デバイスとサービスのオンボーディング

ライブデバイスとモデルデバイスの両方を CDO にオンボーディングできます。モデルデバイスはアップロードされた構成ファイルであり、CDO を使用して閲覧および編集できます。

ほとんどのライブデバイスおよびサービスでは、Secure Device Connector が CDO をデバイスまたはサービスに接続できるように、オープンな HTTPS 接続が必要となります。

SDC とそのステータスの詳細については、 Secure Device Connector（SDC） を参照してください。

この章は、次のセクションで構成されています。

FTD のオンボーディング

FTDデバイスのオンボーディングにはさまざまな方法があります。登録キー方式を使用することが推奨されます。

デバイスのオンボーディング中に問題が発生した場合は、シリアル番号を使用した FTD オンボーディングのトラブルシュートまたはライセンス不足のために失敗で詳細を参照してください。

シリアル番号を使用した FTD のオンボーディング

この手順は、サポートされているバージョンの FTD ソフトウェアを実行している Firepower 1000、2100、または 3100 シリーズの物理デバイスをオンボーディングする簡単な方法です。デバイスをオンボードするには、デバイスのシャーシシリアル番号または PCA シリアル番号が必要です。また、インターネットに接続できるネットワークにデバイスが追加されていることを確認します。

工場から出荷された新しいデバイスも、すでに設定済みのデバイスもオンボーディングすることができます。CDO

詳細については、「デバイスのシリアル番号を使用した FTD の導入準備」を参照してください。

登録キーを使用した FTD のオンボーディング

登録キーを使用してFTDデバイスをオンボーディングすることが推奨されます。これは、FTD に DHCP を使用して IP アドレスが割り当てられている場合に役立ちます。その IP アドレスが何らかの理由で変更された場合、登録キーを使用してオンボードしていれば、FTD は CDO に接続されたままになります。

- 登録キーを使用したソフトウェアバージョン 6.4 または 6.5 を実行する FTD の導入準備
- 登録キーを使用したソフトウェアバージョン 6.6+ を実行する FTD のオンボード

ログイン情報を使用した FTD デバイスのオンボーディング

ネットワーク内でのデバイスの設定に応じて、デバイスの外部インターフェイス、内部インターフェイス、または管理インターフェイスの IP アドレスおよびデバイスのログイン情報を使用して FTD をオンボードできます。ログイン情報を使用してデバイスをオンボードするには、ユーザー名、パスワード、IP アドレスを使用した FTD のオンボーディング （10 ページ）を参照してください。インターフェイスアドレスを使用してオンボードするには、この記事で後述する「FTD のオンボーディング」を参照してください。

CDO を管理するには、FTD への HTTPS アクセスが必要です。デバイスへの HTTPS アクセスを許可する方法は、ネットワークでの FTD の設定方法や、Secure Device Connector と Cloud Connector のどちらを使用してデバイスをオンボードしたかによって異なります。

（注） https://www.defenseorchestrator.eu に接続し、FTD ソフトウェアバージョン 6.4 を使用している場合は、この方法で FTD をオンボードする必要があります。登録キーを使用して FTD デバイスをオンボードすることはできません。

デバイスのログイン情報を使用して CDO をデバイスに接続する場合、CDO とデバイス間の通信を管理するために、ネットワークに Secure Device Connector（SDC）をダウンロードして展開することがベストプラクティスです。通常、これらのデバイスは非境界ベースであり、パブリック IP アドレスを持たないか、外部インターフェイスに開かれたポートを持っています。

ログイン情報を使用してオンボードした FTD デバイスは、SDC を使用して CDO にオンボードできます。

お客様が FTD を VPN 接続のヘッドエンドとしても使用している場合は、外部インターフェイスを使用してデバイスを管理することはできません。

FTD HA ペアのオンボーディング

シリアル番号、登録キー方式、またはログイン情報方式を使用して、CDO の外部で形成された FTD 高可用性ペアをオンボードできます。1 つのピアデバイスをオンボードすると、CDO が別のデバイスとペアリングされていることが自動的に検出されます。CDO は、すでに提供されているログイン情報またはキーを使用して、他のピアデバイスのオンボーディングプロセスを合理化し、ペアを [インベントリ（Inventory）] ページの 1 つのエントリに結合します。

バージョン 6.4 またはバージョン 6.5 を実行する FTD HA ペアのオンボーディング （37 ページ）およびユーザー名、パスワード、IP アドレスを使用した FTD HA ペアの導入準備 （42 ページ）を参照してください。

オンボーディングのための FTD 設定の前提条件

FTD デバイス管理

Firepower Device Manager（FDM）によって管理されている FTD デバイスのみをオンボードできます。これらの FTD デバイスは、ローカル管理用にも設定する必要があります。 Firepower Management Center（FMC）で管理されている FTD デバイスは、CDO では管理できません。

デバイスがローカル管理用に設定されていない場合は、デバイスをオンボードする前にローカル管理に切り替える必要があります。『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「**Switching Between Local and Remote Management**」の章を参照してください。

ライセンシング

デバイスを CDO にオンボードするには、デバイスに少なくとも基本ライセンスがインストールされている必要があります（ただし状況によってはスマートライセンスを適用できる場合もあります）。

オンボーディング方式	FTD ソフトウェアバージョン	90 日間の評価ライセンスは許可されていますか？	オンボーディングするデバイスに予めスマートライセンスを付与できますか？	オンボーディングするデバイスを予め Cisco Cloud サービスに登録できますか？
ログイン情報（ユーザー名とパスワード）	すべて（All）	対応	対応	対応

オンボーディング方式	FTD ソフトウェアバージョン	90 日間の評価ライセンスは許可されていますか？	オンボーディングするデバイスに予めスマートライセンスを付与できますか？	オンボーディングするデバイスを予め Cisco Cloud サービスに登録できますか？
登録キー	6.4 または 6.5	対応	いいえ。スマートライセンスを登録解除してからデバイスをオンボードしてください。	該当なし
登録キー	6.6 以降	対応	対応	いいえ。Cisco Cloud サービスからデバイスを登録解除してからデバイスをオンボードしてください。
Low Touch Provisioning	6.7 以降	対応	対応	対応
シリアル番号によるデバイスのオンボーディング	6.7 以降	対応	対応	対応

詳細については『Cisco Firepower システム機能ライセンス』を参照してください。

デバイスのアドレス指定

FTDデバイスのオンボードに使用するアドレスは、静的アドレスにすることをお勧めします。デバイスの IP アドレスが DHCP によって割り当てられている場合は、DDNS（ダイナミック ドメイン ネーム システム）を使用して、デバイスの新しい IP アドレスが変更された場合に FTD のドメイン名エントリを自動的に更新するのが最適です。

（注） FTD はネイティブで DDNS をサポートしていませんので、独自の DDNS を設定する必要があります。

重要 デバイスが DHCP サーバーから IP アドレスを取得し、DDNS サーバーが FTD のドメイン名エントリを新しい IP アドレスで更新していない場合、または FTD が新しいアドレスを受け取った場合は、CDO がデバイス用に管理する IP アドレスを変更し、その後デバイスを再接続できます。さらに良い方法は、登録キーを使用してデバイスをオンボードすることです。

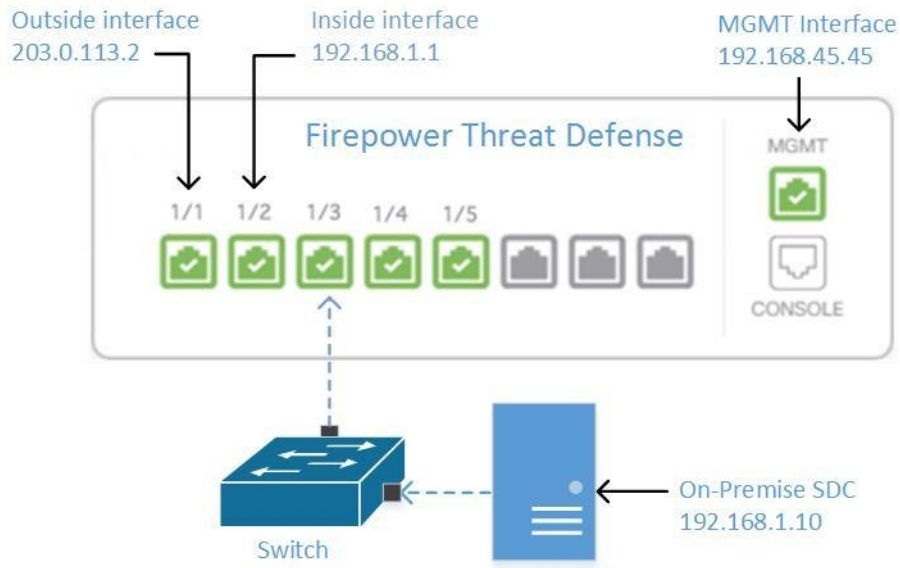
関連情報：

- ユーザー名、パスワード、IP アドレスを使用した FTD のオンボーディング （10 ページ）
- 登録キーを使用したソフトウェアバージョン 6.6+ を実行する FTD のオンボード
- デバイスのシリアル番号を使用した設定済み FTD のオンボード （28 ページ）

内部インターフェイスからの FTD の管理

専用の MGMT インターフェイスに組織内でルーティングできないアドレスが割り当てられている場合は、内部インターフェイスを使用して Firepower Threat Defense（FTD）デバイスを管理することが望ましい場合があります。たとえば、データセンターまたはラボ内からしか到達できない場合などです。

図 *1 : FTD* インターフェイスアドレス



リモートアクセス VPN の要件

CDO で管理する FTD がリモートアクセス VPN（RA VPN）接続を管理する場合、CDO は内部インターフェイスを使用して FTD デバイスを管理する必要があります。

次に行う作業：

FTD を設定する手順については、 内部インターフェイスからの FTD の管理 に進んでください。

内部インターフェイスからの FTD の管理

設定方法は次のとおりです。

- FTD が CDO にオンボードされていないことが前提です。

- データインターフェイスを内部インターフェイスとして設定します。
- MGMT トラフィック（HTTPS）を受信するように内部インターフェイスを設定します。
- SDC またはクラウドコネクタのアドレスが FTD の内部インターフェイスに到達できるようにします。

始める前に

この設定の前提条件を以下で確認してください。

- 内部インターフェイスからの FTD の管理
- Cisco Defense Orchestrator の管理対象デバイスへの接続

手順

ステップ 1 FDM にログインします。

ステップ 2 [システム設定（System Settings）] メニューで、[管理アクセス（Management Access）] をクリックします。

ステップ 3 [データインターフェース（Data Interfaces）] タブをクリックし、[データインターフェースの作成（Create Data Interface）] を選択します。

1. [インターフェース（Interface）] フィールドで、インターフェースのリストから「**inside**」という名前のインターフェースを選択します。
2. [プロトコル（pre-named）] フィールドがまだ選択されていない場合は、[HTTPS] を選択します。
3. [許可されたネットワーク（Allowed Networks）] フィールドで、組織内に配置され FTD の内部アドレスへのアクセスが許可されているネットワークを示すネットワークオブジェクトを選択します。SDC またはクラウドコネクタの IP アドレスは、FTD の内部アドレスへのアクセスが許可されているアドレス群の中にある必要があります。

   「FTD インターフェイスアドレス」図の中では、SDC の IP アドレス 192.168.1.10 が 192.168.1.1 に到達可能である必要があります。

ステップ 4 **変更を展開します**。これで、内部インターフェイスを使用してデバイスを管理できるようになりました。

次のタスク

Cloud Connector を使用している場合

上記の手順に加えて、以下の手順を実行します。

- 外部インターフェイス（203.0.113.2）から内部インターフェイス（192.168.1.1）への「NAT」を実行するステップを追加します。
- 上記の手順のステップ 3c の [許可ネットワーク（Allowed Network）] は、Cloud Connector のパブリック IP アドレスを含むネットワーク グループ オブジェクトになります。
- クラウドコネクタのパブリック IP アドレスから外部インターフェイス（203.0.113.2）へのアクセスを許可するアクセス制御ルールの作成ステップを追加します。

ヨーロッパ、中東、またはアフリカ（EMEA）地域のお客様が https://defenseorchestrator.eu/ で Defense Orchestrator に接続している場合、Cloud Connector のパブリック IP アドレスは、次のようになります。

- 35.157.12.126
- 35.157.12.15

アメリカ合衆国のお客様が https://defenseorchestrator.com/ で Defense Orchestrator に接続する場合、クラウドコネクタのパブリック IP アドレスは、次のようになります。

- 52.34.234.2
- 52.36.70.147

アジア - 太平洋 - 日本 - 中国（APJC）地域のお客様が https://www.apj.cdo.cisco.com/ で Defense Orchestrator に接続する場合は、次の IP アドレスからのインバウンドアクセスを許可します。

- 54.199.195.111
- 52.199.243.0

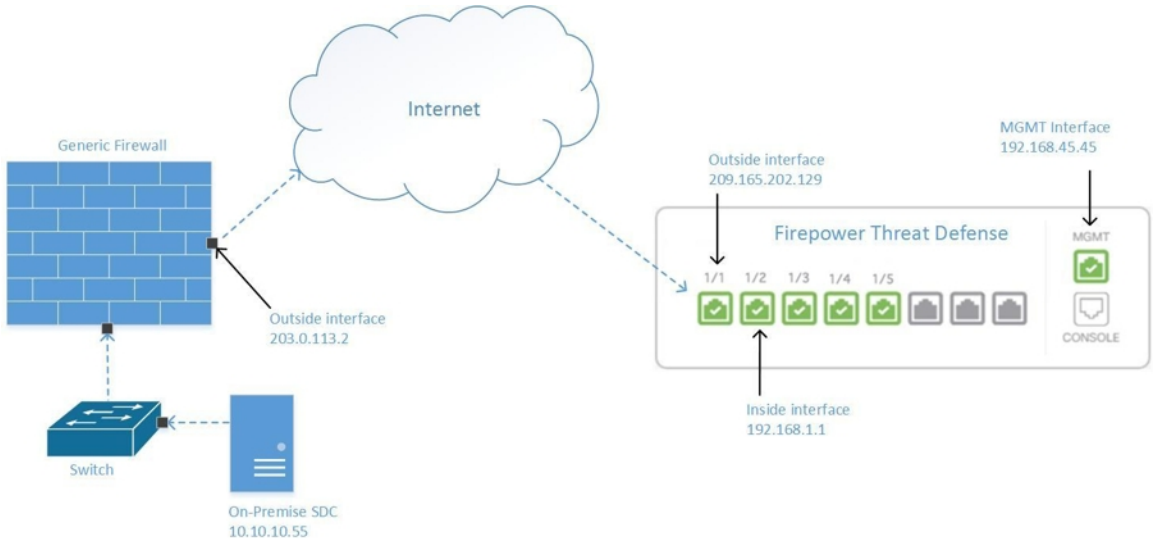
FTD の導入準備

CDO で FTD デバイスの導入準備をする際、登録トークンを使用した導入準備の方法をお勧めします。Cloud Connector から FTD への管理アクセスを許可するように内部インターフェイスを設定した後に、ユーザー名とパスワードを使用して FTD デバイスの導入準備をします。 詳細については、「FTD のオンボーディング」を参照してください。内部インターフェイスの IP アドレスを使用して接続します。上記シナリオでは、そのアドレスは 192.168.1.1 です。

外部インターフェイスから FTD を管理する

分散拠点に 1 つのパブリック IP アドレスが割り当てられていて、CDO が別の場所にある Secure Device Connector（SDC）または Cloud Connector を使用して管理されている場合は、外部インターフェイスから Firepower Threat Defense（FTD）デバイスを管理することを推奨します。

図 *2:* 外部インターフェイスでの *FTD* の管理



この設定により、MGMT 物理インターフェイスがデバイスの管理インターフェイスでなくなるわけではありません。FTD の設置場所にいる場合は、MGMT インターフェイスのアドレスに接続して、FTD を直接管理できます。

リモートアクセス VPN の要件

CDO を使用して管理する FTD で、リモートアクセス VPN（RA VPN）接続を管理する場合、CDO は外部インターフェイスを使用して FTD デバイスを管理できません。代わりに、「内部インターフェイスからの FTD デバイスの管理」を参照してください。

次に行う作業：

FTD を設定する手順については、FTD の外部インターフェイスの管理 に進んでください。

FTD の外部インターフェイスの管理

設定方法は次のとおりです。

1. FTD が CDO にオンボードされていないことが前提です。
2. データインターフェイスを外部インターフェイスとして設定します。
3. 外部インターフェイスで管理アクセスを設定します。
4. SDC または Cloud Connector のパブリック IP アドレス（ファイアウォールによる NAT 処理済み）が外部インターフェイスに到達できるようにします。

始める前に

この設定の前提条件を以下で確認してください。

- FTD の外部インターフェイスの管理

- Cisco Defense Orchestrator の管理対象デバイスへの接続

手順

ステップ 1 FDM にログインします。

ステップ 2 [システム設定（System Settings）] メニューで、[管理アクセス（Management Access）] をクリックします。

ステップ 3 [データインターフェース（Data Interfaces）] タブをクリックし、[データインターフェースの作成（Create Data Interface）] を選択します。

1. [インターフェイス（Interface）] フィールドで、インターフェイスのリストから「**outside**」という名前のインターフェイスを選択します。
2. [プロトコル（pre-named）] フィールドがまだ選択されていない場合は、[HTTPS] を選択します。CDO に必要なのは HTTPS アクセスのみです。
3. [許可ネットワーク（Allowed Networks）] フィールドで、ファイアウォールによる NAT 処理済みの SDC または Cloud Connector のパブリック方向 IP アドレスを含むホスト ネットワーク オブジェクトを作成します。

   「外部インターフェイスからの FTD 管理」のネットワーク図では、SDC または Cloud Connector の IP アドレス 10.10.10.55 が 203.0.113.2 に NAT 処理されています。許可ネットワークの場合は、203.0.113.2 という値を使用してホスト ネットワーク オブジェクトを作成します。

ステップ 4 SDC または Cloud Connector のパブリック IP アドレスから FTD の外部インターフェイスへの管理トラフィック（HTTPS）を許可するアクセス コントロール ポリシーを、FDM で作成します。このシナリオでは、送信元アドレスは 203.0.113.2 で、送信元プロトコルは HTTPS です。また、宛先アドレスは 209.165.202.129 で、宛先プロトコルは HTTPS です。

ステップ 5 **変更を展開します**。これで、外部インターフェイスを使用してデバイスを管理できるようになります。

次のタスク

Cloud Connector を使用している場合

プロセスは非常によく似ていますが、次の 2 つの点が異なります。

- 上記の手順のステップ 3c の [許可ネットワーク（Allowed Network）] は、Cloud Connector のパブリック IP アドレスを含むネットワーク グループ オブジェクトになります。
  - **ヨーロッパ、中東、またはアフリカ（EMEA）地域**のお客様が https://defenseorchestrator.eu/ で Defense Orchestrator に接続している場合、Cloud Connector のパブリック IP アドレスは、次のようになります。
    - 35.157.12.126

- 35.157.12.15

- **アメリカ合衆国**のお客様が https://defenseorchestrator.com/ で CDO に接続している場合、Cloud Connector のパブリック IP アドレスは、次のようになります。
  - 52.34.234.2
  - 52.36.70.147

- **アジア - 太平洋 - 日本 - 中国（APJC）**地域のお客様が https://www.apj.cdo.cisco.com/ で Defense Orchestrator に接続する場合は、次の IP アドレスからのインバウンドアクセスを許可します。
  - 54.199.195.111
  - 52.199.243.0

- 上記の手順のステップ 4 では、Cloud Connector のパブリック IP アドレスから外部インターフェイスへのアクセスを許可するアクセス制御ルールを作成します。

FTD デバイスを CDO にオンボーディングする際は、「登録キーを使用したソフトウェアバージョン 6.6+ を実行する FTD のオンボード」の方法を推奨します。Cloud Connector からの管理アクセスを許可するように外部インターフェイスを設定した後に、FTD デバイスをオンボードします。外部インターフェイスの IP アドレスを使用して接続します。このシナリオでは、そのアドレスは 209.165.202.129 です。

ユーザー名、パスワード、IP アドレスを使用した FTD のオンボーディング

この手順を使用して、デバイスのログイン情報とデバイスの管理 IP アドレスのみを用いた Firepower Threat Defense（FTD）デバイスのオンボーディングを行います。これは、FTD デバイスのオンボーディングを実行する最も簡単な方法です。ただし、CDO への FTD のオンボーディングに推奨される方法は、登録キーを使用したソフトウェアバージョン 6.6+ を実行する FTD のオンボードを使用することです。

始める前に

👉

重要 CDO に FTD デバイスをオンボーディングする前に、『FTD のオンボーディング』と「Cisco Defense Orchestrator の管理対象デバイスへの接続」を確認してください。これらの資料には、デバイスのオンボーディングに必要な一般的なデバイス要件とオンボーディングの前提条件が示されています。

- ログイン情報方式を使用して FTD をオンボーディングするには、次の情報が必要です。
  - CDO が FTD への接続に使用するデバイスログイン情報。

- デバイスの管理に使用しているインターフェイスの IP アドレス。このインターフェイスは、ネットワークの設定方法に応じて、管理インターフェイス、内部インターフェイス、または外部インターフェイスになります。
- FTD を CDO にオンボーディングするには、Firepower Device Manager（FDM）で管理し、ローカル管理用に設定する必要があります。Firepower Management Center（FMC）では管理できません。

（注） FTD がソフトウェアバージョン 6.4 を実行しており、https://www.defenseorchestrator.eu に接続する場合は、この方法を使用する必要があります。ソフトウェア バージョン 6.5 以降を実行している FTD デバイスのみをオンボードできます。

手順

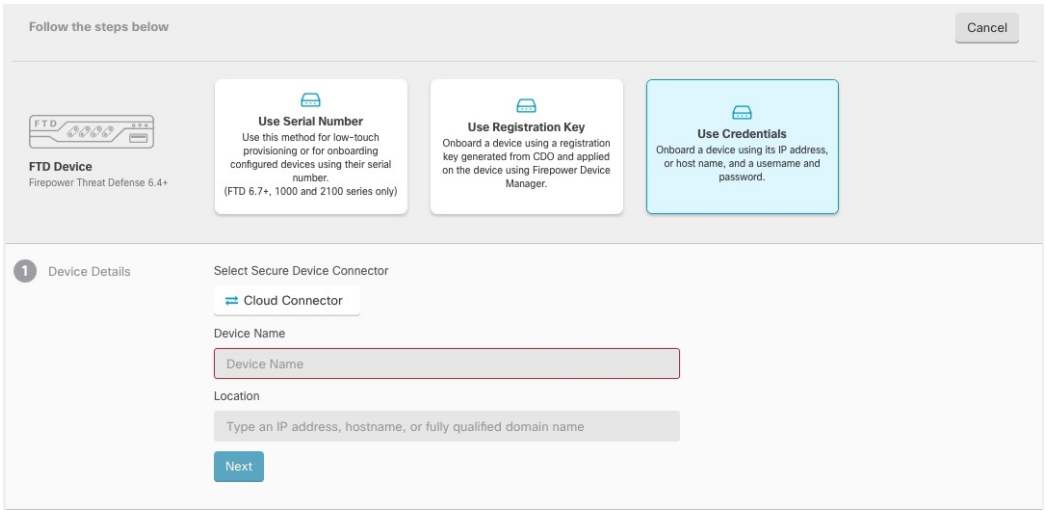
ステップ 1 CDO にログインします。

ステップ 2 ナビゲーションウィンドウで、[インベントリ（Inventory）] をクリックし、青いプラスボタン  をクリックして、デバイスの**オンボーディング**を行います。

