

# Migrazione da ASA a Firepower Threat Defense (FTD) con FMT

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Panoramica](#)

[Premesse](#)

[Recupero del file di configurazione ASA](#)

[Esporta certificato PKI da ASA e importa in Management Center](#)

[Recupero di pacchetti e profili AnyConnect](#)

[Configurazione](#)

[Procedura di configurazione:](#)

[Risoluzione dei problemi](#)

[Strumento di risoluzione dei problemi di migrazione Secure Firewall](#)

---

## Introduzione

In questo documento viene descritta la procedura per eseguire la migrazione di Cisco Adaptive Security Appliance (ASA) a Cisco Firepower Threat Device.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza di Cisco Firewall Threat Defense (FTD) e Adaptive Security Appliance (ASA).

### Componenti usati

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

- Mac OS con Firepower Migration Tool (FMT) versione 7.0.1
- Adaptive Security Appliance (ASA) v9.16(1)
- Secure Firewall Management Center (FMCv) v7.4.2
- Secure Firewall Threat Defense Virtual (FTDv) v7.4.1

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.

## Panoramica

I requisiti specifici per questo documento includono:

- Cisco Adaptive Security Appliance (ASA) versione 8.4 o successive
- Secure Firewall Management Center (FMCv) versione 6.2.3 o successiva

Lo strumento di migrazione del firewall supporta questo elenco di dispositivi:

- Cisco ASA (8.4+)
  - Cisco ASA (9.2.2+) con FPS
  - Cisco Secure Firewall Device Manager (7.2+)
  - Punto di controllo (r75-r77)
  - Punto di controllo (r80)
  - Fortinet (5.0+)
- Palo Alto Networks (6.1+)

## Premesse

Prima di migrare la configurazione ASA, eseguire le seguenti attività:

### Recupero del file di configurazione ASA

Per eseguire la migrazione di un dispositivo ASA, usare il comando `show running-config` per un singolo contesto o `show tech-support` per la modalità multi-contesto per ottenere la configurazione, salvarla come file con estensione `cfg` o `txt` e trasferirla sul computer con lo strumento di migrazione Secure Firewall.

### Esporta certificato PKI da ASA e importa in Management Center

Utilizzare questo comando per esportare il certificato PKI dalla CLI della configurazione ASA di origine con le chiavi in un file PKCS12:

```
ASA(config)#crypto può esportare <nome-trust-point> pkcs12 <passphrase>
```

Importare quindi il certificato PKI in un centro di gestione (Oggetti PKI Gestione oggetti). Per ulteriori informazioni, vedere Oggetti PKI nella [Guida alla configurazione di Firepower Management Center](#).

### Recupero di pacchetti e profili AnyConnect

I profili AnyConnect sono facoltativi e possono essere caricati tramite il centro di gestione o lo strumento di migrazione Secure Firewall.

Utilizzare questo comando per copiare il pacchetto richiesto dall'appliance ASA di origine su un server FTP o TFTP:

```
Copy <percorso file di origine:/nome file di origine> <destinazione>
```

```
ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 ← Esempio di copia di Anyconnect Package.
```

```
ASA# copy disk0:/ external-ss0- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 ← Esempio di copia di un pacchetto del browser esterno.
```

```
ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 ← Esempio di copia di Hostscan Package.
```

```
ASA# copy disk0:/ dap.xml tftp://1.1.1.1. ← Esempio di copia di Dap.xml
```

```
ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 ← Esempio di copia di Data.xml
```

```
ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 ← Esempio di copia di un profilo Anyconnect.
```

Importare i pacchetti scaricati nel centro di gestione (Gestione oggetti > VPN > File AnyConnect).

a-Dap.xml e Data.xml devono essere caricati nel centro di gestione dallo strumento di migrazione Secure Firewall nella sezione Verifica e convalida > VPN ad accesso remoto > File AnyConnect.

I profili b-AnyConnect possono essere caricati direttamente nel centro di gestione o tramite lo strumento di migrazione Secure Firewall nella sezione Revisione e convalida > VPN ad accesso remoto > File AnyConnect.

