

Configurazione di FTD dal file di configurazione ASA con lo strumento di migrazione Firepower

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Verifica](#)

[Bug noti relativi allo strumento di migrazione Firepower](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive un esempio di migrazione di Adaptive Security Appliance (ASA) a Firepower Threat Defense (FTD) su FPR4145.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di ASA
- Conoscenza di Firepower Management Center (FMC) e FTD

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

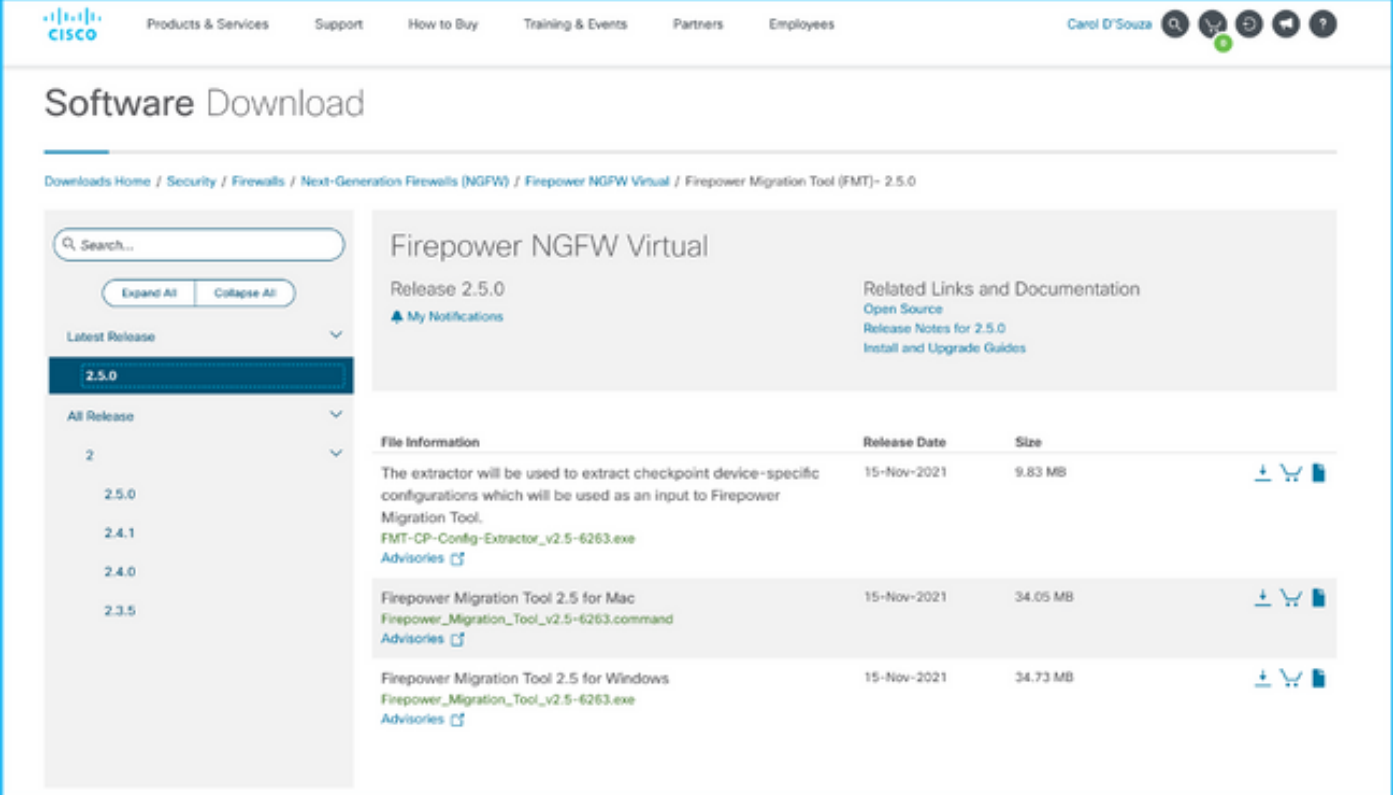
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Esportare il file di configurazione ASA in formato **.cfg** o **.txt**. Il CCP deve essere installato con un FTD registrato.

Configurazione

1. Scaricare Firepower Migration Tool da software.cisco.com come mostrato nell'immagine.



The screenshot shows the Cisco Software Download page for Firepower NGFW Virtual, Release 2.5.0. The page includes a search bar, a list of releases (2.5.0, 2.4.1, 2.4.0, 2.3.5), and a table of file information for the migration tool.

| 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 |

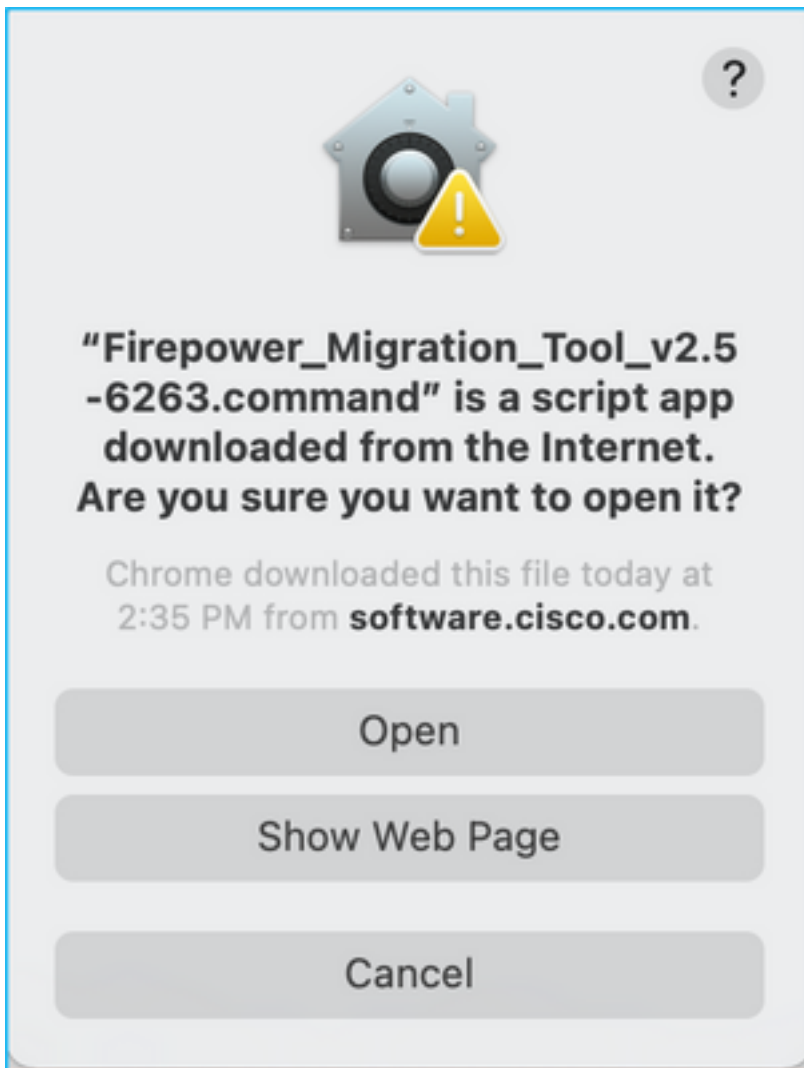
2. Esaminare e verificare i requisiti nella sezione [Linee guida e limitazioni](#) per lo strumento di migrazione Firepower.

3. Se si prevede di eseguire la migrazione di un file di configurazione di grandi dimensioni, configurare le impostazioni di sospensione in modo che il sistema non passi alla modalità sospensione durante un'operazione push di migrazione.

3.1. Per Windows, selezionare Opzioni risparmio energia nel Pannello di controllo. Fare clic su **Modifica impostazioni combinazione** accanto alla combinazione per il risparmio di energia corrente. Modifica **Sospensione computer** impostata su **Mai**. Fare clic su **Salva modifiche**.

3.2. Per MAC, passare a **Preferenze di sistema > Risparmio energetico**. Selezionare la casella accanto a per impedire che il computer si spenga automaticamente quando lo schermo è spento e trascinare **Spegni schermo** dopo il dispositivo di scorrimento su **Mai**.

Nota: Questo avviso viene visualizzato quando gli utenti MAC tentano di aprire il file scaricato. Ignorare l'avviso e seguire il passo 4 A.



