

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

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[クラウドで提供されるFirepower Management CenterをCDOに導入します。](#)

[クラウド配信FMCでのFTDのオンボード](#)

[関連情報](#)

---

## はじめに

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 )

FTDバージョン7.0.3以上

### 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 ( 入手可能 )
- 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、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

Cisco Defense Orchestrator(CDO)は、クラウドで提供されるFirewall Management Center(cdFMC)用のプラットフォームです。クラウドで提供される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のセキュアファイアウォールの脅威防御と同じ機能を多数提供します。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。

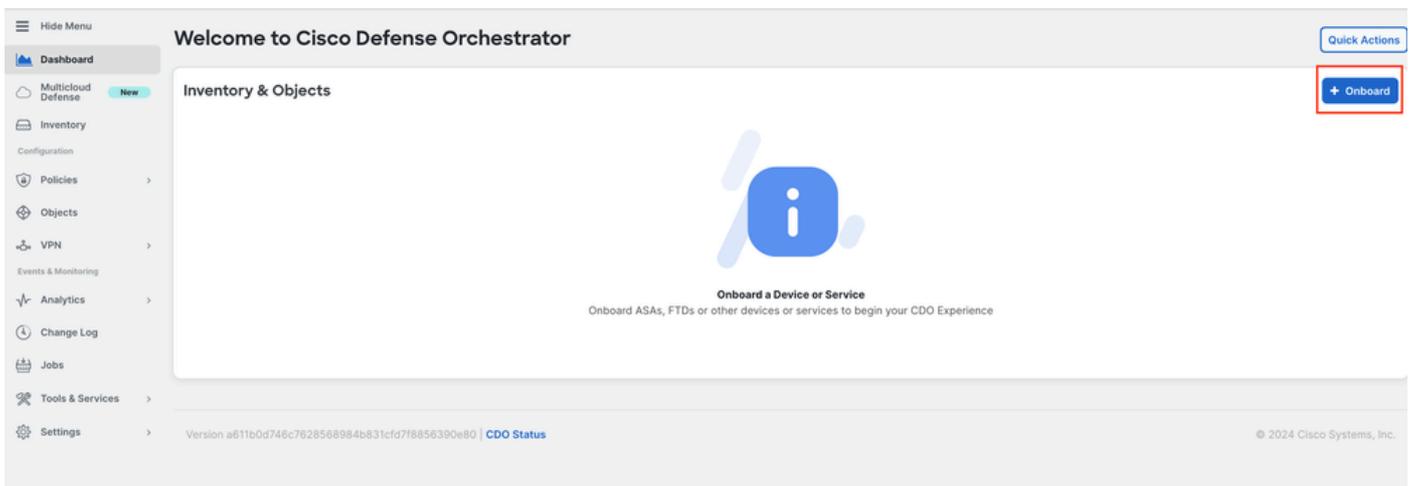
この製品は、オンプレミスのSecure Firewall Management CenterからSecure Firewall Management Center SaaSバージョンへの移行用に設計されています。

