CDOおよびロータッチプロビジョニングを使用したFirepower Threat Defenseの展開

この章の対象読者

ロータッチプロビジョニング（LTP）は、新しいFirepower Threat Defense（FTD）デバイスのCisco Defense Orchestrator（CDO）への導入準備を簡素化し、自動化します。LTPにより、新しいFirepowerデバイスの導入が簡素化されます。ネットワーク管理者が、支社に直接デバイスを配信し、デバイスをCDOクラウドベースのデバイスマネージャに追加し、FTDデバイスがCisco Cloudに正常に接続された後でデバイスを管理できるようになるからです。

この章では、ロータッチプロビジョニングを使用して、FirepowerデバイスをCDOに導入準備する方法について説明します。CDOは、一貫性のあるポリシーの実装を実現するために高度に分散された環境でセキュリティポリシーの管理を容易にするクラウドベースのマルチデバイスマネージャです。CDOは、セキュリティポリシーとの不整合を特定して修正するためのツールを提供することで、セキュリティポリシーを最適化します。CDOは、オブジェクトとポリシーを共有し、設定テンプレートを作成して、デバイス間でポリシーの一貫性を促進する方法を提供します。

（注） この機能を利用するには、Firepowerバージョン6.7以降が必要です。

（注） このドキュメントでは、Firepower 2100ハードウェアにFTDイメージが事前にインストールされていることを前提としています。Firepower 1100ハードウェアでは、FTDソフトウェアまたはASAソフトウェアを実行できます。FTDとASAの間で切り替えを行う際には、デバイスの再イメージ化が必要になります。「Cisco ASA および Firepower Threat Defense 再イメージ化ガイド」を参照してください。

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

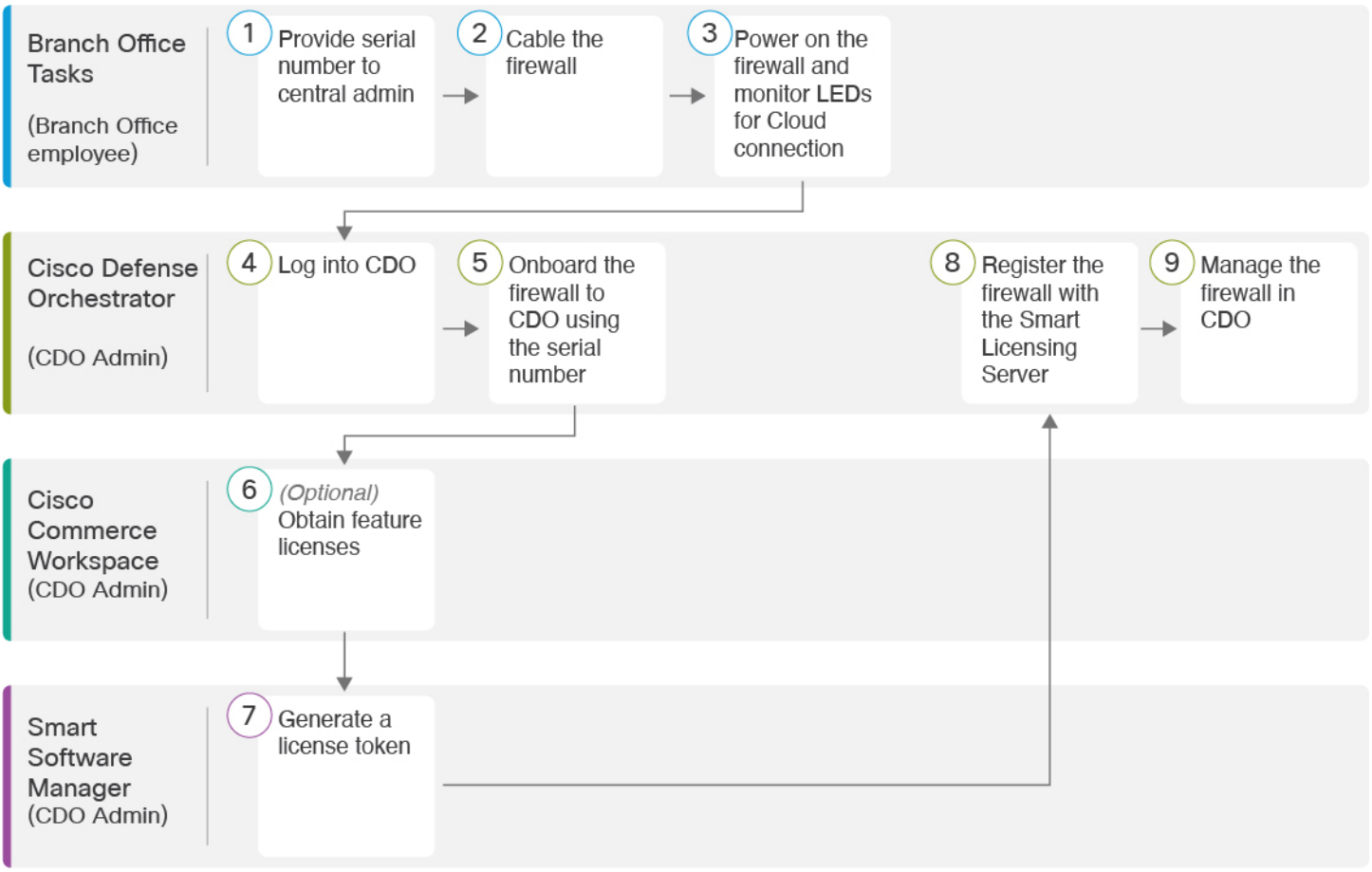
（注） **プライバシー収集ステートメント**：Firepower 2100 シリーズには個人識別情報は不要で、積極的に収集することもありません。ただし、ユーザ名などの設定では、個人識別情報を使用できます。この場合、設定作業時やSNMPの使用時に、管理者が個人識別情報を確認できる場合があります。