4. A. Per MAC: utilizzare il terminale ed eseguire questi comandi.

```
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 HTTP/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. Per Windows - fare doppio clic su Firepower Migration Tool per avviarlo in un browser Google Chrome.

5. Accettare la licenza come illustrato nell'immagine.

← → ↻ 🏠 ⓘ 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 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

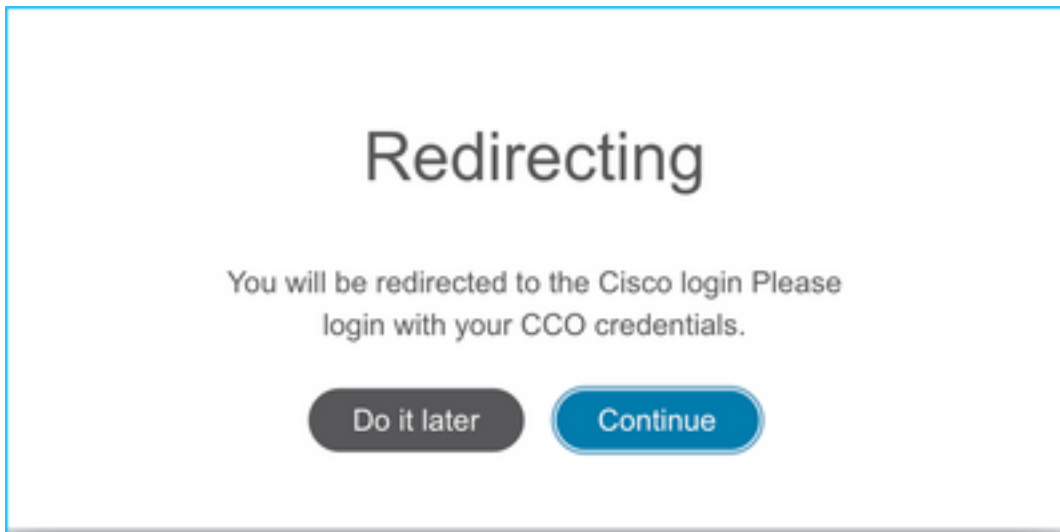
I have read the content of the EULA and SEULA and agree to terms listed.

Proceed

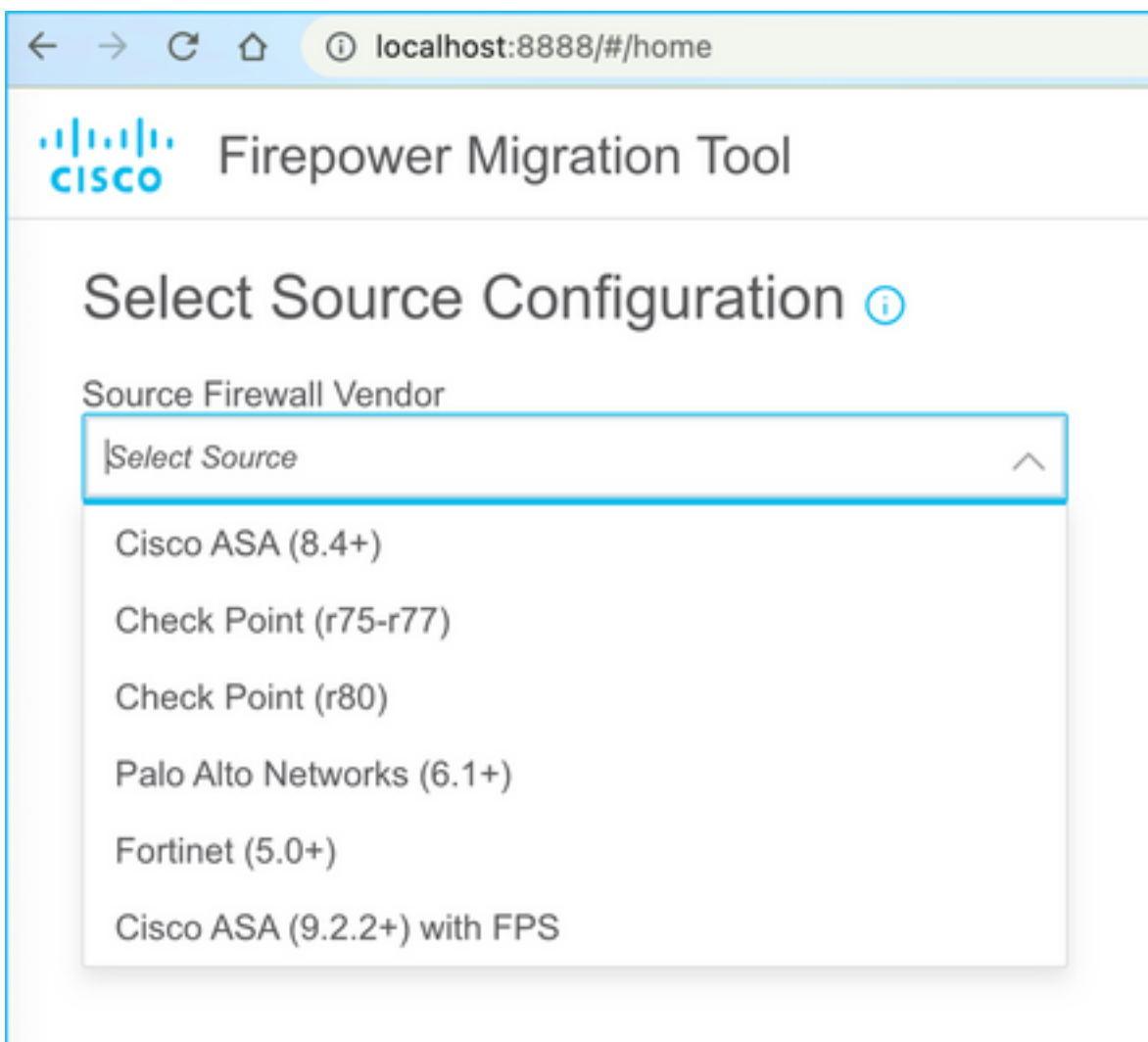
6. Nella pagina di accesso dello strumento di migrazione Firepower, fare clic sul collegamento di accesso con CCO per accedere all'account Cisco.com con le credenziali di accesso singolo.

Nota: Se non si dispone di un account Cisco.com, crearlo nella pagina di accesso