## 設定

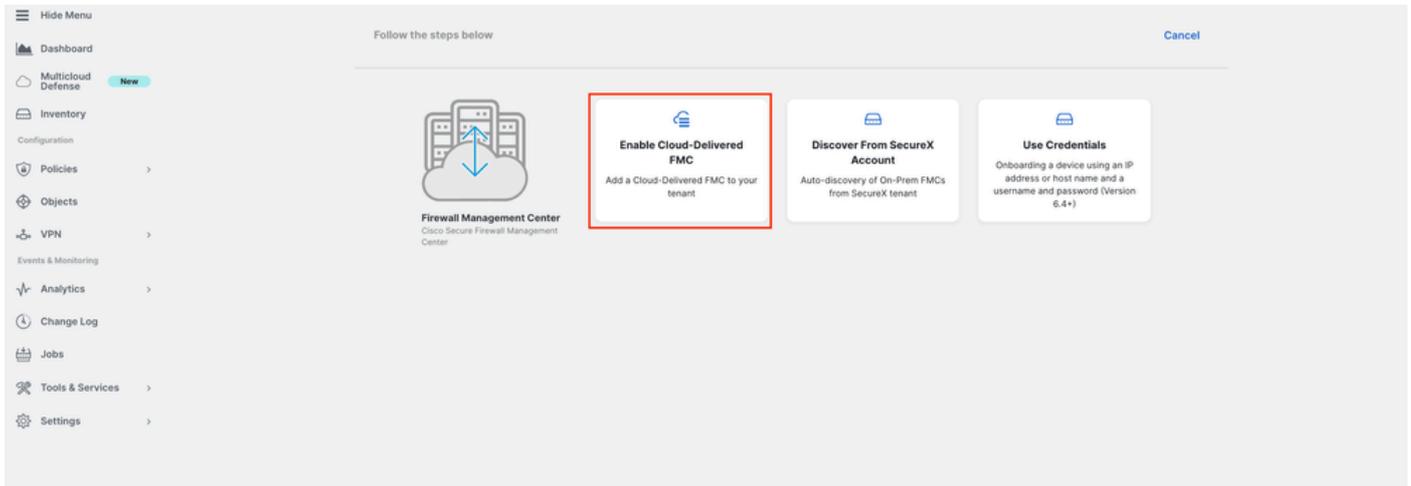
クラウドで提供されるFirepower Management CenterをCDOに導入します。

次の図は、クラウド配信の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。

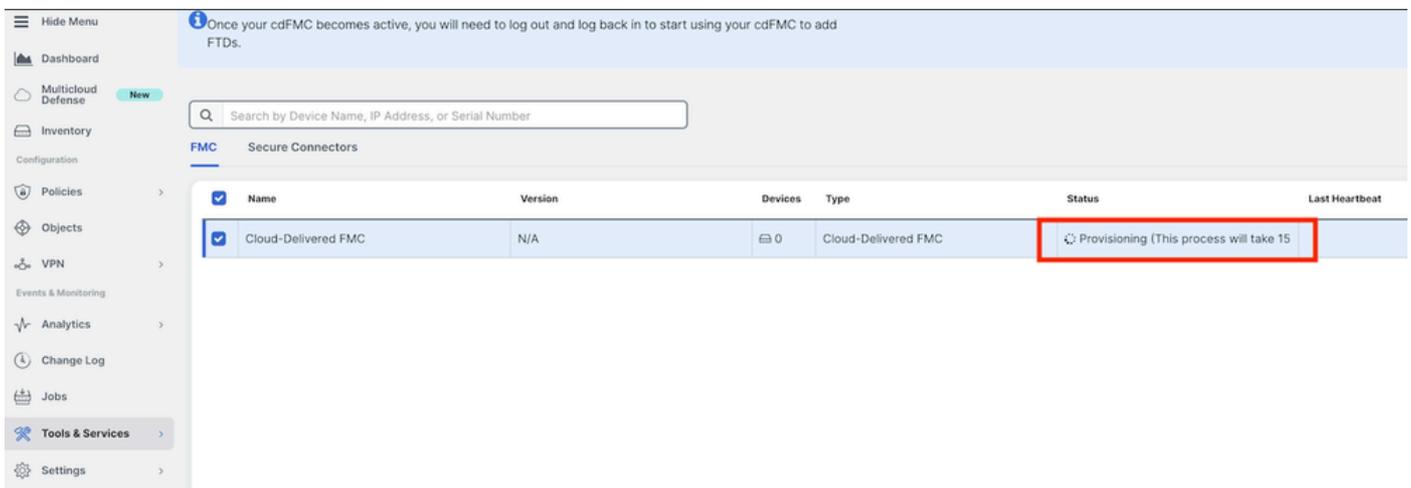
CDOメニューから、 **Tools & Services > Firewall Management Center > Onboard.**



