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

内容

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。

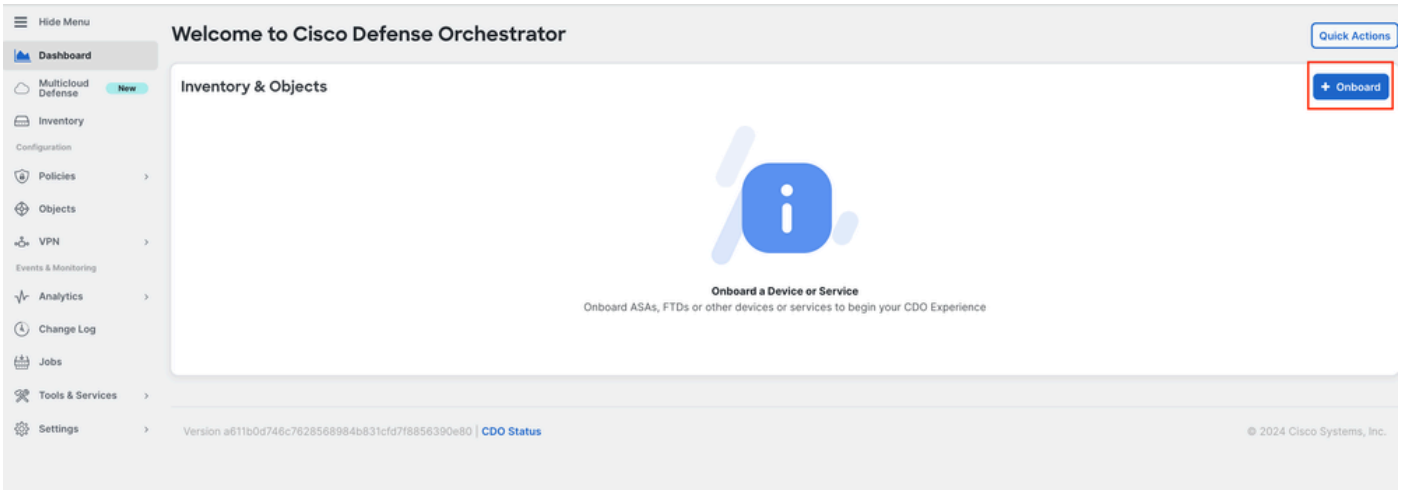
この製品は、オンプレミスのSecure Firewall Management CenterからSecure Firewall Management Center SaaSバージョンへの移行用に設計されています。

設定

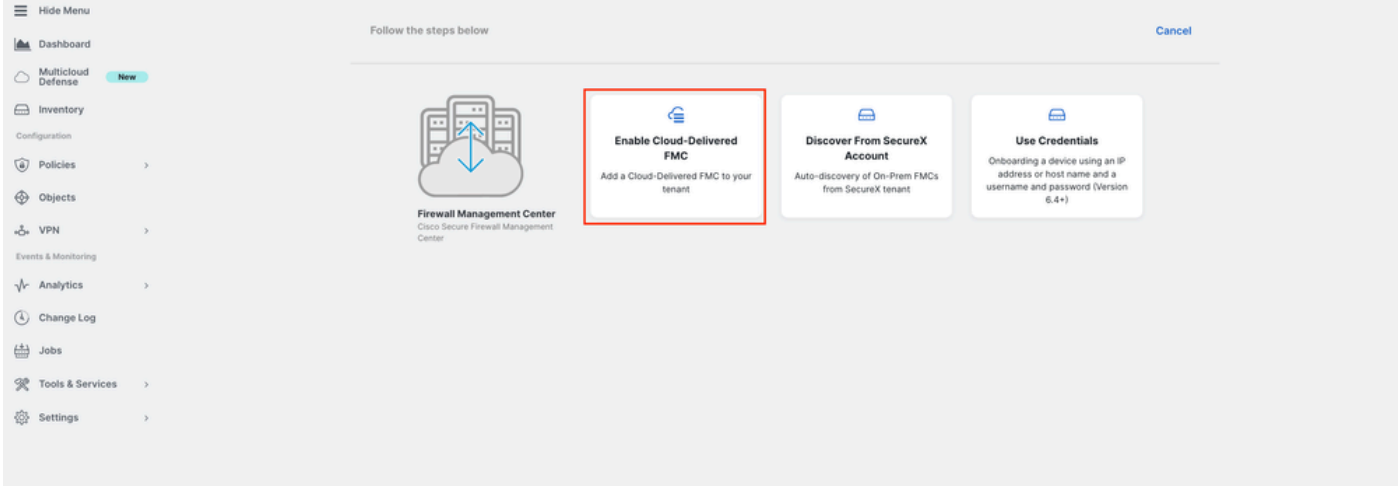
クラウドで提供されるFirepower Management CenterをCDOに導入します。

