



デバイス管理

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

この章では、Secure Firewall Management Center 内のデバイスの追加および管理方法について説明します。

- [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へのログイン \(12 ページ\)](#)
- [手動登録での Threat Defense 初期設定の完了 \(14 ページ\)](#)
- [登録キーを使用した Management Center へのデバイスの追加 \(32 ページ\)](#)
- [シリアル番号 \(ゼロタッチプロビジョニング\) を使用した Management Center へのデバイスの追加 \(36 ページ\)](#)
- [Management Center へのシャーシの追加 \(44 ページ\)](#)
- [Management Center からのデバイスの削除 \(登録解除\) \(47 ページ\)](#)
- [デバイス グループの追加 \(48 ページ\)](#)
- [デバイスのシャットダウンまたは再起動 \(49 ページ\)](#)
- [管理対象デバイスのリストのダウンロード \(50 ページ\)](#)
- [デバイス設定の構成 \(50 ページ\)](#)
- [デバイスの管理設定の変更 \(123 ページ\)](#)
- [Cisco Secure Firewall 3100/4200 での SSD のホットスワップ \(134 ページ\)](#)
- [新しいモデルへの設定の移行 \(136 ページ\)](#)
- [デバイス管理の基本の履歴 \(143 ページ\)](#)

デバイス管理について

Management Center を使用してデバイスを管理します。

Management Center およびデバイス管理について

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 暗号化通信チャンネルをセットアップします。Management Center はこのチャンネルを使用して、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、同じチャンネルを使用してそれらのイベントを Management Center に送信します。

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、Management Center からデバイスのヘルスステータスをモニターできます。



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

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。

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) 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 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 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。

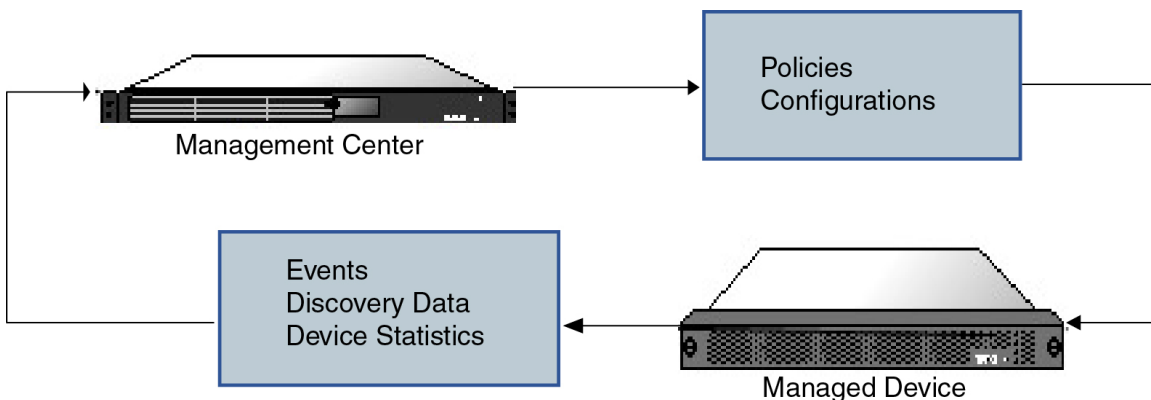
Secure Firewall Management Center で管理できるデバイス

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 暗号化通信チャンネルを介して、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、Management Center と管理対象デバイス間で送信される情報を示します。アプリケーション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

Management Center 情報を使用してデバイスを設定し、デバイスを Management Center に追加した後に、デバイスまたは 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、以下ようになります。

- デバイスまたは 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。
- Management Center のみが開始できる。

初期化は常に 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イスが試行されます。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、インシエータは、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。



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

ポリシーとイベント以外の機能

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

FTDCLI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 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 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

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 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。

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 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。

Management Center が不明な場合、Management Center が最初の接続を確立します。この場合、Threat Defense で指定されたものとは異なる 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 Management Center 管理インターフェイスを使用する必要があります。

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 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、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 Threat Defense データインターフェイスの使用について

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 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と EtherChannel は使用できません。冗長性を目的として、Management Center の単一のセカンダリインターフェイスでマネージャアクセスを有効にすることもできます。
- このインターフェイスは管理専用にはできません。
- ルーテッドインターフェイスを使用するルーテッドファイアウォールモードのみです。
- PPPoE はサポートされていません。ISP で PPPoE が必要な場合は、PPPoE をサポートするルータを Threat Defense と WAN モデムの間に配置する必要があります。
- インターフェイスを配置する必要があるのはグローバル VRF のみです。
- SSH はデータインターフェイスではデフォルトで有効になっていないため、後で Management Center を使用して SSH を有効にする必要があります。また、管理インターフェイス ゲートウェイがデータインターフェイスに変更されるため、**configure network static-routes** コマンドを使用して管理インターフェイス用の静的ルートを追加しない限り、リモートネットワークから管理インターフェイスに SSH 接続することはできません。Amazon Web Services の 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。
- 冗長マネージャアクセス データ インターフェイスはサポートされていません。
- DHCP は使用できません。静的 IP アドレスのみがサポートされています。DDNS やゼロタッチプロビジョニングなど、DHCP に依存する機能は使用できません。
- 同じサブネット内に異なる静的 IP アドレスがあります。
- IPv4 または IPv6 のいずれかを使用します。両方を設定することはできません。
- 同じマネージャ設定 (**configure manager add** コマンド) を使用して、接続が同じであることを確認します。
- データインターフェイスをフェールオーバーリンクまたはステートリンクとして使用することはできません。

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ール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 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 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

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 2100	management0 (注) management0 は管理 1/1 インターフェイスの内部名です。	サポートなし
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 **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 **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、**Management Center** がデバイスの IP アドレスを指定し、デバイスが **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。**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。

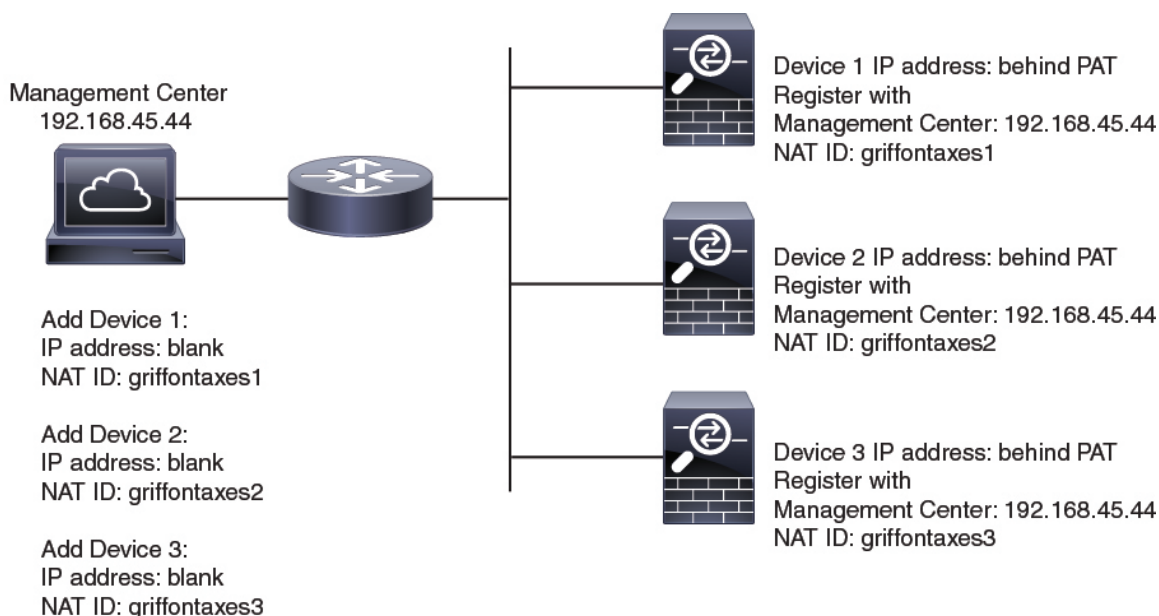
たとえば、デバイスを **Management Center** に追加したときにデバイスの IP アドレスがわからない場合（たとえばデバイスが PAT ルータの背後にある場合）は、NAT ID と登録キーのみを **Management Center** に指定します。IP アドレスは空白のままにします。デバイス上で、**Management Center** の IP アドレス、同じ NAT ID、および同じ登録キーを指定します。デバイスが **Management**

Center の IP アドレスに登録されます。この時点で、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 Management Center に追加することができます。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、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。

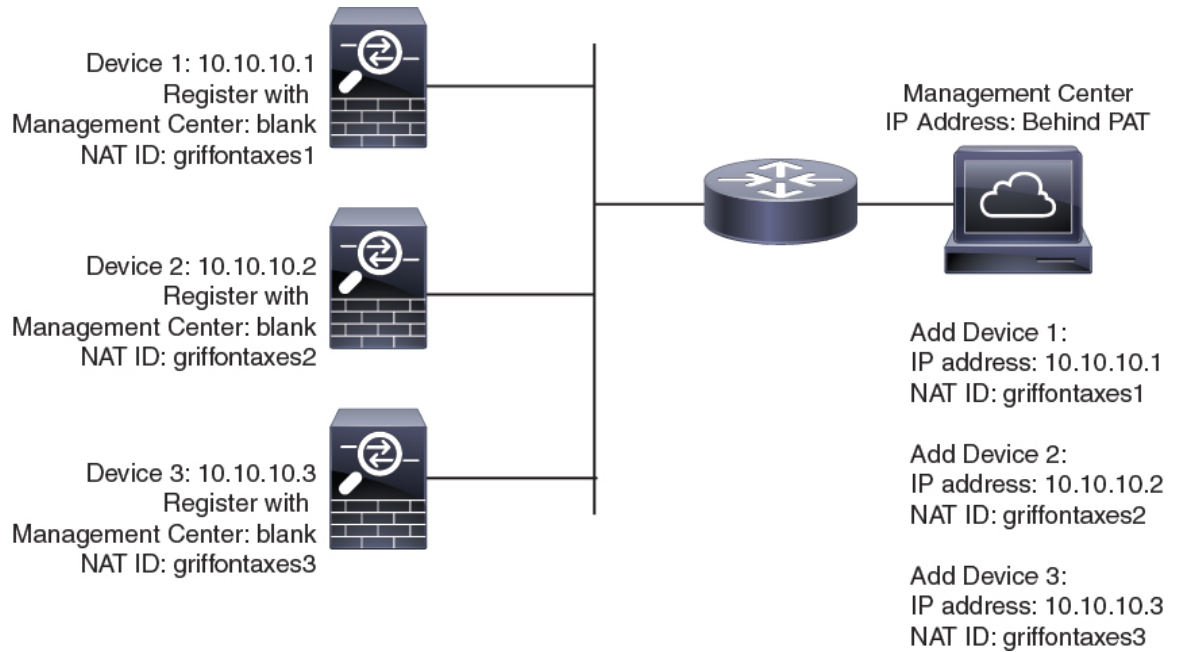
次の例に、PAT IP アドレスの背後にある 3 台のデバイスを示します。この場合、Management Center とデバイスの両方でデバイスごとに一意の NAT ID を指定し、デバイス上の Management Center の IP アドレスを指定します。

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 Management Center を示します。この場合、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、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 Management Center の NAT ID



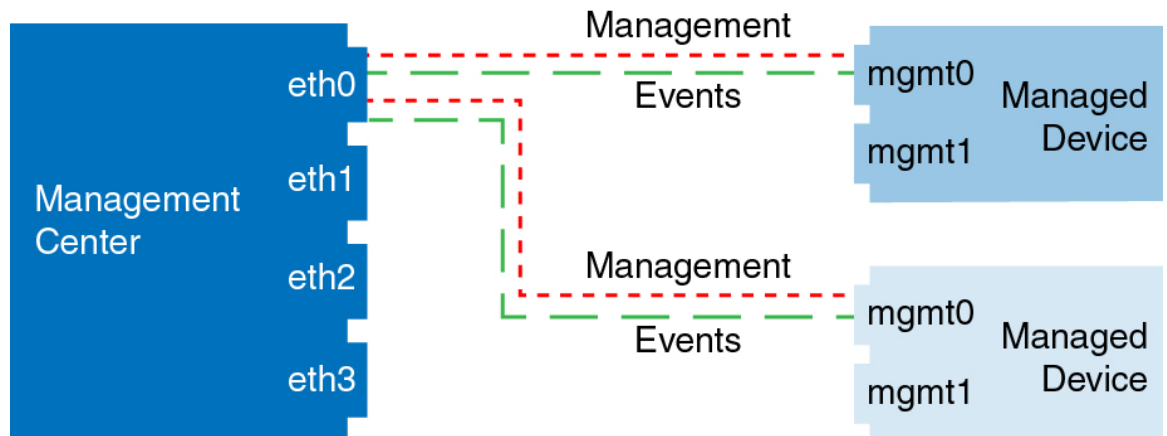
管理およびイベントトラフィック チャンネルの例



(注) 管理用のデータインターフェイスを 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。

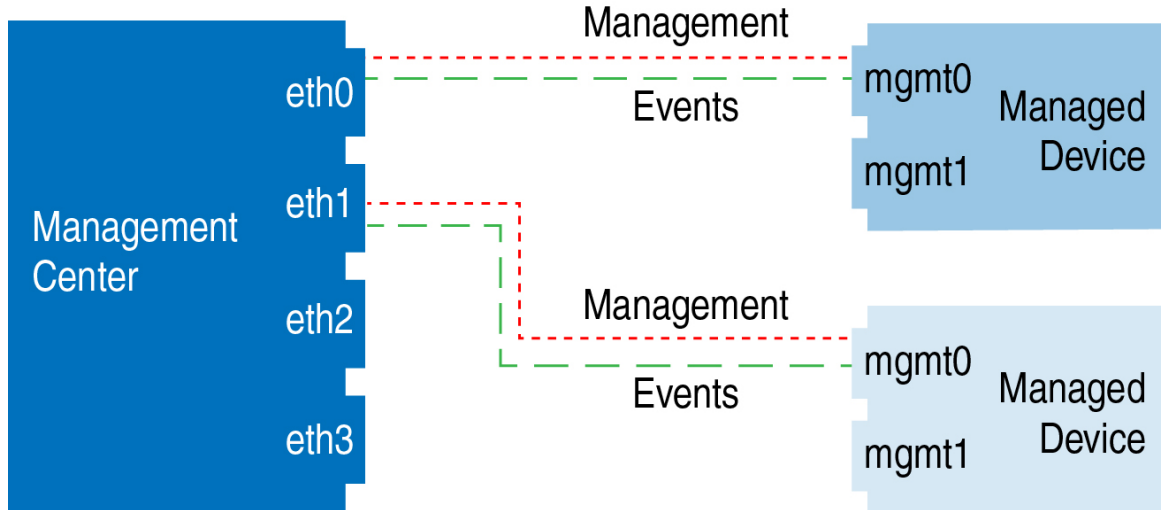
以下に、Management Center と管理対象デバイスでデフォルト管理インターフェイスのみを使用する例を示します。

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



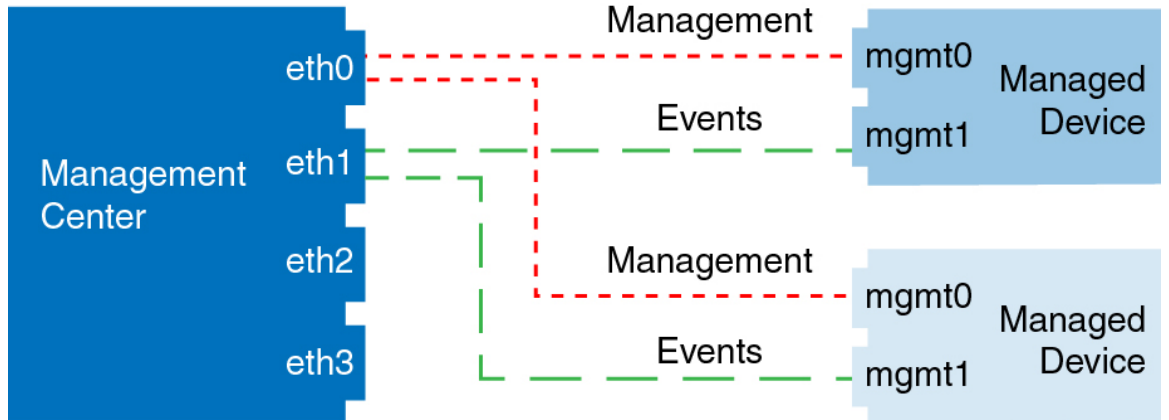
以下に、Management Center でデバイスごとに別個の管理インターフェイスを使用する例を示します。この場合、各管理対象デバイスが1つの管理インターフェイスを使用します。

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



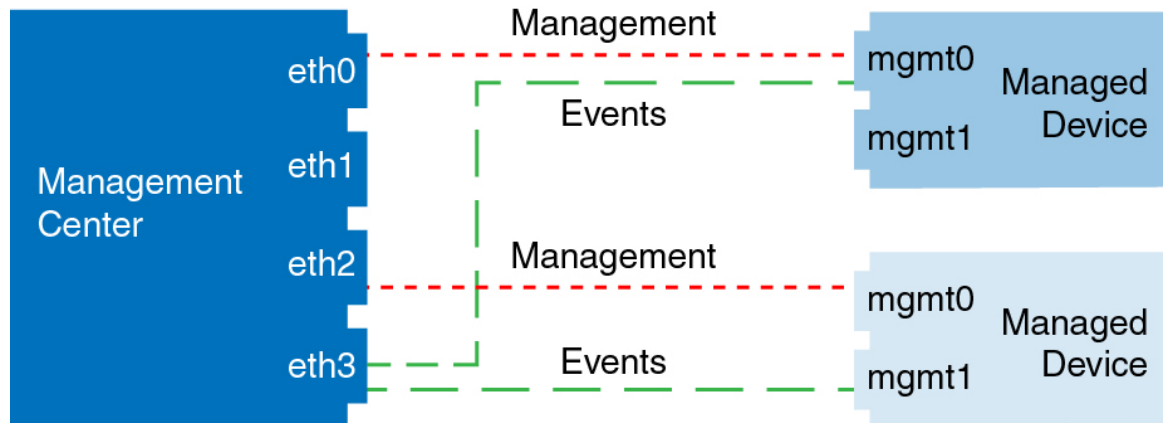
以下に、個別のイベント インターフェイスを使用する Management Center と管理対象デバイスの例を示します。

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

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



デバイス管理の要件と前提条件

サポートされるドメイン

デバイスが存在するドメイン。

ユーザの役割

- 管理者
- ネットワーク管理者

管理接続

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

デバイスのコマンドラインインターフェイスへのログイン

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 **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。



(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。

手順

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

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 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 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 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、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

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2つのサブモード、ユーザー EXEC モードと特権 EXEC モードがあります。特権 EXEC モードではより多くのコマンドが利用できます。特権 EXEC モードを開始するには、**enable** コマンドを入力し、プロンプトに対してパスワードを入力せずに **Enter** を押します。

例：

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

通常の CLI に戻るには、Ctrl+a、d を入力します。

手動登録での 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 Device Manager を使用して 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。

ゼロタッチプロビジョニング (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 \(ゼロタッチプロビジョニング\)](#) を使用した [Management Center](#) へのデバイスの追加 (36 ページ) を参照してください。

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

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

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

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

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

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

- Cisco Secure Firewall 4200 は、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 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 Management Center を分析のみに使用する CDO 管理対象デバイスには適用されません。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 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せん。Device Manager を使用してこれらのデバイスを 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 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 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、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、または手動でスタティック IP アドレス、サブネットマスク、およびゲートウェイを入力できます。[オフ (Off)] を選択して、IPv4 アドレスを設定しないという選択肢もあります。セットアップウィザードを使用して PPPoE を設定することはできません。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。ウィザードの完了後に PPPoE を設定できます。

[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、または手動でスタティック IP アドレス、プレフィックス、およびゲートウェイを入力できます。[オフ (Off)] を選択して、IPv6 アドレスを設定しないという選択肢もあります。

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

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

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

[DNSサーバ (DNS Servers)]: システムの管理アドレス用の DNS サーバ。名前解決用に 1 つ以上の DNS サーバのアドレスを入力します。デフォルトは OpenDNS パブリック DNS サーバです。フィールドを編集し、デフォルトに戻したい場合は、[OpenDNS

を使用 (Use OpenDNS)] をクリックすると、フィールドに適切な IP アドレスがリロードされます。

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

- b) [時刻設定 (NTP) (Time Setting (NTP))] を設定し、[次へ (Next)] をクリックします。
1. [タイムゾーン (Time Zone)] : システムのタイムゾーンを選択します。
 2. [NTPタイムサーバ (NTP Time Server)] : デフォルトの NTP サーバを使用するか、使用している NTP サーバのアドレスを手動で入力するかを選択します。バックアップ用に複数のサーバを追加できます。
- c) [登録せずに 90 日間の評価期間を開始 (Start 90 day evaluation period without registration)] を選択します。
- Threat Defense を Smart Software Manager に登録しないでください。すべてのライセンスは Management Center で実行されます。
- d) [終了 (Finish)] をクリックします。
- e) [クラウド管理 (Cloud Management)] または [スタンドアロン (Standalone)] を選択するよう求められます。Management Center の管理については、[スタンドアロン (Standalone)] を選択してから、[Got It (了解)] を選択します。

ステップ 3 (必要に応じて) 管理インターフェイスを設定します。

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

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

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

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

- ステップ 5 [デバイス (Device)] [システム設定 (Device System Settings)] [中央管理 (Central Management)] [Management Center] [Management Center] [デバイス (Device)] [システム設定 (System Settings)] [中央管理 (Central Management)] [Management Center] の順に選択し、 [続行 (Proceed)] をクリックして Management Center の管理を設定します。
- ステップ 6 [Management Center/CDOの詳細 (Management Center/CDO Details)] を設定します。

図 7: Management Center/CDO の詳細

Configure Connection to Management Center or CDO


Provide details to register to the management center/CDO.

Management Center/CDO Details

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

Yes No


Threat Defense



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

→

Management Center/CDO



10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

●●●● 👁

NAT ID

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

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup ▼

Management Center/CDO Access Interface

Data Interface

Please select an interface ▼

Management Interface [View details](#)

CANCEL
CONNECT

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

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

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

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

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

- d) [NAT ID] を指定します。

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

ステップ 7 [接続の設定 (Connectivity Configuration)] を設定します。

- a) [FTD ホスト名 (FTD Hostname)] を指定します。

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

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

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

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

Management Center では、この Threat Defense デバイスに割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。Management Center に Threat Defense デバイスを追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む Threat Defense デバ

イスに後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。Management Center と Threat Defense デバイスを同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

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

FMC アクセスインターフェイスに管理インターフェイスを選択する場合は、この設定で管理 DNS サーバーを構成します。

- c) **Management Center/CDO アクセスインターフェイス**については、任意の構成済みインターフェイスを選択してください。

管理インターフェイスは、Threat Defense デバイスを Management Center に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。

- ステップ 8** (任意) 外部インターフェイスではないデータインターフェイスを選択した場合は、デフォルトルートを追加します。

インターフェイスを通過するデフォルトルートがあることを確認するように求めるメッセージが表示されます。外部を選択した場合は、セットアップウィザードの一環としてこのルートがすでに設定されています。別のインターフェイスを選択した場合は、Management Center に接続する前にデフォルトルートを手動で設定する必要があります。

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

- ステップ 9** (任意) データインターフェイスを選択した場合は、[ダイナミック DNS (DDNS) 方式の追加 (Add a Dynamic DNS (DDNS) method)]をクリックします。

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

Management Center に Threat Defense デバイスを追加する前に DDNS を設定すると、Threat Defense デバイスは、Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加し、Threat Defense デバイスが HTTPS 接続のために DDNS サーバー証明書を検証できるようにします。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せん。

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

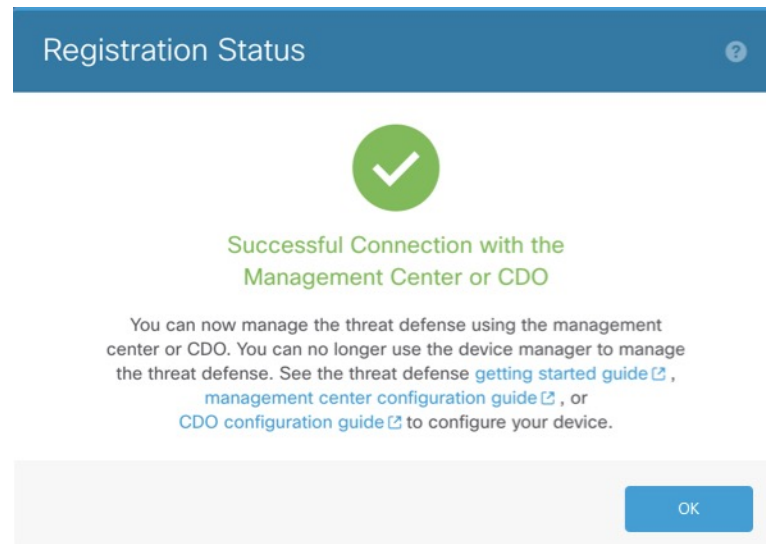
- ステップ 10** [接続 (Connect)]をクリックします。[登録ステータス (Registration Status)]ダイアログボックスには、Management Center への切り替えに関する現在のステータスが表示されます。[Management Center/CDO 登録設定の保存 (Saving Management Center/CDO Registration Settings)]のステップの後、Management Center に移動してファイアウォールを追加します。

Management Center への切り替えをキャンセルする場合は、[登録のキャンセル (Cancel Registration)]をクリックします。キャンセルしない場合は、[Management Center/CDO 登録設

定の保存 (Saving Management Center/CDO Registration Settings)]のステップが完了するまで Device Manager のブラウザウィンドウを閉じないでください。閉じた場合、プロセスは一時停止し、Device Manager に再接続した場合のみ再開されます。

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

図 8: 正常接続



CLI を使用した Threat Defense 初期設定の実行の完了

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、Management Center 通信の設定を行います。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 Management Center に切り替えたときに、Device Manager で完了したすべてのインターフェイス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、Threat Defense CLI に接続します。デフォルトで DHCP サーバーから IP アドレスが取得されます。ネットワーク設定を変更する場合は、切断されないようにコンソールポートを使用することを推奨します。

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

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

(Firepower および Cisco Secure Firewall ハードウェアモデル) コンソールポートで FXOS CLI に接続します。初めて FXOS にログインしたときは、パスワードを変更するよう求められます。このパスワードは、SSH の 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 Cisco Secure Firewall ハードウェアの場合は、[Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 と Threat Defense の Cisco FXOS トラブルシューティングガイド \[英語\]](#) の「[Reimage Procedures](#)」を参照してください。

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

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

connect ftd

例：

```
firepower# connect ftd
>
```

ステップ 4 Threat Defense に初めてログインすると、エンドユーザーライセンス契約書 (EULA) に同意し、SSH 接続を使用している場合は、管理者パスワードを変更するように求められます。その後、CLI セットアップスクリプトが表示されます。

(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。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?)] : Management Center を使用するには「no」を入力します。「yes」と答えると、代わりに Firepower 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:
End User License Agreement
[...]

