



CDO を使用した Firepower Threat Defense の展開

この章の対象読者

この章では、CDO のオンボーディングウィザードを使用して、Firepower Threat Defense (FTD) デバイスを Cisco Defense Orchestrator (CDO) にオンボードする方法について説明します。FTD デバイスをオンボードする前に、デバイスで直接ホストされているローカル Firepower Device Manager (FDM) を使用して初期システム設定を完了する必要があります。

CDO は、一貫性のあるポリシーの実装を実現するために高度に分散された環境でセキュリティポリシーの管理を容易にするクラウドベースのマルチデバイスマネージャです。CDO は、セキュリティポリシーとの不整合を特定し、それらを修正するためのツールを提供することで、セキュリティポリシーを最適化します。CDO は、オブジェクトとポリシーを共有し、設定テンプレートを作成して、デバイス間でポリシーの一貫性を促進する方法を提供します。



- (注) このドキュメントでは、Firepower 2100 ハードウェアに FTD イメージが事前にインストールされていることを前提としています。Firepower 2100 ハードウェアでは、FTD ソフトウェアまたは ASA ソフトウェアを実行できます。FTD と ASA の間で切り替えを行う際には、デバイスの再イメージ化が必要になります。「[Cisco ASA および Firepower Threat Defense 再イメージ化ガイド](#)」を参照してください。



- (注) Firepower 2100 は、Firepower eXtensible Operating System (FXOS) という基礎となるオペレーティングシステムを実行します。Firepower 2100 は FXOS Firepower Chassis Manager をサポートしていません。限られた CLI のみがトラブルシューティングの目的でサポートされています。詳細については、『[FXOS troubleshooting guide](#)』を参照してください。

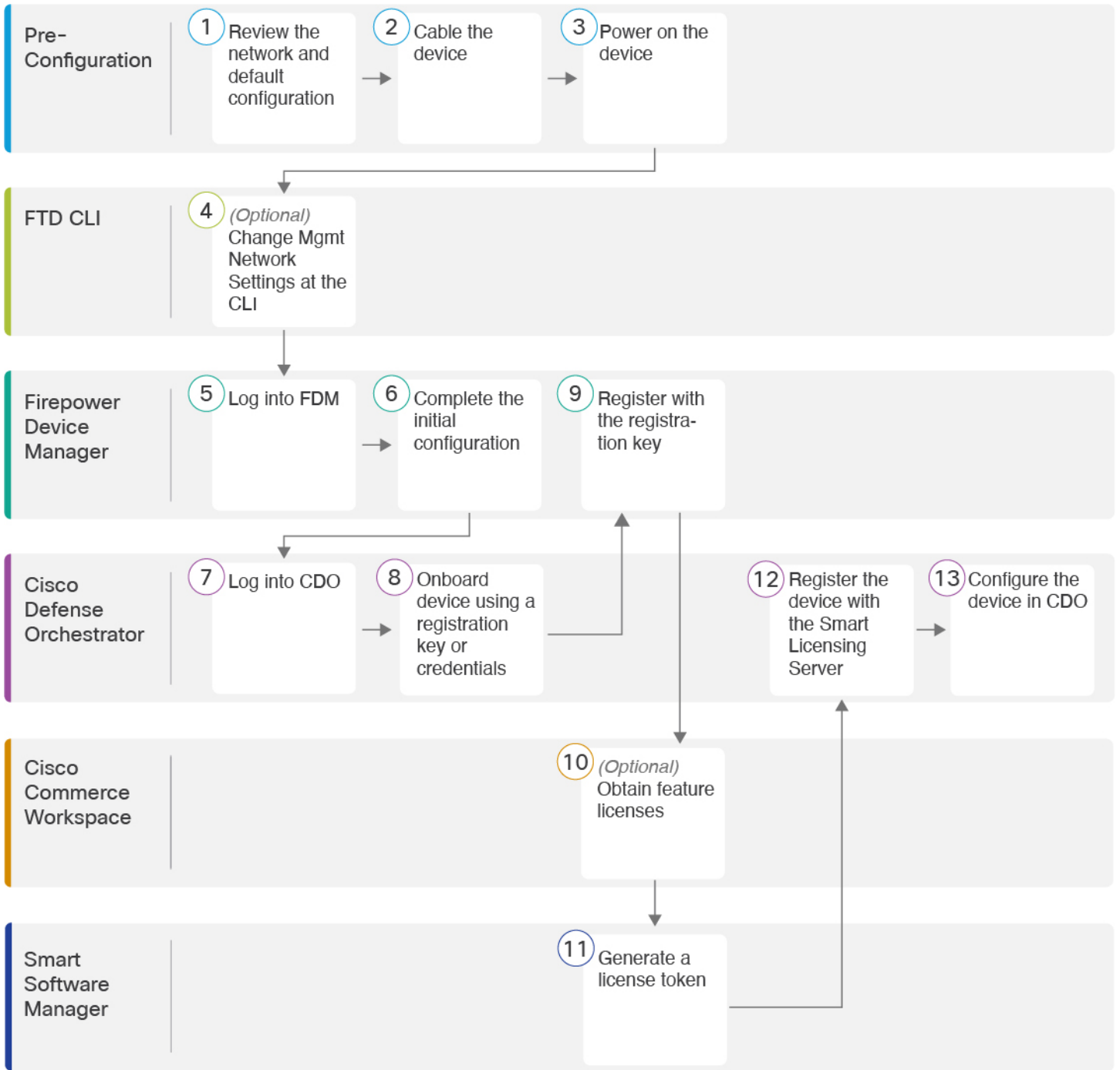


(注) プライバシー収集ステートメント：Firepower 1100 シリーズには個人識別情報は不要で、積極的に収集することはありません。ただし、ユーザ名などの設定では、個人識別情報を使用できます。この場合、設定作業時やSNMPの使用時に、管理者が個人識別情報を確認できる場合があります。

- [エンドツーエンドの手順 \(2 ページ\)](#)
- [Cisco Defense Orchestrator と Firepower Threat Defense の連携の仕組み \(4 ページ\)](#)
- [ネットワーク配置とデフォルト設定の確認 \(5 ページ\)](#)
- [デバイスの配線 \(10 ページ\)](#)
- [デバイスの電源投入 \(11 ページ\)](#)
- [\(任意\) CLI での管理ネットワーク設定の変更 \(12 ページ\)](#)
- [FDM へのログイン \(15 ページ\)](#)
- [初期設定の完了 \(16 ページ\)](#)
- [CDO へのログイン \(17 ページ\)](#)
- [CDO へのデバイスのオンボード \(22 ページ\)](#)
- [CDO でのデバイスの設定 \(30 ページ\)](#)
- [ライセンスの設定 \(35 ページ\)](#)
- [FTD および FXOS CLI へのアクセス \(40 ページ\)](#)
- [FDM を使用したデバイスの電源オフ \(41 ページ\)](#)
- [次のステップ \(42 ページ\)](#)

エンドツーエンドの手順

シャーシで CDO を使用して FTD を展開するには、次のタスクを参照してください。



1	事前設定	ネットワーク配置とデフォルト設定の確認 (5 ページ)。
2	事前設定	デバイスの配線 (10 ページ)。

3	事前設定	デバイスの電源投入 (11 ページ)。
4	FTD CLI	(任意) CLI での管理ネットワーク設定の変更 (12 ページ)。
5	Firepower Device Manager	FDM へのログイン (15 ページ)。
6	Firepower Device Manager	初期設定の完了 (16 ページ)。
7	Cisco Defense Orchestrator	Cisco Secure Sign-On を使用した CDO へのログイン (21 ページ)。
8	Cisco Defense Orchestrator	登録キーまたはログイン情報を使用してデバイスをオンボードします (CDO へのデバイスのオンボード (22 ページ))。
9	Firepower Device Manager	登録キーを使用して登録します (CDO へのデバイスのオンボード (22 ページ))。ログイン情報を使用してオンボードする場合は、FDM にログインする必要はありません。
10	Cisco Commerce Workspace	(任意) 機能ライセンスを取得します (ライセンスの設定 (35 ページ))。
11	Smart Software Manager	ライセンストークンを生成します (ライセンスの設定 (35 ページ))。
12	Cisco Defense Orchestrator	スマートライセンシングサーバにデバイスを登録します (ライセンスの設定 (35 ページ))。
13	Cisco Defense Orchestrator	CDO でのデバイスの設定 (30 ページ)。

Cisco Defense Orchestrator と Firepower Threat Defense の連携の仕組み

CDO と FDM の共同管理

FDM で初期設定を完了してインターネット接続を確立し、基本的なネットワークポリシーを設定したら、デバイスを CDO にオンボードできます。デバイスを CDO にオンボードしたら、必要に応じて FDM を引き続き使用できます。ケースバイケースで CDO のアウトオブバンド変更を受け入れるかどうかを選択できます。

Secure Device Connector (SDC)

CDO と CDO が管理するデバイス間の通信はすべて、SDC を通過します。CDO と CDO が管理するデバイスは直接通信しません。

SDC は、次の方法でクラウドまたはネットワークに展開できます。

- クラウドの Secure Device Connector : CDO サポートチームが、テナントの作成時にすべてのテナントにクラウドベースの SDC を展開します。
- オンプレミスの Secure Device Connector : オンプレミスの SDC は、ネットワークにインストールされる仮想アプライアンスです。ログイン情報ベースのオンボーディングを使用する場合は、オンプレミスの SDC を使用することをお勧めします。代わりにクラウドの SDC を使用する場合は、クラウドの SDC から CDO 管理に使用するインターフェイスへの HTTPS アクセスを許可する必要があります。一般的なネットワーク展開では、FTD 外部インターフェイスで HTTPS アクセスを有効にする必要があります。これにより、セキュリティリスクが発生する可能性があり、VPN クライアントの終了に外部インターフェイスを使用することもできなくなります。

オンプレミスの SDC をインストールするためのリンクや、ネットワークへのアクセスを許可する必要があるクラウドの SDC の IP アドレス (クレデンシャルベースのオンボーディングの場合) などの詳細については、『[Security Device Connector \(SDC\)](#)』を参照してください。

CDO オンボーディングの方式

次の方法でデバイスをオンボードできます。

- 登録キー (推奨) : この方法は、デバイスが DHCP を使用して IP アドレスを取得する場合に特に推奨されます。その IP アドレスが変更されても、デバイスは CDO に接続されたままになります。
- ログイン情報 (ユーザ名/パスワード) と IP アドレス : デバイスマネージャのユーザ名およびパスワードと静的 IP アドレスまたは FQDN を使用して FTD をオンボードできます。この方法では、内部インターフェイスに接続されたオンプレミスの SDC を使用することをお勧めします。
- (6.7以降) シリアル番号 : FDM を使用してデバイスを事前設定する必要がないロータッチプロビジョニングについては、このガイドのロータッチプロビジョニングに関する章を参照してください。すでに FDM でデバイスの設定を開始している場合は、シリアル番号を使用してオンボードすることもできますが、その方法についてはこのガイドでは説明しません。詳細については、『[Onboard an FTD using the Device's Serial Number](#)』を参照してください。

ネットワーク配置とデフォルト設定の確認

Management 1/1 インターフェイスまたは内部インターフェイスから FDM を使用して FTD の初期設定を実行できます。専用管理 (Management) インターフェイスは、トラフィックの通過を許可せず、独自のネットワーク設定を持つ特別なインターフェイスです。