ステップ 3 [FTD] をクリックします。

重要 FTD をオンボーディングしようとすると、CDO では、Firepower Threat Defense エンドユーザーライセンス契約（EULA）に目を通して同意するように求められます。これはテナントでの 1 回限りのアクティビティです。EULA に同意すると、EULA が変更されない限り、CDO が同意を求めるプロンプトを再度表示することはありません。

ステップ 4 [FTDデバイスのオンボーディング（Onboard FTD Device）] 画面で、[ログイン番号の使用（Use Credentials）] をクリックします。



ステップ 5 [デバイスの詳細（Device Details）] ステップで、以下の手順を実行します。

- [Secure Device Connector] ボタンをクリックし、ネットワークにインストールされている Secure Device Connector（SDC）を選択します。SDC を使用しない場合、CDO は Cloud Connector を使用して FTD に接続できます。どちらを選択するかは、CDO を管理対象デバイスに接続する方法によって異なります。
- [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）] フィールドに、デバイスの管理に使用しているインターフェイスの IP アドレス、ホスト名、または FTD の完全修飾ドメイン名を入力します。デフォルトのポートは 443 です。

重要 SecureX または Cisco Threat Response（CTR）アカウントをすでにお持ちの場合、デバイスを SecureX に登録するには、CDO アカウントと SecureX/CTR アカウントをマージする必要があります。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「CDO アカウントと SecureX アカウントのマージ」を参照してください。アカウントがマージされるまで、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。

ステップ 6 [データベースの更新（Database Updates）] 領域では、[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 perform security updates, and enable recurring updates）] がデフォルトで有効になっています。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『セキュリティデータベース更新のスケジュール設定』を参照してください。

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。

[次へ（Next）] をクリックします。

ステップ 7 デバイス管理者のユーザー名とパスワードを入力し、[次へ（Next）] をクリックします。

ステップ 8 デバイスの FDM に保留中の変更がある場合は通知され、変更を元に戻すか、FDM にログインして保留中の変更を展開することができます。FDM に保留中の変更がない場合、プロンプトは表示されません。

ステップ 9 （オプション）ログイン情報が確認されると、デバイスにラベルを付けるように求められます。詳細については、『Labels and Label Groups』を参照してください。

ステップ 10 [インベントリに移動（Go to Inventory）] をクリックします。

ステップ 11 デバイスのオンボーディングが完了すると、CDO はデバイスを [インベントリ（Inventory）] ページに [同期（Synced）] ステータスで表示します。

次のタスク

FTD HA ペアをオンボーディングする場合は、ピアデバイスも CDO にオンボーディングする必要があります。詳細については、「ユーザー名、パスワード、IP アドレスを使用した FTD HA ペアの導入準備 （42 ページ）」のステップ 2 を参照してください。

登録キーを使用したソフトウェアバージョン6.4または6.5を実行するFTDの導入準備

この手順では、登録キーを使用して Firepower Threat Defense（FTD）デバイスをオンボーディングする方法について説明します。この方法はFTDデバイスをCDOにオンボーディングするための推奨される方法であり、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に適しています。その IP アドレスが何らかの理由で変更されても、FTD は CDO に接続されたままになります。さらに、FTDはローカルエリアネットワーク上のアドレスを持つことができ、外部ネットワークにアクセスできる限り、この方法でCDOにオンボーディングできます。

警告 SecureX または Cisco Threat Response（CTR）アカウントをすでにお持ちの場合、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。アカウントがマージされるまで、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、アカウントをマージすることを**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。

オンボーディング前

- FTD リリース 6.4 を実行しているお客様の場合、このオンボーディング方法はUS リージョン（defenseorchestrator.com）でのみサポートされます。
- FTD リリース 6.4 を実行し、EU リージョン（defenseorchestrator.eu）に接続しているお客様の場合、ユーザー名、パスワード、IP アドレスを使用した FTD のオンボーディングを使用してデバイスをオンボードする必要があります。
- FTD リリース 6.5 以降を実行しており、US、EU、または APJC リージョン（apj.cdo.cisco.com）リージョンのいずれかに接続しているお客様は、このオンボーディング方法を使用できます。
- CDO を FTD に接続するために必要なネットワーク要件を Cisco Defense Orchestrator の管理対象デバイスへの接続 で確認します。
- デバイスが、Firepower Management Center（FMC）ではなく、Firepower Device Manager（FDM）によって管理されていることを確認してください。
- FTD ソフトウェアバージョン 6.4 および 6.5 を実行しているデバイスは、登録キーを使用してデバイスをオンボーディングしてから、デバイスを Cisco Smart Software Manager に登録する必要があります。それらの FTD を CDO にオンボーディングする前に、FTD のスマートライセンスを登録解除する必要があります。下の「スマートライセンス取得済みの FTD を登録解除する」を参照してください。
- デバイスが 90 日間の評価ライセンスを使用している可能性があります。
- FTD の FDM にログインし、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。

- 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。

次の作業

次の 2 つの操作のいずれかを実行します。

- FTD にすでにスマートライセンスが適用されている場合は、Cisco Smart Software Manager から FTD の登録を解除します。**登録キーを使用してデバイスを CDO にオンボードする前に、Smart Software Manager からデバイスの登録を解除する必要があります。**スマートライセンス取得済みの FTD を登録解除する （14 ページ）に進みます。
- デバイスにスマートライセンスが適用されていない場合は、登録キーを使用したソフトウェアバージョン 6.4 または 6.5 を実行する FTD の導入準備手順 （15 ページ）に進みます。

スマートライセンス取得済みの FTD を登録解除する

オンボードするデバイスが FTD ソフトウェアバージョン 6.4 または 6.5 を実行しており、すでにスマートライセンスが付与されている場合、デバイスは Cisco Smart Software Manager に登録されている可能性があります。**登録キーを使用してデバイスを CDO にオンボードする前に、Smart Software Manager からデバイスの登録を解除する必要があります。**登録を解除すると、仮想アカウントでデバイスに関連付けられている基本ライセンスとすべてのオプションライセンスが解放されます。

デバイスの登録を解除すると、デバイスの現在の設定とポリシーはそのまま機能しますが、変更を加えたり展開したりすることはできません。

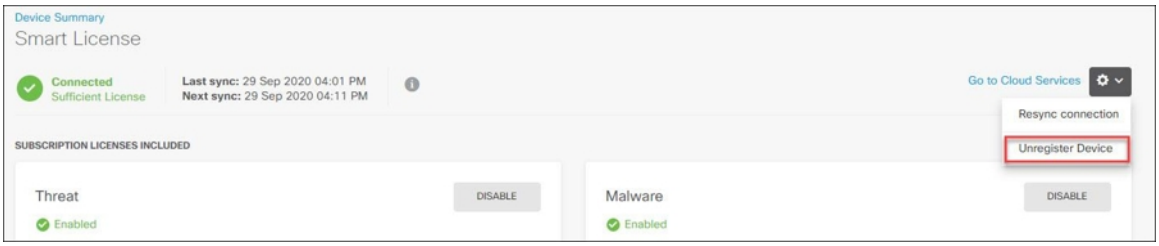
手順

ステップ 1 FDM を使用して FTD にログオンします。

ステップ 2 [FDM] メニューのデバイスアイコンをクリックします。

ステップ 3 [スマートライセンス（Smart License）] 領域で、 [設定の表示（View Configuration）] をクリックします。

ステップ 4 [クラウドサービスに移動（Go to Cloud Services）] 歯車メニューをクリックして、[デバイスの登録解除（Unregister Device）] を選択します。



ステップ 5 警告を確認し、[登録解除（Unregister）] をクリックしてデバイスの登録を解除します。

次のタスク

CDO にオンボーディングするためにデバイスの登録を解除した場合は、登録キーを使用したソフトウェアバージョン 6.4 または 6.5 を実行する FTD の導入準備手順 （15 ページ）に進みます。

登録キーを使用したソフトウェアバージョン 6.4 または 6.5 を実行する FTD の導入準備手順

登録キーを使用して FTD をオンボードするには、次の手順に従います。

始める前に

「登録キーを使用したソフトウェアバージョン 6.4 または 6.5 を実行する FTD の導入準備 （13 ページ）」に記載されている前提条件を確認します。

手順

ステップ 1 CDO にログインします。

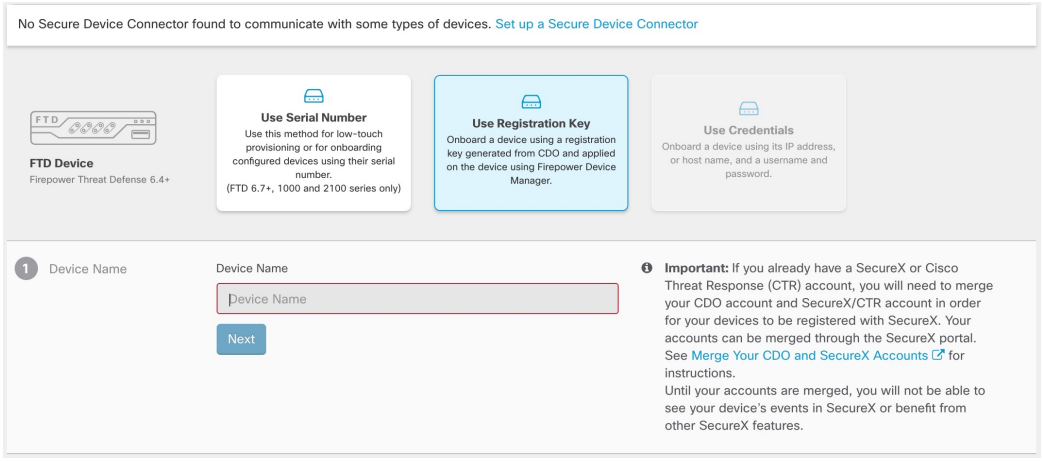
ステップ 2 ナビゲーションウィンドウで、[インベントリ（Inventory）] をクリックし、青いプラスボタン  をクリックして、デバイスの**オンボーディング**を行います。

ステップ 3 [FTD] をクリックします。

重要 FTD デバイスを導入準備しようとすると、CDO では、Firepower Threat Defense エンドユーザーライセンス契約書（EULA）に目を通して同意するように求められます。これはテナントで 1 回限りのアクティビティです。この契約に同意すると、以降の FTD 導入準備で CDO から再度プロンプトが表示されることはありません。EULA 契約に将来変更が生じた場合はプロンプトが表示され、再度同意する必要があります。

ステップ 4 [FTD デバイスのオンボード（Onboard FTD Device）] 画面で、[登録キーの使用（Use Registration Key）] をクリックします。

ステップ 5 [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。



ステップ 6 [データベースの更新（Database Updates）] 領域では、[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（Enable Immediately security updates、and enable recurring updates）] がデフォルトで有効になっています。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『セキュリティデータベース更新のスケジュール設定』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 7 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 [インベントリ（Inventory）] 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。page.デバイスのプレースホルダを選択すると、右側にある操作ウィンドウに、そのデバイスのキーが表示されます。

ステップ 8 [コピー（Copy）] アイコン をクリックして登録キーをコピーします。

（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。

[インベントリ（Inventory）] ページで、 デバイスの接続状態が「プロビジョニング解除（Unprovisioned）」になっていることを確認できます。[Firepower Defense Manager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 9 CDO にオンボーディングする FTD の FDM にログインします。

ステップ 10 [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。

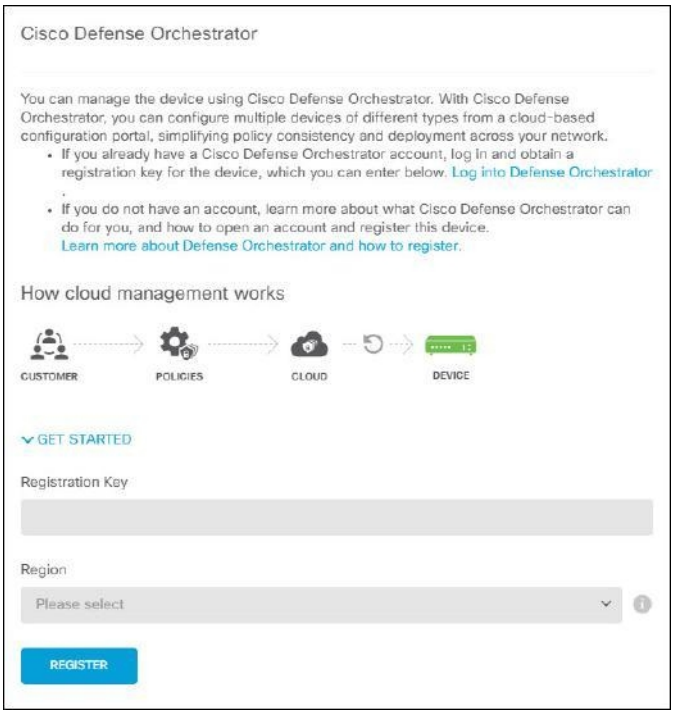
ステップ 11 [Cisco Defense Orchestrator] タイトルで、[始める（Get Started）] をクリックします。

ステップ 12 [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。

（注） この手順は、ソフトウェアバージョン 6.4 を実行している FTD デバイスには適用されません。

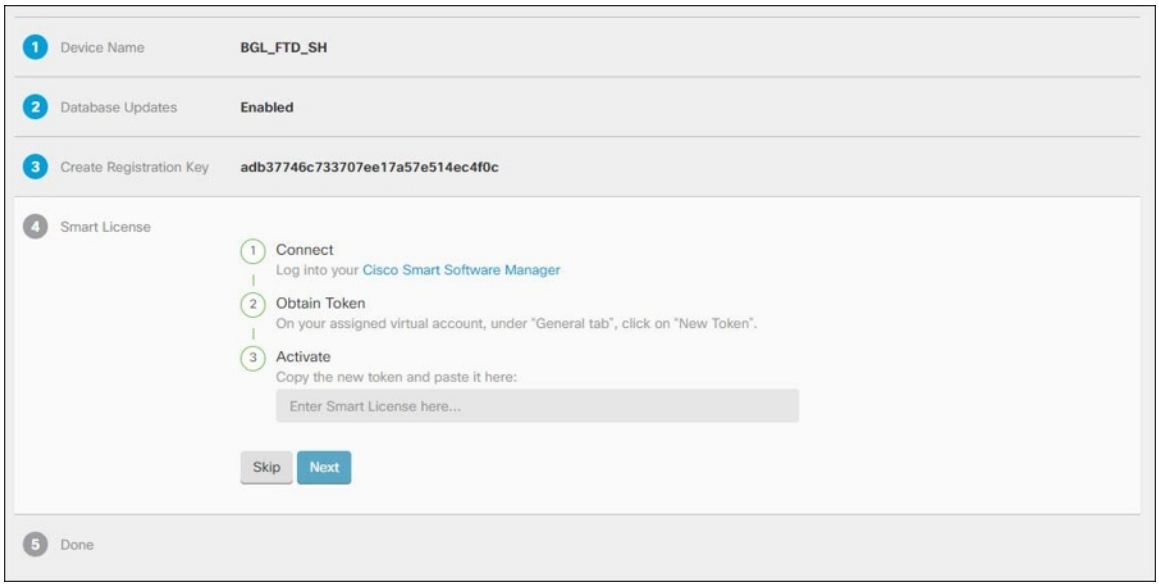
ステップ 13 [登録キー（Registration Key）] フィールドに、CDO で生成した登録キーを貼り付けます。



ステップ 14 [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。

ステップ 15 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、「スマートライセンスの適用または更新」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オンボーディングを続行することもできます。



ステップ 16 CDOに戻り、[インベントリ（Inventory）]ページを開き、デバイスのステータスが[プロビジョニング解除（Unprovisioned）] から [検索中（Locating）]、[同期中（Syncing）]、[同期済み（Synced）] に変わっていくことを確認します。

登録キーを使用したソフトウェアバージョン 6.6+ を実行する FTD のオンボード

この手順では、登録キーを使用して Firepower Threat Defense（FTD）のバージョン 6.6 以降のデバイスをオンボーディングする方法について説明します。この方法は FTD デバイスを CDO にオンボーディングするための推奨される方法であり、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に適しています。そのIPアドレスが何らかの理由で変更されても、FTD は CDO に接続されたままになります。さらに、FTD はローカルエリアネットワーク上のアドレスを持つことができ、外部ネットワークにアクセスできる限り、この方法で CDO にオンボーディングできます。

警告 SecureX または Cisco Threat Response（CTR）アカウントをすでにお持ちの場合、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。アカウントがマージされるまで、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、アカウントをマージすることを**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。

ソフトウェアバージョン 6.4 または 6.5 を実行している FTD をオンボーディングする場合は、『登録キーを使用したソフトウェアバージョン 6.4 または 6.5 を実行する FTD の導入準備』を参照してください。

オンボーディング前

- このオンボーディング方法は、現在、FTD 6.6 リリースで、defenseorchestrator.com、defenseorchestrator.eu、apj.cdo.cisco.com に接続しているお客様が利用できます。
- CDO を FTD に接続するために必要なネットワーク要件を Cisco Defense Orchestrator の管理対象デバイスへの接続 で**確認**します。
- デバイスが、Firepower Management Center（FMC）ではなく、Firepower Device Manager（FDM）によって管理されていることを確認してください。
- デバイスで 90 日間の評価ライセンスを使用することも、スマートライセンスを使用することもできます。FTD ソフトウェアバージョン 6.6 以降を実行しているデバイスは、インストールされているスマートライセンスを登録解除することなく、登録キーを使用して CDO にオンボーディングできます。
- デバイスはまだ Cisco Cloud サービスに登録することはできません。オンボーディングの前に、以下の「Cisco Cloud サービスからの FTD の登録解除」を参照してください。
- FTD の FDM UI にログインし、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。
- 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。

次に行う作業：

次のいずれかの操作を実行します。

- FTD 6.6+ デバイスがすでに Cisco Cloud サービスに登録されている場合は、デバイスをオンボーディングする前に登録を解除する必要があります。Cisco Cloud サービスから FTD を登録解除する （19 ページ）に進みます。
- デバイスが Cisco Cloud サービスに登録されていない場合は、登録キーを使用してソフトウェアバージョン 6.6+ を実行している FTD をオンボードする手順 （20 ページ）に進みます。

Cisco Cloud サービスから FTD を登録解除する

次に、Cisco Cloud サービスからデバイスを登録解除するための最新の手順を示します。登録キーを使用して CDO に FTD デバイスをオンボーディングする前に、この方法を使用します。

（注） バージョン 7.0 以降を実行している FTDv をオンボードする場合、FTDv を CDO に登録すると、パフォーマンス階層型のスマートライセンスの選択が、デフォルトの階層である [可変（Variable）] に自動的にリセットされます。オンボーディング後に、FDM UI を使用して、デバイスに関連付けられたライセンスに一致する層を手動で再選択する**必要があります**。

そのデバイスが Cisco Cloud サービスに登録されていないことを確認するには、次の手順を実行します。

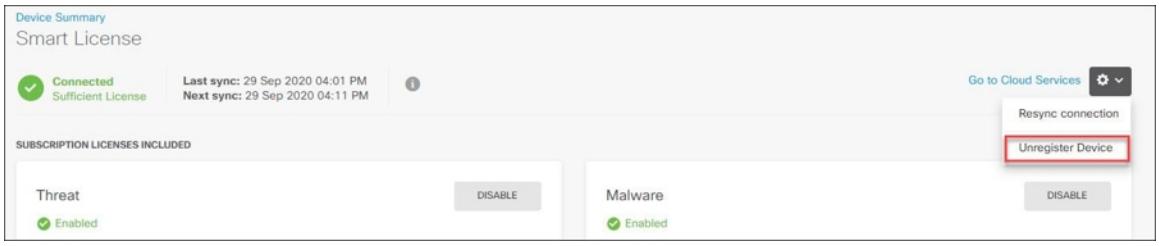
手順

ステップ 1 FDM を使用して FTD にログオンします。

ステップ 2 [FDM] メニューのデバイスアイコンをクリックします。

ステップ 3 [システム設定（System Settings）] メニューを展開し、[クラウドサービス（Cloud Services）] をクリックします。

ステップ 4 [クラウドサービス（Cloud Services）] ページで、歯車メニューをクリックし、[クラウドサービスの登録解除（Unregister Cloud Services）] を選択します。



ステップ 5 警告を確認し、[登録解除（Unregister）] をクリックしてデバイスの登録を解除します。

次のタスク

ソフトウェア 6.6 以降を実行している Firepower Threat Defense デバイスのオンボードを試みている場合は、登録キーを使用してソフトウェアバージョン 6.6+ を実行している FTD をオンボードする手順 （20 ページ）に進みます。

登録キーを使用してソフトウェアバージョン 6.6+ を実行している FTD をオンボードする手順

登録キーを使用して FTD をオンボードするには、次の手順に従います。

手順

ステップ 1 CDO にログインします。

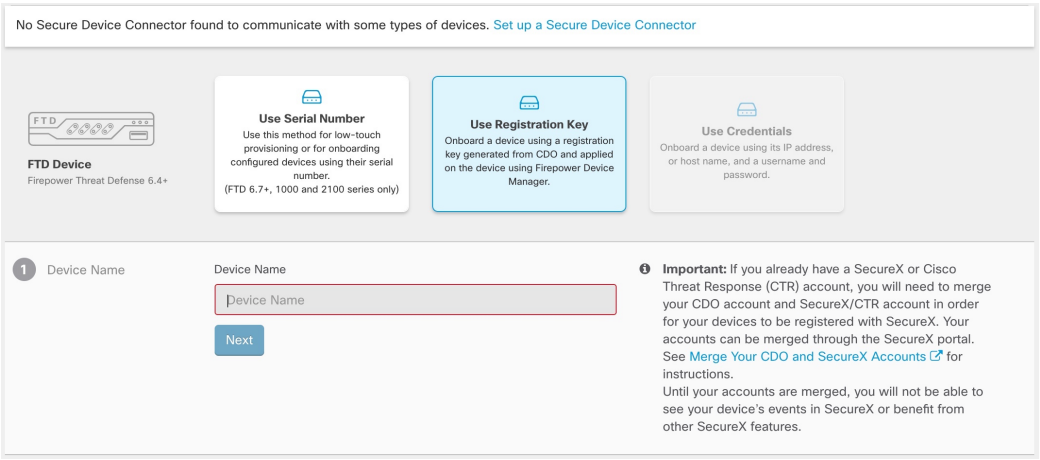
ステップ 2 ナビゲーションウィンドウで、[インベントリ（Inventory）] をクリックし、青いプラスボタン  をクリックして、デバイスの**オンボーディング**を行います。