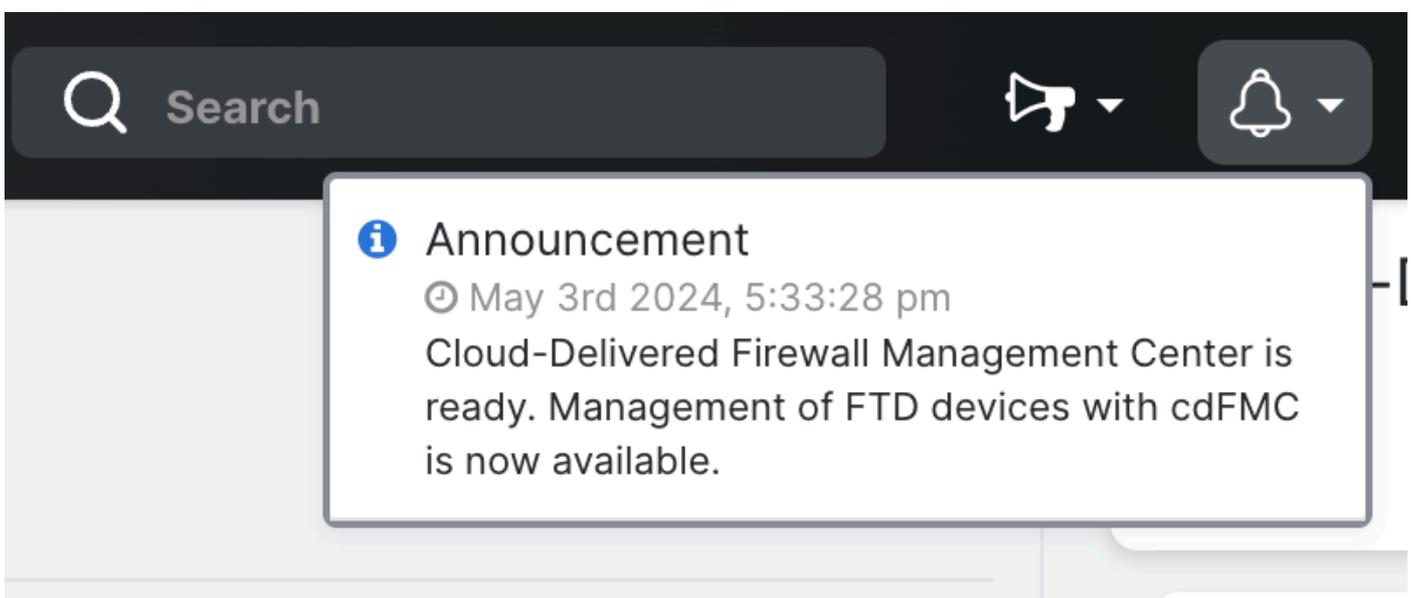
選択 Enable Cloud-Delivered FMC.

