デバイス テンプレートを使用したデバイスの登録

デバイステンプレートを使用して、Firewall Management Center にデバイスを追加できます。

デバイステンプレートを使用したデバイス登録について

デバイステンプレートを使用すると、事前にプロビジョニングされた初期デバイス設定を使用して、複数のブランチデバイスを展開できます。デバイステンプレートを使用して、複数のデバイスの一括ゼロタッチプロビジョニングを実行し、異なるインターフェイス設定を持つ複数のデバイスにDay 2設定変更を適用し、既存のデバイスから設定パラメータを製できます。また、シリアル番号を使用して、一度に複数のデバイスをFirewall Management Centerに登録することもできます。

基本的な初期設定を使用してデバイスを登録する場合、アクセス コントロール ポリシーやライセンスなどの制限された設定を適用できます。その後、デバイス登録後に、インターフェイス、ルーティング、サイト間 VPN 設定などの他のデバイス設定を個別に設定する必要があります。デバイステンプレートでは、これらの設定を事前に設定し、登録時に適用できるようにすることができます。IPアドレスなど、デバイスごとに一意である必要がある値は、登録時に定義する変数およびネットワーク オブジェクト オーバーライドを使用して定義できます。

デバイステンプレートでのサイト間VPN接続を設定することもできます。デバイステンプレートのサイト間 VPN 接続は、デバイスが属する必要があるサイト間 VPN トポロジを定義します。VPN 設定と他のデバイス テンプレート ポリシーおよび設定により、ブランチ デバイスをネットワークに簡単に展開できます。デバイステンプレートは、スポークとしてのデバイス設定のみをサポートします。デバイスは、複数のハブ アンド スポーク サイト間 VPN トポロジの一部にすることができます。

設定されたデバイステンプレートがデバイスに適用されると、変数が解決され、保護されたネットワークのオーバーライドが設定され、デバイスが指定されたVPNトポロジのスポークとして追加されます。

テンプレートを使用してデバイスを登録する方法

次の方法でデバイス テンプレートを使用して、Firewall Management Center にデバイスを登録し、デイゼロ設定をセットアップすることができます。

- 登録キー：登録キーを指定し、Firewall Management Centerで変数を定義することで、単一のデバイスを登録できます。
- シリアル番号：ゼロタッチプロビジョニングを使用して、シリアル番号で1つ以上のデバイスを登録できます。シリアル番号の登録では、アップロードする CSV ファイルですべての変数とオーバーライドを定義します。

変数およびネットワーク オブジェクトのオーバーライド

変数とネットワーク オブジェクトのオーバーライドを使用してテンプレート設定をパラメータ化できます。

変数は、テンプレート構成でサポートされているオブジェクト タイプです。変数は、テンプレートにおけるデバイスの特定の設定値を定義します。これらの変数は、テンプレートの登録時および適用時に、デバイスで定義できます。変数を使用するフィールドには変数アイコン（x）が表示されます。変数は、他の値と区別するために、$ というプレフィックスを付けて表示されます。

サポートされている変数のタイプと変数の作成については、サポートされる変数 と 変数の追加を参照してください。

ネットワーク オブジェクトのオーバーライドは変数に似ています。ただし、これらはネットワーク オブジェクトのオーバーライド値を提供するために使用されます。テンプレートでネットワーク オブジェクトのリストを宣言し、これらのオブジェクトのネットワーク オブジェクト オーバーライドを作成できます。デバイスでテンプレートを適用する際に、これらのネットワーク オブジェクト オーバーライドの値を指定できます。たとえば、テンプレートでホストネットワーク オブジェクトを定義すると、デバイスでのテンプレートの適用前にネットワークオブジェクトのオーバーライドを追加し、デバイスでのテンプレートの適用中に関連する値を指定できます。

サポートされているネットワーク オブジェクトとネットワーク オブジェクト オーバーライドの追加の詳細については、 サポートされているネットワーク オブジェクトのオーバーライド および ネットワーク オブジェクト オーバーライドの追加を参照してください。