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

System initialization in progress. Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 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 Threat Defense を管理する Management Center を特定します。

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

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

- {hostname | IPv4_address | IPv6_address | DONTRESOLVE}—Specifies either the FQDN or IP address of the Management Center. Management Center を直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。また、*nat_id* も指定します。双方向の TLS-1.3 暗号化通信チャンネルを 2 台のデバイス間に確立するには、少なくとも 1 台以上のデバイス (Management Center または Threat Defense) に到達可能な IP アドレスが必要です。このコマンドで **DONTRESOLVE** を指定するには、FTD には到達可能な IP アドレスまたはホスト名が必要です。
- *reg_key* : Threat Defense を登録するときに Management Center でも指定する任意のワнтаイム登録キーを指定します。登録キーは 37 文字以下にする必要があります。有効な文字には、英数字 (A~Z、a~z、0~9)、およびハイフン (-) があります。
- *nat_id* : 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、Threat Defense を登録するときに Management Center にも指定する任意の一意のワнтаイム文字列を指定します。たとえば、Management Center を **DONTRESOLVE** に設定した場合に必要です。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場合にも必要です。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字 (A~Z、a~z、0~9)、およびハイフン (-) があります。この ID は、Management Center に登録する他のデバイスには使用できません。

(注) 管理にデータインターフェイスを使用する場合は、両方の IP アドレスを指定する場合でも、Threat Defense と Management Center の両方で NAT ID を指定する必要があります。

- *display_name* : **show managers** コマンドでこのマネージャを表示するための表示名を指定します。このオプションは、CDO をプライマリマネージャおよび分析専用のオンプレミ

ス 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 :

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 :

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 Management Center IP アドレスまたはホスト名を入力します。

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

ステップ 6 プライマリマネージャとして CDO を使用していて、オンプレミス Management Center を分析のみに使用する場合は、オンプレミス 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、CDO で生成した表示名で CDO 用に生成したコマンドを使用して、分析専用のオンプレミス 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
LzmlH0ynhVUWhXYWz2swmkj2ZWsN3Lb 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 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。管理インターフェイスゲートウェイを **data-interfaces** に設定しなかった場合は、ここでこのコマンドで設定します。
- Threat Defense を Management Center に追加すると、Management Center はインターフェイス設定 (インターフェイス名と IP アドレス、ゲートウェイへの静的ルート、DNS サーバー、DDNS サーバーなど) を検出して維持します。DNS サーバー設定の詳細については、次を参照してください。Management Center では、後でマネージャアクセスインターフェイス構成を変更できますが、Threat Defense または Management Center が管理接続の再確立を妨げるような変更を加えないようにしてください。管理接続が中断された場合、Threat Defense には以前の展開を復元する **configure policy rollback** コマンドが含まれません。
- DDNS サーバー更新の URL を設定すると、Threat Defense は Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加するため、Threat Defense は HTTPS 接続の DDNS サーバー証明書を検証できます。Threat Defense は、DynDNS リモート API 仕様 (<https://help.dyn.com/remote-access-api/>) を使用するすべての DDNS サーバーをサポートします。
- このコマンドは、「データ」インターフェイス DNS サーバーを設定します。セットアップスクリプトで (または **configure network dns servers** コマンドを使用して) 設定した管理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS (設定されている場合) またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。

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

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

また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ Management Center で保持されます。たとえば、管理インターフェイスを使用してデバイスを登録し、後で **configure network management-data-interface** コマンドを使用してデータインターフェイスを設定した場合、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 Management Center で手動で設定する必要があります。

- 管理インターフェイスは、Threat Defense を Management Center に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。
- セットアップウィザードで設定した FQDN がこのインターフェイスに使用されます。

- コマンドの一部としてデバイス設定全体をクリアできます。このオプションはリカバリシナリオで使用できますが、初期セットアップや通常の操作には使用しないでください。
- データ管理を無効にするには、**configure network management-data-interface disable** コマンドを入力します。

例：

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

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

Setting IPv4 network configuration.
Network settings changed.

>
```

例：

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

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

Setting IPv4 network configuration.
Network settings changed.

>
```

ステップ 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 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、Management Center でイベントインターフェイスを有効にする必要もあります。[Cisco Secure Firewall Management Center アドミニストレーションガイド](#)を参照してください。

手順

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

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

必要に応じて、**configure network management-interface disable-events-channel** コマンドを使用してメイン管理インターフェイスのイベントを無効にできます。いずれの場合も、デバイスは、イベントのみのインターフェイス上でイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベントチャン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ン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 Management Center がリモート ネットワーク上にある場合は、イベント専用インターフェイスのスタティックルートを追加します。追加しないと、すべてのトラフィックが管理インターフェイスを通じてデフォルトルートと一致します。

