

Converti in contenitore (modalità MI) in Firepower 4200 con FTD 7.6

Sommario

[Introduzione](#)

[Prerequisiti, Piattaforme supportate, Licenze](#)

[Piattaforme software e hardware minime](#)

[Licenze](#)

[Componenti usati](#)

[Premesse](#)

[Novità](#)

[Piattaforme con supporto multi-istanza FTD](#)

[Differenze tra le serie 3100 e 4200](#)

[Distribuzioni supportate](#)

[Descrizione delle funzionalità e procedura dettagliata](#)

[Specifiche dell'istanza serie 4200](#)

[Numero massimo di istanze supportate](#)

[Dimensioni istanza FTD](#)

[Allocazioni Snort Core Lina \(Data Plane\)](#)

[Configurazione](#)

[Panoramica della configurazione](#)

[Converti serie 4200 in modalità a più istanze in FMC](#)

[Conversione di un singolo dispositivo](#)

[Converti più di un dispositivo \(Conversione in blocco\)](#)

[Monitoraggio dei progressi e completamento](#)

[Pagina Panoramica dello chassis FMC](#)

[Panoramica della pagina Panoramica dello chassis FMC](#)

[Sezioni della scheda Riepilogo pagina chassis](#)

[Gestisci interfacce](#)

[Riepilogo della scheda Interfacce](#)

[Modifica delle configurazioni dell'interfaccia fisica](#)

[Gestisci interfaccia secondaria](#)

[Gestisci EtherChannel](#)

[Configurazioni dispositivo di sincronizzazione](#)

[Supporto Netmod Hot Swap / Break-Out](#)

[Supporto nativo di EPM Hot Swap e Breakout](#)

[OIR: Abilita/Disabilita conferma EPM](#)

[Abilitazione EPM completata: Notifica interfaccia ricevuta](#)

[Notifica modifica interfaccia EPM](#)

[Pagina Opzioni di interruzione/unione nello chassis](#)

[Modifiche all'interfaccia dopo un'interruzione o un'unione](#)

[Impatto delle modifiche dell'interfaccia sull'istanza](#)

[Gestione istanze](#)

[Crea istanza](#)

[Modifica di un'istanza](#)

[Elimina istanza](#)

[Configurazione SNMP](#)

[Importazione/esportazione chassis](#)

[Esporta configurazione](#)

[Importa configurazione](#)

[Informazioni sull'importazione/esportazione dello chassis](#)

[Criteri di impostazione della piattaforma chassis](#)

[Impostazioni piattaforma chassis: DNS](#)

[Impostazioni piattaforma chassis: SSH](#)

[Impostazioni piattaforma chassis: Elenco accessi SSH](#)

[Impostazioni piattaforma chassis: Sincronizzazione ora](#)

[Da NTP da Management Center](#)

[Sul server NTP personalizzato](#)

[Impostazioni piattaforma chassis: Fusi orari](#)

[Impostazioni piattaforma chassis: Syslog](#)

[Impostazioni piattaforma chassis: Salva e distribuisci](#)

[Annullamento della registrazione dello chassis](#)

[Converti da istanza multipla in modalità nativa](#)

[API FMC Rest](#)

[API REST per conversione da native a multi-istanza](#)

[API REST per gestione chassis](#)

[API REST per la gestione di Netmod \(moduli di rete\)](#)

[API REST per gestione istanze](#)

[API REST per gestione SNMP](#)

[API REST da recuperare riepilogo](#)

[API REST per la gestione dell'interfaccia](#)

[Aggiorna interfaccia fisica](#)

[Configura sottointerfacce](#)

[Configurazione delle interfacce EtherChannel](#)

[Interfacce REST API Break/Join](#)

[Flusso REST per interruzione interfaccia](#)

[Flusso REST per join interfaccia](#)

[Sincronizza API REST dispositivo](#)

[Risoluzione dei problemi/Diagnostica](#)

[Registrazione FXOS](#)

[Registrazione FMC](#)

[Risoluzione dei problemi dello chassis](#)

[Procedure dettagliate per la risoluzione dei problemi di esempio](#)

[Registrazione automatica del guasto dello chassis in FMC](#)

[Risoluzione del problema](#)

[Registrazione automatica dell'istanza in FMC](#)

[Risoluzione del problema](#)

[Registrazione del dispositivo nativo in FMC](#)

[Risoluzione del problema](#)

[Riferimenti utili](#)

[Opzioni di interfaccia e alta disponibilità](#)

[Opzioni interfaccia](#)

[Standalone o Alta disponibilità](#)

[Utilizzo delle due interfacce di gestione](#)

Introduzione

Questo documento descrive come configurare un contenitore (modalità a più istanze) nella serie Firepower 4200 Firewall con FTD 7.6 e i dettagli correlati.

Prerequisiti, Piattaforme supportate, Licenze

Piattaforme software e hardware minime

Manager(s) and Version (s)	Application (ASA/FTD) and Minimum Version of Application	Supported Platforms
<ul style="list-style-type: none">FMC 7.6.0	<ul style="list-style-type: none">FTD 7.6.0	4200 Series 4215, 4225, 4245



Nota: Multi-Instance non è supportato con FDM su nessuna piattaforma.

Licenze

- Le licenze per le funzionalità vengono assegnate manualmente a ciascuna istanza, ma si utilizza solo una licenza per ciascuna funzionalità per ciascun dispositivo serie 4200.
 - Ad esempio, per una serie 4200 con 3 istanze FTD, è necessaria una sola licenza URL, indipendentemente dal numero di istanze in uso, a condizione che ci si trovi sullo stesso FMC.
- Tutte le licenze vengono utilizzate per ciascun dispositivo serie 4200 e non per singola istanza del contenitore, a condizione che si trovino sullo stesso FMC. Pertanto, per tutte le istanze su dispositivi serie 4200, si consiglia di utilizzare lo stesso FMC a causa dell'implementazione della licenza.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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

- FTD supporta già Multi-Instance (MI) sui modelli 3100 (nonché sulle serie 9300 e 4100), ma non è supportato per la serie 4200.
- I modelli 4200 sono supportati solo in modalità nativa in FMC.
- Non è possibile creare istanze multiple in 7.4.x in 4200.
- Multi-Instance (MI) su 3100 è supportata a partire dalla versione 7.4.1.
 - Le istanze possono essere create e gestite utilizzando FMC (a differenza delle serie 9300 e 4100, in cui è necessario utilizzare FCM).
 - FXOS può essere aggiornato, in modalità MI, tramite l'interfaccia utente dello chassis di aggiornamento di FMC.
 - La conversione in modalità MI viene eseguita tramite una CLI.

Novità

- È possibile effettuare il provisioning e la gestione delle istanze MI sulla serie 4200.
- FMC - Soluzione di gestione singola per istanze della serie 4200 (modalità MI) e FTD
- Consentire la conversione di dispositivi nativi in modalità MI su FMC per i dispositivi serie 3100 e 4200.
- Mercato di destinazione: Aziende di grandi dimensioni - Internet Edge, centro dati

Piattaforme con supporto multi-istanza FTD

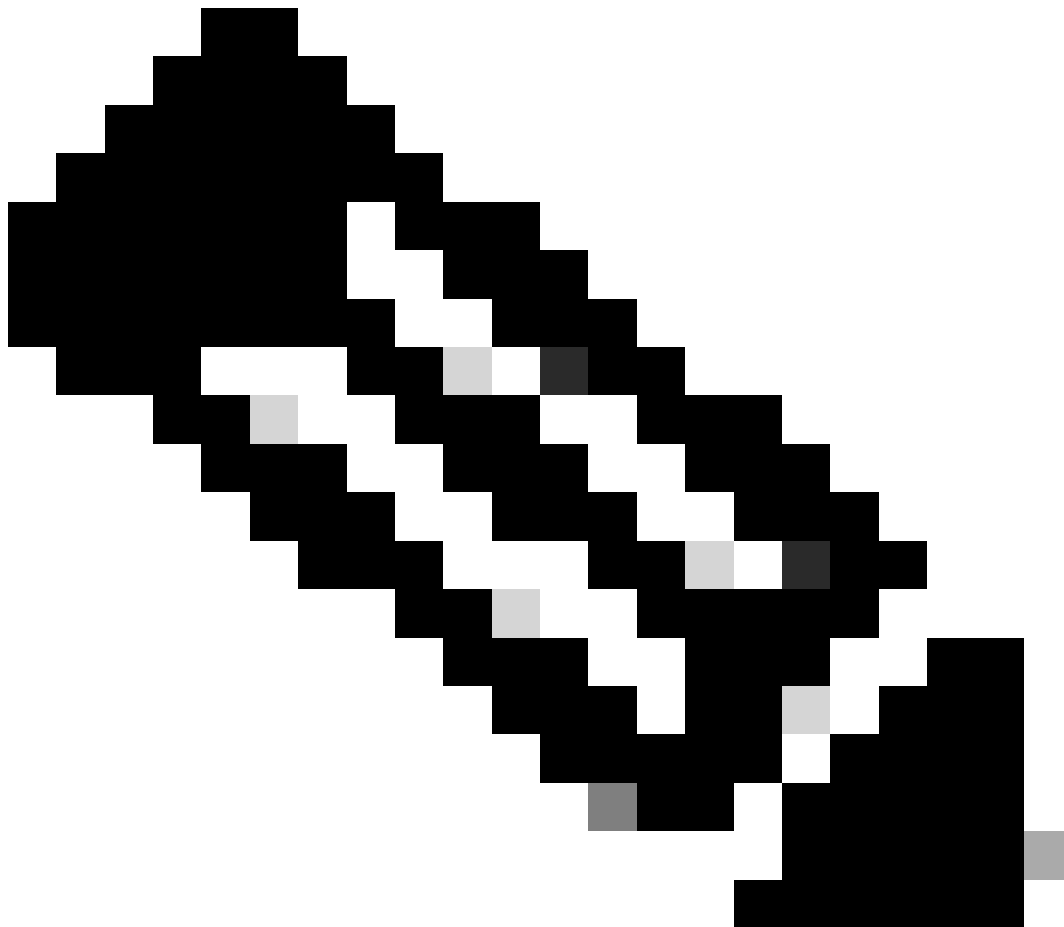
Platform	FTD Version	FTD Multi-Instance Support	Management Solution
Virtual	-	No	-
FPR1000	-	No	-
FPR2100	(not supported in 7.6)	No	-
3105		No	
3110, 3120, 3130, 3140	FTD 7.4.1	Yes	FMC
FPR4100	FTD 6.3.0	Yes	FCM & FMC
4215, 4225, 4245	FTD 7.6.0	Yes	FMC
FPR9300	FTD 6.3.0	Yes	FCM & FMC

Differenze tra le serie 3100 e 4200

- 4200 dispone di due interfacce di gestione, che consentono di utilizzare una per la gestione e l'altra per gli eventi.
 - Le interfacce Management1/1 e Management1/2 vengono entrambe avviate a tutte le istanze del contenitore FTD.
 - In modalità MI è possibile utilizzare una o entrambe le interfacce di gestione.
 - Management1/1 sia per Management che per Events, oppure
 - Management1/1 può essere utilizzato per la gestione e Management1/2 per gli eventi, nel qual caso:
 - È necessario definire route statiche per instradare il traffico utilizzando l'interfaccia di gestione 1/2.
- A causa delle dimensioni maggiori, è possibile creare un numero maggiore di istanze sullo switch 4200 rispetto allo switch 3100.

Distribuzioni supportate

- Gestione della serie 4200 (modalità MI) con istanze FTD autonome
 - Gestione della serie 4200 (modalità MI) con istanze FTD HA*
-



Nota: Per la serie FPR4100, nel caso di FTD-HA, i nodi primario e secondario devono trovarsi su due dispositivi diversi della serie 4200 (modalità MI). Inoltre, il clustering MI non è supportato in questa release.

Descrizione delle funzionalità e procedura dettagliata

Modifiche alla configurazione a più istanze in 7.6.0:

- Supporto per la serie 4200 in modalità MI
- Modifiche apportate al CCP che riguardano anche la gestione della modalità MI della serie 3100:
 - Conversione della periferica dalla modalità nativa alla modalità MI in FMC
 - Controlli di fattibilità per verificare se il dispositivo può essere convertito in modalità MI
 - Registra automaticamente istanza FTD in FMC dopo la conversione

Specifiche dell'istanza serie 4200

Numero massimo di istanze supportate

Platform	Maximum Instance Count	Maximum Logical CPU Cores Supported
FP4215	10	62
FP4225	15	126
FP4245	34	254

La densità delle varianti è determinata da due fattori principali:

1. La quantità di core CPU e la quantità di spazio su disco su una determinata piattaforma
2. Quante di queste risorse sono disponibili per il provisioning delle istanze. La dimensione minima dell'istanza richiede 3 core fisici CPU (6 logici) e 48 GB di spazio su disco.

Dimensioni istanza FTD

Platform	4215	4225	4245
Total CPU cores	32	64	128
Available CPU cores for FTD	30	62	126
Total RAM (GiB)	222	445	875
FXOS RAM (GiB)	6	6	6
DMA RAM (GiB)	11	39	78
Available RAM for FTD (GiB)	7	7	7
Available Disk space for FTD (GiB)	660	864	1794
Max Instances	10	15	34

Allocazioni Snort Core Lina (Data Plane)

	4215	4225	4245			
Dimensione istanza	Core del piano dati	Core snort	Core del piano dati	Core snort	Core del piano dati	Core snort
6	2	2	2	2	2	2
8	2	4	2	4	2	4
10	4	4	4	4	4	4
12	4	6	4	6	4	6
14	6	8	6	6	6	6
16	6	8	6	6	8	8
18	8	10	8	8	8	10
20	8	10	8	8	10	10

22	10	12	10	10	10	12
24	12	12	10	10	10	12
26	12	14	12	12	12	12
28	14	14	12	14	12	14
30	14	16	14	14	14	14
32	14	16	14	16	14	16
34	16	16	16	16	16	16
36	16	18	16	18	16	18
38	18	18	18	18	18	18
40	18	20	18	20	18	20
42	20	20	20	20	20	20
44	20	22	20	22	20	22
46	22	22	22	22	22	22
48	22	24	22	24	22	24
50	24	24	24	24	24	24
52	24	26	24	26	24	26
54	26	26	26	26	24	26
56	26	28	26	28	26	28

58	28	28	28	28	28	28
60	28	30	28	39	28	30
62	30	30	30	30	30	30
64			30	32	30	32
66			30	34	30	34
68			32	34	32	34
70			32	36	32	36
72			34	36	34	36
74			34	38	34	38
76			36	38	36	38
78			36	40	36	40
80			38	40	38	40
82			38	42	38	42
84			40	42	40	42
86			40	44	40	44
88			42	44	42	44
90			42	46	42	46
92			44	46	44	46

94			44	48	44	48
96			46	48	46	48
98			46	50	46	50
100			48	50	48	50
102			48	52	48	52
104			50	52	50	52
106			50	54	50	54
108			52	54	52	54
110			52	56	52	56
112			54	56	54	56
114			54	58	54	58
116			56	58	56	58
118			56	60	56	60
120			58	60	58	60
122			58	62	58	62
124			60	62	60	62
128					60	64
130					60	66

132					62	66
134					62	68
136					64	68
138					64	70
140					66	70
142					66	72
144					68	72
146					68	74
148					70	74
150					70	76
152					72	76
154					72	78
156					74	78
158					74	80
254					120	130

Configurazione

Panoramica della configurazione

1. Registrare il dispositivo serie 4200 (modalità nativa) in FMC.
2. Novità! Nel FMC, selezionare e convertire il dispositivo dalla modalità nativa alla modalità

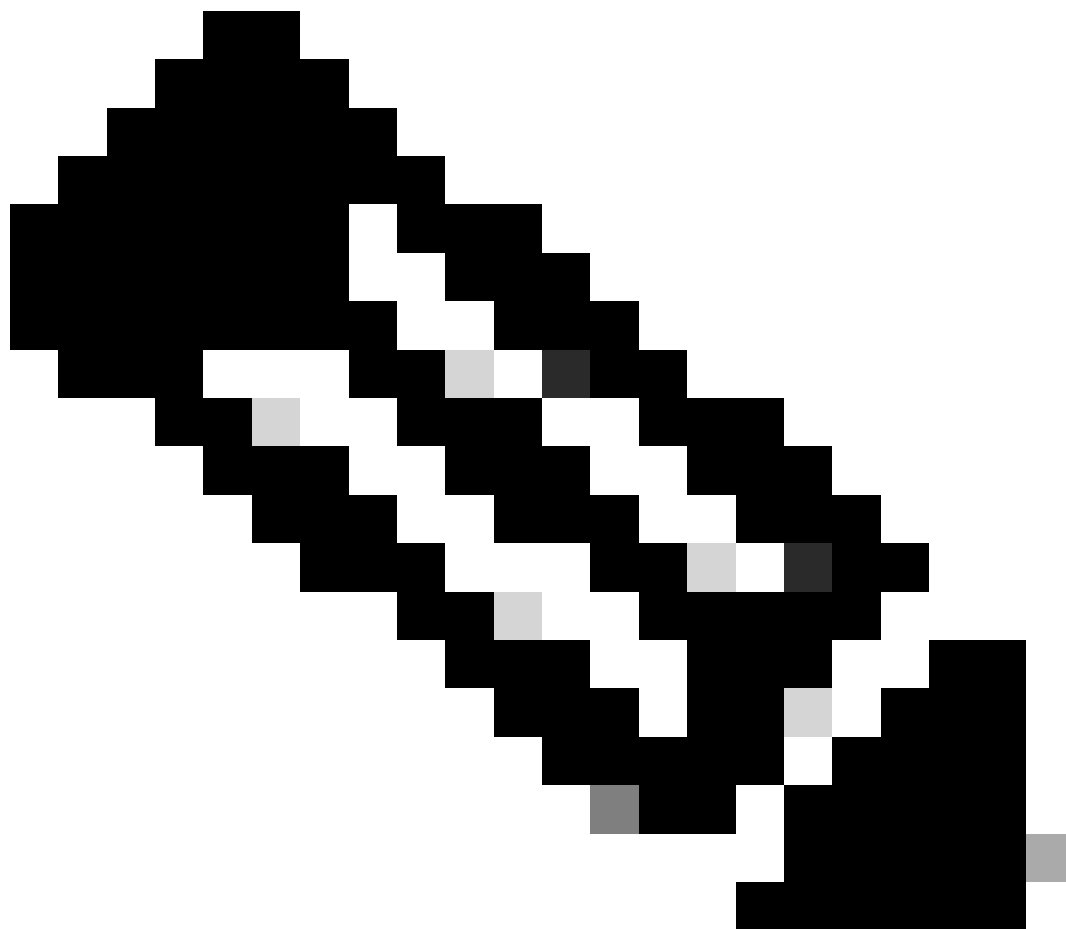
MI.

3. Novità! Dopo la conversione, lo chassis MI si registra automaticamente nel FMC.
4. Aggiorna interfacce fisiche.
5. Creare istanze FTD e assegnare le interfacce.
6. Creare/aggiornare/eliminare il canale della porta e le sottointerfacce da FMC.
7. Configurare le impostazioni della piattaforma.
8. Distribuire le modifiche alla configurazione nel dispositivo.
9. Le istanze FTD vengono registrate automaticamente nel FMC.

Converti serie 4200 in modalità a più istanze in FMC

Per impostazione predefinita, gli access point serie 4200 sono in modalità nativa. Per convertire la serie 4200 in modalità a più istanze in FMC:

1. Connettersi al dispositivo e creare un manager (già documentato).
2. Registrare il dispositivo nativo nel CCP (già documentato).
3. Convertire in istanze multiple utilizzando FMC.
4. In FMC selezionare i dispositivi da convertire in istanze multiple e attivare la conversione. È possibile selezionare uno o più dispositivi.



Nota: Se si passa dalla modalità nativa alla modalità MI, tutta la configurazione sullo chassis viene ripristinata. La conversione dalla modalità MI alla modalità nativa avviene ancora tramite CLI.

Conversione di un singolo dispositivo

1. Per avviare la conversione, passare a Dispositivi > Gestione dispositivi.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rollback
Ungrouped (1)						
4215_Native_Chassis Short 3 192.168.1.80 - Routed	Firewall 4215 Threat Defense	7.6.0	Manage	Essentials, Malware (1 more...)	None	<ul style="list-style-type: none"> Delete Packet Tracer Packet Capture Revert Upgrade Health Monitor Convert to Multi-Instance Troubleshoot Files

On successful registration, 4200 Series (Native mode) device will be listed in the device listing page.

Right click the drop-down menu and select the Convert to Multi-Instance option to convert the Native Device.

2. Convalidare il dispositivo selezionato e fare clic su Continue:

Convert to Multi-Instance Mode

You have selected: 4215_Native_Chassis.

⚠ All the configuration on the selected devices will be erased in the process of Multi-instance mode conversion.

Cancel Continue

Click on continue to trigger conversion readiness checks to ensure device can be converted from Native to MI.

convalida dispositivi selezionati

3. Verifica della preparazione e conversione iniziale:

Step 1: Set the name of the MI Chassis after conversion.

Current selected device

Step 2: Hover over the icon next to the name to check whether the device is ready for conversion.

Step 3: Click on Convert to Multi-Instance to start conversion for the device.

verifica preparazione

Converti più di un dispositivo (Conversione in blocco)

1. Seleziona dispositivi:

Step 1: Successfully register multiple Native mode devices on FMC.

