



# リモート Threat Defense による Management Center の展開

## この章の対象読者

使用可能なすべてのアプリケーションとマネージャを表示するには、[最適なアプリケーションとマネージャを見つける方法](#)を参照してください。この章の内容は、Management Center での脅威に対する防御の展開に適用されます。

この章では、中央本社にある Management Center を使用して脅威に対する防御を管理する方法について説明します。Management Center がローカル管理ネットワークに存在するローカル展開については、[Management Center での Threat Defense の展開](#)を参照してください。

## ファイアウォールについて

ハードウェアでは、Threat Defense ソフトウェアまたは ASA ソフトウェアを実行できます。Threat Defense 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。現在インストールされているものとは異なるソフトウェアバージョンが必要な場合も再イメージ化が必要です。[Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド](#)を参照してください。

ファイアウォールは、Secure Firewall eXtensible オペレーティングシステム (FXOS) と呼ばれる基盤となるオペレーティングシステムを実行します。ファイアウォールは FXOS Secure Firewall Chassis Manager をサポートしていません。トラブルシューティング用として限られた CLI のみがサポートされています。詳細については、[Cisco FXOS トラブルシューティングガイド \(Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け\)](#)を参照してください。

**プライバシー収集ステートメント**：ファイアウォールには個人識別情報は不要で、積極的に収集することはありません。ただし、ユーザー名などの設定では、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。

- [リモート管理の仕組み \(2 ページ\)](#)
- [はじめる前に \(6 ページ\)](#)
- [エンドツーエンドのタスク：ゼロタッチプロビジョニング \(6 ページ\)](#)
- [エンドツーエンドのタスク：手動プロビジョニング \(8 ページ\)](#)

- 中央の管理者による事前設定 (10 ページ)
- 支社へのインストール (25 ページ)
- 中央の管理者による事後設定 (27 ページ)

## リモート管理の仕組み

Management Center でインターネットを介して Threat Defense を管理できるようにするには、Management Center マネージャアクセスについて管理インターフェイスの代わりに外部インターフェイスを使用します。ほとんどのリモート支社には1つのインターネット接続しかないため、外部からマネージャにアクセスして中央管理を行えるようにします。



- (注) 管理接続は、それ自身とデバイス間の安全な TLS-1.3 暗号化通信チャネルです。セキュリティ上の理由から、サイト間 VPN などの追加の暗号化トンネル経由でこのトラフィックを実行する必要はありません。たとえば、VPN がダウンすると、管理接続が失われるため、シンプルな管理パスをお勧めします。

### 登録方法

Threat Defense をプロビジョニングするには、次のいずれかの方法を使用します。

#### ゼロ タッチ プロビジョニング (Management Center 7.4 以降、Threat Defense 7.2 以降)

1. 脅威に対する防御をリモート分散拠点に送信します。ゼロタッチプロビジョニングは事前設定済みのデバイスでは機能しない場合があるため、デバイス上では何も設定しないでください。



- (注) デバイスを分散拠点に送信する前に、Threat Defense のシリアル番号を使用して Threat Defense を事前に Management Center に登録できます。Management Center は、この機能のために Cisco Security Cloud および CDO と統合されます。

2. 分散拠点で、Threat Defense をケーブル接続し、電源をオンにします。
3. CDO を使用して Threat Defense の登録を完了します。

#### 手動プロビジョニング

1. CLI または Device Manager を使用して Threat Defense を事前設定してから、リモート分散拠点に Threat Defense を送信します。
2. 分散拠点で、脅威に対する防御をケーブル接続し、電源をオンにします。
3. Management Center を使用して脅威に対する防御の登録を完了します。

## Threat Defense マネージャ アクセス インターフェイス

このガイドでは外部インターフェイスアクセスについて説明します。これは、リモート分散拠点で発生する可能性が最も高いシナリオであるためです。マネージャアクセスは外部インターフェイスで発生しますが、専用の管理インターフェイスも引き続き関連します。管理インターフェイスは、Threat Defense データインターフェイスとは別に設定される特別なインターフェイスであり、独自のネットワーク設定があります。

- データインターフェイスでマネージャアクセスを有効にした場合でも、管理インターフェイスのネットワーク設定が使用されます。
- すべての管理トラフィックは、引き続き管理インターフェイスを発信元または宛先とします。
- データインターフェイスでマネージャアクセスを有効にすると、Threat Defense はバックプレーンを介して管理インターフェイスに着信管理トラフィックを転送します。
- 発信管理トラフィックの場合、管理インターフェイスはバックプレーンを介してデータインターフェイスにトラフィックを転送します。

## マネージャのアクセス要件

データインターフェイスからのマネージャアクセスには、次の制限があります。

- マネージャアクセスを有効にできるのは、1つの物理的なデータインターフェイスのみです。サブインターフェイスと EtherChannel は使用できません。冗長性を目的として、Management Center の単一のセカンダリインターフェイスでマネージャアクセスを有効にすることもできます。
- このインターフェイスは管理専用にはできません。
- ルーテッドインターフェイスを使用するルーテッドファイアウォールモードのみです。
- PPPoE はサポートされていません。ISP で PPPoE が必要な場合は、PPPoE をサポートするルータを Threat Defense と WAN モデムの間に配置する必要があります。
- インターフェイスを配置する必要があるのはグローバル VRF のみです。
- SSH はデータインターフェイスではデフォルトで有効になっていないため、後で Management Center を使用して SSH を有効にする必要があります。また、管理インターフェイス ゲートウェイがデータインターフェイスに変更されるため、**configure network static-routes** コマンドを使用して管理インターフェイス用の静的ルートを追加しない限り、リモートネットワークから管理インターフェイスに SSH 接続することはできません。

## ハイ アベイラビリティ要件

デバイスのハイアベイラビリティを備えたデータインターフェイスを使用する場合は、次の要件を参照してください。

- マネージャアクセスには、両方のデバイスで同じデータインターフェイスを使用します。
- 冗長マネージャ アクセス データ インターフェイスはサポートされていません。

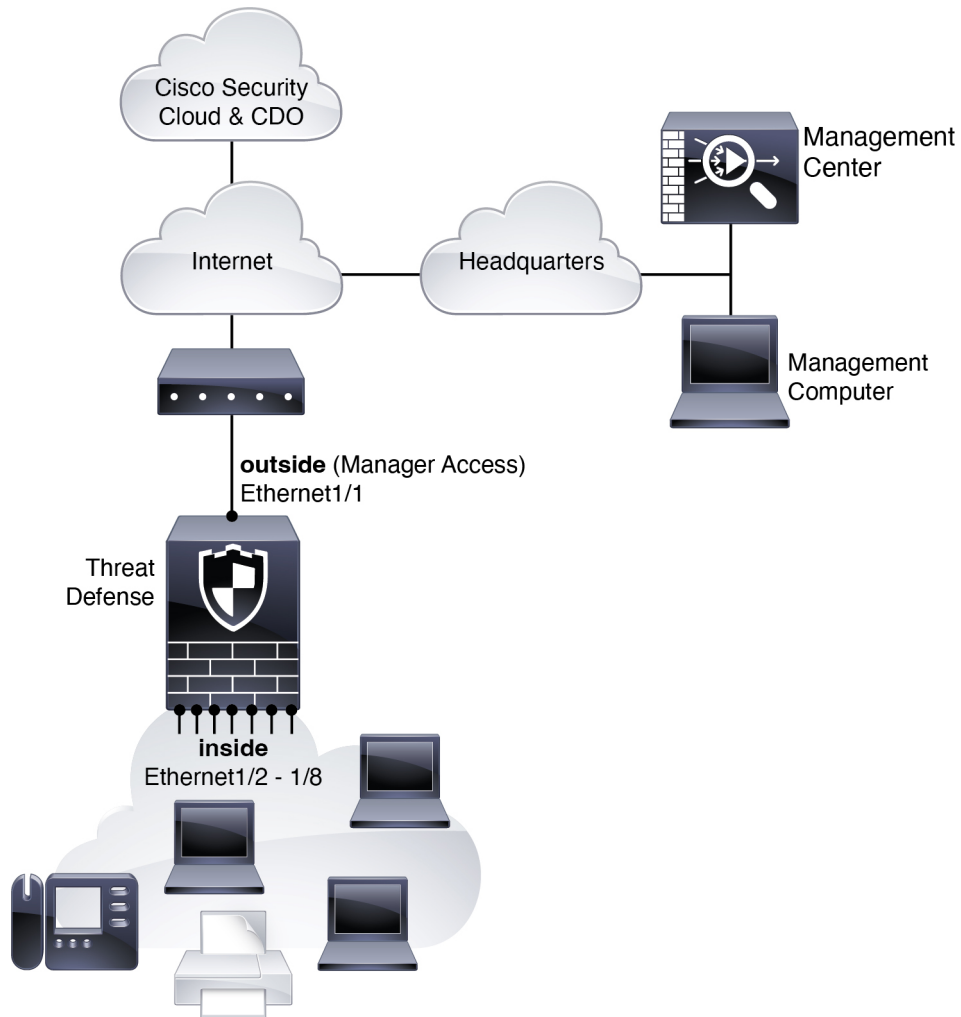
- DHCP は使用できません。静的 IP アドレスのみがサポートされています。DDNS やゼロタッチプロビジョニングなど、DHCP に依存する機能は使用できません。
- 同じサブネット内に異なる静的 IP アドレスがあります。
- IPv4 または IPv6 のいずれかを使用します。両方を設定することはできません。
- 同じマネージャ設定 (**configure manager add** コマンド) を使用して、接続が同じであることを確認します。
- データインターフェイスをフェールオーバーリンクまたはステートリンクとして使用することはできません。

### ゼロ タッチ プロビジョニング ネットワーク

次の図に、ファイアウォールの一般的なネットワーク展開を示します。

- Management Center は中央本社にあります。
- Threat Defense はマネージャアクセスに外部インターフェイスを使用します。
- Threat Defense と Management Center ではどちらも、インバウンド管理接続を許可するためのパブリック IP アドレスまたはホスト名が必要ですが、登録のために IP アドレスを把握しておく必要はありません。7.2(4) より前および 7.3 バージョンの Threat Defense の場合、Management Center はパブリックに到達可能である必要があります。
- Management Center と Threat Defense の両方が、最初に Cisco Security Cloud および CDO と通信して管理接続を確立します。
- 最初の確立後、管理接続が中断された場合は CDO を使用して管理接続を再確立します。たとえば、新しい DHCP の割り当てのために Threat Defense の IP アドレスが変更された場合、CDO はその変更を Management Center に通知します。

図 1: ゼロ タッチ プロビジョニング ネットワーク

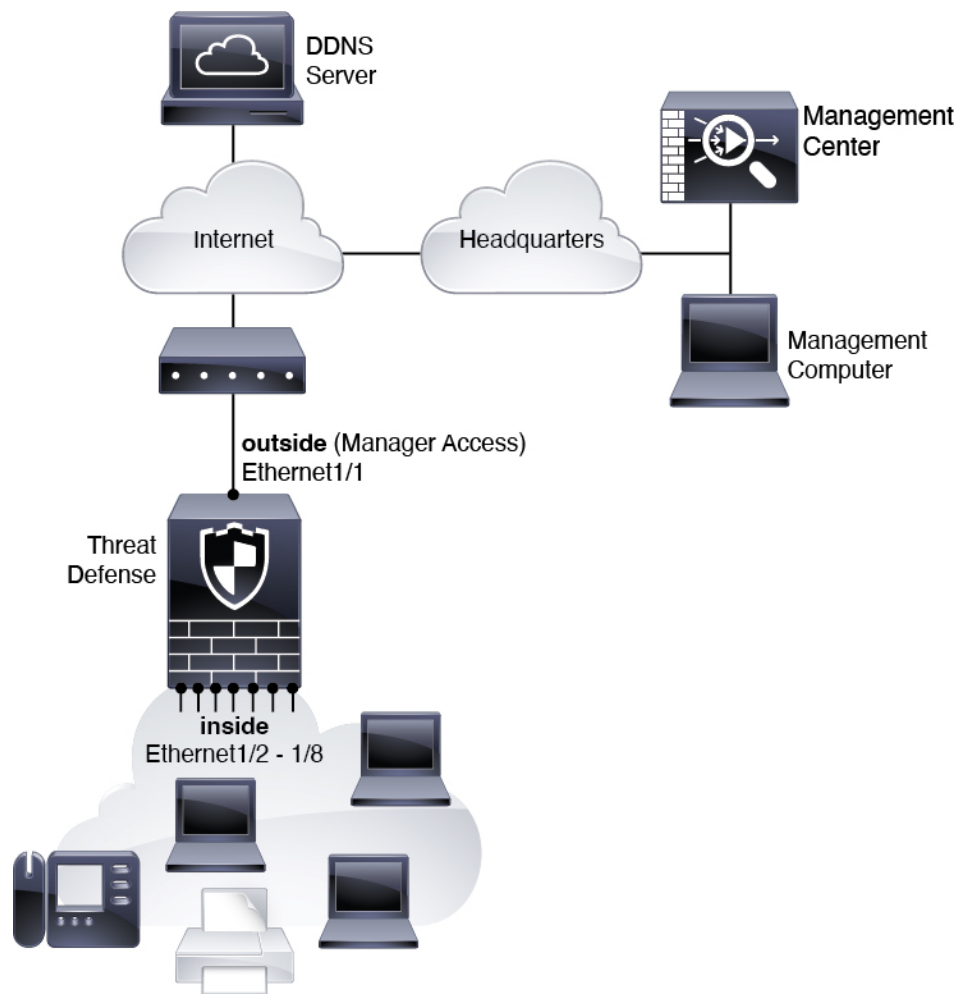


### 手動プロビジョニング ネットワーク

次の図に、ファイアウォールの一般的なネットワーク展開を示します。

- Management Center は中央本社にあります。
- Threat Defense はマネージャアクセスに外部インターフェイスを使用します。
- Threat Defense と Management Center ではどちらも、インバウンド管理接続を許可するためのパブリック IP アドレスまたはホスト名が必要であり、初期設定のためにこのような IP アドレスを把握しておかなければなりません。DHCP IP の割り当ての変更に対応するために、オプションで外部インターフェイスのダイナミック DNS (DDNS) を設定することもできます。