Secure Device Connector (SDC) のタイプとオンボーディング方式に応じて、次の一般的なネットワーク展開を参照してください。

クラウド SDC ネットワーク、登録キーオンボーディング

次の図に、クラウドの SDC を使用した登録キーオンボーディングの場合の推奨されるネットワーク展開を示します。登録キーオンボーディングではオンプレミスの SDC を使用できますが、この例は、より一般的なクラウドの SDC のユースケースを示しています。クラウドの SDC によるログイン情報ベースのオンボーディングも使用できますが、FDM で追加の設定が必要になるため、望ましくない場合があります。

外部インターフェイスをケーブルモデムまたは DSL モデムに直接接続する場合は、FTD が内部ネットワーク用のすべてのルーティングと NAT を実行するように、モデムをブリッジモードにすることをお勧めします。外部インターフェイスが ISP に接続できるように PPPoE を設定する必要がある場合は、その設定を FDM の初期セットアップの後で行うことができます。

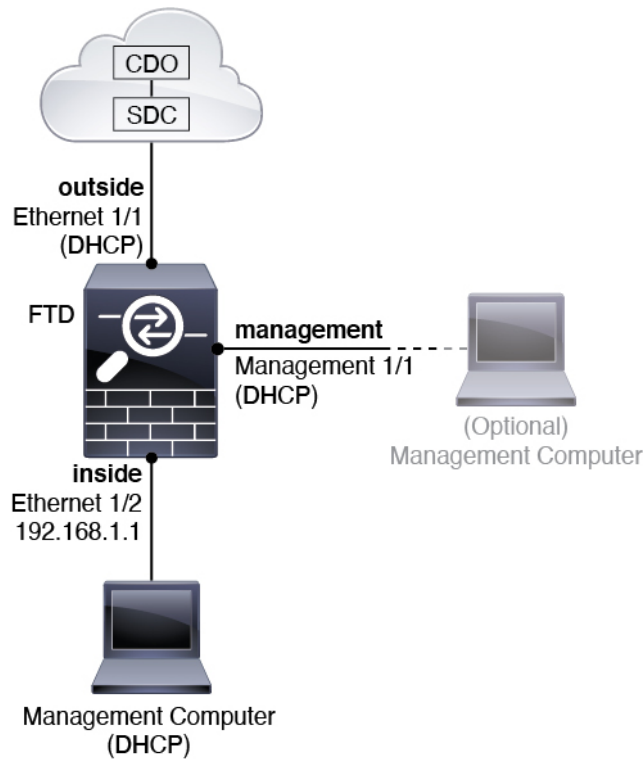


(注) デフォルトの管理 IP アドレスを使用できない場合（管理ネットワークに DHCP サーバが含まれていない場合など）、コンソールポートに接続して、CLI で初期セットアップ（管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定の指定など）を実行できます。

内部 IP アドレスを変更する必要がある場合は、FDM で初期セットアップを完了した後に変更できます。たとえば、次のような状況において、内部 IP アドレスの変更が必要になる場合があります。

- 外部インターフェイスが一般的なデフォルトネットワークである 192.168.1.0 ネットワーク上の IP アドレスの取得を試みる場合、DHCP リースが失敗し、外部インターフェイスが IP アドレスを取得しません。この問題は、FTD が同じネットワーク上に 2 つのインターフェイスを持つことができないために発生します。この場合、内部 IP アドレスが新しいネットワーク上に存在するように変更する必要があります。
- FTD を既存の内部ネットワークに追加する場合は、内部 IP アドレスが既存のネットワーク上に存在するように変更する必要があります。

図 1: 推奨されるネットワーク展開 (クラウドの SDC)



(注) 6.5 以前の場合、Management 1/1 のデフォルト IP アドレスは 192.168.45.45 です。

オンプレミス SDC ネットワーク、ログイン情報オンボーディング

次の図に、内部ネットワークに接続されたオンプレミスの SDC を使用したログイン情報オンボーディングの場合の推奨されるネットワーク展開を示します。ログイン情報オンボーディングでクラウドの SDC を使用できますが、FDM で追加の設定が必要になるため、望ましくない場合があります。この例は、より一般的なオンプレミスの SDC のユースケースを示しています。トラフィックの通過が許可されないオプションの管理ネットワークに SDC を追加する場合は、SDC にインターネットへのパスが必要になります (図には示されていない)。

外部インターフェイスをケーブルモデムまたは DSL モデムに直接接続する場合は、FTD が内部ネットワーク用のすべてのルーティングと NAT を実行するように、モデムをブリッジモードにすることをお勧めします。外部インターフェイスが ISP に接続できるように PPPoE を設定する必要がある場合は、その設定を FDM の初期セットアップの後で行うことができます。

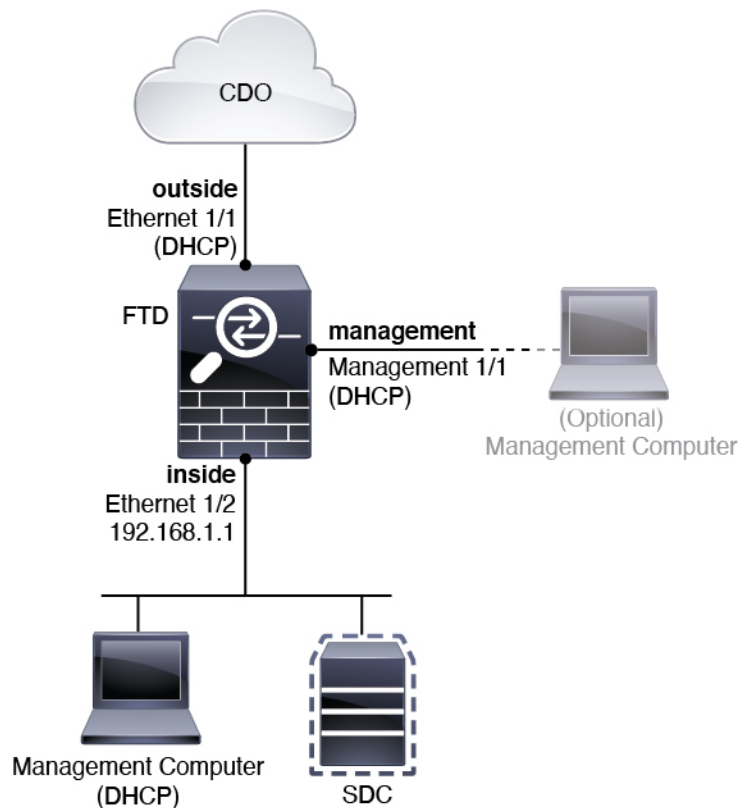


(注) デフォルトの管理 IP アドレスを使用できない場合（管理ネットワークに DHCP サーバが含まれていない場合など）、コンソールポートに接続して、CLI で初期セットアップ（管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定の指定など）を実行できます。

内部 IP アドレスを変更する必要がある場合は、FDM で初期セットアップを完了した後に変更できます。たとえば、次のような状況において、内部 IP アドレスの変更が必要になる場合があります。

- 外部インターフェイスが一般的なデフォルトネットワークである 192.168.1.0 ネットワーク上の IP アドレスの取得を試みる場合、DHCP リースが失敗し、外部インターフェイスが IP アドレスを取得しません。この問題は、FTD が同じネットワーク上に 2 つのインターフェイスを持つことができないために発生します。この場合、内部 IP アドレスが新しいネットワーク上に存在するように変更する必要があります。
- FTD を既存の内部ネットワークに追加する場合は、内部 IP アドレスが既存のネットワーク上に存在するように変更する必要があります。

図 2: 推奨されるネットワーク展開（オンプレミスの SDC）





(注) 6.5 以前の場合、Management 1/1 のデフォルト IP アドレスは 192.168.45.45 です。

デフォルト設定

初期設定後の Firepower デバイスの設定には次のものが含まれます。

- 内部 : Ethernet 1/2、IP アドレス 192.168.1.1。
- 外部 : イーサネット 1/1、IPv4 DHCP からの IP アドレス
- 内部→外部トラフィックフロー
- 管理 : Management 1/1 (管理)
 - (6.6 以降) DHCP からの IP アドレス
 - (6.5 以前) IP アドレス 192.168.45.45



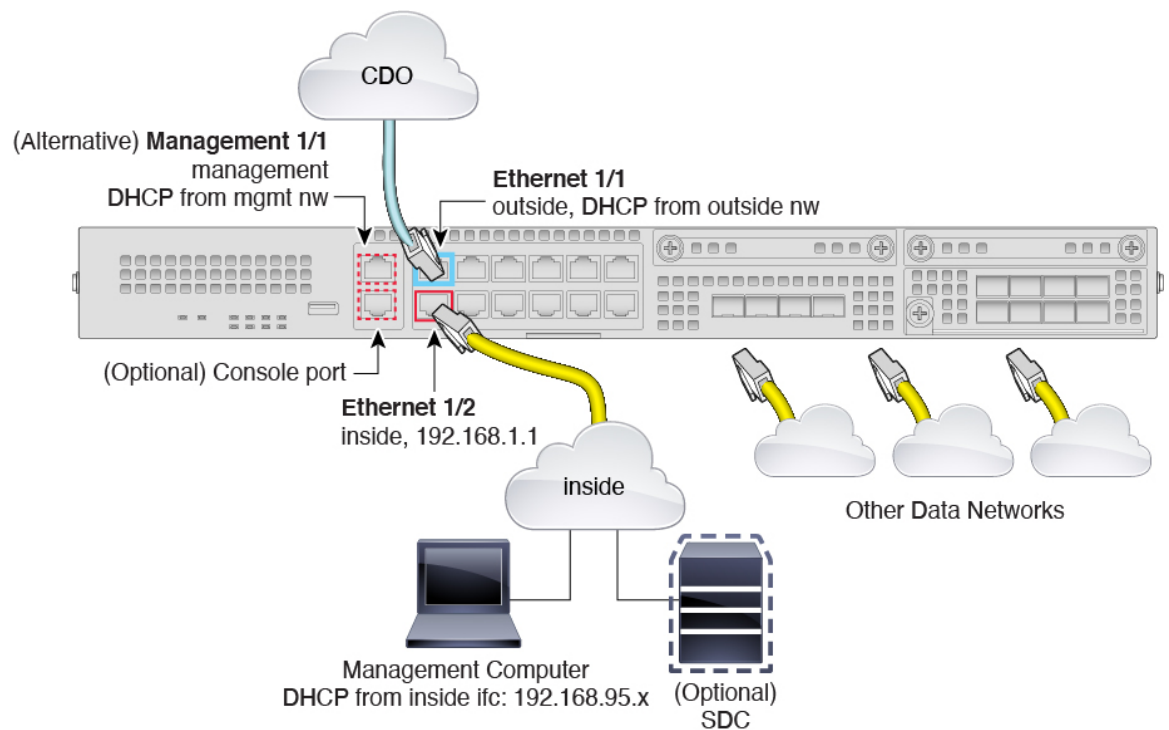
(注) Management 1/1 インターフェイスは、管理、スマートライセンス、およびデータベースの更新に使用されるデータインターフェイスとは別の特別なインターフェイスです。物理インターフェイスは、診断インターフェイスである 2 番目の論理インターフェイスと共有されます。診断はデータインターフェイスですが、syslog や SNMP など、他のタイプの管理トラフィック (デバイスとデバイス間) に限定されます。診断インターフェイスは通常使用されません。詳細については、『[FDM コンフィギュレーションガイド](#)』を参照してください。

