デバイス管理

このガイドは、プライマリマネージャまたは分析専用マネージャとしてのオンプレミスの Secure Firewall Management Center に適用されます。Cisco Defense Orchestrator（CDO）クラウド提供型 Firewall Management Center をプライマリマネージャとして使用する場合、オンプレミスの Firewall Management Center は分析のみに使用できます。クラウド提供型 Firewall Management Center の管理にはこのガイドを使用しないでください。「Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理」を参照してください。

Secure Firewall Management Center でデバイスを追加および管理できます。

デバイス管理について

Firewall Management Center を使用してデバイスを管理します。

Firewall Management Center およびデバイス管理について

Firewall Management Center がデバイスを管理するときは、デバイスとの間に、双方向の SSL 暗号化通信チャネルをセットアップします。Firewall Management Center はこのチャネルを使用して、そのデバイスへのネットワーク トラフィックの分析および管理の方法に関する情報をそのデバイスに送信します。そのデバイスはトラフィックを評価すると、イベントを生成し、同じチャネルを使用してそれらのイベントを Firewall Management Center に送信します。

Firewall Management Center を使用してデバイスを管理すると、以下の利点があります。

- すべてのデバイスのポリシーを一箇所から設定できるため、設定の変更が容易になります。
- さまざまなタイプのソフトウェア アップデートをデバイスにインストールできます。
- 正常性ポリシーを管理対象デバイスに適用して、Firewall Management Center からデバイスのヘルス ステータスをモニターできます。

（注） CDO 管理対象デバイスがあり、オンプレミス Firewall Management Center を分析のみに使用している場合、オンプレミス Firewall Management Center はポリシーの設定またはアップグレードをサポートしません。デバイス設定およびその他のサポートされていない機能に関連するこのガイドの章と手順は、プライマリマネージャが CDO のデバイスには適用されません。

Firewall Management Center は、侵入イベント、ネットワーク検出情報、およびデバイスのパフォーマンスデータを集約して相互に関連付けます。そのため、ユーザはデバイスが相互の関連でレポートする情報をモニタして、ネットワーク上で行われている全体的なアクティビティを評価することができます。

Firewall Management Center を使用することで、デバイス動作のほぼすべての側面を管理できます。

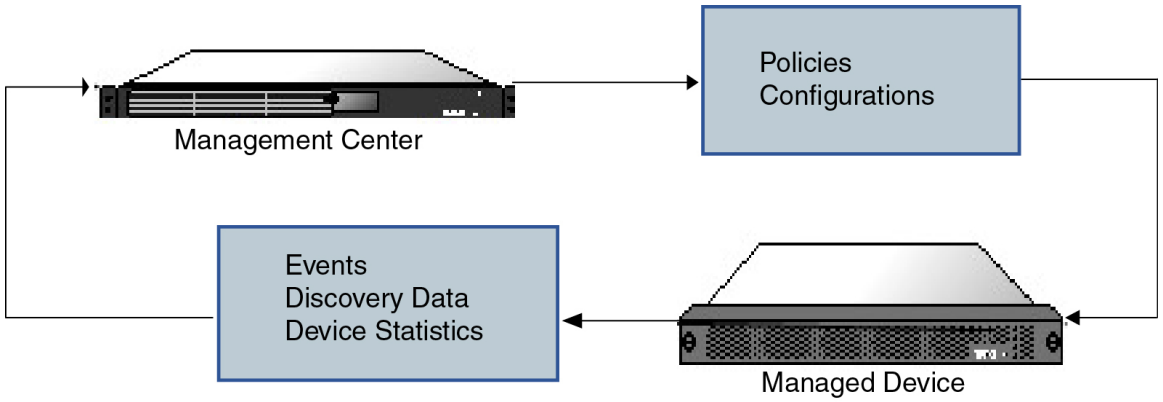
（注） Firewall Management Center は、http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html で入手可能な互換性マトリックスで指定されている特定の以前のリリースを実行しているデバイスを管理できますが、これらの以前のリリースのデバイスでは、最新バージョンの Firewall Threat Defense ソフトウェアが必要な新しい機能は利用できません。一部の Firewall Management Center 機能は、以前のバージョンで使用できる場合があります。

Secure Firewall Management Center で管理できるデバイス

Firewall Threat Defense デバイスを管理するための集中管理ポイントとして Secure Firewall Management Center を使用できます。

デバイスを管理する際の情報は、SSL で暗号化されたセキュアな TLS-1.3 暗号化通信チャネルを介して、Firewall Management Center とデバイスの間で送信されます。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。

次の図に、Firewall Management Center と管理対象デバイスの間で送信される情報を示します。アプライアンス間で送信されるイベントとポリシーのタイプは、デバイスタイプに基づくことに注意してください。



管理接続について

Firewall Management Center 情報を使用してデバイスを設定し、デバイスを Firewall Management Center に追加した後に、デバイスまたは Firewall Management Center のいずれかで管理接続を確立できます。初期設定に応じて、以下のようになります。

- デバイスまたは Firewall Management Center のいずれかから開始できる。
- デバイスのみが開始できる。
- Firewall Management Center のみが開始できる。

初期化は常に Firewall Management Center の eth0 またはデバイスの最も番号が小さい管理インターフェイスから始まります。接続が確立されていない場合は、追加の管理インターフェースが試行されます。Firewall Management Center の複数の管理インターフェイスにより、個別のネットワークに接続したり、管理トラフィックとイベントトラフィックを分離したりできます。ただし、イニシエータは、ルーティングテーブルに基づいて最適なインターフェイスを選択しません。

管理接続が安定しており、過度なパケット損失がなく、少なくとも 5 Mbps のスループットがあることを確認します。デフォルトでは、管理接続は TCP ポート 8305 を使用します（このポートは設定可能です）。デバイスと Firewall Management Center の間に別の Firewall Threat Defense を配置する場合は、管理の中断を防ぐために、プレフィルタポリシーを適用して管理トラフィックをディープインスペクションから除外してください。

（注） 管理接続は、それ自身とデバイスの間の安全な 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。

ポリシーとイベント以外の機能

Firewall Management Center では、ポリシーをデバイスに展開したり、デバイスからイベントを受信するだけでなく、以下のデバイス関連のタスクも実行できます。

デバイスのバックアップ

FTD CLIから物理的な管理対象デバイスをバックアップすることはできません。設定データと統合ファイル（任意）をバックアップするには、デバイスを管理している Firewall Management Center を使用してデバイスのバックアップを実行します。

イベントデータをバックアップするには、デバイスを管理している Firewall Management Center のバックアップを実行します。

デバイスの更新

シスコは適宜、Firepower システムの更新プログラムをリリースしています。これらのアップデートには以下が含まれます。

- 侵入ルールの更新（新しいルールや更新された侵入ルールが含まれる場合があります）
- 脆弱性データベース（VDB）の更新
- 地理位置情報の更新
- ソフトウェア パッチおよびアップデート

Firewall Management Center を使用して、管理対象デバイスに更新プログラムをインストールできます。

デバイス管理インターフェイスについて

各デバイスには Firewall Management Center と通信するための専用の管理インターフェイスが 1 つ含まれています。必要に応じて、専用の管理インターフェイスではなく、管理用のデータインターフェイスを使用するようにデバイスを設定できます。

管理インターフェイスまたはコンソールポートで初期設定を実行できます。

管理インターフェイスは、スマート ライセンス サーバーとの通信、更新プログラムのダウンロード、その他の管理機能の実行にも使用します。

Firewall Threat Defense の管理インターフェイスとイベントインターフェイス

デバイスをセットアップするときに、接続先とする Firewall Management Center の IP アドレスまたはホスト名を指定します（既知の場合）。この場合、デバイスが接続を開始すると、初期登録時には、管理トラフィックとイベントトラフィックの両方がこのアドレスに送信されます。Firewall Management Center が不明な場合、Firewall Management Center が最初の接続を確立します。この場合、Firewall Threat Defense で指定されたものとは異なる Firewall Management Center管理インターフェイスから接続が開始される可能性があります。以降の接続では、指定

された IP アドレスの Firewall Management Center 管理インターフェイスを使用する必要があります。

Firewall Management Center に別のイベント専用インターフェイスがある場合、ネットワークが許可する場合、管理対象デバイスは後続のイベントトラフィックを Firewall Management Center イベント専用インターフェイスに送信します。さらに、一部の管理対象デバイスモデルには、イベント専用トラフィック用に構成できる追加の管理インターフェイスが含まれています。管理用のデータインターフェイスを設定する場合は、個別管理およびイベントインターフェイスを使用できません。イベントネットワークがダウンすると、イベントトラフィックは、Firewall Management Center および/または管理対象デバイスの通常の管理インターフェイスに戻ります。

管理のための Firewall Threat Defense データインターフェイスの使用について

Firewall Management Center との通信には、専用の管理インターフェイスか、または通常のデータインターフェイスを使用できます。データインターフェイスでのマネージャアクセスは、外部インターフェイスからリモートで Firewall Threat Defense を管理する場合、または別の管理ネットワークがない場合に便利です。さらに、データインターフェイスを使用する場合、プライマリインターフェイスがダウンした場合に管理機能を引き継ぐよう、冗長セカンダリインターフェイスを構成することになります。

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のアクセス要件は、次のとおりです。

- 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または EtherChannel を使用することはできません。マネージャアクセスインターフェイスでサブインターフェイスを作成することもできません。冗長性を目的として、Firewall 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 Firewall 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 Firewall 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。Amazon Web Services の Firewall Threat Defense Virtual の場合、コンソールポートは使用できないため、管理インターフェイスへの SSH アクセスを維持する必要があります。設定を続行する前に、管理用の静的ルートを追加します。または、マネージャアクセス用のデータインターフェイスを設定する前に、すべての CLI 構成（**configure manager add** コマンドを含む）を終了してから接続を切断します。

- 管理インターフェイスとイベント専用インターフェイスを別々に使用することはできません。
- クラスタリングはサポートされません。この場合、管理インターフェイスを使用する必要があります。
- ハイアベイラビリティはサポートされません。この場合、管理インターフェイスを使用する必要があります。

デバイスモデルごとの管理インターフェイスのサポート

管理インターフェイスの場所については、ご使用のモデルのハードウェアインストレーションガイドを参照してください。

（注） Firepower 4100/9300 の場合、MGMT インターフェイスは Firewall Threat Defense の論理デバイスを管理するためではなく、シャーシを管理するために使用します。mgmt タイプ（または firepower-eventing タイプあるいはその両方）の別個のインターフェイスを設定してから、そのインターフェイスを Firewall Threat Defense 論理デバイスに割り当てる必要があります。

（注） シャーシ上の Firewall Threat Defense の場合、物理管理インターフェイスは、診断論理インターフェイス（SNMP または syslog に利用できて、Firewall Management Center でデータインターフェイスと併せて設定されます）と、Firewall Management Center 通信用の管理論理インターフェイスの間で共有されます。詳細については、管理/診断インターフェイスを参照してください。

管理対象デバイスの各モデルでサポートされる管理インターフェイスについては、以下の表を参照してください。

表 *1:* 管理対象デバイスでサポートされる管理インターフェイス

モデル	管理インターフェイス	オプションのイベント インターフェイス
Firepower 1000	management0 （注） management0 は管理 1/1 インターフェイスの内部名です。	サポートなし
Firepower 2100	management0 （注） management0 は管理 1/1 インターフェイスの内部名です。	サポートなし

モデル	管理インターフェイス	オプションのイベント インターフェイス
Cisco Secure Firewall 3100	management0 （注） management0 は管理 1/1 インターフェイスの内部名です。	サポートなし
Firepower 4100 および 9300	management0 （注） management0 は、物理インターフェイス ID に関わらず、このインターフェイスの内部名です。	management1 （注） management1 は、物理インターフェイス ID に関わらず、このインターフェイスの内部名です。
ISA 3000	br1 （注） br1 は、管理 1/1 インターフェイスの内部名です。	サポートなし
Secure Firewall Threat Defense Virtual	eth0	サポートなし

管理インターフェイス上のネットワークルート

管理インターフェイス（イベント専用インターフェイスを含む）は、リモート ネットワークに到達するためのスタティック ルートのみをサポートしています。管理対象デバイスをセットアップすると、セットアップ プロセスにより、指定したゲートウェイ IP アドレスへのデフォルトルートが作成されます。このルートを削除することはできません。また、このルートで変更できるのはゲートウェイ アドレスのみです。

