

# Eseguire la migrazione di FDM a FMC tramite FMT utilizzando il file Configuration.zip

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Considerazioni](#)

[Configurazione](#)

[Richieste API - Postman](#)

[Strumento di migrazione firewall](#)

[Verifica FMC](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come generare il file di configurazione.zip di un modulo Secure Firewall Device Manager (FDM) da migrare a un FMC tramite FMT.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Firewall Threat Defense (FTD)
- Cisco Firewall Management Center (FMC)
- Strumento di migrazione firewall (FMT)
- Piattaforma API Postman

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software.

FTD 7.4.2

CCP 7.4.2

FMT 7.7.0.1

Postman 11.50.0

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

- È ora possibile eseguire la migrazione di FDM in FMC in diversi modi. In questo documento, lo scenario da esplorare è la generazione del file .zip di configurazione mediante richieste API e il successivo caricamento di tale file in FMT per migrare la configurazione in FMC.
- I passaggi illustrati in questo documento iniziano a utilizzare direttamente Postman, pertanto si consiglia di avere già installato Postman. Il PC o il notebook che si intende utilizzare, deve avere accesso a FDM e FMC, inoltre FMT deve essere installato e in esecuzione.

## Considerazioni

- Questo documento è incentrato sulla generazione del file .zip di configurazione più che sull'uso di FMT.
- La migrazione di FDM mediante il file .zip di configurazione è per le migrazioni non in tempo reale e non richiede immediatamente un FTD di destinazione.



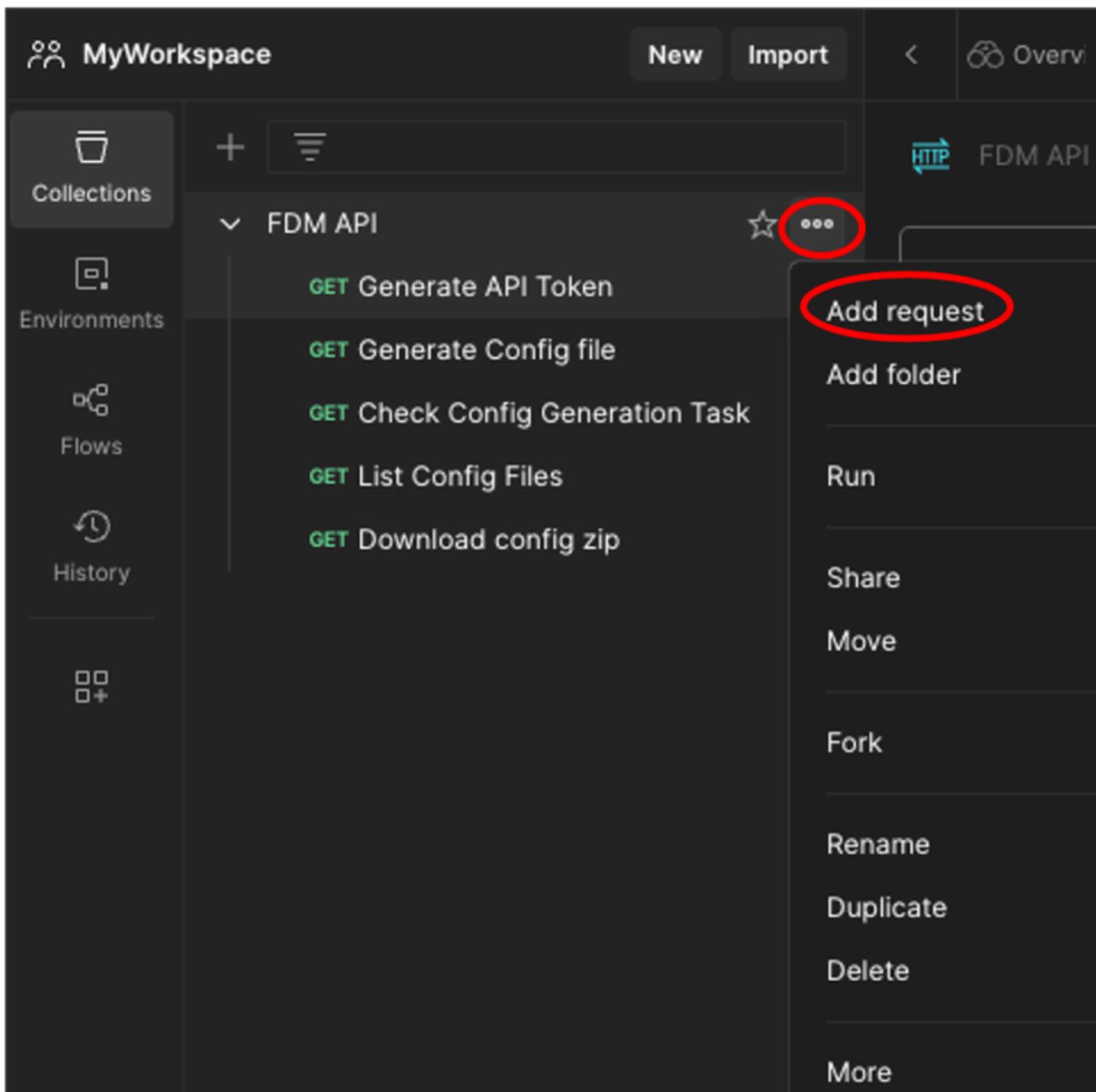
Avviso: La scelta di questa modalità consente di eseguire la migrazione solo di Access Control Policy (ACP), Network Address Translation Policy (NAT) e Oggetti. Per quanto riguarda gli oggetti da utilizzare in una regola ACP o NAT, da migrare, altrimenti vengono ignorati.

---

## Configurazione

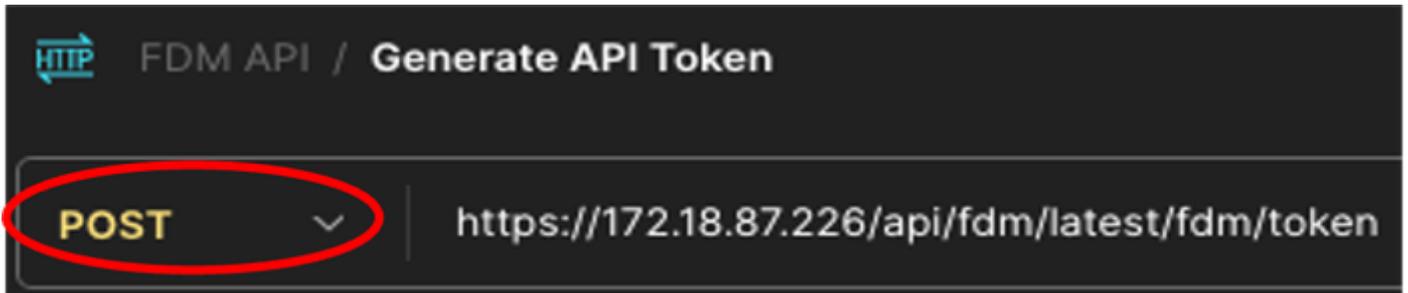
### Richieste API - Postman

1. In Postman, creare una nuova raccolta (in questo scenario viene utilizzata l'API FDM).
2. Fare clic sui 3 punti e dopo fare clic su Aggiungi richiesta.



Postman - Creazione della raccolta e aggiunta della richiesta

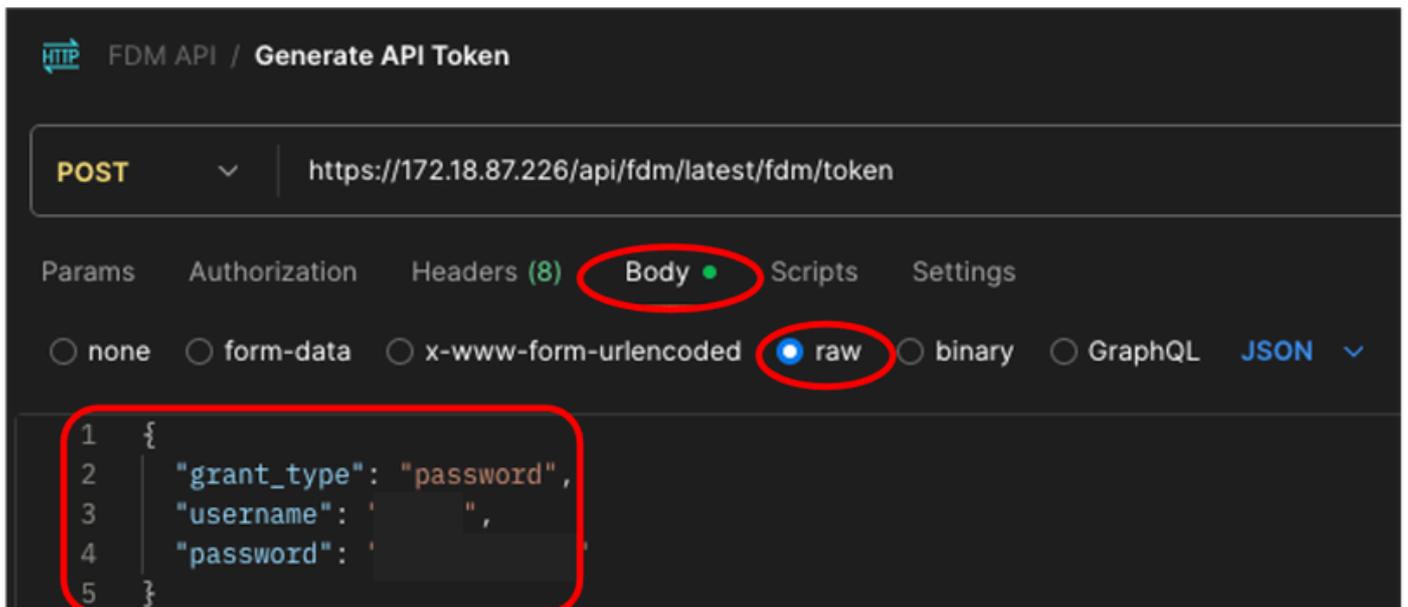
3. Chiama questa nuova richiesta: Generare il token API. Verrà creata come richiesta GET, ma durante l'esecuzione di questa richiesta è necessario selezionare POST dal menu a discesa. Nella casella di testo accanto a POST, inserire la riga successiva `https://<FDM IP ADD>/api/fdm/last/fdm/token`



