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.



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.

cisco Defense Orchestrator	Inventory	Q Search	⁰ ঈr- 众₀- ఊၢ ଉ	-
E Hide Menu	Convices Templates Q Search by Device Name IP Address or Serial Number	Displaying 8 of 8 results		
A Dashboard	All ASA FTD			
Multicloud Defense	Name ‡	Configuration Status \$	Connectivity \$	

FDM integrato, aggiungere opzione

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



Seleziona tipo di dispositivo o servizio

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

Follow the steps below				Cancel
FTD 0000	A Important: This method of onbo delivered Firewall Management Sy	oarding allows for local co-managem stem, click the FTD button instead. I	nent of the firewall via FDM. To man Learn more 🗗	age your device with cloud-
Firewall Threat Defense Management Mode: FTD FTD FFDM FDM (Recommended)	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.	
	X			

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

F		A 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	-
M: C (R	anagement Mode:) FTD () FDM (ecommended)	Use Registration Key Use Serial Number Use Credentials (Basic) Onboard a device using a registration key generated from CD0 and applied on the device using Firepower Device Manager. Use Serial Number Use Credentials (Basic) Onboard a device using Firepower Device Manager. Use this method for low-touch provisioning or for onboarding configured devices using their serial number. Onboard a device using a registration (FTD 6.7+, 1000, 2100 and 3100 series only) Use this method for low-touch provisioning or for onboarding address, or host name, and a username and password.	
1	Device Name		
2	Database Updates	Enabled	
3	Create Registration Key	7a53c	
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.

Monitoring	Policies	 Objects	Device: joroa-fdm-tech
Device Summa Cloud Se Not Reg	ry rvices Istered		
You can register use Cisco Defer register with th auto-enroll with want to use Ser configure Smar register with th	er the device w nse Orchestra e cloud using h CDO or a Se cure Firewall o t Licensing, w e cloud, you c	vith the Cisco clo tor (CDO) for ma your CDO or oth cure Firewall Ma device manager f hich automatical an enable or dis	bud to use additional cloud-based services. If you want to anagement or want to remain in evaluation mode, then er security account registration key. You can alternatively anagement Center using the device serial number. If you for management and are ready to license the device, then lly registers the device with the Cisco cloud. After you able features as needed.
Enrollment Typ	e		
Region US Region			~ ()
Registration Ke	у		
7a53c2t			
Service En	rollment		
Cisco D	efense Orc	hestrator	
Cisco Defe devices. S account.	ense Orchestra elect this optic	ator is a cloud-b on if you want to	ased management tool used for managing network register the device in your Cisco Defense Orchestrator
🔽 Enabl	e Cisco Defen	se Orchestrator	
Cisco S	uccess Net	work	
Cisco Suc essential f product ar of the prod	cess Network or Cisco to pro nd to make you duct in your ne	enablement prov ovide technical s u aware of unuse stwork.	vides usage information and statistics to Cisco which are support. This information also allows Cisco to improve the ad available features so that you can maximize the value
Check out	the Sample D	ata that will be s	ent to Cisco. See more 🗸
🚦 🔽 Enroll	Cisco Succes	s Network	
REGISTER	Need he	lp? 🖸	

Registrazione FDM

Quando si registra FDM, vengono visualizzati i servizi tenancy, Cloud connessi e Registrati.



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.

stitudis cisco: Defense Orchestrator	Inventory		Q Search C 🎝 -	¢•• ±• •••
Hide Menu	Constant Sector Se	umber Disp	laying 9 of 9 results	FOM 2 Device Details
Multicloud Defense	Kane :	Configuration Status 🗢	Connectivity \$	Model Cisco Firepower Threat Defense for Azure Serial
Configuration Policies		•	Unreachable Serial Number Mismatch	Orbaading Registration Key Method Snort Version 3.1.53.100-56
coopects → cb VPN → Events & Monitoring	C FTD	Ø Not Synced	Pending Setup	Syncing CDO is communicating with your device. Please check back in a moment.
√ Analytics →	O FTD		Pending Setup	Device Actions
(+) Jobs			Pending Setup	API Tool Workflows Manage Backups Remove
Settings >	FDM FDM	S Syncing	Online	Management
	O FTD	•	Online	Notes Changelog Executive Report
	O FTD	•	Online	La Conflict Detection
		O Not Synced	A Unreachable	Check every: Tenant default (24 hours) -
				Label Groups and Labels

Inventario CDO integrato in FDM

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

FDM FDM	O Synced	Online

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.