Step 2: Select the devices you want to convert from native to MI using the check box next to them.
Here, both Ungrouped 4200s are picked.

Step 3: After successful registration of multiple native devices and selecting multiple chassis for conversion, click on the drop-down menu to select bulk action and select the "Convert to Multi-Instance" option.

2. Conferma selezione:

Convert to Multi-Instance Mode

1 Selected Devices 2 Readiness Check

All the configuration on the selected devices will be erased in the process of Multi-instance mode conversion.

Device Name	IP	Version	Model	
4215_Native_Chassis	192.168.1.80	7.6.0	Cisco Secure Firewall 4215 Threat Defense	
Native_Chassis_2	192.168.1.106	7.6.0	Cisco Secure Firewall 3130 Threat Defense	

Cancel Next

Step 1: Use the edit button to set the name of the Chassis after conversion.

Current selected devices

Use the delete button to remove a device from bulk conversion.

IP Address that will be applied to chassis after conversion

Step 2: Click on "next" to trigger conversion readiness checks to ensure device can be converted from Native to MI.

3. Verifica preparazione e avvio conversione:

Convert to Multi-Instance Mode

1 Selected Devices 2 Readiness Check

All the configuration on the selected devices will be erased in the process of Multi-instance mode conversion.

Device Name	IP	Version	Model	Status
4215_Native_Chassis	192.168.1.80	7.6.0	Cisco Secure Firewall 4215 Threat Defense	✔
Native_Chassis_2	192.168.1.106	7.6.0	Cisco Secure Firewall 3130 Threat Defense	⌛

Cancel Back Convert to Multi-Instance

This list shows the name, IP, version, and model of the devices that are being converted.

Click on the refresh icon to rerun readiness checks

Hover over the icon next to the name to check whether the device is ready for conversion.

Click on Convert to Multi-Instance to start conversion for the device.

Monitoraggio dei progressi e completamento

1. Notifica di avvio conversione:

Once the conversion is triggered, the status can be monitored using the Task Manager.

2. Registrazione automatica dello chassis:

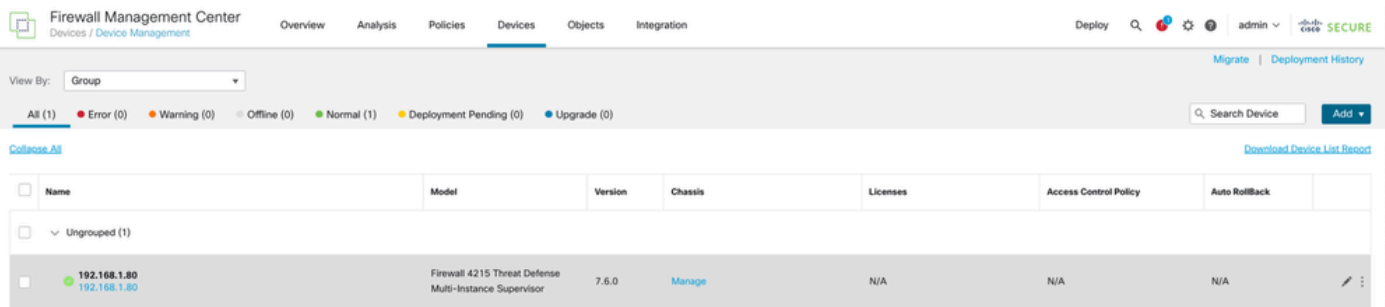
Device gets unregistered as a single device and automatically gets re-registered as a Chassis.

Now the Model column includes both the model and "Multi-Instance Supervisor".

3. Notifica post-conversione:

Successful Conversion Notification with number of devices converted successfully.

Pagina di gestione dei dispositivi risultante in cui sono elencati i dispositivi serie 4200 (modalità MI):



Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
192.168.1.80 192.168.1.80	Firewall 4215 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	N/A	N/A	N/A

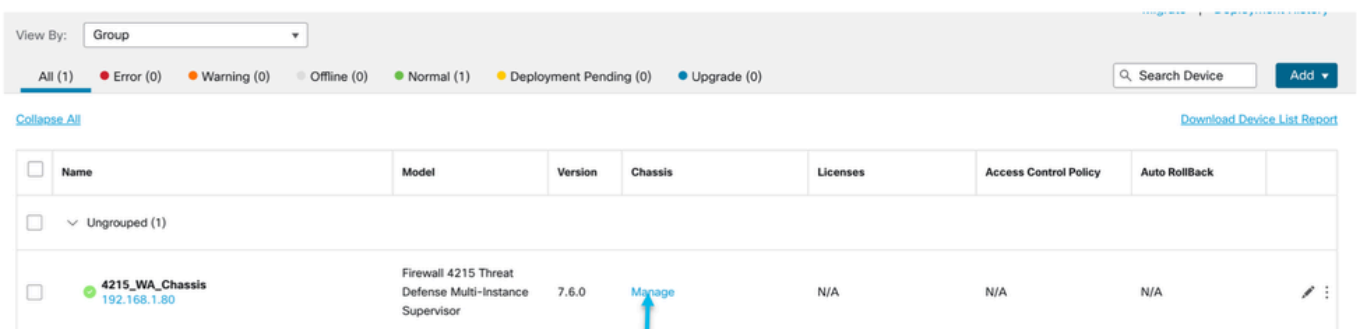
Pagina Panoramica dello chassis FMC

Panoramica della pagina Panoramica dello chassis FMC

La pagina Panoramica dello chassis di FMC fornisce un riepilogo completo del dispositivo serie 4200 (modalità MI). Esso comprende:

- Vista del pannello posteriore illustrativa del dispositivo, inclusi i moduli di rete disponibili.
- Riepilogo degli errori, con la loro criticità.
- Riepilogo interfaccia, stato.
- Riepilogo istanza FTD, stato.
- Statistiche sull'hardware, tra cui ventola, alimentatore, memoria, utilizzo della CPU e storage.

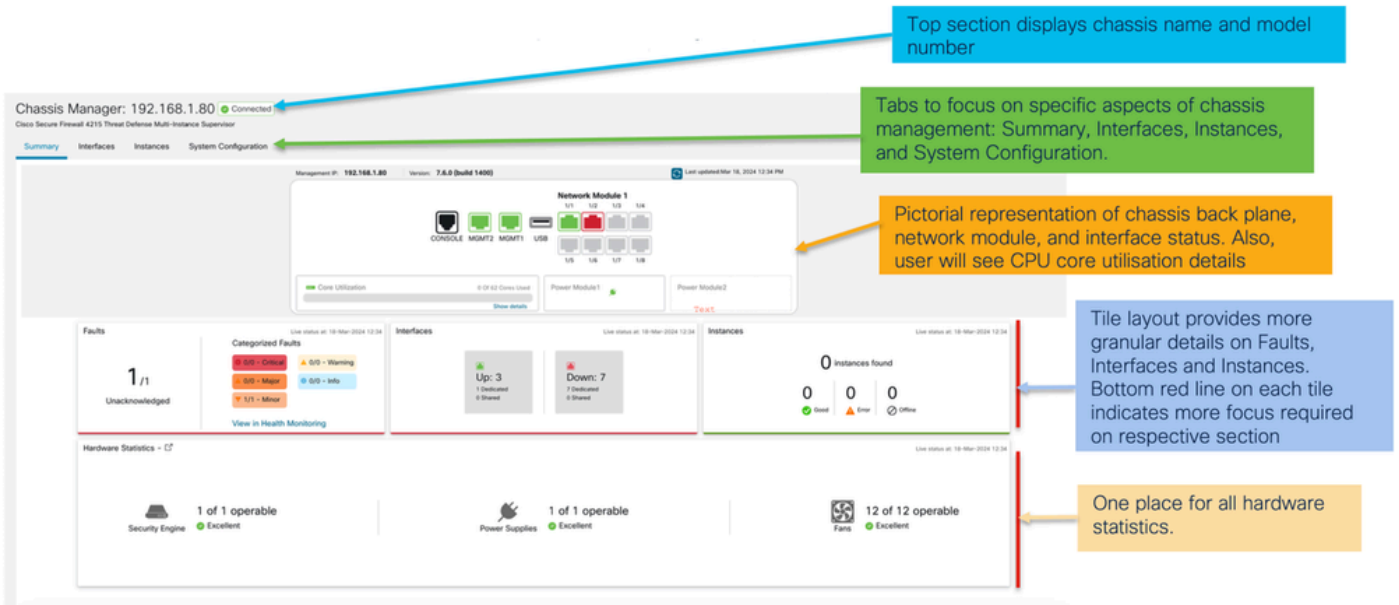
Fare clic su Gestisci per passare a Panoramica chassis:



Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
4215_WA_Chassis 192.168.1.80	Firewall 4215 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	N/A	N/A	N/A

From the Device Management page, click 'Manage' to view 4200 Series (MI mode) Chassis (device) overview.

Scheda Riepilogo pagina chassis:

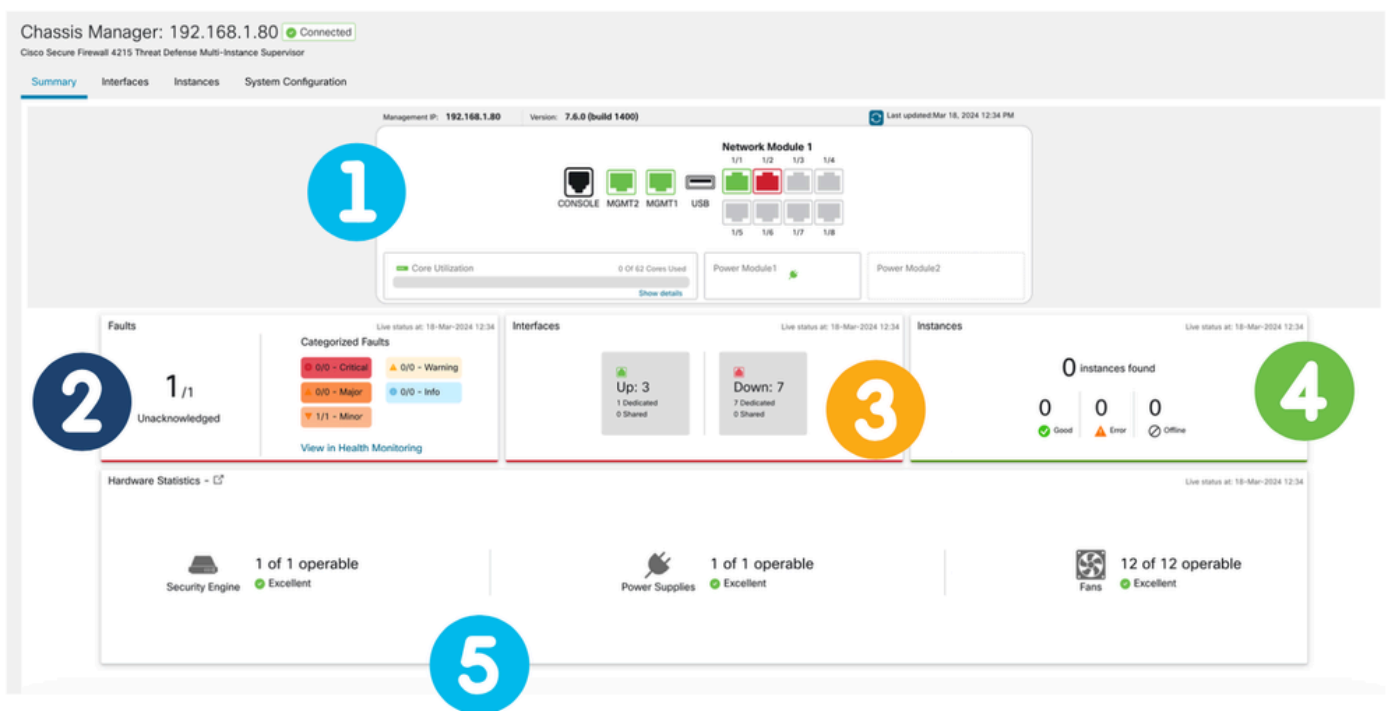


Sezioni della scheda Riepilogo pagina chassis

La scheda Riepilogo contiene delle sezioni. Fare clic per ottenere ulteriori dettagli:

- Piano posteriore
- Errori
- Interfacce
- Istanze
- Statistiche hardware

Le sezioni sono mappate per numero come mostrato in questa immagine:



1. Vista posteriore:



Displays management IP address and running software version/build number on the device.

Available physical ports on the device. Greyed out indicates they are non-actionable/configurable.

Each color indicates the number of cores utilized by individual FTD instances against total available cores.

Hovering over on each color will provide a tool-tip that details more on the FTD instance.

Management IP: 192.168.0.112 Version: 7.6.0 (build 1193) Last updated: Nov 27, 2023 2:52 AM

Network Module 1: 1/1, 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8

Core Utilization: 6 Of 62 Cores Used

Power Module 1, Power Module 2

Done

Click on 'Show Details' to view drill down on core utilisation

Lets user know the last update timestamp. Refresh button allows to configure auto-refresh interval or turn-off auto-refresh

Represents physical interfaces. Shows inline and network modules and interface status. Allows user to enable/disable physical ports.

Represents power supply module. Power supply status is represented with green power plug icon.

2. Sezione Errori:



Live faults on the device are represented. The number indicates presence of fault and fault categories are listed on right side of the tile. Hover over the unacknowledged faults to show a tooltip that lists the faults.

Faults 1/1 Unacknowledged

Categorized Faults

- 0/0 - Critical
- 0/0 - Major
- 1/1 - Minor
- 0/0 - Warning
- 0/0 - Info

View in Health Monitoring

List of Top 1 Faults

- 1/1 - Minor: other port 1/2 on fabric interconnect A oper state: link-down, reason: Down

View All Faults

View in Health Monitoring

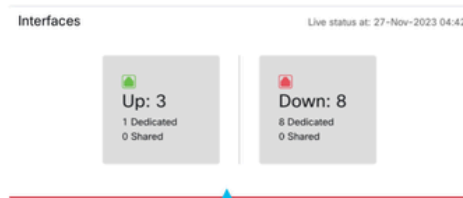
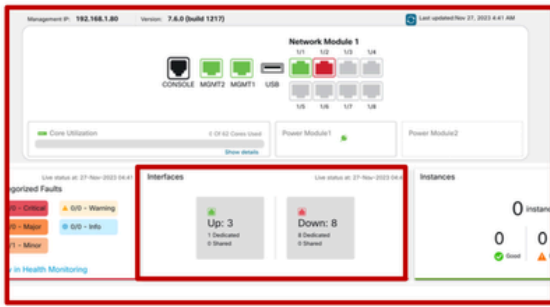
Click on 'View in Health Monitoring' to open a dialog that lists all faults in a table.

Health: 4215_WA_chassis (Critical) Normal

View System & Troubleshoot Details

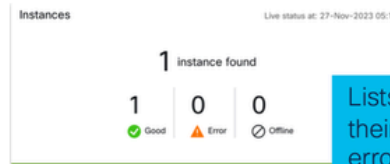
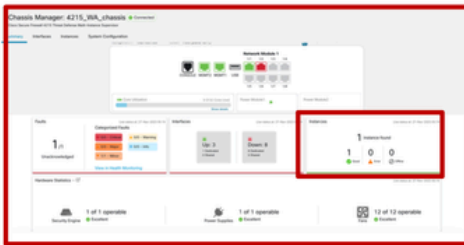
Severity	Code	Faults	Occurrence	Time
Minor	F1150	other port 1/2 on fabric interconnect A oper state: link-down, reason: Down	1	Nov 26, 2023 9:57 PM

3. Sezione Interfacce:

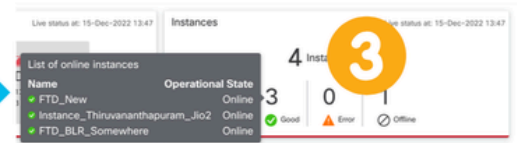
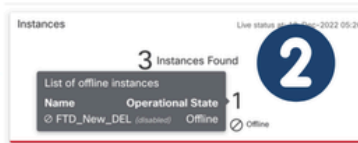
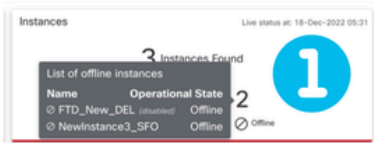


Lists number of interfaces that are operationally up and/or down. It also displays the of dedicated and shared interfaces.

4. Sezione Instances:



Lists number of instances with their state (online, offline, and error). On hovering, live status of instance is displayed



La transizione delle istanze da non in linea a in linea è illustrata nell'immagine precedente.

- Una volta eseguito il provisioning (1)
- L'istanza è offline fino a quando non viene connessa (2)
- Vengono riflessi anche gli stati intermedi (3)

5. Statistiche relative all'hardware:

Management IP: 192.168.1.80 Version: 7.6.0 (build 1217) Last updated: Nov 27, 2023 5:23 AM

Network Module 1
1/1 1/2 1/3 1/4

Detailed Hardware Statistics

Security Engine Fans Power Supplies CPU Memory Storage

Name	Fan	Operabil...	Operatio...	Power	Thermal	Model	Vendor
Fan Tray...	Fan-1	operable	operable	on	ok	N/A	N/A
Fan Tray...	Fan-2	operable	operable	on	ok	N/A	N/A
Fan Tray...	Fan-3	operable	operable	on	ok	N/A	N/A
Fan Tray...	Fan-4	operable	operable	on	ok	N/A	N/A
Fan Tray...	Fan-1	operable	operable	on	ok	N/A	N/A
Fan Tray...	Fan-2	operable	operable	on	ok	N/A	N/A
Fan Tray...	Fan-3	operable	operable	on	ok	N/A	N/A
Fan Tray...	Fan-4	operable	operable	on	ok	N/A	N/A
Fan Tray...	Fan-1	operable	operable	on	ok	N/A	N/A
Fan Tray...	Fan-2	operable	operable	on	ok	N/A	N/A
Fan Tray...	Fan-3	operable	operable	on	ok	N/A	N/A
Fan Tray...	Fan-4	operable	operable	on	ok	N/A	N/A

Faults: 1/1 Unacknowledged

Categorized Faults: 0/0 - Critical, 0/0 - Major, 1/1 - Minor

Hardware Statistics: 1 of 1 operable, Security Engine Excellent

Hardware Statistics provides the status of key hardware components of the chassis: Security Engine, Power Supply, and Fan.

Gestisci interfacce

Operazioni supportate dalla scheda Interfacce:

- Aggiornamento dell'interfaccia fisica
- Creazione/aggiornamento/eliminazione di sottointerfacce.
- Creazione/aggiornamento/eliminazione di interfacce EtherChannel.
- Configurazioni interfaccia di sincronizzazione.
- OIR del modulo Network.
- Break/Join of Physical interface (Interruzione/unione dell'interfaccia fisica).

Riepilogo della scheda Interfacce

Chassis Manager: 4215_WA_chassis Connected

Summary Interfaces Instances System Configuration

Network Module 1
1/1 1/2 1/3 1/4
CONSOLE MGMT2 MGMT1 USB 1/5 1/6 1/7 1/8

Interface Name	Port Type	Instances	VLAN ID	Admin Speed	Admin Duplex	Admin State	Auto Negotiation	Admin FEC
Ethernet1/1	Data	WA_instance_1		Detect SFP	Full	Enabled	Yes	Auto
Ethernet1/2	Data	WA_instance_1		Detect SFP	Full	Enabled	Yes	Auto
Ethernet1/3	Data			Detect SFP	Full	Disabled	Yes	Auto
Ethernet1/4	Data			Detect SFP	Full	Disabled	Yes	Auto
Ethernet1/5	Data			Detect SFP	Full	Disabled	Yes	Auto

La pagina iniziale della scheda Interfacce mostra tutti i tipi di interfacce gestite per uno chassis, ad esempio le interfacce fisiche, le sottointerfacce e le sottointerfacce EtherChannel e EtherChannel.

Modifica delle configurazioni dell'interfaccia fisica

Questi attributi di un'interfaccia fisica possono essere aggiornati:

- Stato (Attivato/Disattivato)
- Tipo di porta (dati) | Condivisione dei dati)
- Admin Duplex
- Velocità amministratore
- Negoziazione automatica

Edit Physical Interface ?

Interface ID
Ethernet1/1 Enabled

Port Type
Data

Admin Duplex
Full

Admin Speed
Detect SFP

Admin FEC
Auto

Auto Negotiation

Cancel OK


Gestisci interfaccia secondaria

Selezionare l'opzione relativa all'interfaccia secondaria dal pulsante Aggiungi per aggiungere una nuova interfaccia.

Gli attributi di una sottointerfaccia possono essere modificati:

- Interfaccia padre

- Tipo di porta (dati/condivisione dati)
- ID sottointerfaccia
- ID VLAN

<input type="text" value="Search Interfaces"/> Sync Device Add		
Auto Negotiation	Admin FEC	Sub Interface EtherChannel Interface
Yes	Auto	

Add Sub Interface ?

Parent Interface

Port Type

SubInterface ID (1-4294967295)

VLAN ID (1-4094)

Gestisci EtherChannel

Per creare una nuova interfaccia EtherChannel, usare l'"interfaccia EtherChannel" sotto il pulsante Add.