Postman - Richiesta token

4. Nella scheda Corpo, selezionare l'opzione raw e introdurre le credenziali per accedere alla periferica FTD (FDM) utilizzando questo formato.

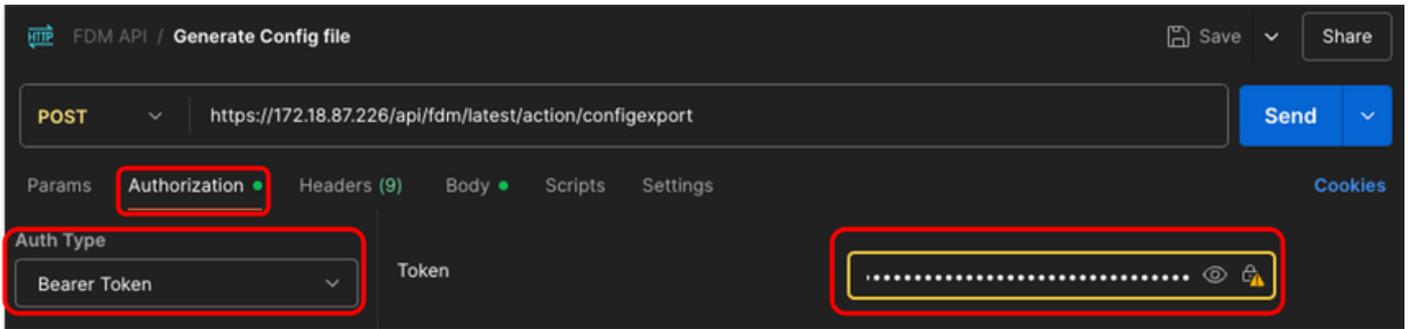
```
{  
  "grant_type": "password"  
  "username": "username",  
  "password": "password"  
}
```



Postman - Corpo richiesta token

5. Infine, fare clic su Send per ottenere il token di accesso. Se tutto va bene, si riceve una risposta di 200 OK. Fare una copia dell'intero token (all'interno delle virgolette doppie) perché verrà utilizzato nei passaggi successivi.





Postman - Genera richiesta file di configurazione - Autorizzazione

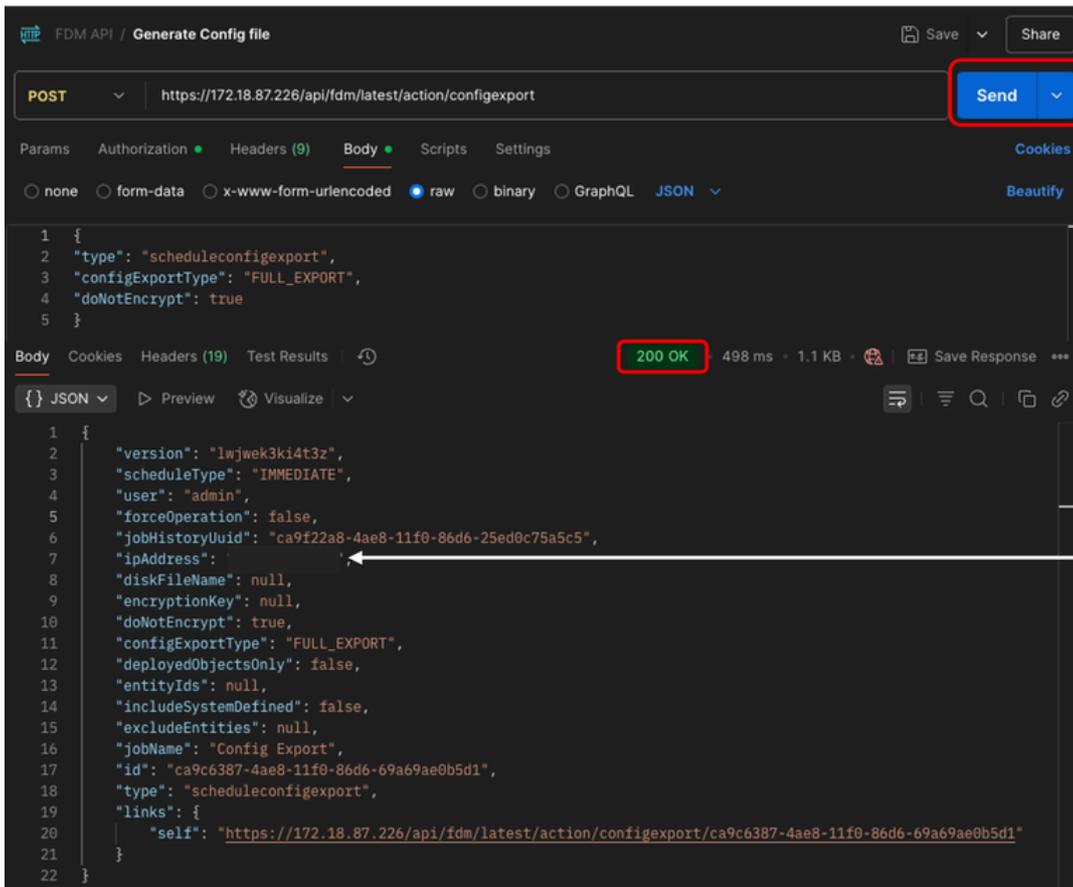
9. Nella scheda Corpo, selezionare l'opzione raw e introdurre queste informazioni.

```
{  
  "tipo": "scheduleconfigexport",  
  "configExportType": "FULL_EXPORT",  
  "doNotEncrypt": vero  
}
```



Postman - Genera richiesta file di configurazione - Corpo

10. Infine, fare clic su Invia. Se tutto va bene, si riceve una risposta di 200 OK.

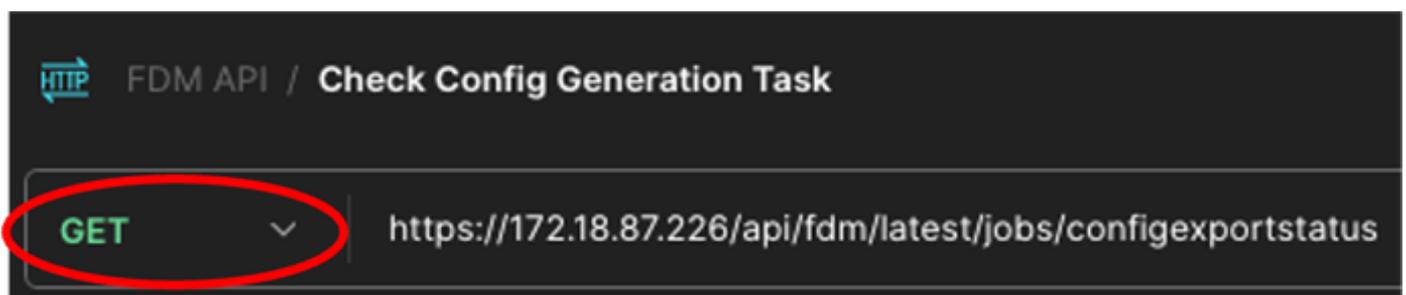


This IP address is the one that is connecting to the FTD through the requests.