図 2: 手動プロビジョニング ネットワーク



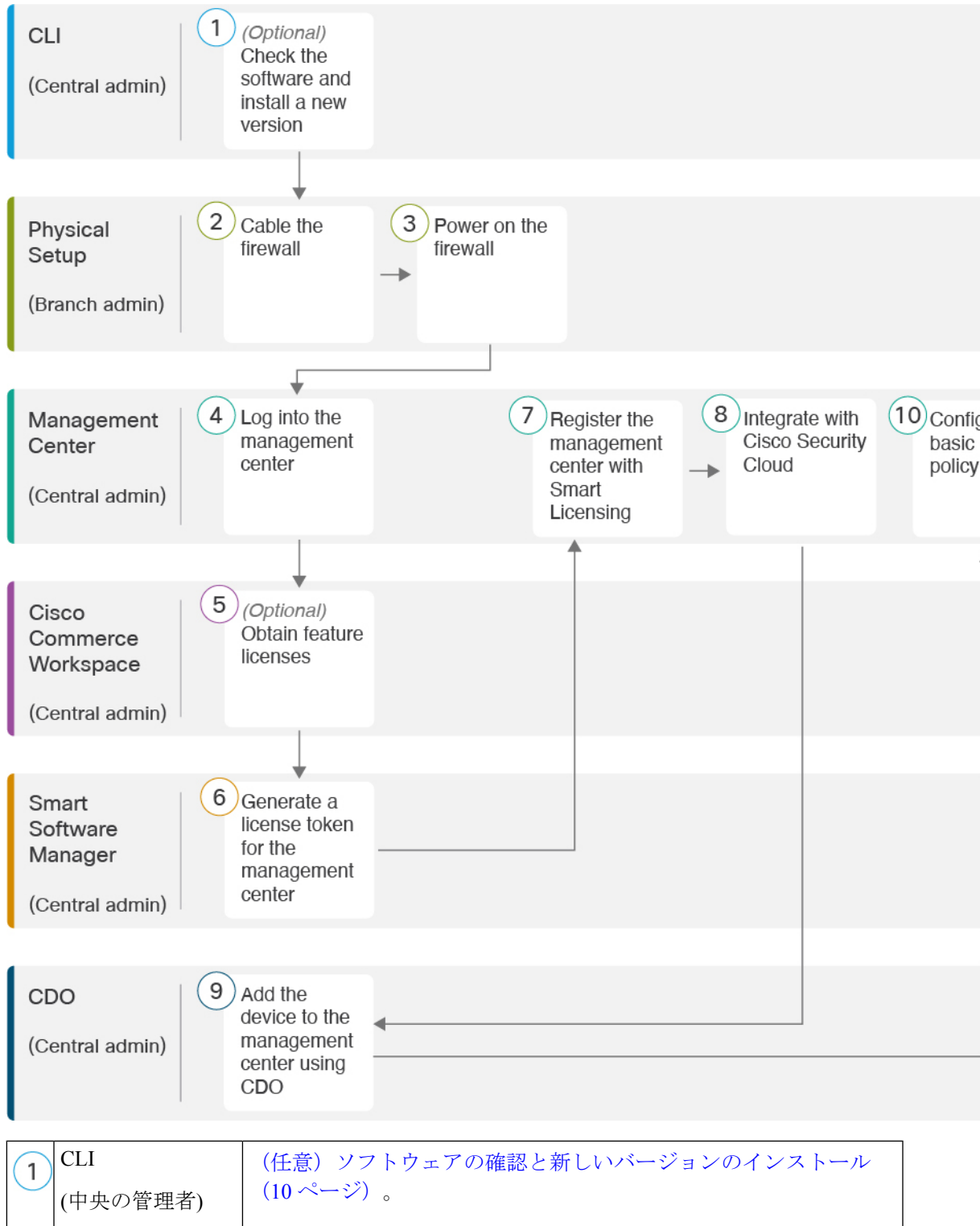
## はじめる前に

Management Center の初期設定を展開して実行します。使用モデルのスタートアップガイドを参照してください。

## エンドツーエンドのタスク：ゼロタッチプロビジョニング

ゼロタッチプロビジョニングを使用して Management Center により Threat Defense を展開するには、次のタスクを参照してください。

図 3: エンドツーエンドのタスク：ゼロ タッチ プロビジョニング



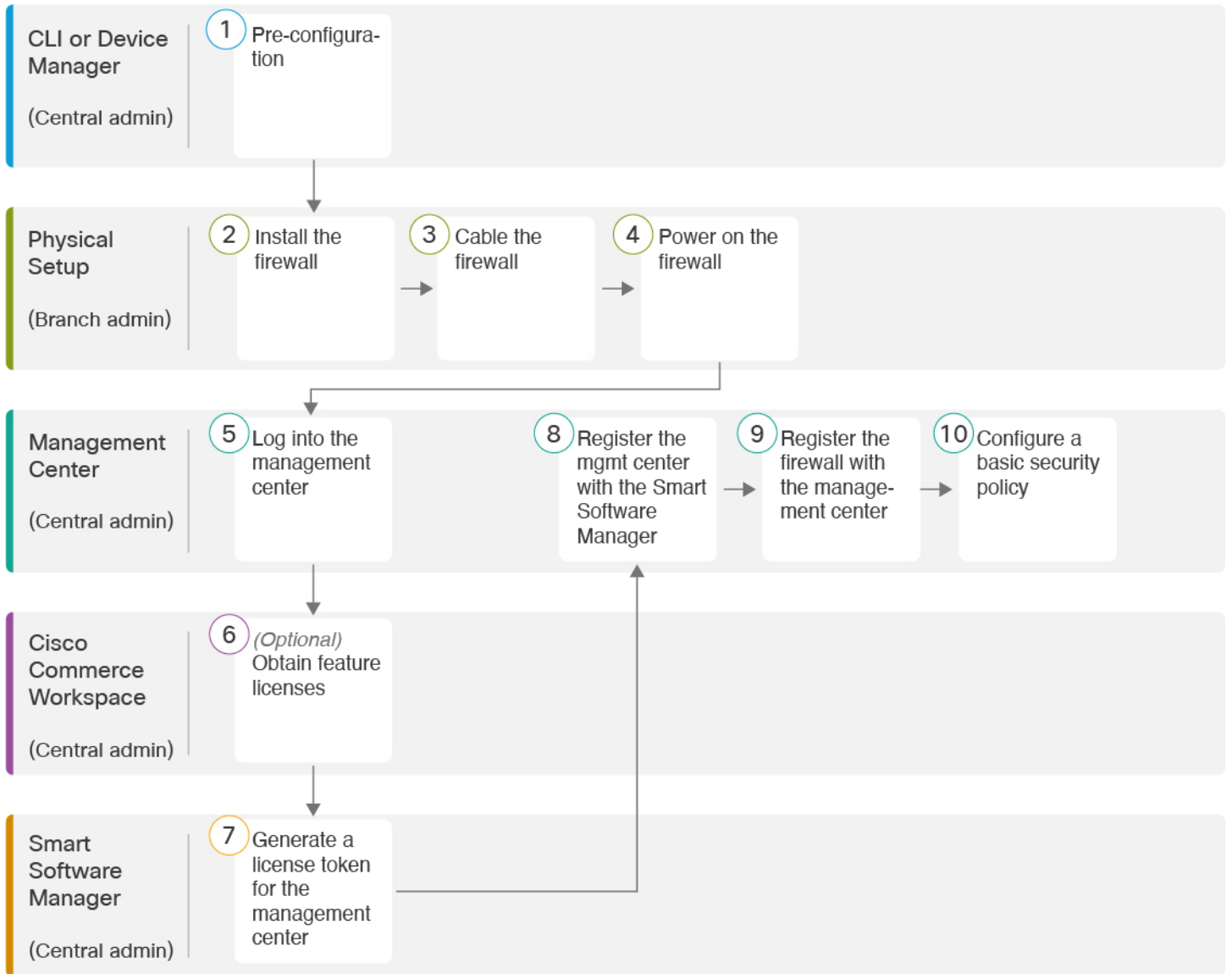
②	物理的なセットアップ (支店の管理者)	ファイアウォールのケーブル接続 (25 ページ)。
③	物理的なセットアップ (支店の管理者)	デバイスの電源投入 (26 ページ)
④	Management Center (中央の管理者)	Management Centerへのログイン。
⑤	Cisco Commerce Workspace (中央の管理者)	(任意) Management Center のライセンスの取得 (27 ページ) : 機能ライセンスを購入します。
⑥	Smart Software Manager (中央の管理者)	Management Center のライセンスの取得 (27 ページ) : Management Center のライセンストークンを生成します。
⑦	Management Center (中央の管理者)	Management Center のライセンスの取得 (27 ページ) : スマートライセンスサーバーに Management Center を登録します。
⑧	Management Center (中央の管理者)	ゼロタッチプロビジョニングを使用した Management Center へのデバイスの追加 (29 ページ) : CDO アカウントの取得を含め、Management Center を Cisco Security Cloud と統合します。
⑨	CDO (中央の管理者)	ゼロタッチプロビジョニングを使用した Management Center へのデバイスの追加 (29 ページ)。
⑩	Management Center (中央の管理者)	基本的なセキュリティポリシーの設定。

## エンドツーエンドのタスク：手動プロビジョニング

手動プロビジョニングを使用して Management Center により 脅威に対する防御 を展開するには、次のタスクを参照してください。



図 4: エンドツーエンドのタスク：手動プロビジョニング



<p>①</p>	<p>CLI または Device Manager (中央の管理者)</p>	<ul style="list-style-type: none"> <li>• (任意) ソフトウェアの確認と新しいバージョンのインストール (10 ページ)</li> <li>• CLI を使用した事前設定 (19 ページ)</li> <li>• Device Manager を使用した事前設定 (12 ページ)</li> </ul>
<p>②</p>	<p>物理的なセットアップ (支社の管理者)</p>	<p>ファイアウォールをインストールします。ハードウェア設置ガイドを参照してください。</p>

③	物理的なセットアップ (支社の管理者)	ファイアウォールのケーブル接続 (25 ページ)。
④	物理的なセットアップ (支社の管理者)	デバイスの電源投入 (26 ページ)
⑤	Management Center (中央の管理者)	中央の管理者 : Management Center へのログイン。
⑥	Cisco Commerce Workspace (中央の管理者)	Management Center のライセンスの取得 (27 ページ) : 機能ライセンスを購入します。
⑦	Smart Software Manager (中央の管理者)	Management Center のライセンスの取得 (27 ページ) : Management Center のライセンストークンを生成します。
⑧	Management Center (中央の管理者)	Management Center のライセンスの取得 (27 ページ) : スマートライセンシング サーバーに Management Center を登録します。
⑨	Management Center (中央の管理者)	手動による Management Center へのデバイスの追加 (36 ページ)。
⑩	Management Center (中央の管理者)	基本的なセキュリティポリシーの設定 (39 ページ)。

## 中央の管理者による事前設定

Threat Defense は、分散拠点に送信する前に手動で事前に設定する必要があります。

### (任意) ソフトウェアの確認と新しいバージョンのインストール

ソフトウェアのバージョンを確認し、必要に応じて別のバージョンをインストールするには、次の手順を実行します。ファイアウォールを設定する前に対象バージョンをインストールすることをお勧めします。別の方法として、稼働後にアップグレードを実行することもできますが、設定を保持するアップグレードでは、この手順を使用するよりも時間がかかる場合があります。

#### 実行するバージョン

ソフトウェアダウンロードページのリリース番号の横にある、金色の星が付いている Gold Star リリースを実行することをお勧めします。 <https://www.cisco.com/c/en/us/products/collateral/>

[security/firewalls/bulletin-c25-743178.html](https://www.cisco.com/c/en/us/qa/security/firewalls/bulletin-c25-743178.html) に記載されているリリース戦略も参照してください。たとえば、この速報では、(最新機能を含む) 短期的なリリース番号、長期的なリリース番号 (より長期間のメンテナンスリリースとパッチ)、または非常に長期的なリリース番号 (政府認定を受けるための最長期間のメンテナンスリリースとパッチ) について説明しています。

## 手順

**ステップ 1** CLI に接続します。詳細については、[Threat Defense および FXOS CLI へのアクセス \(53 ページ\)](#) を参照してください。この手順ではコンソールポートを使用していますが、代わりに SSH を使用することもできます。

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

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

(注) パスワードがすでに変更されていて、パスワードがわからない場合は、初期設定へのリセットを実行して、パスワードをデフォルトにリセットする必要があります。[初期設定へのリセット手順](#)については、『[FXOS troubleshooting guide](#)』を参照してください。

例 :

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

[...]

