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。Security Cloud Control（Security Cloud Control）Cloud-Delivered 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。Cloud-Delivered 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 Security Cloud Control: Cloud-Delivered Firewall Management Center for Firewall Threat Defense*」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 （1 ページ）
- デバイス管理の要件と前提条件 （12 ページ）
- 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 （13 ページ）
- 手動登録での Firewall Threat Defense 初期設定の完了 （15 ページ）
- デバイスの管理 （32 ページ）
- マネージャの切り替え （80 ページ）
- Cisco Secure Firewall 3100/4200 での SSD のホットスワップ （86 ページ）
- USB ポートの無効化 （88 ページ）
- デバイス管理の履歴 （91 ページ）

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） Security Cloud Control 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 Security Cloud Control 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。

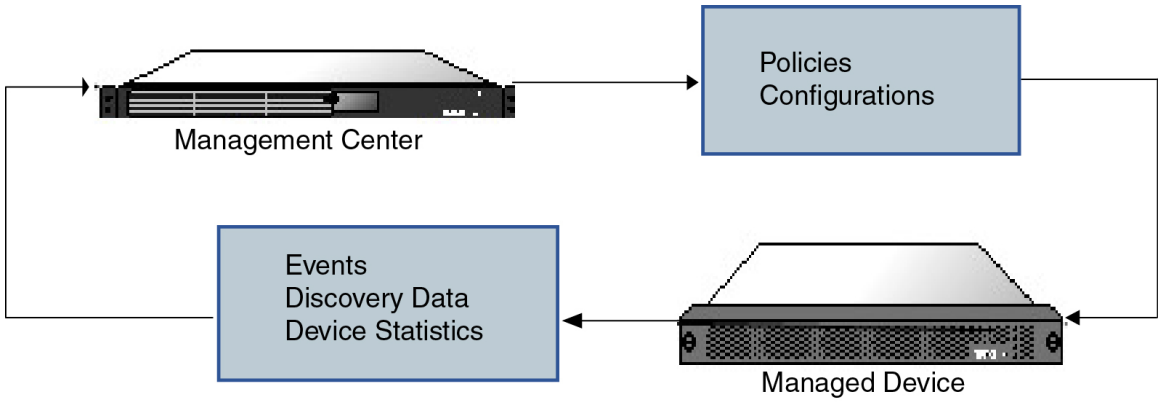
（注） Firewall Management Center は、http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html で入手可能な互換性マトリックスで指定されている特定の以前のリリースを実行しているデバイスを管理できますが、これらの以前のリリースのデバイスでは、最新バージョンの Firewall Threat Defense ソフトウェアが必要な新しい機能は利用できません。一部の Firewall Management Center 機能は、以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

（注） zero-touch provisioningを使用してデバイスを登録する場合は、マネージャアクセス用に外部インターフェイスを使用すると、デフォルトでDHCPが使用されます。高可用性を有効にする前に、IPアドレスを静的アドレスに変更する必要があります。デバイスIPアドレスの変更を参照してください。または、代わりに管理インターフェイスを使用することができます。高可用性を備えた管理で DHCP がサポートされます。

- 同じサブネット内に異なる静的 IP アドレスがあります。
- 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。

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。

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
Cisco Secure Firewall 1200	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
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
Cisco Secure Firewall 4200	management0 （注） management0 は管理 1/1 インターフェイスの内部名です。	management1 （注） management1 は管理 1/2 インターフェイスの内部名です。
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。

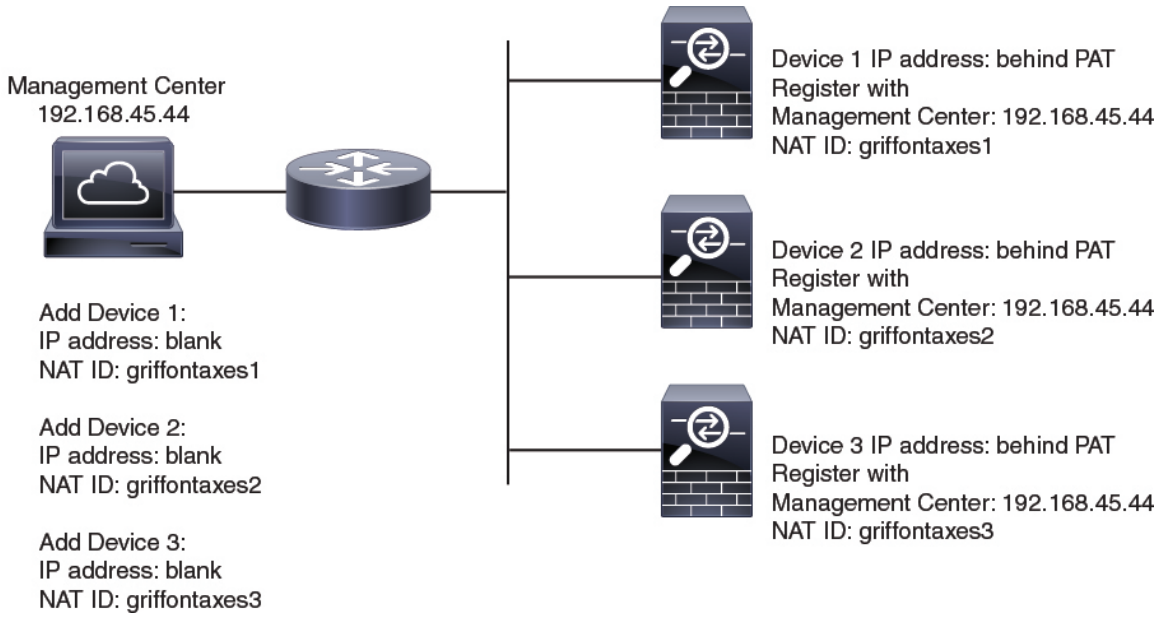
通常は、ルーティングと認証の両方の目的で両方の IP アドレス（登録キー付き）が必要です。デバイスを追加するときに、Firewall Management Center がデバイスの IP アドレスを指定し、デバイスが Firewall Management Center の IP アドレスを指定します。ただし、IP アドレスの 1 つのみがわかっている場合（ルーティング目的の最小要件）は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要もあります。Firewall Management Center およびデバイスでは、初期登録の認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

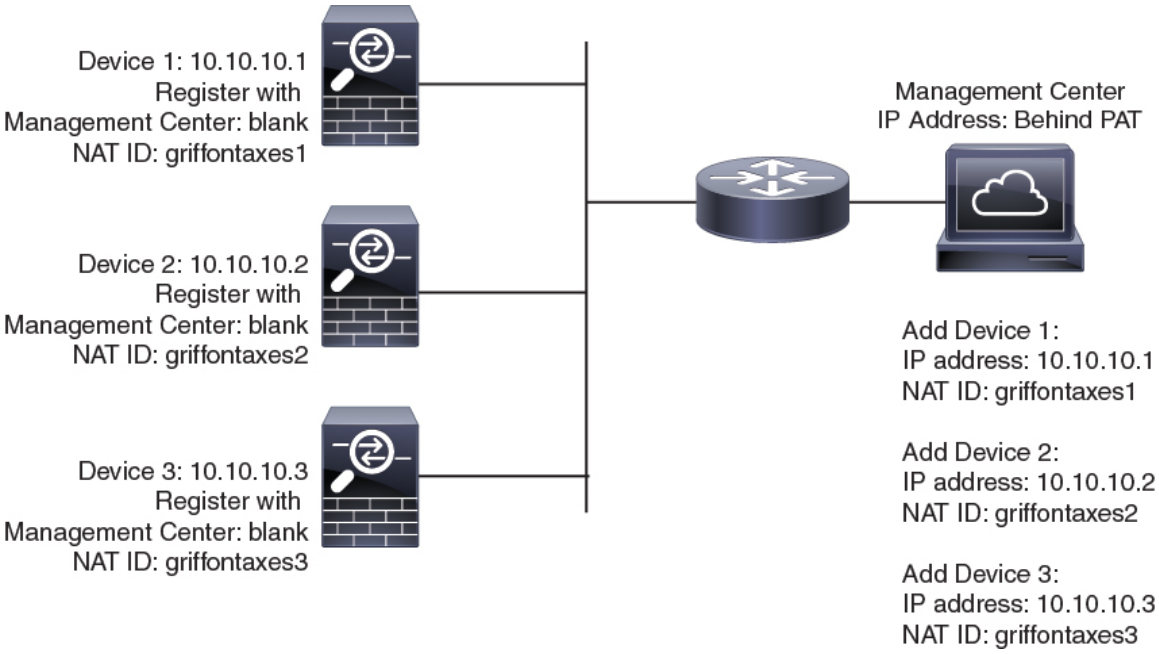
次の例に、PAT IP アドレスの背後にある 3 台のデバイスを示します。この場合、Firewall Management Center とデバイスの両方でデバイスごとに一意の NAT ID を指定し、デバイス上の Firewall Management Center の IP アドレスを指定します。

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*

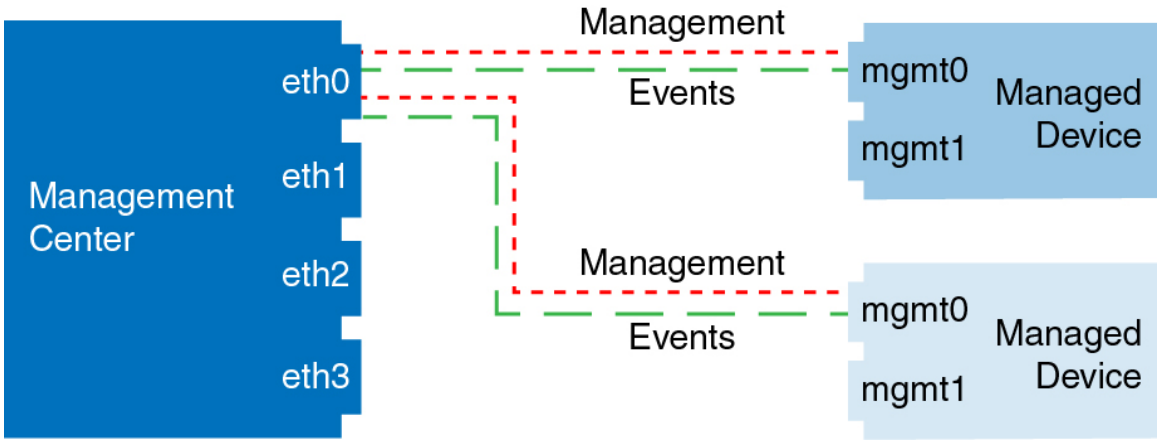


管理およびイベント トラフィック チャネルの例

（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。

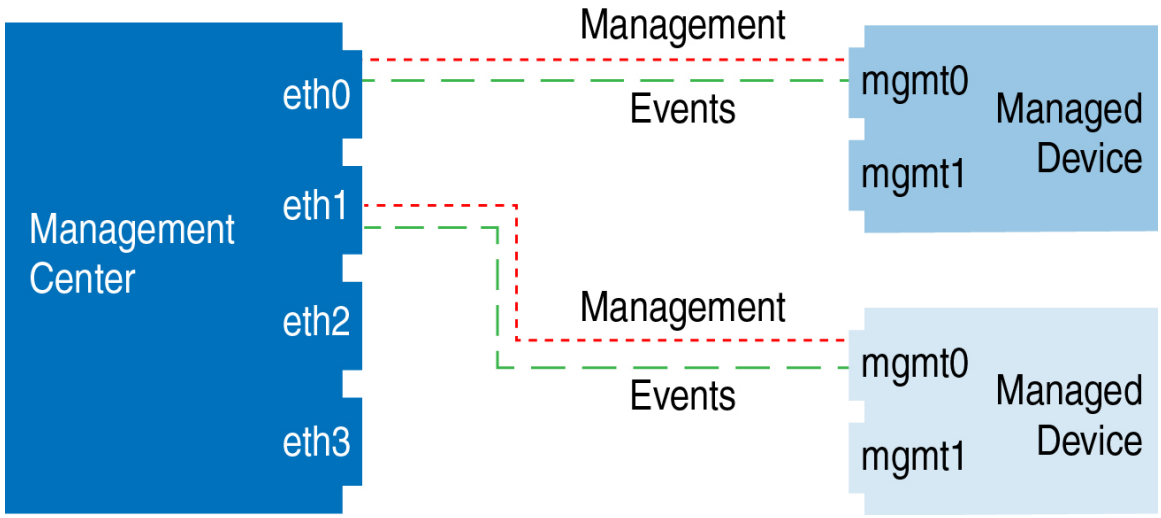
以下に、Firewall Management Center と管理対象デバイスでデフォルト管理インターフェイスのみを使用する例を示します。

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



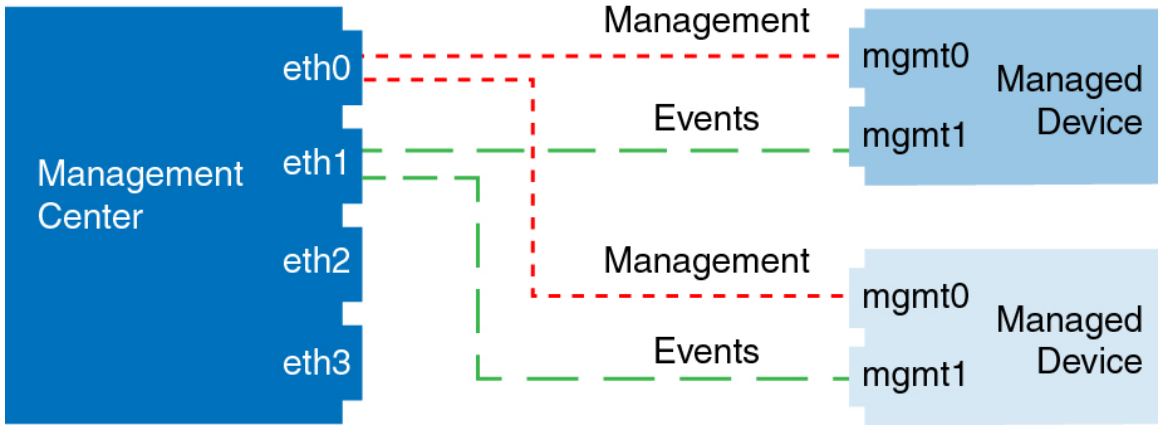
以下に、Firewall Management Center でデバイスごとに別個の管理インターフェイスを使用する例を示します。この場合、各管理対象デバイスが 1 つの管理インターフェイスを使用します。

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



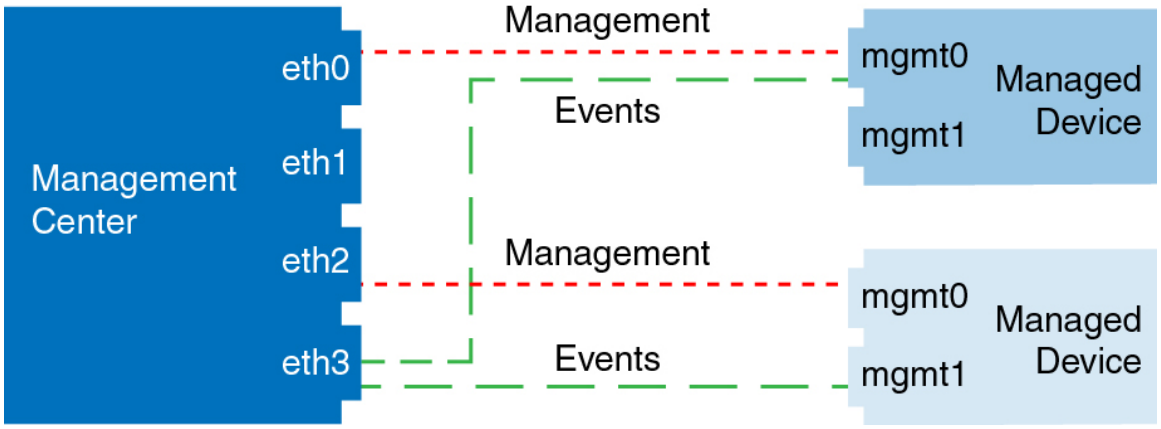
以下に、個別のイベント インターフェイスを使用する Firewall Management Center と管理対象デバイスの例を示します。

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

Supported domains

デバイスが存在するドメイン。

User roles

- Admin
- Network Admin

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。

Zero-Touch Provisioning 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 Zero-Touch Provisioning はサポートされません。

zero-touch provisioning 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。

Zero-Touch Provisioning 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
- Cisco Secure Firewall 1200
- 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 （22 ページ）を参照してください。

zero-touch provisioning の場合、Firewall Threat Defense CLI にアクセスして、セットアップスクリプトを実行したときに次のプロンプトメッセージが表示された場合は、[n] を選択します。「 `Do you want to configure IPv4? (y/n) [y]:`」および「`Do you want to configure IPv6? (y/n) [y]:`」。また、デフォルトのローカルマネージャを承認する必要があります：「`Manage the device locally? (yes/no) [yes]:`」。これらの設定により zero-touch provisioning機能が保持されます。

（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、「SSH アクセスの確保」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。

マルチインスタンスモードのシャーシの場合、コンソールポートの FXOS に接続するか、SSH および SSH アクセスリストの設定 に従って管理インターフェイスの FXOS に対する SSH を有効にすることができます。SSH は、デフォルトでは無効にされています。