Postman - Generate Config File Request - Output

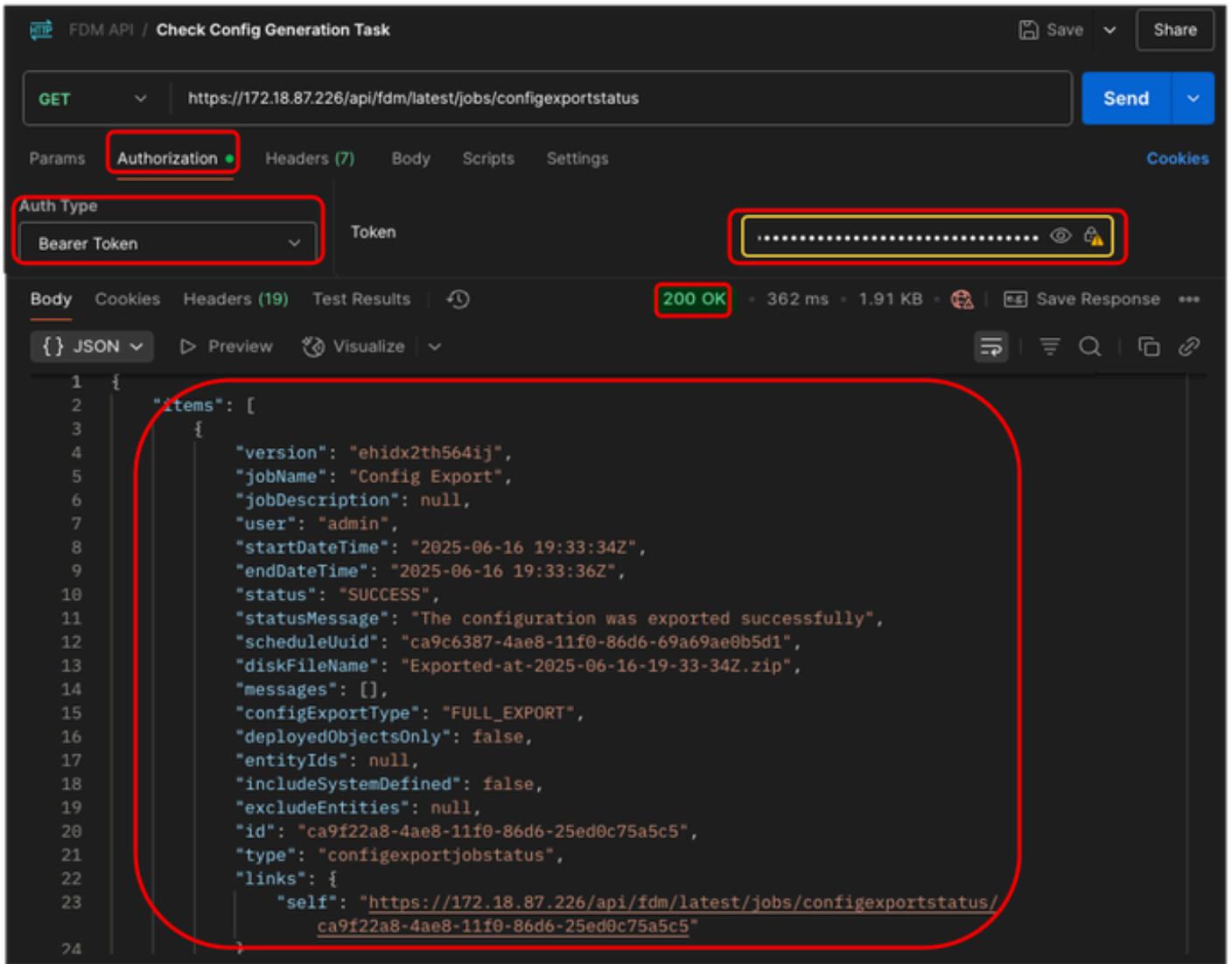
11. Ripetere il passaggio 2 per creare una nuova richiesta. GET verrà utilizzato questa volta.

12. Chiama la nuova richiesta: Controllare l'attività di generazione della configurazione. Verrà creato come richiesta GET. Inoltre, quando si esegue questa operazione, è necessario selezionare GET dal menu a discesa. Nella casella di testo accanto a GET, inserire la riga successiva `https://<FDM IP ADD>/api/fdm/latest/jobs/configexportstatus`



Postman - Richiesta di verifica dello stato di esportazione della configurazione

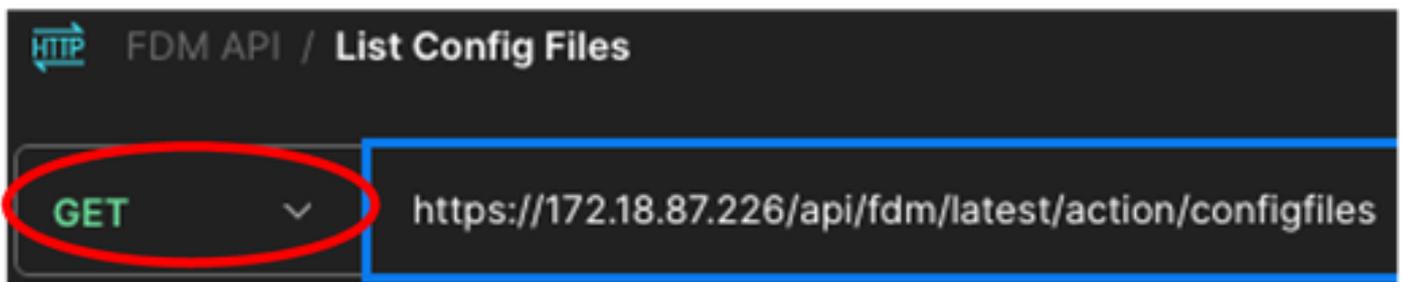
13. Nella scheda Autorizzazione, selezionare Bearer Token as Auth Type nel menu a discesa, e nella casella di testo accanto a Token incollare il token copiato nel passaggio 5. Infine, fare clic su Invia. Se tutto funziona correttamente, si riceve una risposta di 200 OK e nel campo JSON è possibile visualizzare lo stato dell'attività e altri dettagli.



Postman - Richiesta stato esportazione configurazione - Autorizzazione e output

14. Ripetere il passaggio 2 per creare una nuova richiesta. GET verrà utilizzato in questo momento.

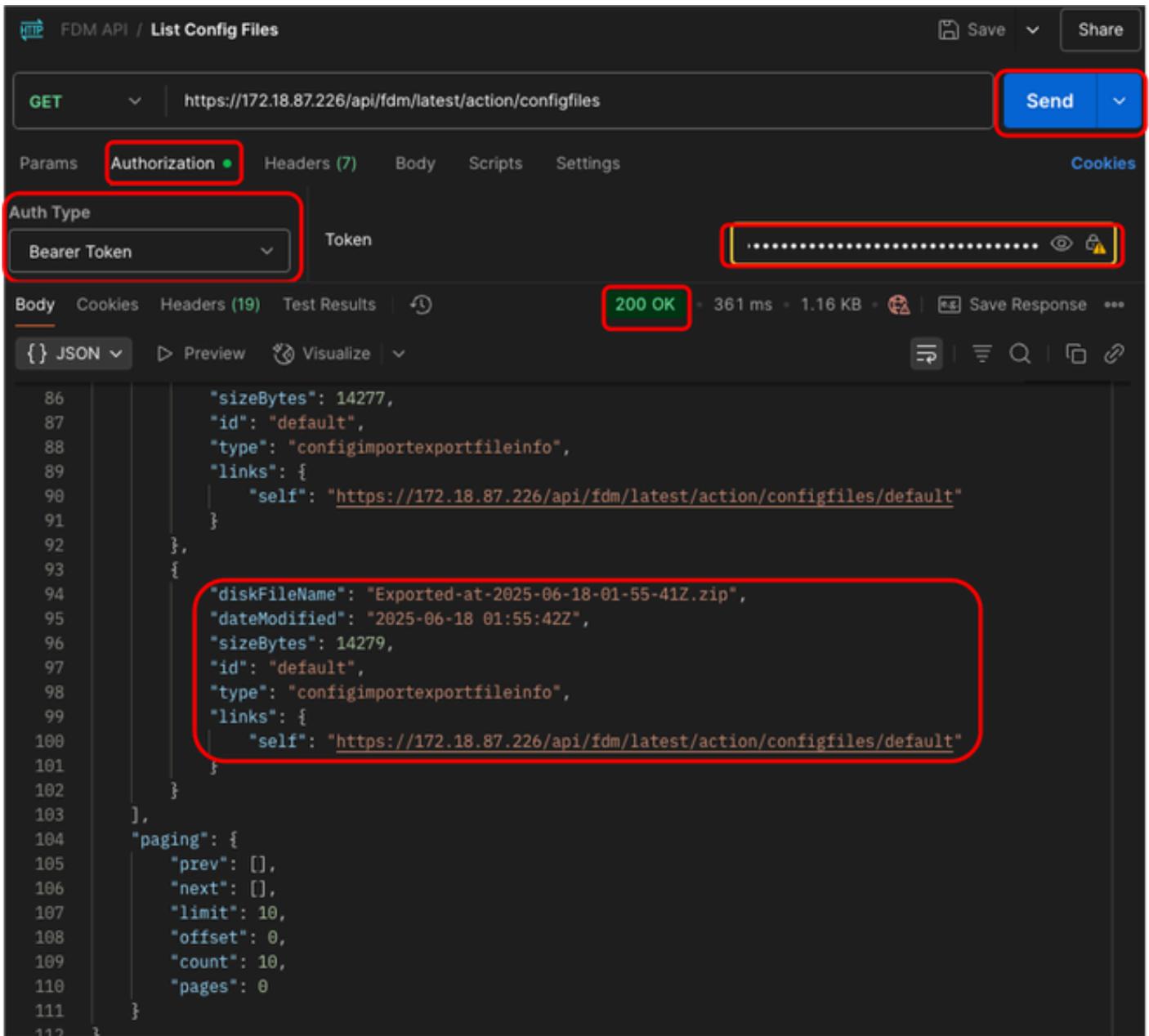
15. Chiama questa nuova richiesta: Elenca i file di configurazione. Verrà creata come richiesta GET. Inoltre, quando si esegue questa richiesta, è necessario selezionare GET dal menu a discesa. Nella casella di testo accanto a GET, inserire la riga successiva `https://<FDM IP ADD>/api/fdm/latest/action/configfiles`