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

[...]

firepower#
```

**ステップ 2** FXOS CLI で、実行中のバージョンを表示します。

**scope ssa**

**show app-instance**

例 :

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name      Slot ID   Admin State   Operational State   Running Version
Startup Version Cluster Oper State
-----
ftd                   1         Enabled       Online               7.6.0.65
7.6.0.65              Not Applicable
```

**ステップ 3** 新しいバージョンをインストールする場合は、次の手順を実行します。

- a) 管理インターフェイスに静的 IP アドレスを設定する必要がある場合は、「[CLI を使用した事前設定（19 ページ）](#)」を参照してください。デフォルトでは、管理インターフェイスは DHCP を使用します。  
管理インターフェイスからアクセスできるサーバーから新しいイメージをダウンロードする必要があります。
- b) [FXOS のトラブルシューティング ガイド](#)に記載されている[再イメージ化の手順](#)を実行します。  
ファイアウォールが再起動したら、FXOS CLI に再度接続します。
- c) FXOS CLI で、管理者パスワードを再度設定するように求められます。  
ゼロタッチプロビジョニングの場合は、デバイスをオンボーディングする際、すでにパスワードが設定されているため、[パスワードのリセット（Password Reset）] エリアで必ず [いいえ（No...）] を選択してください。
- d) デバイスをシャットダウンします。[CLI でのデバイスの電源オフ（60 ページ）](#) を参照してください。

## 初期設定の実行（手動プロビジョニング）

手動でプロビジョニングを行う場合は、CLI または Device Manager を使用して、Threat Defense の初期設定を実行します。

### Device Manager を使用した事前設定

初期セットアップに Device Manager を使用すると、管理インターフェイスとマネージャアクセスの設定に加えて、次のインターフェイスが事前設定されます。

- イーサネット 1/1：「外部」、DHCP からの IP アドレス、IPv6 自動設定
- VLAN1：「内部」、192.168.95.1/24
- デフォルトルート：外部インターフェイスで DHCP を介して取得

他の設定（内部の DHCP サーバー、アクセス コントロール ポリシー、セキュリティゾーンなど）は設定されないことに注意してください。

Management Center に登録する前に Device Manager 内で追加のインターフェイス固有の設定を実行すると、その設定は保持されます。

CLI を使用すると、管理インターフェイスとマネージャアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイス構成は保持されません）。

## 手順

**ステップ 1** 管理コンピュータを内部 (Ethernet 1/2 ~ 1/8) インターフェイスに接続します。

**ステップ 2** ファイアウォールの電源を入れます。

(注) Threat Defense を初めて起動するときは、初期化に約 15 ~ 30 分かかります。

**ステップ 3** Device Manager にログインします。

a) ブラウザに URL (<https://192.168.95.1>) を入力します。

b) ユーザー名 **admin**、デフォルトパスワード **Admin123** を使用してログインします。

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

**ステップ 4** 初期設定を完了するには、最初に Device Manager にログインしたときにセットアップウィザードを使用します。必要に応じて、ページの下部にある [デバイスの設定をスキップ (Skip device setup)] をクリックしてセットアップウィザードをスキップできます。

セットアップウィザードを完了すると、内部インターフェイス (Ethernet1/2 ~ 1/8 (VLAN1 のスイッチポート)) のデフォルト設定に加えて、Management Center の管理に切り替えるときに維持される外部 (イーサネット 1/1) インターフェイスも設定できます。

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

1. [外部インターフェイスアドレス (Outside Interface Address)]—このインターフェイスは通常インターネットゲートウェイであり、マネージャアクセスインターフェイスとして使用される場合があります。デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータインターフェイスがデフォルトの外部インターフェイスです。

マネージャアクセスに外部 (または内部) とは異なるインターフェイスを使用する場合は、セットアップウィザードの完了後に手動で設定する必要があります。

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

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

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

CLI で初期設定を実行した場合、管理インターフェイスの設定は表示されません。

データインターフェイスでマネージャアクセスを有効にした場合でも、管理インターフェイスの設定が使用されます。たとえば、データインターフェイスを介してバックプレーン経由でルーティングされる管理トラフィックは、データインターフェイス DNS サーバーではなく、管理インターフェイス DNS サーバーを使用して FQDN を解決します。

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

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

- b) [時刻設定 (NTP) (Time Setting (NTP)) ] を設定し、[次へ (Next) ] をクリックします。
  1. [タイムゾーン (Time Zone) ]: システムのタイムゾーンを選択します。
  2. [NTPタイムサーバ (NTP Time Server) ]: デフォルトの NTP サーバを使用するか、使用している NTP サーバのアドレスを手動で入力するかを選択します。バックアップ用に複数のサーバを追加できます。
- c) [登録せずに 90 日間の評価期間を開始 (Start 90 day evaluation period without registration) ] を選択します。
 

Threat Defense を Smart Software Manager に登録しないでください。すべてのライセンスは Management Center で実行されます。
- d) [終了 (Finish) ] をクリックします。
- e) [クラウド管理 (Cloud Management) ] または [スタンドアロン (Standalone) ] を選択するよう求められます。Management Center の管理については、[スタンドアロン (Standalone) ] を選択してから、[Got It (了解) ] を選択します。

**ステップ 5** (必要に応じて) 管理インターフェイスを設定します。[デバイス (Device) ] > [インターフェイス (Interfaces) ] の管理インターフェイスを参照してください。

管理インターフェイスには、データインターフェイスに設定されたゲートウェイが必要です。デフォルトでは、管理インターフェイスは DHCP から IP アドレスとゲートウェイを受信します。DHCP からゲートウェイを受信しない場合 (たとえば、管理インターフェイスをネットワークに接続していない場合)、ゲートウェイはデフォルトでデータインターフェイスになり、何も設定する必要はありません。DHCP からゲートウェイを受信した場合は、代わりに管理インターフェイスに静的 IP アドレスを設定し、ゲートウェイをデータインターフェイスに設定する必要があります。

**ステップ 6** マネージャアクセスに使用する外部または内部以外のインターフェイスを含む追加のインターフェイスを設定する場合は、[デバイス (Device) ] を選択し、[インターフェイス (Interface) ] のサマリーのリンクをクリックします。

Device Manager におけるインターフェイスの設定の詳細については、「[Device Manager でのファイアウォールの設定](#)」を参照してください。Management Center にデバイスを登録すると、Device Manager の他の設定は保持されません。

- ステップ 7 [デバイス (Device) ]>[システム設定 (System Settings) ]>[中央管理 (Central Management) ]の順に選択し、[続行 (Proceed) ]をクリックして Management Center の管理を設定します。
- ステップ 8 [Management Center/CDOの詳細 (Management Center/CDO Details) ]を設定します。

図 5: Management Center/CDO の詳細

### Configure Connection to Management Center or CDO


Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

Yes  No


**Threat Defense**



10.89.5.16  
fe80::6a87:c6ff:fea6:4c00/64

→

**Management Center/CDO**



10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

●●●● 👁

NAT ID

Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

---

### Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup ▾

Management Center/CDO Access Interface

Data Interface

Please select an interface ▾

Management Interface [View details](#)

CANCEL
CONNECT

- a) [Management Center/CDOのホスト名またはIPアドレスを知っていますか (Do you know the FMC hostname or IP address)] で、IP アドレスまたはホスト名を使用して Management Center に到達できる場合は [はい (Yes)] をクリックし、Management Center が NAT の背



後にあるか、パブリック IP アドレスまたはホスト名がない場合は[いいえ (No)] をクリックします。

双方向の TLS-1.3 暗号化通信チャネルを 2 台のデバイス間に確立するには、少なくとも 1 台以上のデバイス (Management Center または Threat Defense デバイス) に到達可能な IP アドレスが必要です。

- b) [はい (Yes)] を選択した場合は、**管理センター/CDO のホスト名/IP アドレス**を入力します。
- c) **Management Center/CDO 登録キー**を指定します。

このキーは、Threat Defense デバイスを登録するとき Management Center でも指定する任意の 1 回限りの登録キーです。登録キーは 37 文字以下にする必要があります。有効な文字には、英数字 (A~Z、a~z、0~9)、およびハイフン (-) があります。この ID は、Management Center に登録する複数のデバイスに使用できます。

- d) [NAT ID] を指定します。

この ID は、Management Center でも指定する任意の 1 回限りの文字列です。いずれかのデバイスの IP アドレスのみを指定する場合、このフィールドは必須です。両方のデバイスの IP アドレスがわかっている場合でも、NAT ID を指定することを推奨します。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字 (A~Z、a~z、0~9)、およびハイフン (-) があります。この ID は、Management Center に登録する他のデバイスには使用できません。NAT ID は、正しいデバイスからの接続であることを確認するために IP アドレスと組み合わせて使用されます。IP アドレス/NAT ID の認証後にのみ、登録キーがチェックされます。

#### ステップ 9 [接続の設定 (Connectivity Configuration)] を設定します。

- a) [FTDホスト名 (FTD Hostname)] を指定します。

この FQDN は、外部インターフェイス、または **Management Center/CDO アクセスマスターフェイス**用に選択したインターフェイスに使用されます。

- b) [DNSサーバーグループ (DNS Server Group)] を指定します。

既存のグループを選択するか、新しいグループを作成します。デフォルトの DNS グループは **CiscoUmbrellaDNSServerGroup** と呼ばれ、OpenDNS サーバーが含まれます。

この設定により、データインターフェイス DNS サーバーが設定されます。セットアップウィザードで設定した管理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS (設定されている場合) またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。管理トラフィックとデータトラフィックの両方が外部インターフェイス経由で DNS サーバーに到達するため、管理に使用したものと同一 DNS サーバーグループを選択する可能性があります。

Management Center では、この Threat Defense に割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。Management Center に Threat Defense を追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む Threat Defense に後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。

Management Center と Threat Defense を同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ Management Center で保持されます。

- c) **Management Center/CDO アクセスインターフェイス**については、[外部 (outside)] を選択します。

設定済みの任意のインターフェイスを選択できますが、このガイドでは外部を使用していることを前提としています。

- ステップ 10** 外部とは別のデータインターフェイスを選択した場合は、デフォルトルートを追加します。

インターフェイスを通過するデフォルトルートがあることを確認するように求めるメッセージが表示されます。外部を選択した場合は、セットアップウィザードの一環としてこのルートがすでに設定されています。別のインターフェイスを選択した場合は、Management Center に接続する前にデフォルトルートを手動で設定する必要があります。Device Manager におけるスタティックルートの設定の詳細については、「[Device Manager でのファイアウォールの設定](#)」を参照してください。

- ステップ 11** [ダイナミック DNS (DDNS) 方式の追加 (Add a Dynamic DNS (DDNS) method)] をクリックします。

DDNS は、Threat Defense の IP アドレスが変更された場合に Management Center が完全修飾ドメイン名 (FQDN) で Threat Defense に到達できるようにします。[デバイス (Device)] > [システム設定 (System Settings)] > [DDNS サービス (DDNS Service)] を参照して DDNS を設定します。

Threat Defense を Management Center に追加する前に DDNS を設定すると、Threat Defense は Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加するため、Threat Defense は HTTPS 接続の DDNS サーバー証明書を検証できます。Threat Defense は、DynDNS リモート API 仕様 (<https://help.dyn.com/remote-access-api/>) を使用するすべての DDNS サーバーをサポートします。

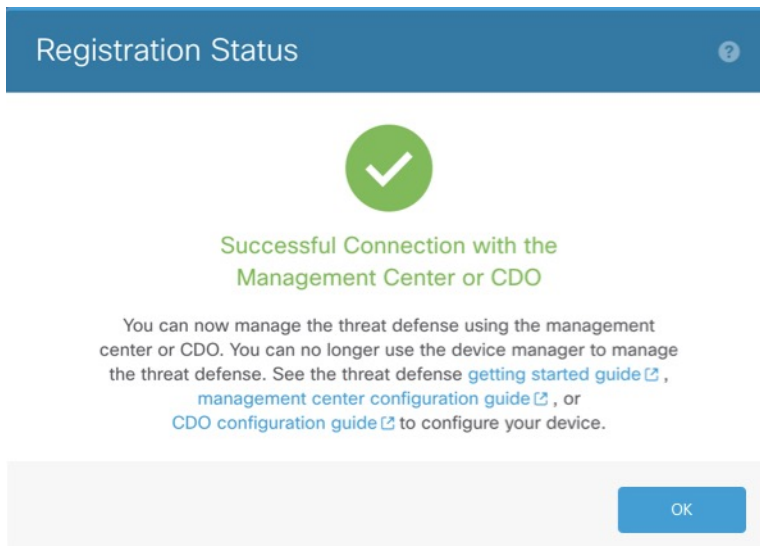
- ステップ 12** [接続 (Connect)] をクリックします。[登録ステータス (Registration Status)] ダイアログボックスには、Management Center への切り替えに関する現在のステータスが表示されます。

[**Management Center/CDO 登録設定の保存 (Saving Management Center/CDO Registration Settings)**] のステップの後、Management Center に移動してファイアウォールを追加します。

Management Center への切り替えをキャンセルする場合は、[登録のキャンセル (Cancel Registration)] をクリックします。キャンセルしない場合は、[**Management Center/CDO 登録設定の保存 (Saving Management Center/CDO Registration Settings)**] のステップが完了するまで Device Manager のブラウザウィンドウを閉じないでください。閉じた場合、プロセスは一時停止し、Device Manager に再接続した場合のみ再開されます。

[**Management Center/CDO 登録設定の保存 (Saving Management Center/CDO Registration Settings)**] のステップの後に Device Manager に接続したままにする場合、その後 [Management Center または CDO との正常接続 (Successful Connection with Management Center or CDO)] ダイアログボックスが表示され、Device Manager から切断されます。

図 6: 正常接続



## CLI を使用した事前設定

セットアップウィザードを使用して、管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定を行います。初期設定で CLI を使用すると、管理インターフェイスとマネージャ アクセス インターフェイスの設定のみが保持されます。Device Manager (7.1 以降) を使用して初期セットアップを実行すると、管理インターフェイスおよびマネージャ アクセス インターフェイスの設定に加えて、管理のために Management Center に切り替えたときに、Device Manager で完了したすべてのインターフェイス設定が保持されます。アクセス コントロール ポリシーなどの他のデフォルト設定は保持されないことに注意してください。

### 手順

**ステップ 1** ファイアウォールの電源を入れます。

(注) Threat Defense を初めて起動するときは、初期化に約 15 ~ 30 分かかります。

**ステップ 2** コンソールポートで Threat Defense CLI に接続します。

コンソールポートは FXOS CLI に接続します。

**ステップ 3** ユーザー名 **admin** およびパスワード **Admin123** でログインします。

初めて FXOS にログインしたときは、パスワードを変更するよう求められます。このパスワードは、SSH の Threat Defense ログインにも使用されます。

(注) パスワードがすでに変更されていてわからない場合は、デバイスを再イメージ化してパスワードをデフォルトにリセットする必要があります。再イメージ化の手順については、FXOS の [トラブルシューティング ガイド](#) を参照してください。

例 :

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

[...]