- 管理用の DNS サーバ : OpenDNS : 208.67.222.222、208.67.220.220、またはセットアップ時に指定したサーバ。DHCP から取得した DNS サーバは使用されません。
- NTP : Cisco NTP サーバ : 0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org、またはセットアップ時に指定したサーバ
- デフォルトルート
 - データインターフェイス : 外部 DHCP から取得したもの、またはセットアップ時に指定したゲートウェイ IP アドレス
 - 管理インターフェイス : (6.6 以降) 管理 DHCP から取得されます。ゲートウェイを受信しない場合、デフォルトルートはバックプレーンを介してデータインターフェイスを経由します。(6.5 以前) バックプレーンを介してデータインターフェイスを経由管理インターフェイスでは、バックプレーンを介した場合でも個別のインターネットゲートウェイを使用する場合でも、ライセンス取得や更新のためにインターネットアクセスが必要であることに注意してください。管理インターフェイスから発信された

トラフィックのみがバックプレーンを通過できることに注意してください。それ以外の場合、ネットワークから管理インターフェイスに入るトラフィックの通過は許可されません。

- **DHCP サーバ** : 内部インターフェイスおよび (6.5 以前のみ) 管理インターフェイスで有効になります
- **FDM アクセス** : すべてのホストが管理インターフェイスと内部インターフェイスで許可されます
- **NAT** : 内部から外部へのすべてのトラフィック用のインターフェイス PAT

デバイスの配線



(注) 6.5 以前の場合、Management 1/1 のデフォルト IP アドレスは 192.168.45.45 です。

Management 1/1 または Ethernet 1/2 のいずれかで Firepower 2100 を管理します。デフォルト設定でも、Ethernet1/1 を外部として設定します。

手順

ステップ 1 管理コンピュータを次のいずれかのインターフェイスに接続します。

- Ethernet 1/2：初期設定のために管理コンピュータを Ethernet 1/2 に直接接続するか、Ethernet 1/2 を内部ネットワークに接続します。イーサネット 1/2 にはデフォルトの IP アドレス（192.168.1.1）があり、クライアント（管理コンピュータを含む）に IP アドレスを提供するために DHCP サーバも実行されるため、これらの設定が既存の内部ネットワーク設定と競合しないようにしてください（[デフォルト設定（9 ページ）](#) を参照）。

- Management 1/1（ラベル MGMT）：Management 1/1 を管理ネットワークに接続し、管理コンピュータが管理ネットワーク上にあるか、またはアクセスできることを確認します。Management 1/1 は、管理ネットワーク上の DHCP サーバから IP アドレスを取得します。このインターフェイスを使用する場合は、管理コンピュータから IP アドレスに接続できるように、FTD に割り当てられている IP アドレスを決定する必要があります。

Management 1/1 IP アドレスをデフォルトから変更し、静的 IP アドレスを設定する必要がある場合は、管理コンピュータをコンソールポートにケーブル接続する必要もあります。「[（任意）CLI での管理ネットワーク設定の変更（12 ページ）](#)」を参照してください。

後で、他のインターフェイスから FDM 管理アクセスを設定できます。『[FDM コンフィギュレーションガイド](#)』を参照してください。

ステップ 2 オプションのオンプレミスの Secure Device Connector（SDC）を内部ネットワークに接続します。

ステップ 3 外部ネットワークを Ethernet 1/1 インターフェイス（ラベル「WAN」）に接続します。

デフォルトでは、IP アドレスは IPv4 DHCP を使用して取得しますが、初期設定時に静的アドレスを設定できます。

ステップ 4 残りのインターフェイスに他のネットワークを接続します。

デバイスの電源投入

電源スイッチは、シャーシの背面の電源モジュール 1 の左にあります。これはシステムへの電源を制御するトグルスイッチです。電源スイッチがスタンバイの位置にある場合は、3.3 V のスタンバイ電源ユニットのみが電源モジュールから有効化され、12 V の主電源はオフになります。スイッチがオンの位置にある場合は、12 V の主電源がオンになり、システムが起動します。

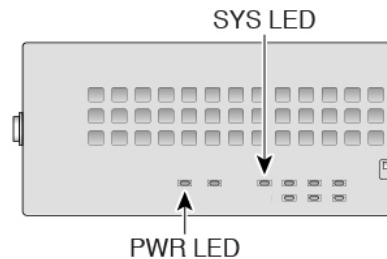
始める前に

デバイスに対して信頼性の高い電力を供給することが重要です（たとえば、無停電電源装置（UPS）を使用）。最初のシャットダウンを行わないで電力が失われると、重大なファイルシ

システムの損傷を引き起こす可能性があります。バックグラウンドでは常に多数のプロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

手順

- ステップ1** 電源コードをデバイスに接続し、電源コンセントに接続します。
- ステップ2** デバイスの背面にある電源スイッチを押します。
- ステップ3** デバイスの前面にある PWR LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。



- ステップ4** デバイスの前面にある SYS LED を確認します。緑色に点灯している場合は、電源投入時診断に合格しています。

(注) 電源スイッチをオフの位置に動かす前に、システムがグレースフルシャットダウンを実行できるように `shutdown` コマンドを使用します。終了するまでに数分かかる場合があります。グレースフルシャットダウンが完了すると、コンソールにはすぐに電源オフすると安全ですと表示されます。前面パネルの青いロケータ ビーコン LED が点灯し、システムの電源をオフにする準備ができていることを示します。これで、スイッチをオフの位置に移動できるようになりました。前面パネルの PWR LED が瞬間的に点滅し、消灯します。PWR LED が完全にオフになるまで電源を抜かないでください。

これらの `shutdown` コマンドの使用の詳細については、『[FXOS コンフィグレーションガイド](#)』を参照してください。

(任意) CLI での管理ネットワーク設定の変更

デフォルトの IP アドレスを使用できない場合（たとえば、デバイスを既存のネットワークに追加する場合）、コンソールポートに接続して、CLI で初期セットアップ（管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定の指定など）を実行できます。管理インターフェイスのみを設定できます。内部インターフェイスや外部インターフェイスは設定できません。これらは後で GUI を使用して設定できます。



- (注) 設定をクリア (たとえば、イメージを再作成することにより) しないかぎり、CLI セットアップスクリプトを繰り返すことはできません。ただし、これらの設定すべては、後から CLI で **configure network** コマンドを使用して変更できます。[FTD のコマンドリファレンス](#) を参照してください。

手順

- ステップ 1** FTD コンソールポートに接続します。詳細については、[FTD および FXOS CLI へのアクセス \(40 ページ\)](#) を参照してください。

admin ユーザとデフォルトパスワードの **Admin123** を使用してログインします。

FXOS CLI に接続します。初めてログインしたとき、パスワードを変更するよう求められます。このパスワードは、SSH の FTD ログインにも使用されます。

- (注) パスワードがすでに変更されていて、パスワードがわからない場合は、デバイスを再イメージ化してパスワードをデフォルトにリセットする必要があります。[再イメージ化の手順](#) については、『[FXOS troubleshooting guide](#)』を参照してください。

例 :

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.

[...]

firepower#
```

- ステップ 2** FTD CLI に接続します。

connect ftd

例 :

```
firepower# connect ftd
>
```

- ステップ 3** FTD に初めてログインすると、エンドユーザライセンス契約書 (EULA) に同意するように求められます。その後、CLI セットアップスクリプトが表示されます。

デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

次のガイドラインを参照してください。

- [管理インターフェイスの IPv4 デフォルトゲートウェイを入力します (Enter the IPv4 default gateway for the management interface)] : 手動 IP アドレスを設定した場合は、「**data-interfaces**」またはゲートウェイルータの IP アドレスのいずれかを入力します。**data-interfaces** を設定すると、アウトバウンド管理トラフィックがバックプレーン経由で送信され、データインターフェイスが終了します。この設定は、インターネットにアクセスできる個別の管理ネットワークがない場合に役立ちます。管理インターフェイスから発信されるトラフィックには、インターネットアクセスを必要とするライセンス登録とデータベースの更新が含まれます。**data-interfaces** を使用する場合、管理ネットワークに直接接続していれば管理インターフェイスで FDM (または SSH) を引き続き使用できますが、特定のネットワークまたはホストのリモート管理の場合は、**configure network static-routes** コマンドを使用して静的ルートを追加する必要があります。データインターフェイスでの FDM 管理は、この設定の影響を受けないことに注意してください。DHCP を使用する場合、システムは DHCP によって提供されるゲートウェイを使用します。DHCP がゲートウェイを提供しない場合は、フォールバックメソッドとして **data-interfaces** を使用します。
- [ネットワーク情報が変更された場合は再接続が必要になります (If your networking information has changed, you will need to reconnect)] : SSH でデフォルトの IP アドレスに接続しているのに、初期セットアップでその IP アドレスを変更すると、接続が切断されます。新しい IP アドレスとパスワードで再接続してください。コンソール接続は影響を受けません。
- [デバイスをローカルで管理しますか (Manage the device locally?)] : CDO または FDM を使用するには [はい (yes)] を入力します。[いいえ (no)] と応えると、デバイスの管理には FMC を使用することになります。

例 :

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress. Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
```

```
For HTTP Proxy configuration, run 'configure network http-proxy'  
  
Manage the device locally? (yes/no) [yes]: yes  
  
>
```

ステップ 4 新しい管理 IP アドレスで FDM にログインしてください。

次のタスク

CLI を使用して管理ネットワークの設定を変更する場合は、EULA に同意し、IP アドレスとパスワードを変更します。これで初期設定は完了です（[初期設定の完了（16 ページ）](#) を参照）。

FDM へのログイン

FDM にログインして FTD を設定します。デバイスを CDO にオンボードする前に、FDM セットアップウィザードを使用して初期セットアップを完了します。

始める前に

- Firefox または Chrome の最新バージョンを使用します。

手順

ステップ 1 ブラウザに次の URL を入力します。

- 内部（イーサネット 1/2） : **https://192.168.1.1**。
- （6.6 以降） 管理 : **https://management_ip**。管理インターフェイスは DHCP クライアントであるため、IP アドレスは DHCP サーバによって異なります。CLI セットアップで管理 IP アドレスを変更した場合は、そのアドレスを入力します。
- （6.5 以前） 管理 : **https://192.168.45.45**。CLI セットアップで管理 IP アドレスを変更した場合は、そのアドレスを入力します。

ステップ 2 ユーザ名 **admin**、デフォルトパスワード **Admin123** を使用してログインします。

次のタスク

- FDM セットアップウィザードを実行します。[初期設定の完了（16 ページ）](#) を参照してください。

初期設定の完了

初期設定を完了するには、最初に FDM にログインしたときにセットアップ ウィザードを使用します。セットアップ ウィザードの完了後、いくつかの基本ポリシーが適切に設定された機能しているデバイスが必要です。

- 外部 (Ethernet1/1) および内部インターフェイス (Ethernet1/2)。
- 内部インターフェイスと外部インターフェイスのセキュリティゾーン。
- 内部から外部へのすべてのトラフィックを信頼するアクセスルール。
- 内部から外部へのすべてのトラフィックを外部インターフェイスの IP アドレスの固有のポートへ変換するインターフェイス NAT ルール。
- 内部インターフェイスで実行されている DHCP サーバ。



(注) (任意) CLIでの管理ネットワーク設定の変更の手順を実行した場合は、これらのタスクの一部、具体的には管理者パスワードの変更、および外部インターフェイスと管理インターフェイスの設定がすでに完了しているはずです。

手順

ステップ 1 エンドユーザ ライセンス契約書を読んで同意し、管理者パスワードを変更するように求められます。

続行するには、これらの手順を完了する必要があります。

ステップ 2 外部インターフェイスおよび管理インターフェイスに対して次のオプションを設定し、[次へ (Next)] をクリックします。

(注) [次へ (Next)] をクリックすると、設定がデバイスに展開されます。インターフェイスの名前は「外部」となり、「outside_zone」セキュリティゾーンに追加されます。設定値が正しいことを確認します。