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

マルチインスタンスモード：

connect ftd *name*

インスタンス名を表示するには、名前を付けずにコマンドを入力します。

（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、およびリカバリ設定モードがあります。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#
```

リカバリ設定モードを使用するには、診断 CLI でのリカバリ設定モードへのアクセスを参照してください。

通常の CLI に戻るには、Ctrl+a、d を入力します。

手動登録での 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。

zero-touch provisioning（シリアル番号登録）の場合、デバイスへのログインや初期設定は行わないでください。シリアル番号を使用したデバイスの追加（ゼロタッチプロビジョニング）：基本設定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 および Secure Firewall 1210/1220 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）。

- Cisco Secure Firewall 4200 は、Firewall Device Manager をサポートしていません。CLI 手順を使用する必要があります（CLI を使用した Firewall Threat Defense 初期設定の実行の完了（22 ページ）を参照）。
- 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 Security Cloud Control 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 （22 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 (Might be required) Configure the Management interface.

You may need to change the Management interface configuration, even if you intend to use a data interface for manager access. You will have to reconnect to the Firewall Device Manager if you were using the Management interface for the Firewall Device Manager connection.

- Data interface for manager access—The Management interface must have the gateway set to data interfaces. By default, the Management interface receives an IP address and gateway from DHCP. If you do not receive a gateway from DHCP (for example, you did not connect this interface to a network), then the gateway will default to data interfaces, and you do not need to configure anything. If you did receive a gateway from DHCP, then you need to instead configure this interface with a static IP address and set the gateway to data interfaces.
- Management interface for manager access—If you want to configure a static IP address, be sure to also set the default gateway to be a unique gateway instead of the data interfaces. If you use DHCP, then you do not need to configure anything assuming you successfully get the gateway from DHCP.

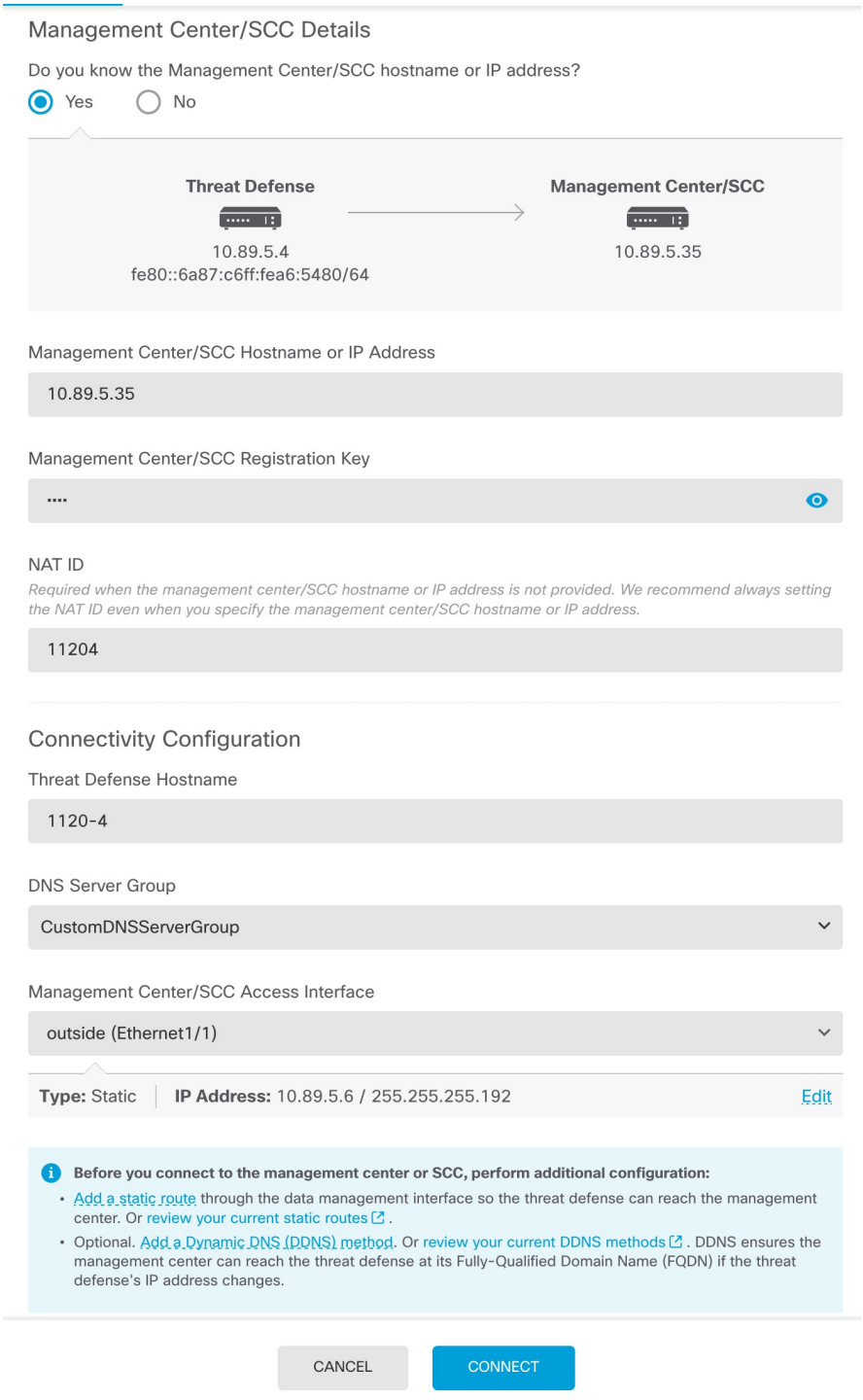
ステップ 4 マネージャアクセスに使用する外部または内部以外のインターフェイスを含む追加のインターフェイスを設定する場合は、[デバイス（Device）] を選択し、[インターフェイス（Interface）] のサマリーのリンクをクリックします。

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 Choose **Device** > **System Settings** > **Central Management**, and click **Proceed** to set up the Firewall Management Center management.

ステップ 6 Configure the **Management Center/SCC Details**.

図 *7 : Management Center/SCC Details*



a) For **Do you know the Management Center/SCC hostname or IP address?**, click **Yes** if you can reach the Firewall Management Center using an IP address or hostname, or **No** if the Firewall Management CenterSecurity Cloud Control is behind NAT or does not have a public IP address or hostname.

At least one of the devices, either the Firewall Management Center or the Firewall Threat Defense device, must have a reachable IP address to establish the two-way, TLS-1.3-encrypted communication channel between the two devices.

b) If you chose **Yes**, then enter the **Management Center/SCC Hostname or IP Address**.

c) Specify the **Management Center/SCC Registration Key**.

This key is a one-time registration key of your choice that you will also specify on the Firewall Management Center when you register the Firewall Threat Defense device. The registration key must be between 2 and 36 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID can be used for multiple devices registering to the Firewall Management Center.

a) Specify a **NAT ID**.

This ID is a unique, one-time string of your choice that you will also specify on the Firewall Management Center. The NAT ID must be between 2 and 36 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID *cannot* be used for any other devices registering to the Firewall Management Center. The NAT ID is used in combination with the IP address to verify that the connection is coming from the correct device; only after authentication of the IP address/NAT ID will the registration key be checked. We recommended that you always use the NAT ID even when it is optional, but it is required if:

- You set the Firewall Management Center IP address to **DONTRESOLVE**.
- When adding the device on the Firewall Management Center, you do not specify a reachable device IP address or hostname.
- You use the data interface for management, even if you specify IP addresses on both sides.
- The Firewall Management Center uses multiple management interfaces.

ステップ 7 Configure the **Connectivity Configuration**.

a) Specify the **FTD Hostname**.

If you use a data interface for the **Management Center/SCC Access Interface** access, then this FQDN will be used for this interface.

b) Specify the **DNS Server Group**.

Choose an existing group, or create a new one. The default DNS group is called **CiscoUmbrellaDNSServerGroup**, which includes the OpenDNS servers.

If you intend to choose a data interface for the **Management Center/SCC Access Interface**, then this setting sets the *data* interface DNS server. The Management DNS server that you set with the setup wizard is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface. You are likely to choose the same DNS server group that you used for Management, because both management and data traffic reach the DNS server through the outside interface.

On the Firewall Management Center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this Firewall Threat Defense device. When you add the Firewall Threat Defense device to the Firewall Management Center, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the Firewall Threat Defense device that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively configure the DNS Platform

Settings to match this setting to bring the Firewall Management Center and the Firewall Threat Defense device into sync.

Also, local DNS servers are only retained by the Firewall Management Center if the DNS servers were discovered at initial registration.

If you intend to choose the Management interface for the **Management Center/SCC Access InterfaceFMC Access Interface**, then this setting configures the Management DNS server.

c) For the **Management Center/SCC Access Interface**, choose any configured interface.

You can change the manager interface after you register the Firewall Threat Defense device to the Firewall Management Center, to either the Management interface or another data interface.

ステップ 8 （任意） If you chose a data interface, and it was not the outside interface, then add a default route.

You will see a message telling you to check that you have a default route through the interface. If you chose outside, you already configured this route as part of the setup wizard. If you chose a different interface, then you need to manually configure a default route before you connect to the Firewall Management Center.

If you chose the Management interface, then you need to configure the gateway to be a unique gateway before you can proceed on this screen.

ステップ 9 （任意） If you chose a data interface, click **Add a Dynamic DNS (DDNS) method**.

DDNS ensures the Firewall Management Center can reach the Firewall Threat Defense device at its Fully-Qualified Domain Name (FQDN) if the IP address changes. See **Device** > **System Settings** > **DDNS Service** to configure DDNS.

If you configure DDNS before you add the Firewall Threat Defense device to the Firewall Management Center, the Firewall Threat Defense device automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the Firewall Threat Defense device can validate the DDNS server certificate for the HTTPS connection. Firewall Threat Defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).

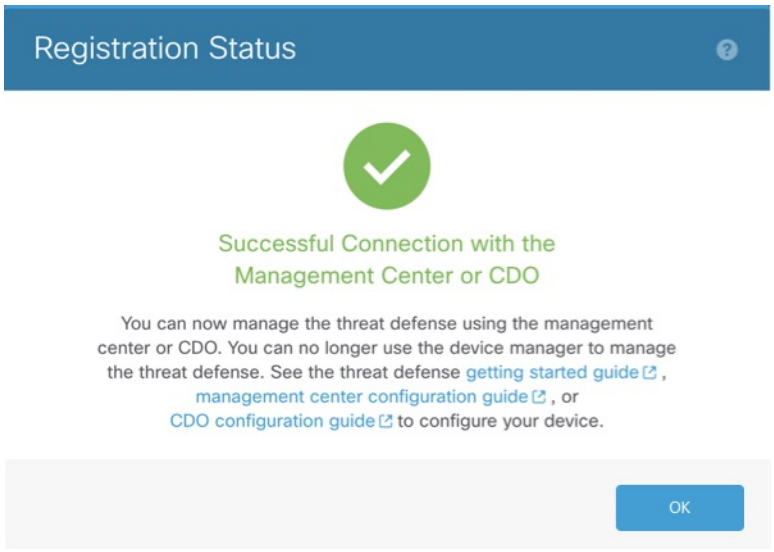
DDNS is not supported when using the Management interface for manager access.

ステップ 10 Click **Connect**. The **Registration Status** dialog box shows the current status of the switch to the Firewall Management Center. After the **Saving Management Center/SCC Registration Settings** step, go to the Firewall Management Center, and add the firewall.

If you want to cancel the switch to the Firewall Management Center, click **Cancel Registration**. Otherwise, do not close the Firewall Device Manager browser window until after the **Saving Management Center/SCC Registration Settings** step. If you do, the process will be paused, and will only resume when you reconnect to the Firewall Device Manager.

If you remain connected to the Firewall Device Manager after the **Saving Management Center/SCC Registration Settings** step, you will eventually see the **Successful Connection with Management Center/SCC** dialog box, after which you will be disconnected from the Firewall Device Manager.

図 *8 : Successful Connection*



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。

手順

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。

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。例外は、コンソール接続が Firewall Threat Defense CLIに接続する ISA 3000 向けです。

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。

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。

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

Firepower および Secure Firewall ハードウェアの場合は、『Firewall Threat Defense 向け Cisco FXOS トラブルシューティングガイド』[英語] の「再イメージ化手順」を参照してください。

ISA 3000 の場合は、『Cisco Secure Firewall ASA および Threat Defense 再イメージ化ガイド』[英語] 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 3 コンソールポートで FXOS に接続している場合は、Firewall Threat Defense CLI に接続します。

connect ftd

例：

```
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（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。

（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。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。

（注）
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。

例：

```
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*]

（注）
管理に Security Cloud Control を使用している場合は、このステップで Security Cloud Control 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。オプション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、Security Cloud Control 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 MC.example.com 123456
Manager successfully configured.
```

例：

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.
```

例：

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 Security Cloud Control 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*]

例：

次の例では、Security Cloud Control で生成した表示名で Security Cloud Control 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 （任意） 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。

（注）

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 （5 ページ）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。

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 8 （任意） 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。

次のタスク

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 や Secure Firewall 4200 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 Administration Guide*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 （31 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

>
```