ステップ 3 [FTD] をクリックします。

重要 FTD デバイスを導入準備しようとすると、CDO では、Firepower Threat Defense エンドユーザーライセンス契約書（EULA）に目を通して同意するように求められます。これはテナントで 1 回限りのアクティビティです。この契約に同意すると、以降の FTD 導入準備で CDO から再度プロンプトが表示されることはありません。EULA 契約に将来変更が生じた場合はプロンプトが表示され、再度同意する必要があります。

ステップ 4 [FTD デバイスのオンボード（Onboard FTD Device）] 画面で、[登録キーの使用（Use Registration Key）] をクリックします。

ステップ 5 [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。



ステップ 6 [データベースの更新（Database Updates）] 領域では、[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 perform security updates, and enable recurring updates）] がデフォルトで有効になっています。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『セキュリティデータベース更新のスケジュール設定』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 Firepower Device Manager 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 7 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 [インベントリ（Inventory）] 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。 page. デバイスのプレースホルダを選択すると、そのページにそのデバイスのキーが表示されます。

ステップ 8 [コピー（Copy）] アイコン をクリックして登録キーをコピーします。

（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。

[インベントリ（Inventory）] ページで、 デバイスの接続状態が「プロビジョニング解除（Unprovisioned）」になっていることを確認できます。[Firepower Defense Manager 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 9 オンボーディング中の FTD の FDM にログインします。

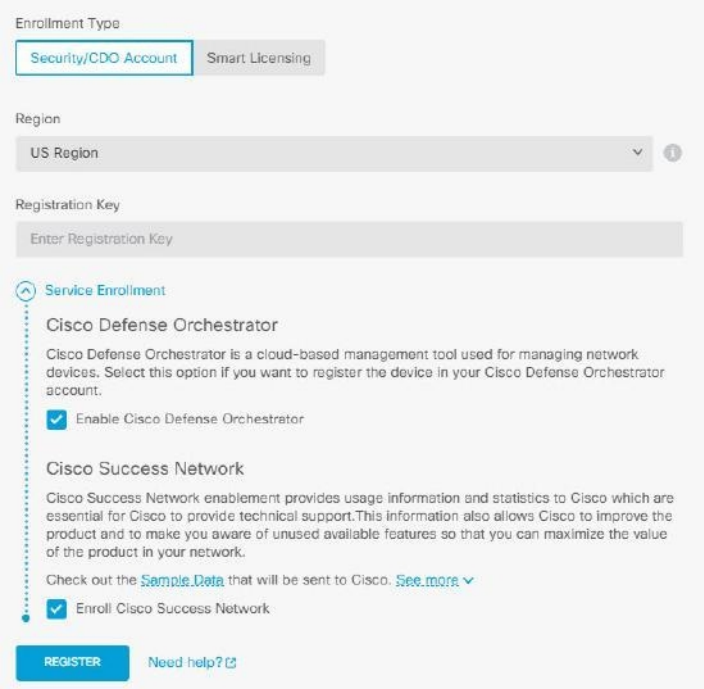
ステップ 10 [システム設定（System Settings）] で、[クラウドサービス（Cloud Services）] をクリックします。

ステップ 11 [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。

ステップ 12 [登録タイプ（Enrollment Type）] 領域で、[セキュリティ/アカウント（Security/Account）] をクリックします。

（注） バージョン 6.6 を実行しているデバイスの場合、CDO の [テナンシー（Tenancy）] タブのタイトルは [セキュリティ アカウント] であり、FDM ダッシュボードで CDO を手動で有効にする必要があることに注意してください。



ステップ 13 [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。

ステップ 14 [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。

ステップ 15 Cisco Success Network Enrollment の登録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）] チェックボックスをオフにします。

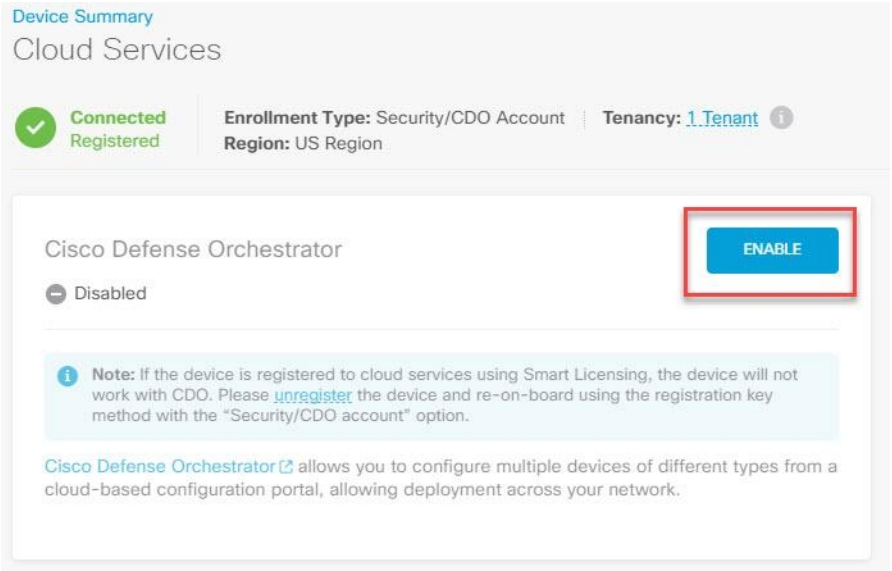
ステップ 16 [登録（Register）] をクリックし、[シスコの開示情報を受け入れる（Accept the Cisco Disclosure）] をクリックします。FDM が CDO に登録要求を送信します。

ステップ 17 CDO に戻り、[登録キーの作成（Create Registration Key）] 領域で [次へ（Next）] をクリックします。

ステップ 18 [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 デバイスに適用して [次へ（Next）] をクリックするか、[スキップ（Skip）] をクリックして、90 日間の評価ライセンスでオンボーディングを続行するか、デバイスがすでにスマートライセンスを取得している場合は、続行できます。詳細については、「スマートライセンスの適用または更新」を参照してください。

詳細については、「スマートライセンスの適用または更新」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オンボーディングを続行することもできます。

（注） デバイスがバージョン6.6を実行している場合は、CDOへの通信を手動で有効にする必要があります。デバイスのFDM UIから、[システム設定] クラウドサービスに移動し、vタイルで [有効化] をクリックします。 >



ステップ 19 CDOに戻り、[インベントリ（Inventory）]ページを開き、デバイスのステータスが[プロビジョニング解除（Unprovisioned）] から [検索中（Locating）]、[同期中（Syncing）]、[同期済み（Synced）] に変わっていくことを確認します。

デバイスのシリアル番号を使用した FTD の導入準備

この手順により、Firepower Threat Defense（FTD）デバイスを簡単にセットアップしてCDOにオンボーディングできます。必要なのは、デバイスのシャーシのシリアル番号またはPCAシリアル番号だけです。デバイスのオンボード時に、スマートライセンスを適用するか、90日間の評価ライセンスを使用できます。

ロータッチプロビジョニングを使用したFirepower Threat Defenseデバイスの導入準備ワークフローと前提条件を実行する前に、使用例を読んで概念を理解してください。

重要 FTD をオンボーディングするためのこれらの方法は、Firepower バージョン 6.7 以降がインストールされているデバイスでのみ使用できます。

使用例

- 新しいFTDデバイスのロータッチプロビジョニング：ネットワークに追加され、インターネットを介して到達できる、工場出荷状態の新しい FTD デバイスのオンボーディング。デバイスの初期デバイス セットアップ ウィザードは完了してしない。

- デバイスのシリアル番号を使用した設定済み FTD のオンボード：ネットワークにすでに追加されインターネットから到達可能な、設定済みのFTDデバイス、またはアップグレードされたデバイスのオンボーディング。初期デバイス セットアップ ウィザードは、デバイスで完了している。

関連情報：

- 用語および定義
- シリアル番号を使用した FTD オンボーディングのトラブルシューティング

新しい FTD デバイスのロータッチ プロビジョニング

ロータッチプロビジョニングは、工場出荷状態の新しい FTD 1000、2100、3100 シリーズのデバイスを自動的にプロビジョニングして設定できるようにする機能です。これにより、CDO へのデバイスのオンボーディングに伴う手動タスクの大部分が不要になります。ロータッチプロビジョニング プロセスにより、物理デバイスにログインする必要性が最小限に抑えられます。これは、従業員がネットワークデバイスの操作に慣れていないリモートオフィスやその他の場所を対象としています。

ロータッチプロビジョニングは、さまざまなハードウェアモデルのサポート対象ソフトウェアバージョンで使用できます。

ロータッチプロビジョニングをサポートするファイアウォールモデル番号	サポート対象のファイアウォール ソフトウェア バージョン	FTDソフトウェア パッケージ
Firepower 1000 シリーズ デバイス モデル：1010、1120、1140、1150	6.7 以降	SF-F1K-TD6.7-K9
Firepower 2100 シリーズ デバイス モデル：2110、2120、2130、2140	6.7 以降	SF-F2K-TD6.7-K9
Secure Firewall 3100 シリーズ デバイスモデル：3110、3120、3130、3140	7.1 以降	SF-F3K-TD7.1.0-K9

重要 この方法を使用して、古いソフトウェアバージョン（6.4、6.5、および6.6）で実行されているFTDデバイスをオンボーディングする場合は、アップグレードではなく、そのデバイスでソフトウェアの新規インストール（再イメージ化）を実行する必要があります。

ロータッチプロビジョニング プロセスを使用するには、FTDデバイスをCDOにオンボーディングし、インターネットにアクセスできるネットワークに接続して、デバイスの電源を入れます。

（注） CDO にオンボーディングする前か後にデバイスの電源を入れますが、**最初にデバイスを CDO にオンボーディングしてから、デバイスの電源を入れてブランチネットワークに接続することをお勧めします。**CDO にデバイスをオンボーディングすると、デバイスは Cisco Cloud の CDO テナントに関連付けられます。デバイスの電源をオンにしてネットワークに接続すると、そのデバイスは Cisco Cloud に接続されます。また、テナントにすでに関連付けられているため、CDO によってデバイスの構成が自動的に同期されます。

デバイスを有効化するには、以下の手順を実行します。

手順

ステップ 1 「ロータッチプロビジョニングを使用した Firepower Threat Defense デバイスの導入準備ワークフローと前提条件」で説明されている手順を使用して、CDO でデバイスをオンボーディングします。ここでは、デバイスパスワードが変更されていないため、[デフォルトパスワード変更なし（Default Password Not Changed）] を選択する必要があります。

ステップ 2 FTD がクラウドに接続されると、テナントはオンボーディングプロセスを完了します。デバイスの [接続（Connectivity）] ステータスが [要求中（Claiming）] に変わります。

ステップ 3 ネットワーク ケーブルをイーサネット 1/1 または管理 1/1 インターフェイスに接続します。インターフェイスにインターネットへのルートがあることを確認します。デバイスの電源を入れると、デバイスは DHCP サーバーから IPv4 アドレスを受け取り、Cisco Cloud に接続します。デバイスのデフォルト設定では、DHCP を使用して外部インターフェイスのアドレスを取得します。

デバイスは、Cisco Cloud ですでに要求されているかどうかを自動的に確認します。この場合、デバイスはすでに CDO で要求されているため、CDO のテナントに直接割り当てられ、CDO にオンボーディングされます。

（注） CDO でデバイスをまだ要求していない場合（つまり、要求する前にデバイスの電源をオンにした場合）、デバイスは要求されるまで Cisco Cloud にパークされます。この状態では、デバイスの構成をプッシュしたり、管理ツールでデバイスを管理したりすることはできません。CDO でデバイスを要求すると、初期プロビジョニングが開始され、デバイスが自動的にオンボーディングされます。

デバイスの [接続（Connectivity）] ステータスが [オンライン（Online）] に変更され、[設定（Configuration）] ステータスが [同期済み（Synced）] に変更されます。FTD デバイスが CDO にオンボードされます。

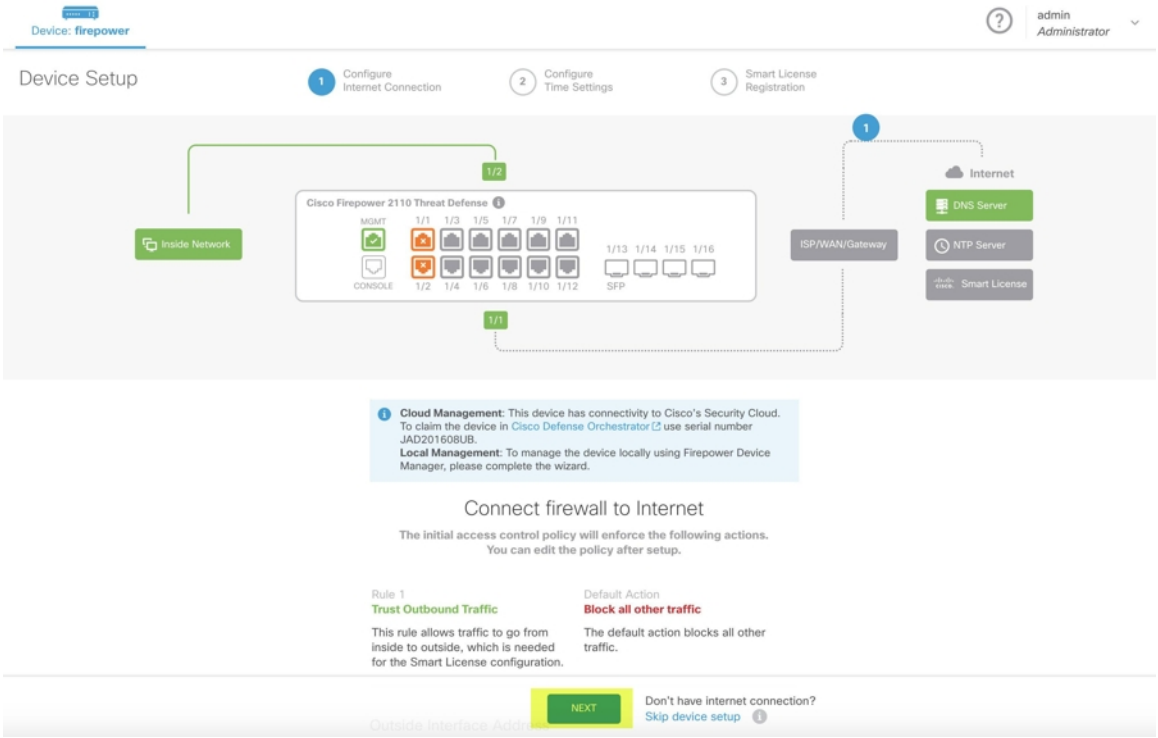
ハードウェアの背面パネルでステータス LED（FTD 1010）、SYS LED（FTD 2100）、または S LED（3100）が緑色に点滅しているのを確認できます。デバイスがクラウドに接続されている場合、デバイスの LED は緑色で点滅し続けます。デバイスが Cisco Cloud に接続できない場合、または接続後に接続が失われた場合、ステータス LED（FTD 1010）、SYS LED（FTD

2100）、または M LED（FTD 3100）が交互に緑色とオレンジ色に点滅しているのを確認できます。

LED インジケータについて理解するには、「ロータッチプロビジョニングを使用した Cisco Firepower ファイアウォールのインストール」のビデオをご覧ください。

重要 これまでに FTD コンソール、SSH、FDM にログインしている場合は、最初のログイン時にデバイスのパスワードを変更しているはずです。それでも、CDO を使用したデバイスのオンボーディングにロータッチ プロビジョニング プロセスを使用できます。FDM にログイン後、デバイスのセットアップウィザードで、外部インターフェイスの設定ステップを完了しないでください。このステップを完了すると、デバイスはクラウドから登録解除され、ロータッチプロビジョニング プロセスを使用できなくなります。

FDM にログインすると、ダッシュボードに次の画面が表示されます。



FDM UI では先に進まず、シリアル番号のオンボーディングウィザードに移動し、デバイスをオンボーディングしてください。ここでは、デバイスパスワードが変更されているため、[デフォルトパスワード変更済み（Default Password Changed）] を選択する必要があります。「ロータッチプロビジョニングを使用した Firepower Threat Defense デバイスの導入準備ワークフローと前提条件」を参照してください。

関連情報：

- デバイスのシリアル番号を使用した設定済み FTD のオンボード

- 用語および定義

デバイスのシリアル番号を使用した設定済み FTD のオンボード

デバイス セットアップ ウィザードは設定済みの FTD デバイスで完了するため、デバイスはクラウドから登録解除され、ロータッチ プロビジョニング プロセスを使用して登録解除されたデバイスを CDO にオンボードすることはできません。

（注） デバイスが Cisco Cloud に接続されていない場合、ステータス LED（FTD 1000 シリーズ）、SYS LED（FTD 2100 シリーズ）、または M LED（3100 シリーズ）が緑色とオレンジ色に交互に点滅しているのを確認できます。

次のタスクを実行するためにデバイス セットアップ ウィザードを完了している可能性があります。

- デバイスが FTD 6.7 以降にアップグレードされている。シリアル番号を使用して FTD を CDO にオンボーディングするには、デバイスに FTD 6.7 がインストールされている必要があります。
- デバイスの管理インターフェイスで静的 IP アドレスを設定します。インターフェイスが必要なダイナミック IP アドレスを取得できない場合、または DHCP サーバーでゲートウェイルートが提供されない場合は、静的 IP アドレスを設定する必要があります。
- PPPoE を使用してアドレスを取得し、外部インターフェイスを設定します。
- FDM または FMC を使用して FTD 6.7 以降のデバイスを管理します。

重要 CDO では、Firepower Management Center（FMC）で管理されている FTD を管理できません。ただし、このデバイスを CDO で引き続き管理する場合は、デバイスをオンボードする前に FTD デバイスをローカル管理に切り替え、後でデバイスをオンボードします。デバイスが実行しているバージョンの Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）[英語] の「System Management」の章にある「Switching Between Local and Remote Management」で説明されている手順を実行します。https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html#anchor854

このようなデバイスをオンボードする場合は、次の手順を実行します。

手順

ステップ 1 「ロータッチプロビジョニングを使用した Firepower Threat Defense デバイスの導入準備ワークフローと前提条件」で説明されている手順を使用して、CDO でデバイスをオンボードします。ここでは、デバイスパスワードが変更されているため、[デフォルトパスワード変更済み（Default Password Changed）] を選択する必要があります。

ステップ 2 FDM UI で、**[システム設定（System Settings）]** > **[クラウドサービス（Cloud Services）]** に移動し、[Cisco Defense Orchestratorからテナントへの自動登録（Auto-enroll with Tenancy from Cisco Defense Orchestrator）] オプションを選択して [登録（Register）] をクリックします。

CDO は、デバイスの [接続（Connectivity）] ステータスを [オンライン（Online）] に変更し、[設定（Configuration）] ステータスを [同期（Synced）] 状態に変更します。FTD デバイスが CDOにオンボーディングされます。ハードウェアの背面パネルでステータスLED（FTD1010）、SYS LED（FTD 2100）、またはM LED が緑色に点滅しているのを確認できます。デバイスが Cisco Cloud に接続されている場合、デバイスの LED は緑色で点滅し続けます。デバイスが Cisco Cloud に接続できない場合、または接続後に接続が失われた場合、同じステータス LED が緑色とオレンジ色に交互に点滅しているのを確認できます。

関連情報：

- ロータッチプロビジョニングを使用した Firepower Threat Defense デバイスの導入準備ワークフローと前提条件
- 用語および定義

ロータッチプロビジョニングを使用した Firepower Threat Defense デバイスの導入準備ワークフローと前提条件

このワークフローは、工場出荷状態の新しい Firepower 1000、Firepower 2100、および Secure Firewall 3100 シリーズデバイスのロータッチプロビジョニングを使用した導入準備に適用されます。

この手順を使用して、外部ベンダーから購入したデバイスをオンボードしたり、別のリージョンにある別のクラウドテナントによってすでに管理されているデバイスをオンボードしたりもできます。ただし、デバイスが外部ベンダーのクラウドテナントまたは別のリージョンのクラウドテナントにすでに登録されている場合、CDO はデバイスをオンボードせず、「デバイスのシリアル番号がすでに要求されている（Device serial number already claimed）」というエラーメッセージを表示します。このような場合、CDO 管理者は、デバイスのシリアル番号を以前のクラウドテナントから登録解除してから、独自のテナントで CDO デバイスを要求する必要があります。トラブルシューティングの章の「デバイスのシリアル番号がすでに要求されている」を参照してください。