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

[...]

firepower#
```

**ステップ 4** Threat Defense CLI に接続します。

**connect ftd**

例 :

```
firepower# connect ftd
>
```

**ステップ 5** Threat Defense に初めてログインすると、エンドユーザーライセンス契約（EULA）に同意し、SSH 接続を使用している場合は、管理者パスワードを変更するように求められます。その後、管理インターフェイスの設定用の CLI セットアップスクリプトが表示されます。

データインターフェイスでマネージャアクセスを有効にした場合でも、管理インターフェイスの設定が使用されます。

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

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

次のガイドラインを参照してください。

- [IPv4を設定しますか? (Do you want to configure IPv4?) ], [IPv6を設定しますか? (Do you want to configure IPv6?) ] : これらのタイプのアドレスの少なくとも1つに **y** を入力します。管理インターフェイスを使用する予定がない場合でも、プライベートアドレスなどの IP アドレスを設定する必要があります。
- **IPv4 は DHCP 経由または手動のどちらで設定しますか? IPv6 は DHCP、ルータ、または手動のどれで設定しますか? :** [手動 (**manual**) ] を選択します。管理インターフェイスが DHCP に設定されている場合、管理用のデータインターフェイスを設定することはできません。これは、**data-interfaces** である必要があるデフォルトルートが DHCP サーバーから受信したルートで上書きされる可能性があるためです。

- 管理インターフェイスの IPv4 デフォルトゲートウェイを入力または管理インターフェイスの IPv6 ゲートウェイを入力：ゲートウェイが **data-interfaces** になるように設定します。この設定は、マネージャ アクセス データ インターフェイスを通じて回送できるように、バックプレーンを介して管理トラフィックを転送します。
- [デバイスをローカルで管理しますか (Manage the device locally?) ] : Management Center を使用するには「**no**」を入力します。**yes** と入力すると、代わりに Device Manager を使用することになります。
- [ファイアウォールモードを設定しますか? (Configure firewall mode?) ] : **routed** と入力します。外部マネージャアクセスは、ルーテッド ファイアウォール モードでのみサポートされています。

例 :

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

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

System initialization in progress. Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Device is in OffBox mode - disabling/removing port 443 from iptables.
Update policy deployment information
- add device configuration
- add network discovery
- add system policy
```

You can register the sensor to a Firepower Management Center and use the Firepower Management Center to manage it. Note that registering the sensor to a Firepower Management Center disables on-sensor Firepower Services management capabilities.

When registering the sensor to a Firepower Management Center, a unique alphanumeric registration key is always required. In most cases, to register a sensor to a Firepower Management Center, you must provide the hostname or the IP address along with the registration key.

```
'configure manager add [hostname | ip address ] [registration key ]'
```

However, if the sensor and the Firepower Management Center are separated by a NAT device, you must enter a unique NAT ID, along with the unique registration key.

```
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

Later, using the web interface on the Firepower Management Center, you must use the same registration key and, if necessary, the same NAT ID when you add this sensor to the Firepower Management Center.

>

## ステップ 6 マネージャアクセス用の外部インターフェイスを設定します。

### configure network management-data-interface

その後、外部インターフェイスの基本的なネットワーク設定を行うように求めるプロンプトが表示されます。このコマンドの使用については、次の詳細を参照してください。

- データインターフェイスを管理に使用する場合、管理インターフェイスではDHCPを使用できません。初期セットアップ時にIPアドレスを手動で設定しなかった場合は、**configure network {ipv4 | ipv6} manual** コマンドを使用して事前に設定できます。管理インターフェイスゲートウェイを **data-interfaces** に設定しなかった場合は、ここでこのコマンドで設定します。
- Threat Defense を Management Center に追加すると、Management Center はインターフェイス設定（インターフェイス名と IP アドレス、ゲートウェイへの静的ルート、DNS サーバー、DDNS サーバーなど）を検出して維持します。DNS サーバー設定の詳細については、次を参照してください。Management Center では、後でマネージャアクセスインターフェイス構成を変更できますが、Threat Defense または Management Center が管理接続の再確立を妨げるような変更を加えないようにしてください。管理接続が中断された場合、Threat Defense には以前の展開を復元する **configure policy rollback** コマンドが含まれません。
- DDNS サーバー更新の URL を設定すると、Threat Defense は Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加するため、Threat Defense は HTTPS 接続の DDNS サーバー証明書を検証できます。Threat Defense は、DynDNS リモート API 仕様 (<https://help.dyn.com/remote-access-api/>) を使用するすべての DDNS サーバーをサポートします。
- このコマンドは、「データ」インターフェイス DNS サーバーを設定します。セットアップスクリプトで（または **configure network dns servers** コマンドを使用して）設定した管理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS（設定されている場合）またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。

Management Center では、この Threat Defense に割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。Management Center に Threat Defense を追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む Threat Defense に後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。Management Center と Threat Defense を同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ Management Center で保持されます。たとえば、管理インターフェイスを使用してデバイスを登録し、後で **configure network management-data-interface** コマンドを使用してデータインターフェイスを設定した場合、Threat Defense 設定と一致するように、DNS サーバーを含むこれらの設定のすべてを Management Center で手動で設定する必要があります。

- 管理インターフェイスは、Threat Defense を Management Center に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。
- セットアップウィザードで設定した FQDN がこのインターフェイスに使用されます。
- コマンドの一部としてデバイス設定全体をクリアできます。このオプションはリカバリシナリオで使用できますが、初期セットアップや通常の操作には使用しないでください。
- データ管理を無効にするには、**configure network management-data-interface disable** コマンドを入力します。

例 :

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://dwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

例 :

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:
```

```
Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.
```

```
Setting IPv4 network configuration.
Network settings changed.
```

```
>
```

**ステップ 7** (任意) 特定のネットワーク上の Management Center へのデータ インターフェイス アクセスを制限します。

```
configure network management-data-interface client ip_address netmask
```

デフォルトでは、すべてのネットワークが許可されます。

**ステップ 8** この Threat Defense を管理する Management Center を特定します。

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key [nat_id]
```

- **{hostname | IPv4\_address | IPv6\_address | DONTRESOLVE}**—Specifies either the FQDN or IP address of the Management Center. Management Center を直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。双方向の SSL 暗号化通信チャネルを 2 台のデバイス間に確立するには、少なくとも 1 台以上のデバイス (Management Center または Threat Defense) に到達可能な IP アドレスが必要です。このコマンドで **DONTRESOLVE** を指定するには、到達可能な IP アドレスまたはホスト名が Threat Defense に必要です。
- **reg\_key** : Threat Defense を登録するときに Management Center でも指定する任意のワнтаイム登録キーを指定します。登録キーは 37 文字以下にする必要があります。有効な文字には、英数字 (A~Z、a~z、0~9)、およびハイフン (-) があります。
- **nat\_id** : Management Center でも指定する、任意で一意的の 1 回限りの文字列を指定します。管理にデータインターフェイスを使用する場合は、登録用に Threat Defense と Management Center の両方で NAT ID を指定する必要があります。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字 (A~Z、a~z、0~9)、およびハイフン (-) があります。この ID は、Management Center に登録する他のデバイスには使用できません。

例 :

