONS'. The table has columns for '#', 'Name', and 'SOURCE'. The 'Name' column contains entries like 'Outside_access_in_#1' through '#6'. The 'SOURCE' column contains 'outside' and 'any'.

	#	Name		SOURCE
<input checked="" type="checkbox"/>			MIGRATION ACTIONS	
			Do not migrate	network
			RULE ACTIONS	
<input checked="" type="checkbox"/>	1	Outside_access_in_#1	File Policy	
<input checked="" type="checkbox"/>	2	Outside_access_in_#2	IPS Policy	
<input checked="" type="checkbox"/>	3	Outside_access_in_#3	Log	
<input checked="" type="checkbox"/>	4	Outside_access_in_#4	Rule Action	
<input checked="" type="checkbox"/>	5	Outside_access_in_#5		
<input checked="" type="checkbox"/>	6	Outside_access_in_#6	outside	any

注：FMCにすでにファイルポリシーが存在する場合は、図に示すように設定されます。IPSポリシーとデフォルトポリシーについても同様です。

The screenshot shows a dialog box titled 'File Policy'. It has a close button (X) in the top right corner. Below the title, there is a label 'Select File Policy *' and a dropdown menu. The dropdown menu is open, showing two options: 'eicar' and 'None'. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Select'.

ログの設定は、必要なルールに対して行うことができます。FMC上に存在するsyslogサーバ設定は、この段階で選択できます。

20.同様に、NAT、ネットワークオブジェクト、ポートオブジェクト、インターフェイス、ルート、VPNオブジェクト、サイト間VPNトンネル、およびその他の要素は、設定に従って手順ごとに確認できます。

注：事前共有キーはASA設定ファイルにコピーされないため、図に示すようにアラートが通知されます。「アクション」>「事前共有キーの更新」を選択して値を入力します。

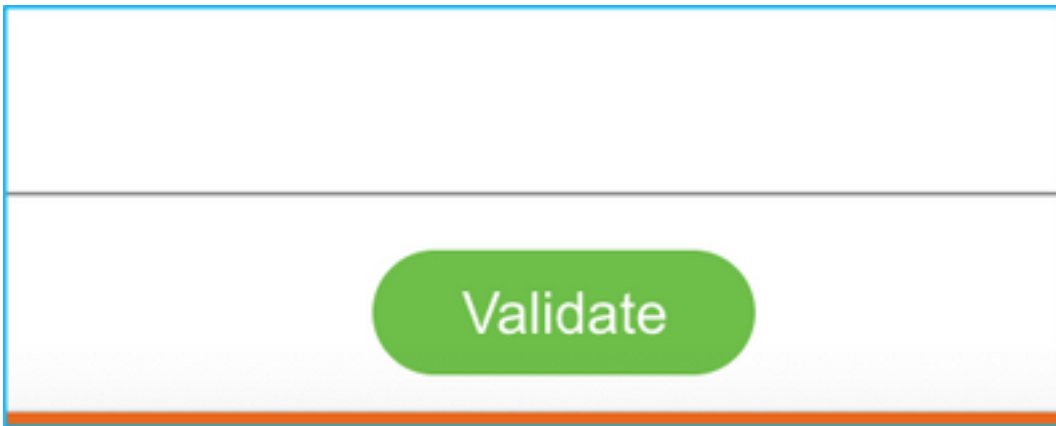
#	Source Interface N...	MIGRATION ACTIONS				Authentication Type		Protected Networks	
		Do not migrate	Update Pre-shared Key	Update Pre-shared Key	Update Pre-shared Key	Preshare...	PKI Cert...	Source Net...	Remote Net...
1	Outside	Pre-shared	Dynamic	Key	ikev2_key_1	AAA/MS/ADIS/ADIS...		any-gw	any-gw

Update Pre-Shared Key

Pre-Shared Key IKEv2

Cancel Save

21.最後に、図に示すように、画面の右下にある[Validate]アイコンをクリックします。



22. 検証が成功したら、図に示すように[Push Configuration]をクリックします。

A dialog box titled "Validation Status" with a close button (X) in the top right corner. It features a green progress bar with a checkmark icon and the text "Successfully Validated". Below this is a section titled "Validation Summary (Pre-push)" containing seven cards with configuration counts: Access Control List Lines (13), Network Objects (37), Port Objects (14), Logical Interfaces (2), Static Routes (9), Network Address Translation (4), and Site-to-Site VPN Tunnels (1). A yellow note at the bottom states: "Note: The configuration on the target FTD device FTD (10.106.52.20) will be overwritten as part of this migration." A green "Push Configuration" button is located at the bottom center.