- a) [外部インターフェイス (Outside Interface)]: これは、ゲートウェイ ルータに接続するためのデータポートです。デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータインターフェイスがデフォルトの外部インターフェイスです。

[IPv4の設定 (Configure IPv4)]: 外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、サブネットマスク、およびゲートウェイを入力できます。[オフ (Off)] を選択して、IPv4 アドレスを設定しないという選択肢もあります。セットアップ ウィザードを使用して PPPoE を設定することはできません。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されて

おり、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。ウィザードの完了後に PPPoE を設定できます。

[IPv6 の設定 (Configure IPv6)] : 外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、プレフィックス、およびゲートウェイを入力できます。[オフ (Off)] を選択して、IPv6 アドレスを設定しないという選択肢もあります。

b) [管理インターフェイス (Management Interface)]

[DNS サーバ (DNS Servers)] : システムの管理アドレス用の DNS サーバ。名前解決用に 1 つ以上の DNS サーバのアドレスを入力します。デフォルトは OpenDNS パブリック DNS サーバです。フィールドを編集し、デフォルトに戻りたい場合は、[OpenDNS を使用 (Use OpenDNS)] をクリックすると、フィールドに適切な IP アドレスがリロードされます。

[ファイアウォールホスト名 (Firewall Hostname)] : システムの管理アドレスのホスト名です。

ステップ 3 システム時刻を設定し、[次へ (Next)] をクリックします。

- a) [タイムゾーン (Time Zone)] : システムのタイムゾーンを選択します。
- b) [NTP タイムサーバ (NTP Time Server)] : デフォルトの NTP サーバを使用するか、使用している NTP サーバのアドレスを手動で入力するかを選択します。バックアップ用に複数のサーバを追加できます。

ステップ 4 [登録せずに 90 日間の評価期間を開始 (Start 90 day evaluation period without registration)] を選択します。

(注) Smart Software Manager アカウントと使用可能なライセンスがある場合でも、90 日間の評価ライセンスの使用を選択します。FTD を CDO にオンボードした後に FTD のライセンスを取得できます。この選択により、ライセンスの登録解除と再登録が不要になります。

Firepower Threat Defense デバイスを購入すると、自動的に基本ライセンスが付いてきます。すべての追加ライセンスはオプションです。

ステップ 5 [終了 (Finish)] をクリックします。

次のタスク

- オンボーディングプロセスを開始するには、[CDO へのログイン \(17 ページ\)](#) に進みます。

CDO へのログイン

CDO は、Cisco Secure Sign-On をアイデンティティプロバイダーとして使用し、Duo Security を多要素認証 (MFA) に使用します。CDO には MFA が必要です。MFA は、ユーザアイデンティ

ティを保護するためのセキュリティを強化します。MFA の一種である二要素認証では、CDO にログインするユーザの ID を確認するために、2 つのコンポーネントまたは要素が必要です。

最初の要素はユーザ名とパスワードで、2 番目の要素は Duo Security からオンデマンドで生成されるワンタイムパスワード (OTP) です。

Cisco Secure Sign-On クレデンシャルを確立したら、Cisco Secure Sign-On ダッシュボードから CDO にログインできます。Cisco Secure Sign-On ダッシュボードから、サポートされている他のシスコ製品にログインすることもできます。

- Cisco Secure Sign-On アカウントをお持ちの場合は、[Cisco Secure Sign-On を使用した CDO へのログイン](#)に進みます。
- Cisco Secure Sign-On アカウントがない場合は、[新しい Cisco Secure Sign-On アカウントの作成 \(18 ページ\)](#)に進んでください。

新しい Cisco Secure Sign-On アカウントの作成

最初のサインオンワークフローは 4 段階のプロセスです。4 段階すべてを完了する必要があります。

始める前に

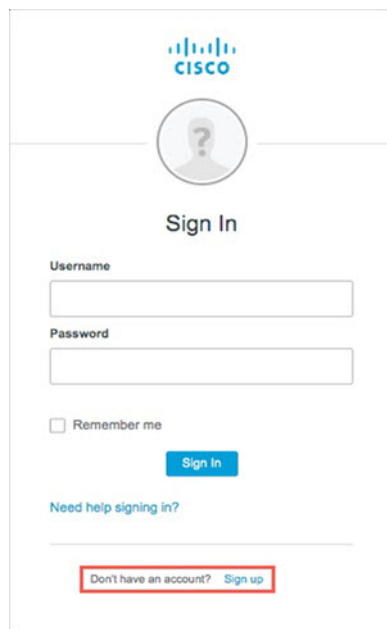
- **DUO Security のインストール** : Duo Security アプリケーションを携帯電話にインストールすることをお勧めします。Duo のインストールについてご質問がある場合は、『[Duo Guide to Two Factor Authentication : Enrollment Guide](#)』を参照してください。
- **時刻の同期** : モバイルデバイスを使用してワンタイムパスワードを生成します。OTP は時間ベースであるため、デバイスのクロックがリアルタイムと同期していることが重要です。デバイスのクロックが正しい時刻に設定されていることを確認します。
- Firefox または Chrome の最新バージョンを使用します。

手順

ステップ 1 新しい Cisco Secure Sign-On アカウントにサインアップします。

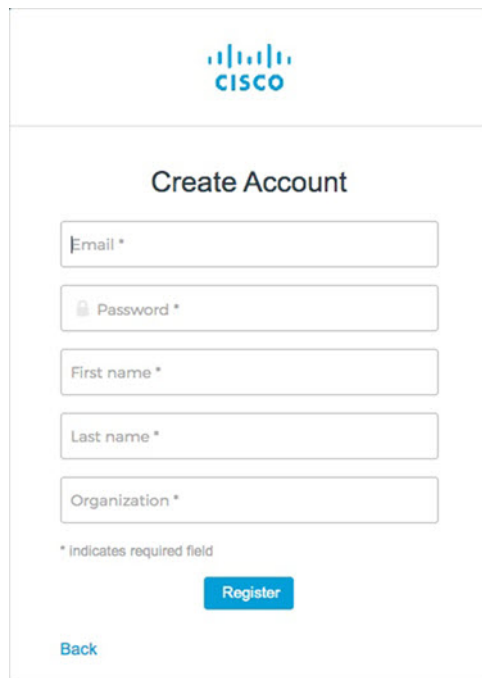
- a) <https://sign-on.security.cisco.com> にアクセスします。
- b) [サインイン (Sign In)] 画面の下部にある [サインアップ (Sign up)] をクリックします。

図 3: Cisco SSO へのサインアップ



- c) [アカウントの作成 (Create Account)]ダイアログのフィールドに入力し、[登録 (Register)]をクリックします。

図 4: アカウントの作成 (Create Account)



ヒント CDOへのログインに使用する予定の電子メールアドレスを入力し、会社を表す組織名を追加します。

- d) [登録 (Register)] をクリックすると、登録したアドレスに確認メールが送信されます。電子メールを開き、[アカウントの有効化 (Activate Account)] をクリックします。

ステップ 2 Duo を使用して多要素認証をセットアップします。

- a) [多要素認証の設定 (Set up multi-factor authentication)] 画面で、[設定 (Configure)] をクリックします。
- b) [セットアップの開始 (Start setup)] をクリックし、プロンプトに従ってデバイスを選択して、そのデバイスとアカウントのペアリングを確認します。

詳細については、『[Duo Guide to Two Factor Authentication : Enrollment Guide](#)』を参照してください。デバイスに Duo アプリケーションがすでにインストールされている場合は、このアカウントのアクティベーションコードが送信されます。Duo は 1 台のデバイスで複数のアカウントをサポートします。

- c) ウィザードの最後で、[ログインを続行する (Continue to Login)] をクリックします。
- d) 二要素認証を使用して Cisco Secure Sign-On にログインします。

ステップ 3 (任意) 追加のオーセンティケータとして Google オーセンティケータを設定します。

- a) Google オーセンティケータとペアリングするモバイルデバイスを選択し、[次へ (Next)] をクリックします。
- b) セットアップウィザードのプロンプトに従って、Google オーセンティケータをセットアップします。

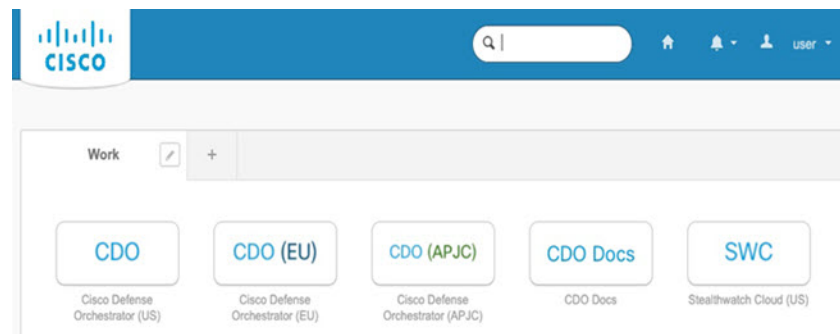
ステップ 4 Cisco Secure Sign-On アカウントのアカウントリカバリのオプションを設定します。

- a) 「パスワードを忘れた場合 (forgot password)」の質問と回答を選択します。
- b) SMS を使用してアカウントをリセットするための予備の電話番号を選択します。
- c) セキュリティイメージを選択します。
- d) [マイアカウントの作成 (Create My Account)] をクリックします。

これで、Cisco Security Sign-On ダッシュボードに CDO アプリケーションのタイルが表示されます。他のアプリケーションタイルも表示される場合があります。

ヒント ダッシュボード上でタイルをドラッグして並べ替えたり、タブを作成してタイルをグループ化したり、タブの名前を変更したりできます。

図 5: Cisco SSO ダッシュボード



Cisco Secure Sign-On を使用した CDO へのログイン

CDO にログインして FTD をオンボードし、管理します。

始める前に

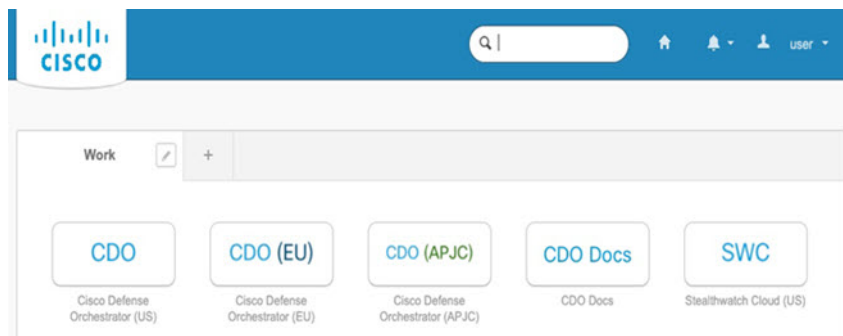
Cisco Defense Orchestrator (CDO) は、Cisco Secure Sign-On をアイデンティティプロバイダーとして使用し、多要素認証 (MFA) に Duo Security を使用します。

- CDO にログインするには、まず Cisco Secure Sign-On でアカウントを作成し、Duo を使用して MFA を設定する必要があります。新しい [Cisco Secure Sign-On アカウントの作成 \(18 ページ\)](#) を参照してください。
- Firefox または Chrome の最新バージョンを使用します。