エンドツーエンドの手順

この章では、ロータッチプロビジョニング機能を使用して、工場出荷時のデフォルトの FTD 1010 デバイスをリモートの支社に展開する方法について説明します。

1. 支社は、シスコから直接出荷されたか、FTD 6.7+ ソフトウェアで再イメージ化された FTD 6.7+ デバイスを受け取ります。
2. 本社の管理者が、デバイスのシリアル番号を使用してデバイスを CDO に導入準備します。
3. 支社の従業員が、FTD をケーブルで接続して電源をオンにします。
4. 本社の管理者が、CDO を使用して FTD の導入準備と設定を完了します。

ロータッチプロビジョニングを使用してシャーシに CDO を使用した FTD を展開するには、次のタスクを参照してください。



1	支社のタスク （支社の従業員）	デバイスが支社からのロータッチプロビジョニングをサポートしていることを確認する （4 ページ）：企業の IT 部門またはマネージド サービス プロバイダーからデバイスを受け取ります。
2	支社のタスク （支社の従業員）	デバイスが支社からのロータッチプロビジョニングをサポートしていることを確認する （4 ページ）：デバイスとパッケージのインベントリを作成し、シリアル番号を記録します。
3	Cisco Defense Orchestrator （CDO 管理者）	Cisco Secure Sign-On を使用した CDO へのログイン （9 ページ）。
4	Cisco Defense Orchestrator （CDO 管理者）	ロータッチプロビジョニングとシリアル番号を使用したデバイスの導入準備 （10 ページ）。
5	支社のタスク （支社の従業員）	デバイスの配線 （12 ページ）。

6	支社のタスク （支社の従業員）	デバイスの電源投入 （13 ページ）：電源コードをデバイスに接続し、電源コンセントに接続します。
7	Cisco Cloud	デバイスの電源投入 （13 ページ）：デバイスのステータス LED で Cisco クラウドへの接続を確認します。
8	Cisco Defense Orchestrator （CDO 管理者）	CDO を使用したデバイスの管理 （20 ページ）。
9	Smart Software Manager （CDO 管理者）	ライセンスの設定 （15 ページ）：オプションで、デバイスをスマート ライセンシング サーバに登録します。あるいは、引き続き 90 日間の評価ライセンスを使用します。
10	Cisco Commerce Workspace （CDO 管理者）	ライセンスの設定 （15 ページ）：オプションで、ライセンストークンを生成します。

支社：デバイスの受け取り

企業の IT 部門から FTD を受け取ったら、デバイスのシリアル番号を記録して、CDO 管理者に送信する必要があります。導入準備プロセスのコミュニケーション計画の概要を示します。完了する主要なタスクを盛り込み、項目ごとに連絡窓口を提供します。

ヒント　このビデオを視聴すると、支社の従業員が CDO とロータッチプロビジョニングを使用して Firepower デバイスを導入準備する方法を確認できます。

デバイスが支社からのロータッチプロビジョニングをサポートしていることを確認する

デバイスをラックに設置する前、または配送ボックスを廃棄する前に、ロータッチプロビジョニングを使用して Firepower デバイスを展開できることを確認します。

（注）　この手順は、FTD バージョン 6.7 以降を実行している新しい Firepower デバイスを使用していることを前提としています。

始める前に

- シャーシとシャーシコンポーネントを開梱します。

- ケーブルを接続する前、またはデバイスの電源をオンにする前に、Firepower デバイスとパッケージのインベントリを確認します。
- IT 部門では、デバイスに接続してリモートで管理するために、デバイスのシリアル番号が必要になります。
- シャーシのレイアウト、コンポーネント、および LED についても理解しておく必要があります。

手順

ステップ 1 配送ボックスの製品 ID（PID）を確認します。デバイスの出荷に使用したダンボール箱には、Firepower ソフトウェアの出荷バージョン（6.7 以降）を示す白い無地のステッカーが付いています。

