

Cisco Defense Orchestrator(CDO)でのクラウド配信FMC(cdFMC)の導入

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[CDOにクラウド提供のFirepower Management Centerを導入します。](#)

[クラウド提供のFMCでのFTDのオンボーディング](#)

[関連情報](#)

概要

このドキュメントでは、CDOプラットフォームでのクラウド配信FMCの導入とオンボードプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- クラウド提供のFirepower Management Center(cdFMC)
- Cisco Defense Orchestrator(CDO)
- Firepower Threat Defense Virtual (FTDv)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- cdFMC 7.2.0
- FTDv 7.2.0

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。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

Cisco Defense Orchestrator(CDO)は、クラウドで提供されるファイアウォール管理センター

(cdFMC)のプラットフォームです。クラウド提供のファイアウォール管理センターは、セキュアなファイアウォール脅威対策デバイスを管理するSoftware-as-a-Service(SaaS)製品です。オンプレミスのセキュアファイアウォールセキュアファイアウォール脅威防御と同じ機能の多くを提供します。これは、オンプレミスのセキュアファイアウォール管理センターと同じ外観と動作を持ち、同じFMCアプリケーションプログラミングインターフェイス(API)を使用します。

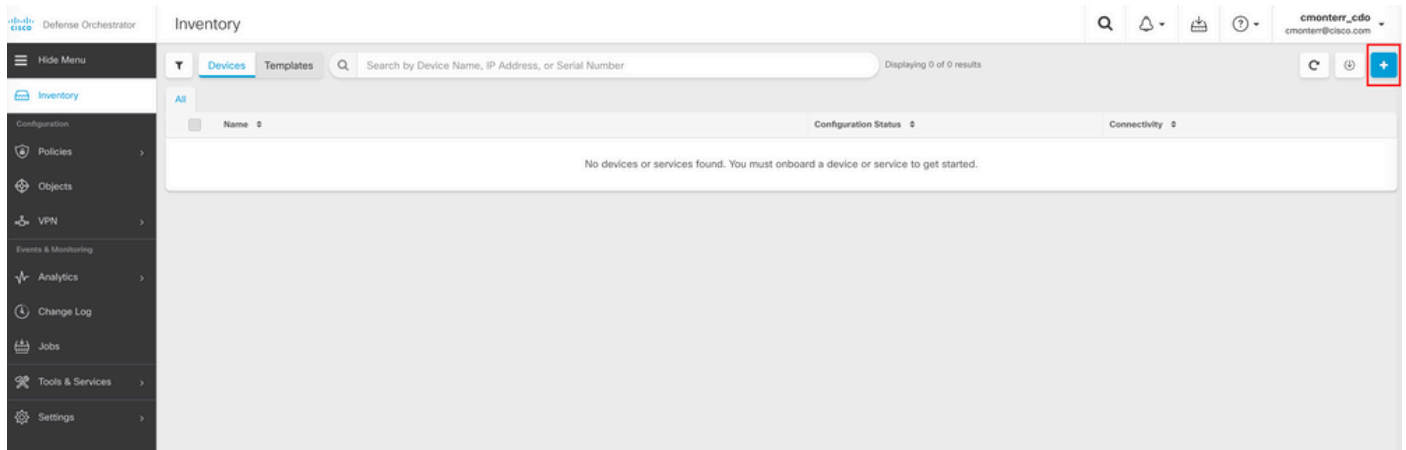
この製品は、オンプレミスのSecure Firewall Management CenterからSecure Firewall Management Center SaaSバージョンへの移行を目的として設計されています。