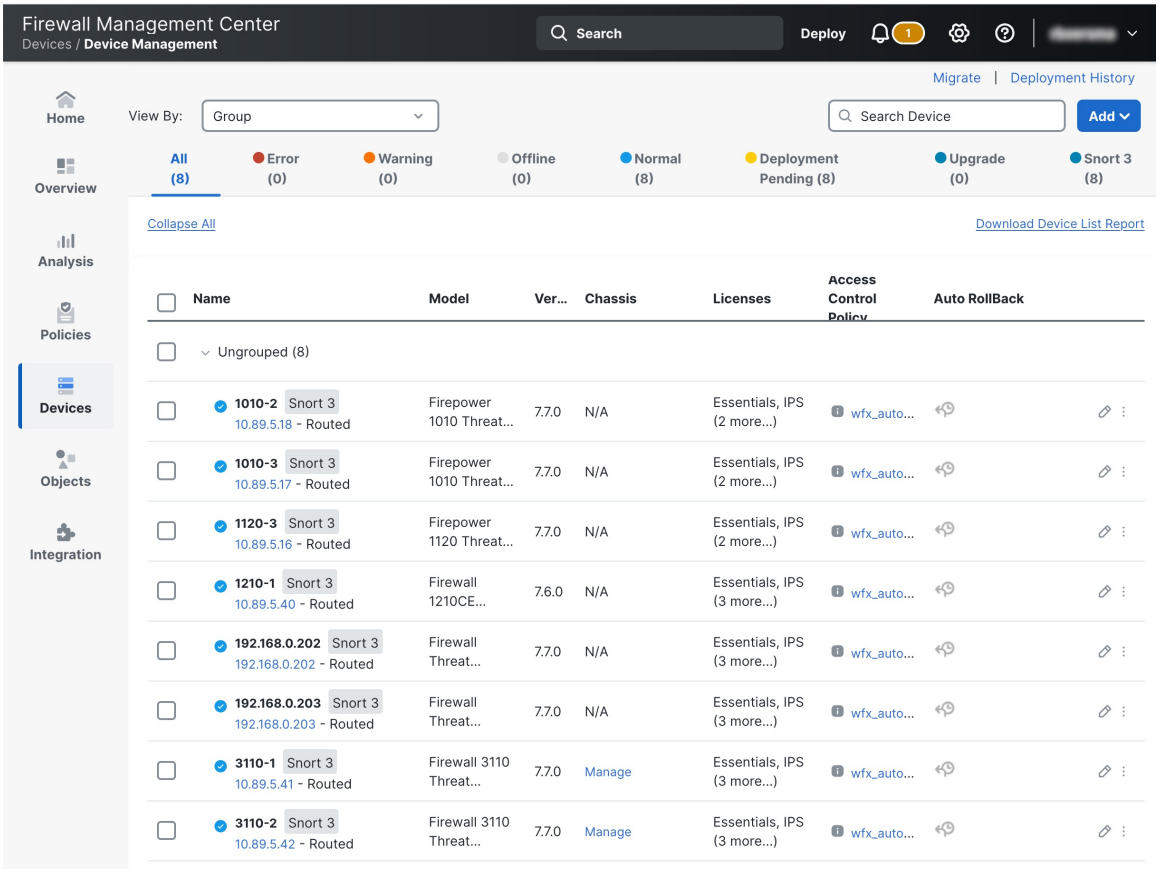
スタティック ルートを表示するには、**show network-static-routes** を入力します（デフォルトルートは表示されません）。

```
> 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

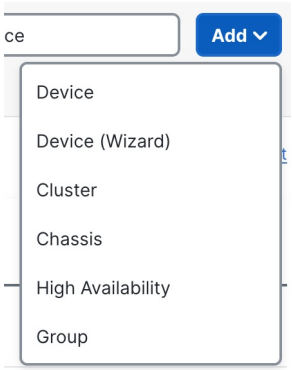
[デバイス（Device）]>**[デバイス管理（Device Management）]**ページには、さまざまな情報とオプションがあります。

図 *9* : *[*デバイス管理（*Device Management*）*]* ページ



- **[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。

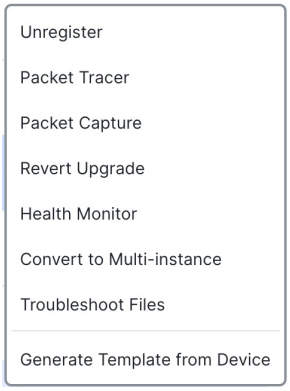
図 *10*：メニューの追加



- 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、**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、**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。

図 *11 : [More]* メニュー



- [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。
- **[マルチインスタンスへの変換（Convert to Multi-instance）]**：サポートされているモデルの場合は、シャーシをマルチインスタンス モードに変換します。
- **[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。
- **[デバイスからテンプレートを生成する（Generate Template from Device）]**：登録済みのデバイスから新しいデバイステンプレートを生成します。新しいテンプレートの設定は、生成元のデバイスと同じです。スタンドアロンデバイスとHAデバイスから新しいデバイス テンプレートを生成できます。ただし、HA デバイスからテンプレートを生成した場合、新しいテンプレートにはフェールオーバー設定が含まれません。

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 **Devices** > **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**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 **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。

登録キーによる方法

Firewall Management Center とデバイスの初期構成の両方で指定した登録キーを使用してデバイスを追加します。

登録キーを使用したデバイスの追加：基本設定

登録キーと基本設定を使用して Firewall Management Center にデバイスを追加するには、次の手順を実行します。デバイステンプレートを使用するには、登録キーを使用したデバイスの追加：デバイステンプレート （47 ページ）を参照してください。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、Cloud-Delivered 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：
  - 手動登録での Firewall Threat Defense 初期設定の完了 （15 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。

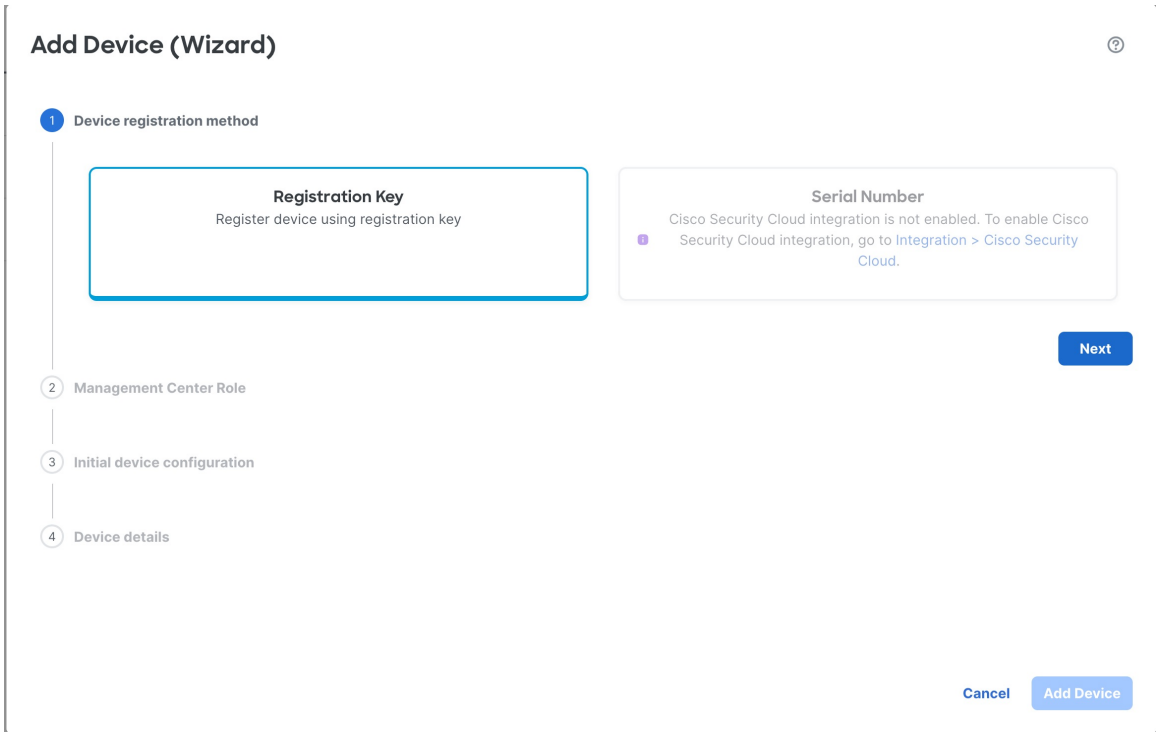
手順

ステップ 1 **Devices** > **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）] [デバイス（ウィザード）（Device (Wizard)）] を選択します。

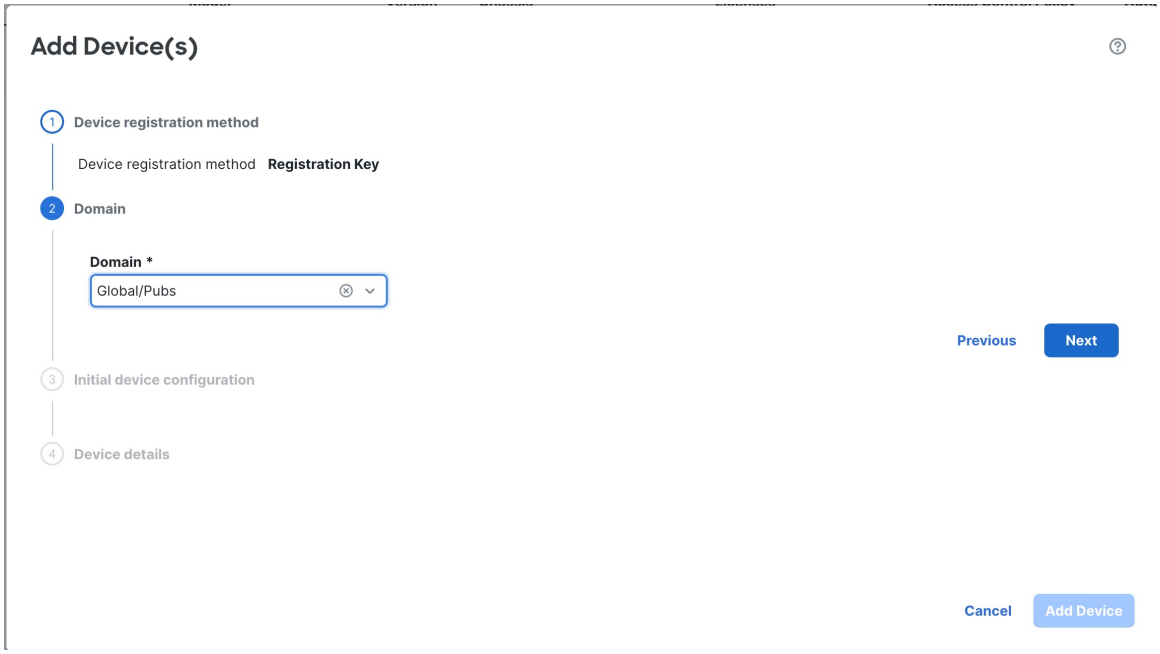
ステップ 3 [登録キー（Registration Key）] をクリックし、[次へ（Next）] をクリックします。

図 *12* : デバイスの登録方法



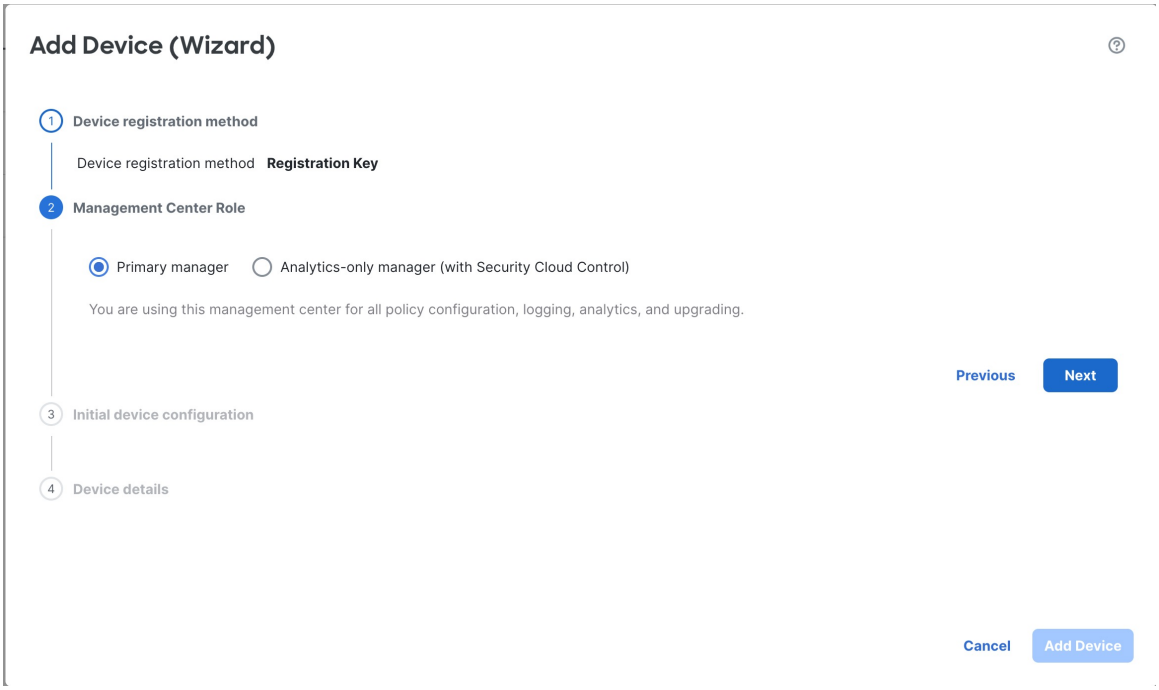
ステップ 4 マルチドメイン環境では、ドロップダウンリストから [ドメイン（Domain）] を選択し、[次へ（Next）] をクリックします。

図 *13* : ドメイン



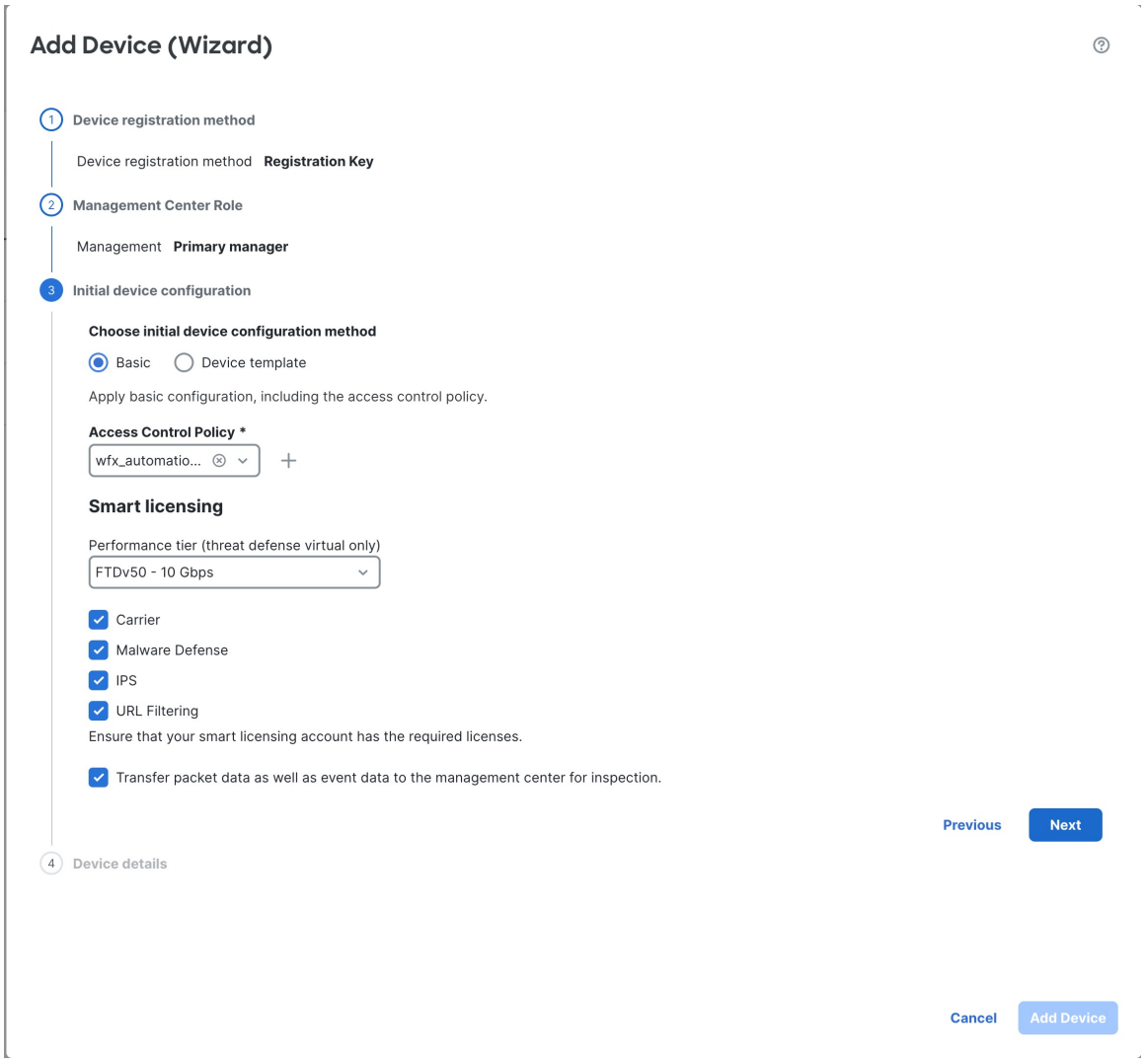
ステップ 5 通常の管理の場合は[プライマリマネージャ（Primary manager）]をクリックし、Cloud-Delivered Firewall Management Center で管理されているデバイスの場合は[分析専用マネージャ（Analytics-only manager）]をクリックします。分析専用モードはマルチドメイン環境をサポートしていないため、この手順は表示されません。

図 *14 : Management Center* のロール



ステップ 6 [デバイスの初期設定（Initial Device Configuration）]で、[基本（Basic）]をクリックします。

図 *15 :* デバイスの初期設定



分析専用モードの場合、これらの設定はSecurity Cloud Controlによって管理されるため、[デバイスの初期設定（Initial Device Configuration）] は表示されません。

a) 登録時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。

b) デバイスに適用する [スマートライセンス（Smart Licensing）] ライセンスを選択します。

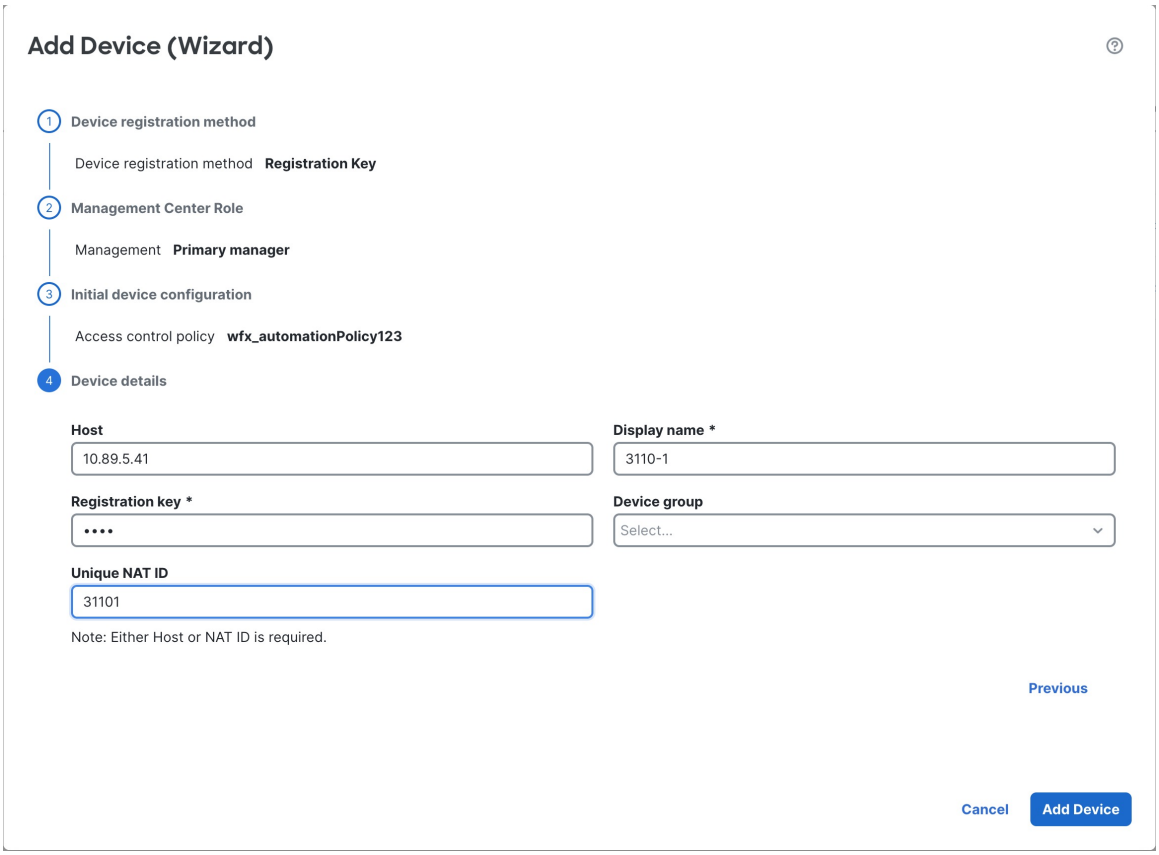
[システム（System）]>[ライセンス（Licenses）]>[スマートライセンス（Smart Licenses）] ページから、デバイスを追加した後にライセンスを適用することもできます（Secure Client リモートアクセス VPN ライセンスを含む）。

Firewall Threat Defense Virtual のみの場合は、[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が設定されます。

c) [次へ（Next）] をクリックします。

ステップ 7 [デバイスの詳細（Device details）] を指定します。

図 *16 :* デバイスの詳細（*Device Details*）



a) [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。

b) [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。

c) [登録キー（Registration key）] には、初期設定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。

d) （任意） デバイスを [デバイスグループ（Device group）] に追加します。

e) [一意のNAT ID（Unique NAT ID）] には、初期設定と同じ 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。

f) [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。

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8 [Add Device] 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。

登録キーを使用したデバイスの追加（従来の画面）：基本設定

登録キーを使用して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、Cloud-Delivered 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。

デバイスを追加するために、この従来の画面を使用することも、[デバイス（ウィザード）（Device (Wizard)）] を使用することもできます。[デバイス（ウィザード）（Device (Wizard)）] には、シリアル番号によるデバイスの追加（zero-touch provisioning）や、テンプレートを使用した 1 つ以上のデバイスの追加などの追加オプションがあります。「シリアル番号を使用したデバイスの追加（ゼロタッチプロビジョニング）：基本設定」を参照してください。

テンプレートを使用してデバイスを追加する方法については、登録キーを使用したデバイスの追加：デバイステンプレート （47 ページ）を参照してください。

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

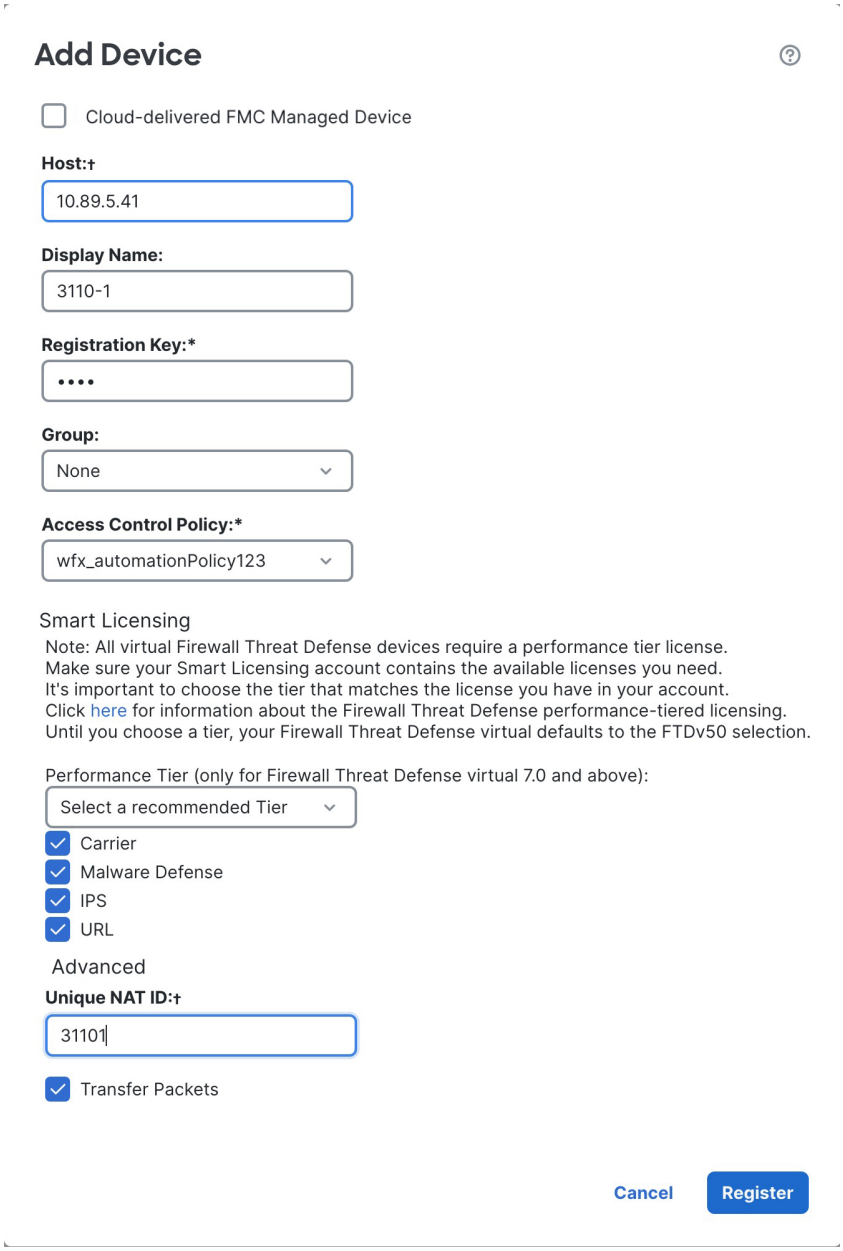
- デバイスを Firewall Management Center の管理対象として設定します。参照：
  - 手動登録での Firewall Threat Defense 初期設定の完了 （15 ページ）
  - 使用モデルのスタートアップガイド
- Firewall Management Center が Smart Software Manager に登録されている必要があります。有効な評価ライセンスで十分ですが、有効期限が切れると、正常に登録するまで新しいデバイスを追加できなくなります。
- IPv4 を使用して登録したデバイスを IPv6 に変換する場合は、デバイスをいったん登録解除してから再登録する必要があります。

手順

ステップ 1 **Devices** > **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。

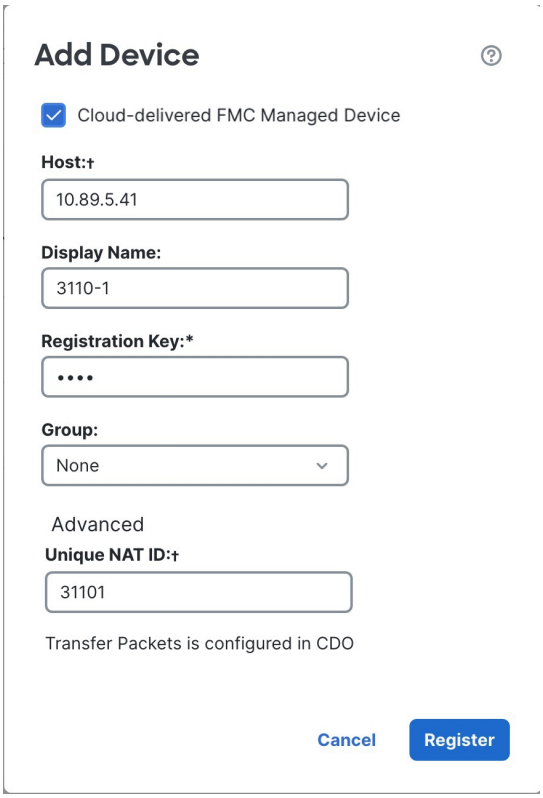
図 *17*：登録キーを使用したデバイスの追加



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、**[クラウド提供型FMCの管理対象デバイス（Cloud-delivered FMC 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 Security Cloud Control（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 *18 : Security Cloud Control* 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ら、[**System** (⚙) > **Licenses** > **Smart Licenses**] ページでライセンスを適用できます。

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 Administration Guide*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。

登録キーを使用したデバイスの追加：デバイステンプレート

テンプレートを使用してデバイスを追加してから、そのデバイスを Firewall Management Center に登録し、特定のテンプレート設定を使用してそのデバイスを起動できます。

始める前に

デバイス テンプレートを使用したデバイスの登録に従ってデバイステンプレートを作成します。必要な変数とネットワークオブジェクトのオーバーライドを各デバイスに指定し、ターゲットのデバイスモデルに対するモデルマッピングが実行されていることを確認する必要があります。

デバイスにテンプレートを適用する前に、テンプレート内のすべての設定が正しく入力されていることを確認するためのチェックリストを作成することをお勧めします。

チェックリストの例を以下に示します。

- バージョン、モデル、動作モードを確認します。
- 変数とオーバーライドのリストを確認します。
- 変数とオーバーライドの値が正しいことを確認します。
- 必要なモデルマッピングが存在するかどうかを確認します。
- デバイステンプレート操作が並行して進行中であるかどうかを確認します。

（注） データインターフェイスによって管理されるデバイスを追加する場合は、デバイスの接続パラメータと互換性があるテンプレートを設定してください。詳細については、「データインターフェイスにより管理される Threat Defense デバイスのテンプレートの設定」を参照してください。

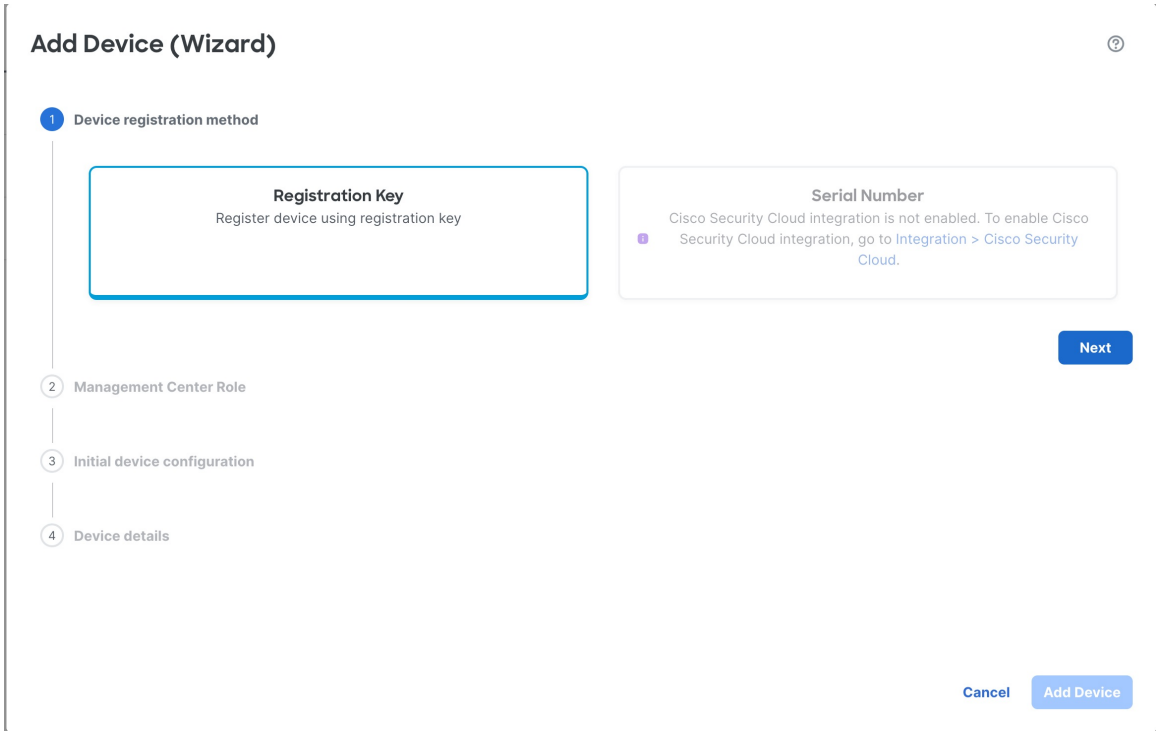
手順

ステップ 1 **Devices** > **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（ウィザード）（Device (Wizard)）]** を選択します。

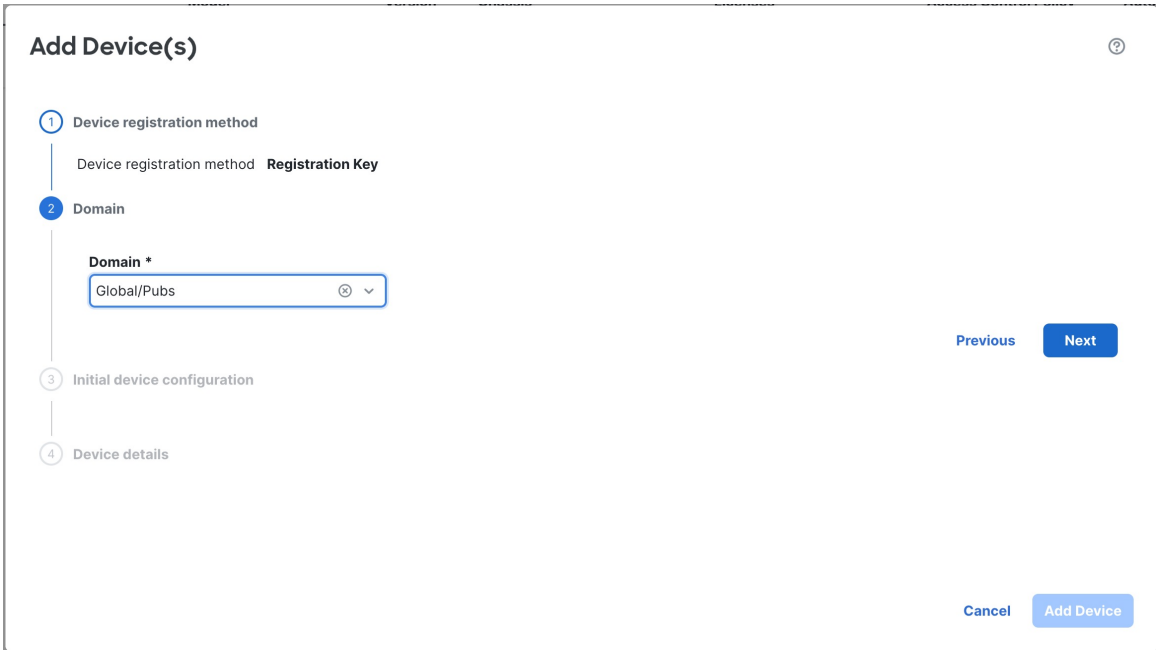
ステップ 3 [登録キー（Registration Key）] をクリックし、[次へ（Next）] をクリックします。

図 *19*：デバイスの登録方法



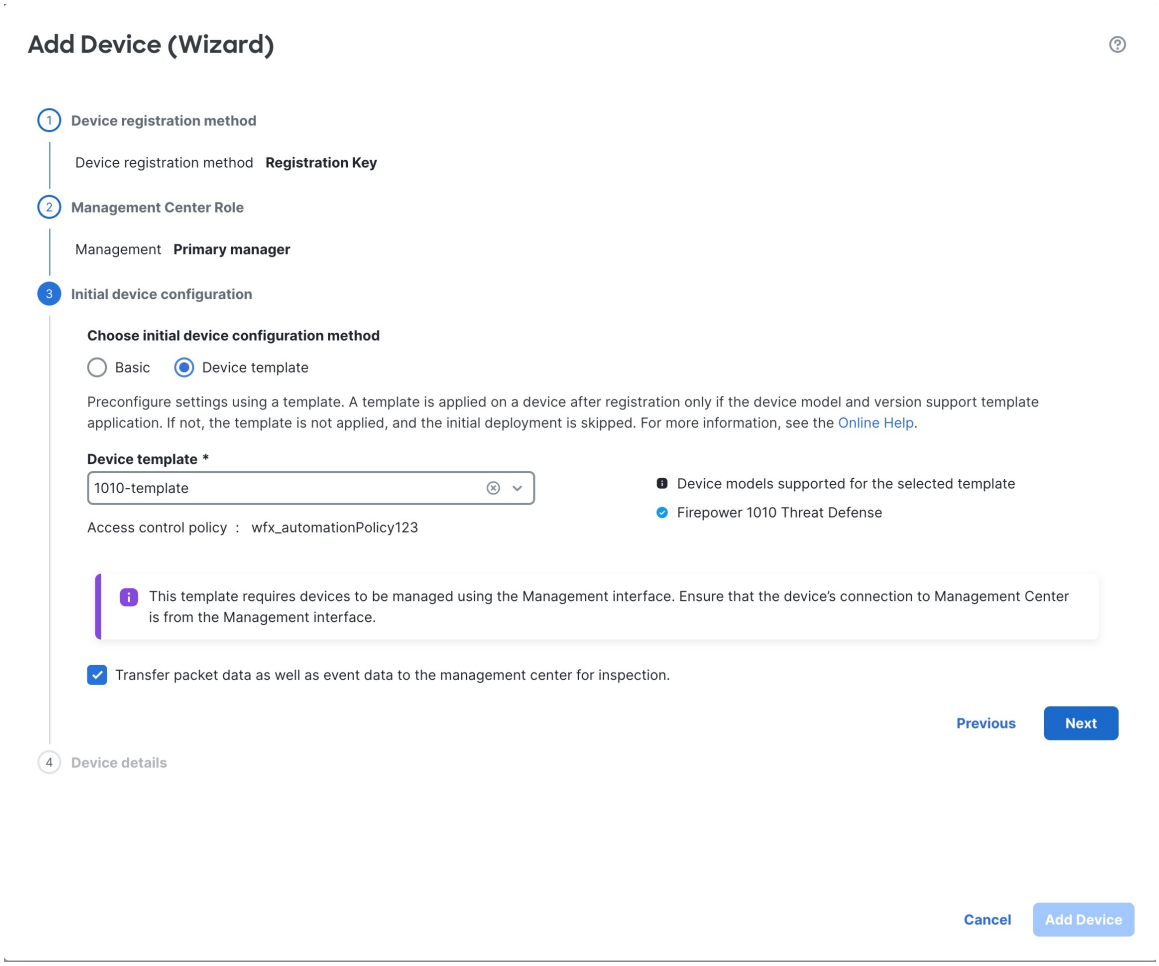
ステップ 4 マルチドメイン環境では、ドロップダウンリストから [ドメイン（Domain）] を選択し、[次へ（Next）] をクリックします。

図 *20*：ドメイン



ステップ 5 [デバイスの初期設定（Initial device configuration）] で、次の設定を行います。

図 *21* : デバイスの初期設定



a) [デバイステンプレート（Device template）] をクリックします。

b) [デバイステンプレート（Device template）] ドロップダウンリストから任意のテンプレートを選択します。

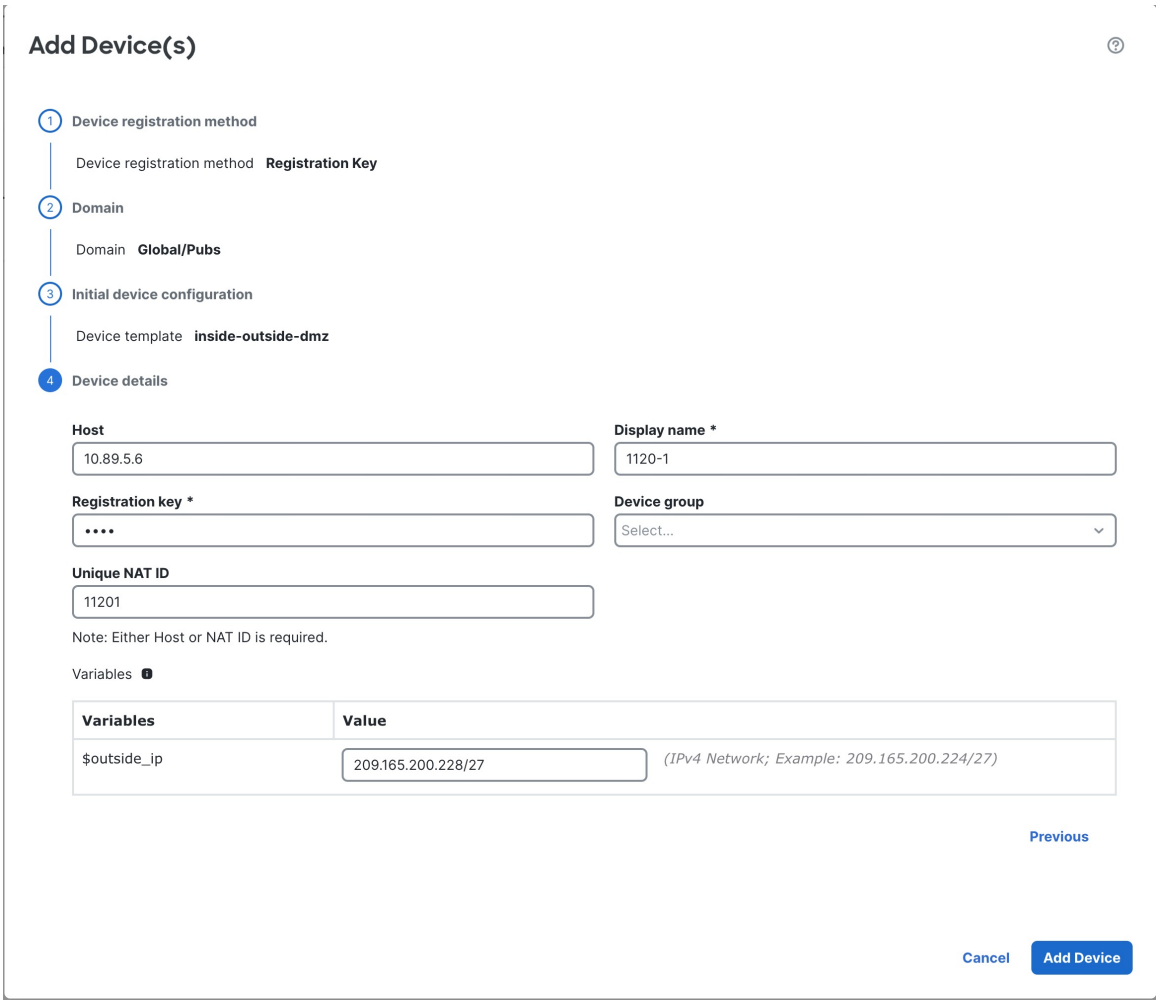
c) （任意）[パケットデータの転送（Transfer packet data）] をクリックすると、侵入イベントが発生するたびに、デバイスが検査のためにパケットを Firewall Management Center に転送します。

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。

d) [次へ（Next）] をクリックします。

ステップ 6 [デバイスの詳細（Device details）] を指定します。

図 *22* : デバイスの詳細（***Device Details***）



a) [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。

b) [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。

c) [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。

d) （任意） デバイスを [デバイスグループ（Device group）] に追加します。

e) 初期設定時に NAT ID を指定した場合は、[一意のNAT ID（Unique NAT ID）] フィールドに同じ 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。

f) [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。

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。

g) [変数（Variables）] および [ネットワークオブジェクトのオーバーライド（Network object overrides）] に値を入力します。

ステップ 7 [デバイスの追加（Add Device）] をクリックすると、デバイスの登録が開始されます。テンプレート設定は、デバイスが Firewall Management Center に正常に登録された後に適用されます。

シリアル番号による方法（ゼロタッチ プロビジョニング）

Zero-Touch Provisioning 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 Firewall Management Center に登録できます。

シリアル番号を使用したデバイスの追加（ゼロタッチプロビジョニング）：基本設定

Zero-Touch Provisioning 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 Firewall Management Center に登録できます。Firewall Management Center は、この機能のために Cisco Security Cloud および Security Cloud Control と統合されます。

次の手順を使用して、基本設定を使用して Firewall Management Center に 1 つのデバイスを追加します。テンプレートを使用して 1 つ以上のデバイスを追加するには、シリアル番号（ゼロタッチプロビジョニング）を使用したデバイスの追加：デバイステンプレートを参照してください

デフォルト設定

zero-touch provisioning 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 および Secure Firewall 1210/1220 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

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 Zero-Touch Provisioning はサポートされません。

zero-touch provisioning 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。

Zero-Touch Provisioning は、7.2 および 7.4 以降を使用する次のモデルでのみサポートされます。7.2.4 より前のバージョンの場合、Firewall Management Center はパブリックに到達可能である必要があります。

- Firepower 1010
- Firepower 1100
- Cisco Secure Firewall 1200
- Firepower 2100（サポートされているバージョンに搭載）
- Cisco Secure Firewall 3100

始める前に