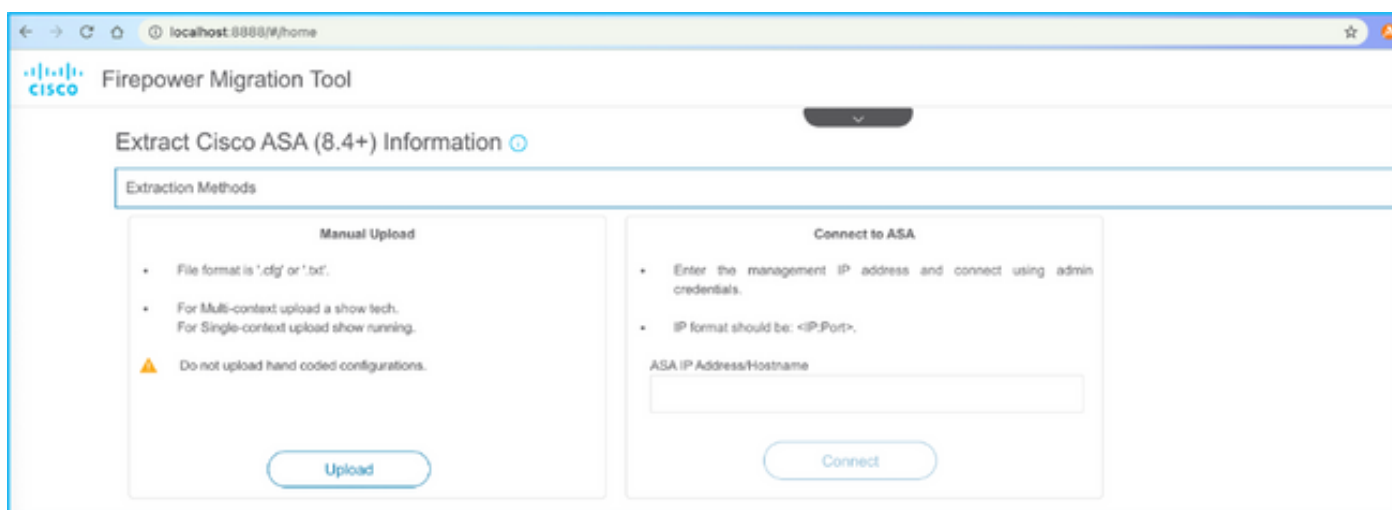
Cisco.com. Accedere con le credenziali predefinite seguenti: Nome utente—Password amministratore—Admin123.



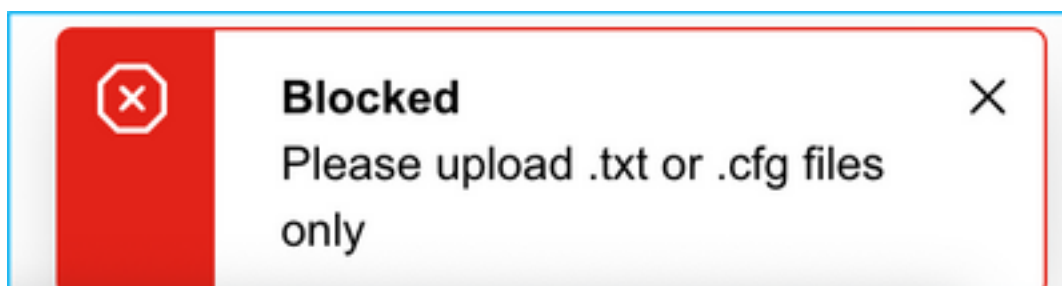
7. Selezionare la configurazione di origine. In questo scenario, è Cisco ASA (8.4+).



8. Se non si dispone della connettività all'appliance ASA, selezionare Caricamento manuale. In caso contrario, è possibile recuperare la configurazione in esecuzione dall'ASA e immettere i dettagli dell'IP di gestione e di accesso. In questo scenario, è stato eseguito un caricamento manuale.

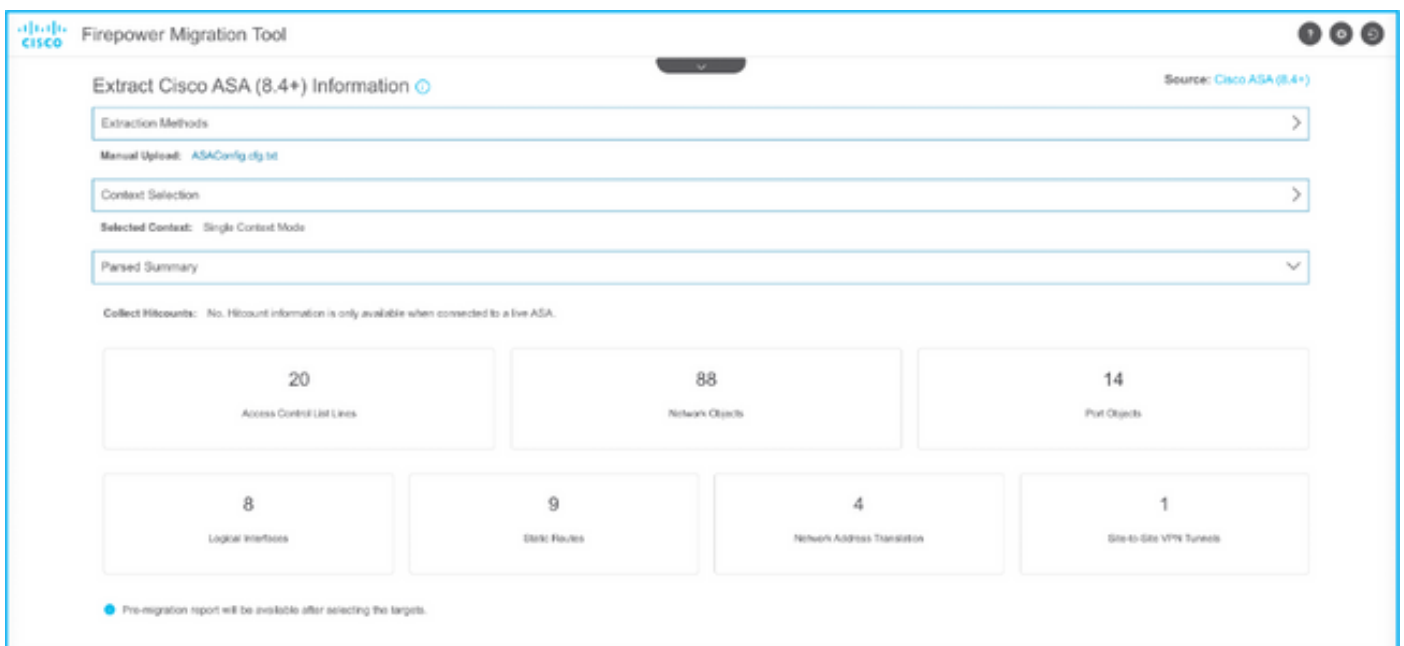


Nota: Questo errore viene visualizzato se il file non è supportato. Assicurarsi di modificare il formato in testo normale. (L'errore si verifica nonostante l'estensione .cfg).

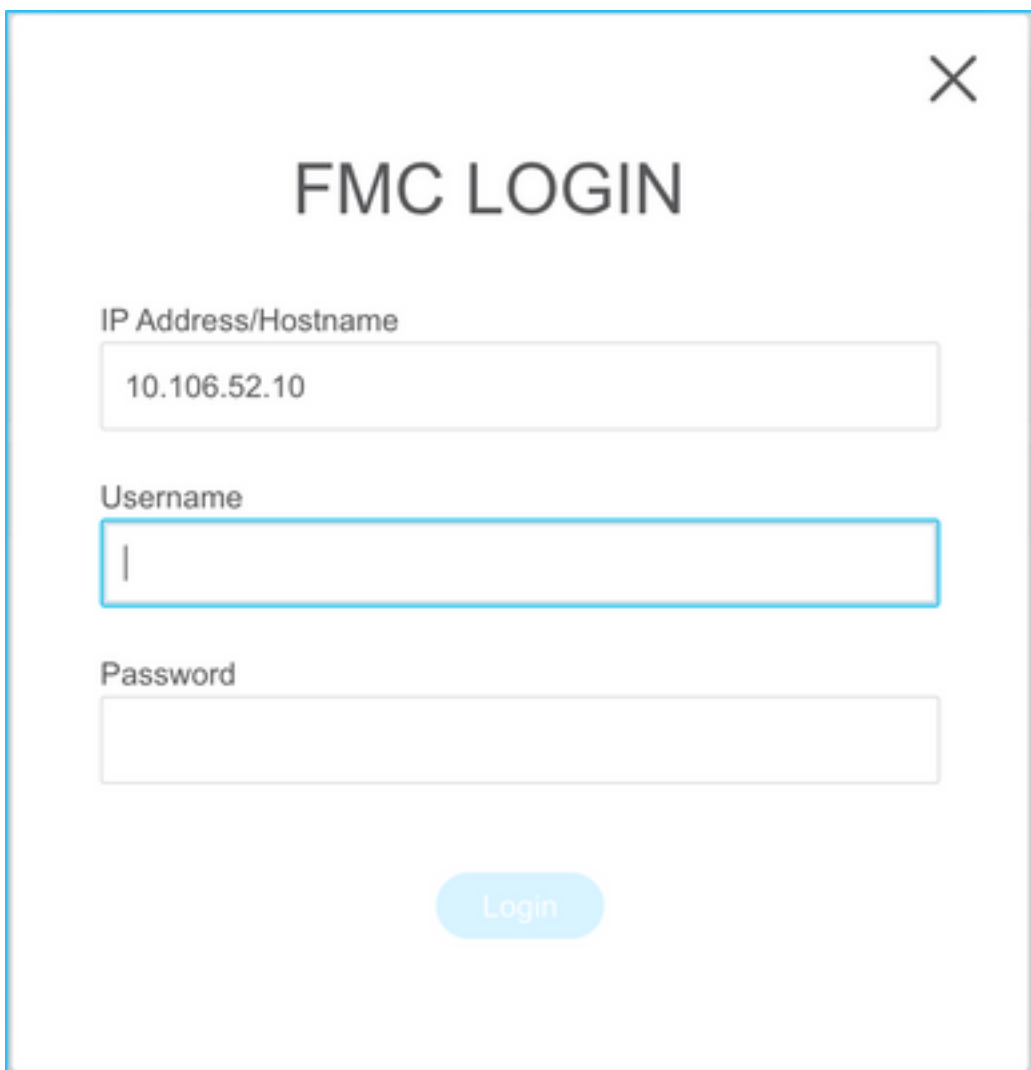
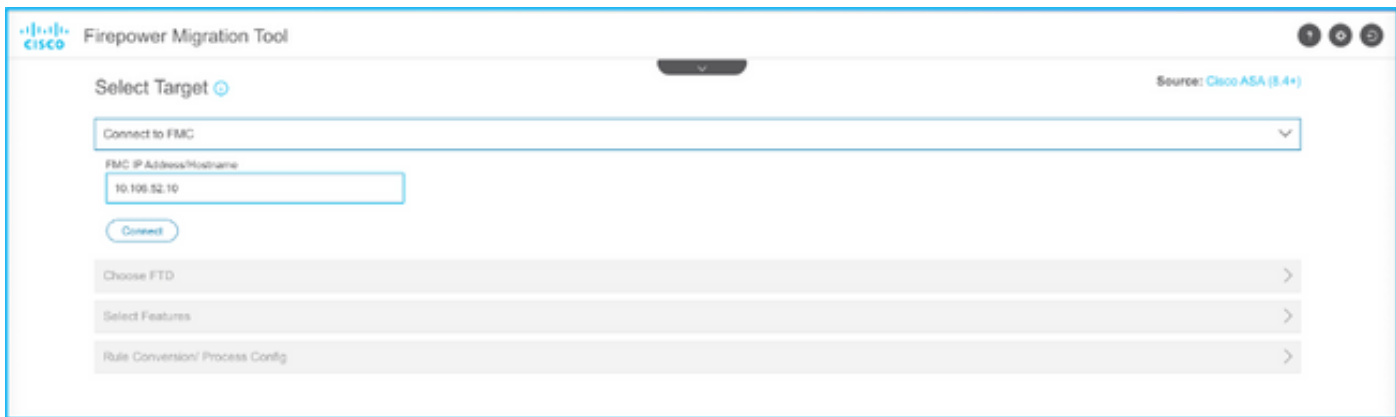


