

# Migrazione da FDM a CdFMC tramite FMT in CDO

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Verifica](#)

---

## Introduzione

In questo documento viene descritto come eseguire la migrazione da Firepower Device Manager (FDM) a Cloud-Delivered FMC (cdFMC) utilizzando Firepower Migration Tool (FMT) in CDO.

## Prerequisiti

### Requisiti

- Firepower Device Manager (FDM) 7.2+
- Centro gestione firewall (cdFMC) distribuito tramite cloud
- Firepower Migration Tool (FMT) incluso in CDO

### Componenti usati

Questo documento è stato creato in base ai requisiti sopra indicati.

- Firepower Device Manager (FDM) sulla versione 7.4.1
- Centro gestione firewall (cdFMC) distribuito tramite cloud
- Cloud Defense Orchestrator (CDO)

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

Gli utenti di CDO admin possono eseguire migrazioni dei propri dispositivi a cdFMC quando i

dispositivi sono nella versione 7.2 o successiva. Nella migrazione descritta in questo documento, cdFMC è già abilitato sul tenant CDO.

## Configurazione

### 1.- Abilitare i servizi cloud Cisco su FDM

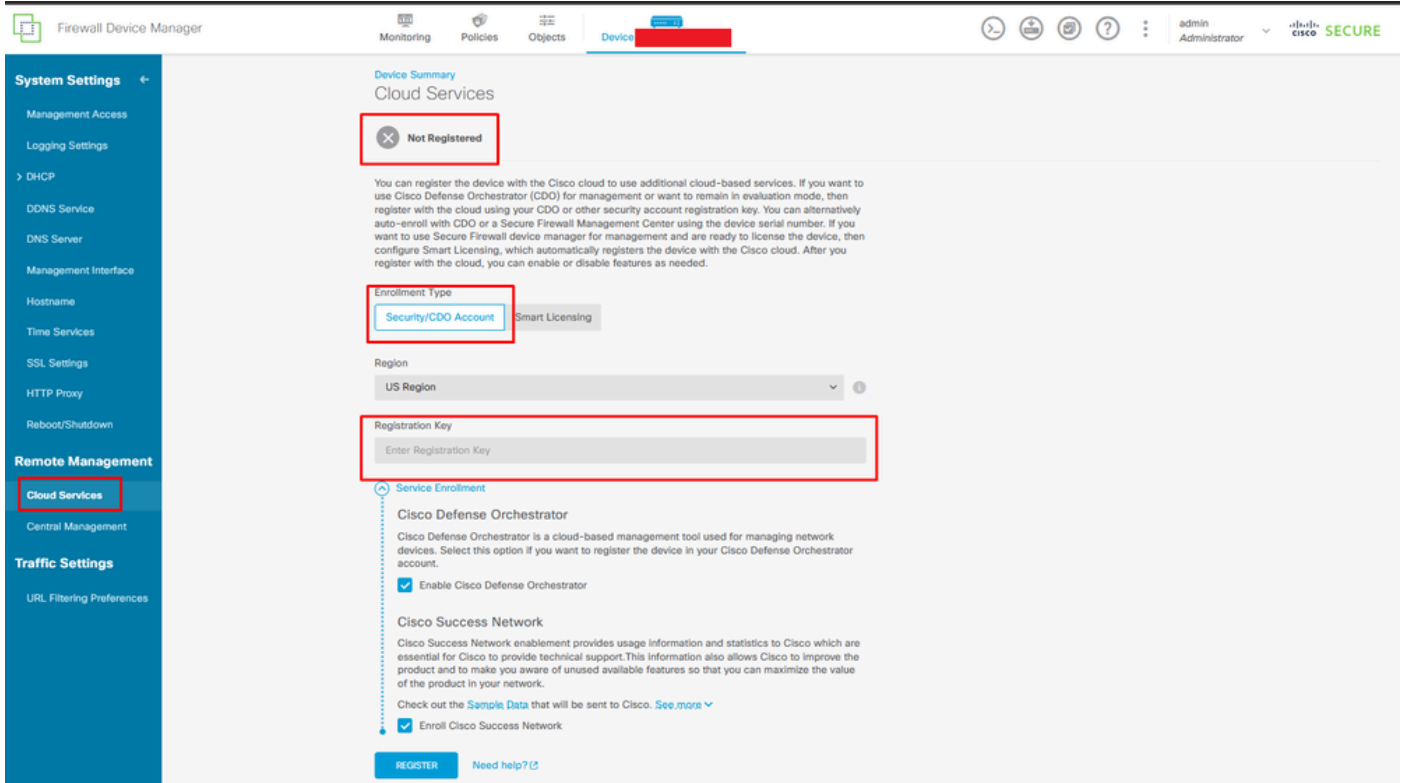
Per iniziare la migrazione, è necessario disporre del dispositivo FDM senza distribuzioni in sospeso e registrarsi ai servizi cloud. Per registrarsi ai servizi cloud, passare a Impostazioni di sistema > Visualizza altro > Servizi cloud.

All'interno della sezione Cloud Services, si trova il dispositivo non è registrato, quindi è necessario eseguire la registrazione con il tipo Security/CDO Account. È necessario configurare una chiave di registrazione, quindi Registra.

The screenshot shows the Cisco Firepower Threat Defense (FTD) configuration interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device'. The main content area displays a network diagram with 'Inside Network', 'Cisco Firepower Threat Defense for Azure', and 'ISP/WAN/Gateway' components. Below the diagram is a grid of configuration tiles: 'Interfaces' (Management: Unmerged, Enabled 2 of 2), 'Smart License' (Registered, Tier: FTDv20 - 3 Gbps), 'Site-to-Site VPN' (No connections yet), 'Routing' (1 static route), 'Backup and Restore', 'Remote Access VPN' (Requires Secure Client License), 'Updates' (Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds), 'Troubleshoot' (No files created yet), 'Advanced Configuration' (Includes: FlexConfig, Smart CLI), 'System Settings' (Management Access, Logging Settings, SSL Settings, Cloud Services, HTTP Proxy, Reboot/Shutdown Interface, Central Management, URL Filtering Preferences), and 'Device Administration' (Audit Events, Deployment History, Download Configuration). A dropdown menu is open over the 'System Settings' tile, highlighting 'Cloud Services'.

Servizi cloud di registrazione

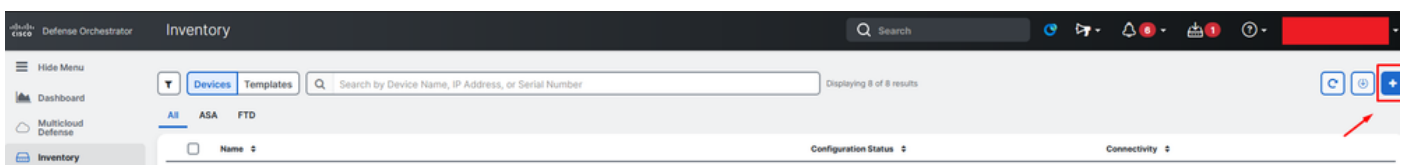
Sui servizi cloud viene mostrato che non è registrato. Selezionare il tipo di registrazione Account CDO e fornire la chiave di registrazione da CDO.



Registrazione ai servizi cloud

La chiave di registrazione si trova all'interno di CDO. Passare a CDO, andare a Magazzino > Aggiungi simbolo.

Viene visualizzato un menu che consente di selezionare il tipo di periferica di cui si dispone. Selezionare l'opzione FTD. È necessario che l'opzione FDM sia abilitata; in caso contrario, non è possibile eseguire la migrazione corrispondente. Il tipo di registrazione utilizza Usa chiave di registrazione. In questa opzione, la chiave di registrazione viene visualizzata nel passaggio numero 3, che è necessario copiare e incollare in FDM.



FDM integrato, aggiungere opzione

Viene visualizzato un menu per selezionare un tipo di dispositivo o di servizio.

## Select a Device or Service Type

No Secure Device Connector found to communicate with some types of devices. [Set up a Secure Device Connector](#)



### ASA

Adaptive Security Appliance  
(8.4+)



### Multiple ASAs

Adaptive Security Appliance  
(8.4+)



### FTD

Cisco Secure  
Firewall Threat Defense

Meraki

### Meraki

Meraki Security Appliance



### Integrations

Enable basic CDO functionality for  
integrations



VPC

### AWS VPC

Amazon Virtual Private Cloud



### Duo Admin

Duo Admin Panel

Umbrella

### Umbrella Organization

View Umbrella Organization Policies  
from CDO



### Import

Import configuration for offline  
management

Seleziona tipo di dispositivo o servizio

Per questo documento è stata selezionata l'opzione Select Registration Key.