Validation Status

Successfully Validated

Validation Summary (Pre-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

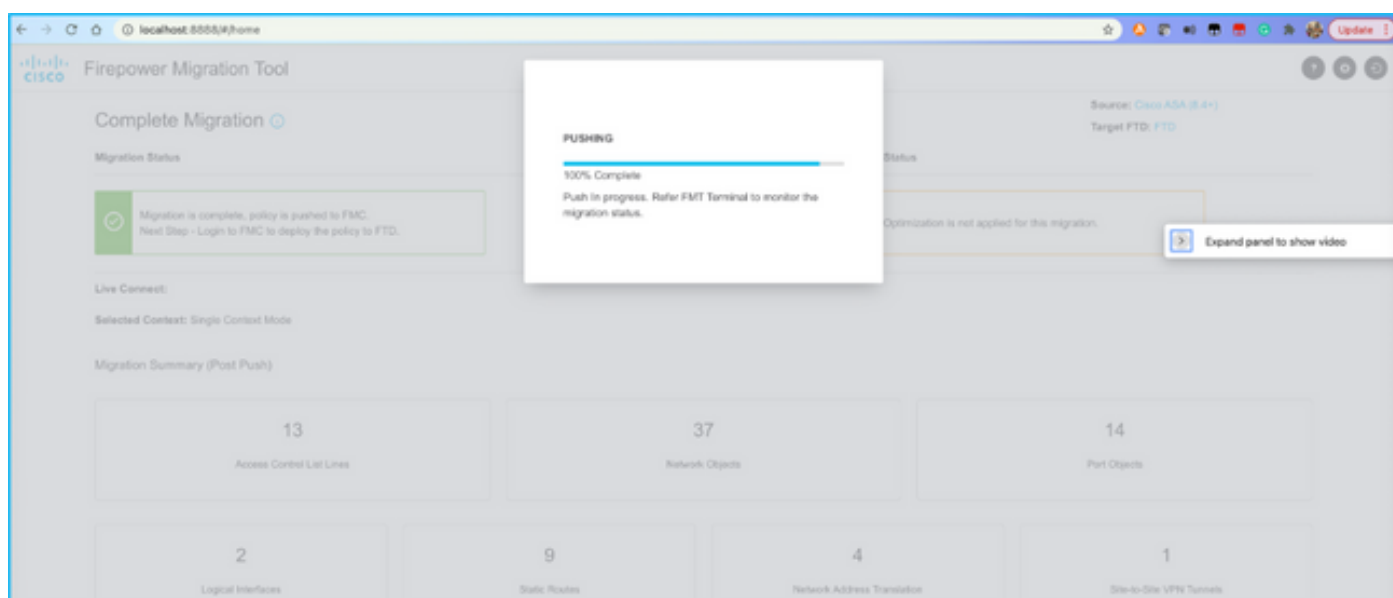
Note: The configuration on the target FTD device FTD (10.106.52.20) will be overwritten as part of this migration.

