

# FTD 7.6搭載Firepower 4200のコンテナ ( MIモード ) への変換

## 内容

---

### [はじめに](#)

#### [前提条件、サポートされるプラットフォーム、ライセンス](#)

[最低限のソフトウェアおよびハードウェアプラットフォーム](#)

[ライセンス](#)

[使用するコンポーネント](#)

### [背景説明](#)

[最新情報](#)

[FTDマルチインスタンスをサポートするプラットフォーム](#)

[3100シリーズと4200シリーズの違い](#)

[サポートされる展開](#)

### [機能説明とウォークスルー](#)

[4200シリーズインスタンスの仕様](#)

[最大インスタンスサポート](#)

[FTDインスタンスのサイズ](#)

[Lina \( データプレーン \) Snortコア割り当て](#)

### [設定](#)

[設定の概要](#)

[FMCで4200シリーズをマルチインスタンスモードに変換](#)

[単一のデバイスの変換](#)

[複数のデバイスを変換する \(一括変換\)](#)

[進行状況の監視と完了](#)

### [FMCシャーシの概要ページ](#)

[FMCシャーシ概要ページの概要](#)

[ChassisページのSummaryタブセクション](#)

### [インターフェイスの管理](#)

[「インタフェース」タブの要約](#)

[物理インターフェイス設定の変更](#)

[サブインターフェイスの管理](#)

[EtherChannelの管理](#)

[デバイス設定の同期](#)

### [Netmodホットスワップ/ブレイクアウトサポート](#)

[4200ネイティブはEPMホットスワップおよびブレイクアウトをサポート](#)

[OIR: EPMの有効化/無効化の確認](#)

[EPM使用可能完了: インタフェース通知を受信しました](#)

[EPMインタフェース変更通知](#)

[シャーシページのブレイク/参加オプション](#)

[ブレイク/ジョイン後のインターフェイスの変更](#)

[インターフェイス変更によるインスタンスへの影響](#)

## [インスタンス管理](#)

[インスタンスの作成](#)

[インスタンスの編集](#)

[インスタンスの削除](#)

## [SNMP の設定 \( SNMP Configuration \)](#)

### [シャーシのインポート/エクスポート](#)

[設定のエクスポート](#)

[設定のインポート](#)

[シャーシのインポート/エクスポートに関する注意事項](#)

### [シャーシプラットフォーム設定ポリシー](#)

[シャーシプラットフォームの設定 : DNS](#)

[シャーシプラットフォームの設定 : SSH](#)

[シャーシプラットフォームの設定 : SSHアクセスリスト](#)

[シャーシプラットフォームの設定 : 時刻の同期](#)

[Management CenterからのNTP](#)

[カスタムNTPサーバ](#)

[シャーシプラットフォームの設定 : タイムゾーン](#)

[シャーシプラットフォーム設定 : Syslog](#)

[シャーシプラットフォームの設定 : 保存と展開](#)

### [シャーシの登録解除](#)

### [マルチインスタンスからネイティブモードへの変換](#)

### [FMC Rest API](#)

[ネイティブからマルチインスタンスへの変換のためのREST API](#)

[シャーシ管理用REST API](#)

[Netmods \( ネットワークモジュール \) 管理用のREST API](#)

[インスタンス管理用REST API](#)

[SNMP管理用REST API](#)

[要約を取得するREST API](#)

[インターフェイス管理用REST API](#)

[物理インターフェイスの更新](#)

[サブインターフェイスの設定](#)

[EtherChannelインターフェイスの設定](#)

[REST APIのBreak/Joinインターフェイス](#)

[インターフェイス切断用のRESTフロー](#)

[インターフェイス結合のためのRESTフロー](#)

[デバイスREST APIの同期](#)

### [トラブルシューティング/診断](#)

[EXOSロギング](#)

[FMCロギング](#)

[シャーシのトラブルシューティング](#)

### [トラブルシューティングの手順に関する問題の例](#)

[FMCでのシャーシ障害の自動登録](#)

[問題のトラブルシューティング](#)

[FMCにおけるインスタンスの自動登録](#)

[問題のトラブルシューティング](#)

[FMCでのネイティブデバイス登録](#)

[参考リンク](#)

[インターフェイスオプションとハイアベイラビリティ](#)

[インターフェイスオプション](#)

[スタンドアロンまたは高可用性](#)

[デュアル管理インターフェイスの活用](#)

---

## はじめに

このドキュメントでは、FTD 7.6を搭載したFirepower 4200ファイアウォールシリーズでコンテナ (マルチインスタンスモード) を設定する方法と関連する詳細について説明します。

## 前提条件、サポートされるプラットフォーム、ライセンス

### 最低限のソフトウェアおよびハードウェアプラットフォーム

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

---

注意：マルチインスタンスは、どのプラットフォームでもFDMではサポートされていません。

---

## ライセンス

- 機能ライセンスは各インスタンスに手動で割り当てられますが、使用するライセンスは4200シリーズのデバイスごとに機能ごとに1つだけです。
  - たとえば、3つのFTDインスタンスを持つ1つの4200シリーズの場合、同じFMC上で使用すれば、使用中のインスタンス数に関係なく、必要なURLライセンスは1つだけです。
- すべてのライセンスは、同じFMC上にある場合、4200シリーズのデバイスごとに消費され、コンテナインスタンスごとに消費されることはありません。したがって、4200シリーズデバイス上のすべてのインスタンスでは、ライセンスの実装のために同じFMCを使用することを推奨します。

## 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

- FTDでは、3100モデル（および9300および4100シリーズ）でマルチインスタンス(MI)がすでにサポートされていますが、4200シリーズではサポートされていません。
- 4200モデルは、FMCのネイティブモードでのみサポートされています。
- 4200の7.4.xには、複数のインスタンスを作成する機能はありません。
- 3100でのマルチインスタンス(MI)は7.4.1でサポートされています。
  - インスタンスはFMCを使用して作成および管理できます（FCMを使用する必要がある9300および4100シリーズとは異なります）。
  - FXOSは、MIモードのときは、FMCのUpgrade Chassis GUIを使用して更新できます。
  - MIモードへの変換はCLIを介して行われます。

## 最新情報

- 4200シリーズでは、MIインスタンスをプロビジョニングおよび管理できます。
- FMC:4200シリーズ（MIモード）およびFTDインスタンス用の単一管理ソリューション
- 3100および4200シリーズのデバイスでは、FMC上でネイティブデバイスをMIモードにシングルおよびバルク変換できます。
- ターゲット市場：エンタープライズ/大規模企業 – インターネットエッジ、データセンター

## FTDマルチインスタンスをサポートするプラットフォーム

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

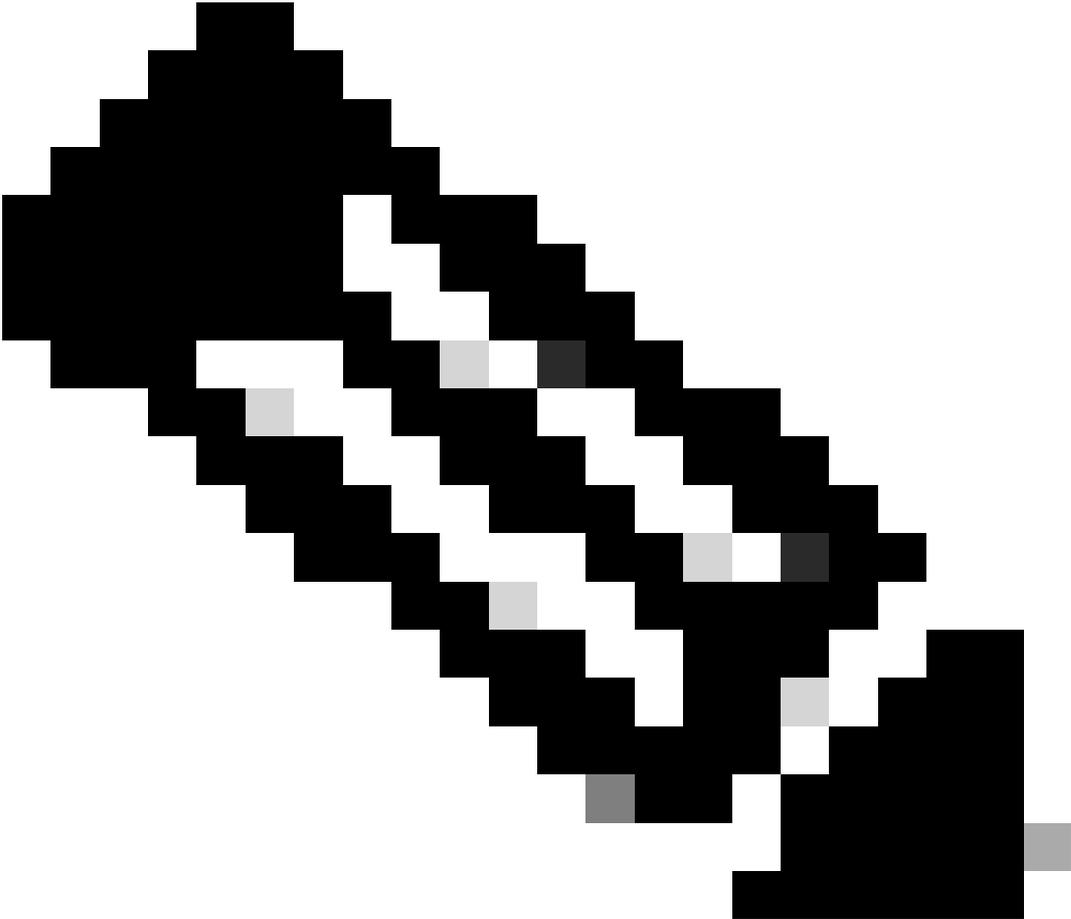
## 3100シリーズと4200シリーズの違い

- 4200には2つの管理インターフェイスがあり、一方を管理用、もう一方をイベント用に使用できます。
  - Management1/1インターフェイスとManagement1/2インターフェイスの両方が、すべてのFTDコンテナインスタンスにブートストラップされます。
  - 一方または両方の管理インターフェイスをMIモードで使用できます。
    - Management1/1 ( 管理とイベントの両方 )、または
    - Management1/1は管理に使用され、Management1/2はイベントに使用されます。この場合、次のようになります。
      - Management 1/2インターフェイスを使用してトラフィックをルーティングするには、スタティックルートを定義する必要があります。
- サイズが大きいため、3100よりも多くのインスタンスを4200で作成できます。

## サポートされる展開

- スタンドアロンFTDインスタンスで4200シリーズ ( MIモード ) を管理
- HA FTDインスタンスを使用した4200シリーズ ( MIモード ) の管理\*

---



注:FPR4100シリーズでは、FTD-HAの場合、プライマリノードとセカンダリノードは2つの異なる4200シリーズ ( MIモード ) デバイス上にある必要があります。また、このリリースではMIクラスタリングはサポートされていません。

---

## 機能説明とワークスルー

7.6.0でのマルチインスタンス設定の変更：

- MIモードでの4200シリーズのサポート
- 3100シリーズのMIモード管理に関連するFMCの変更：
  - FMCでのネイティブモードからMIモードへのデバイスの変換
  - デバイスがMIモードに変換できるかどうかを確認する準備状況のチェック
  - 変換後にFMCでFTDインスタンスを自動登録

4200シリーズインスタンスの仕様

## 最大インスタンスサポート

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

インスタンス密度は、次の2つの主要な要因によって決まります。

1. 特定のプラットフォーム上のCPUコアの量とディスク容量
2. インスタンスにプロビジョニングできるリソースの数。最小のインスタンスサイズには、3つの物理CPU ( 6つの論理 ) コアと48 GBのディスク領域が必要です。

## FTDインスタンスのサイズ

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

## Lina ( データプレーン ) Snortコア割り当て

	4215	4225	4245			
インスタンスサイズ	データプレーンコア	Snortコア	データプレーンコア	Snortコア	データプレーンコア	Snortコア

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

## 設定

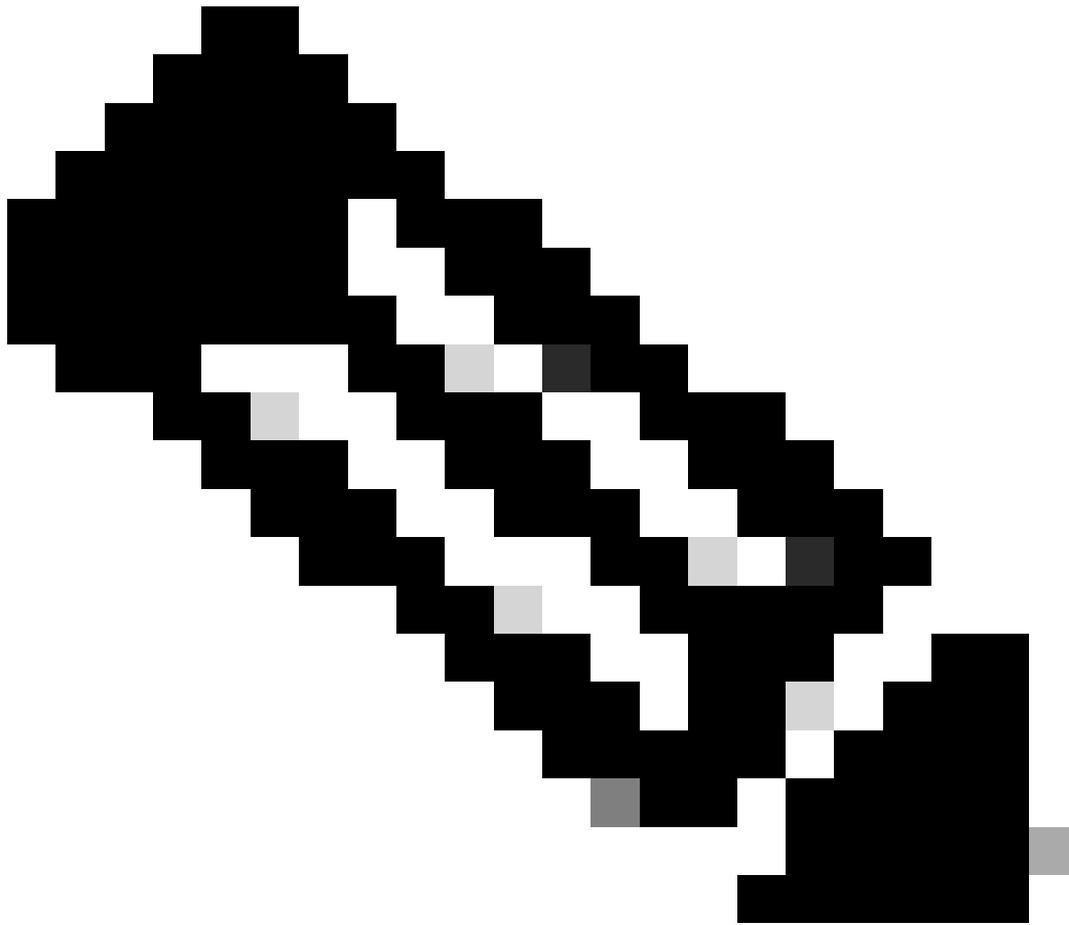
### 設定の概要

1. FMCに4200シリーズ ( ネイティブモード ) デバイスを登録します。
2. 新しいFMCで、デバイスを選択し、ネイティブからMIモードに変換します。
3. 新しいMIシャーシは、変換後にFMCに自動登録されます。
4. 物理インターフェイスを更新します。
5. FTDインスタンスを作成し、インターフェイスを割り当てます。
6. FMCからポートチャンネルとサブインターフェイスを作成/更新/削除します。
7. プラットフォームの設定を行います。
8. 設定変更をデバイスに導入します。
9. FTDインスタンスがFMCに自動登録されます。

### FMCで4200シリーズをマルチインスタンスモードに変換

デフォルトでは、4200はネイティブモードです。FMCで4200シリーズをマルチインスタンスモードに変換するには

1. デバイスに接続し、マネージャを作成します ( すでに文書化されています ) 。
2. ネイティブデバイスをFMCに登録します ( すでに文書化されています ) 。
3. FMCを使用したマルチインスタンスへの変換
4. FMCで、マルチインスタンスに変換する必要があるデバイスを選択し、変換をトリガーします。1つまたは複数のデバイスを選択できます。

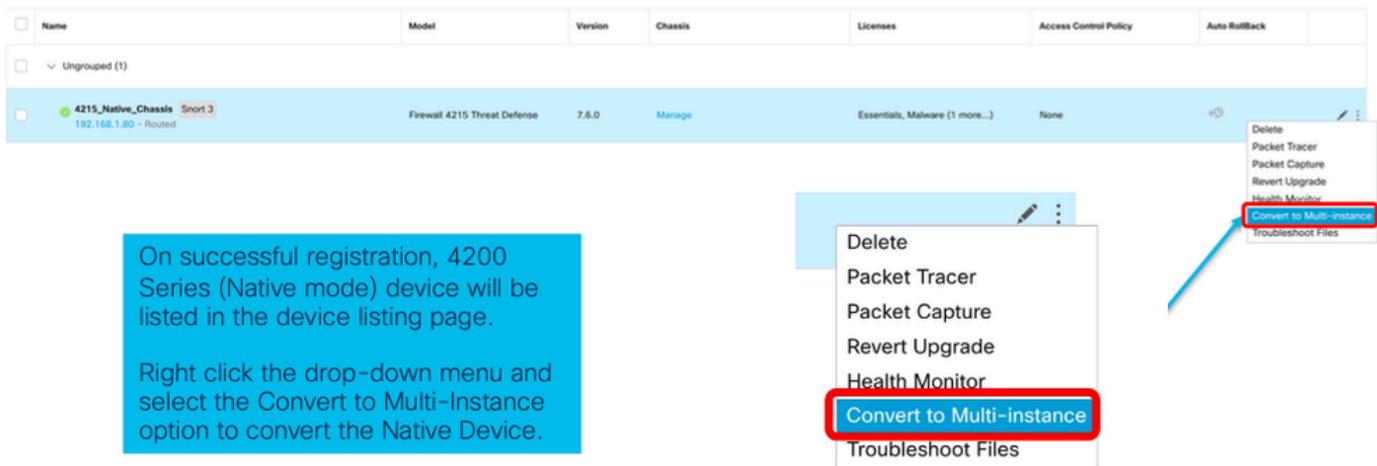


注：ネイティブモードからMIモードに切り替えると、シャーシのすべての設定がリセットされます。MIモードからネイティブモードへの変換は、引き続きCLIを介して行われます。