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。

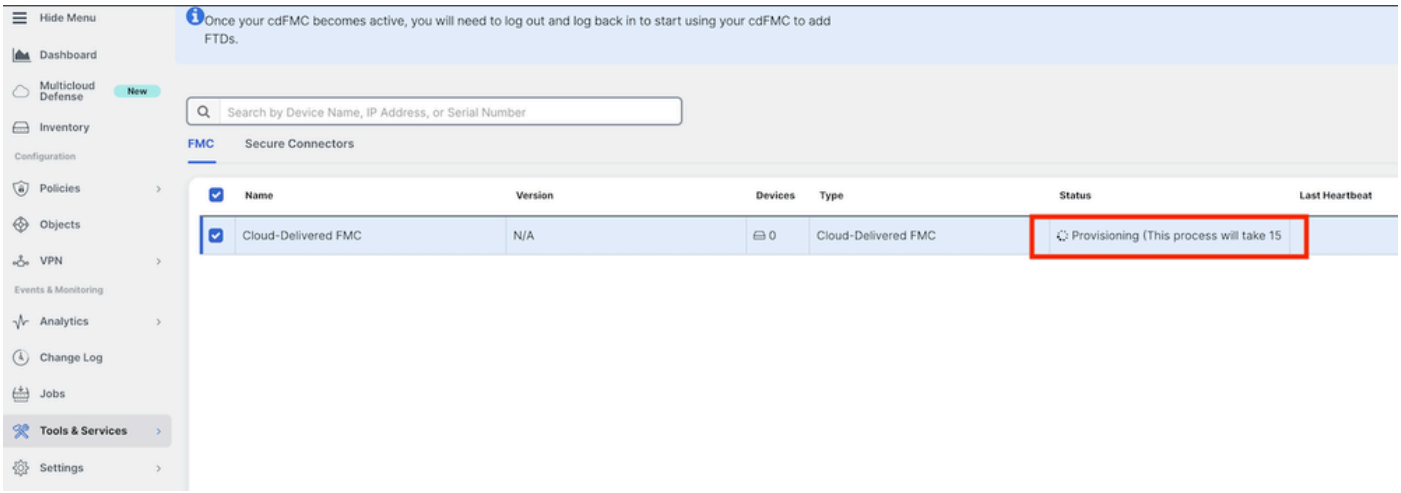
CDOメニューから、 **Tools & Services** > **Firewall Management Center** > **Onboard**.



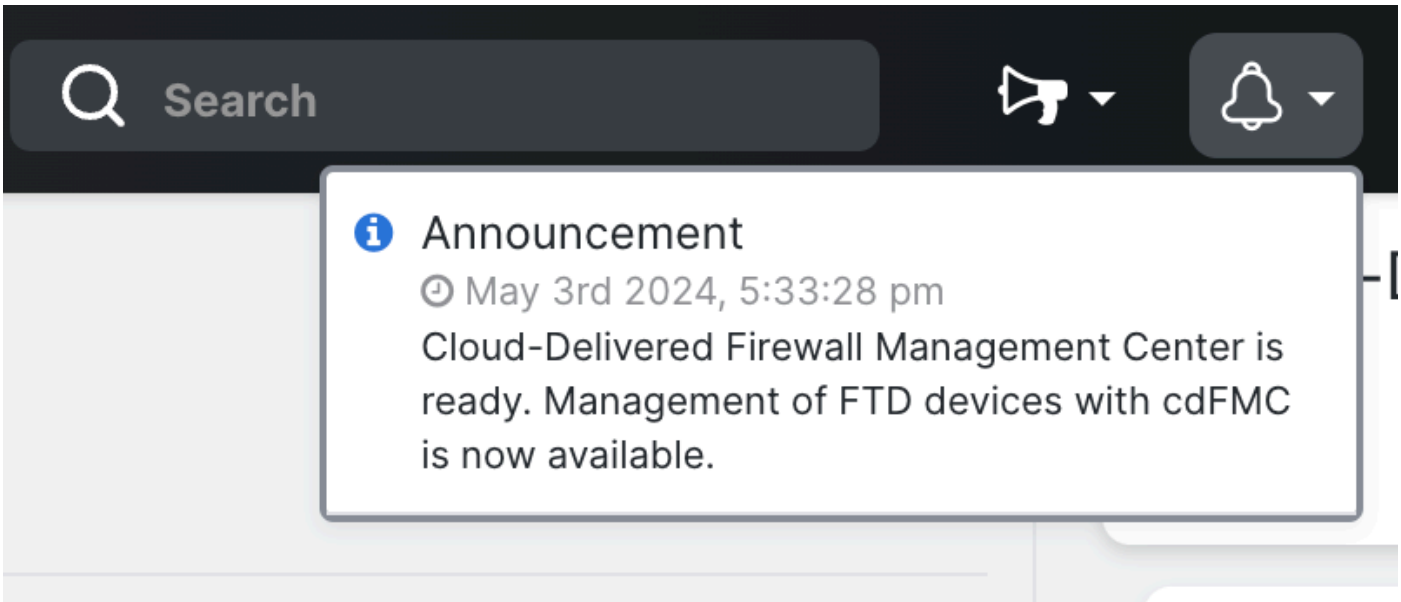
選択 Enable Cloud-Delivered FMC.