手順

- ステップ 1** Web ブラウザで、<https://sign-on.security.cisco.com/>を開きます。
- ステップ 2** [ユーザ名 (Username)] と [パスワード (Password)] に入力します。
- ステップ 3** [ログイン (Log in)] をクリックします。
- ステップ 4** Duo Security を使用して別の認証要素を受け取り、ログインを確認します。システムによってログインが確認され、Cisco Secure Sign-On ダッシュボードが表示されます。
- ステップ 5** Cisco Secure Sign-on ダッシュボードで適切な CDO タイルをクリックします。**CDO** タイルをクリックすると <https://defenseorchestrator.com> に移動し、**CDO (EU)** タイルをクリックすると <https://defenseorchestrator.eu> に移動します。また、**CDO (APJC)** タイルをクリックすると <https://www.apj.cdo.cisco.com> に移動します。

図 6: Cisco SSO ダッシュボード



- ステップ 6** 両方のオーセンティケータを設定している場合は、オーセンティケータのロゴをクリックして [Duo Security] か [Google Authenticator] を選択します。
 - 既存のテナントにすでにユーザレコードがある場合は、そのテナントにログインします。
 - すでに複数のテナントにユーザレコードがある場合は、接続先の CDO テナントを選択できます。

- 既存のテナントにユーザレコードがない場合は、CDO の詳細を確認するか、またはトライアルアカウントを要求できます。

CDO へのデバイスのオンボード

CDO のオンボーディングウィザードを使用してデバイスをオンボードします。

登録キーを使用した FTD のオンボード（推奨）

登録キーを使用して FTD デバイスをオンボードすることを推奨します。DHCP を使用して FTD に IP アドレスが割り当てられている場合、何らかの理由でアドレスが変更されても、FTD は CDO に接続されたままになります。さらに、FTD がパブリック IP アドレスを持つ必要はなく、デバイスが外部ネットワークにアクセスできる限り、この方法で CDO にオンボードできます。



- (注) SecureX または Cisco Threat Response (CTR) アカウントをお持ちの場合、デバイスを SecureX に登録するには、CDO アカウントと SecureX/CTR アカウントを統合する必要があります。アカウントが統合されるまで、デバイスのイベントを SecureX で表示したり、他の SecureX 機能を利用したりすることはできません。SecureX で CDO モジュールを作成する前に、アカウントを統合することを強くお勧めします。アカウントは、SecureX ポータルから統合できます。手順については、「[アカウントの統合](#)」を参照してください。

登録キーを使用した FTD のオンボード（バージョン 6.6+）

登録キーを使用して FTD デバイスをオンボードするには、次の手順を実行します。

始める前に

- この方法を使用して、デバイスを米国、EU、または APJ リージョンにオンボードできません。
- Firepower Device Manager (FDM) によってデバイスが管理されている必要があります。デバイスで待機している保留中の変更がないことを確認します。
- デバイスで 90 日間の評価ライセンスを使用するかスマートライセンスを使用することができます。Cisco Smart Software Manager から、デバイスにインストールされているライセンスの登録を解除する必要はありません。
- FTD デバイスで DNS が正しく設定されていることを確認します。

- FTD デバイスでタイムサービスが正しく設定されていることを確認します。FTD デバイスに正しい日付と時刻が表示されていることを確認します。そうでない場合はオンボーディングは失敗します。

手順

- ステップ 1** CDO のナビゲーションウィンドウで [デバイスとサービス (Devices & Services)] をクリックし、青色のプラスボタン (+) をクリックしてデバイスを [オンボード (Onboard)] します。
- ステップ 2** [FTD] カードをクリックします。
- ステップ 3** [登録キーを使用 (Use Registration Key)] をクリックします。
- ステップ 4** [デバイス名 (Device Name)] 領域のフィールドに値を入力します。

図 7: デバイス名 (Device Name)

Follow the steps below Cancel

FTD Device
Firepower Threat Defense 6.4+

Use Serial Number
Use this method for low-touch provisioning or for onboarding configured devices using their serial number.
(FTD 6.7+, 1000 and 2100 series only)

Use Registration Key
Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.

Use Credentials
Onboard a device using its IP address, or host name, and a username and password.

1 Device Name

Select Secure Device Connector

SDC-2

Device Name

Device Name

Next

Important: If you already have a SecureX or Cisco Threat Response (CTR) account, you will need to merge your CDO account and SecureX/CTR account in order for your devices to be registered with SecureX. Your accounts can be merged through the SecureX portal. See [Merge Your CDO and SecureX Accounts](#) for instructions. Until your accounts are merged, you will not be able to see your device's events in SecureX or benefit from other SecureX features.

- このデバイスが通信する **Secure Device Connector** を選択します。デフォルトの SDC が表示されますが、SDC 名をクリックすることで SDC を変更できます。
- [デバイス (Device Name)] フィールドにデバイス名を入力します。デバイスのホスト名またはその他の任意の名前にすることができます。
- [次へ (Next)] をクリックします。


- ステップ 5** [データベースの更新 (Database Updates)] 領域で、[セキュリティ更新を即時に実行し、定期更新を有効にする (Immediately security updates, and enable recurring updates)] をオンまたはオフにして、[次へ (Next)] をクリックします。

このオプションは、セキュリティ更新をすぐにトリガーするとともに、毎週月曜日の午前2時に追加の更新をチェックするようにデバイスを自動的にスケジュールします。詳細については、『[Update FTD Security Databases](#)』と『[Schedule a Security Database Update](#)』を参照してください。

- (注) このオプションを無効にしても、以前に FDM を使用して設定したスケジュール済みの更新には影響しません。

ステップ 6 CDO によって [登録キーの作成 (Create Registration Key)] 領域に登録キーが生成されます。

- (注) キーが生成された後でデバイスが完全にオンボーディングされる前にオンボーディング画面から移動すると、オンボーディング画面に戻ることができません。ただし、CDO によって [デバイスとサービス (Device & Services)] ページにそのデバイスのプレースホルダが作成されます。デバイスのプレースホルダを選択して、そのデバイスのキーを表示します。

ステップ 7 [コピー (Copy)] アイコン () をクリックして登録キーをコピーし、[次へ (Next)] をクリックします。

- (注) 登録キーのコピーをスキップして [次へ (Next)] をクリックすると、デバイスのプレースホルダエントリを完了した後でデバイスを登録できます。このオプションは、最初にデバイスを作成してから登録する場合、またはシスコネットワークパートナーがカスタマーネットワークに価値の実証 (POV) デバイスをインストールする場合に役立ちます。

この時点で、デバイスの接続状態は「プロビジョニング解除 (Unprovisioned)」になります。[Firepower Defense Manager へのプロビジョニングの解除 (Unprovisioned to Firepower Defense Manager)] の下に表示される登録キーをコピーしてオンボーディングプロセスを完了します。

ステップ 8 CDO にオンボードするデバイスの FDM にログインします。

- [システム設定 (System Settings)] で、[クラウドサービス (Cloud Services)] をクリックします。
- デバイスをすでにシスコスマートライセンスに登録しており、クラウドに登録済みであることがこのページに表示されている場合は、歯車メニューをクリックして、[クラウドサービスの登録解除 (Unregister Cloud Services)] を選択します。ページをリロードして、未登録のオプションを表示します。
- [登録タイプ (Enrollment Type)] 領域で、[セキュリティ/CDOアカウント (Security/CDO Account)] をクリックします。

6.6 では、このタブは [セキュリティアカウント (Security Account)] となっています。

- (6.7以降) [Cisco Defense Orchestratorからテナントへの自動登録 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)] をオンに「しない」でください。

シリアル番号を使用した自動登録の詳細については、[FDM のコンフィギュレーションガイド](#)を参照してください。

- [リージョン (Region)] フィールドで、テナントが割り当てられている Cisco Cloud のリージョンを選択します。

- *defenseorchestrator.com* にログインする場合は、[US] を選択します。

- *defenseorchestrator.eu* にログインする場合は、[EU] を選択します。
 - *apj.cdo.cisco.com* にログインする場合は、[APJ] を選択します。
- f) [登録キー (Registration Key)] フィールドに、CDO で生成した登録キーを貼り付けます。
- g) (6.7以降) [サービス登録 (Service Enrollment)] 領域で、[Cisco Defense Orchestratorを有効にする (Enable Cisco Defense Orchestrator)] をオンにします。
- 6.6 では、CDO を有効にする前にクラウド登録を完了する必要があります (手順 8.j (25 ページ) を参照)。
- h) (6.7以降) Cisco Success Network に関する情報を確認します。参加しない場合は、[Cisco Success Networkに登録 (Enroll Cisco Success Network)] をオフにします。
- 6.6 では、Cisco Success Network を有効にする前にクラウド登録を完了する必要があります。
- i) [登録 (Register)] をクリックし、[シスコの開示情報を受け入れる (Accept the Cisco Disclosure)] をクリックします。FDM が CDO に登録要求を送信します。
- j) (6.6) [クラウドサービス (Cloud Services)] ページを更新します。デバイスが Cisco Cloud に正常に登録されたら、[Cisco Defense Orchestrator] タイルで [有効 (Enable)] をクリックします。
- 6.7 以降では、登録時に CDO を有効にすることができます。

ステップ 9 CDOに戻ります。[スマートライセンス (Smart License)] 領域で、スマートライセンスをFTD デバイスに適用し、[次へ (Next)] をクリックします。

詳細については、「[ライセンスの設定 \(35ページ\)](#)」を参照してください。[スキップ (Skip)] をクリックして、90 日間の評価ライセンスでのオンボーディングを続行します。

ステップ 10 [完了 (Done)] 領域で、[デバイスへ移動 (Go to devices)] をクリックしてオンボードされたデバイスを表示します。

ステップ 11 [デバイスとサービス (Devices & Services)] で、デバイスのステータスが [プロビジョニングされていない (Unprovisioned)] から [検索中 (Locating)]、[同期中 (Syncing)]、[同期済み (Synced)] になっていることを確認します。

登録キーを使用した FTD のオンボード (バージョン 6.4 または 6.5)

登録キーを使用して FTD デバイスをオンボードするには、次の手順を実行します。

始める前に

- (バージョン 6.5) この方法は、米国、EU、および APJ (*apj.cdo.cisco.com*) リージョンでサポートされています。

(バージョン 6.4) この方法は、米国リージョン (*defenseorchestrator.com*) でのみサポートされます。EU リージョン (*defenseorchestrator.eu*) の場合、バージョン 6.4 では、ユーザ

名、パスワード、および IP アドレスを使用した FTD デバイスをオンボードのみが可能です。登録キーは使用できません。

- Firepower Device Manager (FDM) によってデバイスが管理されている必要があります。デバイスで待機している保留中の変更がないことを確認します。
- 90 日間の評価ライセンスを使用するようにデバイスを設定する必要があります。FTD がすでにスマートライセンスを取得している場合は、FTD の登録を解除する必要があります。FDM の [デバイス (Device)] >> [スマートライセンス (Smart License)] ページで、歯車のドロップダウンメニューから [デバイスの登録解除 (Unregister Device)] を選択します。
- FTD デバイスで DNS が正しく設定されていることを確認します。
- FTD デバイスでタイムサービスが正しく設定されていることを確認します。FTD デバイスに正しい日付と時刻が表示されていることを確認します。そうでない場合はオンボーディングは失敗します。

手順

- ステップ 1** CDO のナビゲーションウィンドウで [デバイスとサービス (Devices & Services)] をクリックし、青色のプラスボタン (+) をクリックしてデバイスを [オンボード (Onboard)] します。
- ステップ 2** [FTD] カードをクリックします。
- ステップ 3** [登録キーを使用 (Use Registration Key)] をクリックします。
- ステップ 4** [デバイス名 (Device Name)] 領域のフィールドに値を入力します。

図 8: デバイス名 (Device Name)

Follow the steps below Cancel

FTD Device
Firepower Threat Defense 6.4+

Use Serial Number
Use this method for low-touch provisioning or for onboarding configured devices using their serial number.
(FTD 6.7+, 1000 and 2100 series only)

Use Registration Key
Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.