Follow the steps below

[Cancel](#)



### Firewall Threat Defense

Management Mode:

FTD ⓘ  FDM ⓘ  
*(Recommended)*

**Important:** This method of onboarding allows for local co-management of the firewall via FDM. To manage your device with cloud-delivered Firewall Management System, click the FTD button instead. [Learn more](#)



#### Use Registration Key

Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.



#### Use Serial Number

Use this method for low-touch provisioning or for onboarding configured devices using their serial number.  
(FTD 6.7+, 1000, 2100 and 3100 series only)



#### Use Credentials (Basic)

Onboard a device using its IP address, or host name, and a username and password.

Tipo di registrazione

Qui viene mostrata la chiave di registrazione necessaria per il passaggio precedente.

**Firewall Threat Defense**  
Management Mode:  
 FTD ⓘ  FDM ⓘ  
*(Recommended)*

**Important:** This method of onboarding allows for local co-management of the firewall via FDM. To manage your device with cloud-delivered Firewall Management System, click the FTD button instead. [Learn more](#) ⓘ

**Use Registration Key**  
Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.

**Use Serial Number**  
Use this method for low-touch provisioning or for onboarding configured devices using their serial number.  
(FTD 6.7+, 1000, 2100 and 3100 series only)

**Use Credentials (Basic)**  
Onboard a device using its IP address, or host name, and a username and password.

**1** Device Name [redacted]

**2** Database Updates **Enabled**

**3** Create Registration Key **7a53c:** [redacted]

**4** Smart License **(Skipped)**

**5** Done  
Your device is now onboarding.  
 ⓘ This may take a long time to finish. You can check the status of the device on the Devices and Services page.

**Add Labels** ⓘ

Add label groups and labels +

**Go to Inventory**

Processo di registrazione

Una volta ottenuta la chiave di registrazione, copiarla e incollarla in FDM e fare clic su Registra. Dopo aver registrato FDM all'interno dei servizi cloud, viene visualizzato come Abilitato, come mostrato nell'immagine.

La Smart License è stata ignorata perché il dispositivo verrà registrato una volta che sarà operativo.

Device Summary

# Cloud Services

**Not Registered**

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

Enrollment Type

Security/CDO Account

Smart Licensing

Region

US Region

Registration Key

7a53c2

Service Enrollment

### Cisco Defense Orchestrator

Cisco Defense Orchestrator is a cloud-based management tool used for managing network devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.

Enable Cisco Defense Orchestrator

### Cisco Success Network

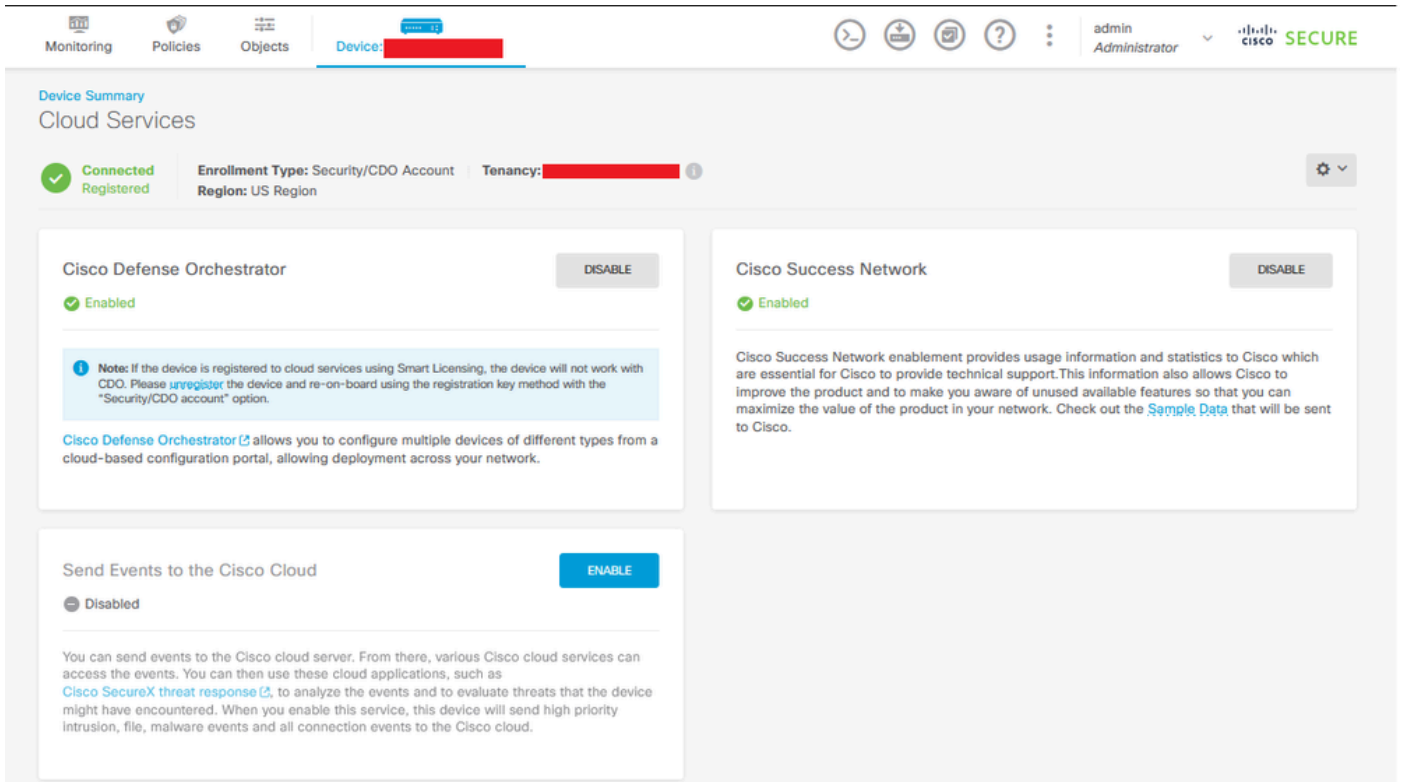
Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#)

Enroll Cisco Success Network

REGISTER

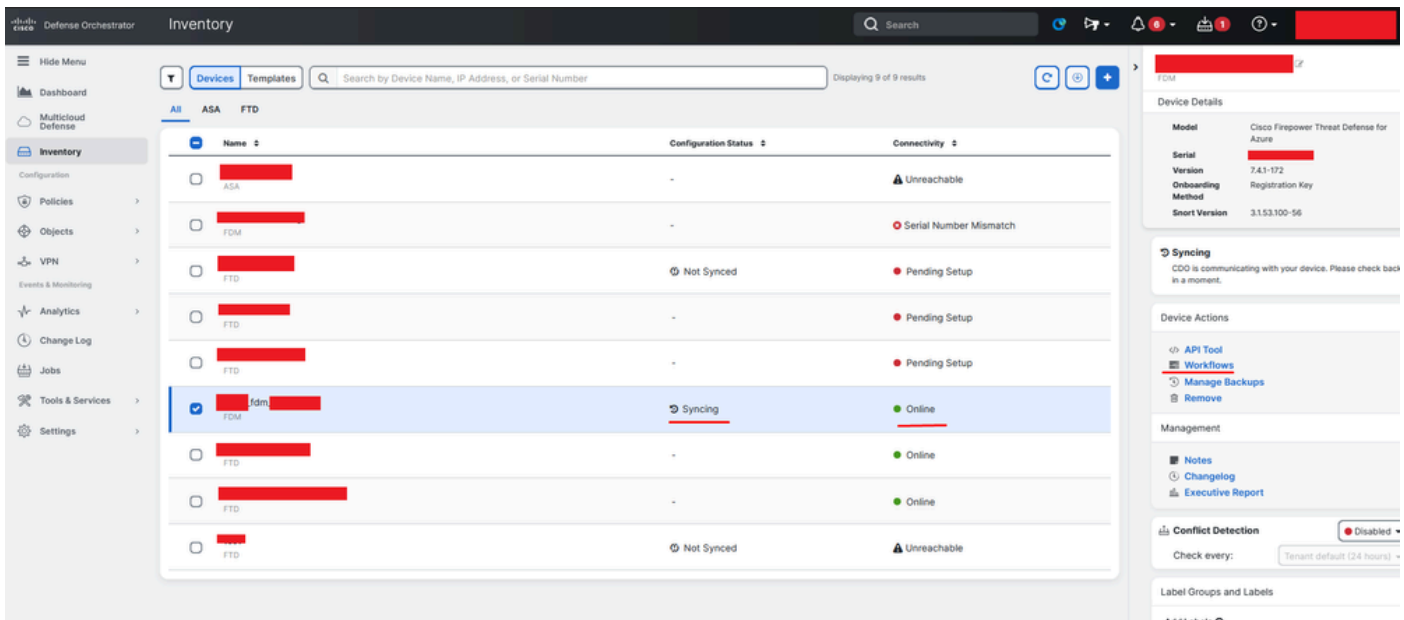
[Need help?](#)



