

Converter em contêiner (modo MI) no Firepower 4200 com FTD 7.6

Contents

[Introdução](#)

[Pré-requisitos, plataformas suportadas, licenciamento](#)

[Plataformas mínimas de software e hardware](#)

[Licenciamento](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[O que há de novo?](#)

[Plataformas com suporte a várias instâncias de FTD](#)

[Diferenças entre as séries 3100 e 4200](#)

[Implantações suportadas](#)

[Descrição do recurso e passo a passo](#)

[Especificações da instância do 4200 Series](#)

[Máx. de suporte a instâncias](#)

[Tamanhos de Instância de FTD](#)

[Alocações de Núcleo Snort de Lina \(Plano de Dados\)](#)

[Configurar](#)

[Visão geral da configuração](#)

[Converta o 4200 Series para o modo de várias instâncias no FMC](#)

[Converter um único dispositivo](#)

[Converter mais de um dispositivo \(conversão em massa\)](#)

[Monitorando o Andamento e Finalizando](#)

[Página de visão geral do chassi do FMC](#)

[Visão geral da página de visão geral do chassi do FMC](#)

[Seções da guia Resumo da página Chassis](#)

[Gerenciar interfaces](#)

[Resumo da guia Interfaces](#)

[Modificar configurações de interface física](#)

[Gerenciar Subinterface](#)

[Gerenciar EtherChannel](#)

[Configurações do Dispositivo de Sincronização](#)

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

[4200 nativo suporta EPM Hot Swap e Breakout](#)

[OIR: Habilitar/Desabilitar Confirmação do EPM](#)

[Ativação Completa do EPM: Notificação de interface recebida](#)

[Notificação de Alteração da Interface do EPM](#)

[Página Opções de quebra/junção no chassi](#)

[Alterações de interface após quebra/junção](#)

[Impacto de alterações de interface na instância](#)

[Gerenciamento de instâncias](#)

[Criar uma instância](#)

[Editar uma instância](#)

[Excluir instância](#)

[Configuração de SNMP](#)

[Importação/exportação de chassi](#)

[Exportar configuração](#)

[Importar configuração](#)

[O que você precisa saber sobre importação/exportação de chassis](#)

[Política de configurações da plataforma do chassi](#)

[Configurações da plataforma do chassi: DNS](#)

[Configurações da plataforma do chassi: SSH](#)

[Configurações da plataforma do chassi: Lista de acesso SSH](#)

[Configurações da plataforma do chassi: Sincronização de horário](#)

[Do NTP do Management Center](#)

[No servidor NTP personalizado](#)

[Configurações da plataforma do chassi: Fusos Horários](#)

[Configurações da plataforma do chassi: Syslog](#)

[Configurações da plataforma do chassi: Salvar e implantar](#)

[Cancelando o registro do chassi](#)

[Converter de Várias Instâncias para o Modo Nativo](#)

[APIs FMC Rest](#)

[APIs REST para conversão de nativo em várias instâncias](#)

[APIs REST para gerenciamento de chassi](#)

[APIs REST para gerenciamento de Netmods \(módulos de rede\)](#)

[APIs REST para gerenciamento de instâncias](#)

[APIs REST para gerenciamento SNMP](#)

[Resumo de APIs REST para busca](#)

[APIs REST para gerenciamento de interface](#)

[Atualizar interface física](#)

[Configurar subinterfaces](#)

[Configurar Interfaces EtherChannel](#)

[Interfaces de interrupção/junção de APIs REST](#)

[Fluxo REST para quebra de interface](#)

[Fluxo REST para junção de interface](#)

[Sincronizar APIs REST de Dispositivo](#)

[Solução de problemas/diagnósticos](#)

[Log FXOS](#)

[Registro do CVP](#)

[Solução de problemas do chassi](#)

[Exemplos de Problemas com Troubleshooting de Passo a Passo](#)

[Registro automático de falha de chassi no FMC](#)

[Solução de problemas](#)

[Autorregistro de instância no CVP](#)

[Solução de problemas](#)

[Registro de dispositivo nativo no FMC](#)

[Solução de problemas](#)

[Referências úteis](#)

[Opções de interface e alta disponibilidade](#)

[Opções de interface](#)

[Independente ou alta disponibilidade](#)

[Aproveitando as interfaces de gerenciamento duplas](#)

Introdução

Este documento descreve como configurar um contêiner (modo de várias instâncias) no Firepower 4200 série de firewall com FTD 7.6 e detalhes relacionados.

Pré-requisitos, plataformas suportadas, licenciamento

Plataformas mínimas de software e hardware

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



Note: Não há suporte para várias instâncias com o FDM em nenhuma plataforma.

Licenciamento

- As licenças de recursos são atribuídas manualmente a cada instância, mas você consome apenas uma licença por recurso por dispositivo 4200-series.
 - Por exemplo, para uma série 4200 com 3 instâncias de FTD, você só precisa de uma licença de URL, independentemente do número de instâncias em uso, desde que esteja no mesmo FMC.
- Todas as licenças são consumidas por dispositivo 4200 Series e não por instância de contêiner, desde que estejam no mesmo FMC. Portanto, para todas as instâncias em dispositivos 4200 Series, é recomendável usar o mesmo FMC devido à implementação da licença.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

- O FTD já suporta a Multi-Instância (MI) em modelos 3100 (assim como as séries 9300 e 4100), mas não há suporte para a série 4200.
- Os modelos 4200 são suportados apenas no modo nativo no FMC.
- Não há provisão para criar várias instâncias no 7.4.x no 4200.
- Várias Instâncias (MI) no 3100 eram suportadas a partir da versão 7.4.1.
 - As instâncias podem ser criadas e gerenciadas usando o FMC (ao contrário das séries 9300 e 4100, em que o FCM deve ser usado).
 - O FXOS pode ser atualizado, quando no modo MI, através da GUI do chassi de atualização do FMC.
 - A conversão para o modo MI é feita por meio de uma CLI.

O que há de novo?

- Você pode provisionar e gerenciar instâncias de MI na série 4200.
- FMC - Solução única de gerenciamento para a série 4200 (modo MI) e instâncias de FTD
- Permitir a conversão em massa e única de dispositivos nativos para o modo MI no FMC para dispositivos das séries 3100 e 4200.
- Mercado-alvo: Empresa/Grande empresa - Borda da Internet, Data Center

Plataformas com suporte a várias instâncias de FTD

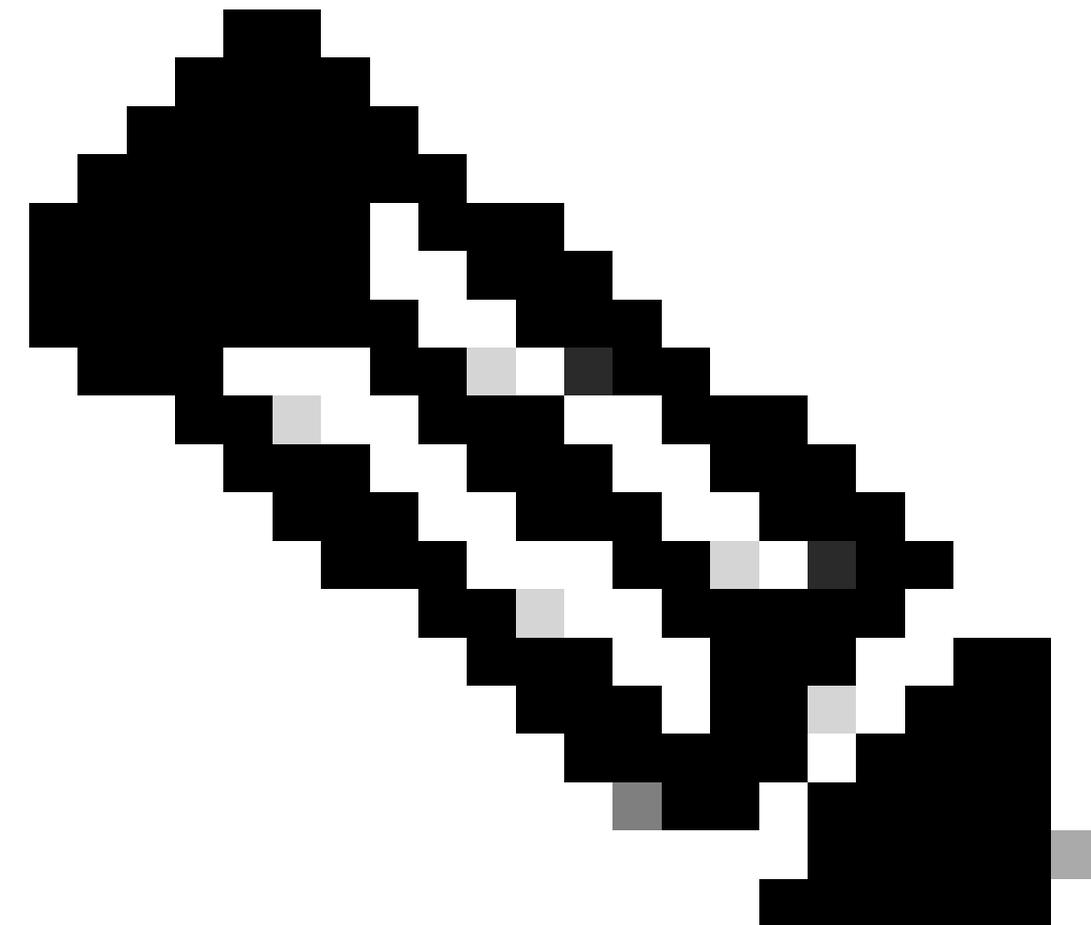
Platform	FTD Version	FTD Multi-Instance Support	Management Solution
Virtual	-	No	-
FPR1000	-	No	-
FPR2100	(not supported in 7.6)	No	-
3105		No	
3110, 3120, 3130, 3140	FTD 7.4.1	Yes	FMC
FPR4100	FTD 6.3.0	Yes	FCM & FMC
4215, 4225, 4245	FTD 7.6.0	Yes	FMC
FPR9300	FTD 6.3.0	Yes	FCM & FMC

Diferenças entre as séries 3100 e 4200

- O 4200 tem duas interfaces de gerenciamento, permitindo o uso de uma para gerenciamento e outra para eventos.
 - As interfaces Management1/1 e Management1/2 são inicializadas para todas as instâncias de contêiner de FTD.
 - Uma ou ambas as interfaces de gerenciamento podem ser usadas no modo MI.
 - Gerenciamento1/1 para Gerenciamento e Eventos ou
 - Gerenciamento1/1 pode ser usado para gerenciamento e Gerenciamento1/2 para eventos, em que o caso:
 - As rotas estáticas precisam ser definidas para rotear o tráfego usando a interface 1/2 de gerenciamento.
- Devido ao tamanho maior, mais instâncias podem ser criadas no 4200 do que no 3100.

Implantações suportadas

- Gerencie a Série 4200 (modo MI) com Instância(s) Autônoma(s) de FTD
 - Gerenciar 4200 Series (modo MI) com Instância(s) HA FTD*
-



Note: Para o FPR4100 Series, no caso do FTD-HA, os nós primário e secundário devem

estar em dois dispositivos 4200 Series (modo MI) diferentes. Além disso, o agrupamento MI não é suportado nesta versão.

Descrição do recurso e passo a passo

Alterações na configuração de várias instâncias na versão 7.6.0:

- Suporte para 4200 Series no modo MI
- Alterações do CVP relativas à gestão em modo IA da série 3100:
 - Conversão do dispositivo do modo Nativo para o modo MI no FMC
 - Readiness Verifica se o dispositivo pode ser convertido para o modo MI
 - Autorregistrar instância de FTD no FMC após a conversão

Especificações da instância do 4200 Series

Máx. de suporte a instâncias

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

A densidade da instância é determinada por dois fatores principais:

1. A quantidade de núcleos de CPU e a quantidade de espaço em disco em uma determinada plataforma
2. Quantos desses recursos estão disponíveis para provisionamento em instâncias. O menor tamanho de instância requer 3 núcleos de CPU física (6 lógicos) e 48 GB de espaço em disco.

Tamanhos de Instância de 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

Alocações de Núcleo Snort de Lina (Plano de Dados)

	4215	4225	4245			
Tamanho da Instância	Núcleos do plano de dados	Núcleos de Snort	Núcleos do plano de dados	Núcleos de Snort	Núcleos do plano de dados	Núcleos de 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

Configurar

Visão geral da configuração

1. Registre o dispositivo 4200 Series (modo nativo) no FMC.
2. Novo! No FMC, selecione e converta o dispositivo do modo Nativo para o modo MI.
3. Novo! O IA registra-se automaticamente no FMC após a conversão.
4. Atualizar interface(s) física(is).
5. Crie instâncias de FTD e atribua interfaces.
6. Criar/Atualizar/Excluir canal de porta e subinterfaces do FMC.
7. Defina as configurações da plataforma.
8. Implantar alterações de configuração no dispositivo.
9. Instância(s) do FTD registra(m) automaticamente no FMC.

Converta o 4200 Series para o modo de várias instâncias no FMC

Por padrão, os 4200s estão no modo nativo. Para converter a série 4200 em modo de várias instâncias no FMC:

1. Conecte-se ao dispositivo e crie um gerenciador (já documentado).
2. Registrar o dispositivo nativo no CVP (já documentado).
3. Converter em Várias Instâncias usando FMC.
4. No FMC, selecione o(s) dispositivo(s) que precisa(m) ser convertido(s) em Várias instâncias e acione a conversão. É possível selecionar um ou mais de um dispositivo.



Note: Alternar entre o modo nativo para o modo MI redefine TODA a configuração no chassi. A conversão do modo MI para o modo nativo ainda é feita via CLI.

Converter um único dispositivo

1. Para iniciar a conversão, navegue até `Devices > Device management`.

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	

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.

- Delete
- Packet Tracer
- Packet Capture
- Revert Upgrade
- Health Monitor
- Convert to Multi-instance**
- Troubleshoot Files

2. Valide o dispositivo selecionado e clique em Continuar:

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.

validar dispositivos selecionados

3. Verificação de preparação e conversão inicial:

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.

verificação de prontidão

Converter mais de um dispositivo (conversão em massa)

1. Selecionar dispositivos:

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. Confirmar seleção:

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	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. Verificação de preparação e início da conversão:

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	Ready
Native_Chassis_2	192.168.1.106	7.6.0	Cisco Secure Firewall 3130 Threat Defense	Ready

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.

Monitorando o Andamento e Finalizando

1. Notificação de início de conversão:

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

2. Autorregistro do 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. Notificação pós-conversão:

Successful Conversion Notification with number of devices converted successfully.