Push Configuration

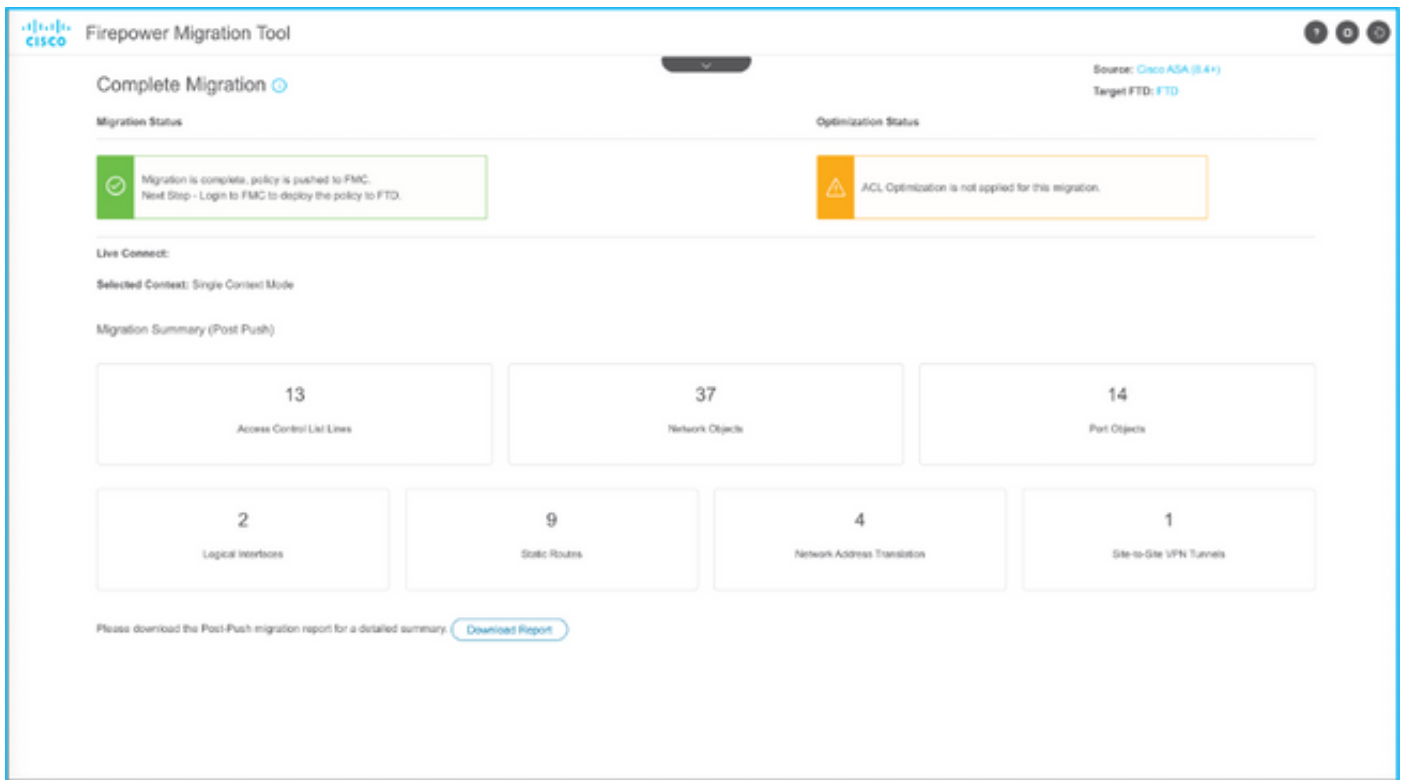
PUSHING

0% Complete

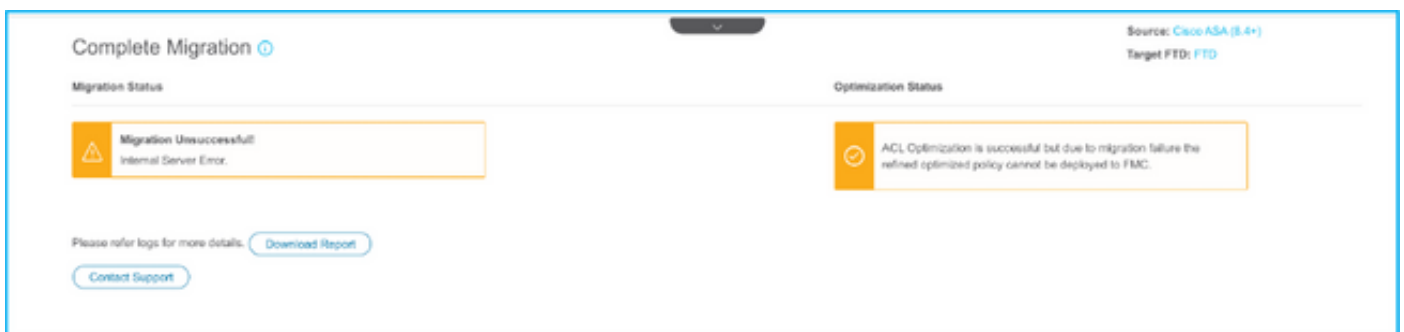
Push In progress. Refer FMT Terminal to monitor the migration status.