PID は、Firepower 2100 シリーズの PID の例（SF-F2K-TD6.7-K9）と同じである必要があります。

ステップ 2 デバイスのシリアル番号を記録します。デバイスのシリアル番号は、配送ボックスに記載されています。また、デバイス前面の引き出しタブにあるステッカーにも記載されています。

ステップ 3 デバイスのシリアル番号を IT 部門/本社の CDO ネットワーク管理者に送信します。

（注） ネットワーク管理者は、ロータッチプロビジョニングを容易にし、デバイスに接続してリモートで設定するためにデバイスのシリアル番号が必要になります。

次のタスク

IT 部門/本社の CDO 管理者と連絡を取って、導入準備のタイムラインを策定します。次の手順は、ネットワーク管理者がデバイスを CDO に導入準備した後でデバイスをケーブルで電源に接続することです。

CDO 管理者：本社

リモート支社の管理者がシリアル番号情報を本社に送信した後、CDO 管理者が FTD を CDO に導入準備します。

CDO へのログイン

CDOは、Cisco Secure Sign-On をアイデンティティプロバイダーとして使用し、Duo Security を多要素認証（MFA）に使用します。CDO には MFA が必要です。MFA は、ユーザアイデンティティを保護するためのセキュリティを強化します。MFA の一種である二要素認証では、CDO にログインするユーザの ID を確認するために、2 つのコンポーネントまたは要素が必要です。

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

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

- Cisco Secure Sign-On アカウントをお持ちの場合は、Cisco Secure Sign-On を使用した CDO へのログイン （9 ページ）に進みます。
- Cisco Secure Sign-On アカウントがない場合は、新しい Cisco Secure Sign-On アカウントの作成に進んでください。

新しい Cisco Secure Sign-On アカウントの作成

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

始める前に

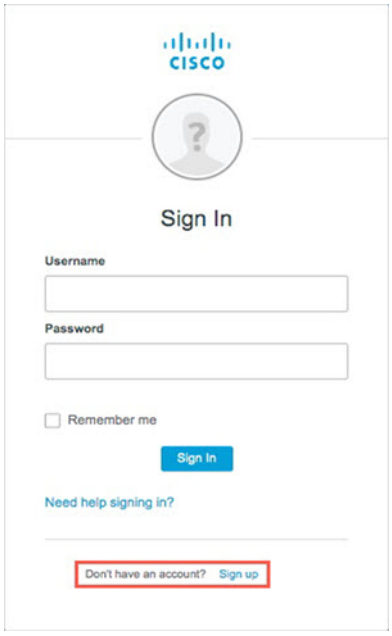
- **DUO Security のインストール**：Duo Security アプリケーションを携帯電話にインストールすることをお勧めします。Duo のインストールについてご質問がある場合は、『Duo Guide to Two Factor Authentication：Enrollment Guide』を参照してください。
- **時刻の同期**：モバイルデバイスを使用してワンタイムパスワードを生成します。OTP は時間ベースであるため、デバイスのクロックがリアルタイムと同期していることが重要です。デバイスのクロックが正しい時刻に設定されていることを確認します。
- Firefox または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

手順

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

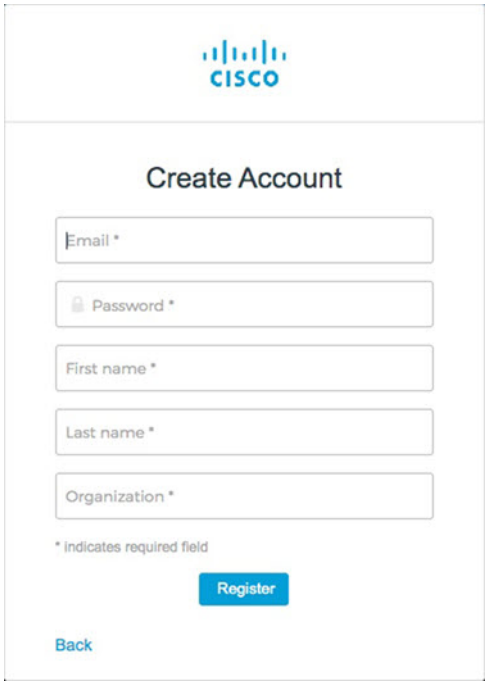
a) https://sign-on.security.cisco.com にアクセスします。
b) [サインイン（Sign In）] 画面の下部にある [サインアップ（Sign up）] をクリックします。