前提条件

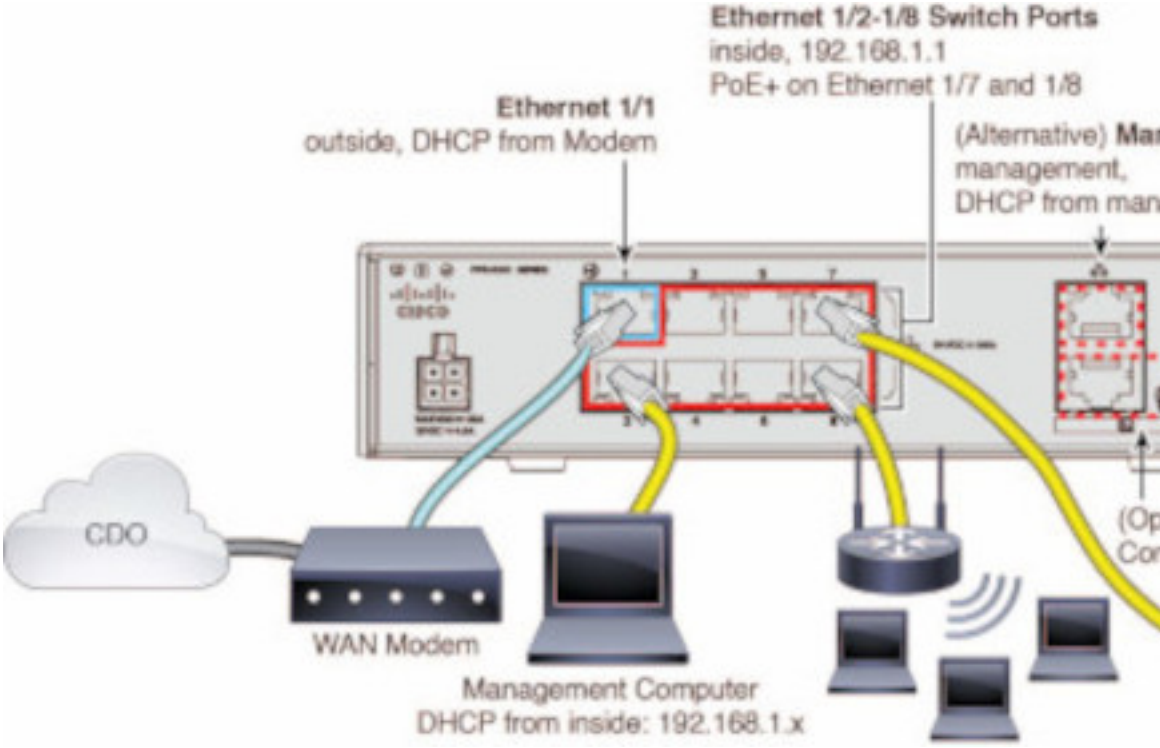
ソフトウェアおよびハードウェアの要件

FTDデバイスは、シリアル番号による導入準備をサポートする脅威防御ソフトウェアを実行している必要があります。

ロータッチプロビジョニングをサポートするファイアウォールモデル番号	サポート対象のファイアウォール ソフトウェア バージョン	FTDソフトウェア パッケージ
Firepower 1000 シリーズ デバイス モデル：1010、1120、1140、1150	6.7 以降	SF-F1K-TD6.7-K9
Firepower 2100 シリーズ デバイス モデル：2110、2120、2130、2140	6.7 以降	SF-F2K-TD6.7-K9
Secure Firewall 3100 シリーズ デバイスモデル：3110、3120、3130、3140	7.1 以降	SF-F3K-TD7.1.0-K9

ハードウェア設置に関する構成の前提条件

- **分散拠点のネットワークは 192.168.1.0/24 アドレス空間を使用できません。**イーサネット 1/1（外部）上のネットワークは、192.168.1.0/24 アドレス空間を使用できません。FTD 6.7 を実行している 1000 および 2100 シリーズ デバイスのイーサネット 1/2 「内部」インターフェイスのデフォルト IP アドレスは 192.168.1.1 であり、WAN モデムがそのサブネット上にある場合、WAN モデムによって割り当てられた DHCP アドレスと競合する可能性があります。
  - **内部**：イーサネット 1/2、IP アドレス 192.168.1.1
  - **外部**：イーサネット 1/1、DHCP からの IP アドレス、またはセットアップ時に指定したアドレス



外部インターフェイスの設定を変更できない場合は、FDM を使用してイーサネット 1/2 の「内部」インターフェイス設定のサブネットを変更し、競合を回避します。たとえば、次のサブネット設定に変更できます。

- IP アドレス：192.168.95.1
- DHCP サーバーの範囲：192.168.95.5 ～ 192.168.95.254

物理インターフェイスの設定手順については、Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）[英語] を参照してください。https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html「Interfaces」の章の「Configure a Physical Interface」を参照してください。

- FTD デバイスがインストールされ、Cisco Cloud に接続されている必要があります。
- デバイスの外部インターフェイスまたは管理インターフェイスは、DHCP アドレッシングを提供するネットワークに接続する必要があります。通常、デバイスには外部インターフェイスまたは管理インターフェイスにデフォルトの DHCP クライアントがあります。

（注） 管理インターフェイスが DHCP サーバーを備えたネットワークに接続されている場合、Linux スタックによって開始されるトラフィックの外部インターフェイスよりも優先されます。

- シリアルオンボーディング方法の次の SSE ドメインにアクセスできるようにするには、外部または管理インターフェイスにアクセスする必要があります。
  - US リージョン
    - api sse.cisco.com
    - est.sco.cisco.com（地理的に共通）
    - mx*.sse.itd.cisco.com（現在は mx01.sse.itd.cisco.com のみ）
    - dex.sse.itd.cisco.com（カスタマーサクセス用）
    - eventing-ingest.sse.itd.cisco.com（CTR および CDO 用）
    - registration.us.sse.itd.cisco.com（地域の Cisco Cloud へのデバイス登録が可能）
  - EU リージョン
    - api.eu.sse.itd.cisco.com
    - est.sco.cisco.com（地理的に共通）
    - mx*.eu.sse.itd.cisco.com（現在は mx01.eu.sse.itd.cisco.com のみ）
    - dex.eu.sse.itd.cisco.com（カスタマーサクセス用）
    - eventing-ingest.eu.sse.itd.cisco.com（CTR および CDO 用）
    - registration.eu.sse.itd.cisco.com（地域の Cisco Cloud へのデバイス登録が可能）
  - APJ リージョン
    - api.apj.sse.itd.cisco.com
    - est.sco.cisco.com（地理的に共通）
    - mx*.apj.sse.itd.cisco.com（現在は mx01.apj.sse.itd.cisco.com のみ）
    - dex.apj.sse.itd.cisco.com（カスタマーサクセス用）
    - eventing-ingest.apj.sse.itd.cisco.com（CTR および CDO 用）
    - http://registration.apj.sse.itd.cisco.com（地域の Cisco Cloud へのデバイス登録が可能）
- デバイスの外部インターフェイスから、Cisco Umbrella DNS に DNS アクセスできる必要があります。

CDO でデバイスを要求する前に

CDO でデバイスを要求する前に、次の情報があることを確認してください。

- FTD デバイスのシャーシのシリアル番号または PCA 番号。この情報は、ハードウェアシャーシの下部、またはデバイスが納品された段ボール箱に記載されています。次の図の例では、FTD 1010 シャーシの下部にシリアル番号「*******X0R9」が表示されています。

- デバイスのデフォルトのパスワード。
- 追加機能を使用するために Cisco Smart Software Manager から生成されたスマートライセンス。ただし、90 日間の評価ライセンスを使用してデバイスのオンボーディングを完了し、後にスマートライセンスを適用できます。

次の作業

ロータッチプロビジョニングに向けた Firepower Threat Defense デバイスのシリアル番号の導入準備 （33 ページ） に進みます。

ロータッチプロビジョニングに向けた Firepower Threat Defense デバイスのシリアル番号の導入準備

注意：CDO で FTD デバイスの導入準備をしている場合は、Firepower Device Manager を使用してデバイスの簡易セットアップを実行しないことをお勧めします。簡易セットアップを実行すると、CDO でプロビジョニングエラーが発生します。

デバイスの電源を入れてブランチネットワークに接続する前に、シリアル番号を使用してデバイスを CDO にオンボーディングすることをお勧めします。

手順

ステップ 1 外部ベンダーから購入したデバイスの導入準備をする場合は、まずデバイスを再イメージ化する必要があります。詳細については、『Cisco FXOS Troubleshooting Guide for the Firepower 1000/21000 with FTD』の「Reimage Procedures」の章を参照してください。

ステップ 2 CDO にログインします。

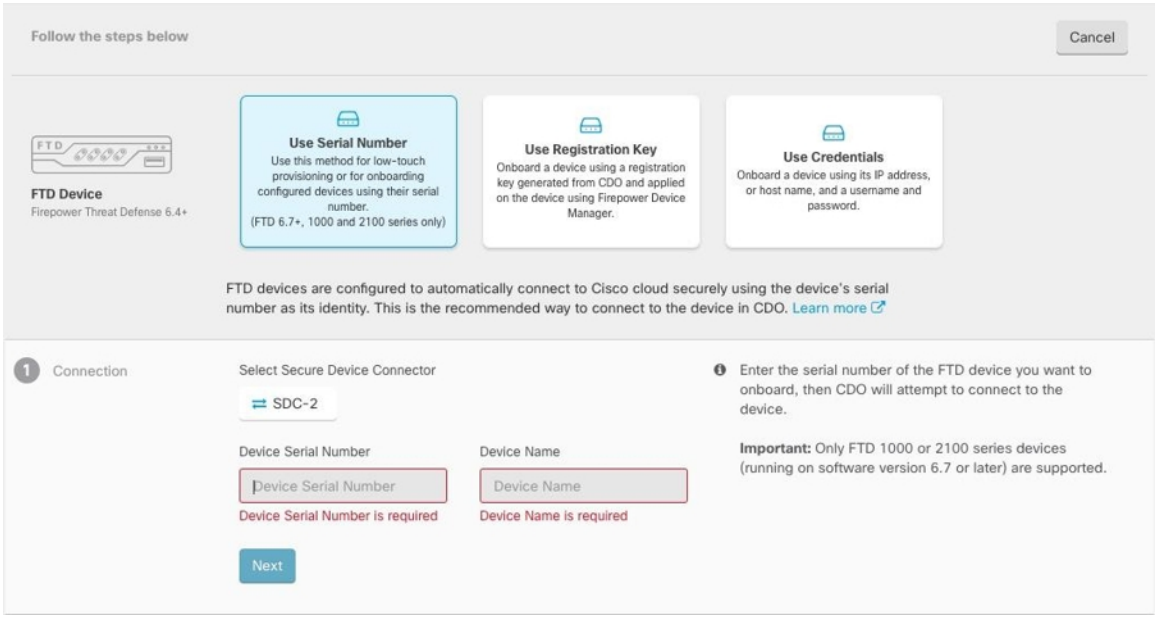
ステップ 3 ナビゲーションウィンドウで、[インベントリ（Inventory）] をクリックし、青いプラスボタン  をクリックして、デバイスの**オンボーディング**を行います。

ステップ 4 FTD をクリックします。

重要 FTD デバイスを導入準備しようとすると、CDO では、Firepower Threat Defense エンドユーザーライセンス契約書（EULA）に目を通して同意するように求められます。これはテナントで 1 回限りのアクティビティです。この契約に同意すると、以降の FTD 導入準備で CDO から再度プロンプトが表示されることはありません。EULA 契約に将来変更が生じた場合はプロンプトが表示され、再度同意する必要があります。

ステップ 5 [FTDデバイスの導入準備（Onboard FTD Device）] 画面で、[シリアル番号の使用（Use Serial Number）] をクリックします。

ステップ 6 [接続（Connection）] ステップで、次の詳細を入力し、[次へ（Next）] をクリックします。



1. このデバイスが通信する Secure Device Connector（SDC）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。
2. [デバイスのシリアル番号（Device Serial Number）]：導入準備するデバイスのシリアル番号または PCA 番号を入力します。
3. [デバイス名（Device Name）]：デバイスの名前を指定します。
4. [パスワードのリセット（Password Reset）] ステップで、次の詳細を入力し、[次へ（Next）] をクリックします。
   - [デフォルトのパスワードが未変更（Default Password Not Changed）]：新しいデバイスのデフォルトパスワードを変更するには、このオプションを選択します。

（注） デバイスのデフォルトパスワードがすでに変更されている場合、このフィールドに入力した内容は無視されます。

- デバイスの新しいパスワードを [新しいパスワード（New Password）] と [パスワードの確認（Confirm Password）] に入力します。新しいパスワードが画面に表示される要件を満たしていることを確認します。

- [デフォルトパスワード変更済み（Default Password Changed）]：FDM または Firepower eXtensible Operating System（FXOS）コンソールでデフォルトパスワードをすでに変更しているデバイスに対してのみ、このオプションを選択します。

5. [スマートライセンス（Smart License）] ステップで、必要なオプションを選択し、[次へ（Next）] をクリックします。

   - [スマートライセンスの適用（Apply Smart License）]：デバイスにまだスマートライセンスが適用されていない場合は、このオプションを選択します。Cisco Smart Software Manager を使用してトークンを生成して、このフィールドにコピーする必要があります。

   - [デバイスにライセンス供与済み（Device Already Licensed）]：デバイスがすでにライセンス供与されている場合は、このオプションを選択します。

     （注） デフォルトパスワードがすでに変更されている場合は、このラジオボタンが自動的に選択されます。ただし、必要に応じて別のオプションを選択できます。

   - [90日間の評価ライセンスの使用（Use 90-day Evaluation License）]：90 日間の評価ライセンスを適用します。

6. [サブスクリプションライセンス（Subscription Licenses）] ステップで、次の操作を実行します。

   重要 [スマートライセンス（Smart License）] ステップで [デバイスにライセンス供与済み（Device Already Licensed）] を選択している場合は、このステップで何らかの選択を行うことはできません。[既存のサブスクリプションの保持（Keep Existing Subscription）] が表示され、[ラベル（Labels）] の手順に進みます。

   - スマートライセンスが適用されている場合は、必要な追加ライセンスを有効にして、[次へ（Next）] をクリックします。

   - 評価ライセンスが有効になっている場合は、RA VPN ライセンスを除く他のすべてのライセンスを使用できます。必要なライセンスを選択し、[次へ（Next）] をクリックして続行します。

     （注） 基本ライセンスのみで続行することもできます。

7. [ラベル（Labels）] ステップで、必要に応じてラベル名を入力できます。[インベントリに移動（Go to Inventory）] をクリックします。

次のタスク

CDO がデバイスの要求を開始すると、右側に [要求中（Claiming）] メッセージが表示されます。CDOは、デバイスがオンラインでクラウドに登録されているかどうかを確認するために、1時間継続的にポーリングします。クラウドに登録されると、CDOは初期プロビジョニングを開始し、デバイスを正常にオンボーディングします。デバイスの LED ステータスが緑色に点滅することで、デバイスが登録されていることを確認できます。デバイスが Cisco Cloud に接続できない場合、または接続後に接続が失われた場合、ステータス LED（FTD 1010）または SYS LED（FTD 2100）が交互に緑色とオレンジ色に点滅します。

最初の 1 時間以内にデバイスがクラウドに登録されない場合、タイムアウトが発生し、CDOは10分ごとに定期的にポーリングしてデバイスのステータスを確認し、[要求中（Claiming）] の状態を維持します。デバイスの電源が入っていてクラウドに接続されている場合、オンボーディングステータスを把握するために10分間待つ必要はありません。いつでも [ステータスの確認（Check Status）] リンクをクリックしてステータスを確認できます。CDO は初期プロビジョニングを開始し、デバイスを正常にオンボーディングします。

重要 デバイス セットアップ ウィザードをすでに完了したと仮定すると（「デバイスのシリアル番号を使用した設定済みFTDのオンボード」を参照）、デバイスはクラウドから登録解除され、この場合、CDO は [要求中（Claiming）] 状態のままになります。FDM を CDO に追加するには、FDM から手動登録を完了する必要があります。（FDM で、[システム設定（System Settings）]>[クラウドサービス（Cloud Services）] に移動し、[Cisco Defense Orchestratorからテナントへの自動登録（Auto-enroll with Tenancy from Cisco Defense Orchestrator）] オプションを選択して [登録（Register）] をクリックします）。次に、[ステータスの確認（Check Status）] をクリックします。

FTD 高可用性ペア

FTD ペアを CDO にオンボーディングするには、ペアの各デバイスを個別にオンボーディングする必要があります。ペアの両方のピアがオンボーディングされると、CDOはそれらを [インベントリ（Inventory）] ページの 1 つのエントリとして自動的に組み合わせます。ログイン情報または登録キーを使用してデバイスをオンボーディングします。**両方**のデバイスを同じ方法でオンボーディングすることをお勧めします。また、先にスタンバイモードのデバイスをオンボーディングすると、CDO はそのデバイスの展開機能または読み取り機能を無効にすることに注意してください。HA ペア内のアクティブなデバイスに対してのみ読み取りまたは展開を実行できます。

（注） CDO は、登録キーを使用して FTD デバイスをオンボーディングすることを強く推奨します。登録キーを使用したオンボーディングは、特定の Firepower ソフトウェアバージョンを実行している FTD デバイスでは若干異なります。詳細については、バージョン 6.4 またはバージョン 6.5 を実行する FTD HA ペアのオンボーディング （37 ページ）とバージョン 6.6 またはバージョン 6.7 以降を実行する FTD HA ペアのオンボーディング （39 ページ）を参照してください。

FTD HA ペアを CDO にオンボードする前に、以下を確認してください。

- HA ペアは、CDO にオンボーディングされる前にすでに形成されている。
- 両方のデバイスは正常な状態である。ペアは、プライマリ/アクティブモードとセカンダリ/スタンバイモード、**または**プライマリ/スタンバイモードとセカンダリ/アクティブモードのいずれかである。異常なデバイスは、CDO に正常に同期されない。
- HA ペアは、Firepower Management Center（FMC）ではなく、Firepower Device Manager（FDM）によって管理されている。
- Cloud Connector が https://www.defenseorchestrator.com で CDO に接続している。

登録キーを使用した FTD HA ペアの導入準備

登録キーを使用して FTD 高可用性（HA）ペアの導入準備を開始する前に、次の前提条件に注意してください。

- FTD バージョン 6.4 を実行するデバイスの登録キーを使用した導入準備は、米国リージョン （defenseorchestrator.com）でのみサポートされています。EU リージョン（defenseorchestrator.eu）に接続するには、ユーザー名、パスワード、および IP アドレスを使用して HA ペアを導入準備する必要があります。
- FTD リリース 6.5 以降を実行しており、US、EU、または APJC リージョンのいずれかに接続しているお客様は、登録キーを使用して導入準備できます。
- FTD ソフトウェアバージョン 6.4 および 6.5 を実行しているデバイスは、登録キーを使用してデバイスをオンボーディングしてから、デバイスを Cisco Smart Software Manager に登録する必要があります。それらの FTD を CDO にオンボーディングする前に、FTD のスマートライセンスを登録解除する必要があります。詳細については、スマートライセンス取得済みの FTD を登録解除する （14 ページ）を参照してください。

バージョン 6.4 またはバージョン 6.5 を実行する FTD HA ペアのオンボーディング

ソフトウェア バージョン 6.4 または 6.5 を実行している FTD HA ペアをオンボーディングするには、一度に 1 つずつデバイスをオンボーディングする必要があります。オンボーディングするデバイスがアクティブであるかスタンバイであるか、プライマリであるかセカンダリであるかは関係ありません。

（注） 登録キーを使用して HA ペアのいずれかのデバイスをオンボーディングする場合、もう一方のピアデバイスのオンボーディングにも同じ方法を使用する必要があります。

バージョン 6.4 または 6.5 を実行している HA ペアをオンボーディングするには、以下の手順に従ってください。

手順

ステップ 1 ピアデバイスをオンボーディングします。ペアのうち最初のデバイスをオンボーディングするには、『登録キーを使用したソフトウェアバージョン 6.4 または 6.5 を実行する FTD の導入準備』を参照してください。

ステップ 2 ナビゲーションウィンドウで、[インベントリ（Inventory）] をクリックします。

ステップ 3 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 4 [FTD] タブをクリックします。デバイスが同期されたら、デバイスを選択してハイライトします。[デバイスの詳細（Devie Details）] のすぐ下にある操作ウィンドウで、[デバイスのオンボーディング（Onboard Device）] をクリックします。

ステップ 5 すでにオンボーディングされているピアデバイスの HA ピアデバイス名を入力します。[次へ（Next）] をクリックします。

ステップ 6 最初のデバイスのスマートライセンスを提示した場合、CDO はそのライセンスを再入力して、このデバイスのオンボーディングに使用できるようにします。[次へ（Next）] をクリックします。

（注） FTD をオンボーディングするためにデバイスのスマートライセンスを登録解除した場合は、ここでスマートライセンスを再適用します。

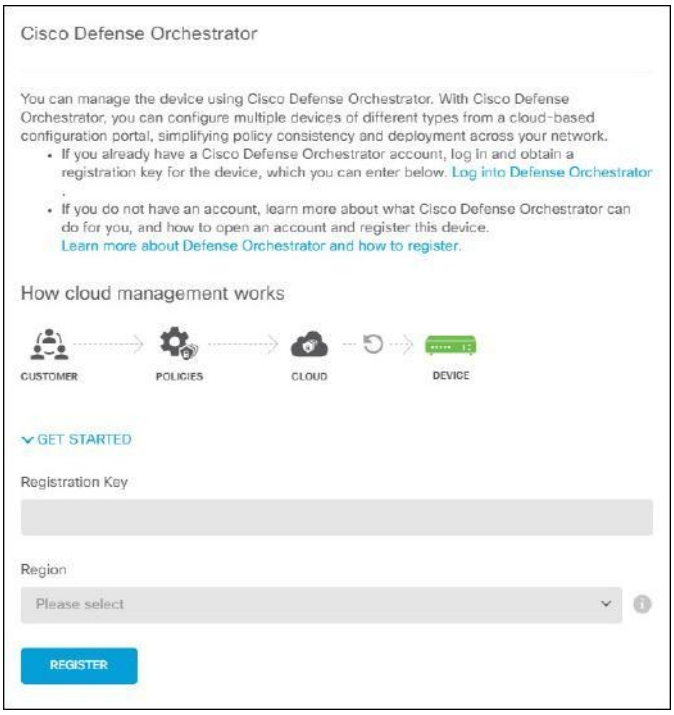
ステップ 7 CDO は、オンボーディングの準備をしているデバイスの登録キーを自動的に生成します。[コピー（**Copy**）] アイコン をクリックして登録キーをコピーします。

ステップ 8 オンボーディング中の FTD の FDM UI にログインします。

ステップ 9 [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。

ステップ 10 [Cisco Defense Orchestrator] タイトルで、[始める（Get Started）] をクリックします。

ステップ 11 [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。



ステップ 12 [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。

（注） この手順は、ソフトウェアバージョン 6.4 を実行している FTD デバイスには適用されません。

ステップ 13 [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。

ステップ 14 CDO に戻り、[登録キーの作成（Create Registration Key）] 領域で [次へ（Next）] をクリックします。

ステップ 15 [インベントリに移動（Go to Inventory）] をクリックします。CDO は自動的にデバイスをオンボーディングし、それらを単一のエントリとして結合します。オンボーディングした最初のピアデバイスと同様に、デバイスのステータスは「プロビジョニング解除（Unprovisioned）」から「取得中（Locating）」、「同期中（Syncing）」、「同期済み（Synced）」に変わります。

バージョン 6.6 またはバージョン 6.7 以降を実行する FTD HA ペアのオンボーディング

バージョン 6.6 または 6.7 を実行している FTD HA ペアをオンボーディングするには、一度に 1 つずつデバイスをオンボーディングする必要があります。オンボーディングするデバイスが

アクティブであるかスタンバイであるか、プライマリであるかセカンダリであるかは関係ありません。

（注） 登録キーを使用して HA ペアのいずれかのデバイスをオンボーディングする場合、もう一方のピアデバイスのオンボーディングにも同じ方法を使用する必要があります。