Página de gerenciamento de dispositivos resultante listando os dispositivos da série 4200 (modo MI):



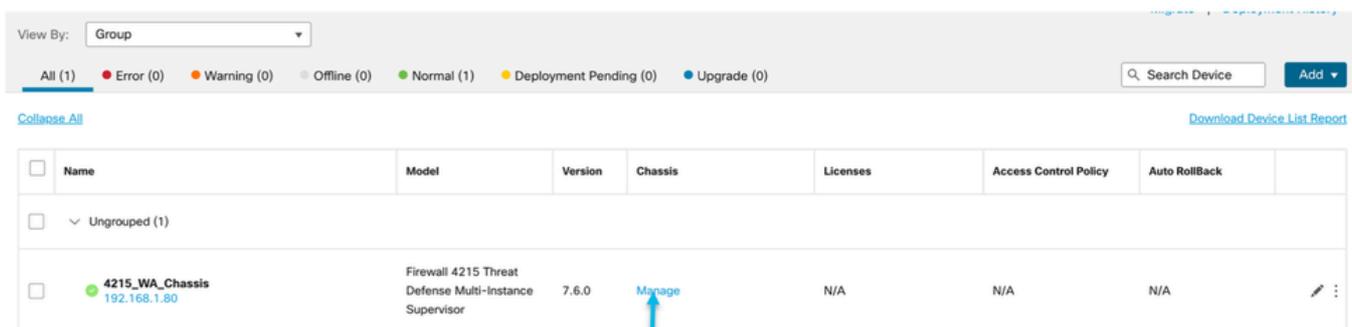
Página de visão geral do chassi do FMC

Visão geral da página de visão geral do chassi do FMC

A página de visão geral do chassi do FMC apresenta um resumo completo do dispositivo 4200 Series (modo MI). Ele inclui:

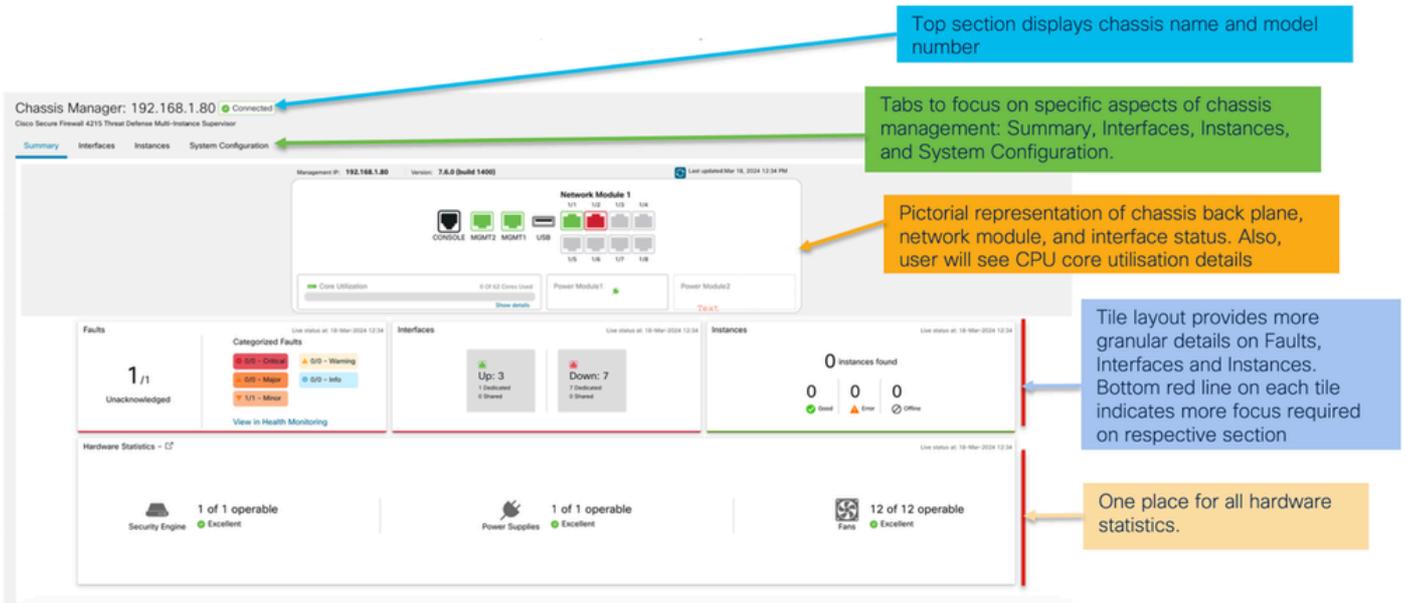
- Visão pictórica do painel traseiro do dispositivo, incluindo módulos de rede disponíveis.
- Resumo de falhas, com sua criticidade.
- Resumo da interface, status.
- Resumo da instância de FTD, status.
- Estatísticas de hardware - incluindo VENTILADOR, fonte de alimentação, memória, uso da CPU e armazenamento.

Clique em Gerenciar para navegar até Visão geral do chassi:



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

Guia de resumo da página do chassi:

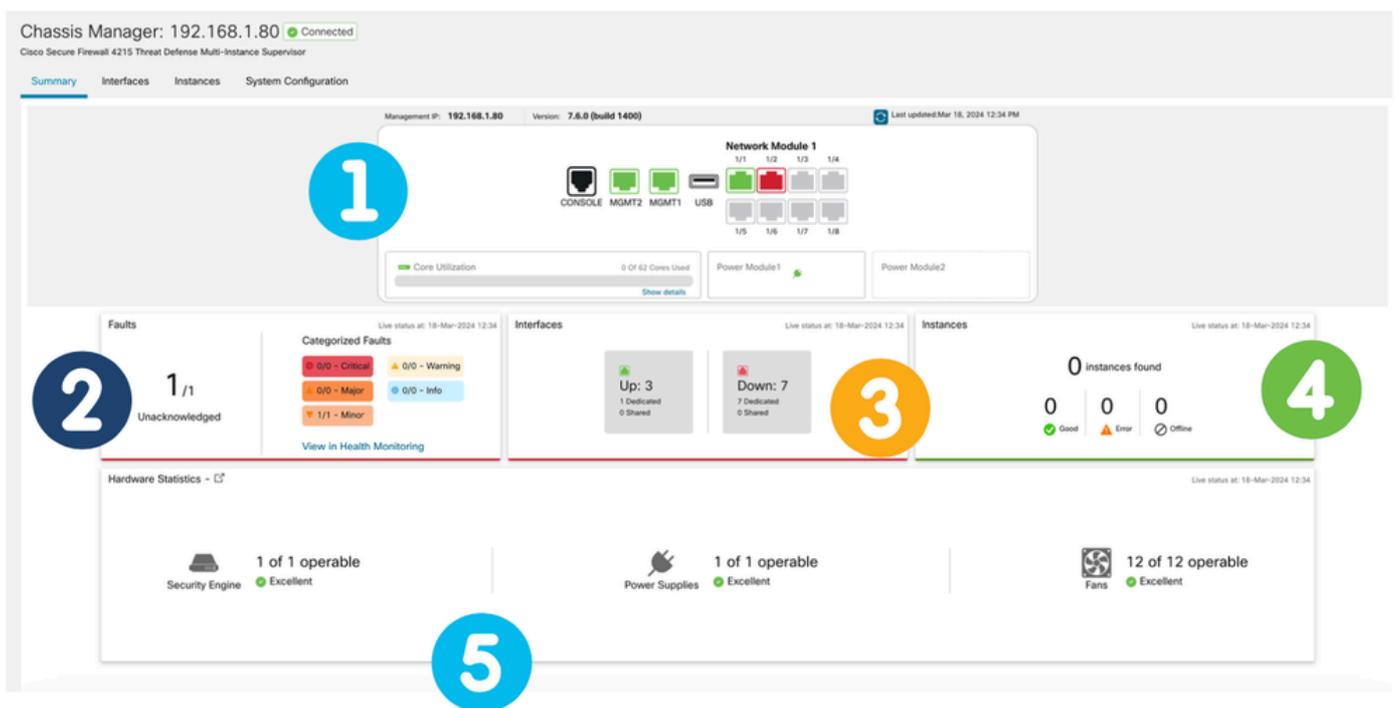


Seções da guia Resumo da página Chassis

A guia Resumo contém seções. Clique para obter mais detalhes:

- Painel traseiro
- Falhas
- Interfaces
- Instâncias
- Estatísticas de hardware

As seções são mapeadas por número conforme mostrado nesta imagem:



1. Vista de retaguarda:



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. Seção das falhas:



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

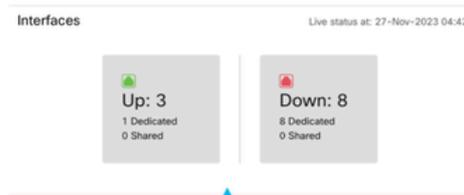
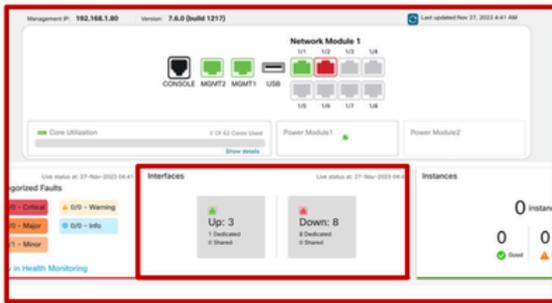
Click on 'View in Health Monitoring' to open a dialog that lists all faults in a table.

3. Seção Interfaces:

Health: 4215_WA_chassis (Critical) Normal

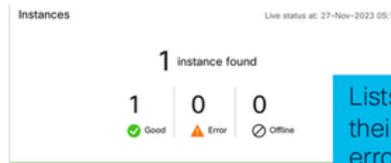
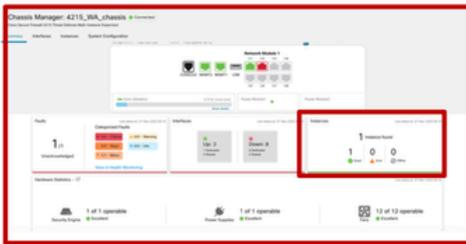
View System & Troubleshoot Details

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



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

4 .Seção Instâncias:



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



A transição de instâncias de off-line para on-line é mostrada na imagem anterior.

- Depois de provisionado (1)
- A instância fica offline até ficar online (2)
- Os estados intermédios também são refletidos (3)

5. Estatísticas de 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.

Gerenciar interfaces

Operações suportadas na guia Interfaces:

- Atualização da interface física.
- Criar/Atualizar/Excluir subinterfaces.
- Criar/Atualizar/Excluir interfaces EtherChannel.
- Configurações da interface de sincronização.
- OIR do módulo de rede.
- Interrupção/junção da interface física.

Resumo da guia Interfaces

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

A página inicial da guia Interfaces mostra todos os tipos de interfaces que são gerenciadas para um chassi, como interfaces físicas, subinterfaces e subinterfaces EtherChannel e EtherChannel.

Modificar configurações de interface física

Estes atributos de uma interface física podem ser atualizados:

- Estado (Habilitado/Desabilitado)
- Tipo de porta (dados | Partilha de dados)
- Admin Duplex
- Velocidade do administrador
- Negociação automática

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

Gerenciar Subinterface

Selecione a opção de sub-interface no botão Add para adicionar uma nova interface.

Estes atributos de uma subinterface podem ser modificados:

- Interface pai
- Tipo de porta (dados / compartilhamento de dados)

- ID da subinterface
- ID da VLAN

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)

Cancel

OK

Gerenciar EtherChannel

Para criar uma nova interface EtherChannel, use a "interface EtherChannel" no botão Add.

Os atributos que podem ser configurados para um EtherChannel são:

- ID do EtherChannel

- Tipo de porta (dados/ compartilhamento de dados)
- Interfaces de membro
- Velocidade do administrador
- Admin Duplex
- Modo LACP
- Taxa de LACP
- Negociação automática

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

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

Add

Selected Interfaces (0)

Cancel OK

Add EtherChannel Interface

Interfaces Configuration

Admin Duplex
 Full

Admin Speed
 1Gbps

LACP Mode
 Active

LACP Rate
 Default

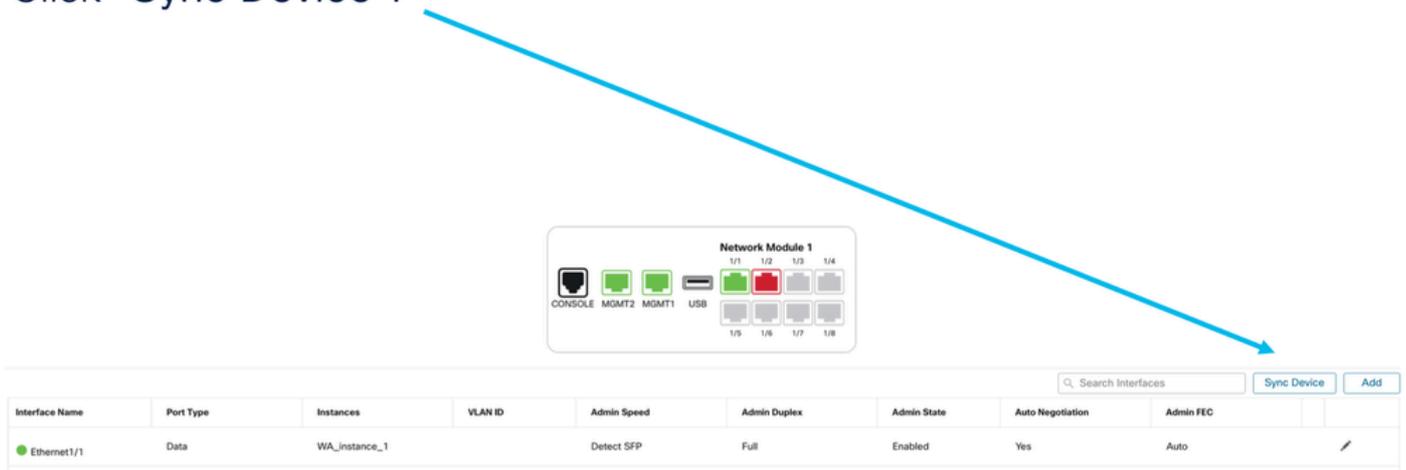
Auto Negotiation

Cancel OK

Configurações do Dispositivo de Sincronização

Há casos em que a configuração do FMC e a configuração do dispositivo podem sair de sincronia. Um caso é quando um usuário remove ou insere um netmod. O dispositivo de sincronização pode ser feito nesses casos.

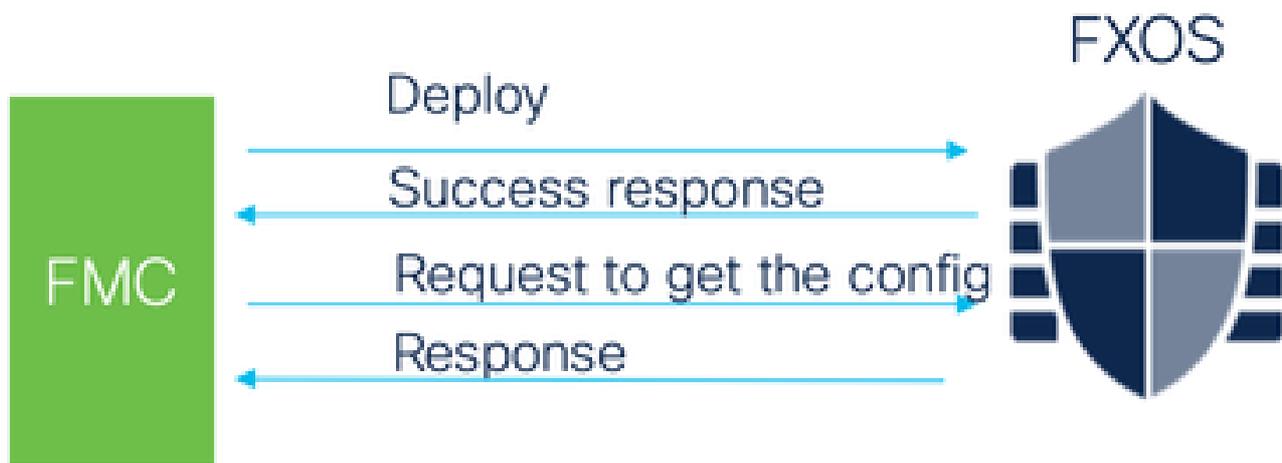
Click "Sync Device".



Suporte A Hot Swap/Break-Out Netmod

A opção "Hot Swap", usada em seus documentos, é conhecida como Inserção e Remoção On-line ou OIR em outra documentação interna.

Há uma implantação imediata ao Habilitar/Desabilitar o Módulo de Rede ou Interromper ou Unir interfaces. O modo de várias instâncias é igual ao 4200 Series no modo nativo.