Registrazione di FDM completata

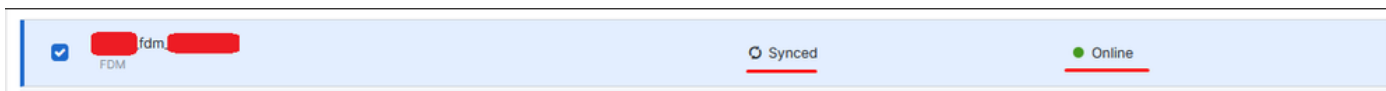
All'interno di CDO, nel menu Inventario, FDM può essere trovato nel processo di essere onboarding e sincronizzazione. L'avanzamento e il flusso di questa sincronizzazione possono essere esaminati nella sezione Flussi di lavoro.

Al termine del processo, verrà visualizzato come Sincronizzato e In linea.



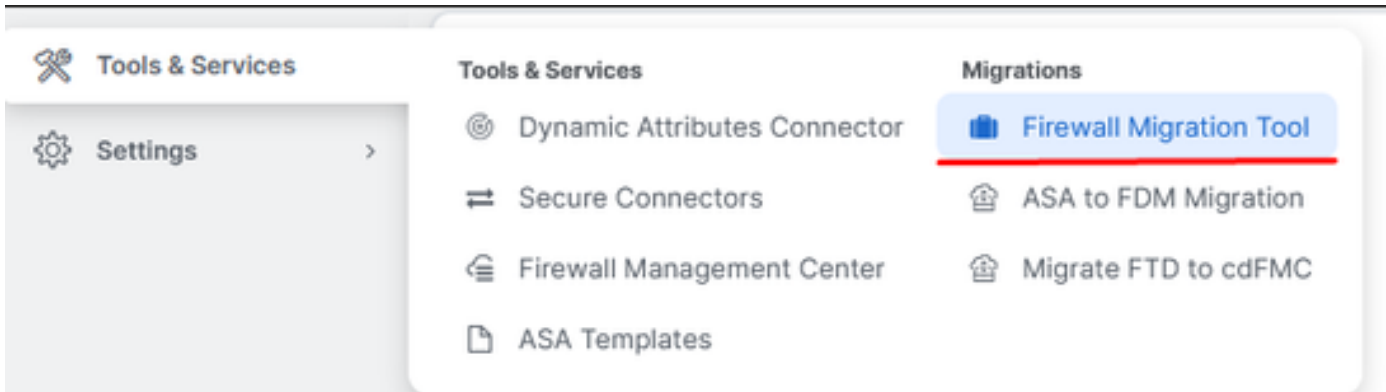
Inventario CDO integrato in FDM

Quando i dispositivi sono stati sincronizzati, vengono visualizzati come In linea e Sincronizzato.



FDM integrato

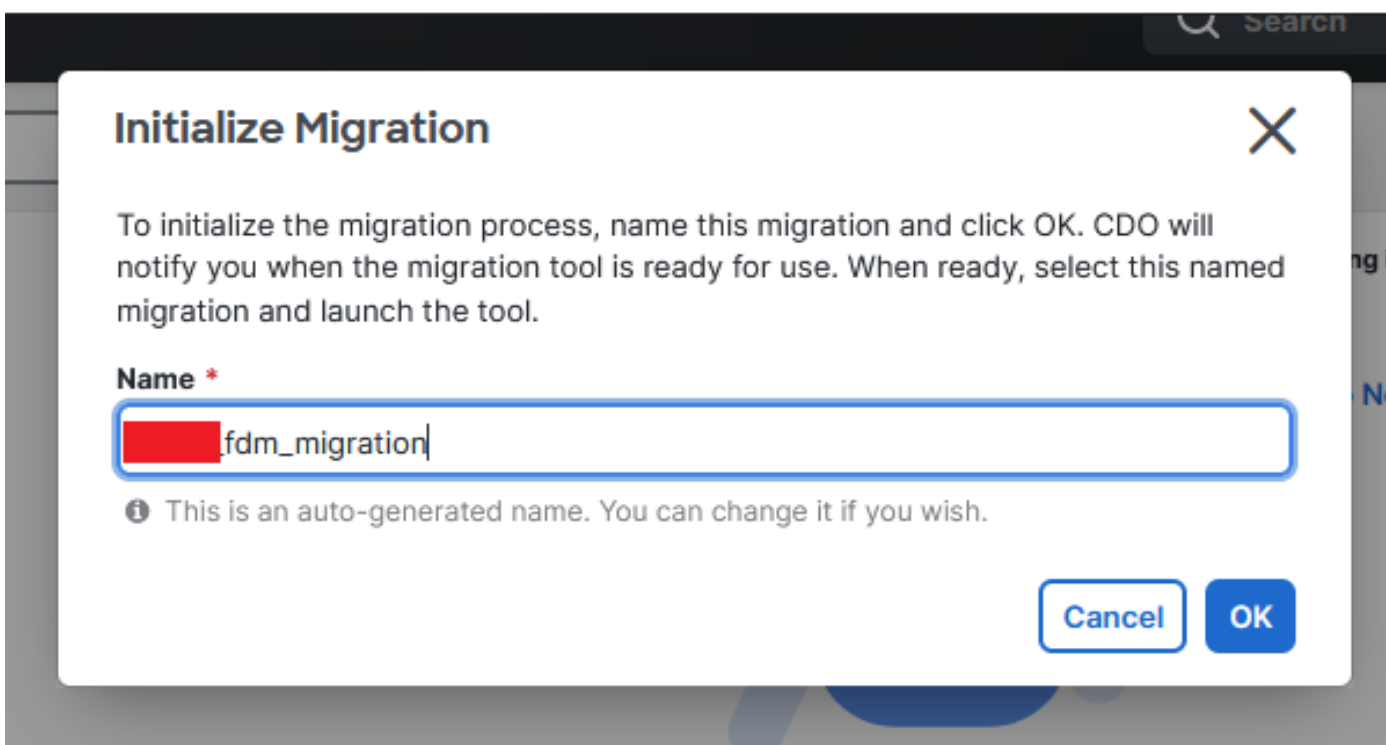
Una volta che FDM è stato caricato correttamente in CDO, è necessario disconnettersi da FDM. Dopo aver effettuato la disconnessione da FDM, passare in CDO a Strumenti e servizi > Migrazione > Strumento di migrazione firewall.



Fare clic sul simbolo Add per visualizzare un nome casuale, che indica che il nome deve essere rinominato per avviare il processo di migrazione.



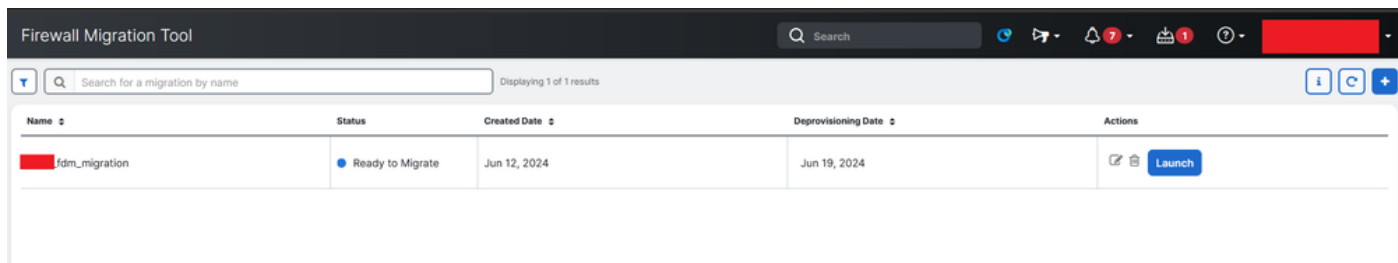
Dopo la ridenominazione, fare clic su Avvia per avviare la migrazione.






Inizializza migrazione

Fare clic su Avvia per avviare la configurazione della migrazione.