設定

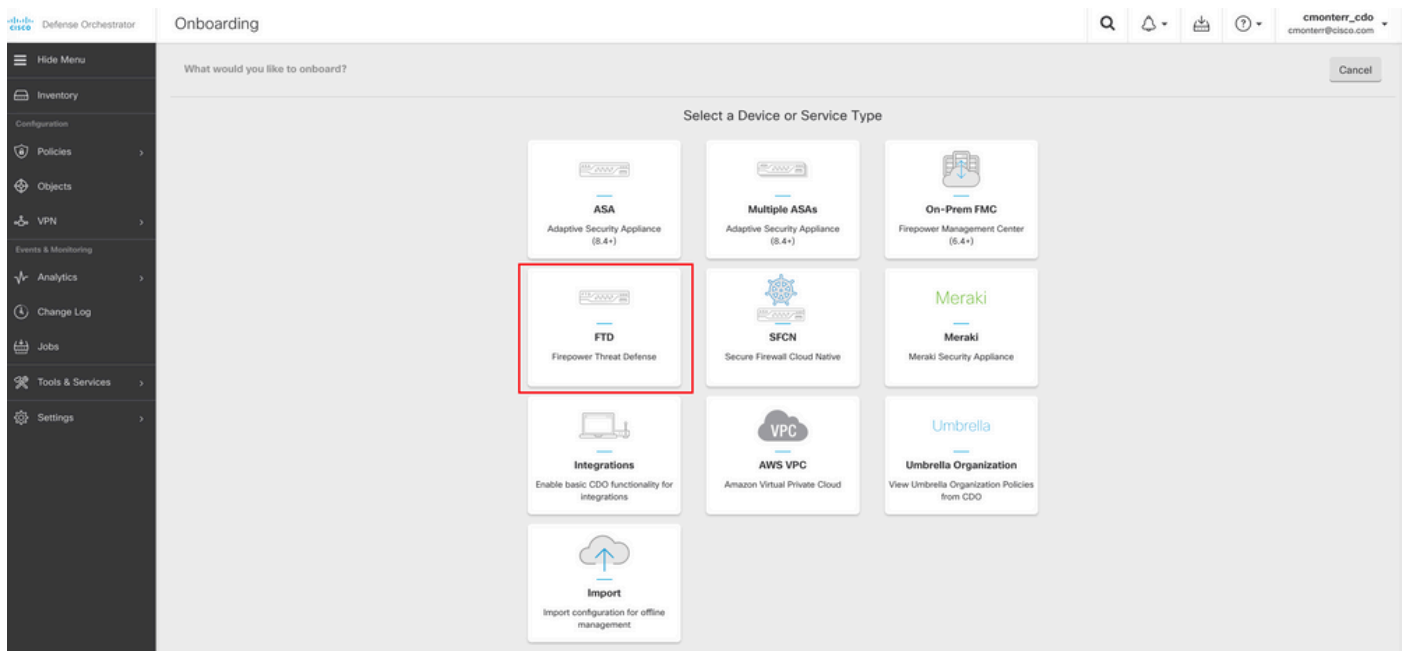
CDOにクラウド提供のFirepower Management Centerを導入します。

次の図は、クラウドで提供されるFMCをCDOに導入するために必要な初期セットアッププロセスを示しています。

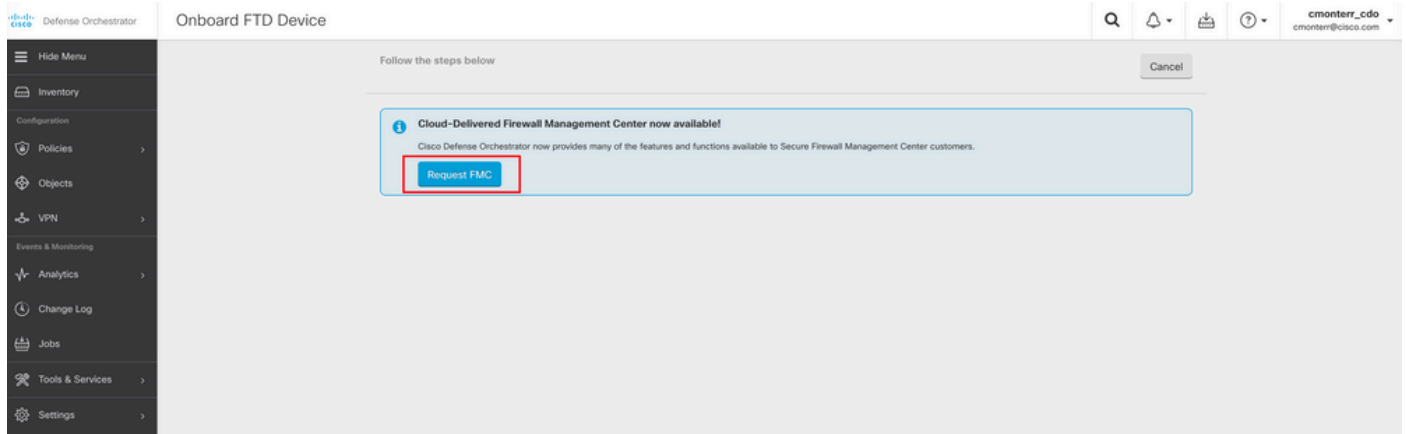
最初に、Menu > Inventory 新しいデバイスを追加します。



選択 Firepower Threat Defense (FTD).