O FMC compara a resposta recebida com a configuração atual e, em seguida, cria a notificação de alteração de interface para confirmação do usuário.

4200 nativo suporta EPM Hot Swap e Breakout

O EPM OIR e o Breakout já são suportados no modo autônomo e nativo do Secure Firewall 4200 Series autônomo.

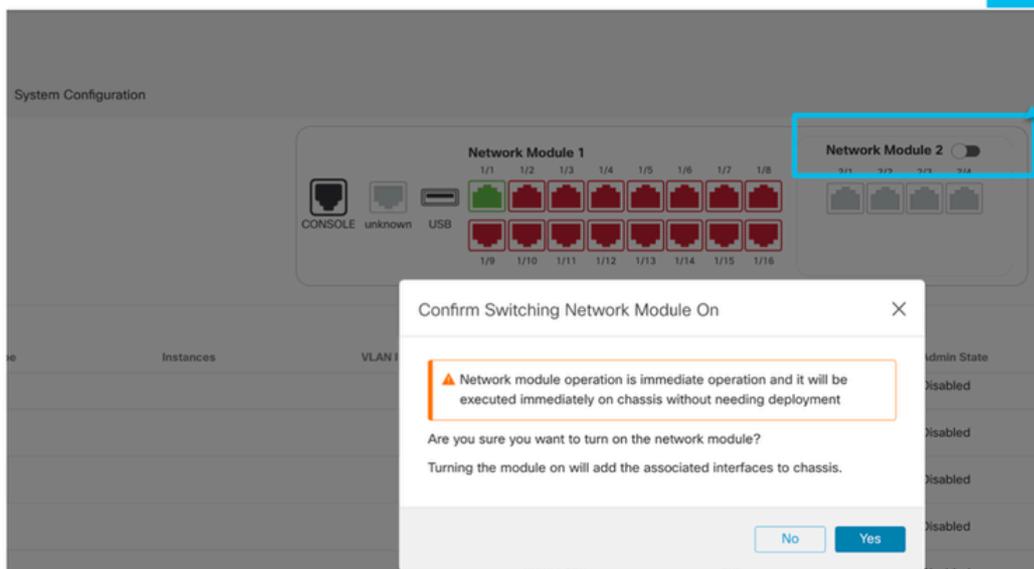
Documentação do 4200 Series EPM OIR e Breakout FMC:

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

OIR: Habilitar/Desabilitar Confirmação do EPM

Quando o usuário alterna para habilitar o módulo, um aviso é exibido para garantir que este não seja um clique acidental.

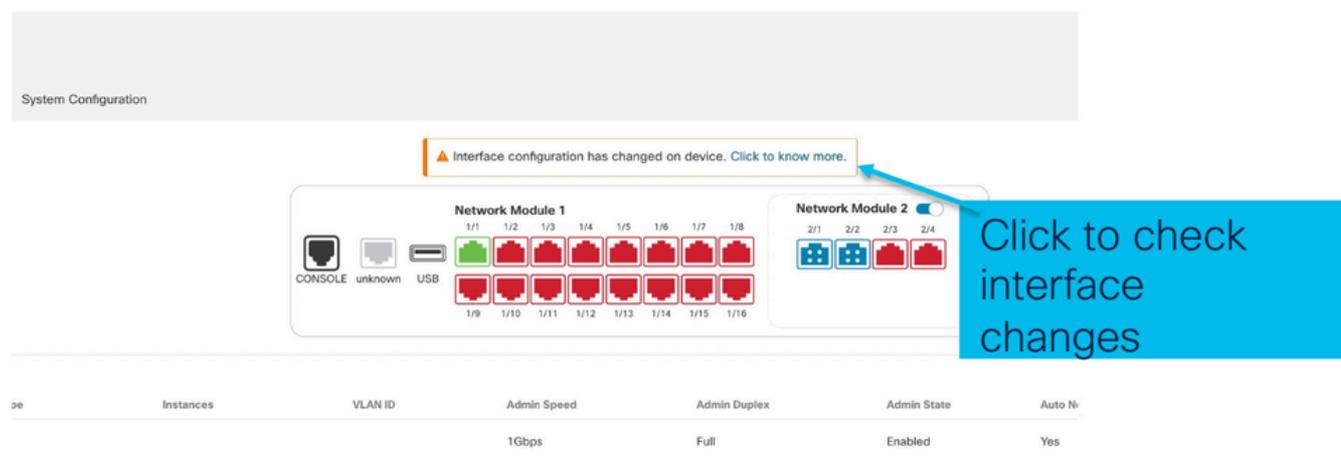
Toggle option to enable/disable module



Ativação Completa do EPM: Notificação de interface recebida

- Ao habilitar um EPM, novas interfaces são associadas ao dispositivo.
- O CVP recebe a notificação sobre as interfaces associadas.
- No FMC, o usuário deve aceitar as alterações.

Esta captura de tela mostra a opção de ver as interfaces associadas:



Notificação de Alteração da Interface do EPM

A página de listagem de interfaces lista as interfaces que são adicionadas quando o EPM está habilitado. Clique para saber mais inicia a caixa de diálogo Alterações de interface.

Clique para saber mais não está disponível após salvar.

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

Página Opções de quebra/junção no chassi

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	✎

O assistente de confirmação de interrupção da interface é aberto quando a opção de interrupção é acionada.

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

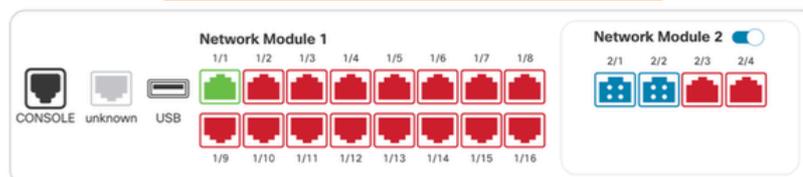


A notificação de atualização da interface fica visível na página do chassi após a confirmação da interrupção da interface.

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

System Configuration

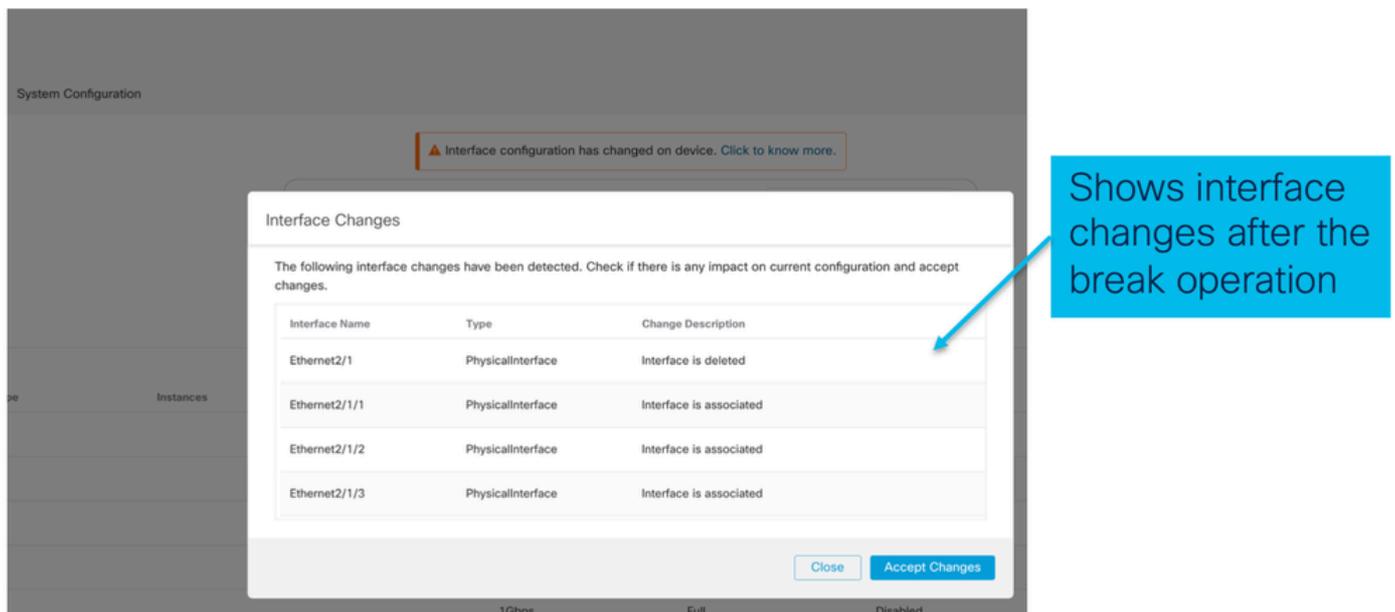
⚠ Interface configuration has changed on device. Click to know more.



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

Alterações de interface após quebra/junção

Ao clicar em Aceitar alterações, essas interfaces ficam disponíveis no FMC para serem usadas:



Impacto de alterações de interface na instância

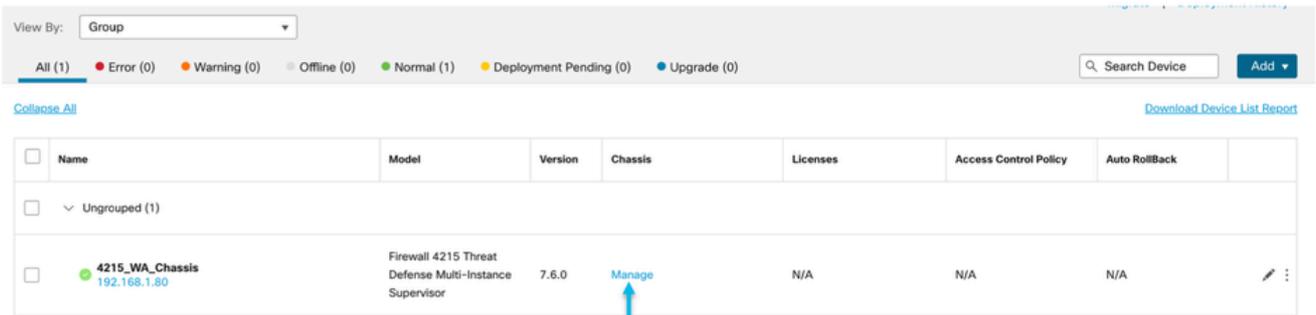
Change	Behavior
Change a dedicated interface to shared	No validation error
Change a shared interface used in multiple instance to dedicated	Validation error will block the change
Disable of Network module with interfaces assigned to Instance	No validation error during the disable operation, but error 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

Gerenciamento de instâncias

O Gerenciamento de Instâncias permite:

- Exibir todas as instâncias de FTD existentes e seus detalhes em um dispositivo 4200 Series (modo MI).
- Crie/Atualize instâncias de FTD com o núcleo da CPU e a versão do software desejados.
- Excluir uma instância de FTD existente.

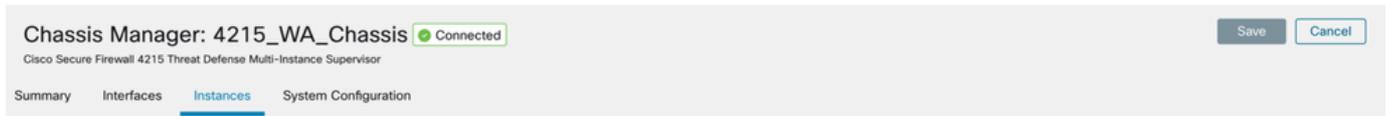
- Permite que o usuário escolha políticas de FTD - Política de acesso e política de Configurações de plataforma para a instância de FTD.
- Registre automaticamente a instância do FTD no FMC quando estiver online.



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

Criar uma instância

Inicie o assistente clicando em Adicionar instância.



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

There are no instances created yet.
Add an instance to get started

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.

Etapa 1. Contrato:

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

Etapa 2.

- Fundamentos da configuração da instância:

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

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

Permit Expert mode for CLI

Resource Profile *
Default-Small

DNS Servers

Device SSH Password *

Confirm Password *

Show 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.

- IPs de Configuração de Instância:

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

Etapa 3. Atribuições de interface:

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.

Etapa 4. Gerenciamento de dispositivos:

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.

Etapa 5. Resumo:

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.

Para concluir a configuração, Salvar e Implantar.

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

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.

Registro automático de uma instância de FTD após a implantação bem-sucedida:

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.

Instância registrada no Management Center:

The screenshot shows the FMC Device Listing Page with a table of devices. The table has the following columns: Name, Model, Version, Chassis, Licenses, Access Control Policy, and Auto RollBack. The data is as follows:

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.

Editar uma instância

Clique no ícone do lápis para editar uma instância de 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.

Etapa 1. Editar instância de 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

FQDN

Firewall Mode *
Routed

DNS Servers

Device SSH Password *
.....

Confirm Password *
.....

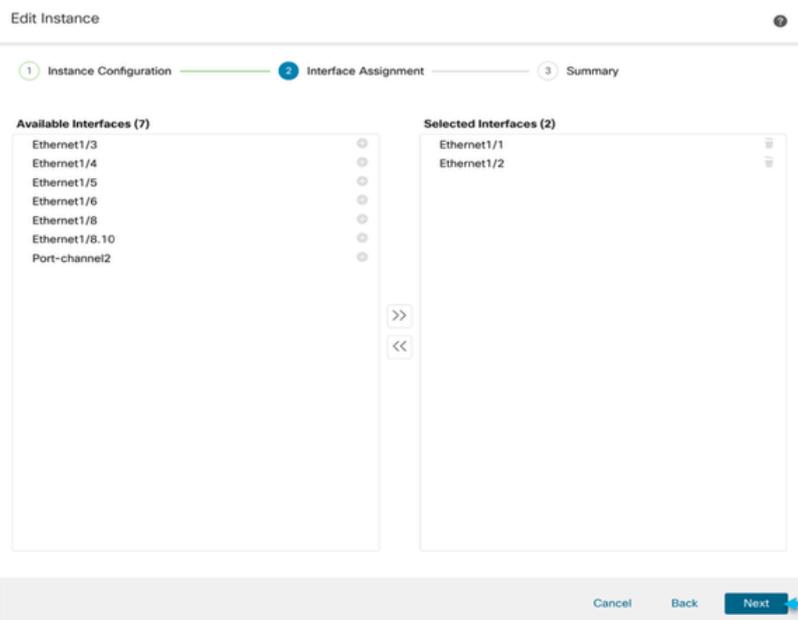
Cancel Next

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

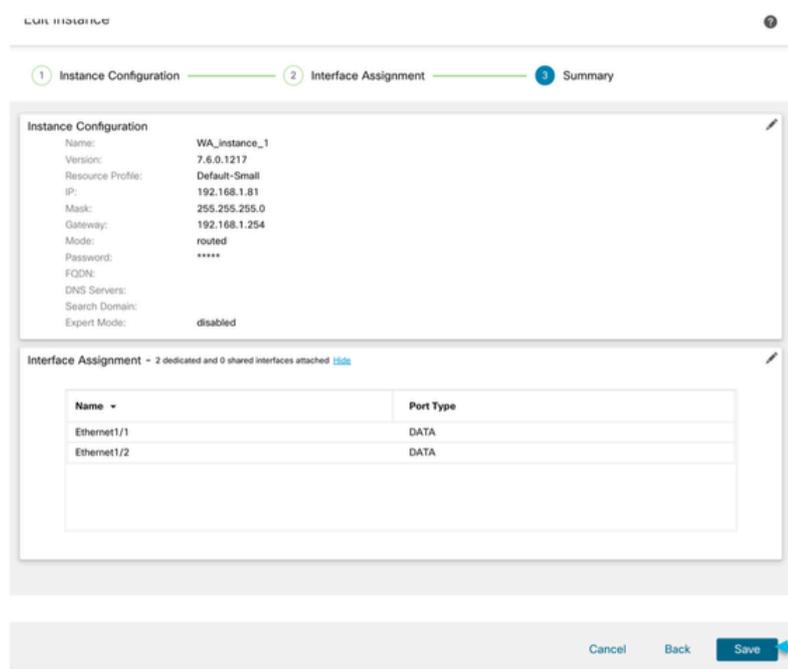
Etapa 2. Editar atribuições de interface para uma instância:



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

Etapa 3. Resumo da instância de edição:

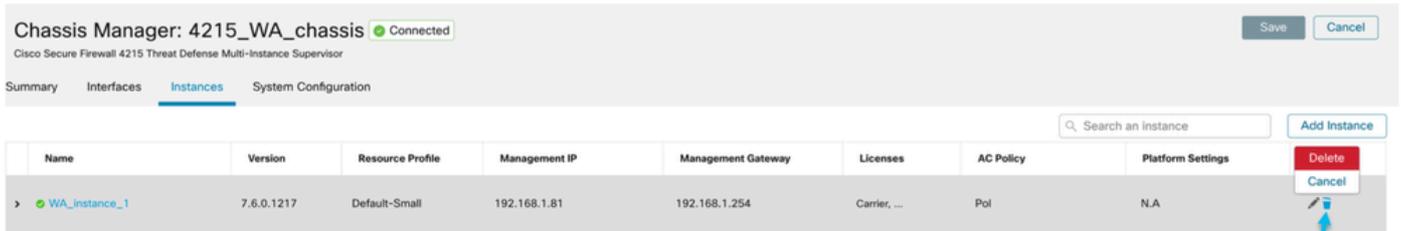


The last step of editing an instance is to view the summary of changes made to the instance.