% Tools & Services		Tools & Services	Migrations
	>	Dynamic Attributes Connector	Firewall Migration Tool
			會 ASA to FDM Migration
		🖨 Firewall Management Center	會 Migrate FTD to cdFMC
		ASA Templates	

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

() GL Search for a migra	ption by name	Displaying 0 of 0 results			IC I
Name 2	Status	Created Date: 0	Depreciationing Date: g	Actions	/
	No mij	rations found. Begin migrating AS	GA, FDM, Checkpoint, Fortinet, or Palo Alto Networks Trewalls to FTD.		

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



Inizializza migrazione

Fare clic su Avvia per avviare la configurazione della migrazione.

Firewall Migration Tool			Q Search	<mark>ଓ</mark> ⊳,-	¢ ? • ∰1	? -	
Q Search for a migration by name		Displaying 1 of 1 results					i C +
Name ©	Status	Created Date ©	Deprovisioning Date		Actions		
fdm_migration	 Ready to Migrate 	Jun 12, 2024	Jun 19, 2024		C 🔒 Launch		

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).

) C	lick 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)	\sim
	 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 polcies 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.	

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
Select FDM Managed Device
fdm_fdm_fdm_fdm_fdm_fdm_fdm_fdm_fdm_fdm_
Connect

Selezione dispositivo FDM

FDM device config extraction successful	
100% Complete	
	_

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.



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?"

Do you want to use an Existing Access Control Policy, NAT or RAVPN Policy on FMC.	
🔿 Yes 💿 No	ī
Save Cancel	

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.

	1	-2	3	4	5	6	7	8	9	
	Extract FDM Information	Select Target	Map FTD Interface	Map Security Zones & Interface Groups	Review & Validate (Shared Config)	Push Shared Config To FMC	Move Manager	Review & Validate (Device Config)	Complete Migration	
	Note: Steps 7,8 and 9 should	d be carried o	out in a maintena	nce window.						
Select Target 🗿					<u>^</u>			Sele	ource: Cisco Secure Fi sted Migration: Includ	rewall Device Manager (7.2+) es Device and Shared Config
Firewall Management - 0	Cloud-delivered FMC									>
Select Features										~
Device Configuration		S	nared Configura	ation				Optimization		
✓ Interfaces		~	Access Control				1	Migrate Only Re	ferenced Objects	
Routes			🧹 Migrate tunr	nelled rules as Pref	ilter		[Object Group S	earch 🕕	
ECMP			NAT							
Static		~	Network Objects							
BGP			Port Objects(no	data)						
EIGRP			Access List Obj	ects(Standard, Ext	ended)					
Site-to-Site VPN Tunn	els (no data)		Access Control	Policy Objects (Ge	olocation, Applic	ation, URL objects a	nd Intrusion Rul	8		
Policy Based (Cry	pto Map)		Group)	octe (no data)						
Route Based (VT	0		Demote Access	VDN						
Platform Settings			File and Mahuam	Doliou						
- DHCP			_ rile and maiware	Poncy						
Server										
Relay										
DDNS										
Proceed										
Note:Platform settings an	d file and malware policy migrat	tion is supporte	d in FMC 7.4 and I	ater versions.						

Caratteristiche da selezionare

Quindi Avvia Conversione.

Firewall Migration Tool (Version 6.	0.1)									
	1	2	3	4	5	6	7	8	9	
	Extract FDM Information	Select Target	Map FTD Interface	Map Security Zones & Interface Groups	Review & Validate (Shared Config)	Push Shared Config To FMC	Move Manager	Review & Validate (Device Config)	Complete Migration	
	Note: Steps 7,8 and 9 should	d be carried ou	t in a maintena	nce window.		_				
Select Target 🕡					^	,		Sciences	ource: Cisco Secure Firewa sted Migration: Includes D	III Device Manager (7.2+) Nevice and Shared Config
Firewall Management -	Cloud-delivered FMC									>
Select Features										>
Rule Conversion/ Proce	ess 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.



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.

	1 Extract FDM Information	2 Select Target Map	9 FTD Interface Map Se Inter	4 eourity Zones & rface Groups	5 Review & Validate (Shared Config)	6 Push Shared Config To FMC	7 Move Manager	8 Review & Validate (Device Config)	9 Complete Migration				
	Note: Steps 7,8 and 9 should	be carried out in	a maintenance wi	indow.									
Map FTD Interface	0					Refresh	Sc Se	elected Option: I	ure Firewall Device Manag ncludes Device and Share	er (7.2+) d Config			
FDM Interface Name		FTD Int	terface Name										
GigabitEthernet0/0		GigabitEther	rnet0/0										
GigabitEthernet0/1		GigabitEther	rnet0/1										
20 v perspage 2 4	A Page 1 of 1 ▶ ▶]									Back	Next	Success Successfully ga	thered details!