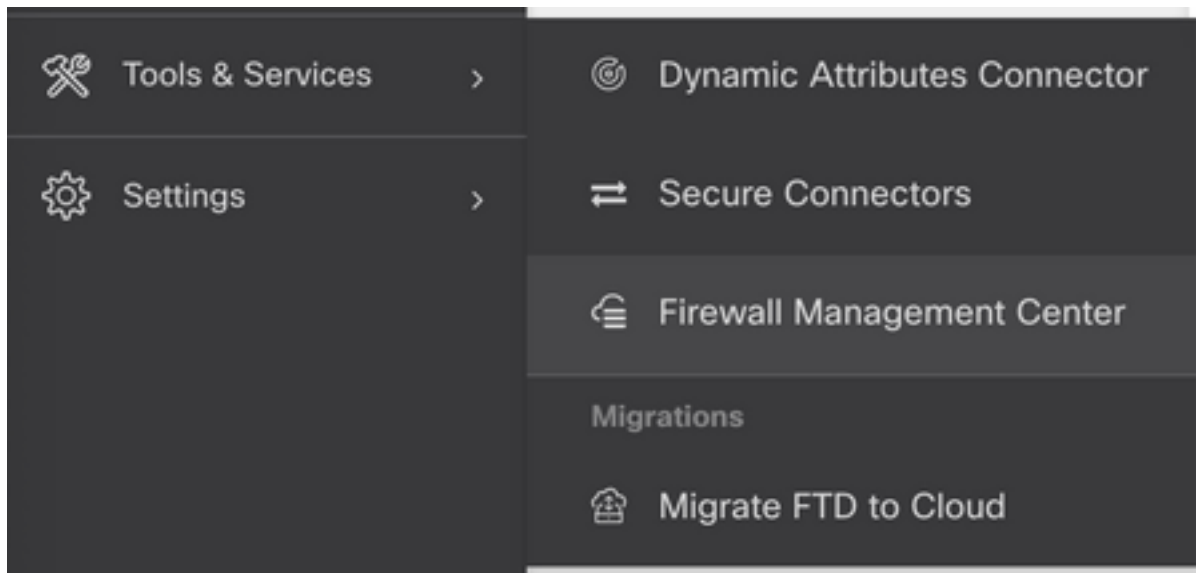


選択 Request FMC Firepower Management Centerを要求します。

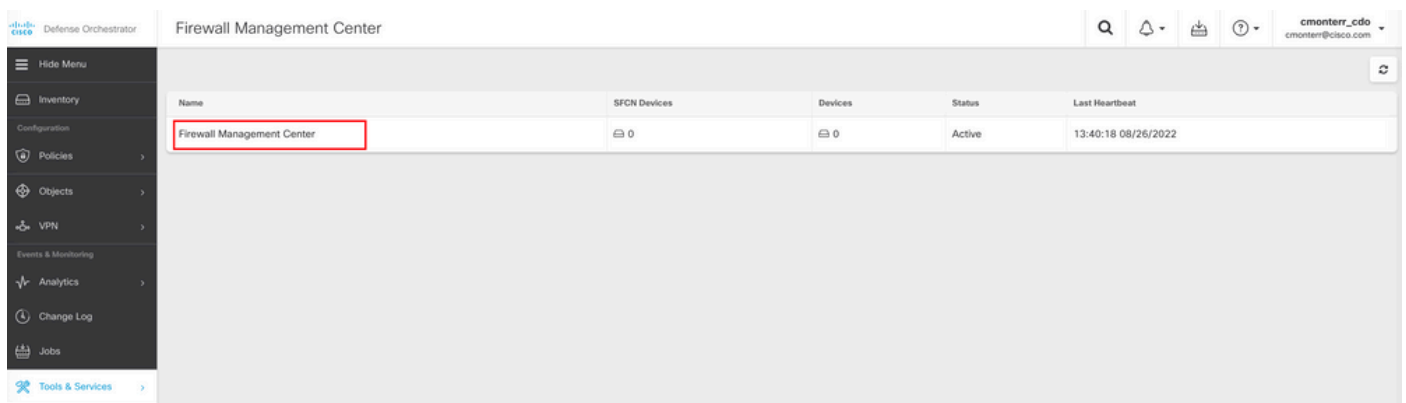