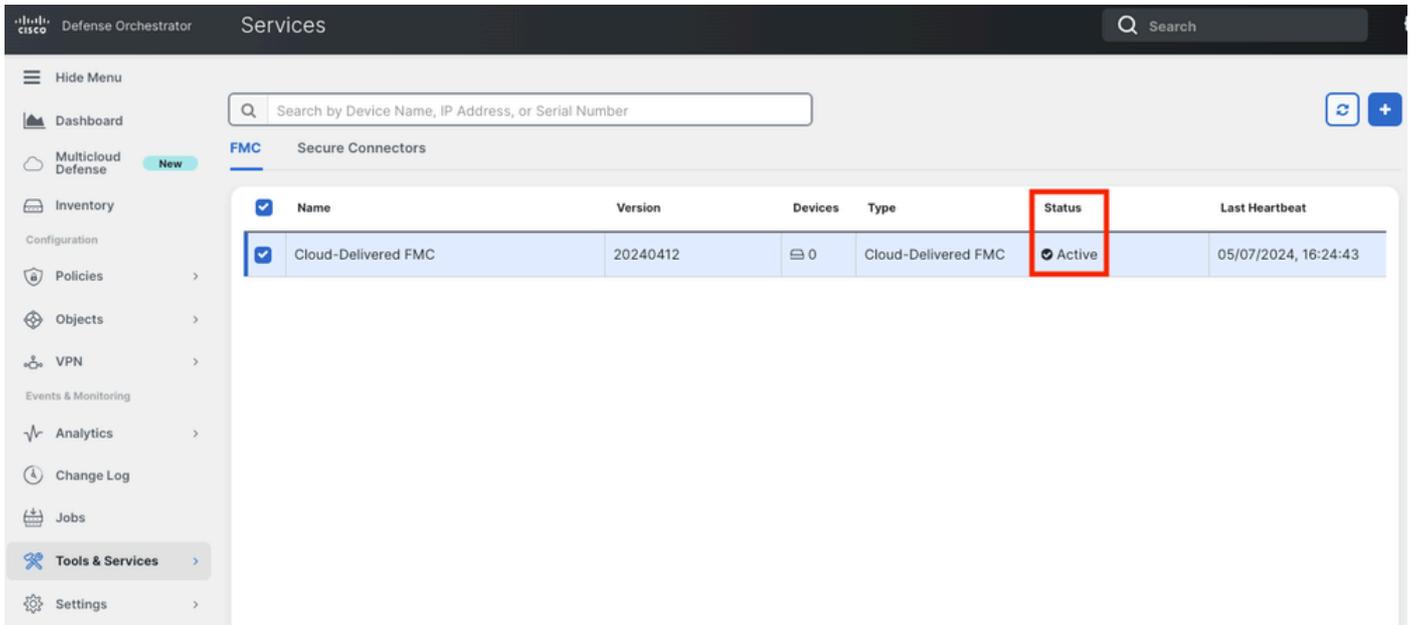


CDOは、クラウドで提供されるFirewall Management Center(FMC)インスタンスをバックグラウンドでプロビジョニングします。この処理が完了するまでに通常15 ~ 30分かかります。プロビジョニングの進行状況は、クラウド配信FMCのステータス列で追跡できます。



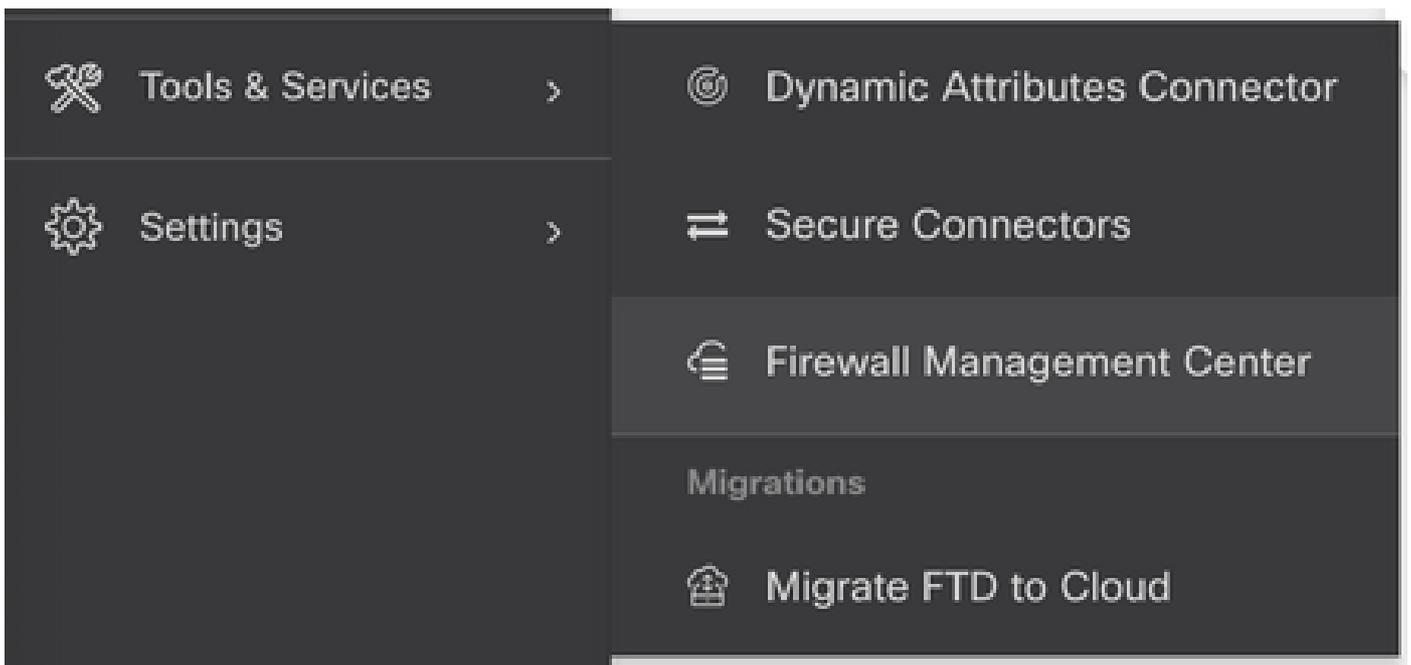
プロビジョニングが完了すると、ステータスが「アクティブ」に変わります。また、CDO通知パネルには、クラウド配信のFirewall Management Center is Ready通知が表示されます。