図 *1 : Cisco SSO* へのサインアップ



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

図 *2 :* アカウントの作成（*Create Account*）



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

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

ステップ 2　Duo を使用して多要素認証をセットアップします。

a) [多要素認証の設定（Set up multi-factor authentication）] 画面で、[設定（Configure）] をクリックします。

b) [セットアップの開始（Start setup）]をクリックし、プロンプトに従ってデバイスを選択して、そのデバイスとアカウントのペアリングを確認します。

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

c) ウィザードの最後で、[ログインを続行する（Continue to Login）] をクリックします。

d) 二要素認証を使用して Cisco Secure Sign-On にログインします。

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

a) Googleオーセンティケータとペアリングするモバイルデバイスを選択し、[次へ（Next）] をクリックします。

b) セットアップウィザードのプロンプトに従って、Google オーセンティケータをセットアップします。

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

a) 「パスワードを忘れた場合（forgot password）」の質問と回答を選択します。

b) SMS を使用してアカウントをリセットするための予備の電話番号を選択します。

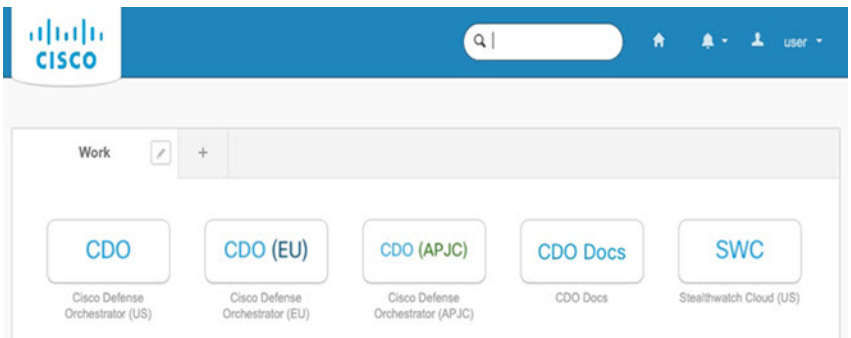
c) セキュリティイメージを選択します。

d) [マイアカウントの作成（Create My Account）] をクリックします。

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

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

図 *3 : Cisco SSO* ダッシュボード



Cisco Secure Sign-On を使用した CDO へのログイン

CDO にログインして FTD をオンボードし、管理します。

始める前に

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

- CDO にログインするには、まず Cisco Secure Sign-On でアカウントを作成し、Duo を使用して MFA を設定する必要があります。新しい Cisco Secure Sign-On アカウントの作成 （6 ページ）を参照してください。
- Firefox または Chrome の最新バージョンを使用します。

手順

ステップ 1 Web ブラウザで、https://sign-on.security.cisco.com/を開きます。

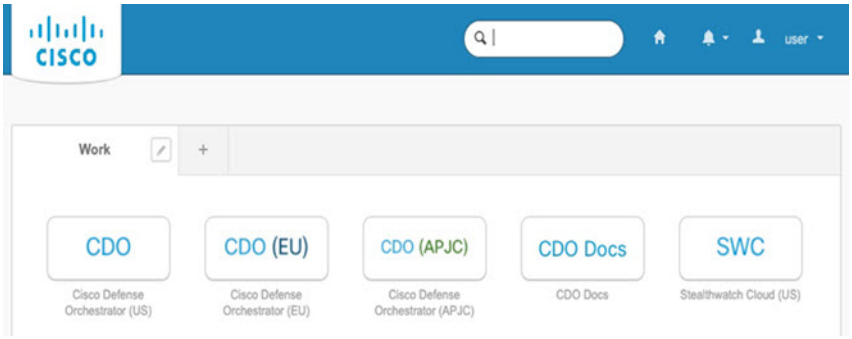
ステップ 2 [ユーザ名（Username）] と [パスワード（Password）] に入力します。

ステップ 3 [ログイン（Log in）] をクリックします。

ステップ 4 Duo Security を使用して別の認証要素を受け取り、ログインを確認します。システムによってログインが確認され、Cisco Secure Sign-On ダッシュボードが表示されます。

ステップ 5 Cisco Secure Sign-on ダッシュボードで適切な CDO タイルをクリックします。**CDO** タイルをクリックすると https://defenseorchestrator.com に移動し、**CDO（EU）**タイルをクリックすると https://defenseorchestrator.eu に移動します。また、**CDO（APJC）**タイルをクリックすると https://www.apj.cdo.cisco.com に移動します。

図 *4 : Cisco SSO* ダッシュボード



ステップ 6 両方のオーセンティケータを設定している場合は、オーセンティケータのロゴをクリックして [Duo Security] か [Google Authenticator] を選択します。

- 既存のテナントにすでにユーザレコードがある場合は、そのテナントにログインします。
- すでに複数のテナントにユーザレコードがある場合は、接続先の CDO テナントを選択できます。

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

ロータッチプロビジョニングとシリアル番号を使用したデバイスの導入準備

LTP を使用して CDO に Firepower デバイスを導入準備するには、この手順を完了し、インターネットに接続できるネットワークにデバイスを接続して、デバイスの電源をオンにします。

始める前に

ロータッチプロビジョニング（LTP）は、工場出荷時の新しい Firepower 2100 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 へのデバイスの導入準備に伴う手動タスクの多くが不要になります。