Interfacce visualizzate

Passare alla sezione Aree 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).

	Extract FDM Information Select T	3 Arget Map FTD Interface Map Sec Interf	6 6 curity Zones & Review & Validate Push Shared of face Groups (Shared Config) FMC	Config To Move Manager Review & Valid (Device Confi	9 ste Complete Migration g)
	Note: Steps 7,8 and 9 should be car	ried out in a maintenance wi	ndow.		
Map Security Zone	es and Interface Groups 💿			Add SZ & IG Auto-Create	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 v	
inside	inside_zone	GigabitEthernet0/1	inside_zone (A)	Select Interface Groups ~	

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.

		Charot
FTD		Group
Gigabiti	Auto-Create	ups
Gigabiti	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.	ups
	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)					
	Extract FDM Information Sele	2 3 ct Target Map FTD Interface Map 5 Interface Map 5	S S	6 7 d Config To Move Manager MC	8 Review & Validate (Device Config)	9 Complete Migration
	Note: Steps 7,8 and 9 should be	carried out in a maintenance w	vindow.			
Map Security Z	ones and Interface Groups	D				Source: Cisco Secure Firewall Device Manager (7.2+) Selected Option: Includes Device and Shared Config
				Add SZ & IG	uto-Create	
FDM Logical Inter	face N FDM Security Zones	FTD Interface	FMC Security Zones	FMC Interface G	roups	
outside	outside_zone	GigabitEthernet0/0	outside_zone (A)	outside_ig (A)	v	
inside	inside_zone	GigabitEthernet0/1	inside_zone (A)	inside_ig (A)	÷	
Note;Click on Auto-Cn	eate button to auto map the FDM nameif a	s the name of the FMC interface of	bjects and security zones. Click on next	button to proceed ahead.		
10 v prr.04939 2	[4 4 Page 1 of 1 ≽ ≽]					×.
						Figsk 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.

Firewall Migration	n Tool	(Versio	on 6.0.1)				
			[1] [2] Extract FDM Information Select Target	3 4 5 Map FTD Interface Map Security Zones & Review & Validate Interface Groups (Shared Config)	B 7 Push Shared Config To Move Manager FMC	8 9 Review & Validate Complete Migration (Device Config)	
			Note: Steps 7,8 and 9 should be carried or	It in a maintenance window.			
	Optir	mize, R	Review and Validate Shared Conf	iguration Only 💿	,	Source: Cisco Secure Fire Selected Migration: Includes	vall Device Manager (7.2+) Device and Shared Config
	Access	Control	Objects NAT Interfaces Routes Site-to-Si	te VPN Tunnels 🕜 Remote Access VPN SI	IMP DHCP		
	Acce	ess List Obj lect all 3 ent	iects Network Objects Port Objects Access Con tries Selected: 0/3 Actions Conversion	trol Policy Objects VPN Objects Dynamic-Rout	e Objects	Q Search	<u>+</u>
	•	*	Name Q	Validation State	Туре	Value	
	0	1	OutsidePv4Gateway	Validation pending	Network Object	172.18.1.1	
		2	OutsideIPv4DefaultRoute	Validation pending	Network Object	0.0.0/0	
		3	Banned	Validation pending	Network Object	103.104.73.155	
erpage 1 to3 of3 [4 ∢	Page	1_ of 1_1	► H			Thirde	1

Controllo dell'accesso, oggetti e configurazioni NAT

Quindi Push solo della configurazione condivisa

		Successfully Validat	ed	
dation Summary (Pre-pu	ush)			
3		4		3
ccess Control List Lines		Network Objects		Access Control Policy
				(Geo, Application, URL objects and Intrusion Rule Group)
2	Not selected for migration			
Network Address Translation				

Push della sola configurazione condivisa

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

Firewall Migrati	on Tool (Version 6.0.1)				
	Push Shared Config to I	FMC		DITCHING	Source: Cisco Secure Firewall Device Manager (7.2+) Selected Migration: Includes Device and Shared Config
	Migration Status			24% Complete	
	Network Objects	Ø		Push to Cloud-delivered FMC is In progress. Please wait for entire push process to complete the migration.	
	Network Address Translation	0			
	Access Control Policies	0			
	Policy Assignment				
	Please download the Post-Push migration	n report for a detailed sur	mmary. Download		

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.