Di seguito sono riportati gli attributi che è possibile configurare per EtherChannel:

- ID EtherChannel
- Tipo di porta (condivisione dati/dati)
- Interfacce membro
- Velocità amministratore
- Admin Duplex
- Modalità LACP
- Frequenza LACP
- Negoziazione automatica

Search Interfaces		Sync Device	Add
Auto Negotiation	Admin FEC	Sub Interface	
Yes	Auto	EtherChannel Interface	

Add EtherChannel Interface

Interfaces Configuration

EtherChannel ID: (1-48)
 Enabled

Port Type
 Data

Select Member Interface(s)

Available Interfaces (7)

- Ethernet1/1
- Ethernet1/2
- Ethernet1/3
- Ethernet1/4
- Ethernet1/5
- Ethernet1/6

Selected Interfaces (0)

Add EtherChannel Interface

Interfaces Configuration

Admin Duplex
Full

Admin Speed
1Gbps

LACP Mode
Active

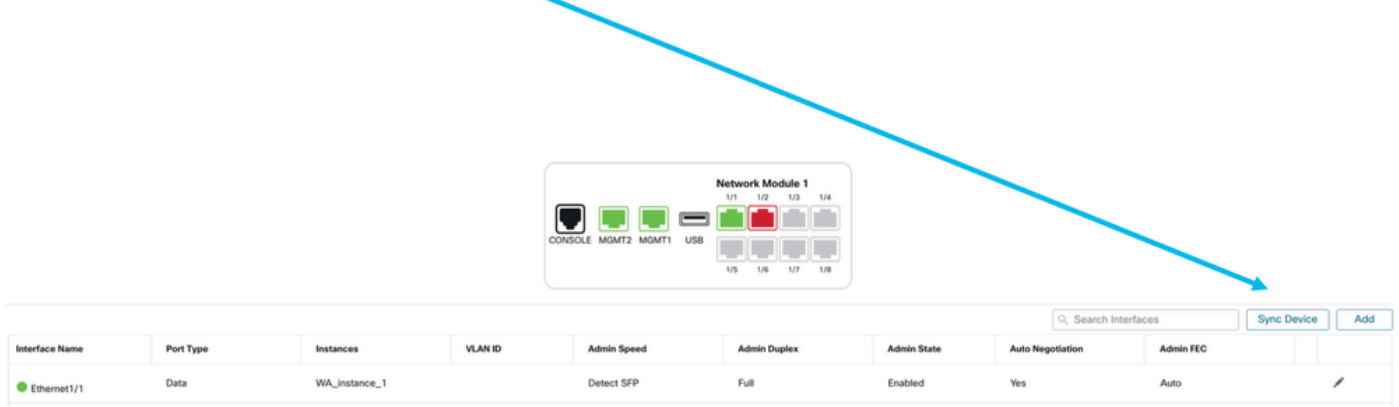
LACP Rate
Default

Auto Negotiation

Configurazioni dispositivo di sincronizzazione

In alcuni casi la configurazione del FMC e quella del dispositivo potrebbero non essere più sincronizzate. Un caso è quello di un utente che rimuove o inserisce una netmod. In questi casi è possibile eseguire la sincronizzazione del dispositivo.

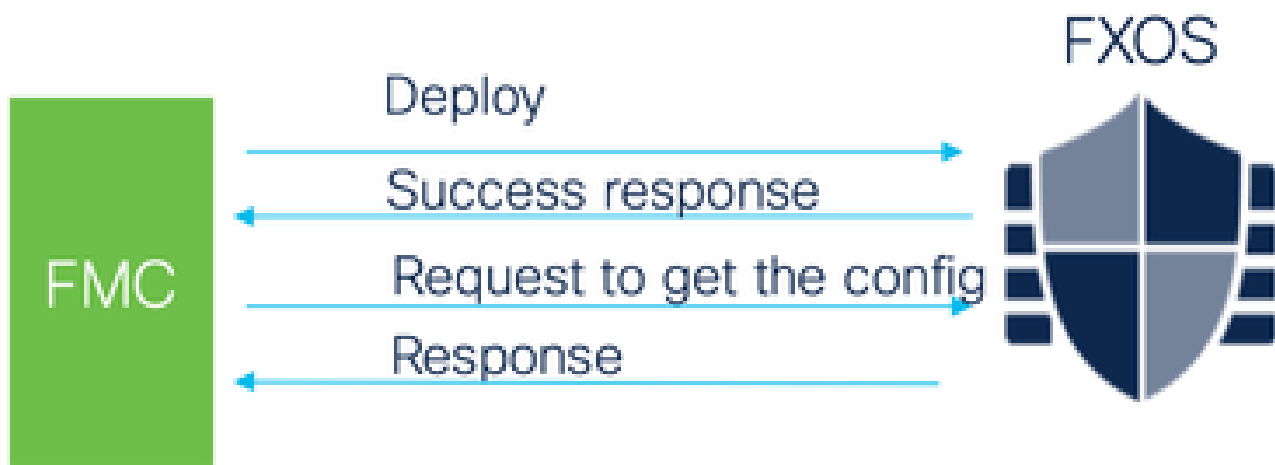
Click "Sync Device".



Supporto Netmod Hot Swap / Break-Out

La parola "sostituzione a caldo", utilizzata nei documenti, è indicata come inserimento e rimozione online o OIR in altra documentazione interna.

L'abilitazione/disabilitazione del modulo di rete, l'interruzione o l'unione di interfacce vengono implementate immediatamente. La modalità a più istanze è uguale alla serie 4200 in modalità nativa.



La risposta ricevuta viene confrontata con la configurazione corrente e quindi viene creata una notifica di modifica dell'interfaccia che l'utente deve confermare.

Supporto nativo di EPM Hot Swap e Breakout

EPM OIR e Breakout sono già supportati sul Secure Firewall serie 4200 standalone in modalità nativa.

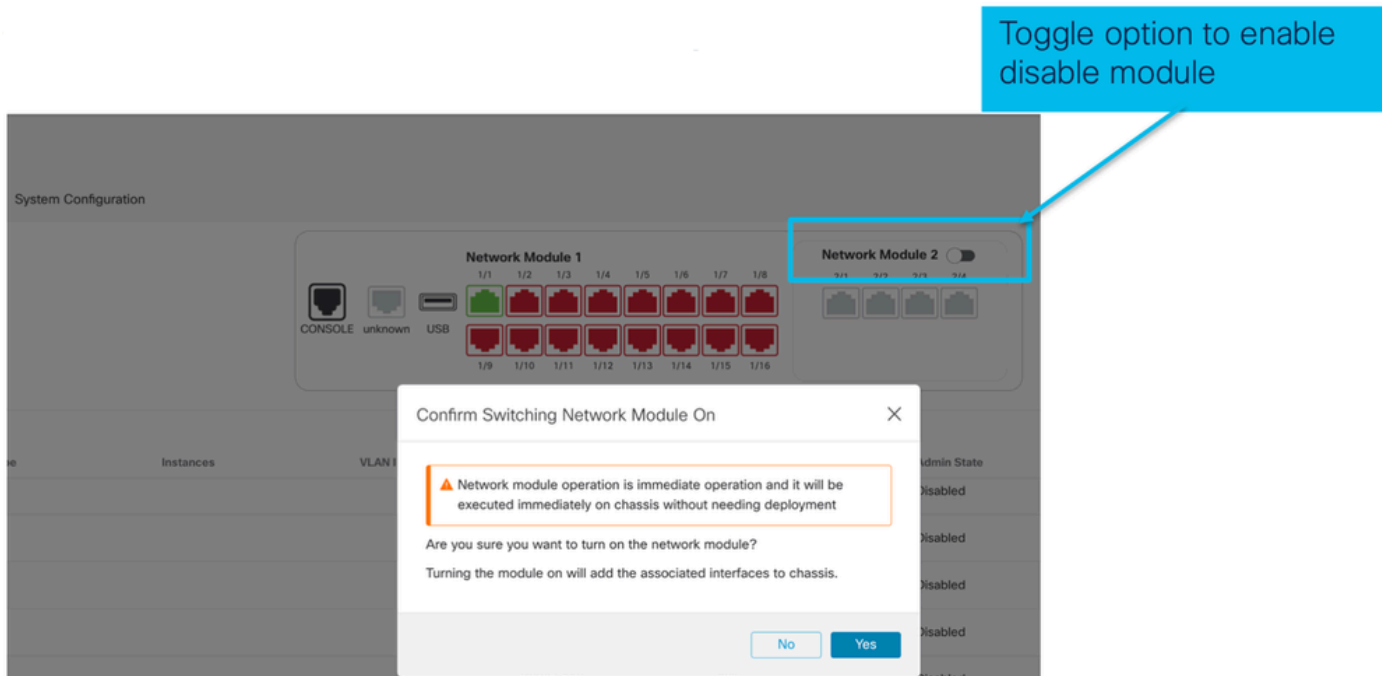
Documentazione relativa a EPM OIR e Breakout FMC serie 4200:

- <https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/4200/fw-4200->

<install/m-overview.html>

OIR: Abilita/Disabilita conferma EPM

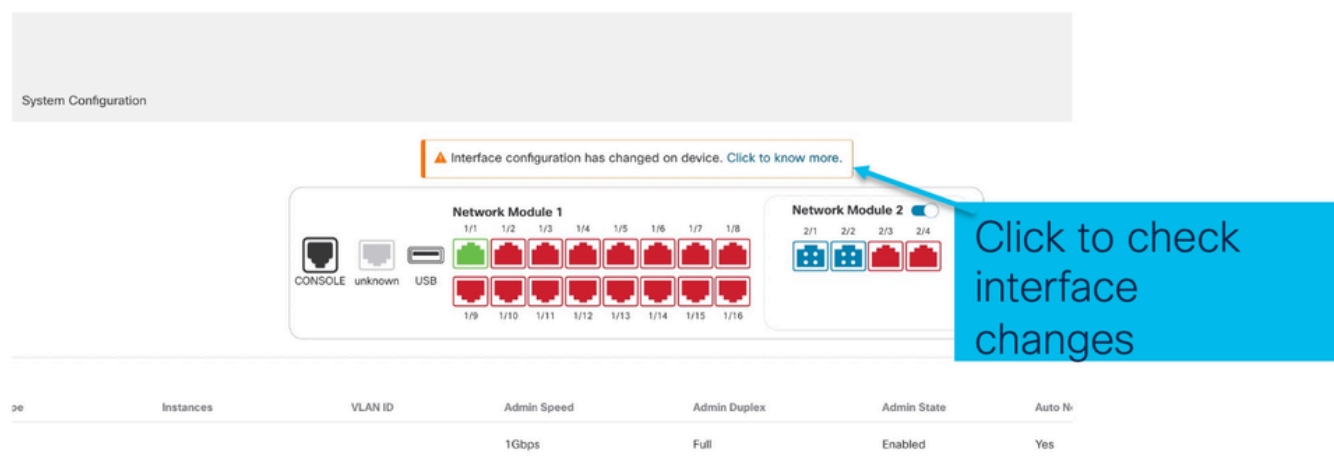
Quando l'utente attiva o disattiva il modulo, viene visualizzato un avviso per assicurarsi che non si tratti di un clic accidentale.



Abilitazione EPM completata: Notifica interfaccia ricevuta

- Quando si abilita un EPM, sul dispositivo vengono associate nuove interfacce.
- FMC riceve la notifica relativa alle interfacce associate.
- In FMC, l'utente deve accettare le modifiche.

In questa schermata viene mostrata l'opzione per visualizzare le interfacce associate:



Notifica modifica interfaccia EPM

La pagina di elenco delle interfacce elenca le interfacce aggiunte quando EPM è abilitato. Fare clic per ulteriori informazioni per aprire la finestra di dialogo Modifiche interfaccia. Fare clic per sapere se non è disponibile ulteriori informazioni dopo il salvataggio.

Interface Name	Type	Change Description
Ethernet2/1/1	PhysicalInterface	Interface is associated
Ethernet2/1/2	PhysicalInterface	Interface is associated
	PhysicalInterface	Interface is associated
	PhysicalInterface	Interface is associated

Pagina Opzioni di interruzione/unione nello chassis

pe	Instances	VLAN ID	Admin Speed	Admin Duplex	Admin State	Auto Negotiation	Admin FEC	
			Detect SFP	Full	Disabled	Yes	Auto	✎
			Detect SFP	Full	Enabled	Yes	Auto	✎
			Detect SFP	Full	Enabled	Yes	Auto	✎
			Detect SFP	Full	Disabled	Yes	Auto	✎
			Detect SFP	Full	Disabled	Yes	Auto	✎
			Detect SFP	Full	Disabled	Yes	Auto	✎
			Detect SFP	Full	Disabled	Yes	Auto	✎
			Detect SFP	Full	Disabled	Yes	Auto	✎
			Detect SFP	Full	Disabled	Yes	Auto	✎
			Detect SFP	Full	Disabled	Yes	Auto	✎

Viene attivata l'opzione Interfaccia interruzione della procedura guidata per la conferma dell'interruzione.

Confirm Interface Break



⚠ Interface break out is immediate operation and it will be executed instantly on device without needing deployment

Break operation splits the port to multiple ports, Are you sure you want to continue?

Ethernet2/2 will break in following interfaces.

Interface Break	Resulting Interface	Admin Speed
Ethernet2/2 (Admin Speed:40G)	Ethernet2/2/1	10G
	Ethernet2/2/2	10G
	Ethernet2/2/3	10G
	Ethernet2/2/4	10G

No

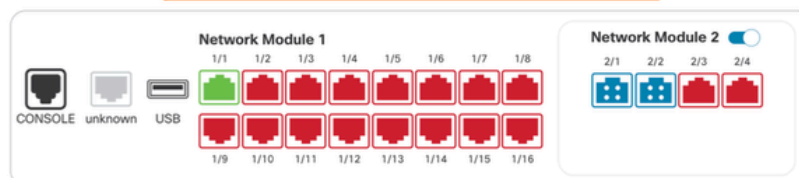


La notifica di aggiornamento dell'interfaccia è visibile sulla pagina dello chassis dopo la conferma dell'interruzione dell'interfaccia.

Click on the "Click to know more" link to notice the interface changes

System Configuration

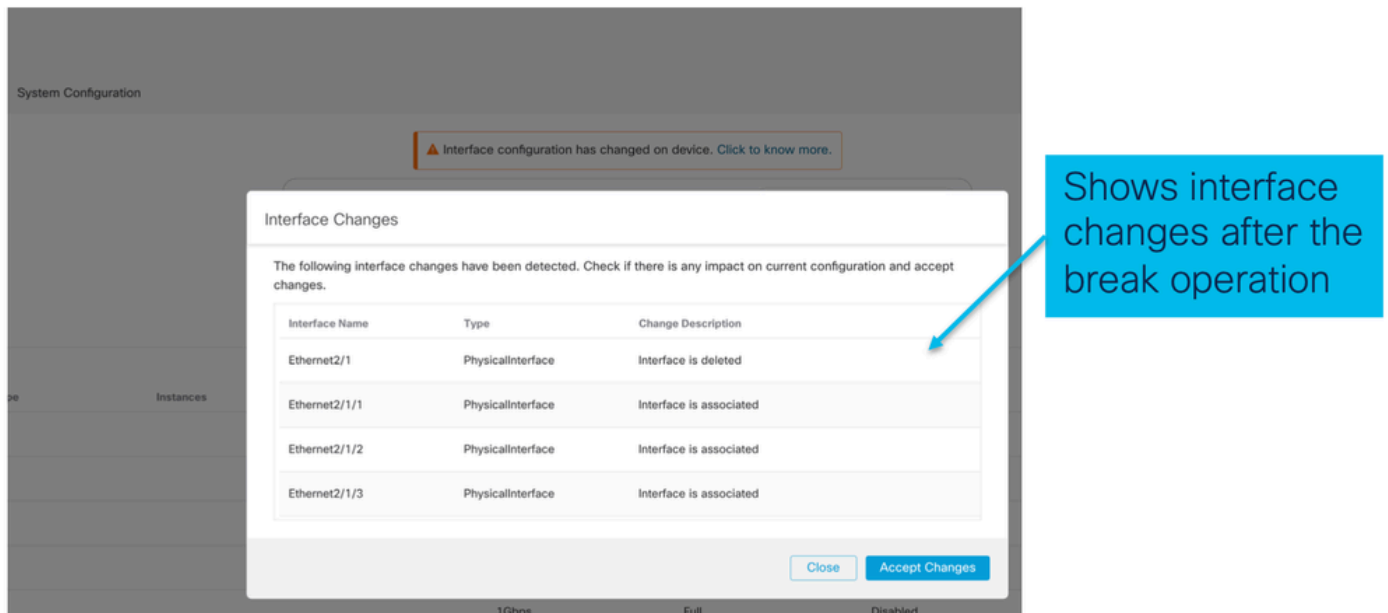
⚠ Interface configuration has changed on device. Click to know more.



pe	Instances	VLAN ID	Admin Speed	Admin Duplex	Admin State	Auto Ni
			1Gbps	Full	Enabled	Yes
			1Gbps	Full	Enabled	Yes

Modifiche all'interfaccia dopo un'interruzione o un'unione

Facendo clic su Accetta modifiche (Accept Changes), queste interfacce diventano disponibili nel CCP per essere utilizzate:



Impatto delle modifiche dell'interfaccia sull'istanza

Change	Behavior
Change a dedicated interface to shared	No validation error
Change a shared interface used in multiple instance to dedicated	Validation error will block the change
Disable of Network module with interfaces assigned to Instance	No validation error during the disable operation, but error will be thrown in case user tries to accept the notifications without removing the assignment from the instance
Break/Join of interfaces assigned to instance	<ul style="list-style-type: none">Validation error will be thrown to initiate such operationUser needs to unassign the interfaces from the Logical Device before initiating Break/Join operation

Gestione istanze

Instance Management consente di:

- Visualizzare tutte le istanze FTD esistenti e i relativi dettagli su un dispositivo serie 4200 (modalità MI).
- Crea/aggiorna istanze FTD con la versione del core CPU e del software desiderati.

- Eliminare un'istanza FTD esistente.
- Consente all'utente di scegliere i criteri FTD - Criteri di accesso e i criteri Impostazioni piattaforma per l'istanza FTD.
- Registra automaticamente l'istanza FTD in FMC quando è in linea.

View By:

All (1) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (1) ● Deployment Pending (0) ● Upgrade (0)

[Collapse All](#) [Download Device List Report](#)

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	▼ Ungrouped (1)							
<input type="checkbox"/>	● 4215_WA_Chassis 192.168.1.80	Firewall 4215 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	N/A	N/A	N/A	

Click 'Manage' to view 4200 Series (MI mode) Chassis overview

Crea istanza

Avviare la procedura guidata facendo clic su Aggiungi istanza.

Chassis Manager: 4215_WA_Chassis ● Connected Save Cancel

Cisco Secure Firewall 4215 Threat Defense Multi-Instance Supervisor

Summary Interfaces **Instances** System Configuration

Add Instance

There are no instances created yet.
[Add an instance to get started](#)

Click 'Instances' tab to navigate to instance listing page.

Click on 'Add an Instance' to launch FTD Instance create wizard. When there are no existing instances, you will see 'Add an FTD Instance' link.

Passaggio 1. Contratto:

Chassis Manager: 421

Firewall Management

Add Instance

1 Agreement 2 Instance Configuration 3 Interface Assignment 4 Device Management 5 Summary

End User License Agreement
Effective: May 10, 2022
Secure Firewall Terms and Conditions
By clicking 'Accept' below or using this Cisco Technology, you agree that such use is governed by the Cisco End User License Agreement and applicable Product Specific Terms available at:
<https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html>
You also acknowledge that you have read the Cisco Privacy Statement at:
<https://www.cisco.com/c/en/us/about/legal/privacy-full.html>
If you are a Cisco partner accepting on behalf of an end customer, you must inform the end customer that the end customer's use of the Cisco Technology and provide the end customer with access to all relevant terms. If you do not have the authority to bind your company and its affiliates, or if you do not agree with the terms of the EULA, do not click 'Accept' to use the Cisco Technology.
 I understand and accept the agreement.

Click on 'Add an Instance' will launch FTD instance creation guided wizard.

Read EULA and click check box to accept. Once accepted 'Next' button will be enabled.

Add FTD instance wizard. First step is to approve EULA

Passaggio 2.

- Nozioni di base sulla configurazione delle istanze:

Add Instance

1 Agreement 2 Instance Configuration 3 Interface Assignment 4 Device Management 5 Summary

Display Name *
WA_instance_1

Device Version *
7.6.0.1208

Resource Profile *
Default-Small

Management IP *
192.168.1.81

Network Mask *
255.255.255.0

Network Gateway *
192.168.1.254

Search Domain

FQDN

Firewall Mode *
Routed

DNS Servers

Device SSH Password *

Confirm Password *

Step 2 in instance creation wizard is to configure FTD instance.

Display name of FTD instance. FMC lists the device with the same name as on listing page.

Allows configuring core allocation for this FTD instance. You can pick a pre-defined resource profile (Default-Small, Default-Medium, or Default-Large) or make a new one. Use the '+' icon to define a custom resource profile object.

FTD version and build number. In 7.6.0, only possible version will be 7.6.0-XX.