モデルマッピング

インターフェイス設定はデバイス モデルによって異なるため、テンプレートのインターフェイス設定をデバイスのターゲット インターフェイスにコピーする必要があります。モデルマッピングを使用すると、テンプレートで定義されたインターフェイスから、必要な Firewall Threat Defense モデルのインターフェイスへのマッピングを定義できます。デバイスでのテンプレートの適用中に、インターフェイス設定の変数は、指定した値で置き換えられ、デバイス上のマッピングされたインターフェイスにコピーされます。デバイスでテンプレートの適用を開始する前に、テンプレートでモデルマッピングを作成する必要があることに注意してください。モデル マッピングの設定の詳細については、 モデルマッピングの追加を参照してください。

テンプレートと高可用性

デバイス登録後に、Firewall Threat Defense 高可用性デバイスにデバイス テンプレートを適用できます。高可用性固有の構成は、デバイス テンプレートではサポートされていません。ターゲットの高可用性デバイス ペア設定の一部である高可用性設定とモニター対象インターフェイスは変更されません。フェールオーバー インターフェイスにテンプレート インターフェイスをマッピングすることはできません。

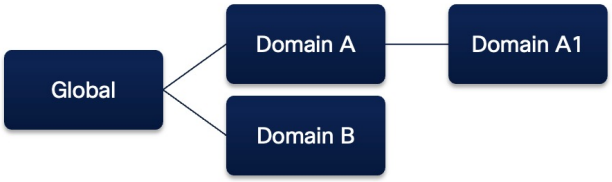
高可用性デバイス ペアからデバイス テンプレートを生成できます。デバイスでのテンプレートの適用、テンプレートの生成、テンプレートのインポート、およびエクスポートなどのテンプレート操作は、アクティブ ユニットでのみ実行できます。スタンバイ装置でこれらの操作を実行することはできません。

テンプレートとドメイン

デバイス テンプレートはどのドメインにも配置できます。子ドメインにいる場合は、ドメイン階層の上のテンプレートへの読み取り専用アクセス権があります。デバイスのドメインまたは親ドメインからテンプレートをデバイスに適用できます。デバイスからテンプレートを生成し、そのテンプレートをドメイン階層内の任意のドメイン内のデバイスに適用できます。

ドメイン階層の例を、サポートされているデバイス テンプレートの適用と生成シナリオを示す表とともに示します。

次のような例が考えられます。



- ドメイン A および B は、グローバル ドメインの子ドメインです。
- ドメイン A1 は、ドメイン A の子ドメインです。

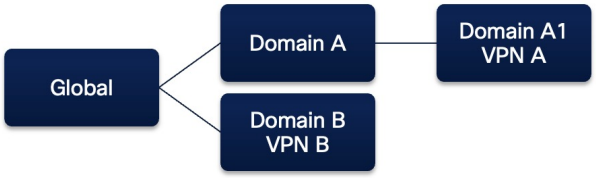
テンプレート ドメイン	デバイス ドメイン	サポートされるデバイス テンプレートの適用/生成
グローバル	A1	Yes
グローバル	B	はい
A	A1	はい
A	B	非対応
B	A1	非対応
B	B	Yes
A1	A1	はい
A1	B	いいえ

ドメインおよび VPN 接続

- テンプレートは、グローバル ドメインまたは子/リーフ ドメインで定義できます。ただし、VPN トポロジはリーフ ドメインでのみ定義できます。
- すべてのドメインのテンプレートで VPN 接続を設定できます。デバイスが VPN トポロジと同じドメインにある場合にのみ、テンプレートの適用中に VPN 接続がデバイスに適用されます。

ドメイン階層の例を、サポートされているデバイステンプレートの適用と生成シナリオを示す表とともに示します。

次のような例が考えられます。



- ドメイン A および B は、グローバル ドメインの子ドメインです。
- ドメイン A1 は、ドメイン A の子ドメインです。
- VPN A はドメイン A1 の一部です。
- VPN B はドメイン B の一部です。

テンプレート ドメイン	テンプレートの VPN トポロジ	デバイス ドメイン	サポートされるデバイス テンプレートの適用/生成
グローバル	VPN A VPN B	A1	いいえ
グローバル	VPN B	B	はい
A	VPN A	A1	対応
B	VPN B	A1	非対応
B	VPN B	B	Yes
A1	VPN A	A1	はい