バージョン 6.6 または 6.7 を実行している HA ペアをオンボーディングするには、以下の手順に従ってください。

手順

ステップ 1 ピアデバイスをオンボーディングします。詳細については、「登録キーを使用したソフトウェアバージョン 6.6+ を実行する FTD のオンボード」を参照してください。

ステップ 2 ナビゲーションウィンドウで、[インベントリ（Inventory）] をクリックします。

ステップ 3 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 4 [FTD] タブをクリックします。デバイスが同期されたら、デバイスを選択してハイライトします。[デバイスの詳細（Devie Details）]のすぐ下にある操作ウィンドウで、[デバイスのオンボーディング（Onboard Device）] をクリックします。

ステップ 5 すでにオンボーディングされているピアデバイスの HA ピアデバイス名を入力します。[次へ（Next）] をクリックします。

ステップ 6 最初のデバイスのスマートライセンスを提示した場合、CDO はそのライセンスを再入力して、このデバイスのオンボーディングに使用できるようにします。[次へ（Next）] をクリックします。

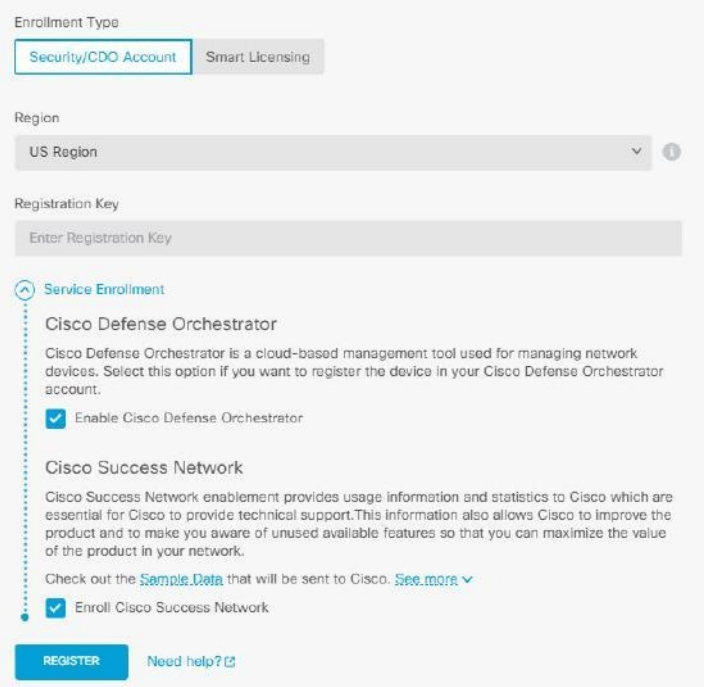
ステップ 7 CDO は、オンボーディングの準備をしているデバイスの登録キーを自動的に生成します。[コピー（Copy）] アイコン をクリックして登録キーをコピーします。

ステップ 8 CDO にオンボーディングする FTD の FDM UI にログインします。

ステップ 9 [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。

ステップ 10 [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。

（注） バージョン 6.6 を実行しているデバイスの場合、CDO の [テナンシー（Tenancy ）] タブのタイトルは [セキュリティアカウント（Security Account）] であり、FDM UI で CDO を手動で有効にする必要があることに注意してください。



ステップ 11 [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。

ステップ 12 [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。

ステップ 13 [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。

ステップ 14 Cisco Success Network Enrollment の登録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）] チェックボックスをオフにします。

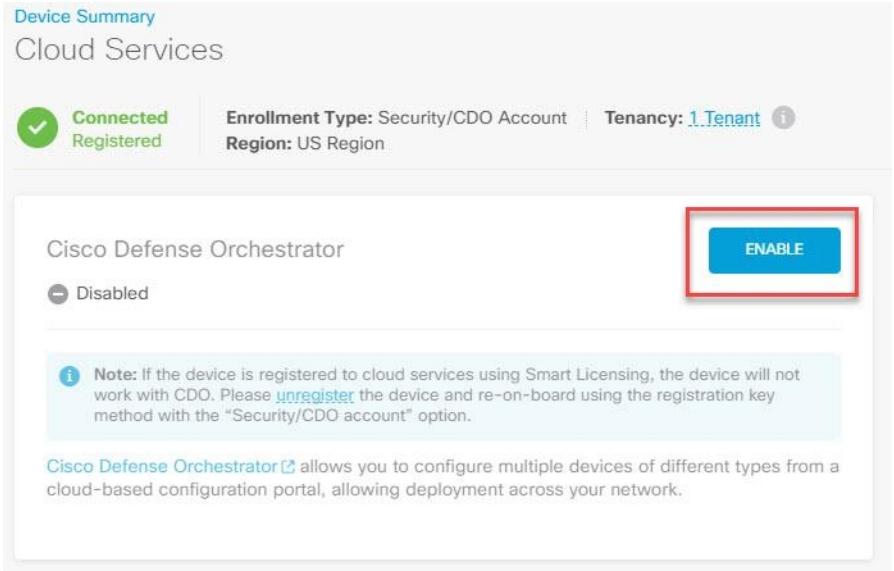
ステップ 15 [登録（Register）] をクリックし、[シスコの開示情報を受け入れる（Accept the Cisco Disclosure）] をクリックします。FDM が CDO に登録要求を送信します。

ステップ 16 CDO に戻り、[登録キーの作成（Create Registration Key）] 領域で [次へ（Next）] をクリックします。

ステップ 17 [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 デバイスに適用して [次へ（Next）] をクリックするか、[スキップ（Skip）] をクリックして、90 日間の評価ライセンスでオンボーディングを続行するか、デバイスがすでにスマートライセンスを取得してい

る場合は、続行できます。詳細については、「FTDデバイスの既存のスマートライセンスの更新」を参照してください。

（注） デバイスがバージョン6.6を実行している場合は、CDOへの通信を手動で有効にする必要があります。デバイスのFDM UIから、[システム設定（System Settings）]>[Cloud Services（クラウドサービス）] に移動し、[Cisco Defense Orchestrator] タイルで [有効化（Enable）] をクリックします。



ステップ 18 CDO に戻り、[インベントリに移動（Go to Inventory）] をクリックします。CDO は自動的にデバイスをオンボーディングし、それらを単一のエントリとして結合します。オンボーディングした最初のピアデバイスと同様に、デバイスのステータスは「プロビジョニング解除（Unprovisioned）」から「取得中（Locating）」、「同期中（Syncing）」、「同期済み（Synced）」に変わります。

ユーザー名、パスワード、IP アドレスを使用した FTD HA ペアの導入準備

（注） ユーザー名とパスワードを使用してHAペアのいずれかのデバイスをオンボーディングする場合、もう一方のピアデバイスのオンボーディングにも同じ方法を使用する必要があります。

CDO の外部で作成された FTD HA ペアをオンボードするには、次の手順に従います。

手順

ステップ 1 HA ペア内のピアデバイスの片方をオンボードします。最初のデバイスのオンボードについては、ユーザー名、パスワード、IP アドレスを使用した FTD のオンボーディング （10 ページ）を参照してください。

ステップ 2 デバイスが同期されたら、[インベントリ（Inventory）] ページで [デバイス（Devices）] タブをクリックします。

ステップ 3 [FTD] タブをクリックします。

ステップ 4 デバイスを選択します。[デバイスの詳細（Devie Details）] のすぐ下にある操作ウィンドウで、[デバイスのオンボーディング（Onboard Device）] をクリックします。

ステップ 5 ポップアップウィンドウで、HA ピアのデバイス名と場所を入力します。

ステップ 6 [デバイスのオンボード（Onboard Device）] をクリックします。両方のデバイスが CDO に正常に同期されると、HA ペアが単一のエンティティとして [インベントリ（Inventory）] ページに表示されます。

スマートライセンスの適用または更新

FTD デバイスへの新しいスマートライセンスの適用

次のいずれかの手順を実行して、Firepower Threat Defense（FTD）デバイスのスマートライセンスを取得します。

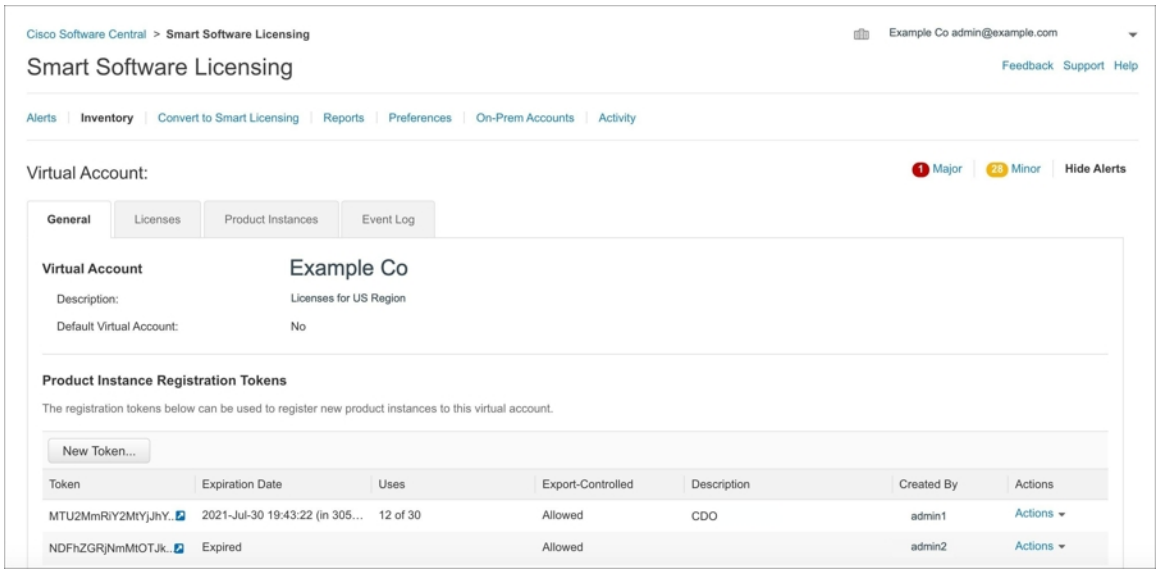
- 登録キーを使用してオンボーディングするときに FTD デバイスにスマートライセンスを付与します。
- 登録キーまたは管理者のログイン情報を使用してデバイスをオンボーディングした後、FTD デバイスにスマートライセンスを付与します。

（注） FTD デバイスで 90 日間の評価ライセンスを使用しているか、ライセンスが登録解除されている可能性があります。

登録キーを使用して導入準備する場合の FTD デバイスのスマートライセンス付与

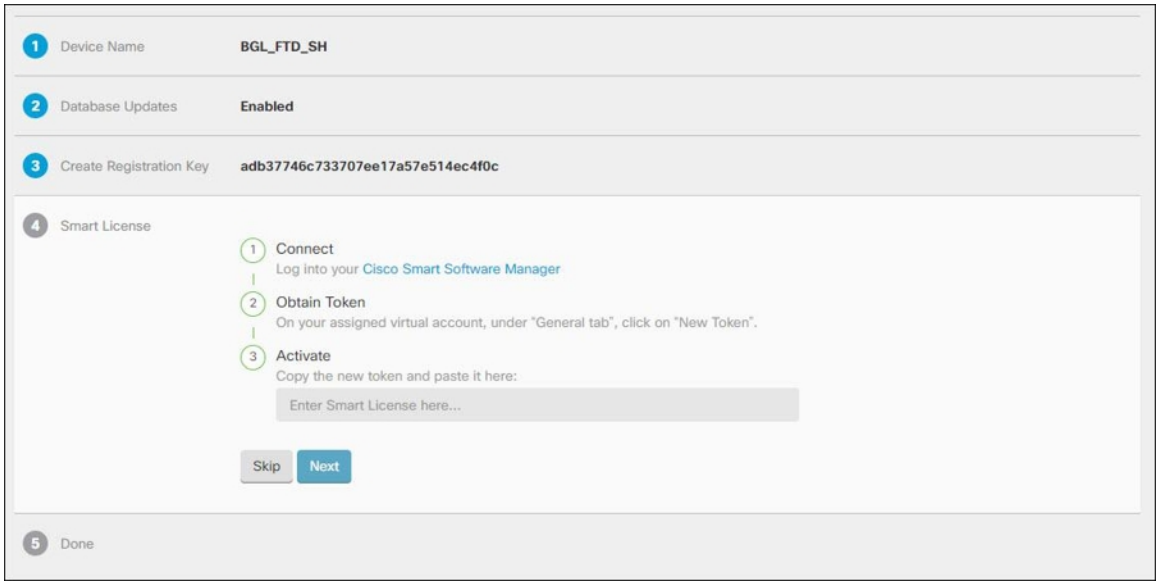
手順

ステップ 1 Cisco Smart Software Manager にログインして、新しいスマートライセンスキーを生成します。新しく生成したキーをコピーします。詳細については、スマートライセンスの生成に関するビデオをご覧ください。



ステップ 2 登録キーを使用して FTD の導入準備を開始します。詳細については、「登録キーを使用したソフトウェアバージョン 6.6+ を実行する FTD のオンボード」または「登録キーを使用したソフトウェアバージョン 6.4 または 6.5 を実行する FTD の導入準備」を参照してください。

ステップ 3 導入準備ウィザードのステップ 4 で、[スマートライセンス情報（Smart License here）] ボックス内の [アクティブ化（Activate）] フィールドにスマートライセンスを貼り付けて、[次へ（Next）] をクリックします。

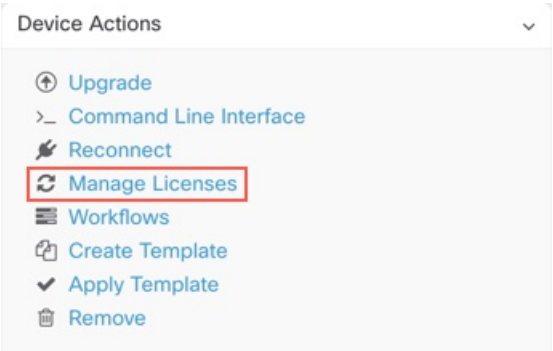


ステップ 4 [インベントリページに移動（Go to Inventory page）] をクリックします。

ステップ 5 [FTD] タブをクリックして、導入準備プロセスの進行状況を確認します。デバイスで同期が開始され、スマートライセンスが適用されます。

デバイスが**オンライン**接続状態になったことを確認する必要があります。デバイスがオンライン接続状態にない場合は、右側の [デバイス アクション（Device Actions）] ペインで、**[ライセンス管理（Manage Licenses）] > [ライセンスの更新（Refresh Licenses）]**をクリックして、接続状態を更新します。

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たら、[ライセンス管理（Manage Licenses）] をクリックします。デバイスのステータスは [接続済み（Connected）]、[十分なライセンス（Sufficient License）] と表示されます。また、オプションライセンスを有効化または無効化できます。詳細については、「FTD のライセンスタイプ」を参照してください。



登録キーまたはログイン情報を使用したデバイスの導入準備の後に、FTD デバイスにスマートライセンスを付与する

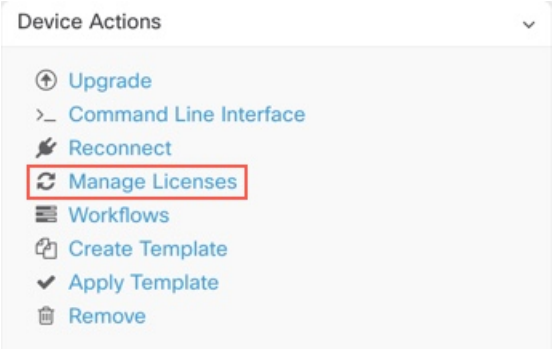
手順

ステップ 1 ナビゲーションウィンドウで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけます。

ステップ 3 [FTD] タブをクリックして、ライセンスを付与するデバイスを選択します。

ステップ 4 右側の [デバイスアクション（Device Actions）] ペインで、[ライセンスの管理（Manage Licenses）] をクリックします。



ステップ 5 画面の指示に従って Smart Software Manager で生成されたスマートライセンスを入力します。

ステップ 6 ボックスに新しいライセンスキーを貼り付け、[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。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（Connected）]、[十分なライセンス（Sufficient License）] と表示されます。また、オプションライセンスを有効化または無効化できます。詳細については、「FTD のライセンスタイプ」を参照してください。

FTD デバイスの既存のスマートライセンスの更新

スマートライセンスが適用された FTD デバイスに、新しいスマートライセンスを適用できます。デバイスのオンボーディングで選択した方法に基づいて、適切な手順を選択します。

登録キーを使用して導入準備した FTD デバイスのスマートライセンスの変更

手順

ステップ 1 対応する FTD デバイスを CDO から削除します。

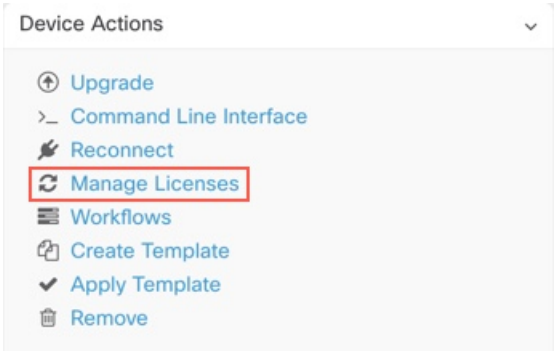
ステップ 2 FTD の Firepower Device Manager（FDM）にログインし、スマートライセンスを登録解除します。 詳細については、「登録キーを使用したソフトウェアバージョン 6.6+ を実行する FTD のオンボード」を参照してください。

ステップ 3 CDO で、再び登録キーを使用して FTD デバイスの導入準備をします。詳細については、「登録キーを使用したソフトウェアバージョン 6.6+ を実行する FTD のオンボード」を参照してください。

ステップ 4 [デバイス（Devices）] タブをクリックしてデバイスを見つけます。

ステップ 5 [] タブをクリックします。

ステップ 6 新しいスマートライセンスの適用は導入準備プロセス中に行うか、または右側の [デバイスアクション（Device Actions）] ペインで [ライセンス管理（Manage Licenses）] をクリックします。



ログイン情報を使用して導入準備した FTD デバイスのスマートライセンスの変更

手順

ステップ 1 FTD の Firepower Device Manager（FDM）にログインし、スマートライセンスを登録解除します。 詳細については、「登録キーを使用したソフトウェアバージョン 6.6+ を実行する FTD のオンボード」を参照してください。

ステップ 2 FDM の FTD デバイスに新しいスマートライセンスを適用します。

1. [スマートライセンス（Smart License）] 領域で、 [設定の表示（View Configuration）] をクリックします。
2. [今すぐ登録（Register Now）] をクリックして、画面上の指示に従います。

ステップ 3 CDO の [インベントリ（Inventory）] ページで [デバイス（Devices）] タブをクリックします。

ステップ 4 **FTD** デバイスをクリックします。FTD 設定の変更内容を確認します。これにより、CDO では FTD の展開された設定のコピーが作成され、CDO 独自のデータベースに保存されます。詳細については、「設定変更の読み取り、破棄、チェック、および展開」を参照してください。

FTD デバイスの DHCP アドレス指定の CDO サポート

Firepower Threat Defense Device（FTD）で使用される IP アドレスが変更された場合について説明します。

適応型セキュリティアプライアンス（ASA）や FTD を使用する Cisco Defense Orchestrator（CDO）のお客様の多くは、DHCP を介してサービスプロバイダーから提供される IP アドレスを使用してデバイスをオンボードします。

デバイスの IP アドレスが何らかの理由で変更された場合、それが静的 IP アドレスの変更であるか、DHCP による IP アドレスの変更であるかにかかわらず、CDO がデバイスへの接続に使用する IP アドレスを変更して、デバイスを再接続できます。

分散拠点に展開されている FTD デバイスを CDO によって管理することについて、開発現場では懸念の声が上がっています。FTD の外部インターフェイスでは静的 IP が必要です。一部の SE は、FTD で外部インターフェイスに DHCP アドレスが設定されている場合、CDO を管理ソリューションとして使用することは不可能だという見解を示しています。

ただし、この状況は、リモートブランチファイアウォールへの VPN トンネルを使用しているお客様には影響しません。また、お客様の大多数が、分散拠点からデータセンターへのサイト間トンネルを使用していることがわかっています。サイト間 VPN を使用してデバイスからセントラルサイトに接続する場合、外部インターフェイスの DHCP は問題になりません。CDO（および任意の管理プラットフォーム）は内部の静的アドレスが指定されたインターフェイスを介して（そのように設定されている場合）FW に接続できるためです。これは推奨される方法であり、デバイス数が多い（1000 超）CDO のお客様は、この展開モードを使用しています。

また、インターフェイスの IP アドレスが DHCP 経由で発行されている場合でも、お客様がその IP を使用してデバイスを管理することの妨げにはなりません。繰り返しますが、これは最適な方法ではありませんが、CDO で IP アドレスを定期的に変更する必要があっても、お客様の不利益になるとは考えられません。この状況はCDOに限ったものではなく、ASDM、FDM、または SSH などの外部インターフェイスを使用するすべてのマネージャで発生します。

FTD のライセンスタイプ

スマート ライセンスのタイプ

次の表に、Firepower Threat Defense（FTD）デバイスで使用可能なライセンスの説明を示します。

FTD を購入すると、自動的に基本ライセンスが含まれます。すべての追加ライセンスはオプションです。

ライセンス	期間	付与される機能
基本ライセンス（自動的に含まれます）	永続	サブスクリプション ターム ライセンスでカバーされないすべての機能。 [このトークンに登録した製品でエクスポート制御機能を許可する（Allow export-controlled functionality on the products registered with this token）] かどうかも指定する必要があります。このオプションは、自国が輸出管理の標準規格に適合している場合のみ選択できます。このオプションは、高度な暗号化や、高度な暗号化を必要とする機能の使用を制御します。

ライセンス	期間	付与される機能
脅威	ターム ベース	**侵入検知および防御**：侵入ポリシーが侵入とエクスプロイトを検出するためネットワークトラフィックを分析し、またオプションで違反パケットをドロップします。 **ファイル制御**：ファイルポリシーが特定タイプのファイルを検出し、オプションでこれらのファイルのアップロード（送信）またはダウンロード（受信）をブロックできます。マルウェア ライセンスが必要な AMP for Firepower を使用すると、マルウェアを含むファイルのインスペクションを実行してブロックできます。任意のタイプのファイルポリシーを使用するには、脅威ライセンスが必要です。 **セキュリティ インテリジェンス フィルタ**：トラフィックがアクセスコントロールルールによって分析を受ける前に、選択されたトラフィックをドロップします。ダイナミックフィードを使用することで、最新のインテリジェンスに基づいて接続をただちにドロップできます。
マルウェア（Malware）	ターム ベース	マルウェアを確認するポリシーであり、Cisco Advanced Malware Protection（AMP）と一緒に AMP for Firepower（ネットワークベースの高度なマルウェア保護）と Cisco Threat Grid を使用します。 ファイル ポリシーは、ネットワーク上で伝送されるファイルに存在するマルウェアを検出してブロックできます。