Postman - Richiesta elenco file di configurazione esportati

16. Nella scheda Autorizzazione, selezionare Bearer Token come Auth Type nel menu a discesa,

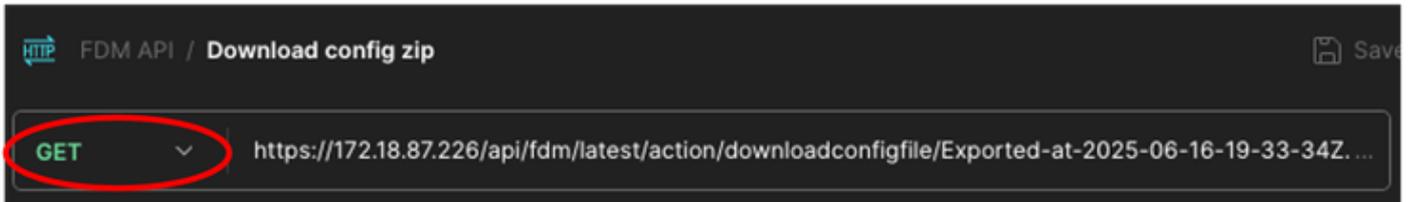
e nella casella di testo accanto a Token incollare il token copiato nel passaggio 5. Infine, fare clic su Invia. Se tutto va bene, si riceve una risposta 200 OK e nel campo JSON viene visualizzato l'elenco dei file esportati. Quella più recente è elencata in basso. Copiare il nome file più recente (la data più recente nel nome file) perché verrà utilizzato nell'ultimo passaggio.



Postman - Richiesta elenco file di configurazione esportati - Autorizzazione e output

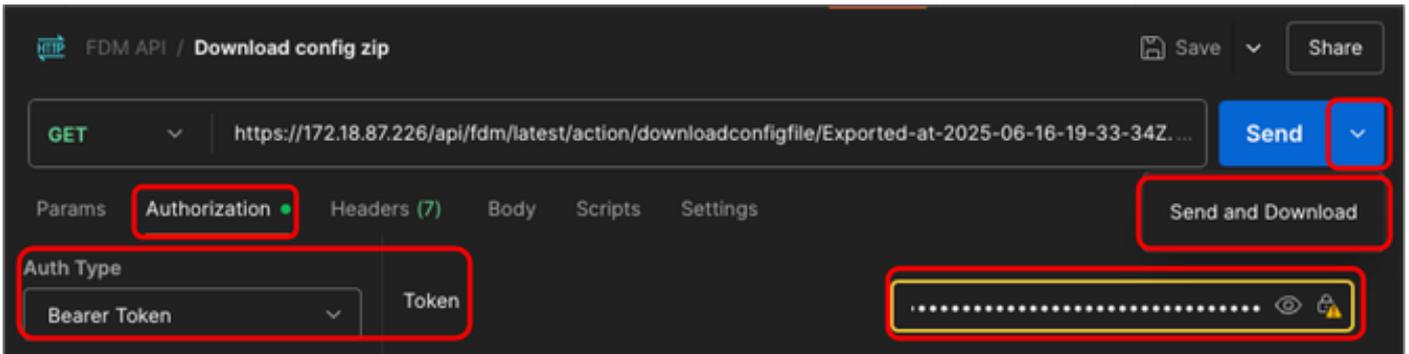
17. Ripetere il passaggio 2 per creare una nuova richiesta. GET verrà utilizzato questa volta.

18. Chiama questa nuova richiesta: Scarica il file zip della configurazione. Verrà creata come richiesta GET. Inoltre, quando si esegue questa richiesta, è necessario selezionare GET dal menu a discesa. Nella casella di testo accanto a GET, introdurre la riga successiva, incollando alla fine il nome di file copiato nel passaggio 16. `https://<FDM IP ADD>/api/fdm/last/action/downloadconfigfile/<nome_file_esportato.zip >`



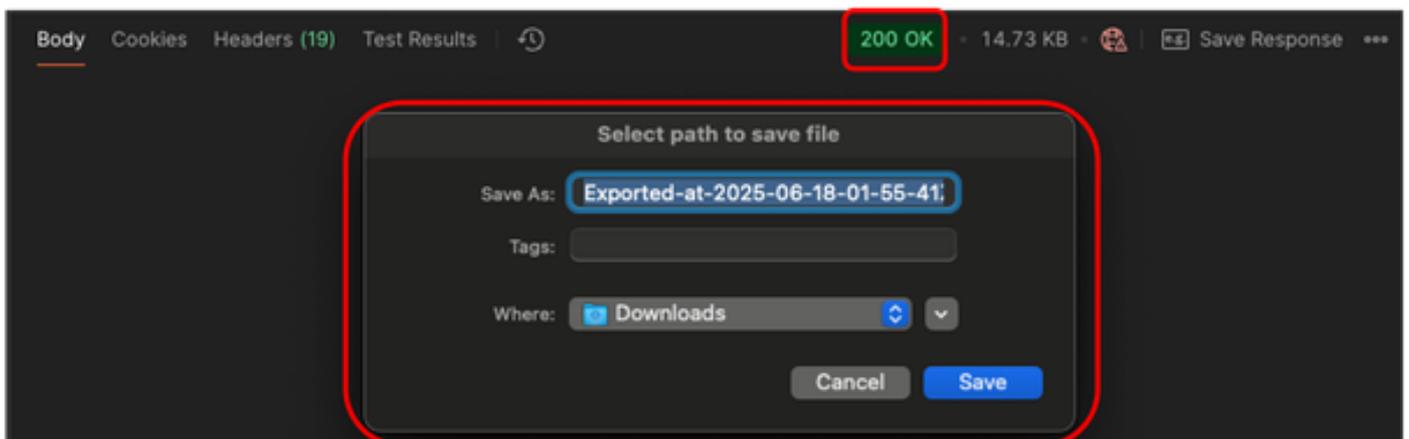
Postman - Richiesta di download del file Config.zip

19. Nella scheda Autorizzazione, selezionare Bearer Token as Auth Type nel menu a discesa, e nella casella di testo accanto a Token incollare il token copiato nel passaggio 5. Infine, fare clic sulla freccia giù accanto a Invia e scegliere Invia e scarica.



Postman - Richiesta di download del file Config.zip - Autorizzazione

20. Se tutto va bene, si riceve una risposta di 200 OK e viene visualizzata una finestra popup che richiede la cartella di destinazione in cui il file configuration.zip verrà salvato. È ora possibile caricare il file .zip nello strumento di migrazione del firewall.



Postman - Download Richiesta file Config.zip - Salvataggio

## Strumento di migrazione firewall

21. Aprire lo strumento di migrazione del firewall e nel menu a discesa Seleziona configurazione di origine, selezionare Cisco Secure Firewall Device Manager (7.2+) e fare clic su Avvia migrazione.

**Select Source Configuration**

Source Firewall Vendor  
Cisco Secure Firewall Device Manager (7.2+)

Start Migration Demo Mode

### Cisco Secure Firewall Device Manager (7.2+) Pre-Migration Instructions

This migration may take a while. Do not make any changes to the Firewall Management Center (FMC) and Firewall Device Manager (FDM) when migration is in progress. FDM to FMC manager movement process should be done over a downtime/maintenance window. FDM Devices enrolled with the cloud management will lose access upon registration with FMC.