on Tool (Version 6.0.	1)					
	Extract P	1 2 3 DM Information Select Target Map FTD Inte	rface Map Security Zones & Review & Validate Interface Groups (Shared Config)	A shared Config Nove Manager Review & Valdam Do FINC (Device Config)	9 Complete Migration	
1	Note: Steps 7,8	and 9 should be carried out in a main	tenance window.			
Push Shared Con	nfig to FM	С		s	Source: Cisco Secure Firewall Device Mar	nager (7.2+) bared Confin
Migration Status					erected migration. Includes bence and on	larea coning
Migration of Shared C Next Step - Login to I Live Connect: Selected Context: Single Co	Config is complet FMC to deploy th	e, policy is pushed to FMC. te policy to FTD.				
Migration Summary (Post P	'ush)					
3 Access Control List Lines	5		4 Network: Objects		3 Access Control Policy Objects	
					(Geo, Application, URL objects and Intrusion Rule Group)	
		2				
		Network Address Translation				
	Push Shared Col Migration Status Migration Status Migration of Shared of Next Step - Login to Live Connect: Selected Context: Single Co Migration Summary (Post P Access Control List Line Not selected for migrated	Image: Status Image: Status <td< td=""><td>Image: Control List Lines Image: Control List Lines Image:</td><td>Image: Device of bit Memories Image: Device of bit Microsoft Device Control Config to FMCC Mage: Device of bit Microsoft Device of bit Mic</td><td>Image: Control List Lines Image: Control List Lines <td>Image: State of Control List List Control Image: Control List List Control C</td></td></td<>	Image: Control List Lines Image:	Image: Device of bit Memories Image: Device of bit Microsoft Device Control Config to FMCC Mage: Device of bit Microsoft Device of bit Mic	Image: Control List Lines Image: Control List Lines <td>Image: State of Control List List Control Image: Control List List Control C</td>	Image: State of Control List List Control Image: Control List List Control C

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 maintainence window to be scheduled FDM manager will be moved to be managed in FMC.



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.

Firewall Migration Tool (Version	n 6.0.1)										
		1	2 3			6	0	8	9		
		Extract FDM Information	Select Target Map FTD Inter	face Map Security Zones & Interface Groups	Review & Validate (Shared Config)	Push Shared Config To FMC	Move Manager	Review & Validate (Device Config)	Complete Migration		
	Note:	Steps 7,8 and 9 should I	e carried out in a maint	enance window.							
Move Manag	ger				^			Selec	urce: Cisco Sec ted Migration:	cure Firewall Device Includes Device an	e Manager (7.2+) nd Shared Config
	e Details	d be performed during a	a downtime window. Aft	er you register the de	vice with the ma	anagement center	or Cloud delive	red EMC, you ca	n no longer use	the device manage	er to manage it
Management Ce	nt M	anagement Cente 🕕	NAT ID 🕢	Threat D	efense Hostn	DNS Server	Group	Managemer	nt Center/	Data Interface	
cisco	cdo			i	Lciouda	app.n CiscoUmbrellaDN	SServerGroup ~	💿 Data 🔵 Ma	inagement	Select Data Interface	×

ID centro gestione e ID NAT

wall Migration Tool (version 6.	0.1)			×			
	1 Extract FCM Information Set	2 Upd	ate Device Name for F	Registration	8 9 Review & Validate Complete Migration (Device Config)		
	Note: Steps 7,8 and 9 should be	carried - fdm-					
Move Manager			Cancel Save		Source: Cisco Se Selected Migration:		
	_						
Update De This step is mandatory a	ails	downtime			d FMC, you can no longer use	the device manager to	manage it.
Update De This step is mandatory a Management Cent	nd should be performed during a d	Jowntime NAT ID 💿	Threat Defense Hostn	DNS Server Group	d FMC, you can no longer use Management Center/	the device manager to Data Interface	manage it.
Update Det This step is mandatory a Management Cent cisco-mex-optie-lac app us co	aais and should be performed during a d Management Cente •	Jowntime NAT ID	Threat Defense Hostn	DNS Server Group CiscoUmbrellaDNSServerGroup ~	d FMC, you can no longer use Management Center/	be the device manager to a Data Interface	manage it. v

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.