Name	Status	Created Date	Deprovisioning Date	Actions
fdm_migration	Ready to Migrate	Jun 12, 2024	Jun 19, 2024	

Processo di avvio della migrazione

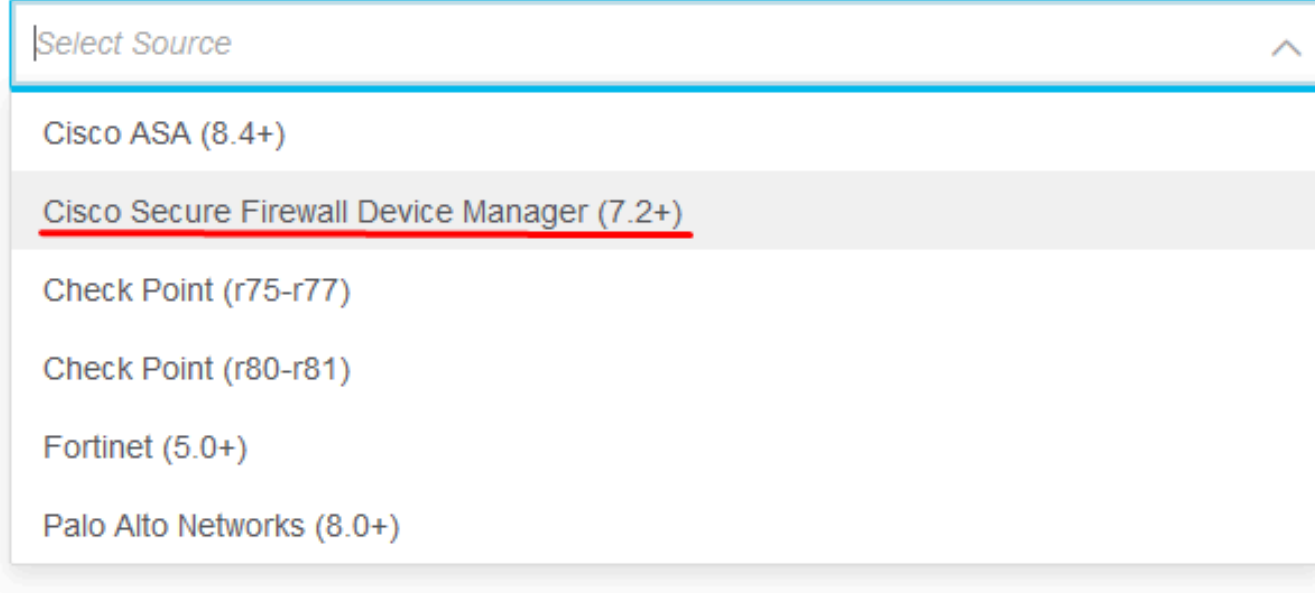
Dopo aver fatto clic su Launch (Avvia), viene visualizzata una finestra per il processo di migrazione in cui è selezionata l'opzione Cisco Secure Firewall Device Manager (7.2+). Come accennato in precedenza, questa opzione è abilitata a partire dalla versione 7.2.



## Firewall Migration Tool (Version 6.0.1)

### Select Source Configuration

Source Firewall Vendor



*Select Source*

- Cisco ASA (8.4+)
- Cisco Secure Firewall Device Manager (7.2+)
- Check Point (r75-r77)
- Check Point (r80-r81)
- Fortinet (5.0+)
- Palo Alto Networks (8.0+)

Configurazione selezione origine FMT

Una volta selezionate, vengono presentate tre diverse opzioni di migrazione: Solo configurazione condivisa, Include il dispositivo e le configurazioni condivise e Include il dispositivo e le configurazioni condivise per il nuovo hardware FTD.

Per questa istanza, viene eseguita la seconda opzione, Migrate Firepower Device Manager (Include Device & Shared Configuration).

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



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

Migrate Firepower Device Manager (Shared Configurations Only) >

Migrate Firepower Device Manager (Includes Device & Shared Configurations) v

- 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.
- User should provide FDM credentials to fetch details.
- 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 completely removed from FDM before migration.
- FMC should be registered to Smart Licensing Server.

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

### **Note :**

Opzioni di migrazione

Una volta selezionato il metodo di migrazione, procedere con la selezione del dispositivo dall'elenco fornito.

### Live Connect to FDM

- Select any FDM device onboarded on CDO from the below dropdown.
- Only devices with online connectivity and synced status will be displayed in the dropdown.
- Click on change device status button to update the FDM device status from In-Use to Available.

Select FDM Managed Device

████████\_fdm\_████████ - Available

Connect



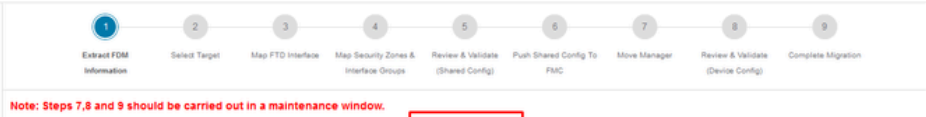
Selezione dispositivo FDM

**FDM device config extraction successful**



Estrazione configurazione completata

Si consiglia di aprire la scheda nella parte superiore per esaminare e capire in quale fase si trova quando il dispositivo è stato selezionato.



Note: Steps 7,8 and 9 should be carried out in a maintenance window.

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

Extraction Methods >

FDM IP Address:

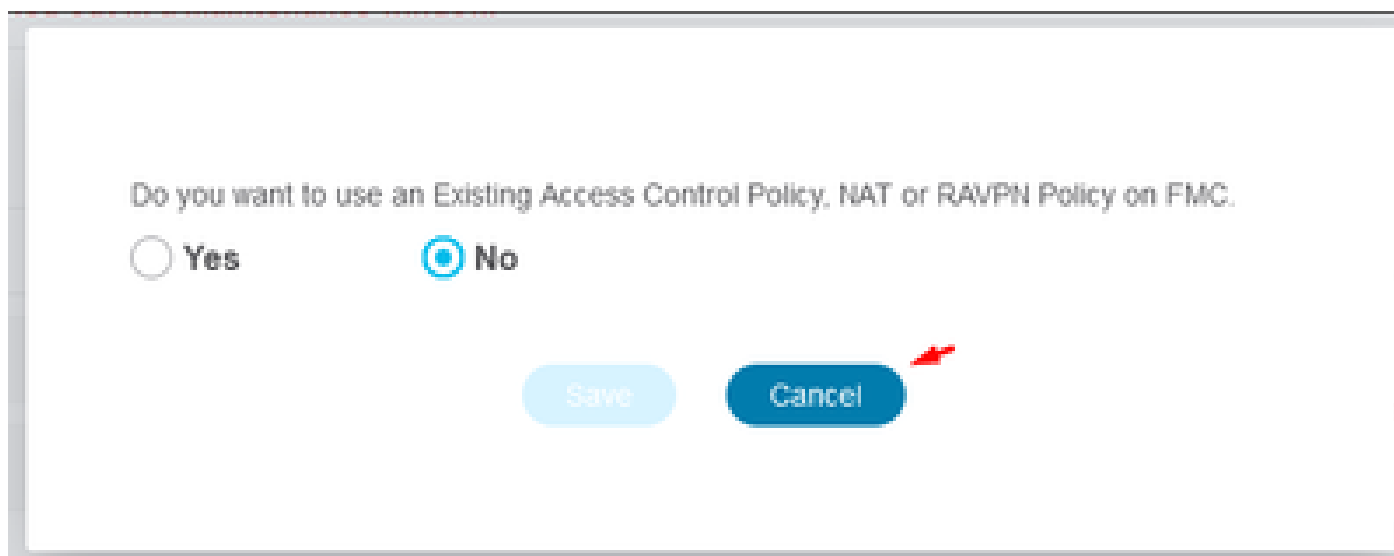
Parsed Summary

3 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/ RAVPN/IGRP)	4 Network Objects	0 Port Objects	1 Access Control Policy Objects (Geo, Application, URL, objects and Intrusion Rule Group)
0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)	2 Network Address Translation	2 Logical Interfaces	1 Routes (Static Routes, ECMP)	1 DHCP (Server, Relay, DDNS)
0	0	0	0	

Back Next

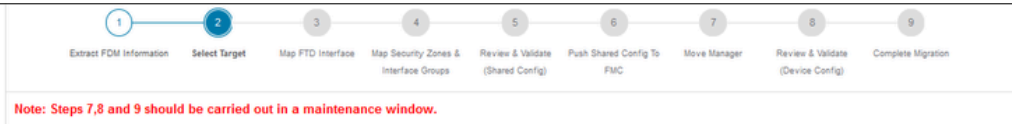
Fasi del processo di migrazione

Poiché si tratta di una nuova migrazione, selezionare Annulla quando richiesto con l'opzione "Utilizzare un criterio di controllo dell'accesso esistente, un criterio NAT o RAVPN in FMC?"