- IP configurazione istanza:

Add Instance

1 Agreement 2 Instance Configuration 3 Interface Assignment 4 Device Management 5 Summary

Display Name *
WA_Instance_1

Device Version *
7.6.0.1208

Resource Profile *
Default-Small

Permit Expert mode for CLI

IPv4 IPv6 Both

IPv4 Management IP *
192.168.1.81

Network Mask *
255.255.255.0

Network Gateway *
192.168.1.254

Search Domain

FQDN

Firewall Mode *
Routed

DNS Servers

Device SSH Password *

Confirm Password *

Show Password

Cancel Back Next

Allows user to configure IPv4, IPv6 or Both IPv4 and IPv6 management IP address for FTD instance. Customer will be able to SSH to FTD device using this management IP address

IPv4 IPv6 Both

IPv6 Management IP *
2001:a00::192:168:1235

Prefix *
112

Network Gateway *
2001:a00::192:168:1240

IPv4 IPv6 Both

IPv4 Management IP *
192.168.1.81

Network Mask *
255.255.255.0

Network Gateway *
192.168.1.254

IPv6 Management IP *
2001:a00::192:168:1235

Prefix *
112

Network Gateway *
2001:a00::192:168:1240

Passaggio 3. Assegnazioni interfaccia:

Add Instance

1 Agreement 2 Instance Configuration 3 Interface Assignment 4 Device Management 5 Summary

Available Interfaces (14)

Ethernet1/1
Ethernet1/3
Ethernet1/5
Ethernet1/5.11
Ethernet1/5.12
Ethernet1/9
Ethernet1/10
Ethernet1/11
Ethernet1/12
Ethernet1/13
Ethernet1/14
Ethernet1/15
Ethernet1/16
Port-channel1

Selected Interfaces (2)

Ethernet1/2
Ethernet1/4

Cancel Back Next

Step 3 allows you to assign interfaces to FTD instance.

Lists all available physical, sub-interfaces and port-channel interfaces.

Lists all interfaces selected for this instance.

Bulk add all and remove all interfaces. Moves all available interfaces as selected interfaces and vice-versa.

Delete icon allows you to remove interface from the Selected to Available lists.

Add icon '+' allows you to add an available interface as selected interface.

A share icon Indicates the interface is shared.

Passaggio 4. Gestione dei dispositivi:

Add Instance

1 Agreement 2 Instance Configuration 3 Interface Assignment 4 Device Management 5 Summary

Device Group: Select...

Access Control Policy*: Policy1

Platform Settings: Select...

Smart Licensing:

- Carrier
- Malware Defense
- IPS
- URL

Cancel Back Next

Step 4 allows to assign default access policy, platform setting, device group and choose smart license for FTD.

Select an existing device group. FTD instance will be part of the group once online.

Select default access policy. The '+' icon allows creation of a new access policy. It is mandatory to assign an access policy.

Select default platform settings policy. The '+' icon allows creation of a new chassis platform setting policy. It is not mandatory.

Select smart license(s) applicable for FTD instance.

Passaggio 5. Riepilogo:

Add Instance

1 Agreement 2 Instance Configuration 3 Interface Assignment 4 Device Management 5 Summary

Instance Configuration

Name: WA_Instance_1

Version: 7.6.0.1208

Resource Profile: Default-Small

IP: 192.168.1.81

Mask: 255.255.255.0

Gateway: 192.168.1.254

Mode: routed

Password: *****

FQDN:

DNS Servers:

Search Domain:

Expert Mode: disabled

Device Management - This info is required only during instance creation.

Access Policy: Policy1

Device Group:

Platform Policy:

Licenses: Carrier, Malware Defense

Interface Assignment - 2 dedicated and 0 shared interfaces attached [Hide](#)

Name	Port Type
Ethernet1/1	DATA
Ethernet1/2	DATA

Cancel Back Save

Last step towards creating an FTD instance. Summary tab allows you to review and edit configuration before staging it. (Final step is Deploy.)

Each tile summarizes sections of configuration performed in previous steps of the wizard.

Edit icon in each tile will navigate user to respective section of the wizard, allowing them to edit configuration.

Final step is to click 'Save'. Configuration will be staged in FMC.

Per completare la configurazione, salvare e distribuire.

Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy

Chassis Manager: 4215_WA_Chassis Connected You have unsaved changes Save Cancel

Summary Interfaces Instances System Configuration

Name	Version	Resource Profile	Management IP	Management Gateway	Licenses
WA_instance_1	7.6.0.1208	Default-Small	192.168.1.81	192.168.1.254	Carrier, ... Policy1 N.A

1 Step 1. Click on the Save button to save the changes on the chassis.

2 Step 2. Click on Deploy to push the staged configuration in FMC to Chassis.

Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy

Chassis Manager: 4215_WA_Chassis Connected

Instance configuration has changed. A deployment is required.

Summary Interfaces Instances System Configuration

Name	Version	Resource Profile	Management IP	Management Gateway
WA_instance_1	7.6.0.1208	Default-Small	192.168.1.81	192.168.1.254

Advanced Deploy Deploy All Cancel

4215_WA_Chassis | Ready for Deployment

1 device is available for deployment

3 Step 3. Select the device and click on Deploy All to immediately deploy the changes or click on 'Advanced Deploy' to review the changes and then deploy.

Registrazione automatica di un'istanza FTD dopo la corretta distribuzione:

The screenshot shows the Chassis Manager interface for a device named '4215_WA_chassis'. The 'Instances' tab is active, displaying a table with the following data:

Name	Version	Resource Profile	Management IP	Management Gateway	Licenses	AC Policy
starting_1	7.6.0.1217	Default-Small	192.168.1.81	192.168.1.254	Carrier, ...	Pol

On the right, a notification panel shows two messages:

- Chassis 4215_WA_chassis WA_instance_1: provisioning
- Chassis 4215_WA_chassis WA_instance_1: installing

On successful deployment, FTD instance will boot up. Instance will transition from offline to starting, and, then, online state. Once online, auto-registration will kick in and FTD instance will get registered and listed in the device listing page. Task Manager messages will inform the user on progress of instance creation and registration.

Istanza registrata nel centro di gestione:

The screenshot shows the FMC Device Listing Page. At the top, there are status indicators for various device states: All (2), Error (1), Warning (0), Offline (0), Normal (1), Deployment Pending (1), Upgrade (0), and Snort 3 (1). A search bar and an 'Add' button are also visible.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
4215_WA_chassis 192.168.1.80	Firewall 4215 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	N/A	N/A	N/A
WA_instance_1 192.168.1.81 - Routed	Firewall 4215 Threat Defense	7.6.0	N/A	Essentials, Malware (1 more...)	None	

FMC Device Listing Page
Once auto-registration is successful, the FTD instance gets listed on the device listing page.

Modifica di un'istanza

Fare clic sull'icona a forma di matita per modificare un'istanza FTD:

Chassis Manager: 4215_WA_chassis Connected Save Cancel

Cisco Secure Firewall 4215 Threat Defense Multi-Instance Supervisor

Summary Interfaces **Instances** System Configuration

Search an instance Add Instance

Name	Version	Resource Profile	Management IP	Management Gateway	Licenses	AC Policy	Platform Settings	
WA_instance_1	7.6.0.1217	Default-Small	192.168.1.81	192.168.1.254	Carrier, ...	Pol	N.A	

Click on the pencil icon to open the edit instance dialog.

Passaggio 1. Modifica istanza FTD:

Edit Instance

1 Instance Configuration 2 Interface Assignment 3 Summary

Display Name *
WA_instance_1

Device Version *
7.6.0.1217

Admin State Permit Expert mode for CLI

Resource Profile *
Default-Small

IPv4 IPv6 Both

IPv4

Management IP *
192.168.1.81

Network Mask *
255.255.255.0

Network Gateway *
192.168.1.254

Search Domain

QDN

Firewall Mode *
Routed

DNS Servers

Device SSH Password *

Confirm Password *

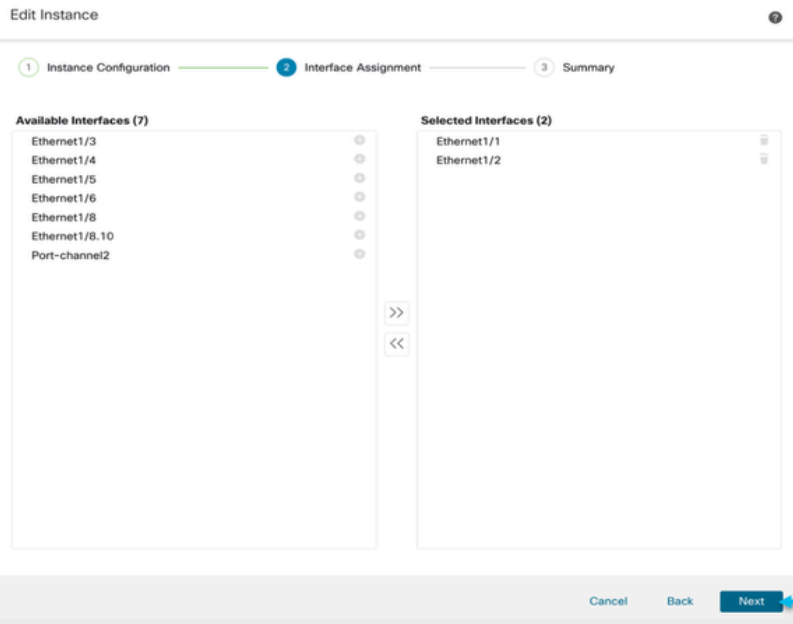
Cancel Next

The Edit Instance dialog is like the Create Instance wizard.

However, the user does not have the option to edit EULA, display name, or device version.

Click on the 'Next' button to edit interface assignments

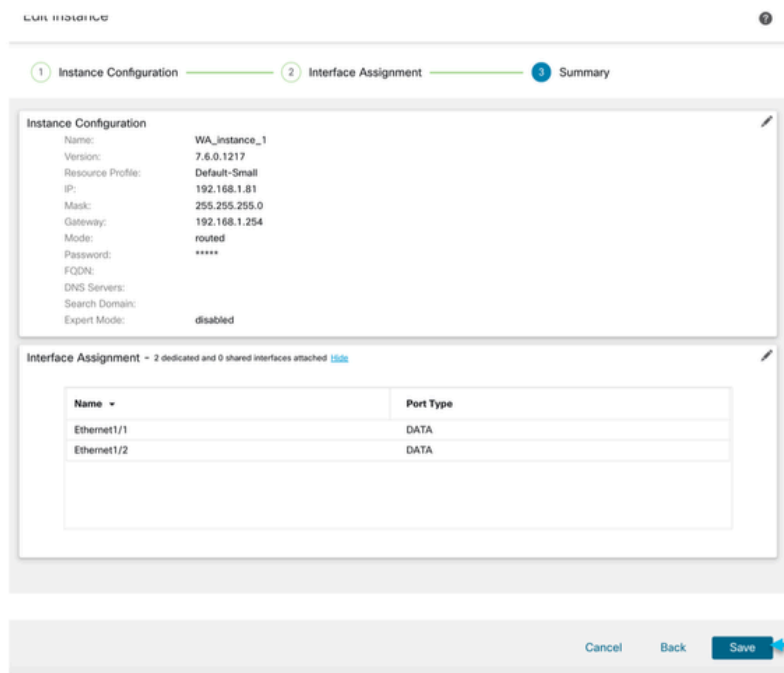
Passaggio 2. Modificare le assegnazioni di interfaccia per un'istanza:



The next step allows the user to modify interface assignments. User can add new interface or remove existing interfaces.

Click on the 'Next' button to view a summary of changes made to the instance

Passaggio 3. Riepilogo dell'istanza di modifica:



The last step of editing an instance is to view the summary of changes made to the instance.

Each tile has a pencil icon that navigates user to respective section of the edit steps.

Click the 'Save' button to stage the configuration changes in FMC. The user can review and deploy the changes at a later point in time.

Elimina istanza



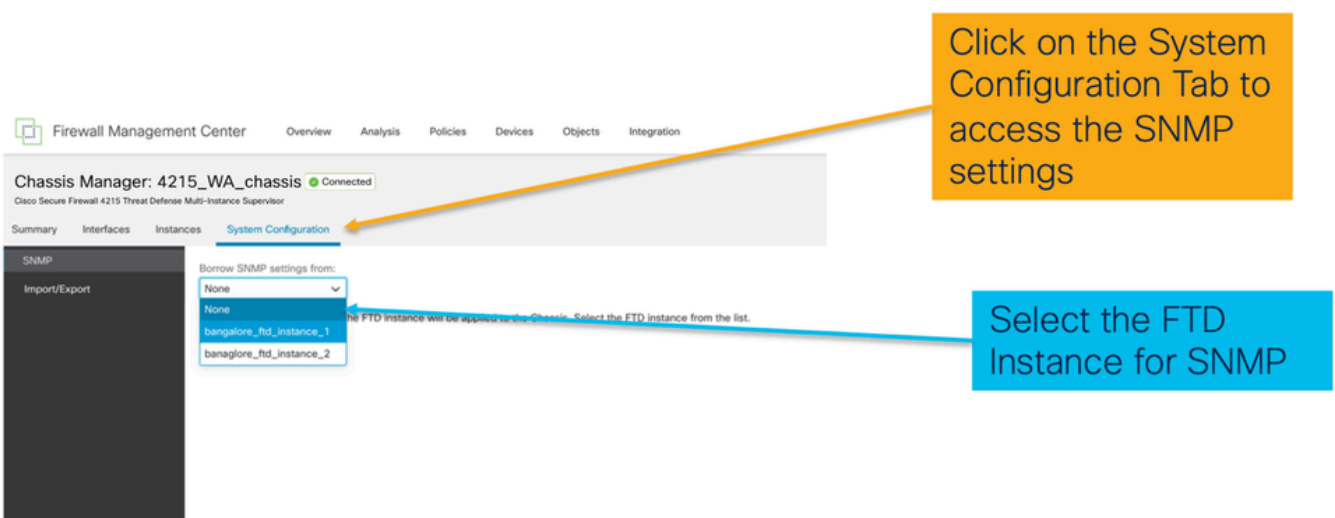
Use the Delete option (from the trash can icon) to delete an existing instance.

Deleting an instance will stage the changes in FMC. Clicking delete will not impact device unless configuration saved and then deployed.

Deleting an instance will free up core allocation.

Configurazione SNMP

Passare alla scheda di configurazione del sistema per la configurazione di SNMP:



Importazione/esportazione chassis

Esporta configurazione

Selezionare Gestione chassis > Configurazione di sistema > Importazione/esportazione:

Chassis Manager: 4215_WA_chassis Connected
Cisco Secure Firewall 4215 Threat Defense Multi-Instance Supervisor

Summary Interfaces Instances **System Configuration**

SNMP
Import/Export

Import
This will replace the current chassis configuration with new configuration
Drop File here

Export
This will create a Device Export configuration file
[Click here to export](#)

Download
This will download the config file exported
[Download](#)

Dismiss all notifications

Global **Device Configuration Export**
Device Configuration Export
Exporting device configurations

Global **Device Configuration Export**
Export file created successfully
Download Export Package

Click on the Import/Export subsection to access these settings.

Exports the chassis configuration and progress can be tracked in the Task Manager.

Export Bundle Can be downloaded from the link.

Importa configurazione

Selezionare Gestione chassis > Configurazione di sistema > Importazione/esportazione:

Chassis Manager: 4215_WA_chassis Connected
Cisco Secure Firewall 4215 Threat Defense Multi-Instance Supervisor

Summary Interfaces Instances **System Configuration**

SNMP
Import/Export

Import
This will replace the current chassis configuration with new configuration
Drop File here

Export
This will create a Device Export configuration file
[Click here to export](#)

Download
This will download the config file exported
[Download](#)

Dismiss all notifications

Global **Device Configuration Export**
Device Configuration Export
Exporting device configurations

Global **Device Configuration Export**
Export file created successfully
Download Export Package

Download the generated exported *.sfo file

Import the configuration using Import option

Informazioni sull'importazione/esportazione dello chassis

- Tutte le configurazioni esistenti sullo chassis vengono sostituite dalla configurazione nel file importato.
- La versione del software della piattaforma in cui viene importata la configurazione deve corrispondere alla versione esportata.
- Lo chassis in cui si sta importando la configurazione deve avere lo stesso numero di moduli di rete installati al momento dell'esportazione.
- Lo chassis in cui viene importata la configurazione deve avere la stessa immagine dell'applicazione installata per le periferiche logiche.
- Le impostazioni di configurazione specifiche dell'applicazione non vengono esportate.

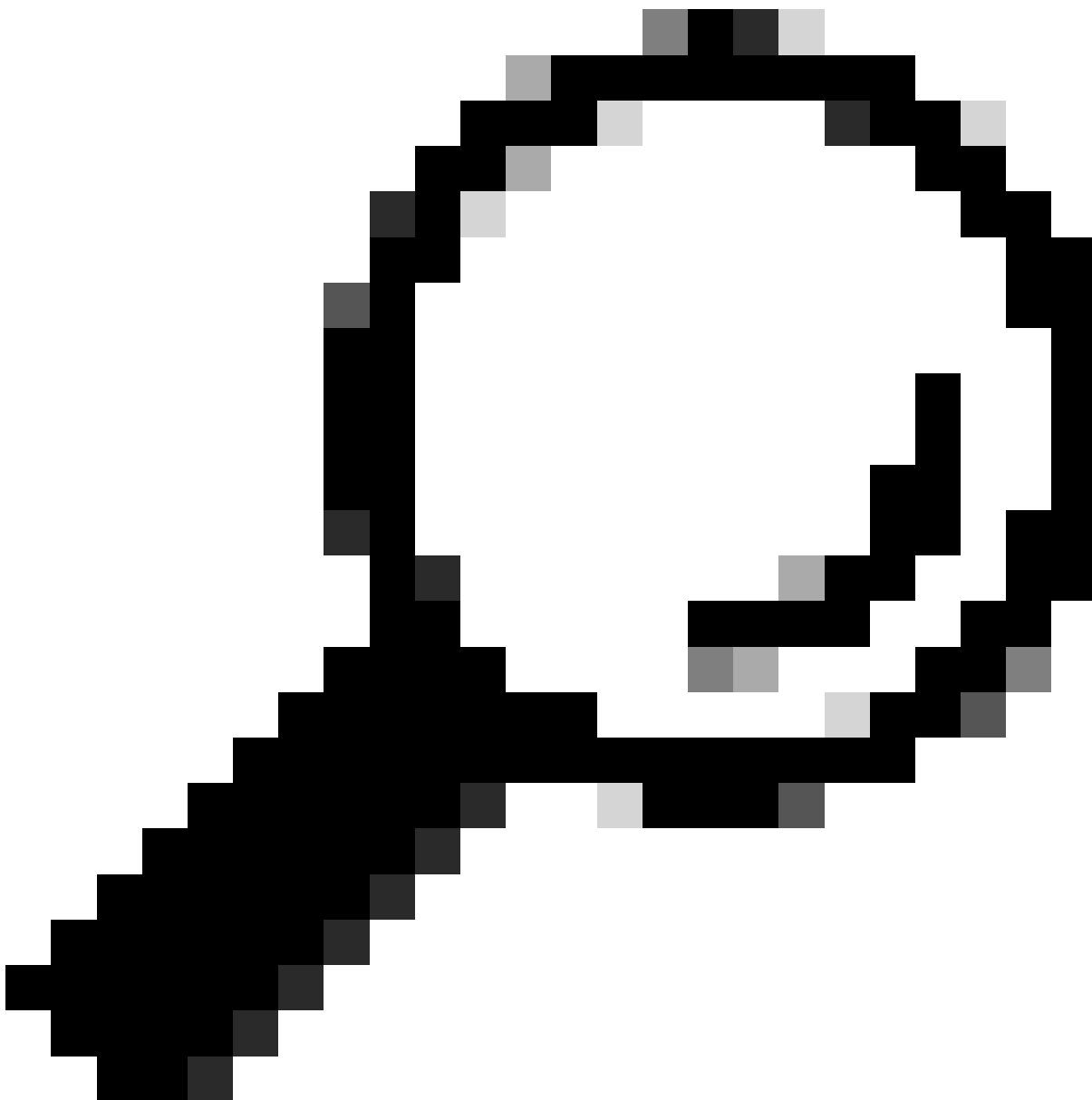
Vengono esportate solo le configurazioni dello chassis.

- Il backup delle istanze FTD deve essere eseguito separatamente.

Criteri di impostazione della piattaforma chassis

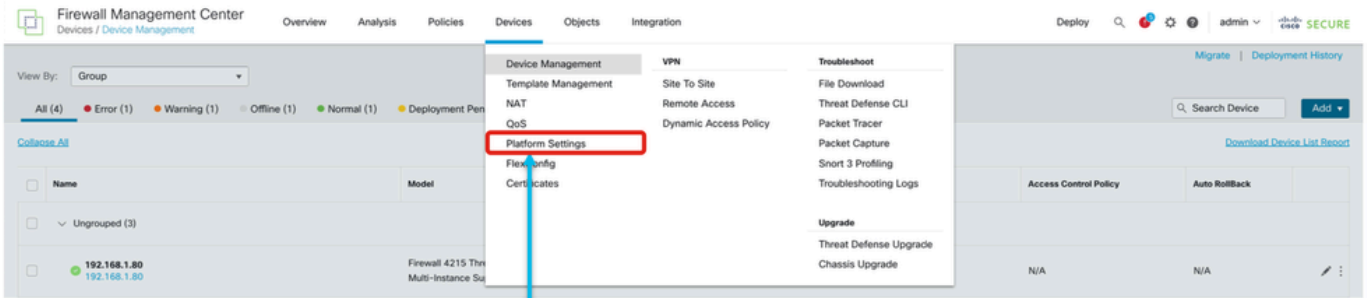
Il criterio relativo alle impostazioni della piattaforma dello chassis consente agli utenti di configurare le seguenti configurazioni specifiche della piattaforma:

- Sincronizzazione ora (NTP)
- DNS
- Syslog
- Fuso orario
- L'utente può creare una nuova regola "Chassis Platform Setting" (Impostazione piattaforma chassis) e assegnarla a più chassis serie 4200 (modalità MI).