Image: Second	Image: the set of the se										
Excest FDM Information Select Target Map FTD Interface Map FTD Interface Review & Valdatas Pach Shand Gorfg To New Manager Review & Valdatas Comparis Map store Move Steps 7,8 and 9 should be carried out in a maintenance window. Interface Groups Review & Valdatas Comparis Map store Source: Cisco Secure Firewall Device Map Selected Migration: Includes Device and Sh Update Details Threat Defense Hostn DNS Server Group Management Center/ Data Interface Gisco us.ob. 699 4560W 104V 3PRIf Min-Azure CiscoUnterelaDNISServerGroup Management Select Data Interface	Extract FDU Internation Select Target Hag FTD Interface Review & Valdatas Pack Braved Config % Neve Manager Review & Valdatas Complete Manager Move Manager Source: Cisco Secure: Firewall Device Manager Source: Cisco Secure: Firewall Device Manager Update Details Image: Config % Nat ID % The real Defense Hostin DNS Server Group Management Center/ Data Interface Management Center NAT ID % Threat Defense Hostin DNS Server Group Management Center/ Data Interface Gisco us colo 999 9660W 104V 3aPU Gisco/UnderlaDNSServerGroup Data Management Select Data Interface		()	-2(3(5	-6	-0-	8	9	
Note: Steps 7,8 and 9 should be carried out in a maintenance window.	Note: Steps 7,8 and 9 should be carried out in a maintenance window.		Extract FOM Information	Select Target Map FTC	D Interface Map Security Zones & Interface Groups	Review & Validate (Shared Config)	Push Shared Config To FMC	Move Manager	Review & Validate (Device Config)	Complete Migration	
Move Manager Update Details This step is mandatory and should be performed during a downline window. After you register the device with the management center or Cloud-delivered FMC, you can no longer use the device manager to Management Center Management Center Management Center Management Center Management Center Management Center Data Interface ge #860W/ 104V BARM Hoth Azure CascoUntertaIDNSServerGroup Data Management Select Data Interface CascoUntertaIDNSServerGroup Data Management Select Data Interface CascoUntertaIDNSServerGroup Data Management Select Data Interface CascoUntertaIDNSServerGroup Management Select Data Interface CascoUntertaIDNS Select S	Move Manager Update Details This step is mandatory and should be performed during a downline window. After you register the device with the management center or Cloud-delivered FMC, you can no longer use the device manager to Management Cente Nat ID Threat Defense Hostn DNS Server Group Management Center/ Data Interface us.cos us.cos 099 10500W 104'9 28PW1 10m-Azure ClacoUmbretaDNSServerGroup ClacoUmbretaDNSSe		Note: Steps 7,8 and 9 shou	Ild be carried out in a m	naintenance window.						
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 Management Center. Management Center. NAT ID NAT ID Threat Defense Hostn DNS Server Group Management Center/ Data Interface Gisco	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 Management Center Management Cent Management Center NAT ID • Threat Defense Hostn DNS Server Group Management Center/ Data Interface cisco us colo. 0go 104/v 3aPUi fdm-Azure CiscoUnbretaDNSServerGroup ~ • Data Interface	Move Manage	r			^			Sol		
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 Management Cente Management Cente NAT ID NAT ID Threat Defense Hostn DNS Server Group Management Center/ Data Interface Select Data Interface Ogu Select Data Interface CascoUntrelaDNSServerGroup Data Management Select Data Interface	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 Management Cent Management Cente NAT ID • Threat Defense Hostn DNS Server Group Management Center/ Data Interface Cisco us.cdo 0po 1660W (104V 3aPW) Mm-Azure CiscoUmbreIsDNSServerGroup ~ • Data Management Select Data Interface								Select	ed Migration:	cure Firewall Device Includes Device and
Management Cent Management Cente NAT ID Threat Defense Hostn DNS Server Group Management Center/ Data Interface Cisce uis cdu Dgu i866W 104V 35PH 1dm.Azure CiscoUnbrelaDNSServerGroup Imagement Select Data Interface	Management Cent Management Cente NAT ID Threat Defense Hostn DNS Server Group Management Center/ Data Interface cisco uis.cdo ogo 1660W 104V 3sPit fdm-Azure CiscoUntretaDNSServerGroup ~ © Data Management Select Data Interface	_							Select	ed Migration:	cure Firewall Device I Includes Device and
cisco us.cdo ogu 19560W 104V 3sPM 16th-Azure CiscoUmbrelaDHSServerGroup ~ O Data Management Select Data Interface	ciaco us.odo ogu 1660W 104'u 3a9M 1dm-Azure CiacoUmbretaDNSServerGroup ~ O Data Management Select Data Interface	Update D	Details	ng a downtime window	. After you register the de	vice with the ma	nagement center	or Cloud-delive	Selection select	a no longer use	the device manager
cisco us.cdo. ogo 19660W 104V 3aPM, fdm-Azure CiscoUmbrelaDNSServerGroup v Olata Management Select Data Interface	cisco us.cdo. ogu 9660W 104V 3sPU) fdm.Azure CiscoUnterelaDNSServerGroup ~	Update D This step is mandatory Management Cent.	Details r and <u>should be performed duri</u> Managoment Cento	ng a downtime window	. <u>After you regi</u> ster the de Threat Do	vice with the ma efense Hostn	nagement center DNS Server	or Cloud-delive Group	Selection of the select	rce: Cisco Se ed Migration: <u>n no longer use</u> t Center/	cure Firewall Device i Includes Device and the device manager Data Interface
		Update D This step is mandatory Management Cent.	Petails r and should be performed duri Management Cente	ng a downtime window	<u>. After you regi</u> ster the de Threat D	vice with the ma elense Hostn	DNS Server	or Cloud-delive Group	Select	nce: Cisco Se ed Migration: <u>n no longer use</u> t Center/	cure Firewall Device includes Device and the device manager Data Interface
		Update D This step is mandatory Management Cent cisco us	Management Cente	A Constraint of the second secon	3aPUN Idm-Azu	vice with the ma efense Hostn	DNS Server CiscoUmbreliaDNS	o <mark>r Cloud-delive</mark> Group ServerGroup ~	red FMC, you car Management	a no longer use t Center/	the device manager Data Interface Select Data Interface
		Update D This step is mandatory Management Cent. Cisco us	Management Cente	NAT ID • NECON 104V	3aPM	vice with the ma efense Hostn re	DNS Server CiscoUmbretaDNS	o <mark>r Cloud-delive</mark> Group ServerGroup ~	Select	a no longer use Center/	the device manager Data Interface Select Data Interface