Opzione Annulla per la configurazione esistente

In seguito, saranno disponibili opzioni per selezionare le funzionalità da migrare, come mostrato nell'immagine. Fare clic su Continua.



### Select Target ⓘ

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

Firewall Management - Cloud-delivered FMC

Select Features

#### Device Configuration

- Interfaces
- Routes
  - ECMP
  - Static
  - BGP
  - EIGRP
- Site-to-Site VPN Tunnels (no data)
  - Policy Based (Crypto Map)
  - Route Based (VTI)
- Platform Settings
  - DHCP
    - Server
    - Relay
    - DDNS

#### Shared Configuration

- Access Control
  - Migrate tunnelled rules as Prefilter
- NAT
  - Network Objects
  - Port Objects(no data)
  - Access List Objects(Standard, Extended)
  - Access Control Policy Objects (Geolocation, Application, URL objects and Intrusion Rule Group)
  - Time based Objects (no data)
  - Remote Access VPN
  - File and Malware Policy

#### Optimization

- Migrate Only Referenced Objects
- Object Group Search ⓘ

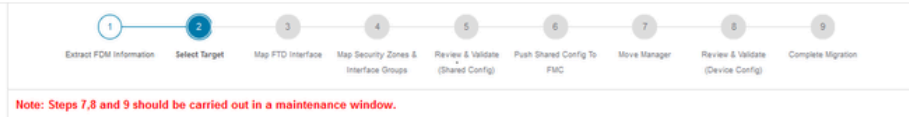
Proceed

Note: Platform settings and file and malware policy migration is supported in FMC 7.4 and later versions.

Caratteristiche da selezionare

Quindi Avvia Conversione.

Firewall Migration Tool (Version 6.0.1)



### Select Target ⓘ

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

Firewall Management - Cloud-delivered FMC

Select Features

Rule Conversion/ Process Config

Start Conversion

Avviare la conversione.

Al termine del processo di analisi, è possibile utilizzare due opzioni: Scaricare il documento e continuare con la migrazione facendo clic su Avanti.

## Select Target

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

Firewall Management - Cloud-delivered FMC

Select Features

Rule Conversion/ Process Config

Start Conversion

No parsing error 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

3 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/ RAVPI/EIGRP)	3 Network Objects	0 Port Objects	3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)	2 Network Address Translation	2 Logical Interfaces	1 Routes (Static Routes, ECMP)	1 DHCP (Server, Relay, DNS)
0 Site-to-Site VPN Tunnels	0 Remote Access VPN (Connection Profiles)			

Back

Next

Scarica il report.

Le interfacce del dispositivo sono impostate per la visualizzazione. È buona norma fare clic su **Aggiorna** per aggiornare le interfacce. Una volta convalidati, è possibile procedere facendo clic su **Avanti**.



Note: Steps 7,8 and 9 should be carried out in a maintenance window.

## Map FTD Interface

Source: Cisco Secure Firewall Device Manager (7.2+)  
Selected Option: Includes Device and Shared Config

Refresh

FDM Interface Name	FTD Interface Name
GigabitEthernet0/0	GigabitEthernet0/0
GigabitEthernet0/1	GigabitEthernet0/1

20 per page 2 | Page 1 of 1

Success  
Successfully gathered details!

Back

Next

Interfacce visualizzate

Passare alla sezione **Are** di sicurezza e gruppi di interfacce, dove è necessario aggiungere

manualmente con Add SZ & IG. Per questo esempio è stata scelta Creazione automatica. In questo modo è possibile generare automaticamente le interfacce all'interno del FMC in cui si esegue la migrazione. Al termine, fare clic sul pulsante Next (Avanti).

Firewall Migration Tool (Version 6.0.1)

Note: Steps 7,8 and 9 should be carried out in a maintenance window.

Map Security Zones and Interface Groups

Source: Cisco Secure Firewall Device Manager (7.2+)  
Selected Option: Includes Device and Shared Config

FDM Logical Interface ...	FDM Security Zones	FTD Interface	FMC Security Zones	FMC Interface Groups
outside	outside_zone	GigabitEthernet0/0	outside_zone (A)	Select Interface Groups
inside	inside_zone	GigabitEthernet0/1	inside_zone (A)	Select Interface Groups

Note: Click on Auto-Create button to auto map the FDM name as the name of the FMC interface objects and security zones. Click on next button to proceed ahead.

Aree di sicurezza e gruppi di interfaccia

L'opzione Creazione automatica mappa le interfacce FDM alle aree di sicurezza FTD e ai gruppi di interfacce esistenti in FMC con lo stesso nome.

## Auto-Create

Auto-create maps FDM 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 FDM interfaces

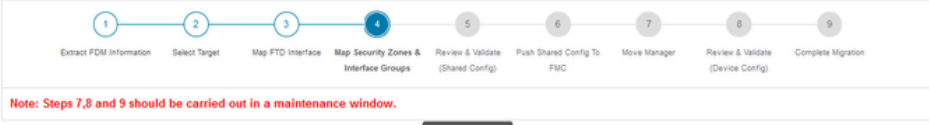
Security Zones  Interface Groups

Cancel Auto-Create


Opzione di creazione automatica.

Quindi scegliere Avanti.

Firewall Migration Tool (Version 6.0.1)





Note: Steps 7,8 and 9 should be carried out in a maintenance window.


Map Security Zones and Interface Groups 

Source: Cisco Secure Firewall Device Manager (7.2+)  
Selected Option: Includes Device and Shared Config

[Add SZ & IG](#) [Auto-Create](#)

FDM Logical Interface N...	FDM Security Zones	FTD Interface	FMC Security Zones	FMC Interface Groups
outside	outside_zone	GigabitEthernet0/0	outside_zone (A)	outside_ig (A) 
inside	inside_zone	GigabitEthernet0/1	inside_zone (A)	inside_ig (A) 

Note: Click on Auto-Create button to auto map the FDM name as the name of the FMC interface objects and security zones. Click on next button to proceed ahead.

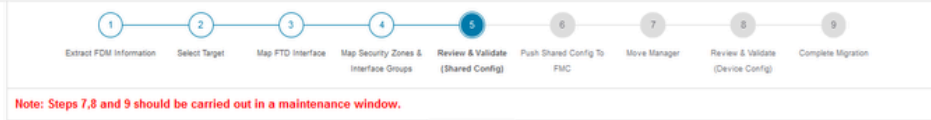
10  def.p938 2 |< < Page 1 of 1 > >|

[Back](#) [Next](#)

Dopo la creazione automatica, opzione.

Nel passaggio 5, come mostrato nella barra superiore, prendere il tempo necessario per esaminare i criteri di controllo di accesso (ACP), gli oggetti e le regole NAT. Continuare esaminando attentamente ciascun elemento e quindi fare clic su Convalida per confermare che non vi sono problemi con i nomi o le configurazioni.