## Configurazione

Procedura di configurazione:

1. Scarica l'ultima versione di Firepower Migration Tool da Cisco Software Central:

# Software Download

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

Expand All Collapse All

Latest Release ▼

7.0.1

All Release ▼

7 ▼

7.0.1

7.0.0

## Secure Firewall Migration Tool

Release 7.0.0

[My Notifications](#)

Related Links and Documentation

[Open Source](#)

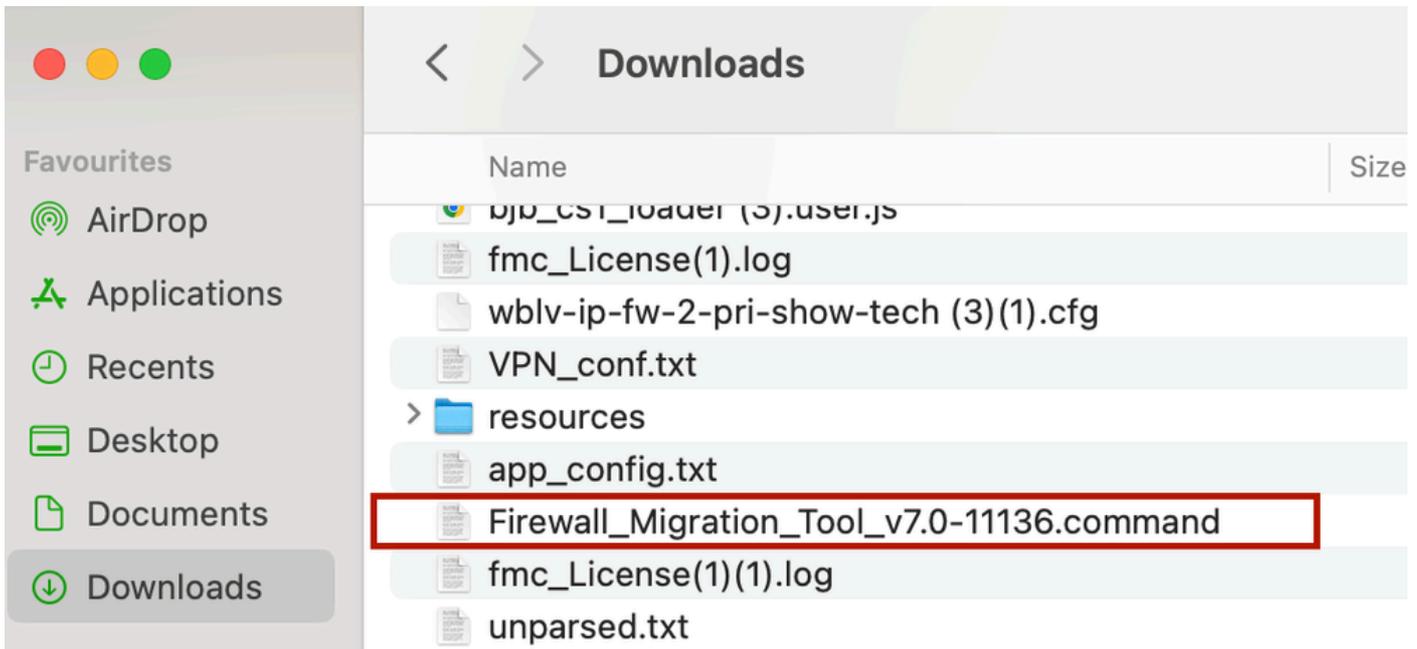
[Release Notes for 7.0.0](#)

[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 <a href="#">Advisories</a>	04-Sep-2024	41.57 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>
Firewall Migration Tool 7.0.0.1 for Windows Firewall_Migration_Tool_v7.0.0.1-11241.exe <a href="#">Advisories</a>	04-Sep-2024	39.64 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>
Firewall Migration Tool 7.0.0 for Mac Firewall_Migration_Tool_v7.0-11136.command <a href="#">Advisories</a>	05-Aug-2024	41.55 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>
Firewall Migration Tool 7.0.0 for Windows Firewall_Migration_Tool_v7.0-11136.exe <a href="#">Advisories</a>	05-Aug-2024	39.33 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>

Download del software

2. Fare clic sul file scaricato in precedenza sul computer.



Il file

```
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 -
```



Nota: Il programma si apre automaticamente e una console genera automaticamente il contenuto nella directory in cui è stato eseguito il file.