- デバイスが未設定または新規インストールであることを確認します。Zero-Touch Provisioning は新しいデバイスのみを対象としています。事前設定では、デバイスの設定に応じて zero-touch provisioning を無効にすることができます。
- 外部インターフェイスまたは管理インターフェイスをケーブル接続して、インターネットに接続できるようにします。zero-touch provisioning に外部インターフェイスを使用する場合は、管理インターフェイスにケーブル接続しないでください。管理インターフェイスが DHCP から IP アドレスを取得すると、外部インターフェイスのルーティングが正しく行われなくなります。
- 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、Firewall Management Center のパブリック IP アドレス/FQDN を設定し（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。**[システム（System）]** > **[設定（Configuration）]** > **[マネージャのリモートアクセス（Manager Remote Access）]** を参照してください。
- 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登録解除してから再登録する必要があります。

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場合は、Firewall Management Center と Cisco Security Cloud を統合します。

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

a) **Integration** > **Cisco Security Cloud**を選択します。
b) [Cisco Security Cloudの有効化（Enable Cisco Security Cloud）] 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。Cisco Security Cloud および Security Cloud Control アカウントをまだお持ちでない場合は、この手順の途中で追加できます。

この統合の詳細については、「」『*Cisco Secure Firewall Management Center Administration Guide*』の「System Configuration」の章を参照してください。

Firewall Management Center と Cisco Security Cloud を統合した後、Security Cloud Control はオンプレミスの Firewall Management Center をオンボーディングします。Security Cloud Control は、zero-touch provisioning を動作させるためにインベントリに Firewall Management Center を必要とします。ただし、Security Cloud Control を直接使用する必要はありません。Security Cloud Control を使用する場合、その Firewall Management Center のサポートは、デバイスの導入準備、管理対象デバイスの表示、Firewall Management Center に関連付けられたオブジェクトの表示、および Firewall Management Center の相互起動に限定されています。

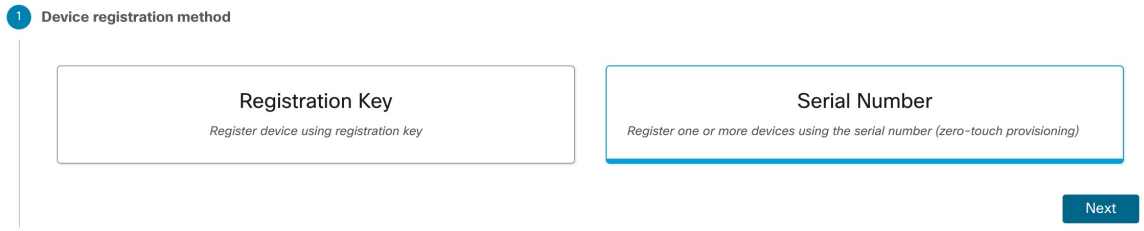
c) [ゼロタッチプロビジョニングの有効化（Enable Zero-Touch Provisioning）] がオンになっていることを確認します。
d) [保存（Save）] をクリックします。

ステップ 2 **Devices** > **Device Management**を選択します。

ステップ 3 **[追加（Add）]** ドロップダウンメニューから、**[デバイス（ウィザード）（Device (Wizard)）]** を選択します。

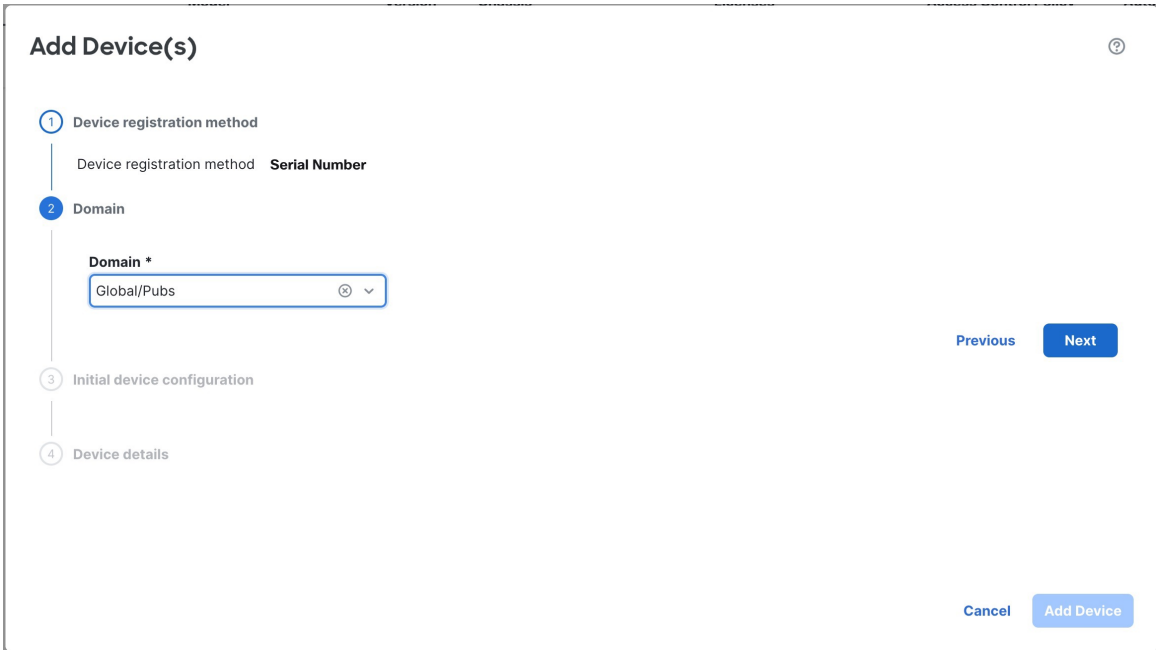
ステップ 4 [シリアル番号を使用（Use Serial Number）] をクリックし、[次へ（Next）] をクリックします。

図 *23* : デバイスの登録方法



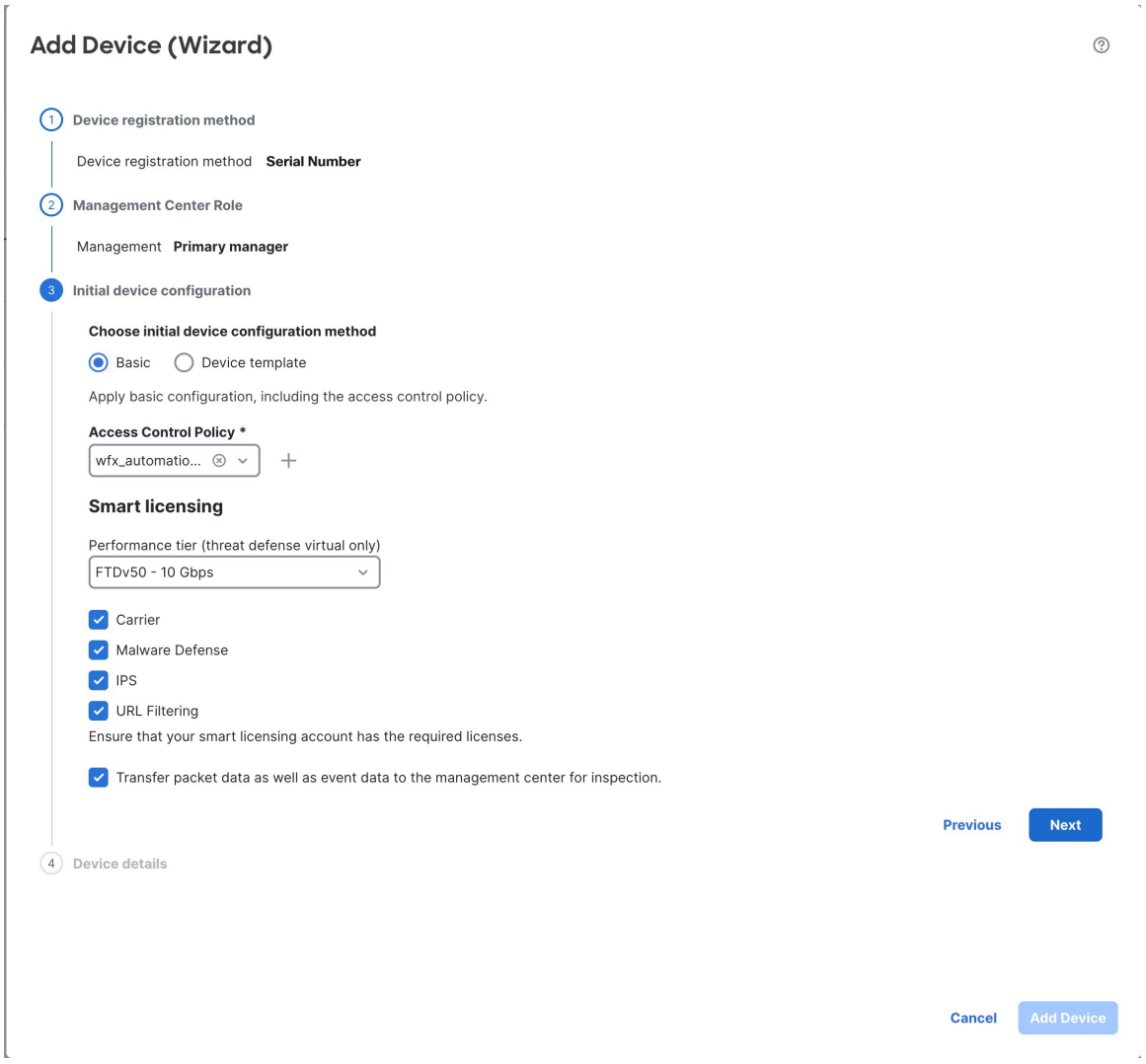
ステップ 5 マルチドメイン環境では、ドロップダウンリストから [ドメイン（Domain）] を選択し、[次へ（Next）] をクリックします。

図 *24* : ドメイン



ステップ 6 [デバイスの初期設定（Initial device configuration）] で、[基本（Basic）] オプションボタンをクリックします。

図 *25 :* デバイスの初期設定方法



a) 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。

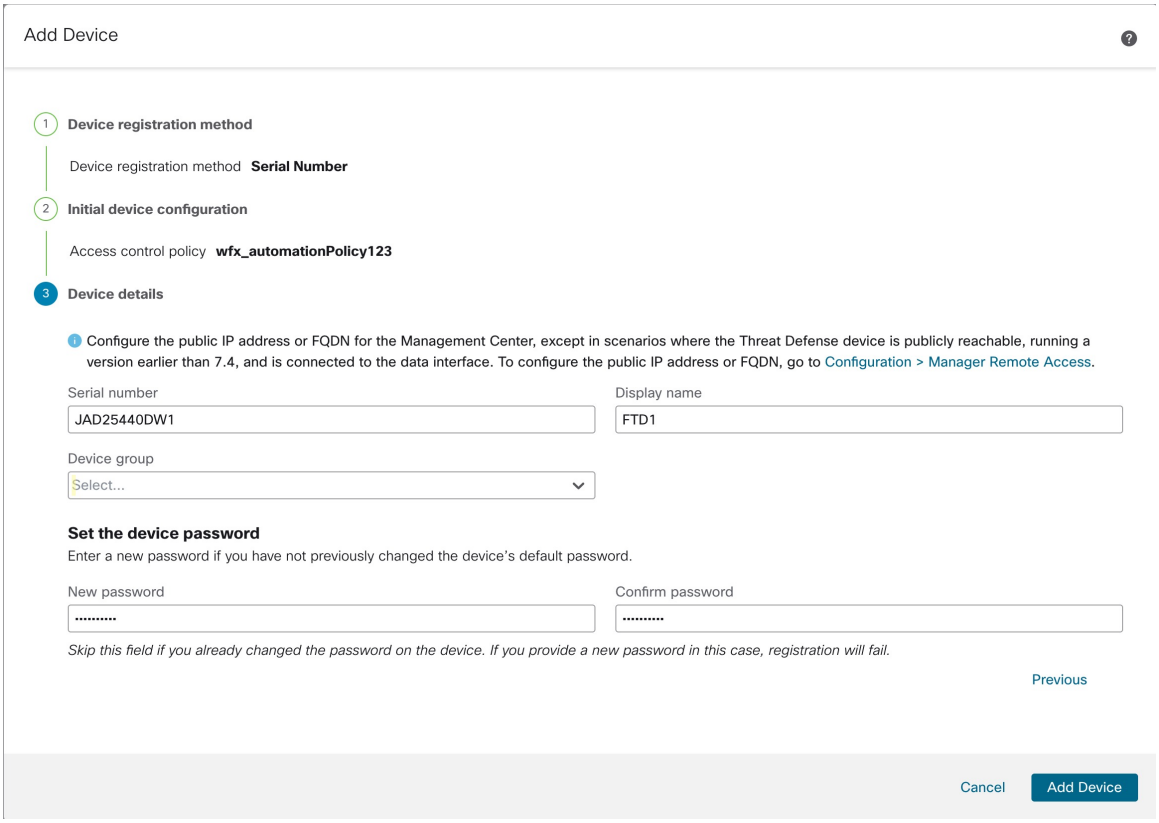
b) デバイスに適用する[スマートライセンス（Smart licensing）]ライセンスを選択します。

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。

c) [次へ（Next）]をクリックします。

ステップ 7 [デバイスの詳細（Device details）]を設定します。

図 *26* : デバイスの詳細



a) [シリアル番号（Serial number）] にシリアル番号を入力します。
b) [表示名（Display name）] に、Firewall Management Center に表示する名前を入力します。
c) （任意） [デバイスグループ（Device Group）] を選択します。
d) **デバイスパスワードを設定します。**

このデバイスが未設定の場合、または新規インストールの場合は、新しいパスワードを設定する必要があります。すでにログインしてパスワードを変更している場合は、このフィールドを空白のままにします。そうしなければ、登録が失敗します。

ステップ 8 [Add Device] 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。

外部インターフェイスで zero-touch provisioning を使用する場合、Security Cloud Control は DDNS プロバイダーとして機能し、以下を実行します。

- [FMCのみ（FMC Only）] 方式を使用して外部で DDNS を有効にします。この方式は、zero-touch provisioning 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 Firewall 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 Firewall Management Center に通知します。

管理インターフェイスで zero-touch provisioning 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、Firewall Management Center はパブリックに到達可能である必要があります。

Security Cloud Control を引き続き DDNS プロバイダーとして使用することも、後で Firewall Management Center の DDNS 設定を別の方式に変更することもできます。詳細については、ダイナミック DNS の設定を参照してください。

デバイスの登録に失敗した場合は、「シリアル番号（ゼロタッチプロビジョニング）登録の問題の解決 （69 ページ）」を参照してください。

シリアル番号（ゼロタッチプロビジョニング）を使用したデバイスの追加：デバイステンプレート

Zero-Touch Provisioning 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 Firewall Management Center に登録できます。Firewall Management Center は、この機能のために Cisco Security Cloud および Security Cloud Control と統合されます。

テンプレートを使用してデバイスを追加してから、そのデバイスを Firewall Management Center に登録し、特定のテンプレート設定を使用してそのデバイスを起動できます。

次の手順を使用して、シリアル番号とデバイステンプレートを使用して Firewall Management Center にデバイスを追加します。テンプレートを使用せずにデバイスを追加する方法については、シリアル番号を使用したデバイスの追加（ゼロタッチプロビジョニング）：基本設定を参照してください。

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 Zero-Touch Provisioning はサポートされません。

zero-touch provisioning 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。

テンプレートを使用したZero-Touch Provisioning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
- Cisco Secure Firewall 1200
- Firepower 2100（サポートされているバージョンに搭載）
- Cisco Secure Firewall 3100

始める前に

- デバイスが未設定または新規インストールであることを確認します。Zero-Touch Provisioning は新しいデバイスのみを対象としています。事前設定では、デバイスの設定に応じて zero-touch provisioning を無効にすることができます。
- 外部インターフェイスまたは管理インターフェイスをケーブル接続して、インターネットに接続できるようにします。zero-touch provisioning に外部インターフェイスを使用する場合は、管理インターフェイスにケーブル接続しないでください。管理インターフェイスが DHCP から IP アドレスを取得すると、外部インターフェイスのルーティングが正しく行われなくなります。
- 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、Firewall Management Center のパブリック IP アドレス/FQDN を設定し（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。**[システム（System）] > [設定（Configuration）] > [マネージャのリモートアクセス（Manager Remote Access）]** を参照してください。
- 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登録解除してから再登録する必要があります。
- デバイステンプレートを使用したデバイスの登録に従ってデバイステンプレートを作成します。必要な変数とネットワークオブジェクトのオーバーライドを各デバイスに指定し、ターゲットのデバイスモデルに対するモデルマッピングが実行されていることを確認する必要があります。

  デバイスにテンプレートを適用する前に、テンプレート内のすべての設定が正しく入力されていることを確認するためのチェックリストを作成することをお勧めします。

  チェックリストの例を以下に示します。

  - バージョン、モデル、動作モードを確認します。
  - 変数とオーバーライドのリストを確認します。
  - 変数とオーバーライドの値が正しいことを確認します。
  - 必要なモデルマッピングが存在するかどうかを確認します。
  - デバイステンプレート操作が並行して進行中であるかどうかを確認します。

（注） データインターフェイスによって管理されるデバイスを追加する場合は、デバイスの接続パラメータと互換性があるテンプレートを設定してください。詳細については、「データインターフェイスにより管理される Threat Defense デバイスのテンプレートの設定」を参照してください。

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場合は、Firewall Management Center と Cisco Security Cloud を統合します。

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

a) **Integration** > **Cisco Security Cloud**を選択します。
b) [Cisco Security Cloudの有効化（Enable Cisco Security Cloud）] 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。Cisco Security Cloud および Security Cloud Control アカウントをまだお持ちでない場合は、この手順の途中で追加できます。

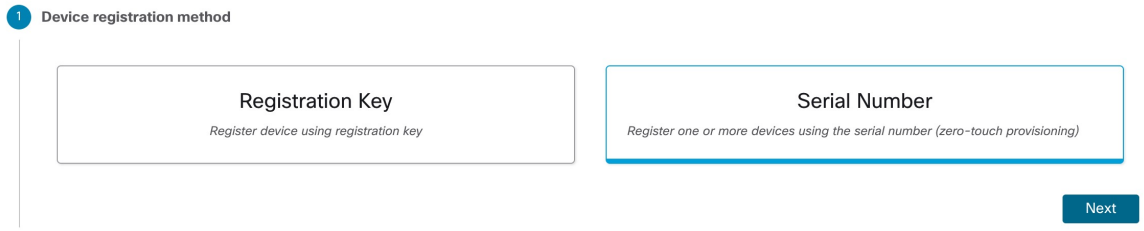
この統合の詳細については、「」『*Cisco Secure Firewall Management Center Administration Guide*』の「System Configuration」の章を参照してください。

Firewall Management Center と Cisco Security Cloud を統合した後、Security Cloud Control はオンプレミスの Firewall Management Center をオンボーディングします。Security Cloud Control は、zero-touch provisioning を動作させるためにインベントリに Firewall Management Center を必要とします。ただし、Security Cloud Control を直接使用する必要はありません。Security Cloud Control を使用する場合、その Firewall Management Center のサポートは、デバイスの導入準備、管理対象デバイスの表示、Firewall Management Center に関連付けられたオブジェクトの表示、および Firewall Management Center の相互起動に限定されています。

c) [ゼロタッチプロビジョニングの有効化（Enable Zero-Touch Provisioning）] がオンになっていることを確認します。
d) [保存（Save）] をクリックします。

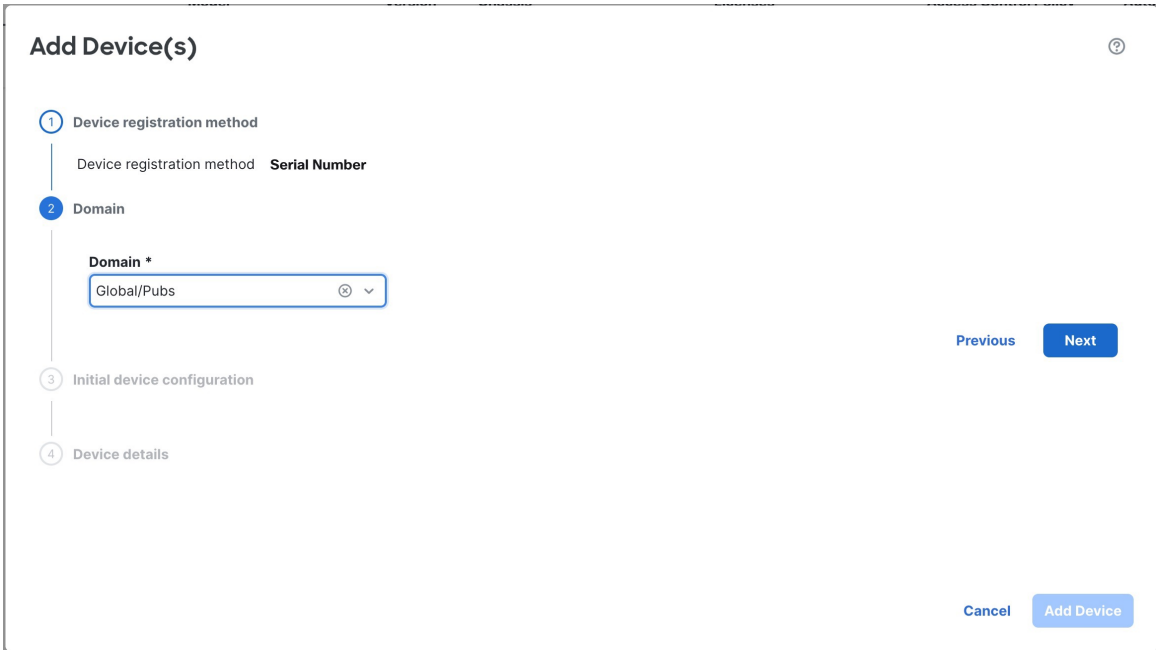
ステップ 2 **Devices** > **Device Management**を選択します。
ステップ 3 **[追加（Add）]** ドロップダウンメニューから、**[デバイス（ウィザード）（Device (Wizard)）]** を選択します。
ステップ 4 [シリアル番号を使用（Use Serial Number）] をクリックし、[次へ（Next）] をクリックします。

図 *27* : デバイスの登録方法



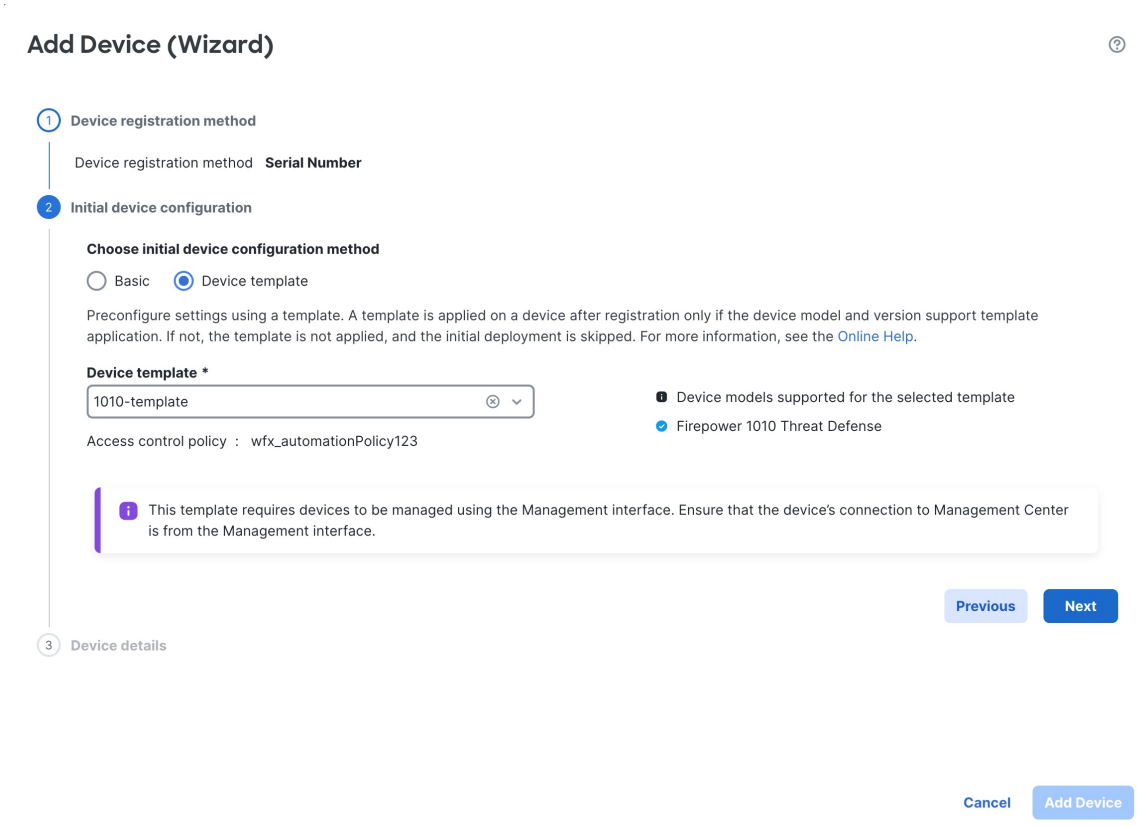
ステップ 5 マルチドメイン環境では、ドロップダウンリストから [ドメイン（Domain）] を選択し、[次へ（Next）] をクリックします。

図 *28* : ドメイン



ステップ 6 [デバイスの初期設定（Initial device configuration）] で、[デバイステンプレート（Device template）] オプションボタンをクリックします。

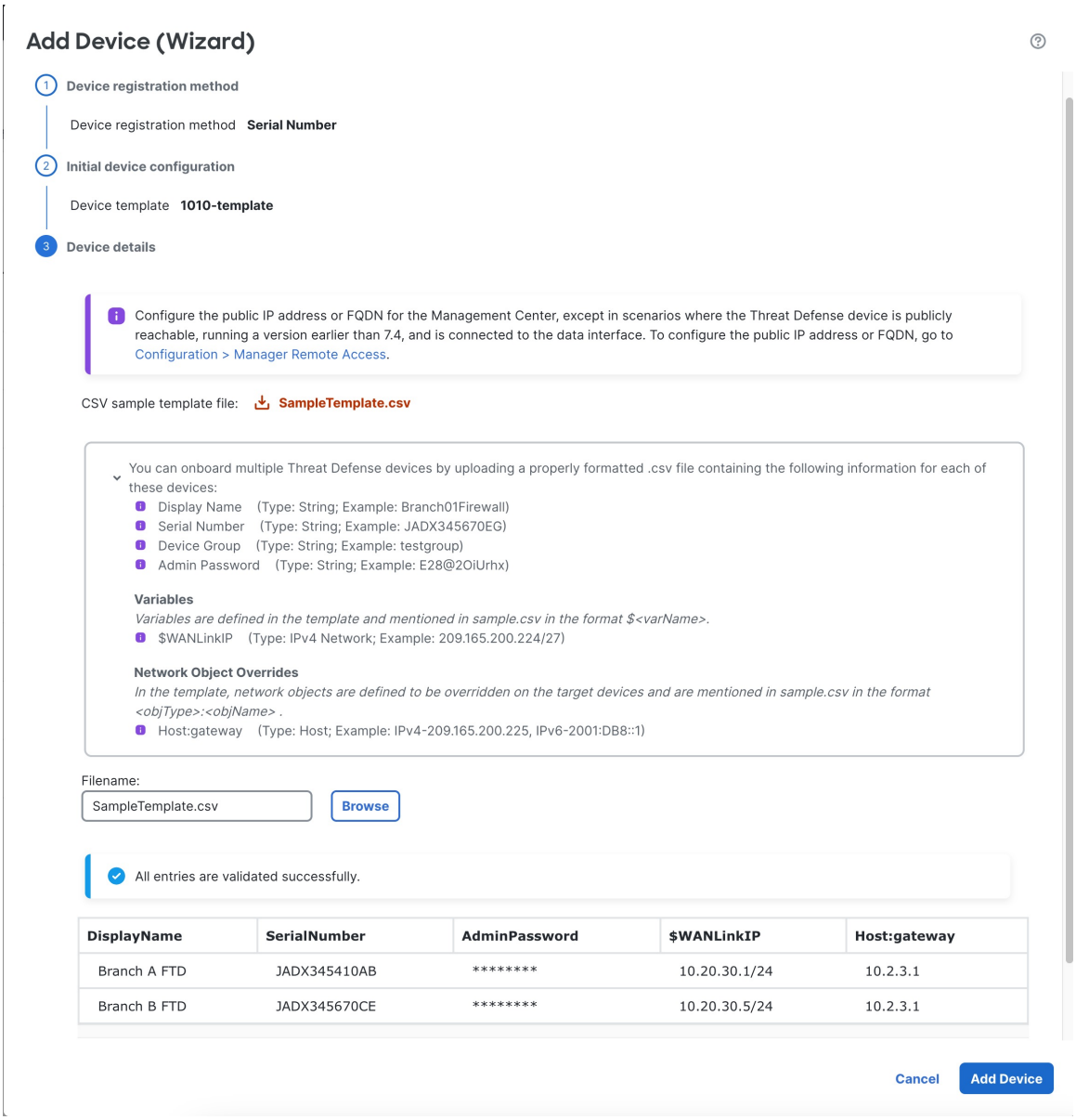
図 *29 :* デバイスの初期設定



ステップ 7 ドロップダウンリストから[デバイステンプレート（Device template）]を選択し、[次へ（Next）]をクリックします。

ステップ 8 [デバイスの詳細（Device details）]で、テンプレートに必要なデバイスの詳細情報を含む CSV ファイルをアップロードします。

図 *30* : デバイスの詳細



a) **SampleTemplate.csv** をダウンロードします。このファイルには、デバイスごとに定義する必要がある値に必要なすべてのヘッダーが含まれています。CSVテンプレートファイルのフィールドの詳細については、「CSV テンプレートファイル」を参照してください。

b) CSVテンプレートファイルを **ドラッグアンドドロップ**するか、[参照（Browse）]をクリックして、アップロードする CSV テンプレートファイルを選択します。アップロード後にファイルに対して有効性検査が実行されます。

CSVテンプレートファイルが正常にアップロードされると、CSVテンプレートファイルの内容が表形式で表示されます。

ステップ 9 [デバイスの追加（Add Device）] をクリックしてデバイスを登録します。

外部インターフェイスで zero-touch provisioning を使用する場合、Security Cloud Control 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、zero-touch provisioning 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 Firewall 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 Firewall Management Center に通知します。

管理インターフェイスで zero-touch provisioning 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、Firewall Management Center はパブリックに到達可能である必要があります。

Security Cloud Control を引き続き DDNS プロバイダーとして使用することも、後で Firewall Management Center の DDNS 設定を別の方式に変更することもできます。詳細については、ダイナミック DNS の設定を参照してください。

デバイスの登録に失敗した場合は、「シリアル番号（ゼロタッチプロビジョニング）登録の問題の解決 （69 ページ）」を参照してください。

デバイステンプレートにシリアル番号を登録するための *CSV* テンプレートファイル

CSV テンプレートファイルのサイズは 2 MB 未満である必要があります。ファイル名は、次の基準を満たす必要があります。

- 64 文字以内で指定できます。
- 英数字と、ダッシュ（-）、ピリオド（.）、アンダースコア（_）などの特殊文字のみを使用できます。
- スペースを含めることはできません。

2 つのデバイスの設定を含む次のサンプル CSV テンプレートファイルを参照してください。