Optimize, Review and Validate Shared Configuration Only

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

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

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

Select all 3 entries Selected: 0 / 3 Actions Save

Search

#	Name	Validation State	Type	Value
1	OutsidePv4Gateway	Validation pending	Network Object	172.16.1.1
2	OutsidePv4DefaultRoute	Validation pending	Network Object	0.0.0.0/0
3	Banned	Validation pending	Network Object	103.104.73.155

Page 1 to 3 of 3 | Page 1 of 1



Controllo dell'accesso, oggetti e configurazioni NAT

Quindi Push solo della configurazione condivisa

### Validation Status

✔ Successfully Validated

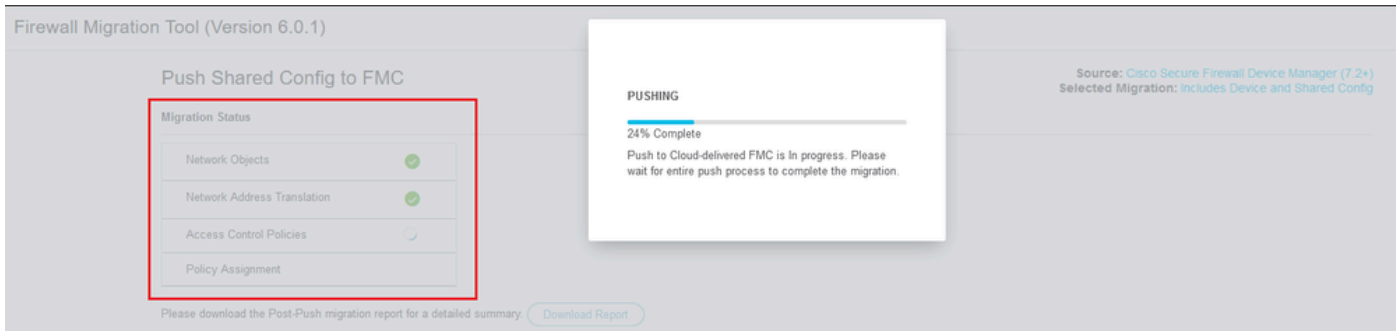
Validation Summary (Pre-push)

<b>3</b> Access Control List Lines	Not selected for migration Access List Objects <small>(Standard, Extended used in BGP/RAVPNEIGRP)</small>	<b>4</b> Network Objects	Not selected for migration Port Objects	<b>3</b> Access Control Policy Objects <small>(Geo, Application, URL objects and Intrusion Rule Group)</small>
<b>2</b> Network Address Translation	Not selected for migration Remote Access VPN <small>(Connection Profiles)</small>			

Push Shared Configuration Only

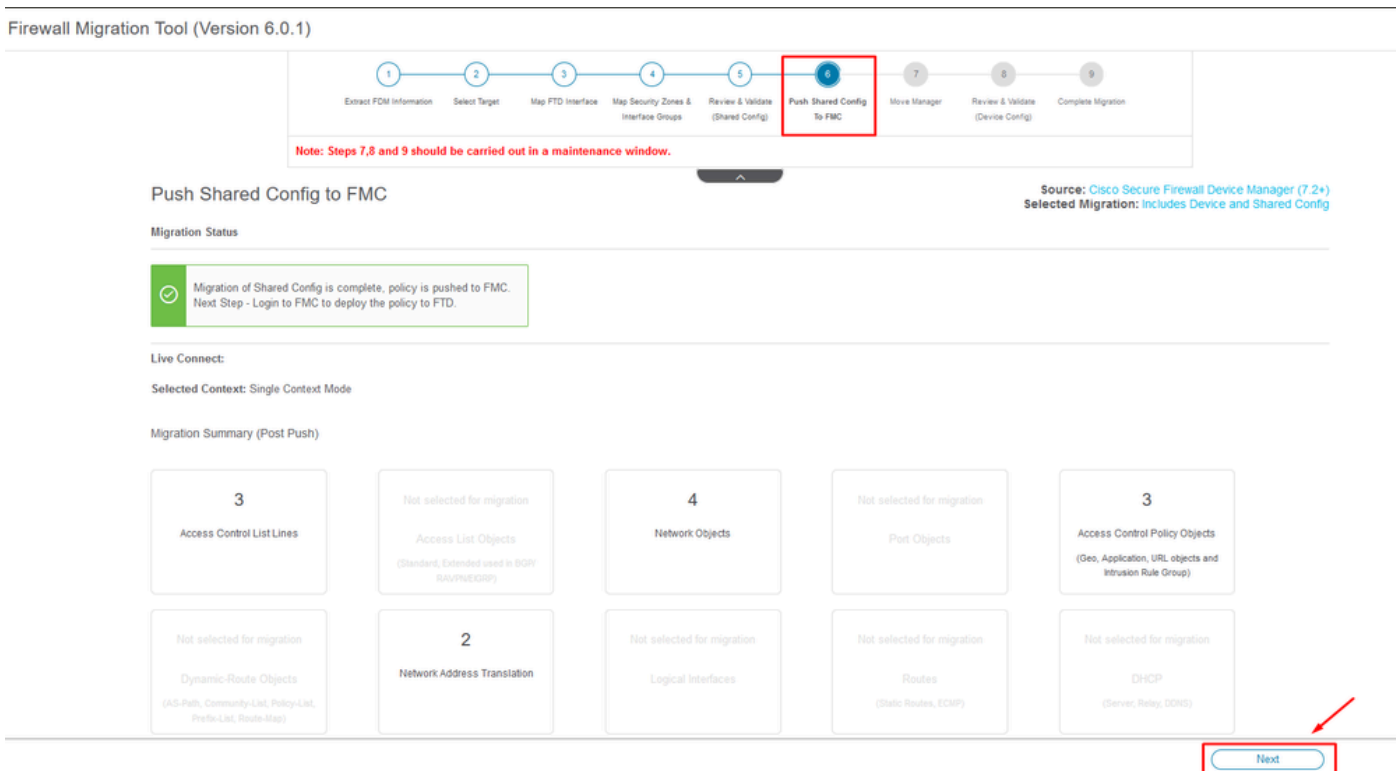
Push della sola configurazione condivisa

È possibile osservare la percentuale di completamento e l'attività specifica in corso di elaborazione.



Percentuale push

Dopo aver completato il passaggio 5, procedere al passaggio 6, come indicato nella barra superiore, in cui viene eseguita l'operazione Push Shared Configuration to FMC. A questo punto, selezionare il pulsante Avanti per avanzare.



Push della configurazione condivisa in FMC completato

Questa opzione attiva un messaggio di conferma che richiede di continuare la migrazione del manager.

---

# Confirm Move Manager

**Requires maintenance window to be scheduled**

**FDM manager will be moved to be managed in FMC.**

The steps outlined below should be performed in a maintenance window as 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.
- FDM devices enrolled with the cloud management will lose access upon registration with FMC.
- Ensure out-of-band access to the FTD device is available 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.
- FMC should be registered to Smart Licensing Server.

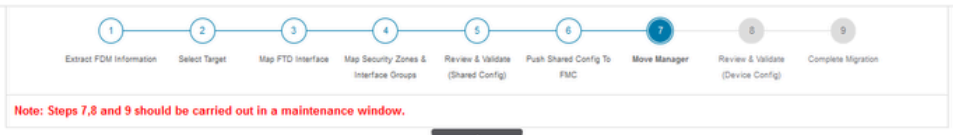
**I acknowledge all the steps mentioned above have been completed.**

Proceed

Cancel

Conferma gestione spostamenti

Per procedere con la migrazione del manager, è necessario disporre dell'ID del Management Center e dell'ID NAT, che è essenziale. Questi ID possono essere recuperati selezionando **Aggiorna dettagli**. Questa azione consente di avviare una finestra popup in cui viene immesso il nome desiderato per la rappresentazione FDM all'interno di cdFMC, quindi di salvare le modifiche.



### Move Manager

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

**Update Details**

This step is mandatory and should be performed during a downtime window. After you register the device with the management center or Cloud-delivered FMC, you can no longer use the device manager to manage it.

Management Cent...	Management Cente...	NAT ID	Threat Defense Hostn...	DNS Server Group	Management Center/ ...	Data Interface	
cisco	cdo			cloudapp.ni	CiscoUmbrellaDNSServerGroup	<input checked="" type="radio"/> Data <input type="radio"/> Management	Select Data Interface

Move Manager

### ID centro gestione e ID NAT

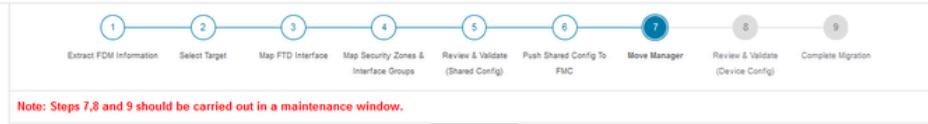
Aggiorna il nome del dispositivo per la registrazione.

Al termine dell'operazione, verranno visualizzati gli ID dei campi sopra indicati.



Avviso: non apportare modifiche all'interfaccia del centro di gestione. Per impostazione predefinita, l'opzione Gestione è selezionata. Lasciare questa opzione come impostazione predefinita.

---



Note: Steps 7,8 and 9 should be carried out in a maintenance window.

Move Manager

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

Update Details

This step is mandatory and should be performed during a downtime window. After you register the device with the management center or Cloud-delivered FMC, you can no longer use the device manager to manage it.

Management Cent...	Management Cente...	NAT ID	Threat Defense Hostn...	DNS Server Group	Management Center/ ...	Data Interface
cisco	us.cdo...	ogp	166GW/ 104v	3aPMT	fdm-Azure	CiscoUmbrellaDNSServerGroup
						<input checked="" type="radio"/> Data <input type="radio"/> Management
						Select Data interface

Save

Move Manager

ID centro di gestione e ID NAT.