Use Credentials
Onboard a device using its IP address, or host name, and a username and password.

1 Device Name

Select Secure Device Connector

SDC-2

Device Name

Next

! **Important:** If you already have a SecureX or Cisco Threat Response (CTR) account, you will need to merge your CDO account and SecureX/CTR account in order for your devices to be registered with SecureX. Your accounts can be merged through the SecureX portal. See [Merge Your CDO and SecureX Accounts](#) for instructions. Until your accounts are merged, you will not be able to see your device's events in SecureX or benefit from other SecureX features.

- a) このデバイスが通信する **Secure Device Connector** を選択します。デフォルトの SDC が表示されますが、SDC 名をクリックすることで SDC を変更できます。

- b) [デバイス (Device Name)]フィールドにデバイス名を入力します。デバイスのホスト名またはその他の任意の名前にすることができます。
- c) [次へ (Next)]をクリックします。


ステップ 5 [データベースの更新 (Database Updates)]領域で、[セキュリティ更新を即時に実行し、定期更新を有効にする (Immediately security updates, and enable recurring updates)]をオンまたはオフにして、[次へ (Next)]をクリックします。

このオプションは、セキュリティ更新をすぐにトリガーするとともに、毎週月曜日の午前2時に追加の更新をチェックするようにデバイスを自動的にスケジュールします。詳細については、『[Update FTD Security Databases](#)』と『[Schedule a Security Database Update](#)』を参照してください。

(注) このオプションを無効にしても、以前に FDM を使用して設定したスケジュール済みの更新には影響しません。

ステップ 6 CDO によって [登録キーの作成 (Create Registration Key)]領域に登録キーが生成されます。

(注) キーが生成された後でデバイスが完全にオンボーディングされる前にオンボーディング画面から移動すると、オンボーディング画面に戻ることができません。ただし、CDO によって [デバイスとサービス (Device & Services)]ページにそのデバイスのプレースホルダが作成されます。デバイスのプレースホルダを選択して、そのデバイスのキーを表示します。

ステップ 7 [コピー (Copy)]アイコン () をクリックして登録キーをコピーし、[次へ (Next)]をクリックします。

(注) 登録キーのコピーをスキップして [次へ (Next)]をクリックすると、デバイスのプレースホルダエントリを完了した後でデバイスを登録できます。このオプションは、最初にデバイスを作成してから登録する場合、またはシスコネットワークパートナーがカスタマーネットワークに価値の実証 (POV) デバイスをインストールする場合に役立ちます。

この時点で、デバイスの接続状態は「プロビジョニング解除 (Unprovisioned) 」になります。[Firepower Defense Manager へのプロビジョニングの解除 (Unprovisioned to Firepower Defense Manager)]の下に表示される登録キーをコピーしてオンボーディングプロセスを完了します。

ステップ 8 CDO にオンボードするデバイスの FDM にログインします。

- a) [システム設定 (System Settings)]で、[クラウドサービス (Cloud Services)]をクリックします。
- b) [Cisco Defense Orchestrator] グループで、[始める (Get Started)]をクリックします。
- c) [リージョン (Region)]フィールドで、テナントが割り当てられている Cisco Cloud のリージョンを選択します。
 - *defenseorchestrator.com* にログインする場合は、[US] を選択します。
 - *defenseorchestrator.eu* にログインする場合は、[EU] を選択します (バージョン 6.5) 。

- apj.cdo.cisco.com にログインする場合は、[APJ] を選択します (バージョン 6.5)。

- d) [登録キー (Registration Key)] フィールドに、CDO で生成した登録キーを貼り付けます。
- e) [登録 (Register)] をクリックし、[シスコの開示情報を受け入れる (Accept the Cisco Disclosure)] をクリックします。FDM が CDO に登録要求を送信します。

ステップ 9 CDOに戻ります。[スマートライセンス (Smart License)] 領域で、スマートライセンスを FTD デバイスに適用し、[次へ (Next)] をクリックします。

詳細については、「[ライセンスの設定 \(35 ページ\)](#)」を参照してください。[スキップ (Skip)] をクリックして、90 日間の評価ライセンスでのオンボーディングを続行します。

ステップ 10 [完了 (Done)] 領域で、[デバイスへ移動 (Go to devices)] をクリックしてオンボードされたデバイスを表示します。

ステップ 11 [デバイスとサービス (Devices & Services)] で、デバイスのステータスが [プロビジョニングされていない (Unprovisioned)] から [検索中 (Locating)]、[同期中 (Syncing)]、[同期済み (Synced)] になっていることを確認します。

クレデンシャルと IP アドレスを使用した FTD のオンボード

ログイン情報 (ユーザ名/パスワード) と IP アドレスまたは FQDN を使用して FTD をオンボーディングできます。ただし、デバイスが静的 IP アドレスに依存せず、オンプレミスの SDC を必要としない、登録キーを使用したデバイスのオンボードをお勧めします。[登録キーを使用した FTD のオンボード \(推奨\) \(22 ページ\)](#) を参照してください。

始める前に

- この方法を使用して、デバイスを米国、EU、または APJ リージョンにオンボードできません。
- Firepower Device Manager (FDM) によってデバイスが管理されている必要があります。デバイスで待機している保留中の変更がないことを確認します。
- デバイスで 90 日間の評価ライセンスを使用するかスマートライセンスを使用することができます。Cisco Smart Software Manager から、デバイスにインストールされているライセンスの登録を解除する必要はありません。
- 内部インターフェイスに接続されたオンプレミスの Secure Device Connector (SDC) を展開することをお勧めします。代わりに、外部インターフェイスを介してクラウドの SDC を使用する場合は、外部での HTTPS アクセスを許可 (FDM の [システム設定 (System Settings)] > [管理アクセス (Management Access)]) する必要がありますが、セキュリティ上の理由からお勧めできません。SDC の詳細については、[Cisco Defense Orchestrator と Firepower Threat Defense の連携の仕組み \(4 ページ\)](#) を参照してください。
- 静的 IP アドレスを使用して CDO の管理/SDC の通信に使用するインターフェイスを設定するか、動的 DNS (DDNS) を使用して一貫性のある FQDN を維持します。FDM で DDNS を設定することはできません。

手順

- ステップ 1** CDO のナビゲーションウィンドウで [デバイスとサービス (Devices & Services)] をクリックし、青色のプラスボタン (+) をクリックしてデバイスを [オンボード (Onboard)] します。
- ステップ 2** [FTD] カードをクリックします。
- ステップ 3** [ログイン情報を使用 (Use Credentials)] をクリックします。
- ステップ 4** [デバイス名 (Device Name)] 領域のフィールドに値を入力します。

図 9: デバイス名 (Device Name)

The screenshot shows the 'Device Details' section of the FTD Onboard interface. It includes a 'Select Secure Device Connector' dropdown menu with 'cisco-security-docs-SDC' selected. Below this are three input fields: 'Device Name' (containing 'FTD1'), 'Location' (containing '10.88.6.67'), and a 'Next' button.

- このデバイスが通信する **Secure Device Connector** を選択します。デフォルトの SDC が表示されますが、SDC 名をクリックすることで SDC を変更できます。
 - [デバイス (Device Name)] フィールドにデバイス名を入力します。デバイスのホスト名またはその他の任意の名前にすることができます。
 - [ロケーション (Location)] に IP アドレス、ホスト名、または FQDN を入力します。
デフォルトポートは 443 です。デバイスの設定を反映するようにポート番号を変更できます。
 - [次へ (Next)] をクリックします。
- ステップ 5** [データベースの更新 (Database Updates)] 領域で、[セキュリティ更新を即時に実行し、定期更新を有効にする (Immediately security updates, and enable recurring updates)] をオンまたはオフにして、[次へ (Next)] をクリックします。

このオプションは、セキュリティ更新をすぐにトリガーするとともに、毎週月曜日の午前 2 時に追加の更新をチェックするようにデバイスを自動的にスケジュールします。詳細については、『[Update FTD Security Databases](#)』と『[Schedule a Security Database Update](#)』を参照してください。

(注) このオプションを無効にしても、以前に FDM を使用して設定したスケジュール済みの更新には影響しません。

ステップ 6 [ログイン情報 (Credentials)] 領域で、ユーザ名を「admin」と入力し、初期設定時に指定したパスワードを入力します。次に、[次へ (Next)] をクリックします。

CDO が接続をテストし、デバイスに到達できることを確認します。成功すると、[ログイン情報 (Credentials)] 領域に「接続中 (Connected)」と表示され、[オンボーディングチェック (Onboarding Checks)] 領域に「完了 (Done)」と表示されます。

ステップ 7 [完了 (Done)] 領域で、[デバイスへ移動 (Go to devices)] をクリックしてオンボードされたデバイスを表示します。

CDO でのデバイスの設定

次の手順では、追加機能の設定の概要を説明します。各手順について詳細な情報を表示するには、ページのヘルプ ボタン (?) をクリックしてください。

手順

ステップ 1 CDO ポータルにログインし、CDO メニューから [デバイスとサービス (Devices & Services)] を選択し、オンボードしたデバイスを選択します。

ステップ 2 [管理 (Management)] > [インターフェイス (Interfaces)] を選択し、設定する物理インターフェイスを選択します。

ステップ 3 設定する各インターフェイスの編集アイコン (🔗) をクリックし、インターフェイスに [論理名 (Logical Name)] と、必要に応じて [説明 (Description)] を入力します。

サブインターフェイスを設定する場合を除き、インターフェイスには名前が必要です。

(注) 名前を変更すると、その変更は古い名前を使用しているすべての場所 (セキュリティゾーン、syslog サーバオブジェクト、DHCP サーバの定義を含む) に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

ステップ 4 [タイプ (Type)] を設定し、IP アドレスとその他の設定を定義します。

次の例では、Web サーバなどのパブリックアクセス可能な資産を配置する「緩衝地帯」 (DMZ) として使用するためのインターフェイスを構成します。完了したら [保存 (Save)] をクリックします。

図 10: インターフェイスの編集

Editing Physical Interface

Logical Name: dmz State

Description

IPv4 Address | IPv6 Address | Advanced

Type: Static

IP Address and Subnet Mask: 192.168.6.1 / 24
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

DHCP Address Pool: Enter DHCP address pool
e.g. 192.168.5.20-192.168.5.30 or 192.168.5.20

Standby IP Address: Enter IP address / 24
e.g. 192.168.5.16

Cancel Save

ステップ 5 新しいインターフェイスを設定した場合は、[管理 (Management)] > [オブジェクト (Objects)] を選択します。

必要に応じて、新しい[セキュリティゾーン (Security Zone)]を作成または編集します。インターフェイスではなく、セキュリティゾーンに基づいてポリシーを構成するため、各インターフェイスはゾーンに属している必要があります。インターフェイスを構成する場合、ゾーンにインターフェイスを置くことはできません。このため、新しいインターフェイスを作成した後、または既存のインターフェイスの目的を変更した後は常にゾーンオブジェクトを編集する必要があります。

次の例では、DMZインターフェイスのために新しいDMZゾーンを作成する方法を示します。

図 11: セキュリティゾーンオブジェクト

Adding FTD Security Zone

Object Name: dmz-zone

Description: Object description

Select Interfaces

Search for interfaces or devices

<input checked="" type="checkbox"/>	Name	Devices
<input checked="" type="checkbox"/>	dmz	ftd-650-1543-180