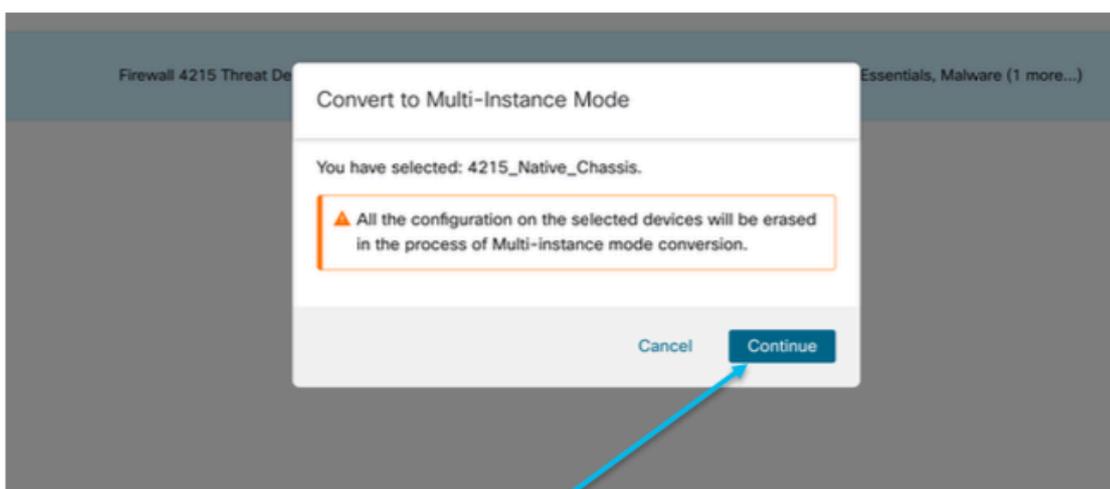
---

## 単一のデバイスの変換

1. 変換を開始するには、デバイス>デバイス管理に移動します。



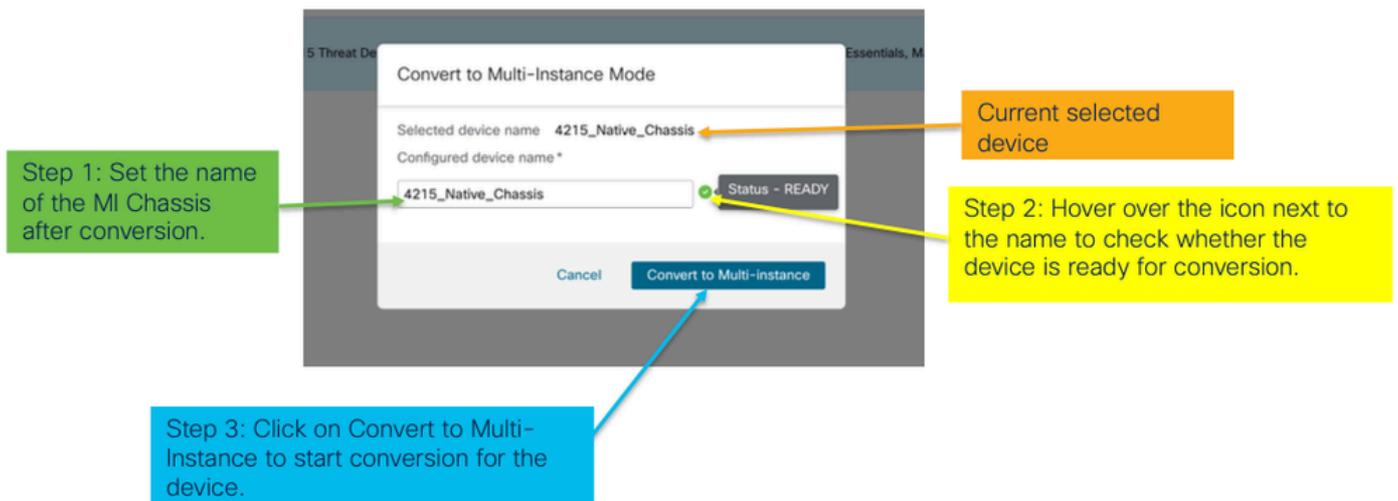
2. 選択したデバイスを検証し、Continueをクリックします。



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

選択したデバイスの検証

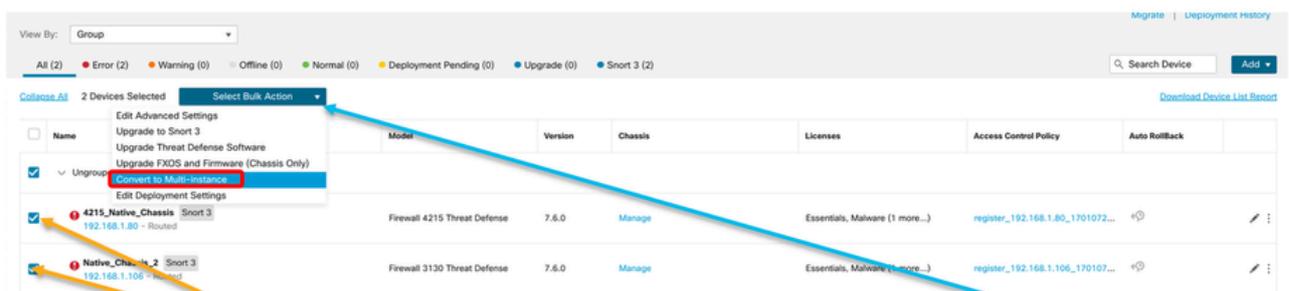
3. 準備状況の確認と初期変換：



準備状況のチェック

## 複数のデバイスを変換する（一括変換）

### 1. デバイスの選択：



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. 選択の確認：

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. 準備状況の確認と変換の開始 :

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.

### 進行状況の監視と完了

#### 1. 変換の開始通知 :

Firewall Management Center  
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

View By: Group

All (1) Error (1) Warning (0) Offline (0) Normal (0) Deployment Pending (0) Upgrade (0) Snort 3 (1)

Name	Model	Version	Chassis
192.168.1.80 192.168.1.80 - Routed	Firewall 4215 Threat Defense	7.6.0	N/A

Deployments Upgrades Health **Tasks**

- Switch Mode  
Conversion of 192.168.1.80 in progress  
Status: Fetching configuration data from the device 9s
- Switch Mode  
Chassis Conversion  
Chassis Conversion started for 1 device(s) 10s

No more older tasks

Remove completed tasks

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

## 2. シャーシの自動登録 :

Firewall Management Center  
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

View By: Group

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

Name	Model	Version	Chassis
192.168.1.80 192.168.1.80	Firewall 4215 Threat Defense Multi-Instance Supervisor	7.6.0	Manage

Deployments Upgrades Health **Tasks**

- Discovery  
192.168.1.80 - Discovery from the device is successful. 15s
- Register  
Registration  
192.168.1.80: Successfully registered 19s
- Switch Mode  
Conversion of 192.168.1.80 in progress  
Status: Trying chassis registration for 192.168.1.80, try 1 of 3 times 14m 25s
- Register  
Unregistration  
Unregistration completed.  
192.168.1.80 - Did not update device 7s

Remove completed tasks

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. 変換後の通知 :

Firewall Management Center  
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

View By: Group

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

Name	Model	Version	Chassis
192.168.1.80 192.168.1.80	Firewall 4215 Threat Defense Multi-Instance Supervisor	7.6.0	Manage

Deployments Upgrades Health **Tasks**

- Switch Mode  
Chassis Conversion Summary  
Success: 1  
Failed: 0 14m 32s
- Switch Mode  
Conversion of 192.168.1.80 is successful  
It is added with name 192.168.1.80 14m 31s
- Discovery  
192.168.1.80 - Discovery from the device is successful. 15s
- Register  
Registration  
192.168.1.80: Successfully registered 19s

Remove completed tasks

Successful Conversion Notification with number of devices converted successfully.

4200シリーズ ( MIモード ) デバイスをリストした結果のデバイス管理ページ :

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

## FMCシャーシの概要ページ

### FMCシャーシ概要ページの概要

FMC Chassis Overviewページには、4200シリーズ ( MIモード ) デバイスの完全な要約が表示されます。内容は以下を含みます。

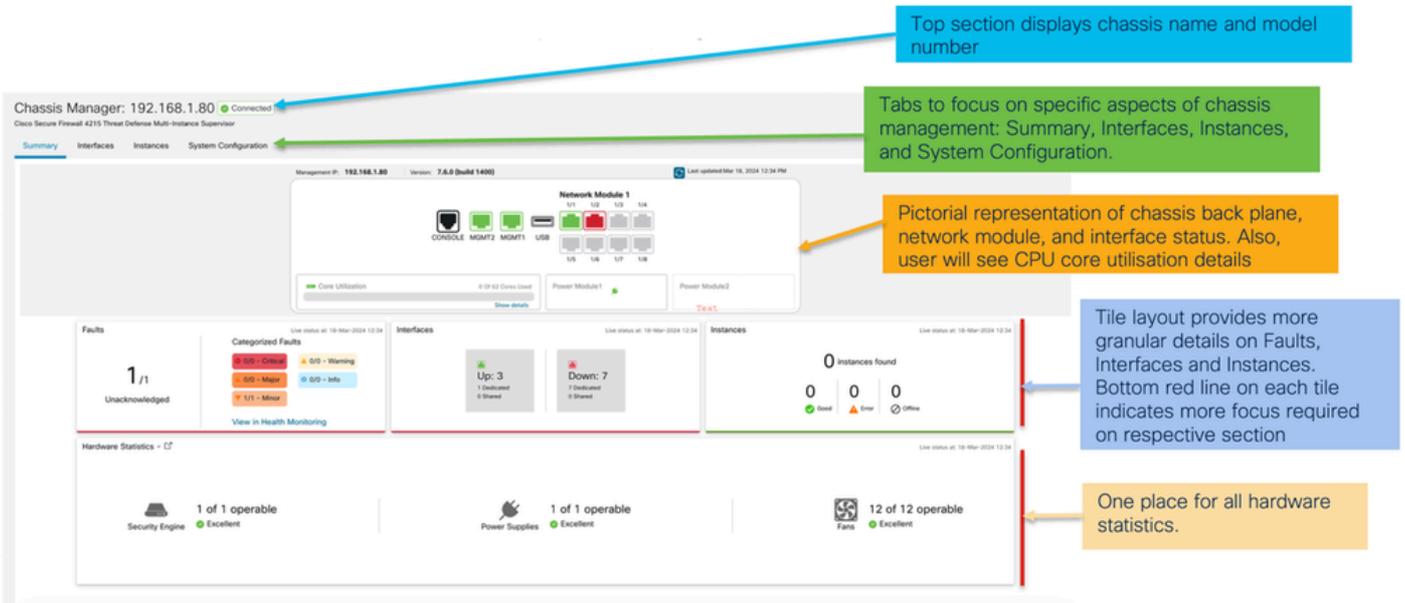
- 利用可能なネットワークモジュールを含む、デバイスの背面パネルの画像。
- 障害の概要、およびその重要度。
- インターフェ이스の概要、ステータス。
- FTDインスタンスのサマリー、ステータス。
- ハードウェアの統計情報 ( ファン、電源、メモリ、CPU使用率、ストレージなど ) 。

Manageをクリックして、Chassis Overviewに移動します。

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

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

シャーシページの概要タブ :

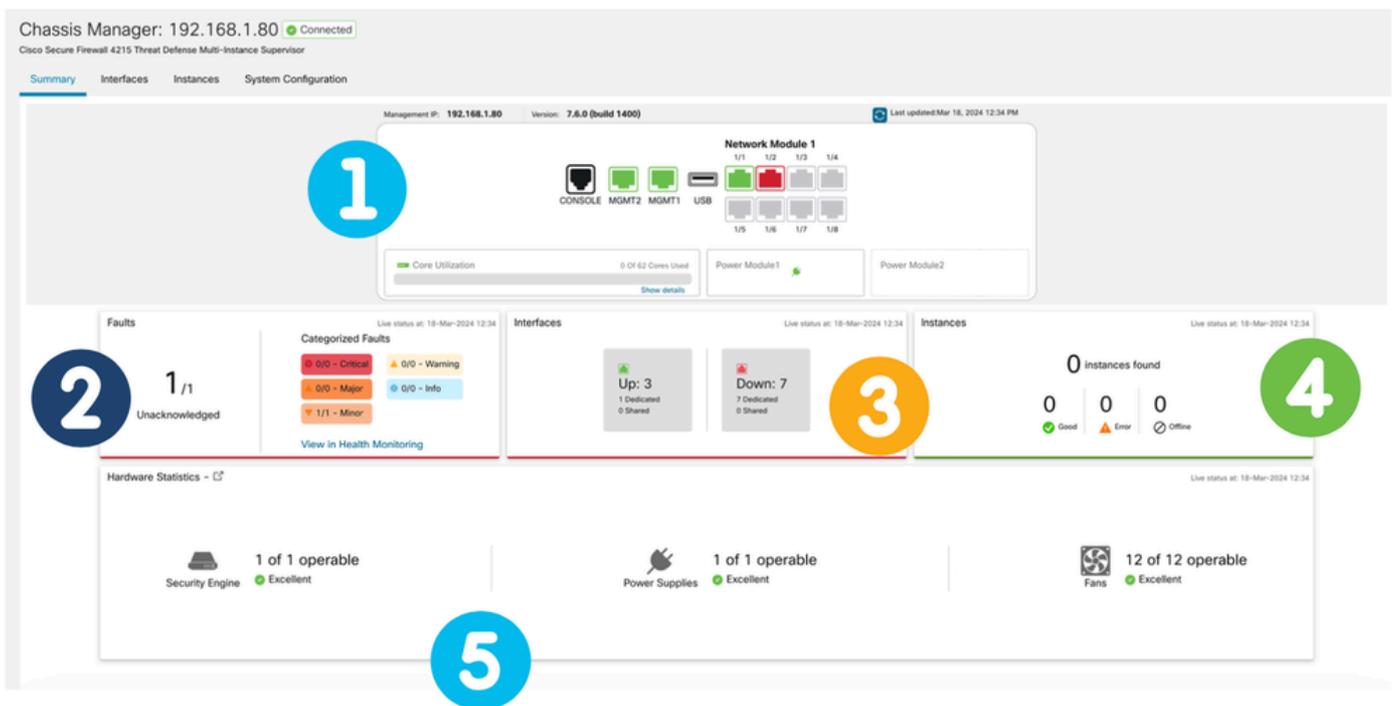


## ChassisページのSummaryタブセクション

[概要]タブにはセクションがあります。クリックして詳細を表示：

- バックプレーン
- 障害
- インターフェイス
- インスタンス
- ハードウェア統計

セクションは、次の図に示すように番号別にマッピングされます。



1. バックプレーンビュー：



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.

Tooltip for Core Utilization:

Name	Operational state	Management IP	Cores used
WA_instance_1	Installing	192.168.0.112	6

## 2. 障害セクション :



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

Live status at: 27-Nov-2023 04:37

Categorized Faults:

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

View in Health Monitoring

Tooltip for Unacknowledged Faults:

List of Top 1 Faults

- 0/0 - Minor
- either port 1/2 on fabric interconnect A oper state: link-down, reason: Down

View All Faults

View in Health Monitoring

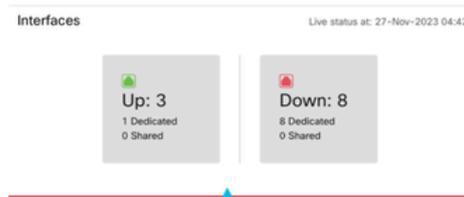
Click on 'View in Health Monitoring' to open a dialog that lists all faults in a table.

## 3. インターフェイスセクション :

Health: 4215\_WA\_chassis (Critical) Normal

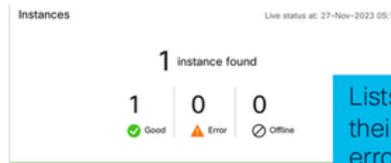
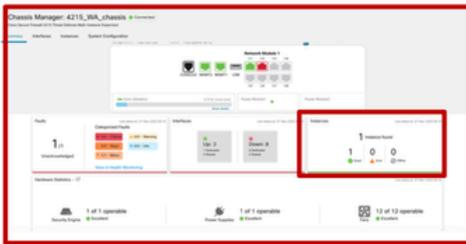
View System & Troubleshoot Details

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

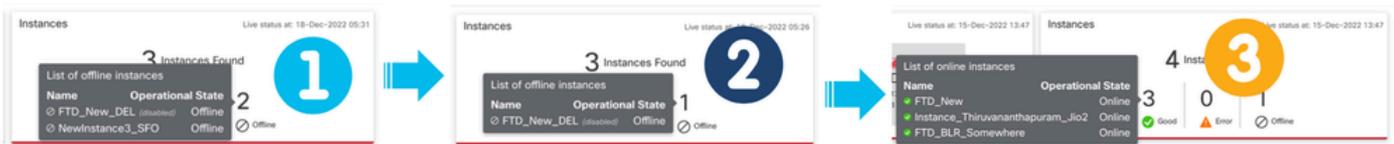


Lists number of interfaces that are operationally up and/or down. It also displays the of dedicated and shared interfaces.

#### 4. インスタンスセクション :



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



前の図に、オフラインからオンラインへのインスタンスの移行を示します。

- プロビジョニング後(1)
- インスタンスはオンラインになるまでオフラインである(2)
- 中間状態も反映される(3)

#### 5. ハードウェア統計 :

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.