Dopo aver scelto l'opzione Update Details (Aggiorna dettagli), indica il dispositivo da sincronizzare.

Sincronizzazione dispositivo FDM

Dopo aver completato la migrazione, il passaggio successivo consiste nell'esaminare le interfacce, le route e le impostazioni DHCP configurate in FDM selezionando Convalida.



Optimize, Review and Validate Device Configuration Page

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

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

Static PPPoE

Select all 2 entries Selected: 0 / 2

Search

#	Interface	Zone	IP Address	State
1	GigabitEthernet0/0	outside_zone		Enabled
2	GigabitEthernet0/1	inside_zone	10.1.1.1	Enabled

Page 1 to 2 of 2 Page 1 of 1

Validate

Convalida impostazioni di configurazione di FDM

Dopo la convalida, scegliere Push Configuration per avviare il processo di push della configurazione, che continuerà fino al termine della migrazione. È inoltre possibile monitorare le attività in esecuzione.

### Validation Status

✔ Successfully Validated

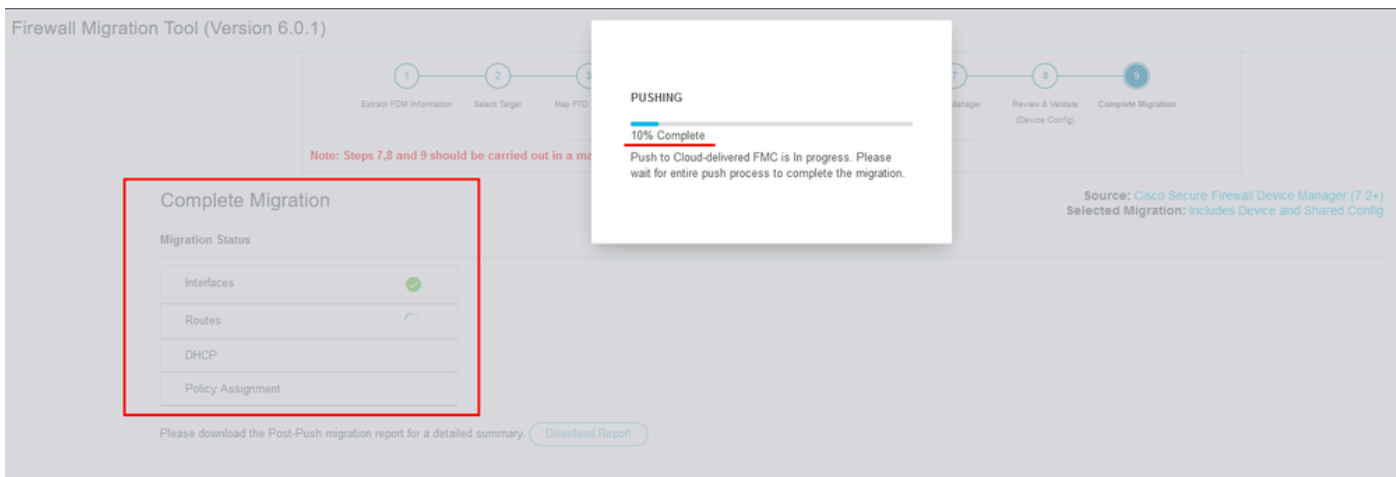
Validation Summary (Pre-push)

Not selected for migration Access List Objects <small>(Standard, Extended used in BGP/RAVPN/EIGRP)</small>	Not selected for migration Dynamic-Route Objects <small>(AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)</small>	2 Logical Interfaces	1 Routes <small>(Static Routes, ECMP)</small>	1 DHCP <small>(Server, Relay, DDNS)</small>
Not selected for migration Site-to-Site VPN Tunnels	0 Platform Settings <small>(snmp,http)</small>	0 Malware & File Policy		

Push Configuration

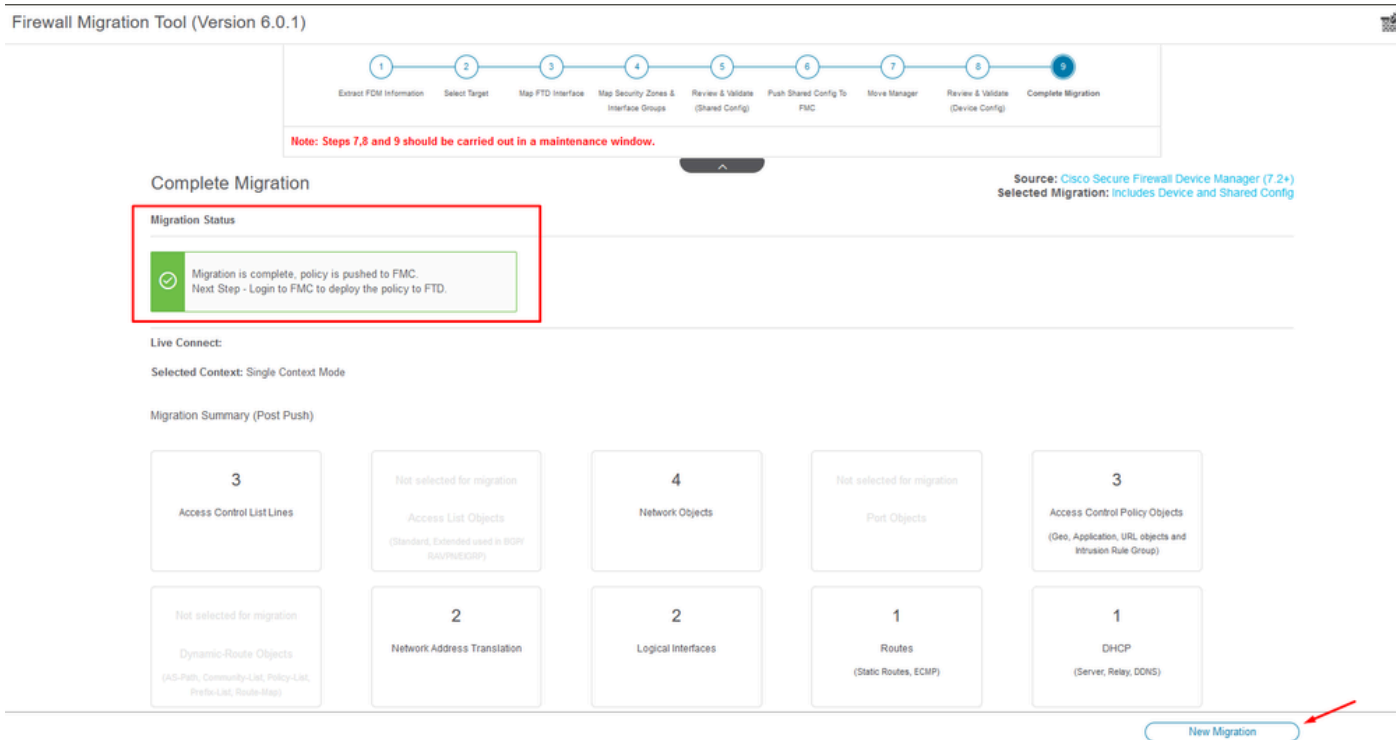
Stato convalida - Configurazione push.

Finestra popup con la configurazione di push percentuale.



Percentuale push completata

Al termine, viene presentata un'opzione per avviare una nuova migrazione, che segna la fine del processo di migrazione da FDM a cdFMC.