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

**Acronyms used:**

FMT: Firewall Migration Tool	FMC: Firewall Management Center
FTD: Firewall Threat Defense	FDM: Firewall Device Manager

Before you begin your Firewall Device Manager (FDM) to Firewall Threat Defense migration, you must have the following items:

- Stable IP Connection:**  
Ensure that the connection is stable between FMT, FDM and FMC. The host-pc from which the Firewall Migration tool is being run, should have connectivity to the FDM and the FMC.
- FMC and FDM Version:** Ensure that the FMC version is 7.3 or later and FDM version is 7.2 or later. FDM version should be always equal or less than the FMC version. For optimal migration time, improved software quality and stability, use the suggested release for your **FTD** and **FMC**. Refer to the gold star on CCO for the suggested release.
- FMC Requirements:**  
Create a dedicated user account with administrative privileges for the FMT and use the credentials during migration. RestAPI is enabled on FMC by default. It is highly recommended that this is checked before migration. FMC should be registered with smart licensing server, and the licenses enabled on FDM must be enabled on FMC for smooth onboarding.
- FDM Migration Options :**  
Migration from FDM is supported in following ways.
  - Migrate Firewall Device Manager (Shared Configurations Only)**
    - This option migrates shared configuration to FMC.
    - This approach should be used to stage shared configuration to FMC. Maintenance window is not required.
    - User can either upload a configuration bundle or provide FDM credentials to fetch details.
    - Automated fetching of configuration is a preferred method.
  - Migrate Firewall Device Manager (Includes Device & Shared Configurations)**
    - This option migrates both device and shared configuration. Same FTD is moved from FDM managed to FMC managed.
    - The migration process is to be done over a scheduled downtime or maintenance window. There is device downtime involved in this migration process.**
    - Ensure connectivity between FDM device and FMC to move the device from FDM to FMC using FDM.
    - Ensure FDM Configuration has AD Realm with encryption set to NONE. [Click here](#) for more info.
    - User should provide FDM IP and credentials to fetch details. Uploading configuration bundle is not supported.
    - FDM Devices enrolled with the cloud management will lose access upon registration with FMC.
    - Ensure out-of-band access to FTD device is available, to access the device in case of accessibility issues during migration.
    - It is highly recommended that a backup (export) of the FDM configuration is performed to restore the original state of the firewall managed by FDM if required.
    - If the FTD devices are in a failover pair, failover needs to be disabled (break HA) before proceeding with moving manager from FDM to FMC.
    - FDM with Universal PLR cannot be moved from FDM to FMC.
    - FDM with flexConfig objects or flexconfig policies cannot be moved from FDM to FMC. The flexconfig objects and policies must be

FMT - Selezione FDM

2. Selezionare il primo pulsante di opzione, Migrare Gestione periferiche firewall (solo configurazioni condivise) e fare clic su Continua.

## How would you like to migrate from Firewall Device Manager :



Click on text below to get additional details on each of the migration options

Migrate Firewall Device Manager (Shared Configurations Only)

- This option migrates shared configuration to FMC.
- This approach should be used to stage shared configuration to FMC. Maintenance window is not required.
- User can either upload a configuration bundle or provide FDM credentials to fetch details.
- Automated fetching of configuration is a preferred method.

Migrate Firewall Device Manager (Includes Device & Shared Configurations)

Migrate Firewall Device Manager (Includes Device & Shared Configurations) to FTD Device (New Hardware)

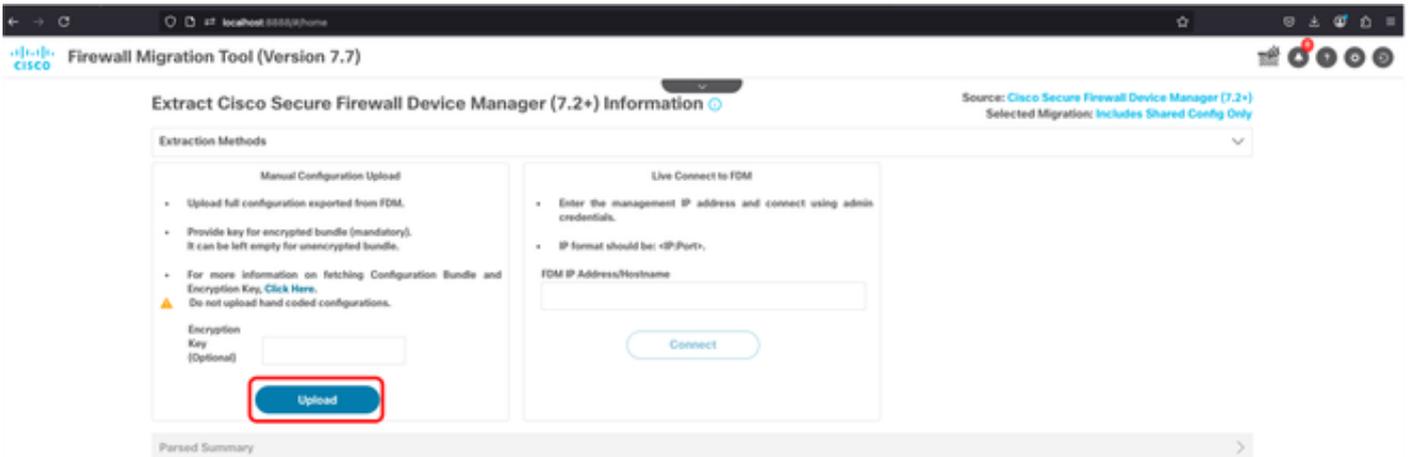
### Note :

- Device configuration includes Interfaces, Routes and Site to Site VPN based features.
- Shared configuration includes Access control Policy, Remote Access VPN, NAT and Objects based features.

Continue

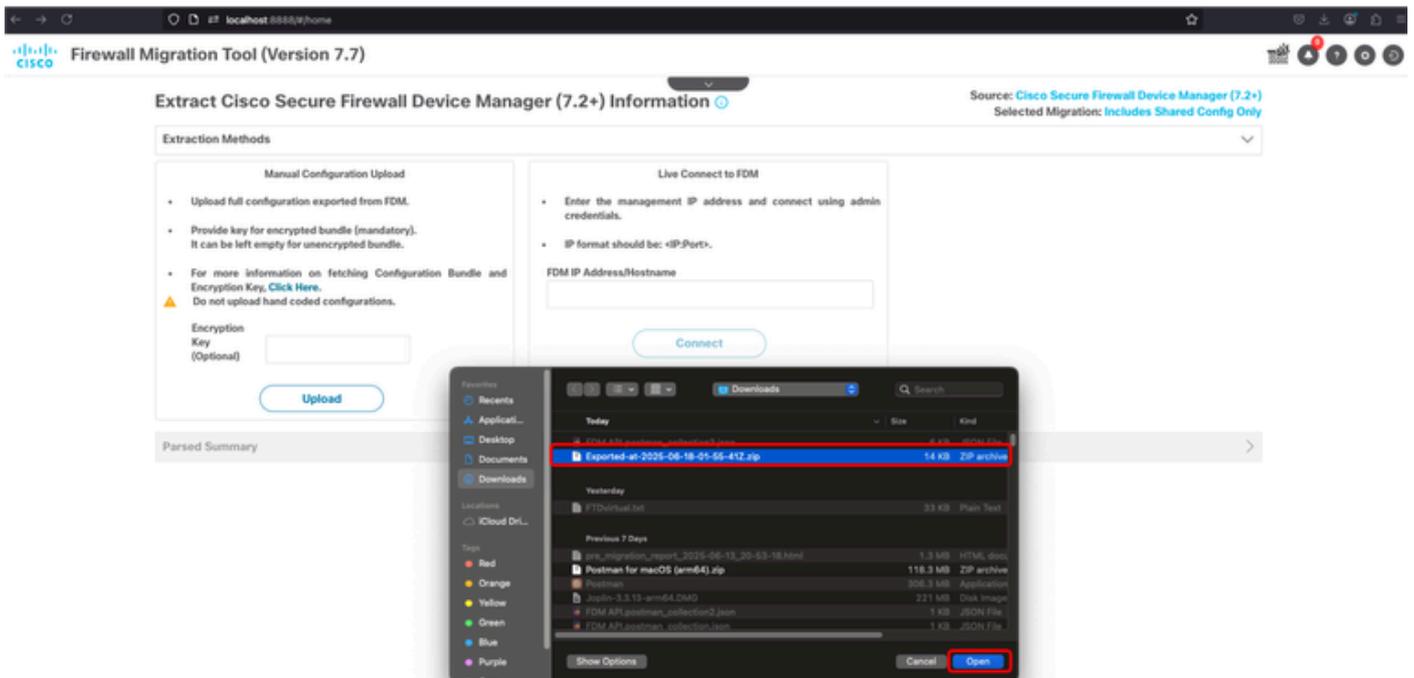
FMT - Solo configurazioni condivise di migrazione FDM