（注） 管理インターフェイスのルーティングは、データインターフェイスに対して設定するルーティングとは完全に別のものです。専用の管理インターフェイスを使用する代わりに管理用のデータインターフェイスを設定すると、トラフィックはバックプレーンを介してルーティングされ、データルーティングテーブルが使用されます。ここで説明する内容は適用されません。

一部のプラットフォームでは、複数の管理インターフェイス（管理インターフェイスとイベント専用インターフェイス）を設定できます。デフォルトルートには出力インターフェイスが含まれていないため、選択されるインターフェイスは、指定したゲートウェイアドレスと、ゲートウェイが属するインターフェイスのネットワークによって異なります。デフォルト ネットワーク上に複数のインターフェイスがある場合、デバイスは出力インターフェイスとして番号の小さいインターフェイスを使用します。

リモートネットワークにアクセスするには、管理インターフェイスごとに1つ以上のスタティックルートを使用することをお勧めします。他のデバイスから Firewall Threat Defense へのルーティングの問題など、潜在的なルーティングの問題を回避するために、各インターフェイスを個別のネットワークに配置することをお勧めします。

（注） 管理接続に使用されるインターフェイスは、ルーティングテーブルによって決定されません。常に最も番号の小さいインターフェイスを最初に使用して接続が試行されます。

NAT 環境

ネットワーク アドレス変換（NAT）とは、ルータを介したネットワーク トラフィックの送受信方式であり、送信元または宛先 IP アドレスの再割り当てが行われます。NAT の最も一般的な用途は、プライベートネットワークがインターネットと通信できるようにすることです。スタティック NAT は 1:1 変換を実行し、デバイスとの Firewall Management Center 通信に支障はありませんが、ポート アドレス変換（PAT）がより一般的です。PAT では、単一のパブリック IP アドレスと一意のポートを使用してパブリック ネットワークにアクセスできます。これらのポートは必要に応じて動的に割り当てられるため、PAT ルータの背後にあるデバイスへの接続は開始できません。

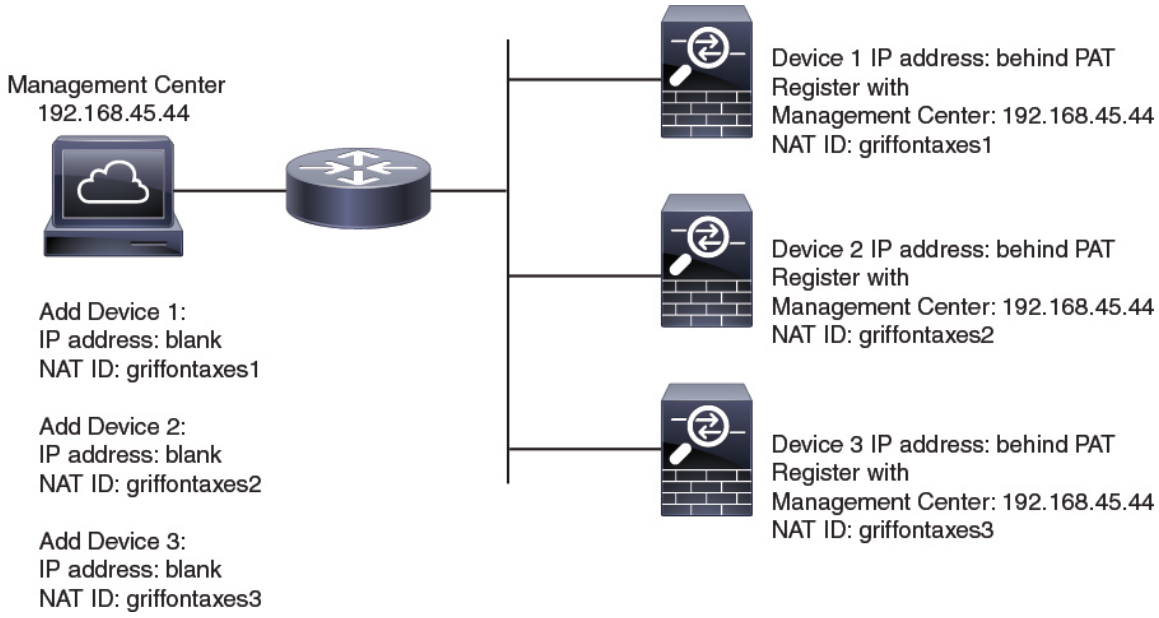
通常は、ルーティングと認証の両方の目的で両方の IP アドレス（登録キー付き）が必要です。デバイスを追加するときに、Firewall Management Center がデバイスの IP アドレスを指定し、デバイスが Firewall Management Center の IP アドレスを指定します。ただし、IP アドレスの 1 つのみがわかっている場合（ルーティング目的の最小要件）は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要もあります。Firewall Management Center およびデバイスでは、初期登録の認証と承認を行うために、登録キーおよび NAT ID（IP アドレスではなく）を使用します。

たとえば、デバイスを Firewall Management Center に追加したときにデバイスの IP アドレスがわからない場合（たとえばデバイスが PAT ルータの背後にある場合）は、NAT ID と登録キーのみを Firewall Management Center に指定します。IP アドレスは空白のままにします。デバイス上で、Firewall Management Center の IP アドレス、同じ NAT ID、および同じ登録キーを指定します。デバイスが Firewall Management Center の IP アドレスに登録されます。この時点で、Firewall Management Center は IP アドレスの代わりに NAT ID を使用してデバイスを認証します。

NAT 環境では NAT ID を使用するのが最も一般的ですが、NAT ID を使用することで、多数のデバイスを簡単に Firewall Management Center に追加することができます。Firewall Management Center で、追加するデバイスごとに IP アドレスは空白のままにして一意の NAT ID を指定し、次に各デバイスで、Firewall Management Center の IP アドレスと NAT ID の両方を指定します。注：NAT ID はデバイスごとに一意でなければなりません。

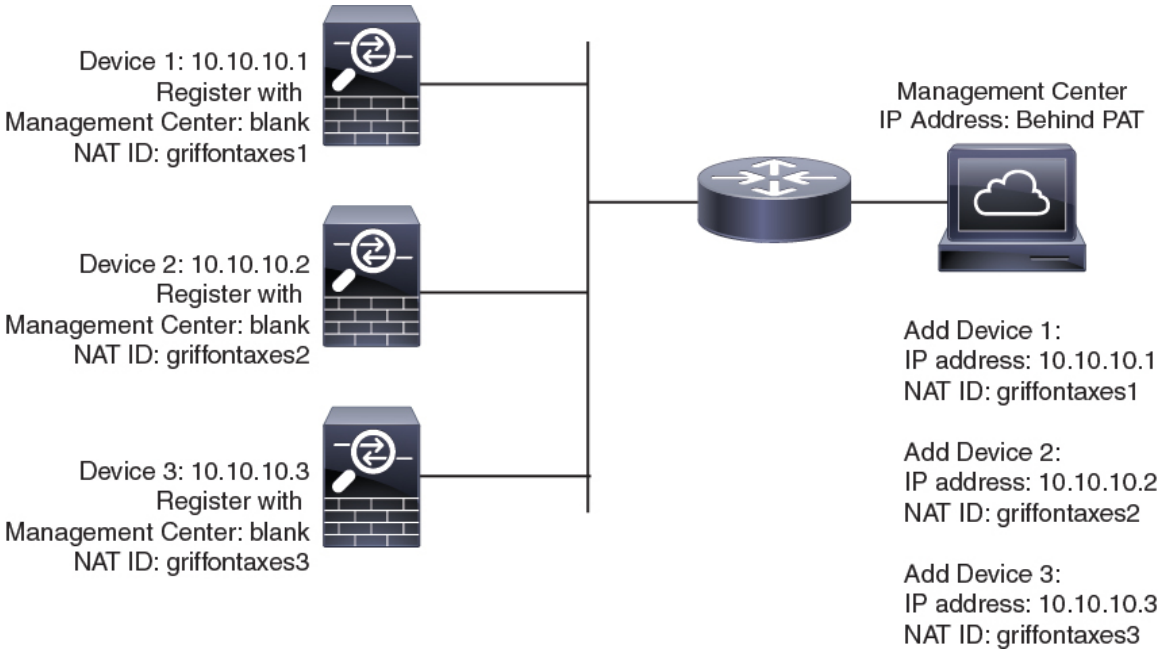
次の例に、PAT IP アドレスの背後にある 3 台のデバイスを示します。この場合、Firewall Management Center とデバイスの両方でデバイスごとに一意の NAT ID を指定し、デバイス上の Firewall Management Center の IP アドレスを指定します。

図 *1 : PAT* の背後にある管理対象デバイスの *NAT ID*



次の例に、PAT IP アドレスの背後にある Firewall Management Center を示します。この場合、Firewall Management Center とデバイスの両方でデバイスごとに一意の NAT ID を指定し、Firewall Management Center 上のデバイスの IP アドレスを指定します。

図 *2 : PAT* の背後にある *FMC* の *NAT ID*

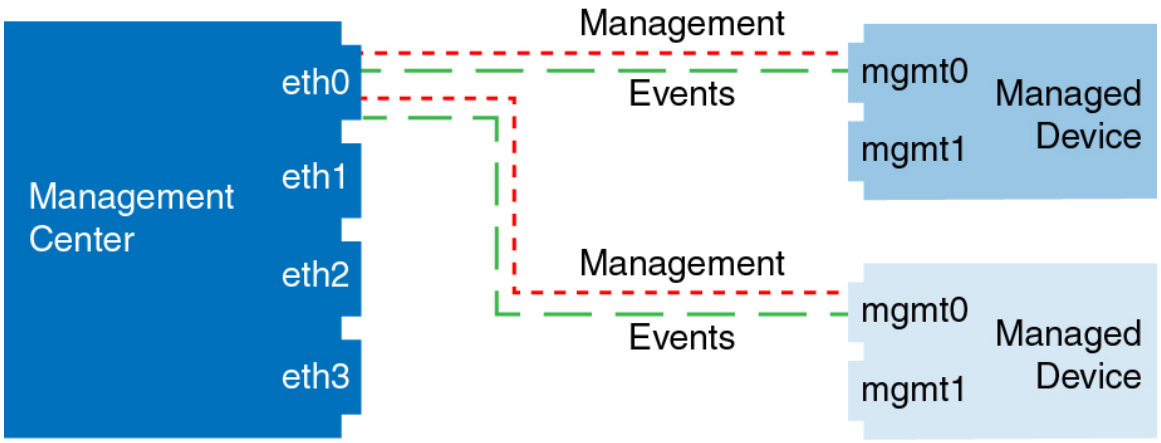


管理およびイベント トラフィック チャネルの例

（注） 管理用のデータインターフェイスを Firewall Threat Defense で使用する場合は、そのデバイスに個別の管理インターフェイスとイベントインターフェイスを使用することはできません。

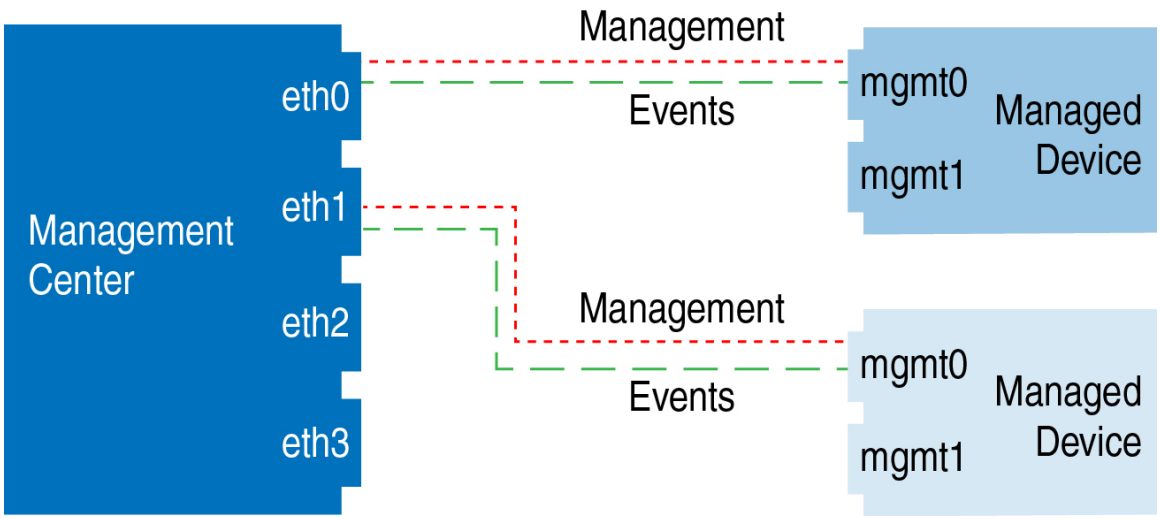
以下に、Firewall Management Center と管理対象デバイスでデフォルト管理インターフェイスのみを使用する例を示します。