## インターフェイスの管理

「インタフェース」タブでサポートされる操作：

- 物理インターフェイスのアップデート。
- サブインターフェイスの作成/更新/削除
- EtherChannelインターフェイスの作成、更新、削除
- インターフェイス設定を同期します。
- ネットワークモジュールのOIR。
- 物理インターフェイスの切断/結合。

「インタフェース」タブの要約

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

Interfacesタブのランディングページには、物理インターフェイス、サブインターフェイス、EtherChannel、EtherChannelサブインターフェイスなど、シャーシで管理されるすべてのタイプのインターフェイスが表示されます。

## 物理インターフェイス設定の変更

物理インターフェイスの次の属性を更新できます。

- 状態 (有効/無効)
- ポートタイプ (データ|データ共有)
- 管理デュプレックス
- 管理速度
- 自動ネゴシエーション

### 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

## サブインターフェイスの管理

Addボタンからサブインターフェイスオプションを選択して、新しいインターフェイスを追加します。

サブインターフェイスの次のアトリビュートを変更できます。

- 親インターフェイス
- ポートタイプ ( データ/データ共有 )
- サブインターフェイスID
- VLAN ID

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

## EtherChannelの管理

新しいEtherChannelインターフェイスを作成するには、Addボタンの下にある「EtherChannel interface」を使用します。

EtherChannelに設定できる属性は次のとおりです。

- イーサチャネルID
- ポートタイプ ( データ/データ共有 )
- メンバーインターフェイス
- 管理速度
- 管理デュプレックス
- LACPモード
- LACPレート
- 自動ネゴシエーション

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

Selected Interfaces (0)

### Add EtherChannel Interface

**Interfaces** Configuration

Admin Duplex  
Full

Admin Speed  
1Gbps

LACP Mode  
Active

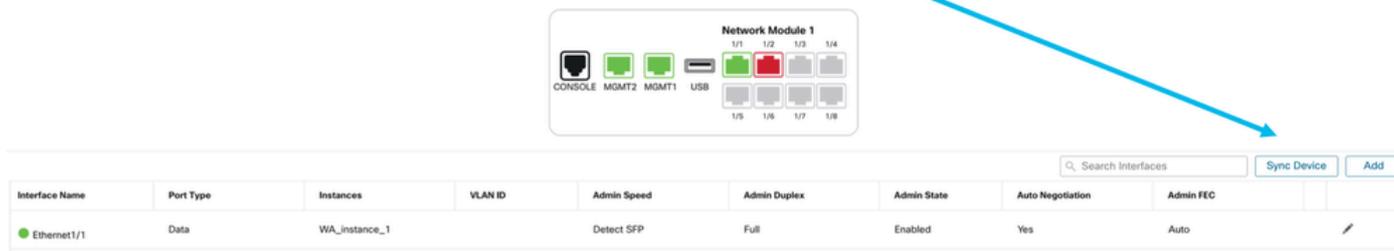
LACP Rate  
Default

Auto Negotiation

## デバイス設定の同期

FMCの設定とデバイスの設定が同期されない場合があります。1つのケースは、ユーザがnetmodを削除または挿入した場合です。このような場合、同期デバイスを実行できます。

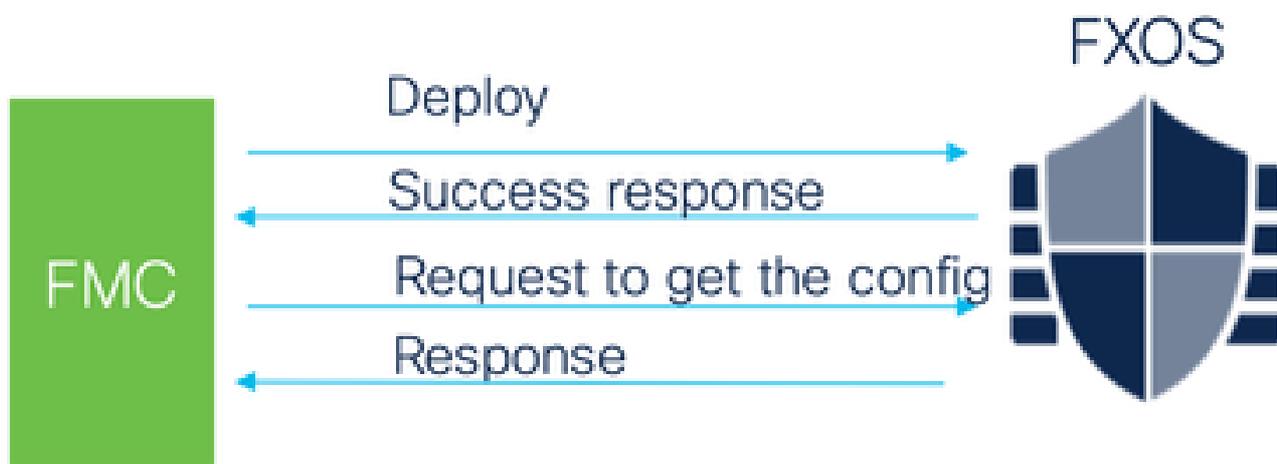
Click "Sync Device".



## Netmodホットスワップ/ブレイクアウトサポート

ドキュメントで使用されている「ホットスワップ」は、他の内部ドキュメントでは活性挿抜(OIR)と呼ばれています。

ネットワークモジュールのイネーブル/ディセーブル時、またはインターフェイスのブレイクや参加の際に、すぐに展開されます。マルチインスタンスモードは、ネイティブモードの4200シリーズと同じです。



FMCは、受信した応答を現在の設定と比較し、ユーザが確認応答するためのインターフェイス変更通知を作成します。

4200ネイティブはEPMホットスワップおよびブレイクアウトをサポート

EPM OIRおよびブレイクアウトは、スタンドアロンのネイティブモードのセキュアファイアウォール4200シリーズのスタンドアロンですでにサポートされています。

4200シリーズEPM OIRおよびブレイクアウトFMCドキュメント：

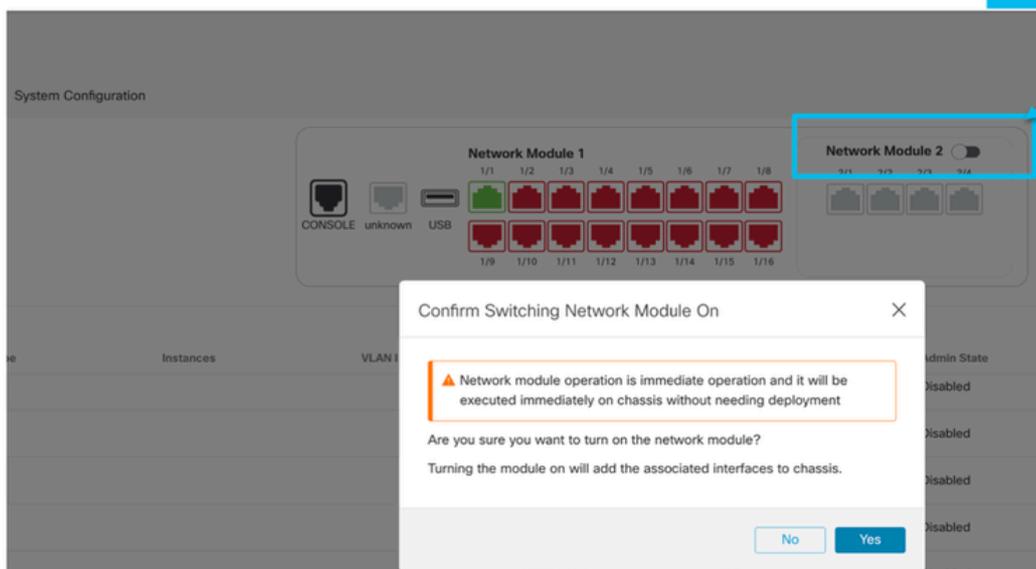
- <https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/4200/fw-4200->

<install/m-overview.html>

## OIR: EPMの有効化/無効化の確認

ユーザがモジュールの有効化に切り替えると、誤ってクリックしていないことを確認する警告が表示されます。

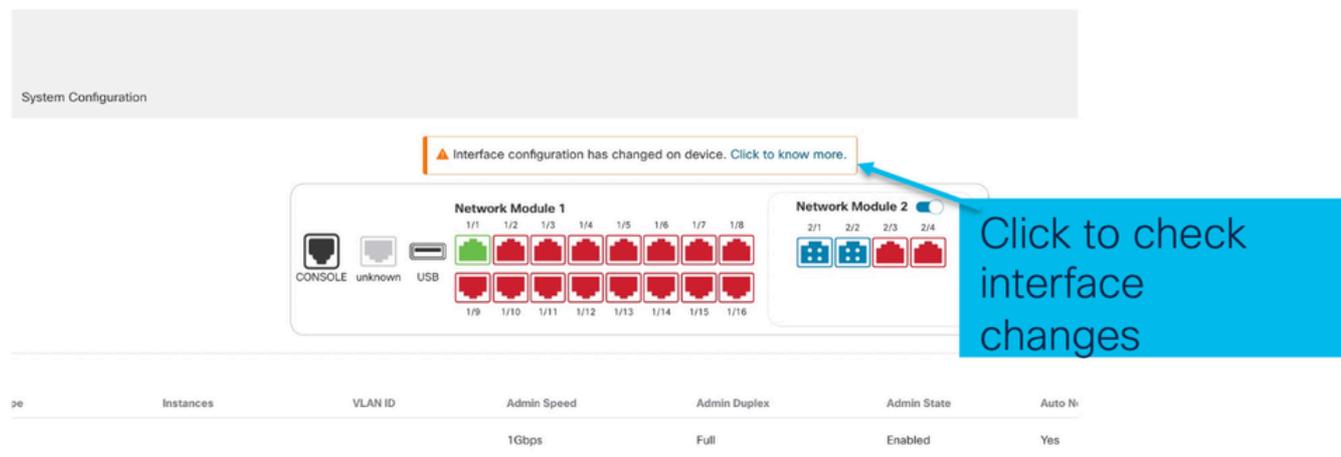
Toggle option to enable/disable module



## EPM使用可能完了：インターフェイス通知を受信しました

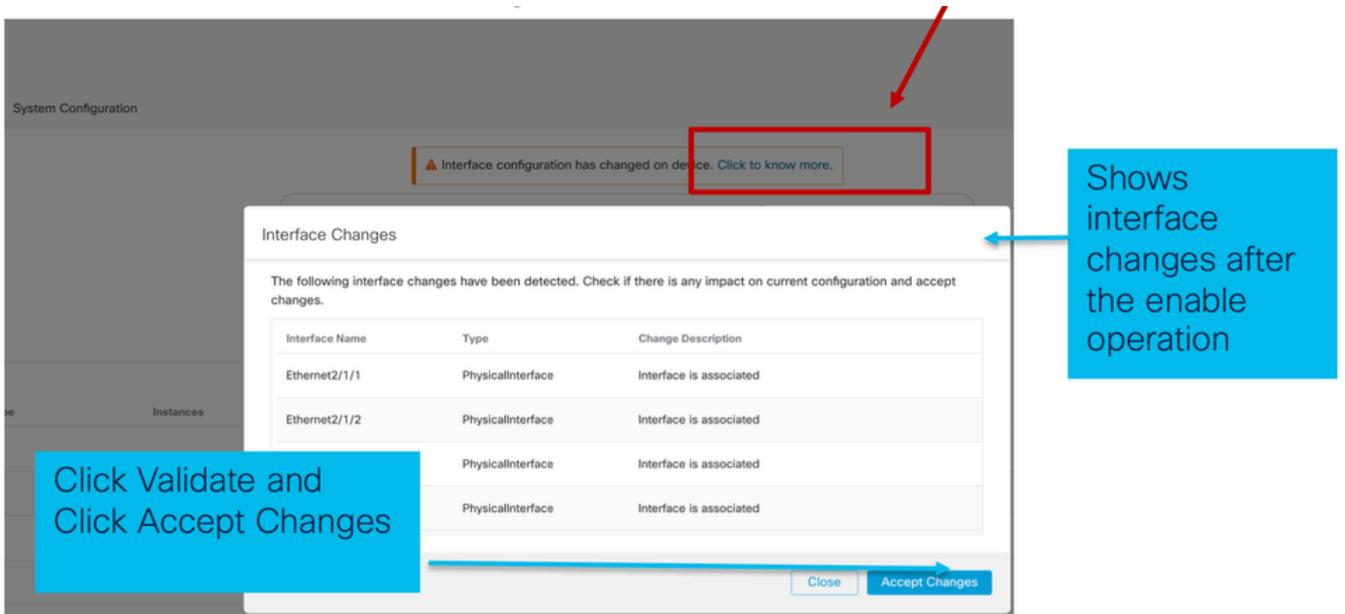
- EPMを有効にすると、新しいインターフェイスがデバイスに関連付けられます。
- FMCは、関連付けられたインターフェイスに関する通知を受信します。
- FMCで、ユーザは変更を受け入れる必要があります。

次のスクリーンショットは、関連付けられたインターフェイスを表示するオプションを示しています。

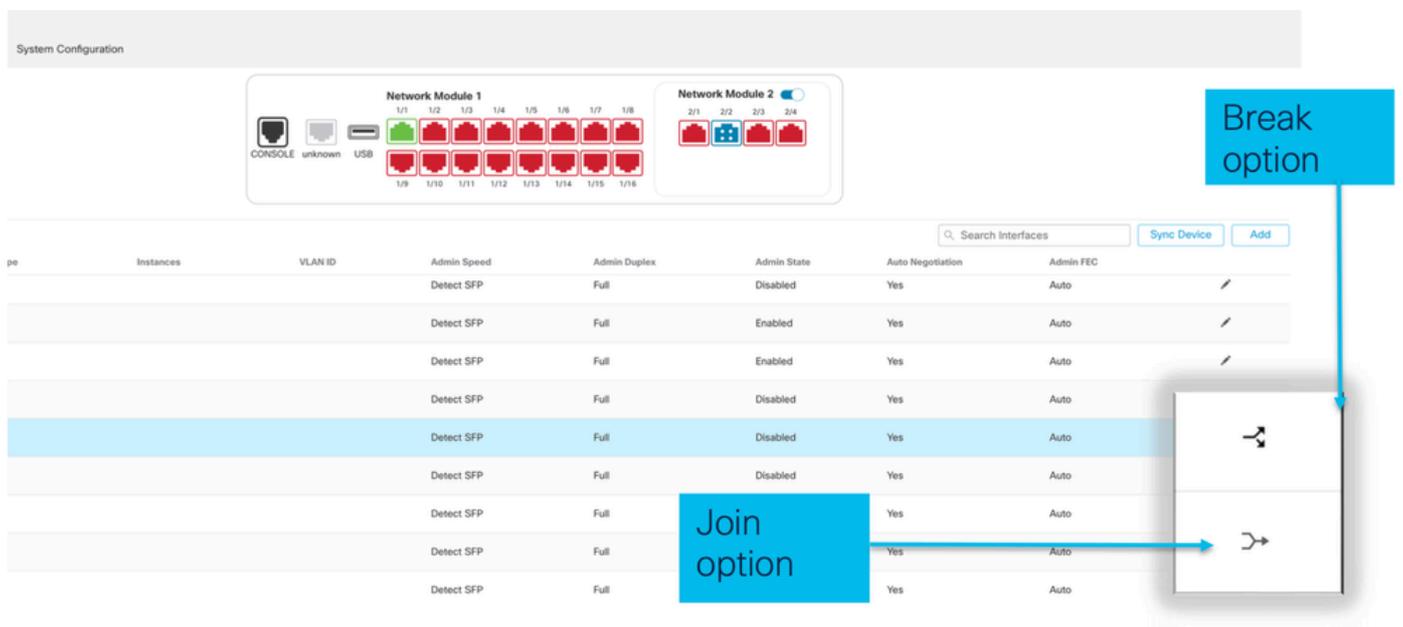


## EPMインターフェイス変更通知

「インターフェースのリスト」ページには、EPMが使用可能なときに追加されるインターフェースがリストされます。詳細を確認するには、ここをクリックして[インターフェイスの変更]ダイアログを開きます。  
 保存後に詳細が利用できないかどうかを確認するには、ここをクリックします。



## シャーシページのブレイク/参加オプション



インターフェイスのブレイク確認ウィザードは、ブレイクオプションがトリガーされると起動します。

# 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

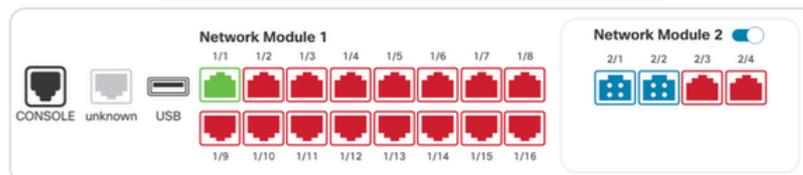
No

インターフェイスのブレイクが確認された後、シャーシのページにインターフェイスのアップデート通知が表示されます。

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

System Configuration

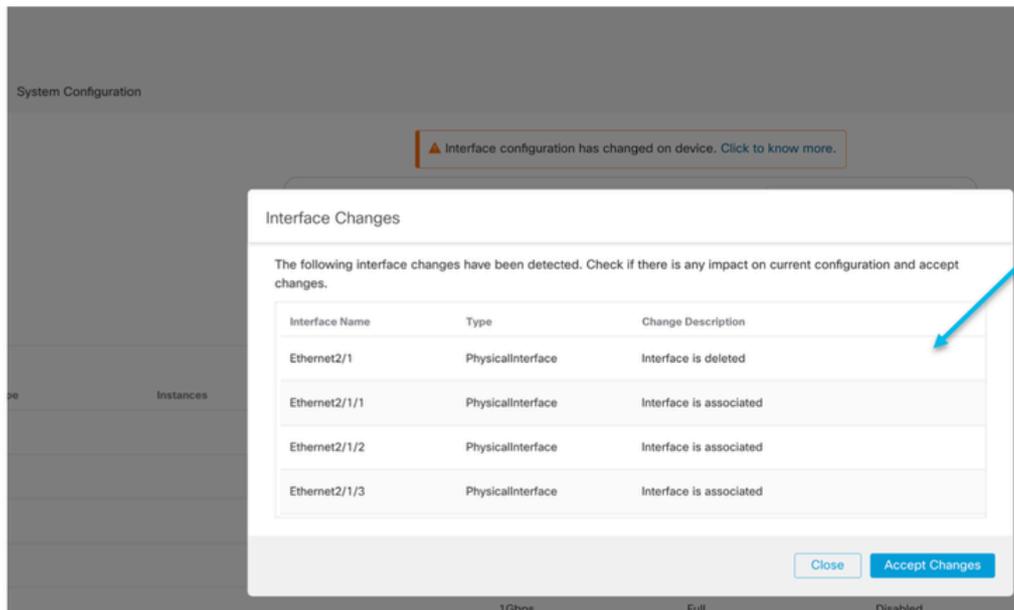
⚠ Interface configuration has changed on device. Click to know more.