デバイスでのテンプレートの適用前と後のテンプレート設定の検証

テンプレート設定の検証は、デバイスでのテンプレートの適用の前後に行われます。

タスクの開始時に、次の検証チェックが実行され、デバイスにテンプレートが適用されます。

- ターゲット デバイス モデルとバージョンがサポートされていることを確認します。
- クラスタとコンテナのチェック: デバイスは、クラスタまたはマルチインスタンスの一部であってはなりません。
- モデル マッピングの検証：ターゲット デバイス モデルのモデル マッピングが存在し、有効であること。
- テンプレート パラメータ値の健全性チェック。たとえば、インターフェイスの IP アドレスとして使用する 2 つの変数に同じ値を指定することはできません。

デバイスにテンプレートを適用するタスクの最後に次の検証チェックが実行され、適用された設定が有効であることが確認されます。

- インターフェイス構成たとえば、2 つ以上のインターフェイスの IP アドレス フィールドに使用する変数に同じ IP アドレス値を設定することはできません。
- ルーティング ポリシーの検証たとえば、BGP ネイバー コンフィギュレーションの IPv4 アドレスが、インターフェイスの IP アドレスと重複しないようにする必要があります。

デバイスにテンプレートを適用するタスクの最後に行われる検証チェックが失敗した場合、適用された設定がロールバックされ、デバイスは元の状態に復元されます。

デバイス テンプレートを使用したデバイス登録の前提条件

モデルのサポート

デバイス テンプレートは、Secure Firewall バージョン7.4.1以降を実行している次のモデルで、オンプレミス Firewall Management Center、Cloud-Delivered Firewall Management Center（cdFMC）でサポートされています。

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

デバイス テンプレートでの VPN 接続の前提条件

- デバイス テンプレートで使用する必要があるサイト間 VPN トポロジを設定します。
- 認証方式、IKE ポリシー、IPsec ポリシーなど、すべてのハブおよび VPN トポロジ関連の設定が完了していることを確認します。
- VPN ハブ アンド スポーク トポロジでサポートされているタイプは次のとおりです。
  - ポリシーベース
  - ルートベース
  - SD-WAN
- Firewall Threat Defense デバイスのインターフェイスに、適切な論理名とIPアドレスを割り当てます。たとえば、LANに接続されたインターフェイスには*inside*を使用し、インターネットまたは WAN に接続されたインターフェイスには *outside* を使用します。
- スポーク デバイスはバージョン 7.4.1 以降である必要があります。

デバイス テンプレートを使用したデバイス登録のライセンス

- デバイス テンプレートには、特定のライセンス要件はありません。

- スマート ライセンス アカウントには、ターゲット デバイスのライセンス利用資格が必要です。
- テンプレートで VPN を設定するには、Essentials ライセンスによりエクスポート制御機能が許可されている必要があります。Firewall Management Center でこの機能を確認するには、**System** (⚙) > **Licenses** > **Smart Licenses** を選択します。
- デバイスにテンプレートを適用する場合は、Secure Client ライセンスに関する次の条件に注意してください。

Secure Client ライセンスを持つデバイス	Secure Client ライセンスを持つテンプレート	デバイス テンプレート適用後の Secure Client ライセンス
はい	はい	テンプレート ライセンス
はい	いいえ	デバイスライセンス
非対応	○	テンプレート ライセンス