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

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

例：

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

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
```

```
2001:0DB8:BA98::3211
Configuration updated successfully
```

```
>
```

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

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

登録キーを使用した Management Center へのデバイスの追加

登録キーを使用して 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。

オンプレミス Management Center を使ってイベントロギングと分析を行うクラウド管理対象デバイスを追加することもできます。

Management Center ハイアベイラビリティを確立したか、または確立する予定がある場合、デバイスをアクティブな（またはアクティブにする予定の）Management Center にのみ追加します。ハイアベイラビリティを確立すると、アクティブ Management Center に登録されたデバイスが自動的にスタンバイに登録されます。

始める前に

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

手順

- ステップ1 [デバイス (Devices)]> [デバイス管理 (Device Management)]を選択します。
- ステップ2 [追加 (Add)] ドロップダウンメニューから、[デバイス (Device)]を選択します。
登録キー方式がデフォルトで選択されています。

図 9: 登録キーを使用したデバイスの追加

Add Device ?

Select the Provisioning Method:

Registration Key Serial Number

CDO Managed Device

Host:†

Display Name:

Registration Key: *

Group:

Access Control Policy: *

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

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

Carrier
 Malware Defense
 IPS
 URL

Advanced
Unique NAT ID: †

Transfer Packets

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

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

図 10: CDO にデバイスを追加

The screenshot shows the 'Add Device' dialog box. At the top, it says 'Add Device' with a help icon. Below that, it asks to 'Select the Provisioning Method:' with two radio buttons: 'Registration Key' (selected) and 'Serial Number'. Under 'Registration Key', there is a checked checkbox for 'CDO Managed Device'. The 'Host:' field contains '10.89.5.40'. The 'Display Name:' field also contains '10.89.5.40'. The 'Registration Key:*' field is empty. The 'Group:' dropdown menu is set to 'None'. In the 'Advanced' section, the 'Unique NAT ID:*' field contains 'test'. A note below says 'Transfer Packets is configured in CDO'. At the bottom, there are 'Cancel' and 'Register' buttons.

ステップ 4 [ホスト (Host)] フィールドに、追加するデバイスの IP アドレスまたはホスト名を入力します。

デバイスのホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前です。ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、ホスト名を使用します。

NAT 環境では、Management Center の管理対象としてデバイスを設定するときに Management Center の IP アドレスまたはホスト名をすでに指定した場合、デバイスの IP アドレスまたはホスト名を指定する必要がない場合があります。詳細については、[NAT 環境 \(8 ページ\)](#) を参照してください。

(注) Management Center ハイアベイラビリティ環境で両方の Management Center が NAT の背後にある場合、セカンダリ Management Center でデバイスを登録するには、[ホスト (Host)] フィールドで値を指定する必要があります。

- ステップ 5** [表示名 (Display Name)] フィールドに、Management Center でのデバイスの表示名を入力します。
- ステップ 6** [登録キー (Registration Key)] フィールドに、Management Center の管理対象としてデバイス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。
- ステップ 7** 必要に応じて、デバイスをデバイス グループに追加します。
- ステップ 8** 登録後すぐに、デバイスに展開する最初の [アクセス コントロール ポリシー (Access Control Policy)] を選択するか、新しいポリシーを作成します。

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

- ステップ 9** デバイスに適用するライセンスを選択します。
- デバイスを追加した後、[システム (System)] > [ライセンス (Licenses)] > [スマートライセンス (Smart Licenses)] ページからライセンスを適用することもできます。
- 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。Threat Defense Virtual で使用可能なパフォーマンス階層ソフトウェア利用資格の詳細については、[Cisco Secure Firewall Management Center アドミニストレーションガイド](#)の「*FTDv Licenses*」を参照してください。
- (注) 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** デバイスの設定時に NAT ID を使用した場合は、[詳細 (Advanced)] セクションで、[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、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、初期セットアップ時にデバイスにも指定する任意の一意のワнтаイム文字列を指定します。たとえば、[ホスト (Host)] フィールドを空白のままにした場合は必須です。IP アドレスを指定する場合でも、管理にデバイスのデータインターフェイスを使用する場合にも必要です。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字 (A~Z、a~z、0~9) 、およびハイフン (-) があります。この ID は、Management Center に登録する他のデバイスには使用できません。
- (注) 管理にデバイスのデータインターフェイスを使用する場合は、両方の IP アドレスを指定する場合でも、デバイスと Management Center の両方で NAT ID を指定する必要があります。

- 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、デバイスで Management Center にパケットを転送することを許可します。
- このオプションは、デフォルトで有効です。このオプションを有効にして IPS や Snort などのイベントがトリガーされた場合は、デバイスが検査用としてイベントメタデータ情報とパケッ

トデータを Management Center に送信します。このオプションを無効にした場合は、イベント情報だけが Management Center に送信され、パケット データは送信されません。

ステップ 12 [登録 (Register)] をクリックします。

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 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 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。

シリアル番号（ゼロタッチプロビジョニング）を使用した Management Center へのデバイスの追加

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

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

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

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

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

ゼロタッチプロビジョニングは、以下のモデルでのみサポートされます。

- Firepower 1010
- Firepower 1100
- Firepower 2100
- 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。ゼロタッチプロビジョニング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、設定に応じてゼロタッチプロビジョニング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。ゼロタッチプロビジョニング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。
- 新しいデバイスに割り当てることができるように、少なくとも1つのアクセスコントロールポリシーがManagement Centerに設定されていることを確認します。CDOを使用してポリシーを追加することはできません。
- デバイスにパブリックIPアドレスまたはFQDNがない場合、または管理インターフェイスを使用する場合は、Management CenterのパブリックIPアドレス/FQDNを設定し（Management Center管理インターフェイスのIPアドレスと異なる場合。たとえば、NATの背後にある場合）、デバイスが管理接続を開始できるようにします。[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。この手順中にCDOでパブリックIPアドレス/FQDNを設定することもできます。
- 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** シリアル番号を使用してデバイスを初めて追加するときは、次の前提条件を満たしている必要があります。初回以降は、スキップして、CDOにデバイスを直接追加できます。

- Management Center で、[デバイス (Devices)] > [デバイス管理 (Device Management)] を選びます。
- [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。
- プロビジョニング方式の [シリアル番号 (Serial Number)] をクリックします。

図 11: シリアル番号でデバイスを追加

Add Device ?

Select the Provisioning Method:

Registration Key Serial Number

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

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

ⓘ Complete above prerequisites before registering

Cancel Launch CDO

- CDO アカウントを作成します。

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

まだアカウントがない場合は、次の手順を実行してください。

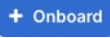
- Cisco Security Cloud (旧 SecureX) アカウントを作成します。作成方法については、[CDO のマニュアル](#)を参照してください。
 - CDO テナントをリクエストします。新しい CDO テナントのリクエストについては、[CDO のマニュアル](#)を参照してください。
- Management Center を Cisco Security Cloud (旧 SecureX) と統合します。リンクをクリックして、Management Center の [SecureXとの統合 (SecureX Integration)] ページを開きます。
 [SecureXの有効化 (Enable SecureX)] をクリックして別のブラウザタブを開き、Cisco Security Cloud アカウントにログインし、表示されたコードを確認します。このページがポップアップブロッカーによってブロックされていないことを確認してください。
 詳細については、『[Cisco Secure Firewall Management Center アドミニストレーションガイド](#)』の「Event Analysis Using External Tools」の章を参照してください。

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

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

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

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

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

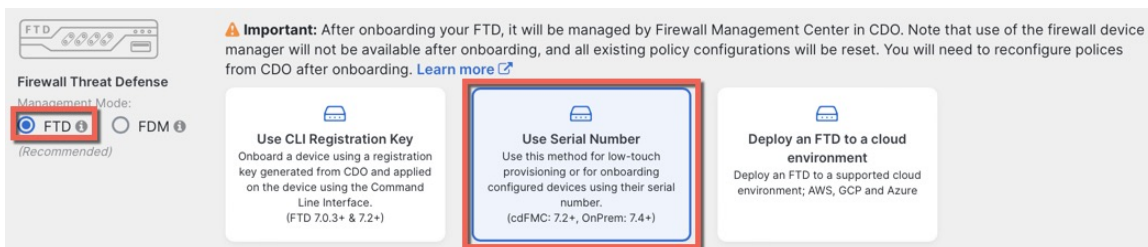
ステップ 3 [FTD] タイルをクリックします。

図 12: FTD タイル



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

図 13: シリアル番号を使用



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

図 14: FMCの選択

1 Select FMC

Select FMC ⓘ For more details, [Click Here](#)

Select

Cloud-Delivered FMC

Firepower Management Center (Recommended)

On-Prem FMCs (7.4+) ⓘ

FMC-Securex-Onboarding-1654149835633

FMC-Securex-Onboarding-1658238180734

FMC-Securex-Onboarding-1681247022490

FMC-Securex-Onboarding-1681762232392

FMC-Securex-Onboarding-1681830086235

Boulder FMC 740-48 1543

[+ Onboard On-Prem FMC](#)

2 Connection

3 Password Reset

4 Policy Assignment

5 Subscription License

6 Done

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

図 15: パブリック IP アドレス/FQDN

1 Select FMC

Select FMC ⓘ For more details, [Click Here](#)

Boulder FMC 740-48 1543

(IP/FQDN: fmc-techpubs.cisco.com)

ⓘ Specify the IP/FQDN value unless the FTD is publicly reachable, running a version older than 7.4 and connected with the data interface. Click [FMC Public IP](#) to configure FMC's FQDN.

[Next](#)

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

図 16: FMCパブリックIP/FQDNの設定

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

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

図 17: 接続

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

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

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

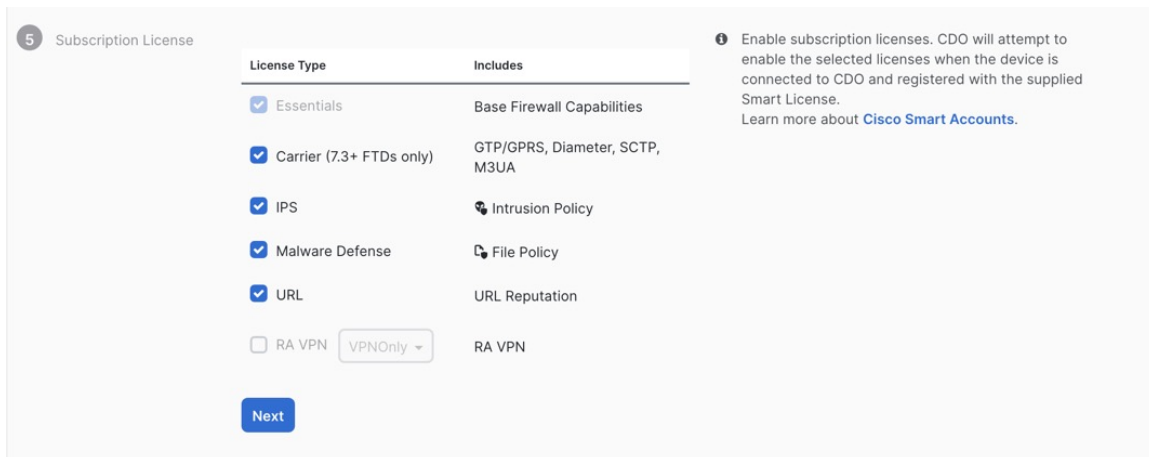
図 18: パスワードのリセット

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

図 19: ポリシー割り当て

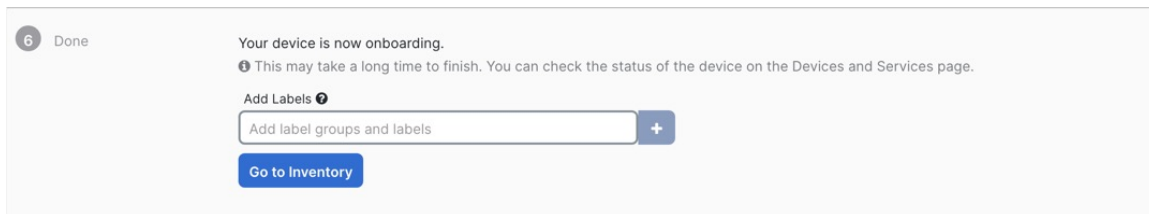
ステップ 9 [サブスクリプションライセンス (Subscription License)] で、デバイスのライセンスを選択します。[Next] をクリックします。

図 20: サブスクリプションライセンス



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

図 21: 終了



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

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

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

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

CDO を引き続き DDNS プロバイダーとして使用することも、後で Management Center の DDNS 設定を別の方式に変更することもできます。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（ロータッチプロビジョニング）登録の問題の解決（132 ページ）](#)」を参照してください。

Management Center へのシャーシの追加

Firepower 4100/9300 シャーシを 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。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 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マネージャの設定が完了します。[マルチインスタンスモードの有効化](#)を参照してください。マルチインスタンスモードを有効にしたら、[Management Center へのマルチインスタンスシャーシの追加](#)を参照してください。

手順

- ステップ 1** コンソールポートまたは SSH を使用して、シャーシ FXOS CLI に接続します。
ステップ 2 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*} : 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、少なくとも 1 台以上のデバイス (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 Management Center でも指定する任意の一意のワント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 (-) があります。このIDは、Management Center に登録する他のデバイスには使用できません。

- **Registration Key: *reg_key*** : シャーシを登録するときに 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 (-) 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 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 22: シャーシの追加

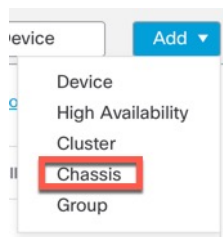


図 23: シャーシの追加

- 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、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、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。

Management Center からのデバイスの削除（登録解除）

デバイスを管理する必要がなくなった場合、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：

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

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

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

始める前に

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

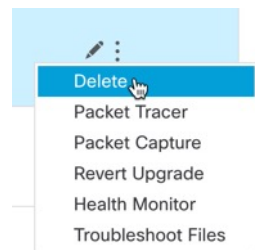
- デバイス設定をエクスポートします。 [デバイス設定のエクスポートとインポート（60 ページ）](#) を参照してください。

手順

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

ステップ2 登録を解除するデバイスの横にある **その他** (⋮) をクリックし、**[削除 (Delete)]** をクリックします。

図 24: 消去



ステップ3 デバイスの登録を解除することを確認します。

ステップ4 マネージャを変更できるようになりました。

- この 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、[登録キーを使用した Management Center へのデバイスの追加 \(32 ページ\)](#) を実行できます。それらをリセットする必要がある場合は、マネージャを新しいものであるかのように再設定できます。[新しい Management Center の特定 \(124 ページ\)](#) を参照してください。
- 新しい Management Center に登録する：[新しい Management Center の特定 \(124 ページ\)](#)。
- Device Manager に変更を加える：[Management Center から Device Manager への切り替え \(130 ページ\)](#)。
- 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）、Threat Defense で管理接続を切断するには、Threat Defense の CLI から **configure manager delete** コマンドを使用します。



デバイス グループの追加

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

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

手順

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

- ステップ2** [追加 (Add)] ドロップダウンメニューから、[グループの追加 (Add Group)] を選択します。
- 既存のグループを編集するには、編集するグループの[編集 (Edit)] () をクリックします。
- ステップ3** 名前を入力します。
- ステップ4** [使用可能なデバイス (Available Devices)] から、デバイス グループに追加するデバイスを1つ以上選択します。複数のデバイスを選択する場合は、Ctrl または Shift キーを押しながらクリックします。
- ステップ5** [追加 (Add)] をクリックして、選択したデバイスをデバイス グループに追加します。
- ステップ6** 必要に応じて、デバイスグループからデバイスを削除するには、削除するデバイスの横にある[削除 (Delete)] () をクリックします。
- ステップ7** [OK] をクリックして、デバイス グループを追加します。

デバイスのシャットダウンまたは再起動



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

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



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

手順

- ステップ1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ2** 再起動するデバイスの横にある[編集 (Edit)] () をクリックします。
- ステップ3** [デバイス (Device)] をクリックします。
- ステップ4** デバイスを再起動するには、次の手順を実行します。
- [デバイスの再起動 (Restart Device)] () をクリックします。
 - プロンプトが表示されたら、デバイスを再起動することを確認します。
- ステップ5** デバイスをシャットダウンするには、次の手順を実行します。

- a) [システム (System)]セクションで[デバイスのシャットダウン (Shut Down Device)] (⊗) をクリックします。
- b) プロンプトが表示されたら、デバイスのシャットダウンを確認します。
- c) コンソールからファイアウォールに接続している場合は、ファイアウォールがシャットダウンするときにシステムプロンプトをモニターします。次のプロンプトが表示されます。

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

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

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

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。

デバイス設定の構成

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

- [表示単位 (View By)]: このオプションを使用して、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。

- [デバイスの状態 (Device State)] : 状態に基づいてデバイスを表示することもできます。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。
- [検索 (Search)] : デバイス名、ホスト名、または IP アドレスを指定して、設定済みのデバイスを検索できます。
- [オプションの追加 (Add options)] : デバイス、高可用性ペア、クラスタ、およびグループを追加できます。
- 編集およびその他のアクション : 設定された各デバイスに対して、[編集 (Edit)] (✎) アイコンを使用してデバイスのパラメータと属性を編集します。その他 (⋮) アイコンをクリックして、他のアクションを実行します。
 - [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。
 - [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。
 - [ヘルスマニター (Health Monitor)] : デバイスのヘルスマニタリングページに移動します。
 - [トラブルシューティングファイル (Troubleshooting Files)] : レポートに含めるデータのタイプを選択できるトラブルシューティング ファイルを生成します。
 - Firepower 4100/9300 シリーズ デバイスの場合は、Chassis Manager Web インターフェイスへのリンク。

デバイスをクリックすると、いくつかのタブがあるデバイスのプロパティページが表示されます。タブを使用してデバイス情報を表示し、ルーティング、インターフェイス、インラインセット、および DHCP を設定できます。

全般設定の編集

[デバイス (Device)] タブの [全般 (General)] セクションには、以下の表に記載された設定が表示されます。

図 25: 一般

表 2: [全般 (General)] セクションテーブルのフィールド

フィールド	説明
名前 (Name)	Management Center でのデバイスの表示名。
パケット転送 (Transfer Packets)	管理対象デバイスがイベントを含むパケット データを Management Center に送信するかどうかを表示します。
トラブルシューティング (Troubleshoot)	トラブルシューティングファイルを生成およびダウンロードできます。また、CLI コマンド出力も表示できます。 トラブルシューティングファイルの生成 (53 ページ) および CLI 出力の表示 (56 ページ) を参照してください。
モード (Mode)	デバイスの管理インターフェイスのモード ([ルーテッド (routed)] または [トランスペアレント (transparent)]) を表示します。
コンプライアンスモード (Compliance Mode)	デバイスのセキュリティ認定準拠が表示されます。有効な値は、CC、UCAPL および None です。
パフォーマンスプロファイル (Performance Profile)	プラットフォーム設定ポリシーで設定された、デバイスのコア割り当てパフォーマンスプロファイルが表示されます。
TLS 暗号化アクセラレーション: (TLS Crypto Acceleration:)	TLS 暗号化アクセラレーションが有効か無効かを示します。
デバイス設定 (Device Configuration)	構成をコピー、エクスポート、またはインポートできます。 別のデバイスへの構成のコピー (58 ページ) および デバイス設定のエクスポートとインポート (60 ページ) を参照してください。

フィールド	説明
オンボーディング方式 (OnBoarding Method)	デバイスが登録キーを使用して登録されたか、シリアル番号 (ゼロタッチプロビジョニング) を使用して登録されたかを示します。

これらの設定の一部は、このセクションから編集できます。

手順

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

ステップ 2 変更するデバイスの横にある [編集 (Edit)] (✎) をクリックします。

ステップ 3 [Device] をクリックします。

ステップ 4 [General] セクションで、[編集 (Edit)] (✎) をクリックします。

- [Name] に、管理対象デバイスの名前を入力します。
- パケットデータをイベントと一緒に Management Center に保存できるようにするには、[パケットの転送 (Transfer Packets)] チェックボックスをオンにします。
- [Force Deploy] をクリックし、デバイスに現在のポリシーとデバイス設定の展開を強制します。

(注) 強制展開は、Threat Defense に展開されるポリシールールの完全な生成をともなうため、通常の展開よりも時間がかかります。

ステップ 5 [トラブルシューティング (Troubleshooting)] アクションについては、[トラブルシューティング ファイルの生成 \(53 ページ\)](#) および [CLI 出力の表示 \(56 ページ\)](#) を参照してください。

ステップ 6 [デバイス構成 (Device Configuration)] アクションについては、[別のデバイスへの構成のコピー \(58 ページ\)](#) および [デバイス設定のエクスポートとインポート \(60 ページ\)](#) を参照してください。

ステップ 7 [Deploy] をクリックします。

次のタスク

- 設定変更を展開します [設定変更の展開](#) を参照してください。

トラブルシューティング ファイルの生成

各デバイスとすべてのクラスタノードのトラブルシューティング ファイルを生成およびダウンロードできます。クラスタの場合、すべてのファイルを単一の圧縮ファイルとしてダウンロードできます。クラスタノードのクラスタのクラスタログを含めることもできます。

または、[デバイス (Devices)]>[デバイス管理 (Device Management)]>その他 (⋮) >[トラブルシューティング ファイル (Troubleshoot Files)] メニューからファイル生成をトリガーできます。

手順

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

ステップ2 表示するデバイスまたはクラスタの横にある [編集 (Edit)] (✎) をクリックします。

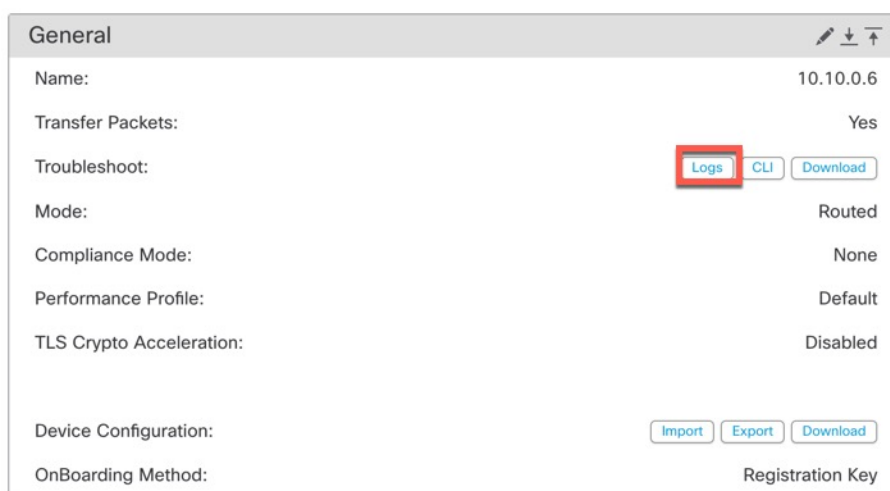
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ3 [デバイス (Device)]または[クラスタ (Cluster)]をクリックします。

ステップ4 デバイスまたはすべてのクラスタノードのログを生成します。

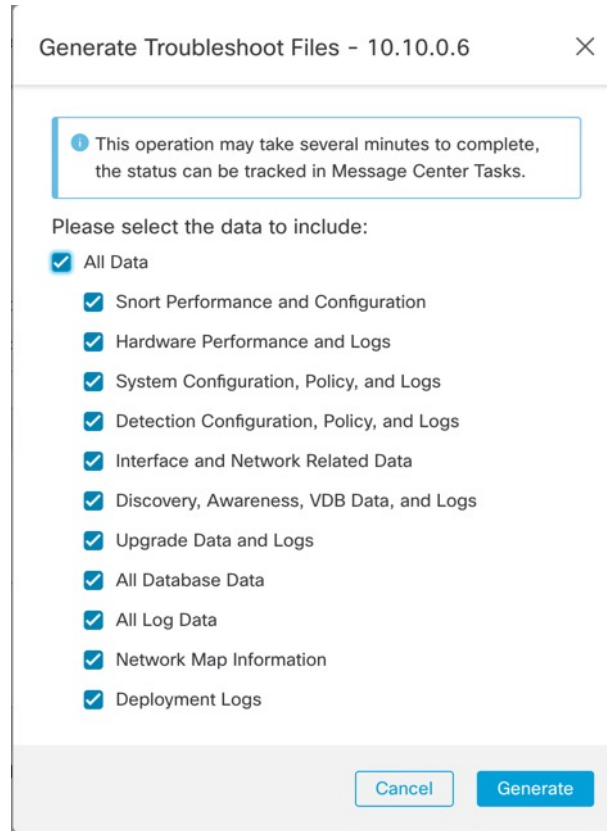
a) [全般 (General)]>[トラブルシュート (Troubleshoot)]セクションで、[ログ (Logs)]をクリックします。

図 26: ログ



b) 含めるログを選択するように求められます。クラスタの場合、[デバイス (Device)]で、[すべてのデバイス (All Devices)]または個々のノードを選択できます。クラスタには、使用可能な**クラスタログ**もあります。

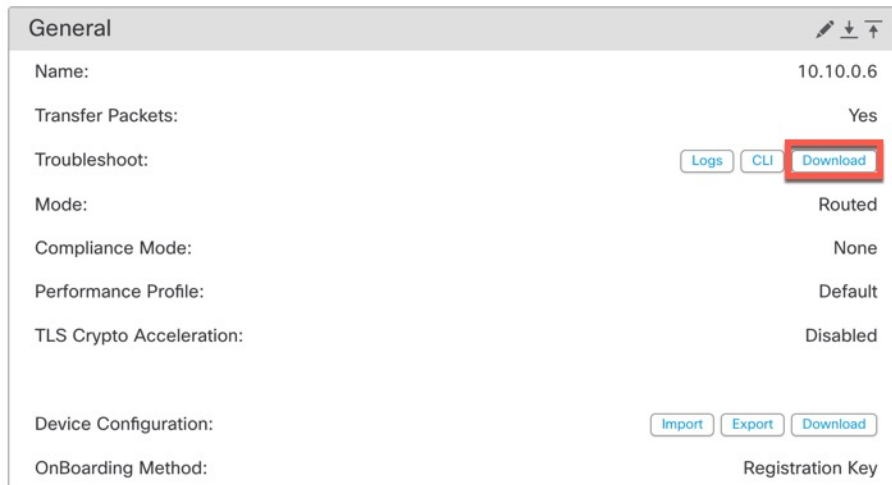
図 27: トラブルシューティング ファイルの生成



c) [生成 (Generate)]をクリックします。

ステップ 5 生成されたログをダウンロードするには、[全般 (General)]>[トラブルシュート (Troubleshoot)]セクションで、[ダウンロード (Download)]をクリックします。

図 28: ダウンロード



ログがコンピュータにダウンロードされます。

CLI 出力の表示

デバイスまたはクラスタのトラブルシューティングに役立つ一連の定義済みCLI出力を表示できます。任意の **show** コマンドを入力して、出力を確認することもできます。

デバイスの場合、以下のコマンドが実行されます。

- **show version**
- **show asp drop**
- **show counters**
- **show int ip brief**
- **show blocks**
- **show cpu detailed**

クラスタまたはクラスタノードの場合：

- **show running-config cluster**
- **show cluster info**
- **show cluster info health**
- **show cluster info transport cp**
- **show version**
- **show asp drop**
- **show counters**
- **show arp**
- **show int ip brief**
- **show blocks**
- **show cpu detailed**
- **show interface *ccl_interface***
- **ping *ccl_ip* size *ccl_mtu* repeat 2**

手順

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

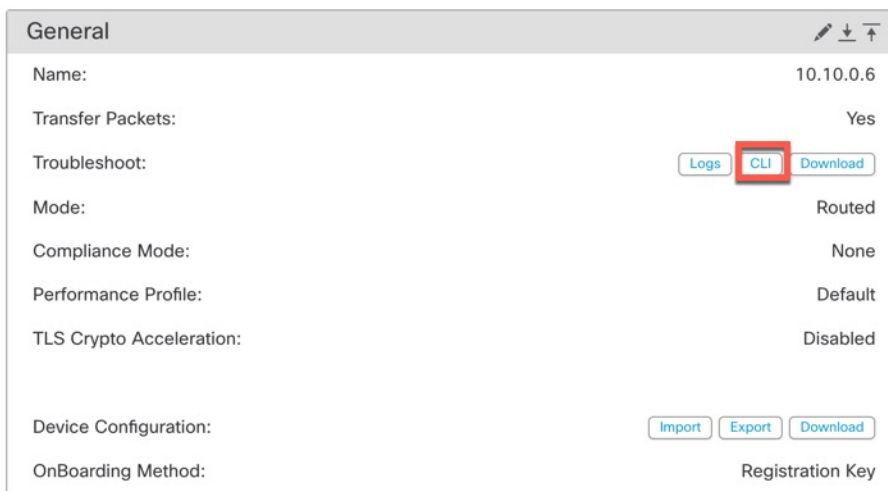
ステップ 2 表示するデバイスまたはクラスタの横にある [編集 (Edit)] (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス (Device)]または[クラスター (Cluster)]をクリックします。

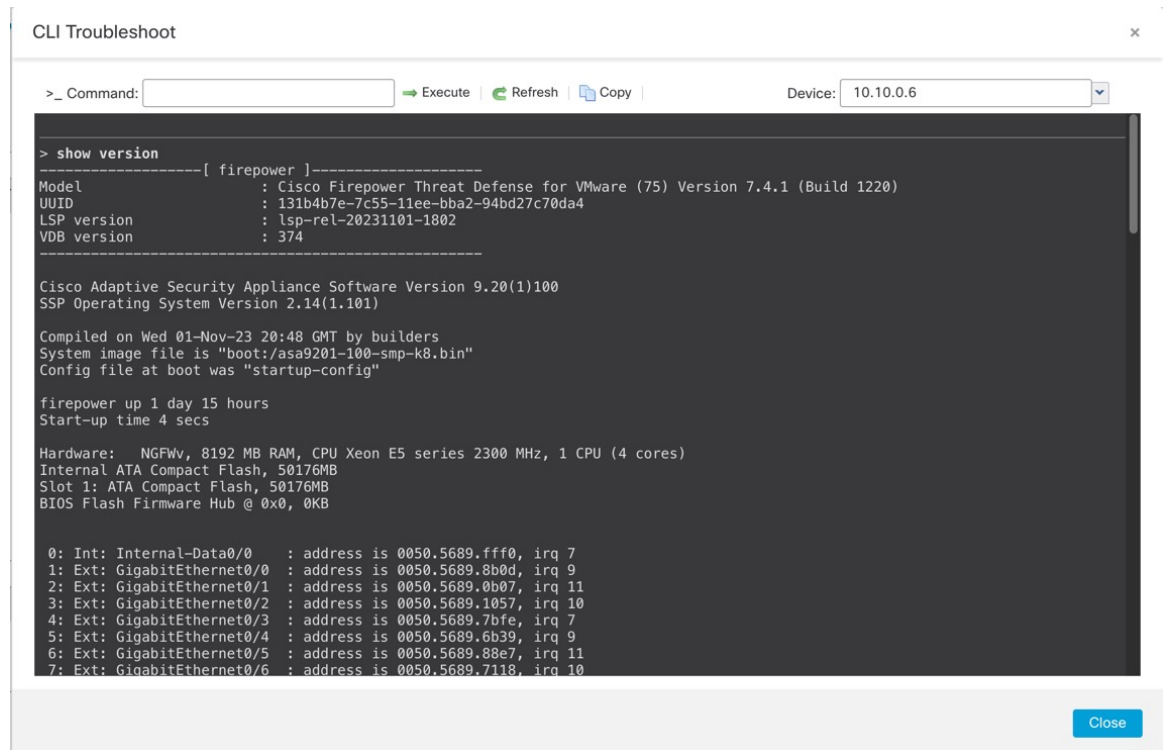
ステップ 4 [全般 (General)]>[トラブルシューティング (Troubleshoot)]セクションで、[CLI]をクリックします。

図 29: CLI



[CLIのトラブルシューティング (CLI Troubleshoot)] ダイアログボックスが表示され、事前定義された CLI が実行されます。

図 30: CLI のトラブルシュート



ステップ 5 [CLI のトラブルシュート (CLI Troubleshoot)] ダイアログボックスでは、次のタスクを実行できます。

- [コマンド (Command)] フィールドに **show** コマンドを入力して、[実行 (Execute)] をクリックします。新しいコマンド出力がウィンドウに追加されます。
- [更新 (Refresh)] をクリックして、定義済みの CLI を再実行します。
- [コピー (Copy)] をクリックし、クリップボードに出力をコピーします。
- クラスタの場合は、[デバイス (Device)] ドロップダウンリストから別のノードを選択します。

ステップ 6 [閉じる (Close)] をクリックします。

別のデバイスへの構成のコピー

新しいデバイスをネットワークに展開する場合、新しいデバイスを手動で再設定する代わりに、事前設定されているデバイスの設定とポリシーを簡単にコピーすることができます。

始める前に

次の項目を確認します。

- 送信元と宛先の Threat Defense デバイスが同じモデルであり、同じバージョンのソフトウェアを実行している。
- 送信元がスタンドアロン Secure Firewall Threat Defense デバイスまたは Secure Firewall Threat Defense 高可用性ペアである。
- 宛先のデバイスがスタンドアロン Threat Defense デバイスである。
- 送信元と宛先の Threat Defense デバイスに同じ数の物理インターフェイスがある。
- 送信元と宛先の Threat Defense デバイスが同じ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）になっている。
- 送信元と宛先の Threat Defense デバイスが同じセキュリティ認定コンプライアンス モードになっている。
- 送信元と宛先の Threat Defense デバイスが同じドメインにある。
- 送信元または宛先 Threat Defense デバイスのいずれでも設定の展開が進行中ではない。

手順

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

ステップ 2 変更するデバイスの横にある [編集 (Edit)] (✎) をクリックします。

ステップ 3 [デバイス (Device)] をクリックします。

ステップ 4 [全般 (General)] セクションで、次のいずれかの操作を実行します。

- [デバイス構成の取得 (Get Device Configuration)] (↓) をクリックして、別のデバイスのデバイス設定を新しいデバイスにコピーします。[デバイス設定の取得 (Get Device Configuration)] ページの [デバイスの選択 (Select Device)] ドロップダウンリストで、送信元デバイスを選択します。
- [デバイス構成のプッシュ (Push Device Configuration)] (↑) をクリックして、現在のデバイスのデバイス設定を新しいデバイスにコピーします。[デバイス設定のプッシュ (Push Device Configuration)] ページの [ターゲットデバイス (Target Device)] ドロップダウンリストで、設定をコピーする宛先を選択します。

ステップ 5 (オプション) [共有ポリシーの設定を含める (Include shared policies configuration)] チェックボックスをオンにして、ポリシーをコピーします。

AC ポリシー、NAT、プラットフォーム設定、および FlexConfig ポリシーなどの共有ポリシーは、複数のデバイス間で共有できます。

ステップ 6 [OK] をクリックします。

デバイス設定のコピータスクのステータスは、メッセージセンターの [タスク (Tasks)] でモニターできます。

デバイス設定のコピー タスクが開始されると、ターゲット デバイスの設定が削除され、送信元デバイスの設定が宛先のデバイスにコピーされます。



警告 デバイス設定のコピー タスクの完了後に、ターゲット デバイスを元の設定に戻すことはできません。

デバイス設定のエクスポートとインポート

[デバイス (Device)] ページで設定可能な、次のようなデバイス固有の設定をすべてエクスポートできます。

- インターフェイス
- インラインセット
- ルーティング
- DHCP
- VTEP
- 関連オブジェクト

次の使用例で、同じデバイスに保存された設定をインポートできます。

- 別の Management Center へのデバイスの移動：最初に元の Management Center からデバイスを削除してから、新しい Management Center にデバイスを追加します。これで保存された設定をインポートできます。
- ドメイン間でのデバイスの移動：ドメイン間でデバイスを移動する場合、サポートするオブジェクト（セキュリティゾーンのインターフェイスグループなど）が新しいドメインに存在しないため、一部のデバイス固有の設定が保持されません。ドメインの移動後に設定をインポートすると、そのドメインに必要なオブジェクトが作成され、デバイス設定が復元されます。
- 古い設定の復元：デバイスの動作に悪影響を与える変更を展開した場合は、既知の動作設定のバックアップコピーをインポートして、以前の動作状態を復元できます。
- デバイスの再登録：デバイスを Management Center から削除した後で追加し直す場合は、保存した設定をインポートできます。

次のガイドラインを参照してください。

- 設定は同じデバイスにのみインポートできます（UUID が一致する必要があります）。同じモデルであっても、設定を別のデバイスにインポートすることはできません。
- エクスポートとインポートの間に、デバイスで実行されているバージョンを変更しないでください。バージョンは一致する必要があります。

- 異なる Management Center にデバイスを移動する場合、ターゲットの Management Center バージョンは、ソースバージョンと同じである必要があります。
- オブジェクトが存在しない場合は作成されます。オブジェクトが存在するが値が異なる場合は、以下を参照してください。

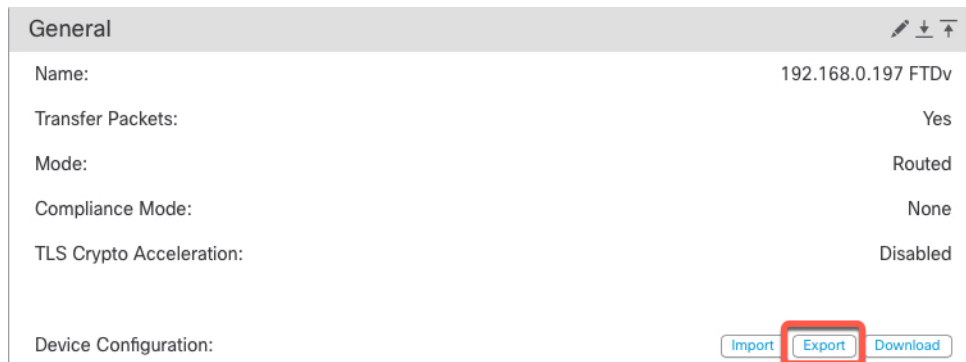
表 3: オブジェクトのインポートアクション

シナリオ	インポートアクション
同じ名前と値のオブジェクトが存在する。	既存のオブジェクトを再利用します。
同じ名前でも値が異なるオブジェクトが存在する。	<p>ネットワークおよびポートオブジェクト：このデバイスのオブジェクトオーバーライドを作成します。「オブジェクトのオーバーライド」を参照してください。</p> <p>インターフェイスオブジェクト：新しいオブジェクトを作成します。たとえば、タイプ（セキュリティゾーンまたはインターフェイスグループ）とインターフェイスタイプ（ルーテッドまたはスイッチドなど）の両方が一致しない場合、新しいオブジェクトが作成されます。</p> <p>他のすべてのオブジェクト：値が異なっても、既存のオブジェクトを再利用します。</p>
オブジェクトが存在しない。	新しいオブジェクトを作成します。

手順

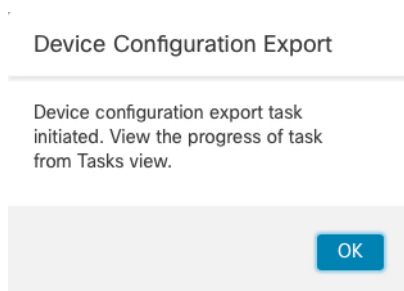
- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 編集するデバイスの横にある [編集 (Edit)] (✎) をクリックします。
- ステップ 3 [デバイス (Device)] をクリックします。
- ステップ 4 設定をエクスポートします (設定のエクスポート)。
 - a) [General (全般)] エリアで [エクスポート (Export)] をクリックします。

図 31: デバイス設定のエクスポート



エクスポートを確認するよう求められます。[OK] をクリックします。

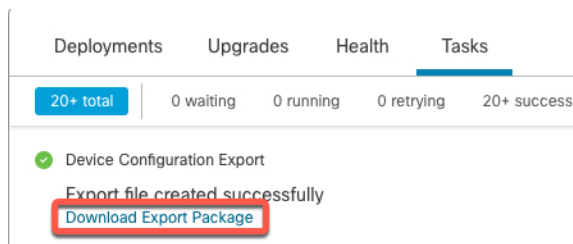
図 32: エクスポートの確認



[タスク (Tasks)] ページでエクスポートの進行状況を表示できます。

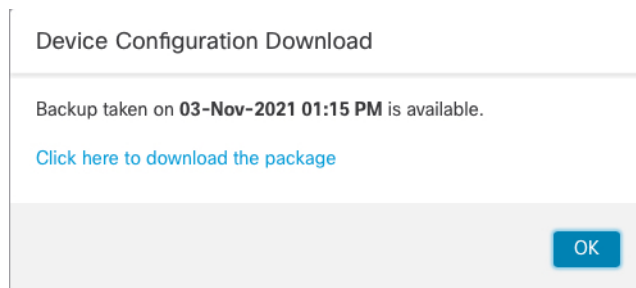
- b) [通知 (Notifications)]>[タスク (Tasks)] ページで、エクスポートが完了したことを確認します。[エクスポートパッケージのダウンロード (Download Export Package)] をクリックします。または、[全般 (General)] エリアの [ダウンロード (Download)] ボタンをクリックすることもできます。

図 33: タスクのエクスポート



パッケージをダウンロードするように求められます。[ここをクリックしてパッケージをダウンロード (Click here to download the package)] をクリックしてローカルでファイルを保存し、[OK] をクリックしてダイアログボックスを終了します。

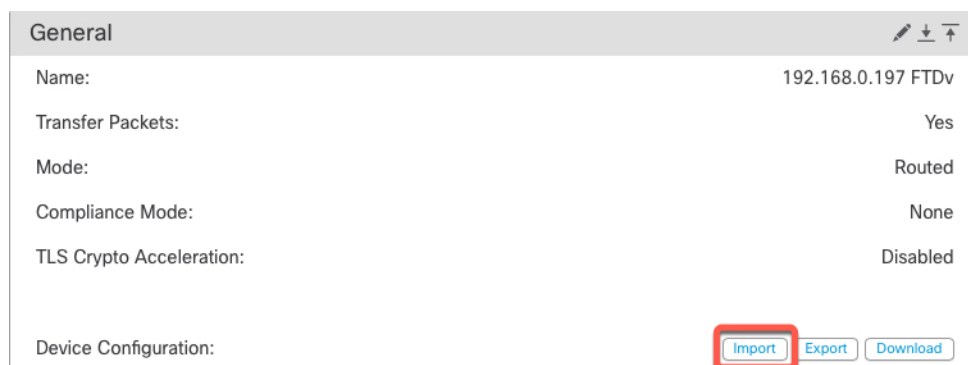
図 34: パッケージのダウンロード



ステップ 5 設定をインポートします。

- a) [General (全般)] エリアで [インポート (Import)] をクリックします。

図 35: デバイス設定のインポート



現在の設定が置き換えられることを確認するよう求められます。[はい (Yes)] をクリックし、設定パッケージに移動します (接尾辞 .sfo が付いています。このファイルはバックアップファイルや復元ファイルとは異なることに注意してください)。

図 36: パッケージのインポート

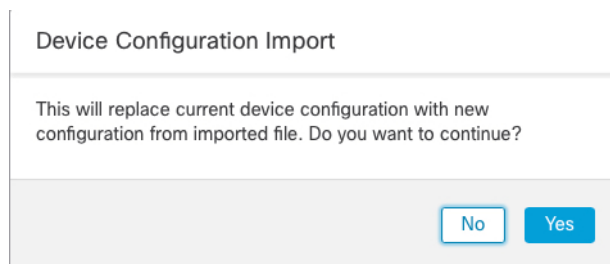
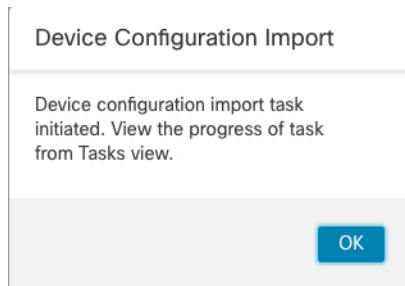


図 37: パッケージに移動



インポートを確認するよう求められます。[OK] をクリックします。

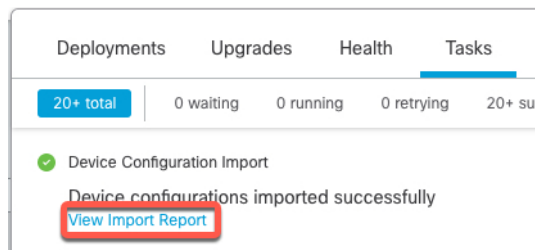
図 38: インポートの確認



[タスク (Tasks)] ページでインポートの進行状況を表示できます。

- b) インポートレポートを表示して、何がインポートされたかを確認します。インポートタスクの[通知 (Notifications)] > [タスク (Tasks)] ページで、[インポートレポートの表示 (View Import Report)] をクリックします。

図 39: インポートレポートの表示



[デバイス設定のインポートレポート (Device Configuration Import Reports)] ページには、利用可能なレポートへのリンクが表示されます。

Cisco Firepower Management Center

Device Configuration Import Reports

Device	Shared Policies	Device Configurations
0434ef00-15bb-11ec-bb94-93bdde3ad19d	Report does not exist	Device configurations import report

ライセンス設定の編集

[デバイス (Device)] ページの [ライセンス (License)] セクションでは、そのデバイスに対して有効になっているライセンスが表示されます。

Management Center で使用可能なライセンスがある場合、デバイスでそのライセンスを有効にすることができます。

手順

- ステップ1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ2 ライセンスを有効または無効にするデバイスの横にある[編集 (Edit)] (✎) をクリックします。
- ステップ3 [デバイス (Device)] をクリックします。
- ステップ4 [ライセンス (License)] セクションで、[編集 (Edit)] (✎) をクリックします。
- ステップ5 管理対象デバイスに対して有効または無効にするライセンスの横にあるチェックボックスをオンまたはオフにします。
- ステップ6 [保存 (Save)] をクリックします。

次のタスク

- 設定変更を展開します [設定変更の展開](#) を参照してください。

システム情報の表示

[デバイス (Device)] ページの [システム (System)] セクションには、次の表に示すように、システム情報の読み取り専用テーブルが表示されます。

デバイスをシャットダウンまたは再起動することもできます。

表 4: [システム (System)] セクションテーブルのフィールド

フィールド	説明
モデル	管理対象デバイスのモデル名と番号。
シリアル (Serial)	管理対象デバイスのシャーシのシリアル番号。
Time	デバイスの現在のシステム時刻。
タイムゾーン	タイムゾーンを表示します。
Version	管理対象デバイスに現在インストールされているソフトウェアのバージョン。
時刻ベースルール のタイムゾーン設定 (Time Zone setting for time-based rules)	デバイスのプラットフォーム設定で指定されたタイムゾーンでの、 デバイスの現在のシステム時刻。

検査エンジンの表示

[デバイス (Device)] ページの [検査エンジン (Inspection Engine)] セクションには、デバイスが Snort2 と Snort3 のどちらを使用しているのかが表示されます。検索エンジンを切り替えるには、[Cisco Secure Firewall Management Center Snort 3 Configuration Guide](#)を参照してください。

正常性情報の表示

[デバイス (Device)] ページの [正常性 (Health)] セクションには、以下の表に記載された情報が表示されます。

表 5: [ヘルス (Health)] セクション テーブルのフィールド

フィールド	説明
ステータス (Status)	デバイスの現在のヘルスステータスを表すアイコン。アイコンをクリックすると、アプライアンスのヘルス モニタが表示されます。
ポリシー	現在デバイスで展開されている、読み取り専用バージョンの正常性ポリシーへのリンク。
除外 (Excluded)	[正常性除外 (Health Exclude)] ページへのリンク。このページでは、正常性除外モジュールを有効化および無効化できます。

管理設定の編集

[管理 (Management)] エリアで管理設定を編集できます。

Management Center でのホスト名または IP アドレスの更新

(デバイスの CLI を使用するなどして) デバイスを Management Center に追加した後にそのデバイスのホスト名または IP アドレスを編集する場合は、次の手順を使用して管理側の Management Center のホスト名または IP アドレスを手動で更新する必要があります。

デバイスのデバイス管理 IP アドレスを変更するには、[Threat Defense 管理インターフェイスの CLI での変更 \(90 ページ\)](#) を参照してください。

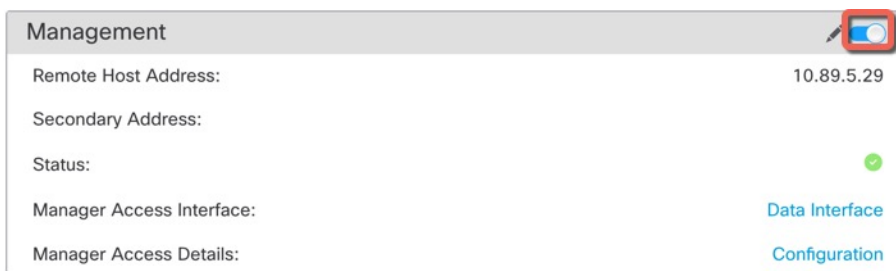
デバイスの登録時に NAT ID のみを使用した場合、IP はこのページに [NO-IP] として表示され、IP アドレス/ホスト名を更新する必要はありません。

ゼロタッチプロビジョニングを使用して外部インターフェイスでデバイスを登録した場合、ホスト名は一致する DDNS 設定とともに自動的に生成されます。この場合、ホスト名は編集できません。

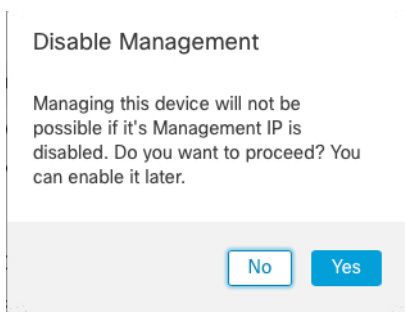
手順

- ステップ 1 [デバイス (Devices)]> [デバイス管理 (Device Management)] を選択します。
- ステップ 2 管理オプションを変更するデバイスの横にある [編集 (Edit)] (✎) をクリックします。
- ステップ 3 [Device] をクリックし、[Management] 領域を表示します。
- ステップ 4 スライダをクリックして管理を一時的に無効にすることで、(☐) を無効化します。

図 40: 管理を無効にする



管理の無効化を続行するように求められます。[Yes] をクリックします。



管理を無効化すると、Management Center とデバイス間の接続がブロックされますが、Management Center からデバイスは削除されません。

- ステップ 5 [リモートホストアドレス (Remote Host Address)] の IP アドレスおよびオプションの [セカンダリアドレス (Secondary Address)] (冗長データインターフェイスを使用する場合) または [編集 (Edit)] (✎) をクリックしてホスト名を編集します。

図 41: 管理アドレスの編集



ステップ 6 [管理 (Management)] ダイアログボックスの [リモートホストアドレス (Remote Host Address)] フィールドおよびオプションの [セカンダリアドレス (Secondary Address)] フィールドで名前または IP アドレスを変更し、[保存 (Save)] をクリックします。

セカンダリ マネージャ アクセス データ インターフェイスの使用については、[冗長マネージャ アクセス用データインターフェイスの設定 \(80 ページ\)](#) を参照してください。

図 42: 管理 IP アドレス

The screenshot shows a dialog box titled "Management" with a question mark icon in the top right corner. It contains two input fields: "Remote Host Address" with the value "10.89.5.29" and "Secondary Address" with the value "10.99.11.6". At the bottom, there are two buttons: "Cancel" and "Save".

ステップ 7 スライダをクリックして管理を再度有効 () にします。

図 43: 管理接続の有効化

The screenshot shows the "Management" dialog box with a toggle switch in the top right corner, which is now turned on (indicated by a red box around the switch). The "Remote Host Address" field contains "10.89.5.4". The "Secondary Address" field is empty. The "Status" field shows a green checkmark. The "Manager Access Interface" field is labeled "Management Interface".


Management Center と Threat Defense の両 IP アドレスの変更

Management Center と Threat Defense の IP アドレスを新しいネットワークに移動する場合は、両方を変更することをお勧めします。

手順

ステップ 1 管理接続を無効にします。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

- [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- デバイスの横にある [編集 (Edit)] () をクリックします。
- [Device] をクリックし、[Management] 領域を表示します。


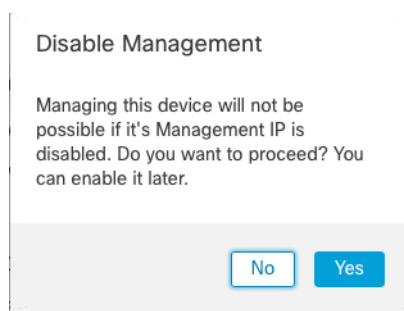
- d) スライダをクリックして管理を一時的に無効にすることで、 を無効化します。

図 44: 管理を無効にする



管理の無効化を続行するように求められます。[Yes] をクリックします。



ステップ 2 Management Center 内のデバイスの IP アドレスを新しいデバイスの IP アドレスに変更します。

デバイスの IP アドレスは後で変更します。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。


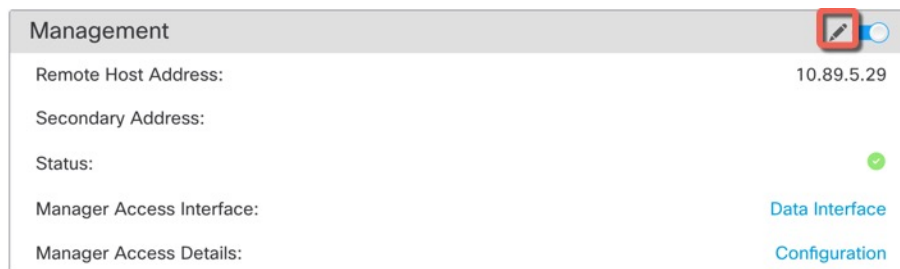
- a) [リモートホストアドレス (**Remote Host Address**)] の IP アドレスおよびオプションの [セカンダリアドレス (**Secondary Address**)] (冗長データインターフェイスを使用する場合) または [編集 (**Edit**)] () をクリックしてホスト名を編集します。

図 45: 管理アドレスの編集



- b) [管理 (Management)] ダイアログボックスの [リモートホストアドレス (**Remote Host Address**)] フィールドおよびオプションの [セカンダリアドレス (**Secondary Address**)] フィールドで名前または IP アドレスを変更し、[保存 (Save)] をクリックします。

図 46: 管理 IP アドレス

ステップ 3 Management Center の IP アドレスを変更してください。

注意 Management Center インターフェイスを変更する場合は十分にご注意ください。設定エラーのために再接続できない場合は、Management Center コンソールポートにアクセスして、Linux シェルでネットワーク設定を再設定する必要があります。この操作では、Cisco TAC に連絡する必要があります。

- システム (⚙) > [構成 (Configuration)] を選択し、次に [管理インターフェイス (Management Interfaces)] を選択します。
- [インターフェイス (Interfaces)] エリアで、設定するインターフェイスの横にある [編集 (Edit)] をクリックします。
- IP アドレスを変更し、[保存 (Save)] をクリックします。

ステップ 4 デバイスのマネージャ IP アドレスを変更します。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

- Threat Defense CLI で、Management Center 識別子を表示します。

show managers

例 :