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

## ブレイク/ジョイン後のインターフェイスの変更

Accept Changesをクリックすると、使用するFMCで次のインターフェイスが使用可能になります。



Shows interface changes after the break operation

## インターフェイス変更によるインスタンスへの影響

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"><li>Validation error will be thrown to initiate such operation</li><li>User needs to unassign the interfaces from the Logical Device before initiating Break/Join operation</li></ul>

## インスタンス管理

Instance Managementでは、次のことが可能です。

- 4200シリーズ ( MIモード ) デバイス上の既存のすべてのFTDインスタンスとその詳細を表示します。
- 目的のCPUコアとソフトウェアバージョンでFTDインスタンスを作成/更新します。

- 既存のFTDインスタンスを削除します。
- ユーザはFTDポリシー ( FTDインスタンスのアクセスポリシーとプラットフォーム設定ポリシー ) を選択できます。
- FTDインスタンスがオンラインになったら、それをFMCに自動登録します。

View By: Group

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

Search Device Add

Collaps All Download Device List Report

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (1)							
4215_WA_Chassis 192.168.1.80	Firewall 4215 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	N/A	N/A	N/A	

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

## インスタンスの作成

Add Instanceをクリックしてウィザードを起動します。

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

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

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

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

ステップ 1 : 契約 :

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

## ステップ 2 :

- インスタンス設定の基本 :

Add Instance

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

Display Name \*  
WA\_instance\_1

Device Version \*  
7.6.0.1208

Resource Profile \*  
Default-Small

Management IP \*  
192.168.1.81

Network Mask \*  
255.255.255.0

Network Gateway \*  
192.168.1.254

Firewall Mode \*  
Routed

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.

- インスタンス構成IP:

**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

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

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

### ステップ 3 : インターフェイス割り当て :

**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.

### ステップ 4 : デバイス管理 :

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.

## ステップ 5 : 要約 :

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.

設定を完了するには、保存して展開します。

Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy

Chassis Manager: 4215\_WA\_Chassis Connected You have unsaved changes Save Cancel

Summary Interfaces Instances System Configuration

Name	Version	Resource Profile	Management IP	Management Gateway	Licenses
WA_Instance_1	7.6.0.1208	Default-Small	192.168.1.81	192.168.1.254	Carrier, ... Policy1 N.A

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

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

Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy

Chassis Manager: 4215\_WA\_Chassis Connected

Instance configuration has changed. A deployment is required.

Summary Interfaces Instances System Configuration

Name	Version	Resource Profile	Management IP	Management Gateway
WA_Instance_1	7.6.0.1208	Default-Small	192.168.1.81	192.168.1.254

Advanced Deploy Deploy All Cancel

4215\_WA\_Chassis | Ready for Deployment

1 device is available for deployment

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

導入の成功後のFTDインスタンスの自動登録：

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.

Management Centerに登録されているインスタンス :

The screenshot shows the FMC Device Listing Page with a status bar at the top indicating: All (2), Error (1), Warning (0), Offline (0), Normal (1), Deployment Pending (1), Upgrade (0), Snort 3 (1). The table below lists the registered instances:

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.

### インスタンスの編集

鉛筆アイコンをクリックして、FTDインスタンスを編集します。

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.

### ステップ 1 : FTDインスタンスの編集 :

Edit Instance

1 Instance Configuration 2 Interface Assignment 3 Summary

Display Name \*  
WA\_instance\_1

Device Version \*  
7.6.0.1217

Admin State  Permit Expert mode for CLI

Resource Profile \*  
Default-Small

IPv4  IPv6  Both

IPv4

Management IP \*  
192.168.1.81

Network Mask \*  
255.255.255.0

Network Gateway \*  
192.168.1.254

Search Domain

QDN

Firewall Mode \*  
Routed

DNS Servers

Device SSH Password \*  
.....

Confirm Password \*  
.....

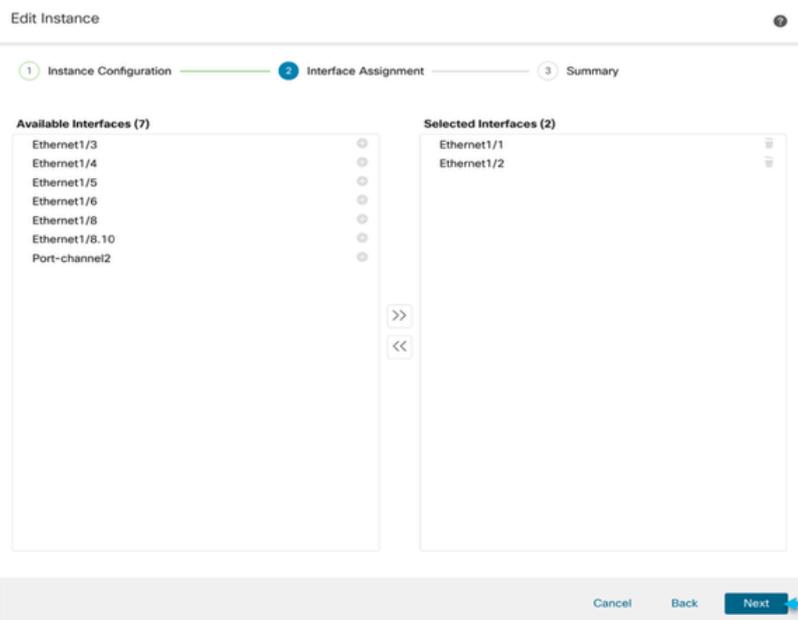
Cancel Next

The Edit Instance dialog is like the Create Instance wizard.

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

Click on the 'Next' button to edit interface assignments

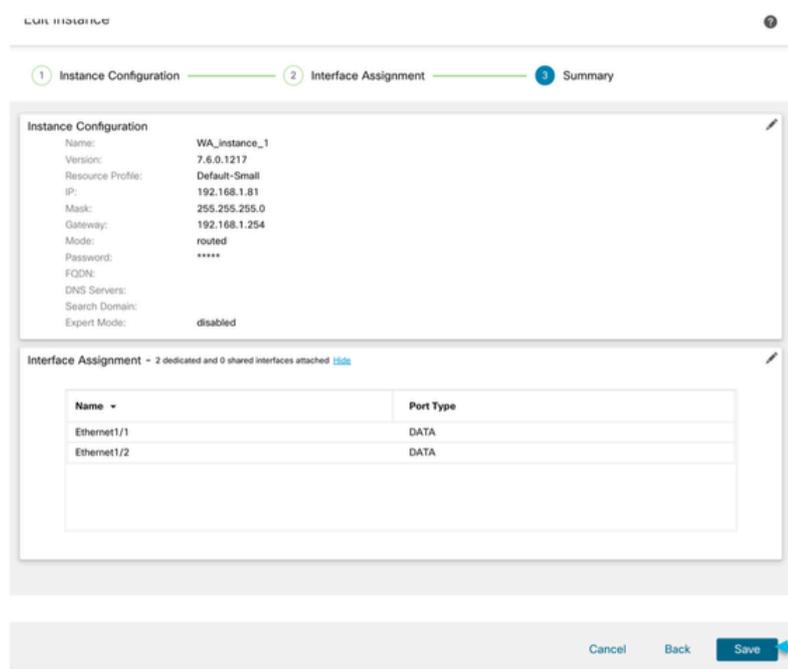
### ステップ2: インスタンスのインターフェイス割り当てを編集する :



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

### ステップ 3 : 編集インスタンスの概要 :

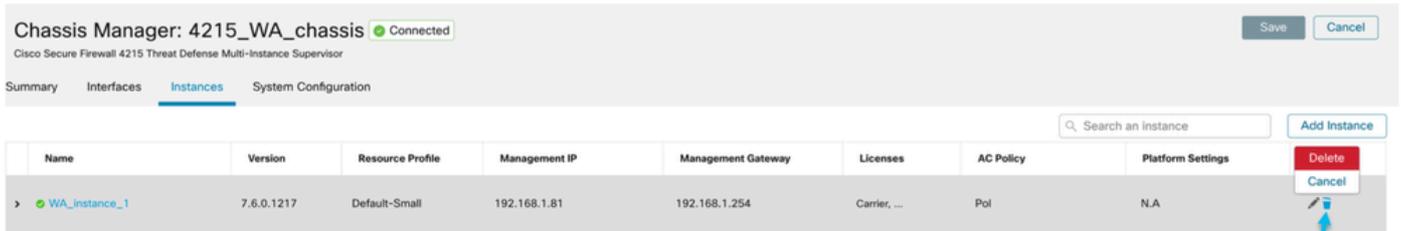


The last step of editing an instance is to view the summary of changes made to the instance.

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.

### インスタンスの削除



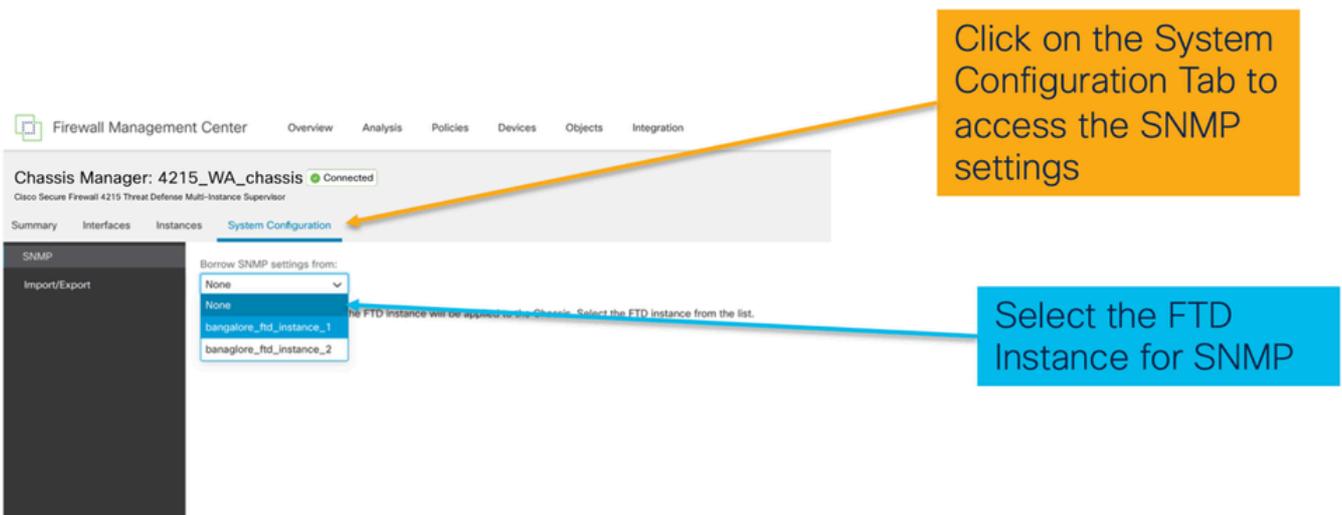
Use the Delete option (from the trash can icon) to delete an existing instance.

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.

## SNMP の設定 ( SNMP Configuration )

SNMPを設定するには、システム設定タブに移動します。



## シャーシのインポート/エクスポート

### 設定のエクスポート

Manage Chassis > System Configuration > Import/Exportの順に選択します。

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.

## 設定のインポート

Manage Chassis > System Configuration > Import/Exportの順に選択します。

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

## シャーシのインポート/エクスポートに関する注意事項

- シャーシ上の既存の設定はすべて、インポートされたファイル内の設定に置き換えられます。
- 構成がインポートされるプラットフォームソフトウェアのバージョンは、エクスポートされたバージョンと同じである必要があります。
- 設定をインポートするシャーシには、エクスポートを実行したときにインストールされたネットワークモジュールの数と同じ数のモジュールが必要です。
- 設定がインポートされるシャーシには、論理デバイス用に同じアプリケーションイメージがインストールされている必要があります。
- アプリケーション固有の構成設定はエクスポートされません。シャーシ構成のみがエクスポートされます。

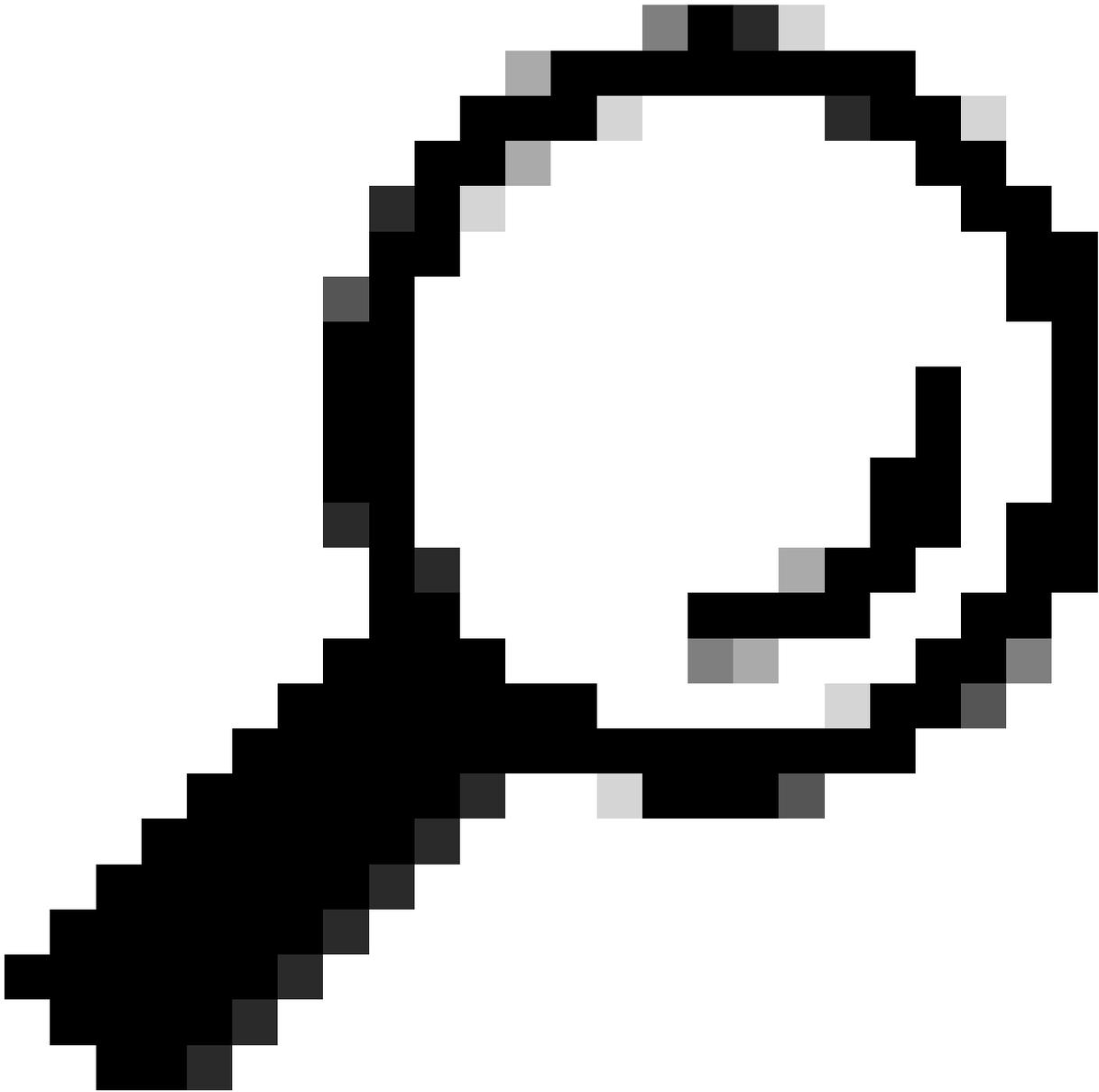
ートされます。

- FTDインスタンスのバックアップは個別に行う必要があります。

## シャーシプラットフォーム設定ポリシー

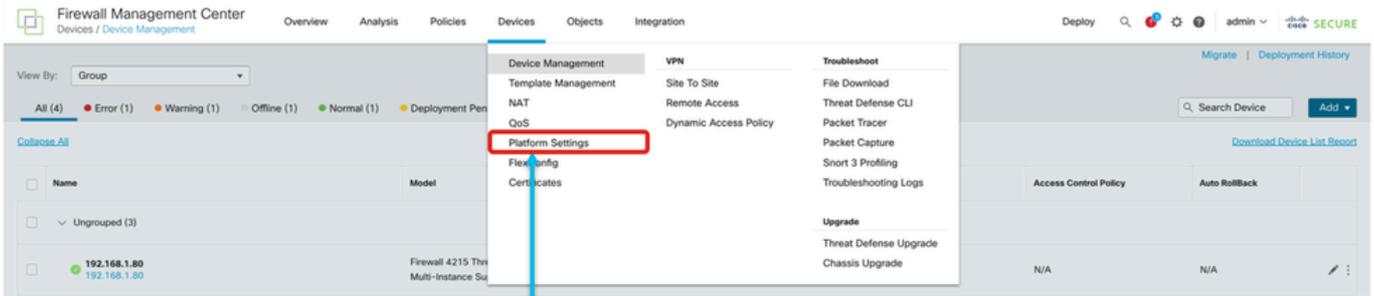
シャーシプラットフォーム設定ポリシーを使用すると、次のプラットフォーム固有の設定を行うことができます。

- 時刻同期(NTP)
- DNS
- Syslog
- タイムゾーン
- 新しい「Chassis Platform Setting」ポリシーを作成し、複数の4200シリーズ ( MIモード ) シャーシに割り当てることができます。



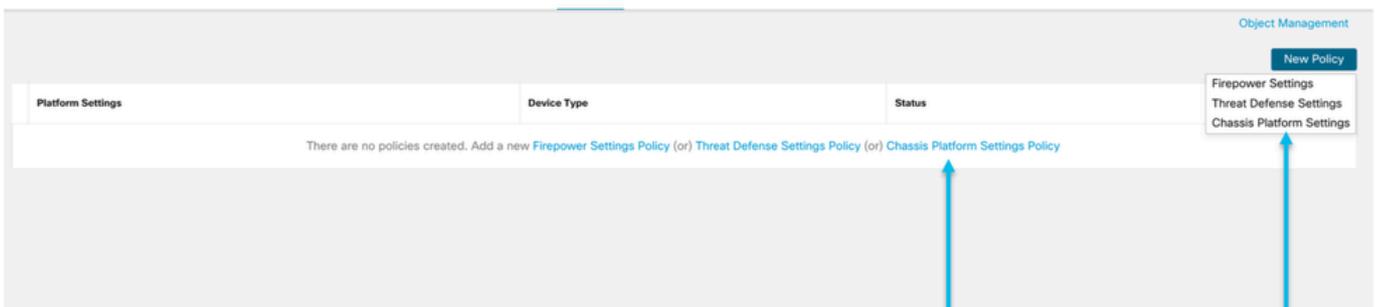
ヒント：シャーシプラットフォームの設定は、シャーシにのみ適用されます。インスタンスにプラットフォーム設定を適用する場合は、脅威対策プラットフォーム設定ポリシーを使用できます。