注:[Request FMC]オプションは、テナントにcdFMCがない場合にのみ表示されます。

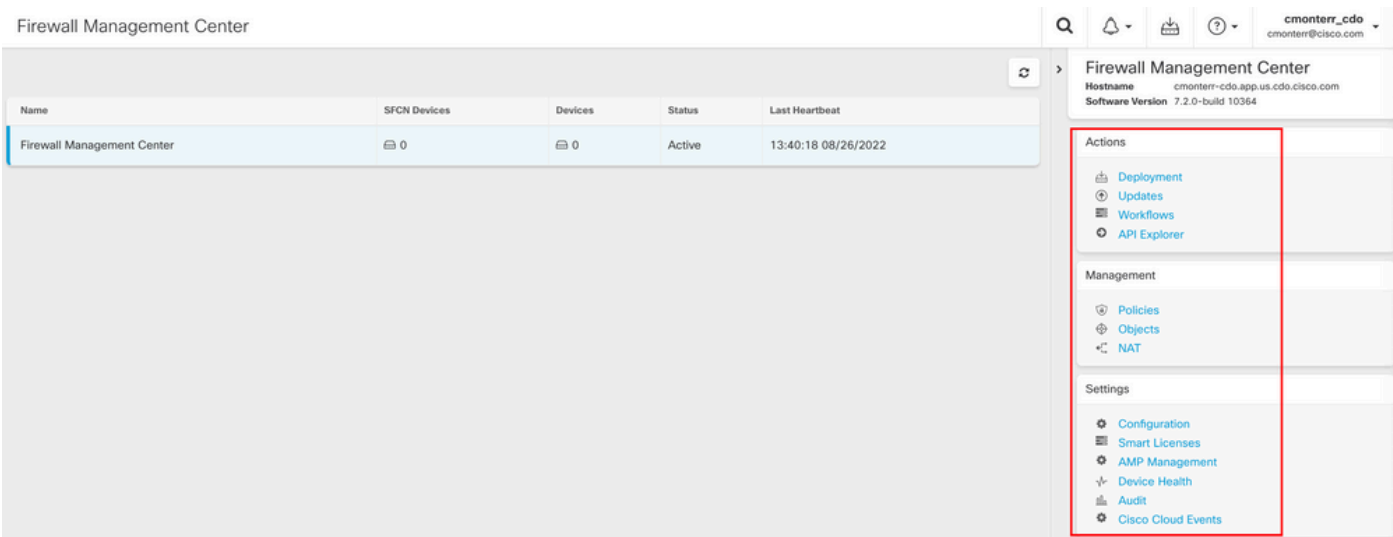
移動先 Menu > Tools & Services > Firewall Management Center cdFMCを使用する準備が整ったら、次の手順を実行します。