- 
3. Dopo l'esecuzione del programma, viene aperto un browser Web che visualizza il "Contratto di licenza con l'utente finale".
    1. Selezionare la casella di controllo per accettare termini e condizioni.
    2. Fare clic su Continua.

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 specific product terms at [www.cisco.com/go/software/terms](http://www.cisco.com/go/software/terms) (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. It makes no warranty, no applicable law. You are not licensed to Use the

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

Proceed

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. Effettuare l'accesso con un account CCO valido e l'interfaccia GUI FMT viene visualizzata sul browser Web.



## Security Cloud Sign On

Email

Continue

Don't have an account? [Sign up now](#)

Or

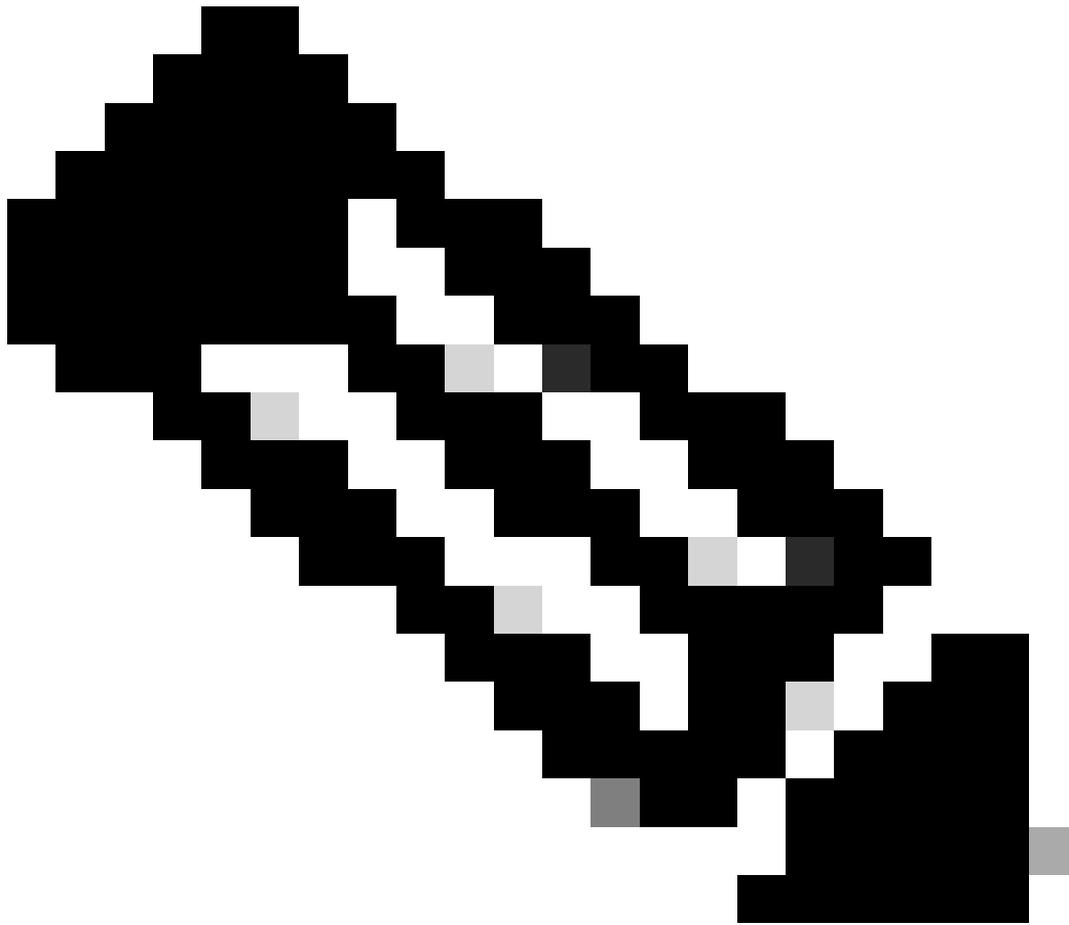
[Other login options](#)