Selected Interfaces: 1 Clear

dmz

ステップ 6 内部クライアントで DHCP を使用してデバイスから IP アドレスを取得する場合は、[管理 (Management)] > [設定 (Settings)] > [DHCPサーバ (DHCP Server)] を選択してから、[DHCPサーバ (DHCP Servers)] セクションを確認します。

すでに内部インターフェイス用に構成されている DHCP サーバがありますが、アドレスプールを編集したり、それを削除したりすることができます。他の内部インターフェイスを構成した場合は、それらのインターフェイス上に DHCP サーバをセットアップするのがごく一般的です。[+] をクリックして各内部インターフェイスのサーバとアドレスプールを構成します。

[DNSサーバ (DNS Server)] タブでは、クライアントに提供する DNS 設定を確認することもできます。次に、アドレスプール 192.168.45.46 ~ 192.168.45.254 を使用して inside2 インターフェイス上の DHCP サーバを設定する例を示します。

図 12: DHCP サーバ



ステップ 7 [管理 (Management)] > [ルーティング (Routing)] を選択し、[追加 (Add)] アイコンをクリックしてデフォルトルートを設定します。

デフォルトルートは通常、外部インターフェイス以外に存在するアップストリームまたは ISP ルータを指しています。デフォルトの IPv4 ルートは任意の ipv4 (0.0.0.0/0)、デフォルトの IPv6 ルートは任意の ipv6 (::0/0) です。使用する IP バージョンごとにルートを作成します。外部インターフェイスのアドレスの取得に DHCP を使用する場合、必要なデフォルトルートをすでに持っていることがあります。

(注) このページで定義したルートは、データインターフェイス用のみです。管理インターフェイスには影響しません。管理ゲートウェイは [管理 (Management)] > [設定 (Settings)] > [管理アクセス (Management Settings)] で設定します。

次の例に、IPv4 のデフォルトルートを示します。この例では、isp ゲートウェイは ISP ゲートウェイの IP アドレスを識別するネットワーク オブジェクトです (アドレスは ISP から取得する必要があります)。このオブジェクトを作成するには、[ゲートウェイ (Gateway)] ドロップダウンリストの下部にある [新しいオブジェクトの作成 (Create New Object)] をクリックします。

図 13: デフォルトルート

The screenshot shows the 'Add Static Route' configuration window. It includes the following fields and options:

- Name:** isp-gateway
- Description:** isp-gateway
- Protocol:** IPv4 (selected), IPv6
- Gateway:** isp-gateway
- Interface:** outside
- Metric:** 1 (range 1 - 255)
- Destination Networks:** any-ipv4

Buttons for 'Cancel' and 'OK' are visible at the bottom right.

ステップ 8 [管理 (Management)] > [ポリシー (Policies)] を選択してネットワークのセキュリティポリシーを設定します。

初期セットアップでは、内部ゾーンと外部ゾーン間のトラフィックフローを有効にします。また、外部インターフェイスを使用する場合に、全インターフェイスに対するインターフェイス NAT も有効にします。新しいインターフェイスを構成した場合でも、内部ゾーンオブジェクトに追加する場合はそれらにアクセス制御ルールが自動的に適用されます。

ただし、複数の内部インターフェイスがある場合は、内部ゾーンから内部ゾーンへのトラフィックフローを許可するアクセス制御ルールが必要です。他のセキュリティゾーンを追加する場合は、それらのゾーンとのトラフィックを許可するルールが必要です。これらは最低限の変更になります。

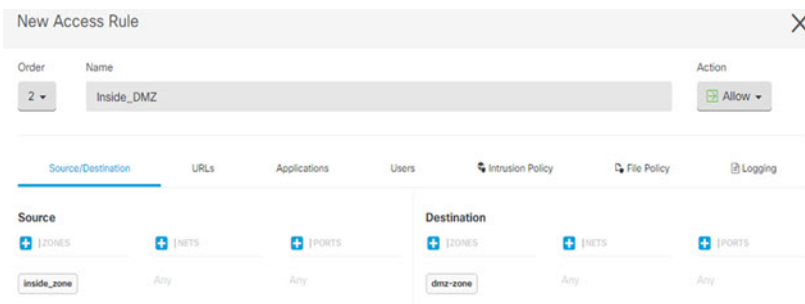
さらに、組織が必要とする結果を得るために、その他のポリシーを設定して、追加サービスの提供や、NAT およびアクセスルールを微調整できます。次のポリシーを設定できます。

- [SSL復号 (SSL Decryption)] : 侵入、マルウェアなどについて暗号化された接続 (HTTPS など) を検査する場合は、接続を復号化する必要があります。どの接続を復号する必要があるかを判断するには SSL 復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。
- [アイデンティティ (Identity)] : 個々のユーザにネットワークアクティビティを関連付ける、またはユーザまたはユーザグループのメンバーシップに基づいてネットワークアクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザを判定するためにアイデンティティポリシーを使用します。

- [セキュリティインテリジェンス (Security Intelligence)] : ブラックリスト登録済みの IP アドレスまたは URL の接続をただちにドロップするには、セキュリティ インテリジェンス ポリシーを使用します。既知の不正なサイトをブラックリストに登録すれば、アクセスコントロールポリシーでそれらを考慮する必要がなくなります。Cisco では、セキュリティ インテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスや URL の定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。
- [アクセス制御 (Access Control)] : ネットワーク上で許可する接続の決定にアクセスコントロール ポリシーを使用します。セキュリティゾーン、IP アドレス、プロトコル、ポート、アプリケーション、URL、ユーザまたはユーザグループによってフィルタ処理できます。また、アクセス制御ルールを使用して侵入やファイル (マルウェア) ポリシーを適用します。このポリシーを使用して URL フィルタリングを実装します。

次の例では、アクセス制御ポリシーで内部ゾーンと DMZ ゾーンの間でのトラフィックを許可する方法を示します。この例では、[接続の最後で (At End of Connection)] が選択されている場合、[ロギング (Logging)] を除いて他のいずれのタブでもオプションは設定されません。

図 14: アクセスコントロールポリシー



ステップ 9 [セキュリティデータベースの更新 (Security Database Updates)] セクションを見つけて、FTD デバイスのセキュリティデータベースを確認および更新するスケジュール済みタスクを作成します。

FTD デバイスを CDO にオンボードする場合、オンボーディングプロセスの一部を使用して、[データベースの予約済みの定期更新の有効化 (Enable scheduled recurring updates for databases)] を許可します。このオプションは、デフォルトでオンです。有効にすると、CDO はすぐにセキュリティの更新を確認して適用し、追加の更新を確認するようにデバイスを自動的にスケジュールします。また、デバイスがオンボードされた後は、スケジュール済みのタスクの日時を変更することもできます。

侵入ポリシーを使用している場合は、ルールと VDB のデータベースを定期的な更新を設定します。セキュリティ情報フィードを使用する場合は、それらの更新スケジュールを設定します。一致基準としてセキュリティポリシーで地理位置情報を使用する場合は、そのデータベースの更新スケジュールを設定します。

ステップ 10 メニューの [プレビューと展開 (Preview and Deploy)] ボタンをクリックしてから [今すぐ展開 (Deploy Now)] ボタンをクリックし、変更をデバイスに展開します。

変更は、それらを展開するまでデバイスで有効になりません。

次のタスク

- オンボード後にデバイスを登録し、ライセンスを付与する必要があります。[ライセンスの設定 \(35 ページ\)](#) を参照してください。

ライセンスの設定

ライセンスの設定

FTD は、ライセンスの購入およびライセンス プールの一元管理を可能にするシスコ スマート ソフトウェア ライセンシングを使用します。

シャーンを登録すると、License Authority によってシャーンと License Authority 間の通信に使用される ID 証明書が発行されます。また、適切な仮想アカウントにシャーンが割り当てられます。

基本ライセンスは自動的に含まれます。スマートライセンスでは、まだ購入していない製品の機能を使用できます。Cisco Smart Software Manager に登録すると、すぐにライセンスの使用を開始できます。また、後でライセンスを購入することもできます。これによって、機能の展開および使用が可能になり、発注書の承認による遅延がなくなります。次のライセンスを確認してください。

- **脅威** : セキュリティ インテリジェンスと Cisco Firepower の次世代 IPS
- **マルウェア** : 強化されたネットワーク向けの高度なマルウェア防御 (AMP)
- **URL** : URL フィルタリング
- **RA VPN** : AnyConnect Plus、AnyConnect Apex、または AnyConnect VPN 専用。

システムのライセンシングの詳細については、『[FDM コンフィグレーション ガイド](#)』を参照してください。

始める前に

- [Cisco Smart Software Manager](#) にマスター アカウントを持ちます。
まだアカウントをお持ちでない場合は、このリンクをクリックして[新しいアカウントをセットアップ](#)してください。Smart Software Manager では、組織のマスター アカウントを作成できます。
- (輸出コンプライアンスフラグを使用して有効化される) 機能を使用するには、ご使用のシスコ スマート ソフトウェア ライセンシング アカウントで強力な暗号化 (3DES/AES) ライセンスを使用できる必要があります。

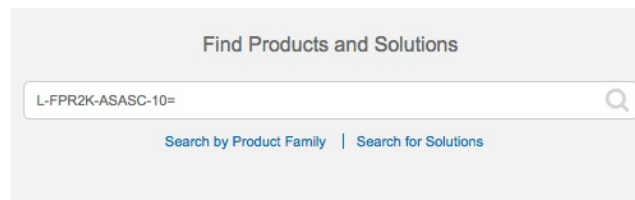
- CDO にデバイスをオンボードするまでは評価ライセンスを使用します。Smart Software Manager に登録する追加のライセンスは、CDO にオンボードして再登録する前に登録解除する必要があります。

手順

ステップ 1 お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマートソフトウェア ライセンシング アカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、[Cisco Commerce Workspace](#) で [製品とソリューションの検索 (Find Products and Solutions)] 検索フィールドを使用します。次のライセンス PID を検索します。

図 15: ライセンス検索



(注) PID が見つからない場合は、注文に手動で PID を追加できます。

- 脅威、マルウェア、および URL ライセンスの組み合わせ：
 - L-FPR2110T-TMC=
 - L-FPR2120T-TMC=
 - L-FPR2130T-TMC=
 - L-FPR2140T-TMC=

上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。

- L-FPR2110T-TMC-1Y
- L-FPR2110T-TMC-3Y
- L-FPR2110T-TMC-5Y
- L-FPR2120T-TMC-1Y
- L-FPR2120T-TMC-3Y
- L-FPR2120T-TMC-5Y
- L-FPR2130T-TMC-1Y
- L-FPR2130T-TMC-3Y

- L-FPR2130T-TMC-5Y
- L-FPR2140T-TMC-1Y
- L-FPR2140T-TMC-3Y
- L-FPR2140T-TMC-5Y

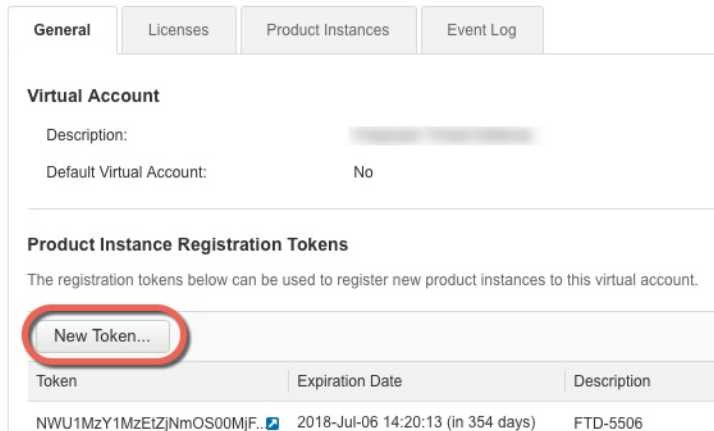
• RA VPN : 『Cisco AnyConnect Ordering Guide』を参照してください。