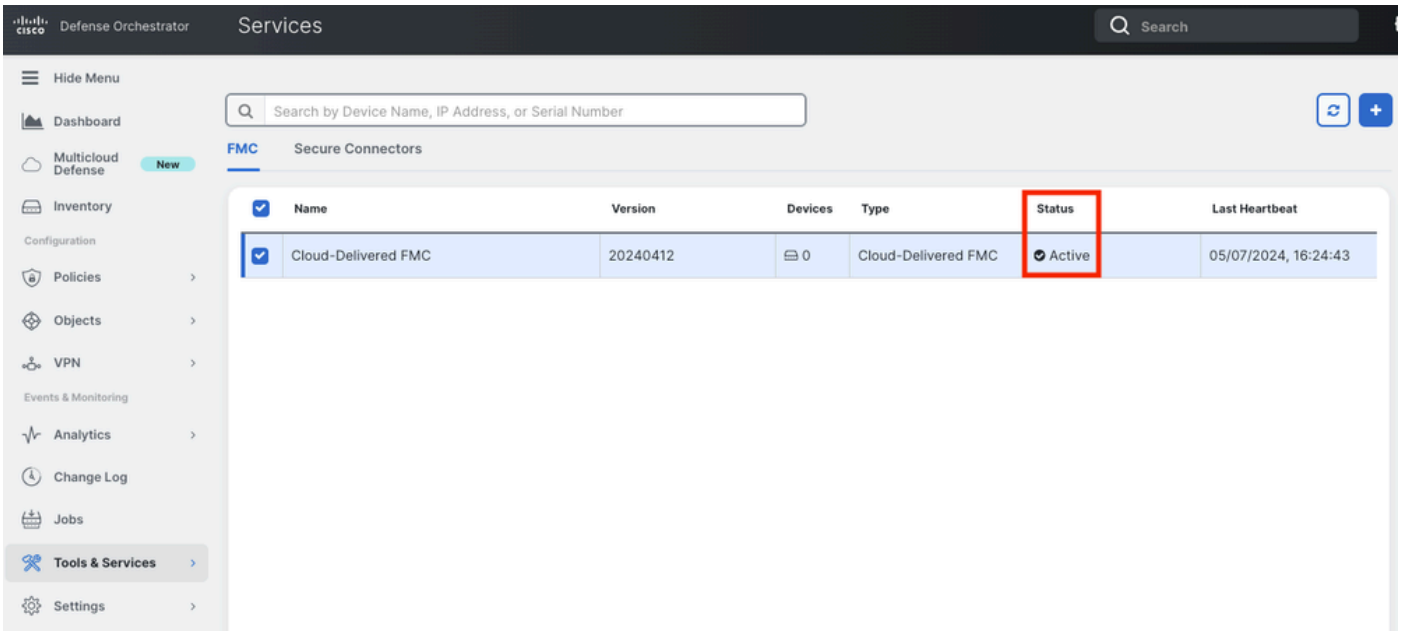


CDOは、クラウドで提供されるFirewall Management Center(FMC)インスタンスをバックグラウンドでプロビジョニングします。この処理が完了するまでに通常15 ~ 30分かかります。プロビジョニングの進行状況は、クラウド配信FMCのステータス列で追跡できます。



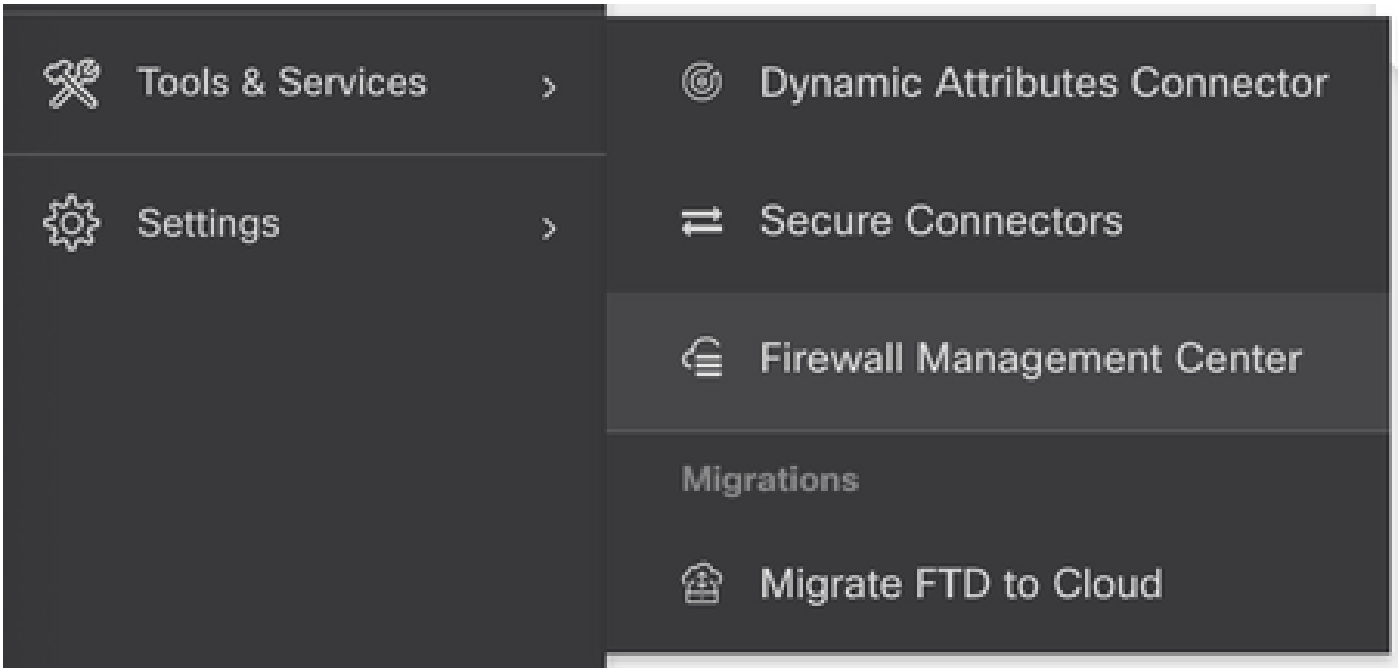
プロビジョニングが完了すると、ステータスが「アクティブ」に変わります。また、CDO通知パネルには、クラウド配信のFirewall Management Center is Ready通知が表示されます。