[System status](#) [Policy statement](#)

Accesso FMT

5. Selezionare il firewall di origine da migrare.





Nota: Per questo esempio, connettersi direttamente all'appliance ASA.

- 
7. Un riepilogo della configurazione rilevata sul firewall viene visualizzato come dashboard. Fare clic su Avanti.

## Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

Extraction Methods &gt;

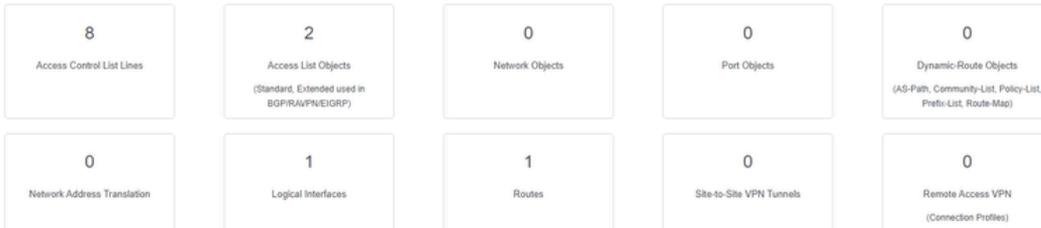
ASA IP Address: 192.168.1.20

Context Selection &gt;

Single Context Mode: Download config

Parsed Summary v

Collect Hitcounts: No



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

<https://cisco.com>

Back

Next

Riepilogo

8. Selezionare il CCP di destinazione da utilizzare per la migrazione.

Fornire l'indirizzo IP del CCP. Verrà aperta una finestra popup in cui verranno richieste le credenziali di accesso del CCP.

## Select Target

Source: Cisco ASA (8.4+)

Firewall Management v

 On-Prem/Virtual FMC Cloud-delivered FMC

FMC IP Address/Hostname

192.168.1.18

Connect

1 FTD(s) Found

Proceed

 Successfully connected to FMC

Choose FTD &gt;

Select Features &gt;

Rule Conversion/ Process Config &gt;

Back

Next

IP FMC

9. (Facoltativo) Selezionare l'FTD di destinazione che si desidera utilizzare.

1. Se si sceglie di eseguire la migrazione a un FTD, selezionare l'FTD che si desidera utilizzare.
2. Se non si desidera utilizzare un FTD, è possibile compilare la casella di controllo Proceed

without FTD

Firewall Migration Tool

Source: Cisco ASA (8.4+)

Select Target

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

Back Next

FTD destinazione

10. Selezionare le configurazioni di cui si desidera eseguire la migrazione. Le opzioni vengono visualizzate negli screenshot.

Firewall Migration Tool

Source: Cisco ASA (8.4+)

Select Target

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

**Device Configuration**

- Interfaces
- Routes
  - Static
  - BGP
  - EIGRP
- Site-to-Site VPN Tunnels (no data)
- Policy Based (Crypto Map)
- Route Based (VTI)

**Shared Configuration**

- Access Control
  - Populate destination security zones
    - Route-lookup logic is limited to Static Routes and Connected Routes. PBR, Dynamic-Routes & NAT are not considered.
  - Migrate tunnelled rules as Prefilter
- NAT (no data)
- Network Objects (no data)
- Port Objects (no data)
- Access List Objects(Standard, Extended)
- Time based Objects (no data)
- Remote Access VPN

Remote Access VPN migration is supported on FMC/FTD 7.2 and above.