図 *3 : Secure Firewall Management Center* 上で単一の管理インターフェイスを使用する場合



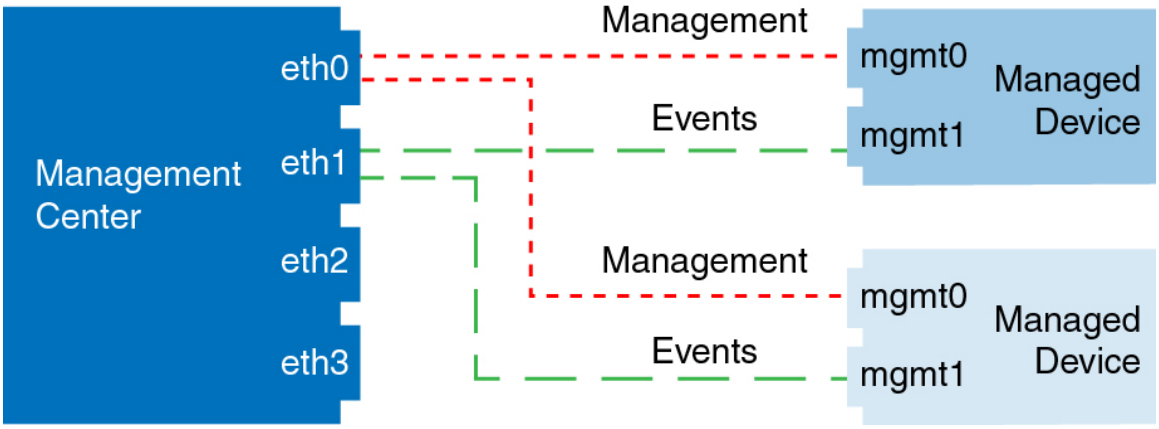
以下に、Firewall Management Center でデバイスごとに別個の管理インターフェイスを使用する例を示します。この場合、各管理対象デバイスが 1 つの管理インターフェイスを使用します。

図 *4 : Secure Firewall Management Center* の複数の管理インターフェイス



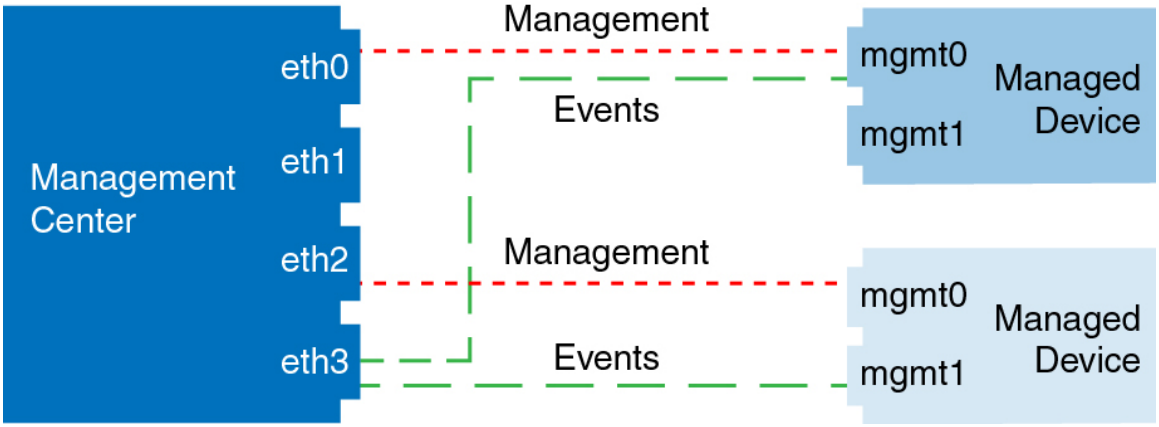
以下に、個別のイベント インターフェイスを使用する Firewall Management Center と管理対象デバイスの例を示します。

図 *5 : Secure Firewall Management Center*上の個別のイベント インターフェイスと管理対象デバイスを使用する場合



以下に、Firewall Management Center 上で複数の管理インターフェイスと個別のイベント インターフェイスが混在し、個別のイベントインターフェイスを使用する管理対象デバイスと単一の管理インターフェイスを使用する管理対象デバイスが混在する例を示します。

図 *6 :* 管理インターフェイスとイベント インターフェイスを混在させて使用する場合



デバイス管理の要件と前提条件

サポートされるドメイン

デバイスが存在するドメイン。

ユーザの役割

- 管理者
- ネットワーク管理者

管理接続

管理接続が安定しており、過度なパケット損失がなく、少なくとも 5 Mbps のスループットがあることを確認します。

ゼロ タッチ プロビジョニング の要件

クラスタリングまたはマルチインスタンスモードではゼロ タッチ プロビジョニング はサポートされません。

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にのみサポートされます。

ゼロ タッチ プロビジョニング は、7.4 以降を使用する次のモデルでサポートされます。

- Firepower 1010
- Firepower 1100
- Firepower 2100（サポートされているバージョンに搭載）
- Cisco Secure Firewall 3100

デバイスのコマンド ライン インターフェイス（CLI）へのログイン

Firewall Threat Defense デバイスのコマンドライン インターフェイスに直接ログインできます。初めてログインする場合は、デフォルトの **admin** ユーザーを使用して初期設定プロセスを完了します。CLI を使用した Firewall Threat Defense 初期設定の実行の完了 （21 ページ）を参照してください。

（注） SSH を介した CLI へのログイン試行が 3 回連続して失敗すると、SSH 接続は終了します。

始める前に

- **configure user add** コマンドを使用して、CLI にログインできる追加のユーザー アカウントを作成します。
- コンソールポートに接続したときに、読み取れない文字が表示される場合は、ポートの設定を確認してください。設定が正しい場合は、同じ設定を使用して別のデバイスでそのケーブルを試します。ケーブルに問題がない場合は、コンソールポートのハードウェアを交換する必要がある可能性があります。別のワークステーションでの接続を試みることも検討してください。

手順

ステップ 1 コンソール ポートまたは SSH を使用して、Firewall Threat Defense CLI に接続します。

Firewall 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。SSH 接続用のインターフェイスを開いている場合、データ インターフェイス上のアドレスにも接続できます。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。特定のデータ インターフェイスへの SSH 接続を許可する方法については、Shellの確保を参照してください。

物理デバイスの場合、デバイスのコンソールポートに直接接続できます。コンソール ケーブルの詳細については、デバイスのハードウェア ガイドを参照してください。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

コンソールポートの CLI は FXOS です（通常の Firewall Threat Defense CLI である ISA 3000 を除く）。基本設定、モニタリング、および通常のシステムのトラブルシューティングには Firewall Threat Defense CLI を使用します。FXOS コマンドの詳細については、FXOS のマニュアルを参照してください。

ステップ 2 **admin** のユーザー名とパスワードでログインします。

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 3 コンソールポートを使用した場合は、 Firewall Threat Defense CLI にアクセスします。

connect ftd

（注）
この手順は、ISA 3000 には適用されません。

例：

```
firepower# connect ftd
>
```

ステップ 4 CLI プロンプト（>）で、コマンドライン アクセス レベルで許可されている任意のコマンドを使用します。

コンソールポートの FXOS に戻るには、**exit**と入力します。

ステップ 5 （任意） SSH を使用した場合は、FXOS に接続できます。

connect fxos

Firewall Threat Defense CLI に戻るには、**exit** と入力します。

ステップ 6 （オプション）診断 CLI にアクセスします。

system support diagnostic-cli

この CLI を使用して、高度なトラブルシューティングを行います。この CLI には追加の **show** およびその他のコマンドがあります。

この CLI にはサブモードとして、ユーザー実行モード、特権 EXEC モードがあります。特権 EXEC モードでは、ユーザー実行モードよりも多くのコマンドを利用できます。特権 EXEC モードを開始するには、**enable** コマンドを入力し、プロンプトに対してパスワードを入力せずに Enter を押します。

例：

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

通常の CLI に戻るには、**Ctrl+a**、**d** を入力します。

Firewall Threat Defense 初期設定の完了

Firepower 4100/9300 を除くすべてのモデルについて、CLI または Firewall Device Managerを使用して Firewall Threat Defense の初期設定を実行できます。Firepower 4100/9300 の場合、論理デバイスを展開する際に初期設定を実行します。Firepower 4100/9300 の論理デバイスを参照してください。

Firewall Device Manager を使用した Firewall Threat Defense の初期設定の完了

初期セットアップに Firewall 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
- Ethernet 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

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。

Firewall Management Center に登録する前に Firewall 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）。

- この手順は、オンプレミスの Firewall Management Center を分析のみに使用する CDO 管理対象デバイスには適用されません。Firewall Device Manager の構成は、プライマリマネージャを構成するためのものです。分析用にデバイスを構成する方法の詳細については、CLI を使用した Firewall Threat Defense 初期設定の実行の完了 （21 ページ） を参照してください。
- この手順は、Firepower 4100/9300 と ISA 3000 を除く他のすべてのデバイスに適用されます。Firewall Device Manager を使用してこれらのデバイスを Firewall Management Center にオンボーディングできますが、他のプラットフォームとはデフォルト設定が異なるため、この手順の詳細はこれらのプラットフォームには適用されない場合があります。

手順

ステップ 1 Firewall Device Manager にログインします。

a) ブラウザに次の URL を入力します。

- 内部：**https://192.168.95.1**。
- 管理：**https://***management_ip*。管理インターフェイスは DHCP クライアントであるため、IP アドレスは DHCP サーバーによって異なります。この手順の一環として、管理 IP アドレスを静的アドレスに設定する必要があるため、接続が切断されないように内部インターフェイスを使用することをお勧めします。

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 2 初期設定を完了するには、最初に Firewall 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のデフォルト設定に加えて、Firewall Management Center の管理に切り替えるときに維持される外部（Ethernet1/1）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、手動で静的 IP アドレス、サブネットマスク、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv4 アドレスを設定しないという選択肢もあります。セットアップウィザードを使用して PPPoE を設定することはできません。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。ウィザードの完了後に PPPoE を設定できます。

   [IPv6の設定（Configure IPv6）]：外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、手動で静的 IP アドレス、プレフィックスマスク、およびゲートウェイを入力できます。[オフ（Off）] を選択して、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の DNS サーバ。名前解決に使用する DNS サーバのアドレスを 1 つ以上入力します。デフォルトは、OpenDNS パブリック DNS サーバーです。フィールドを編集した後、デフォルトに戻す場合は、[OpenDNS を使用（Use OpenDNS）] をクリックすると該当する IP アドレスがフィールドにリロードされます。

   [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、手動で NTP サーバのアドレスを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。

Firewall 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 Firewall 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。Firewall 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 3 （必要に応じて）管理インターフェイスを設定します。

マネージャアクセスにデータインターフェイスを使用する場合でも、管理インターフェイスの設定を変更する必要がある場合があります。Firewall Device Manager 接続に管理インターフェイスを使用していた場合は、Firewall Device Manager に再接続する必要があります。

- マネージャアクセス用のデータインターフェイス：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。
- マネージャアクセス用の管理インターフェイス：静的 IP アドレスを設定する場合は、デフォルトゲートウェイもデータインターフェイスではなく一意のゲートウェイに設定してください。DHCP を使用する場合は、DHCP からゲートウェイを正常に取得できると仮定して、何も設定する必要はありません。