```
ASAConfig.cfg — Edited
asa# show running-config
: Saved
:
:
: Serial Number: FLM22160652
: Hardware: FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
:
ASA Version 9.12(2)
:
hostname asa
enable password ***** pbkdf2
:
license smart
feature tier standard
names
no mac-address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

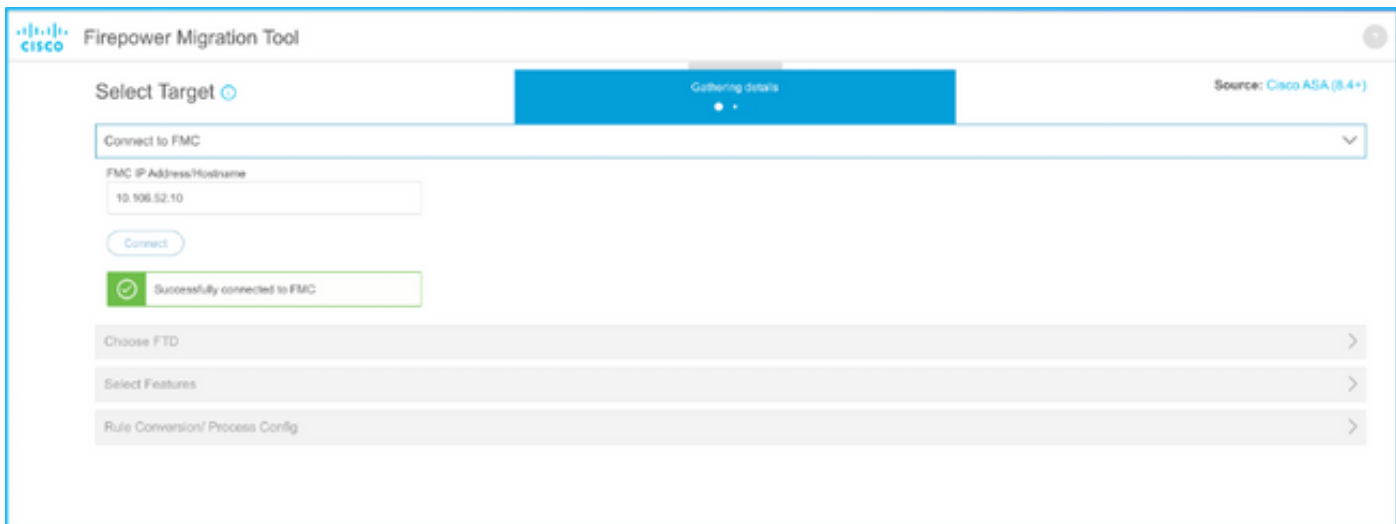
9. Una volta caricato il file, gli elementi vengono analizzati fornendo un riepilogo come mostrato nell'immagine:



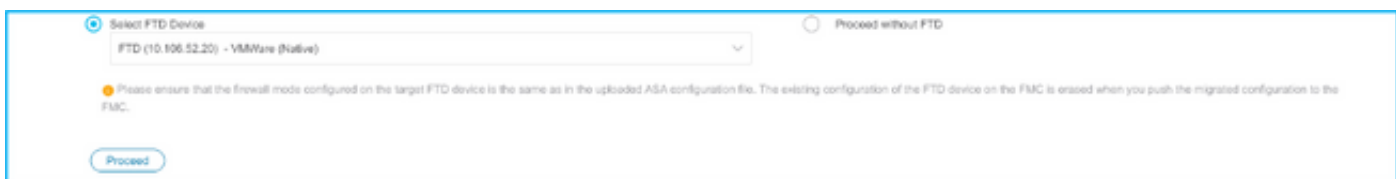
10. Immettere le credenziali di accesso e l'indirizzo IP del controller di dominio a cui migrare la configurazione ASA. Verificare che l'indirizzo IP del CCP sia raggiungibile dalla postazione di lavoro.



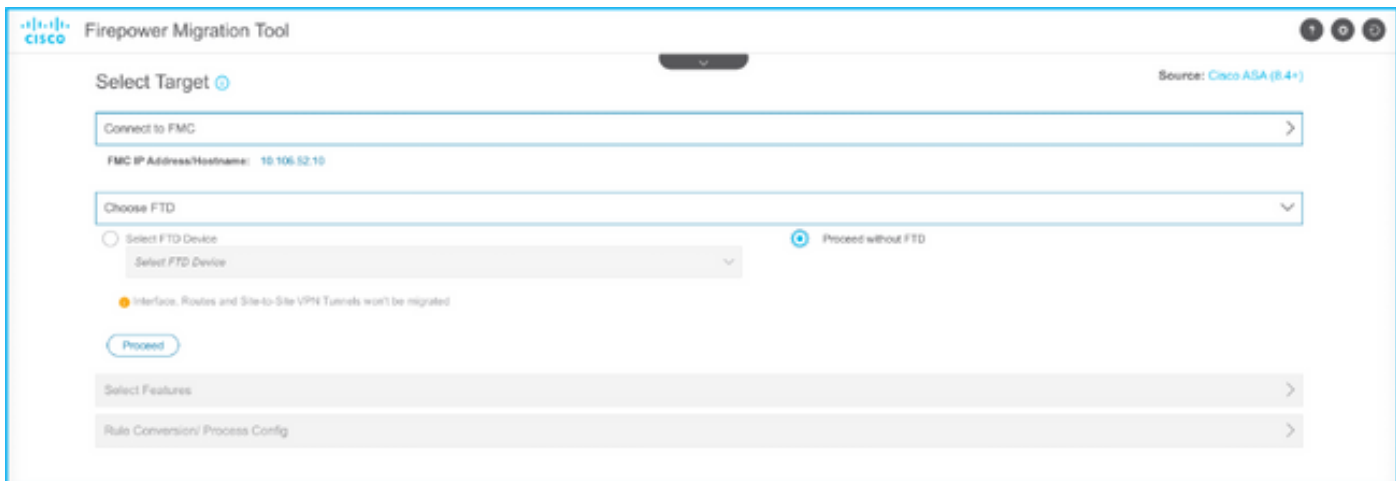
11. Una volta collegato il CCP, vengono visualizzati gli FTD gestiti al suo interno.