**Optimization**

- Migrate Only Referenced Objects
- Object Group Search

**Inline Grouping**

- CSM/ASDM

Proceed

Back Next

Configurazioni

11. Avviare la conversione delle configurazioni da ASA a FTD.



Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

Rule Conversion/ Process Config

Start Conversion

Back Next

Avvia conversione

12. Al termine della conversione, viene visualizzato un dashboard con il riepilogo degli oggetti da migrare (limitato alla compatibilità).

1. Se lo si desidera, è possibile fare clic su **Download Report** per ricevere un riepilogo delle configurazioni da migrare.

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

Rule Conversion/ Process Config

Start Conversion

0 parsing errors found. Refer to the pre-migration report for more details.

Please download the Pre-Migration report for a detailed summary of the parsed configuration. [Download Report](#)

0 Access Control List Lines	0 Access List Objects <small>(Standard, Extended used in BGP/RAVP/NEIGRP)</small>	1 Network Objects	0 Port Objects	0 Dynamic-Route Objects <small>(AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)</small>
0 Network-Address Translation	1 Logical Interfaces	1 Routes	0 Site-to-Site VPN Tunnels	0 Remote Access VPN <small>(Connection Profiles)</small>

Back Next

Scarica rapporto

Esempio di report pre-migrazione, come mostrato nell'immagine:

**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	ASA; 2048 MB RAM, CPU Xeon 4100 6100 8100 series 2200 MHz
Hat 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

Report pre-migrazione

13. Mappare le interfacce ASA con le interfacce FTD sullo strumento di migrazione.

Firewall Migration Tool

Map FTD Interface

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

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

20 per page 1 to 1 of 1 Page 1 of 1

Back Next

Mapping interfacce

14. Creare le aree di sicurezza e i gruppi di interfacce per le interfacce sull'FTD

Map Security Zones and Interface Groups

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

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

10 per page 1 to 1 of 1 |< < Page 1 of 1 > >|

Back Next

Aree di sicurezza e gruppi di interfaccia

Le aree di sicurezza (SZ) e i gruppi di interfaccia (IG) vengono creati automaticamente dallo strumento, come mostrato nell'immagine:



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_lg (A)

10 per page 1 to 1 of 1 |< < Page 1 of 1 > >|

Back Next

Crea automaticamente, strumento

15. Rivedere e convalidare le configurazioni da migrare sullo strumento di migrazione.

1. Se l'analisi e l'ottimizzazione delle configurazioni sono già state completate, fare clic **SU**Validate.



### Optimize, Review and Validate Configuration

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

Access Control **Objects** NAT Interfaces Routes Site-to-Site VPN Tunnels Remote Access VPN

Access List Objects **Network Objects** Port Objects VPN Objects Dynamic-Route Objects

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

Validate

Verifica e convalida

16. Se lo stato di convalida ha esito positivo, eseguire il push delle configurazioni nei dispositivi di destinazione.

**Validation Status**

Successfully Validated

Validation Summary (Pre-push)