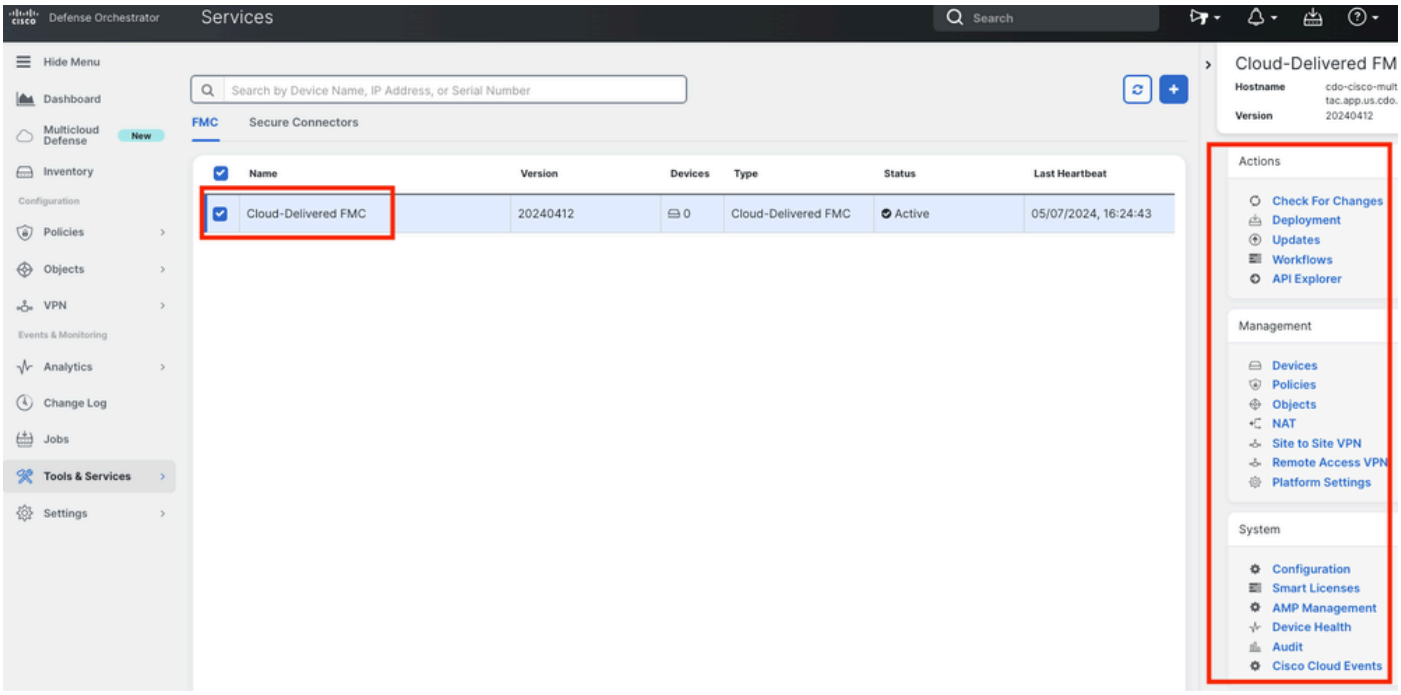


その後、脅威に対する防御デバイスをクラウド提供のFirewall Management Centerにオンボーディングし、管理できます。

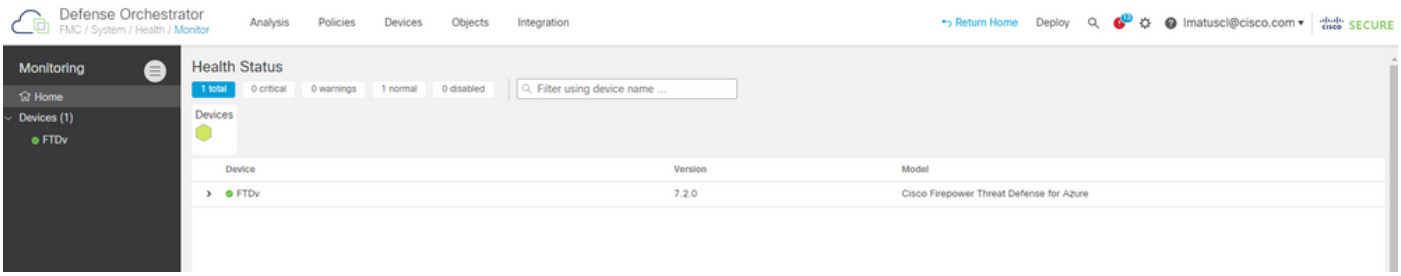
Menu > **Tools & Services** > **Firewall Management Center**に移動します。