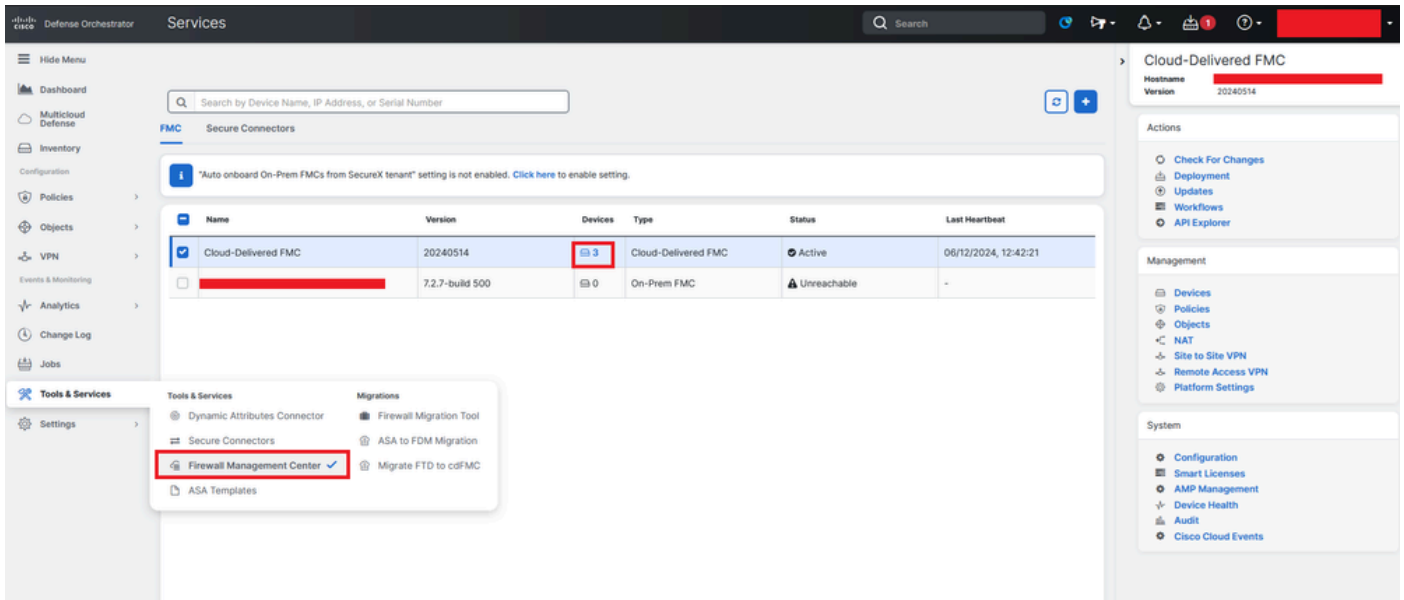
Migrazione completa

## Verifica

Per verificare che la migrazione di FDM a cdFMC sia stata completata.

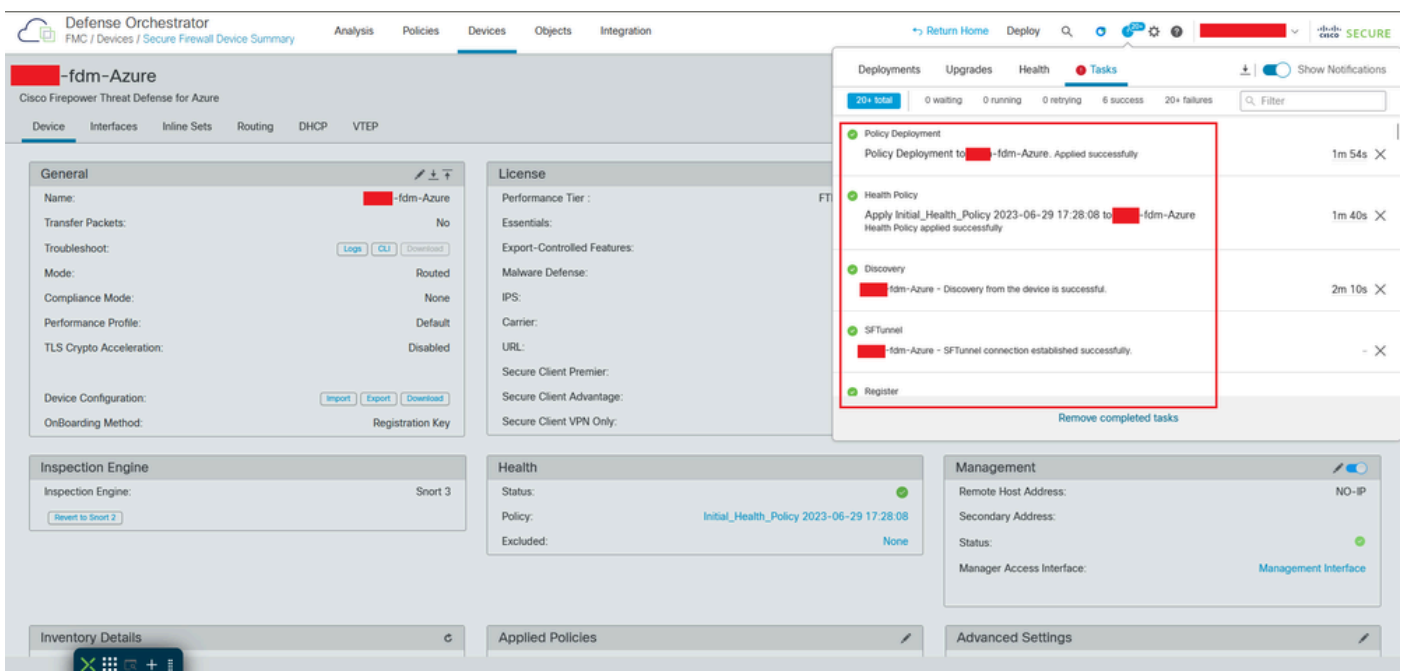
Selezionare CDO > Strumenti e servizi > Firepower Management Center. In questo caso, il numero di dispositivi registrati è aumentato.





Dispositivi registrati in cdFMC

Controllare il dispositivo in Dispositivi > Gestione dispositivi. Inoltre, nell'ambito delle attività del FMC, è possibile verificare quando il dispositivo è stato registrato correttamente e la prima distribuzione è stata completata correttamente.



Attività di registrazione di cdFMC completata.

La periferica è su cdFMC > Periferica > Gestione periferiche.

Defense Orchestrator  
FMC / Devices / Device Management

Analysis Policies Devices Objects Integration

Return Home Deploy Search

View By: Group

All (3) Error (0) Warning (0) Offline (0) Normal (3) Deployment Pending (3) Upgrade (0) Short 3 (3)

Migrate | Deployment History

Search Device Add

Download Device List Report

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rollback
Ungrouped (3)						
fdm-Azure N/A - Routed	FTDv for Azure	7.4.1	N/A	Essentials	None	

Periferica registrata su cdFMC

Criteri di controllo di accesso migrati in Criteri > Controllo di accesso.

Defense Orchestrator  
FMC / Policies / Access Control / Access Control

Analysis Policies Devices Objects Integration

Return Home Deploy Search

Object Management | Intrusion | Network Analysis Policy | DNS | Import/Export

New Policy

Access Control Policy	Status	Last Modified	Lock Status
Default Access Control Policy Default Access Control Policy with default action block	Targeting 0 devices	2024-06-11 22:28:19 Modified by "Firepower System"	
FTD-Mig-ACP-1718216278	Targeting 1 devices Up-to-date on all targeted devices	2024-06-12 12:18:00 Modified by [redacted]	

Criteri di migrazione

Analogamente, è possibile esaminare gli oggetti creati in FDM di cui è stata eseguita correttamente la migrazione a cdFMC.

Network

Add Network Filter

Show Unused Objects

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.

Name	Value	Type	Override
any	0.0.0.0/0 :::0	Group	
any-ipv4	0.0.0.0/0	Network	
any-ipv6	:::0	Host	
Banned	103.104.73.155	Host	✔
Gw_test01	172.22.2.1	Host	
Inside_Network_IP	192.168.192.10	Host	✔
IPv4-Benchmark-Tests	198.18.0.0/15	Network	
IPv4-Link-Local	169.254.0.0/16	Network	
IPv4-Multicast	224.0.0.0/4	Network	
IPv4-Private-10.0.0.0-8	10.0.0.0/8	Network	
IPv4-Private-172.16.0.0-12	172.16.0.0/12	Network	
IPv4-Private-192.168.0.0-16	192.168.0.0/16	Network	
IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group	
IPv6-IPv4-Mapped	:::ffff:0.0.0.0/96	Network	

Oggetti migrati da FDM a cdFMC

Interfacce di gestione degli oggetti migrate.

Defense Orchestrator  
FMC / Objects / Object Management

Analysis Policies Devices **Objects** Integration

Return Home Deploy Q Filter

SECURE

### Interface

Add Filter

Interface objects segment your network to help you manage and classify traffic flow. An interface object simply groups interfaces. These groups may span multiple devices; you can also configure multiple interface objects on a single device.

Name	Type	Interface Type	
inside_ig	Interface Group	Routed	
> fdm-Azure			
inside_zone	Security Zone	Routed	
> fdm-Azure			
outside_ig	Interface Group	Routed	
> fdm-Azure			
outside_zone	Security Zone	Routed	
> fdm-Azure			

Migrazione delle interfacce di gestione degli oggetti completata.

## 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).