デバイステンプレートを使用したデバイス登録のガイドライン

一般的なガイドライン

- VNI と VTEP 以外のすべてのデバイス設定がサポートされます。
- 共有ポリシーと S2S VPN ポリシーをテンプレートにアタッチできます。これらのポリシーは、テンプレートの適用中に割り当てられます。
- テンプレートは HA デバイスに適用可能ですただし、HA デバイス ペア登録中のデバイス テンプレートの適用はサポートされていません。また、フェールオーバー リンク、スタンバイ IP アドレスなどの HA 関連の設定を管理することもできません。詳細については、Threat Defense HA デバイスでのデバイステンプレートの操作を参照してください。
- デバイス テンプレートの操作は、アクティブな Firewall Management Center でのみサポートされます。スタンバイ ピアは、デバイス テンプレートの操作をサポートしていません。
- テンプレート名とデバイス表示名が同じでないことを確認します。
- デバイスのバックアップまたは復元操作中にテンプレートを作成または削除しないでください。
- デバイスにテンプレートを適用した後、マネージャ アクセスが管理からデータインターフェイスに、またはその逆に変更された場合、デバイスとの管理接続を再確立する必要があります。テンプレートの適用中にマネージャ アクセス インターフェイスを変更することはできないことに注意してください。

- Firewall Management Center には最大 250 のデバイステンプレートを追加できます。
- データ インターフェイスを介して管理されるデバイス用に作成および設定されたテンプレートを使用して、管理インターフェイスを介して管理されるデバイスを登録および適用することはできません。
- デバイスの登録とテンプレートの適用は、変更管理ワークフローでは処理されません。アクセス ポリシー、テンプレート、テンプレート変数、テンプレートで宣言されたネットワーク オーバーライド、テンプレート適用操作で使用されるテンプレート設定など、承認済みのデータのみが使用されます。
- シリアル番号とアクセス コントロール ポリシーを使用したデバイス登録は、一度に 1 つのデバイスでのみサポートされます。
- シリアル番号を使用してデバイスを追加する場合、IPv6 DHCP 検出可能性を備えたデバイスはサポートされません。
- すでに登録されているデバイスにテンプレートを適用すると、テンプレート内の設定はターゲット デバイスにのみコピーされます。その後、設定を手動でデバイスに展開するか、コピーした設定をデバイスにそのままにして後で展開するかを選択できます。ただし、デバイスのオンボーディング中にテンプレートを適用すると、テンプレートの設定がターゲットデバイスにコピーされ、既存の動作に従って、デバイス登録後にデバイスに自動的に展開されます。
- モデルマッピングに変更を加えると、デバイスが「非同期」としてマークされます。対応するモデル マッピングでインターフェイス マッピングに変更を加えた場合、または以前のテンプレートの適用後に設定を変更した場合は、テンプレートをデバイスに再適用することを検討してください。
- デバイステンプレートは、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でのみサポートされます。詳細については、コンフィギュレーション ガイドの管理インターフェイスと診断インターフェイスのマージを参照してください。
- テンプレート設定の更新は、変更管理によってサポートされています。デバイス テンプレートの作成と適用は、変更管理ではサポートされていません。
- デバイスの設定変更をテンプレートに同期することはできません。テンプレートを使用してデバイス設定を変更する際のいくつかのサンプル シナリオと、推奨される解決策を次に示します。
  - 複数のデバイスに変更を反映する前に 1 つのデバイスで新しい設定変更をテストする場合は、テンプレートに変更を加え、そのテンプレートを 1 つのデバイスに適用することを推奨します。そのデバイスで変更を検証してから、テンプレートを他のデバイスに適用します。
  - デバイスの現在の設定との間に重要な逸脱が生じるような多くの変更を行い、それらの変更を他のデバイスに反映させる場合は、次のいずれかのオプションを選択できます。
    - 現在のテンプレートをエクスポートして、テンプレートのコピーを取得します。その後、テンプレートに必要な変更を加えて、1 つのデバイスに適用できます。

そのデバイスで変更を検証してから、テンプレートを他のデバイスに適用します。

- また、デバイスに必要な変更を加えて、そのデバイスからテンプレートを作成することもできます。その後、他のデバイスに変更を適用して検証できます。ただし、変数やネットワーク オブジェクト オーバーライドなどのテンプレート パラメータが作成されたテンプレートに存在しないため、これはお勧めしません。

- 特定のデバイスの設定がテンプレートの設定と大幅に異なっている場合は、このデバイスにテンプレートを使用しないようにして、デバイスとテンプレートの関連付けを **[関連デバイス（Associated Devices）]** ウィンドウから削除することもできます。