ライセンス	期間	付与される機能
URL ライセンス	ターム ベース	カテゴリとレピュテーションに基づく URL フィルタリング。 このライセンスなしでも、個々の URL で URL フィルタリングを実行できます。
RA VPN Only ライセンス RA VPN Plus ライセンス RA VPN Apex ライセンス	ライセンスタイプに基づきタームベースまたは永久	リモート アクセス VPN の設定 RA VPN を設定するには、基本ライセンスによるエクスポート制御機能を許可する必要があります。デバイスを登録するときに、エクスポート要件を満たすかどうかを選択します。 Firepower Device Manager は、AnyConnect の任意の有効なライセンスを使用できます。使用可能な機能は、ライセンスタイプによる違いはありません。まだライセンスを購入していない場合は、「リモート アクセス VPN のライセンス要件」を参照してください。 『Cisco AnyConnect 発注ガイド』（[illegible]）も参照してください。

FTDv の階層型ライセンス

FTD バージョン 7.0 では、スループット要件と RA VPN セッションの制限に基づいて、仮想 FTD（FTDv）デバイスのパフォーマンス階層型のスマートライセンスをサポートするようになりました。使用可能なパフォーマンスライセンスのいずれかで FTDv のライセンスが付与されると、次の 2 つのことが発生します。RA VPN のセッション制限が、インストールされている FTDv プラットフォームのエンタイトルメント層によって決定され、レートリミッタを介して適用されます。

現時点では、CDO は階層型スマートライセンスを完全にはサポート**していません**。次の制限事項を参照してください。

- CDO を介して階層型ライセンスを変更できません。FDM UI で変更する必要があります。

- クラウドサービスの CDO に FTDv を登録すると、階層型ライセンスの選択が自動的にデフォルト階層の [変数（Variable）] にリセットされます。
- バージョン 7.0 以降を実行している FTDv の導入準備プロセス中にデフォルトライセンス**ではない**ライセンスを選択すると、階層型ライセンスの選択は、デフォルト階層の [変数（Variable）] に自動的にリセットされます。

上記の問題を回避するために、デバイスの導入準備後に FTDv ライセンスの階層を選択することを強く推奨します。詳細については、「スマートライセンスの管理」を参照してください。

デバイスのスマートライセンスの表示

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 [FTD] タブをクリックします。

ステップ 4 FTD デバイスを選択して、現在のライセンスステータスを表示します。

ステップ 5 右側の [デバイスアクション（Device Actions）] ペインで、[ライセンスの管理（Manage Licenses）] をクリックします。[ライセンスの管理] 画面には、次の情報が表示されます。

- [スマート ライセンス エージェントのステータス（Smart License Agent status）]：90 日間の評価ライセンスを使用しているかどうか、または Cisco Smart Software Manager に登録済みかどうかが表示されます。スマート ライセンス エージェントのステータスは次のとおりです。
  - [接続済み（Connected）]、[十分なライセンス（Sufficient Licenses）]：デバイスは認証局に正しく登録され、アプライアンスのソフトウェア利用資格が承認されています。このデバイスはインコンプライアンスの状態です。
  - [コンプライアンス違反（Out-of-Compliance）]：デバイスで使用可能なソフトウェア利用資格がありません。ライセンスされた機能は動作を継続します。ただし、コンプライアンスに遵守するためには、追加の権限を購入するか、権限を解放する必要があります。
  - [認証期限切れ（Authorization Expired）]：デバイスは 90 日以上ライセンス認証局と通信していません。ライセンスされた機能は動作を継続します。この状態の場合、スマート ライセンス エージェントは認証要求を再試行します。再試行に成功すると、エージェントは [コンプライアンス違反（Out-of-Compliance）] または [認証済み（Authorized）] 状態に切り替わり、新しい認証期間が開始されます。手動でデバイスの同期を試します。
- [ライセンス登録（License Registration）]：導入準備が完了している FTD デバイスにスマートライセンスを適用できます。詳細については、「登録キーを使用したソフトウェアバージョン 6.6+ を実行する FTD のオンボード」を参照してください。登録が完了すると、

Cisco Smart Software Manager への接続のステータス、および各ライセンスタイプのステータスを確認できます。

- [ライセンスステータス（License Status）]：FTD デバイスで使用可能なオプションライセンスのステータスが表示されます。ライセンスを有効にすると、ライセンスによって制御される機能を使用できます。

オプション ライセンスの有効化または無効化

90 日間の評価ライセンスまたはフルライセンスが採用されている FTD デバイスでオプションライセンスを有効化（登録）できます。ライセンスによって制御される機能を使用するには、ライセンスを有効にする必要があります。

オプションのタームライセンスの対象となる機能を使用しなくなった場合、ライセンスを無効化（解除）できます。ライセンスを無効にすると、Cisco Smart Software Manager アカウントでライセンスが解除されるため、別のデバイスにそのライセンスを適用できるようになります。

評価モードでは、オプションライセンスの評価版を有効にして、すべての操作を実行することもできます。このモードでは、デバイスを登録するまでライセンスは Cisco Smart Software Manager に登録されません。

（注） 評価モードでは RA VPN ライセンスを有効にすることはできません。

始める前に

ライセンスを無効にする前に、そのライセンスが使用中でないことを確認します。ライセンスを必要とするポリシーは書き換えるか削除します。

高可用性の設定で動作する装置の場合は、アクティブな装置でのみライセンスを有効化または無効化します。スタンバイ装置が必要なライセンスを要求（または解放）すると、次の設定の展開時にスタンバイ装置に変更内容が反映されます。ライセンスを有効にする際は、Cisco Smart Software Manager アカウントで十分な数のライセンスが使用可能であることを確認する必要があります。これを確認しないと、一方の装置が準拠、もう一方の装置が非準拠になる可能性があります。

オプションライセンスを有効または無効にするには、次の手順を実行します。

手順

ステップ 1 [インベントリ（Inventory）] ページで、必要な FTD デバイスを選択し、[デバイスアクション（Device Actions）] ペインで [ライセンスの管理（Manage Licenses）] をクリックします。[ライセンスの管理（Manage Licenses）] 画面が表示されます。

ステップ 2 それぞれのオプションライセンスのスライダコントロールをクリックして、ライセンスを有効または無効にします。有効になっている場合、ライセンスのステータスには [OK] と表示されます。

- [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。

ステップ 3 [保存（Save）] をクリックして、変更内容を保存します。

期限切れまたは無効なオプション ライセンスの影響

オプションのライセンスが期限切れになっても、そのライセンスを必要とする機能を使用し続けることはできます。ただし、ライセンスは非準拠とマークされます。ライセンスを準拠状態に戻すには、ライセンスを購入してアカウントに追加する必要があります。

オプションのライセンスを無効にすると、システムは次のように反応します。

- [マルウェアライセンス（Malware license）]：システムはAMPクラウドへの問い合わせを停止し、AMP レトロスペクションクラウドから送信されたレトロスペクティブイベントの認証も停止します。既存のアクセス コントロール ポリシーにマルウェア検出を適応するファイル ポリシーが含まれている場合、このアクセス コントロール ポリシーを再展開することはできません。マルウェアライセンスが無効にされた後、システムが既存のキャッシュファイルの性質を使用できるのは極めて短時間のみであることに注意してください。この時間枠の経過後、システムはUnavailableという性質をこれらのファイルに割り当てます。
- [脅威（Threat）]：システムは侵入またはファイル制御ポリシーを適用しなくなります。セキュリティ インテリジェンス ポリシーの場合、システムはこのポリシーを適用せず、フィード更新のダウンロードを停止します。ライセンスを必要とする既存のポリシーを再展開することはできません。
- [URLフィルタリング（URL Filtering）]：URLカテゴリ条件が指定されたアクセス制御ルールはURLのフィルタリングをただちに停止し、システムはURLデータへの更新をダウンロードしなくなります。既存のアクセス コントロール ポリシーに、カテゴリ ベースまたはレピュテーション ベースのURL 条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。
- [RA VPN]：リモートアクセスVPN設定は編集できませんが、削除は可能です。ユーザーは引き続きRA VPN設定を使用して接続できます。ただし、デバイスの登録を変更してシステムがエクスポートに準拠しなくなると、リモートアクセス VPN 設定はただちに停止し、リモートユーザーはVPNに接続できなくなります。

FTD モデルの作成とインポート

CDO では、CDO テナントにある FTD デバイスの完全な設定を JSON ファイル形式でエクスポートできます。エクスポートしたファイルは、FTDモデルとして別のテナントにインポートし、そのテナントの新しいデバイスに適用できます。この機能は、管理対象のさまざまなテナントで FTD デバイスの設定を使用する際に役立ちます。

（注） FTDデバイスにルールセットが存在する場合、設定をエクスポートすると、そのルールセットに関連付けられている共有ルールはローカルルールとして変更されます。その後、モデルが別のテナントにインポートされ、FTDデバイスに適用されると、デバイスにローカルルールが表示されます。

FTD 設定のエクスポート

FTD デバイスに次の設定がある場合、エクスポート設定機能は使用できません。

- 高可用性
- Snort 3 の有効化

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [FTD] タブをクリックします。

ステップ 4 FTD デバイスを選択し、右側の [デバイスアクション（Device Actions）] ペインで、[設定のエクスポート（Export Configuration）] をクリックします。

FTD 設定のインポート

手順

ステップ 1 FTD の設定をインポートするには、[インベントリ（Inventory）] ページで青いプラス（ ）ボタンをクリックします。

ステップ 2 [インポート（Import）] をクリックして、オフライン管理用に設定をインポートします。

ステップ 3 [デバイスタイプ（Device Type）] として [FTD] を選択します。

ステップ 4 [参照（Browse）] をクリックし、アップロードする設定ファイル（JSON形式）を選択します。

ステップ 5 設定が確認されると、デバイスまたはサービスにラベルを設定するよう求められます。詳細については、『Labels and Label Groups』を参照してください。

ステップ 6 モデルデバイスにラベルを設定すると、[インベントリ（Inventory）] リストに表示できます。

（注） 設定のサイズ、および他のデバイスまたはサービスの数によっては、設定の分析に時間がかかる場合があります

CDO からのデバイスの削除

CDO からデバイスを削除するには、次の手順を使用します。

手順

ステップ 1 CDO にログインします。

ステップ 2 [インベントリ（Inventory）] ページに移動します。

ステップ 3 削除するデバイスを見つけ、そのデバイスの行でデバイスをチェックして選択します。

ステップ 4 右側にある [デバイスアクション（Device Actions）] パネルで、[削除（Remove）] を選択します。

ステップ 5 プロンプトが表示されたら、[OK] を選択して、選択したデバイスの削除を確認します。[キャンセル（Cancel）] を選択して、デバイスをオンボードしたままにします。

FTD HA ペアの両方のデバイスを同時に削除する必要があることに注意してください。個々のピアではなく、FTD HA ペア名をクリックします。

オフライン管理用にデバイスの設定をインポートする

オフライン管理用にデバイスの設定をインポートすると、ネットワーク内の稼働中のデバイスを操作することなく、デバイスの設定を確認して最適化できます。CDO では、アップロードされたこれらの設定ファイルは「モデル」とも呼ばれます。

以下のデバイスの設定を CDO にインポートできます。

- 適応型セキュリティアプライアンス（ASA）。
- Firepower Threat Defense（FTD）。「FTD モデルの作成とインポート」を参照してください。
- Aggregation Services Routers（ASR）や Integrated Services Routers（ISR）などの Cisco IOS デバイス。

FTD のバックアップ

CDO を使用して FTD のシステム設定をバックアップし、デバイスを以前の状態に復元することができます。バックアップには設定だけが含まれ、システム ソフトウェアは含まれません。デバイスを完全に再イメージ化する必要がある場合、ソフトウェアを再インストールしてからバックアップをアップロードして、設定を回復する必要があります。CDO は、デバイスに対して作成された最新の 5 つのバックアップを保存します。新しいバックアップが作成されると、最新のバックアップを保存するために、最も古いバックアップが削除されます。

（注） バックアップには管理 IP アドレスの設定は含まれません。したがって、バックアップ ファイルを復元しても、管理アドレスがバックアップ コピーにより置き換えられることはありません。これにより、アドレスに対する変更はすべて保持され、また異なるネットワーク セグメント上の別のデバイスに設定を復元することもできます。

バックアップ中は設定データベースがロックされます。バックアップの間はポリシー、ダッシュボードなどを表示できますが、設定を変更することはできません。復元を行っている間、システムは完全に使用できません。

デバイス間でバックアップスケジュールの一貫性を保つために、独自のデフォルトのバックアップスケジュールを設定できます。特定のデバイスのバックアップをスケジュールする場合、独自のデフォルト設定を使用するか、設定を変更することができます。毎日から月に一度の頻度で定期的なバックアップをスケジュールでき、オンデマンドバックアップを実行できます。バックアップをダウンロードし、FDM を使用してバックアップを復元することもできます。

CDO を使用して FTD デバイスをバックアップおよび復元するための要件とベストプラクティス

- CDOは、ソフトウェアバージョン6.5以降を実行しているFTDをバックアップできます。
- FTD は、登録キーを使用して CDO にオンボードする必要があります。
- 交換用デバイスにバックアップを復元できるのは、2 つのデバイスが同じモデルであり、同じリリースというだけでなく、同じバージョンのソフトウェア（ビルド番号を含む）を実行している場合のみです。たとえば、ソフトウェアバージョン 6.6.0-90 を実行しているFTD のバックアップは、6.6.0-90 を実行している FTD にのみ復元できます。アプライアンス間で設定をコピーするためにバックアップおよび復元プロセスを使用しないでください。バックアップ ファイルには、この方法で共有することができないようにアプライアンスを一意に特定する情報が含まれます。

ベスト プラクティス

バックアップするデバイスは、CDO で [同期（Synced）] 状態になっている必要があります。CDO は、CDO からではなく、デバイスからデバイスの設定をバックアップします。したがっ

て、デバイスが [非同期（Not Synced）] 状態の場合、CDO での変更はバックアップされません。デバイスが [競合検出（Conflict Detected）] 状態の場合、変更はバックアップされます。

関連情報：

- すべての FTD のデフォルトの定期バックアップスケジュールの設定
- 単一 FTD の定期バックアップスケジュールの設定
- オンデマンドの FTD バックアップ
- FTD バックアップのダウンロード
- FTD バックアップの編集
- FTD デバイスへのバックアップの復元

オンデマンドの FTD バックアップ

この手順では、必要に応じて復元できるように FTD デバイスをバックアップする方法について説明します。

はじめる前に

FTD をバックアップする前に、FTD のバックアップを参照してください。

手順

手順

ステップ 1 （任意）バックアップの変更要求を作成します。

ステップ 2 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 3 [デバイス] タブをクリックします。

ステップ 4 [FTD] タブをクリックして、バックアップするデバイスを選択します。

ステップ 5 右側の [デバイスアクション（Device Actions）] ウィンドウで、[バックアップの管理（Manage Backups）] をクリックします。

ステップ 6 [すぐにバックアップ（Backup Now）] をクリックします。デバイスはバックアップ構成の状態になります。

バックアップが完了すると、CDO ではバックアップ開始前のデバイス構成の状態が表示されます。変更ログページを開くと、「バックアップが正常に完了しました」という説明が付けられた直近の変更ログレコードが見つかります。

ステップ 1 で変更要求を作成した場合は、変更要求の値でフィルタ処理して、変更ログエントリを見つけることもできます。

ステップ 7 ステップ 1 で変更要求を作成した場合は、変更要求の値をクリアして、誤って別の変更をその変更要求に関連付けないようにします。

単一 FTD の定期バックアップスケジュールの設定

はじめる前に

FTD をバックアップする前に、FTD のバックアップを参照してください。

手順

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックして、バックアップするデバイスを選択します。

ステップ 4 右側の [デバイスアクション（Device Actions）] ウィンドウで、[バックアップの管理（Manage Backups）] をクリックします。

ステップ 5 [バックアップデバイス（Backup Device）] ページで、[定期バックアップの設定（Set Recurring Backup）] をクリックするか、[定期バックアップ（Recurring Backup）] フィールドのスケジュールをクリックします。CDO では、テナントにあるすべての FTD デバイスに設定されたデフォルトのバックアップスケジュールが提示されます。詳細については、「すべての FTD のデフォルトの定期バックアップスケジュールの設定」を参照してください。

ステップ 6 バックアップを実行する時間を 24 時間制で選択します。協定世界時（UTC）でバックアップ時間をスケジュールすることに注意してください。

ステップ 7 [頻度（Frequency）] フィールドで、 [日次（Daily）]、[週次（Weekly）]、または [月次（Monthly）] を選択します。

- 日次バックアップの場合：スケジュールしたバックアップに名前と説明を付けます。
- 週次バックアップの場合：バックアップを実行する曜日のチェックボックスをオンにします。スケジュールしたバックアップの時間に名前と説明を付けます。
- 月次バックアップの場合：[日付（Days of Month）] フィールドをクリックして、バックアップをスケジュールする日付を追加します。注：31 日を入力しても、その月に 31 日が含まれていない場合、バックアップは行われません。スケジュールしたバックアップの時間に名前と説明を付けます。

ステップ 8 [保存（Save）] をクリックします。[バックアップ デバイス（Backup Device）] ページの [定期バックアップ（Recurring Backup）] フィールドは、設定したバックアップスケジュールに置き換えられ、現地時間が反映されます。

FTD バックアップのダウンロード

この手順では、Firepower Threat Defense（FTD）デバイスのバックアップを含む .tar ファイルをダウンロードする方法を説明します。

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックし、バックアップをダウンロードするデバイスをクリックします。

ステップ 4 右側の操作ウィンドウで、[バックアップの管理（Manage Backups）] をクリックします。

ステップ 5 ダウンロードするバックアップを選択し、その行で [ダウンロードリンクを生成（Generate Download Link）] ボタンをクリックします。ボタンが [バックアップイメージのダウンロード（Download Backup Image）] に変わります。

ステップ 6 [バックアップイメージのダウンロード（Download Backup Image）] というボタンが表示されたら、次のいずれかの操作を実行します。

- 復元するデバイスの Firepower Device Manager（FDM）にもアクセスできるデバイスを使用している場合は、[バックアップイメージのダウンロード（Download Backup Image）] ボタンをクリックして、ダウンロードしたファイルを保存します。覚えやすい名前で保存してください。
- 復元するデバイスの FDM にもアクセスできるデバイスを使用していない場合は以下を実行します。
  1. [バックアップイメージのダウンロード（Download Backup Image）] ボタンを右クリックし、リンクのアドレスをコピーします。

     重要 リンクのアドレスは、[ダウンロードリンクの生成（Generate Download Link）] ボタンをクリックしてから 15 分後に期限切れになります。

  2. イメージを復元する FTD の FDM にもアクセスするデバイスでブラウザを開きます。
  3. ブラウザのアドレスバーにダウンロードリンクを入力し、バックアップファイルをそのデバイスにダウンロードします。覚えやすい名前で保存してください。

FTD バックアップの編集

この手順では、成功した FTD ダウンロードの名前または説明を編集できます。

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックして、編集するデバイスを選択します。

ステップ 4 右側の [操作（Actions）] ウィンドウで、[バックアップの管理（Manage Backups）] をクリックします。

ステップ 5 編集するバックアップとその行を選択し、編集アイコンをクリックします。

ステップ 6 バックアップの名前または説明を変更します。[デバイスのバックアップ（Device Backups）] ページで新しい情報を確認できます。

FTD バックアップの削除

CDO は、デバイスに対して作成された最新の 5 つのバックアップを保存します。新しいバックアップが作成されると、最新のバックアップを保存するために、最も古いバックアップが削除されます。既存のバックアップを削除すると、保持するバックアップと削除するバックアップの管理に役立つ場合があります。

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックして、削除するデバイスを選択します。

ステップ 4 右側の [操作（Actions）] ウィンドウで、[バックアップの管理（Manage Backups）] をクリックします。

ステップ 5 削除するバックアップとその行を選択し、ゴミ箱アイコン をクリックします。

ステップ 6 [OK] をクリックして確認します。

FTD バックアップの管理

CDO を使用して作成した FTD デバイスのバックアップは、[デバイスバックアップ（Device Backups）] ページに表示されます。

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックして、該当するデバイスを選択します。

ステップ 4 [デバイスアクション（Device Actions）] ペインで、[バックアップの管理（Manage Backups）] をクリックします。そのデバイスから作成された最新のバックアップが最大 5 つ表示されます。

FTD デバイスへのバックアップの復元

- バックアップ を FTD に復元する前に、FTD のバックアップを確認してください。
- 復元するバックアップコピーがまだデバイスに存在しない場合、復元する前にまずバックアップを**アップロード**する必要があります。
- 復元している間、システムはまったく使用できません。バックアップが復元された後、FTD が再起動します。
- この手順では、デバイスに復元する準備ができているデバイスの既存のバックアップがあることを前提としています。
- このデバイスがハイアベイラビリティペアの一部である場合、バックアップは復元できません。まず、[デバイス（Device）] > [ハイアベイラビリティ（High Availability）] ページから HA を無効化することで、バックアップを復元できます。バックアップに HA の設定が含まれている場合、デバイスは HA グループに再度参加します。両方のユニットで同じバックアップを復元しないでください（両方のユニットがアクティブになってしまうため）。代わりに、まず、アクティブにする装置でバックアップを復元し、その後に、別のユニットで同等のバックアップを復元してください。

（注） バックアップには管理 IP アドレスの設定は含まれません。したがって、バックアップ ファイルを復元しても、管理アドレスがバックアップ コピーにより置き換えられることはありません。これにより、アドレスに対する変更はすべて保持され、また異なるネットワーク セグメント上の別のデバイスに設定を復元することもできます。

手順

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックして、復元するデバイスを選択します。

ステップ 4 右側の [デバイスアクション（Device Actions）] ウィンドウで、[バックアップの管理（Manage Backups）] をクリックします。

ステップ 5 復元するバックアップを選択します。その行で、[ダウンロードリンクの生成（Generate Download Link）] ボタン をクリックします。

（注） リンクのアドレスは、[ダウンロードリンクの生成（Generate Download Link）] ボタンをクリックしてから 15 分後に期限切れになります。