ID centro di gestione e ID NAT.

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

							0				
	Extract FD	M Information Select Target	Map FTD Interface	Map Security Zones & Interface Groups	Review & Validate P (Shared Config)	Push Shared Config To	Move Manager	Review & Validate (Device Config)	Complete Migration		
	Note: Steps 7,8 a	and 9 should be carried	out in a maintena	ance window.							
Nove Mana	ager							Selec	ource: Cisco Sec ted Migration:		
Move Mana				CAN	CING the EDM Dev	lice		Selec	ource: Cisco Sec ted Migration:		
Move Mana Upd his step is mand	ager Sate Details Jatory and should be perfo	rmed during a downtin	ne window.	SYN	CING the FDM Dev	rice	ıd-delive	Solec Selec red FMC, you ca	ource: Cisco Sec ted Migration: In no longer use	the device manager	lanager (7.2 Shared Conf to manage it
Move Mana Upd his step is mand Management O	ager sate Details latory and should be perfo Cent Management	rmed during a downtin t Cente ① NAT	ne window. ID 💿	SYN	CING the FDM Dev 9% Complete	lice	id-delive	selec Selec Managemen	urce: Cisco Sec ted Migration: In no longer use In Center/	the device manager	lanager (7.3 Shared Coni

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.

ewall Migratio	on Tool (Vers	ion 6.0.1)				
		Extract FDM Information Select	z Target Map FTD Interface Map Security Zones & Review interface Groups (Shared	& Validate Push Shared Config To Move Manager (Config) FMC	Review & Validate Complete Migration (Device Config)	
		Note: Steps 7,8 and 9 should be o	arried out in a maintenance window.			
	Optimize,	Review and Validate Device	Configuration Page 0	<u>^</u>	Source: Cisco Secure Firewall Selected Migration: Includes Dev	Device Manager (7.2)
		Objects NAT Interfaces Routes	Site-to-Site VPN Tunnels 👔 Remote Access VPN	SNMP DHCP		
	Static PPP	WE)				
	Select all 2 e	entries Selected: 0 / 2			Q Search	4
	• *	Interface	Zone Q	IP Address	State	
	0 1	GigabitEthernet0/0	outside_zone	_	Enabled	
	2	GigabitEthernet0/1	inside_zone	45.1	Enabled	
1 to 2 of 2 4 4	Page 1 of 1	⊁ H			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.

	\odot	Successfully Validated		
alidation Summary (Pre-provide the selected for migration	Jsh) Not selected for migration	2	1	1
		Logical Interfaces	Routes (Static Routes, ECMP)	DHCP (Server, Relay, DDNS)
	O Platform Settings (snmp,http)	O Malware & File Policy		

Stato convalida - Configurazione push.

Finestra popup con la configurazione di push percentuale.

Firewall Migration Tool (Ver	sion 6.0.1)		
	1 Extract FOM Information Se Note: Steps 7,8 and 9 should be	Carried out in a mu	Torver & Values Complete Migration (Device Confg)
Complete	Migration		Source: Cisco Secure Firewall Device Manager (7.2+) Selected Migration: includes Device and Shared Config
Migration Stat	15		
Interfaces	o		
Routes	0		
DHCP			
Policy As:	ignment		
Please downlos	d the Post-Push migration report for a detailed s	ummary. Download Report	

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.