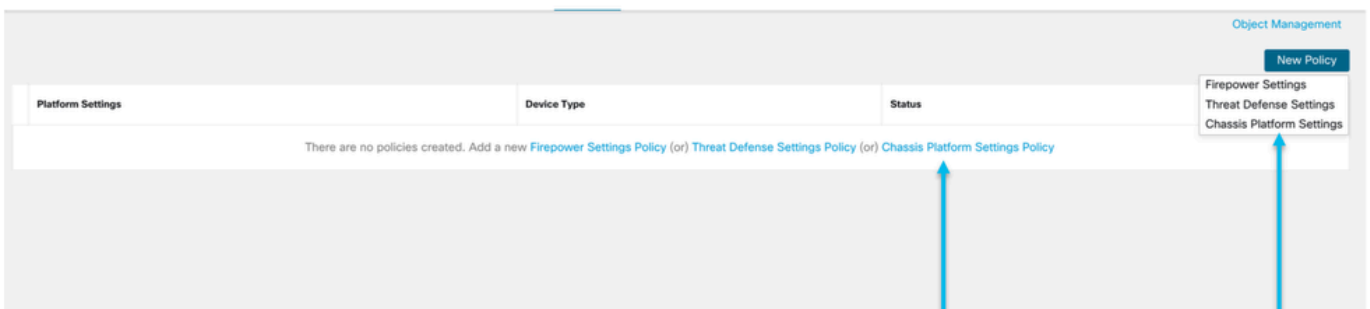
Suggerimento: Le impostazioni della piattaforma dello chassis si applicano solo allo chassis. Se l'utente desidera applicare le impostazioni della piattaforma alle proprie istanze, può utilizzare un criterio Impostazioni piattaforma di difesa dalle minacce.

1. Passare al criterio Impostazioni piattaforma dello chassis:



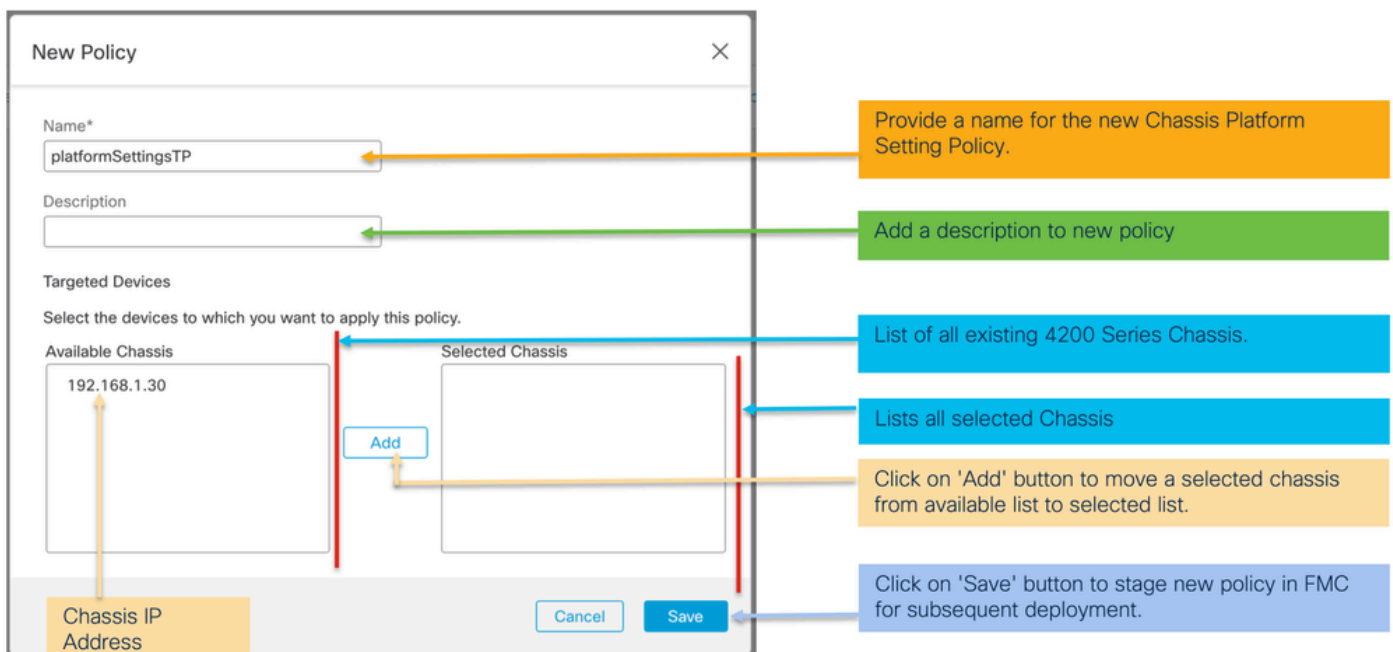
Head to the Platform Settings page to manage your Chassis Platform Settings.

2. Creare le impostazioni della piattaforma dello chassis:



'Chassis Platform Settings' was added in 7.4.1.

- To create a new Chassis Platform Settings Policy click on 'Chassis Platform Settings' under 'New Policy' to launch new platform settings dialog.
- When there are no existing platform setting policies, you will see the 'Chassis Platform Settings Policy' link. This is your launch point to create.



3. Pagina dei criteri di impostazione della piattaforma chassis:

PlatformSettingsTP / You have unsaved changes Cancel Save

Enter Description

DNS Resolution Settings

Specify DNS servers groups.

Enable DNS name resolution by device

DNS Server Groups Add

Policy Assignments (1)

Each platform setting has its own individual tab. Click on a tab to make configuration changes.

Shows the number of 4200 Series (MI mode) Chassis assigned to this policy. (In this screenshot, there is one.)

Impostazioni piattaforma chassis: DNS

Abilitare e aggiungere gruppi di server DNS nella sezione DNS del criterio Impostazioni piattaforma chassis:

platformSettingsTP / You have unsaved changes Cancel Save

Enter Description

DNS Resolution Settings

Specify DNS servers groups.

Enable DNS name resolution by device

DNS Server Groups Add

dns_serverTP (default)

Add DNS Server Group

Select DNS Server Group* dns_serverTP + New Group

Make as default

Cancel Save

Enable/Disable DNS resolution on the device

Select an existing DNS server group. User can choose an existing server group available in objects page

Click on \"+\" to create a new server group

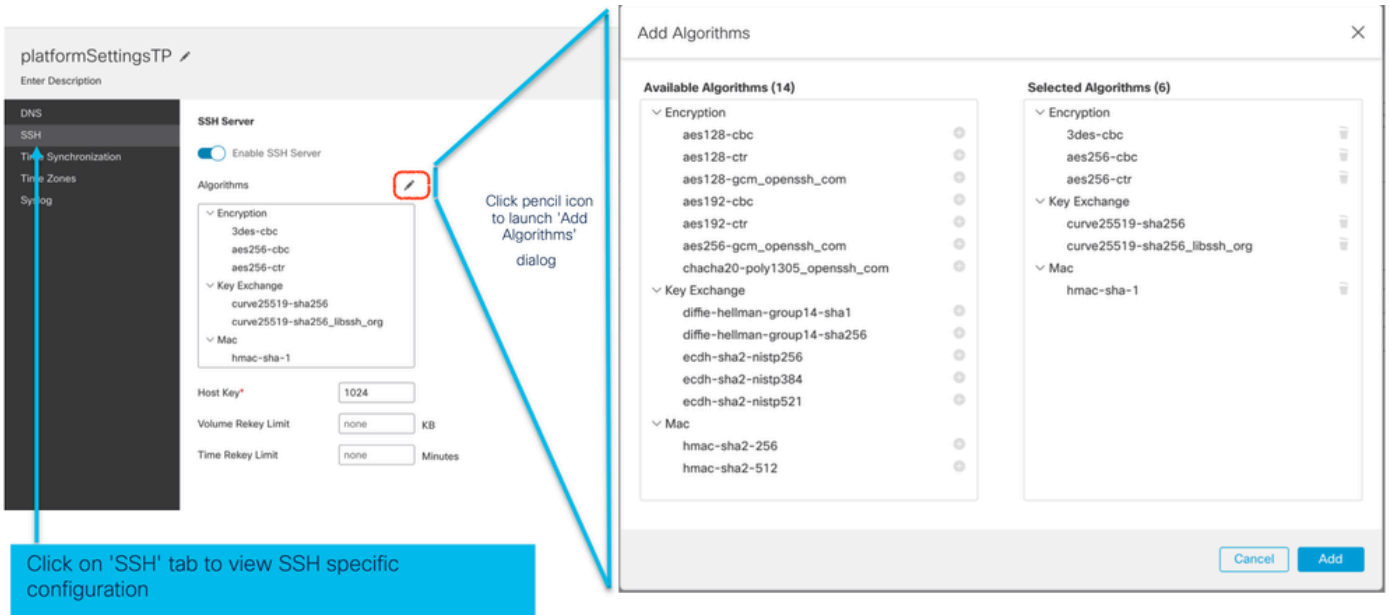
Click on delete icon to delete an existing DNS server group. Click on edit icon to launch dialog to edit DNS server group.

Lists of all DNS server groups

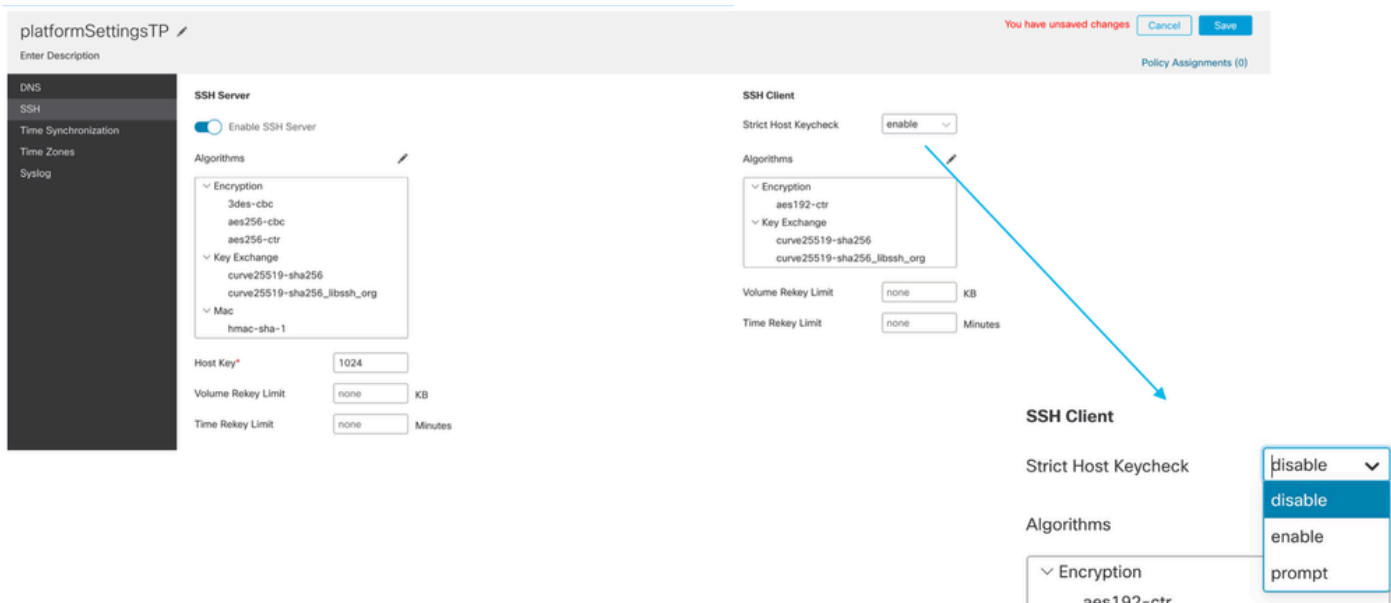
Click on 'DNS' tab to view DNS specific configuration

Impostazioni piattaforma chassis: SSH

- Abilitare e aggiungere il server SSH nella sezione SSH del criterio Impostazioni piattaforma chassis:



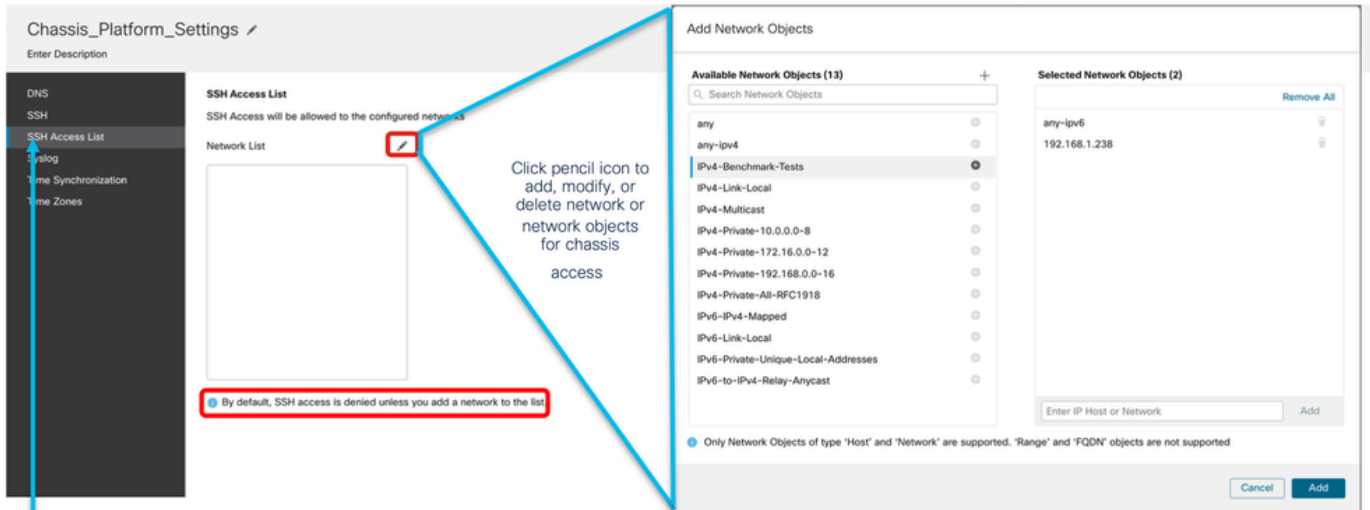
- Abilitare e aggiungere il client SSH:



Impostazioni piattaforma chassis: Elenco accessi SSH

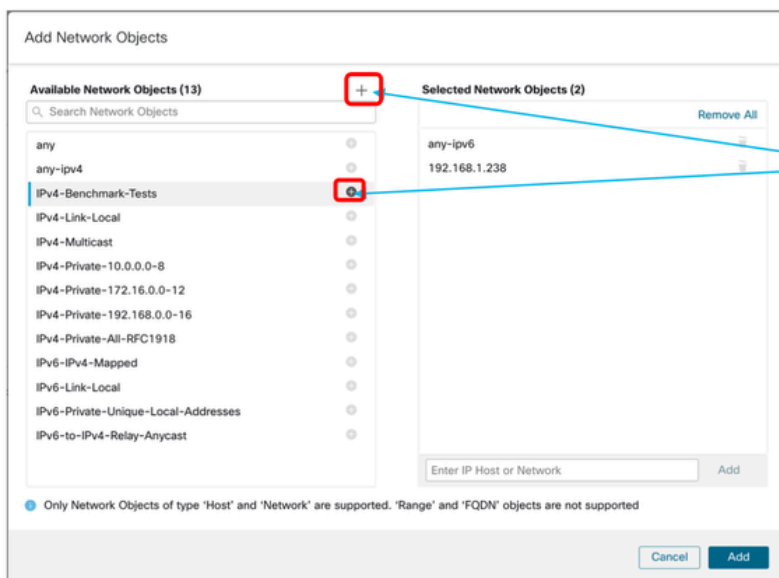
Questa scheda viene visualizzata solo dopo aver abilitato SSH nella sezione SSH delle impostazioni della piattaforma chassis.

- Creazione elenco accessi SSH:



Click on 'SSH Access List' tab to view Access List specific configuration

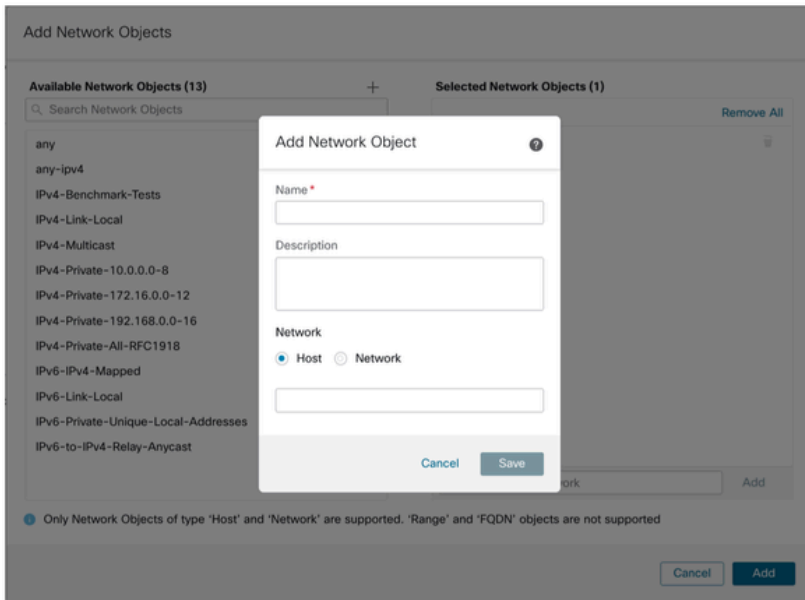
- Aggiungere l'elenco degli oggetti di rete per l'accesso SSH:



Network objects can be selected by:

1. Choosing from left side pane.
2. By creating a new object using the "+" icon.

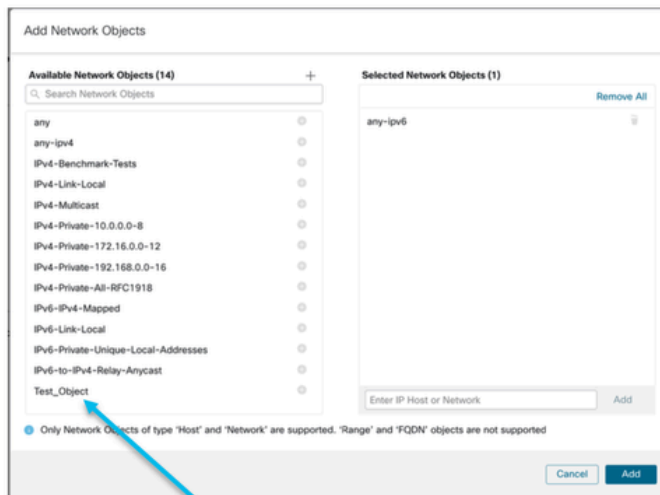
- Aggiungere un nuovo oggetto di rete:



Only Host and Network types are supported for chassis access list.

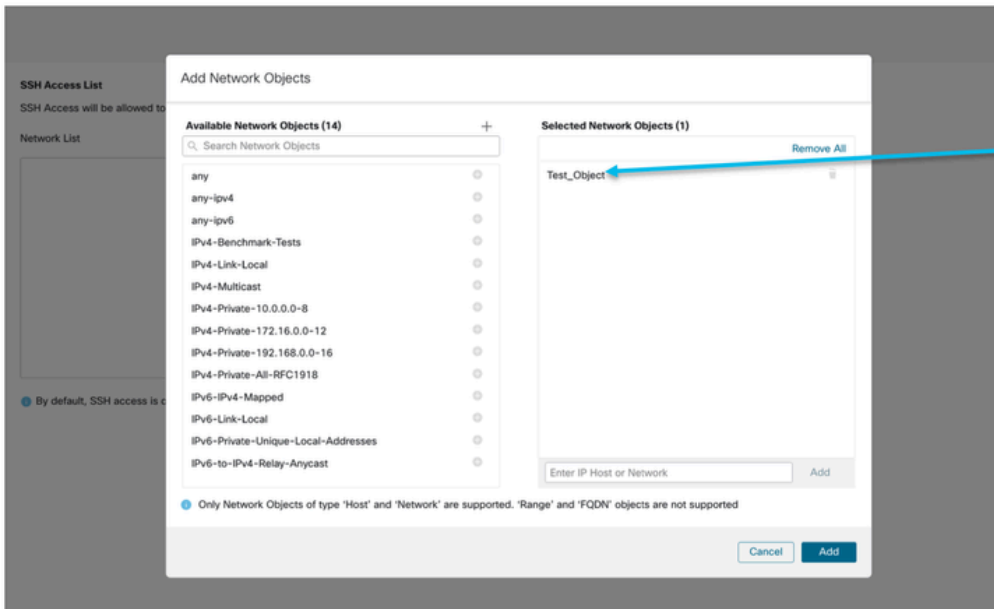
Range and FQDN are NOT allowed.