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。



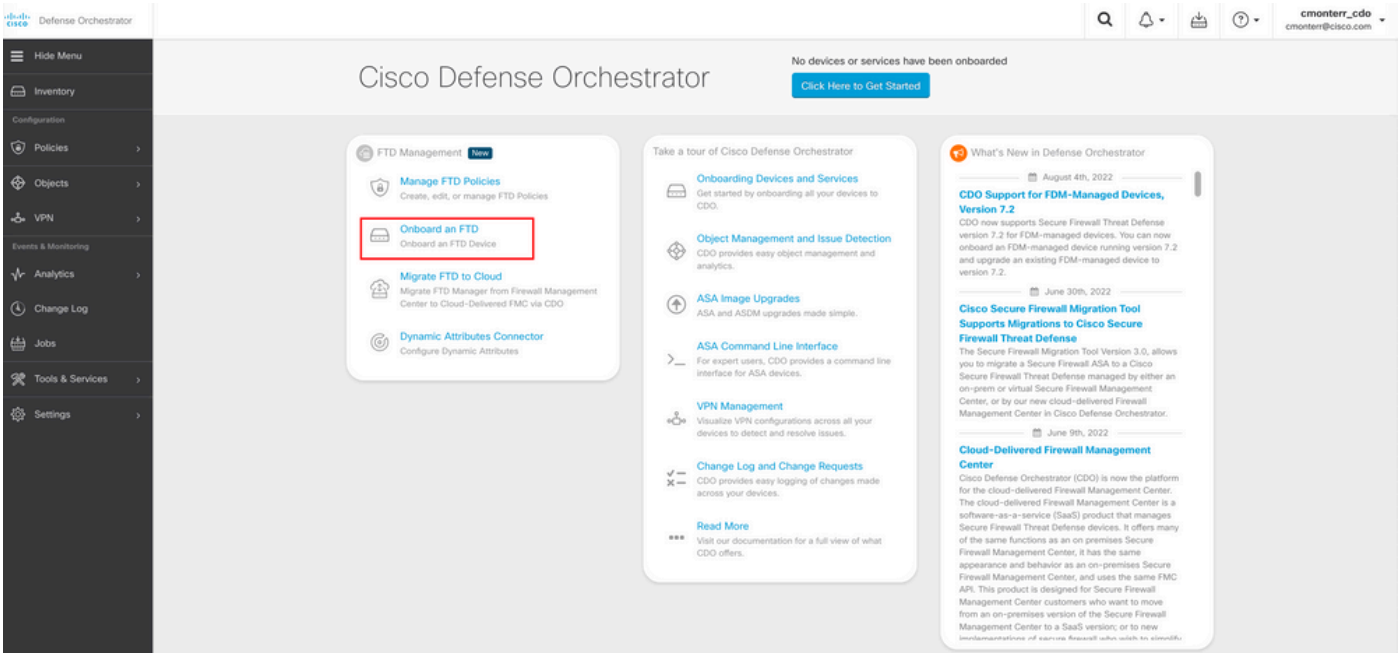
cdFMCのGUIが表示されます。



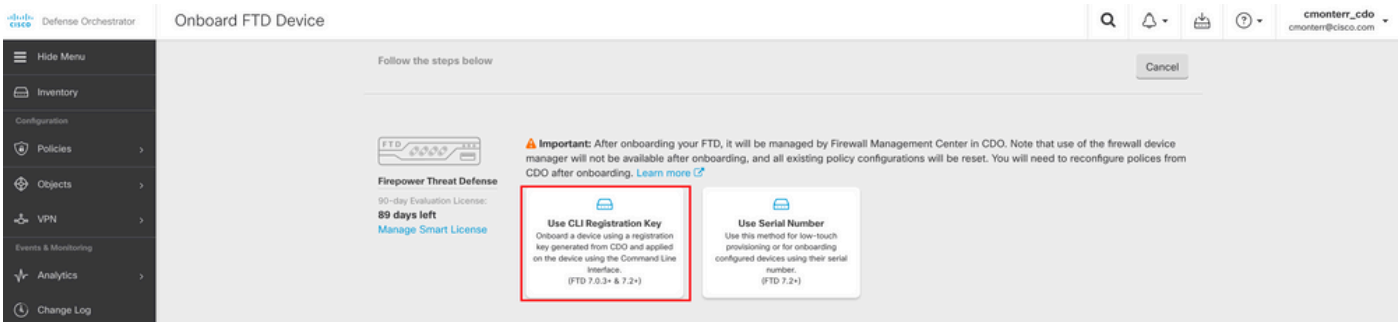
クラウド配信FMCでのFTDのオンボード

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。

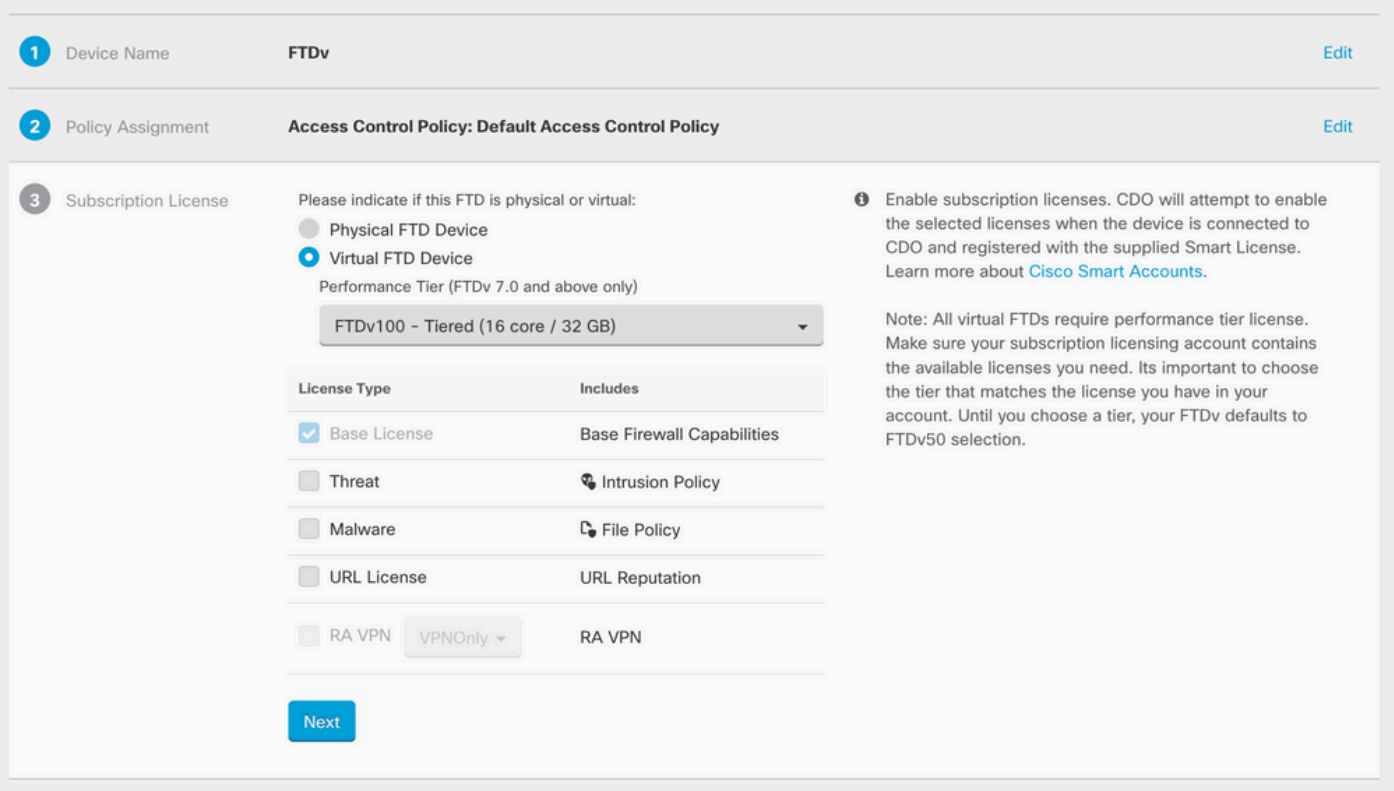
まず、CDOホームページで **Onboard an FTD** を選択します。