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.

Excluir instância



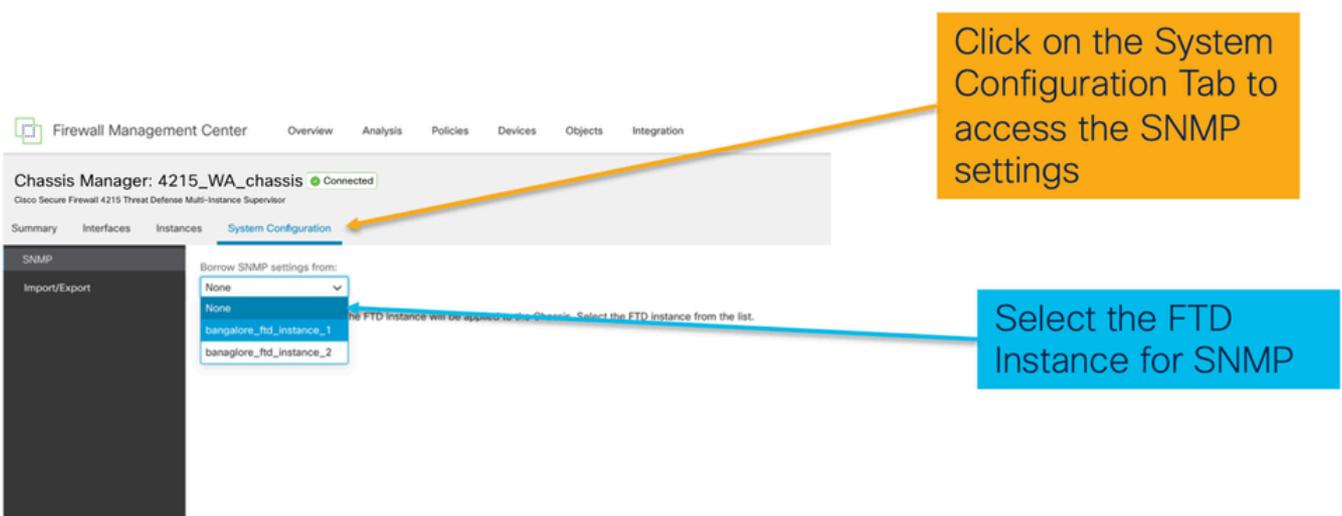
Use the Delete option (from the trash can icon) to delete an existing instance.

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.

Configuração de SNMP

Navegue até a guia de configuração do sistema para configurar o SNMP:



Importação/exportação de chassi

Exportar configuração

Navegue para Gerenciar chassi > Configuração do sistema > Importar/exportar:

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.

Importar configuração

Navegue para Gerenciar chassis > Configuração do sistema > Importar/exportar:

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

O que você precisa saber sobre importação/exportação de chassis

- Todas as configurações existentes no chassi são substituídas pela configuração no arquivo importado.
- A versão do software da plataforma onde a configuração é importada deve ser a mesma da versão exportada.
- O chassi para o qual você está importando a configuração deve ter o mesmo número de módulos de rede instalados quando a exportação foi realizada.
- O chassi onde a configuração é importada deve ter a mesma imagem de aplicativo instalada para dispositivos lógicos.
- As configurações específicas do aplicativo não são exportadas. Somente as configurações

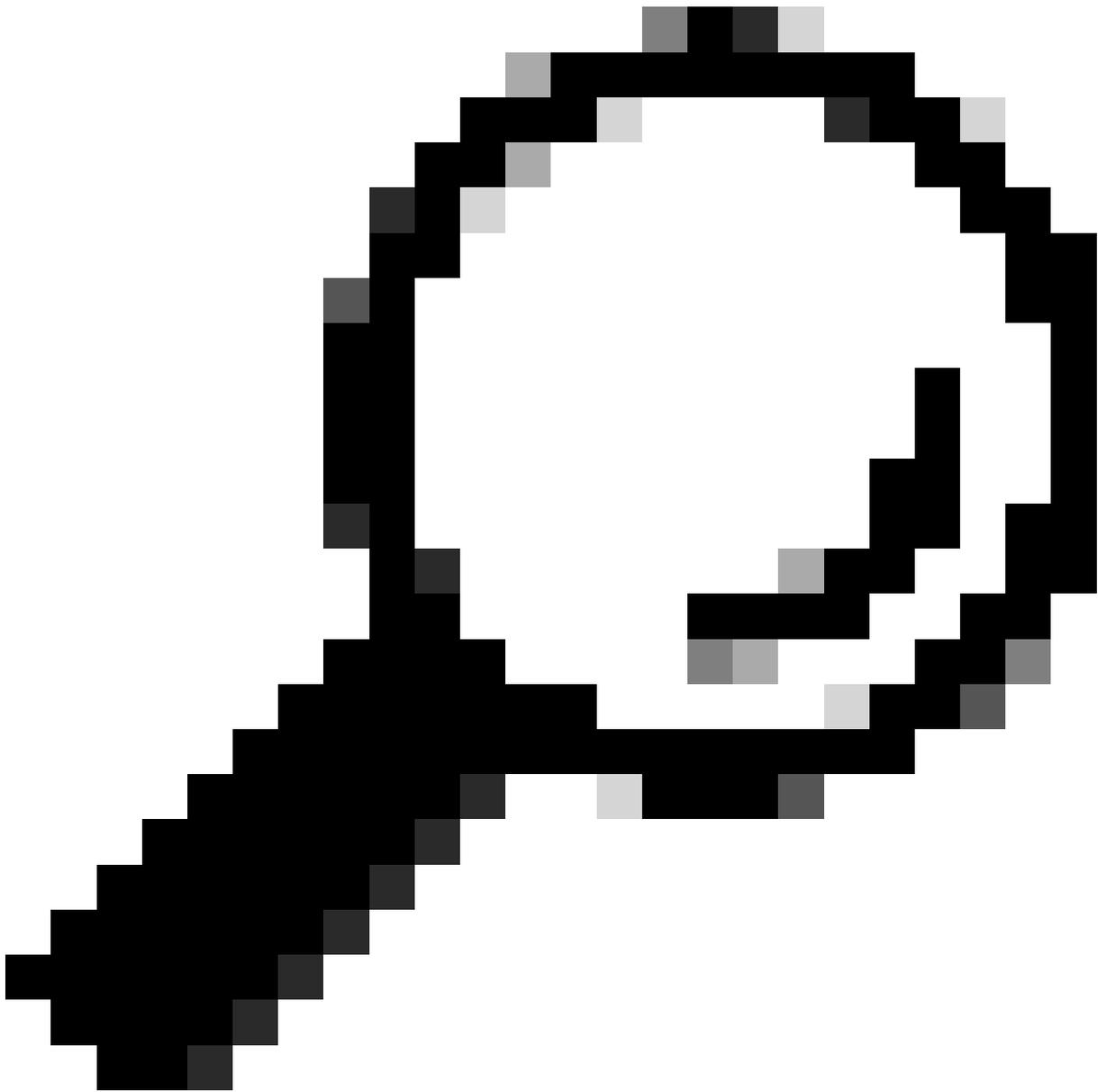
de chassi são exportadas.

- O backup da(s) Instância(s) do FTD deve ser feito separadamente.

Política de configurações da plataforma do chassi

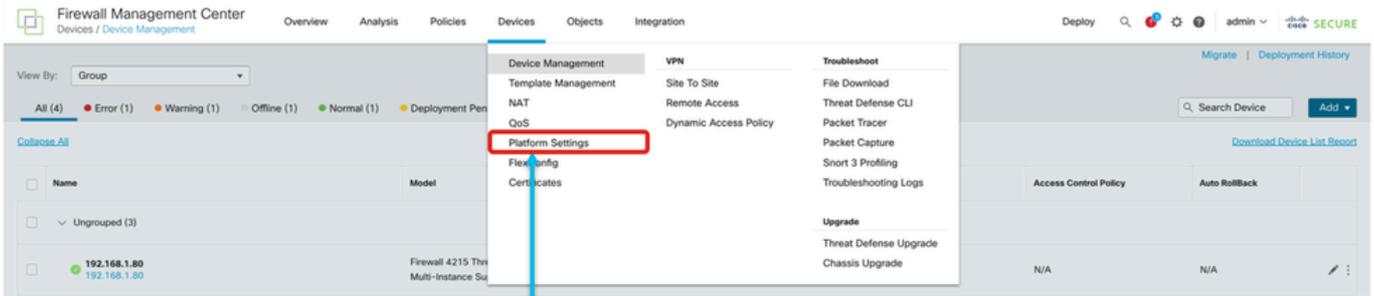
A política de configurações da plataforma do chassi permite que os usuários definam as seguintes configurações específicas da plataforma:

- Sincronização de horário (NTP)
- DNS
- Syslog
- Fuso horário
- O usuário pode criar uma nova política "Configuração da plataforma do chassi" e atribuí-la a vários chassis 4200 Series (modo MI).



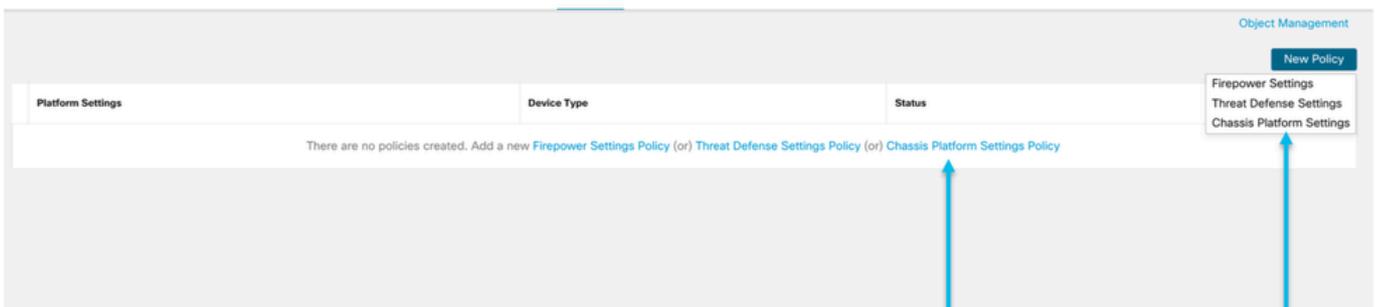
Tip: As configurações da plataforma do chassi aplicam-se apenas ao chassi. Se o usuário quiser aplicar as configurações da plataforma às suas instâncias, poderá usar uma Política de configurações da plataforma Threat Defense.

1. Navegue até chassis Platform Settings policy:



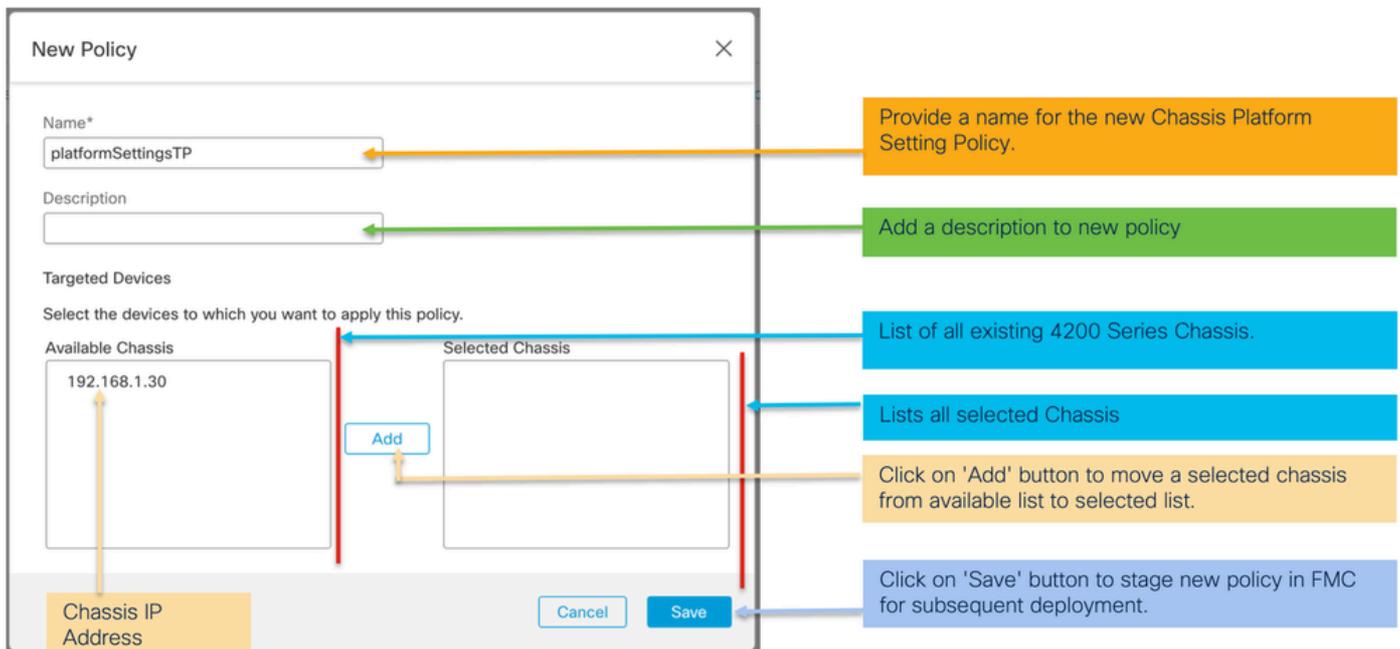
Head to the Platform Settings page to manage your Chassis Platform Settings.

2. Criar Configurações de Plataforma do Chassi:



'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. Página Política de Configurações de Plataforma do Chassi:

The screenshot shows the 'PlatformSettingsTP' configuration page. On the left is a sidebar with tabs for DNS, SSH, SSH Access List, Syslog, Time Synchronization, and Time Zones. The main area is titled 'DNS Resolution Settings' and includes a toggle for 'Enable DNS name resolution by device' and a section for 'DNS Server Groups' with an 'Add' button. At the top right, there are 'Cancel' and 'Save' buttons and a notification 'You have unsaved changes'. A 'Policy Assignments (1)' link is also visible.