```
> configure manager add fmc-1.example.com regk3y78 natid56
Manager successfully configured.
```

**ステップ 9** デバイスをリモート支社に送信できるように Threat Defense をシャットダウンします。

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたり、電源スイッチを押したりすると、重大なファイルシステムの損傷を引き起こすことがあります。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おり、電源プラグを抜いたり、電源を切断したりすると、システムをグレースフルシャットダウンできないことを覚えておいてください。

- a) **shutdown** コマンドを入力します。
- b) 電源 LED とステータス LED を観察して、シャーシの電源が切断されていることを確認します (LED が消灯)。



- c) シャーシの電源が正常に切断されたら、必要に応じて電源プラグを抜き、シャーシから物理的に電源を取り外すことができます。

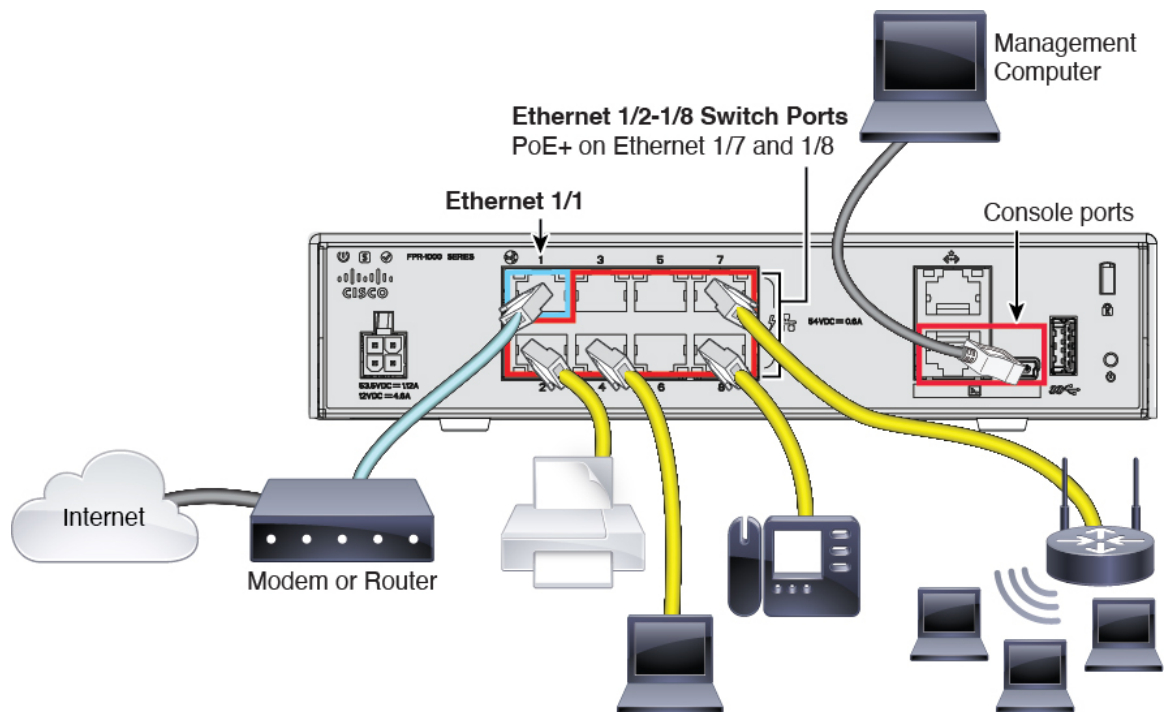
## 支社へのインストール

中央の本社から Threat Defense を受け取ったら、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、ファイアウォールにケーブルを接続して電源をオンにするだけです。そうすると、中央の管理者は設定を完了できます。

## ファイアウォールのケーブル接続

Management Center と管理コンピュータはリモートの本社にあり、Threat Defense にはインターネット経由で到達できます。Firepower 1010 でケーブル接続を行うには、次の手順を参照してください。

図 7: リモート管理展開のケーブル接続



(注) PoE は Firepower 1010E ではサポートされていません。

## 手順

- ステップ1 シャーシを取り付けます。ハードウェア設置ガイドを参照してください。
- ステップ2 外部インターフェイス (Ethernet 1/1) を外部ルータに接続します。
- ステップ3 内部デバイスをスイッチポートの Ethernet 1/2 ~ 1/8 にケーブルで接続します。
- ステップ4 (任意) 管理コンピュータをコンソールポートに接続します。

支社では、日常的に使用するためのコンソール接続は必要ありません。ただし、トラブルシューティングに必要な場合があります。

## デバイスの電源投入

システムの電源は電源コードで制御されます。電源ボタンはありません。



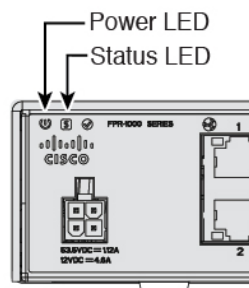
(注) Threat Defense を初めて起動するときは、初期化に約 15 ~ 30 分かかります。

### 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

- 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。  
電源コードを差し込むと電源が自動的に入ります。
- ステップ2 デバイスの背面または上部にある電源 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 3** デバイスの背面または上部にあるステータス LED を確認します。緑色に点灯している場合は、電源投入時診断に合格しています。

## 中央の管理者による事後設定

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リモート支社の管理者が Threat Defense をケーブル接続すると、Threat Defense を Management Center に登録してデバイスの設定を完了できます。

### Management Center へのログイン

Management Center を使用して、Threat Defense を設定および監視します。

#### 手順

**ステップ 1** サポートされているブラウザを使用して、次の URL を入力します。

`https://fmc_ip_address`

**ステップ 2** ユーザー名とパスワードを入力します。

**ステップ 3** [ログイン (Log In) ] をクリックします。

### Management Center のライセンスの取得

すべてのライセンスは、Management Center によって脅威に対する防御に提供されます。オプションで、次の機能ライセンスを購入できます。

- **Essentials** (必須) Essentials ライセンス。
- **IPS** : セキュリティインテリジェンスと次世代 IPS
- **マルウェア防御** : マルウェア防御
- **URL フィルタリング** : URL フィルタリング
- **Cisco Secure Client** : Secure Client Advantage、Secure Client Premier、または Secure Client VPN のみ

シスコライセンスの概要については詳しくは、[cisco.com/go/licensingguide](https://www.cisco.com/go/licensingguide) を参照してください。

#### 始める前に

- **Smart Software Manager** のアカウントが必要です。

まだアカウントをお持ちでない場合は、リンクをクリックして[新しいアカウントを設定](#)してください。Smart Software Manager では、組織のアカウントを作成できます。

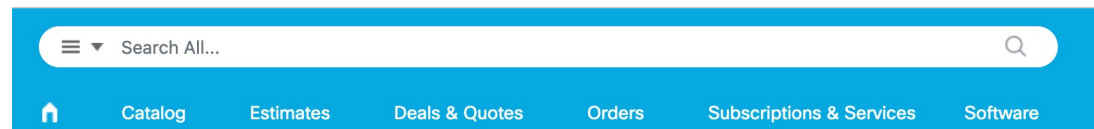
- (輸出コンプライアンスフラグを使用して有効化される) 機能を使用するには、ご使用のスマートソフトウェア ライセンシング アカウントで強力な暗号化 (3DES/AES) ライセンスを使用できる必要があります。

## 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。

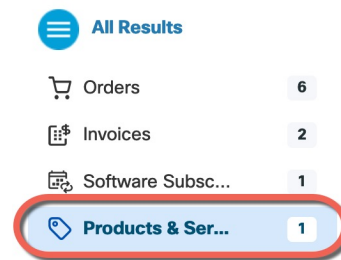
ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマートソフトウェア ライセンシングアカウントにリンクされています。ただし、自身でライセンスを追加する必要がある場合は、[Cisco Commerce Workspace](#) で [すべて検索 (Search All) ] フィールドを使用します。

図 8: ライセンス検索



結果から、[製品とサービス (Products and Services) ] を選択します。

図 9: 結果



次のライセンス PID を検索します。

(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。

- IPS、マルウェア防御、および URL ライセンスの組み合わせ：
  - L-FPR1010T-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-FPR1010T-TMC-1Y

- L-FPR1010T-TMC-3Y
- L-FPR1010T-TMC-5Y

• Cisco Secure Client : 『[Cisco Secure Client 発注ガイド](#)』を参照してください。

**ステップ 2** まだの場合は、Smart Software Manager に Management Center を登録します。

登録を行うには、Smart Software Manager で登録トークンを生成する必要があります。詳細については、『[Management Center コンフィグレーションガイド](#)』を参照してください。

## Management Center への Threat Defense の登録

使用している展開方法に応じて Threat Defense を Management Center に登録します。

### ゼロタッチプロビジョニングを使用した Management Center へのデバイスの追加

ゼロタッチプロビジョニングを使用すると、デバイスで初期設定を実行することなく、シリアル番号でデバイスを Management Center に登録できます。Management Center は、この機能のために Cisco Defense Orchestrator (CDO) と統合されます。

ゼロタッチプロビジョニングを使用すると、以下のインターフェイスが事前設定されます。他の設定 (内部の DHCP サーバー、アクセスコントロールポリシー、セキュリティゾーンなど) は設定されないことに注意してください。

- イーサネット 1/1 : 「外部」、DHCP からの IP アドレス、IPv6 自動設定
- イーサネット 1/2 (Firepower 1010 の場合は VLAN1 インターフェイス) : 「内部」、192.168.95.1/24
- デフォルトルート : 外部インターフェイスで DHCP を介して取得

ゼロタッチプロビジョニングは DHCP を使用しますが、データインターフェイスと高可用性では DHCP がサポートされていないため、高可用性は管理インターフェイスを使用する場合のみサポートされます。

#### 始める前に

- 新しいデバイスに割り当てることができるように、少なくとも 1 つのアクセスコントロールポリシーが Management Center に設定されていることを確認します。CDO を使用してポリシーを追加することはできません。
- デバイスにパブリック IP アドレスまたは FQDN がない場合、または管理インターフェイスを使用する場合は、Management Center のパブリック IP アドレス/FQDN を設定し (Management Center 管理インターフェイスの IP アドレスと異なる場合。たとえば、NAT の背後にある場合)、デバイスが管理接続を開始できるようにします。を参照してください。この手順中に CDO でパブリック IP アドレス/FQDN を設定することもできます。

## 手順

**ステップ 1** シリアル番号を使用してデバイスを初めて追加するときは、次の前提条件を満たしている必要があります。初回以降は、スキップして、CDO にデバイスを直接追加できます。

- a) Management Center で、[デバイス (Devices)] > [デバイス管理 (Device Management)] を選びます。
- b) [追加 (Add)] ドロップダウンメニューから、[デバイス (Device)] を選択します。
- c) プロビジョニング方式の [シリアル番号 (Serial Number)] をクリックします。

図 10: シリアル番号でデバイスを追加

Add Device ?

Select the Provisioning Method:

Registration Key     Serial Number

**1 Step 1: Create Cisco Defense Orchestrator (CDO) and SecureX accounts**  
 CDO and SecureX are cloud services that are required for serial-number onboarding. If you already have separate accounts, you need to link them. [Learn more](#)  
 If you don't already have accounts, perform the following:  
 • Request a CDO tenant. [Learn more](#)  
 • Create a SecureX user. [Learn more](#)

**2 Step 2: Integrate the Management Center with SecureX**  
 SecureX integration is required to add an on-prem management center to CDO. [SecureX Integration](#)

**i Complete above prerequisites before registering**

Cancel Launch CDO

- d) CDO アカウントを作成します。

(注) 既存の別々の SecureX および CDO アカウントをすでに持っている場合は、それらをリンクさせる必要があります。アカウントのリンクの詳細については、<https://cisco.com/go/cdo-securex-link> を参照してください。

まだアカウントがない場合は、次の手順を実行してください。

- Cisco Security Cloud (旧 SecureX) アカウントを作成します。作成方法については、[CDO のマニュアル](#)を参照してください。
- CDO テナントをリクエストします。新しい CDO テナントのリクエストについては、[CDO のマニュアル](#)を参照してください。

- e) Management Center を Cisco Security Cloud (旧 SecureX) と統合します。リンクをクリックして、Management Center の [SecureXとの統合 (SecureX Integration)] ページを開きます。

[SecureXの有効化 (Enable SecureX)] をクリックして別のブラウザタブを開き、Cisco Security Cloud アカウントにログインし、表示されたコードを確認します。このページがポップアップブロッカーによってブロックされていないことを確認してください。

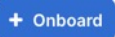
詳細については、を参照してください。

Management Center と Cisco Security Cloud を統合した後、CDO はオンプレミスの Management Center をオンボーディングします。CDO は、ゼロタッチプロビジョニング を動作させるためにインベントリに Management Center を必要とします。CDO による Management Center のサポートは、デバイスのオンボーディング、管理対象デバイスの表示、Management Center に関連付けられたオブジェクトの表示、および Management Center の相互起動に限定されています。

(注) Management Center ハイアベイラビリティペアの場合は、セカンダリ Management Center を Cisco Security Cloud と統合する必要もあります。

- f) まだ開いていない場合は[CDOの起動 (Launch CDO)] をクリックするか、右記からログインします：<https://www.defenseorchestrator.com/>。

CDO がポップアップブロッカーによってブロックされていないことを確認してください。

ステップ 2 CDO ダッシュボード (<https://www.defenseorchestrator.com/>) で、[オンボード (Onboard)] () をクリックします。

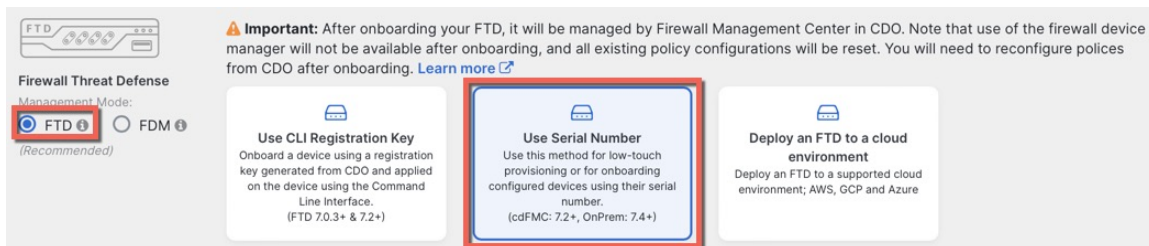
ステップ 3 [FTD] タイルをクリックします。

図 11: FTD タイル



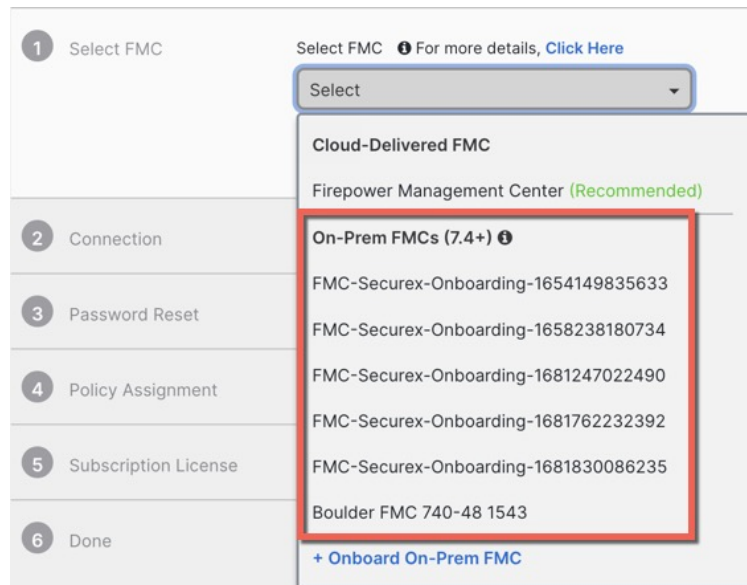
ステップ 4 [FTDデバイスの導入準備 (Onboard FTD Device)] 画面で、[シリアル番号の使用 (Use Serial Number)] をクリックします。

図 12: シリアル番号を使用



ステップ 5 [FMCの選択 (Select FMC)] で、リストから [オンプレミスFMC (On-Prem FMC)] を選択し、[次へ (Next)] をクリックします。

図 13: FMC の選択



Management Center にパブリック IP アドレスまたは FQDN が設定されている場合は、選択後に表示されます。

図 14: パブリック IP アドレス/FQDN



デバイスにパブリック IP アドレス/FQDN がない場合、またはゼロタッチプロビジョニングに管理インターフェイスを使用する場合は、Management Center にパブリック IP アドレス/FQDN が必要です。[FMCパブリックIP (FMC Public IP)] リンクをクリックすると、Management Center パブリック IP アドレス/FQDN を設定できます。次のダイアログボックスが表示されます。



図 15: FMCパブリック IP/FQDNの設定

(注) Management Center ハイアベイラビリティペアの場合は、セカンダリ Management Center でパブリック IP アドレス/FQDN を設定する必要もあります。CDO を使用して値を設定することはできません。セカンダリ Management Center で設定する必要があります。を参照してください。

**ステップ 6** [接続 (Connection)] で、デバイスのシリアル番号とデバイス名を入力します。[Next] をクリックします。

図 16: 接続

**ステップ 7** [パスワードのリセット (Password Reset)] で、[はい... (Yes...)] をクリックします。 。デバイスの新しいパスワードを入力し、この新しいパスワードを確認して、[次へ (Next)] をクリックします。

ゼロタッチプロビジョニングの場合、デバイスは新規であるか、再イメージ化されている必要があります。

(注) デバイスにログインしてパスワードをリセットし、ゼロタッチプロビジョニングを無効にするように設定を変更しなかった場合は、[いいえ... (No...)] オプションを選択する必要があります。ゼロタッチプロビジョニングを無効にする設定は多数あるため、再イメージ化などの必要がある場合を除き、デバイスにログインすることは推奨されません。

図 17: パスワードのリセット

3 Password Reset

1 Please review all the prerequisites for onboarding with a serial number. [Learn more](#)

2 Is this a new device that has never been logged into or configured for a manager?

Yes, this new device has never been logged into or configured for a manager

Enter a new password for devices that have never been configured for a manager.

**Important:** If you select this option and the device's default password has already been changed, onboarding fails.

New Password