目的のcdFMCを選択して、cdFMC情報を表示します。



cdFMCのグラフィカルユーザインターフェイス(GUI)にアクセスするには、右側にあるオプションのいずれかを選択します。



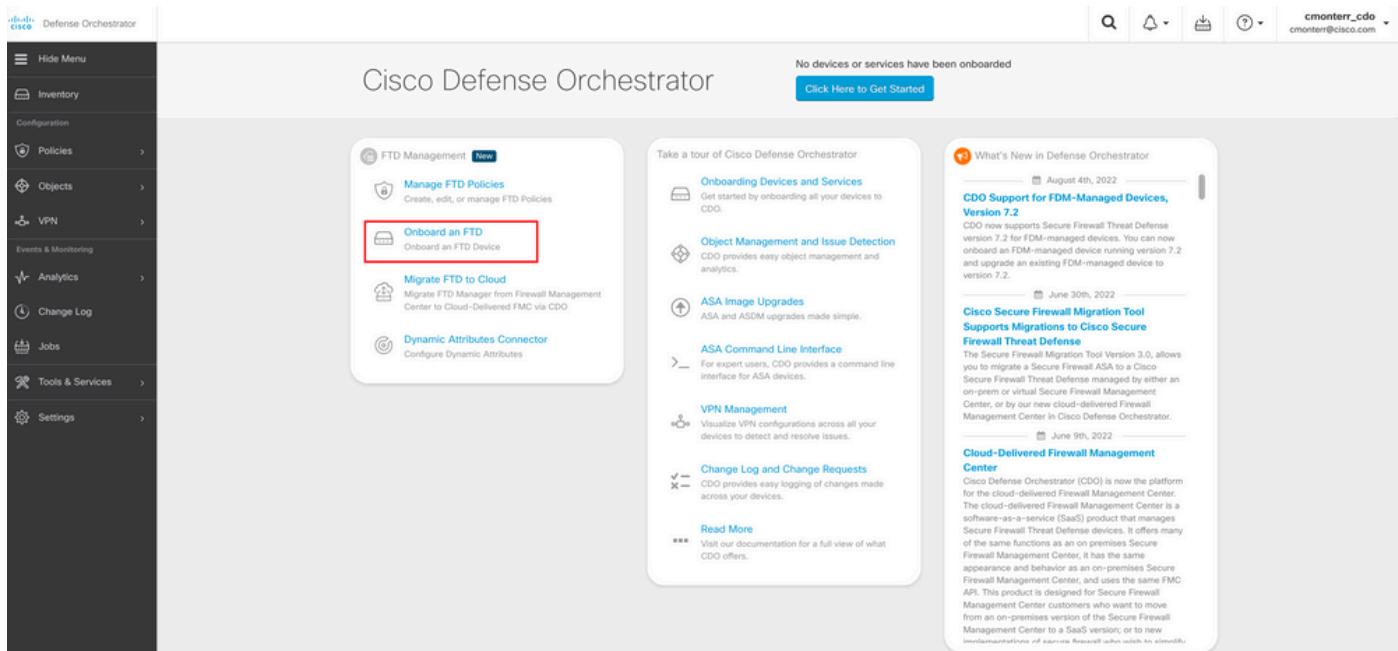
これでcdFMCのGUIが表示されます。



クラウド提供のFMCでのFTDのオンボーディング

次の図は、コマンドラインインターフェイス(CLI)登録キーを使用してcdFMCに登録するためにFTDをオンボードする方法を示しています。

最初に、 **Onboard an FTD CDO** ホームページで確認できます。



次に、 **Use CLI Registration Key** オプション。

Onboard FTD Device

Follow the steps below

Cancel

Firepower Threat Defense
90-day Evaluation License:
89 days left
[Manage Smart License](#)

Important: After onboarding your FTD, it will be managed by Firewall Management Center in CDO. Note that use of the firewall device manager will not be available after onboarding, and all existing policy configurations will be reset. You will need to reconfigure policies from CDO after onboarding. [Learn more](#)

Use CLI Registration Key
Onboard a device using a registration key generated from CDO and applied on the device using the Command Line Interface. (FTD 7.0.3+ & 7.2+)

Use Serial Number
Use this method for low-touch provisioning or for onboarding configured devices using their serial number. (FTD 7.2+)

続いて、要求されたFTDv情報と必要なFTDv情報を入力します。

1 Device Name **FTDv** [Edit](#)

2 Policy Assignment **Access Control Policy: Default Access Control Policy** [Edit](#)

3 Subscription License

Please indicate if this FTD is physical or virtual:

Physical FTD Device

Virtual FTD Device

Performance Tier (FTDv 7.0 and above only)

FTDv100 - Tiered (16 core / 32 GB)

License Type	Includes
<input checked="" type="checkbox"/> Base License	Base Firewall Capabilities
<input type="checkbox"/> Threat	Intrusion Policy
<input type="checkbox"/> Malware	File Policy
<input type="checkbox"/> URL License	URL Reputation
<input type="checkbox"/> RA VPN VPNOnly	RA VPN

[Next](#)

Enable subscription licenses. CDO will attempt to enable the selected licenses when the device is connected to CDO and registered with the supplied Smart License. [Learn more about Cisco Smart Accounts.](#)

Note: All virtual FTDs require performance tier license. Make sure your subscription licensing account contains the available licenses you need. Its important to choose the tier that matches the license you have in your account. Until you choose a tier, your FTDv defaults to FTDv50 selection.