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.)

Configurações da plataforma do chassi: DNS

Habilite e adicione grupos de servidores DNS na seção DNS da política de configurações da plataforma do chassi:

This screenshot shows the 'platformSettingsTP' configuration page with several annotations. The 'DNS' tab is selected in the sidebar. The 'DNS Resolution Settings' section has a toggle for 'Enable DNS name resolution by device'. Below it is a list of 'DNS Server Groups' with an 'Add' button. An 'Add DNS Server Group' dialog is open, showing a dropdown for 'Select DNS Server Group*' with 'dns_serverTP' selected, and a '+ New Group' button. Annotations include: 'Enable/Disable DNS resolution on the device' pointing to the toggle; 'Select an existing DNS server group. User can choose an existing server group available in objects page' pointing to the dropdown; 'Click on '+' to create a new server group' pointing to the '+ New Group' button; 'Click on 'Add' to launch Add DNS Server Group dialog' pointing to the 'Add' button; 'Lists of all DNS server groups' pointing to the list; 'Click on 'DNS' tab to view DNS specific configuration' pointing to the sidebar; and 'Click on delete icon to delete an existing DNS server group. Click on edit icon to launch dialog to edit DNS server group.' pointing to the edit and delete icons in the list.

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 'Add' to launch Add DNS Server Group dialog

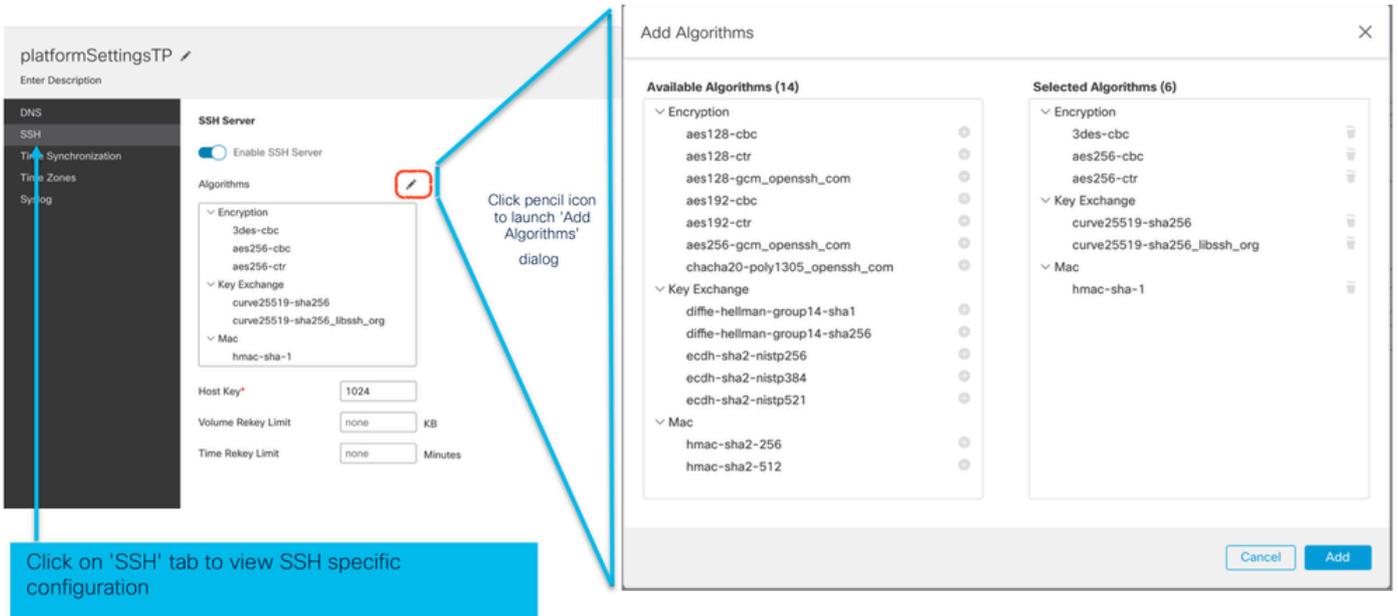
Lists of all DNS server groups

Click on 'DNS' tab to view DNS specific configuration

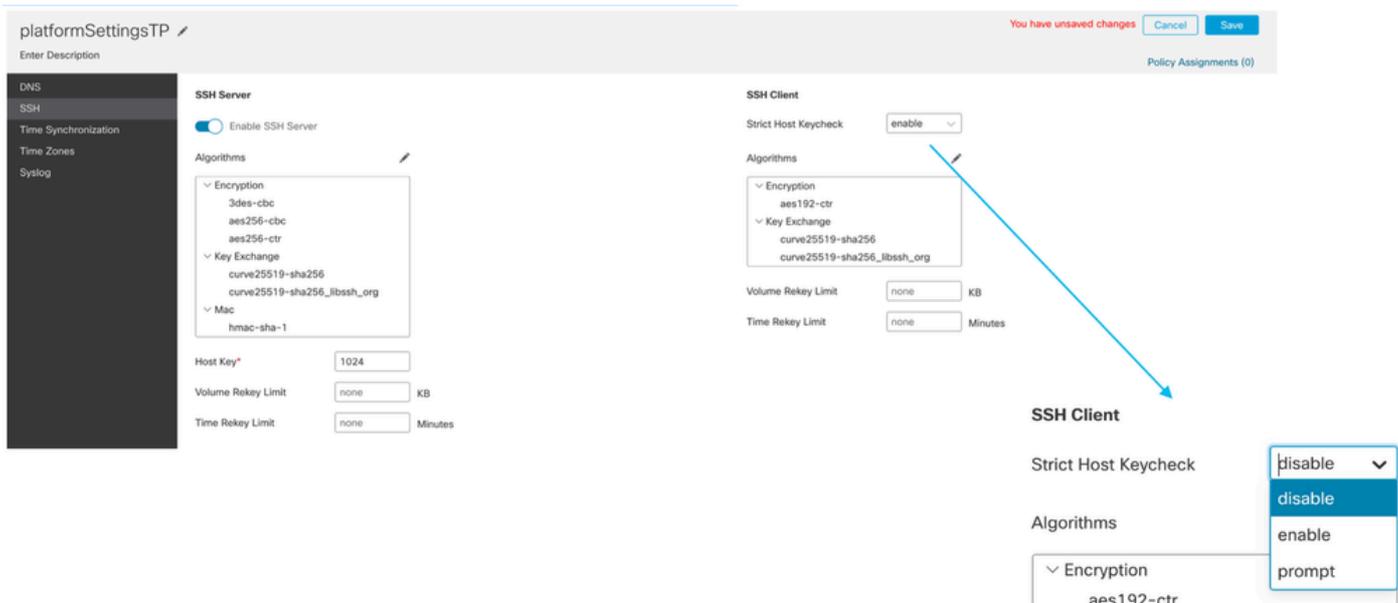
Click on delete icon to delete an existing DNS server group. Click on edit icon to launch dialog to edit DNS server group.

Configurações da plataforma do chassi: SSH

- Habilite e adicione o servidor SSH na seção SSH da política de configurações da plataforma de chassi:



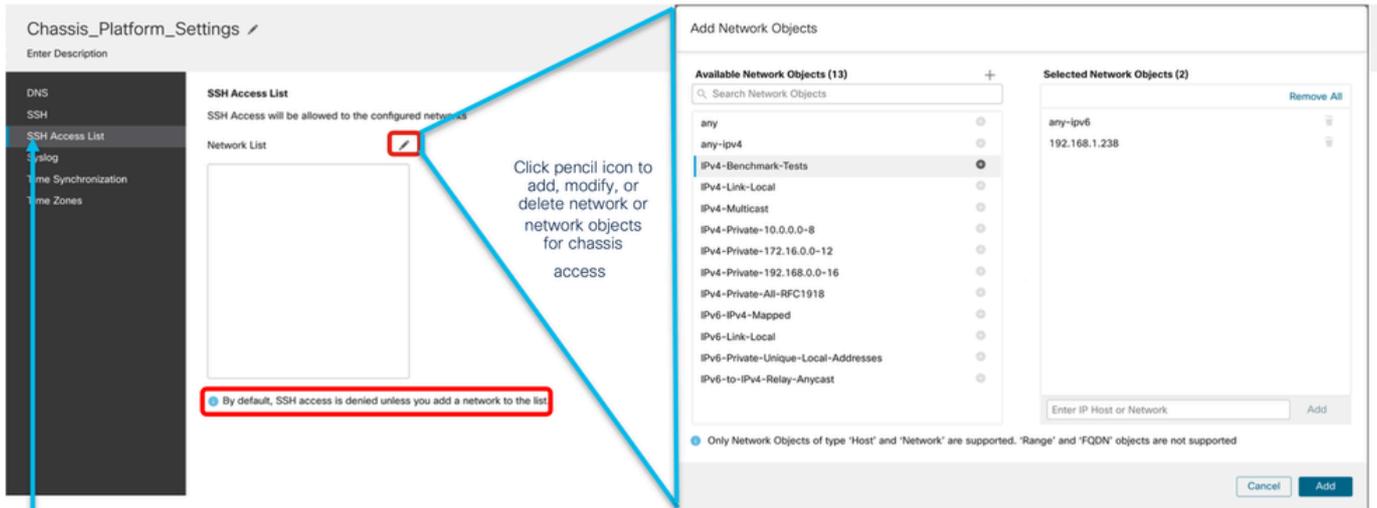
- Habilitar e adicionar cliente SSH:



Configurações da plataforma do chassi: Lista de acesso SSH

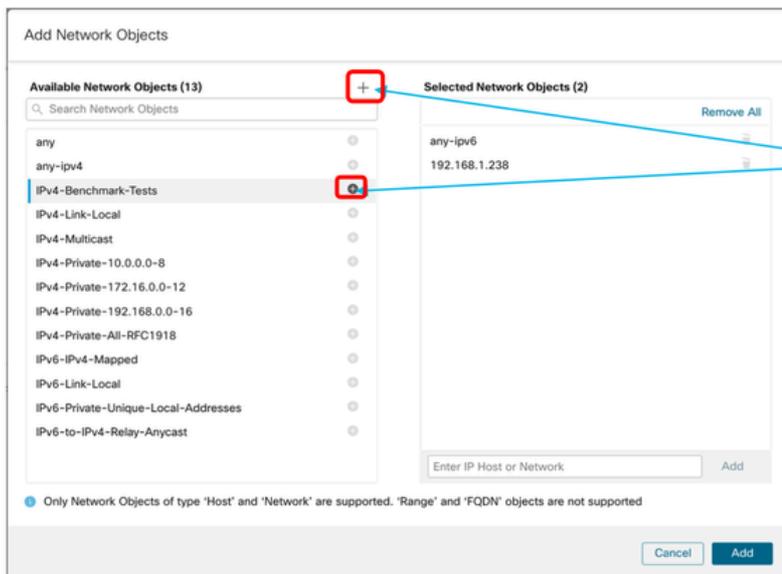
Esta guia aparece somente após a ativação do SSH na seção SSH das configurações da plataforma do chassi.

- Criar lista de acesso SSH:



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

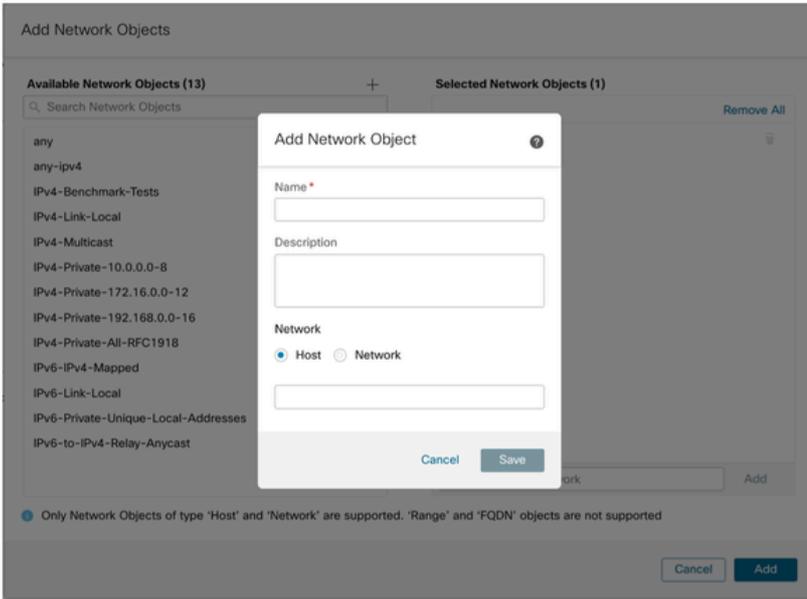
- Adicione objetos de rede à lista de acesso SSH:



Network objects can be selected by:

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

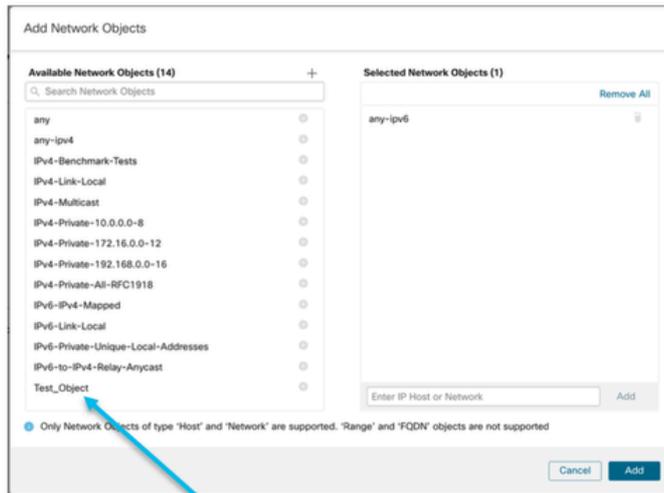
- Adicionar um novo objeto de rede:



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

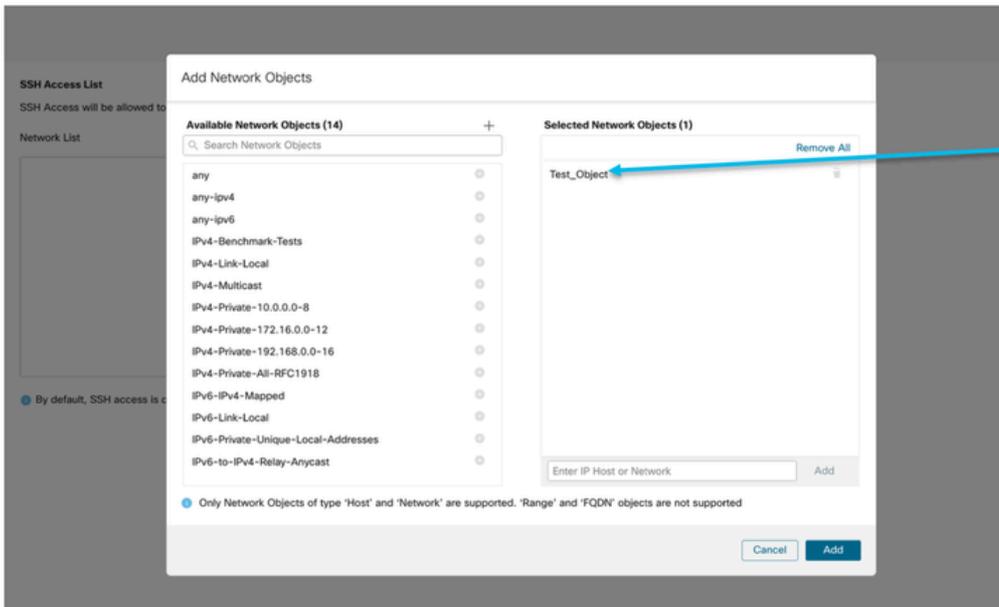
Range and FQDN are NOT allowed.