```
> 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
```

- Management Center IP アドレスまたはホスト名を編集します。

configure manager edit identifier {hostname {ip_address | hostname} | displayname display_name}

Management Center が **DONTRESOLVE** と NAT ID によって最初に識別された場合、このコマンドを使用して値をホスト名または IP アドレスに変更できます。IP アドレスまたはホスト名を **DONTRESOLVE** に変更することはできません。

例 :

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

ステップ 5 コンソールポートでマネージャ アクセス インターフェイスの IP アドレスを変更します。
高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。
専用管理インターフェイスを使用している場合：

configure network ipv4

configure network ipv6

専用管理インターフェイスを使用している場合：

configure network management-data-interface disable

configure network management-data-interface


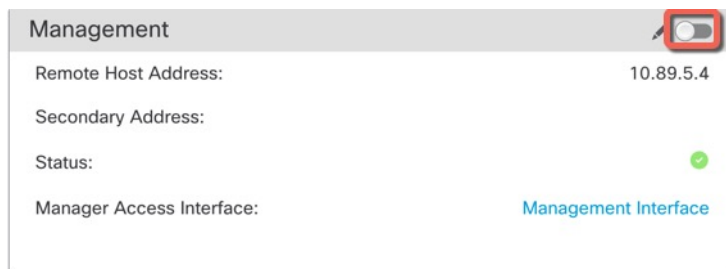
ステップ 6 スライダをクリックして管理を再度有効 () にします。
高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

図 47: 管理接続の有効化



ステップ 7 (マネージャアクセスにデータインターフェイスを使用している場合) Management Center でデータインターフェイス設定を更新します。

高可用性ペアの場合は、両方のユニットでこの手順を実行します。

- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [管理 (Management)] > [マネージャアクセス - 構成詳細 (Manager Access - Configuration Details)] を選択し、[更新 (Refresh)] をクリックします。
- b) [デバイス (Devices)] > [デバイス管理 (Device Management)] > [インターフェイス (Interfaces)] を選択し、新しいアドレスと一致するように IP アドレスを設定します。
- c) [マネージャアクセス - 構成詳細 (Manager Access - Configuration Details)] [FMCアクセス - 構成詳細 (FMC Access - Configuration Details)] ダイアログボックスに戻り、[確認 (Acknowledge)] をクリックして展開ブロックを削除します。

ステップ 8 管理接続が再確立されたことを確認します。

Management Center で、[Devices] [Device Management] [Device] [Management] [Manager Access - Configuration Details] [FMC Access - Configuration Details] [Connection Status] ページで管理接続ステータスを確認します。

管理接続のステータスを表示するには、Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

次のステータスは、データインターフェイスの接続が成功したことを示し、内部の「tap_nlp」インターフェイスを示しています。

図 48: 接続ステータス

The screenshot shows a web interface titled "Manager access - Configuration Details". Below the title, it states "Manager access configuration on device is in sync with the manager." There are three tabs: "Configuration", "CLI Output", and "Connection Status", with "Connection Status" being the active tab. Below the tabs, it says "sftunnel-status-brief command output from Firewall Threat Defense" and includes a "[Refresh]" link. The main content is a terminal window showing the following output:

```
> sftunnel-status-brief
PEER:10.89.5.35
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Registration: Completed.
IPv4 Connection to peer '10.89.5.35' Start Time: Mon May 23 22:55:01 2022 UTC
Heartbeat Send Time: Mon May 23 22:56:21 2022 UTC
Heartbeat Received Time: Mon May 23 22:55:58 2022 UTC
Last disconnect time : Mon May 23 22:54:39 2022 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

At the bottom right of the terminal window, there is a "Close" button.

ステップ 9 (高可用性 Management Center ペアの場合) セカンダリ Management Center で設定変更を繰り返します。

- a) セカンダリ Management Center IP アドレスを変更します。
- b) 両方のユニットで新しいピアアドレスを指定します。
- c) セカンダリユニットをアクティブユニットにします。
- d) デバイスの管理接続を無効にします。
- e) Management Center でデバイスの IP アドレスを変更します。
- f) 管理接続を再度有効にします。

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

専用の管理インターフェイスまたはデータインターフェイスから Threat Defense を管理できません。デバイスを Management Center に追加した後にマネージャアクセスインターフェイスを変更する場合は、次の手順に従って管理インターフェイスからデータインターフェイスに移行します。逆の方向に移行するには、[マネージャアクセスインターフェイスをデータから管理に変更する \(77 ページ\)](#) を参照してください。

管理からデータへのマネージャアクセスの移行を開始すると、Management Center は Threat Defense への展開時にブロックを適用します。ブロックを削除するには、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ます。

次の手順を参照して、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、その他の必要な設定も構成します。

始める前に

ハイアベイラビリティペアの場合、特に明記されていない限り、すべての手順はアクティブユニットでのみ実行します。設定の変更が展開されると、スタンバイユニットはアクティブユニットから設定およびその他のステート情報を同期します。

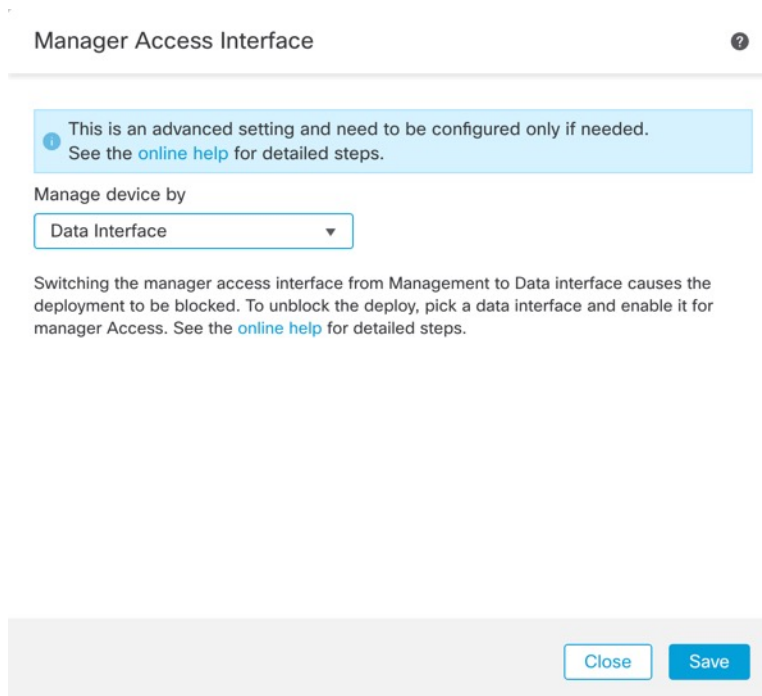
手順

ステップ 1 インターフェイスの移行を開始します。

- a) [デバイス (Devices)] > [デバイス管理 (Device Manageme)] ページで、デバイスの [編集 (Edit)] (✎) をクリックします。
- b) [デバイス (Device)] > [管理 (Management)] セクションに移動し、[マネージャ アクセス インターフェイス (Manager Access Interface)] [FMC アクセス インターフェイス (FMC Access Interface)] のリンクをクリックします。 >

[マネージャ アクセス インターフェイス (Manager Access Interface)] [FMC アクセス インターフェイス (FMC Access Interface)] フィールドには、現在の管理インターフェイスが表示されます。リンクをクリックしたら、[デバイスの管理 (Manage device by)] ドロップダウンリストで新しいインターフェイスタイプである [データインターフェイス (Data Interface)] を選択します。

図 49: マネージャ アクセス インターフェイス



- c) [保存 (Save)] をクリックします。

データインターフェイスでマネージャアクセスを有効にするには、残りの手順を完了する必要があります。[管理 (Management)] 領域には、[マネージャ アクセス インターフェイス : データインターフェイス (Manager Access Interface: Management Interface)] [FMC アクセスインターフェイス : データインターフェイス (FMC Access Interface: Management Interface)] と、[マネージャアクセスの詳細 : 構成 (Manager Access Details: Configuration)] [FMCアクセスの詳細 : 構成 (FMC Access Details: Configuration)] が表示されます。

図 50: マネージャアクセス



[構成 (Configuration)] をクリックすると、[マネージャアクセス - 構成の詳細 (Manager Access - Configuration Details)] [FMCアクセス - 構成の詳細 (FMC Access - Configuration Details)] ダイアログボックスが開きます。[マネージャアクセスモード (Manager Access Mode)] [FMCアクセスモード (FMC Access Mode)] は、展開保留状態を示しています。

ステップ 2 [デバイス (Devices)]>[デバイス管理 (Device Management)]>[インターフェイス (Interfaces)]>[物理インターフェイスの編集 (Edit Physical Interface)]>[マネージャアクセス (Manager Access)] [FMCアクセス (FMC Access)] ページで、データインターフェイスでのマネージャアクセスを有効にします。 > > >

[ルーテッドモードのインターフェイスの設定](#)を参照してください。マネージャアクセスは1つのルーテッドデータ インターフェイスとオプションのセカンダリインターフェイスで有効にできます。これらのインターフェイスが名前と IP アドレスで完全に構成され、有効になっていることを確認してください。

冗長性のためにセカンダリインターフェイスを使用する場合は、必要な追加構成について[冗長マネージャアクセス用データインターフェイスの設定 \(80 ページ\)](#)を参照してください。

ステップ 3 (任意) インターフェイスに DHCP を使用する場合は、[デバイス (Devices)]>[デバイス管理 (Device Management)]>[DHCP]>[DDNS] ページで Web タイプ DDNS 方式を有効にします。

[ダイナミック DNS の設定](#)を参照してください。DDNS は、FTD の IP アドレスが変更された場合に Management Center が完全修飾ドメイン名 (FQDN) で Threat Defense に到達できるようにします。

ステップ 4 Threat Defense がデータインターフェイスを介して Management Center にルーティングできることを確認します。必要に応じて、[デバイス (Devices)]>[デバイス管理 (Device Management)]>[ルーティング (Routing)]>[スタティックルート (Static Route)]でスタティックルートを追加します。 > > >

[スタティック ルートの追加](#)を参照してください。

ステップ 5 (任意) プラットフォーム設定ポリシーで DNS を構成し、[デバイス (Devices)]>[プラットフォーム設定 (Platform Settings)]>[DNS]でこのデバイスに適用します。

[DNS](#)を参照してください。DDNS を使用する場合は DNS が必要です。セキュリティポリシーで FQDN に DNS を使用することもできます。

ステップ 6 (任意) 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の SSH を有効にし、[デバイス (Devices)]> [プラットフォーム設定 (Platform Settings)]>[セキュアシェル (Secure Shell)]でこのデバイスに適用します。

[SSH アクセスの確保](#)を参照してください。SSH はデータインターフェイスでデフォルトで有効になっていないため、SSH を使用して Threat Defense を管理する場合は、明示的に許可する必要があります。

ステップ 7 設定変更を展開します[設定変更の展開](#)を参照してください。

Management Center は、現在の管理インターフェイスを介して設定の変更を展開します。展開後、データインターフェイスを使用できるようになりましたが、管理への元の管理接続はアクティブなままです。

ステップ 8 Threat Defense CLI (できればコンソールポートから) で、静的 IP アドレスを使用するように管理インターフェイスを設定し、データインターフェイスを使用するようにゲートウェイを設定します。ハイアベイラビリティの場合は、両方のユニットでこの手順を実行します。

configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces

- **ip_address netmask** : 管理インターフェイスを使用する予定はありませんが、ゲートウェイを [データインターフェイス (data-interfaces)] に設定できるように、プライベートアドレスなどの静的 IP アドレスを設定する必要があります (次の箇条書きを参照)。
[data-interfaces] である必要があるデフォルトルートは、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、DHCP は使用できません。
- **data-interfaces** — 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。

管理インターフェイスのネットワーク設定を変更すると、SSHセッションが切断されるため、SSH 接続の代わりにコンソールポートを使用することをお勧めします。

ステップ 9 必要に応じて、データインターフェイスの Management Center に到達できるように Threat Defense のケーブルを再接続します。ハイアベイラビリティの場合は、両方のユニットでこの手順を実行します。

ステップ 10 Management Center で、管理接続を無効にし、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [管理 (Management)] セクションで Threat Defense の [リモートホストアドレス (Remote Host Address)] IP アドレスとオプションの [セカンダリアドレス (Secondary Address)] を更新して、接続を再度有効にします。

Management Center でのホスト名または IP アドレスの更新 (66 ページ) を参照してください。Threat Defense を Management Center に追加したときに Threat Defense ホスト名または NAT ID のみを使用した場合は、値を更新する必要はありません。ただし、接続を再開するには、管理接続を無効にしてから再度有効にする必要があります。