ステップ 2 [Smart Software Manager](#) で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

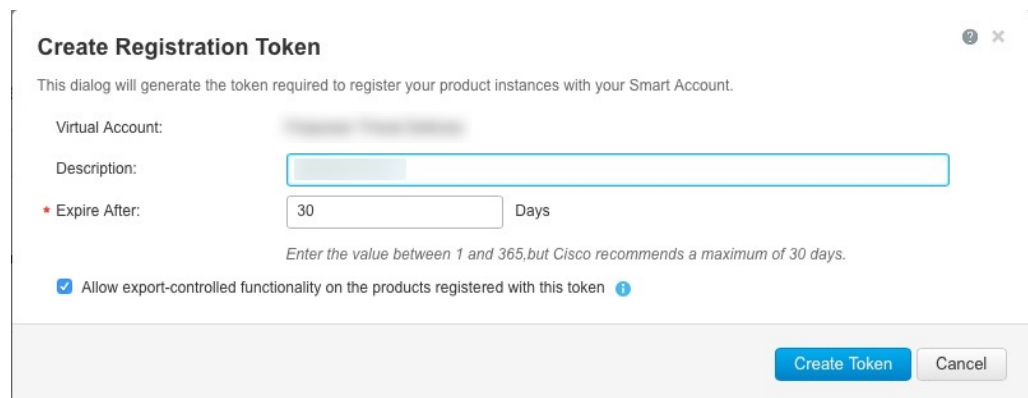
a) [インベントリ (Inventory)] をクリックします。



b) [全般 (General)] タブで、[新規トークン (New Token)] をクリックします。



c) [登録トークンを作成 (Create Registration Token)] ダイアログボックスで、以下の設定値を入力してから [トークンを作成 (Create Token)] をクリックします。



- [説明 (Description)]

- [有効期限 (Expire After)] : 推奨値は 30 日です。

- [このトークンに登録された製品で輸出管理機能を許可する (Allow export-controlled functionality on the products registered with this token)] : 高度暗号化が許可されている国の場合は輸出コンプライアンスフラグを有効にします。

トークンはインベントリに追加されます。

- d) トークンの右側にある矢印アイコンをクリックして [トークン (Token)] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。FTD の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 16: トークンの表示

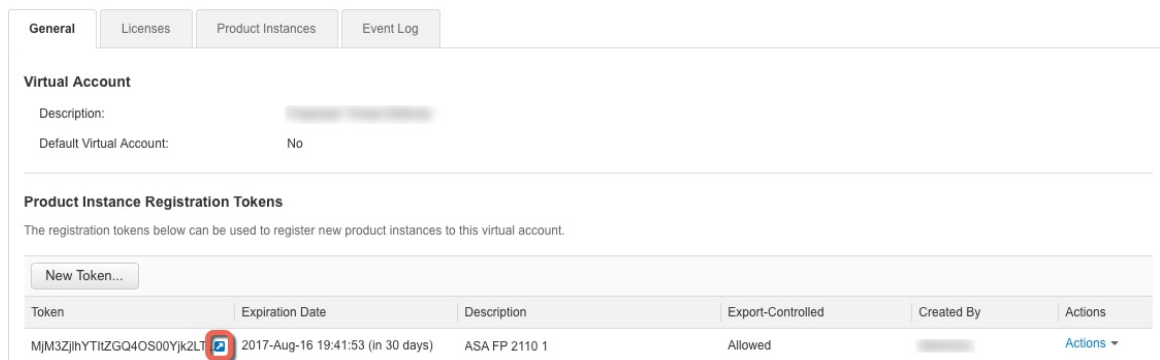
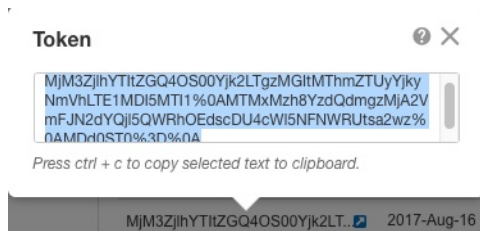


図 17: トークンのコピー



ステップ 3 CDOで、[デバイスとサービス (Devices & Services)] をクリックし、ライセンスを付与する FTD デバイスを選択します。

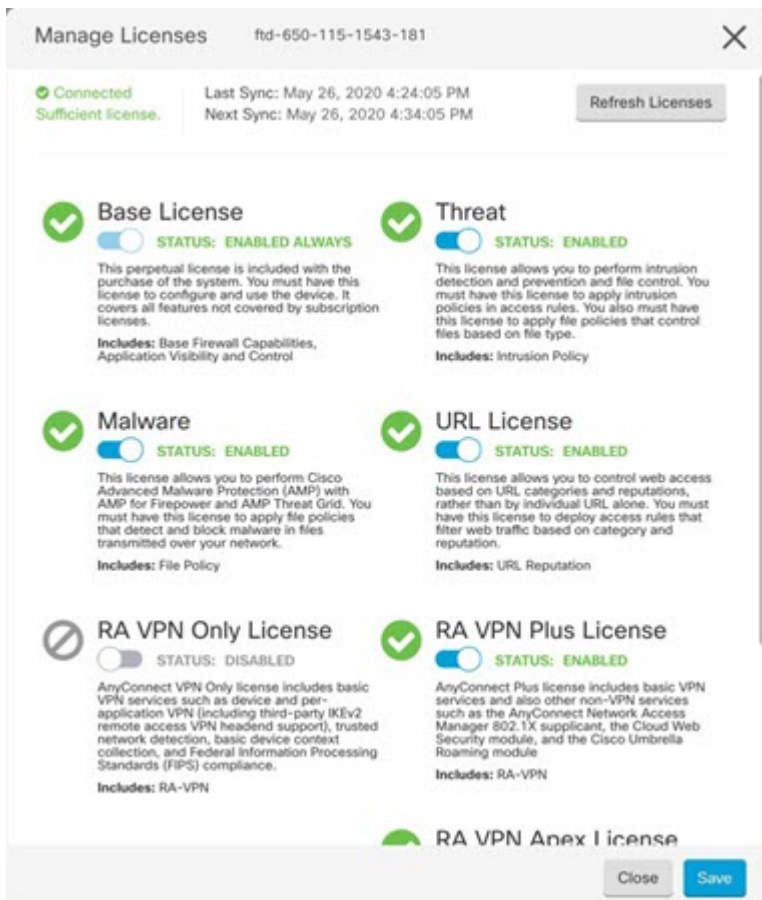
ステップ 4 [デバイスのアクション (Device Actions)] ペインで、[ライセンスの管理 (Manage Licenses)] をクリックし、画面の指示に従って Smart Software Manager から生成されたスマートライセンスを入力します。

ステップ 5 [デバイスの登録 (Register Device)] をクリックします。デバイスと同期すると、接続状態が「オンライン (Online) 」に変わります。

[ライセンスの管理 (Manage License)] ページに戻ります。デバイス登録中は次のメッセージが表示されます。

Registration request sent on 10 Jul 2019. Please wait. Normally, it takes about one minute to complete the registration. You can check the task status in Task List. Refresh this page to see the updated status.

ステップ 6 スマートライセンスが FTD デバイスに正常に適用されると、デバイスのステータスに [接続済み、十分なライセンス (Connected, Sufficient License)] と表示されます。必要に応じて、それぞれのオプションライセンスの [有効化/無効化 (Enable/Disable)] スライダコントロールをクリックします。



- [有効化 (Enable)] : Cisco Smart Software Manager アカウントにライセンスを登録し、制御された機能が有効になります。ライセンスによって制御されるポリシーを設定し、展開できます。
- [無効化 (Disable)] : Cisco Smart Software Manager アカウントのライセンスを登録解除し、制御された機能が無効になります。新しいポリシーの機能の設定も、その機能を使用するポリシーの展開もできません。
- **RA VPN** ライセンスを有効にした場合は、使用するライセンスのタイプ ([Plus]、[Apex]、[VPN 専用 (VPN Only)]、または [Plus と Apex (Plus and Apex)]) を選択します。

機能を有効にすると、アカウントにライセンスがない場合は [ライセンスの問題、コンプライアンス違反 (License Issue, Out of Compliance)] ページを更新した後に次の非準拠メッセージが表示されます。

ステップ7 [ライセンスの更新 (Refresh Licenses)] を選択し、ライセンス情報を Cisco Smart Software Manager と同期します。

FTD および FXOS CLI へのアクセス

コマンドラインインターフェイス (CLI) を使用してシステムのセットアップを行い、基本的なシステムのトラブルシューティングを行います。CLIセッションからポリシーを設定することはできません。CLIには、コンソールポートに接続してアクセスできます。

トラブルシューティングのために、FXOS CLIにアクセスすることもできます。



(注) または、FTD デバイスの管理インターフェイスに SSH で接続できます。コンソールセッションとは異なり、SSHセッションはデフォルトで FTD CLI になり、**connect fxos** コマンドを使用しても FXOS CLI には接続できません。SSH 接続用のインターフェイスを開いている場合、後でデータインターフェイス上のアドレスに接続できます。データインターフェイスへの SSH アクセスはデフォルトで無効になっています。この手順では、デフォルトで FXOS CLI となるコンソールポートアクセスについて説明します。

手順

ステップ1 CLIにログインするには、管理コンピュータをコンソールポートに接続します。Firepower2100にはDB-9 to RJ-45 シリアルケーブルが付属しているため、接続するためにはサードパーティ製のシリアル to USB ケーブルが必要です。ご使用のオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください。コンソールポートはデフォルトでFXOS CLIになります。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

FXOS CLIに接続します。ユーザ名 **admin** と、初期セットアップ時に設定したパスワードを使用して CLI にログインします (デフォルトは **Admin123**) 。

例 :

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

ステップ2 FTD CLI にアクセスします。

connect ftd

例 :

```
firepower# connect ftd
>
```

ログイン後に、CLI で使用可能なコマンドの情報を確認するには、**help** または **?** を入力します。使用法の詳細については、『[Cisco Firepower Threat Defense Command Reference](#)』を参照してください。

ステップ3 FTD CLI を終了するには、**exit** または **logout** コマンドを入力します。

このコマンドにより、FXOS CLI プロンプトに戻ります。FXOS CLI で使用可能なコマンドの情報を確認するには、**?** を入力します。

例 :

```
> exit
firepower#
```

FDM を使用したデバイスの電源オフ

FDM を使用してシステムを適切にシャットダウンできます。

手順

ステップ1 (6.5 以降) FDM を使用してデバイスをシャットダウンします。

(注) 6.4 以前の場合は、FDM CLI で **shutdown** コマンドを入力します。

- [デバイス (Device)] をクリックし、[システム設定 (System Settings)] > [再起動/シャットダウン (Reboot/Shutdown)] リンクをクリックします。
- [シャットダウン (Shut Down)] をクリックします。

- ステップ2** 電源 LED とステータス LED を観察して、シャーシの電源が切断されていることを確認します (LED が消灯)。
- ステップ3** シャーシの電源が正常に切断されたら、必要に応じて電源プラグを抜き、シャーシから物理的に電源を取り外すことができます。
-

次のステップ

CDO を使用した FTD デバイスの設定を続行するには、『[CDO コンフィギュレーション ガイド](#)』を参照してください。

CDO の使用に関する追加情報については、[Cisco Defense Orchestrator](#) のホームページを参照してください。