- Exibir objeto(s) de rede:



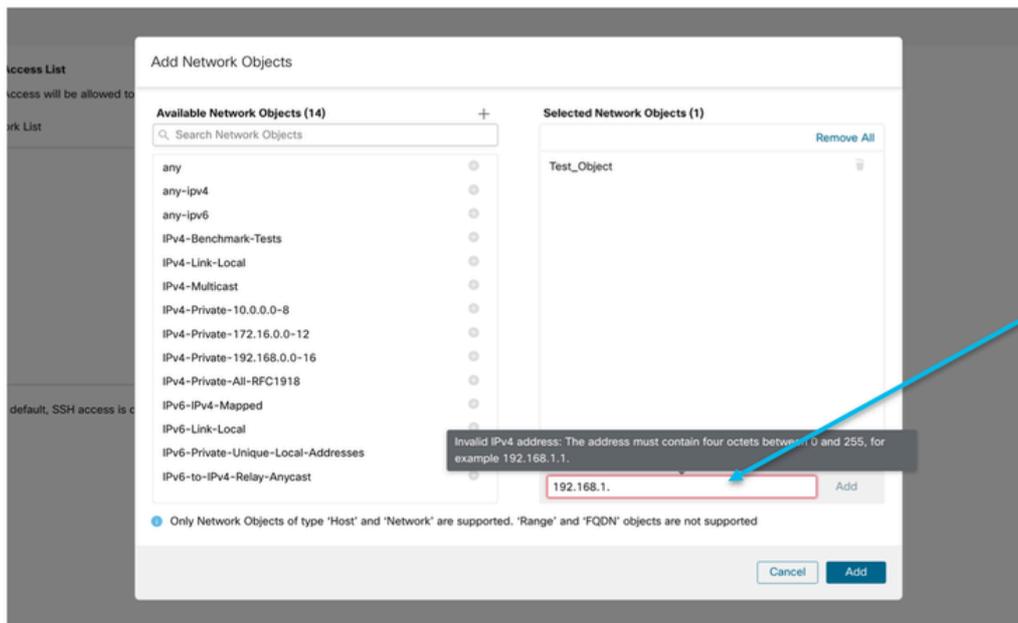
After creation of host object, it will be listed in the available network objects.

- Selecionar objeto(s) de rede:



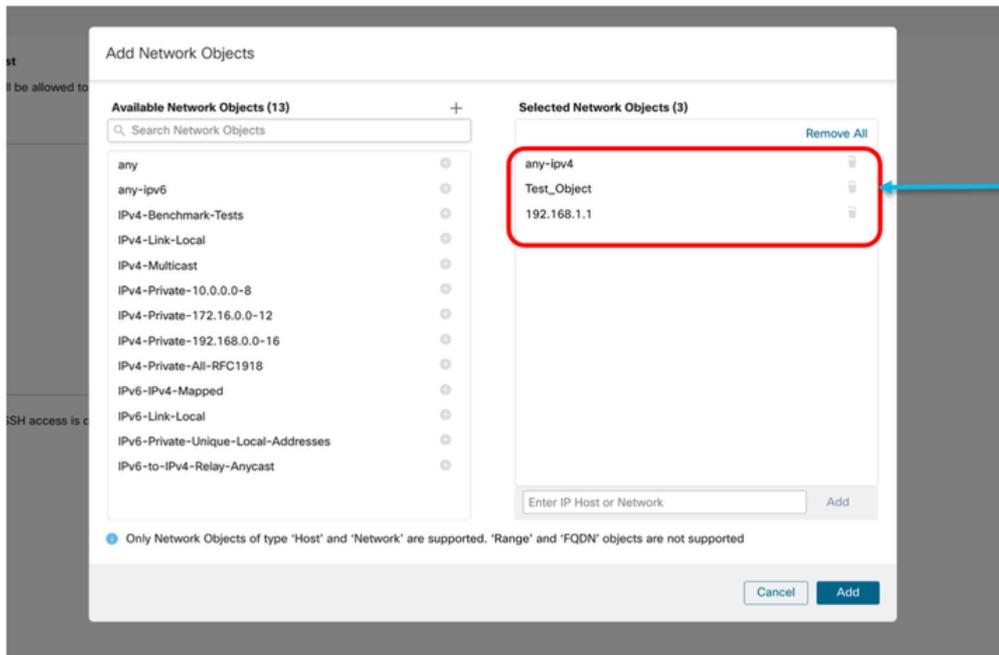
After selecting Network Objects using the “+” icon from available network objects, it will be listed in the selected pane.

- Objetos de rede podem ser criados como também mostrado nesta imagem:



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

- Exibir objetos de rede adicionados:



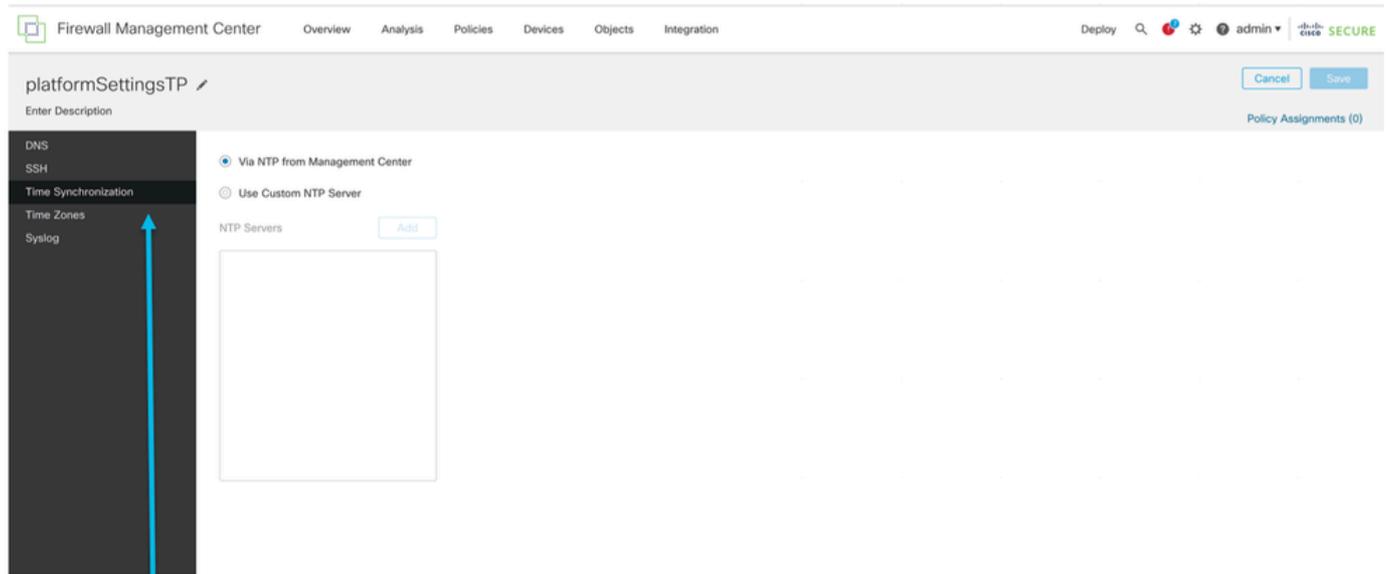
Once the objects are added, they will be listed in the Selected Network Objects pane.

Configurações da plataforma do chassi: Sincronização de horário

A Sincronização de Tempo pode ser feita de duas maneiras:

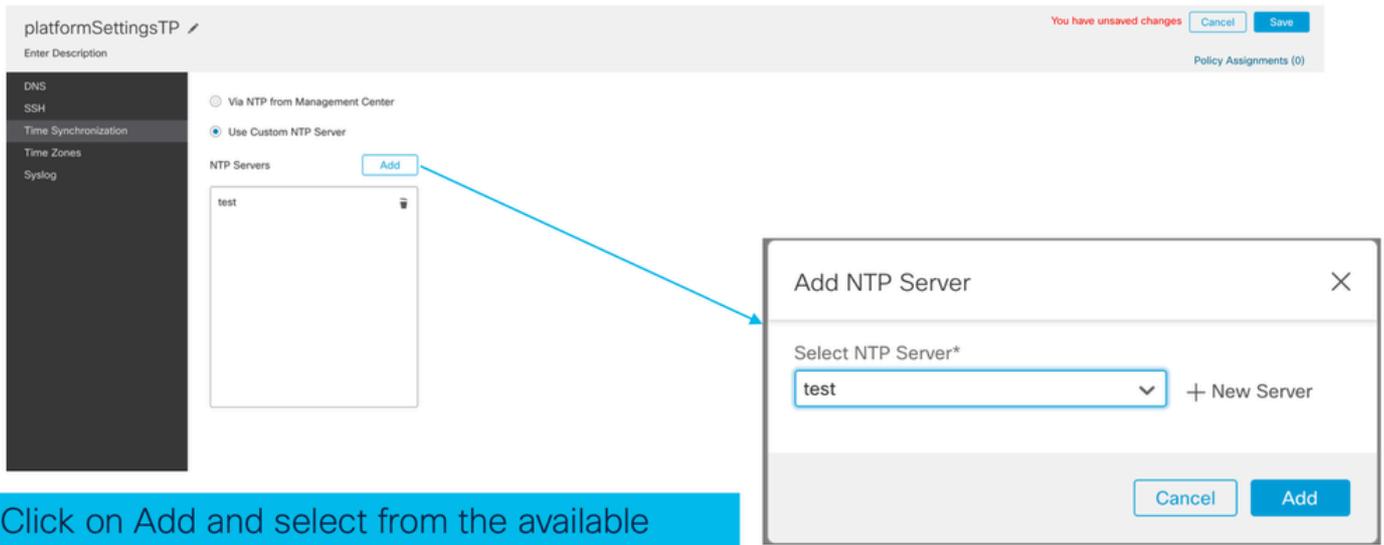
1. Via NTP do Management Center
2. No servidor NTP personalizado

Do NTP do Management Center



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

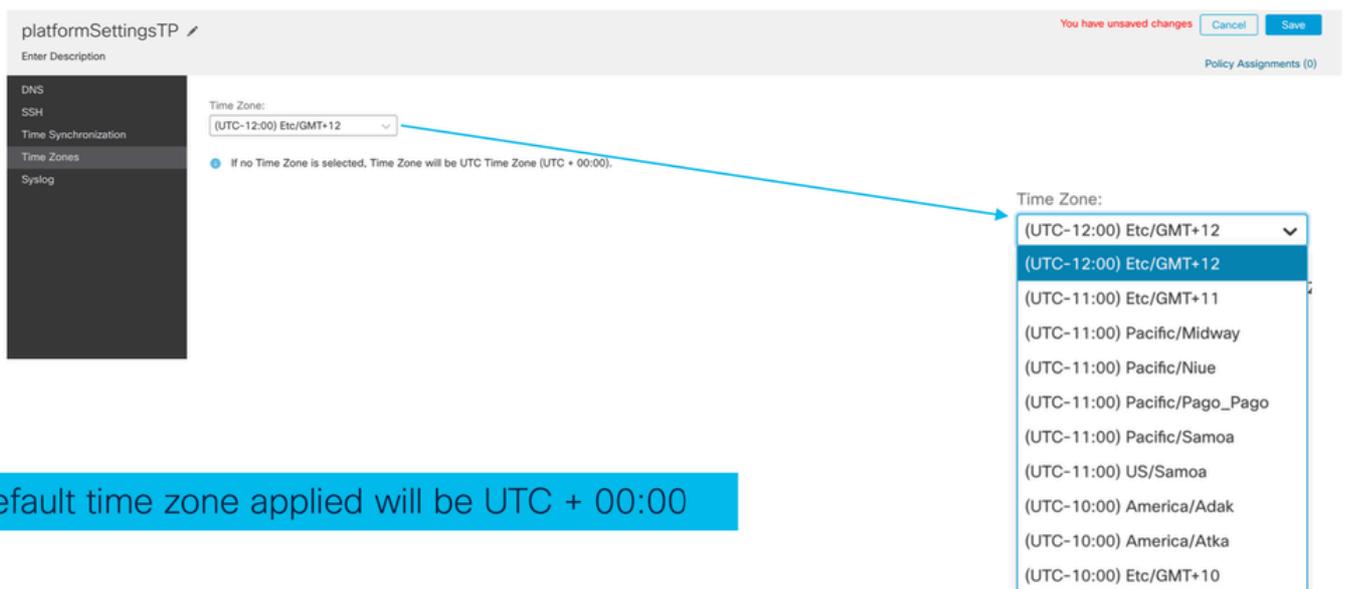
No servidor NTP personalizado



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

Configurações da plataforma do chassi: Fusos Horários

Definir fusos horários:



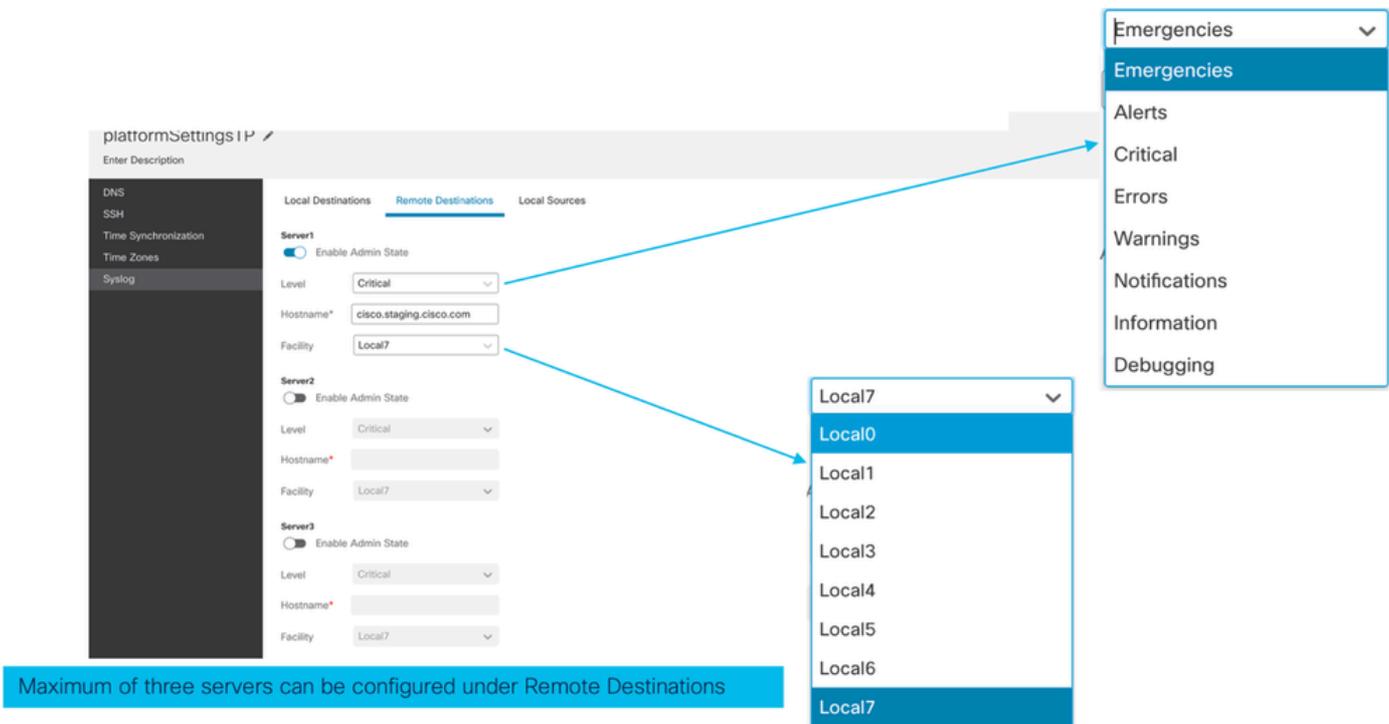
Default time zone applied will be UTC + 00:00