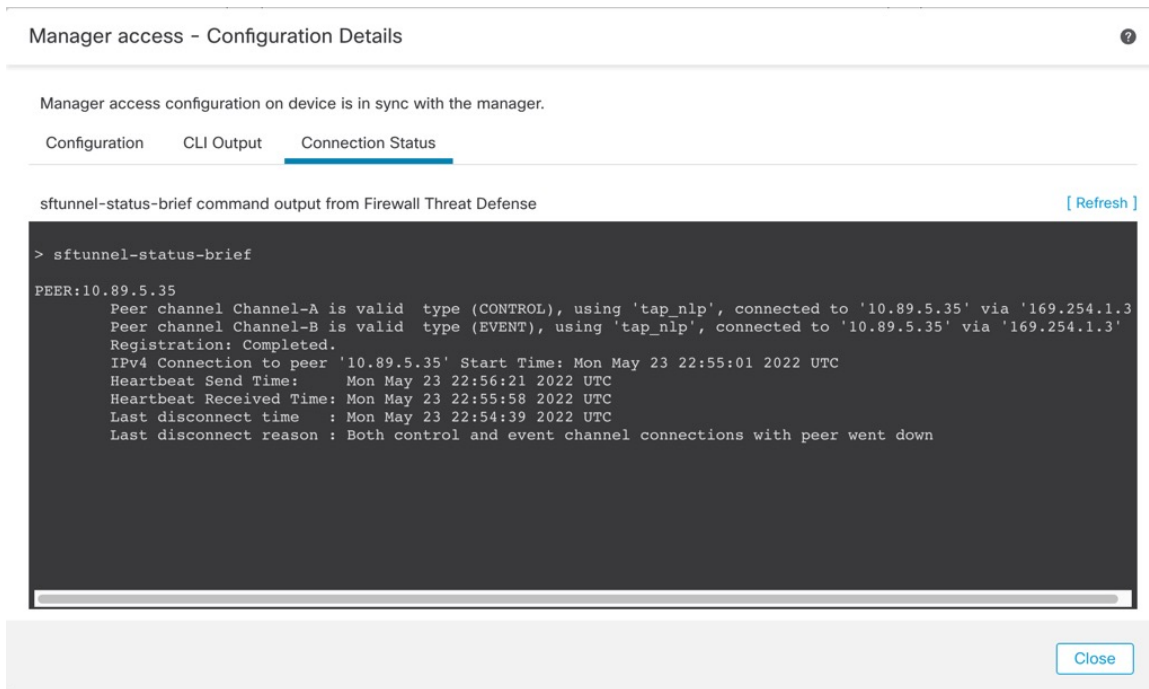
ステップ 11 管理接続が再確立されたことを確認します。

Management Center で、[Devices] [Device Management] [Device] [Management] [Manager Access - Configuration Details] [FMC Access - Configuration Details] [Connection Status] ページで管理接続ステータスを確認します。

管理接続のステータスを表示するには、Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

次のステータスは、データインターフェイスの接続が成功したことを示し、内部の「tap_nlp」インターフェイスを示しています。

図 51: 接続ステータス



接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。データインターフェイスでの管理接続のトラブルシューティング (102 ページ) を参照してください。

マネージャ アクセス インターフェイスをデータから管理に変更する

専用の管理インターフェイスまたはデータインターフェイスから Threat Defense を管理できます。デバイスを Management Center に追加した後にマネージャ アクセス インターフェイスを変更する場合は、次の手順に従ってデータインターフェイスから管理インターフェイスに移行します。逆の方向に移行するには、[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 \(72 ページ\)](#) を参照してください。

データから管理へのマネージャアクセスの移行を開始すると、Management Center は Threat Defense への展開時にブロックを適用します。ブロックを削除するには、データインターフェイスでマネージャアクセスを無効にする必要があります。

次の手順を参照して、データインターフェイスでマネージャアクセスを無効にし、その他の必要な設定も構成します。

始める前に

ハイアベイラビリティペアの場合、特に明記されていない限り、すべての手順はアクティブユニットでのみ実行します。設定の変更が展開されると、スタンバイユニットはアクティブユニットから設定およびその他のステート情報を同期します。

手順

ステップ1 インターフェイスの移行を開始します。

- a) [デバイス (Devices)]>[デバイス管理 (Device Manageme)]ページで、デバイスの [編集 (Edit)] (✎) をクリックします。
- b) [デバイス (Device)]>[管理 (Management)]セクションに移動し、[マネージャアクセスインターフェイス (Manager Access Interface)] [FMCアクセスインターフェイス (FMC Access Interface)]のリンクをクリックします。 >

[マネージャアクセスインターフェイス (Manager Access Interface)] [FMCアクセスインターフェイス (FMC Access Interface)]フィールドには、現在の管理インターフェイスが表示されます。リンクをクリックしたら、[デバイスの管理 (Manage device by)]ドロップダウンリストで新しいインターフェイスタイプである [管理インターフェイス (Management Interface)]を選択します。

図 52: マネージャアクセスインターフェイス

- c) [保存 (Save)]をクリックします。

管理インターフェイスでマネージャアクセスを有効にするには、残りの手順を完了する必要があります。[管理 (Management)]領域には、[マネージャアクセスインターフェイス : 管理インターフェイス (Manager Access Interface: Management Interface)] [FMCアクセスインターフェイス : 管理インターフェイス (FMC Access Interface: Management Interface)]と、[マネージャアクセスの詳細 : 構成 (Manager Access Details: Configuration)] [FMCアクセスの詳細 : 構成 (FMC Access Details: Configuration)]が表示されます。

図 53: マネージャアクセス



[構成 (Configuration)] をクリックすると、[マネージャアクセス - 構成の詳細 (Manager Access - Configuration Details)] [FMCアクセス - 構成の詳細 (FMC Access - Configuration Details)] ダイアログボックスが開きます。[マネージャアクセスモード (Manager Access Mode)] [FMCアクセスモード (FMC Access Mode)] は、展開保留状態を示しています。

ステップ 2 [デバイス (Devices)] > [デバイス管理 (Device Management)] > [インターフェイス (Interfaces)] > [物理インターフェイスの編集 (Edit Physical Interface)] > [マネージャアクセス (Manager Access)] ページで、データインターフェイスでのマネージャアクセスを無効にします。

[ルーテッドモードのインターフェイスの設定](#)を参照してください。この手順により、展開時のブロックが削除されます。

ステップ 3 まだ行っていない場合は、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の DNS 設定を構成し、[デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] > [DNS] でこのデバイスに適用します。

[DNS](#)を参照してください。データインターフェイスでマネージャアクセスを無効にする Management Center 展開では、ローカル DNS 設定が削除されます。その DNS サーバーがアクセスルールの FQDN などのセキュリティポリシーで使用されている場合は、Management Center を使用して DNS 設定を再適用する必要があります。

ステップ 4 設定変更を展開します [設定変更の展開](#)を参照してください。

Management Center は、現在のデータインターフェイスを介して設定の変更を展開します。

ステップ 5 必要に応じて、管理インターフェイスの Management Center に到達できるように Threat Defense のケーブルを再接続します。ハイアベイラビリティの場合は、両方のユニットでこの手順を実行します。

ステップ 6 Threat Defense CLI で、静的 IP アドレスまたは DHCP を使用して、管理インターフェイスの IP アドレスとゲートウェイを設定します。ハイアベイラビリティの場合は、両方のユニットでこの手順を実行します。

最初に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たとき、管理ゲートウェイはデータインターフェイスに設定されていました。これにより、バックプレーン経由で管理トラフィックが転送され、マネージャアクセス データ インターフェイスを介してルーティングできるようになりました。ここで、管理ネットワーク上のゲートウェイの IP アドレスを設定する必要があります。

スタティック IP アドレス :

```
configure network {ipv4 | ipv6} manual ip_address netmask gateway_ip
```

DHCP :

```
configure network {ipv4 | ipv6} dhcp
```

ステップ 7 Management Center で、管理接続を無効にし、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [管理 (Management)] セクションで Threat Defense の [リモートホストアドレス (Remote Host Address)] IP アドレスを更新してオプションの [セカンダリアドレス (Secondary Address)] を削除し、接続を再度有効にします。

[Management Center](#) でのホスト名または IP アドレスの更新 (66 ページ) を参照してください。Threat Defense を Management Center に追加したときに Threat Defense ホスト名または NAT ID のみを使用した場合は、値を更新する必要はありません。ただし、接続を再開するには、管理接続を無効にしてから再度有効にする必要があります。

ステップ 8 管理接続が再確立されたことを確認します。

Management Center で、[デバイス (Devices)] [デバイス管理 (Device Management)] [デバイス (Device)] [管理 (Management)] [ステータス (Status)] フィールドで管理接続ステータスを確認するか、Management Center で通知を表示します。> > >

管理接続のステータスを表示するには、Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。[データインターフェイスでの管理接続のトラブルシューティング \(102 ページ\)](#) を参照してください。

冗長マネージャアクセス用データインターフェイスの設定

マネージャアクセスにデータインターフェイスを使用する場合、プライマリインターフェイスがダウンしたときに管理機能を引き継ぐよう、セカンダリインターフェイスを構成できます。セカンダリインターフェイスは1つだけ構成できます。デバイスは、SLA モニタリングを使用して、スタティックルートの実行可能性と、両方のインターフェイスを含む ECMP ゾーンを追跡し、管理トラフィックで両方のインターフェイスが使用できるようにします。

ハイアベイラビリティはサポートされません。

始める前に

- セカンダリインターフェイスは、プライマリインターフェイスとは別のセキュリティゾーンにある必要があります。
- プライマリインターフェイスに適用されるのと同じすべての要件がセカンダリインターフェイスに適用されます。[管理のための Threat Defense データインターフェイスの使用について \(5 ページ\)](#) を参照してください。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Managem)] ページで、デバイスの [編集 (Edit)] (✎) をクリックします。

ステップ 2 セカンダリインターフェイスのマネージャアクセスを有効にします。

この設定は、インターフェイスの有効化、名前設定、セキュリティゾーンの設定、スタティック IPv4 アドレスの設定など、標準のインターフェイス設定に加えて行うものです。

- a) [インターフェイス (Interfaces)] > [物理インターフェイスの編集 (Edit Physical Interface)] > [マネージャアクセス (Manager Access)] を選択します。
- b) [このインターフェイス上の管理をマネージャに対して有効にする (Enable management on this interface for the Manager)] をオンにします。
- c) [OK] をクリックします。

どちらのインターフェイスも、インターフェイスリストに [(マネージャアクセス) ((Manager Access))] と表示されます。

図 54: インターフェイスリスト

Interface	Logical Name	Type	Security Zones
● Diagnostic1/1	diagnostic	Physical	
● Ethernet1/1 (Manager Access)	outside	Physical	outside
🔒 Ethernet1/2		Physical	
🔒 Ethernet1/3		Physical	
🔒 Ethernet1/4		Physical	
🔒 Ethernet1/5		Physical	
🔒 Ethernet1/6		Physical	
🔒 Ethernet1/7		Physical	
● Ethernet1/8 (Manager Access)	redundant	Physical	mgmt

ステップ 3 [管理 (Management)] 設定にセカンダリアドレスを追加します。

- a) [Device] をクリックし、[Management] 領域を表示します。
- b) [.] をクリックします。[編集 (Edit)] (✎)

図 55: 管理アドレスの編集

Management	
Remote Host Address:	10.89.5.29
Secondary Address:	
Status:	✓
Manager Access Interface:	Data Interface
Manager Access Details:	Configuration

- c) [管理 (Management)]ダイアログボックスで、[セカンダリアドレス (Secondary Address)]フィールドの名前または IP アドレスを変更します。

図 56: 管理 IP アドレス

Management	
Remote Host Address:	10.89.5.29
Secondary Address:	10.99.11.6
<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

- d) [保存 (Save)]をクリックします。

ステップ 4 両方のインターフェイスで ECMP ゾーンを作成します。

- [ルーティング (Routing)]をクリックします。
- 仮想ルータドロップダウンから、プライマリインターフェイスとセカンダリインターフェイスが存在する仮想ルータを選択します。
- [ECMP]をクリックし、[追加 (Add)]をクリックします。
- [名前 (Name)]に ECMP ゾーンの名前を入力します。
- [使用可能なインターフェイス (Available Interfaces)]ボックスでプライマリおよびセカンダリインターフェイスを選択し、[追加 (Add)]をクリックします。

図 57: ECMP ゾーンの追加

The screenshot shows a dialog box titled "Add ECMP". At the top right of the dialog are a help icon (question mark) and a close icon (X). Below the title bar is a text input field labeled "Name" containing the text "redundant-mgmt". Below this are two columns: "Available Interfaces" on the left, which is currently empty, and "Selected Interfaces" on the right, which contains two entries: "outside" and "redundant", each with a trash can icon to its right. A blue "Add" button is located between the two columns. At the bottom right of the dialog are two buttons: "Cancel" and "OK".

f) [OK] をクリックし、[保存 (Save)] をクリックします。

ステップ 5 両方のインターフェイスに等コストのデフォルトスタティックルートを追加し、両方で SLA トラッキングを有効にします。

ルートは、ゲートウェイを除いて同一であり、両方のメトリックが 1 である必要があります。プライマリインターフェイスには、編集可能なデフォルトルートがすでに存在している必要があります。

図 58 : Add/Edit Static Route

- a) [Static Route] をクリックします。
- b) [ルートを追加 (Add Route)] をクリックして新しいルートを追加するか、既存のルートの場合は [編集 (Edit)] (✎) をクリックします。
- c) [インターフェイス (Interface)] ドロップダウンリストから、インターフェイスを選択します。
- d) 宛先ネットワークとして、[使用可能なネットワーク (Available Networks)] ボックスから [any-ipv4] を選択し、[追加 (Add)] をクリックします。
- e) デフォルトの [ゲートウェイ (Gateway)] を入力します。
- f) [ルートトラッキング (Route Tracking)] の場合、**Add (+)** をクリックして新しい SLA モニターオブジェクトを追加します。
- g) 次を含む必要なパラメータを入力します。
 - Management Center IP アドレスとしての [モニターアドレス (Monitor Address)]。

- [使用可能なゾーン (Available Zones)]のプライマリまたはセカンダリ管理インターフェイスのゾーン。たとえば、プライマリインターフェイスオブジェクトには外部ゾーンを選択し、セカンダリインターフェイスオブジェクトには管理ゾーンを選択します。

詳細については、[SLA モニタ](#)を参照してください。

図 59: SLA モニターの追加

The screenshot shows a web-based configuration form titled "New SLA Monitor Object". The form is organized into two columns. The left column contains fields for Name (mgmt-secondary), Frequency (60), Threshold, Data Size (28), Number of Packets (1), and Available Zones (with a search bar and a list containing 'mgmt' and 'outside'). The right column contains fields for Description, SLA Monitor ID (2), Timeout (5000), ToS, and Monitor Address (10.89.5.35). Below the Available Zones list is an "Add" button. At the bottom right, there is a "Selected Zones/Interfaces" list containing "mgmt" and a trash icon. At the very bottom, there are "Cancel" and "Save" buttons.

- h) [保存 (Save)]をクリックし、[ルートトラッキング (Route Tracking)]ドロップダウンリストで、作成した SLA オブジェクトを選択します。
- i) [OK]をクリックし、[保存 (Save)]をクリックします。
- j) もう一方の管理インターフェイスのデフォルトルートについてこの手順を繰り返します。

ステップ 6 設定変更を展開します。設定変更の展開を参照してください。

この機能の展開において、Management Center は管理トラフィック用のセカンダリインターフェイスを有効にします。これには、管理トラフィックが適切なデータインターフェイスに到達するための自動生成されたポリシーベースのルーティング構成が含まれます。Management Center は、**configure network management-data-interface** コマンドの 2 番目のインスタンスも展開します。CLI でセカンダリインターフェイスを編集する場合、ゲートウェイを設定したり、デフォルトルートを変更したりすることはできません。このインターフェイスのスタティックルートは Management Center でしか編集できません。

データインターフェイス管理用のマネージャアクセスの詳細を表示する

モデルのサポート : Threat Defense

専用の管理インターフェイスを使用する代わりに、Management Center 管理にデータインターフェイスを使用する場合は、Management Center でデバイスのインターフェイスとネットワークの設定を変更するときに接続を中断しないように注意します。デバイスのデータインターフェイス設定をローカルで変更することもできます。その場合は、Management Center でそれらの変更を手動で調整する必要があります。[デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [管理 (Management)] > [マネージャアクセス - 構成詳細 (Manager Access - Configuration Details)] [FMCアクセス - 構成詳細 (FMC Access - Configuration Details)] ダイアログボックスは、Management Center と Threat Defense のローカル設定の間の矛盾を解決するために役立ちます。 > > >

通常、Threat Defense を Management Center に追加する前に、Threat Defense の初期設定の一環としてマネージャアクセスデータインターフェイスを構成します。Threat Defense を Management Center に追加すると、Management Center はインターフェイス設定（インターフェイス名と IP アドレス、ゲートウェイへの静的ルート、DNS サーバー、DDNS サーバーなど）を検出して維持します。DNS サーバーの場合、登録中に検出された場合、構成はローカルに保持されます。ただし、Management Center のプラットフォーム設定ポリシーには追加されません。

Threat Defense を Management Center に追加した後、**configure network management-data-interface** コマンドを使用してローカルで Threat Defense のデータインターフェイス構成を変更すると、Management Center が構成変更を検出し、Threat Defense への展開をブロックします。Management Center は、以下のいずれかの方法を使用して構成の変更を検出します。

- Threat Defense への展開。Management Center の展開の前に、構成の差異を検出してデプロイを停止します。
- [インターフェイス (Interfaces)] ページの [同期 (Sync)] ボタン。
- [マネージャアクセス - 構成の詳細 (Manager Access - Configuration Details)] [FMCアクセス - 構成の詳細 (FMC Access - Configuration Details)] ダイアログボックスの [更新 (Refresh)] ボタン

ブロックを削除するには、[マネージャアクセス - 構成詳細 (Manager Access - Configuration Details)] [FMCアクセス - 構成詳細 (FMC Access - Configuration Details)] ダイアログボックスに

移動し、[確認 (Acknowledge)] をクリックする必要があります。Management Center 設定は、次回展開時に ThreatDefense の残りの競合する設定を上書きします。再展開の前に Management Center の設定を手動で修正する必要があります。

このダイアログボックスに関する以下のページを参照してください。

設定

Management Center および Threat Defense のマネージャ アクセス データ インターフェイスの構成比較を表示します。

次の例は、**configure network management-data-interface** コマンドが Threat Defense に入力された Threat Defense の構成詳細を示しています。ピンクのハイライトは、相違点を確認したものの、Management Center の構成と一致しない場合、Threat Defense の構成が削除されることを示しています。青色のハイライトは、Threat Defense で変更される構成を示しています。緑のハイライトは、Threat Defense に追加される構成を示しています。

Manager access - Configuration Details ?

Manager access configuration on device have been updated outside of Manager. Review the differences and update Manager values accordingly.

Configuration CLI Output Connection Status

Last updated: 2022-09-02 at 20:35:58 UTC [\[Refresh \]](#)

	Configuration on Manager	Configuration on Device
4. Ethernet1/1		
Interface Configuration		
FMC Access Enabled	Disabled	Enabled
FMC Access - Allowed Networks		any
Interface Name		outside
IPv4/IPv6 Address		10.89.5.29/26
Static Route Configuration		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		
5. Ethernet1/8		

Legend: Above configurations will be ■ added, ■ modified or ■ disassociated from manager access interface on next deploy to device.

Management Center でインターフェイスを設定した後のこのページの例を以下に示します。インターフェイス設定が一致し、ピンクのハイライトが消えています。

Manager access - Configuration Details

Manager access configuration on device is different from Manager. Review the differences and deploy the changes.

Configuration CLI Output Connection Status

Last updated: 2022-09-09 at 07:10:54 UTC [Refresh]

	Configuration on Manager	Configuration on Device
Web Update Type		
4. GigabitEthernet0/0		
Interface Configuration		
FMC Access Enabled	Enabled	Enabled
FMC Access - Allowed Networks	any	any
Interface Name	outside	outside
IPv4/IPv6 Address	10.89.5.29 255.255.255.192	10.89.5.29 255.255.255.192
Static Route Configuration		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		

Legend: Above configurations will be added, modified or disassociated from manager access interface on next deploy to device.

Close

CLI 出力

マネージャアクセスデータインターフェイスのCLI構成を表示します。これは、基盤となるCLIに精通している場合に役立ちます。

図 60: CLI 出力

Manager access - Configuration Details

Manager access configuration on device is different from Manager. Review the differences and deploy the changes.

Configuration CLI Output Connection Status

Show command output of Manager Access associated configuration from Firewall Threat Defense

```
> show running-config dns
DNS server-group DefaultDNS

> show sftunnel interfaces
Physical Interface      Name of the Interface

> show running-config interface

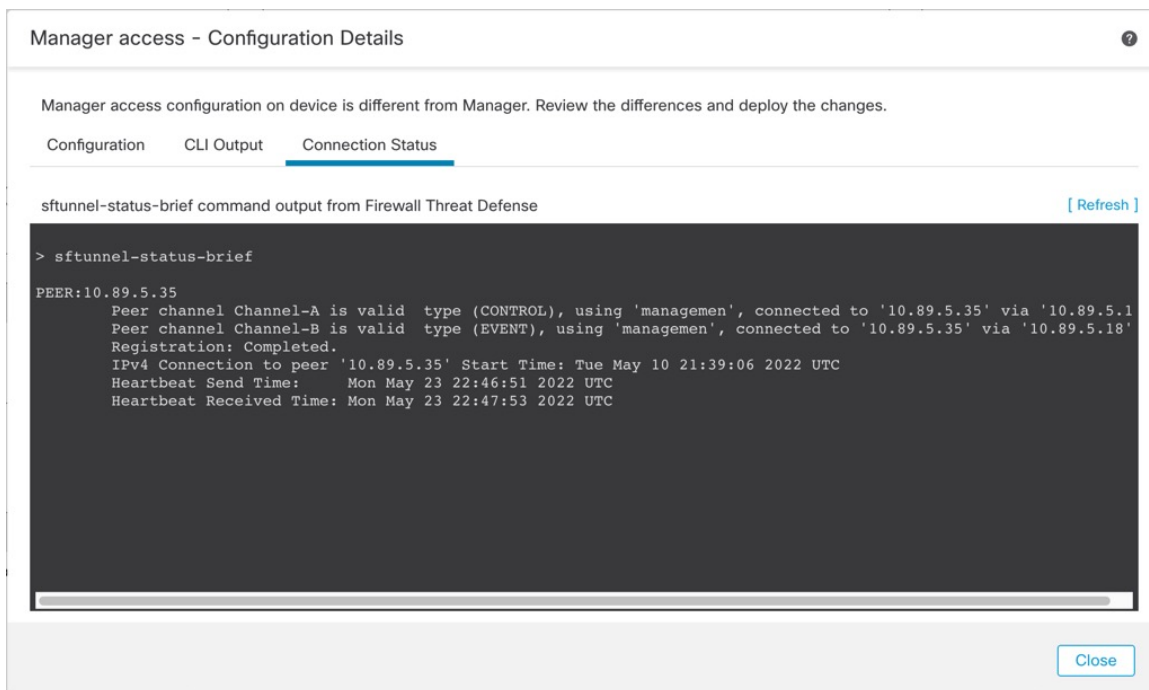
> show version
-----[ 1010-2 ]-----
Model      : Cisco Firepower 1010 Threat Defense (78) Version 7.2.0 (Build 2028)
UUID      : ebf1f518-d0a0-11ec-bb8f-90ce044ba76f
LSP version : lsp-rel-20220519-1116
VDB version  : 354
-----
Cisco Adaptive Security Appliance Software Version 9.18(0)104
```

Close

接続ステータス

管理接続ステータスの表示次の例は、管理接続で引き続き管理「management0」インターフェイスが使用されていることを示しています。

図 61: 接続ステータス



The screenshot displays the 'Manager access - Configuration Details' page. At the top, it states: 'Manager access configuration on device is different from Manager. Review the differences and deploy the changes.' Below this, there are three tabs: 'Configuration', 'CLI Output', and 'Connection Status'. The 'Connection Status' tab is selected. The main content area shows the output of the 'sftunnel-status-brief' command from the Firewall Threat Defense. The output indicates that two peer channels, Channel-A and Channel-B, are valid and connected to the peer IP 10.89.5.35. Channel-A is of type CONTROL and Channel-B is of type EVENT. The registration is completed, and the IPv4 connection to peer '10.89.5.35' started on Tue May 10 21:39:06 2022 UTC. The heartbeat send time is Mon May 23 22:46:51 2022 UTC, and the heartbeat received time is Mon May 23 22:47:53 2022 UTC. There are 'Refresh' and 'Close' buttons in the interface.

```
> sftunnel-status-brief
PEER:10.89.5.35
Peer channel Channel-A is valid type (CONTROL), using 'managemen', connected to '10.89.5.35' via '10.89.5.1'
Peer channel Channel-B is valid type (EVENT), using 'managemen', connected to '10.89.5.35' via '10.89.5.18'
Registration: Completed.
IPv4 Connection to peer '10.89.5.35' Start Time: Tue May 10 21:39:06 2022 UTC
Heartbeat Send Time: Mon May 23 22:46:51 2022 UTC
Heartbeat Received Time: Mon May 23 22:47:53 2022 UTC
```

次のステータスは、データインターフェイスの接続が成功したことを示し、内部の「tap_nlp」インターフェイスを示しています。

図 62: 接続ステータス

Manager access - Configuration Details

Manager access configuration on device is in sync with the manager.