最後に、cdFMCは特定の CLI KeyデバイスのCLIキー。

4 CLI Registration Key

1 Ensure the device's initial configuration is complete before trying to apply the registration key. [Learn more](#)

2 Copy the CLI Key below and paste it into the CLI of the FTD

```
configure manager add cmonterr-cdo.app.us.cdo.cisco.com
NaRZpWdiG4waNYJMqVAXdKqsukd2nDTn 6qDJQJAYKn53d0TnEifT0XF5nseZ43pd cmonterr-
cdo.app.us.cdo.cisco.com
```

[Next](#)

コピー : CLI Key CLIにログインします。

```
> configure manager add cmonterr-cdo.app.us.cdo.cisco.com NaRZpWdiG4waNYJMQVAXdK
qsukd2nDTn 6qDJQJAYKn53d0TnEifT0XF5nseZ43pd cmonterr-cdo.app.us.cdo.cisco.com
File HA_STATE is not found.
```

Manager cmonterr-cdo.app.us.cdo.cisco.com successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

```
>
> show managers
Type                : Manager
Host                 : cmonterr-cdo.app.us.cdo.cisco.com
Display name        : cmonterr-cdo.app.us.cdo.cisco.com
Identifier           : 6qDJQJAYKn53d0TnEifT0XF5nseZ43pd
Registration         : Pending
```

cdFMCが登録タスクを開始します。

The screenshot shows the Cisco Defense Orchestrator (CDO) interface. The 'Inventory' section is active, displaying a table with one device: 'FTDv' (FTD). The 'Connectivity' column for this device shows 'Onboarding', which is highlighted with a red box. To the right, the 'Device Details' section is expanded, and the 'Registration Pending' status is highlighted with a red box. Below this, there is a message: 'Waiting for Device Registration to start. Please complete the onboarding process by executing the following registration command on the device (ignore if already done). Make sure your FTD can connect to cmonterr-cdo.app.us.cdo.cisco.com.' Below the message, the command 'configure manager add cmonterr-cdo.a...' is shown with a copy icon.

注：登録プロセスを完了するには、FTDデバイスがポート8305(sftunnel)および443を介してCDOテナントと通信していることを確認してください。詳細な[ネットワーク要件](#)を参照してください。

注：ホストに接続できない場合は、`configure network dns <address>`コマンドを使用してFTD-CLIのDNS設定を修正できます。

登録プロセスを監視するには、 **Device Actions > Workflows..**

The screenshot shows the 'Workflows' page in the CDO interface. The table below shows the status of two workflows:

Name	Priority	Condition	Current State	Last Active	Time
fmceRegisterFtdStateMachine	On Demand	Done	Done	8/30/2022, 3:35:50 PM	8/30/2022, 3:33:11 PM / 8/30/2022, 3:35:50 PM
ftdcOnboardingStateMachine	On Demand	Done	Done	8/30/2022, 3:32:50 PM	8/30/2022, 3:32:50 PM / 8/30/2022, 3:32:50 PM

[Expand the] Active 追加情報を得るために、次の図はFTDvが正常に登録された方法を示しています。

Workflows

Return to Inventory

FTDv (FTD)