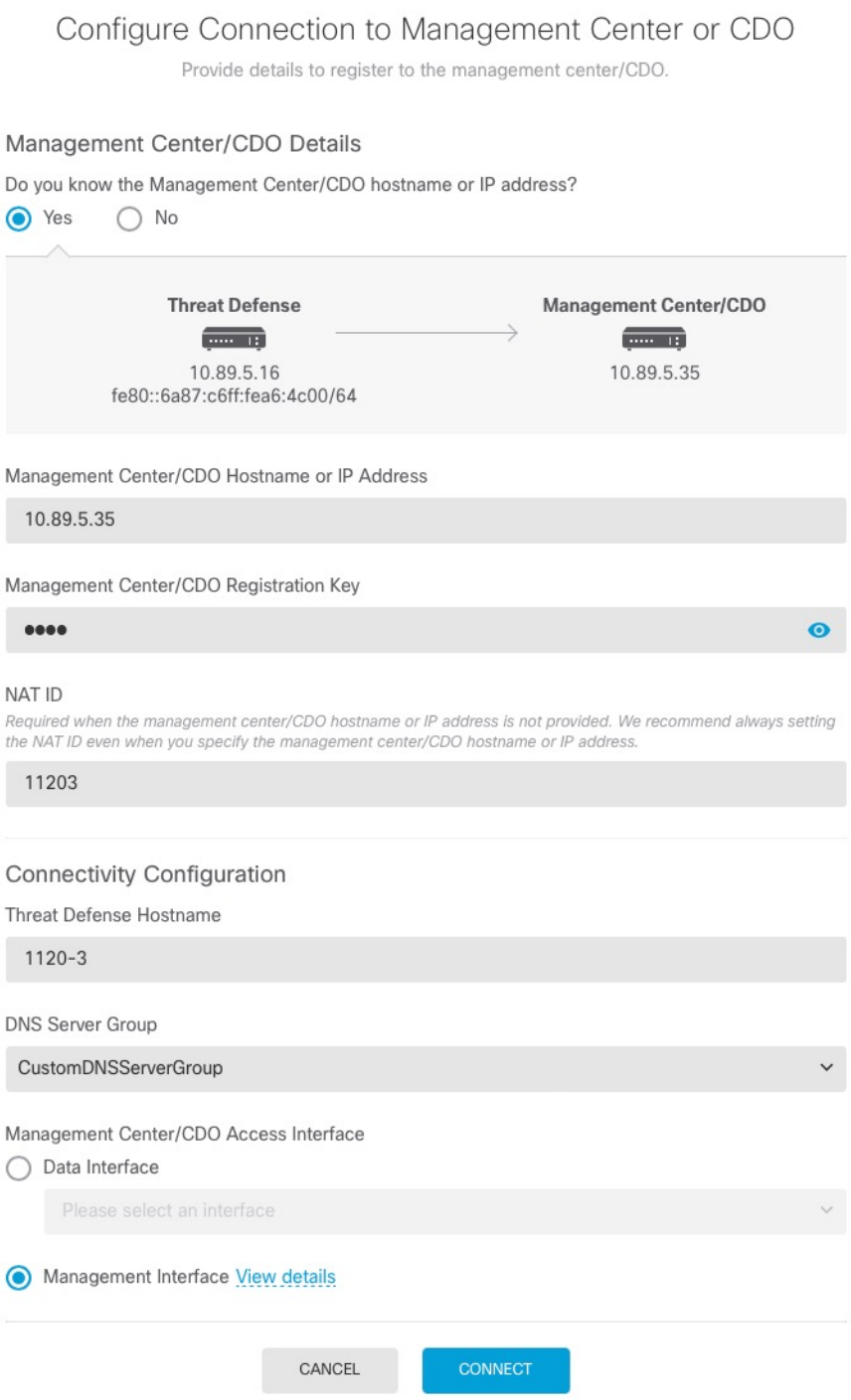
ステップ 4 マネージャアクセスに使用する外部または内部以外のインターフェイスを含む追加のインターフェイスを設定する場合は、[デバイス（Device）] を選択し、[インターフェイス（Interface）] のサマリーのリンクをクリックします。

Firewall Management Center にデバイスを登録すると、Firewall Device Manager の他の構成は保持されません。

ステップ 5 **[デバイス（Device）]** > **[システム設定（System Settings）]** > **[集中管理（Central Management）]** の順に選択し、[続行（Proceed）] をクリックして Firewall Management Center の管理を設定します。

ステップ 6 [Management Center/SCCCDOの詳細（Management Center/**CDO** Details）] を設定します。

図 *7 : Management Center/CDO* の詳細



a) [Management Center/SCCCDO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 Management Center/**CDO** hostname or IP address?）] で、IP アドレスまたはホスト名を使用して Firewall Management Center に到達できる場合は [はい（Yes）] をクリックし、Firewall

Management CenterCDO 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、少なくても 1 台以上のデバイス（Firewall Management Center または Firewall 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、[Management Center/SCCCDOのホスト名/IPアドレス（Management Center/**CDO** Hostname or IP Address）] を入力します。

c) [Management Center/SCCCDO登録キー（Management Center/**CDO** Registration Key）] を指定します。

このキーは、Firewall Threat Defense デバイスを登録するときに Firewall 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 2 ～ 36 文字である必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Firewall Management Center に登録する複数のデバイスに使用できます。

a) [NAT ID] を指定します。

この ID は、Firewall Management Center でも指定する任意の 1 回限りの文字列です。NAT ID は 2 ～ 36 文字である必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Firewall 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、接続元が正しいデバイス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、登録キーが確認されます。任意である場合でも常にNAT IDを使用することを推奨しますが、次の場合は必須です。

- Firewall Management Center IP アドレスを **DONTRESOLVE** に設定する。
- Firewall Management Center でデバイスを追加するときに、到達可能なデバイスの IP アドレスまたはホスト名を指定していない。
- 両側でIPアドレスを指定する場合でも、管理にデータインターフェイスを使用する。
- Firewall Management Center が複数の管理インターフェイスを使用する。

ステップ 7 [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。

[Management Center/SCCCDOアクセスインターフェイス（Management Center/**CDO** Access Interface）] のアクセスにデータインターフェイスを使用する場合、FQDN がこのインターフェイスに使用されます。

b) [DNSサーバグループ（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 サーバが含まれます。

[Management Center/SCCCDOアクセスインターフェイス（Management Center/**CDO** Access Interface）] のデータインターフェイスを選択する場合は、この設定でデータインターフェイス DNS サーバーを設定します。セットアップウィザードで設定した管理 DNS サーバ

は、管理トラフィックに使用されます。データ DNS サーバは、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じ DNS サーバーグループを選択する可能性があります。

Firewall Management Center では、この Firewall Threat Defense デバイス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。Firewall Management Center に Firewall Threat Defense デバイスを追加すると、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 Firewall Threat Defense デバイス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。Firewall Management Center と Firewall Threat Defense デバイスを同期させるには、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 Firewall Management Center で保持されます。

[Management Center/SCCCDOアクセスインターフェイス（Management Center/**CDO** Access Interface）]**[FMCアクセスインターフェイス（FMC Access Interface）]** の管理インターフェイスを選択する場合は、この設定で管理 DNS サーバーを設定します。

c) [Management Center/SCCCDOアクセスインターフェイス（Management Center/**CDO** Access Interface）] については、任意の設定済みインターフェイスを選択します。

管理インターフェイスは、Firewall Threat Defense デバイスを Firewall 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。

ステップ 8 （任意）外部インターフェイスではない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、Firewall 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。

管理インターフェイスを選択した場合は、この画面に進む前に、ゲートウェイを一意のゲートウェイとして設定する必要があります。

ステップ 9 （任意） データインターフェイスを選択した場合は、[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、 IP アドレスが変更された場合に Firewall Management Center が完全修飾ドメイン名（FQDN）で Firewall Threat Defense デバイス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。

Firewall Management Center に Firewall Threat Defense デバイスを追加する前に DDNS を設定すると、Firewall Threat Defense デバイスは、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し、Firewall Threat Defense デバイスが HTTPS 接続のために DDNS サーバー証明書を検証できるようにします。 Firewall 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。

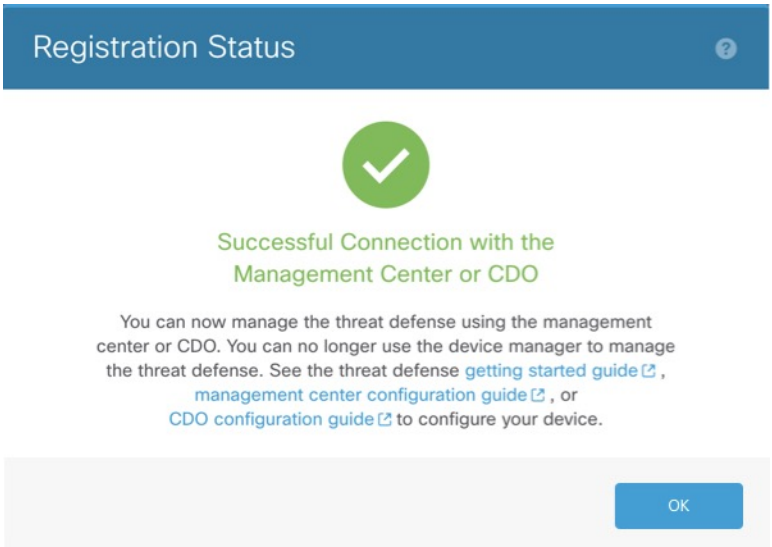
マネージャアクセスに管理インターフェイスを使用する場合、DDNS はサポートされません。

ステップ 10 [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、Firewall 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/SCCCDO登録設定の保存（Saving Management Center/**CDO** Registration Settings）] のステップの後、Firewall Management Center に移動してファイアウォールを追加します。

Firewall 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/SCCCDO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 Firewall 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、Firewall Device Manager に再接続した場合のみ再開されます。

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

図 *8* : 正常接続



CLI を使用した Firewall Threat Defense 初期設定の実行の完了

Firewall Threat Defense CLI に接続して初期設定を実行します。これには、セットアップウィザードを使用した管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定の

指定などが含まれます。専用の管理インターフェイスは、独自のネットワーク設定を持つ特別なインターフェイスです。マネージャアクセスに管理インターフェイスを使用しない場合は、代わりに CLI を使用してデータインターフェイスを設定できます。また、Firewall Management Center 通信の設定を行います。Firewall Device Manager 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 Firewall Management Center に切り替えたときに、Firewall Device Manager で完了したすべてのインターフェイス構成が保持されます。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。

この手順は、Firepower 4100/9300 を除くすべてのモデルに適用されます。Firepower 4100/9300 で論理デバイスを展開し、初期構成を完了するには、「Firepower 4100/9300 の論理デバイス」を参照してください。

Procedure

ステップ 1 コンソールポートから、または管理インターフェイスへの SSH を使用して、Firewall Threat Defense CLI に接続します。デフォルトで DHCP サーバーから IP アドレスが取得されます。ネットワーク設定を変更する場合は、切断されないようにコンソールポートを使用することを推奨します。

（Firepower および Cisco Secure Firewall ハードウェアモデル）コンソールポートは FXOS CLI に接続します。SSH セッションは Firewall Threat Defense CLI に直接接続します。

ステップ 2 ユーザー名 **admin** およびパスワード **Admin123** でログインします。

（Firepower および Cisco Secure Firewall ハードウェアモデル）コンソールポートで FXOS CLI に接続します。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 Firewall Threat Defense ログインにも使用されます。

Note
パスワードがすでに変更されていて、パスワードがわからない場合は、デバイスを再イメージ化してパスワードをデフォルトにリセットする必要があります。

Firepower および Cisco Secure Firewall ハードウェアの場合は、Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 と Threat Defense の Cisco FXOS トラブルシューティング ガイド [英語] の「Reimage Procedures」を参照してください。

ISA 3000 の場合は、『Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide』を参照してください。

Example:

```
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 3 （Firepower および Cisco Secure Firewall ハードウェアモデル）コンソールポートで FXOS に接続した場合は、Firewall Threat Defense CLI に接続します。

connect ftd

Example:

```
firepower# connect ftd
>
```

ステップ 4 Firewall 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書（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、CLI セットアップスクリプトが表示されます。

Note
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。threat defense の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。

Note
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。

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のIPv4デフォルトゲートウェイを入力（Enter the IPv4 default gateway for the management interface）]、[管理インターフェイスのIPv6ゲートウェイを入力（Enter the IPv6 gateway for the management interface）]：管理インターフェイスではなくデータインターフェイスをマネージャアクセスに使用する場合は、[手動（manual）] を選択します。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。ルーティングの問題を防ぐために、このインターフェイスがマネージャ アクセス インターフェイスとは異なるサブネット上にあることを確認してください。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（Enter the IPv4 default gateway for the management interface）]、[DHCP、ルータ経由、または手動でIPv6を設定しますか?（Configure IPv6 via DHCP, router, or manually?）]：管理インターフェイスではなくデータインターフェイスをマネージャアクセスに使用する場合は、ゲートウェイを[data-interfaces]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。マネージャアクセスに管理インターフェイスを使用する場合は、管理 1/1 ネットワークでゲートウェイ IP アドレスを設定する必要があります。
- **ネットワーク情報が変更された場合は再接続が必要**：SSHで接続しているのに、初期セットアップでその IP アドレスを変更すると、接続が切断されます。新しい IP アドレスとパスワードで再接続してください。コンソール接続は影響を受けません。
- [デバイスをローカルで管理しますか（Manage the device locally?）]：Firewall 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 Secure Firewall 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?）]：初期設定でファイアウォールモードを設定することをお勧めします。初期設定後にファイアウォールモードを変更すると、実行コンフィギュレーションが消去されます。データ インターフェイス 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ることに注意してください。

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
[...]

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]: 10.89.5.1
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: 10.89.5.1 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 5 この Firewall Threat Defense を管理する Firewall Management Center を特定します。

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

Note
管理に CDO を使用している場合は、このステップで CDO が生成した **configure manager add** コマンドを使用します。

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the Firewall Management Center.Firewall 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。また、*nat_id* も指定します。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、少なくても 1 台以上のデバイス（Firewall Management Center または Firewall 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 Firewall Threat Defense に必要です。
- reg_key：Firewall Threat Defense を登録するときに Firewall Management Center でも指定する任意のワンタイム登録キーを指定します。登録キーは 2 ～ 36 文字である必要がありま

す。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。

- nat_id：Firewall Threat Defense を登録するときに Firewall Management Center でも指定する、任意で一意の 1 回限りの文字列を指定します。NAT ID は 2 ～ 36 文字である必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Firewall 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。任意である場合でも常にNAT IDを使用することを推奨しますが、次の場合は必須です。
  - Firewall Management Center IP アドレスを **DONTRESOLVE** に設定する。
  - Firewall Management Center でデバイスを追加するときに、到達可能なデバイスの IP アドレスまたはホスト名を指定していない。
  - 両側でIPアドレスを指定する場合でも、管理にデータインターフェイスを使用する。
  - Firewall Management Center が複数の管理インターフェイスを使用する。
- *display_name*：**show managers** コマンドでこのマネージャを表示するための表示名を指定します。このオプションは、CDO をプライマリマネージャおよび分析専用のオンプレミス Firewall Management Center として識別する場合に役立ちます。この引数を指定しない場合、ファイアウォールは以下のいずれかの方法を使用して表示名を自動生成します。
  - *hostname* | *IP_address*（**DONTRESOLVE** キーワードを使用しない場合）
  - **manager-***timestamp*

Example:

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

Example:

Firewall Management Center が NAT デバイスの背後にある場合は、次の例に示すように、一意の NAT ID とともに登録キーを入力し、ホスト名の代わりに DONTRESOLVE を指定します。

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

Example:

Firewall Threat Defense が NAT デバイスの背後にある場合は、次の例に示すように、一意の NAT ID とともに Firewall Management Center IP アドレスまたはホスト名を入力します。

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

ステップ 6 プライマリマネージャとして CDO を使用していて、オンプレミス Firewall Management Center を分析のみに使用する場合は、オンプレミス Firewall Management Center を特定します。

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

Example:

次の例では、CDO で生成した表示名で CDO 用に生成したコマンドを使用して、分析専用のオンプレミス Firewall Management Center を表示名「analytics-FMC」を使用して指定しています。

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
> configure manager add 10.70.45.5 regk3y78 natid56 analytics-FMC
Manager successfully configured.
```

ステップ 7 (Optional) マネージャアクセス用のデータインターフェイスを設定します。

configure network management-data-interface

その後、データ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。

Note
このコマンドを使用する場合は、コンソールポートを使用する必要があります。管理インターフェイスに SSH を使用すると、接続が切断され、コンソールポートに再接続する必要が生じる場合があります。SSH の詳細な使用方法については、次を参照してください。

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。管理のための Firewall Threat Defense データインターフェイスの使用について, on page 5も参照してください。

- データインターフェイスを管理に使用する場合、元の管理インターフェイスは 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設定できるようになりました。ルーティングの問題を防ぐために、このインターフェイスがマネージャ アクセス インターフェイスとは異なるサブネット上にあることを確認してください。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。
- Firewall Threat Defense を Firewall Management Center に追加すると、Firewall 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。Firewall 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、Firewall Threat Defense または Firewall 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、Firewall 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す。
- DDNS は、IP アドレスが変更された場合に Firewall Management Center が完全修飾ドメイン名（FQDN）で Firewall Threat Defense に到達できるようにします。DDNS サーバー更新の URL を設定すると、Firewall 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、Firewall Threat Defense は HTTPS 接続の DDNS サーバー証明書を検証できます。Firewall 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。

  Firewall Management Center では、この Firewall 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。Firewall Management Center に Firewall 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 Firewall 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。Firewall Management Center と Firewall 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 Firewall 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、FTD 設定と一致するように、DNS サーバーを含むこれらの設定すべてを Firewall 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、Firewall Threat Defense を Firewall 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。

Example:

```
> 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.

>
```

Example:

```
> 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 8 (Optional) 特定のネットワーク上のマネージャへのデータ 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。

What to do next

デバイスを Firewall Management Center に登録します。

イベントインターフェイスの設定

管理トラフィック用の管理インターフェイスが常に必要です。デバイスに 2 番目の管理インターフェイス（Firepower 4100/9300 など）がある場合は、イベント専用トラフィックに対してそのインターフェイスを有効にすることができます。

始める前に

別のイベントインターフェイスを使用するには、Firewall Management Center でイベントインターフェイスを有効にする必要もあります。Cisco Secure Firewall Management Center アドミニストレーション ガイドを参照してください。

手順

ステップ 1 2 番目の管理インターフェイスをイベント専用インターフェイスとして有効にします。

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

必要に応じて、**configure network management-interface disable-events-channel** コマンドを使用してメイン管理インターフェイスのイベントを無効にできます。いずれの場合も、デバイスは、イベントのみのインターフェイス上でイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベントチャネルが無効になっていても、管理インターフェイス上でイベントを送信します。

インターフェイス上でイベントチャネルと管理チャンネルの両方を無効にすることはできません。

例：

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Configuration updated successfully

>
```

ステップ 2 イベントインターフェイスの IP アドレスを設定します。

イベントインターフェイスは、管理インターフェイスの個別のネットワーク、または同じネットワークに配置できます。

a) IPv4 アドレスを設定します。

configure network ipv4 manual *ip_address netmask gateway_ip* **management1**

このコマンド内の *gateway_ip* は、デバイスのデフォルトルートを作成するために使用されることに注意してください。つまり、management0 インターフェイスにすでに設定した値を入力する必要があります。イベントインターフェイス用の個別のスタティックルートは作成されません。管理インターフェイスとは異なるネットワークでイベント専用インターフェイスを使用している場合は、イベント専用インターフェイス用に別のスタティックルートを作成することを推奨します。

例：

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.

>
```

b) IPv6 アドレスを設定します。

- ステートレス自動設定

  configure network ipv6 router management1

  例：

  ```
  > configure network ipv6 router management1
  Setting IPv6 network configuration.
  Network settings changed.
  ```

```
>
```

- 手動設定

  configure network ipv6 manual *ip6_address ip6_prefix_length* **management1**

  例：

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.

>
```

ステップ 3 Firewall Management Center がリモート ネットワーク上にある場合は、イベント専用インターフェイスのスタティック ルートを追加します。追加しないと、すべてのトラフィックが管理インターフェイスを通じてデフォルト ルートと一致します。

configure network static-routes {**ipv4** | **ipv6**}**add management1** *destination_ip netmask_or_prefix gateway_ip*

デフォルトルートの場合は、このコマンドを使用しないでください。デフォルト ルート ゲートウェイの IP アドレスの変更は、**configure network ipv4** コマンドまたは **ipv6** コマンドを使用した場合のみ可能です（「ステップ 2 （30 ページ）」を参照）。

例：

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully

>
```

スタティック ルートを表示するには、**show network-static-routes** を入力します（デフォルトルートは表示されません）。

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                : management1
Destination              : 192.168.6.0
Gateway                  : 10.10.10.1
Netmask                  : 255.255.255.0
[…]
```

デバイスの管理

[デバイス（Device）]>**[デバイス管理（Device Management）]**ページには、さまざまな情報とオプションがあります。

- **[表示単位（View By）]**：グループ、ライセンス、モデル、バージョン、またはアクセスコントロール ポリシーに基づいてデバイスが表示されます。
- **[デバイス状態（Device State）]**：デバイスを状態（**エラー**、**警告**など）に基づいて表示します。状態アイコンをクリックして、その状態に属するデバイスを表示できます。状態に属するデバイスの数は、括弧内に示されます。
- **[デバイスの検索（Search Device）]**：デバイス名、ホスト名またはIPアドレスを使用して、デバイスを検索します。
- **[追加（Add）]**：デバイスおよびその他の管理可能なコンポーネントを追加します。
- 列の見出しをクリックすると列ごとにソートできます。
  - **[名前（Name）]**
  - **モデル**
  - **バージョン**
  - **[シャーシ（Chassis）]**：サポートされているモデルの場合、**[管理（Manage）]**をクリックすると統合シャーシ マネージャが表示されます。Firepower 4100/9300の場合、リンクは Firewall Chassis Manager を相互起動します。
  - **ライセンス**
  - **[アクセス コントロール ポリシー（Access Control Policy）]**：デバイスに展開されているポリシーを表示するには、[アクセス コントロール ポリシー（Access Control Policy）] 列のリンクをクリックします。
  - **[自動ロールバック（Auto-Rollback）]**：展開によって管理接続がダウンした場合に、構成の自動ロールバックが有効（）か無効（）かを示します。「展開設定の編集」を参照してください。
- **[編集（Edit）]**：デバイスごとに、[編集（Edit）]（）アイコンを使用してデバイス設定を編集します。

  単にデバイス名または IP アドレスをクリックすることもできます。
- **[詳細（More）]**：デバイスごとに、[その他（More）]（）アイコン をクリックして、他のアクションを実行します。
  - [登録解除（Unregister）] [削除（Unregister）]：デバイスの登録を解除します。

- **[パケット トレーサ（Packet Tracer）]**：モデルパケットをシステムに挿入することにより、デバイスのポリシー設定を調べるためのパケットトレーサページに移動します。
- **[パケット キャプチャ（Packet Capture）]**：パケット キャプチャ ページに移動します。このページでは、パケットの処理中にシステムが実行する判定とアクションを表示できます。
- **[アップグレードを元に戻す（Revert Upgrade）]**：最後のアップグレード後に行われたアップグレードと構成の変更を元に戻します。この操作により、デバイスがアップグレード前のバージョンに復元されます。
- **[ヘルスモニター（Health Monitor）]**：デバイスのヘルス モニタリング ページに移動します。
- **[トラブルシューティング ファイル（Troubleshooting Files）]**：レポートに含めるデータのタイプを選択できるトラブルシューティング ファイルを生成します。

デバイス グループの追加

Firewall Management Center でデバイスをグループ化すると、複数のデバイスへのポリシーの展開やアップデートのインストールを簡単に行えます。グループに属するデバイスのリストは、展開または縮小表示できます。

高可用性ペア内のプライマリデバイスをグループに追加すると、両方のデバイスがグループに追加されます。高可用性ペアを分解しても、これらのデバイスは両方ともグループに属したままになります。

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 [追加（Add）] ドロップダウン メニューから、[グループの追加（Add Group）] を選択します。

既存のグループを編集するには、編集するグループの[編集（Edit）]（✎）をクリックします。

ステップ 3 名前を入力します。

ステップ 4 [使用可能なデバイス（Available Devices）] から、デバイス グループに追加するデバイスを 1 つ以上選択します。複数のデバイスを選択する場合は、Ctrl または Shift キーを押しながらクリックします。