ステップ 6 [バックアップイメージのダウンロード（Download Backup Image）] というボタンが表示されたら、次のいずれかの操作を実行します。

- 復元するデバイスの Firepower Device Manager（FDM）にもアクセスできるデバイスを使用している場合は、[バックアップイメージのダウンロード（Download Backup Image）] ボタンをクリックして、ダウンロードしたファイルを保存します。覚えやすい名前で保存してください。
- 復元するデバイスの FDM にもアクセスできるデバイスを使用していない場合は以下を実行します。
  1. [バックアップイメージのダウンロード（Download Backup Image）] ボタンを右クリックし、リンクのアドレスをコピーします。
  2. イメージを復元する FTD の FDM にもアクセスするデバイスでブラウザを開きます。
  3. ブラウザのアドレスバーにダウンロードリンクを入力し、バックアップファイルをそのデバイスにダウンロードします。覚えやすい名前で保存してください。

ステップ 7 復元するデバイスの Firepower Device Manager にログインします。

ステップ 8 『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用』の 6.5 以降を開きます。「システム管理」の章に移動し、「**バックアップの復元**」を見つけます。この手順に従って、FTD にダウンロードしたイメージを復元します。

ヒント 復元するには、イメージを FDM にアップロードする必要があります。

ステップ 9 FDM のプロンプトに従います。復元が開始されると、ブラウザは FDM から切断されます。復元が終了すると、FTD が再起動します。

関連情報：

- FTD のバックアップ
- オンデマンドの FTD バックアップ
- 単一 FTD の定期バックアップスケジュールの設定
- FTD バックアップのダウンロード
- FTD バックアップの編集

Firepower Threat Defense ソフトウェアのアップグレードパス

Firepower Threat Defense バージョンのアップグレード

CDO を使用して Firepower Threat Defense（FTD）ファイアウォールをアップグレードする場合、どの FTD バージョンがアップグレード可能かを CDO が判断するので、このトピックは必要ありません。このトピックでは、FTDイメージの独自のリポジトリを保持している状況で、独自のイメージを使用して FTD をアップグレードする場合に使用可能なアップグレードパスについて説明します。

FTD は、あるメジャーバージョンまたはメンテナンスバージョンから別のバージョンに直接アップグレードできます。たとえば、バージョン 6.4.0 > 6.5.0、またはバージョン 6.4.0 > 7.0.1 のようにアップグレードできます。特定のパッチレベルを実行する必要はありません。

直接アップグレードが不可能な場合は、アップグレードパスに中間バージョンを含める必要があります（バージョン 6.4.0 > 7.0.0 > 7.1.0 など）。

表 *1:* メジャーリリースのアップグレードパス

ターゲットバージョン	ターゲットバージョンにアップグレードできる最も古いリリース
7.1.x	6.5.0
7.0.x	6.4.0
6.7.x	6.4.0
6.6.x	6.4.0
6.5.0	6.4.0

Firepower Threat Defense へのパッチ適用

バージョン 6.4.0.1 > 6.5.0.1 など、あるバージョンのパッチから別のバージョンのパッチに直接アップグレードすることはできません。まずメジャーリリースにアップグレードしてから、そのリリースにパッチを適用する必要があります。たとえば、バージョン 6.4.0.1 > 6.5.0 > 6.5.0.1 のようにアップグレードする必要があります。

Firepower のホットフィックス

CDO は、ホットフィックスの更新またはインストールをサポートしていません。使用中のデバイスモデルまたはソフトウェアバージョンで利用可能なホットフィックスがある場合は、設定済みマネージャのダッシュボードまたは UI を使用することを強くお勧めします。ホットフィックスがデバイスにインストールされると、CDO はアウトオブバンドの設定変更を検出します。

FTD アップグレードの削除

CDO を使用して、メジャー、メンテナンス、またはパッチのいずれかのリリースタイプを削除またはダウングレードすることはできません。

Firepower Threat Defense バージョン 6.7.0 以降では、Firepower Device Manager または FTD CLI を使用して、正常にアップグレードされたデバイスを、最後のメジャーアップグレードまたはメンテナンスアップグレードの直前の状態（スナップショットとも呼ばれる）に戻すことができます。パッチ適用後に復元すると、パッチも必然的に削除されます。復元の後、**アップグレード**と復元の間に行った設定変更があれば再適用する必要があります。**メジャーアップグレードまたはメンテナンスアップグレードを FTD バージョン 6.5.0 ～ 6.6.x に戻すには、再イメージ化が必要であることに注意してください。**詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「System Management」セクションを参照してください。

FTD パッチの削除

CDO または FDM のいずれかを使用して FTD パッチを削除することはできません。パッチを削除するには、メジャーリリースまたはメンテナンスリリースに再イメージ化する必要があります。

Snort のアップグレード

Snort はこの製品の主要な検査エンジンであり、利便性のために Firepower ソフトウェアにパッケージ化されています。バージョン 6.7 では、パッケージの更新が導入されており、いつでもアップグレードまたは元に戻すことができます。Snort のバージョンは自由に切り替えることができますが、Snort 2.0 の一部の侵入ルールは Snort 3.0 に存在しない場合があり、その逆の場合もあります。詳細については、Firepower Device Manager バージョン 6.7.0 のコンフィギュレーション ガイドで、両者の相違点を確認することを強くお勧めします。

Snort 3 を使用できるように FTD システムをアップグレードするか、CDO UI を使用して Snort 3 から Snort 2 に戻すには、「Snort 3.0 へのアップグレード」および「FTD の Snort 3.0 からの復元」をそれぞれ参照してください。

その他アップグレードの制限事項

2100 シリーズデバイス

Firepower 2100 シリーズデバイスがアプライアンスモードで実行している場合のみ、CDO はデバイスをアップグレードできます。

- Firepower Threat Defense デバイスは常にアプライアンスモードです。

次のタスク

これらのコマンドの詳細については、『Cisco Firepower 2100 スタートアップガイド』を参照してください。

4100 シリーズおよび 9300 シリーズデバイス

CDO は、4100 または 9300 シリーズデバイスのアップグレードをサポートしていません。これらのデバイスは CDO の外部でアップグレードする必要があります。

関連情報：

- FTD アップグレードの前提条件
- 単一 FTD デバイスのアップグレード
- FTD の一括 アップグレード
- FTD ハイアベイラビリティペアのアップグレード

FTD アップグレードの前提条件

Cisco Defense Orchestrator（CDO）では、個々のデバイスまたは HA ペアにインストールされている Firepower Threat Defense（FTD）イメージをアップグレードするのに役立つウィザードを使用できます。

このウィザードに従って、互換性のあるイメージを選択してインストールし、デバイスを再起動してアップグレードを完了するプロセスを実行できます。CDO で選択したイメージが FTD デバイスにコピーおよびインストールされたものであることを検証することにより、アップグレードプロセスを保護します。アップグレードする FTD デバイスのインターネットへのアウトバウンドアクセスを可能にすることを強くお勧めします。

FTD にインターネットへのアウトバウンドアクセスがない場合は、必要なイメージを Cisco.com からダウンロードして独自のリポジトリに保存し、アップグレードウィザードにそれらのイメージへのカスタム URL を入力できます。そうすると、CDO はそれらのイメージを使ってアップグレードを実行します。とはいえ、このケースでは、アップグレードするイメージを自分で決定することになります。CDO は、イメージの完全性チェックやディスク容量チェックを実施しません。

設定要件

- FTD デバイスで DNS を有効にする必要があります。詳細については、デバイスが実行しているバージョンの『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』に含まれる「**System Administration**」の章の「Configuring DNS」セクションを参照してください。
- CDO のイメージリポジトリからのアップグレードイメージを使用する場合、FTD デバイスはインターネットに接続できる必要があります。
- FTD デバイスが CDO に正常にオンボーディングされました。
- FTD デバイスは到達可能です。
- FTD デバイスは同期しています。

- CDO に保留中の変更があるデバイスの変更を受け入れずにそのデバイスを更新した場合、保留中の変更はアップグレードの完了後に失われます。ベストプラクティスは、保留中の変更をすべて展開してからアップグレードすることです。
- FDM で変更を段階的に実行しており、デバイスが同期されていない場合、CDO でのアップグレードは利用資格のチェックで失敗します。

FTD を実行中の 4100 および 9300 シリーズ

CDO は、4100 または 9300 シリーズデバイスのアップグレードをサポートしていません。これらのデバイスは CDO の外部でアップグレードする必要があります。

ソフトウェアおよびハードウェアの要件

CDO はクラウド管理プラットフォームです。ソフトウェアの更新は時間の経過とともに継続的にリリースされ、通常はハードウェアに依存しません。サポートされているハードウェアタイプの詳細については、「CDO でサポートされるソフトウェアとハードウェア」を参照してください。

FTD ソフトウェアを実行しているデバイスには、最適なパフォーマンスを得るための推奨されるアップグレードパスがあります。詳細については、「Firepower Threat Defense ソフトウェアのアップグレードパス」を参照してください。

アップグレードに関する注意事項

アップグレード中にデバイスに変更を展開することはできません。

関連情報：

- Firepower Threat Defense ソフトウェアのアップグレードパス
- 単一 FTD デバイスのアップグレード
- FTD の一括 アップグレード
- FTD ハイアベイラビリティペアのアップグレード

単一 FTD デバイスのアップグレード

はじめる前に

アップグレードする前に、「FTD アップグレードの前提条件」、「Firepower Threat Defense ソフトウェアのアップグレードパス」、および「CDO でサポートされるソフトウェアとハードウェア」を必ずお読みください。このドキュメントでは、目的のバージョンの Firepower ソフトウェアにアップグレードする前に知っておくべき要件と注意について説明します。

CDO のリポジトリからのイメージで単一の FTD をアップグレードする

CDO のリポジトリに保存されているソフトウェアイメージを使用してスタンドアロン FTD デバイスをアップグレードするには、以下の手順を実行してください。

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけます。

ステップ 3 [FTD] タブをクリックします。

ステップ 4 アップグレードするデバイスを選択します。

ステップ 5 [デバイスアクション（Device Actions）] ペインで、[アップグレード（Upgrade）] をクリックします。

ステップ 6 手順 1 で、[CDO イメージリポジトリの使用（Use CDO Image Repository]）] をクリックしてアップグレードするソフトウェアイメージを選択し、[続行（Continue）] をクリックします。アップグレード可能なデバイス互換性のある選択肢のみが表示されます。

ステップ 7 手順2 で、選択内容を確認し、デバイスへのイメージのダウンロードのみを実行するか、それともイメージをコピーしてインストールしデバイスを再起動するかを決定します。

ステップ 8 準備ができたら、[アップグレードの実行（Perform Upgrade）] をクリックします。[インベントリ（Inventory）] ページで、アップグレード中のデバイスの設定ステータスが「アップグレード中（Upgrade in Progress）」になります。

警告 アップグレードの進行中にアップグレードをキャンセルする場合は、[アップグレード（Upgrade）] ページで [アップグレードの中止（Abort Upgrade）] をクリックします。開始後にアップグレードをキャンセルすると、CDO はデバイスからの変更をチェックしたり、展開したりせず、デバイスは以前の設定にロールバックしません。その結果、デバイスが異常な状態になる場合があります。アップグレードの過程で何らかの問題が発生した場合は、Cisco TAC までお問い合わせください。

ステップ 9 後でCDOにアップグレードを実行させる場合は、[アップグレードのスケジュール設定（Schedule Upgrade）] チェックボックスをオンにします。フィールドをクリックして、将来の日時を選択します。日時の選択が完了したら、[アップグレードのスケジュール設定（Schedule Upgrade）] ボタンをクリックします。

ステップ 10 [通知（notifications）] タブで一括アップグレードアクションの進行状況を確認します。managing-ftd-with-cisco-defense-orchestrator_chapter4.pdf#nameddest=unique_194 unique_194_Connect_42_notificationtab一括アップグレードジョブのアクションがどのように成功または失敗したかについての詳細な情報が必要な場合は、青色の [レビュー（Review）] リンクをクリックして [ジョブ（Jobs）] ページに移動します。[ジョブ（Jobs）] ページ

ステップ 11 システムデータベースをアップグレードします。この手順をFDMで実行する必要があります。詳細については、『Firepower Device Manager 向け Cisco Firepower Threat Defense 構成ガイド』、バージョン 6.4 の「システムデータベースのアップデート」を参照してください。

独自リポジトリからのイメージを使用した単一 FTD のアップグレード

ソフトウェアイメージを見つけるための URL プロトコルを使用してスタンドアロン FTD デバイスをアップグレードするには、次の手順を実行します。

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけます。

ステップ 3 [FTD] タブをクリックします。

ステップ 4 アップグレードするデバイスを選択します。

ステップ 5 [デバイスアクション（Device Actions）] ペインで、[アップグレード（Upgrade）] をクリックします。

ステップ 6 手順 1 で、[イメージURLの指定（Specify Image URL）] をクリックしてアップグレードするソフトウェアイメージを選択し、[続行（Continue）] をクリックします。アップグレード可能なデバイス互換性のある選択肢のみが表示されます。

ステップ 7 手順 2 で、選択内容を確認し、デバイスへのイメージのダウンロードのみを実行するか、それともイメージをコピーしてインストールしデバイスを再起動するかを決定します。

ステップ 8 準備ができたら、[アップグレードの実行（Perform Upgrade）] をクリックします。[インベントリ（Inventory）] ページで、アップグレード中のデバイスの設定ステータスが「アップグレード中（Upgrade in Progress）」になります。

警告 アップグレードの進行中にアップグレードをキャンセルする場合は、[アップグレード（Upgrade）] ページで [アップグレードの中止（Abort Upgrade）] をクリックします。開始後にアップグレードをキャンセルすると、CDO はデバイスからの変更をチェックしたり、展開したりせず、デバイスは以前の設定にロールバックしません。その結果、デバイスが異常な状態になる場合があります。アップグレードの過程で何らかの問題が発生した場合は、Cisco TAC までお問い合わせください。

ステップ 9 後でCDOにアップグレードを実行させる場合は、[アップグレードのスケジュール設定（Schedule Upgrade）]チェックボックスをオンにします。フィールドをクリックして、将来の日時を選択します。日時の選択が完了したら、[アップグレードのスケジュール設定（Schedule Upgrade）] ボタンをクリックします。

ステップ 10 [通知（notifications）] タブで一括アップグレードアクションの進行状況を確認します。managing-ftd-with-cisco-defense-orchestrator_chapter4.pdf#nameddest=unique_194 unique_194_Connect_42_notificationtab一括アップグレードジョブのアクションがどのように成功または失敗したかについての詳細な情報が必要な場合は、青色の [レビュー（Review）] リンクをクリックして [ジョブ（Jobs）] ページに移動します。[ジョブ（Jobs）] ページ

ステップ 11 システムデータベースをアップグレードします。この手順を FDM で実行する必要があります。詳細については、『Firepower Device Manager 向け Cisco Firepower Threat Defense 構成ガイド』、バージョン 6.4 の「システムデータベースのアップデート」を参照してください。

アップグレードプロセスの監視

単一のデバイスの進行状況を表示するには、[インベントリ（Inventory）] ページでそのデバイスを選択し、[アップグレード（Upgrade）] ボタンをクリックします。CDOに、該当するデバイスの [デバイスのアップグレード（Device Upgrade）] ページが表示されます。

いずれかの時点でアップグレードが失敗すると、CDO からメッセージが表示されます。CDO は、アップグレードプロセスを自動的に再開しません。

警告 自己署名証明書を持つデバイスをアップグレードすると、問題が発生する可能性があります。詳細については、「新しい証明書の検出」を参照してください。

FTD の一括 アップグレード

はじめる前に

アップグレードする前に、「FTD アップグレードの前提条件」、「Firepower Threat Defense ソフトウェアのアップグレードパス」、および「CDO でサポートされるソフトウェアとハードウェア」を必ずお読みください。このドキュメントでは、目的のバージョンの Firepower ソフトウェアにアップグレードする前に知っておくべき要件と注意について説明します。

（注） すべてを同じソフトウェアバージョンにアップグレードする場合にのみ、FTDデバイスを一括アップグレードできます。

CDO のリポジトリからのイメージを使用したバルク FTD デバイスのアップグレード

CDO のリポジトリに保存されているソフトウェアイメージを使用して複数の FTD デバイスをアップグレードするには、以下の手順を実行してください。

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。
ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。
ステップ 3 [FTD] タブをクリックします。
ステップ 4 フィルタを使用して、一括アップグレードに含めるデバイスのリストを絞り込みます。
ステップ 5 フィルタ処理されたデバイスのリストから、アップグレードするデバイスを選択します。

ステップ 6 [デバイスアクション（Device Actions）] ペインで、[アップグレード（Upgrade）] をクリックします。

ステップ 7 [デバイスの一括アップグレード（Bulk Device Upgrade）] ページに、アップグレード可能なデバイスが表示されます。選択したどのデバイスもアップグレードできない場合、CDO にはアップグレードできないデバイスのリンクが表示されます。

ステップ 8 後でCDOにアップグレードを実行させる場合は、[アップグレードのスケジュール設定（Schedule Upgrade）]チェックボックスをオンにします。フィールドをクリックして、将来の日時を選択します。日時の選択が完了したら、[アップグレードのスケジュール設定（Schedule Upgrade）] ボタンをクリックします。

ステップ 9 手順 1 で、[CDOイメージリポジトリの使用（Use CDO Image Repository）] をクリックしてアップグレードするソフトウェアイメージを選択します。アップグレード可能なデバイスと互換性のある選択肢のみが表示されます。[続行（Continue）] をクリックします。

ステップ 10 手順 2 で、選択内容を確認し、デバイスへのイメージのダウンロードのみを実行するか、それともイメージをコピーしてインストールしデバイスを再起動するかを決定します。

ステップ 11 準備ができたら、[アップグレードの実行（Perform Upgrade）] をクリックします。[インベントリ（Inventory）] ページで、アップグレード中のデバイスの設定ステータスが「アップグレード中（Upgrade in Progress）」になります。

警告 アップグレードの進行中にアップグレードをキャンセルする場合は、[アップグレード（Upgrade）] ページで [アップグレードの中止（Abort Upgrade）] をクリックします。開始後にアップグレードをキャンセルすると、CDO はデバイスからの変更を展開したり、変更に関してポーリングしたりしません。アップグレードがキャンセルされた後も、デバイスは以前の構成にロールバックしません。その結果、デバイスが異常な状態になる場合があります。アップグレードの過程で何らかの問題が発生した場合は、Cisco TAC までお問い合わせください。

ステップ 12 [通知（notifications）] タブで一括アップグレードアクションの進行状況を確認します。managing-ftd-with-cisco-defense-orchestrator_chapter4.pdf#nameddest=unique_194 unique_194_Connect_42_notificationtab一括アップグレードジョブのアクションがどのように成功または失敗したかについての詳細な情報が必要な場合は、青色の [レビュー（Review）] リンクをクリックして [ジョブ（Jobs）] ページに移動します。[ジョブ（Jobs）] ページ

ステップ 13 システムデータベースをアップグレードします。この手順を FDM で実行する必要があります。デバイスが実行しているバージョンについては、『Firepower Device Manager 向け Cisco Firepower Threat Defense 構成ガイド』の「**システムデータベースのアップデート**」を参照してください。

独自のリポジトリからのイメージを使用したバルク FTD デバイスのアップグレード

次の手順に従って、ソフトウェアイメージを見つけるための URL プロトコルを使用して複数の FTD デバイスをアップグレードします。

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 [FTD] タブをクリックします。

ステップ 4 フィルタを使用して、一括アップグレードに含めるデバイスのリストを絞り込みます。

ステップ 5 フィルタ処理されたデバイスのリストから、アップグレードするデバイスを選択します。

ステップ 6 [デバイスアクション（Device Actions）] ペインで、[アップグレード（Upgrade）] をクリックします。

ステップ 7 [デバイスの一括アップグレード（Bulk Device Upgrade）] ページに、アップグレード可能なデバイスが表示されます。選択したどのデバイスもアップグレードできない場合、CDO にはアップグレードできないデバイスのリンクが表示されます。

ステップ 8 後でCDOにアップグレードを実行させる場合は、[アップグレードのスケジュール設定（Schedule Upgrade）]チェックボックスをオンにします。フィールドをクリックして、将来の日時を選択します。日時の選択が完了したら、[アップグレードのスケジュール設定（Schedule Upgrade）] ボタンをクリックします。

ステップ 9 手順 1 で、[イメージURLの指定（Specify Image URL）] をクリックしてアップグレードするソフトウェアイメージを選択し、[続行（Continue）] をクリックします。

ステップ 10 手順2で、選択内容を確認し、デバイスへのイメージのダウンロードのみを実行するか、それともイメージをコピーしてインストールしデバイスを再起動するかを決定します。

ステップ 11 準備ができたら、[アップグレードの実行（Perform Upgrade）]をクリックします。[インベントリ（Inventory）] ページで、アップグレード中のデバイスの設定ステータスが「アップグレード中（Upgrade in Progress）」になります。

警告 アップグレードの進行中にアップグレードをキャンセルする場合は、[アップグレード（Upgrade）] ページで [アップグレードの中止（Abort Upgrade）] をクリックします。アップグレードの開始後にアップグレードをキャンセルすると、CDO はデバイスからの変更を展開したり変更に関してポーリングしたりせず、デバイスは以前の設定にロールバックしません。その結果、デバイスが異常な状態になる場合があります。アップグレードの過程で何らかの問題が発生した場合は、Cisco TAC までお問い合わせください。

ステップ 12 [通知（notifications）] タブで一括アップグレードアクションの進行状況を確認します。managing-ftd-with-cisco-defense-orchestrator_chapter4.pdf#nameddest=unique_194 unique_194_Connect_42_notificationtab一括アップグレードジョブのアクションがどのように成功または失敗したかについての詳細な情報が必要な場合は、青い[確認（Review）] リンクをクリックすると、[ジョブ（Jobs）] ページに移動します。

ステップ 13 システムデータベースをアップグレードします。この手順をFDMで実行する必要があります。詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』、バージョン 6.4 の「Updating System Databases」を参照してください。

一括アップグレードプロセスの監視

[インベントリ（Inventory）]ページでデバイスを選択してアップグレードボタンをクリックすると、一括アップグレードに含まれていた単一のデバイスでの進行状況を表示できます。ナビゲーションウィンドウで[ジョブ（Jobs）]をクリックして一括操作を展開しても、進行状況の詳細を表示できます。

いずれかの時点でアップグレードが失敗すると、CDO からメッセージが表示されます。CDO は、アップグレードプロセスを自動的に再開しません。

FTD ハイアベイラビリティペアのアップグレード

スタンバイデバイスが、セカンダリデバイスがアップグレードされている間もトラフィック検出を処理し続けるため、トラフィックを中断することなく HA ペアをアップグレードします。