Name	Priority	Condition	Current State	Last Active	Time
ACTION	TIME	START STATE	END STATE	RESULT	
PollingDelayedCheckAction	15:34:46.812 / 15:34:46.819	POLLING_WAIT_BEFORE_CHECK_REGISTER_FTD	● INITIATE_GET_TASK_STATUS	● SUCCESS	
FmcRequestGetAction	15:35:17.324 / 15:35:17.724	INITIATE_GET_TASK_STATUS	● WAIT_FOR_GET_TASK_STATUS	● SUCCESS	
FmcQueryTaskStatusResponseHandler	15:35:18.223 / 15:35:18.244	AWAIT_RESPONSE_FROM_executeFmcRequests	● POLLING_WAIT_BEFORE_CHECK_REGISTER_FTD	JOB_IN_PROGRESS	
PollingDelayedCheckAction	15:35:18.288 / 15:35:18.299	POLLING_WAIT_BEFORE_CHECK_REGISTER_FTD	● INITIATE_GET_TASK_STATUS	● SUCCESS	
FmcRequestGetAction	15:35:48.708 / 15:35:49.173	INITIATE_GET_TASK_STATUS	● WAIT_FOR_GET_TASK_STATUS	● SUCCESS	
FmcQueryTaskStatusResponseHandler	15:35:49.639 / 15:35:49.652	AWAIT_RESPONSE_FROM_executeFmcRequests	● INITIATE_GET_DEVICE_RECORDS_REGISTER_FTD	JOB_SUCCEEDED	
FmcRequestDeviceRecordsAction	15:35:49.674 / 15:35:50.084	INITIATE_GET_DEVICE_RECORDS_REGISTER_FTD	● WAIT_FOR_DEVICE_RECORDS_REGISTER_FTD	● SUCCESS	
FmcFilterDeviceResponseHandler	15:35:50.496 / 15:35:50.510	AWAIT_RESPONSE_FROM_executeFmcRequests	● DONE	● SUCCESS	
HOOK	TYPE	TIME	RESULT		
SaveInitialConnectivityStateBeforeHook	Before	15:33:11.229 / 15:33:11.231	Saved Connectivity State to context		
UpdateSMContextWithDeviceVersionHook	Before	15:33:11.231 / 15:33:11.234	setDeviceVersionInSMContext		
DeviceStateMachineClearErrorBeforeHook	Before	15:33:11.234 / 15:33:11.236	noErrorOccurred		
FmcRegisterFtdcStatusPreHook	Before	15:33:11.236 / 15:33:11.289	Executed pre hook successfully for FTD device: FTDv		
FmcRegisterFtdcStatusHook	After	15:35:50.517 / 15:35:50.519	Executed hook successfully		
NotifyOnConnectivityStateChangeAfterHook	After	15:35:50.519 / 15:35:50.521	Notification skipped for this event		
UpdateSMContextWithDeviceAsaNgPolicyFlagHook	After	15:35:50.521 / 15:35:50.523	notAsaDevice		
AddDeviceNameToStateMachineDebugAfterHook	After	15:35:50.523 / 15:35:50.528	Added device name to debug record		
DeviceStateMachineSetEmpirAfterHook	After	15:35:50.528 / 15:35:50.530	noErrorOccurred		
ftdcOnboardingStateMachine	● On Demand	● Done	● Done	8/30/2022, 3:32:50 PM	8/30/2022, 3:32:50 PM / 8/30/2022, 3:32:50 PM

Inventory

Devices Templates

Search by Device Name, IP Address, or Serial Number

Displaying 1 of 1 results

FTDv

Name	Configuration Status	Connectivity
FTDv FTD	○ Synced	● Online

Device Details

Location: n/a
Model: Cisco Firepower Threat Defense for Azure
Serial: 9AGTAFW24C6
Version: 7.2.0
Onboarding Method: Registration Key
Short Version: 3.1.21.1-126

Synced
Your device's configuration is up-to-date.

Device Actions

- Check for Changes
- Manage Licenses
- Workflows
- Remove

Monitoring

- Health

Device Management

- Device Overview
- Routing
- Interfaces
- Inline Sets
- DHCP
- VTEP
- High Availability

最後に、Device Management > Device Overview cdfmcにアクセスして、FTDvの概要ステータスを確認します。

FTDv

Cisco Firepower Threat Defense for Azure

Device Routing Interfaces Inline Sets DHCP VTEP

General	License	System
Name: FTDv Transfer Packets: No Mode: Routed Compliance Mode: None TLS Crypto Acceleration: Disabled Device Configuration: Import Export Download	Performance Tier: FTDv100 - Tiered (Core 16 / 32 GB) Base: Yes Export-Controlled Features: No Malware: No Threat: No URL Filtering: No AnyConnect Apex: No AnyConnect Plus: No AnyConnect VPN Only: No	Model: Cisco Firepower Threat Defense for Azure Serial: 9AGTAFW2406 Time: 2022-08-30 21:04:27 Time Zone: UTC (UTC+0:00) Version: 7.2.0 Time Zone setting for Time based Rules: UTC (UTC+0:00)
Inspection Engine	Health	Management
Inspection Engine: Snort 3 Revert to Snort 2	Status: ● Policy: Initial_Health_Policy 2022-06-04 01:25:03 Excluded: None	Host: NO-IP Status: ● Manager Access Interface: Management Interface

関連情報

- [テクニカル サポートとドキュメント – Cisco Systems](#)
- [クラウド提供のファイアウォール管理センターでCisco Secure Firewall Threat Defenseデバイスを管理](#)

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。