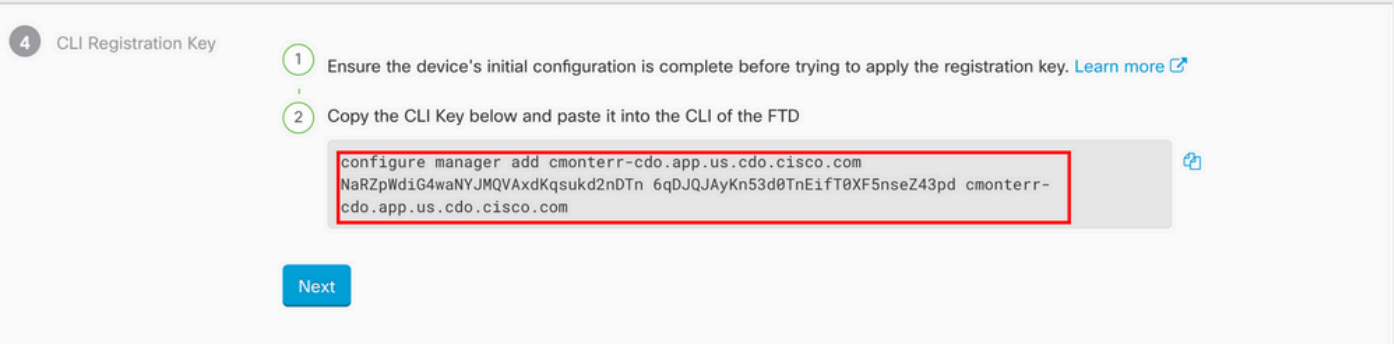
次に、オプ**Use CLI Registration Key** ションを選択します。



要求された必要なFTDv情報の入力に進みます。



最後に、cdFMCはデバイス固有の **CLI Key**を作成します。



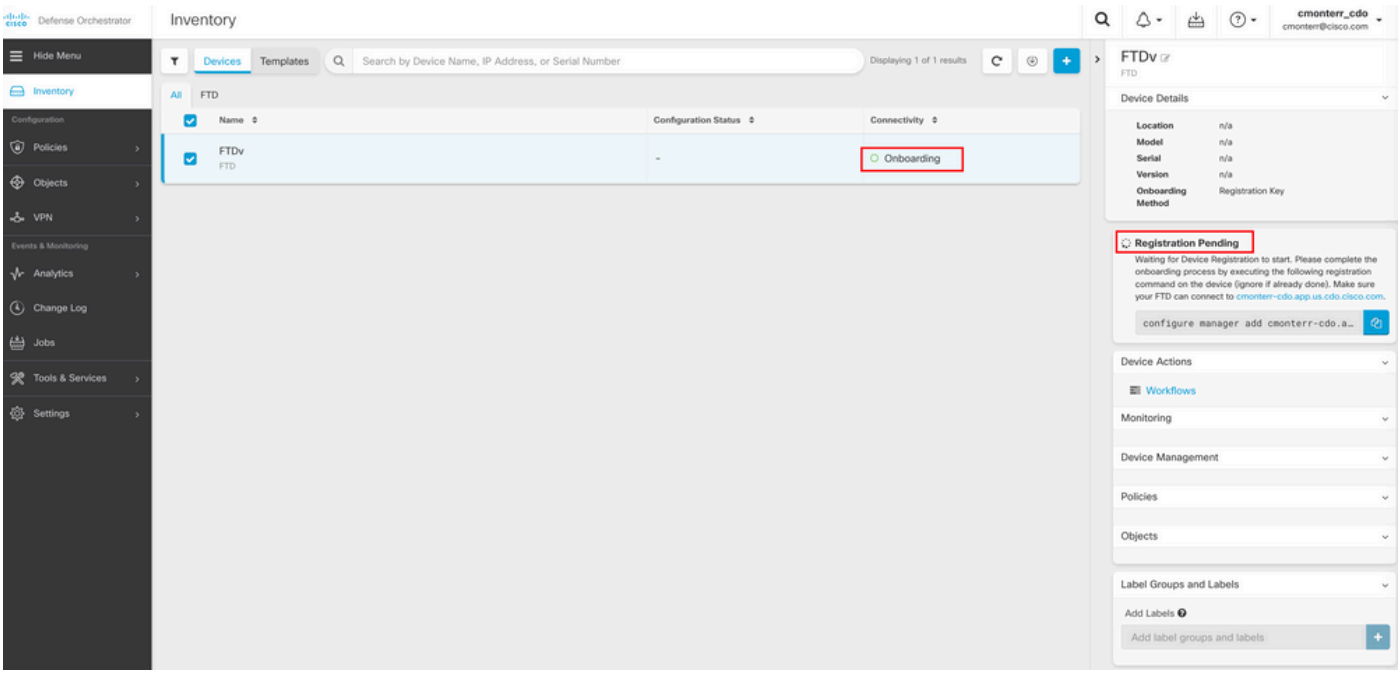
CLI Key を管理対象デバイスのCLIにコピーします。

```
> 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
```