VPN 接続に関するガイドライン

- VPN トポロジでサポートされるインターフェイスは、次のとおりです。

トポロジタイプ	インターフェイス タイプ

ポリシーベース および SD-WAN	• 物理インターフェイス
	  • 非管理
	  • インターフェイスモードは「ルーテッド」または「なし」のいずれかにする必要があります
	• サブインターフェイス
	• 冗長インターフェイス
	• EtherChannel インターフェイス
	• VLAN インターフェイス

ルートベース	スタティック仮想トンネル インターフェイス

- VPN トポロジの一部であるデバイスにテンプレートを適用する場合は、トポロジで使用されるすべてのインターフェイスのインターフェイス設定がテンプレートに含まれていることを確認する必要があります。

- VPN接続を含むテンプレートを複数のデバイスに適用する場合は、次の点に注意してください。

  テンプレートは、デバイスを選択した順序で複数のデバイスに適用されます。テンプレートに VPN 接続がある場合、対応する VPN トポロジがロックされます。

- SD-WAN トポロジ VPN 接続の場合：インターフェイスの IP アドレス サブネットが、SD-WAN ハブの IP アドレス プールのサブネットと競合しないことを確認します。

- Domain：
  - テンプレートは、グローバル ドメインまたはリーフ ドメインで定義できます。ただし、VPN トポロジはリーフ ドメインでのみ定義できます。
  - すべてのドメインのテンプレートで VPN 接続を設定できます。デバイスが VPN トポロジと同じドメインにある場合にのみ、テンプレートの適用中に VPN 接続がデバイスに適用されます。

  詳細については、「テンプレートとドメイン （3 ページ）」を参照してください。
- 変更管理：デバイス テンプレートをデバイスに適用する前に、VPN トポロジが変更管理チケットによってロックされていないことを確認してください。

未サポートの構成

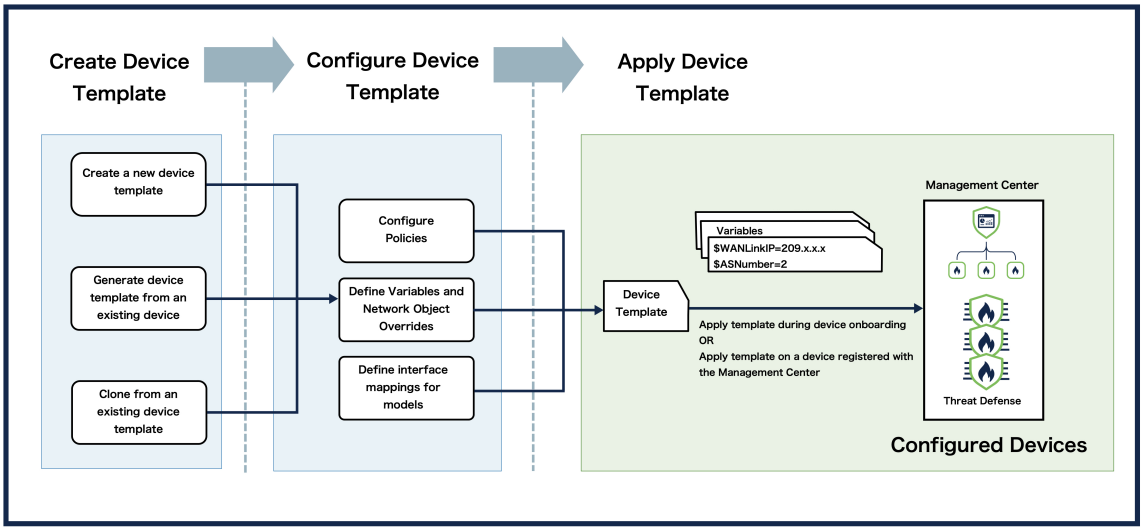
- 次の機能と設定は、デバイス テンプレートを使用してサポートされていません。
  - マルチインスタンス モード
  - クラスタ
  - 非統合管理インターフェイス
  - トランスペアレント モード
  - HA フェールオーバー設定
  - シャーシの設定
  - 論理デバイス
  - ネストされたオブジェクトの変数
  - ネットワーク グループ、およびその他のオブジェクト タイプのサポートのオーバーライド