Configuration CLI Output **Connection Status**

sftunnel-status-brief command output from Firewall Threat Defense [\[Refresh \]](#)

```
> sftunnel-status-brief
PEER:10.89.5.35
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Registration: Completed.
IPv4 Connection to peer '10.89.5.35' Start Time: Mon May 23 22:55:01 2022 UTC
Heartbeat Send Time: Mon May 23 22:56:21 2022 UTC
Heartbeat Received Time: Mon May 23 22:55:58 2022 UTC
Last disconnect time : Mon May 23 22:54:39 2022 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

[Close](#)

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

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

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

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

Threat Defense 管理インターフェイスの CLI での変更

CLIを使用して、管理対象デバイスの管理インターフェイスの設定を変更します。これらの設定の多くは、初期セットアップ時に設定されたものです。この手順に従うことで、それらの設

定を変更でき、さらに設定を追加できます（例：モデルでサポートされる場合にイベントインターフェイスを有効化する、スタティック ルートを追加する）。



- (注) このトピックは、専用管理インターフェイスに適用されます。代わりに、管理用のデータインターフェイスを設定することもできます。このインターフェイスのネットワーク設定を変更する場合は、CLI ではなく **Management Center** 内で行う必要があります。切断された管理接続をトラブルシューティングする必要があり、**Threat Defense** で直接変更する必要がある場合は、[管理に使用される Threat Defense データインターフェイスの CLI での変更 \(98 ページ\)](#) を参照してください。

Threat Defense CLI の詳細については、[Cisco Secure Firewall Threat Defense コマンドリファレンス](#) を参照してください。



- (注) SSH を使用する際は、慎重に管理インターフェイスに変更を加えてください。構成エラーで再接続できなくなると、デバイスのコンソール ポートへのアクセスが必要になります。



- (注) デバイス管理 IP アドレスを変更する場合は、**configure manager add** コマンド ([新しい Management Center の特定 \(124 ページ\)](#)) を参照) を使用してデバイスの初期設定時に **Management Center** を特定した方法に応じて、**Management Center** 接続に関する次のタスクを参照してください。

- **IP アドレス—アクションなし**。到達可能な IP アドレスを使用して **Management Center** を特定した場合、管理接続は数分後に自動的に再確立されます。情報の同期を維持するために、**Management Center** に表示されるデバイス IP アドレスも変更することを推奨します。[Management Center でのホスト名または IP アドレスの更新 \(66 ページ\)](#) を参照してください。このアクションは、接続の再確立を高速化するのに役立ちます。**注**：到達不能な **Management Center** IP アドレスを指定した場合は、以下の **NAT ID** の手順を参照してください。
- **NAT ID のみ：接続を手動で再確立**。NAT ID のみを使用して **Management Center** を識別した場合、接続は自動的に再確立されません。この場合、[Management Center でのホスト名または IP アドレスの更新 \(66 ページ\)](#) に従って **Management Center** のデバイス管理 IP アドレスを変更します。



- (注) ハイアベイラビリティ Management Center 構成では、管理 IP アドレスをデバイスの CLI または Management Center から変更した場合、HA 同期後も、セカンダリ Management Center には変更が反映されません。セカンダリ Management Center も更新されるようにするには、2 つの Management Center の間でロールを切り替えて、セカンダリ Management Center をアクティブユニットにします。現在アクティブな Management Center のデバイス管理のページで、登録されているデバイスの管理 IP アドレスを変更します。

始める前に

- **configure user add** コマンドを使用して CLI にログイン可能なユーザー アカウントを作成できます。次を参照してください：[CLI での内部ユーザーの追加外部認証](#)に従って AAA ユーザーを設定することもできます。

手順

- ステップ 1** コンソール ポートから、または SSH を使用して、デバイス CLI に接続します。
「[デバイスのコマンドラインインターフェイスへのログイン \(12 ページ\)](#)」を参照してください。
- ステップ 2** 管理者のユーザー名とパスワードでログインします。
- ステップ 3** (Firepower 4100/9300 および Cisco Secure Firewall 4200 のみ) 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

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。

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、イベントチャン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ン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。

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

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4 管理インターフェイスまたはイベントインターフェイスの IP アドレスを設定します。

management_interface 引数を指定しない場合は、デフォルトの管理インターフェイスのネットワーク設定を変更します。イベントインターフェイスを設定する際は、必ず *management_interface* 引数を指定してください。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。自分で設定するインターフェイスに接続すると、切断されます。新しい IP アドレスに再接続できます。

a) IPv4 アドレスを設定します。

- 手動設定

```
configure network ipv4 manual ip_address netmask gateway_ip [management_interface]
```

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。イベント専用インターフェイスを設定する場合は、コマンドの一部として *gateway_ip* を入力する必要があります。ただし、このエントリは、指定した値にデフォルトルートを設定するだけで、イベントインターフェイスの個別のスタティックルートは作成しません。管理インターフェイスと別の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、管理インターフェイスと共に使用するよう *gateway_ip* を設定し、**configure network static-routes** コマンドを使用してイベント専用インターフェイス用に個別に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.

>
```

- DHCP（デフォルト管理インターフェイスのみでサポート）。

```
configure network ipv4 dhcp
```

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 [management_interface]
```

例：

```
> configure network ipv6 router management0
```

```
Setting IPv6 network configuration.
Network settings changed.
```

```
>
```

- 手動設定

```
configure network ipv6 manual ip6_address ip6_prefix_length [ip6_gateway_ip]
[management_interface]
```

このコマンド内の *ip6_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。イベント専用インターフェイスを設定する場合は、コマンドの一部として *ip6_gateway_ip* を入力する必要があります。ただし、このエントリは、指定した値にデフォルトルートを設定するだけで、イベントインターフェイスの個別のスタティックルートは作成しません。管理インターフェイスと別の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、管理インターフェイスと共に使用するように *ip6_gateway_ip* を設定し、**configure network static-routes** コマンドを使用してイベント専用インターフェイス用に個別に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 ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.
```

```
>
```

- DHCPv6（デフォルト管理インターフェイスのみでサポート）。

```
configure network ipv6 dhcp
```

ステップ 5 IPv6 の場合、ICMPv6 エコー応答と宛先到達不能メッセージを有効または無効にします。デフォルトでは、これらのメッセージは有効になっています。

```
configure network ipv6 destination-unreachable {enable | disable}
```

```
configure network ipv6 echo-reply {enable | disable}
```

これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、デバイスの管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。

例：

```
> configure network ipv6 destination-unreachable disable
> configure network ipv6 echo-reply disable
```

ステップ 6 デフォルト管理インターフェイスの DHCP サーバーが、接続されているホストに IP アドレスを提供することを可能にします。

```
configure network ipv4 dhcp-server-enable start_ip_address end_ip_address
```

例 :

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254
DHCP Server Enabled
```

>

管理インターフェイスの IP アドレスを手動で設定するときのみ、DHCP サーバーを設定できます。このコマンドは、Management Center Virtual ではサポートされません。DHCP サーバーのステータスを表示するには、**show network-dhcp-server** を入力します。

```
> show network-dhcp-server
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

ステップ 7 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 management_interface 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 4 \(93 ページ\)](#)」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
[...]
```

ステップ 8 ホスト名の設定

```
configure network hostname name
```

例 :

```
> configure network hostname farscape1.cisco.com
```

Syslog メッセージは、再起動するまで新しいホスト名を反映しません。

ステップ 9 検索ドメインを設定します。

```
configure network dns searchdomains domain_list
```

例 :

```
> configure network dns searchdomains example.com,cisco.com
```

カンマで区切ったデバイスの検索ドメインを設定します。これらのドメインは、コマンド (**ping system** など) に完全修飾ドメイン名を指定しない場合にホスト名に追加されます。ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。

ステップ 10 カンマで区切った 3 つの DNS サーバーを設定します。

```
configure network dns servers dns_ip_list
```

例 :

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

ステップ 11 Management Center で通信のリモート管理ポートを設定します。

```
configure network management-interface tcpport number
```

例 :

```
> configure network management-interface tcpport 8555
```

Management Center および管理対象デバイスは、双方向の TLS-1.3 暗号化通信チャネル (デフォルトではポート 8305) を使用して通信します。

(注) シスコは、リモート管理ポートをデフォルト設定のままにしておくことを強く推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要があるすべてのデバイスの管理ポートを変更する必要があります。

ステップ 12 (Threat Defense のみ) 管理インターフェイスまたはイベントインターフェイスの MTU を設定します。デフォルトの MTU は 1500 バイトです。

```
configure network mtu [bytes] [interface_id]
```

- *bytes* : MTU をバイト単位で設定します。管理インターフェイスでは、IPv4 を有効にした場合は 64~1500、IPv6 を有効にした場合は 1280~1500 の値を指定できます。イベントインターフェイスでは、IPv4 を有効にした場合は 64~9000、IPv6 を有効にした場合は 1280~9000 です。IPv4 と IPv6 の両方を有効にした場合、最小値は 1280 です。*bytes* を入力しない場合、値の入力を求められます。

- **interface_id** : MTU を設定するインターフェイス ID を指定します。プラットフォームに応じて使用可能なインターフェイス ID (management0、management1、br1、eth0など) を表示するには、**show network** コマンドを使用します。インターフェイスを指定しない場合は、管理インターフェイスが使用されます。

例 :

```
> configure network mtu 8192 management1
MTU set successfully to 1500 from 8192 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

ステップ 13 HTTP プロキシを設定します。デバイスは、ポート TCP/443 (HTTPS) および TCP/80 (HTTP) でインターネットに直接接続するように設定されています。HTTP ダイジェスト経由で認証できるプロキシサーバを使用できます。コマンド発行後に、HTTP プロキシのアドレスとポート、プロキシの認証が必要かどうかをユーザーは尋ねられます。認証が必要な場合はプロキシのユーザー名、プロキシのパスワード、およびプロキシのパスワードの確認を入力するよう要求されます。

(注) Threat Defense のプロキシパスワードには、A~Z、a~z と 0~9 の文字のみを使用できます。

configure network http-proxy

例 :

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

ステップ 14 デバイス管理 IP アドレスを変更する場合は、**configure manager add** コマンド ([新しい Management Center の特定 \(124 ページ\)](#)) を参照) を使用してデバイスの初期設定時に Management Center を特定した方法に応じて、Management Center 接続に関する次のタスクを参照してください。

- **IP アドレス—アクションなし**。到達可能な IP アドレスを使用して Management Center を特定した場合、管理接続は数分後に自動的に再確立されます。情報の同期を維持するために、Management Center に表示されるデバイス IP アドレスも変更することを推奨します。[Management Center でのホスト名または IP アドレスの更新 \(66 ページ\)](#) を参照してください。このアクションは、接続の再確立を高速化するのに役立ちます。**注** : 到達不能な Management Center IP アドレスを指定した場合は、[Management Center でのホスト名または IP アドレスの更新 \(66 ページ\)](#) を使用して手動で接続を再確立する必要があります。

- **NAT IDのみ**：接続を手動で再確立。NAT ID のみを使用して Management Center を識別した場合、接続は自動的に再確立されません。この場合、[Management Center でのホスト名または IP アドレスの更新 \(66 ページ\)](#) に従って Management Center のデバイス管理 IP アドレスを変更します。

管理に使用される Threat Defense データインターフェイスの CLI での変更

Threat Defense と Management Center の間の管理接続が中断され、古いインターフェイスを置き換える新しいデータインターフェイスを指定する場合は、Threat Defense CLI を使用して新しいインターフェイスを設定します。この手順では、同じネットワーク上の古いインターフェイスを新しいインターフェイスに置き換えることを想定しています。管理接続がアクティブな場合は、Management Center を使用して既存のデータインターフェイスを変更する必要があります。データ管理インターフェイスの初期設定については、「[CLI を使用した Threat Defense 初期設定の実行の完了 \(22 ページ\)](#)」の `configure network management-data-interface` コマンドを参照してください。

ハイアベイラビリティペアの場合は、両方のユニットですべての CLI 手順を実行します。Management Center 内では、アクティブユニットでのみ手順を実行します。設定の変更が展開されると、スタンバイユニットはアクティブユニットから設定およびその他のステート情報を同期します。



- (注) このトピックは、専用の管理インターフェイスではなく、管理用に設定したデータインターフェイスに適用されます。管理インターフェイスのネットワーク設定を変更する場合は、[Threat Defense 管理インターフェイスの CLI での変更 \(90 ページ\)](#) を参照してください。

Threat Defense CLI の詳細については、[Cisco Secure Firewall Threat Defense コマンドリファレンス](#) を参照してください。

始める前に

`configure user add` コマンドを使用して CLI にログイン可能なユーザー アカウントを作成できます。次を参照してください：[CLI での内部ユーザーの追加外部認証](#)に従って AAA ユーザーを設定することもできます。

手順

- ステップ 1** データ管理インターフェイスを新しいインターフェイスに変更する場合は、現在のインターフェイスケーブルを新しいインターフェイスに移動します。
- ステップ 2** デバイスの CLI に接続します。
これら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。初期設定の実行中に、管理インターフェイスから切断される可能性があります。管理接続が中断された

ために設定を編集しており、専用管理インターフェイスに SSH アクセスできる場合は、その SSH 接続を使用できます。

「[デバイスのコマンドラインインターフェイスへのログイン \(12 ページ\)](#)」を参照してください。

ステップ 3 管理者のユーザー名とパスワードでログインします。

ステップ 4 インターフェイスを無効にして、設定を再構成できるようにします。

configure network management-data-interface disable

例 :

```
> configure network management-data-interface disable
```

```
Configuration updated successfully..!!
```

```
Configuration disable was successful, please update the default route to point to a gateway on management interface using the command 'configure network'
```

ステップ 5 マネージャアクセス用の新しい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。

データ管理インターフェイスを同じネットワーク上の新しいインターフェイスに変更する場合は、インターフェイス ID を除き、前のインターフェイスと同じ設定を使用します。さらに、**Do you wish to clear all the device configuration before applying ? (y/n) [n]:** オプションに **y** を選択します。この選択により、古いデータ管理インターフェイスの設定がクリアされるため、IP アドレスとインターフェイス名を新しいインターフェイスで正常に再利用できます。

```
> configure network management-data-interface
```

```
Data interface to use for management: ethernet1/4
```

```
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]: y
```

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

configure network management-data-interface client ip_address netmask

デフォルトでは、すべてのネットワークが許可されます。

ステップ 7 接続は自動的に再確立されますが、Management Center で接続を無効にしてから再度有効にすると、接続の再確立を速く実行できます。「[Management Center でのホスト名または IP アドレスの更新 \(66 ページ\)](#)」を参照してください。

ステップ 8 管理接続が再確立されたことを確認します。

sftunnel-status-brief

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

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

ステップ 9 Management Center で、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [管理 (Management)] > [マネージャアクセス - 構成詳細 (Manager Access - Configuration Details)] を選択し、[更新 (Refresh)] をクリックします。

Management Center はインターフェイスとデフォルトルートの設定変更を検出し、Threat Defense への展開をブロックします。デバイスのデータインターフェイス設定をローカルで変更する場合は、Management Center でそれらの変更を手動で調整する必要があります。[構成 (Configuration)] タブで、Management Center と Threat Defense の不一致を確認できます。

ステップ 10 [Devices] > [Device Management] > [Interfaces] の順に選択して、次の変更を行います。

- a) 古いデータ管理インターフェイスから IP アドレスと名前を削除し、このインターフェイスのマネージャアクセスを無効にします。
- b) 古いインターフェイス (CLI で使用したインターフェイス) の設定を使用して新しいデータ管理インターフェイスを設定し、マネージャアクセスを有効にします。

ステップ 11 [デバイス (Devices)] > [デバイス管理 (Device Management)] > [ルーティング (Routing)] > [スタティックルート (Static Route)] を選択し、デフォルトルートを古いデータ管理インターフェイスから新しいインターフェイスに変更します。

ステップ 12 [マネージャアクセス - 構成詳細 (Manager Access - Configuration Details)] [FMC アクセス - 構成詳細 (FMC Access - Configuration Details)] ダイアログボックスに戻り、[確認 (Acknowledge)] をクリックして展開ブロックを削除します。

Management Center 設定は、次回展開時に Threat Defense の残りの競合する設定を上書きします。再展開の前に Management Center の設定を手動で修正する必要があります。

「Config was cleared」および「Manager Access changed and acknowledged」という想定されるメッセージが表示されます。

Management Center の接続が失われた場合の構成の手動ロールバック

Threat Defense でマネージャアクセス用にデータインターフェイスを使用し、ネットワーク接続に影響する Management Center からの構成変更を展開する場合、Threat Defense の構成を最後に展開した構成にロールバックして、管理接続を復元できます。その後、ネットワーク接続が維持されるように Management Center で構成設定を調整し、再展開できます。ロールバック機能は、接続が失われていない場合でも使用でき、このトラブルシューティングの状況以外でも使用できます。

または、展開後に接続が失われた場合は、構成の自動ロールバックを有効にすることもできます。展開設定の編集 (115 ページ) を参照してください。

次のガイドラインを参照してください。

- 前回の展開のみ Threat Defense でローカルに使用できます。さらに以前の展開にロールバックすることはできません。
- ロールバックは、高可用性ではサポートされていますが、クラスタリングの展開ではサポートされていません。
- ロールバックは、Management Center で設定できる構成にのみ影響します。たとえば、ロールバックは、Threat Defense CLI でのみ設定できる専用管理インターフェイスに関連するローカル構成には影響しません。 **configure network management-data-interface** コマンドを使用した最後の Management Center 展開後にデータインターフェイス設定を変更し、rollback コマンドを使用すると、それらの設定は保持されないことに注意してください。最後に展開された Management Center 設定にロールバックされます。
- UCAPL/CC モードはロールバックできません。
- 以前の展開中に更新されたアウトオブバンド SCEP 証明書データはロールバックできません。
- ロールバック中に、現在の設定がクリアされるため、接続がドロップされます。

手順

ステップ 1 Threat Defense CLI で、以前の構成へロールバックします。

configure policy rollback

ロールバック後、Threat Defense はロールバックが正常に完了したことを Management Center に通知します。Management Center では、構成がロールバックされたことを示すバナーが展開画面に表示されます。

(注) ロールバックが失敗し、Management Center 管理が復元された場合、一般的な展開の問題について<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html>を参照してください。場合によっては、Management Center 管理アクセスの復元後にロールバックが失敗することがあります。この場合、Management Center 構成の問題を解決して、Management Center から再展開できます。

例：

マネージャアクセスにデータインターフェイスを使用する Threat Defense の場合：

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....
.....
>
```

ステップ 2 管理接続が再確立されたことを確認します。

Management Center で、[Devices] [Device Management] [Device] [Management] [Manager Access - Configuration Details] [FMC Access - Configuration Details] [Connection Status] ページで管理接続ステータスを確認します。

管理接続のステータスを表示するには、Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。[データインターフェイスでの管理接続のトラブルシューティング \(102 ページ\)](#) を参照してください。

データインターフェイスでの管理接続のトラブルシューティング

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

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

管理接続ステータスの表示

Management Center で、[Devices] [Device Management] [Device] [Management] [Manager Access - Configuration Details] [FMC Access - Configuration Details] [Connection Status] ページで管理接続ステータスを確認します。

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

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

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

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

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

Threat Defense ネットワーク情報の表示

Threat Defense CLI で、管理および マネージャ アクセス データ インターフェイスのネットワーク設定を表示します。

show network

```
> show network
===== [ System Information ] =====
Hostname                : FTD-4
Domains                 : cisco.com
DNS Servers             : 72.163.47.11
DNS from router        : enabled
Management port        : 8305
IPv4 Default route
  Gateway                : data-interfaces

===== [ management0 ] =====
Admin State             : enabled
Admin Speed             : 1gbps
Operation Speed        : 1gbps
Link                   : up
```

```

Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : 68:87:C6:A6:54:80
-----[ IPv4 ]-----
Configuration           : Manual
Address                 : 10.89.5.4
Netmask                 : 255.255.255.192
Gateway                 : 169.254.1.1
-----[ IPv6 ]-----
Configuration           : Disabled

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

=====[ System Information - Data Interfaces ]=====
DNS Servers             : 72.163.47.11
Interfaces              : Ethernet1/1

=====[ Ethernet1/1 ]=====
State                   : Enabled
Link                    : Up
Name                    : outside
MTU                     : 1500
MAC Address             : 68:87:C6:A6:54:A4
-----[ IPv4 ]-----
Configuration           : Manual
Address                 : 10.89.5.6
Netmask                 : 255.255.255.192
Gateway                 : 10.89.5.1
-----[ IPv6 ]-----
Configuration           : Disabled

```

Management Center への Threat Defense の登録の確認

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

show managers

```

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

```

Management Center に ping する

Threat Defense CLI で、次のコマンドを使用して、データインターフェイスから Management Center に ping します。

ping *fmc_ip*

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

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

Threat Defense CLI で、内部バックプレーン インターフェイス (nlp_int_tap) でパケットをキャプチャして、管理パケットが送信されているかどうかを確認します。

```
capture name interface nlp_int_tap trace detail match ip any any
```

```
show capture name trace detail
```

内部インターフェイスのステータス、統計、およびパケット数の確認

Threat Defense CLI で、内部バックプレーン インターフェイス (nlp_int_tap) に関する情報を参照してください。

```
show interface detail
```

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

ルーティングと NAT の確認

Threat Defense CLI で、デフォルトルート (S*) が追加されていること、および管理インターフェイス (nlp_int_tap) に内部 NAT ルールが存在することを確認します。

```
show route
```

```
> show route
```

```

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

Gateway of last resort is 10.89.5.1 to network 0.0.0.0

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

>

```

show nat

```

> show nat

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

>

```

その他の設定の確認

次のコマンドを参照して、他のすべての設定が存在することを確認します。これらのコマンドの多くは、Management Center の [Devices] [Device Management] [Device] [Management] [Manager Access - Configuration Details] [FMC Access - Configuration Details] [CLI Output] ページでも確認できます。

show running-config sftunnel

```

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

```

show running-config ip-client

```

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

```

show conn address fmc_ip

```

> show conn address 10.89.5.35
5 in use, 16 most used

```

```
Inspect Snort:
  preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

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

DDNS の更新が成功したかどうかを確認する

Threat Defense CLI で、DDNS の更新が成功したかどうかを確認します。

debug ddns

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

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

show crypto ca certificates trustpoint_name

DDNS の動作を確認するには :

show ddns update interface fmc_access_ifc_name

```
> show ddns update interface outside

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

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

Management Center ログファイルの確認

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

インベントリ詳細の表示

[デバイス (Device)] ページの [インベントリの詳細 (Inventory Details)] セクションには、シャーシの詳細情報 (CPU やメモリ など) が表示されます。

図 63: インベントリの詳細 (Inventory Details)

Inventory Details		↻
CPU Type:	CPU Xeon E5 series 2300 MHz	
CPU Cores:	1 CPU (4 cores)	
Memory:	8192 MB RAM	
Storage:	N/A	
Chassis URL:	N/A	
Chassis Serial Number:	N/A	
Chassis Module Number:	N/A	
Chassis Module Serial Number:	N/A	

情報を更新するには、[Refresh] (↻) をクリックします。

適用されたポリシーの編集

[デバイス (Device)] ページの [適用されたポリシー (Applied Policies)] セクションには、ファイアウォールに適用されている次のポリシーが表示されます。

図 64: [適用されたポリシー (Applied Policies)]

[適用されたポリシー (Applied Policies)]

Applied Policies		✎
Access Control Policy:	Initial AC Policy	ⓘ
Prefilter Policy:	Default Prefilter Policy	
SSL Policy:		
DNS Policy:	Default DNS Policy	
Identity Policy:		
NAT Policy:		
Platform Settings Policy:		
QoS Policy:		
FlexConfig Policy:		

リンクのあるポリシーの場合、リンクをクリックしてポリシーを表示できます。

アクセスコントロールポリシーについては、[感嘆符 (Exclamation)] (ⓘ) アイコンをクリックして [トラブルシューティングのためのアクセスポリシー情報 (Access Policy Information for Troubleshooting)] ダイアログボックスを表示します。このダイアログボックスには、アクセスルールがアクセスコントロールエントリ (ACE) に展開される方法が表示されます。

図 65: [トラブルシューティングのためのアクセスポリシー情報 (Access Policy Information for Troubleshooting)]

[トラブルシューティングのためのアクセスポリシー情報 (Access Policy Information for Troubleshooting)]

```

Access Policy Information for Troubleshooting
-----
Cisco Firepower Management Center for VMware - v7.1.0 - (build 90)
Access Control Rule Expansion Computer

Device:

  UUID: 4f12c89a-5705-11ec-b324-b3df319dfb31
  Name: 7.10 FCS FTD

Access Control Policy:

  UUID: 00000000-0000-0ed3-0000-004294968119
  Name: Initial AC Policy
  Description:

Intrusion Policies:
-----
|  UUID          |  NAME          |
-----
-----
Date: 2022-Mar-31 at 20:22:22 UTC

NOTE: Computation is done on per rule basis. Count from shadow rules will not be applicable on device.
Run "Rule Conflict Detection" tool on AC Policy for specified device to detect and optimise such rules.

|  UUID          |  NAME          |  COUNT  |
-----
-----
| TOTAL: 0
-----

```

[デバイス管理 (Device Management)]ページから、個々のデバイスにポリシーを割り当てることができます。

手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 ポリシーを割り当てるデバイスの横にある [編集 (Edit)] (✎) をクリックします。
- ステップ 3 [デバイス (Device)] をクリックします。
- ステップ 4 [適用されたポリシー (Applied Policies)] セクションで、[編集 (Edit)] (✎) をクリックします。

図 66: ポリシー割り当て

[ポリシー割り当て (Policy Assignments)]

Policy Assignments ?

Access Control Policy: ▼

NAT Policy: ▼

Platform Settings Policy: ▼

QoS Policy: ▼

FlexConfig Policy: ▼

ステップ 5 ポリシータイプごとに、ドロップダウンメニューからポリシーを選択します。既存のポリシーのみが一覧表示されます。

ステップ 6 [保存 (Save)] をクリックします。

次のタスク

- 設定変更を展開します [設定変更の展開](#) を参照してください。

詳細設定の編集

[デバイス (Device)] ページの [詳細設定 (Advanced Settings)] セクションには、以下で説明する詳細設定のテーブルが表示されます。これらの設定はいずれも編集できます。

表 6: [詳細設定 (Advanced)] セクションのテーブルのフィールド

フィールド	説明
アプリケーションバイパス (Application Bypass)	デバイスでの自動アプリケーションバイパスの状態。
バイパスしきい値 (Bypass Threshold)	自動アプリケーションバイパスのしきい値 (ミリ秒) 。

フィールド	説明
オブジェクトグループの検索	<p>デバイスでのオブジェクトグループ検索の状態。動作中、FTD デバイスは、アクセスルールで使用されるネットワークオブジェクトまたはインターフェイス オブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセス制御リストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセス制御ルールの検索に必要なメモリを抑えることができます。オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトまたはインターフェイス オブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。オブジェクトグループ検索は、アクセスルールがどのように定義されるか、または Firepower Management Center にどのように表示されるかには影響しません。アクセス制御ルールと接続を照合するときに、デバイスがアクセス制御ルールを解釈して処理する方法のみに影響します。</p> <p>(注) デフォルトでは、Management Center で初めて Threat Defense を追加すると、[オブジェクトグループ検索 (Object Group Search)] が有効になります。</p>
インターフェイスオブジェクトの最適化	<p>デバイスでのインターフェイス オブジェクトの最適化の状態。展開時に、アクセス制御とプレフィルタポリシーで使用されるインターフェイスグループとセキュリティゾーンは、送信元/宛先インターフェイスペアごとに個別のルールを生成します。インターフェイス オブジェクトの最適化を有効にすると、システムはアクセス制御/プレフィルタルールごとに1つのルールを展開します。これにより、デバイス設定の簡素化および展開のパフォーマンス向上が可能になります。このオプションを選択する場合は、[オブジェクトグループ検索 (Object Group Search)] オプションも選択して、デバイスのメモリ使用量を減らします。</p>

次のトピックでは、デバイスの詳細設定を編集する方法について説明します。



(注) [パケットの転送 (Transfer Packets)] 設定については、[全般設定の編集 \(51 ページ\)](#) を参照してください。

自動アプリケーションバイパスの設定

自動アプリケーションバイパス (AAB) を使用すると、Snort がダウンしている場合や、従来型デバイスで、パケットの処理に時間がかかりすぎる場合に、パケットが検出をバイパスできます。AAB により、Snort は障害から 10 分以内に再起動します。また、Snort 障害の原因を調査するために分析できるトラブルシューティング データが生成されます。



注意 AABのアクティブ化は、いくつかのパケットのインスペクションを一時的に中断する Snort プロセスを部分的に再起動します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細は[Snort の再起動によるトラフィックの動作](#)を参照してください。

次の動作を確認してください。

Threat Defense の動作 : Snort がダウンしている場合、指定されたタイマー期間の後に AAB がトリガーされます。Snort が稼働している場合、パケット処理が設定されたタイマーを超えても、AAB はトリガーされません。

従来型デバイスの動作 : AAB は、インターフェイスを介してパケットを処理するために許可される時間を制限します。パケット処理の遅延は、ネットワークで許容できるパケットレイテンシとバランスを取って調整します。

この機能は任意の展開で使用できますが、インライン展開ではとりわけ価値があります。

一般に、遅延しきい値を超えた後は、高速パスパケットに対して侵入ポリシーの [ルール遅延しきい値 (Rule Latency Thresholding)] を使用します。[ルール遅延しきい値 (Rule Latency Thresholding)] により、エンジンがシャットダウンされたり、トラブルシューティングデータが生成されることはありません。

検出がバイパスされると、デバイスがヘルス モニタリング アラートを生成します。

AAB はデフォルトで無効になっています。AAB を有効にするには、次の手順を実行します。

手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 詳細設定を編集するデバイスの横にある [編集 (Edit)] (✎) をクリックします。
- ステップ 3 [デバイス (Devices)] をクリックし、[詳細設定 (Advanced Settings)] セクションの [編集 (Edit)] (✎) をクリックします。
- ステップ 4 [自動アプリケーションバイパス (Automatic Application Bypass)] をオンにします。
- ステップ 5 [バイパスしきい値 (Bypass Threshold)] に 250 ~ 60,000 ミリ秒を入力します。デフォルト設定は 3000 ミリ秒 (ms) です。
- ステップ 6 [保存 (Save)] をクリックします。

次のタスク

- 設定変更を展開します [設定変更の展開](#) を参照してください。

オブジェクトグループ検索の構成

動作中、Threat Defense デバイスは、アクセスルールで使用されるネットワークオブジェクトまたはインターフェイスオブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセス制御リストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセス制御ルールの検索に必要なメモリを抑えることができます。オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトまたはインターフェイスオブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。オブジェクトグループ検索は、アクセスルールがどのように定義されているかや、Management Center にどのように表示されるかには影響しません。アクセス制御ルールと接続を照合するときに、デバイスがアクセス制御ルールを解釈して処理する方法のみに影響します。

オブジェクトグループ検索を有効にすると、ネットワークオブジェクトまたはインターフェイスオブジェクトを含むアクセスコントロールポリシーのメモリ要件が軽減されます。ただし、オブジェクトグループ検索では、ルールルックアップのパフォーマンスが低下して、CPU使用率が増大する可能性があることに注意してください。CPU に対する影響と、特定のアクセスコントロールポリシーに関するメモリ要件の軽減とのバランスをとる必要があります。ほとんどの場合、オブジェクトグループ検索を有効にすると、ネット運用が改善されます。

デフォルトでは、Management Center で初めて追加された Threat Defense デバイスではオブジェクトグループ検索が有効になっています。アップグレードされたデバイスの場合、デバイスでオブジェクトグループ検索が無効に設定されている場合は、手動で有効にする必要があります。一度に1つのデバイスで有効にできます。グローバルに有効にすることはできません。ネットワークオブジェクトまたはインターフェイスオブジェクトを使用するアクセスルールを展開するすべてのデバイスで有効にすることを推奨します。



- (注) オブジェクトグループの検索を有効にしてから、デバイスを設定し、しばらくの間操作した場合、後からこの機能を無効にすると、望ましくない結果になる可能性があることに注意してください。オブジェクトグループの検索を無効にすると、既存のアクセス制御ルールがデバイスの実行コンフィギュレーションで拡張されます。デバイスで使用可能なメモリよりも多くのメモリが拡張に必要な場合、デバイスが不整合状態になり、パフォーマンスに影響する可能性があります。デバイスが正常に動作している場合は、一度有効にしたオブジェクトグループ検索を無効にしないでください。

始める前に

- モデルのサポート：Threat Defense
- 各デバイスでトランザクションコミットも有効にすることを推奨します。デバイスCLIから **asp rule-engine transactional-commit access-group** コマンドを入力します。
- この設定を変更すると、デバイスが ACL を再コンパイルしている間、システムの動作が中断される可能性があります。この設定はメンテナンス期間中のみ変更することを推奨します。

- FlexConfig を使用して **object-group-search threshold** コマンドを設定し、しきい値を有効にしてパフォーマンスの低下を防止することができます。しきい値を使用した動作では、接続ごとに送信元と宛先の両方の IP アドレスがネットワークオブジェクトと照合されます。発信元アドレスに一致するオブジェクトの数が、宛先アドレスと一致する数の 1 万倍を超えると接続が切断されます。一致件数が膨大になることを防ぐためにルールを設定します。

手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択します。
- ステップ 2** ルールを設定する Threat Defense デバイスの横にある[編集 (Edit)] (✎) をクリックします。
- ステップ 3** [デバイス (Devices)] タブをクリックし、[詳細設定 (Advanced Settings)] セクションの[編集 (Edit)] (✎) をクリックします。
- ステップ 4** [オブジェクトグループの検索 (Object Group Search)] をオンにします。
- ステップ 5** ネットワークオブジェクトに加えてインターフェイスオブジェクトでオブジェクトグループの検索を機能させるには、[インターフェイスオブジェクトの最適化 (Interface Object Optimization)] をオンにします。

[インターフェイスオブジェクトの最適化 (Interface Object Optimization)] を選択しない場合は、システムで、ルールで使用されているセキュリティゾーンとインターフェイスグループが使用されずに、送信元/インターフェイスのペアごとに個別のルールが展開されます。これは、インターフェイスグループがオブジェクトグループの検索処理に使用できないことを意味します。
- ステップ 6** [保存 (Save)] をクリックします。

インターフェイスオブジェクトの最適化の設定

展開時に、アクセス制御とプレフィルタポリシーで使用されるインターフェイスグループとセキュリティゾーンは、送信元/宛先インターフェイスペアごとに個別のルールを生成します。インターフェイスオブジェクトの最適化を有効にすると、システムはアクセス制御/プレフィルタルールごとに1つのルールを展開します。これにより、デバイス設定の簡素化および展開のパフォーマンス向上が可能になります。このオプションを選択する場合は、[オブジェクトグループ検索 (Object Group Search)] オプションも選択して、デバイスのメモリ使用量を減らします。

インターフェイスオブジェクトの最適化はデフォルトで無効になっています。一度に1つのデバイスで有効にできます。グローバルに有効にすることはできません。



- (注) インターフェイス オブジェクトの最適化を無効にすると、既存のアクセス制御ルールはインターフェイス オブジェクトを使用せずに展開されるため、展開に時間がかかる場合があります。また、オブジェクトグループ検索が有効になっている場合、その利点はインターフェイス オブジェクトには適用されず、デバイスの実行中の設定のアクセス制御ルールが拡張されることがあります。デバイスで使用可能なメモリよりも多くのメモリが拡張に必要な場合、デバイスが不整合状態になり、パフォーマンスに影響する可能性があります。

始める前に

モデルのサポート : Threat Defense

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 ルールを設定する Threat Defense デバイスの横にある [編集 (Edit)] (✎) をクリックします。
- ステップ 3 [デバイス (Devices)] タブをクリックし、[詳細設定 (Advanced Settings)] セクションの [編集 (Edit)] (✎) をクリックします。
- ステップ 4 [インターフェイスオブジェクトの最適化 (Interface Object Optimization)] をオンにします。
- ステップ 5 [保存 (Save)] をクリックします。

展開設定の編集

[Device] ページの [Deployment Settings] セクションには、以下の表に記載された情報が表示されます。

図 67: 展開設定



Deployment Settings 	
Auto Rollback Deployment if Connectivity fails	Disabled
Connectivity Monitor Interval (in Minutes) 	20 Mins.

表 7: 展開設定

フィールド	説明
Auto Rollback Deployment if Connectivity Fails	[Enabled] と [Disabled] があります。 展開の結果として管理接続が失敗した場合は、自動ロールバックを有効にすることができます。特に、管理センターへのアクセスにデータを使用し、データインターフェイスを誤って構成した場合に当てはまります。
Connectivity Monitor Interval (in Minutes)	構成をロールバックする前に待機する時間を示します。

[デバイス管理 (Device Management)] ページから展開設定を設定できます。展開設定には、展開の結果として管理接続が失敗した場合の展開の自動ロールバックの有効化が含まれます。特に、管理センターへのアクセスにデータを使用し、データインターフェイスを誤って構成した場合です。代替として、**configure policy rollback** コマンドを使用して、構成を手動でロールバックすることもできます ([Management Center の接続が失われた場合の構成の手動ロールバック \(101 ページ\)](#) を参照)。

次のガイドラインを参照してください。

- 前回の展開のみ Threat Defense でローカルに使用できます。さらに以前の展開にロールバックすることはできません。
- ロールバックは、高可用性ではサポートされていますが、クラスタリングの展開ではサポートされていません。
- ロールバックは、Management Center で設定できる構成にのみ影響します。たとえば、ロールバックは、Threat Defense CLI でのみ設定できる専用管理インターフェイスに関連するローカル構成には影響しません。**configure network management-data-interface** コマンドを使用した最後の Management Center 展開後にデータインターフェイス設定を変更し、rollback コマンドを使用すると、それらの設定は保持されないことに注意してください。最後に展開された Management Center 設定にロールバックされます。
- UCAPL/CC モードはロールバックできません。
- 以前の展開中に更新されたアウトオブバンド SCEP 証明書データはロールバックできません。
- ロールバック中に、現在の設定がクリアされるため、接続がドロップされます。

手順

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

ステップ 2 ポリシーを割り当てるデバイスの横にある [編集 (Edit)] (✎) をクリックします。

ステップ 3 [デバイス (Device)] をクリックします。

ステップ4 [展開設定 (Deployment Settings)] セクションで、[編集 (Edit)] (✎) をクリックします。

図 68: 展開設定

Deployment Settings

Auto Rollback Deployment if Connectivity Fails:

Connectivity Monitor Interval (in Minutes): 20

The connectivity failure timeout will be applicable from next deployment incase, the deployment for this device is already in progress.

Cancel Save

ステップ5 自動ロールバックを有効にするには、[接続が失敗した場合の自動ロールバック展開 (Auto Rollback Deployment if Connectivity Fails)] をオンにします。

ステップ6 [接続モニタ間隔 (分) (Connectivity Monitor Interval (in Minutes))] を設定して、構成をロールバックする前に待機する時間を設定します。デフォルトは 20 分です。

ステップ7 ロールバックが発生した場合は、次の手順について以下を参照してください。

- 自動ロールバックが成功した場合は、フル展開を行うように指示する成功メッセージが表示されます。
- [展開 (Deploy)] > [高度な展開 (Advanced Deploy)] 画面に移動し、[プレビュー (Preview)] (👁️) アイコンをクリックして、ロールバックされた設定の一部を表示することもできます ([設定変更の展開](#)を参照)。[\[ロールバックの変更を表示 \(Show Rollback Changes\)\]](#) をクリックして変更を表示し、[\[ロールバックの変更を非表示 \(Hide Rollback Changes\)\]](#) をクリックして変更を非表示にします。

図 69: ロールバックの変更

Routing:| **Virtual Router: Virtual Router (Global)** | | |
Static Route IPv4:		
IPv4 Route:		
Static Route Interface(Unchanged): outside	outside	admin
Static Route Network(Unchanged): any-ipv4	any-ipv4	
Gateway: literal:10.10.35.63	literal:10.10.35.64	
Static Route IPv6:		
IPv6 Route:		
IPv6 Static Route Interface(Unchanged): inside	inside	admin
IPv6 Static Route Network(Unchanged): any-ipv6	any-ipv6	
IPv6 Static Route gateway: literal:20::20	literal:20::23	

 At the bottom right of the interface, there are buttons for 'Download as PDF' and 'OK'."/>

- [展開履歴のプレビュー (Deployment History Preview)] で、ロールバックの変更を表示できます。「[展開履歴の表示](#)」を参照してください。

ステップ 8 管理接続が再確立されたことを確認します。

Management Center で、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [管理 (Management)] > [FMCアクセスの詳細 (FMC Access Details)] > [接続ステータス (Connection Status)] ページで管理接続ステータスを確認します。

管理接続のステータスを表示するには、Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。[データインターフェイスでの管理接続のトラブルシューティング \(102 ページ\)](#) を参照してください。

クラスタのヘルスマニター設定の編集

[クラスタ (Cluster)] ページの [クラスタヘルスマニターの設定 (Cluster Health Monitor Settings)] セクションには、次の表で説明されている設定が表示されます。

図 70: クラスタのヘルスマニターの設定

Cluster Health Monitor Settings			
Timeouts			
Hold Time			3 s
Interface Debounce Time			9000 ms
Monitored Interfaces			
Service Application			Enabled
Unmonitored Interfaces			None
Auto-Rejoin Settings			
	Attempts	Interval Between Attempts	Interval Variation
Cluster Interface	-1	5	1
Data Interface	3	5	2
System	3	5	2

表 8: [クラスタヘルスマニターの設定 (Cluster Health Monitor Settings)] セクションテーブルのフィールド

フィールド	説明
タイムアウト	
保留時間 (Hold Time)	ノードの状態を確認するため、クラスタノードはクラスタ制御リンクで他のノードにハートビートメッセージを送信します。ノードが保留時間内にピアノードからハートビートメッセージを受信しない場合、そのピアノードは応答不能またはデッド状態と見なされます。
インターフェイスのデバウンス時間 (Interface Debounce Time)	インターフェイスのデバウンス時間は、インターフェイスで障害が発生していると思われ、クラスタからノードが削除されるまでの時間です。
Monitored Interfaces (モニタリング対象インターフェイス)	インターフェイスのヘルス チェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、またはクラスタに参加しようとしているかによって異なります。
サービスアプリケーション (Service Application)	Snort プロセスおよび disk-full プロセスが監視されているかどうかを示します。

フィールド	説明
モニタリング対象外のインターフェイス (Unmonitored Interfaces)	モニタリング対象外のインターフェイスを表示します。
自動再結合の設定	
クラスタインターフェイス (Cluster Interface)	クラスタ制御リンクの自動再結合の設定の不具合を表示します。
データインターフェイス (Data Interfaces)	データインターフェイスの自動再結合の設定を表示します。
システム (System)	内部エラー時の自動再結合の設定を表示します。内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーションステータスなどがあります。



(注) システムのヘルスチェックを無効にすると、システムのヘルスチェックが無効化されている場合に適用されないフィールドは表示されません。

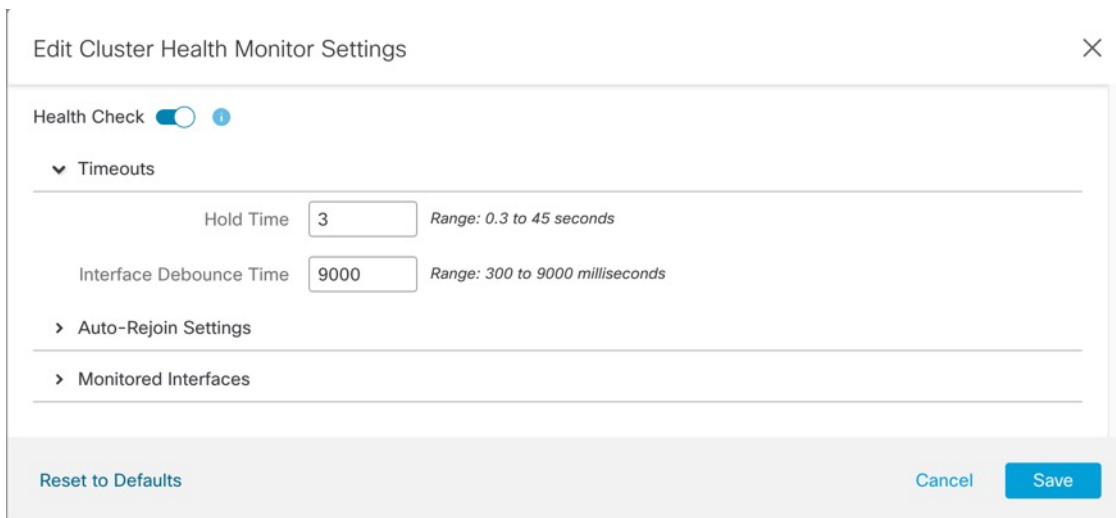
このセクションからこれらの設定を行うことができます。

任意のポートチャネル ID、単一の物理インターフェイス ID、Snort プロセス、および disk-full プロセスを監視できます。ヘルスマニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニターされています。

手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 変更するクラスタの横にある [編集 (Edit)] (✎) をクリックします。
- ステップ 3 [クラスタ (Cluster)] をクリックします。
- ステップ 4 [クラスタのヘルスマニターの設定 (Cluster Health Monitor Settings)] セクションで、[編集 (Edit)] (✎) をクリックします。
- ステップ 5 [ヘルスチェック (Health Check)] スライダをクリックして、システムのヘルスマニタリングを無効にします。

図 71: システムヘルスチェックの無効化



Edit Cluster Health Monitor Settings

Health Check ⓘ

▼ Timeouts

Hold Time Range: 0.3 to 45 seconds

Interface Debounce Time Range: 300 to 9000 milliseconds

> Auto-Rejoin Settings

> Monitored Interfaces

Reset to Defaults Cancel Save

何らかのトポロジ変更（たとえばデータインターフェ이스の追加/削除、ノードやスイッチのインターフェ이스の有効化/無効化、VSSやvPCを形成するスイッチの追加）を行うときには、システムのヘルスチェック機能を無効にし、無効化したインターフェ이스のモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェ이스をモニタリングできます。

ステップ 6 ホールド時間とインターフェ이스のデバウンス時間を設定します。

- [ホールド時間 (Hold Time)]: ノードのハートビート ステータス メッセージの時間間隔を指定します。指定できる範囲は3～45秒で、デフォルトは3秒です。
- [インターフェ이스のデバウンス時間 (Interface Debounce Time)]: デバウンス時間は300～9000 msの範囲で値を設定します。デフォルトは500 msです。値を小さくすると、インターフェ이스の障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェ이스のステータス更新が発生すると、インターフェ이스障害としてマーク付けされるまで、ノードは指定されたミリ秒数待機します。その後、ノードはクラスタから削除されます。EtherChannelがダウン状態からアップ状態に移行する場合（スイッチがリロードされた、スイッチでEtherChannelが有効になったなど）、デバウンス時間がより長くなり、ポートのバンドルにおいて別のクラスタノードの方が高速なため、クラスタノードでインターフェ이스の障害が表示されることを妨げることがあります。

ステップ 7 ヘルス チェック失敗後の自動再結合クラスタ設定をカスタマイズします。

図 72: 自動再結合の設定

▼ Auto-Rejoin Settings

Cluster Interface

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

Data Interface

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

System

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

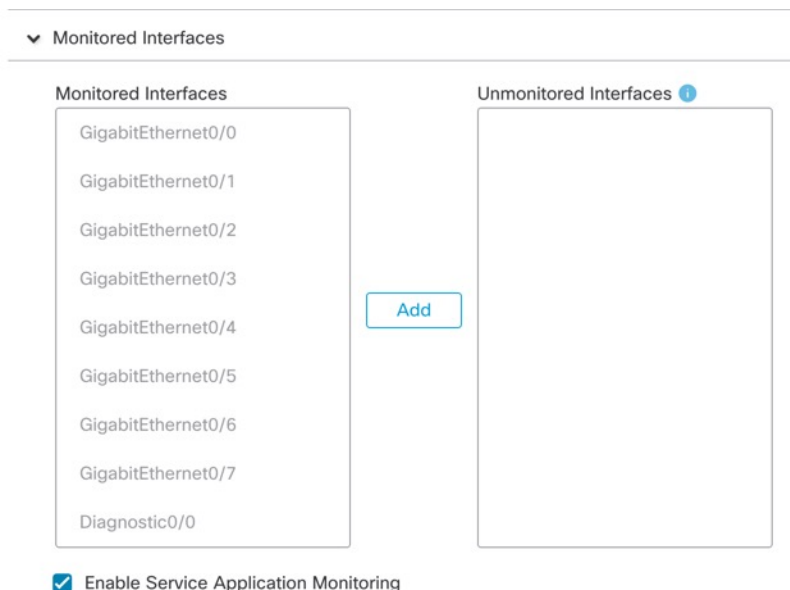
Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

[クラスタインターフェイス (Cluster Interface)]、[データインターフェイス (Data Interface)]、および[システム (System)]に次の値を設定します (内部エラーには、アプリケーションの同期タイムアウト、一貫性のないアプリケーションステータスなどがあります)。

- [試行数 (Attempts)]: 再結合の試行回数を 0 ~ 65535 の範囲の値に設定します。0 は自動再結合を無効化します。[クラスタインターフェイス (Cluster Interface)]のデフォルト値は -1 (無制限) です。[データインターフェイス (Data Interface)]と[システム (System)]のデフォルト値は 3 です。
- [試行の間隔 (Interval Between Attempts)]: 再結合試行の間隔を 2 ~ 60 の分単位で定義します。デフォルト値は 5 分です。クラスタへの再参加をノードが試行する最大合計時間は、最後の障害発生時から 14400 分 (10 日) に制限されます。
- [間隔のバリエーション (Interval Variation)]: 間隔を増加させるかどうかを定義します。1 ~ 3 の範囲で値を設定します (1: 変更なし、2: 直前の間隔の 2 倍、3: 直前の間隔の 3 倍)。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後 (2 x 5)、3 階目の試行が 20 分後 (2 x 10) となります。デフォルト値は、[クラスタインターフェイス (Cluster Interface)]の場合は 1、[データインターフェイス (Data Interface)]および[システム (System)]の場合は 2 です。

ステップ 8 [モニタリング対象のインターフェイス (Monitored Interfaces)]または[モニタリング対象外のインターフェイス (Unmonitored Interfaces)]ウィンドウでインターフェイスを移動して、モニタリング対象のインターフェイスを設定します。[サービスアプリケーションのモニタリングを有効にする (Enable Service Application Monitoring)]をオンまたはオフにして、Snort プロセスと disk-full プロセスのモニタリングを有効または無効にすることもできます。

図 73: モニタリング対象インターフェイスの設定



インターフェイスのヘルスチェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されません。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、またはクラスタに参加しようとしているかによって異なります。デフォルトでは、ヘルスチェックはすべてのインターフェイス、および Snort プロセスと disk-full プロセスで有効になっています。

必須以外のインターフェイスのヘルス モニタリングを無効にできます。

何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ノードやスイッチのインターフェイスの有効化/無効化、VSSやvPCを形成するスイッチの追加）を行うときには、システムのヘルスチェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェイスをモニタリングできます。

ステップ 9 [保存 (Save)] をクリックします。

ステップ 10 設定変更を展開します [設定変更の展開](#) を参照してください。

デバイスの管理設定の変更

マネージャの変更、マネージャの IP アドレスの変更などの管理タスクの実行が必要になる場合があります。

デバイスの Management Center IP アドレスまたはホスト名を編集する

Management Center の IP アドレスまたはホスト名を変更する場合は、設定が一致するようにデバイス CLI で値を変更する必要があります。ほとんどの場合、管理接続はデバイスの Management Center IP アドレスまたはホスト名を変更せずに再確立されますが、少なくともデバイスを Management Center に追加して NAT ID のみを指定した場合は、接続が再確立されるようにするために、このタスクを実行する必要があります。他の場合でも、Management Center IP アドレスまたはホスト名を最新の状態に維持して、ネットワークの復元力を高めることを推奨します。

手順

ステップ 1 Threat Defense CLI で、Management Center 識別子を表示します。

show managers

例 :