- 
1. シャーシプラットフォーム設定ポリシーに移動します。



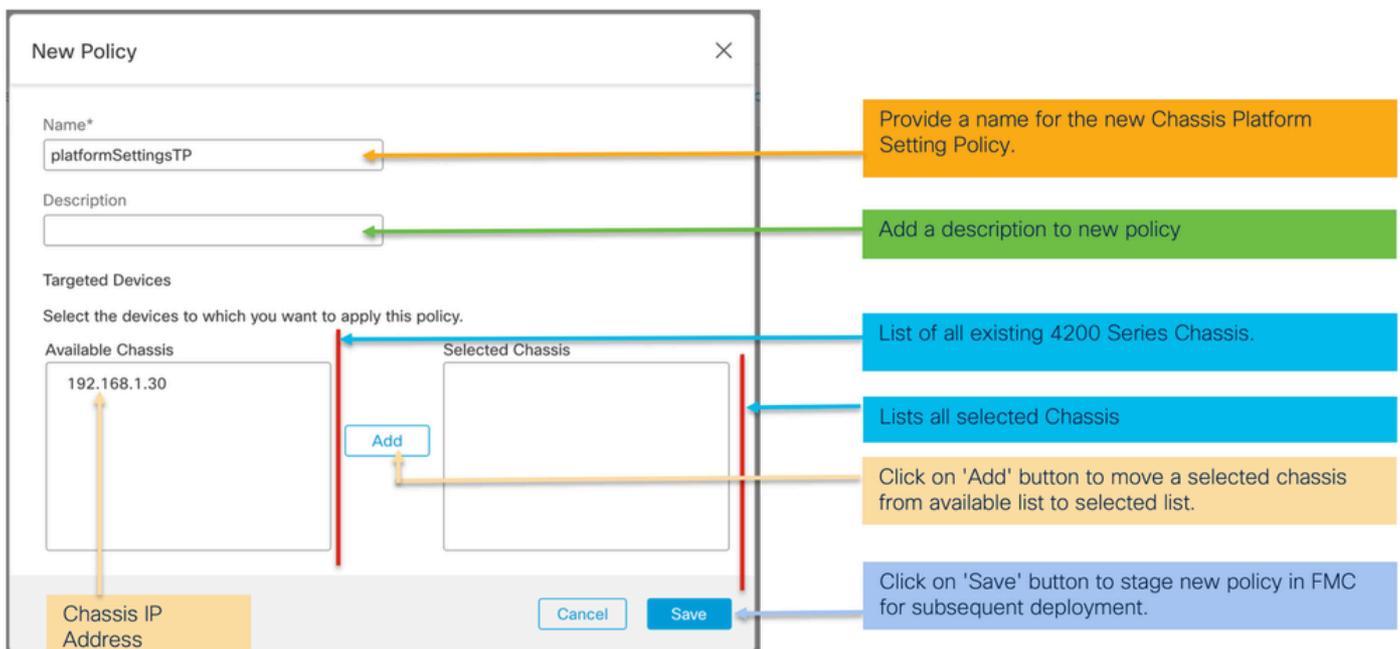
Head to the Platform Settings page to manage your Chassis Platform Settings.

## 2. シャーシプラットフォーム設定を作成します。

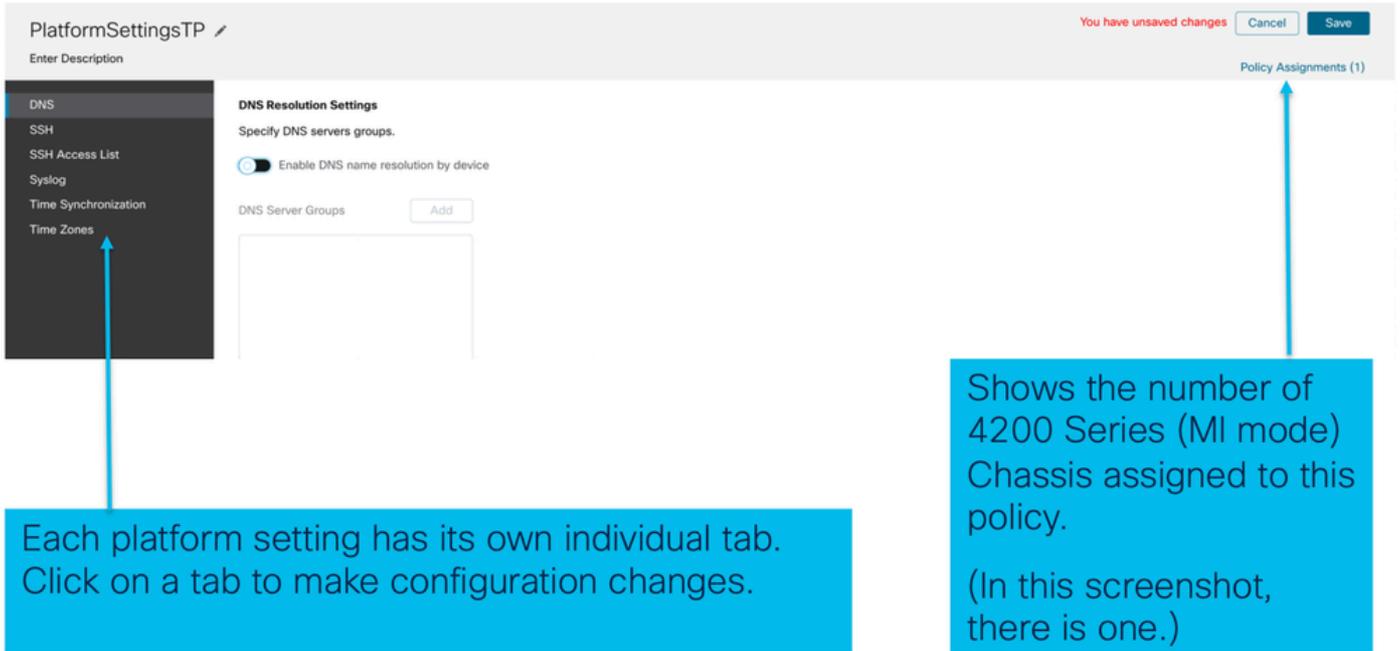


'Chassis Platform Settings' was added in 7.4.1.

- 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. シャーシプラットフォーム設定ポリシーページ :



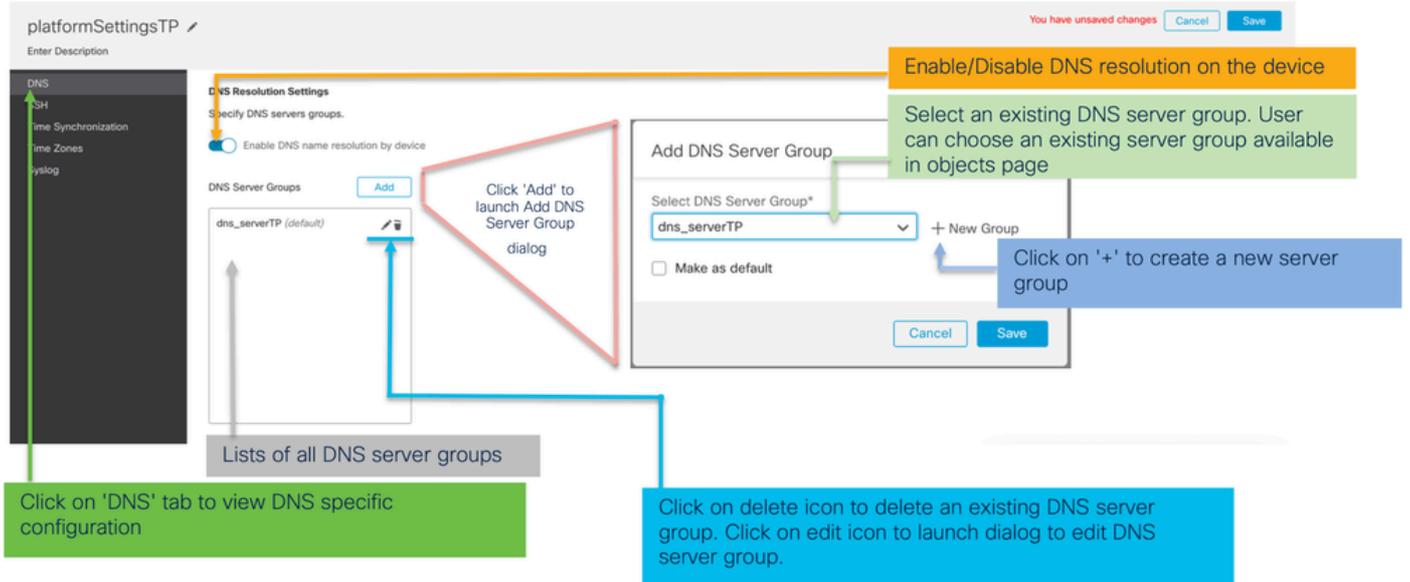
The screenshot shows the 'PlatformSettingsTP' interface with the 'DNS' tab selected. The 'DNS Resolution Settings' section includes a toggle for 'Enable DNS name resolution by device' and a list of 'DNS Server Groups'. A blue arrow points from the 'DNS' tab in the left sidebar to a text box. Another blue arrow points from the 'Policy Assignments (1)' indicator in the top right to another text box.

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.)

### シャーシプラットフォームの設定 : DNS

シャーシプラットフォーム設定ポリシーのDNSセクションのDNSサーバグループの有効化と追加 :

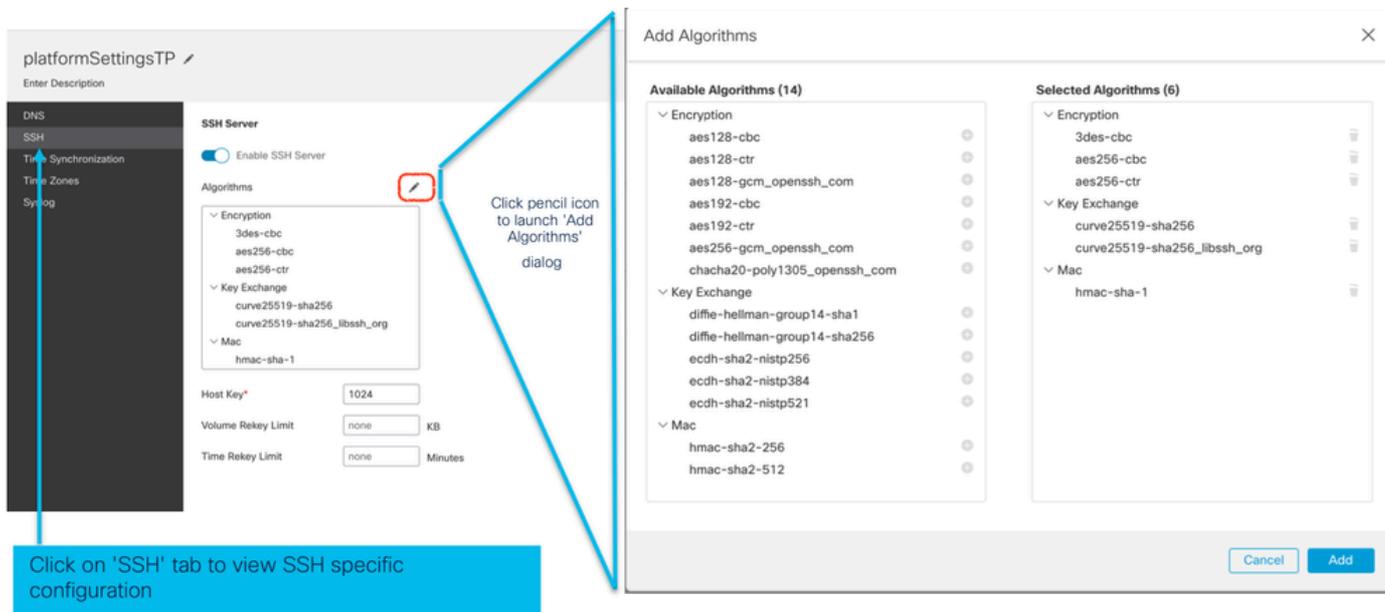


This screenshot provides a detailed view of the DNS Resolution Settings page with several callouts explaining the interface elements:

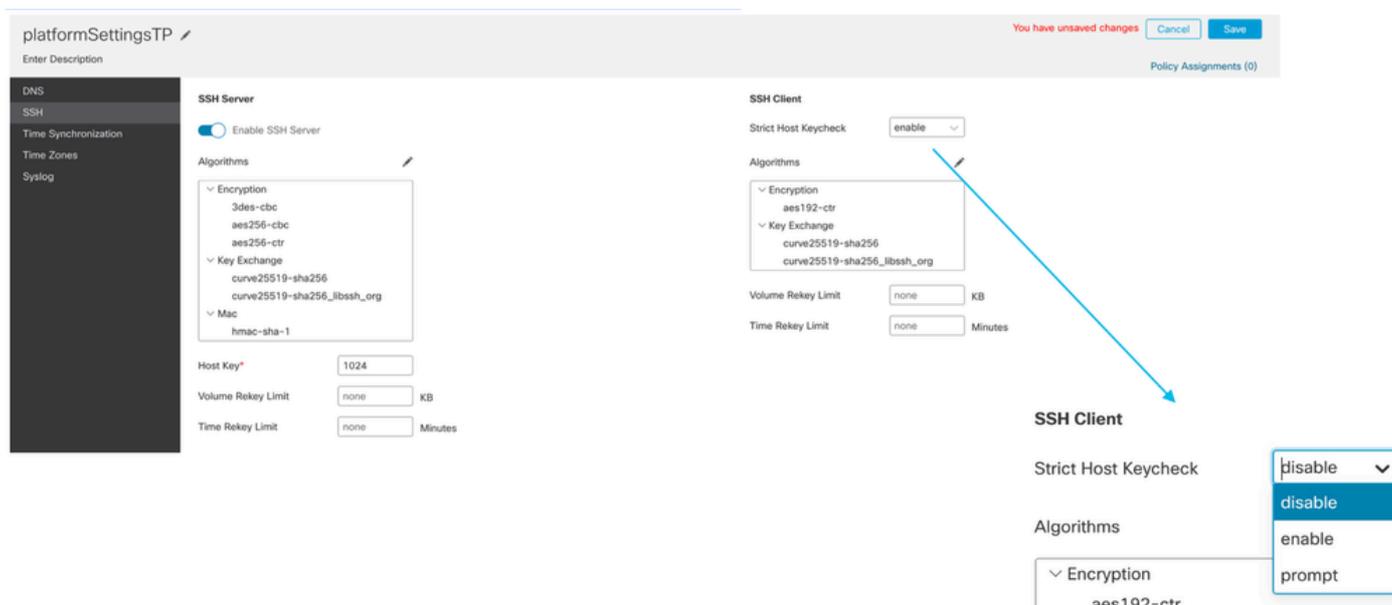
- Enable/Disable DNS resolution on the device:** Points to the 'Enable DNS name resolution by device' toggle.
- Select an existing DNS server group. User can choose an existing server group available in objects page:** Points to the 'Select DNS Server Group\*' dropdown menu.
- Click on '+' to create a new server group:** Points to the '+ New Group' button.
- Click on 'DNS' tab to view DNS specific configuration:** Points to the 'DNS' tab in the left sidebar.
- Lists of all DNS server groups:** Points to the 'DNS Server Groups' list.
- Click on 'Add' to launch Add DNS Server Group dialog:** Points to the 'Add' button.
- Click on delete icon to delete an existing DNS server group. Click on edit icon to launch dialog to edit DNS server group:** Points to the edit and delete icons for the 'dns\_serverTP (default)' group.