- Visualizza oggetti di rete:



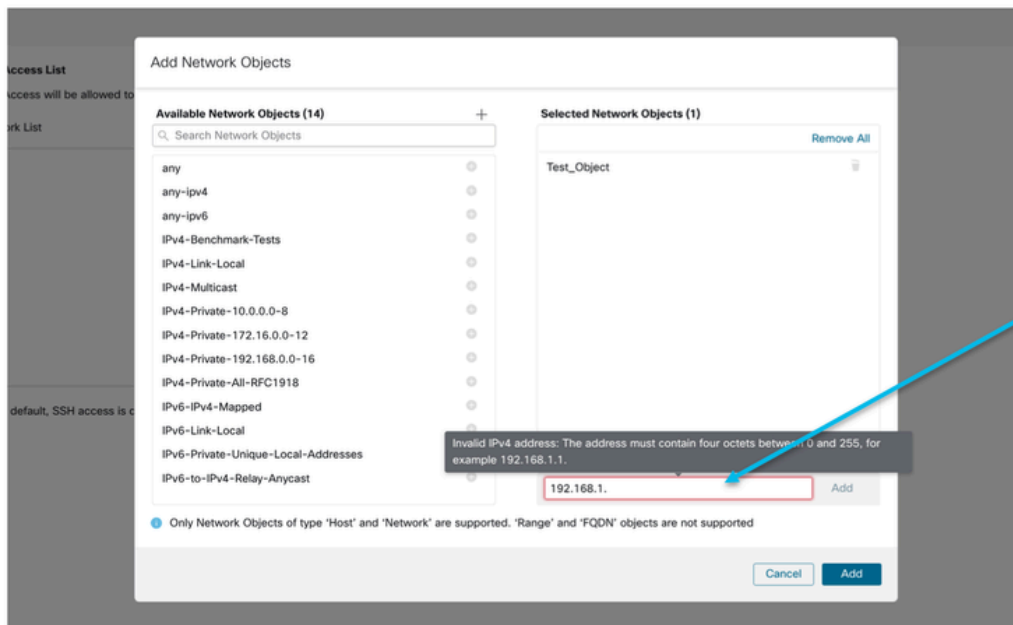
After creation of host object, it will be listed in the available network objects.

- Seleziona oggetti di rete:



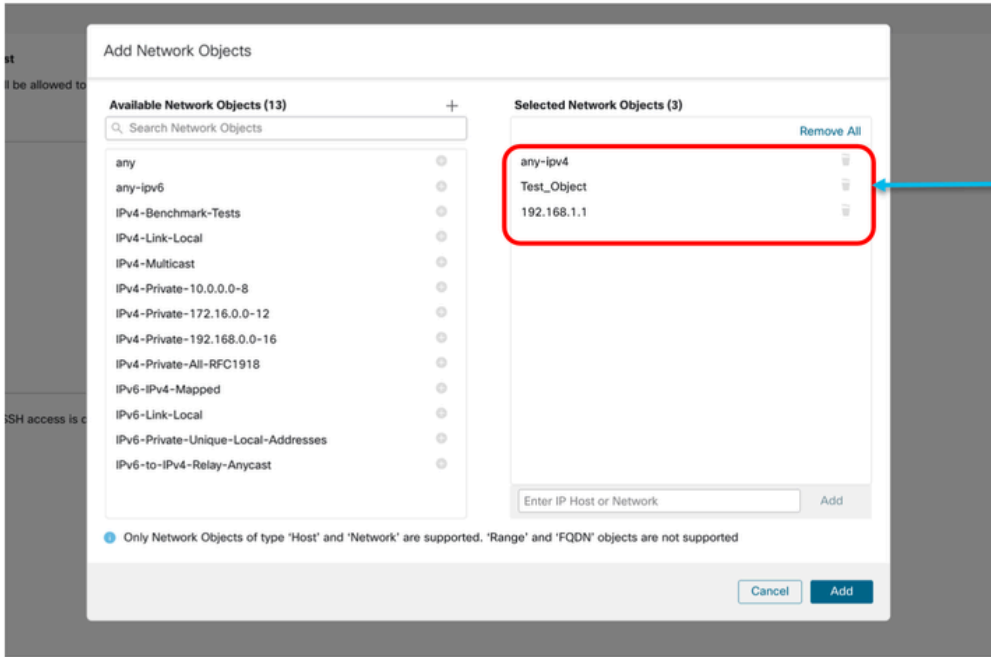
After selecting Network Objects using the “+” icon from available network objects, it will be listed in the selected pane.

- Gli oggetti di rete possono essere creati come mostrato nella seguente immagine:



Host and network objects can also be added directly from here by providing host IP or Network IP.

- Visualizza oggetti di rete aggiunti:



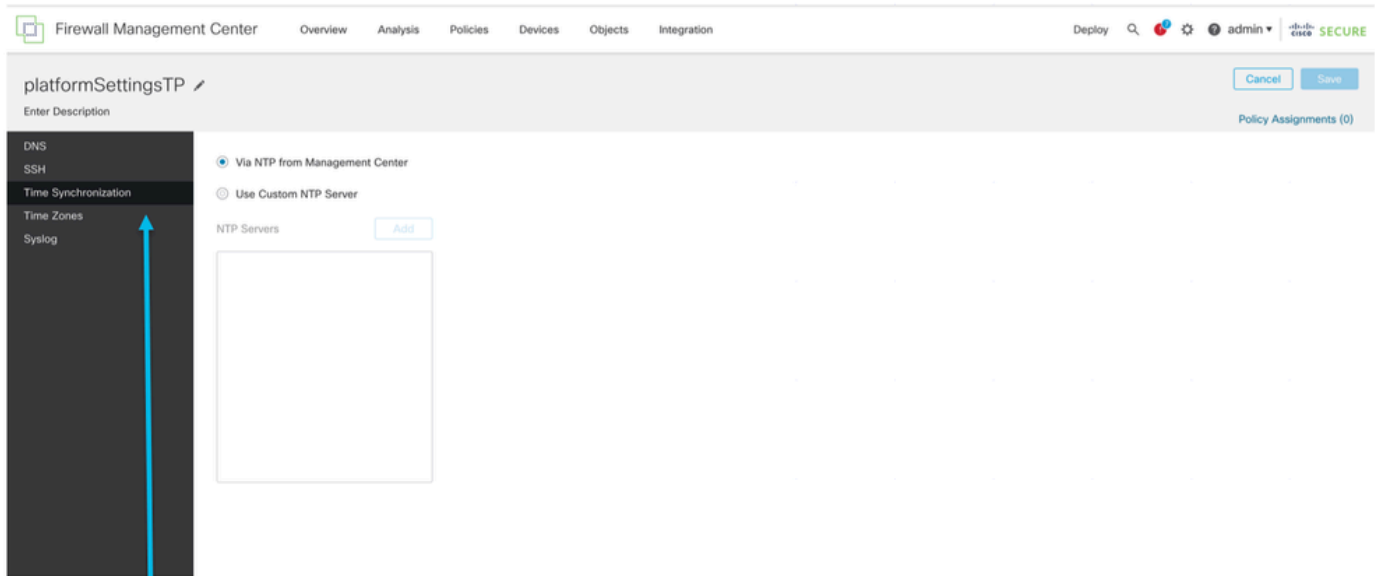
Once the objects are added, they will be listed in the Selected Network Objects pane.

Impostazioni piattaforma chassis: Sincronizzazione ora

La sincronizzazione dell'ora può essere eseguita in due modi:

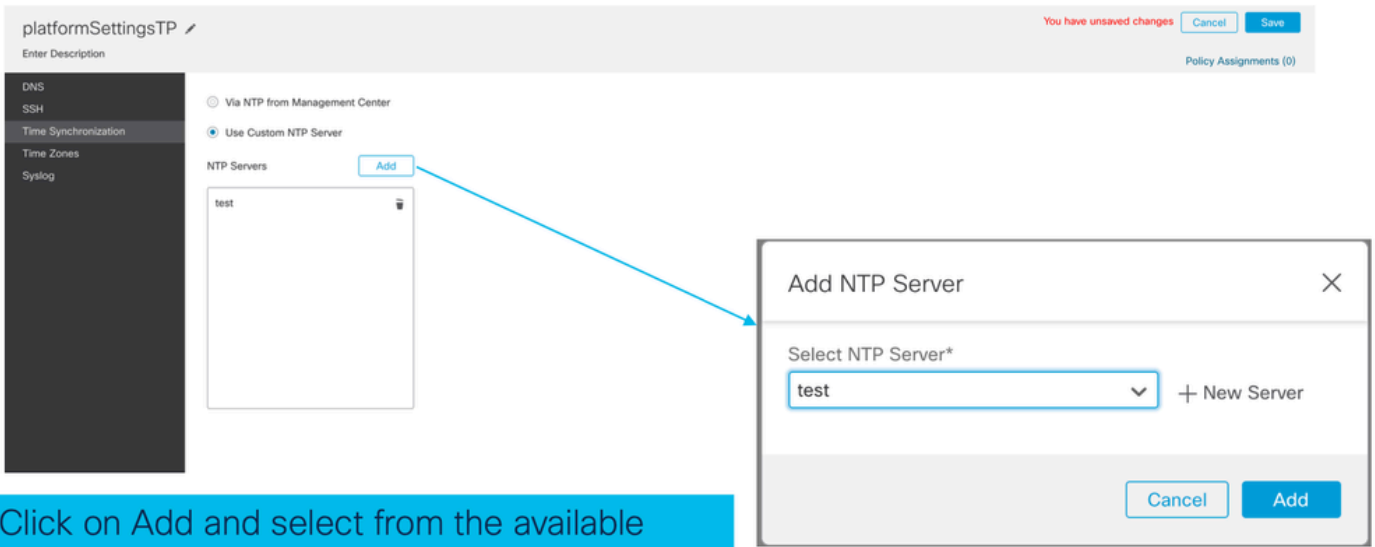
1. Tramite NTP dal centro di gestione
2. Sul server NTP personalizzato

Da NTP da Management Center



Time Synchronization can be achieved via NTP from Management Center or using a custom NTP Server

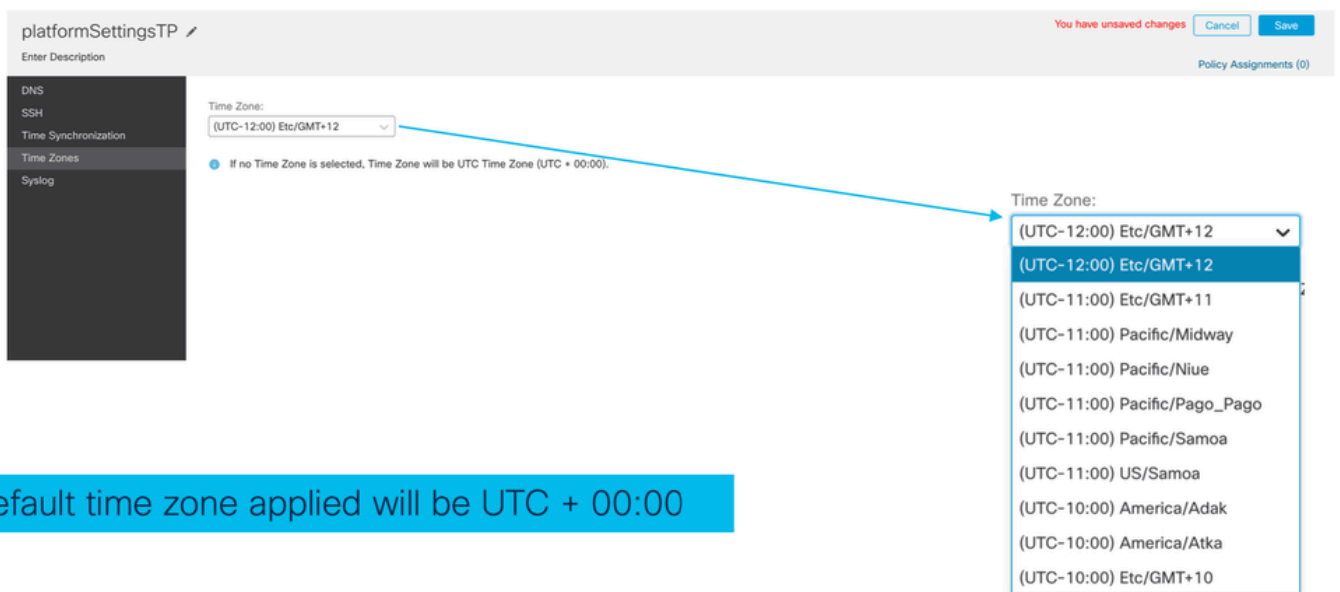
Sul server NTP personalizzato



Click on Add and select from the available NTP Server to Use Custom NTP

Impostazioni piattaforma chassis: Fusi orari

Fusi orari:



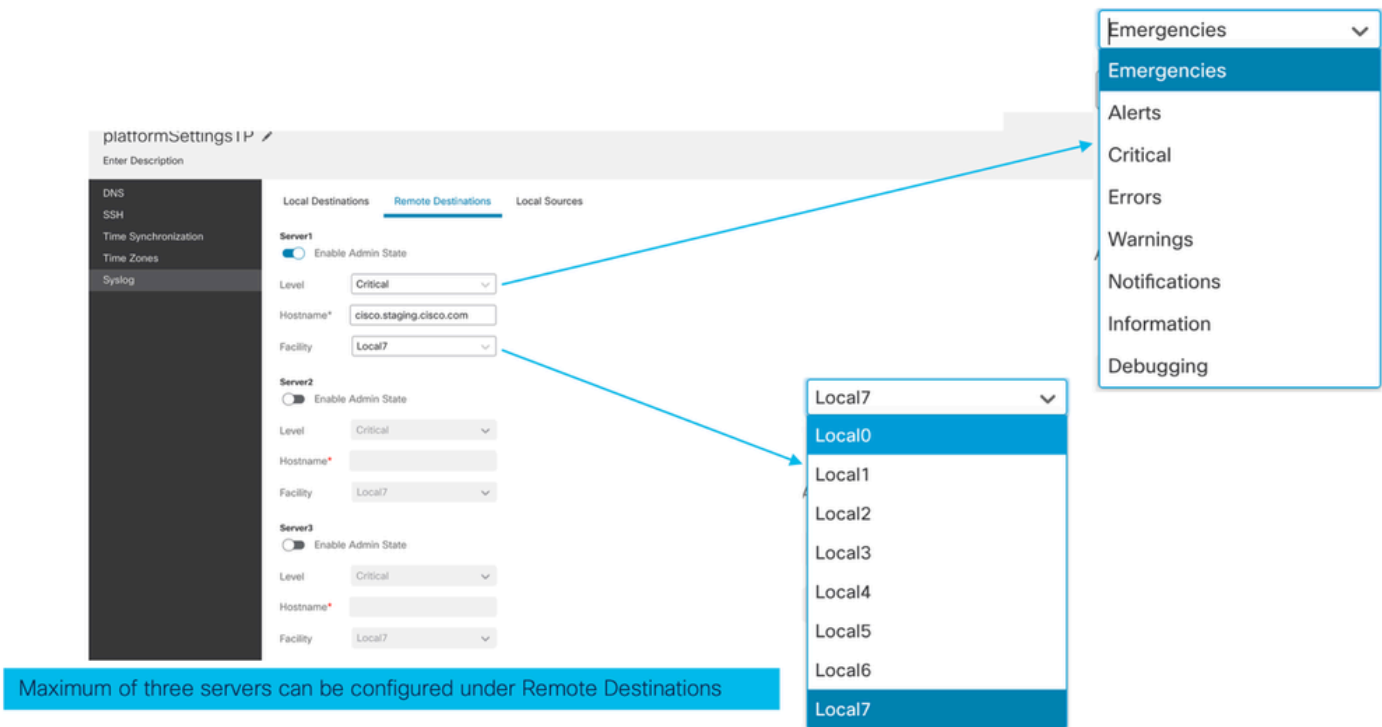
Default time zone applied will be UTC + 00:00

Impostazioni piattaforma chassis: Syslog

- Scheda Destinazioni locali Syslog:



- Scheda Destinazioni remote Syslog:



Maximum of three servers can be configured under Remote Destinations

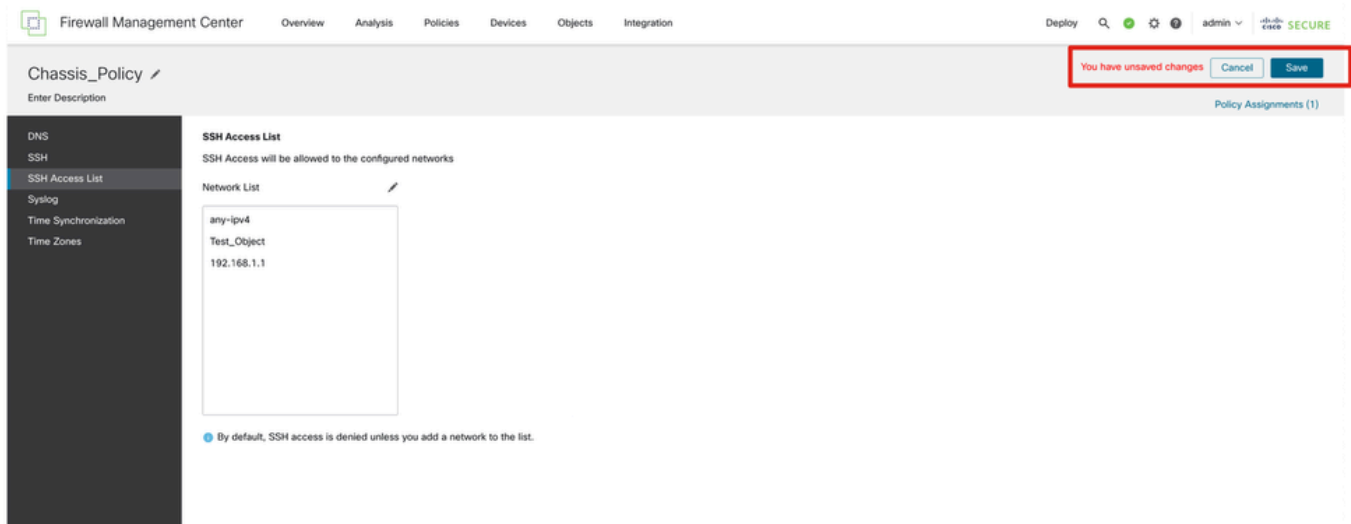
- Scheda Origini locali Syslog:



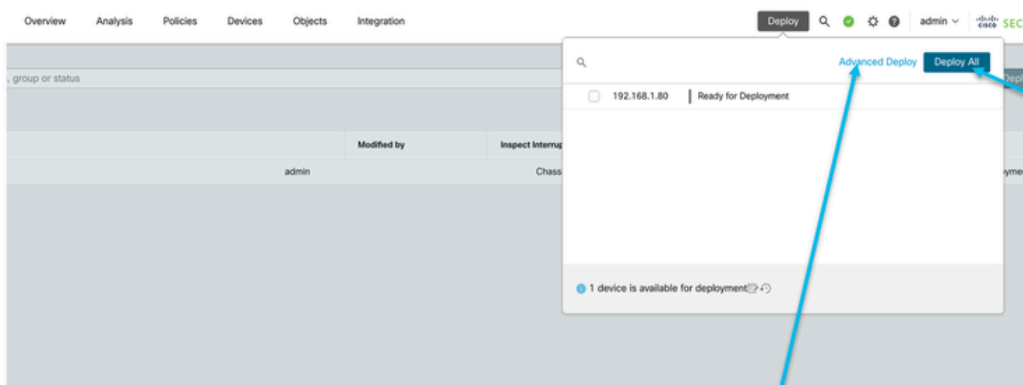
Click on the Local Sources tab to configure Faults/Audits/Events for Local Sources

Impostazioni piattaforma chassis: Salva e distribuisci

Salvare le modifiche alle impostazioni della piattaforma chassis, quindi distribuire:



Now, save the changes which has all the platform settings. Chassis will go for pending deployment.

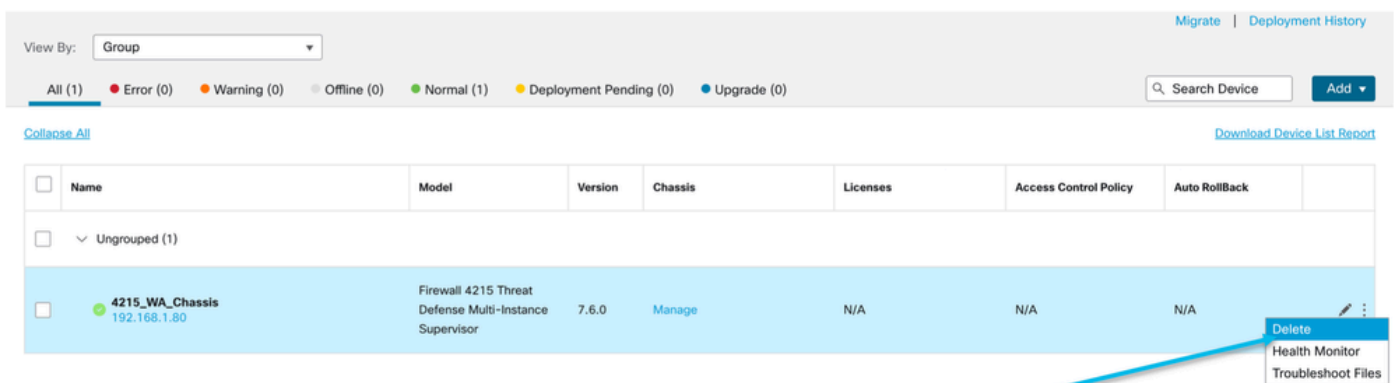


1. Trigger deployment.
2. Once deployment is completed, all chassis platform settings are deployed.

Now, chassis is ready for deployment. User can check the deployment preview for changes done.