23. Nel pannello sinistro (Caricamento manuale della configurazione), fare clic su Upload (Carica).



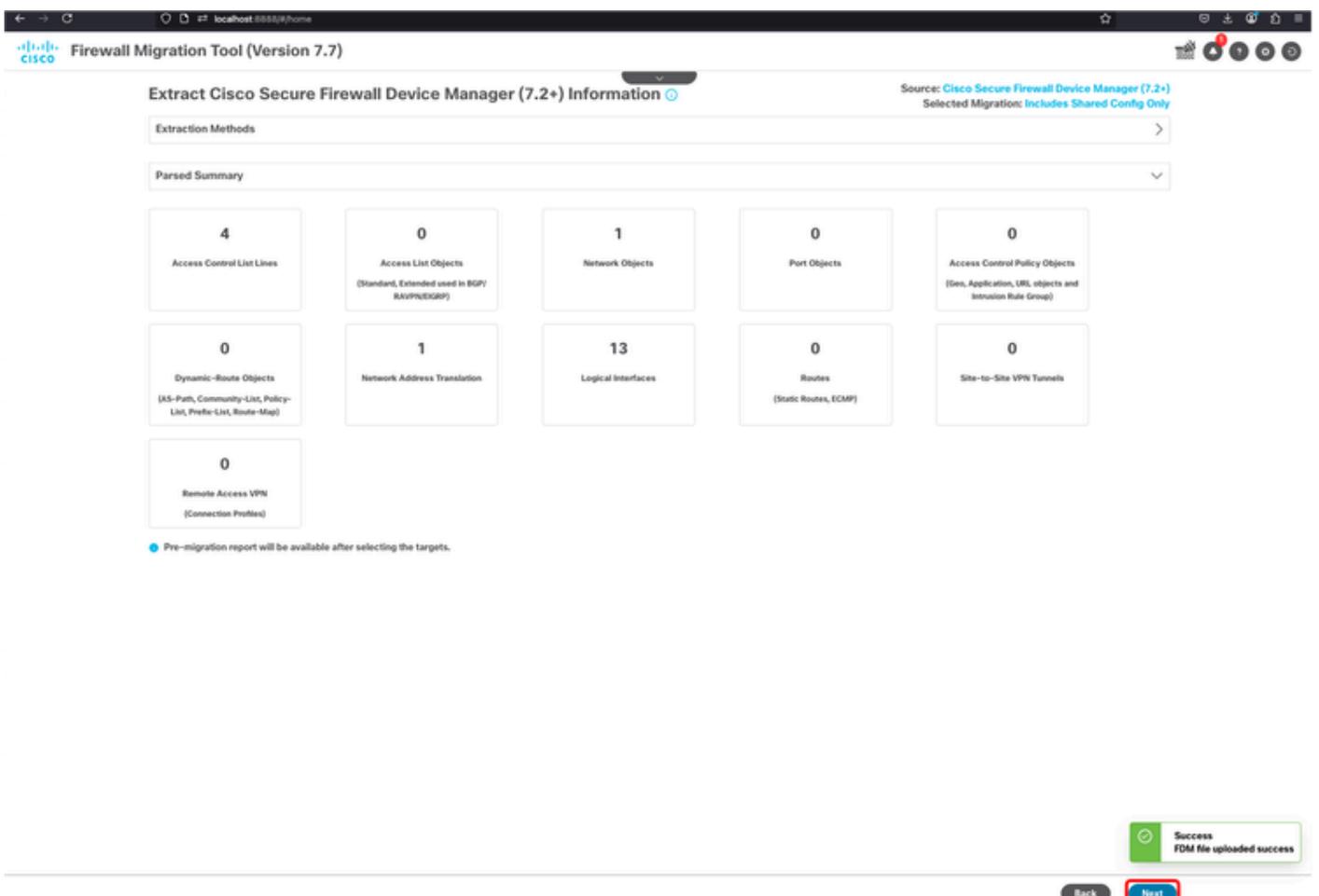
FMT - Carica file Config.zip

24. Selezionare il file zip config esportato nella cartella salvata in precedenza e fare clic su Apri.



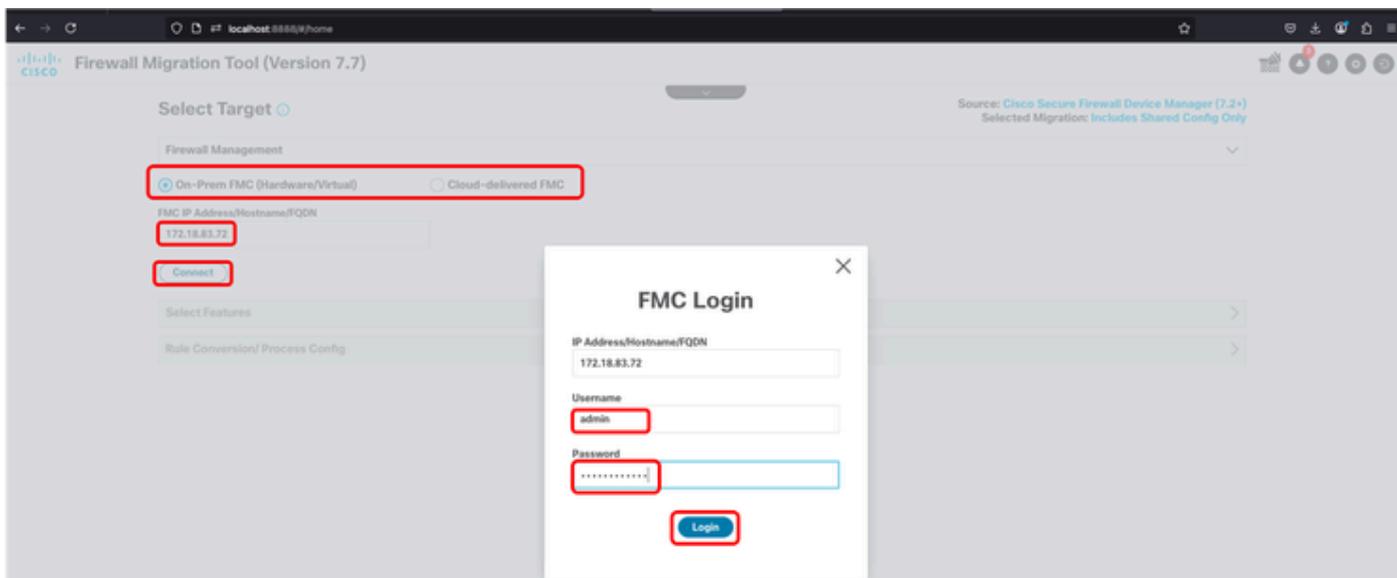
FMT - Selezione file Config.zip

25. Se tutto procede come previsto, viene visualizzato il Riepilogo analizzato. Inoltre, nell'angolo in basso a destra è possibile visualizzare un popup che informa che il file FDM è stato caricato correttamente. Fare clic su Next (Avanti).



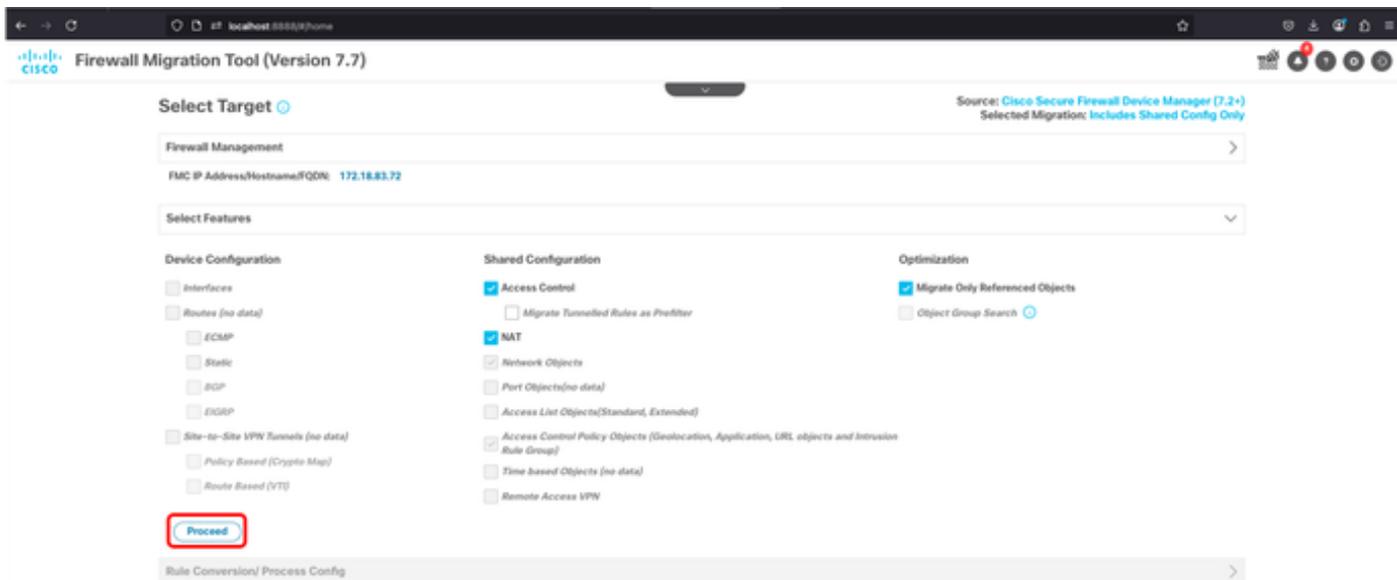
FMT - Riepilogo analisi

26. Selezionare l'opzione più adatta all'ambiente (CCP locale o Cd-FMC). In questo scenario viene utilizzato un CCP locale. Digitare l'indirizzo IP del CCP e fare clic su Connetti. Viene visualizzata una nuova schermata di popup in cui viene richiesto di immettere le credenziali FMC, quindi fare clic su Accesso.