### シャーシプラットフォームの設定 : SSH

- シャーシプラットフォーム設定ポリシーのSSHセクションでSSHサーバをイネーブルにして追加します。



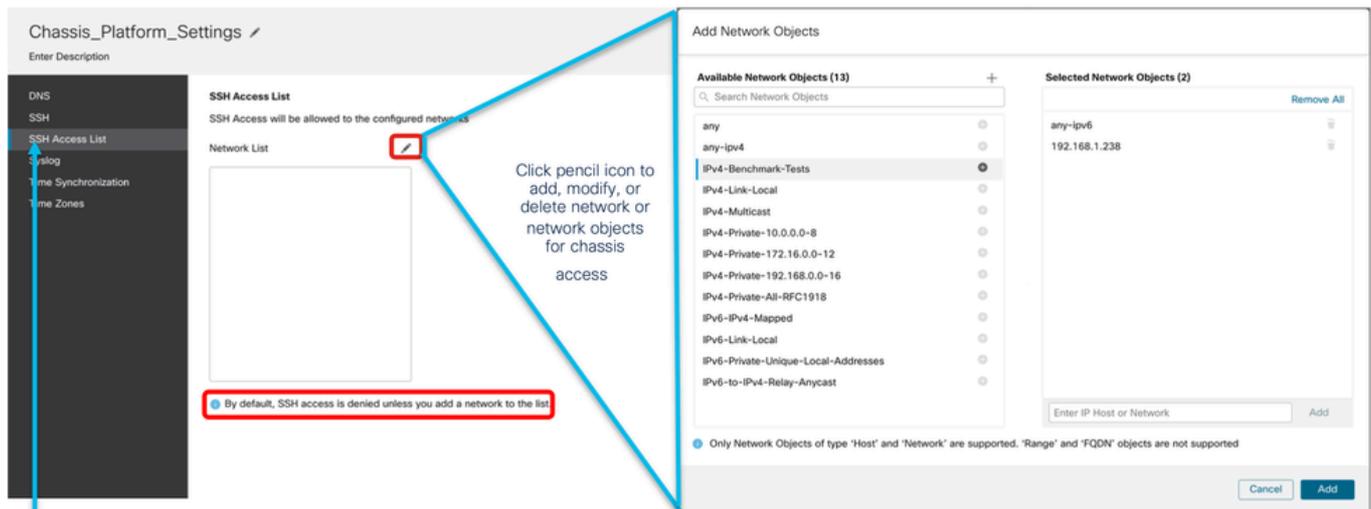
- SSHクライアントの有効化と追加 :



## シャーププラットフォームの設定 : SSHアクセスリスト

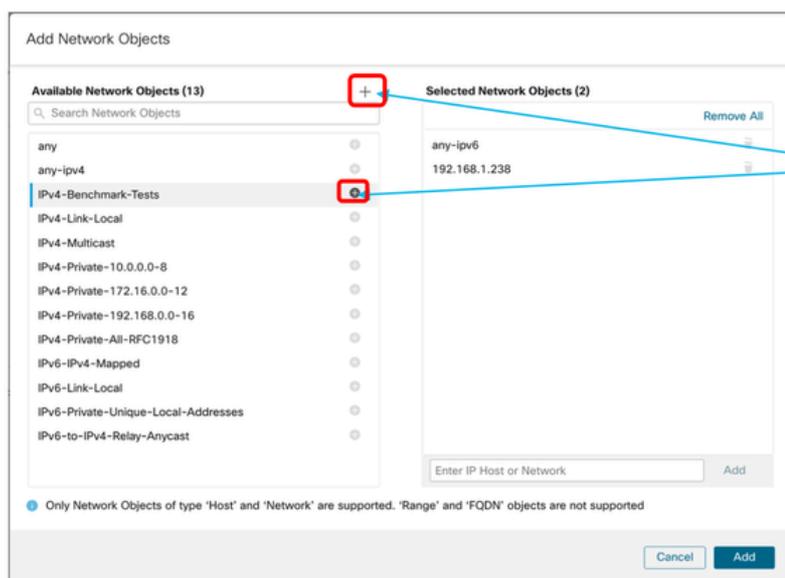
このタブは、「シャーププラットフォームの設定」の「SSH」セクションでSSHを有効にした後  
にのみ表示されます。

- SSHアクセスリストを作成します。



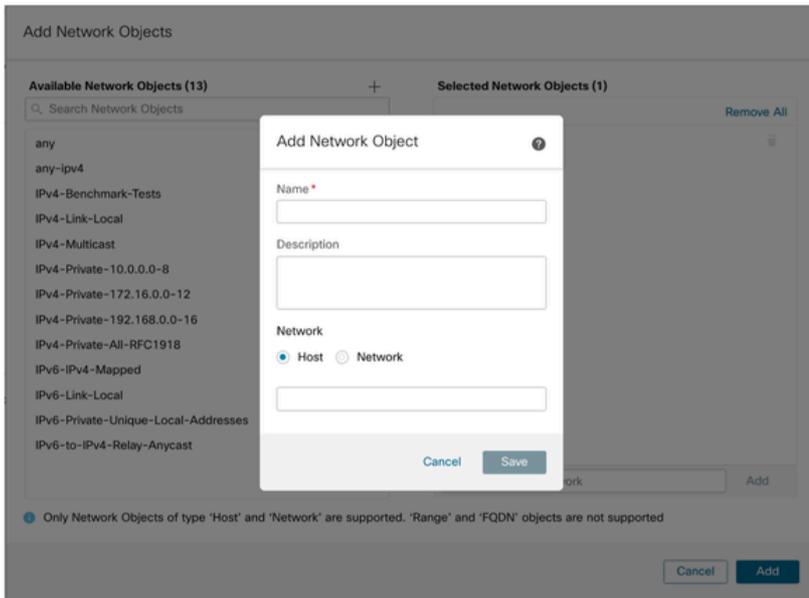
Click on 'SSH Access List' tab to view Access List specific configuration

- SSHアクセスリストのネットワークオブジェクトを追加します。



Network objects can be selected by:  
 1. Choosing from left side pane.  
 2. By creating a new object using the "+" icon.

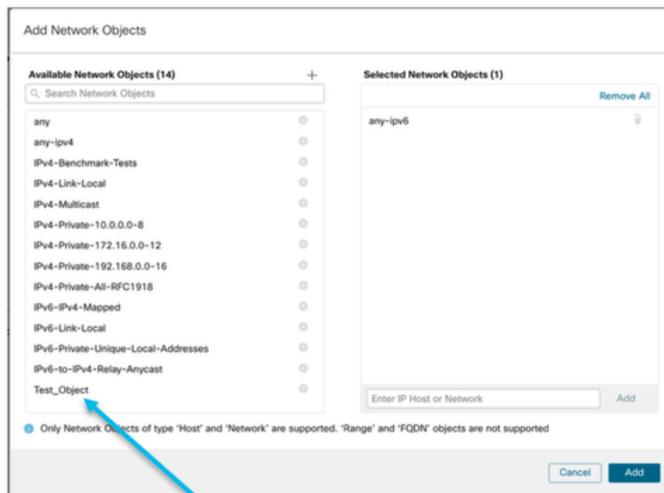
- 新しいネットワークオブジェクトを追加します。



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

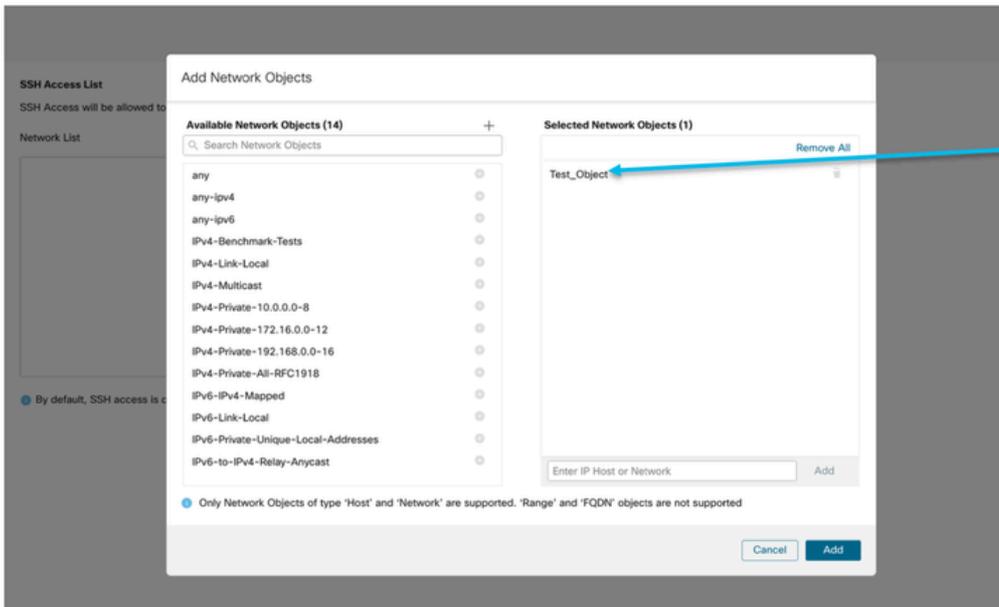
Range and FQDN are NOT allowed.

- ネットワークオブジェクトの表示 :



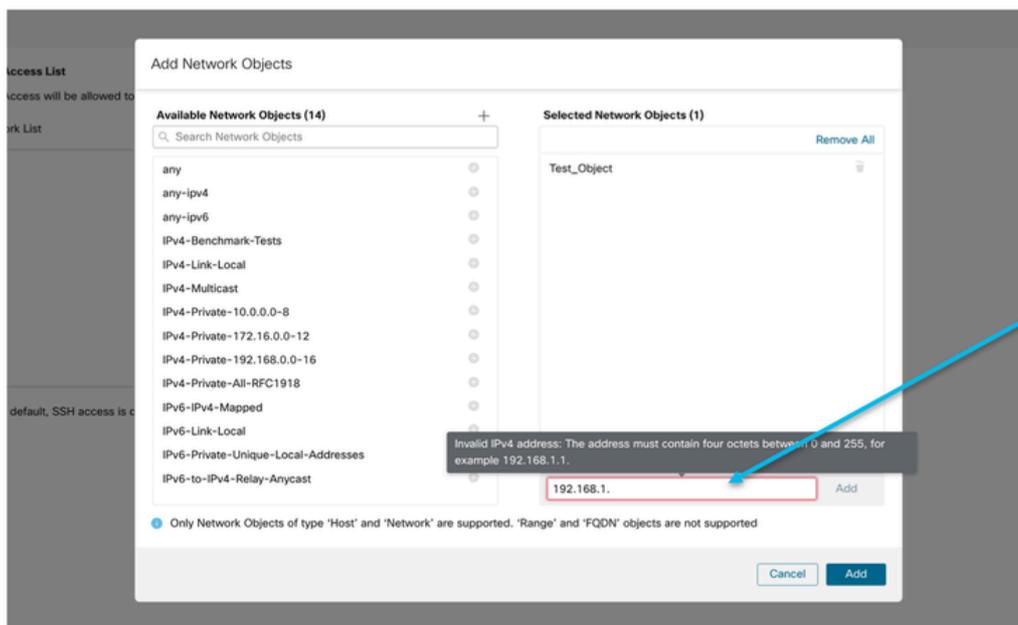
After creation of host object, it will be listed in the available network objects.

- ネットワークオブジェクトを選択 :



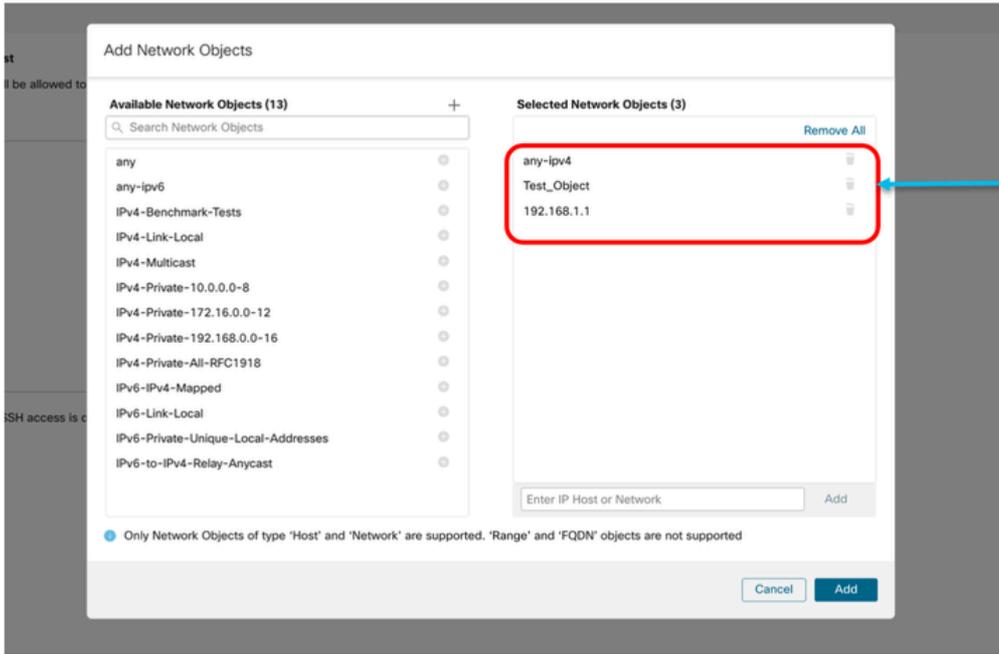
After selecting Network Objects using the “+” icon from available network objects, it will be listed in the selected pane.

- ネットワークオブジェクトは、次の図に示すように作成できます。



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

- 追加されたネットワークオブジェクトの表示：



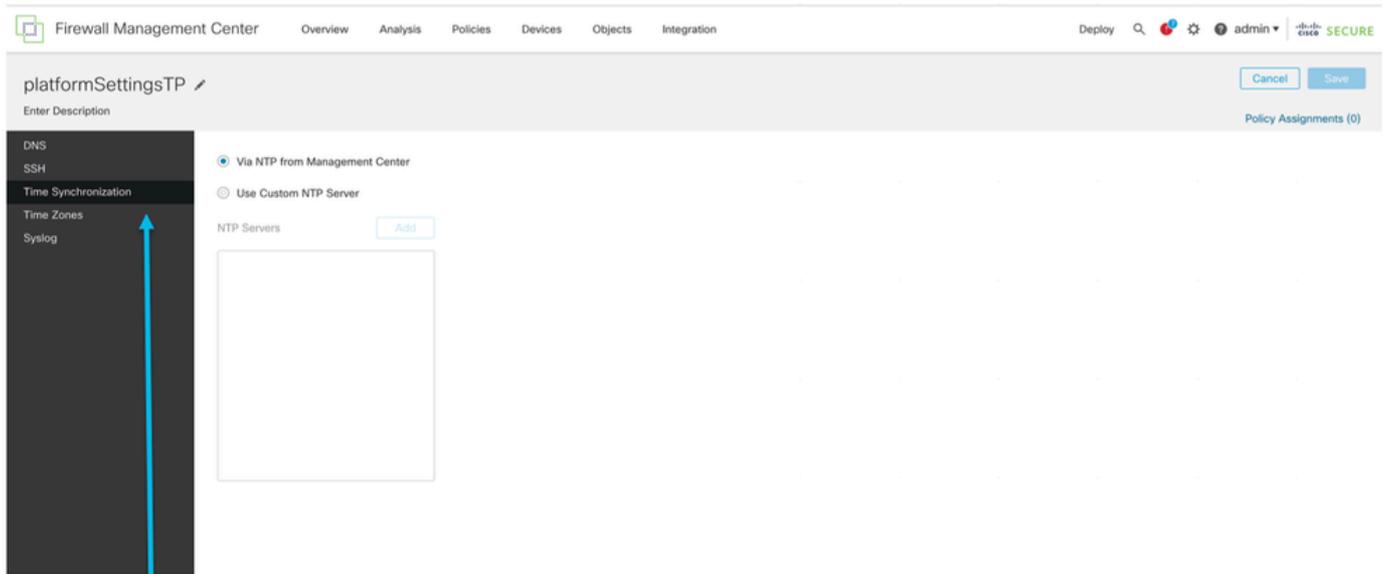
Once the objects are added, they will be listed in the Selected Network Objects pane.

## シャーシプラットフォームの設定：時刻の同期

時刻の同期は、次の2つの方法で実行できます。

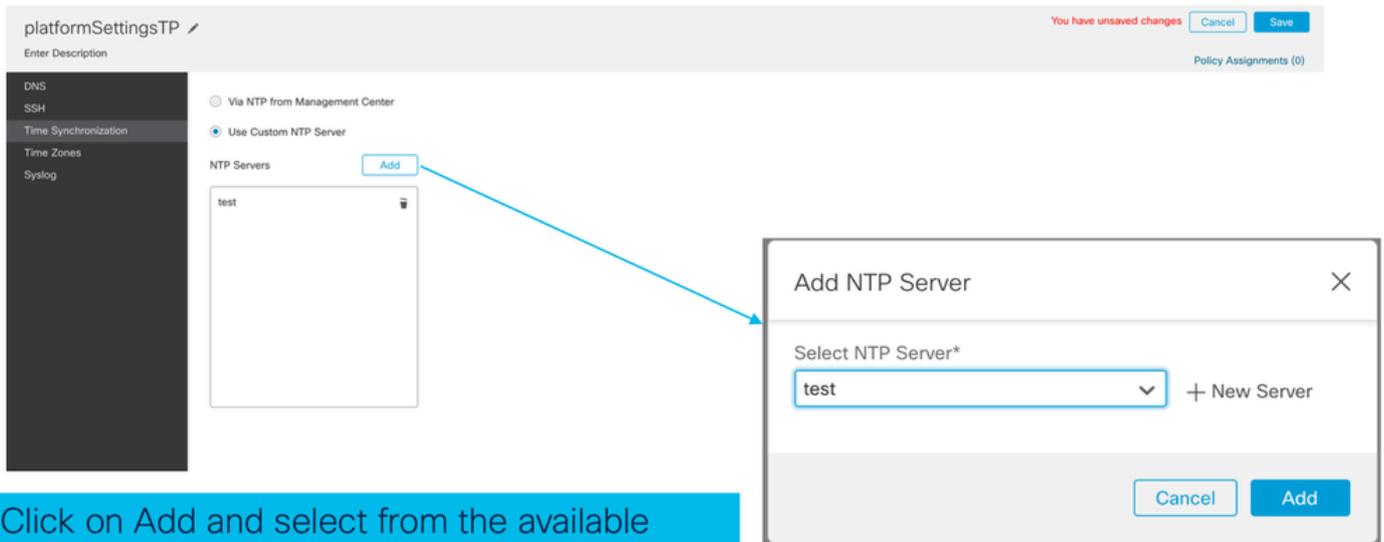
1. Management CenterからのNTP経由
2. カスタムNTPサーバ