（注） LTP を使用するには、デバイスにバージョン 6.7 以降がインストールされている必要があります。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 デバイスを導入準備する場合は、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を実行する必要があります。

手順

ステップ 1 ナビゲーションウィンドウで [デバイスとサービス（Devices & Services）] をクリックし、青色のプラスボタンをクリックしてデバイスを [導入準備（Onboard）] します。

ステップ 2 [FTD] カードをクリックします。

（注） 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 3 [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 4 [接続（Connection）] 領域で、次の情報を入力してください。

a) 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、青色の [変更（Change）] リンクをクリックして変更できます。

b) [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。
c) [デバイス名（Device Name）]：デバイスの名前を指定します。

ステップ 5 [Next] をクリックします。

ステップ 6 [パスワードのリセット（Password Reset）] 領域で、次の情報を入力してください。

a) [デフォルトパスワード未変更（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。

- 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。

（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。

b) [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。

ステップ 7 [Next] をクリックします。

ステップ 8 [スマートライセンス（Smart License）] 領域で、必要なオプションのいずれかを選択します。

- [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。

ステップ 9 [Next] をクリックします。

ステップ 10 [サブスクリプションライセンス（Subscription Licenses）] 領域で、次の操作を実行します。

- 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。
- 基本ライセンスのみで続行することもできます。

（注） [スマートライセンス（Smart License）] の手順で [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、ここ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。

ステップ 11 （オプション）[ラベル（Labels）] 領域で、必要に応じてラベル名を入力できます。

ステップ 12 [デバイスとサービスへの移動（Go to Devices and Services）] をクリックします。

次のタスク

デバイスを展開中の支社と連絡を取ります。支社の管理者が FTD にケーブルを接続して電源をオンにしたら、次の手順は導入準備プロセスを完了し、デバイスを設定/管理することです。

支社：デバイスの設置

CDO 管理者が FTD を CDO に導入準備した後、外部インターフェイスからインターネットにアクセスできるように、デバイスにケーブルを接続して電源をオンにする必要があります。これで、CDO 管理者は導入準備プロセスを完了できます。

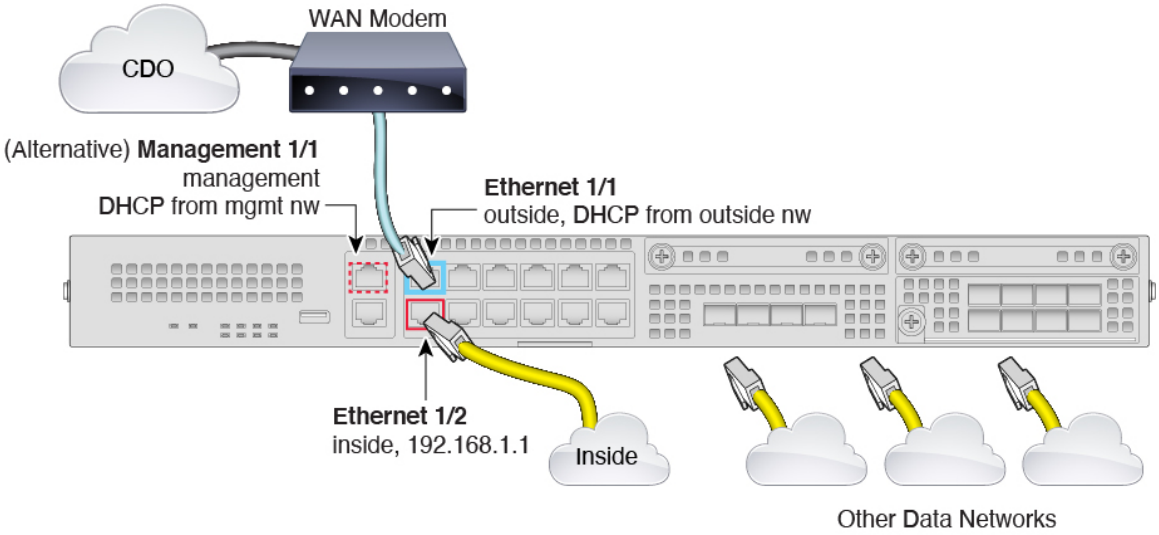
デバイスの配線

このトピックでは、CDO 管理者がリモートで管理できるように Firepower 2100 をネットワークに接続する方法について説明します。

- 支社で Firepower ファイアウォールを受け取ってネットワークに接続することが目的の場合は、このビデオをご覧ください。

  ビデオでは、Firepower デバイスと、デバイスのステータスを示すデバイス上の LED シーケンスについて説明しています。必要に応じて、IT 部門と一緒に LED を見るだけでデバイスのステータスを確認できます。

図 *5 : Firepower 2100* のケーブル配線



ロータッチプロビジョニングは、イーサネット 1/1（外部）での CDO への接続をサポートしています。あるいは、Management 1/1 インターフェイスでロータッチプロビジョニングを使用することもできます。