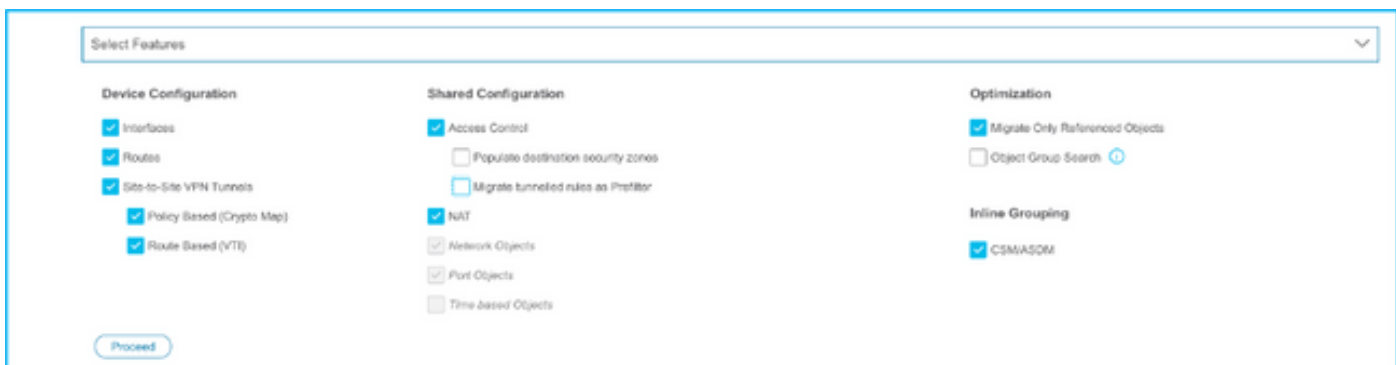
12. Scegliere l'FTD su cui eseguire la migrazione della configurazione ASA.



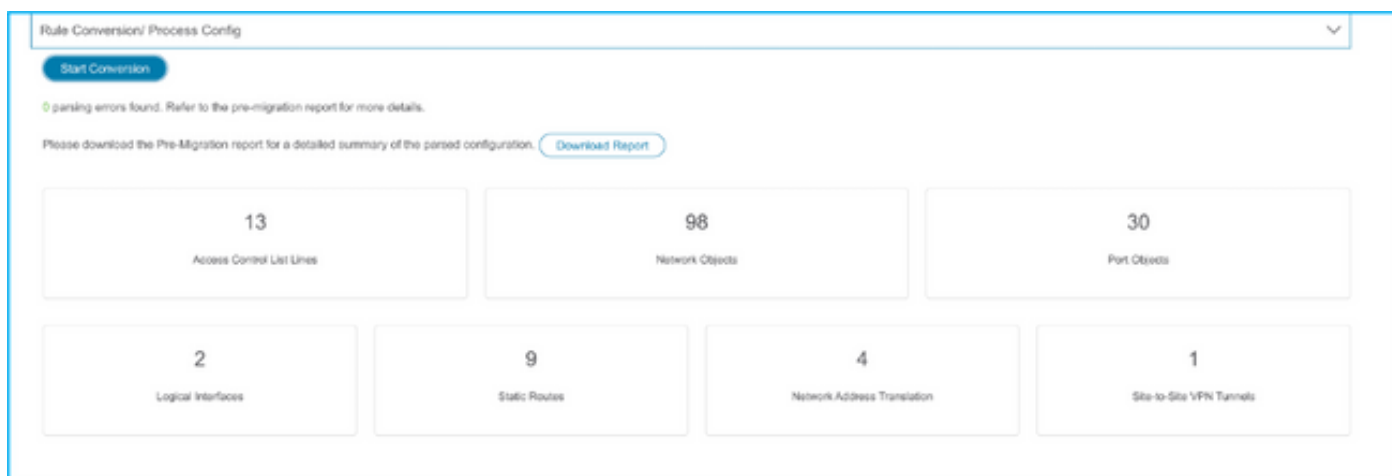
Nota: Si consiglia di selezionare il dispositivo FTD, altrimenti le interfacce, i percorsi e la configurazione della VPN da sito a sito dovranno essere eseguiti manualmente.



13. Selezionare le funzionalità da migrare, come illustrato nell'immagine.



14. Selezionare **Avvia conversione** per avviare la pre-migrazione che popolerà gli elementi relativi alla configurazione FTD.




The screenshot displays the 'Rule Conversion/ Process Config' interface. At the top, there is a 'Start Conversion' button. Below it, a message states '0 parsing errors found. Refer to the pre-migration report for more details.' A 'Download Report' button is also visible. The main area contains seven summary cards for different configuration elements:

| Element | Count |
|-----------------------------|-------|
| Access Control List Lines | 13 |
| Network Objects | 98 |
| Port Objects | 30 |
| Logical Interfaces | 2 |
| Static Routes | 9 |
| Network Address Translation | 4 |
| Site-to-Site VPN Tunnels | 1 |

15. Fare clic su **Scarica report** visualizzato in precedenza per visualizzare il report di pre-migrazione, come mostrato nell'immagine.

← → ↻ 🏠 📄 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 |

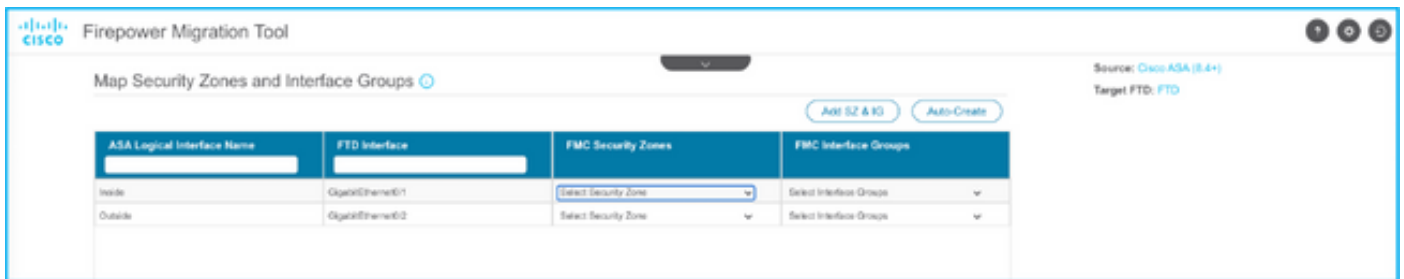
Note: ACEs that are applied outbound or not attached to interfaces using the access-group command are ignored.