Confirm Password

No, this device has been logged into and configured for a manager

Use this option if you already changed the password in the device CLI.

**Important:** If you select this option and the device's default password has not been changed, onboarding fails.

Next

6 Password must:

- Be 8-128 characters
- Have at least one lower and one upper case letter
- Have at least one digit
- Have at least one special character.
- Not contain consecutive repeated letters

**ステップ 8** [ポリシー割り当て (Policy Assignment)] で、ドロップダウンメニューを使用して、デバイスのアクセスコントロールポリシーを選択します。Management Center にポリシーを追加していない場合は、ここで Management Center に移動し、追加する必要があります。[Next] をクリックします。

図 18: ポリシー割り当て

4 Policy Assignment

Access Control Policy

Default Access Control Policy ▼

Next

**ステップ 9** [サブスクリプションライセンス (Subscription License)] で、デバイスのライセンスを選択します。[Next] をクリックします。

図 19: サブスクリプションライセンス

License Type	Includes
<input checked="" type="checkbox"/> Essentials	Base Firewall Capabilities
<input checked="" type="checkbox"/> Carrier (7.3+ FTDs only)	GTP/GPRS, Diameter, SCTP, M3UA
<input checked="" type="checkbox"/> IPS	Intrusion Policy
<input checked="" type="checkbox"/> Malware Defense	File Policy
<input checked="" type="checkbox"/> URL	URL Reputation
<input type="checkbox"/> RA VPN	RA VPN

Next

Enable subscription licenses. CDO will attempt to enable the selected licenses when the device is connected to CDO and registered with the supplied Smart License. Learn more about [Cisco Smart Accounts](#).

ステップ 10 [終了 (Done)] で、CDO に表示されるデバイスにラベルを追加できます。これらは Management Center では使用されません。

図 20: 終了

6 Done

Your device is now onboarding.

This may take a long time to finish. You can check the status of the device on the Devices and Services page.

Add Labels

Add label groups and labels +

Go to Inventory

Management Center で、デバイスが [デバイス管理 (Device Management)] ページに追加されます。[インベントリに移動 (Go to Inventory)] をクリックして、CDO 内のデバイスを表示することもできます。オンプレミス Management Center デバイスは、情報目的で CDO インベントリに表示できます。

外部インターフェイスでゼロタッチプロビジョニングを使用する場合、CDO は DDNS プロバイダーとして機能し、以下を実行します。

- 「fmcOnly」方式を使用して外部で DDNS を有効にします。この方式は、ゼロタッチプロビジョニング デバイスでのみサポートされます。
- 外部 IP アドレスをホスト名 **serial-number.local** にマッピングします。
- IP アドレス/ホスト名マッピングを Management Center に提供し、ホスト名を正しい IP アドレスに解決できるようにします。
- DHCP リースが更新された場合など、IP アドレスが変更された場合に Management Center に通知します。

管理インターフェイスでゼロタッチプロビジョニングを使用する場合、DDNS はサポートされません。デバイスが管理接続を開始できるように、Management Center はパブリックに到達可能である必要があります。

CDO を引き続き DDNS プロバイダーとして使用することも、後で Management Center の DDNS 設定を別の方式に変更することもできます。

---

## 手動による Management Center へのデバイスの追加

デバイスの IP アドレスまたはホスト名と登録キーを使用して、手動で Threat Defense を Management Center

### 手順

---

- ステップ 1 Management Center で、[デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択します。
- ステップ 2 [追加 (Add)] ドロップダウン リストから、[デバイスの追加 (Add Device)] を選択します。  
登録キー方式がデフォルトで選択されています。

図 21: 登録キーを使用したデバイスの追加

**Add Device** ?

Select the Provisioning Method:

Registration Key  Serial Number

CDO Managed Device

Host:†

Display Name:

Registration Key: \*

Group:

Access Control Policy: \*

**Smart Licensing**

Note: All virtual Firewall Threat Defense devices require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click [here](#) for information about the Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

Carrier  
 Malware Defense  
 IPS  
 URL

**Advanced**

Unique NAT ID: †

Transfer Packets

次のパラメータを設定します。

- [ホスト (Host) ] : 追加する Threat Defense の IP アドレスかホスト名を入力します。Threat Defense の最初の設定で Management Center の IP アドレスと NAT ID の両方を指定した場合は、このフィールドを空のままにしておくことができます。

(注) HA 環境では、両方の Management Center が NAT の背後にある場合、プライマリ Management Center のホスト IP または名前なしで Threat Defense を登録できます。ただし、Threat Defense をセカンダリ Management Center に登録するには、Threat Defense の IP アドレスかホスト名を指定する必要があります。

- [表示名 (Display Name) ] フィールドに、Management Center に表示する Threat Defense の名前を入力します。
- [登録キー (Registration key) ] : Threat Defense の最初の設定で指定したものと同一登録キーを入力します。
- [ドメイン (Domain) ] : マルチドメイン環境を使用している場合は、デバイスをリーフドメインに割り当てます。
- [グループ (Group) ] : グループを使用している場合は、デバイスグループに割り当てます。
- [アクセスコントロールポリシー (Access Control Policy) ] : 初期ポリシーを選択します。使用する必要があることがわかっているカスタマイズ済みのポリシーがすでにある場合を除いて、[新しいポリシーの作成 (Create new policy) ] を選択し、[すべてのトラフィックをブロック (Block all traffic) ] を選択します。後でこれを変更してトラフィックを許可することができます。「[内部から外部へのトラフィックの許可](#)」を参照してください。

図 22: 新しいポリシー

The screenshot shows a web form titled "New Policy" with a help icon. It contains the following fields and options:

- Name:** A text input field containing "ftd-ac-policy".
- Description:** An empty text input field.
- Select Base Policy:** A dropdown menu currently set to "None".
- Default Action:** Three radio button options:
  - Block all traffic (highlighted with a red box)
  - Intrusion Prevention
  - Network Discovery

At the bottom right, there are two buttons: "Cancel" and "Save".

- **スマートライセンス** : 展開する機能に必要なスマートライセンスを割り当てます。注 : デバイスを追加した後、[システム (System) ] > [ライセンス (Licenses) ] > [スマートライセンス (Smart Licenses) ] ページからセキュアクライアントリモートアクセス VPN のライセンスを適用できます。

- [一意のNAT ID (Unique NAT ID)] : Threat Defense の最初の設定で指定した NAT ID を指定します。
- [パケットの転送 (Transfer Packets)] : デバイスから Management Center へのパケット転送を許可します。このオプションを有効にして IPS や Snort などのイベントがトリガーされた場合は、デバイスが検査用としてイベントメタデータ情報とパケットデータを Management Center に送信します。このオプションを無効にした場合は、イベント情報だけが Management Center に送信され、パケットデータは送信されません。

**ステップ 3** [登録 (Register)] をクリックし、正常に登録されたことを確認します。

登録が成功すると、デバイスがリストに追加されます。失敗した場合は、エラーメッセージが表示されます。Threat Defense が登録に失敗した場合は、次の項目を確認してください。

- ping : Threat Defense CLI にアクセスし、次のコマンドを使用して Management Center の IP アドレスへの ping を実行します。

**ping system ip\_address**

ping が成功しない場合は、**show network** コマンドを使用してネットワーク設定を確認します。Threat Defense 管理 IP アドレスを変更する必要がある場合は、**configure network management-data-interface** コマンドを使用します。

- 登録キー、NAT ID、および Management Center IP アドレス : 両方のデバイスで同じ登録キーを使用していることを確認し、使用している場合は NAT ID を使用していることを確認します。**configure manager add** コマンドを使用して、Threat Defense で登録キーと NAT ID を設定することができます。

トラブルシューティングの詳細については、<https://cisco.com/go/fmc-reg-error> を参照してください。

## 基本的なセキュリティポリシーの設定

ここでは、次の設定を使用して基本的なセキュリティポリシーを設定する方法について説明します。

- 内部インターフェイスと外部インターフェイス : 内部インターフェイスにスタティック IP アドレスを割り当てます。マネージャアクセス設定の一部として外部インターフェイスの基本設定を構成しましたが、まだそのインターフェイスをセキュリティゾーンに割り当てる必要があります。
- DHCP サーバー : クライアントの内部インターフェイスで DHCP サーバーを使用します。
- NAT : 外部インターフェイスでインターフェイス PAT を使用します。
- アクセスコントロール : 内部から外部へのトラフィックを許可します。
- SSH : マネージャアクセス インターフェイスで SSH を有効にします。

## インターフェイスの設定

ロータッチプロビジョニングまたは初期設定に Device Manager を使用する場合、次のインターフェイスが事前設定されます。

- イーサネット 1/1：「外部」、DHCP からの IP アドレス、IPv6 自動設定
- VLAN1：「内部」、192.168.95.1/24
- デフォルトルート：外部インターフェイスで DHCP を介して取得

Management Center に登録する前に Device Manager 内で追加のインターフェイス固有の設定を実行した場合、その設定は保持されます。

いずれにしても、デバイスの登録後に追加のインターフェイス設定を実行する必要があります。インターフェイスの事前設定を行っていない場合は、内部スイッチポートに VLAN1 インターフェイスを追加する必要があります。追加の設定では、必要に応じてスイッチポートをファイアウォールインターフェイスに変換し、インターフェイスをセキュリティゾーンに割り当てて、IP アドレスを変更します。

次の例では、DHCP によるスタティックアドレスとルーテッドモードの外部インターフェイスを使用して (Ethernet1/1)、ルーテッドモードの内部インターフェイス (VLAN1) を設定します。

### 手順

**ステップ 1** [デバイス (Devices) ]、[デバイス管理 (Device Management) ] の順に選択し、デバイスの [編集 (Edit) ] (✎) をクリックします。 >

**ステップ 2** [インターフェイス (Interfaces) ] をクリックします。

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Ethernet1/2		Physical			
Ethernet1/3.1		Subinterface			
Ethernet1/4	diagnostic	Physical			
Ethernet1/5		Physical			

**ステップ 3** (任意) [スイッチポート (SwitchPort) ] 列のスライダをクリックしてスイッチポート (イーサネット 1/2 ~ 1/8) のいずれかのスイッチポートモードを無効にすると、無効 (🔌) と表示されます。

**ステップ 4** スwitchポートを有効にします。

- a) スwitchポートの [編集 (Edit) ] (✎) をクリックします。



**Edit Physical Interface** ? x

**General** Hardware Configuration

Interface ID:   Enabled

Description:

Port Mode:  ▼

VLAN ID:  (1 - 4070)

Protected:

OK Cancel

- b) [有効 (Enabled) ] チェックボックスをオンにして、インターフェイスを有効化します。
- c) (任意) VLAN ID を変更します。デフォルトは 1 です。次に、この ID に一致する VLAN インターフェイスを追加します。
- d) [OK] をクリックします。

**ステップ 5** 内部 VLAN インターフェイスを追加します。

- a) [インターフェイスの追加 (Add Interfaces) ]>[VLAN インターフェイス (VLAN Interface) ] をクリックします。

[全般 (General) ] ページが表示されます。

**Add VLAN Interface** ? x

**General** IPv4 IPv6 Advanced

Name:   Enabled

Description:

Mode:  ▼

Security Zone:  ▼

MTU:  (64 - 9198)

VLAN ID \*:  (1 - 4070)

Disable Forwarding on Interface Vlan:  ▼

Associated Interface	Port Mode
No records to display	

OK Cancel

- b) 48 文字までの [名前 (Name)] を入力します。  
たとえば、インターフェイスに **inside** という名前を付けます。
- c) [有効 (Enabled)] チェックボックスをオンにします。
- d) [モード (Mode)] は [なし (None)] に設定したままにします。
- e) [セキュリティゾーン (Security Zone)] ドロップダウンリストから既存の内部セキュリティゾーンを選択するか、[新規 (New)] をクリックして新しいセキュリティゾーンを追加します。

たとえば、「inside」という名前のゾーンを追加します。各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てる必要があります。インターフェイスは、1つのセキュリティゾーンにのみ属することも、複数のインターフェイスグループに属することもできます。ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。この場合、トラフィックが内部から外部に移動できるようにアクセスコントロールポリシーを設定することはできますが、外部から内部に向けては設定できません。ほとんどのポリシーはセキュリティゾーンのみをサポートしています。NATポリシー、プレフィルタポリシー、およびQoSポリシーで、ゾーンまたはインターフェイスグループを使用できます。

- f) [VLAN ID] を **1** に設定します。