### Management CenterからのNTP



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

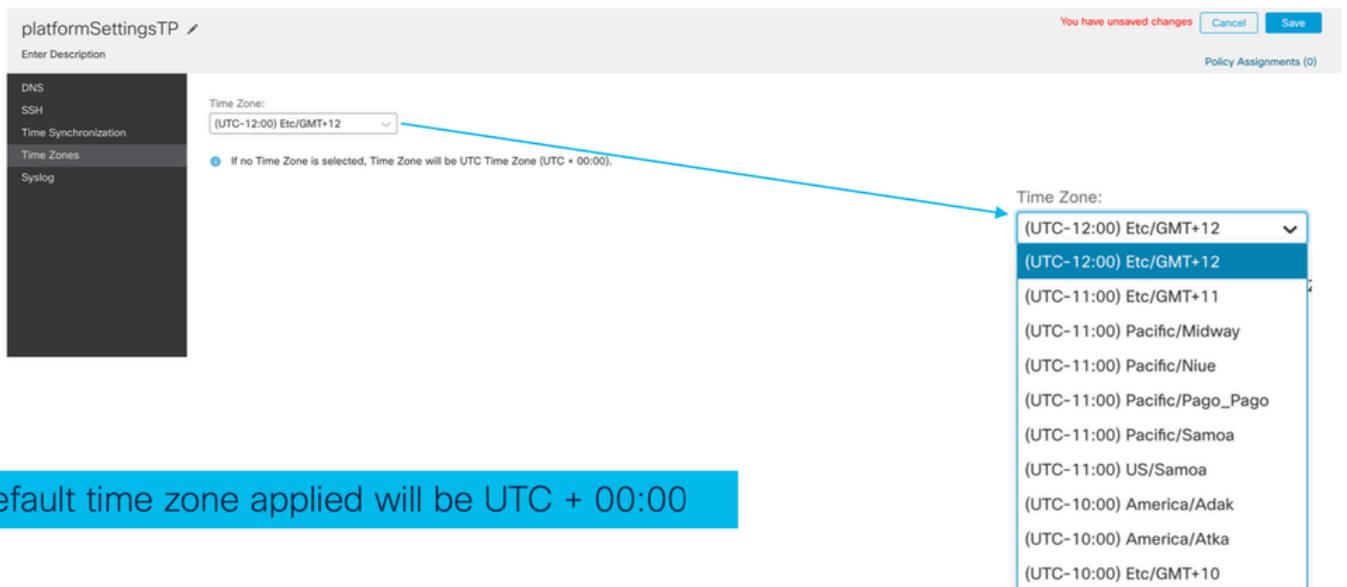
### カスタムNTPサーバ



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

## シャーシプラットフォームの設定：タイムゾーン

タイムゾーンの設定：



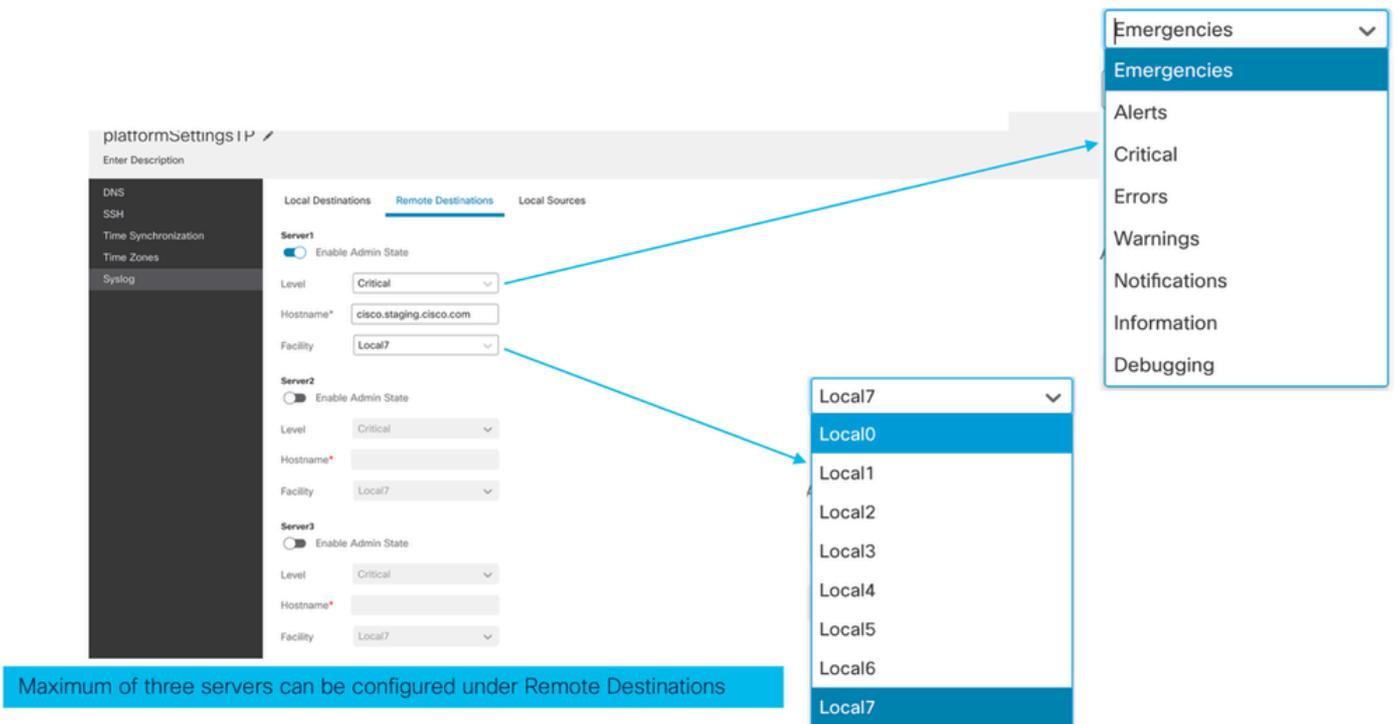
Default time zone applied will be UTC + 00:00

## シャーシプラットフォーム設定：Syslog

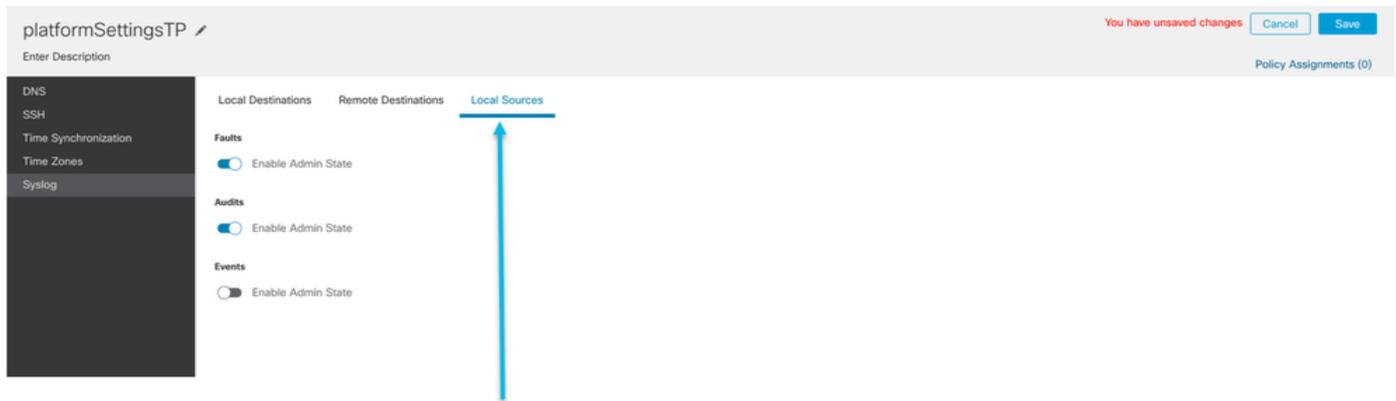
- Syslog Local Destinationsタブ：



- Syslogのリモート接続先タブ :



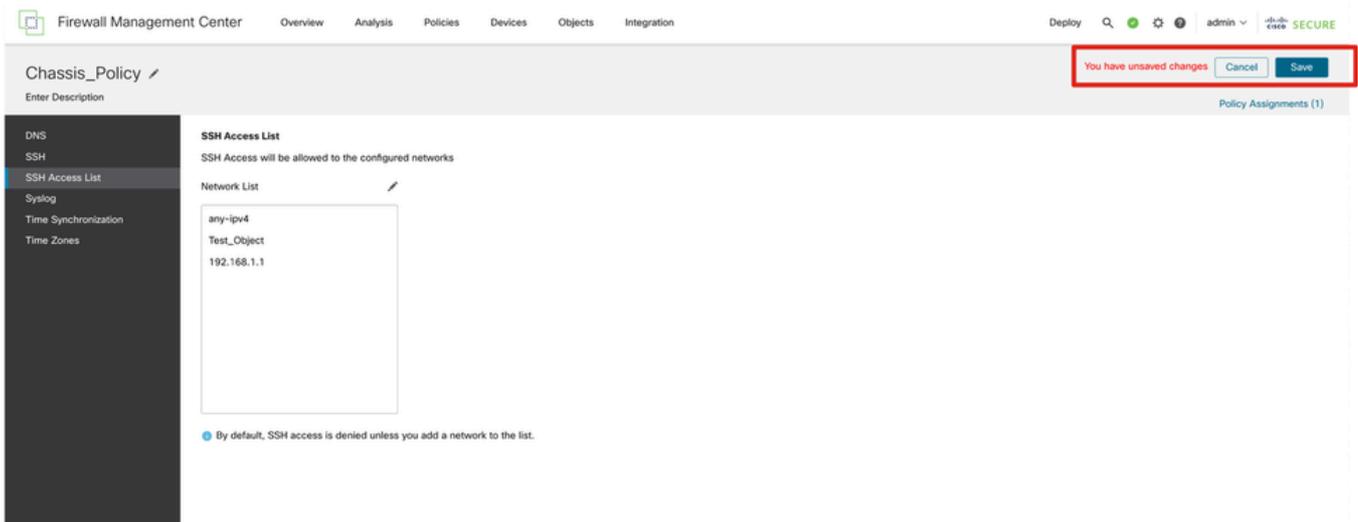
- Syslog Local Sourcesタブ :



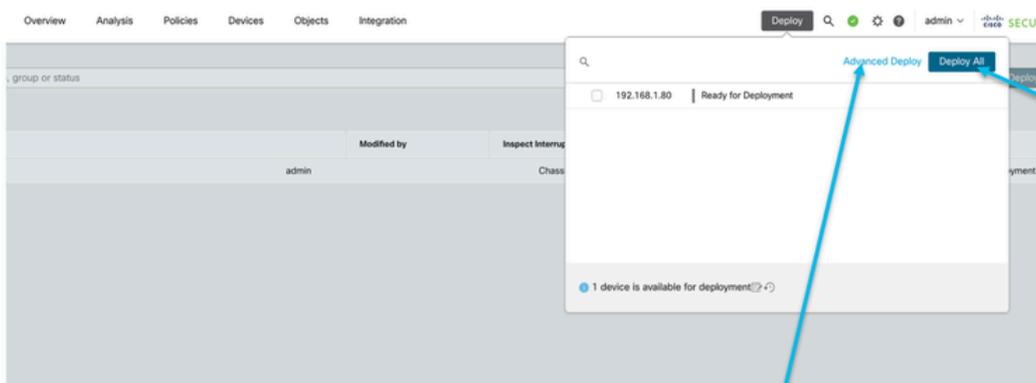
Click on the Local Sources tab to configure Faults/Audits/Events for Local Sources

## シャーシプラットフォームの設定：保存と展開

シャーシプラットフォーム設定の変更を保存し、展開します。



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

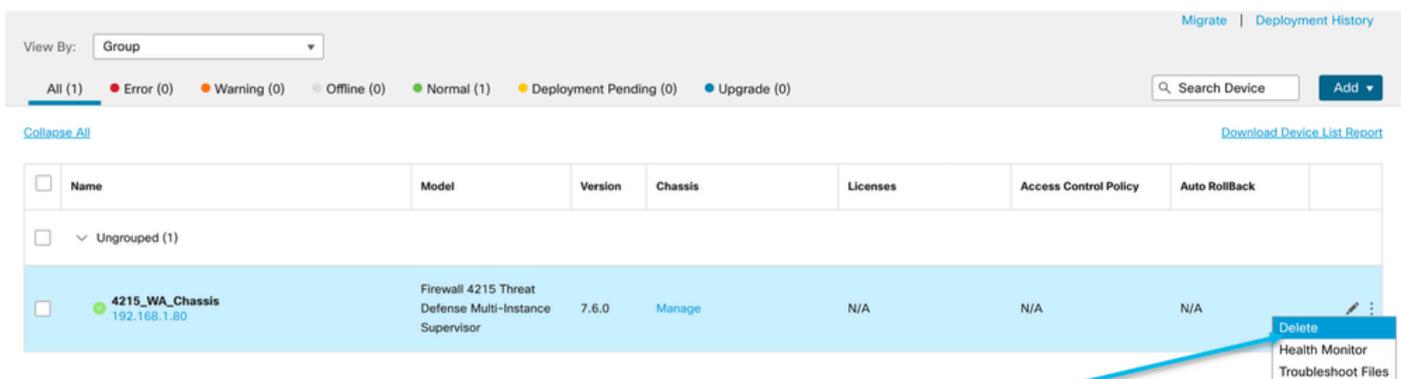


1. Trigger deployment.
2. Once deployment is completed, all chassis platform settings are deployed.

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

## シャーシの登録解除

FMCからシャーシの登録を解除するには、Devices > Device Management > deleteの順に選択します。



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

## マルチインスタンスからネイティブモードへの変換

現在、FMCはネイティブからマルチインスタンスへの変換のみをサポートしています。したがって、デバイスをネイティブモードに戻すには、ユーザはCLIを使用する必要があります。

ステップ1:FMCからシャーシの登録を解除します。

ステップ2 : 次のCLIコマンドを使用して、4200シリーズのデバイスをネイティブモードに変換します。

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

# FMC Rest API

FMCパブリックREST APIは、FMCからサポートされるすべての操作で使用できます。

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

## ネイティブからマルチインスタンスへの変換のためのREST API

ネイティブ・デバイスがマルチインスタンス変換に対応しているかどうかを確認するためのPOST API:

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/operational/switchmodereadiness

サンプルPOSTリクエストJSON:

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

シングルネイティブからマルチインスタンスへの変換をトリガーするPOST API:

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/operational/switchmode

サンプルPOSTリクエストJSON:

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

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

POST APIを使用して、ネイティブからマルチインスタンスへの一括の変換をトリガーする。

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/operational/switchmode

サンプルPOSTリクエストJSON:

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

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

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

## シャーシ管理用REST API

POST管理センターへのシャーシの追加 :

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis

すべてのシャーシを取得 :

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/

uuidによる特定のシャーシの取得 :

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{objectId}

uuidによるシャーシの削除 :

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{objectId}

サンプルPOSTリクエストJSON:

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

## Netmods ( ネットワークモジュール ) 管理用のREST API

uuidによるネットワークモジュールの取得 :

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/networkmodules/

すべてのネットワークモジュールを取得 :

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/networkmodules/

PUT:uuidによる既存のネットワークモジュールの編集 :

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/networkmodules/

PUT - FXOSからネットワークモジュールデータを取得し、Management Centerを更新します。

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operational/syncr

サンプルGET応答

```
{
  "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"
}

```

## インスタンス管理用REST API

POST管理センターへのシャーシの追加 :

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

すべてのシャーシを取得 :

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

uuidによる特定のインスタンスの取得 :

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

PUT - uuidによるインスタンスの編集 :

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

uuidによるシャーシの削除 :

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

サンプルPUT要求 :

```

{
  "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" }
```

## SNMP管理用REST API

uuidによるSNMP設定の取得 :

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

すべてのSNMP設定を取得します。

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

PUT : 既存のネットワークモジュールをuuidで編集します。

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

GET応答の例 :

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

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

## 要約を取得するREST API

このリストには、サマリーをフェッチするためのREST APIに関する詳細情報が含まれています。

- 障害
- インスタンス
- インベントリ
- インターフェイス
- アプリ情報

シャーシのGET障害サマリー :

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

サンプル応答 :

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

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

シャーシのGETインスタンスの概要 :

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

サンプル応答 :

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

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/instancesummary?offs

シャーシのインベントリの概要を取得：

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/inventorysummary

サンプル応答：

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

```

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/inventorysummary?offs

シャーシのインターフェイスサマリーを取得します。

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/interfacesummary

サンプル応答：

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

```

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/interfacesummary?offs

シャーシのアプリ情報の取得：

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}

/inventorysummary

サンプル応答：

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

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

## インターフェイス管理用REST API

このセクションでは、インターフェイスコンフィギュレーション管理のREST APIについて詳しく説明します。

- インターフェイス設定の変更に使用されるURL
- インターフェイスのブレイク/ジョインに使用されるURL
- 同期デバイスの構成に使用するURL

### 物理インターフェイスの更新

物理インターフェイスのアップデートをサポートするために、次のURLが導入されました。

すべての物理インターフェイスの取得：

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

インターフェイスuuidによって特定の物理インターフェイスを取得します。

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

インターフェイスuuidでインターフェイスを更新します。

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

物理インターフェイスモデルは次のようになります。

```
{
```

```

"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": "*****"
}

```

## サブインターフェイスの設定

サブインターフェイスの管理をサポートするために、次のURLが導入されました。

すべてのサブインターフェイスを取得：

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

インターフェイスuuidによって特定のサブインターフェイスを取得します。

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

新しいサブインターフェイスの投稿：

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

インターフェイスuuidによるインターフェイスの更新：

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

インターフェイスuuidによってサブインターフェイスを削除します。

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

サブインターフェイスモデルは次のようになります。

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

## EtherChannelインターフェイスの設定

EtherChannel EtherChannelインターフェイスの管理をサポートするために、次のURLが導入されました。

すべてのEtherChannelインターフェイスを取得します。

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

インターフェイスuuidによって特定のEtherChannelインターフェイスを取得します。

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

新しいEtherChannelインターフェイスのPOST:

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

インターフェイスuuidによるインターフェイスの更新:

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

インターフェイスuuidによってEtherChannelインターフェイスを削除します。

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

EtherChannelインターフェイスモデルは次のようになります。

```

{
  "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-*****"
}

```

## REST APIのBreak/Joinインターフェイス

4200シリーズのインターフェイスのブレイクアウト/加入をサポートするには、次のURLを使用できます。

GET :

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/chassisinterfaces

インターフェイスのブレイク/ジョインの実行可能性を評価します。

POST:

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operational/break

インターフェイスを中断します。

POST:

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operational/joinin

破損したインターフェイスのセットを結合します。

インターフェイス切断用のRESTフロー

1. fmcmanagedchassisエンドポイントを使用してFMC管理対象シャーシデバイス(4200)を見つけます。

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassisを取得

FMC管理対象シャーシデバイスのリストと、各デバイスのID、名前、モデルなどの詳細を含むマルチインスタンスデバイスを返します。「MULTIINSTANCE」デバイスを選択します。

サンプル応答 :

```
{
  "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. interfaces/physicalinterfacesエンドポイントを使用して、インターフェイスがブレイクアウト可能かどうかを確認します。

ブレイクアウトは、「isBreakoutCapable」がtrueで、mediaTypeがQSFPの場合にのみ可能です。

GET

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/interfaces

サンプル応答 :

```
{
  "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. インターフェイス上で、evaluateoperationエンドポイントを使用してブレイク操作の実行可能性を評価します。

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/chassisinterfaces  
 得します

応答に警告やエラーがない場合、ユーザはブレイク操作を実行できます。

サンプル応答：

```

{
  "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"
}

```

応答にエラーがある場合、ユーザはブレイク操作を実行できません。

```
{
```

```

"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. インターフェイスがブレイクアウト対応で、準備状態が「READY」の場合、ブレイクアウトインターフェイスエンドポイントを使用してインターフェイスをブレイクします。

POST

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operational/break

要求:

```

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

```

レスポンス:

```

{
  "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. ブレーク応答でタスクIDを使用して、タスク完了を追跡します。「Task status」を「Interface Notification received」に設定します。