16. Mappare le interfacce ASA alle interfacce FTD come richiesto, come mostrato nell'immagine.

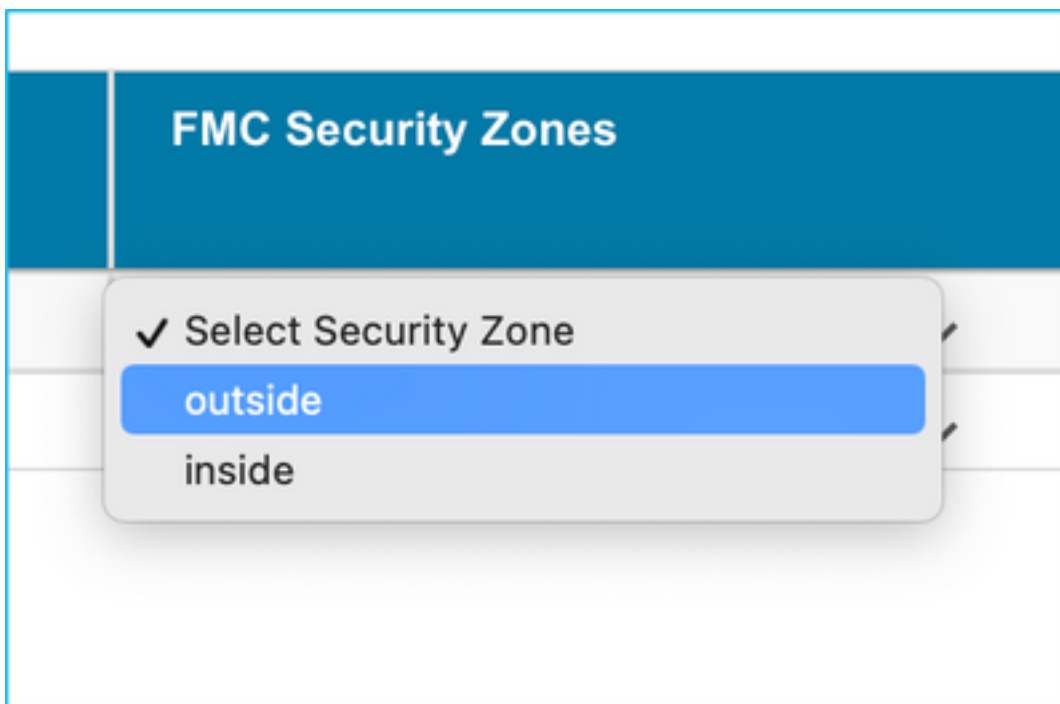
Refresh

| ASA Interface Name | FTD Interface Name |
|----------------------|----------------------|
| <input type="text"/> | Select Interface |
| Ethernet1/2 | GigabitEthernet0/0 |
| Ethernet1/3 | GigabitEthernet0/1 |
| | ✓ GigabitEthernet0/2 |

17. Assegnare zone di sicurezza e gruppi di interfacce alle interfacce FTD.



R. Se nel CCP sono già state create zone di sicurezza e gruppi di interfacce, è possibile selezionarli in base alle esigenze:



B. Se è necessario creare aree di sicurezza e un gruppo di interfacce, fare clic su **Add SZ & IG** come mostrato nell'immagine.

✕

Add SZ & IG

Security Zones (SZ) **Interface Groups (IG)**

Add

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

| Interface Groups | Type | Actions |
|--|--------|---|
| <input style="width: 100%;" type="text" value="Inside"/> | ROUTED | ✕ ✓ |

0 - 0 of 0 |< < > >|

Close

C. In caso contrario, selezionare l'opzione **Auto-Create** per creare le zone di sicurezza e i gruppi di interfacce denominati rispettivamente **ASA logical interface_sz** e **ASA logical interface_ig**.

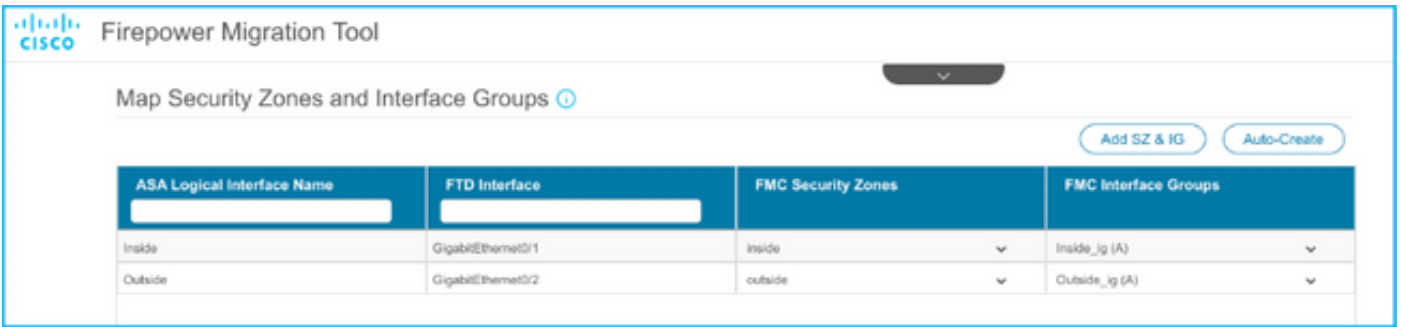
Auto-Create

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.

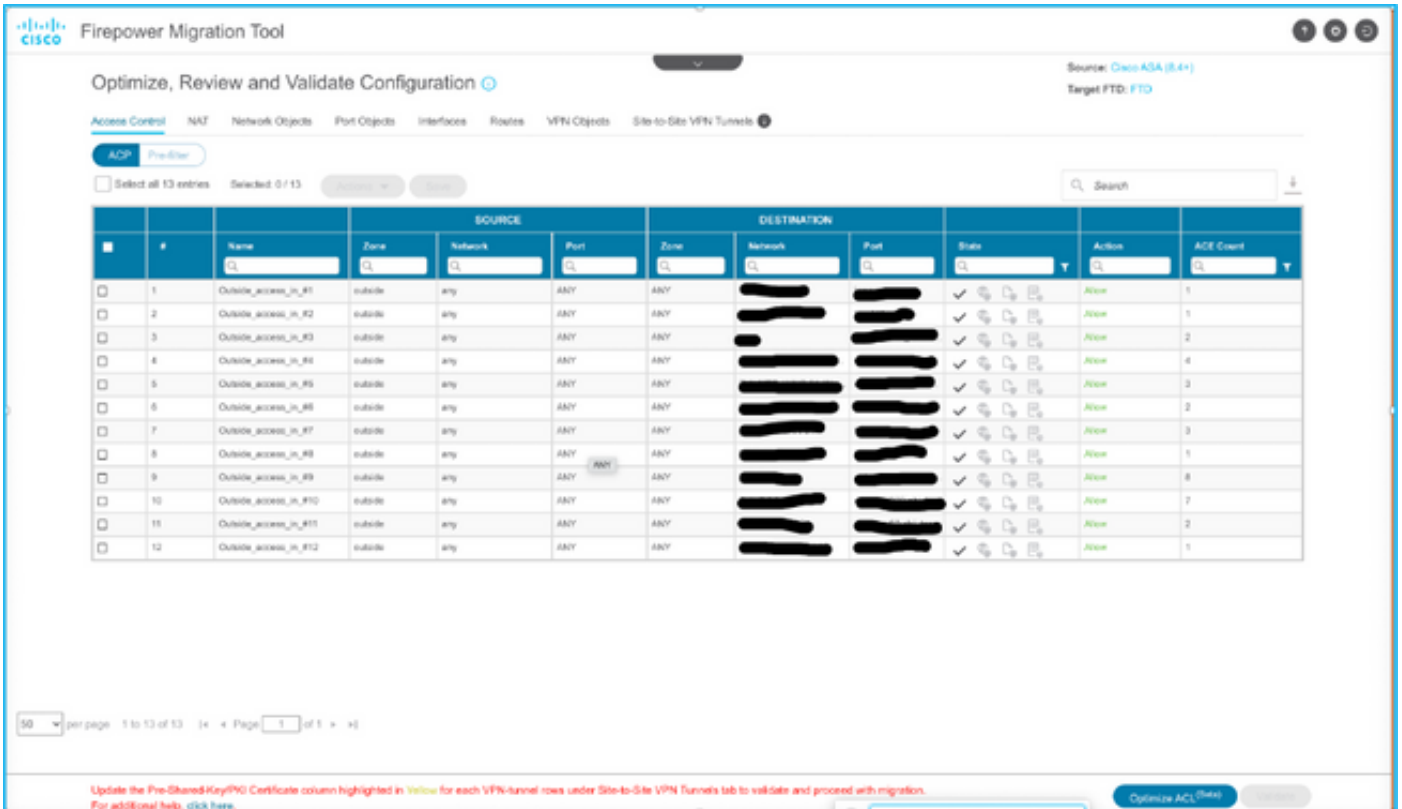
Select the objects that you want to map to ASA interfaces

Security Zones Interface Groups

CancelAuto-Create



18. Esaminare e convalidare ogni elemento FTD creato. Gli avvisi vengono visualizzati in rosso, come mostrato nell'immagine.



19. Le azioni di migrazione possono essere selezionate come mostrato nell'immagine se si desidera modificare qualsiasi regola. In questa fase è possibile aggiungere funzioni FTD e criteri IPS.

ACP Pre-filter

Select all 13 entries Selected: 13 / 13 Actions Save

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

Nota: Se i criteri file esistono già nel FMC, verranno popolati come illustrato nell'immagine. Lo stesso vale per i criteri IPS e i criteri predefiniti.

✕

File Policy

Select File Policy *

^

eicar

None

Cancel
Select

È possibile eseguire la configurazione del registro per le regole richieste. In questa fase è possibile selezionare la configurazione del server Syslog esistente nel FMC.