```
DisplayName,SerialNumber,AdminPassword,$WANLinkIP,Host:gateway
Branch A FTD,JADX345410AB,C15c05n0rt#,10.20.30.1/24,10.2.3.1
Branch B FTD,JADX345670CE,Admin123!,10.20.30.5/24,10.2.3.1
```

適切にフォーマットされた CSV ファイルには、次のフィールドがあります。

Mandatory Fields

- **DisplayName**：デバイスの名前。タイプ：文字列例：test1

- **SerialNumber**：デバイスのシリアル番号。タイプ：文字列。例：JADX345670EG
- **AdminPassword**：管理者アクセス用のパスワード、タイプ：文字列、例：E28@2OiUrhx

オプションフィールド

- **DeviceGroup**：デバイスグループの名前、タイプ：文字列、例：testgroup

変数

$*varName* の形式を使用します。

変数のサンプル：**$LAN-Devices-IPv4Address**（LAN デバイスの IPv4 アドレス）。タイプ：文字列例：10.2.3.4/24。

ネットワークオブジェクトのオーバーライド

objType:*objName* の形式を使用します。

ネットワークオブジェクトのオーバーライドの例：**Network:LAN-Devices-Network**（LAN デバイスのネットワークの IP アドレス）。タイプ：文字列例：10.2.3.0/24

FQDN

シリアル番号の登録では、DDNS が自動的に有効になります。[FMCのみ（FMC Only）] タイプの DDNS のデフォルトとは異なる値を設定する場合は、テンプレートで設定を指定できます。この場合、ホスト名の CSV 値を指定するときには、必ず *serialnumber***.local** として指定してください。

シャーシの追加

Firepower 4100/9300 シャーシを Firewall Management Center に追加できます。管理センターとシャーシは、シャーシ MGMT インターフェイスを使用して個々の管理接続を共有します。Firewall Management Center は、シャーシレベルの正常性アラートを提供します。設定については、引き続き Secure Firewall Chassis Manager または FXOS CLI を使用する必要があります。

（注） Cisco Secure Firewall 3100/4200 の場合は、マルチインスタンスモードへの変換の一部としてシャーシが Firewall Management Center に追加されます。デバイスのマルチインスタンスモードへの変換を参照してください。ただし、CLI を使用してマルチインスタンスモードに変換（CLI のマルチインスタンスモードの有効化）した場合は、この手順のステップ 3 （66 ページ） に進み、シャーシを Management Center に追加します。

手順

ステップ 1 コンソール ポートまたは SSH を使用して、シャーシ FXOS CLI に接続します。

ステップ 2 Firewall Management Centerを設定します。

create device-manager *manager_name* [**hostname** {*hostname* | *ipv4_address* | *ipv6_address*}] [**nat-id** *nat_id*]

登録キーの入力を求められます。

このコマンドは、どのスコープからでも入力できます。このコマンドは、**commit-buffer** を使用せずにすぐに受け入れられます。

- **hostname** {*hostname* | *ipv4_address* | *ipv6_address*}：Firewall Management Center の FQDN または IP アドレスを指定します。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 またはシャーシ）に到達可能な IP アドレスが必要です。**hostname** を指定しない場合は、シャーシに到達可能な IP アドレスまたはホスト名が必要となり、nat-id を指定する必要があります。
- **nat-id** *nat_id*：一方の側で到達可能な IP アドレスまたはホスト名が指定されていない場合は、シャーシを登録するときに Firewall Management Center でも指定する任意の一意のワンタイム文字列を指定します。これは **hostname** を指定しない場合に必須となりますが、ホスト名または IP アドレスを指定する場合でも、常に NAT ID を設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（-）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。
- **Registration Key:** *reg_key*：シャーシを登録するときに Firewall Management Center でも指定する任意のワンタイム登録キーを要求するプロンプトが表示されます。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（-）などがあります。

例：