23.移行が成功すると、表示されるメッセージが画像に表示されます。



注：移行に失敗した場合は、[Download Report]をクリックして、移行後レポートを表示します。

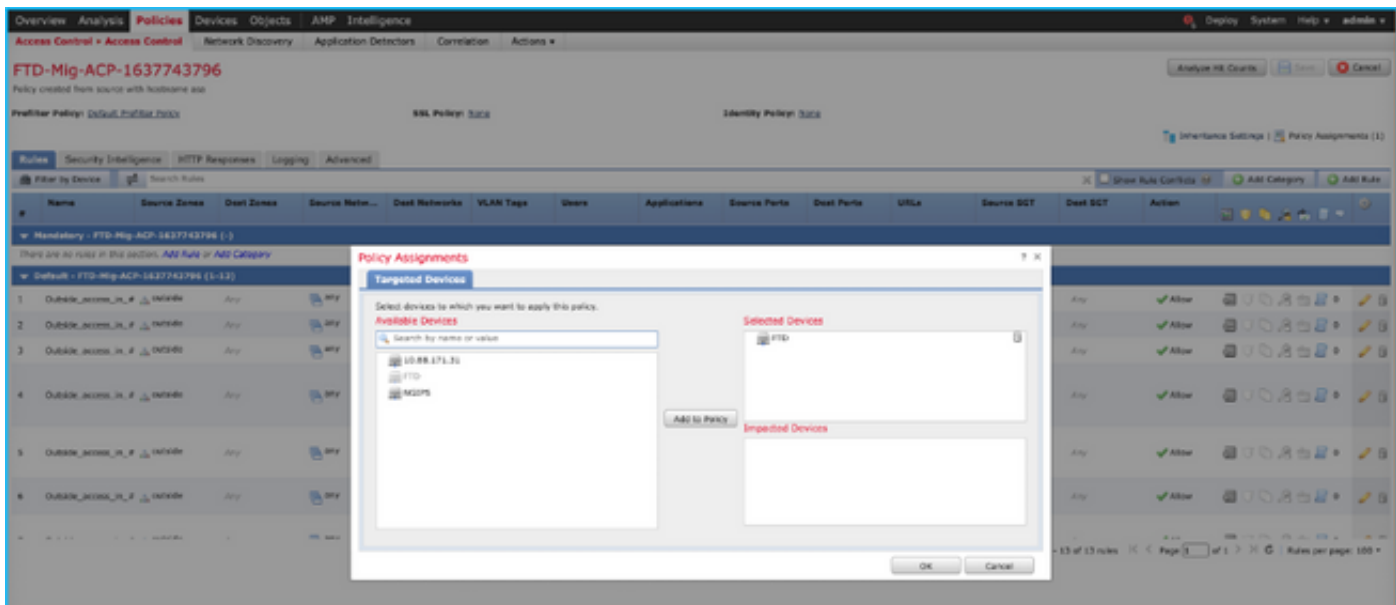


確認

ここでは、設定が正常に機能しているかどうかを確認します。

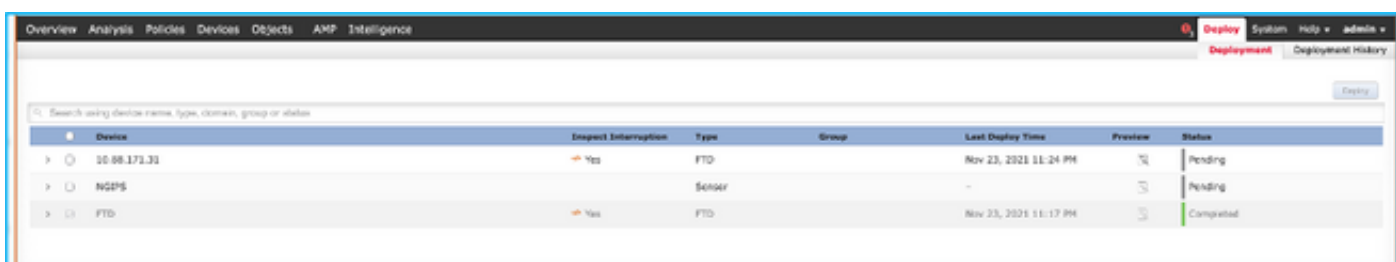
FMCの検証

1. [Policies] > [Access Control] > [Access Control Policy] > [Policy Assignment]に移動し、選択したFTDが入力されていることを確認します。



注：移行アクセス制御ポリシーの名前には、プレフィックスFTD-Mig-ACPを使用します。ステップ2.8でFTDを選択しなかった場合は、FMCでFTDを選択する必要があります。

2.ポリシーをFTDにプッシュします。図に示すように、[Deploy] > [Deployment] > [FTD Name] > [Deploy]に移動します。



Firepower移行ツールに関連する既知のバグ

- Cisco Bug ID [CSCwa56374](#) - FMTツールがゾーンマッピングページでハングし、メモリ使用率が高い
- Cisco Bug ID [CSCvz88730](#) - FTDポートチャンネル管理インターフェイスタイプのインターフェイスプッシュ障害
- Cisco Bug ID [CSCvx21986](#) - ターゲットプラットフォームへのポートチャンネル移行 - 仮想FTDはサポートされていません
- Cisco Bug ID [CSCvy63003](#) - FTDがすでにクラスタに属している場合、移行ツールはインターフェイス機能を無効にする必要があります
- Cisco Bug ID [CSCvx08199](#) : アプリケーション参照が50を超える場合、ACLを分割する必要があります

関連情報

- [ファイアウォール移行ツールによるASAファイアウォールの脅威防御への移行](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)