20. Analogamente, NAT, oggetto di rete, oggetti porta, interfacce, route, oggetti VPN, tunnel VPN da sito a sito e altri elementi in base alla configurazione possono essere rivisti passo dopo passo.

Nota: L'avviso viene notificato come mostrato nell'immagine per aggiornare la chiave già condivisa, in quanto non viene copiata nel file di configurazione dell'ASA. Selezionare **Azioni** > **Aggiorna chiave già condivisa** per immettere il valore.

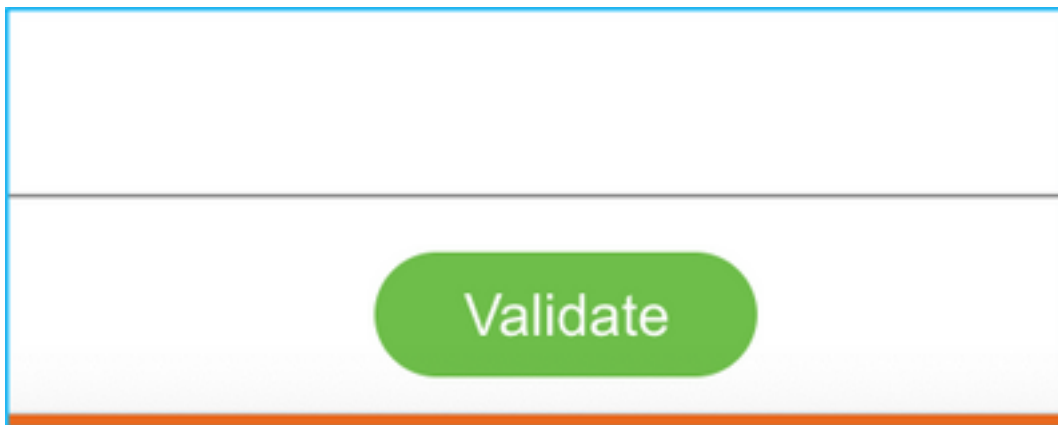
| # | Source Interface N... | Peer IP | IKE | IKEv1/IKEv2 P... | IKEv1/IKEv2 PSEC P... | Auth-entication Type | Protected Networks |
|---|-----------------------|---------|-------|---------------------|------------------------|-------------------------|-----------------------------|
| 1 | Outside | dynamic | Ikev2 | asa_ikev2_psk_key_1 | AES256AES192AES30ES... | Pre-shar... PKI Cert... | Source Net... Remote Net... |

Update Pre-Shared Key

Pre-Shared Key IKEv2

Cancel Save

21. Infine, fare clic sull'icona **Convalida** nella parte inferiore destra della schermata, come mostrato nell'immagine.



22. Una volta completata la convalida, fare clic su **Push Configuration** (Configurazione push) come mostrato nell'immagine.

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 |

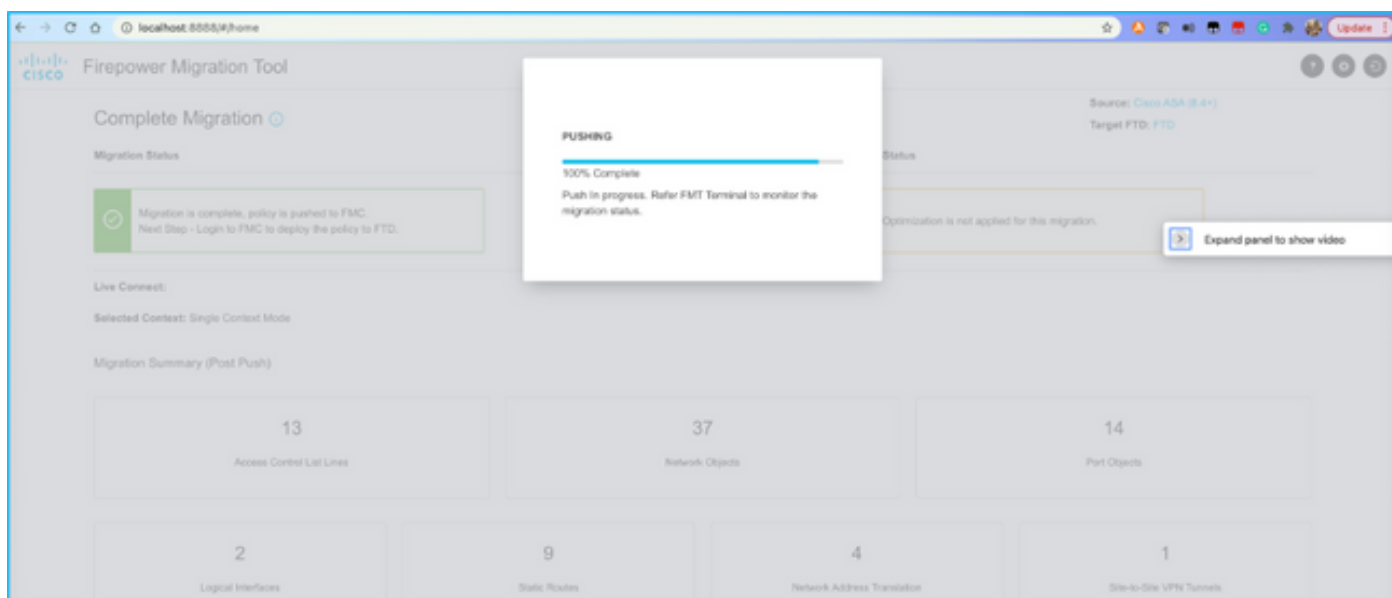
Note: The configuration on the target FTD device FTD (10.106.52.20) will be overwritten as part of this migration.