FMT - Accesso destinazione FMC

27. La schermata successiva mostra il CCP di destinazione e le funzionalità che verranno migrate. Fare clic su Continua.



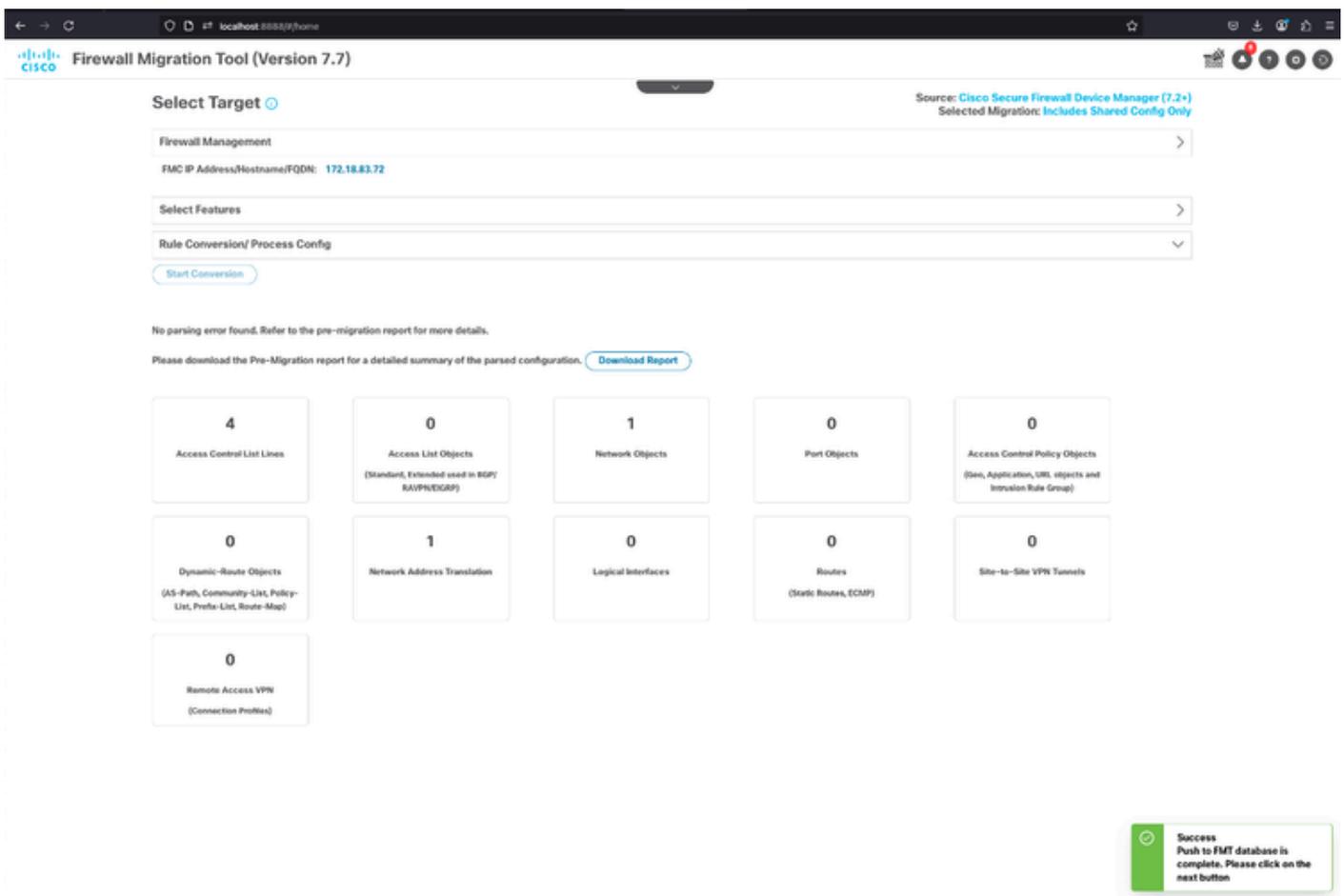
FMT - Destinazione FMC - Selezione funzionalità

28. Una volta confermata la destinazione FMC, fare clic sul pulsante Avvia conversione.



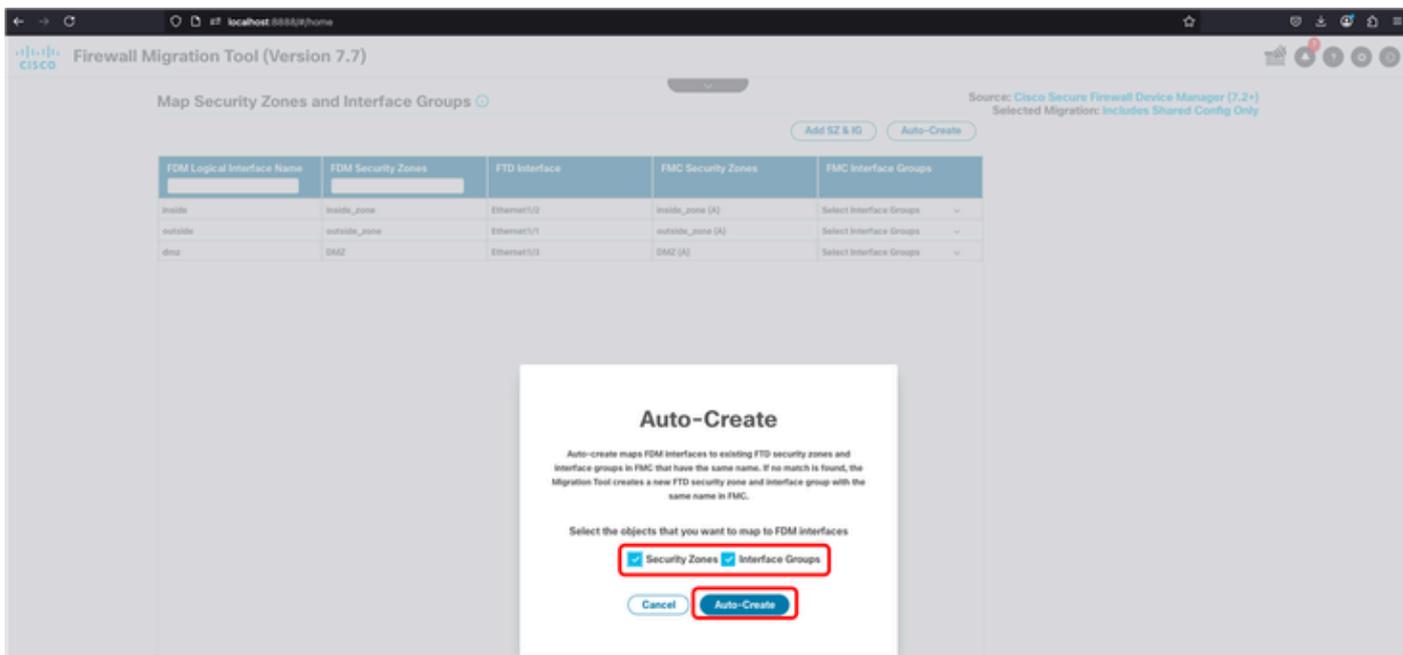
FMT - Avvio conversione configurazione

29. Se tutto procede come previsto, viene visualizzato un popup nell'angolo in basso a destra che informa che il push al database FMT è completato. Fare clic su Next (Avanti).



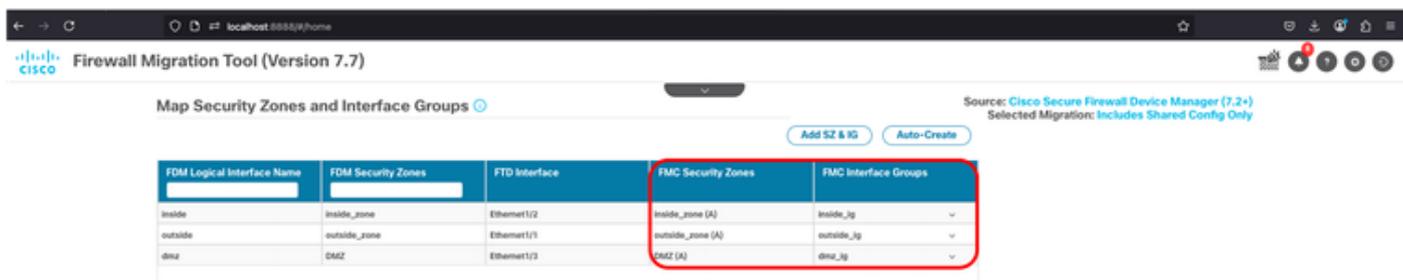
FMT - Push del database completato

30. Nella schermata successiva, è necessario creare manualmente le aree di sicurezza e i gruppi di interfacce o scegliere di crearli automaticamente. In questo scenario viene utilizzata la creazione automatica.



FMT - Creazione automatica di aree di sicurezza e gruppi di interfacce

31. Una volta completata, la tabella mostra rispettivamente nella quarta e nella quinta colonna la zona di sicurezza e il gruppo di interfacce.



FMT - Creazione delle aree di sicurezza e dei gruppi di interfacce completata

32. Nella schermata successiva, è possibile ottimizzare l'ACL o semplicemente convalidare gli ACL, gli oggetti e il NAT. Al termine, fare clic sul pulsante Convalida.