```
> 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
```

ステップ 2 Threat Defense CLI で、Management Center IP アドレスまたはホスト名を編集します。

configure manager edit identifier {hostname {ip_address | hostname} | displayname display_name}

Management Center が **DONTRESOLVE** と NAT ID によって最初に識別された場合、このコマンドを使用して値をホスト名または IP アドレスに変更できます。IP アドレスまたはホスト名を **DONTRESOLVE** に変更することはできません。

管理接続がダウンした後、再確立されます。 **sftunnel-status** コマンドを使用して、接続の状態をモニターできます。

例 :

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

新しい Management Center の特定

この手順は、管理対象デバイスの新しい Management Center を識別する方法を示します。新しい Management Center が古い 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 Management Center に管理対象デバイスが存在する場合はこれを削除します。Management Center からのデバイスの削除（登録解除）（47 ページ）を参照してください。

Management Center とのアクティブな接続がある場合は、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 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} : 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** : 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 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 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。Threat Defense を追加するときに、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、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。Threat Defense を追加するときに、Management Center で同じ NAT ID を指定します。
- *display_name* : **show managers** コマンドでこのマネージャを表示するための表示名を指定します。このオプションは、CDO をプライマリマネージャおよび分析専用のオンプレミス 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 Management Center に追加します。登録キーを使用した Management Center へのデバイスの追加 (32 ページ) を参照してください。

Device Manager から Management Center への切り替え

Device Manager から 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。

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

始める前に

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

手順

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

ステップ2 (必要に応じて) 管理インターフェイスを設定します。

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

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

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

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

図 74 : Management Center/CDO の詳細

Configure Connection to Management Center or CDO


Provide details to register to the management center/CDO.

Management Center/CDO Details

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

Yes No


Threat Defense



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

→

Management Center/CDO



10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

●●●● 👁

NAT ID

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

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup ▼

Management Center/CDO Access Interface

Data Interface

Please select an interface ▼

Management Interface [View details](#)

CANCEL
CONNECT

- a) [Management Center/CDOのホスト名またはIPアドレスを知っていますか (Do you know the FMC hostname or IP address)] で、IP アドレスまたはホスト名を使用して Management

Center に到達できる場合は [はい (Yes)] をクリックし、Management Center が NAT の背後にあるか、パブリック IP アドレスまたはホスト名がない場合は [いいえ (No)] をクリックします。

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

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

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

- d) [NAT ID] を指定します。

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

ステップ 5 [接続の設定 (Connectivity Configuration)] を設定します。

- a) [FTD ホスト名 (FTD Hostname)] を指定します。

Management Center/CDO アクセスマインターフェイスのアクセスにデータインターフェイスを使用する場合、この FQDN がこのインターフェイスに使用されます。

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

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

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

Management Center では、この Threat Defense デバイスに割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。Management Center に Threat Defense デバイスを追加すると、ローカル設定が維持され、DNS サーバーはプラッ

トフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む Threat Defense デバイスに後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。Management Center と Threat Defense デバイスを同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

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

FMC アクセスインターフェイスに管理インターフェイスを選択する場合は、この設定で管理 DNS サーバーを構成します。

- c) **Management Center/CDO アクセスインターフェイス**については、任意の構成済みインターフェイスを選択してください。

管理インターフェイスは、Threat Defense デバイスを Management Center に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。

- ステップ 6** (任意) 外部インターフェイスではないデータインターフェイスを選択した場合は、デフォルトルートを追加します。

インターフェイスを通過するデフォルトルートがあることを確認するように求めるメッセージが表示されます。外部を選択した場合は、セットアップウィザードの一環としてこのルートがすでに設定されています。別のインターフェイスを選択した場合は、Management Center に接続する前にデフォルトルートを手動で設定する必要があります。

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

- ステップ 7** (任意) データインターフェイスを選択した場合は、[ダイナミック DNS (DDNS) 方式の追加 (Add a Dynamic DNS (DDNS) method)] をクリックします。

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

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

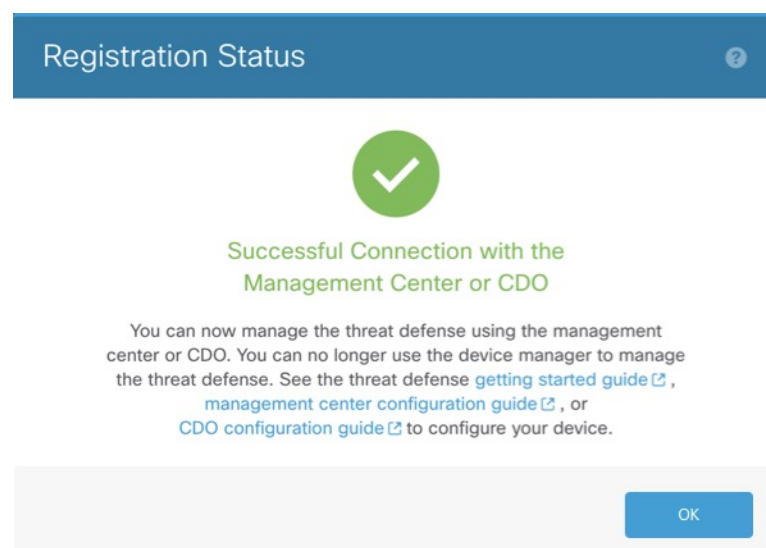
マネージャアクセスに管理インターフェイスを使用する場合、DDNS はサポートされません。

- ステップ 8** [接続 (Connect)] をクリックします。[登録ステータス (Registration Status)] ダイアログボックスには、Management Center への切り替えに関する現在のステータスが表示されます。[Management Center/CDO 登録設定の保存 (Saving Management Center/CDO Registration Settings)] のステップの後、Management Center に移動してファイアウォールを追加します。

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

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

図 75: 正常接続



Management Center から Device Manager への切り替え

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

ソフトウェアを再インストールすることなく、Management Center から Device Manager に切り替えることができます。Management Center から Device Manager に切り替える前に、Device Manager がすべての設定要件を満たしていることを確認します。Device Manager から Management Center に切り替える場合は、[Device Manager から Management Center への切り替え \(126 ページ\)](#) を参照してください。



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

手順

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

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

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

管理 IP アドレスに接続できない場合は、次のいずれかを実行します。

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

ステップ 3 現在リモート管理モードになっていることを確認します。

show managers

例 :

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

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

configure manager delete uuid

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

例 :

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

>
> show managers
No managers configured.
```

ステップ 5 ローカル マネージャを設定します。

configure manager local

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

例：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

シリアル番号（ロー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 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（ゼロタッチプロビジョニング）を使用した Management Center へのデバイスの追加（36 ページ）](#)」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。

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 Threat Defense 初期設定の完了（14 ページ）](#) または [Device Manager を使用した 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 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、CDOに「シリアル番号がすでに要求されている (Serial Number Already Claimed)」というエラーが表示されます。

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、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（ゼロタッチプロビジョニング）を使用した Management Center へのデバイスの追加（36 ページ）](#)

Device Manager を使用したロータッチプロビジョニングの再起動

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、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 \(133 ページ\)](#) を参照してください。

1. 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. [Cisco Defense Orchestrator または 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 (ゼロ タッチ プロビジョニング) を使用した [Management Center へのデバイスの追加 \(36 ページ\)](#)

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 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。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。

新しいモデルへの設定の移行

Firewall Threat Defense のモデル移行ウィザードを使用すると、古い脅威防御モデルから新しいモデルに設定を移行できます。ソースデバイスインターフェイスをターゲットデバイスインターフェイスにマップできます。移行前のソースデバイスとターゲットデバイスはロックされています。

移行でサポートされるデバイス

サポートされているソースデバイス

- Cisco Firepower 1120

- Cisco Firepower 1140
- Cisco Firepower 1150
- Cisco Firepower 2110
- Cisco Firepower 2120
- Cisco Firepower 2130
- Cisco Firepower 2140



(注) ソースデバイスはバージョン 7.0 以降である必要があります。

サポートされるターゲットデバイス

- Cisco Secure Firewall 3105
- Cisco Secure Firewall 3110
- Cisco Secure Firewall 3120
- Cisco Secure Firewall 3130
- Cisco Secure Firewall 3140



(注) Cisco Secure Firewall 3110、3120、3130、および 3140 デバイスは、バージョン 7.1 以降である必要があります。Cisco Secure Firewall 3105 は、バージョン 7.3 以降である必要があります。

移行用のライセンス

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

- ソースデバイスとターゲットデバイスを **Management Center** に登録する必要があります。
- 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。
- ターゲットデバイスは、何も設定されていない新しく登録されたデバイスにすることを推奨します。
- ソースデバイスとターゲットデバイスは以下の点と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
- ターゲットデバイスは以下の状態にはできません。
 - マルチインスタンスモード
 - クラスタの一部
- ユーザーは、デバイスの変更権限を持っている必要があります。
- 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。
- ソースデバイスには、保留中の展開を設定できます。ただし、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。
- ソースデバイスが HA ペアの一部である場合、ターゲットデバイスが HA ペアの一部である必要はなく、その逆も同様です。移行によって HA ペアが形成されることも、分断されることもありません。

ウィザードで移行される設定

移行ウィザードにより、次の設定が送信元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
- 仮想ルータ設定
- 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送信元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
- マルウェアポリシーとファイルポリシー
- アイデンティティ 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送信元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
- Static Route
- マルチキャスト ルーティング
- [仮想ルータ (Virtual Router)]

移行ウィザードにより、次のインターフェイスが送信元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

移行の制限事項

- ウィザードは移行しません。
 - サイト間 VPN ポリシー
 - SNMP の構成

移行後、デバイスのプラットフォーム設定を使用して SNMP を設定できます。
- 一度に実行できる移行は 1 つだけです。
- 送信元インターフェイスの速度、自動ネゴシエーション、およびデュプレックス設定がターゲットデバイスのマッピングされたインターフェイスに対して有効な場合、値がコピーされます。有効でない場合、これらのパラメータはデフォルト値に設定されます。
- リモートアクセス VPN トラストポイント証明書が登録されていません。トラストポイント証明書は、展開前に手動で登録する必要があります。
- デフォルトでは、移行後にソースデバイスで Snort2 が使用されている場合でも、ターゲットデバイスでは Snort 2 ではなく Snort 3 が使用されます。
- HA デバイスの場合：
 - ターゲットデバイス：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。
 - ソースデバイスとターゲットデバイス：ウィザードでは、監視対象インターフェイス、フェールオーバーのトリガー基準、インターフェイス MAC アドレスなどの HA 構成は移行されません。移行後に、必要なパラメータを手動で設定する必要があります。

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** [デバイス (Devices)] > [デバイス管理 (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、[移行のベストプラクティス \(141 ページ\)](#) に記載されているアクションを実行してください。

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。

- 送信元デバイスが稼働中の場合は、インターフェイスの IP アドレスを変更します（それらのアドレスが送信元デバイスからターゲットデバイスにコピーされるため）。
- 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。
- HAセットアップがある場合は、監視対象インターフェイス、フェールオーバーのトリガー基準、インターフェイス MAC アドレスなどの HA パラメータを設定します。
- 移行後にリセットされる診断インターフェイスを設定します。
- (任意) デバイスのプラットフォーム設定を使用して 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 Device Configuration Guide』またはオンラインヘルプの「*Change the Manager Access Interface from Management to Data*」を参照してください。
- (任意) 必要に応じてサイト間 VPN を設定します。これらの設定は、送信元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)] > [高度な展開 (Advanced Deploy)] を選択し、デバイスの [プレビュー (Preview)] (🔍) アイコンをクリックします。

デバイス管理の基本の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
Firepower 4100/9300 のシャーシレベルのヘルスアラート。	7.4.1	7.4.1	<p>アップグレードの影響。新しい正常性モジュールを有効にし、アップグレード後にデバイス正常性ポリシーを適用します。</p> <p>シャーシを読み取り専用デバイスとして Management Center に登録することで、Firepower 4100/9300 のシャーシレベルのヘルスアラートを表示できるようになりました。また、Firewall Threat Defense プラットフォーム障害のヘルスマジュールを有効にして、ヘルスポリシーを適用する必要があります。アラートは、メッセージセンター、ヘルスマニター（左側のペインの [デバイス (Devices)] でシャーシを選択）、およびヘルスイベントビューに表示されます。</p> <p>マルチインスタンスモードで Cisco Secure Firewall 3100 のシャーシを追加し、正常性アラートを表示することもできます。これらのデバイスの場合は、Management Center を使用してシャーシを管理します。ただし、Firepower 4100/9300 シャーシの場合は、シャーシマネージャまたは FXOS CLI を使用する必要があります。</p> <p>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)]>[シャーシ (Chassis)]</p> <p>参照：「Add a Chassis to the Management Center」</p>
デバイスまたはデバイスクラスターの CLI 出力を表示します。	7.4.1	任意 (Any)	<p>デバイスまたはクラスターのトラブルシューティングに役立つ一連の定義済み CLI 出力を表示できます。また、任意の show コマンドを入力して、出力を確認できます。</p> <p>新規/変更された画面：[デバイス (Devices)]>[デバイス管理 (Device Management)]>[クラスター (Cluster)]>[全般 (General)]</p>

機能	最小 Management Center	最小 Threat Defense	詳細
<p>トラブルシューティングファイルの生成とダウンロードは、[デバイス (Device)]および[クラスタ (Cluster)]ページから実行できます。</p>	<p>7.4.1</p>	<p>7.4.1</p>	<p>[デバイス (Device)]ページの各デバイス、および[クラスタ (Cluster)]ページのすべてのクラスタノードのトラブルシューティングファイルを生成およびダウンロードできます。クラスタの場合、すべてのファイルを単一の圧縮ファイルとしてダウンロードできます。クラスタノードのクラスタのクラスタログを含めることもできます。または、[デバイス (Devices)]>[デバイス管理 (Device Management)]>その他 (☰) >[トラブルシューティングファイル (Troubleshoot Files)]メニューからファイル生成をトリガーできます。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • [デバイス (Devices)]>[デバイス管理 (Device Management)]>[デバイス (Device)]>[全般 (General)] • [デバイス (Devices)]>[デバイス管理 (Device Management)]>[クラスタ (Cluster)]>[全般 (General)]
<p>シリアル番号を使用して Firepower 1000/2100 および Cisco Secure Firewall 3100を Management Center に登録するゼロ タッチ プロビジョニング。</p>	<p>7.4.0</p>	<p>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</p>	<p>ゼロ タッチ プロビジョニングを使用すると、Firepower 1000/2100 および Cisco Secure Firewall 3100 デバイスで初期セットアップを実行することなく、シリアル番号でデバイスを Management Center に登録できます。Management Center は、この機能のために SecureX および Cisco Defense Orchestrator と統合されています。</p> <p>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 (Device)]>[シリアル番号 (Serial Number)]</p> <p>その他のバージョンの制限：この機能は、Management Center がパブリックに到達できない場合、バージョン7.3.xまたは7.4.0 Threat Defense デバイスではサポートされません。サポートは、バージョン7.4.1 で再開されています。</p>

機能	最小 Management Center	最小 Threat Defense	詳細
マージされた管理インターフェイスと診断インターフェイス。	7.4.0	7.4.0	<p>アップグレードの影響。アップグレード後にインターフェイスをマージします。</p> <p>7.4以降を使用している新しいデバイスの場合、レガシー診断インターフェイスは使用できません。マージされた管理インターフェイスのみを使用できます。</p> <p>7.4 以降にアップグレードした場合：</p> <ul style="list-style-type: none"> 診断インターフェイスの設定がない場合は、インターフェイスが自動的にマージされます。 診断インターフェイスの設定がある場合は、インターフェイスを手動でマージすることも、診断インターフェイスを引き続き個別に使用することもできます。ただし、診断インターフェイスのサポートは今後のリリースで廃止されるため、できるだけ早くインターフェイスをマージしてください。 <p>マージモードでは、デフォルトでデータルーティングテーブルを使用するように AAA トラフィックの動作も変更されます。管理専用ルーティングテーブルは、設定で管理専用インターフェイス（管理を含む）を指定した場合にのみ使用できるようになりました。</p> <p>プラットフォーム設定の場合、これは次のことを意味します。</p> <ul style="list-style-type: none"> 診断インターフェイスで、HTTP、ICMP、または SMTP を有効にすることはできなくなりました。 SNMP については、診断インターフェイスではなく管理インターフェイスでホストを許可できます。 Syslog サーバーについては、診断インターフェイスではなく管理インターフェイスでアクセスできます。 Syslog サーバーまたは SNMP ホストのプラットフォーム設定で診断インターフェイスが名前指定されている場合、マージされたデバイスとマージされていないデバイスに別々のプラットフォーム設定ポリシーを使用する必要があります。 インターフェイスを指定しない場合、DNS ルックアップは管理専用ルーティングテーブルにフォールバックしなくなりました。 <p>新規/変更された画面：[デバイス (Devices)]>[デバイス管理 (Device Management)]>[インターフェイス (Interfaces)]</p> <p>新規/変更されたコマンド： show management-interface convergence</p>

機能	最小 Management Center	最小 Threat Defense	詳細
Firepower 1000/2100 から Cisco Secure Firewall 3100 への移行。	7.4.0	いずれか	<p>Firepower 1000/2100 から Cisco Secure Firewall 3100 に設定を簡単に移行できるようになりました。</p> <p>新規/変更された画面：[デバイス (Devices)]>[デバイス管理 (Device Management)]>[移行 (Migrate)]</p> <p>プラットフォームの制限：Firepower 1010 または 1010E からの移行はサポートされていません。</p>
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	いずれか	<p>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。</p>
データインターフェイスを使用して、Threat Defense ハイアベイラビリティペアを管理します。	7.4.0	7.4.0	<p>Threat Defense ハイアベイラビリティでは、Management Center との通信に通常のデータインターフェイスを使用できるようになりました。以前は、スタンドアロンデバイスのみがこの機能をサポートしていました。</p> <p>参照：「Using the Threat Defense Data Interface for Management」</p>
クラスタのヘルスマニターの設定。	7.3.0	いずれか	<p>クラスタのヘルスマニター設定を編集できるようになりました。</p> <p>新規/変更された画面：[デバイス (Devices)]>[デバイス管理 (Device Management)]>[クラスタ (Cluster)]>[クラスタのヘルスマニターの設定 (Cluster Health Monitor Settings)]</p> <p>(注) 以前に FlexConfig を使用してこれらの設定を行った場合は、展開前に必ず FlexConfig の設定を削除してください。削除しなかった場合は、FlexConfig の設定によって Management Center の設定が上書きされます。</p>

機能	最小 Management Center	最小 Threat Defense	詳細
冗長マネージャアクセス データ インターフェイス。	7.3.0	7.3.0	<p>マネージャアクセスにデータインターフェイスを使用する場合、プライマリインターフェイスがダウンしたときに管理機能を引き継ぐよう、セカンダリインターフェイスを構成できます。デバイスは、SLA モニタリングを使用して、スタティックルートの実行可能性と、両方のインターフェイスを含むECMPゾーンを追跡し、管理トラフィックで両方のインターフェイスが使用できるようにします。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • [デバイス (Devices)]>[デバイス管理 (Device Management)]> [デバイス (Device)]>[管理 (Management)] • [デバイス (Devices)]>[デバイス管理 (Device Management)]> [デバイス (Devices)]>[インターフェイス (Interfaces)]>[マネージャアクセス (Manager Access)]
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。
ポリシーのロールバックは高可用性デバイスでサポートされています。	7.2.0	7.2.0	configure policy rollback コマンドは高可用性デバイスでサポートされています。

機能	最小 Management Center	最小 Threat Defense	詳細
マルチマネージャのサポート。	7.2.0	7.2.0	<p>クラウド提供型の管理センターを導入しました。このクラウド提供型の管理センターは、Cisco Defense Orchestrator (CDO) プラットフォームを使用して、複数の Cisco 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。</p> <p>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。</p> <p>新規/変更されたコマンド：configure manager add、configure manager delete、configure manager edit、show managers</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> クラウド管理型デバイスをハードウェアまたは仮想管理センターに追加する場合は、新しい[CDO管理対象デバイス (CDO Managed Device)]チェックボックスをオンにして、それが分析専用であることを指定します。 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択すると、分析専用のデバイスが表示されます。 <p>詳細については、CDO ドキュメントを参照してください。</p>
アクセスコントロールルールではオブジェクトグループ検索がデフォルトで有効です。	7.2.0	7.2.0	<p>バージョン 7.2.0 以降の管理対象デバイスでは、オブジェクトグループ検索の設定がデフォルトで有効です。このオプションは、[デバイス管理 (Device Management)] ページでデバイス設定を編集するときの [詳細設定 (Advanced Settings)] セクションにあります。</p>
展開で管理接続が失われた場合の自動ロールバック。	7.2.0	7.2.0	<p>展開によって Management Center と Threat Defense 間の管理接続がダウンした場合に備えて、設定の自動ロールバックを有効にできるようになりました。以前は、configure policy rollback コマンドを使用して手動で設定をロールバックすることしかできませんでした。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> [デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [展開設定 (Deployment Settings)] [展開 (Deploy)] > [高度な展開 (Advanced Deploy)] > [プレビュー (Preview)] [展開 (Deploy)] > [展開履歴 (Deployment History)] > [プレビュー (Preview)]

機能	最小 Management Center	最小 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。
デバイス設定のインポート/エクスポート。	7.1.0	7.1.0	次の使用例で、デバイス固有の設定をエクスポートし、同じデバイスに保存された設定をインポートできます。 <ul style="list-style-type: none"> • デバイスを別の FMC に移動する。 • 古い設定を復元する。 • デバイスを再登録する。 新規/変更された画面: [デバイス (Devices)]>[デバイス管理 (Device Management)]>[デバイス (Device)]>[全般 (General)]
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。FMCCLI 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)]
FTD での FMC IP アドレスの更新。	6.7.0	6.7.0	FMC IP アドレスを変更する場合に、FTD CLI を使用してデバイスを更新できるようになりました。 新規/変更されたコマンド: configure manager edit

機能	最小 Management Center	最小 Threat Defense	詳細
Firepower Chassis Manager へのリンクアクセス。	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。