手順

ステップ 1 イーサネット 1/1 インターフェイスからワイドエリアネットワーク（WAN）モデムにネットワークケーブルを接続します。WAN モデムは、支社からインターネットへの接続であり、Firepower デバイスからインターネットへのルートにもなります。

（注） あるいは、デバイスの Management 1/1 インターフェイスから WAN にネットワークケーブルを接続することもできます。どのインターフェイスを使用する場合でも、インターネットへのルートが必要です。CLI で IP アドレスを手動で設定した場合、管理インターフェイスは IPv6 をサポートします。「（任意）CLI での管理ネットワーク設定の変更」を参照してください。管理インターフェイスで IPv6 を使用するには、IPv4 アドレスも保持または設定してください。IPv6 が機能するには、デュアルスタックが必要です。外部イーサネット 1/1 インターフェイスは、ロータッチプロビジョニング用の IPv4 のみをサポートします。

ステップ 2 内部ネットワークをイーサネット 1/2 に接続します。

ステップ 3 必要に応じて、残りのインターフェイスに他のネットワークを接続します。

デバイスの電源投入

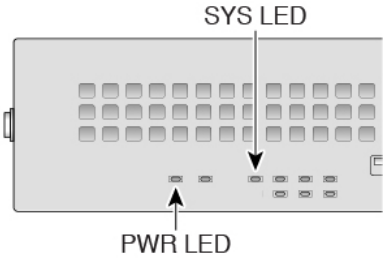
電源スイッチは、シャーシの背面の電源モジュール 1 の左にあります。これはシステムへの電源を制御するトグル スイッチです。電源スイッチがスタンバイの位置にある場合は、3.3 V の

スタンバイ電源ユニットのみが電源モジュールから有効化され、12 V の主電源はオフになります。スイッチがオンの位置にある場合は、12 V の主電源がオンになり、システムが起動します。

始める前に

デバイスに対して信頼性の高い電力を供給することが重要です（たとえば、無停電電源装置（UPS）を使用）。最初のシャットダウンを行わないで電力が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。バックグラウンドでは常に多数のプロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

手順

	コマンドまたはアクション	目的
ステップ 1	電源コードをデバイスに接続し、電源コンセントに接続します。	
ステップ 2	デバイスの背面にある電源スイッチを押します。	
ステップ 3	デバイスの前面にある PWR LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。	
ステップ 4	デバイスの前面にあるステータス LED を確認します。デバイスが正常に起動していると、ステータス LED が緑色にすばやく点滅します。	問題がある場合は、ステータス LED がオレンジ色にすばやく点滅します。この場合は、IT 部門に連絡してください。
ステップ 5	前面のステータス LED を確認します。デバイスが Cisco Cloud に接続すると、ステータス LED が緑色にゆっくりと点滅します。	問題がある場合は、ステータス LED がオレンジ色と緑色に点滅し、デバイスが Cisco Cloud に到達しなかったことになります。この場合は、ネットワークケーブルがイーサネット 1/1 インターフェイスと WAN モデムに接続されていることを確認します。ネットワークケーブルを調整した後、10 分ほど経過してもデバイスが Cisco Cloud に到達しない場合は、IT 部門に連絡してください。

次のタスク

- IT 部門と連絡を取って、導入準備のタイムラインとアクティビティを確認します。本社の CDO 管理者とともにコミュニケーション計画を導入する必要があります。
- このタスクを完了すると、CDO 管理者は Firepower デバイスをリモートから設定および管理できるようになります。これで完了です。

CDO 管理者：導入準備を完了する

シリアル番号を使用して CDO でデバイスを導入準備すると、デバイスは Cisco Cloud の CDO テナントに関連付けられます。支社の管理者が FTD をケーブルで接続して電源をオンにすると、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設定が自動的に同期されます。

これで、CDO を使用してデバイスを設定および管理できます。オプションで、評価ライセンスを使用している場合は、機能ライセンスを取得し、デバイスにライセンスを付与する手順を完了できます。

ライセンスの設定

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

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

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

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

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

始める前に

- Cisco Smart Software Manager にマスター アカウントを持ちます。

まだアカウントをお持ちでない場合は、このリンクをクリックして新しいアカウントをセットアップしてください。Smart Software Manager では、組織のマスター アカウントを作成できます。

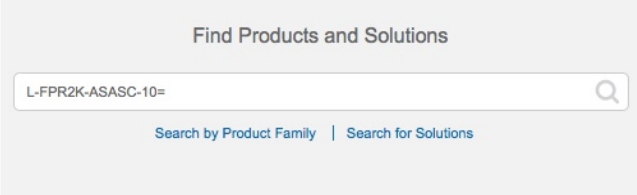
- （輸出コンプライアンス フラグを使用して有効化される）機能を使用するには、ご使用のシスコ スマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。
- CDO にデバイスをオンボードするまでは評価ライセンスを使用します。Smart Software Managerに登録する追加のライセンスは、CDOにオンボードして再登録する前に登録解除する必要があります。