VPN 接続の制限

- VPN トポロジの一部であるデバイスからテンプレートを作成した場合（**Devices** > **Device Management More** (⋮) > **[デバイスからテンプレートを生成（Generate Template from Device）]**）、VPN 設定はテンプレートの一部にはなりません。テンプレートで VPN 構成を再構成する必要があります。
- 1 つ以上の VPN 接続を含むデバイス テンプレートをエクスポートする場合（**[テンプレートの設定（Template Settings）]** > **[全般（General）]** > **[全般（General）]** ペイン > **[エクスポート（Export）]**）、VPN接続はエクスポートされません。インポートしたテンプレートで VPN 接続を再構成する必要があります。
- 証明書ベースの認証
  - デバイス テンプレートは、デバイスの自動証明書登録をサポートしていません。

- VPN設定を含むテンプレートを使用してデバイスをオンボーディングするとき、VPNトポロジで証明書ベースの認証が使用されている場合、デバイスへの最初の展開は失敗します。デバイス登録後にデバイス証明書を手動で登録し、デバイスに設定を再度展開してください。

デバイス テンプレートを使用したデバイス管理のワークフロー



デバイス テンプレートの設定

テンプレートを追加してから、テンプレートで設定を指定します。

デバイス テンプレートの追加

必要な設定を含む新しいデバイス テンプレートを追加するか、既存のデバイスからデバイス テンプレートを生成できます。

デバイス テンプレートの新規作成

デバイス テンプレートの名前、説明、アクセス コントロール ポリシー、およびルーティング モードを指定できます。テンプレートが作成されたら、さらに構成を追加できます。デバイス テンプレートを作成するには、次の手順を実行します。

手順

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

ステップ 2 **[デバイス テンプレートの追加（Add Device Templates）]** をクリックします。

ステップ 3 **[デバイス テンプレートの追加（Add Device Templates）]**ウィンドウで、デバイステンプレートの **[名前（Name）]** を入力します。

ステップ 4 （任意） テンプレートの [Description] を入力します。

ステップ 5 ドロップダウン リストから **[アクセス コントロール ポリシー（Access Control Policy）]** を選択します。

ステップ 6 ドロップダウン リストから**[モード（Mode）]** を選択します。

ステップ 7 **[OK]** をクリックします。

既存のデバイスから新しいデバイス テンプレートを生成する

Firewall Management Centerに登録されているデバイスから新しいデバイス テンプレートを生成できます。新しいテンプレートの設定は、生成元のデバイスと同じです。スタンドアロンデバイスと HA デバイスから新しいデバイス テンプレートを生成できます。ただし、HA デバイスからテンプレートを生成した場合、新しいテンプレートにはフェールオーバー設定が含まれません。

既存のデバイスから新しいデバイス テンプレートを生成するには、次の手順を実行します。

手順

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

ステップ 2 **More** (⋮) アイコンをクリックし、**[デバイスからテンプレートを生成する（Generate Template from Device）]** をクリックします。

ステップ 3 **[テンプレート名（Template Name）]** ウィンドウに、デバイス テンプレートの **[名前（Name）]** を入力します。

ステップ 4 （任意） テンプレートの [Description] を入力します。

ステップ 5 ドロップダウン リストから **[アクセス コントロール ポリシー（Access Control Policy）]** を選択します。

（注）
このポリシーは、生成されたテンプレートに割り当てられます。テンプレートの生成元であるデバイスに関連付けられている他の共有ポリシーは、そのポリシーが生成されているドメインで表示されている場合にのみ、生成されたテンプレートに割り当てられます。

ステップ 6 **[OK]**をクリックします。テンプレート作成のステータスを表示するには、**[通知（Notifications）]** に移動し、**[タスク（Tasks）]**タブをクリックします。

ステップ 7 **Devices** > **Template Management** を選択して、新しく作成されたテンプレートを表示します。

デバイス テンプレートのインポート

Firewall Management Center にテンプレートをインポートしたり、ローカル システムにテンプレートをエクスポートしたりできます。この機能は、次のシナリオで使用されます。