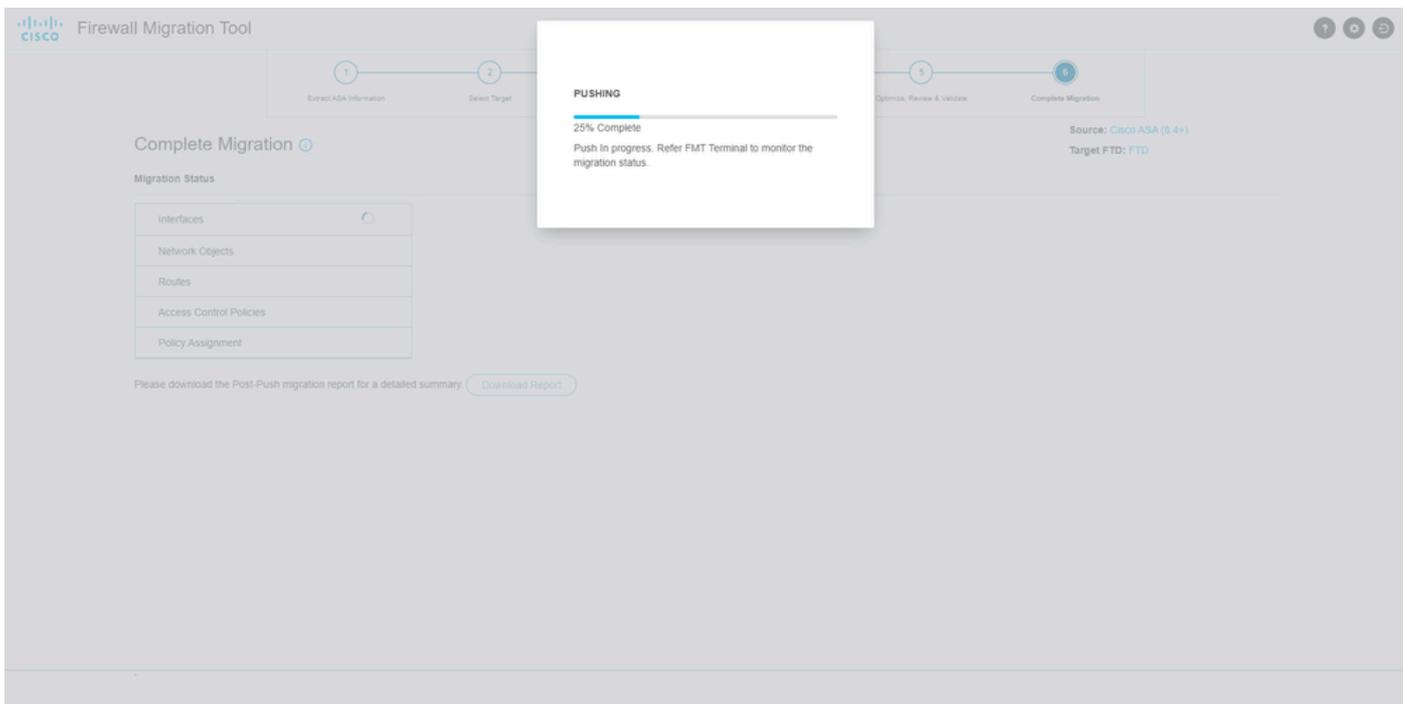
0	Not selected for migration Access Control List Lines Access List Objects (Standard, Extended used in BGP/RAVP/VEIGRP)	1	Not selected for migration Network Objects	Not selected for migration Port Objects	Not selected for migration Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
Not selected for migration Network Address Transl...	1 Logical Interfaces	1 Routes	Not selected for migration Site-to-Site VPN Tunnels	Not selected for migration Remote Access VPN (Connection Profiles)	

Note: The configuration on the target FTD device FTD (192.168.1.17) will be overwritten as part of this migration.