ステップ 5 [追加（Add）] をクリックして、選択したデバイスをデバイス グループに追加します。

ステップ 6 必要に応じて、デバイスグループからデバイスを削除するには、削除するデバイスの横にある[削除（Delete）]（🗑）をクリックします。

ステップ 7 [OK] をクリックして、デバイス グループを追加します。

Management Center への登録

Firewall Management Center では、デバイスを登録するための複数の方法が提供されています。

デバイスの追加

Firewall Management Center に 1 つのデバイスを追加するには、次の手順を実行します。ハイアベイラビリティのためにデバイスをリンクする場合でも、この手順を使用する必要があります。ハイ アベイラビリティ ペアの追加 を参照してください。クラスタリングについては、お使いのモデルのクラスタリングに関する章を参照してください。

この手順を使用して、クラウド提供型 Firewall Management Center によって管理されるデバイスを追加することもできます。オンプレミスの Firewall Management Center はイベントのロギングと分析の目的のみに使用します。

Firewall Management Center ハイアベイラビリティを使用する場合は、アクティブ Firewall Management Center にのみデバイスを追加します。アクティブな Firewall Management Center に登録されているデバイスはスタンバイに自動的に登録されます。

始める前に

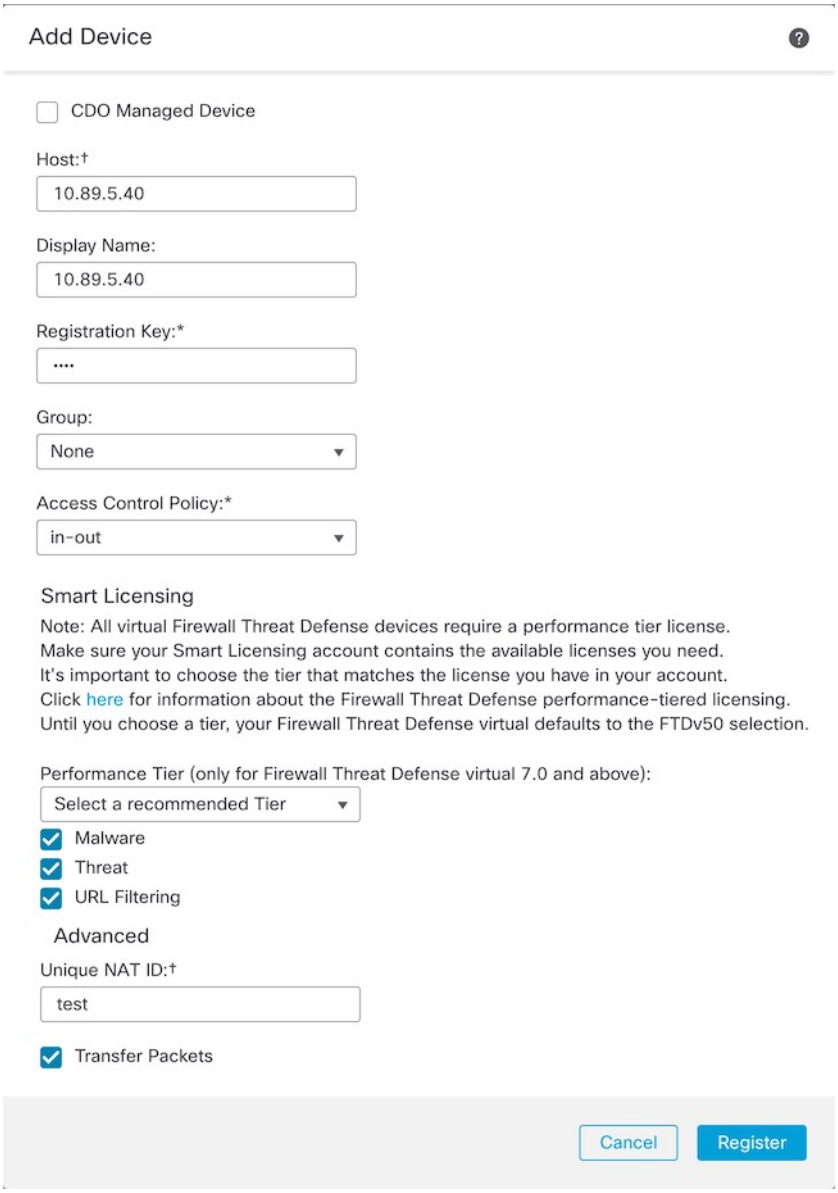
- デバイスを Firewall Management Center の管理対象として設定します。参照：
  - Firewall Threat Defense 初期設定の完了 （14 ページ）
  - 使用モデルのスタートアップガイド
- Firewall Management Center が Smart Software Manager に登録されている必要があります。有効な評価ライセンスで十分ですが、有効期限が切れると、正常に登録するまで新しいデバイスを追加できなくなります。
- IPv4 を使用して登録したデバイスを IPv6 に変換する場合は、デバイスをいったん削除してから再登録する必要があります。

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 [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。

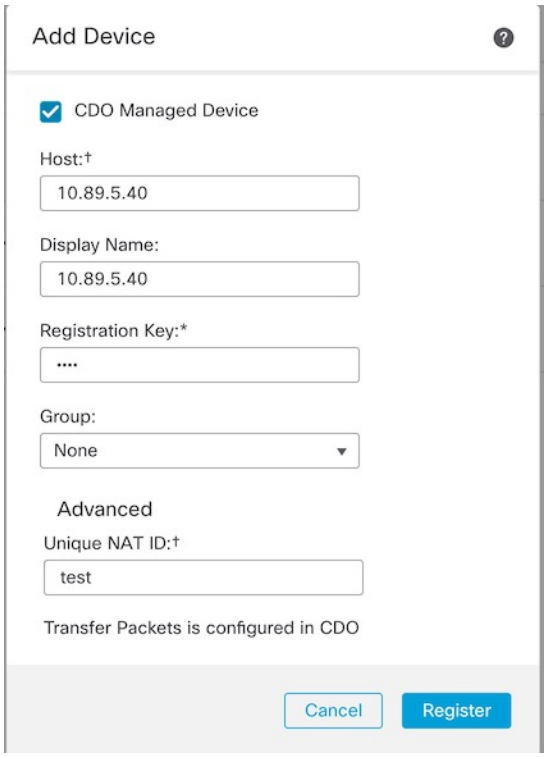
図 *9*: デバイスの追加



ステップ 3 分析専用にクラウド管理対象デバイスをオンプレミスの Firewall Management Center に追加する場合は、**[CDO管理対象デバイス（CDO Managed Device）]** をオンにします。

ライセンスとパケット転送の設定は CDO（旧 CDO）によって管理されるため、システムでは表示されません。これらのステップはスキップできます。

図 *10 : CDO* 用のデバイスの追加



ステップ 4 [ホスト（Host）] には、追加デバイスの IP アドレスまたはホスト名を入力します。デバイスの IP アドレスが不明な場合（NAT の背後にある場合など）は、このフィールドを空白のままにします。

このフィールドを空白のままにする場合は、デバイスの初期設定で、到達可能な Firewall Management Center の IPアドレスまたはホスト名と NAT ID が指定されている必要があります。詳細については、NAT 環境 （8 ページ）を参照してください。

ステップ 5 [表示名（Display name）] フィールドに、Firewall Management Center でのデバイスの表示名を入力します。この名前は変更できません。

ステップ 6 [登録キー（Registration key）] には、初期設定で指定したものと同じ登録キーを入力します。登録キーは、1 回限り使用可能な共有シークレットです。キーは英数字（A～Z、a～z、0～9）、およびハイフン（-）を使用して、37 文字以内で指定します。登録キーはデバイスごとに一意である必要はありません。

ステップ 7 （任意） デバイスをデバイス**グループ**に追加します。

ステップ 8 登録後すぐに、デバイスに展開する最初の [アクセス コントロール ポリシー（Access Control Policy）] を選択するか、新しいポリシーを作成します。

デバイスが選択したポリシーに適合しない場合、展開は失敗します。この不適合には、複数の要因が考えられます。たとえば、ライセンスの不一致、モデルの制限、パッシブとインラインの問題、その他の構成ミスなどです。この障害の原因を解決した後、デバイスに手作業で設定を行います。

ステップ 9 デバイスに適用するライセンスを選択します。

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）]** ページからライセンスを適用することもできます。

Firewall Threat Defense Virtual の場合は、[パフォーマンス階層（Performance Tier）] も選択する必要があります。使用アカウントにあるライセンスと一致する階層を選択することが重要です。階層を選択するまで、デバイスではデフォルトで FTDv50 が選択されます。Firewall Threat Defense Virtual で使用可能なパフォーマンス階層ソフトウェア利用資格の詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*FTDv Licenses*」を参照してください。

（注）
Firewall Threat Defense Virtual をバージョン 7.0 以上にアップグレードする場合は、[FTDv -変数（FTDv - Variable）] を選択して現在のライセンスコンプライアンスを維持できます。

ステップ 10 初期設定時に NAT ID を指定した場合は、[詳細（Advanced）] セクションの [一意のNAT ID（Unique NAT ID）] に同じ NAT ID を入力します。

[一意のNAT ID（Unique NAT ID）] には、任意の一意のワンタイム文字列を指定します。この文字列は、初期設定時にデバイスでも指定します。このワンタイム文字列は、一方の側で到達可能な IPアドレスやホスト名が指定されていない場合に必要になります。たとえば、[ホスト（Host ）] フィールドを空白のままにした場合などです、技術的にはオプションですが、特定の状況で必要になるため、両側の IP アドレスがわかっている場合でも、常に NAT ID を指定することを推奨します。ID は英数字（A～Z、a～z、0～9）、およびハイフン（-）を使用して、37 文字以内で指定します。この ID は、Firewall Management Center に登録する他のデバイスには使用できません。

ステップ 11 [パケットの転送（Transfer Packets）] チェックボックスをオンにして、侵入イベントが発生するたびに、デバイスが検査のためにパケットを Firewall Management Center に転送するようにします。

このオプションは、デフォルトで有効です。侵入イベントごとに、デバイスは、イベント情報とイベントをトリガーしたパケットを検査のために Firewall 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 Firewall Management Center に送信され、パケットは送信されません。

ステップ 12 [登録（Register）] をクリックします。

Firewall Management Center がデバイスのハートビートを確認して通信を確立するまでに、最大 2 分かかる場合があります。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。デバイスの登録に失敗した場合は、次の項目を確認してください。

- ping：デバイスの CLI にアクセスし、次のコマンドを使用して Firewall 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。デバイスの IP アドレスを変更する必要がある場合は、**configure network** {**ipv4** | **ipv6**} **manual** コマンドを使用します。

- 登録キー、NAT ID、および Firewall 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、デバイスで登録キーと 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。

新しい Management Center への登録

この手順では、新しい Firewall Management Center に登録する方法を示します。新しい Firewall Management Center が古い Firewall Management Center の IP アドレスを使用している場合でも、次の手順を実行する必要があります。

手順

ステップ 1 古い Firewall Management Center に管理対象デバイスが存在する場合はこれを削除します。Firewall Management Center からのデバイスの削除（登録解除） （39 ページ）を参照してください。

Firewall Management Center とのアクティブな接続がある場合は、Firewall Management Center IP アドレスを変更できません。

ステップ 2 SSH などを使用して、デバイスの CLI に接続します。

ステップ 3 新しい Firewall Management Center を設定します。

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *regkey* [*nat_id*] [*display_name*]

- {*hostname* | *IPv4_address* | *IPv6_address*}：Firewall Management Center のホスト名、IPv4 アドレス、または IPv6 アドレスを設定します。
- **DONTRESOLVE**：Firewall Management Center を直接アドレス指定できない場合は、ホスト名または IP アドレスの代わりに **DONTRESOLVE** を使用します。**DONTRESOLVE** を使用する場合は、*nat_id* が必要です。このデバイスを Firewall Management Center に追加する場合は、デバイスの IP アドレスと *nat_id* の両方を必ず指定してください。接続の片側で IP アドレスを指定し、両側で同じ一意の NAT ID を指定する必要があります。
- *regkey*：登録時に Firewall Management Center とデバイス間で共有する登録キーを作成します。このキーには、1 ～ 37 文字の任意のテキスト文字列を選択できます。Firewall Threat Defense を追加するときに、Firewall Management Center に同じキーを入力します。