GET /api/fmc\_config/v1/domain/{domainUUID}/job/taskstatuses/{objectId}

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

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

6. chassisinterfaceeventsエンドポイントを使用して、インターフェイスの変更を取得します。

/api/fmc\_config/v1/domain/{domainUUID}/chassis/  
fmcmanagedchassis/{containerUUID}/chassisinterfaceeventsを取得します。

サンプル応答：

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

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

7. インターフェイス通知を受信しない場合は、chassisinterfaceeventsエンドポイントを使用してデバイスを同期し、保留中の変更があることを確認します。

POST /api/fmc\_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/chassisinterfaceevents

要求: :

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

レスポンス :

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

8. 通知を受信したら、chassisinterfaceeventsエンドポイントを使用して変更を受け入れます。

POST /api/fmc\_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/chassisinterfaceevents

要求: :

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

9. すべてのシャシーインターフェイスを取得し、インターフェイスエンドポイントを使用して分割された ( 破損した ) インターフェイスを見つけます。

GET

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

1つの40Gインターフェイス ( eth2/2など ) は、4x10Gインターフェイス ( eth2/2/1、eth2/2/2、eth2/2/3、およびeth2/2/4 ) に分割されます

インターフェイス結合のためのRESTフロー

1. interfaces/physicalinterfacesエンドポイントを使用して、インターフェイスが故障しているかどうかを確認します。

結合操作は、"isSplitInterface"がtrueで、mediaTypeがSFPの場合にのみ可能です

GET

```
/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/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. 4つの分割インターフェイスの1つに対してevaluateoperationエンドポイントを使用して、Join操作の実行可能性を評価します。

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/chassisinterfaces/{interfaceUUID}/evaluateoperationを取得します

- 応答に警告やエラーがない場合、ユーザは参加操作を実行できます。

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

- 応答にエラーがある場合、ユーザは参加操作を実行できません。

```
{
  "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. インターフェイスが壊れ、準備状態が「READY」の場合、joininterfacesエンドポイントを使用してインターフェイスに参加します。interface\_uuidは、4つの破損したインターフェイスのIDにすることができます。

POST/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operational

要求: :

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

```

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

```

レスポンス :

```

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

```

```

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

```

4. 加入応答のタスクIDを使用してタスク完了を追跡します。「Task status」を「Interface Notification received」に設定します。

GET /api/fmc\_config/v1/domain/{domainUUID}/job/taskstatuses/{objectId}

レスポンス :

```

{
  "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. chassisinterfaceeventsエンドポイントを使用して、インターフェイスの変更を取得します。

/api/fmc\_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/chassisinterfaceevents  
 得します。

回答 :

```
[
  {
    "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. インターフェイス通知を受信しない場合は、chassisinterfaceeventsエンドポイントを使用してデバイスを同期し、保留中の変更があることを確認します。

POST

/api/fmc\_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/chassisinterfaceevents

要求: :

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

レスポンス :

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

7. 通知を受信したら、chassisinterfaceeventsエンドポイントを使用して変更を受け入れます。

/api/fmc\_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/chassisinterfaceeventsの後

要求: :

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

8. すべてのシャーシインターフェイスを取得し、参加しているインターフェイス、およびインターフェイスエンドポイントを使用している他のインターフェイスを見つけます。

GET

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/interfaces

たとえば、10Gインターフェイス(eth2/2/1)でJoinが開始されると、応答では40Gインターフェイスeth2/2が使用可能になります。

## デバイスREST APIの同期

ネットワークモジュールとインターフェイスの同期をサポートするために、次のURLが導入されました。

POST:

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/chassisinterfaceevents

ペイロードあり

{"action": "SYNC\_WITH\_DEVICE"} - >同期をトリガーします

{"action": "ACCEPT\_CHANGES"} - >変更を承諾します

GET :

/api/fmc\_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/chassisinterfaceevents

生成された変更イベントを一覧表示します

# トラブルシューティング/診断

## FXOSロギング

登録が失敗した場合、これらのFXOS CLIを使用して、sftunnel、sfiproxyプロセスが起動しているかどうかを確認できます。

```
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.
```

CLIでターミナルコンソールを使用している場合は、次に示すCLIを使用してターミナル幅を適切な値に設定することにより、show processesの出力が切り捨てられていないことを確認します。

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

SFTunnelプロセスが起動して実行されているにもかかわらず、登録が失敗する場合は、次のコマンドを使用して失敗の潜在的な原因を調べることができます。

/opt/cisco/platform/logs/sfmessagesでsyslogメッセージを表示するために、connect local-mgmtからFXOSに新しいCLIを導入

```
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
```

## FMCOロギング

- デバイスの登録が失敗した場合は、この場所でusmsharedsvcs.logとvmssharedsvcs.logを検索し、文字列「CHASSIS DISCOVERY」または「NATIVE\_TO\_MULTI\_INSTANCE」を検索して、失敗の潜在的な原因を見つけます。

- また、SFTunnelの問題については、/var/log/action\_queue.logと/var/sf/messagesを参照してください。
- /var/opt/CSCOpX/MDC/log/operation/usmsharedsvcs.log  
/var/opt/CSCOpX/MDC/log/operation/vmssharedsvcs.log
- シャーシの自動登録が失敗した場合、usmsharedsvcs.logとvmssharedsvcs.logを検索し、文字列「CHASSIS DISCOVERY」と「NATIVE\_TO\_MULTI\_INSTANCE」を検索して、失敗の潜在的な原因を見つけます。
- インスタンスの自動登録が失敗した場合、usmsharedsvcs.log およびvmssharedsvcs.log を検索し、文字列「MI\_FTD\_INSTANCE\_AUTO\_REGISTRATION」を検索して失敗の考えられる原因を見つけます。
- デバイスに導入エラーがある場合は、「導入 ->導入履歴 ->失敗した導入をクリック ->トランスクリプトを開く」に移動します。このファイルには失敗の理由が含まれています。

## シャーシのトラブルシューティング

FMCは、デバイス管理ページからのシャーシトラブルシューティング(FPRM)の生成をサポートします。

- FTDデバイスと同様に、シャーシデバイスに使用できるトラブルシューティングオプションがあります。このオプションでは、シャーシのトラブルシューティングを生成し、ユーザがFMCからトラブルシューティングバンドルをダウンロードできます。
- これにより、シャーシから「show tech-support form」バンドルが収集されます。

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
▼ Ungrouped (2)							
4215_WA_chassis 192.168.1.80	Firewall 4215 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	N/A	N/A	N/A	Delete Health Monitor Troubleshoot Files
WA_Instance_1 192.168.1.81 - Routed	Firewall 4215 Threat Defense	7.6.0	N/A	Essentials, Malware (1 more...)	Pol		

シャーシのトラブルシューティングオプションと生成：

- 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:

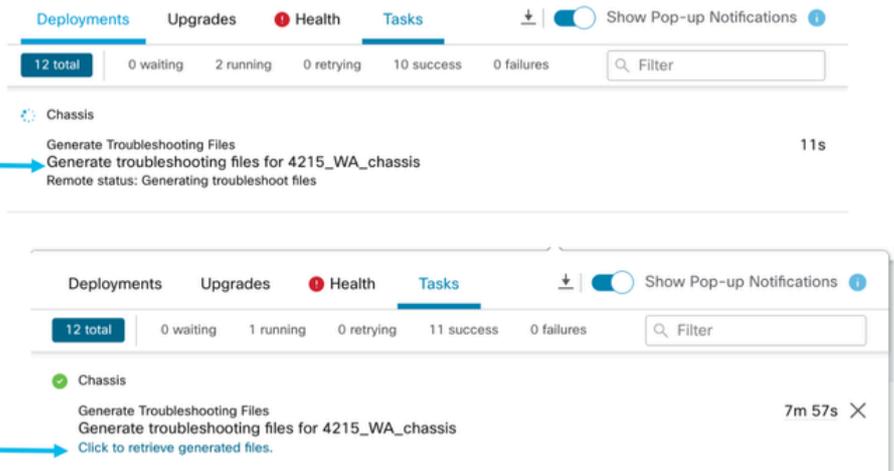
All Data

FXOS Logs

Cancel Generate

シャーシのトラブルシューティングの進行状況とダウンロード：

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



## トラブルシューティングの手順に関する問題の例

### FMCでのシャーシ障害の自動登録

問題：FMCでシャーシの自動登録が失敗する。

予想される結果：

- FMCから変換が始まると、FMCで登録解除されて自動登録されることが想定されます。

実際の結果

- シャーシの自動登録に失敗

問題のトラブルシューティング

1. 変換を確認します。

- FMCで変換がトリガーされたことを確認します。
- デバイスにログインし、デバイスがコンテナモードに変換されているかどうかを確認します。
- デバイスが変換されたかどうかを確認するには、次のコマンドを実行します。

```
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. デバイスマネージャを確認します。

- デバイスマネージャが正しく設定されているかどうかを確認します。

```
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. 確認するログ :

3.1. /var/opt/CSCOpX/MDC/log/operation/vmssharedsvcs.logおよび  
/var/opt/CSCOpX/MDC/log/operation/usmsharedsvcs.logに移動します。

3.2. ファイル内で「NATIVE\_TO\_MI\_CONVERSION」および「CHASSIS DISCOVERY」というキーワードを検索し、障害の原因を見つけます。

## FMCにおけるインスタンスの自動登録

問題 : FMCでインスタンスの自動登録が失敗します。

予想される結果 :

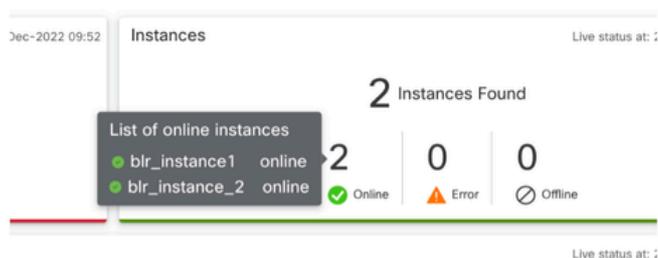
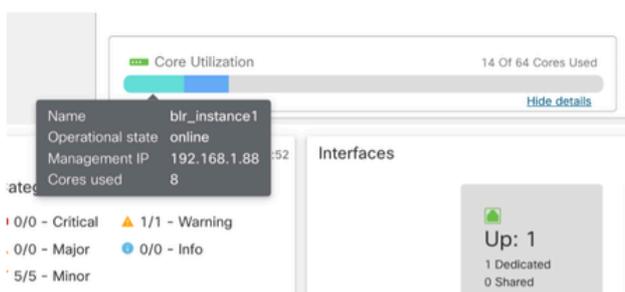
- インスタンスがFMCからプロビジョニングされると、FMCに自動登録されます。

実際の結果

- インスタンスの自動登録に失敗しました

### 問題のトラブルシューティング

- インスタンスの作成後にデプロイがトリガーされたことを確認します。
  - 展開が実行されない場合は、デバイスに変更を展開してください。
  - 導入に失敗した場合は、「導入履歴 -> トランスクリプトをクリックする」に進みます。失敗の理由を確認し、修正して展開を再試行してください。
- インスタンスがインストールされており、その動作状態がオンラインであることを確認します。シャーシのサマリーページを使用して、インスタンスプロビジョニングのステータスを確認できます。



- 次のコマンドを使用して、インスタンスFTDでSFTunnelがアップ状態で実行中であることを確認します。

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

- SFTunnelが実行されていない場合は、restartコマンドを実行してみてください。

```
pmtool restartById sftunnel
```

- /var/opt/CSCOpX/MDC/log/operation/vmssharedsvcs.logおよび /var/opt/CSCOpX/MDC/log/operation/usmssharedsvcs.logに移動します。
- ファイル内でキーワード「MI\_FTD\_INSTANCE\_AUTO\_REGISTRATION」を検索して、失敗の理由を見つけます。

## FMCでのネイティブデバイス登録

問題：デバイスをネイティブモードに戻した後、FMCでネイティブデバイス登録が失敗する

- ユーザがシャーシ（MIモード）をネイティブモードに戻しても、FMCからシャーシを削除し忘れた場合、デバイスはFMC上でオフラインになります。
- ユーザがこのネイティブデバイスをFMCに再登録しようとする、登録が失敗します。

問題のトラブルシューティング

- デバイスをネイティブモードに戻す前に、FMCからシャーシエントリが削除されていることを確認してください。
- エントリが削除されたら、ネイティブデバイスをFMCに再登録してみてください。

## 参考リンク

- 共有インターフェイスに関する情報

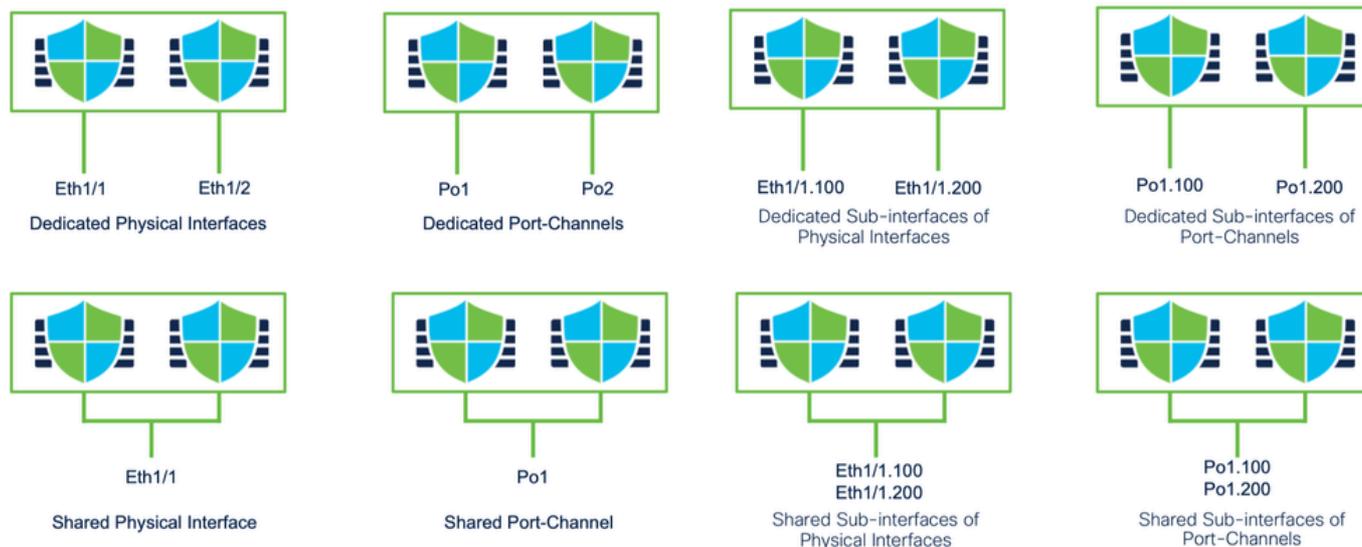
<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/threat-defense/use-case/multi-instance-sec-fw/multi-instance-sec-fw.html#shared-interface-scalability-WGUIEF>

- 3100マルチインスタンスページ（シスコサポートサイト）:

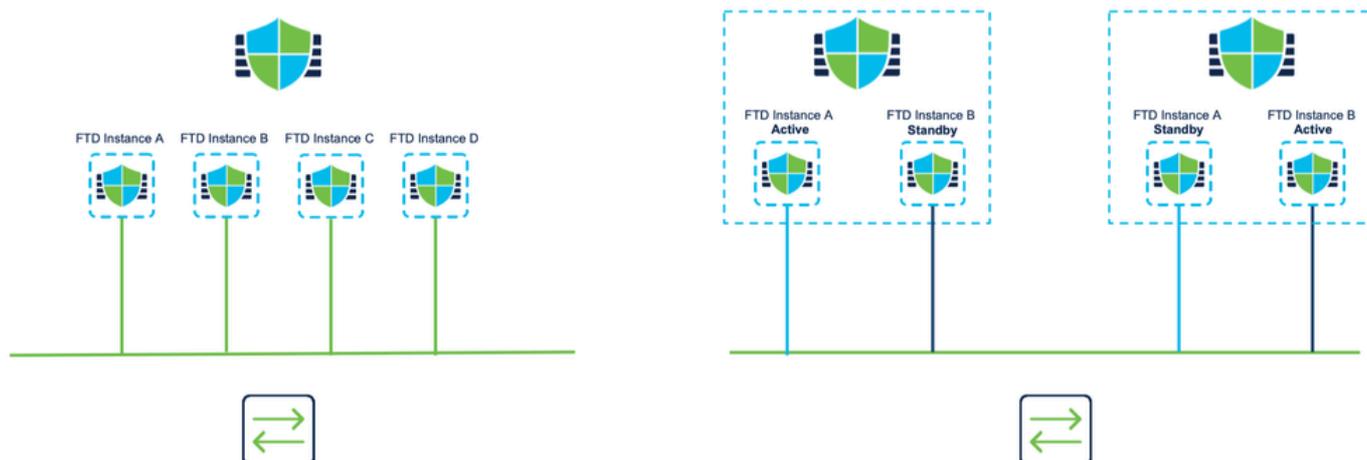
<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/threat-defense/use-case/multi-instance-sec-fw/multi-instance-sec-fw.html>

## インターフェイスオプションとハイアベイラビリティ

## インターフェイスオプション



## スタンドアロンまたは高可用性



## デュアル管理インターフェイスの活用

- ネイティブモードの4200と同様に、2つの物理管理ポートは、管理トラフィック用にインターフェイスの冗長性をサポートするため、または管理とイベント用に個別のインターフェイスをサポートするために提供されます。
  - 9300および4100デバイス、ならびに4200シリーズには、デュアル管理インターフェイスがあります。2つ目の管理インターフェイスであるManagement 1/2は、イベントに使用することを目的としています。
- マルチインスタンス（別名「コンテナ」）モードでは、各インスタンスの脅威対策CLIでこのインターフェイスを設定できます。各インスタンスに同じネットワーク上のIPアドレスを割り当てます。
- コンテナモードでは、各FTDインスタンスにManagement 1/1とManagement 1/2の両方のインターフェイスが自動的に割り当てられます。
  - 2番目の管理インターフェイスは、デフォルトでは無効になっています。
  - FMCを使用してManagement 1/2を設定することはできません。FTD CLISHを使用して

設定する必要があります ( 9300/4100ではFXOS CLIで行われます )。目的のIPアドレスタイプ、アドレス、サブネット、およびスタティックルートを指定して次のコマンドを使用します。

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

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。