```
firepower# create device-manager boulder_fmc hostname 10.89.5.35 nat-id 93002
(Valid registration key characters: [a-z],[A-Z],[0-9],[-]. Length: [2-36])
Registration Key: Impala67
```

ステップ 3 Firewall Management Center で、シャーシ管理 IP アドレスまたはホスト名を使用してシャーシを追加します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）]**の順に選択してから、**[追加（Add）] > [シャーシ（Chassis）]**の順に選択します。

図 *31* : シャーシの追加

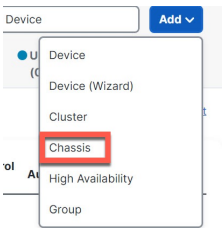
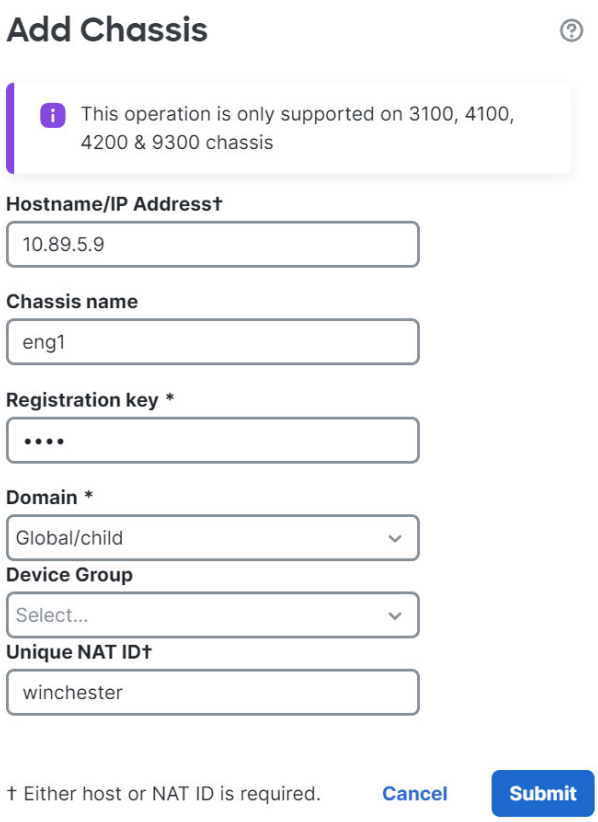


図 *32* : シャーシの追加



b) [ホスト名/IPアドレス（Hostname/IP Address）] フィールドに、追加するシャーシの IP アドレスまたはホスト名を入力します。

ホスト名またはIPアドレスがわからない場合は、このフィールドを空白のままにして、一意の NAT ID を指定できます。

c) [シャーシ名（Chassis Name）] フィールドに、Firewall Management Center でのシャーシの表示名を入力します。

d) [登録キー（Registration Key）] フィールドに、Firewall Management Center の管理対象としてシャーシを設定したときに使用した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。キーには、英数字とハイフン（-）を含めることができます。

e) マルチドメイン展開では、現在のドメインに関係なく、シャーシをリーフドメインに割り当てます。

現在のドメインがリーフドメインである場合、シャーシは自動的に現在のドメインに追加されます。現在のドメインがリーフドメインでない場合、登録後、シャーシを設定するために、リーフドメインに切り替える必要があります。シャーシは 1 つのドメインにのみ属することができます。

f) （任意） シャーシを**デバイスグループ**に追加します。

g) シャーシの設定時に NAT ID を使用した場合、[一意のNAT ID（Unique NAT ID）] フィールドに同じ NAT ID を入力します。

NAT ID には、英数字とハイフン（-）を含めることができます。

h) **[送信（Submit）]** をクリックします。

シャーシが**[デバイス（Device）]** > **[デバイス管理（Device Management）]**ページに追加されます。

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登録解除します。Firewall Management Center からのデバイスの登録解除 （71 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、Security Cloud Control 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。

シリアル番号（ゼロタッチプロビジョニング）登録の問題の解決

シリアル番号を使用したデバイスの登録に失敗した場合は、デバイスがクラウドに正常に接続されていない可能性があります。クラウド接続を確認するには、管理ステータス LED が緑色に点滅していることを確認します。緑色に点滅していない場合、この障害は次の理由で発生している可能性があります。

- CLI または Firewall Device Manager で初期設定を実行し、ロータッチプロビジョニングを無効にした
- シリアル番号がすでに別のマネージャによって要求されている

シリアル番号登録のその他の要件については、「シリアル番号を使用したデバイスの追加（ゼロタッチプロビジョニング）：基本設定」を参照してください。

登録の失敗を回避するには、次のいずれかのタスクを実行します。

デバイスのリセット

次のモデルでサポートされています。

- Firepower 1010
- Firepower 1100
- Cisco Secure Firewall 1200
- Cisco Secure Firewall 3100

CLI にアクセスできないときに、デバイスが未設定で zero-touch provisioning の準備ができていることを確認する場合は、小さな埋め込み型のリセットボタンを 5 秒以上押して、デバイスをデフォルトの状態にリセットします。詳細については、ハードウェア設置ガイドを参照してください。

手動登録と登録キーの使用

ロータッチプロビジョニングが失敗した場合、登録を完了する最も簡単な方法は、登録キー方式を使用することです。

1. 手動登録での Firewall Threat Defense 初期設定の完了 （15 ページ）またはFirewall Device Manager を使用した Firewall Threat Defense の初期設定の完了 （15 ページ）を参照してください。
2. 初期設定タスクが表示されない場合は、デバイスが別の Firewall Management Center に正常に登録されている可能性があります。まず、管理接続を削除してから、正しいマネージャに再登録する必要があります。
   1. 最初に、登録が完了しているかどうかを確認します。