Push Configuration

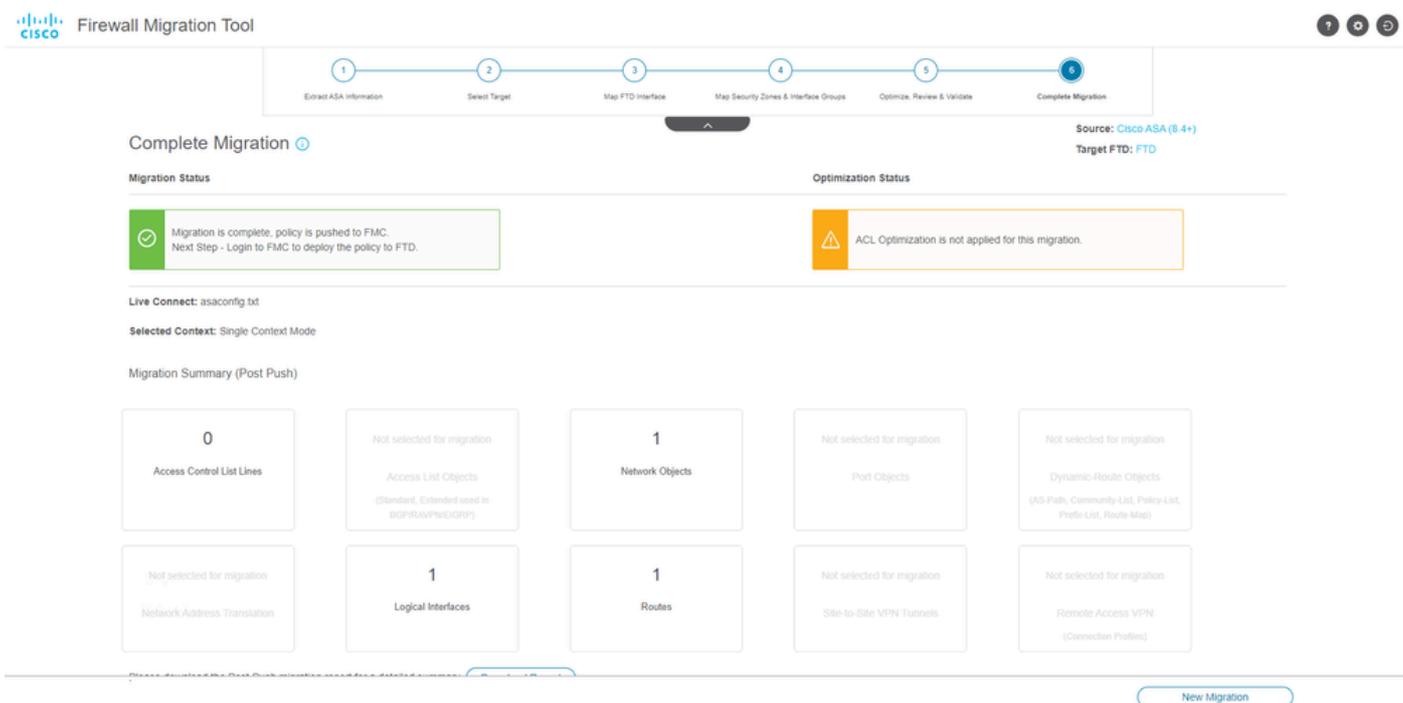
Convalida

Esempio di configurazione sottoposta a push tramite lo strumento di migrazione, come mostrato nell'immagine:



Spingi

Esempio di migrazione riuscita, come mostrato nell'immagine:



Migrazione completata

(Facoltativo) Se si è scelto di eseguire la migrazione della configurazione in un FTD, è necessaria una distribuzione per eseguire il push della configurazione disponibile dal FMC al firewall.

Per distribuire la configurazione:

1. Accedere alla GUI del CCP.
2. Passare alla `Deploy` scheda.

3. Selezionare la distribuzione per eseguire il push della configurazione nel firewall.
4. Fare clic su `. Deploy`

## Risoluzione dei problemi

### Strumento di risoluzione dei problemi di migrazione Secure Firewall

- Errori comuni di migrazione:
  - Caratteri sconosciuti o non validi nel file di configurazione ASA.
  - Elementi di configurazione mancanti o incompleti.
  - Problemi di connettività di rete o latenza.
- Problemi durante il caricamento del file di configurazione ASA o il push della configurazione al centro di gestione.
- I problemi più comuni sono:
- Utilizzo del pacchetto di supporto per la risoluzione dei problemi:
  - Nella schermata "Complete Migration" (Completa migrazione), fare clic sul pulsante Support (Supporto).
  - Selezionare Support Bundle e scegliere i file di configurazione da scaricare.
  - I file di log e DB sono selezionati per impostazione predefinita.
  - Fare clic su Download per ottenere un file .zip.
  - Estrarre il file .zip per visualizzare i log, il database e i file di configurazione.
  - Fare clic su Invia e-mail per inviare i dettagli dell'errore al team tecnico.
  - Allegare il pacchetto di supporto nell'e-mail.
  - Per assistenza, fare clic su Visita la pagina TAC per creare una richiesta Cisco TAC.
- Lo strumento consente di scaricare un bundle di supporto per i file di log, il database e i file di configurazione.
- Passaggi da scaricare:
- Per ulteriore supporto:

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).