Annullamento della registrazione dello chassis

Per annullare la registrazione di uno chassis da FMC, selezionare Dispositivi > Gestione dispositivi > Elimina.



Click 'Delete' to unregister 4200 Series (MI mode) device from FMC

Converti da istanza multipla in modalità nativa

Attualmente, FMC supporta solo la conversione da Nativo a Multiistanza. Di conseguenza, per riconvertire un dispositivo alla modalità nativa, l'utente deve utilizzare la CLI.

Passaggio 1: Annullare la registrazione dello chassis dal FMC.

Passaggio 2: Utilizzare questo comando CLI per convertire la periferica serie 4200 in modalità nativa:

```
firepower-4215# scope system
firepower-4215 /system # set deploymode native
```

API FMC Rest

Le API REST pubbliche di FMC sono disponibili per tutte le operazioni supportate da FMC.

Chassis	
GET	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{objectId}
DELETE	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{objectId}
GET	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis
POST	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis
GET	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/networkmodules/{objectId}
PUT	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/networkmodules/{objectId}
PUT	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operational/syncnetworkmodule
GET	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/interfaces/{interfaceUUID}
GET	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/chassisinterfaces/{interfaceUUID}
POST	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operational/breakoutinterfaces
POST	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operational/joininterfaces
GET	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/chassisinterfaces/{interfaceUUID}/evaluateoperation
GET	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/logicaldevices/{objectId}
PUT	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/logicaldevices/{objectId}
DELETE	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/logicaldevices/{objectId}
GET	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/logicaldevices
POST	/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/logicaldevices

API REST per conversione da native a multi-istanza

API POST per verificare se il dispositivo nativo è pronto per la conversione a più istanze:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/operating/switchmodereadinessch

JSON richiesta POST di esempio:

```
{
  "devices": [
    {
      "id": "DeviceUUID",
      "type": "Device"
    }
  ],
  "conversionType": "NATIVE_TO_MULTI_INSTANCE"
}
```

API POST per attivare la conversione da singola istanza a più istanze:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/operating/switchmode

JSON richiesta POST di esempio:

```
{
  "items": [
    {
      "id": "

", "displayName": "Sample_Chassis_Name1" } ], "conversionType": "NATIVE_TO_MULTI_INSTANCE" }
```

API POST per attivare la conversione da nativa a più istanze in blocco:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/operating/switchmode

JSON richiesta POST di esempio:

```
{
  "items": [
    {
      "id": "

", "displayName": "Sample_Chassis_Name1" }, { "id": "

", "displayName": "Sample_Chassis_Name2" } ], "conversionType": "NATIVE_TO_MULTI_INSTANCE" }
```

API REST per gestione chassis

POST Aggiunta di uno chassis al centro di gestione:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis

GET all Chassis (OTTIENI tutto lo chassis):

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/

GET a specific Chassis by uid (Ottieni uno chassis specifico da uuid):

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{objectId}

Eliminare uno chassis tramite uuid:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{objectId}

JSON richiesta POST di esempio:

```
{
  "type": "FMCMangedChassis",
  "chassisName": "CHASSIS123",
  "chassisHostName": "192.168.xx.74",
  "regKey": "*****"
}
```

API REST per la gestione di Netmod (moduli di rete)

GET a Network Module by uid (OTTIENI modulo di rete da uuid):

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/networkmodules/

GET ALL Network Module:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/networkmodules/

PUT - Modifica un modulo di rete esistente tramite uuid:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/networkmodules/

PUT - Recupero dei dati del modulo di rete da FXOS e aggiornamento di Management Center:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operating/syncne

Risposta GET di esempio

```
{
  "metadata": {
    "timestamp": 1688670821060,
    "domain": {
      "name": "Global",
      "id": "e276abec-e0f2-11e3-8169-*****",
    }
  }
}
```

```

    "type": "Domain"
  }
},
"links": {
  "self": "https://u32c01p10-vrouter.cisco.com:32300/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169",
},
"id": "0050568A-3F3F-0ed3-0000-*****",
"moduleState": "ENABLED",
"type": "NetworkModule",
"description": "Cisco FPR 8X1G 8X10G 1RU Module",
"model": "FPR-3120",
"operationState": "ok",
"numOfPorts": 16,
"slotId": "1",
"vendor": "Cisco Systems, Inc.",
"name": "Network Module 1"
}

```

API REST per gestione istanze

POST Aggiunta di uno chassis al centro di gestione:

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/logicaldevices
```

GET all Chassis (OTTIENI tutto lo chassis):

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/logicaldevices
```

GET a specific Instance by uuid (Ottieni un'istanza specifica per uuid):

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/logicaldevices/{objectId}
```

PUT - Modificare un'istanza in base a uuid:

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/logicaldevices/{objectId}
```

Eliminare uno chassis tramite uuid:

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/logicaldevices/{objectId}
```

Richiesta PUT di esempio:

```

{
  "name": "ftd1",
  "operationalState": "string",
  "deviceRegistration": {
    "licenseCaps": [
      "MALWARE",
      "URLFilter",
      "CARRIER",
      "PROTECT"
    ],
    "accessPolicy": {
      "name": "AC Policy name",

```

```
"id": "
```

```
", "type": "AccessPolicy" }, "deviceGroup": { "name": "DeviceGroup name", "id": "
```

```
", "type": "DeviceGroup" } }, "managementBootstrap": { "ipv4": { "gateway": "192.168.xx.68", "ip
```

```
", "type": "ChassisInterface" }, { "name": "Ethernet2/2.1", "id": "
```

```
", "type": "ChassisInterface" } ], "type": "LogicalDevice" }
```

API REST per gestione SNMP

GET an SNMP Setting by uid (OTTIENI impostazione SNMP per uuid):

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/snmpsettings/{ID}
```

OTTIENI TUTTE LE impostazioni SNMP:

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/snmpsettings/
```

PUT - Modificare un modulo di rete esistente con uuid:

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/snmpsettings/{ID}
```

Risposta GET di esempio:

```
{  
  "snmpAdminInstance": {  
    "id": "logicalDeviceUuid",  
    "type": "LogicalDevice",  
    "name": "ftd3"  
  },  
}
```

```
"id": "snmpsettingsUUID2",  
"type": "SnmpSetting"  
}
```

API REST da recuperare riepilogo

Questo elenco contiene informazioni dettagliate sulle API REST per il recupero del riepilogo:

- Errori
- Istanze
- Inventario
- Interfacce
- Informazioni sull'app

Riepilogo degli errori GET per uno chassis:

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/faultsummary
```

Risposta di esempio:

```
{  
  "links": {  
    "self": "  

```

```
/api/fmc_config/v1/domain/domainUUID/chassis/fmcmanagedchassis/containerUUID/faultsummary?offset=
```

Riepilogo delle istanze GET per uno chassis:

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/instancessummary
```

Risposta di esempio:

```
{  
  "links": {  
    "self": "  

```


/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/instancesummary?offs

GET Inventory Summary per uno chassis:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/inventorysummary

Esempio di risposta:

```
{  
  "links": {  
    "self": "
```

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/inventorysummary?offs

GET Interface Summary per uno chassis:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/interfacesummary

Risposta di esempio:

```
{  
  "links": {  
    "self": "
```

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/interfacesummary?offs

OTTENERE informazioni sull'app per uno chassis:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}

/inventorysummary

Risposta di esempio:

```
{  
  "links": {  
    "self": "
```

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/appinfo?offset=0&lim
```

API REST per la gestione dell'interfaccia

In questa sezione vengono fornite informazioni dettagliate sulle API REST per la gestione della configurazione dell'interfaccia:

- URL da utilizzare per le modifiche alla configurazione dell'interfaccia
- URL da utilizzare per l'interruzione o il join delle interfacce
- URL da utilizzare per le configurazioni dei dispositivi di sincronizzazione

Aggiorna interfaccia fisica

Per supportare l'aggiornamento delle interfacce fisiche, sono stati introdotti questi URL.

OTTIENI tutte le interfacce fisiche:

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/interfacce  
fisiche
```

GET a specific physical interface by interface uuid (OTTIENI un'interfaccia fisica specifica per uuid interfaccia):

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/physical  
interface s/{interfaceUUID}
```

Aggiorna interfaccia in base all'uuid interfaccia:

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/physical  
interface s/{interfaceUUID}
```

Il modello di interfaccia fisica è simile al seguente:

```

{
  "metadata": {
    "supportedSpeed": "TEN_GBPS,ONE_GBPS,TWENTY_FIVE_GBPS,DETECT_SFP",
    "mediaType": "sfp",
    "sfpType": "none",
    "isBreakoutCapable": false,
    "isSplitInterface": false,
    "timestamp": 1692344434067,
    "domain": {
      "name": "Global",
      "id": "e276abec-e0f2-11e3-8169-*****",
      "type": "Domain"
    }
  },
  "type": "PhysicalInterface",
  "name": "Ethernet2/2",
  "portType": "DATA",
  "adminState": "DISABLED",
  "hardware": {
    "flowControlSend": "OFF",
    "fecMode": "AUTO",
    "autoNegState": true,
    "speed": "DETECT_SFP",
    "duplex": "FULL"
  },
  "LLDP": {
    "transmit": false,
    "receive": false
  },
  "id": "*****"
}

```

Configura sottointerfacce

Per supportare la gestione delle sottointerfacce, sono stati introdotti questi URL.

GET a sub interfaces:

`/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/sottointerfacce`

GET a specific sub interface by interface uid (Ottieni una sottointerfaccia specifica per uuid interfaccia):

`/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/subinterfaces/{int`

POST una nuova sottointerfaccia:

`/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/sottointerfacce`

AGGIORNA interfaccia per uuid interfaccia:

`/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/subinterfaces/{int`

DELETE a sub interface by interface uid (ELIMINA un'interfaccia secondaria tramite l'uuid interfaccia):

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/subinterfaces/{int

Il modello di sottointerfaccia è simile al seguente:

```
{
  "metadata": {
    "isBreakoutCapable": false,
    "isSplitInterface": false,
    "timestamp": 1692536476265,
    "domain": {
      "name": "Global",
      "id": "e276abec-e0f2-11e3-8169-*****",
      "type": "Domain"
    }
  },
  "type": "SubInterface",
  "name": "Ethernet1/3.3",
  "portType": "DATA",
  "subIntfId": 3,
  "parentInterface": {
    "type": "PhysicalInterface",
    "id": "00505686-9A51-0ed3-0000-*****",
    "name": "Ethernet1/3"
  },
  "vlanId": 3,
  "id": "*****"
}
```

Configurazione delle interfacce EtherChannel

Per supportare la gestione delle interfacce EtherChannel, questi URL sono stati introdotti.

GET a etherchannel interfaces:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/etherchannelinter

GET a specific etherchannel interface by interface uid (Ottieni un'interfaccia etherchannel specifica per uid interfaccia):

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/etherchannelinter

Pubblicare una nuova interfaccia etherchannel:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/etherchannelinter

AGGIORNA interfaccia per uid interfaccia:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/etherchannelinter

DELETE a etherchannel interface by interface uid:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/etherchannelinter

Il modello di interfaccia EtherChannel è simile al seguente:

```
{
  "metadata": {
    "supportedSpeed": "HUNDRED_MBPS,TEN_MBPS,ONE_GBPS",
    "timestamp": 1692536640172,
    "domain": {
      "name": "Global",
      "id": "e276abec-e0f2-11e3-8169-*****",
      "type": "Domain"
    }
  },
  "type": "EtherChannelInterface",
  "name": "Port-channel45",
  "portType": "DATA",
  "etherChannelId": 45,
  "selectedInterfaces": [
    {
      "type": "PhysicalInterface",
      "id": "00505686-9A51-0ed3-0000-*****",
      "name": "Ethernet1/4"
    },
    {
      "type": "PhysicalInterface",
      "id": "00505686-9A51-0ed3-0000-*****",
      "name": "Ethernet1/5"
    }
  ],
  "lacpMode": "ON",
  "lacpRate": "FAST",
  "adminState": "DISABLED",
  "hardware": {
    "flowControlSend": "OFF",
    "autoNegState": true,
    "speed": "ONE_GBPS",
    "duplex": "FULL"
  },
  "LLDP": {
    "transmit": true,
    "receive": true
  },
  "id": "00505686-9A51-0ed3-0000-*****"
}
```

Interfacce REST API Break/Join

Per supportare la separazione/join delle interfacce nella serie 4200, è possibile utilizzare i seguenti URL:

SCARICA:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/chassisinterfaces

Valuta la fattibilità di break/join per un'interfaccia

POST:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operating/breakout

Interrompe un'interfaccia

POST:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operating/jointinterface

Unisce un insieme di interfacce interrotte

Flusso REST per interruzione interfaccia

1. Individuare il dispositivo chassis gestito FMC (4200) utilizzando l'endpoint chassis fmcmanaged.

GET /api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis

Restituisce l'elenco dei dispositivi chassis gestiti da FMC insieme ai dispositivi a più istanze con i dettagli quali ID, nome e modello di ciascun dispositivo. Scegliere i dispositivi "MULTIINSTANCE".

Risposta di esempio:

```
{
  "id": "fcaa9ca4-85e5-4bb0-b049-*****",
  "type": "FMCManagedChassis",
  "chassisName": "192.168.0.75",
  "chassisMode": "MULTIINSTANCE",
  "links": {
    "self": "https://u32c01p06-vrouter.cisco.com:22512/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169"
  }
}
```

2. Verificare se l'interfaccia è breakout in grado di utilizzare l'endpoint interfacce/interfacce fisiche.

Breakout è possibile solo se "isBreakoutCapable" è true e mediaType è QSFP.

GET

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/interfacce

Risposta di esempio:

```
{
  "metadata": {
    "supportedSpeed": "FORTY_GBPS, DETECT_SFP", >>>>>>>>
    "mediaType": "qsfp", >>>>>>>>
    "sfpType": "none",
    "isBreakoutCapable": true, >>>>>>>>
    "breakoutFactor": "4", >>>>>>>>
    "isSplitInterface": false,
  }
}
```

```

    "timestamp": 1692344434067,
    "domain": {
      "name": "Global",
      "id": "e276abec-e0f2-11e3-8169-*****",
      "type": "Domain"
    }
  },
  "type": "PhysicalInterface",
  "name": "Ethernet2/4",
  "portType": "DATA",
  "adminState": "DISABLED",
  "hardware": {
    "flowControlSend": "OFF",
    "fecMode": "AUTO",
    "autoNegState": true,
    "speed": "DETECT_SFP",
    "duplex": "FULL"
  },
  "LLDP": {
    "transmit": false,
    "receive": false
  },
  "id": "00505686-9A51-0ed3-0000-*****"
}

```

3. Nell'interfaccia, valutare la fattibilità dell'operazione break utilizzando l'endpoint `evaluateoperation`.

GET

`/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/chassisinterfaces`

Se nella risposta non sono presenti avvisi/errori, l'utente può eseguire un'operazione di interruzione.

Risposta di esempio:

```

{
  "operationType": "BREAKOUT",
  "readinessState": "READY",
  "links": {
    "self": "https://u32c01p06-
vrouter.cisco.com:22542/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-
6d9ed49b625f/chassis/fmcmanagedchassis/19d967e6-ef81-4f2e-b311-
85ff6cef6d3f/chassisinterfaces/00505686-662F-0ed3-0000-
004294969274/evaluateoperation/00505686-662F-0ed3-0000-004294969274"
  },
  "type": "ChassisInterface",
  "id": "00505686-662F-0ed3-0000-004294969274"
}

```

Se nella risposta sono presenti errori, l'utente non è autorizzato a eseguire l'operazione di interruzione:

```

{
  "operationType": "BREAKOUT",
  "interfaceUsages": [
    {
      "conflictType": "Interface usage on instance(s)",
      "severity": "ERROR", >>>>>>>>
      "description": "Interface Ethernet2/4 can not be split. Remove it from instances [FTD1] and try a
    }
  ],
  "readinessState": "NOT_READY", >>>>>>>>
  "links": {
    "self": "https://u32c01p06-vrouter.cisco.com:22542/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169
  },
  "type": "ChassisInterface",
  "id": "00505686-662F-0ed3-0000-*****"
}

```

4. Se l'interfaccia è breakout e lo stato di preparazione è "READY", interrompere l'interfaccia utilizzando l'endpoint breakoutinterfaces.

POST

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operating/breakout

Richiesta:

```

{
  "targetInterfaces": [
    {
      "id": "*****ed3-0000-004294969276",
      "metadata": {
        "type": "PhysicalInterface"
      }
    }
  ],
  "type": "BreakoutInterface"
}

```

Risposta:

```

{
  "id": "4294969716",
  "type": "TaskStatus",
  "links": {
    "self": "https://u32c01p06-vrouter.cisco.com:22542/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169
  },
  "taskType": "DEVICE_DEPLOYMENT",
  "message": "Deployment status for *****: SUCCEEDED",
  "status": "Interface notification received"
}

```


5. Registrare il completamento del task utilizzando l'ID task nella risposta di interruzione. Impostare lo stato del task su "Notifica interfaccia ricevuta".

GET /api/fmc_config/v1/domain/{domainUUID}/job/taskstatuses/{objectId}

```
{
  "metadata": {
    "task": {
      "id": "4294969699",
      "links": {
        "self": "https://u32c01p06-vrouter.cisco.com:22542/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-000000000000"
      }
    }
  },
  "targetInterfaces": [
    {
      "id": "00505686-662F-0ed3-0000-*****",
      "type": "PhysicalInterface"
    }
  ],
  "type": "BreakoutInterface"
}

{
  "id": "4294969716",
  "type": "TaskStatus",
  "links": {
    "self": "https://u32c01p06-vrouter.cisco.com:22542/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-000000000000"
  },
  "taskType": "DEVICE_DEPLOYMENT",
  "message": "Deployment status for *****: SUCCEEDED",
  "status": "Interface notification received"
}
```

6. Ottenere le modifiche delle interfacce utilizzando l'endpoint chassisinterfaceevents.

GET /api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/chassisinterfaceevents

Risposta di esempio:

```
[
  {
    "change": "Interface is deleted",
    "type": "PhysicalInterface",
    "state": "DISASSOCIATED",
    "name": "Ethernet2/3"
  },
  {
    "change": "Interface is associated",
    "type": "PhysicalInterface",
    "state": "ASSOCIATED",
    "name": "Ethernet2/3/2"
  }
]
```

```
},
{
  "change": "Interface is associated",
  "type": "PhysicalInterface",
  "state": "ASSOCIATED",
  "name": "Ethernet2/3/3"
},
{
  "change": "Interface is associated",
  "type": "PhysicalInterface",
  "state": "ASSOCIATED",
  "name": "Ethernet2/3/4"
}
]
```

7. Se la notifica dell'interfaccia non viene ricevuta, sincronizzare il dispositivo utilizzando l'endpoint `chassisinterfaceevents` e verificare che siano presenti modifiche in sospeso.

POST `/api/fmc_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/chassisinterfaceevents`

Richiesta:

```
{
  "action": "SYNC_WITH_DEVICE"
}
```

Risposta:

```
{
  "action": "SYNC_WITH_DEVICE",
  "hasPendingChanges": true
}
```

8. Una volta ricevuta la notifica, accettare le modifiche utilizzando l'endpoint `chassisinterfaceevents`.

POST `/api/fmc_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/chassisinterfaceevents`

Richiesta:

```
{
  "action": "ACCEPT_CHANGES"
}
```

9. Ottenere tutte le interfacce dello chassis e trovare le interfacce divise (interrotte) utilizzando l'endpoint delle interfacce.

GET

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/interfacce

Un'interfaccia 40G, ad esempio eth2/2, è suddivisa in interfacce 4x10G - eth2/2/1, eth2/2/2, eth2/2/3 ed eth2/2/4

Flusso REST per join interfaccia

1. Verificare se l'interfaccia è interrotta utilizzando l'endpoint interfacce/interfacce fisiche.

L'operazione di join è possibile solo se "isSplitInterface" è true e mediaType è SFP

GET

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/interfacce

```
{
  "metadata": {
    "supportedSpeed": "TEN_GBPS,DETECT_SFP",
    "mediaType": "sfp",
    "sfpType": "none",
    "isBreakoutCapable": false,
    "breakoutFactor": "4",
    "isSplitInterface": true,
    "timestamp": 1692541554935,
    "domain": {
      "name": "Global",
      "id": "e276abec-e0f2-11e3-8169-*****",
      "type": "Domain"
    }
  },
  "type": "PhysicalInterface",
  "name": "Ethernet2/3/4",
  "portType": "DATA",
  "adminState": "DISABLED",
  "LLDP": {
    "transmit": false,
    "receive": false
  },
  "hardware": {
    "flowControlSend": "OFF",
    "speed": "DETECT_SFP",
    "duplex": "FULL",
    "fecMode": "AUTO",
    "autoNegState": true
  },
  "id": "00505686-662F-0ed3-0001-*****"
}
```

2. Valutare la fattibilità dell'operazione Join utilizzando l'endpoint valuateoperation su una delle

quattro interfacce divise.