	Default FDM Information Select Target Map FTD Into	4 5 rface Map Security Zones & Review & Validate Pus Interface Groups (Shared Config)	6 7 8 h Shared Config To Move Manager Review & Va FMC (Device Co	läiris Complete Migration
	Note: Steps 7,8 and 9 should be carried out in a main	itenance window.		
Complete Migrati	on			Source: Cisco Secure Firewall Device Manager (7.2 Selected Migration: Includes Device and Shared Conf
Migration Status				
Migration is complet Next Step - Login to	e, policy is pushed to FMC. FMC to deploy the policy to FTD.			
Live Connect:				
Selected Context: Single Co	antext Mode			
Migration Summary (Post P	ush)			
Migration Summary (Post P	lush) Not selected for migration	4		3
Migration Summary (Post P 3 Access Control List Line	Not selected for migration Access List Objects	4 Network Objects		3 Access Control Policy Objects
Migration Summary (Post F 3 Access Control List Line	Not selected for migration Access List Objects (Bandard, Edended used in 8097 RAVINECORP)	4 Network Objects		3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Onsup)
Migration Summary (Post P 3 Access Control List Line	Push) PHot selected for migration Access List Objects (Bandard, Extended used in BDW RAVINECORP.	4 Network Objects	Not selected for migration Port Objects	3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Oncup)
Migration Summary (Post F 3 Access Control List Line Not selected for migratic	Not selected for migration Access List Objects (Bandert, Extended used in BOPF RAVERDORY) N	4 Network Objects 2	Not selected for migration Port Objects	3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)

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.

-dhal ciso	Defense Orchestra	tor	Ser	vices						Q Search	o 😽	٤	¢- ⇔(D ().		•
=	Hide Menu											>	Cloud-De	livered FN	NC	
	Dashboard		Q	Search by Device Name, IP Addres	is, or Serial N	umber					0	L	Version	20240514		
0	Multicloud Defense		FMC	Secure Connectors			_						Actions			
0	Inventory		-										O Check	For Changes		
Co	nfiguration		1	"Auto onboard On-Prem FMCs from S	ecureX tenant*	setting is not enabled. Click here	to enable settin	9.					d Deploy	ment		
۲	Policies	>	-			No.							Workf	ows		
0	Objects	>		Name		version	Devices	туре	Status	Last Heartbeat			O APIEX	plorer		
-8	VPN	>		Cloud-Delivered FMC		20240514	⊕ 3	Cloud-Delivered FMC	O Active	06/12/2024, 12:4	2:21		Managemen	t.		
Eve	ints & Monitoring					7.2.7-build 500	⊜0	On-Prem FMC	A Unreachable	-			Device			
*	Analytics	>											Policie	5		
٢	Change Log												< NAT	-		
(Jobs												-5- Site to -5- Remot	Site VPN e Access VPN		
%	Tools & Services		Tools	& Services	Migrations								Platfor	m Settings		
٢	Settings	>	6	Dynamic Attributes Connector	Firewall	Migration Tool							System			
			= :	Secure Connectors	ASA to F	DM Migration							O Config	uration		
			41	Firewall Management Center 🗸	Migrate	FTD to cdFMC							Smart	Licenses		
				ASA Templates									+ Device	Health		
													Audit Cisco	Cloud Events		

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.

Defense Orchestrator PMC / Devices / Secure Firewall Device Summary Analysis Policies	Devices Objects Integration	*) I	Return Home Deploy Q 🔿 🌮 🌣 🖉 📕	 which secure
-fdm-Azure		Deployments	Upgrades Health O Tasks	+ Show Notifications
Cisco Firepower Threat Defense for Azure		20+ total 0	waiting 0 running 0 retrying 6 success 20+ failures	Q. Filter
Device Interfaces Inline Sets Routing DHCP VTEP		Policy Deploym	ent	to the V
General / ± +	License	Policy Deploy	ment to Prom-Acure, Appleo successfully	1m 545 X
Name: -fdm-Azure	Performance Tier : FT	Health Policy		
Transfer Packets: No	Essentials:	Apply Initial_H Health Policy ap	Health_Policy 2023-06-29 17:28:08 to -fdm-Azure oplied successfully	1m 40s 🗙
Troubleshoot: Logs CL Download	Export-Controlled Features:			
Mode: Routed	Malware Defense:	 Discovery 		
Compliance Mode: None	IPS:	fdm-Azur	e - Discovery from the device is successful.	2m 10s 🗙
Performance Profile: Default	Carrier:	SFTunnel		
TLS Crypto Acceleration: Disabled	URL:	-fdm-Azur	e - SFTunnel connection established successfully.	- ×
	Secure Client Premier:			
Device Configuration: Import Export Download	Secure Client Advantage:	Register		
OnBoarding Method: Registration Key	Secure Client VPN Only:		Remove completed tasks	
Inspection Engine	Health		Management	/
Inspection Engine: Snort 3	Status:	•	Remote Host Address:	NO-IP
Revert to Snort 2	Policy: Initial_Health_Policy 2023-	06-29 17:28:08	Secondary Address:	
	Excluded:	None	Status:	•
			Manager Access Interface:	Management Interface
Inventory Details	Applied Policies	1	Advanced Settings	1
		,		

Attività di registrazione di cdFMC completata.