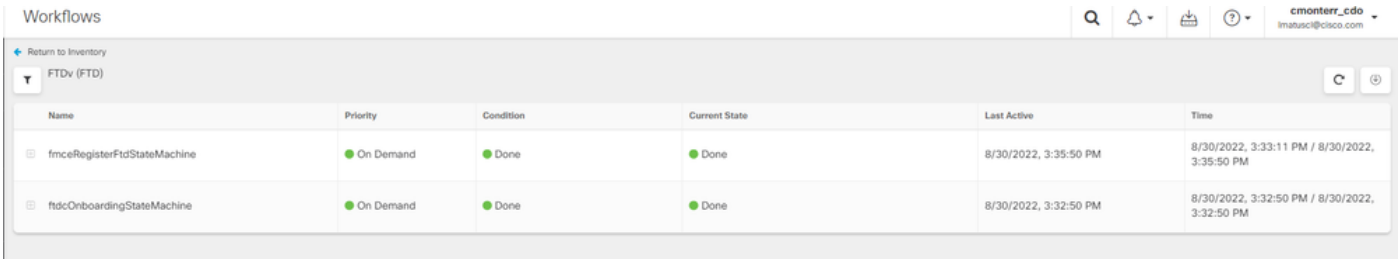
cdFMCが登録タスクを開始します。



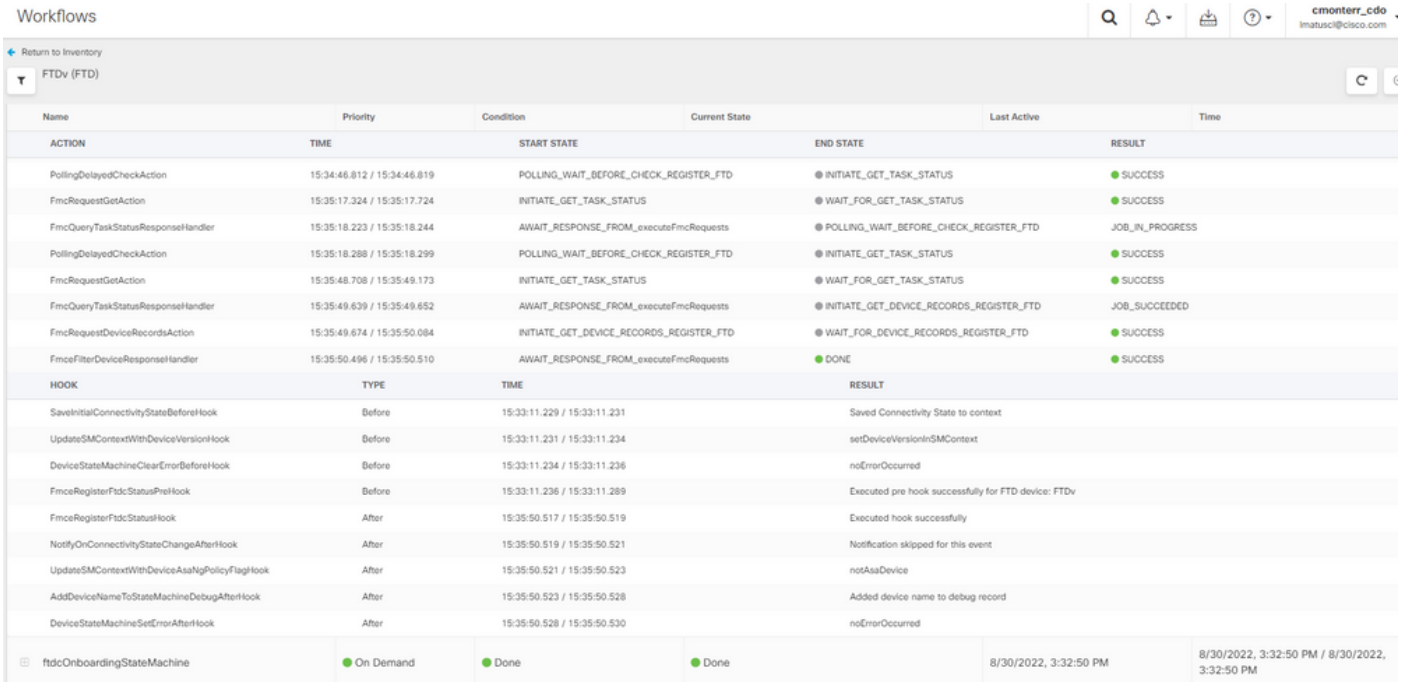
注：登録プロセスを完了するには、FTDデバイスがポート8305(sftunnel)と443を介してCDOテナントと通信できることを確認します。詳細な「ネットワーク要件」を参照してください。