Configurações da plataforma do chassi: Syslog

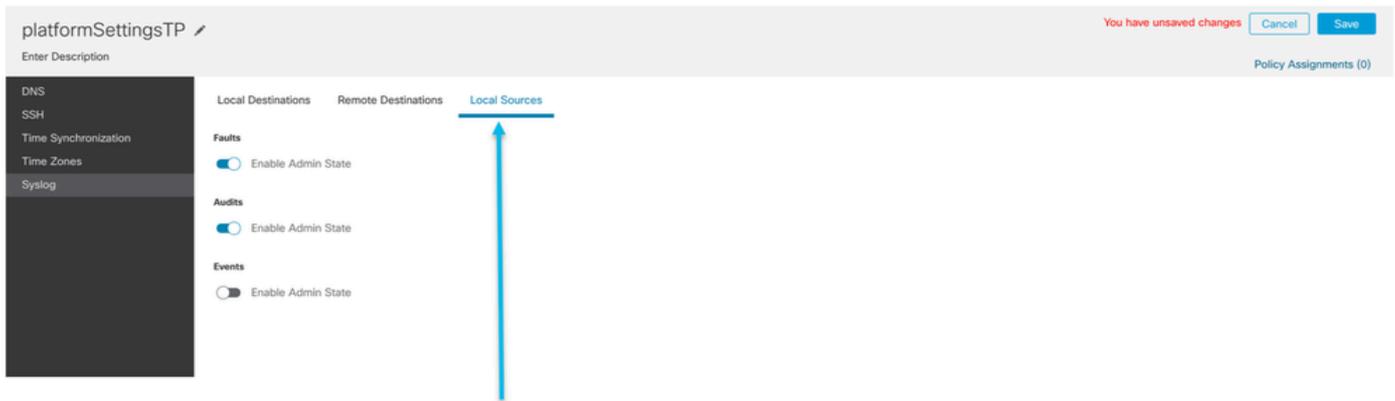
- Guia Destinos locais de Syslog:



- Guia Destinos remotos de Syslog:



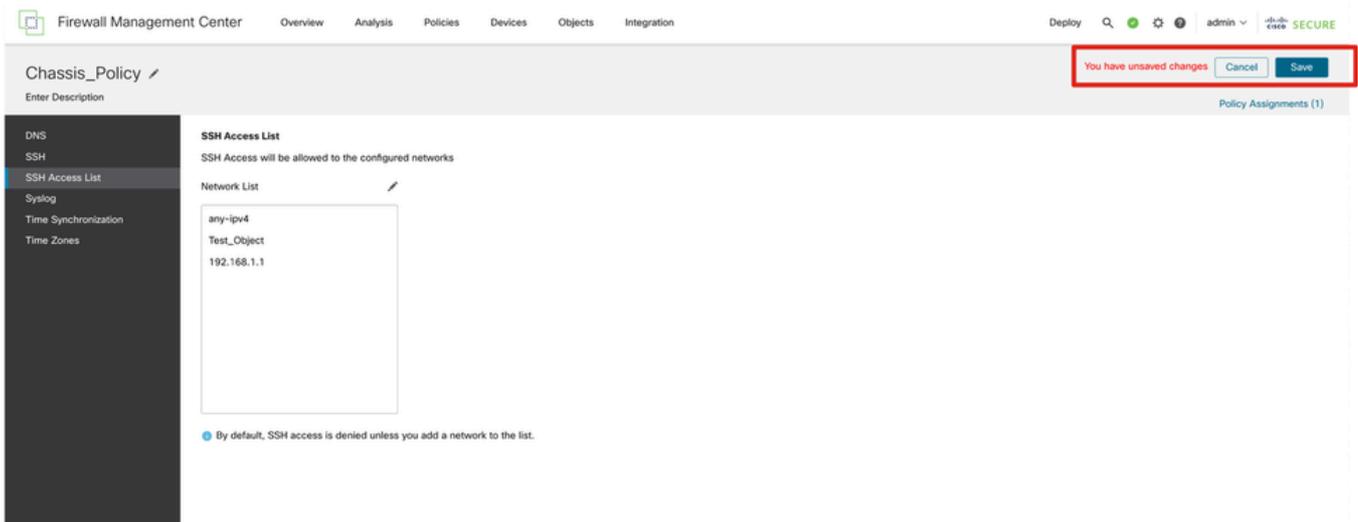
- Guia Origens Locais de Syslog:



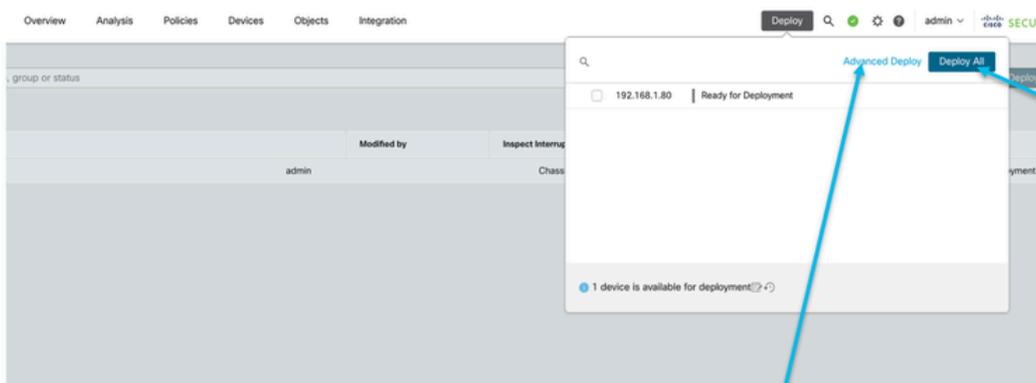
Click on the Local Sources tab to configure Faults/Audits/Events for Local Sources

Configurações da plataforma do chassi: Salvar e implantar

Salve as alterações de configuração da plataforma do chassi e implante:



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

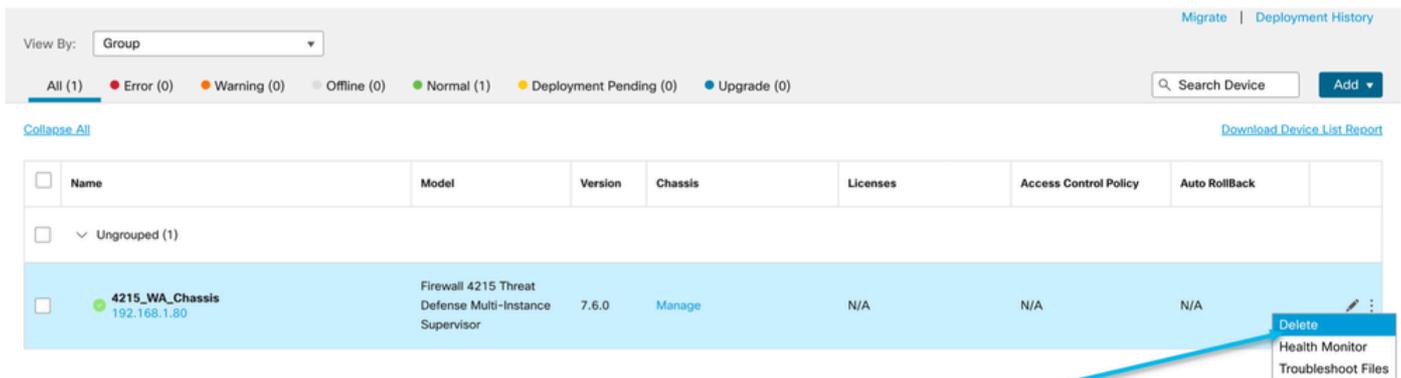


1. Trigger deployment.
2. Once deployment is completed, all chassis platform settings are deployed.

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

Cancelando o registro do chassi

Para cancelar o registro de um chassi no FMC, navegue para Devices > Device Management > delete.



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

Converter de Várias Instâncias para o Modo Nativo

Atualmente, o FMC só oferece suporte à conversão de Nativo para Várias Instâncias. Conseqüentemente, para converter um dispositivo de volta ao modo Nativo, o usuário precisa usar a CLI.

Passo 1: Cancele o registro do chassi no FMC.

Passo 2: Use este comando CLI para converter o dispositivo 4200 Series para o modo nativo:

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

APIs FMC Rest

As APIs REST públicas do FMC estão disponíveis para todas as operações apoiadas pelo 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

APIs REST para conversão de nativo em várias instâncias

API POST para verificar se o dispositivo nativo está pronto para a Conversão de Várias Instâncias:

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

Exemplo de solicitação POST JSON:

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

API POST para disparar conversão nativa única em Várias Instâncias:

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

Exemplo de solicitação POST JSON:

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

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

API POST para disparar conversão em massa nativa em Várias Instâncias:

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

Exemplo de solicitação POST JSON:

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

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

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

APIs REST para gerenciamento de chassi

POST Adicione um chassi ao centro de gerenciamento:

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

OBTER todos os chassis:

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

OBTENHA um chassi específico pelo uuid:

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

Excluir um chassi pelo uuid:

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

Exemplo de solicitação POST JSON:

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

APIs REST para gerenciamento de Netmods (módulos de rede)

OBTENHA um módulo de rede pelo uuid:

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

OBTENHA TODOS os módulos de rede:

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

PUT - Edite um Módulo de Rede existente pelo uuid:

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

PUT - Recuperar dados do módulo de rede do FXOS e atualizar o Centro de Gerenciamento:

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

Exemplo de resposta GET

```
{
  "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"
}

```

APIs REST para gerenciamento de instâncias

POST Adicione um chassi ao centro de gerenciamento:

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

OBTER todos os chassis:

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

OBTER uma instância específica por uuid:

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

PUT - Editar uma Instância por uuid:

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

Excluir um chassi pelo uuid:

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

Exemplo de solicitação PUT:

```

{
  "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" }
```

APIs REST para gerenciamento SNMP

OBTER uma configuração SNMP por uuid:

```
/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/snmpsettings/{objectUID}
```

OBTER TODAS as configurações SNMP:

```
/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/snmpsettings/
```

PUT - Edite um Módulo de Rede existente pelo uuid:

```
/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/snmpsettings/{objectUID}
```

Resposta GET de exemplo:

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

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

Resumo de APIs REST para busca

Esta lista contém informações detalhadas sobre as APIs REST para buscar o resumo:

- Falhas
- Instâncias
- Inventário
- Interfaces
- Informações do aplicativo

Resumo de falhas GET para um chassi:

`/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/faultsummary`

Resposta de exemplo:

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

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

Resumo de Instâncias GET para um chassi:

`/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/instancessummary`

Resposta de exemplo:

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

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

GET Resumo de inventário para um chassi:

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

Resposta de exemplo:

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

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

Resumo da interface GET para um chassi:

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

Resposta de exemplo:

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

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

OBTER Informações do aplicativo para um chassi:

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

/inventorysummary

Resposta de exemplo:

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

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

APIs REST para gerenciamento de interface

Esta seção tem informações detalhadas sobre as APIs REST para gerenciamento de configuração de interface:

- URLs a serem usados para modificações de configuração de interface
- URLs a serem usados para Interrupção/Junção de interfaces
- URLs a serem usadas para configurações do Dispositivo de Sincronização

Atualizar interface física

Para suportar a atualização de interfaces físicas, esses URLs foram apresentados.

OBTER todas as interfaces físicas:

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

OBTENHA uma interface física específica pelo uuid da interface:

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

Atualizar interface pelo uuid da interface:

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

O modelo de interface física é semelhante a este:

```
{
```

```

"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": "*****"
}

```

Configurar subinterfaces

Para suportar o gerenciamento de subinterfaces, esses URLs foram apresentados.

OBTER todas as subinterfaces:

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

OBTENHA uma sub-interface específica pelo uuid da interface:

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUID}/subinterfaces/{interfaceName}
```

POST para uma nova sub-interface:

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

ATUALIZE a interface pelo uuid da interface:

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUID}/subinterfaces/{interfaceName}
```

EXCLUIR uma sub-interface pelo uuid da interface:

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUID}/subinterfaces/{interfaceName}
```

O modelo de subinterface se parece com este:

```
{
  "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": "*****"
}
```

Configurar Interfaces EtherChannel

Para suportar o gerenciamento de interfaces EtherChannel EtherChannel, esses URLs foram apresentados.

OBTENHA todas as interfaces etherchannel:

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

OBTENHA uma interface etherchannel específica pelo uuid da interface:

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

POST para uma nova interface etherchannel:

```
/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/etherchannelinterfac
```

ATUALIZE a interface pelo uuid da interface:

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

EXCLUIR uma interface etherchannel pelo uuid da interface:

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

O modelo de interface EtherChannel se parece com isto:

```

{
  "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-*****"
}

```

Interfaces de interrupção/junção de APIs REST

Para suportar a Divisão/Junção de interfaces no 4200 Series, estes URLs podem ser usados:

GET:

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

Avalia a viabilidade de interrupção/junção para uma interface

POST:

`/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUID}/operational/break`

Interrompe uma interface

POST:

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

Une um conjunto de interfaces quebradas

Fluxo REST para quebra de interface

1. Localize o dispositivo de chassi gerenciado do FMC (4200) usando o endpoint fmcmanagedchassis.

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

Retorna a lista de dispositivos de chassi gerenciados do FMC junto com dispositivos de Várias Instâncias com detalhes como ID, nome e modelo de cada dispositivo. Escolha os dispositivos "MULTIINSTANCE".

Resposta de exemplo:

```
{
  "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. Verifique se a interface tem capacidade de breakout usando o ponto final interfaces/physical interfaces.

A reunião à parte só será possível se "isBreakoutCapable" for verdadeiro e mediaType for QSFP.

GET

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

Resposta de exemplo:

```
{
  "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. Na interface, avalie a viabilidade da operação de quebra usando o ponto final de avaliação operação.

GET

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/chassisinterfaces/{in

Se não houver avisos/erros na resposta, o usuário poderá executar a operação de interrupção.

Resposta de exemplo:

```

{
  "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 houver erros na resposta, o usuário não poderá executar a operação de interrupção:

```

{
  "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 a interface for habilitada para breakout e o estado de prontidão for "READY", quebre a interface usando o ponto final breakoutinterfaces.

POST

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

Solicitação:

```

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

```

Resposta:

```

{
  "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. Rastreie a conclusão da tarefa usando o id da tarefa na resposta à interrupção. Defina o status da tarefa como "Notificação de interface recebida".

GET /api/fmc_config/v1/domain/{domainUID}/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. Obtenha as alterações de interface usando o ponto de extremidade chassisinterfaceevents.

GET /api/fmc_config/v1/domain/{domainUID}/chassis/
fmcmanagedchassis/{containerUID}/chassisinterfaceevents

Resposta de exemplo:

```
[
  {
    "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": "Ethernet2/3/2"
  }
]
```

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

7. Se a notificação de interface não for recebida, sincronize o dispositivo usando o ponto de extremidade `chassisinterfaceevents` e verifique se há alterações pendentes.

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

Solicitação:

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

Resposta:

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

8. Quando a notificação for recebida, aceite as alterações usando o ponto final `chassisinterfaceevents`.

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

Solicitação:

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

9. Obtenha todas as interfaces do chassi e localize as interfaces divididas (quebradas) usando o

endpoint de interfaces.