Firewall Migration Tool (Version 7.7)

Optimize, Review and Validate Shared Configuration Only

Source: Cisco Secure Firewall Device Manager (7.2+)  
Selected Migration: Includes Shared Config Only

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

AGP Pre-filter Intrusion Policy

Select all 4 entries Selected: 0 / 4

#	Name	SOURCE			DESTINATION			ACCESS CONTROL POLICY ...			ACE Count	TIME BASED
		Zone	Network	Port	Zone	Network	Port	Applications	URLs	State		
<input type="checkbox"/>	Inside_Outside_Bu...	inside_zone	ANY	ANY	outside_m...	ANY	ANY	ANY	ANY	deny	1	None
<input type="checkbox"/>	AD-Srvr_81	DMZ	AD-Srvr	ANY	inside_zone	ANY	ANY	ANY	ANY	permit	1	None
<input type="checkbox"/>	DMZ-Inside_81	DMZ	ANY	ANY	inside_zone	ANY	ANY	ANY	ANY	deny	1	None
<input type="checkbox"/>	Outside_DMZ_81	outside_m...	ANY	ANY	DMZ	ANY	ANY	ANY	ANY	permit	1	None

50 per page 1 to 4 of 4 Page 1 of 1

Optimize ACL Validate

FMT - Ottimizzazione ACL - Convalida migrazione

33. La convalida richiede un paio di minuti per essere completata.

Firewall Migration Tool (Version 7.7)

Optimize, Review and Validate Shared Configuration

Validation in progress. It will take a while

Source: Cisco Secure Firewall Device Manager (7.2+)  
Selected Migration: Includes Shared Config Only

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

AGP Pre-filter Intrusion Policy

Select all 4 entries Selected: 0 / 4

#	Name	SOURCE			DESTINATION			ACCESS CONTROL POLICY ...			ACE Count	TIME BASED
		Zone	Network	Port	Zone	Network	Port	Applications	URLs	State		
<input type="checkbox"/>	Inside_Outside_Bu...	inside_zone	ANY	ANY	outside_m...	ANY	ANY	ANY	ANY	deny	1	None
<input type="checkbox"/>	AD-Srvr_81	DMZ	AD-Srvr	ANY	inside_zone	ANY	ANY	ANY	ANY	permit	1	None
<input type="checkbox"/>	DMZ-Inside_81	DMZ	ANY	ANY	inside_zone	ANY	ANY	ANY	ANY	deny	1	None
<input type="checkbox"/>	Outside_DMZ_81	outside_m...	ANY	ANY	DMZ	ANY	ANY	ANY	ANY	permit	1	None

FMT - Convalida in corso

34. Al termine, FMT indica che la configurazione è stata convalidata e il passo successivo è fare clic sul pulsante Push Configuration.

# Validation Status



 Successfully Validated

## Validation Summary (Pre-push)

<b>4</b> Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	<b>1</b> Network Objects	Not selected for migration Port Objects	<b>0</b> Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
Not selected for migration Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)	<b>1</b> Network Address Translation	Not selected for migration Logical Interfaces	Not selected for migration Routes (Static Routes, ECMP)	Not selected for migration Site-to-Site VPN Tunnels
Not selected for migration Remote Access VPN (Connection Profiles)				

**Push Configuration**

FMT - Convalida completata - Push della configurazione in FMC

35. Infine, fare clic sul pulsante Continua.

The Step of final push to target FMC/FTD is subjected to zero, limited or many push errors that largely depend on the success or failure of API execution between migration tool and firewall management center.



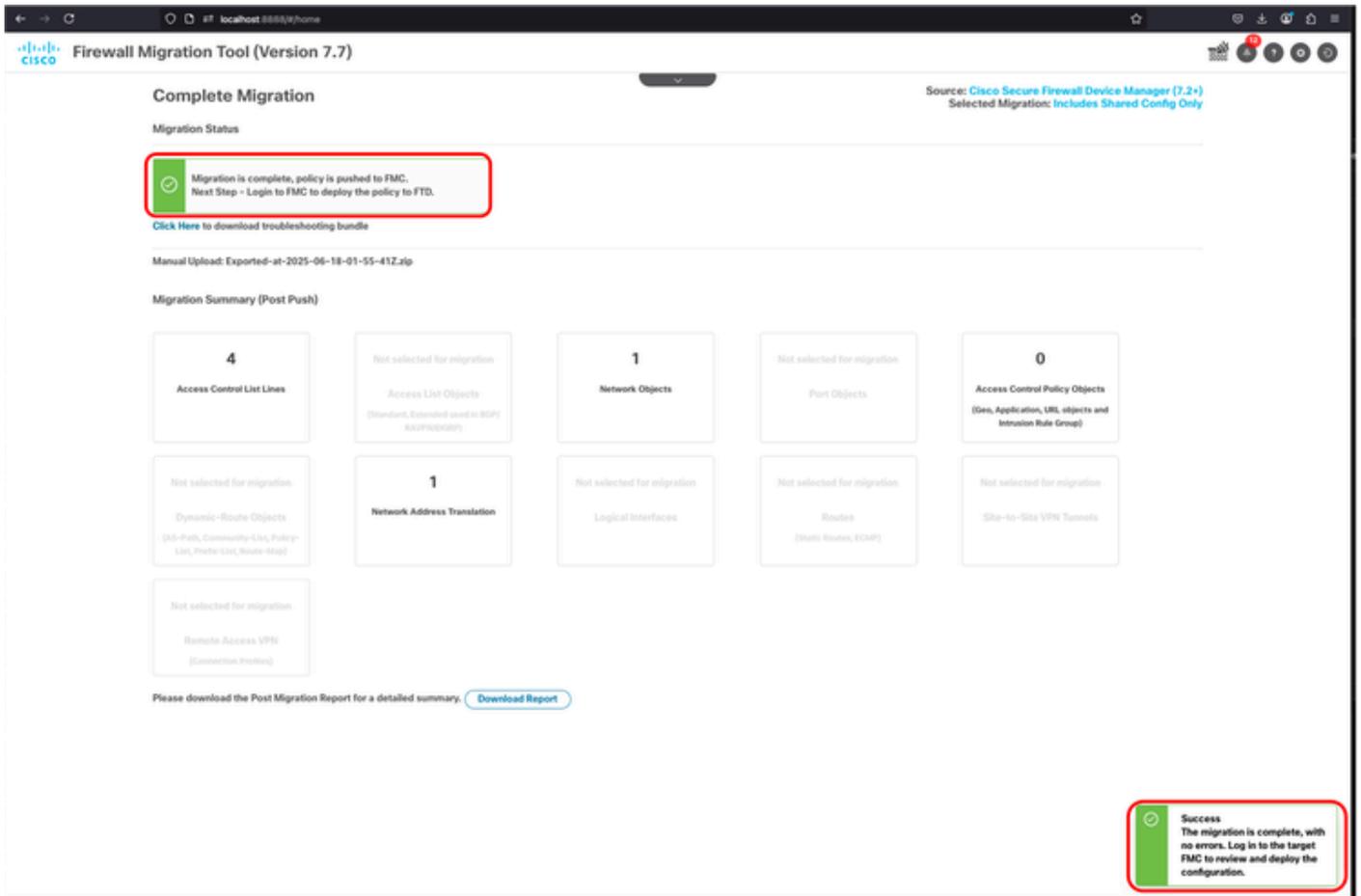
Click on Proceed to continue.

**Proceed**

**Recommendation:** Please review the migration fallout report during the course of final push stage to understand firewall configurations that will not be migrated in addition to review the suggested actions to be taken on target FMC for "Abort Migration".

FMT - Procedi con Push di configurazione

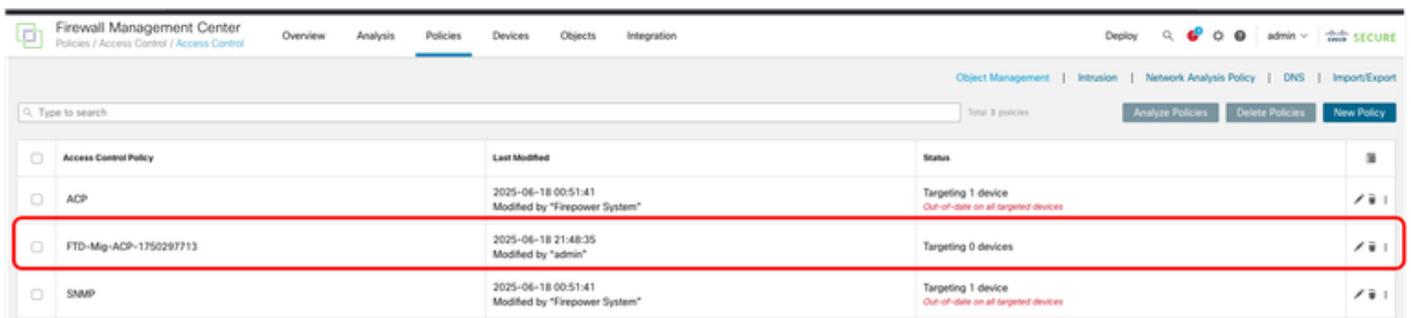
36. Se tutto procede come previsto, viene visualizzata la notifica Migrazione completata. FMT richiede di accedere a FMC e di distribuire il criterio migrato a FTD.



FMT - Notifica migrazione completata

## Verifica FMC

37. Dopo aver effettuato l'accesso al CCP, le politiche ACP e NAT sono indicate come FTD-Mig. È ora possibile procedere con la distribuzione nel nuovo FTD.



FMC - ACP migrati



FMC - Criterio NAT migrato

## Informazioni correlate

- [FMT - Guida alla migrazione da FDM a FMC](#)
- [Note release FMT](#)

## 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).