デフォルトでは、すべてのスイッチポートは VLAN 1 に設定されます。ここで別の VLAN ID を選択する場合は、新しい VLAN ID の各スイッチポートを編集する必要があります。

インターフェイスを保存した後、VLAN ID を変更することはできません。ここでの VLAN ID は、使用される VLAN タグと設定内のインターフェイス ID の両方です。

- g) [IPv4] と [IPv6] のいずれかまたは両方のページをクリックします。

- [IPv4]: ドロップダウンリストから [スタティックIPを使用する (Use Static IP)] を選択し、IP アドレスとサブネットマスクをスラッシュ表記で入力します。

たとえば、**192.168.1.56/24** と入力します。

The screenshot shows the 'Edit Physical Interface' configuration window. The 'IPv4' tab is active. Under 'IP Type', 'Use Static IP' is selected. The 'IP Address' field contains '192.168.1.1/24'. To the right of the IP address field, there is a note: 'eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25'.

- [IPv6]: ステートレス自動設定の場合は [自動設定 (Autoconfiguration)] チェックボックスをオンにします。

- h) [OK] をクリックします。

**ステップ 6** 外部用に使用する Ethernet1/1 の [編集 (Edit)] (✎) をクリックします。

[全般 (General)] ページが表示されます。

マネージャアクセス用にこのインターフェイスを事前に設定しているため、インターフェイスにはすでに名前が付けられており、有効化とアドレス指定が完了しています。これらの基本設定は変更しないでください。変更すると、Management Center の管理接続が中断されます。この画面でも、通過トラフィックポリシーのセキュリティゾーンを設定する必要があります。

- a) [セキュリティゾーン (Security Zone)] ドロップダウンリストから既存の外部セキュリティゾーンを選択するか、[新規 (New)] をクリックして新しいセキュリティゾーンを追加します。

たとえば、「outside」という名前のゾーンを追加します。

- b) [OK] をクリックします。

**ステップ 7** [保存 (Save)] をクリックします。

## DHCP サーバーの設定

クライアントで DHCP を使用して脅威に対する防御から IP アドレスを取得するようにする場合は、DHCP サーバーを有効にします。

### 手順

**ステップ 1** [デバイス (Devices)]、[デバイス管理 (Device Management)] の順に選択し、デバイスの [編集 (Edit)] (✎) をクリックします。 >

**ステップ 2** [DHCP] > [DHCPサーバー (DHCP Server)] を選択します。

図 23: DHCP サーバー

The screenshot shows the DHCP configuration interface. On the left, there is a sidebar with 'DHCP Server' selected. The main area contains several input fields and checkboxes. A red box highlights the '+ Add' button in the bottom right corner of the configuration area.

ステップ3 [サーバー (Server)] ページで、[追加 (Add)] をクリックして、次のオプションを設定します。

図 24: サーバーの追加

The 'Add Server' dialog box is shown. It has three main sections: 'Interface\*' with a dropdown menu showing 'inside', 'Address Pool\*' with a text input field containing '10.9.7.9-10.9.7.25', and a checked checkbox labeled 'Enable DHCP Server'. At the bottom, there are 'Cancel' and 'OK' buttons.

- [インターフェイス (Interface)] : ドロップダウンリストからインターフェイスを選択します。
- [アドレスプール (Address Pool)] : DHCP サーバーが使用する IP アドレスの最下位から最上位の間の範囲を設定します。IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることはできません。
- [DHCPサーバーを有効にする (Enable DHCP Server)] : 選択したインターフェイスの DHCP サーバーを有効にします。

ステップ4 [OK] をクリックします。

ステップ 5 [保存 (Save) ] をクリックします。

## NAT の設定

一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポート アドレス変換 (PAT) と呼びます。

### 手順

ステップ 1 [デバイス (Devices) ]>[NAT] をクリックし、[新しいポリシー (New Policy) ]>[Threat Defense NAT] をクリックします。

ステップ 2 ポリシーに名前を付け、ポリシーを使用するデバイスを選択し、[保存 (Save) ] をクリックします。

図 25: 新しいポリシー

New Policy

Name:  
interface\_PAT

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Search by name or value

10.10.0.6  
10.10.0.7

Add to Policy

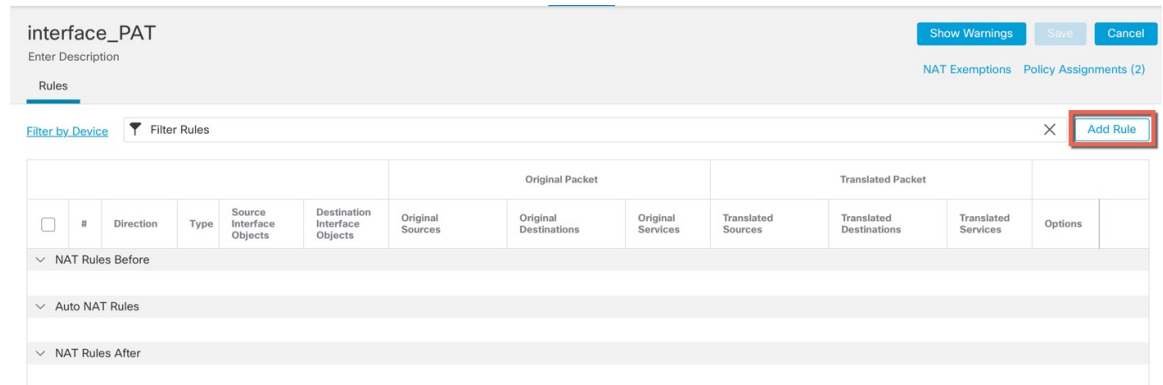
Selected Devices

10.10.0.6  
10.10.0.7

Cancel Save

ポリシーが Management Center に追加されます。引き続き、ポリシーにルールを追加する必要があります。

図 26: NAT ポリシー

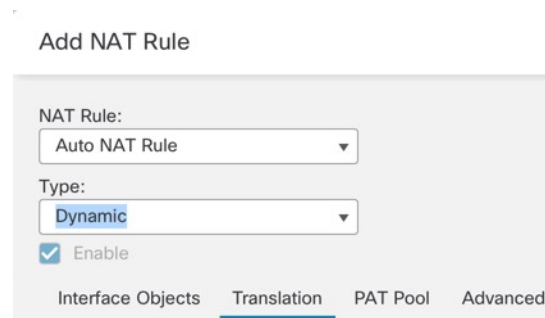


**ステップ 3** [ルール の追加 (Add Rule) ] をクリックします。

[NATルール の追加 (Add NAT Rule) ] ダイアログボックスが表示されます。

**ステップ 4** 基本ルール のオプションを設定します。

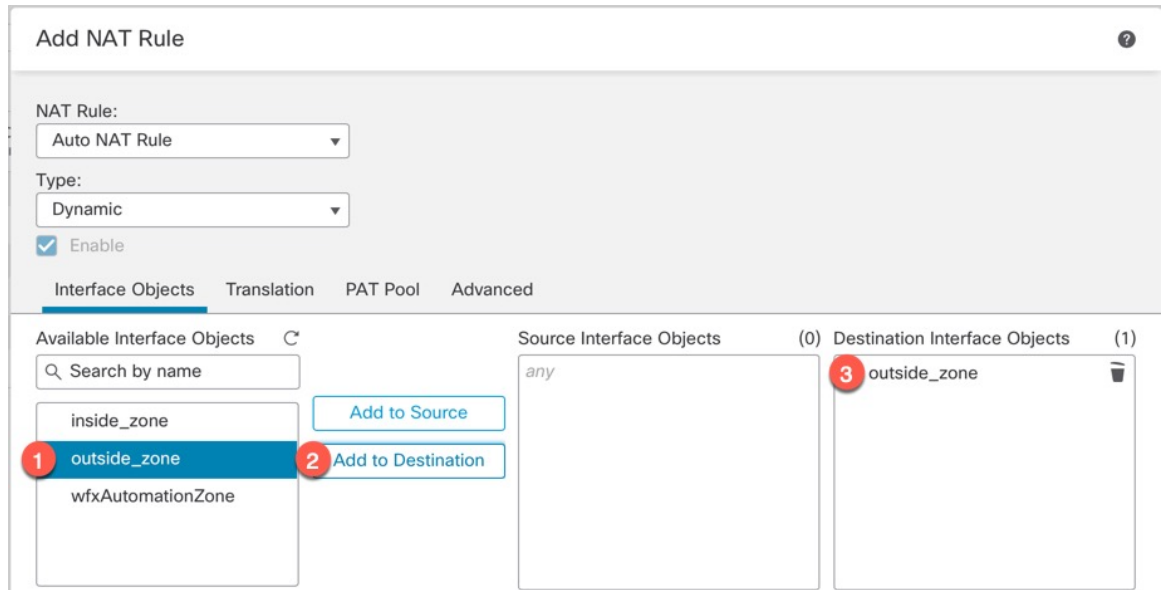
図 27: 基本ルール のオプション



- [NATルール (NAT Rule) ] : [自動NATルール (Auto NAT Rule) ] を選択します。
- [タイプ (Type) ] : [ダイナミック (Dynamic) ] を選択します。

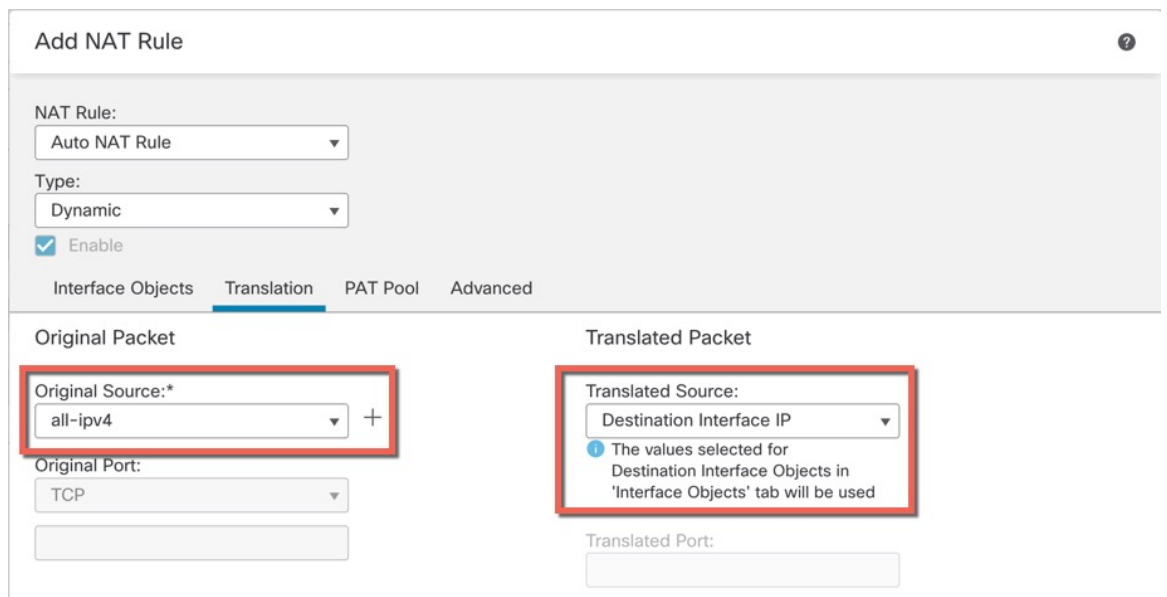
**ステップ 5** [インターフェイスオブジェクト (Interface objects) ] ページで、[使用可能なインターフェイスオブジェクト (Available Interface Objects) ] 領域から [宛先インターフェイスオブジェクト (Destination Interface Objects) ] 領域に外部ゾーンを追加します。

図 28: インターフェイス オブジェクト



ステップ 6 [変換 (Translation) ] ページで、次のオプションを設定します。

図 29: トランスレーション



- [元の送信元 (Original Source) ] : Add (+) をクリックして、すべての IPv4 トラフィック (0.0.0.0/0) のネットワークオブジェクトを追加します。

図 30: 新しいネットワークオブジェクト

(注) 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [変換済みの送信元 (Translated Source) ] : [宛先インターフェイス IP (Destination Interface IP) ] を選択します。

**ステップ 7** [保存 (Save) ] をクリックしてルールを追加します。

ルールが [ルール (Rules) ] テーブルに保存されます。

**ステップ 8** NAT ページで [保存 (Save) ] をクリックして変更を保存します。

## 内部から外部へのトラフィックの許可

脅威に対する防御を登録したときに、基本の [すべてのトラフィックをブロック (Block all traffic) ] アクセスコントロールポリシーを作成した場合は、デバイスを通るトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

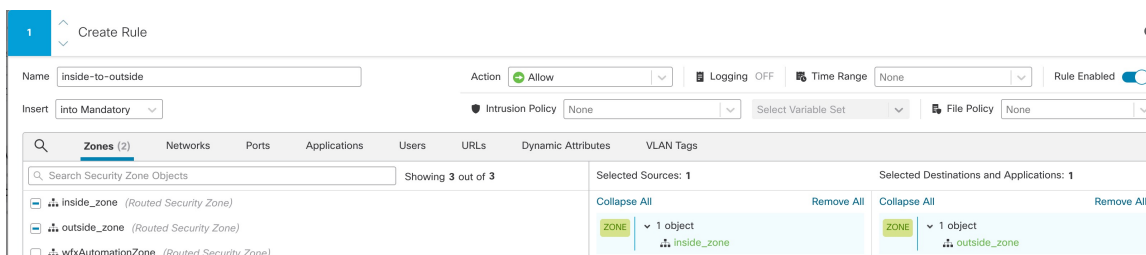
### 手順

**ステップ 1** [ポリシー (Policy) ]、[アクセスポリシー (Access Policy) ]、[アクセスポリシー (Access Policy) ] の順に選択し、脅威に対する防御に割り当てられているアクセスコントロールポリシーの [編集 (Edit) ] (✎) をクリックします。 > >



ステップ 2 [ルールを追加 (Add Rule)] をクリックし、次のパラメータを設定します。

図 31: ルールの追加



- [名前 (Name)] : このルールに名前を付けます (たとえば、**inside-to-outside**) 。
- [選択した送信元 (Selected Sources)] : [ゾーン (Zones)] から内部ゾーンを選択し、[送信元ゾーンを追加 (Add Source Zone)] をクリックします。
- [選択した宛先とアプリケーション (Selected Destinations and Applications)] : [ゾーン (Zones)] から外部ゾーンを選択し、[宛先ゾーンを追加 (Add Destination Zone)] をクリックします。

他の設定はそのままにしておきます。

ステップ 3 [Apply] をクリックします。

ルールが [ルール (Rules)] テーブルに追加されます。

ステップ 4 [保存 (Save)] をクリックします。

## マネージャ アクセス データ インターフェイスでの SSH の設定

外部インターフェイスなどのデータインターフェイスで Management Center アクセスを有効にした場合は、この手順に従ってそのインターフェイスで SSH を有効にする必要があります。ここでは、Threat Defense で 1 つ以上のデータインターフェイスに対して SSH 接続を有効にする方法について説明します。



(注) SSH は管理インターフェイス上でデフォルトで有効になっていますが、この画面は管理 SSH アクセスに影響しません。

管理インターフェイスは、デバイスの他のインターフェイスとは分離されています。Management Center にデバイスを設定し、登録するために使用されます。データ インターフェイスの SSH は、管理インターフェイスの SSH と内部および外部ユーザー リストを共有します。その他の設定は個別に設定されます。データ インターフェイスでは、この画面を使用して SSH とアクセス リストを有効にします。データ インターフェイスの SSH トラフィックは通常のルーティング設定を使用し、設定時に設定されたスタティック ルートや CLI で設定されたスタティック ルートは使用しません。

管理インターフェイスの場合、SSH アクセスリストを構成するには [Cisco Secure Firewall Threat Defense コマンドリファレンス](#) の `configure ssh-access-list` コマンドを参照してください。スタティック ルートを設定するには、`configure network static-routes` コマンドを参照してください。デフォルトでは、初期設定時に管理インターフェイスからデフォルトルートを設定しません。

SSH を使用するには、ホスト IP アドレスを許可するアクセスルールは必要ありません。このセクションの手順に従って、SSH アクセスを設定する必要があるだけです。

SSH は、到達可能なインターフェイスにのみ使用できます。SSH ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。

SSH は、次の暗号およびキー交換をサポートしています。

- 暗号化 : aes128-cbc、aes192-cbc、aes256-cbc、aes128-ctr、aes192-ctr、aes256-ctr
- 完全性 : hmac-sha2-256
- キー交換 : dh-group14-sha256



(注) SSH を使用した CLI へのログイン試行が 3 回連続して失敗すると、デバイスの SSH 接続は終了します。

#### 始める前に

- SSH 内部ユーザーは、`configure user add` コマンドを使用して CLI でのみ設定できます。。デフォルトでは、初期設定時にパスワードを設定した **Admin** ユーザーが存在します。LDAP または RADIUS 上の外部ユーザーは、プラットフォーム設定で [外部認証 (External Authentication)] を設定することによっても設定できます。
- デバイスへの SSH 接続を許可するホストまたはネットワークを定義するネットワーク オブジェクトが必要です。オブジェクトをプロシージャの一部として追加できますが、IP アドレスのグループを特定するためにオブジェクトグループを使用する場合は、ルールで必要なグループがすでに存在することを確認します。[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択して、オブジェクトを設定します。



(注) システムが提供する **any** ネットワーク オブジェクトは使用できません。代わりに、**any-ipv4** または **any-ipv6** を使用します。

#### 手順

**ステップ 1** [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Threat Defense ポリシーを作成または編集します。

**ステップ 2** [SSHアクセス (SSH Access)] を選択します。

**ステップ 3** SSH 接続を許可するインターフェイスと IP アドレスを指定します。

この表を使用して、SSH 接続を受け入れるインターフェイス、およびそれらの接続を許可されるクライアントの IP アドレスを制限します。個々の IP アドレスはなく、ネットワーク アドレスを使用できます。

- a) [追加 (Add)] をクリックして新しいルールを追加するか、[編集 (Edit)] をクリックして既存のルールを編集します。
- b) ルールのプロパティを設定します。
  - [IP Address] : SSH 接続を許可するホストまたはネットワークを特定するネットワークオブジェクトまたはグループ。オブジェクトをドロップダウンメニューから選択するか、または [+] をクリックして新しいネットワークオブジェクトを追加します。
  - [使用可能なゾーン/インターフェイス (Available Zones/Interfaces)] : SSH 接続を許可するインターフェイスを含むゾーンを追加します。ゾーンにないインターフェイスでは、[選択したゾーン/インターフェイス (Selected Zones/Interfaces)] リストの下のフィールドにインターフェイス名を入力し、[追加 (Add)] をクリックします。ルールバックインターフェイスを追加することもできます。選択されているインターフェイスまたはゾーンがデバイスに含まれているときにのみ、これらのルールがデバイスに適用されます。
- c) [OK] をクリックします。

**ステップ 4** [Save (保存)] をクリックします。

これで、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更はポリシーを展開するまで有効になりません。

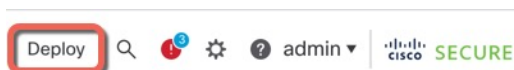
## 設定の展開

設定の変更を脅威に対する防御に展開します。変更を展開するまでは、デバイス上でどの変更もアクティブになりません。

### 手順

**ステップ 1** 右上の [展開 (Deploy)] をクリックします。

図 32: 展開



**ステップ 2** 迅速な展開の場合は、特定のデバイスのチェックボックスをオンにして [展開 (Deploy)] をクリックするか、[すべて展開 (Deploy All)] をクリックしてすべてのデバイスを展開します。

それ以外の場合は、追加の展開オプションを設定するために、[高度な展開 (Advanced Deploy)] をクリックします。

図 33: すべて展開

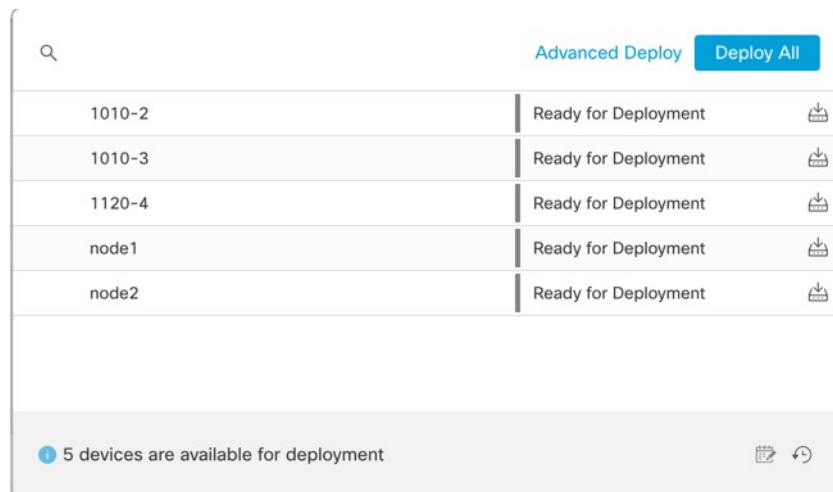
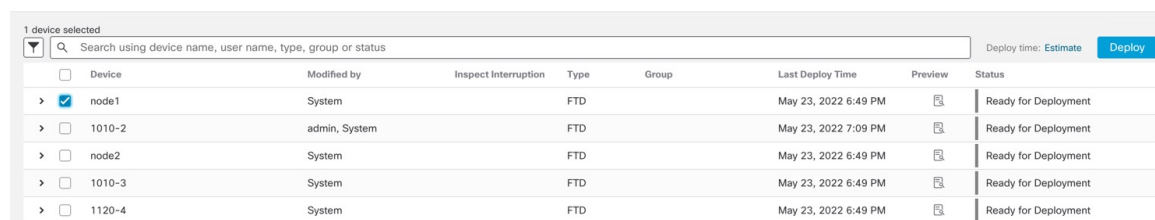
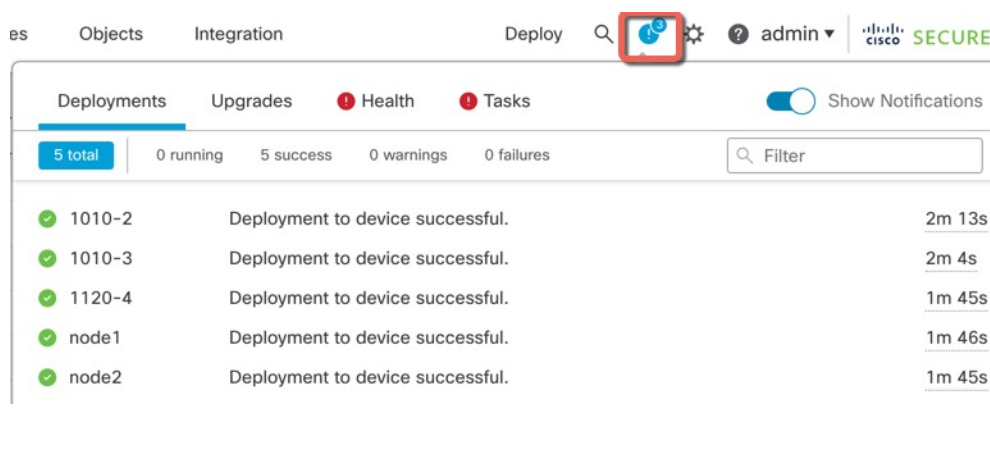


図 34: 高度な展開



**ステップ 3** 展開が成功したことを確認します。展開のステータスを表示するには、メニューバーの [展開 (Deploy)] ボタンの右側にあるアイコンをクリックします。

図 35: 展開ステータス



## Threat Defense および FXOS CLI へのアクセス

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

トラブルシューティングのためにも FXOS CLI にアクセスできます。



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

### 手順

**ステップ 1** CLI にログインするには、管理コンピュータをコンソールポートに接続します。Firepower 1000 には、USB A to B シリアルケーブルが付属しています。ご使用のオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください。コンソールポートはデフォルトで FXOS CLI になります。次のシリアル設定を使用します。

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

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

例 :

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

firepower#
```