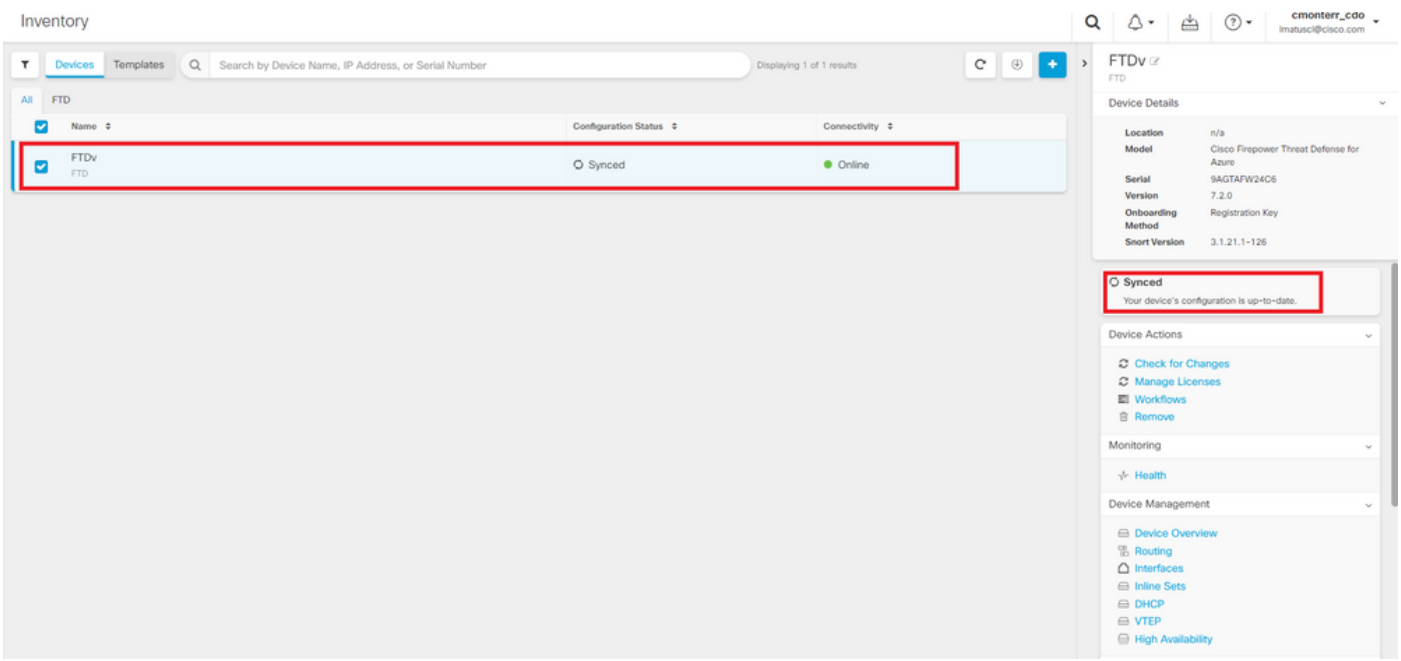
注：ホストに接続できない場合は、**configure network dns <address>**コマンドを使用してFTD-CLIのDNS設定を修正できます。

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

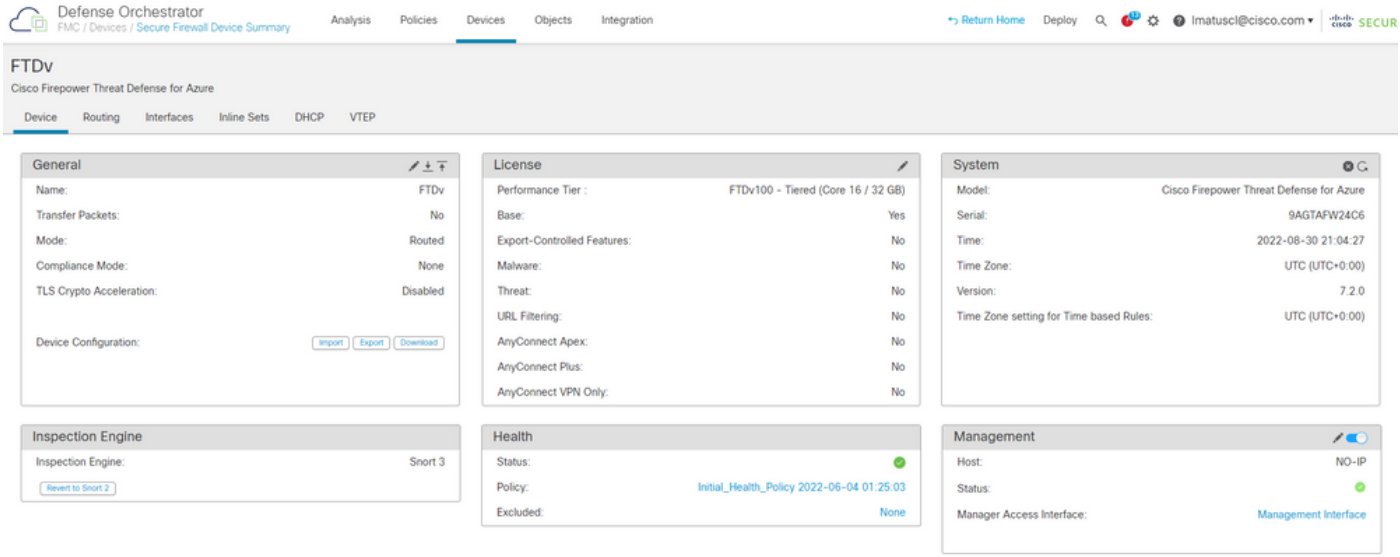


追加の情報を得るために **Active** 状態を展開します。次の図は、FTDvが正常に登録された方法を示しています。





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。



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。