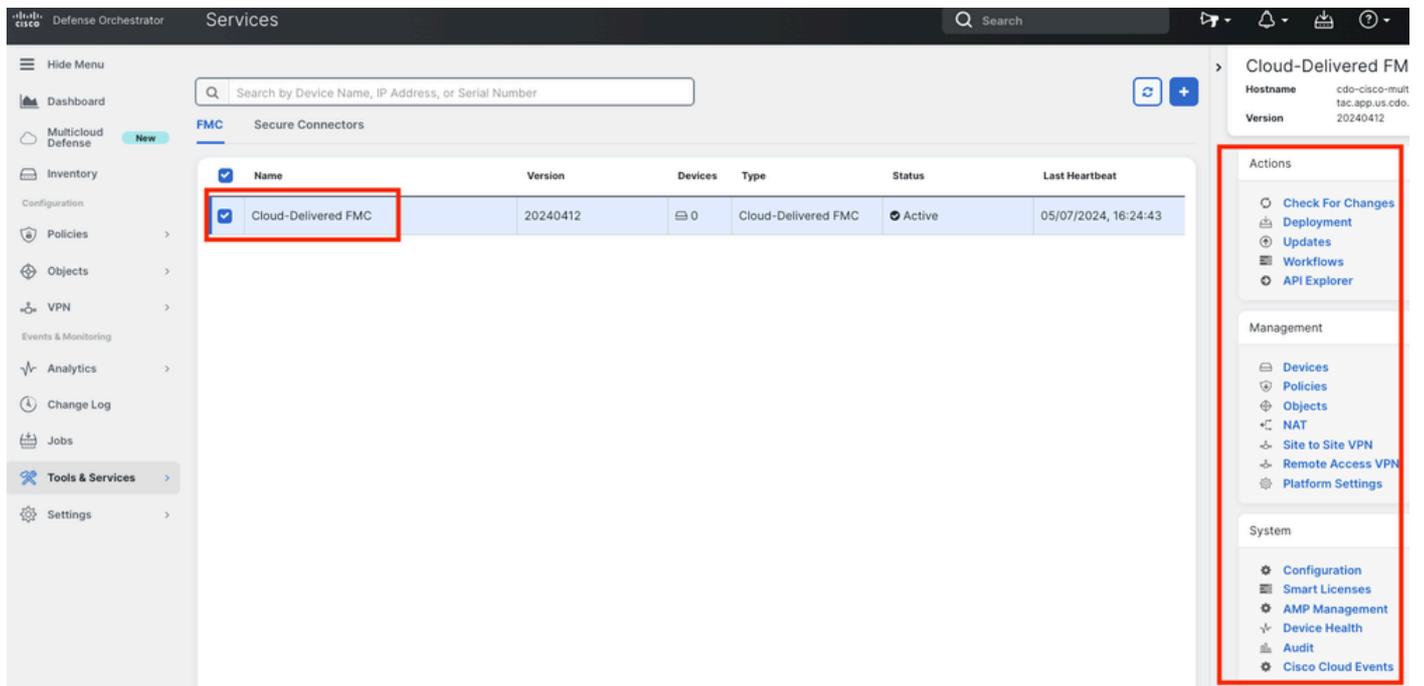


その後、脅威に対する防御デバイスをクラウド提供のFirewall Management Centerにオンボーディングし、管理できます。

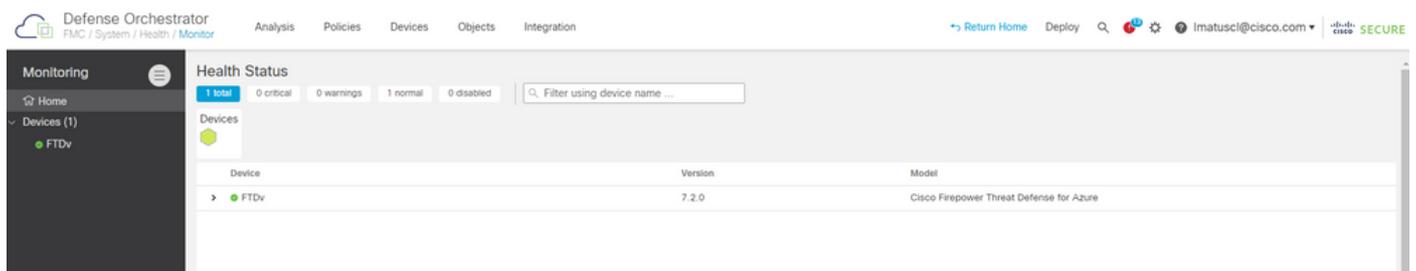
Menu > Tools & Services > Firewall Management Centerに移動します。



cdFMCを選択してcdFMC情報を表示し、cdFMCのグラフィカルユーザインターフェイス(GUI)にアクセスするために、右側で使用可能なオプションのいずれかを選択します。



cdFMCのGUIが表示されます。



クラウド配信FMCでのFTDのオンボード

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。

まず、CDOホームページで **Onboard an FTD** を選択します。

Defense Orchestrator

Hide Menu

Inventory

Configuration

Policies

Objects

VPN

Events & Monitoring

Analytics

Change Log

Jobs

Tools & Services

Settings

Cisco Defense Orchestrator

No devices or services have been onboarded

Click Here to Get Started

FTD Management **New**

- Manage FTD Policies  
Create, edit, or manage FTD Policies
- Onboard an FTD**  
Onboard an FTD Device
- Migrate FTD to Cloud  
Migrate FTD Manager from Firewall Management Center to Cloud-Delivered FMC via CDO
- Dynamic Attributes Connector  
Configure Dynamic Attributes

Take a tour of Cisco Defense Orchestrator

- Onboarding Devices and Services  
Get started by onboarding all your devices to CDO.
- Object Management and Issue Detection  
CDO provides easy object management and analytics.
- ASA Image Upgrades  
ASA and ASDM upgrades made simple.
- ASA Command Line Interface  
For expert users, CDO provides a command line interface for ASA devices.
- VPN Management  
Visualize VPN configurations across all your devices to detect and resolve issues.
- Change Log and Change Requests  
CDO provides easy logging of changes made across your devices.