GET /api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/chassisinterfaces/{interfaceUUID}/valuateoperation

- Se nella risposta non sono presenti avvisi/errori, l'utente può eseguire l'operazione di join.

```
{
  "operationType": "JOIN",
  "readinessState": "READY",
  "links": {
    "self": "https://u32c01p06-vrouter.cisco.com:22542/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169",
  },
  "type": "ChassisInterface",
  "id": "00505686-662F-0ed*****"
}
```

- Se nella risposta sono presenti errori, l'utente non è autorizzato a eseguire l'operazione di join.

```
{
  "operationType": "JOIN",
  "interfaceUsages": [
    {
      "conflictType": "Interface used in EtherChannel Configuration",
      "severity": "ERROR",
      "description": "Interface (Ethernet2/3/4) referred to in Ether Channel Interface (Port-channel132)"
    }
  ],
  "readinessState": "NOT_READY",
  "links": {
    "self": "https://u32c01p06-vrouter.cisco.com:22542/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169",
  },
  "type": "ChassisInterface",
  "id": "00505686-662F-0ed*****"
}
```

3. Se l'interfaccia è interrotta e lo stato di preparazione è "READY", unire l'interfaccia utilizzando l'endpoint delle interfacce join. Interface_uuid può essere identificata da una qualsiasi delle 4 interfacce interrotte.

POST /api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operating/join

Richiesta:

```
{
  "targetInterfaces": [
    {
```

```
    "id": "*****ed3-0001-692539698200",
    "type": "PhysicalInterface"
  }
],
"type": "JoinInterface"
}
```

Risposta:

```
{
  "metadata": {
    "task": {
      "id": "4294970217",
      "links": {
        "self": "
```

```
/api/fmc_config/v1/domain/e27*****-8169-6d9ed49b625f/job/taskstatuses/4294970217" } }
```

4. Tenere traccia del completamento del task utilizzando l'ID task nella risposta join. Impostare lo stato del task su "Notifica interfaccia ricevuta".

GET /api/fmc_config/v1/domain/{domainUUID}/job/taskstatuses/{objectId}

Risposta:

```
{
  "id": "4294970237",
  "type": "TaskStatus",
  "links": {
    "self": "https://u32c01p06-vrouter.cisco.com:22542/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169",
  },
  "taskType": "SSP_EPM_OIR",
  "message": "Deployment status for 19d967e6-xxxx-xxxx-xxxx-85ff6cef6d3f: SUCCEEDED",
  "status": "Interface notification received"
}
```

5. Ottenere le modifiche delle interfacce utilizzando l'endpoint chassisinterfaceevents.

GET

/api/fmc_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/chassisinterfaceevents

Risposta:

```
[
  {
    "change": "Interface is associated",
    "type": "PhysicalInterface",
    "state": "ASSOCIATED",
    "name": "Ethernet2/3"
  },
  {
    "change": "Interface is deleted",
    "type": "PhysicalInterface",
    "state": "DISASSOCIATED",
    "name": "Ethernet2/3/1"
  },
  {
    "change": "Interface is deleted",
    "type": "PhysicalInterface",
    "state": "DISASSOCIATED",
    "name": "Ethernet2/3/2"
  },
  {
    "change": "Interface is deleted",
    "type": "PhysicalInterface",
    "state": "DISASSOCIATED",
    "name": "Ethernet2/3/3"
  },
  {
    "change": "Interface is deleted",
    "type": "PhysicalInterface",
    "state": "DISASSOCIATED",
    "name": "Ethernet2/3/4"
  }
]
```

6. Se la notifica dell'interfaccia non viene ricevuta, sincronizzare il dispositivo utilizzando l'endpoint `chassisinterfaceevents` e verificare che siano presenti modifiche in sospeso.

POST

`/api/fmc_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/chassisinterfaceevents`

Richiesta:

```
{
  "action": "SYNC_WITH_DEVICE"
}
```

Risposta:

```
{
  "action": "SYNC_WITH_DEVICE",
  "hasPendingChanges": true
}
```

7. Una volta ricevuta la notifica, accettare le modifiche utilizzando l'endpoint `chassisinterfaceevents`.

POST

`/api/fmc_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/chassisinterfaceevents`

Richiesta:

```
{
  "action": "ACCEPT_CHANGES"
}
```

8. Ottenere tutte le interfacce dello chassis e trovare le interfacce unite e le altre interfacce che utilizzano l'endpoint delle interfacce.

GET

`/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/interfacce`

Si supponga che il join sia stato avviato su un'interfaccia 10G, ad esempio `eth2/2/1`, quindi che nella risposta sia disponibile un'interfaccia 40G `eth2/2`.

Sincronizza API REST dispositivo

Per supportare la sincronizzazione del modulo di rete e delle interfacce, sono stati introdotti questi URL.

POST:

`/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/eventichassisinterface`

Con payload

`{"azione": "SYNC_WITH_DEVICE"}` - > Attiva la sincronizzazione

`{"azione": "ACCEPT_CHANGES"}` - > Accetta le modifiche

SCARICA:

`/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/eventichassisinterface`

Elenca gli eventi modificati generati

Risoluzione dei problemi/Diagnostica

Registrazione FXOS

Se la registrazione non riesce, queste CLI di FXOS possono essere usate per controllare se sftunnel e i processi sfiproxy sono attivi.

```
firepower# connect local-mgmt
firepower-4215(local-mgmt)# show processes | include sftunnel grep: (standard input): binary file match
3323 root 20 0 80328 2024 1544 S 0.0 0.0 0:11.53 /opt/cisco/sftunnel/sfiproxy -d -f /etc/sf/sfiproxy.
22066 root 20 0 376880 7140 5944 S 0.0 0.0 0:41.18 /opt/cisco/sftunnel/sftunnel -d -f /etc/sf/sftunnel.
```

Se si utilizza la console del terminale per la CLI, verificare che l'output del comando show processes non venga troncato impostando la larghezza del terminale su un valore appropriato usando questa CLI mostrata:

```
firepower-4215(local-mgmt)# terminal width 100
```

Se il processo SFTunnel è attivo e in esecuzione, ma la registrazione non riesce, questi comandi possono essere utilizzati per individuare qualsiasi possibile causa di errore.

Introdotta una nuova CLI in FXOS da connect local-mgmt per visualizzare i messaggi syslog in /opt/cisco/platform/logs/sfmessages

```
firepower# connect local-mgmt
firepower(local-mgmt)# tail-mgmt-log sfmessages
```

```
Dec 9 18:31:17 firepower Ipc [30483]: add ep: 1,0x5613aa0e2fe8 total = 1 Dec 9 18:31:17 firepower
```

Registrazione FMC

- Se la registrazione del dispositivo non riesce, individuare usmsharedsvcs.log e vmssharedsvcs.log in questa posizione e cercare la stringa "CHASSIS DISCOVERY" o "NATIVE_TO_MULTI_INSTANCE" per individuare la potenziale causa dell'errore.
 - Inoltre, cercare i problemi relativi al tunnel SFT in /var/log/action_queue.log e /var/sf/messages.
 - /var/opt/CSCOpX/MDC/log/operation/usmsharedsvcs.log
/var/opt/CSCOpX/MDC/log/operation/vmssharedsvcs.log
- Se la registrazione automatica dello chassis non riesce, individuare i file usmsharedsvcs.log e vmssharedsvcs.log e cercare le stringhe "CHASSIS DISCOVERY" e "NATIVE_TO_MULTI_INSTANCE" per individuare la potenziale causa del problema.
- Se la registrazione automatica dell'istanza non riesce, individuare usmsharedsvcs.log e vmssharedsvcs.log e cercare la stringa "MI_FTD_INSTANCE_AUTO_REGISTRATION" per individuare la potenziale causa dell'errore.
- In caso di errore di distribuzione nel dispositivo, passare a Distribuisci -> Cronologia distribuzione -> Fare clic sulla distribuzione non riuscita -> Apri trascrizione. Il file contiene il motivo dell'errore.

Risoluzione dei problemi dello chassis

FMC supporta la generazione di FPRM (Chassis Probleshoot) dalla pagina di gestione dei dispositivi.

- Come per il dispositivo FTD, è disponibile un'opzione di risoluzione dei problemi per il dispositivo chassis che genera la risoluzione dei problemi dello chassis e consente all'utente di scaricare il pacchetto di risoluzione dei problemi da FMC.
- Questo raccoglie il bundle "show tech-support form" dallo chassis:

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (2)							
4215_WA_chassis 192.168.1.80	Firewall 4215 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	N/A	N/A	N/A	Delete Health Monitor Troubleshoot Files
WA_instance_1 192.168.1.81 - Routed	Firewall 4215 Threat Defense	7.6.0	N/A	Essentials, Malware (1 more...)	Pol	↶	

Opzioni di risoluzione dei problemi dello chassis e generazione:

- Click On Generate to start generating troubleshoot.

Generate Troubleshoot Files - 4215_WA_chassis

This operation generates troubleshoot logs for Secure Firewall 3100 chassis

This operation may take several minutes to complete, the status can be tracked in Message Center Tasks.

Please select the data to include:

All Data

FXOS Logs

Cancel Generate

Stato risoluzione problemi chassis e download:

- Task Manager messages show the progress of troubleshoot generation.
- Once completed, the user can download the troubleshoot bundle.

Deployments Upgrades Health Tasks Show Pop-up Notifications

12 total 0 waiting 2 running 0 retrying 10 success 0 failures Filter

Chassis

Generate Troubleshooting Files
Generate troubleshooting files for 4215_WA_chassis
Remote status: Generating troubleshoot files 11s

Deployments Upgrades Health Tasks Show Pop-up Notifications

12 total 0 waiting 1 running 0 retrying 11 success 0 failures Filter

Chassis

Generate Troubleshooting Files
Generate troubleshooting files for 4215_WA_chassis
Click to retrieve generated files. 7m 57s X

Procedure dettagliate per la risoluzione dei problemi di esempio

Registrazione automatica del guasto dello chassis in FMC

Problema: Errore durante la registrazione automatica dello chassis nel FMC.

Risultato previsto:

- Una volta avviata la conversione dal CCP, è prevista l'annullamento della registrazione e la registrazione automatica nel CCP.

Risultato effettivo:

- Registrazione automatica chassis non riuscita

Risoluzione del problema

1. Verificare la conversione:

- Verificare che la conversione sia stata attivata in FMC.
- Accedere al dispositivo e verificare se è stato convertito in modalità contenitore.
- Eseguire i comandi per verificare se la periferica è stata convertita:

```
firepower# scope sys
firepower /system # show
Systems:
Name Mode Deploy Mode System IP Address System IPv6 Address
-----
firepower Stand Alone Container 192.168.xx.xx ::
```

2. Controllare Gestione periferiche:

- Verificare che Gestione periferiche sia stato impostato correttamente:

```
firepower# show device-manager
Device manager:
  Name: manager
  Hostname: 10.10.xx.xx
  NAT id: 3ab4bb1a-d723-11ee-a694-89055xxxxxxx
  Registration Status: Completed
  Error Msg:
```

3. Registri da controllare:

3.1. Accedere a `/var/opt/CSCOpX/MDC/log/operation/vmssharedsvcs.log` e `/var/opt/CSCOpX/MDC/log/operation/usmsharedsvcs.log`

3.2. Cercare le parole chiave "NATIVE_TO_MI_CONVERSION" e "CHASSIS DISCOVERY" nei file per individuare la causa dell'errore.

Registrazione automatica dell'istanza in FMC

Problema: Errore durante la registrazione automatica dell'istanza in FMC.

Risultato previsto:

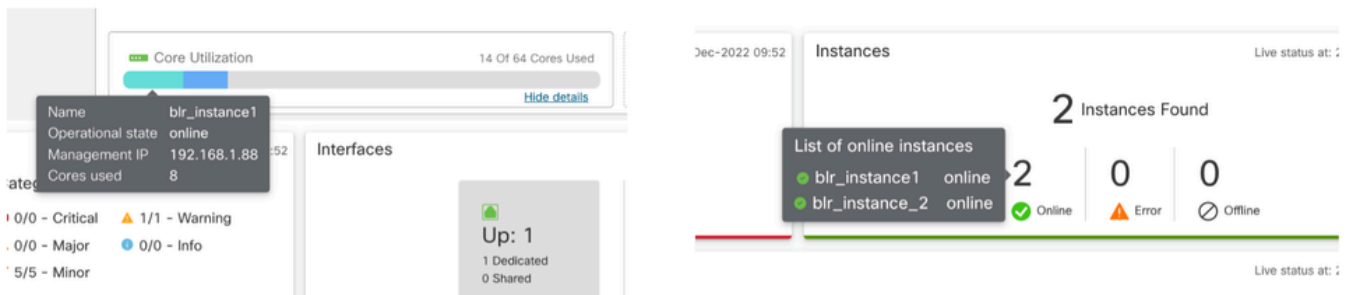
- Dopo il provisioning dell'istanza da FMC, è prevista la registrazione automatica in FMC

Risultato effettivo:

- Registrazione automatica istanza non riuscita

Risoluzione del problema

- Verificare che la distribuzione sia stata attivata dopo la creazione dell'istanza.
 - Se la distribuzione non viene eseguita, assicurarsi di distribuire le modifiche nel dispositivo.
 - In caso di errore nella distribuzione, passare a Cronologia distribuzione -> Fare clic su Trascrizione. Verificare la causa dell'errore, correggere e riprovare la distribuzione.
- Verificare che l'istanza sia installata e che il relativo stato operativo sia in linea. È possibile utilizzare la pagina di riepilogo dello chassis per controllare lo stato del provisioning dell'istanza.



- Verificare che SFTunnel sia attivo e in esecuzione sull'FTD dell'istanza utilizzando questo comando:

```
ps -ef | grep -i "sftunnel"
```

- Se SFTunnel non è in esecuzione, provare a eseguire un comando di riavvio:

```
pmtool restartById sftunnel
```

- Accedere a `/var/opt/CSCOpX/MDC/log/operation/vmssharedsvcs.log` e `/var/opt/CSCOpX/MDC/log/operation/usmssharedsvcs.log`
- Cercare la parola chiave "MI_FTD_INSTANCE_AUTO_REGISTRATION" nel file per individuare la causa dell'errore.

Registrazione del dispositivo nativo in FMC

Problema: Errore di Native Device Registration in FMC dopo la riconversione della periferica in modalità nativa

- Se l'utente riconverte lo chassis (modalità MI) in modalità nativa ma dimentica di eliminarlo dal FMC, il dispositivo non sarà in linea nel FMC.
- Se l'utente tenta di registrare nuovamente la periferica nativa nel FMC, la registrazione non riesce.

Risoluzione del problema

- Verificare che la voce relativa allo chassis sia stata eliminata dal FMC prima di riconvertire il dispositivo in modalità nativa.
- Una volta eliminata la voce, provare a registrare nuovamente la periferica nativa in FMC.

Riferimenti utili

- Informazioni sulle interfacce condivise:

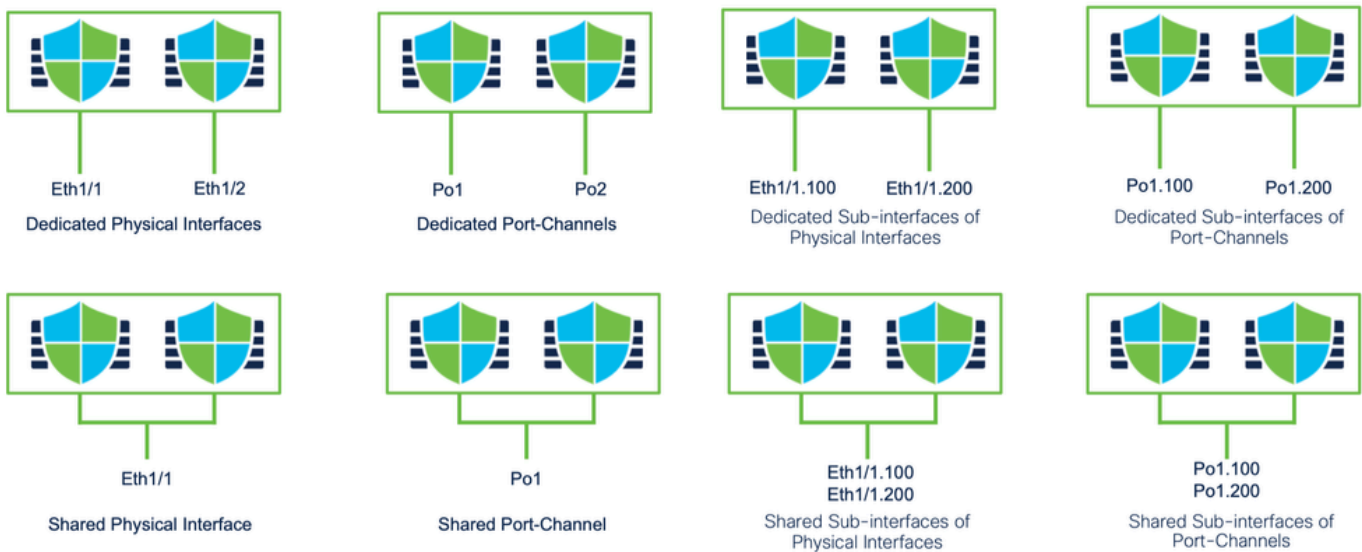
<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/threat-defense/use-case/multi-instance-sec-fw/multi-instance-sec-fw.html#shared-interface-scalability-WGUIEF>

- Pagina 3100 Multi-Instance sul sito del supporto Cisco:

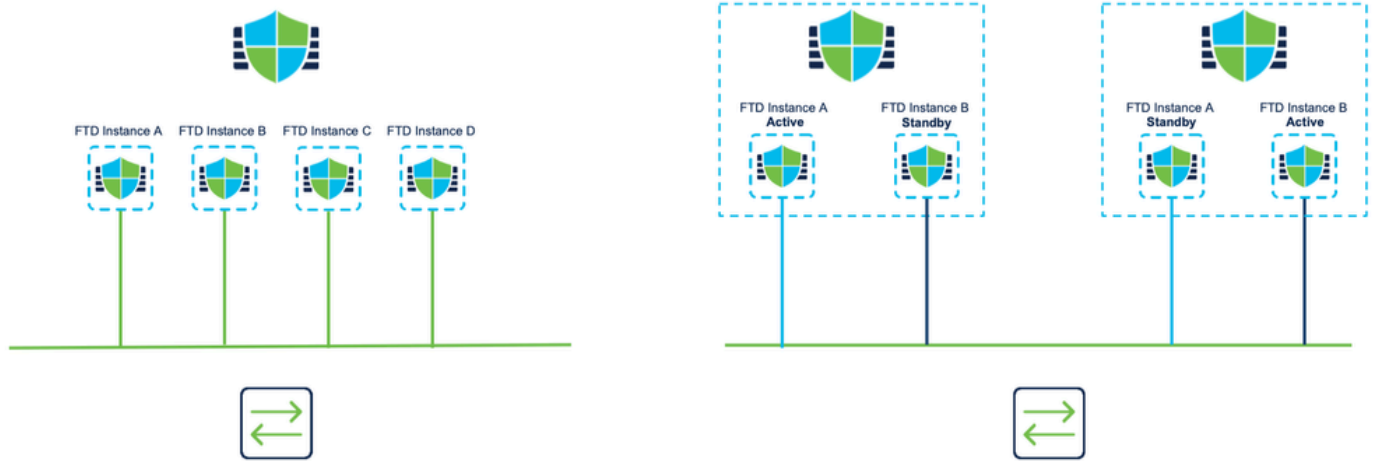
<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/threat-defense/use-case/multi-instance-sec-fw/multi-instance-sec-fw.html>

Opzioni di interfaccia e alta disponibilità

Opzioni interfaccia



Standalone o Alta disponibilità



Utilizzo delle due interfacce di gestione

- Come il modello 4200 in modalità nativa, le due porte di gestione fisiche sono fornite per supportare la ridondanza dell'interfaccia per il traffico di gestione o per supportare interfacce separate per la gestione e gli eventi.
 - I dispositivi 9300 e 4100, nonché la serie 4200, dispongono di due interfacce di gestione. La seconda interfaccia di gestione, Management 1/2, è destinata all'utilizzo per gli eventi.
- In modalità a più istanze (aka "contenitore"), è possibile configurare questa interfaccia dalla CLI di Threat Defense in ciascuna istanza. Assegnare un indirizzo IP nella stessa rete per ogni istanza.
- In modalità contenitore, a ogni istanza FTD vengono assegnate automaticamente entrambe le interfacce di gestione 1/1 e 1/2.
 - La seconda interfaccia di gestione è disabilitata per impostazione predefinita.
 - Non è possibile configurare Management1/2 utilizzando FMC; è necessario configurarlo tramite FTD CLISH (sui modelli 9300/4100, che, al contrario, viene eseguita nella CLI di FXOS). Utilizzare questo comando con il tipo di indirizzo IP, l'indirizzo, la subnet e la route statica desiderati:

```
configure network ipv4 manual 192.168.0.xx 255.255.255.0 192.168.0.1 management1
```

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).