- *nat_id*：一方が IP アドレスを指定しない場合に、Firewall Management Center とデバイス間の登録プロセス中のみに使用する 1 ～ 37 文字の英数字文字列を作成します。この NAT ID は、登録時にのみ使用されるワンタイムパスワードです。NAT ID が一意であり、登録を待機している他のデバイスによって使用されていないことを確認します。Firewall Threat Defense を追加するときに、Firewall Management Center で同じ NAT ID を指定します。
- *display_name*：**show managers** コマンドでこのマネージャを表示するための表示名を指定します。このオプションは、CDO をプライマリマネージャおよび分析専用のオンプレミス Firewall Management Center として識別する場合に役立ちます。この引数を指定しない場合、ファイアウォールは以下のいずれかの方法を使用して表示名を自動生成します。
  - *hostname* | *IP_address*（**DONTRESOLVE** キーワードを使用しない場合）
  - **manager-***timestamp*

例：

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

ステップ 4 デバイスを Firewall Management Center に追加します。

Firewall Management Center からのデバイスの削除（登録解除）

デバイスを管理する必要がなくなった場合、Firewall Management Center からデバイスの登録を解除できます。

クラスタ、クラスタノード、または高可用性ペアの登録を解除するには、それらの展開の章を参照してください。

デバイスの登録解除：

- Firewall Management Center とそのデバイスとの間のすべての通信が切断されます。
- [デバイス管理（Device Management）] ページからデバイスが削除されます。
- デバイスのプラットフォーム設定ポリシーで、NTP を使用して Firewall Management Center から時間を受信するように設定されている場合は、デバイスがローカル時間管理に戻されます。
- 設定はそのままになるため、デバイスはトラフィックの処理を続行します。

  NAT や VPN などのポリシー、ACL、およびインターフェイス構成は維持されます。

同じまたは別の Firewall Management Center にデバイスを再登録すると、設定が削除されるため、デバイスはその時点でトラフィックの処理を停止します。

デバイスを削除する前に、再登録時にデバイスレベルの設定（インターフェイス、ルーティングなど）を再適用できるように、設定のエクスポート、を行ってください。保存された設定がない場合は、デバイス設定を再構成する必要があります。

デバイスを再度追加し、保存した設定をインポートするか、または設定を再構成した後、トラフィックの受け渡しを再開する前に、設定を展開する必要があります。

始める前に

Firewall Management Center に再度追加した場合に、デバイスレベルの設定を再適用するには

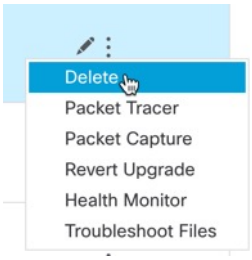
- デバイス設定をエクスポートします。デバイス設定のエクスポートとインポートを参照してください。

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 登録を解除するデバイスの横にある[その他（More）] (⋮) をクリックし、**[削除（Delete）]**をクリックします。

図 *11* : 消去



ステップ 3 デバイスの登録を解除することを確認します。

ステップ 4 マネージャを変更できるようになりました。

- この Firewall Management Center にデバイスを再登録する：登録キーと NAT ID が分かっている場合は、デバイスの追加 （34 ページ） を実行できます。それらをリセットする必要がある場合は、マネージャを新しいものであるかのように再設定できます。新しい Management Center への登録 （38 ページ） を参照してください。
- 新しい Firewall Management Center に登録する：新しい Management Center への登録 （38 ページ）。
- Firewall Device Manager に変更を加える：Firewall Management Center から Firewall Device Manager への切り替え （48 ページ）。

- 新しいマネージャを指定せずにマネージャを削除する：新しいマネージャを識別せずに（マネージャなしのモード）、Firewall Threat Defense で管理接続を切断するには、Firewall Threat Defense の CLI から **configure manager delete** コマンドを使用します。

デバイスのシャットダウンまたは再起動

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。

システムを適切にシャットダウンまたは再起動するには、以下のタスクを参照してください。

（注） デバイスを再起動すると、管理接続を再確立できなかったというエラーが表示される場合があります。場合により、デバイスの管理インターフェイスの準備が整う前に接続が試行されます。接続は自動的に再試行され、15 分以内に確立されます。

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）] をクリックします。

ステップ 4 デバイスを再起動するには、次の手順を実行します。

a) [デバイスの再起動（Restart Device）]（） をクリックします。
b) プロンプトが表示されたら、デバイスを再起動することを確認します。

ステップ 5 デバイスをシャットダウンするには、次の手順を実行します。

a) [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。
b) 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。
c) 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 分間待ってシステムがシャットダウンしたことを確認します。

ISA 3000 の場合、シャットダウンが完了すると、システム LED が消灯します。電源を切る前に、少なくとも 10 秒待ってください。

マネージャの切り替え

必要に応じてマネージャを切り替えることができます。

Firewall Device Manager から Firewall Management Center への切り替え

Firewall Device Manager から Firewall Management Center へ切り替えると、管理インターフェイスとマネージャアクセス設定に加えて、すべてのインターフェイス構成が保持されます。アクセス コントロール ポリシーやセキュリティゾーンなどの他の設定は保持されないことに注意してください。

Firewall Management Center に切り替えると、Firewall Device Manager を使用して Firewall Threat Defense デバイスを管理できなくなります。

始める前に

ファイアウォールが高可用性用に設定されている場合は、まず、Firewall Device Manager（可能な場合）または **configure high-availability disable** コマンドを使用して、高可用性設定を中断する必要があります。アクティブなユニットから高可用性を中断することをお勧めします

手順

ステップ 1 Firewall Device Manager で、Cisco Smart Software Manager からデバイスを登録解除します。

ステップ 2 （必要に応じて）管理インターフェイスを設定します。

マネージャアクセスにデータインターフェイスを使用する場合でも、管理インターフェイスの設定を変更する必要がある場合があります。Firewall Device Manager 接続に管理インターフェイスを使用していた場合は、Firewall Device Manager に再接続する必要があります。

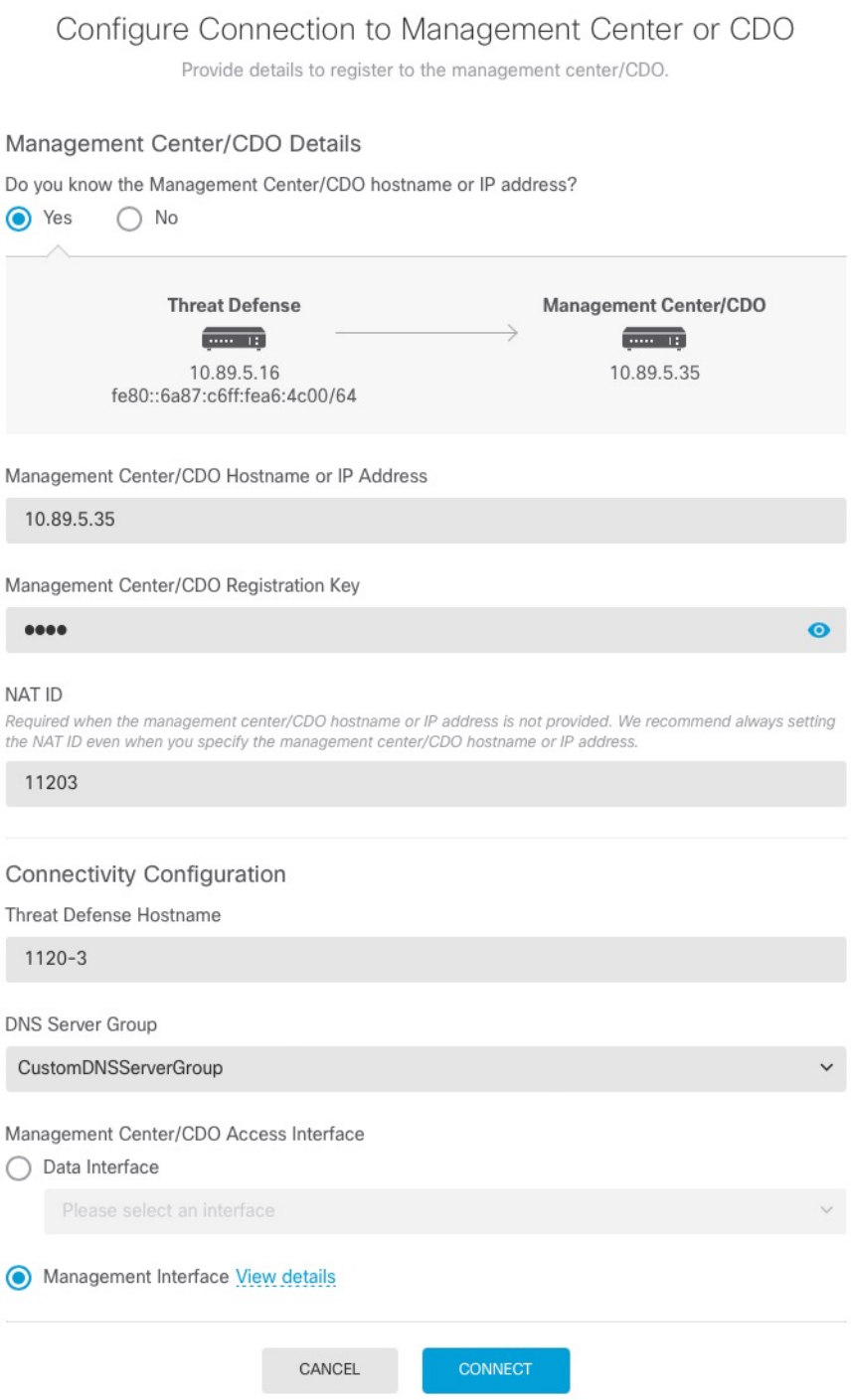
- マネージャアクセス用のデータインターフェイス：管理インターフェイスには、データインターフェイスに設定されたゲートウェイが必要です。デフォルトでは、管理インターフェイスは DHCP から IP アドレスとゲートウェイを受信します。DHCP からゲートウェイを受信しない場合（たとえば、管理インターフェイスをネットワークに接続していない場合）、ゲートウェイはデフォルトでデータインターフェイスになり、何も設定する必要はありません。DHCP からゲートウェイを受信した場合は、代わりに管理インターフェイスに静的 IP アドレスを設定し、ゲートウェイをデータインターフェイスに設定する必要があります。
- マネージャアクセス用の管理インターフェイス：静的 IP アドレスを設定する場合は、デフォルトゲートウェイもデータインターフェイスではなく一意のゲートウェイに設定して

ください。DHCP を使用する場合は、DHCP からゲートウェイを正常に取得できると仮定して、何も設定する必要はありません。

ステップ 3 **[デバイス（Device）]**>**[システム設定（System Settings）]**>**[集中管理（Central Management）]** の順に選択し、[続行（Proceed）] をクリックして Firewall Management Center の管理を設定します。

ステップ 4 [Management Center/SCCCDOの詳細（Management Center/**CDO** Details）] を設定します。

図 *12 : Management Center/CDO* の詳細



a) [Management Center/SCCCDO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 Management Center/**CDO** hostname or IP address?）] で、IP アドレスまたはホスト名を使用して Firewall Management Center に到達できる場合は [はい（Yes）] をクリックし、Firewall

Management CenterCDO 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、少なくても 1 台以上のデバイス（Firewall Management Center または Firewall 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、[Management Center/SCCCDOのホスト名/IPアドレス（Management Center/**CDO** Hostname or IP Address）] を入力します。

c) [Management Center/SCCCDO登録キー（Management Center/**CDO** Registration Key）] を指定します。

このキーは、Firewall Threat Defense デバイスを登録するときに Firewall 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 2 ～ 36 文字である必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Firewall Management Center に登録する複数のデバイスに使用できます。

a) [NAT ID] を指定します。

この ID は、Firewall Management Center でも指定する任意の 1 回限りの文字列です。NAT ID は 2 ～ 36 文字である必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Firewall 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、接続元が正しいデバイス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、登録キーが確認されます。任意である場合でも常にNAT IDを使用することを推奨しますが、次の場合は必須です。

- Firewall Management Center IP アドレスを **DONTRESOLVE** に設定する。
- Firewall Management Center でデバイスを追加するときに、到達可能なデバイスの IP アドレスまたはホスト名を指定していない。
- 両側でIPアドレスを指定する場合でも、管理にデータインターフェイスを使用する。
- Firewall Management Center が複数の管理インターフェイスを使用する。