GET

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/interfaces

Uma interface 40G, digamos eth2/2, é dividida em interfaces 4x10G - eth2/2/1, eth2/2/2, eth2/2/3 e eth2/2/4

Fluxo REST para junção de interface

1. Verifique se a interface está quebrada usando o endpoint interfaces/physicalinterfaces.

A operação de junção só será possível se "isSplitInterface" for verdadeiro e mediaType for SFP

GET

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/interfaces

```
{
  "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. Avalie a viabilidade da operação Join usando o ponto final de avaliaçãooperation em uma das quatro interfaces de divisão.

GET /api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/chassisinterfaces/{interfaceUUID}/valuateoperation

- Se não houver avisos/erros na resposta, o usuário poderá executar a operação Ingressar.

```
{
  "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 houver erros na resposta, o usuário não poderá executar a operação de junção.

```
{
  "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 a interface estiver quebrada e o estado de prontidão for "PRONTO", una-se à interface usando o ponto final joininterfaces. Interface_uuid pode ser o id de qualquer uma das 4 interfaces quebradas.

POST/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/operational

Solicitação:

```
{
  "targetInterfaces": [
    {
      "id": "*****ed3-0001-692539698200",
      "type": "PhysicalInterface"
    }
  ],
}
```

```
"type": "JoinInterface"
}
```

Resposta:

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

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

4. Rastreie a conclusão da tarefa usando o id da tarefa na resposta de junção. Defina o status da tarefa como "Notificação de interface recebida".

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

Resposta:

```
{
  "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: SUCCEDED",
  "status": "Interface notification received"
}
```

5. Obtenha as alterações de interface usando o ponto de extremidade chassisinterfaceevents.

GET

/api/fmc_config/v1/domain/{domainUID}/devices/devicerecords/{containerUID}/chassisinterfaceevents

Resposta:

```
[
  {
    "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 a notificação de interface não for recebida, sincronize o dispositivo usando o ponto de extremidade `chassisinterfaceevents` e verifique se há alterações pendentes.

POST

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

Solicitação:

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

Resposta:

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

7. Quando a notificação for recebida, aceite as alterações usando o ponto final chassisinterfaceevents.

POST

/api/fmc_config/v1/domain/{domainUID}/devices/devicerecords/{containerUID}/chassisinterfaceevents

Solicitação:

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

8. Obtenha todas as interfaces do chassi e localize as interfaces unidas, bem como as outras interfaces, usando o endpoint de interfaces.

GET

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/interfaces

Digamos que a união tenha sido iniciada na interface 10G, digamos eth2/2/1, então uma interface 40G eth2/2 estará disponível na resposta.

Sincronizar APIs REST de Dispositivo

Para suportar a Sincronização do Módulo de Rede e das Interfaces, esses URLs foram apresentados.

POST:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/chassisinterfaceevents

Com payload

{"ação": "SYNC_WITH_DEVICE"} - > Aciona a sincronização

{"ação": "ACCEPT_CHANGES"} - > Aceitar as alterações

GET:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/chassisinterfaceevents

Lista os eventos alterados gerados

Solução de problemas/diagnósticos

Log FXOS

Se o registro falhar, essas CLIs FXOS podem ser usadas para verificar se os processos sftunnel e sfiproxy estão ativos.

```
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 estiver usando o console do terminal para a CLI, certifique-se de que a saída de show processes não esteja truncada, definindo a largura do terminal com um valor apropriado usando esta CLI mostrada:

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

Se o processo SFTunnel estiver ativo e em execução, mas o registro estiver falhando, esses comandos podem ser usados para encontrar qualquer motivo potencial para a falha.

Introduziu a nova CLI no FXOS do connect local-mgmt para exibir mensagens de syslog em /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
```

Registro do CVP

- Se o registro do dispositivo falhar, localize usmsharedsvcs.log e vmssharedsvcs.log neste local e procure a string "CHASSIS DISCOVERY" ou "NATIVE_TO_MULTI_INSTANCE" para encontrar a causa potencial da falha.
 - Além disso, procure em /var/log/action_queue.log e /var/sf/messages problemas de SFTunnel.

- /var/opt/CSCOpX/MDC/log/operation/usmsharedsvcs.log
/var/opt/CSCOpX/MDC/log/operation/vmssharedsvcs.log
- Se o registro automático do chassi falhar, localize usmsharedsvcs.log e vmssharedsvcs.log e procure a string "CHASSIS DISCOVERY" e "NATIVE_TO_MULTI_INSTANCE" para encontrar a causa potencial da falha.
- Se o registro automático da instância falhar, localize usmsharedsvcs.log e vmssharedsvcs.log e procure a string "MI_FTD_INSTANCE_AUTO_REGISTRATION" para localizar a causa potencial da falha.
- Se houver uma falha de implantação no dispositivo, navegue para Implantar -> Histórico de implantação -> Clique na implantação com falha -> Abrir transcrição. Este arquivo contém o motivo da falha.

Solução de problemas do chassi

O FMC suporta a geração de solução de problemas de chassi (FPRM) na página de gerenciamento de dispositivos.

- Como o dispositivo FTD, há uma opção de solução de problemas disponível para o dispositivo de chassi que gera solução de problemas de chassi e permite que o usuário faça o download do pacote de solução de problemas do FMC.
- Isso coleta o pacote "show tech-support form" (mostrar formulário de suporte técnico) do chassi:

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	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		

Opções de solução de problemas e geração de chassis:

- Click On Generate to start generating troubleshoot.

Generate Troubleshoot Files - 4215_WA_chassis

1 This operation generates troubleshoot logs for Secure Firewall 3100 chassis

1 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

Progresso e download da solução de problemas do chassi:

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

Exemplos de Problemas com Troubleshooting de Passo a Passo

Registro automático de falha de chassi no FMC

Problema: O registro automático do chassi está falhando no FMC.

Resultado esperado:

- Uma vez iniciada a conversão a partir do CVP, espera-se que não seja registrada e que seja registrada automaticamente no CVP.

Resultado real:

- Falha no registro automático do chassi

Solução de problemas

1. Verificar conversão:

- Verificar se a conversão foi desencadeada no CVP.
- Faça login no dispositivo e verifique se o dispositivo foi convertido para o modo de contêiner.
- Execute os comandos para ver se o dispositivo foi convertido:

```
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. Verifique o gerenciador de dispositivos:

- Verifique se o gerenciador de dispositivos foi definido corretamente:

```
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. Logs a verificar:

3.1. Navegue até `/var/opt/CSCOpX/MDC/log/operation/vmssharedsvcs.log` e `/var/opt/CSCOpX/MDC/log/operation/usmsharedsvcs.log`

3.2. Procure as palavras-chave "NATIVE_TO_MI_CONVERSION" e "CHASSIS DISCOVERY" nos arquivos para encontrar o motivo da falha.

Autorregistro de instância no CVP

Problema: Falha no registro automático da instância no FMC.

Resultado esperado:

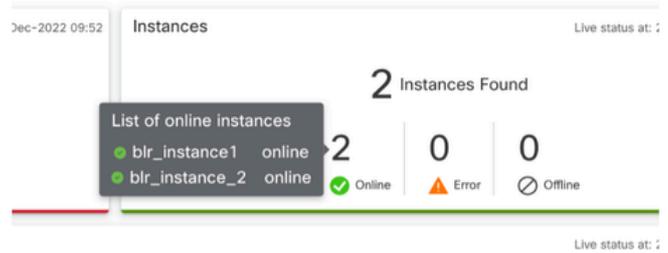
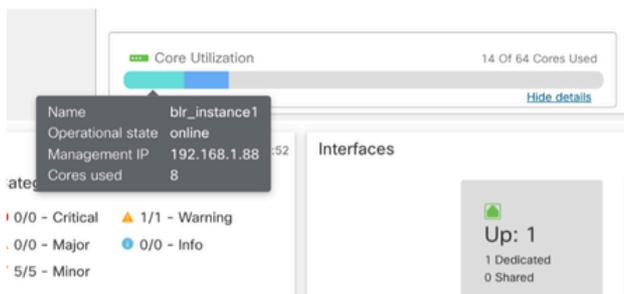
- Quando a instância for provisionada pelo FMC, ela deverá ser registrada automaticamente no FMC

Resultado real:

- Falha no registro automático da instância

Solução de problemas

- Verifique se a implantação foi disparada após a criação da instância.
 - Se a implantação não estiver concluída, assegure-se de implantar as alterações no dispositivo.
 - Se houver uma falha na implantação, vá para Histórico de implantação -> Clique em Transcrição. Verifique o motivo da falha, corrija e repita a implantação.
- Verifique se a instância está instalada e se seu estado operacional está online. Você pode usar a página de resumo do chassi para verificar o status do provisionamento da Instância.



- Verifique se o SFTunnel está ativo e em execução no FTD da instância usando este comando:

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

- Se o SFTunnel não estiver em execução, tente executar um comando de reinicialização:

```
pmtool restartById sftunnel
```

- Navegue até `/var/opt/CSCOpX/MDC/log/operation/vmssharedsvcs.log` e `/var/opt/CSCOpX/MDC/log/operation/usmsharedsvcs.log`
- Procure a palavra-chave "MI_FTD_INSTANCE_AUTO_REGISTRATION" no arquivo para encontrar o motivo da falha.

Registro de dispositivo nativo no FMC

Problema: O Native Device Registration está falhando no FMC após a conversão do dispositivo de volta ao modo nativo

- Caso o usuário converta o chassi (modo MI) de volta para o modo nativo, mas se esqueça de excluir o chassi do FMC, o dispositivo fica off-line no FMC.
- Se o usuário tentar registrar novamente esse dispositivo nativo no FMC, o registro falhará.

Solução de problemas

- Verifique se a entrada do chassi foi excluída do FMC antes de converter o dispositivo de volta ao modo nativo.
- Quando a entrada for excluída, tente registrar novamente o dispositivo nativo no FMC.

Referências úteis

- Informações sobre interfaces compartilhadas:

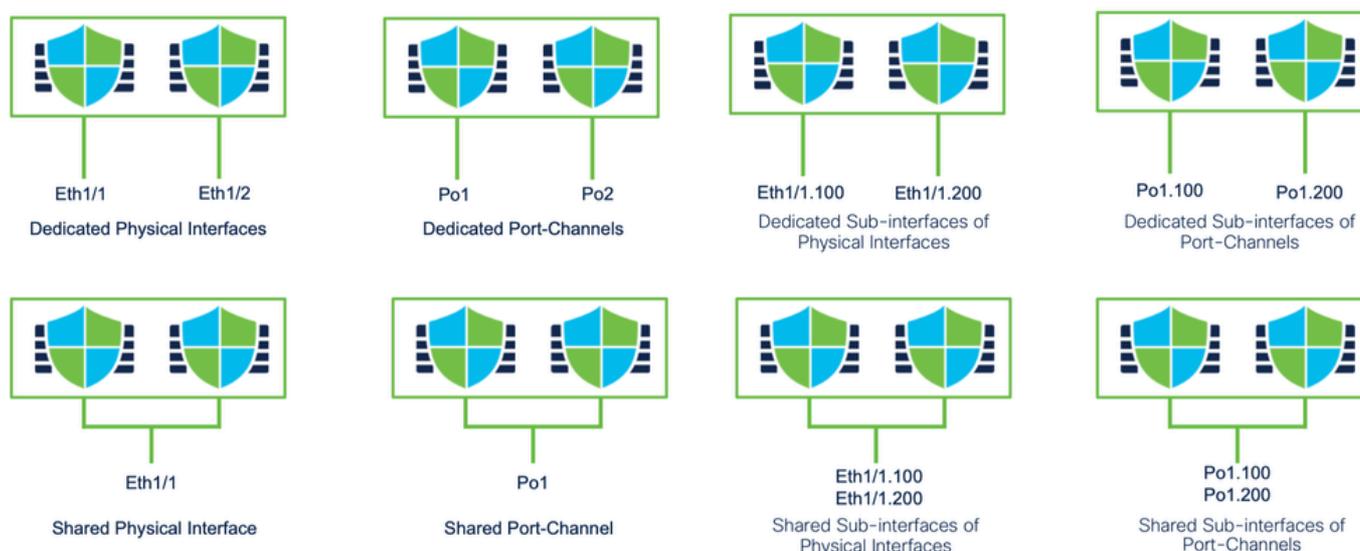
<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/threat-defense/use-case/multi-instance-sec-fw/multi-instance-sec-fw.html#shared-interface-scalability-WGUIEF>

- 3100 Página de várias instâncias no site de suporte da Cisco:

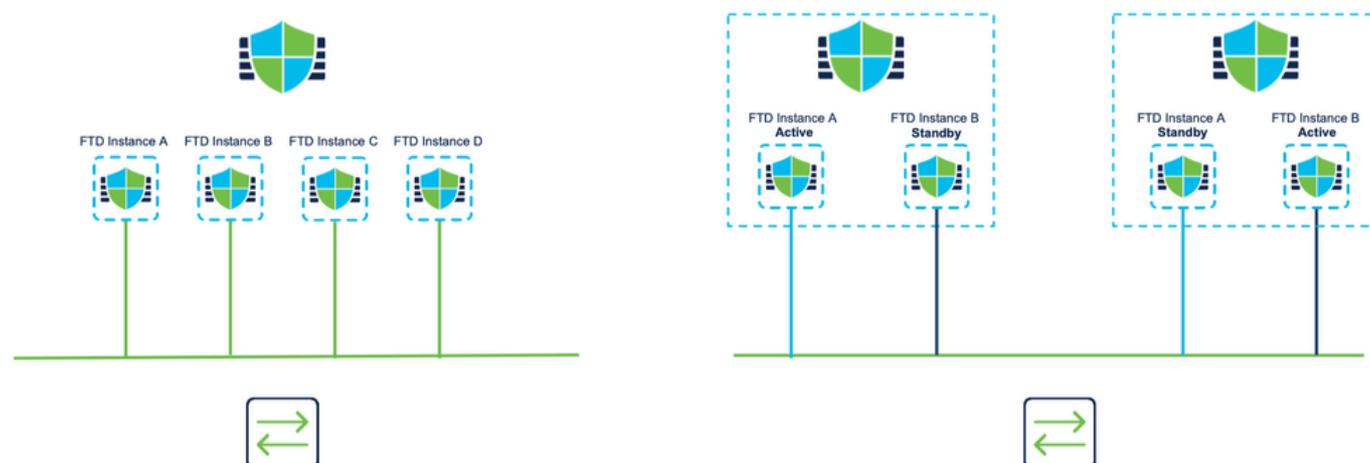
<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/threat-defense/use-case/multi-instance-sec-fw/multi-instance-sec-fw.html>

Opções de interface e alta disponibilidade

Opções de interface



Independente ou alta disponibilidade



Aproveitando as interfaces de gerenciamento duplas

- Como o 4200 no modo nativo, as duas portas de gerenciamento físico são fornecidas para suportar redundância de interface para tráfego de gerenciamento ou para suportar interfaces separadas para gerenciamento e eventos.

- Os dispositivos 9300 e 4100, assim como o 4200 Series, têm interfaces de gerenciamento duplas. A segunda interface de gerenciamento, Gerenciamento 1/2, é destinada a ser usada para eventos.
- No modo de várias instâncias (também conhecido como "contêiner"), você pode configurar essa interface na CLI do Threat Defense em cada instância. Atribua um endereço IP na mesma rede para cada instância.
- Quando no modo de contêiner, cada instância de FTD tem interfaces de Gerenciamento 1/1 e Gerenciamento 1/2 automaticamente atribuídas a ela.
 - A segunda interface de gerenciamento é desativada por padrão.
 - Não é possível configurar o Management1/2 usando o FMC; você precisa configurá-lo por meio do FTD CLISH (no 9300/4100, que, por outro lado, é feito na CLI FXOS). Use este comando com o tipo de endereço IP, endereço, sub-rede e rota estática desejados:

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.