**ステップ 2** Threat Defense CLI にアクセスします。

**connect ftd**

例 :

```
firepower# connect ftd
>
```

ログイン後に、CLI で使用可能なコマンドの情報を確認するには、**help** または **?** を入力します。使用方法については、『Cisco Secure Firewall Threat Defense コマンドリファレンス』を参照してください。

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

このコマンドにより、FXOS CLI プロンプトに戻ります。FXOS CLI で使用可能なコマンドについては、**?** を入力してください。

例：

```
> exit
firepower#
```

## データインターフェイスでの管理接続のトラブルシューティング

モデルのサポート：Threat Defense

専用の管理インターフェイスを使用する代わりに、Management Center にデータインターフェイスを使用する場合は、Management Center で脅威に対する防御のインターフェイスとネットワークの設定を変更するときに接続を中断しないように注意します。脅威に対する防御を Management Center に追加した後に管理インターフェイスタイプを変更する場合（データから管理へ、または管理からデータへ）、インターフェイスとネットワークの設定が正しく構成されていないと、管理接続が失われる可能性があります。

このトピックは、管理接続が失われた場合のトラブルシューティングに役立ちます。

### 管理接続ステータスの表示

Management Center で、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [管理 (Management)] > [FMC アクセスの詳細 (FMC Access Details)] > [接続ステータス (Connection Status)] ページの順に選択して管理接続のステータスを確認します。

管理接続のステータスを表示するには、脅威に対する防御 CLI で、**sftunnel-status-brief** コマンドを入力します。**sftunnel-status** を使用して、より完全な情報を表示することもできます。

ダウン状態の接続の出力例を次に示します。ピアチャネルの「接続先」情報やハートビート情報が表示されていません。

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
```

```
Last disconnect reason : Both control and event channel connections with peer went down
```

アップ状態の接続の出力例を次に示します。ピアチャンネルとハートビート情報が表示されています。

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to
'10.10.17.202' via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to
'10.10.17.202' via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

### Threat Defense ネットワーク情報の表示

脅威に対する防御 CLI で、管理および Management Center アクセス データ インターフェイスのネットワーク設定を表示します。

#### show network

```
> show network
===== [ System Information ] =====
Hostname           : 5516X-4
DNS Servers        : 208.67.220.220,208.67.222.222
Management port    : 8305
IPv4 Default route
  Gateway           : data-interfaces
IPv6 Default route
  Gateway           : data-interfaces

===== [ brl ] =====
State              : Enabled
Link               : Up
Channels           : Management & Events
Mode               : Non-Autonegotiation
MDI/MDIX           : Auto/MDIX
MTU                : 1500
MAC Address        : 28:6F:7F:D3:CB:8D
----- [ IPv4 ] -----
Configuration      : Manual
Address            : 10.99.10.4
Netmask            : 255.255.255.0
Gateway            : 10.99.10.1
----- [ IPv6 ] -----
Configuration      : Disabled

===== [ Proxy Information ] =====
State              : Disabled
Authentication     : Disabled

===== [ System Information - Data Interfaces ] =====
DNS Servers        :
Interfaces         : GigabitEthernet1/1

===== [ GigabitEthernet1/1 ] =====
State              : Enabled
```

```

Link                : Up
Name                : outside
MTU                 : 1500
MAC Address         : 28:6F:7F:D3:CB:8F
-----[ IPv4 ]-----
Configuration       : Manual
Address             : 10.89.5.29
Netmask             : 255.255.255.192
Gateway             : 10.89.5.1
-----[ IPv6 ]-----
Configuration       : Disabled

```

### Management Center への Threat Defense の登録の確認

脅威に対する防御 CLI で、Management Center 登録が完了したことを確認します。このコマンドは、管理接続の現在のステータスを表示するものではないことに注意してください。

#### show managers

```

> show managers
Type                : Manager
Host                : 10.89.5.35
Registration        : Completed
>

```

### Management Center に ping する

脅威に対する防御 CLI で、次のコマンドを使用して、データインターフェイスから Management Center に ping します。

#### ping fmc\_ip

脅威に対する防御 CLI で、次のコマンドを使用して、管理インターフェイスから Management Center に ping します。これは、バックプレーンを介してデータインターフェイスにルーティングされます。

#### ping system fmc\_ip

### Threat Defense 内部インターフェイスでのパケットのキャプチャ

脅威に対する防御 CLI で、内部バックプレーンインターフェイス (nlp\_int\_tap) でパケットをキャプチャして、管理パケットが送信されているかどうかを確認します。

#### capture name interface nlp\_int\_tap trace detail match ip any any

#### show capture name trace detail

### 内部インターフェイスのステータス、統計、およびパケット数の確認

脅威に対する防御 CLI で、内部バックプレーンインターフェイス (nlp\_int\_tap) に関する情報を参照してください。

#### show interace detail

```

> show interface detail
[...]
```



```

Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
  (Full-duplex), (1000 Mbps)
  Input flow control is unsupported, output flow control is unsupported
  MAC address 0000.0100.0001, MTU 1500
  IP address 169.254.1.1, subnet mask 255.255.255.248
  37 packets input, 2822 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  5 packets output, 370 bytes, 0 underruns
  0 pause output, 0 resume output
  0 output errors, 0 collisions, 0 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 0 output reset drops
  input queue (blocks free curr/low): hardware (0/0)
  output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
  37 packets input, 2304 bytes
  5 packets output, 300 bytes
  37 packets dropped
    1 minute input rate 0 pkts/sec,  0 bytes/sec
    1 minute output rate 0 pkts/sec,  0 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec,  0 bytes/sec
    5 minute output rate 0 pkts/sec,  0 bytes/sec
    5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
  Interface number is 14
  Interface config status is active
  Interface state is active

```

## ルーティングと NAT の確認

脅威に対する防御 CLI で、デフォルトルート (S\*) が追加されていること、および管理インターフェイス (nlp\_int\_tap) に内部 NAT ルールが存在することを確認します。

### show route

```

> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF

Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*      0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C       10.89.5.0 255.255.255.192 is directly connected, outside
L       10.89.5.29 255.255.255.255 is directly connected, outside

>

```

### show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface
service tcp 8305 8305
   translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface service
tcp ssh
   translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6 service tcp 8305 8305
   translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
   translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
   translate_hits = 0, untranslate_hits = 0
>
```

### その他の設定の確認

次のコマンドを参照して、他のすべての設定が存在することを確認します。これらのコマンドの多くは、Management Center の [デバイス (Devices) ]>[デバイス管理 (Device Management) ]>[デバイス (Device) ]>[管理 (Management) ]>[FMCアクセスの詳細 (FMC Access Details) ]>[CLI出力 (CLI Output) ] ページでも確認できます。

#### show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

#### show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

#### show conn address fmc\_ip

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
   preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap 10.89.5.29(169.254.1.2):51231 outside 10.89.5.35:8305, idle 0:00:04,
bytes 86684, flags UxIO
TCP nlp_int_tap 10.89.5.29(169.254.1.2):8305 outside 10.89.5.35:52019, idle 0:00:02,
bytes 1630834, flags UIO
>
```

### DDNS の更新が成功したかどうかを確認する

脅威に対する防御 CLI で、DDNS の更新が成功したかどうかを確認します。

#### debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfully updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
```

```
DDNS: IDB SB total = 0
```

更新に失敗した場合は、**debug http** コマンドと **debug ssl** コマンドを使用します。証明書の検証が失敗した場合は、ルート証明書がデバイスにインストールされていることを確認します。

```
show crypto ca certificates trustpoint_name
```

DDNS の動作を確認するには :

```
show ddns update interface fmc_access_ifc_name
```

```
> show ddns update interface outside
```

```
Dynamic DNS Update on outside:  
  Update Method Name Update Destination  
  RBD_DDNS not available
```

```
Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020  
Status : Success  
FQDN : domain.example.org  
IP addresses : 209.165.200.225
```

### Management Center ログファイルの確認

<https://cisco.com/go/fmc-reg-error> を参照してください。

## ファイアウォールの電源の切断

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたりすると、重大なファイルシステムの損傷を引き起こすことがあります。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おり、電源プラグを抜いたり、電源を切断したりすると、ファイアウォールシステムをグレースフルシャットダウンできないことを覚えておいてください。

Firepower 1010 シャーシには外部電源スイッチはありません。Management Center のデバイス管理ページを使用してデバイスの電源を切断するか、FXOS CLI を使用できます。

### Management Center を使用したファイアウォールの電源の切断

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたり、電源スイッチを押したりすると、重大なファイルシステムの損傷を引き起こすことがあります。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、電源プラグを抜いたり、電源を切断したりすると、ファイアウォールをグレースフルシャットダウンできないことを覚えておいてください。

Management Center を使用してシステムを適切にシャットダウンできます。

#### 手順

---

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

- ステップ2** 再起動するデバイスの横にある **[編集 (Edit)]** (✎) をクリックします。
- ステップ3** **[デバイス (Device)]** タブをクリックします。
- ステップ4** **[システム (System)]** セクションで **[デバイスのシャットダウン (Shut Down Device)]** (✕) をクリックします。
- ステップ5** プロンプトが表示されたら、デバイスのシャットダウンを確認します。
- ステップ6** コンソールからファイアウォールに接続している場合は、ファイアウォールがシャットダウンするときにシステムプロンプトをモニターします。次のプロンプトが表示されます。

```
System is stopped.
It is safe to power off now.
```

```
Do you want to reboot instead? [y/N]
```

コンソールから接続していない場合は、約3分間待つてシステムがシャットダウンしたことを確認します。

- ステップ7** 必要に応じて電源プラグを抜いてシャーシから物理的に電源を取り外すことができます。

## CLI でのデバイスの電源オフ

FXOS CLI を使用すると、システムを安全にシャットダウンし、デバイスの電源をオフにできます。CLI には、コンソールポートに接続してアクセスします。[Threat Defense および FXOS CLI へのアクセス \(53 ページ\)](#) を参照してください。

### 手順

- ステップ1** FXOS CLI で local-mgmt に接続します。

```
firepower # connect local-mgmt
```

- ステップ2** **shutdown** コマンドを発行します。

```
firepower(local-mgmt) # shutdown
```

例：

```
firepower(local-mgmt)# shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense.....ok
```

- ステップ3** ファイアウォールのシャットダウン時にシステムプロンプトをモニターします。次のプロンプトが表示されます。

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

**ステップ 4** 必要に応じて電源プラグを抜いてシャーシから物理的に電源を取り外すことができます。

---

## 次のステップ

Threat Defense の設定を続行するには、「[Cisco Secure Firewall Threat Defense ドキュメントにアクセス](#)」にあるお使いのソフトウェアバージョンのマニュアルを参照してください。

Management Center の使用に関する情報については、「[Cisco Secure Firewall Management Center デバイス構成ガイド](#)」を参照してください。



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。