- Read More  
Visit our documentation for a full view of what CDO offers.

What's New in Defense Orchestrator

August 4th, 2022

**CDO Support for FDM-Managed Devices, Version 7.2**

CDO now supports Secure Firewall Threat Defense version 7.2 for FDM-managed devices. You can now onboard an FDM-managed device running version 7.2 and upgrade an existing FDM-managed device to version 7.2.

June 30th, 2022

**Cisco Secure Firewall Migration Tool Supports Migrations to Cisco Secure Firewall Threat Defense**

The Secure Firewall Migration Tool Version 3.0, allows you to migrate a Secure Firewall ASA to a Cisco Secure Firewall Threat Defense managed by either an on-prem or virtual Secure Firewall Management Center, or by our new cloud-delivered Firewall Management Center in Cisco Defense Orchestrator.

June 9th, 2022

**Cloud-Delivered Firewall Management Center**

Cisco Defense Orchestrator (CDO) is now the platform for the cloud-delivered Firewall Management Center. The cloud-delivered Firewall Management Center is a software-as-a-service (SaaS) product that manages Secure Firewall Threat Defense devices. It offers many of the same functions as an on-premises Secure Firewall Management Center, it has the same appearance and behavior as an on-premises Secure Firewall Management Center, and uses the same FMC API. This product is designed for Secure Firewall Management Center customers who want to move from an on-premises version of the Secure Firewall Management Center to a SaaS version, or to new implementations of secure firewall with its cloud.