ステップ 5 [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。

[Management Center/SCCCDOアクセスインターフェイス（Management Center/**CDO** Access Interface）] のアクセスにデータインターフェイスを使用する場合、FQDN がこのインターフェイスに使用されます。

b) [DNSサーバグループ（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 サーバが含まれます。

[Management Center/SCCCDOアクセスインターフェイス（Management Center/**CDO** Access Interface）] のデータインターフェイスを選択する場合は、この設定でデータインターフェイス DNS サーバーを設定します。セットアップウィザードで設定した管理 DNS サーバ

は、管理トラフィックに使用されます。データDNSサーバは、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じ DNS サーバーグループを選択する可能性があります。

Firewall Management Center では、この Firewall Threat Defense デバイス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。Firewall Management Center に Firewall Threat Defense デバイスを追加すると、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Firewall Threat Defenseデバイス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。Firewall Management Center とFirewall Threat Defenseデバイスを同期させるには、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Firewall Management Center で保持されます。

[Management Center/SCCCDOアクセスインターフェイス（Management Center/**CDO** Access Interface）]**[FMCアクセスインターフェイス（FMC Access Interface）]** の管理インターフェイスを選択する場合は、この設定で管理 DNS サーバーを設定します。

c) [Management Center/SCCCDOアクセスインターフェイス（Management Center/**CDO** Access Interface）] については、任意の設定済みインターフェイスを選択します。

管理インターフェイスは、Firewall Threat Defense デバイスを Firewall 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。

ステップ 6 （任意）外部インターフェイスではない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、Firewall 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。

管理インターフェイスを選択した場合は、この画面に進む前に、ゲートウェイを一意のゲートウェイとして設定する必要があります。

ステップ 7 （任意） データインターフェイスを選択した場合は、[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、 IP アドレスが変更された場合に Firewall Management Center が完全修飾ドメイン名（FQDN）でFirewall Threat Defenseデバイス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。

Firewall Management Center に Firewall Threat Defense デバイスを追加する前に DDNS を設定すると、Firewall Threat Defense デバイスは、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し、Firewall Threat Defense デバイスが HTTPS 接続のために DDNS サーバー証明書を検証できるようにします。 Firewall 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。

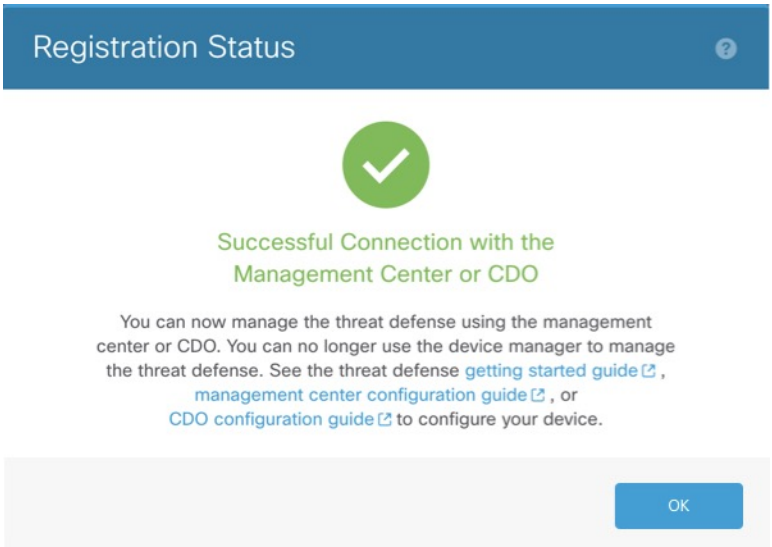
マネージャアクセスに管理インターフェイスを使用する場合、DDNS はサポートされません。

ステップ 8 [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、Firewall 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/SCCCDO登録設定の保存（Saving Management Center/**CDO** Registration Settings）] のステップの後、Firewall Management Center に移動してファイアウォールを追加します。

Firewall 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/SCCCDO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 Firewall 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、Firewall Device Manager に再接続した場合のみ再開されます。

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

図 *13*：正常接続



Firewall Management Center から Firewall Device Manager への切り替え

代わりにFirewall Device Managerを使用するように、オンプレミスまたはクラウド提供型のFirewall Management Centerによって現在管理されている Firewall Threat Defense デバイスを設定できます。

ソフトウェアを再インストールすることなく、Firewall Management CenterからFirewall Device Managerに切り替えることができます。Firewall Management CenterからFirewall Device Managerに切り替える前に、Firewall Device Managerがすべての設定要件を満たしていることを確認します。Firewall Device Manager から Firewall Management Center に切り替える場合は、Firewall Device Manager から Firewall Management Center への切り替え （42 ページ） を参照してください。

注意 Firewall Device Manager に切り替えると、デバイスの設定は削除され、システムはデフォルト設定に戻ります。ただし、管理 IP アドレスとホスト名は維持されます。

手順

ステップ 1 Firewall Management Center で、**[デバイス（Devices）]**>**[デバイス管理（Device Management）]** ページからファイアウォールを削除します。

ステップ 2 SSH またはコンソールポートを使用して、Firewall Threat Defense CLI に接続します。SSH の場合、管理 IP アドレスへの接続を開き、admin ユーザー名（または管理者権限を持つ他のユーザー）で Firewall Threat Defense CLI にログインします。

（Firepower モデル）コンソールポートはデフォルトで FXOS CLI になります。**connect ftd** コマンドを使用して、Firewall Threat Defense CLI に接続します。SSH セッションは Firewall Threat Defense CLI に直接接続します。

管理 IP アドレスに接続できない場合は、次のいずれかを実行します。

- 管理物理ポートが、機能しているネットワークに接続されていることを確認します。
- 管理ネットワークに管理IPアドレスとゲートウェイが設定されていることを確認します。**configure network ipv4/ipv6 manual**コマンドを使用します。

ステップ 3 現在、リモート管理モードになっていることを確認します。

show managers

例：

```
> show managers
Type                       : Manager
Host                       : 10.89.5.35
Display name               : 10.89.5.35
Identifier                 : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration               : Completed
```

ステップ 4 リモート マネージャを削除すると、マネージャなしのモードになります。

configure manager delete *uuid*

リモート管理からローカル管理に直接移行することはできません。複数のマネージャが定義されている場合は、識別子（UUID とも呼ばれます。**show managers** コマンドを参照）を指定する必要があります。各マネージャ エントリを個別に削除します。

例：

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

ステップ 5 ローカル マネージャを設定します。

configure manager local

これで、Web ブラウザで **https://***management-IP-address* にアクセスしてローカル マネージャを開くことができるようになりました。

例：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

Cisco Secure Firewall 3100 での SSD のホットスワップ

SSD が 2 つある場合、起動時に RAID が形成されます。ファイアウォールの電源が入っている状態で Firewall Threat Defense CLI で次のタスクを実行できます。

- SSD の 1 つをホットスワップする：SSD に障害がある場合は、交換できます。SSD が 1 つしかない場合、ファイアウォールの電源がオンになっている間 SSD は取り外せません。
- SSD の 1 つを取り外す：SSD が 2 つある場合は、1 つを取り外すことができます。
- 2 つ目の SSD を追加する：SSD が 1 つの場合は、2 つ目の SSD を追加して RAID を形成できます。

注意 この手順を使用して、SSD を RAID から削除する前に SSD を取り外さないでください。データが失われる可能性があります。

手順

ステップ 1 SSD の 1 つを取り外します。

a) SSD を RAID から取り外します。

configure raid remove-secure local-disk {**1** | **2**}

remove-secure キーワードは SSD を RAID から削除し、自己暗号化ディスク機能を無効にして、SSD を安全に消去します。SSD を RAID から削除するだけでデータをそのまま維持する場合は、**remove** キーワードを使用できます。

例：

```
> configure raid remove-secure local-disk 2
```

b) SSD がインベントリに表示されなくなるまで、RAID ステータスを監視します。

show raid

SSD が RAID から削除されると、**操作性**と**ドライブの状態**が**劣化**として表示されます。2 つ目のドライブは、メンバーディスクとして表示されなくなります。

例：

```
> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                operable
Presence:                   equipped
Lifecycle:                  available
Drive State:                optimal
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
```

```
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) SSD をシャーシから物理的に取り外します。

ステップ 2 SSD を追加します。

a) SSD を空のスロットに物理的に追加します。

b) SSD を RAID に追加します。

configure raid add local-disk {**1** | **2**}

新しい SSD と RAID の同期が完了するまでに数時間かかることがありますが、その間、ファイアウォールは完全に動作します。再起動もでき、電源投入後に同期は続行されます。ステータスを表示するには、**show raid** コマンドを使用します。

以前に別のシステムで使用されており、まだロックされている SSD を取り付ける場合は、次のコマンドを入力します。

configure raid add local-disk {**1** | **2**} *psid*

psid は SSD の背面に貼られたラベルに印刷されています。または、システムを再起動し、SSD を再フォーマットして RAID に追加できます。

デバイス管理の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
ISA 3000 システム LED によるシャットダウンのサポート。	7.0.5/7.3.0	7.0.5/7.3.0	ISA 3000 をシャットダウンすると、システム LED が消灯します。電源を切る前に、少なくとも 10 秒待ってください。
ISA 3000 によるシャットダウンのサポート。	7.0.2/7.2.0	7.0.2/7.2.0	ISA 3000 をシャットダウンできるようになりました。以前は、デバイスを再起動することしかできませんでした。
マルチマネージャのサポート。	7.2.0	7.2.0	クラウド提供型の管理センターを導入しました。このクラウド提供型の管理センターは、Cisco Defense Orchestrator（CDO）プラットフォームを使用して、複数のシスコのセキュリティ ソリューションの管理を統合します。マネージャの更新についてはシスコが行います。 バージョン 7.2 以降を実行しているハードウェアまたは仮想管理センターでは、クラウド管理型のデバイスを「共同管理」できますが、用途はイベントのロギングと分析に限られます。このハードウェアまたは仮想管理センターからは、デバイスにポリシーを展開できません。 新規/変更されたコマンド：**configure manager add**、**configure manager delete**、**configure manager edit**、**show managers** 新規/変更された画面： • クラウド管理型デバイスをハードウェアまたは仮想管理センターに追加する場合は、新しい [CDO管理対象デバイス（CDO Managed Device）] チェックボックスをオンにして、それが分析専用であることを指定します。 • **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択すると、分析専用のデバイスが表示されます。 詳細については、CDOのドキュメントを参照してください。
Cisco Secure Firewall 3100 での SSD の RAID サポート。	7.1.0	7.1.0	SSD は自己暗号化ドライブ（SED）です。SSD が 2 つある場合、ソフトウェア RAID を形成します。 新規/変更されたコマンド： **configure raid, show raid, show ssd**
管理接続での TLS 1.3 のサポート。	7.1.0	7.1.0	FMC デバイス管理接続で TLS 1.3 が使用されるようになりました。以前は、TLS 1.2 がサポートされていました。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
FDM を使用して、FMC による管理用に FTD を設定します。	7.1.0	7.1.0	FDMを使用して初期設定を実行すると、管理およびマネージャアクセス設定に加えて、管理のためにFMCに切り替えたときに、FDM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やセキュリティゾーン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。FMC CLIを使用すると、管理設定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）。 FMC に切り替えると、FDM を使用して FTD を管理できなくなります。 新規/変更された FDM 画面：**[システム設定（System Settings）] > [管理センター（Management Center）]**
アップグレードステータスでデバイスをフィルタする。	6.7.0	6.7.0	[デバイス管理（Device Management）]ページに、デバイスがアップグレードされているかどうか（およびそのアップグレードパス）や、最後のアップグレードが成功したか失敗したかなどの、管理対象デバイスに関するアップグレード情報が表示されるようになりました。 新規/変更された画面：**[デバイス（Devices）]>[デバイス管理（Device Management）]**
Firepower Chassis Manager へのワンクリックアクセス。	6.4.0	6.4.0	Firepower 4100/9300 シリーズデバイスの場合は、[デバイス管理（Device Management）] ページに、Firepower Chassis Manager Web インターフェイスへのリンクが表示されます。 新規/変更された画面：**[デバイス（Devices）]>[デバイス管理（Device Management）]**
正常性と展開のステータスでデバイスをフィルタする。バージョン情報を表示する。	6.2.3	6.2.3	[デバイス管理（Device Management）] ページに管理対象デバイスのバージョン情報が表示されるようになり、正常性および展開のステータスでデバイスをフィルタする機能が追加されました。 新規/変更された画面：**[デバイス（Devices）]>[デバイス管理（Device Management）]**

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。