Push Configuration

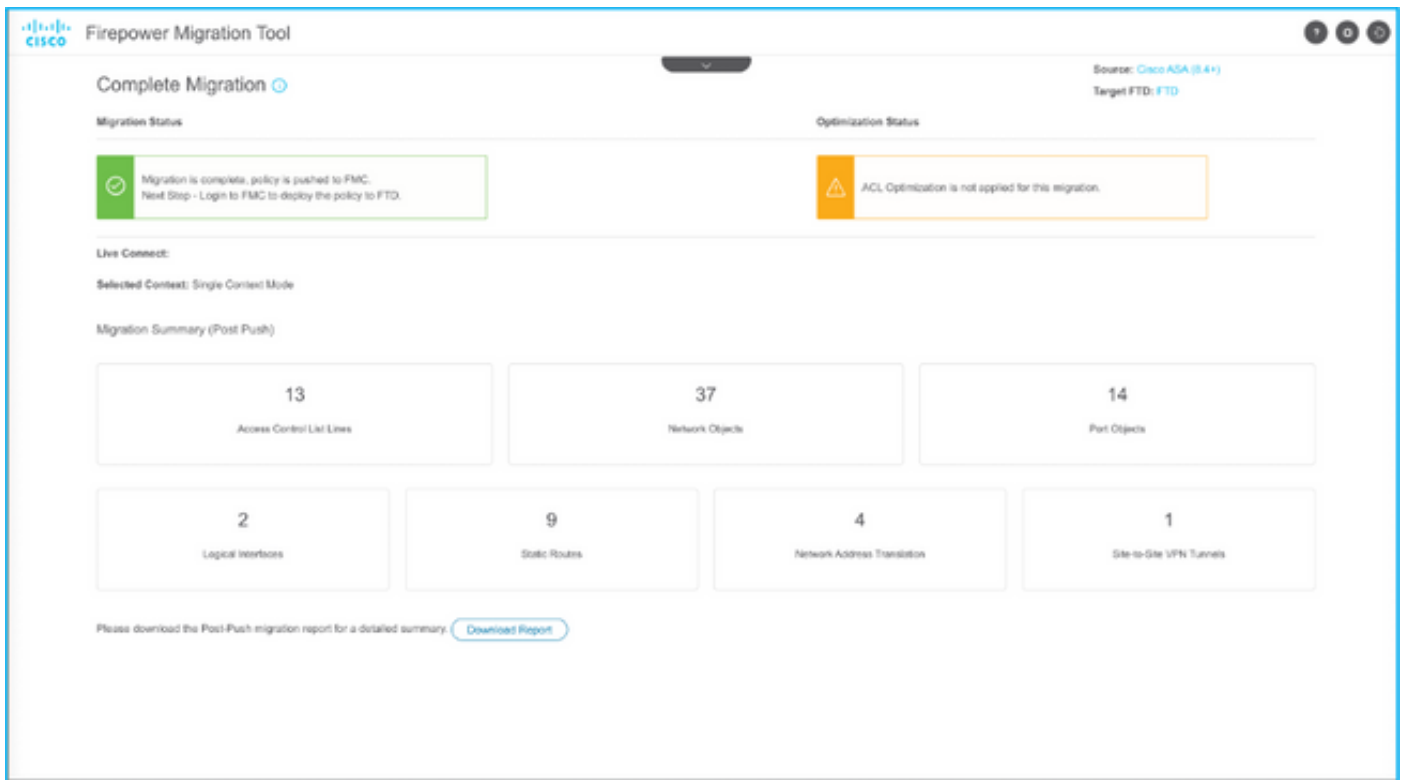
PUSHING

0% Complete

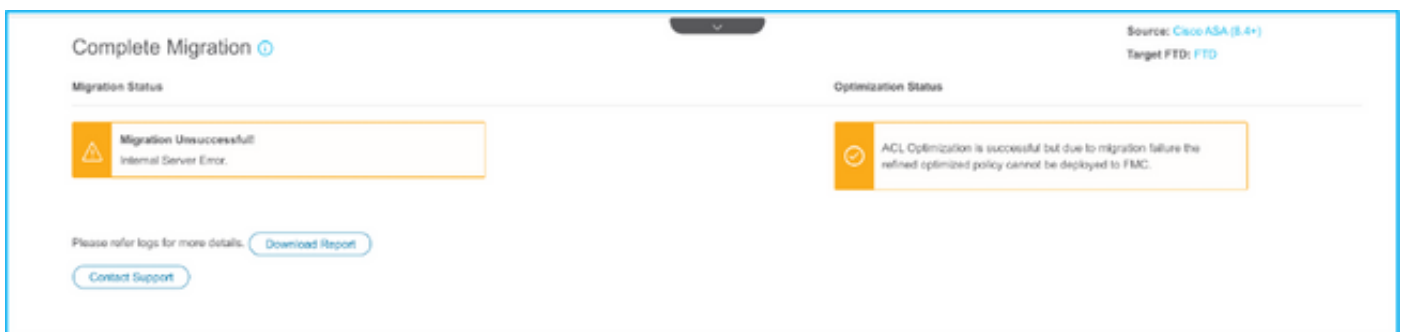
Push In progress. Refer FMT Terminal to monitor the migration status.



23. Una volta completata la migrazione, il messaggio visualizzato viene visualizzato nell'immagine.



Nota: Se la migrazione non riesce, fare clic su **Scarica report** per visualizzare il report di post-migrazione.

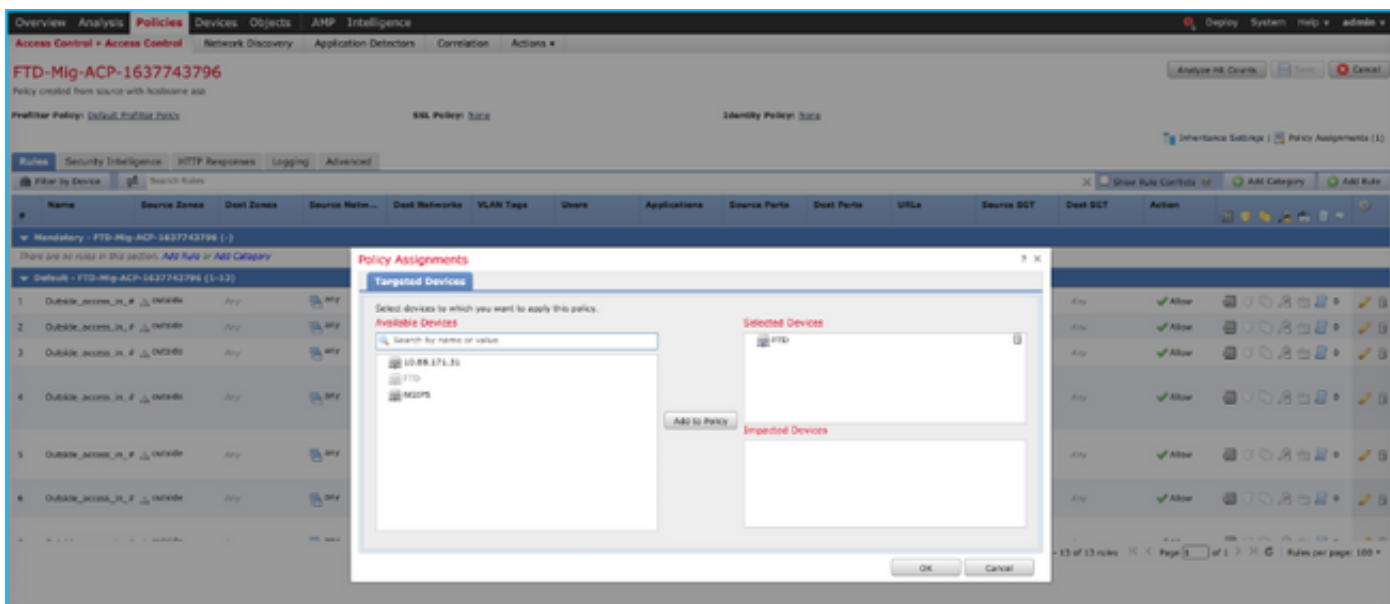


Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

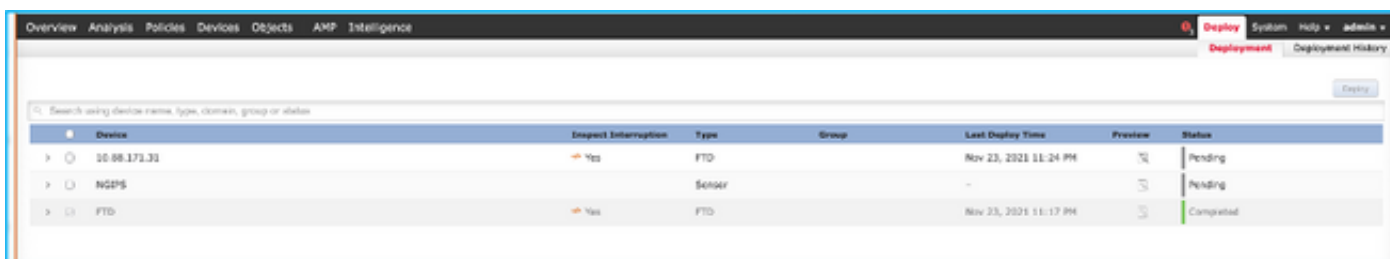
Convalida sul CCP.

1. Per verificare che l'FTD selezionato sia compilato, selezionare **Criteri > Controllo di accesso > Criteri di controllo di accesso > Assegnazione criteri**.



Nota: Il criterio di controllo dell'accesso alla migrazione dovrebbe avere un nome con il prefisso **FTD-Mig-ACP**. Se al punto 2.8 non è stato selezionato alcun FTD, l'FTD deve essere selezionato sul CCP.

2. Spostare il criterio nell'FTD. Passare a **Distribuisce > Distribuzione > Nome FTD > Distribuisce** come mostrato nell'immagine.



Bug noti relativi allo strumento di migrazione Firepower

- ID bug Cisco [CSCwa56374](#) - Lo strumento FMT si blocca sulla pagina di mappatura della zona a causa di un errore dovuto all'elevato utilizzo della memoria
- Cisco ID bug [CSCvz88730](#) - Errore di push dell'interfaccia per il tipo di interfaccia di gestione del canale della porta FTD
- ID bug Cisco [CSCvx21986](#) - Migrazione porta-canale alla piattaforma di destinazione - FTD virtuale non supportato
- ID bug Cisco [CSCvy63003](#) - Lo strumento di migrazione deve disabilitare la funzione di interfaccia se FTD fa già parte del cluster
- ID bug Cisco [CSCvx08199](#) - È necessario suddividere l'ACL quando il riferimento all'applicazione è superiore a 50

Informazioni correlate

- [Migrazione di ASA Firewall a Threat Defense con lo strumento di migrazione del firewall](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)