```
> show managers
Type                       : Manager
Host                       : 10.10.1.4
Display name               : 10.10.1.4
Identifier                 : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration               : Completed
Management type            : Configuration
```

   2. [登録（Registration）] に [完了（Completed）] と表示されている場合は、マネージャを削除する必要があります。

      configure manager delete

   3. その後、CLI で **configure manager add** を使用してデバイスを登録できます。

CLI でのロータッチプロビジョニングの再起動

以前にロータッチプロビジョニングを使用してデバイスが登録されていた場合、再登録は失敗し、Security Cloud Control に「シリアル番号はすでに要求されています（Serial Number Already Claimed）」というエラーメッセージが表示されます。

シリアル番号の登録を解除し、設定と既存の管理接続をクリアして、プロセスを最初からやり直すことができます。

1. SSH またはコンソールポートを使用して、FXOS CLI に接続します。

   SSH を使用した場合は、Firewall Threat Defense CLI に接続します。この場合は、**connect fxos** と入力します。コンソールポートを使用した場合は、FXOS に直接接続します。

```
> connect fxos
firepower#
```

2. ローカル管理を開始します。

   connect local-mgmt

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

3. Cisco Cloud からデバイスを登録解除します。

   cloud deregister

   ```
   firepower(local-mgmt)# cloud deregister
   Release Image Detected RESULT=success MESSAGE=SUCCESS 10, X-Flow-Id:
   2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
   ```

4. 設定を消去してクラウド接続を復元します。

   erase configuration

   ```
   firepower(local-mgmt)# erase configuration
   All configurations will be erased and system will reboot. Are you sure? (yes/no):yes
   Removing all the configuration. Please wait....
   Configurations are cleaned up. Rebooting....
   ```

5. シリアル番号を使用したデバイスの追加（ゼロタッチプロビジョニング）：基本設定

Firewall Device Manager を使用したロータッチプロビジョニングの再起動

Firewall Device Manager にログインすると、誤ってロータッチプロビジョニングを無効にしてしまう可能性があります。このような場合には、Firewall Device Manager 内でロータッチプロビジョニングを再開できます。

（注） シリアル番号がすでに要求されている場合は、代わりにCLI でのロータッチプロビジョニングの再起動 （70 ページ）を参照してください。

1. Firewall Device Manager で、[デバイス（Device）] をクリックしてから、**[システム設定（System Settings）] > [クラウドサービス（Cloud Services）]** をクリックします。
2. [Security Cloud ControlまたはCisco Secure Firewall Management Centerの自動登録（Auto-enroll with Cisco Defense Orchestrator or Secure Firewall Management Center）] をオンにします。
3. [登録（Register）] をクリックします。
4. シリアル番号を使用したデバイスの追加（ゼロタッチプロビジョニング）：基本設定

Firewall Management Center からのデバイスの登録解除

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。

デバイスを登録解除する前に、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、またはテンプレートの作成を行ってください。保存された設定またはテンプレートがない場合は、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、テンプレートを使用するか、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、次のいずれかを実行します。

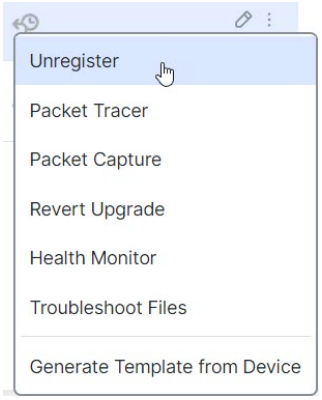
- デバイス設定をエクスポートします。デバイス設定のエクスポートとインポートを参照してください。
- デバイスのテンプレートを作成します。

手順

ステップ 1 **Devices** > **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 **More** (⋮) をクリックし、**[登録解除（Unregister）]** をクリックします。

図 *33* : 登録解除



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、「登録キーによる方法（36ページ）」を参照してください。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 （68 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 （68 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 （84 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 **Devices** > **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 **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) **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 **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。

管理対象デバイスのリストのダウンロード

すべての管理対象デバイスのレポートをダウンロードできます。

始める前に

次のタスクを実行するには、管理者ユーザーである必要があります。

手順

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

ステップ 2 [デバイスリストレポートのダウンロード（Download Device List Report）] リンクをクリックします。

ステップ 3 デバイスリストは CSV 形式または PDF 形式でダウンロードできます。[CSVのダウンロード（Download CSV）] または [PDFのダウンロード（Download PDF）] を選択してレポートをダウンロードします。

Firewall Threat Defense デバイスの移行

Cisco Firewall Threat Defense Firewall Threat Defense のモデル移行ウィザードを使用すると、古い Firewall Threat Defense モデルから新しいモデルに設定を移行できます。移行後、ソース Firewall Threat Defense デバイスからのすべてのルーティングおよびインターフェイス設定はターゲット Firewall Threat Defenseで使用できます。

このウィザードは、ソースデバイスとターゲットデバイスとして複数のモデルをサポートしています。詳細については、移行でサポートされるデバイス （75 ページ）を参照してください。

移行でサポートされるデバイス

移行用のライセンス

- スマート ライセンス アカウントには、ターゲットデバイスのソフトウェア利用資格が必要です。
- スマートライセンスアカウントにデバイスを登録する必要があります。移行すると、ソースデバイスのライセンスがターゲットデバイスにコピーされます。

移行の前提条件

- **一般的な前提条件**
  - ソース デバイスとターゲット デバイスを Firewall Management Center に登録する必要があります。
  - ターゲットデバイスが、何も設定されていない新しく登録されたデバイスであることを確認します。
  - ソース デバイスとターゲット デバイスは以下の状態とモードが同じである必要があります。
    - ドメイン
    - ファイアウォールモード：ルーテッドまたはトランスペアレント

- コンプライアンスモード（CC または UCAPL）

- デバイスに対する変更権限を持っていることを確認します。
- ソース デバイスの設定は有効で、エラーがない必要があります。
- 移行中は、いずれのデバイスでも展開、インポート、またはエクスポートタスクを実行しないでください。ソースデバイスには、保留中の展開を設定できます。

- **HA デバイスの前提条件**

ウィザードで移行される設定

移行ウィザードにより、次の設定がソースデバイスからターゲットデバイスにコピーされます。

- ライセンス
- インターフェイス設定
- インラインセット設定
- ルーティング設定
- DHCP および DDNS 構成
- ポリシー
- 関連するオブジェクトとオブジェクトのオーバーライド
- プラットフォーム設定
- リモートブランチ展開の構成

移行ウィザードにより、次のポリシー設定がソースデバイスからターゲットデバイスにコピーされます。

- 正常性ポリシー
- NAT ポリシー
- QoS ポリシー
- リモート アクセス VPN ポリシー
- FlexConfig ポリシー
- アクセス コントロール ポリシー
- プレフィルタ ポリシー
- IPS ポリシー
- DNS ポリシー

- SSL ポリシー
- マルウェアおよびファイルポリシー
- ID ポリシー

移行ウィザードにより、次のルーティング設定がソースデバイスからターゲットデバイスにコピーされます。

- ECMP
- BFD
- OSPFv2/v3
- EIGRP
- RIP
- BGP
- ポリシーベースルーティング
- スタティックルート
- マルチキャストルーティング
- 仮想ルータ

移行ウィザードにより、次のインターフェイスがソースデバイスからターゲットデバイスにコピーされます。

- 物理インターフェイス
- サブインターフェイス
- EtherChannel インターフェイス
- □ブリッジ グループ インターフェイス
- VTI インターフェイス
- VNI インターフェイス
- ループバック インターフェイス

移行ウィザードは、ターゲット デバイスのデバイス グループを保持します。

制限事項

- ウィザードは以下のものを移行しません：
  - サイト間 VPN ポリシー
- 一度に実行できる移行は 1 つだけです。

- リモート アクセス VPN トラストポイント証明書は移行後、登録されません。
- HA デバイスの場合：
  - ターゲットデバイス：スタンドアロンデバイスをHAデバイスに移行することはできません。

Cisco Secure Firewall Threat Defense の移行

始める前に

移行に関する前提条件と制限事項を確認してください。

手順

ステップ 1 **Devices** > **Device Management**を選択します。

ステップ 2 ページの右上にある [移行（Migrate）] をクリックします。

ステップ 3 [ようこそ（Welcome）] 画面で [開始（Start）] をクリックします。

ステップ 4 [ソースデバイス（Source Device）] ドロップダウンリストからデバイスを選択します。

デバイスが HA ペアの一部である場合、HA ペアのコンテナ名のみが表示されます。

ステップ 5 [Next] をクリックします。

ステップ 6 [ターゲットデバイス（Target Device）] ドロップダウンリストからデバイスを選択します。

デバイスが HA ペアの一部である場合、HA ペアのコンテナ名のみが表示されます。

ステップ 7 [Next] をクリックします。

ステップ 8 [インターフェイスの設定（Configure Interfaces）] ステップで、ソースデバイスの物理インターフェイスをターゲットデバイスの物理インターフェイスにマッピングします。

すべてのインターフェイスのマッピングは、必須ではありません。すべての名前付きインターフェイスと、他のインターフェイスの一部であるインターフェイスをマッピングする必要があります。HA フェールオーバー構成の一部であるインターフェイスはマッピングできません。それらのインターフェイスは、ウィザードで無効化されています。ウィザードでは、ユーザーが提供するインターフェイスマッピングに従って、論理インターフェイスが作成されます。

- [デフォルトのマッピング（Map Default）] をクリックして、デフォルトのインターフェイスマッピングを設定します。

  たとえば、ソースデバイスの Ethernet1/1 は、ターゲットデバイスの Ethernet1/1 にマッピングされます。

- すべてのマッピングをクリアするには、[すべてをクリア（Clear All）] をクリックします。

ステップ 9 [Next] をクリックします。

ステップ 10 [マッピングの表示（View Mappings）] をクリックして、インターフェイスマッピングを確認します。

ステップ 11 [送信（Submit）] をクリックして移行を開始します。

ステップ 12 [通知（Notifications）] > [タスク（Tasks）] ページに移行ステータスが表示されます。

次のタスク

移行が成功したら、デバイスを展開できます

展開は必須ではなく、構成を検証し、必要に応じて展開できます。ただし、展開前に、Threat Defense デバイス移行のベストプラクティス （79 ページ）に記載されているアクションを実行してください。

Threat Defense デバイス移行のベストプラクティス

移行が成功したら、展開前に次のアクションを実行することをお勧めします。

- インターフェイスの IP アドレスがソースデバイスからターゲットデバイスにコピーされます。ソースデバイスが稼働中の場合は、ターゲット デバイス インターフェイスの IP アドレスを変更します
- 必ず、変更した IP アドレスで NAT ポリシーを更新してください。
- 移行後にインターフェイスの速度がデフォルト値に設定される場合は、それらの速度を設定します。
- ターゲットデバイスにデバイス証明書がある場合は、再登録します。
- （オプション）デバイスのプラットフォーム設定を使用して Firepower 1100 および 2100 の SNMP を設定します。
- （任意）リモートブランチ展開の設定を指定します。

  ソースデバイスまたはターゲットデバイスにデータインターフェイスを介したマネージャアクセス権があった場合、移行後にマネージャアクセス権が失われます。ターゲットデバイスのマネージャアクセス設定を更新します。詳細については、『Cisco Secure Firewall Management Center デバイス設定ガイド』またはオンラインヘルプの「管理アクセスインターフェイスの管理からデータへの変更」を参照してください。
- 必要に応じてサイト間 VPN を設定します。これらの設定は、ソースデバイスから移行されません。
- 展開前に展開プレビューを表示します。**[展開（Deploy）]** ドロップダウンメニューから、**[高度な展開（Advanced Deploy）]** をクリックし、デバイスの **Preview** アイコンをクリックします。
- 正常性監視でデバイスの正常性を監視します（[トラブルシューティング（Troubleshooting）] > [正常性（Health）] > [監視（Monitor）] を選択します）。**System** > **Health** > **Monitor**

移行後は、ソースデバイスの正常性ポリシーがターゲットデバイスの正常性ポリシーになります。デバイスに新しい正常性ポリシーを設定することもできます。

移行後は、デバイスの UUID が移行前後で異なるため、デバイス モニタリング ダッシュボードに一時的に冗長な色付きの行が表示される場合があります。この冗長性は移行時にのみ表示されます。移行から 1 時間経つと、ダッシュボードでメトリックごとに 1 行で表示されるようになります。

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

If the firewall is configured for high availability, you must first break the high availability configuration using the Firewall Device Manager (if possible) or the **configure high-availability disable** command. Ideally, break high availability from the active unit.

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 (Might be required) Configure the Management interface.

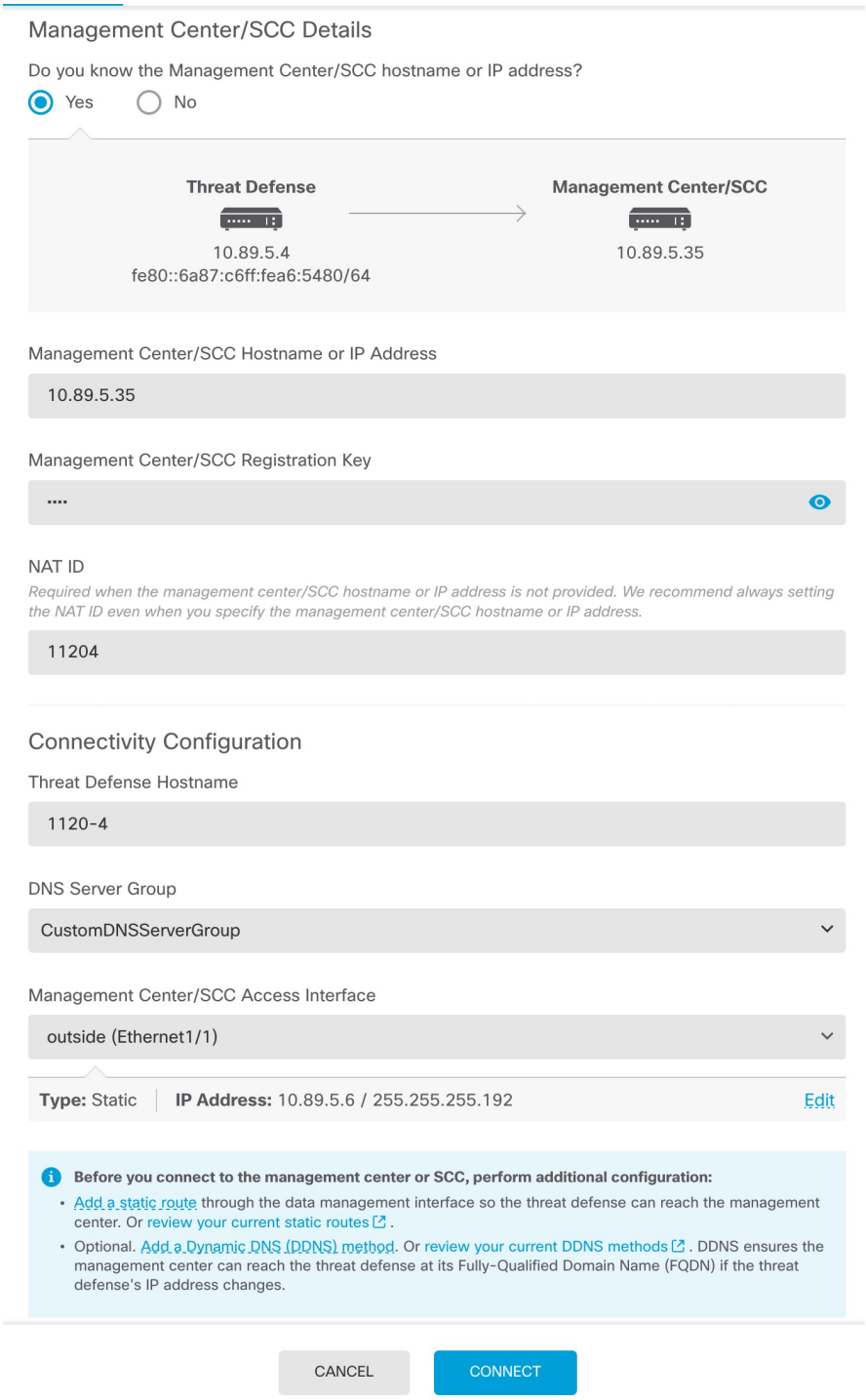
You may need to change the Management interface configuration, even if you intend to use a data interface for manager access. You will have to reconnect to the Firewall Device Manager if you were using the Management interface for the Firewall Device Manager connection.

- Data interface for manager access—The Management interface must have the gateway set to data interfaces. By default, the Management interface receives an IP address and gateway from DHCP. If you do not receive a gateway from DHCP (for example, you did not connect this interface to a network), then the gateway will default to data interfaces, and you do not need to configure anything. If you did receive a gateway from DHCP, then you need to instead configure this interface with a static IP address and set the gateway to data interfaces.
- Management interface for manager access—If you want to configure a static IP address, be sure to also set the default gateway to be a unique gateway instead of the data interfaces. If you use DHCP, then you do not need to configure anything assuming you successfully get the gateway from DHCP.

ステップ 3 Choose **Device** > **System Settings** > **Central Management**, and click **Proceed** to set up the Firewall Management Center management.

ステップ 4 Configure the **Management Center/SCC Details**.

図 *34 : Management Center/SCC Details*



a) For **Do you know the Management Center/SCC hostname or IP address?**, click **Yes** if you can reach the Firewall Management Center using an IP address or hostname, or **No** if the Firewall Management CenterSecurity Cloud Control is behind NAT or does not have a public IP address or hostname.

At least one of the devices, either the Firewall Management Center or the Firewall Threat Defense device, must have a reachable IP address to establish the two-way, TLS-1.3-encrypted communication channel between the two devices.

b) If you chose **Yes**, then enter the **Management Center/SCC Hostname or IP Address**.

c) Specify the **Management Center/SCC Registration Key**.

This key is a one-time registration key of your choice that you will also specify on the Firewall Management Center when you register the Firewall Threat Defense device. The registration key must be between 2 and 36 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID can be used for multiple devices registering to the Firewall Management Center.

a) Specify a **NAT ID**.

This ID is a unique, one-time string of your choice that you will also specify on the Firewall Management Center. The NAT ID must be between 2 and 36 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID *cannot* be used for any other devices registering to the Firewall Management Center. The NAT ID is used in combination with the IP address to verify that the connection is coming from the correct device; only after authentication of the IP address/NAT ID will the registration key be checked. We recommended that you always use the NAT ID even when it is optional, but it is required if:

- You set the Firewall Management Center IP address to **DONTRESOLVE**.
- When adding the device on the Firewall Management Center, you do not specify a reachable device IP address or hostname.
- You use the data interface for management, even if you specify IP addresses on both sides.
- The Firewall Management Center uses multiple management interfaces.

ステップ 5 Configure the **Connectivity Configuration**.

a) Specify the **FTD Hostname**.

If you use a data interface for the **Management Center/SCC Access Interface** access, then this FQDN will be used for this interface.

b) Specify the **DNS Server Group**.

Choose an existing group, or create a new one. The default DNS group is called **CiscoUmbrellaDNSServerGroup**, which includes the OpenDNS servers.

If you intend to choose a data interface for the **Management Center/SCC Access Interface**, then this setting sets the *data* interface DNS server. The Management DNS server that you set with the setup wizard is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface. You are likely to choose the same DNS server group that you used for Management, because both management and data traffic reach the DNS server through the outside interface.

On the Firewall Management Center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this Firewall Threat Defense device. When you add the Firewall

Threat Defense device to the Firewall Management Center, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the Firewall Threat Defense device that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively configure the DNS Platform Settings to match this setting to bring the Firewall Management Center and the Firewall Threat Defense device into sync.

Also, local DNS servers are only retained by the Firewall Management Center if the DNS servers were discovered at initial registration.

If you intend to choose the Management interface for the **Management Center/SCC Access InterfaceFMC Access Interface**, then this setting configures the Management DNS server.

c) For the **Management Center/SCC Access Interface**, choose any configured interface.

You can change the manager interface after you register the Firewall Threat Defense device to the Firewall Management Center, to either the Management interface or another data interface.

ステップ 6 （任意） If you chose a data interface, and it was not the outside interface, then add a default route.

You will see a message telling you to check that you have a default route through the interface. If you chose outside, you already configured this route as part of the setup wizard. If you chose a different interface, then you need to manually configure a default route before you connect to the Firewall Management Center.

If you chose the Management interface, then you need to configure the gateway to be a unique gateway before you can proceed on this screen.

ステップ 7 （任意） If you chose a data interface, click **Add a Dynamic DNS (DDNS) method**.

DDNS ensures the Firewall Management Center can reach the Firewall Threat Defense device at its Fully-Qualified Domain Name (FQDN) if the IP address changes. See **Device** > **System Settings** > **DDNS Service** to configure DDNS.

If you configure DDNS before you add the Firewall Threat Defense device to the Firewall Management Center, the Firewall Threat Defense device automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the Firewall Threat Defense device can validate the DDNS server certificate for the HTTPS connection. Firewall Threat Defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).

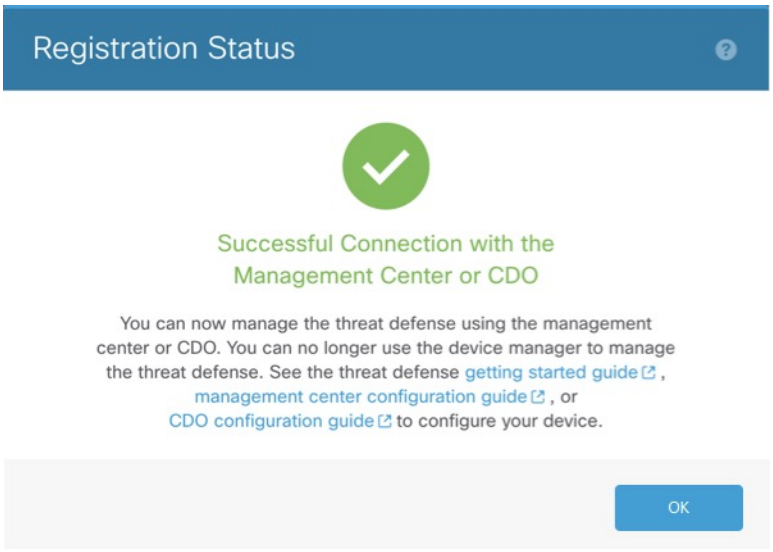
DDNS is not supported when using the Management interface for manager access.

ステップ 8 Click **Connect**. The **Registration Status** dialog box shows the current status of the switch to the Firewall Management Center. After the **Saving Management Center/SCC Registration Settings** step, go to the Firewall Management Center, and add the firewall.

If you want to cancel the switch to the Firewall Management Center, click **Cancel Registration**. Otherwise, do not close the Firewall Device Manager browser window until after the **Saving Management Center/SCC Registration Settings** step. If you do, the process will be paused, and will only resume when you reconnect to the Firewall Device Manager.

If you remain connected to the Firewall Device Manager after the **Saving Management Center/SCC Registration Settings** step, you will eventually see the **Successful Connection with Management Center/SCC** dialog box, after which you will be disconnected from the Firewall Device Manager.

図 *35 : Successful Connection*



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

You can configure the Firewall Threat Defense device currently being managed by the on-premises or cloud-delivered Firewall Management Center to use the Firewall Device Manager instead.

You can switch from the Firewall Management Center to the Firewall Device Manager without reinstalling the software. Before switching from the Firewall Management Center to the Firewall Device Manager, verify that the Firewall Device Manager meets all of your configuration requirements. If you want to switch from the Firewall Device Manager to the Firewall Management Center, see Firewall Device Manager から Firewall Management Center への切り替え.

⚠

注意 Switching to the Firewall Device Manager erases the device configuration and returns the system to the default configuration. However, the Management IP address and hostname are preserved.

手順

ステップ 1 In the Firewall Management Center, unregister the firewall from the **Devices** > **Device Management** page.

ステップ 2 Connect to the Firewall Threat Defense CLI using SSH or the console port. For SSH, open a connection to the **management IP address**, and log into the Firewall Threat Defense CLI with the **admin** username (or any other user with admin privileges).

The console port defaults to the FXOS CLI. Connect to the Firewall Threat Defense CLI using the **connect ftd** command. The SSH session connects directly to the Firewall Threat Defense CLI.

If you cannot connect to the management IP address, do one of the following:

- Ensure that the Management physical port is wired to a functioning network.
- Ensure that the management IP address and gateway are configured for the management network. Use the **configure network ipv4/ipv6 manual** command.

ステップ 3 Verify you are currently in remote management mode.

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 Delete the remote manager and go into no manager mode.

configure manager delete *uuid*

You cannot go directly from remote management to local management. If you have more than one manager defined, you need to specify the identifier (also known as the UUID; see the **show managers** command). Delete each manager entry separately.

例：

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

>
> show managers
No managers configured.
```