La periferica è su cdFMC > Periferica > Gestione periferiche.

6	Defense Orchestrator FMC / Devices / Device Management	Analysis	Policies	Devices	Objects	Integrati	on		*> Return Home	Deploy	۹	•	¢	0	~	tisce SECURE
View Al	By: Group + (3) • Error (0) • Warning (0)	Offline (0)	Normal (3)	 Deplo 	syment Pendinç	a (3) 🔹	Upgrade (0)	 Snort 3 (3) 							Migrate Deplo	ayment History
Collar	se All														Download	Device List Report
	Name			Model			Version	Chassis	Licenses		Acces	ss Contr	ol Policy		Auto RollBack	
	 Ungrouped (3) 															
	N/A - Routed Short 3			FTDv fo	r Azure		7.4.1	N/A	Essentials		None				«ڳ	1

Periferica registrata su cdFMC

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

٤	Defense Orchestrator FMC / Policies / Access Control / Access Control	Analysis	Policies	Devices	Objects	Integration		+> Return Home	Deploy	Q	o	6 24	6		Ŷ	-ab-ab- cisco	SECURE
								Object M	anagement	Intr	usion	Netw	ork Ana	alysis Policy	DNS	Impor	rt/Export
																Ne	ew Policy
	Access Control Policy		Sta	tus			Last Modified		Lock 5	Status							
	Default Access Control Policy Default Access Control Policy with default action block		Targ	eting 0 devices			2024-06-11 22:28:19 Modified by "Firepower System"									њ (11
	FTD-Mig-ACP-1718216278		Targ Up-t	eting 1 devices o-date on all targ	eted devices		2024-06-12 12:18:00 Modified by									6 B	11

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	۲ Q, Fil	ter									
			Sh	ow Unused Ob	jects							
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		Туре	Override								
any	0.0.0.0/0 ::/0		Group		¶a q ≣ #							
any-ipv4	0.0.0.0/0		Network		¶∎ Q ≣ M							
any-ipv6	::/0		Host		¶a q ≣ #							
Banned	103.104.73.155		Host	0	◎/〒約							
Gw_test01	172.22.2.1		Host		┗/〒め							
Inside_Network_IP	192.168.192.10		Host	0	┗/〒め							
IPv4-Benchmark-Tests	198.18.0.0/15		Network		¶a () ₩							
IPv4-Link-Local	169.254.0.0/16		Network		¶a a ∰ M							
IPv4-Multicast	224.0.0.0/4		Network		¶a q ⊕ M							
IPv4-Private-10.0.0.0-8	10.0.0/8		Network		¶∎ ⊂ ≣ M							
IPv4-Private-172.16.0.0-12	172.16.0.0/12		Network		¶∎ Q ≣ M							
IPv4-Private-192.168.0.0-16	192.168.0.0/16		Network		¶∎ Q 🗑 🕅							
IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16		Group		¶∎ Q ≣ #							
IPv6-IPv4-Mapped	::##:0.0.0.0/96		Network		¶∎ Q ≣ M							

Oggetti migrati da FDM a cdFMC

Interfacce di gestione degli oggetti migrate.

FMC / Objects / Object Mana	DF agement	Analysis	Policies	Devices	Objects	Integration		•> Return H	Home	Deploy	Q	•	¢	0		~	ideade SECURE
> AAA Server	Inter	rface								Add				•	Q, Filter		
Access List Address Pools	Interfac	ce objects segmen	nt your networ	rk to help you r	manage and c	lassify traffic flow. An in	terface object simply groups interfaces. These groups	s may span mult	tiple dev	rices; you o	an also	configu	re multipl	e interfa	ice objects	on a single	e device.
Application Filters AS Path	Name	*					Туре		Interfac	е Туре							
BFD Template Cipher Suite List	× 4	inside_ig					Interface Group		Routed								/18
> Community List DHCP IPv6 Pool	> 1	-fdm-Azure	0														
> Distinguished Name DNS Server Group	~ *	inside_zone					Security Zone		Routed								/
> External Attributes File List	~ 4	outside_ig	_				Interface Group		Routed								/ ¥ A
> FlexConfig Geolocation	>	-fdm-Azure	•														
Interface Key Chain	~ 📥	outside_zone					Security Zone		Routed								/14
Network > PKI	>	-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).