手順

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

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

図 *6:* ライセンス検索



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

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

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-FPR2110T-TMC-1Y
  - L-FPR2110T-TMC-3Y
  - L-FPR2110T-TMC-5Y

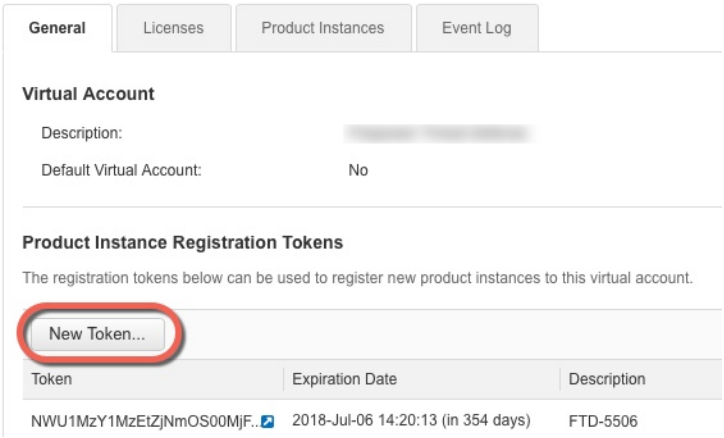
- L-FPR2120T-TMC-1Y
- L-FPR2120T-TMC-3Y
- L-FPR2120T-TMC-5Y
- L-FPR2130T-TMC-1Y
- L-FPR2130T-TMC-3Y
- L-FPR2130T-TMC-5Y
- L-FPR2140T-TMC-1Y
- L-FPR2140T-TMC-3Y
- L-FPR2140T-TMC-5Y

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

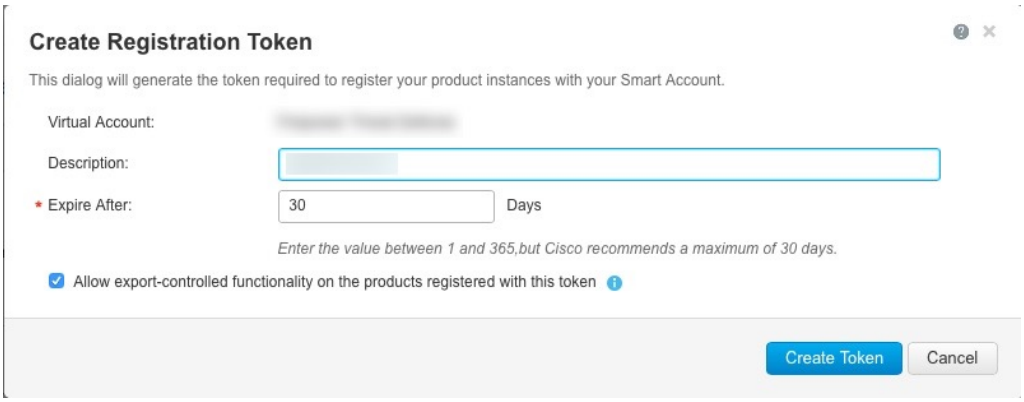
ステップ 2 Smart Software Manager で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

a) [インベントリ（Inventory）] をクリックします。

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



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



- **[説明（Description）]**
- [有効期限（Expire After）]：推奨値は 30 日です。
- [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：高度暗号化が許可されている国の場合は輸出コンプライアンスフラグを有効にします。

トークンはインベントリに追加されます。

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

図 *7*: トークンの表示

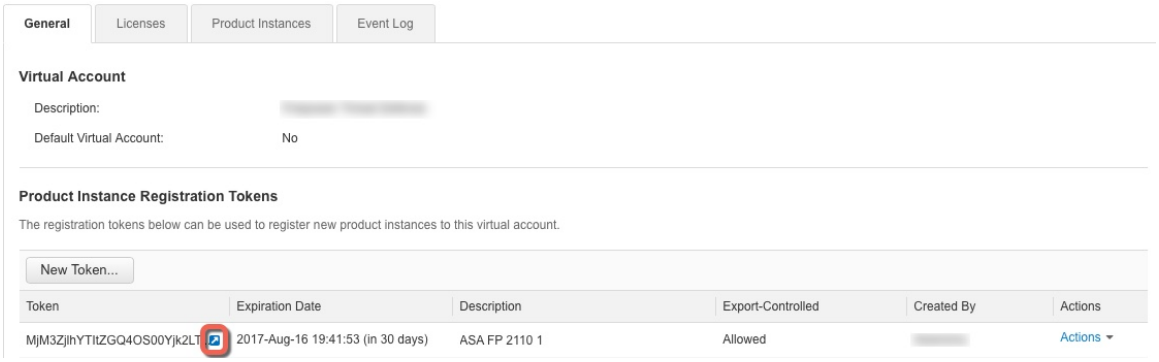
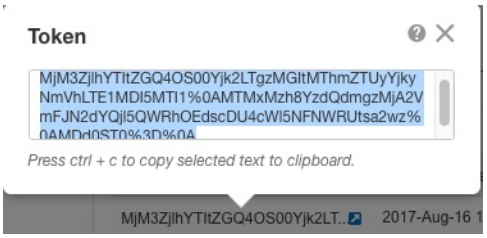