ステップ 5 Configure the local manager.

configure manager local

You can now use a web browser to open the local manager at **https://***management-IP-address*.

例：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

Cisco Secure Firewall 3100/4200 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。

USB ポートの無効化

By default, the type-A USB port is enabled. You might want to disable USB port access for security purposes. Disabling USB is supported on the following models:

- Firepower 1000 Series
- Secure Firewall 3100
- Secure Firewall 4200

Guidelines

- Enabling or disabling the USB port requires a reboot.
- If the USB port is disabled and you downgrade to a version that does not support this feature, the port will remain disabled, and you cannot re-enable it without erasing the NVRAM (the FXOS local-mgmt **erase secure all** command).
- If you perform a ROMMON **factory-reset** or FXOS local-mgmt **erase secure**, the USB port will be re-enabled.
- For high availability or clustering, you must disable or re-enable the port individually on each unit.

（注） This feature does not affect the USB console port, if present.

デバイスでの USB ポートの無効化

デバイスで USB ポートを無効化にするには、Firewall Threat Defense CLIを使用します。

手順

ステップ 1 USB ポートを無効化します。

system support usb configure disable

reboot

USB ポートを再度有効にするには、**system support usb configure enable** と入力します。

例：

```
>system support usb configure disable
USB Port Admin State set to 'disabled'.
Please reboot the system to apply any control state changes.

>reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': YES
```

ステップ 2 ポートステータスを表示します。

system support usb show

[管理ステータス（Admin State）] には、USB ポートの設定が表示されます。[動作ステータス（Oper State）] には、現在の動作が表示されます。たとえば、USB ポートを無効化してリロードしていない場合、[管理ステータス（Admin State）] には無効と表示され、[動作ステータス（Oper State）] は有効になります。

例：

```
>system support usb show
USB Port Info
---------------
Admin State: disabled
Oper State: disabled
```

マルチインスタンスモードでの USB ポートの無効化

マルチインスタンス モードで USB ポートを無効化にするには、FXOS CLI を使用します。

手順

ステップ 1 USB ポートを無効にして再起動し、変更を有効にします。

a) USB ポートを無効化します。

scope fabric-interconnect

disable usb-port

commit buffer

b) シャーシをリブートします。

connect local-mgmt

reboot

例：

```
firepower-4245 /fabric-interconnect # disable usb-port
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:
device /fabric-interconnect* # commit buffer
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:yes
firepower-4245 /fabric-interconnect # connect local-mgmt
firepower-4245(local-mgmt)# reboot
Before rebooting, please take a configuration backup.
Do you still want to reboot? (yes/no):yes
Broadcast message from admin@firepower-4245 (Wed Feb 21 05:59:55 2024):
All shells being terminated due to system /sbin/reboot
```

ステップ 2 USB ポートを有効にして再起動し、変更を有効にします。

a) USB ポートを有効にします。

scope fabric-interconnect

enable usb-port

commit buffer

b) シャーシをリブートします。

connect local-mgmt

reboot

例：

```
firepower-4245 /fabric-interconnect # enable usb-port
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:
device /fabric-interconnect* # commit buffer
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:yes
firepower-4245 /fabric-interconnect # connect local-mgmt
firepower-4245(local-mgmt)# reboot
Before rebooting, please take a configuration backup.
Do you still want to reboot? (yes/no):yes
Broadcast message from admin@firepower-4245 (Wed Feb 21 05:59:55 2024):
All shells being terminated due to system /sbin/reboot
```

ステップ 3 USB ポートのステータスを表示します。

scope fabric-interconnect

show usb-port

[管理ステータス（Admin State）] には、USB ポートの設定が表示されます。[動作ステータス（Oper State）] には、現在の動作が表示されます。たとえば、USB ポートを無効化してリロードしていない場合、[管理ステータス（Admin State）] には [無効（Disabled）] と表示され、[動作ステータス（Oper State）] は [有効（Enabled）] になります。

例：

```
firepower-4245# scope fabric-interconnect
firepower-4245 /fabric-interconnect # show usb-port
```

```
Usb Port:
Equipment         Admin State Oper State
----------------- ----------- ----------
A                 Disabled    Disabled
```

デバイス管理の履歴

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
[デバイス（ウィザード）（Device (Wizard)）] に追加された基本初期設定を使用して、登録キーでデバイスを追加する	7.7.0	いずれか	[デバイス（ウィザード）（Device (Wizard)）] の基本初期設定では、登録キーを使用してデバイスを追加できるようになりました。この機能は、**[追加（Add）]** > **[デバイス（Device）]**画面にも引き続き表示されます。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[追加（Add）]** > **[デバイス（ウィザード）（Device (Wizard)）]**
Serial-number registration (zero-touch provisioning) supported from an on-prem Firewall Management Center.	7.6.0	Management Center がパブリックに到達できる必要がある：7.2.0 削除された制限事項：7.2.4/7.4.0	You can now register a device using its serial number from an on-prem Firewall Management Center. With templates (requires Firewall Threat Defense 7.4.1+ on the device), you can register multiple devices at once. This feature was previously known as low-touch provisioning. Requires Cisco Security Cloud. For upgraded Firewall Management Centers, your existing Security Cloud Control integration continues to work until you enable Cisco Security Cloud. New/modified screens: **Devices** > **Device Management** > **Add** > **Device (Wizard)** Supported platforms: Firepower 1000/2100, Secure Firewall 1200/3100. Note that Firepower 2100 support is for Firewall Threat Defense 7.4.1–7.4.x only; those devices cannot run Version 7.6.0.
[削除（Delete）] メニュー項目の名前が [登録解除（Unregister）] に変更されました	7.6.0	任意	The **Delete** menu choice was renamed to **Unregister** to better indicate that the device, high-availability pair, or cluster is being unregistered from the Firewall Management Center and not deleted from the high availability pair or cluster or having its configuration erased. The device, high-availability pair, or cluster continues to pass traffic until it is re-registered. New/modified screens: **Devices** > **Device Management** > **More**

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
テンプレートを使用したデバイスの追加	7.6.0	7.4	**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[追加（Add）]** > **[デバイス（ウィザード）（Device (Wizard)）]** 画面では、テンプレートを使用してデバイスを追加できます。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[追加（Add）]** > **[デバイス（ウィザード）（Device (Wizard)）]**
Disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100/4200.	7.6.0	7.6.0	You can now disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100/4200. By default, the port is enabled. New/modified Firewall Threat Defense CLI commands: **system support usb show**, **system support usb port disable**, **system support usb port enable** New/modified FXOS CLI commands for the Secure Firewall 3100/4200 in multi-instance mode: **show usb-port**, **disable USB port**, **enable usb-port** See: *Cisco Secure Firewall Threat Defense Command Reference* and *Cisco Firepower 4100/9300 FXOS Command Reference*
Chassis-level health alerts for the Firepower 4100/9300.	7.4.1	7.4.1	You can now view chassis-level health alerts for Firepower 4100/9300 by registering the chassis to the Firewall Management Center as a read-only device. You must also enable the Firewall Threat Defense Platform Faults health module and apply the health policy. The alerts appear in the Message Center, the health monitor (in the left pane, under Devices, select the chassis), and in the health events view. You can also add a chassis (and view health alerts for) the Secure Firewall 3100 in multi-instance mode. For those devices, you use the Firewall Management Center to manage the chassis. But for the Firepower 4100/9300 chassis, you still must use the chassis manager or the FXOS CLI. New/modified screens: **Devices** > **Device Management** > **Add** > **Chassis**
Zero-Touch Provisioning to register the Firepower 1000/2100 and Secure Firewall 3100 to the Firewall Management Center using a serial number.	7.4.0	Management Center がパブリックに到達可能：7.2.0 Management Center がパブリックに到達できない：7.2.4/7.4.0	Zero-Touch Provisioning (also called low-touch provisioning) lets you register Firepower 1000/2100 and Secure Firewall 3100 devices to the Firewall Management Center by serial number without having to perform any initial setup on the device. The Firewall Management Center integrates with SecureX and Security Cloud Control for this functionality. New/modified screens: **Devices** > **Device Management** > **Add** > **Device** > **Serial Number**

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Merged management and diagnostic interfaces.	7.4.0	7.4.0	**Upgrade impact. Merge interfaces after upgrade.** For new devices using 7.4 and later, you cannot use the legacy diagnostic interface. Only the merged management interface is available. If you upgraded to 7.4 or later and: • You did not have any configuration for the diagnostic interface, then the interfaces will merge automatically. • You have configuration for the diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate diagnostic interface. Note that support for the diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible. Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including Management) in the configuration. For platform settings, this means: • You can no longer enable HTTP, ICMP, or SMTP for diagnostic. • For SNMP, you can allow hosts on management instead of diagnostic. • For Syslog servers, you can reach them on management instead of diagnostic. • If Platform Settings for syslog servers or SNMP hosts specify the diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices. • DNS lookups no longer fall back to the management-only routing table if you do not specify interfaces. New/modified screens: **Devices** > **Device Management** > **Interfaces** New/modified commands: **show management-interface convergence**
Migrate Firepower 1000/2100 to Secure Firewall 3100.	7.4.0	任意（Any）	You can now easily migrate configurations from the Firepower 1000/2100 to the Secure Firewall 3100. New/modified screens: **Devices** > **Device Management** > **Migrate** Platform restrictions: Migration not supported from the Firepower 1010 or 1010E.

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
すべての登録済みデバイスのレポートをダウンロードします。	7.4.0	任意（Any）	すべての登録済みデバイスのレポートをダウンロードできるようになりました。**[デバイス（Devices）]** > **[デバイス管理（Device Management）]**に移動し、ページの右上にある新しい [デバイスリストレポートのダウンロード（Download Device List Report）] リンクをクリックします。
Manage Firewall Threat Defense high availability pairs using a data interface.	7.4.0	7.4.0	Firewall Threat Defense high availability now supports using a regular data interface for communication with the Firewall Management Center. Previously, only standalone devices supported this feature. See: Device Management
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、Security Cloud Control（Security Cloud Control）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 [Security Cloud Control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、Security Cloud Controlのドキュメントを参照してください。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
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。
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。