HA ペアをアップグレードすると、CDO は適格性チェックを実行し、アップグレードを開始する前にイメージの場所をコピーまたは識別します。ハイ アベイラビリティ ペアのセカンダリデバイスは、それが現在アクティブなデバイスであっても、最初にアップグレードされます。セカンダリデバイスがアクティブなデバイスの場合、ペアリングされたデバイスはアップグレードプロセスの役割を自動的に切り替えます。セカンダリデバイスが正常にアップグレードされたら、デバイスの役割が切り替わり、新しいスタンバイデバイスがアップグレードされます。アップグレードが完了すると、プライマリデバイスがアクティブになり、セカンダリデバイスがスタンバイになるように、デバイスが自動的に構成されます。

アップグレードプロセス中に HA ペアに展開することはお勧めしません。

はじめる前に

- アップグレードする前に、保留中のすべての変更をアクティブなデバイスに展開します。
- アップグレード中に実行されるタスクがないことを確認します。
- HA ペアの両方のデバイスが正常で、
- アップグレードする準備ができていることを確認します。CDO で以前のバージョンにロールバックすることはできません。
- 「FTD アップグレードの前提条件」、「Firepower Threat Defense ソフトウェアのアップグレードパス」、および「CDO がサポートするソフトウェアとハードウェア」を読み、アップグレードプロセス中に発生する可能性のある要件と警告を確認します。

CDO のリポジトリからのイメージを使用した FTD HA ペアのアップグレード

CDO のリポジトリに保存されているソフトウェアイメージを使用して FTD HA ペアをアップグレードするには、以下の手順を実行します。

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 [FTD] タブをクリックします。

ステップ 4 アップグレードする HA ペアを選択します。

ステップ 5 [デバイスアクション（Device Actions）] ペインで、[アップグレード（Upgrade）] をクリックします。

ステップ 6 手順 1 で、[CDO イメージリポジトリの使用（Use CDO Image Repository]）] をクリックしてアップグレードするソフトウェアイメージを選択し、[続行（Continue）] をクリックします。アップグレード可能なデバイス互換性のある選択肢のみが表示されます。

ステップ 7 手順2で、選択内容を確認し、デバイスへのイメージのダウンロードのみを実行するか、それともイメージをコピーしてインストールしデバイスを再起動するかを決定します。

ステップ 8 準備ができたら、[アップグレードの実行（Perform Upgrade）] をクリックします。[インベントリ（Inventory）] ページで、アップグレード中のデバイスの設定ステータスが「アップグレード中（Upgrade in Progress）」になります。

警告 アップグレードの進行中にアップグレードをキャンセルする場合は、[アップグレード（Upgrade）] ページで [アップグレードの中止（Abort Upgrade）] をクリックします。開始後にアップグレードをキャンセルすると、CDO はデバイスからの変更を展開したり、ポーリングしたりせず、デバイスは以前の設定にロールバックしません。その結果、デバイスが異常な状態になる場合があります。アップグレードの過程で何らかの問題が発生した場合は、Cisco TAC までお問い合わせください。

ステップ 9 後でCDOにアップグレードを実行させる場合は、[アップグレードのスケジュール設定（Schedule Upgrade）]チェックボックスをオンにします。フィールドをクリックして、将来の日時を選択します。日時の選択が完了したら、[アップグレードのスケジュール設定（Schedule Upgrade）] ボタンをクリックします。

ステップ 10 [通知（notifications）] タブで一括アップグレードアクションの進行状況を確認します。managing-ftd-with-cisco-defense-orchestrator_chapter4.pdf#nameddest=unique_194 unique_194_Connect_42_notificationtab一括アップグレードジョブのアクションがどのように成功または失敗したかについての詳細な情報が必要な場合は、青色の [レビュー（Review）] リンクをクリックして [ジョブ（Jobs）] ページに移動します。[ジョブ（Jobs）] ページ

ステップ 11 システムデータベースをアップグレードします。この手順をFDMで実行する必要があります。詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』、バージョン 6.4 の「Updating System Databases」を参照してください。

独自のリポジトリからのイメージを使用した FTD HA ペアのアップグレード

ソフトウェアイメージを見つけるための URL プロトコルを使用して FTD HA ペアをアップグレードするには、次の手順を実行します。

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 [FTD] タブをクリックします。

ステップ 4 アップグレードする HA ペアを選択します。

ステップ 5 [デバイスアクション（Device Actions）] ペインで、[アップグレード（Upgrade）] をクリックします。

ステップ 6 手順 1 で、[イメージURLの指定（Specify Image URL）] をクリックしてアップグレードするソフトウェアイメージを選択し、[続行（Continue）] をクリックします。アップグレード可能なデバイス互換性のある選択肢のみが表示されます。

ステップ 7 手順 2 で、選択内容を確認し、デバイスへのイメージのダウンロードのみを実行するか、それともイメージをコピーしてインストールしデバイスを再起動するかを決定します。

ステップ 8 準備ができたら、[アップグレードの実行（Perform Upgrade）] をクリックします。[インベントリ（Inventory）] ページで、アップグレード中のデバイスの設定ステータスが「アップグレード中（Upgrade in Progress）」になります。

警告 アップグレードの進行中にアップグレードをキャンセルする場合は、[アップグレード（Upgrade）] ページで [アップグレードの中止（Abort Upgrade）] をクリックします。開始後にアップグレードをキャンセルすると、CDO はデバイスからの変更を展開したり、ポーリングしたりせず、デバイスは以前の設定にロールバックしません。その結果、デバイスが異常な状態になる場合があります。アップグレードの過程で何らかの問題が発生した場合は、Cisco TAC までお問い合わせください。

ステップ 9 後でCDOにアップグレードを実行させる場合は、[アップグレードのスケジュール設定（Schedule Upgrade）] チェックボックスをオンにします。フィールドをクリックして、将来の日時を選択します。日時の選択が完了したら、[アップグレードのスケジュール設定（Schedule Upgrade）] ボタンをクリックします。

ステップ 10 [通知（notifications）] タブで一括アップグレードアクションの進行状況を確認します。managing-ftd-with-cisco-defense-orchestrator_chapter4.pdf#nameddest=unique_194 unique_194_Connect_42_notificationtab一括アップグレードジョブのアクションがどのように成功または失敗したかについての詳細な情報が必要な場合は、青色の [レビュー（Review）] リンクをクリックして [ジョブ（Jobs）] ページに移動します。[ジョブ（Jobs）] ページ

ステップ 11 システムデータベースをアップグレードします。この手順をFDMで実行する必要があります。詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』、バージョン 6.4 の「Updating System Databases」を参照してください。

アップグレードプロセスの監視

単一のデバイスの進行状況を表示するには、[インベントリ（Inventory）] ページでそのデバイスを選択し、[アップグレード（Upgrade）] ボタンをクリックします。CDOに、該当するデバイスの [デバイスのアップグレード（Device Upgrade）] ページが表示されます。

アップグレードの間、システムライブラリの更新中（自動展開を含む）に HA が一時停止され、アップグレードプロセス全体が正常な状態ではないことがあります。これは予想どおりの結果です。このプロセスの最後の部分で、デバイスは SSH 接続が可能になるため、アップグレードの適用後すぐにログインすると、HA が一時停止ステータスになっている場合があります。アップグレードプロセス中にシステムで問題が発生し、HA ペアが一時停止しているように見える場合は、アクティブデバイスの FDM コンソールから手動で HA を再開します。

（注） いずれかの時点でアップグレードが失敗すると、CDO からメッセージが表示されます。CDO は、アップグレードプロセスを自動的に再開しません。

警告 自己署名証明書を持つデバイスをアップグレードすると、問題が発生する可能性があります。詳細については、「新しい証明書の検出」を参照してください。

Snort 3.0 へのアップグレード

Snort 3 は、最新の Snort エンジン、つまりオープンソースの侵入防御システム（IPS）を使用する強力なプリプロセッサであり、Firepower バージョン 6.7 以降で使用できます。Snort エンジンは、悪意のあるネットワークアクティビティを定義するのに役立つ一連のルールを使用して、ルールに一致するパケットを見つけ、ユーザーに対してアラートを生成します。Snort エンジンは、パケットスニファ、パケットロガー、またはより従来型のスタンドアロンネットワーク IPS として使用するのに適しています。

Snort 3 では、カスタム侵入ポリシーの作成が可能で、Snort 3 を実行するすべての FTD には、シスコの Talos Intelligence Group（Talos）が事前定義した一連の侵入ポリシーがあります。Snort 3 ではこれらのデフォルトポリシーを変更できますが、より堅牢なポリシーに対するベースの上に構築することを強くお勧めします。

Snort 2 ではカスタムポリシーは作成できません。

Snort 2 から Snort 3 への切り替え

Snort のバージョンは自由に切り替えられますが、Snort 2.0 の一部の侵入ルールは Snort 3.0 に存在しない場合があります（その逆もあります）。既存ルールのルールアクションを変更した場合、Snort 3 に切り替えてから Snort 2 に戻るか、または再度 Snort 3 に戻った場合、変更は保持されません。両方のバージョンに存在するルールのルールアクションに対する変更は保持されます。Snort 3 と Snort 2 のルール間マッピングは 1 対 1 または 1 対多にすることができるため、変更の保存はベストエフォートベースで行われることに注意してください。

Snort 2 から Snort 3 へのアップグレードを選択した場合、Snort エンジンのアップグレードはシステムアップグレードと同等であることに注意してください。ネットワークのトラフィックモニタリングの中断を最小限に抑えるために、メンテナンス時間中にアップグレードすることを強くお勧めします。Snort バージョンの切り替えがルールのトラフィック処理にどのように影響するかについては、*Firepower Device Manager* 設定ガイド [英語] の「Managing Intrusion Policies (Snort3)」を参照してください。https://www.cisco.com/c/en/us/td/docs/security/firepower/670/fdm/fptd-fdm-config-guide-670/fptd-fdm-intrusion.html#Cisco_Task_in_List_GUI.dita_9a2ed29f-0ef8-47bf-ac36-2f183fd2b055

ヒント [インベントリ（Inventory）] ページでは Snort バージョンでフィルタリングできます。選択したデバイスの [詳細（Details）] ウィンドウには、デバイスで実行されている現在のバージョンが表示されます。

Snort 3 の制限事項

ライセンス要件

Snort エンジンが侵入およびマルウェア分析のトラフィックを処理できるようにするには、FTD に対して**脅威ライセンス**を有効にする必要があります。FDM を介して脅威ライセンスを有効にするには、FDM UI にログインし、**[デバイス（Device）]** > **[設定の表示（View Configuration）]** > **[有効化/無効化（Enable/Disable）]** に移動し、脅威ライセンスを有効にします。

ハードウェア サポート

次のデバイスは Snort 3 をサポートしています。

- FTD 1000 シリーズ
- FTD 2100 シリーズ
- FTD 4100 シリーズ
- AWS を搭載した FTD 仮想
- AWS を搭載した FTD 仮想
- FTD を搭載した ASA 5500-X シリーズ

ソフトウェアサポート

デバイスは、少なくとも FTD バージョン 6.7 を実行している必要があります。CDO は、バージョン 6.7 以降を実行しているデバイスの Snort 3 機能をサポートします。

FTD 1000 および 2000 シリーズの場合、FXOS パッチサポートの詳細については、「FXOS bundled support」を参照してください。

設定の制限

デバイスに次の設定がある場合、CDO は Snort 3 へのアップグレードをサポートしません。

- デバイスがバージョン 6.7 以降を実行していない。
- デバイスに保留中の変更がある場合。アップグレードする前に変更を展開します。
- デバイスが現在アップグレード中の場合。デバイスが同期されるまで、デバイスへのアップグレードや展開を試みないでください。
- デバイスが仮想ルータで設定されている場合。

（注） Snort のバージョンをアップグレードまたは元に戻すと、Snort 2 侵入ポリシーと Snort 3 侵入ポリシー間の変更を実装するために自動的に展開されます。

ルールセットと Snort 3

現時点では、Snort 3 は完全な機能をサポートしていないことに注意してください。CDO ルールセットは Snort 3 デバイスではサポートされていません。デバイスを FTD 6.7 以降にアップグレードし、同時に Snort 2 から Snort 3 にアップグレードする場合、アップグレード前に設定されたルールセットはすべて分割され、ルールは個別のルールとして保存されます。

Snort 3 用に設定されたデバイスに関するルールセットサポートの完全なリストについては、FTD ルールセットを参照してください。

デバイスと侵入防御エンジンの同時アップグレード

CDO では、デバイスをバージョン 6.7 および Snort 3 にアップグレードできます。FTD システムをアップグレードするには以下の手順を実行します。

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックし、アップグレードする 1 つまたは複数のデバイスを選択します。

ステップ 4 右側にある [デバイスアクション（Device Actions）] ペインで、[アップグレード（Upgrade）] をクリックします。

ステップ 5 アップグレードの切り替えを [FTD システムアップグレード（FTD System Upgrade）] に設定します。

ステップ 6 （オプション）後でCDOにアップグレードを実行させる場合は、[アップグレードのスケジュール設定（Schedule Upgrade）]チェックボックスをオンにします。フィールドをクリックして、将来の日時を選択します。

ステップ 7 手順 1 でアップグレード方法を選択します。CDO イメージリポジトリか自分のリポジトリのイメージを使用します。

- [CDO イメージリポジトリの使用（Use CDO Image Repository]）] - このオプションをクリックしてアップグレードするソフトウェアイメージを選択し、[続行（Continue）] をクリックします。アップグレード可能なデバイス互換性のある選択肢のみが表示されます。
- [イメージ URL の指定（Specify Image URL）] - このオプションをクリックして現在自分のリポジトリに保存されているソフトウェアイメージを選択し、[続行（Continue）]をクリックします。アップグレード可能なデバイス互換性のある選択肢のみが表示されます。

ステップ 8 手順2で、選択内容を確認し、デバイスへのイメージのダウンロードのみを実行するか、それともイメージをコピーしてインストールしデバイスを再起動するかを決定します。

ステップ 9 [Snort 3 エンジンへのアップグレード（Upgrade to Snort 3 Engine）] をチェックします。

ステップ 10 準備ができたら、[アップグレードの実行（Perform Upgrade）]をクリックします。[インベントリ（Inventory）] ページで、アップグレード中のデバイスの設定ステータスが「アップグレード中（Upgrade in Progress）」になります。

警告 アップグレードの進行中にアップグレードをキャンセルする場合は、[アップグレード（Upgrade）] ページで [アップグレードの中止（Abort Upgrade）] をクリックします。開始後にアップグレードをキャンセルすると、CDO はデバイスからの変更をチェックしたり、展開したりせず、デバイスは以前の設定にロールバックしません。その結果、デバイスが異常な状態になる場合があります。アップグレードの過程で何らかの問題が発生した場合は、Cisco TAC までお問い合わせください。

侵入防御エンジンのアップグレード

Snort 2 でバージョン 6.7 を既に実行しているデバイスの場合、次の手順を使用して、Snort エンジンのみをバージョン 3 に更新します。

手順

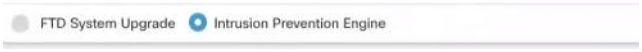
ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

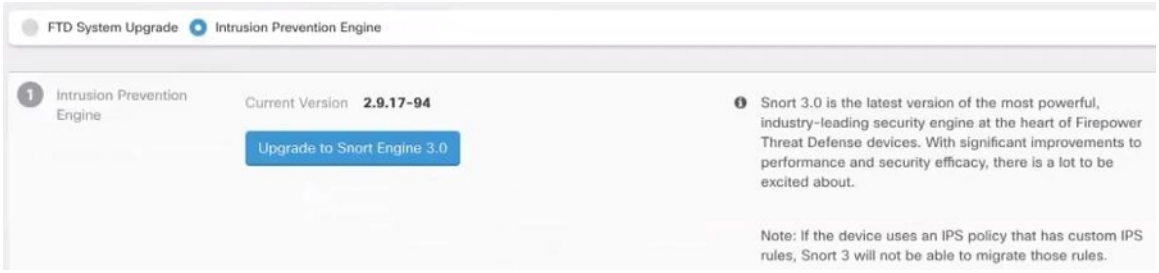
ステップ 3 [FTD] タブをクリックし、アップグレードする 1 つまたは複数のデバイスを選択します。

ステップ 4 右側にある [デバイスアクション（Device Actions）] ペインで、[アップグレード（Upgrade）] をクリックします。

ステップ 5 アップグレードトグルを [侵入防御エンジン（Intrusion Prevention Engine）] に切り替えます。



ステップ 6 [Snort 3.0へのアップグレード（Upgrade to Snort 3.0）] をクリックします。



ステップ 7 [インベントリ（Inventory）]ページで、アップグレード中のデバイスの設定ステータスが「アップグレード中（Upgrade in Progress）」になります。

アップグレードプロセスの監視

警告 アップグレードの進行中にアップグレードをキャンセルする場合は、[アップグレード（Upgrade）]ページで[アップグレードの中止（Abort Upgrade）]をクリックします。開始後にアップグレードをキャンセルすると、CDO はデバイスからの変更をチェックしたり、展開したりせず、デバイスは以前の設定にロールバックしません。その結果、デバイスが異常な状態になる場合があります。アップグレードの過程で何らかの問題が発生した場合は、Cisco TAC までお問い合わせください。

単一のデバイスの進行状況を表示するには、[インベントリ（Inventory）] ページでそのデバイスを選択し、[アップグレード（Upgrade）] ボタンをクリックします。CDOに、該当するデバイスの [デバイスのアップグレード（Device Upgrade）] ページが表示されます。

いずれかの時点でアップグレードが失敗すると、CDO からメッセージが表示されます。CDO は、アップグレードプロセスを自動的に再開しません。

警告 自己署名証明書を持つデバイスをアップグレードすると、問題が発生する可能性があります。詳細については、「新しい証明書の検出」を参照してください。

FTD の Snort 3.0 からの復元

Snort 2.0 の一部の侵入ルールは Snort 3.0 には存在しない場合があります。2.0 にダウングレードすると、作成したカスタム侵入ポリシーはすべて、カスタムポリシーで使用される基本ポリ

シーに変換されます。可能なかぎり、ルール アクション オーバーライドは保持されます。複数のカスタムポリシーが同じ基本ポリシーを使用する場合は、最も多くのアクセス制御ポリシーで使用されるカスタムポリシーのオーバーライドが保持され、その他のカスタムポリシーのオーバーライドは失われます。これらの「重複」ポリシーを使用していたアクセス制御ルールは、最もよく使用されるカスタムポリシーから作成された基本ポリシーを使用するようになります。すべてのカスタムポリシーが削除されます。

Snort 3.0 からの復帰を選択する前に、『*Firepower Device Manager* コンフィギュレーションガイド』の「侵入ポリシーの管理（Snort2）」を読み、snortエンジンのバージョンの切り替えが現在のルールとポリシーにどのように影響するかを確認してください。

（注） バージョン2に戻しても、Firepower ソフトウェアバージョンはアンインストールされません。

Snort 3.0 からの復元

Snort バージョンを変更すると、システムは自動展開を実行して変更を実装します。Snort 3.0 からバージョン 2 に戻すことができるのは個々のデバイスのみであることに注意してください。

侵入防御エンジンを元に戻すには、次の手順を使用します。

手順

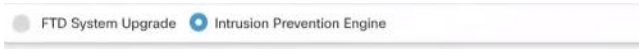
ステップ 1 ナビゲーションウィンドウで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

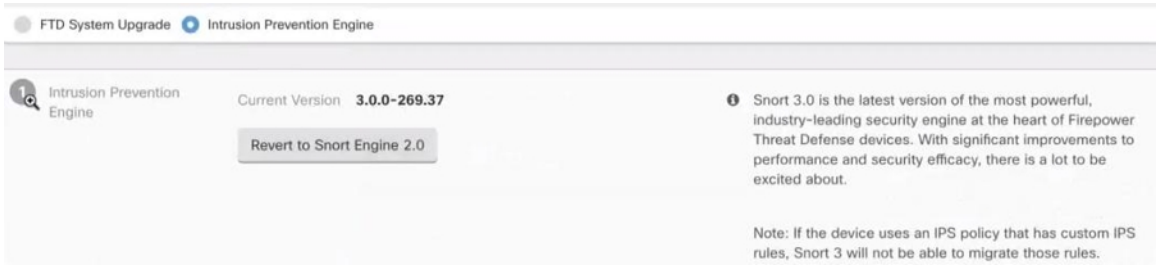
ステップ 3 [FTD] タブをクリックし、元に戻すデバイスをクリックします。

ステップ 4 右側にある [デバイスアクション（Device Actions）] ペインで、[アップグレード（Upgrade）] をクリックします。

ステップ 5 アップグレードトグルを [侵入防御エンジン（Intrusion Prevention Engine）] に切り替えます。



ステップ 6 ステップ 1 で、Snort バージョン 3 から元に戻すことを確認し、[Snortエンジン2に戻す（Revert to Snort Engine 2）] をクリックします。



ステップ 7 [インベントリ（Inventory）]ページで、アップグレード中のデバイスの設定ステータスが「アップグレード中（Upgrade in Progress）」になります。

セキュリティデータベース更新のスケジュール設定

次の手順を使用して、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されたタスクを作成します。

手順

ステップ 1 ナビゲーションウィンドウで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックし、目的の FTD デバイスを選択します。

ステップ 4 [アクション（Actions）] ペインで、[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、追加ボタン [+] をクリックします。

（注） 選択したデバイスに既存のスケジュールされたタスクがある場合は、編集アイコンをクリックして新しいタスクを作成します。新しいタスクを作成すると、既存のタスクが上書きされます。

ステップ 5 スケジュールされたタスクを次のように設定します。

- [頻度（Frequency）]：日次、週次、または 月次から更新の頻度を選択します。
- [時刻（Time）]：時刻を選択します。時刻はUTC で表示されることに注意してください。
- [曜日の選択（Select Days）]：更新を実行する曜日を選択します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 デバイスの [設定ステータス（Configuration Status）] が [データベースの更新中（Updating Databases）] に変わります。

セキュリティデータベースの更新スケジュールの編集

次の手順を使用して、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、既存のスケジュールされたタスクを編集します。

手順

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックし、目的の FTD デバイスを選択します。

ステップ 4 [操作（Actions）] ウィンドウで、[データベースの更新（Database Updates）] セクションを見つけて、編集アイコンをクリックします。

ステップ 5 次の項目を使用して、スケジュールされたタスクを編集します。

- [頻度（Frequency）]：日次、週次、または 月次から更新の頻度を選択します。
- [時刻（Time）]：時刻を選択します。時刻はUTC で表示されることに注意してください。
- [曜日の選択（Select Days）]：更新を実行する曜日を選択します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 デバイスの [設定ステータス（Configuration Status）] が [データベースの更新中（Updating Databases）] に変わります。