図 *8*: トークンのコピー



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

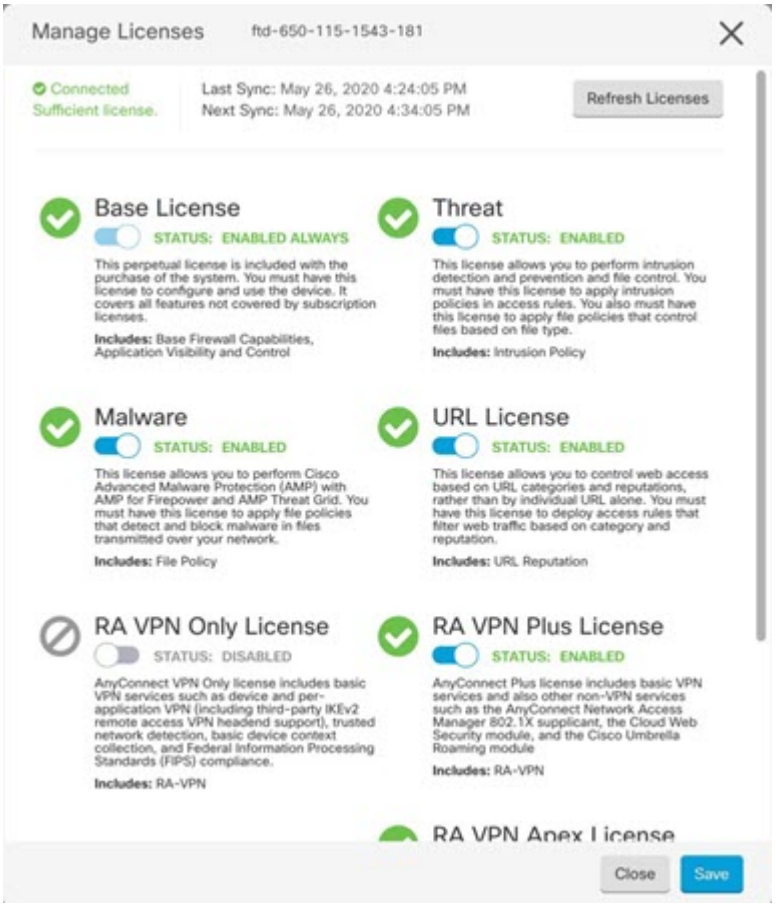
ステップ 4 [デバイスのアクション（Device Actions）] ペインで、[ライセンスの管理（Manage Licenses）] をクリックし、画面の指示に従って Smart Software Manager から生成されたスマートライセンスを入力します。

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

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

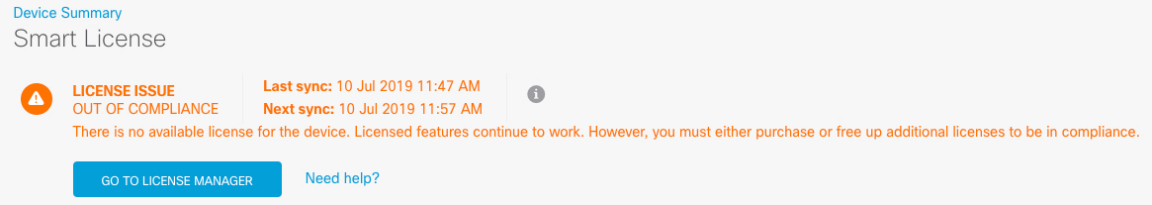
Registration request sent on 10 Jul 2019. Please wait. Normally, it takes about one minute to complete the registration. You can check the task status in Task List. Refresh this page to see the updated status.

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



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

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



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

CDO を使用したデバイスの管理

デバイスを CDO にオンボードした後は、CDO を使用してデバイスを管理できます。CDO で FTD を管理するには、次の手順を実行します。

1. https://sign-on.security.cisco.com にアクセスします。
2. 新しい Cisco Secure Sign-On アカウントの作成で作成したユーザとしてログインします。
3. 一般的な管理タスクへのリンクについては、『Managing FTD with Cisco Defense Orchestrator』を参照してください。

次の作業

これで、FTD デバイスを設定し、CDO にオンボードしました。これにより、FTD デバイスへのシンプルな管理インターフェイスとクラウドアクセスが提供されます。CDO を使用してソフトウェアをアップグレードし、高可用性を設定し、FTD デバイスのデバイス設定とネットワークリソースの設定を行います。