次に、**Use CLI Registration Key** ショーンを選択します。

Defense Orchestrator

Onboard FTD Device

Follow the steps below

Cancel

FTD

**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+)

要求された必要なFTDv情報の入力に進みます。

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 <span>VPNOnly</span>	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はデバイス固有の CLI Keyを作成します。

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

CLI Key を管理対象デバイスのCLIにコピーします。

```
> 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 'Inventory' page in Cisco Defense Orchestrator. The main table lists one device: 'FTDv' (FTD) with a connectivity status of 'Onboarding'. The right-hand panel displays 'Device Details' for 'FTDv', including fields for Location, Model, Serial, Version, Onboarding Method, and Registration Key. A 'Registration Pending' section is highlighted, containing instructions: '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.cisco.com.' Below this is a button labeled 'configure manager add cmonterr-cdo.a...'.

 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)と443を介してCDOテナントと通信できることを確認します。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。

登録プロセスをモニタするには、**Device Actions > Workflows**.に移動します。

The screenshot shows the 'Workflows' page in Cisco Defense Orchestrator. The table displays the following data:

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

追加の情報を得るために **Active** 状態を展開します。次の図は、FTDvが正常に登録された方法を示しています。

Return to Inventory

FTDv (FTD)

Name	Priority	Condition	Current State	Last Active	Time
<b>ACTION</b>	<b>TIME</b>	<b>START STATE</b>	<b>END STATE</b>	<b>RESULT</b>	
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	
<b>HOOK</b>	<b>TYPE</b>	<b>TIME</b>	<b>RESULT</b>		
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		
DeviceStateMachineSetErrorAfterHook	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
Search by Device Name, IP Address, or Serial Number
Displaying 1 of 1 results

All	Name	Configuration Status	Connectivity
<input checked="" type="checkbox"/>	FTDv FTD	○ Synced	● Online

**FTDv**  
FTD

**Device Details**

- Location: n/a
- Model: Cisco Firepower Threat Defense for Azure
- Serial: 9AGTAFW24C6
- Version: 7.2.0
- Onboarding Method: Registration Key
- Smart 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、cdFMCにアクセスし、FTDvの概要のステータスを確認するために、**Device Management > Device Overview** に移動します

。

## FTDv

Cisco Firepower Threat Defense for Azure

Device Routing Interfaces Inline Sets DHCP VTEP

<p><b>General</b></p> <p>Name: FTDv</p> <p>Transfer Packets: No</p> <p>Mode: Routed</p> <p>Compliance Mode: None</p> <p>TLS Crypto Acceleration: Disabled</p> <p>Device Configuration: <a href="#">Import</a> <a href="#">Export</a> <a href="#">Download</a></p>	<p><b>License</b></p> <p>Performance Tier: FTDv100 - Tiered (Core 16 / 32 GB)</p> <p>Base: Yes</p> <p>Export-Controlled Features: No</p> <p>Malware: No</p> <p>Threat: No</p> <p>URL Filtering: No</p> <p>AnyConnect Apex: No</p> <p>AnyConnect Plus: No</p> <p>AnyConnect VPN Only: No</p>	<p><b>System</b></p> <p>Model: Cisco Firepower Threat Defense for Azure</p> <p>Serial: 9AGTAFW24C6</p> <p>Time: 2022-08-30 21:04:27</p> <p>Time Zone: UTC (UTC+0:00)</p> <p>Version: 7.2.0</p> <p>Time Zone setting for Time based Rules: UTC (UTC+0:00)</p>
<p><b>Inspection Engine</b></p> <p>Inspection Engine: Snort 3</p> <p><a href="#">Revert to Snort 2</a></p>	<p><b>Health</b></p> <p>Status: <span style="color: green;">●</span></p> <p>Policy: Initial_Health_Policy 2022-06-04 01:25:03</p> <p>Excluded: None</p>	<p><b>Management</b></p> <p>Host: NO-IP</p> <p>Status: <span style="color: green;">●</span></p> <p>Manager Access Interface: <a href="#">Management Interface</a></p>

### 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。