- デバイスからテンプレートのコピーを生成し、エクスポートし、そのテンプレートを別の Firewall Management Center または Cloud-Delivered Firewall Management Centerにインポートします。
- テンプレートのコピーを生成してエクスポートし、必要に応じて変更して既存のテンプレートのバリエーションを作成し、テンプレートを Firewall Management Centerにインポートします。
- テンプレートのコピーを生成してエクスポートし、ソーステンプレートが表示されていない別のドメインにそのテンプレートをインポートします。

テンプレートをドメインにインポートすると、構成の一部であるオブジェクトはすべて、新規に作成されるか、テンプレートをインポートするドメインで同じ名前のオブジェクトが表示される場合には再利用されます。ドメイン階層のために表示されない、一致する名前を持つオブジェクトは、サフィックスが _x の名前の新しいオブジェクトとしてインポートされます。

別のドメインから複製したテンプレートを使用してあるドメイン内のデバイスをオンボーディングする際に、変数名に不一致がある場合は、.csv ファイルで新しい変数名を指定してデバイスをオンボーディングする必要があります。

ローカルシステムから Firewall Management Center にデバイス テンプレートをインポートするには、次の手順を実行します。

手順

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

ステップ 2 インポートしたテンプレートと置き換えるテンプレートの **More** (⋮) アイコンをクリックします。

ステップ 3 **[インポート（Import）]** をクリックし、**[インポート（Import）]** をもう一度クリックします。

テンプレートをエクスポートする場合は、**[エクスポート（Export）]** をクリックし、**[OK]**をクリックします。

ステップ 4 インポート タスクのステータスを表示するには、**[通知（Notifications）]**をクリックし、**[タスク（Tasks）]** タブをクリックします。

ステップ 5 ローカル システム上のテンプレート SFO ファイルを選択し、**[開く（Open）]**をクリックします。インポートするこのテンプレート SFO ファイルは、新しく作成するか、デバイスから生成するか、既存のテンプレートから複製することができます。

ステップ 6 インポート タスクのステータスを表示するには、**[通知（Notifications）]**をクリックし、**[タスク（Tasks）]** タブをクリックします。インポートまたはエクスポート タスクが正常に完了したことを通知する通知が表示されます。テンプレートをエクスポートする場合は、**[通知（Notifications）]** をクリックし、**[タスク（Tasks）]**タブをクリックします。タブ ページで **[エクスポートパッケージのダウンロード（Download Export Package）]** をクリックして、テンプレート構成を SFO ファイルとしてダウンロードします。

（注）
または、**[テンプレート管理（Template Management）]** ウィンドウに移動し、テンプレートの **Edit** (✎) アイコンをクリックすることもできます。次に、**[テンプレート設定（Template Settings）]** に移動し、**[一般（General）]**をクリックします。**[一般（General）]** で **[インポート（Import）]** または **[エクスポート（Export）]** をクリックして、テンプレートをインポートまたはエクスポートします。

テンプレートでのデバイス設定の構成

テンプレートを作成したら、デバイス構成をセットアップし、テンプレートを編集してデバイスに適用する設定を指定できます。

物理インターフェイスの追加

デフォルトでは、デバイステンプレートは次の物理インターフェイスを使用してデバイスを起動できます。

- 管理インターフェイス
- 内部インターフェイス
- 外部インターフェイス

物理インターフェイスを作成するには、次の手順を実行します。

手順

ステップ 1 **Devices** > **Template Management**を選択します。
ステップ 2 物理インターフェイスを追加するテンプレートの **Edit** (✎) アイコンをクリックします。
ステップ 3 **[インターフェイス（Interfaces）]** タブで、**[物理インターフェイスの追加（Add Physical Interface）]** をクリックします。
ステップ 4 ドロップダウン リストから **[スロット（Slot）]** と **[ポート インデックス（Port Index）]** を選択します。
ステップ 5 **[インターフェイスの作成（Create Interface）]** をクリックします。

論理インターフェイスの追加

Firewall Management Center での作成と同じ方法で、テンプレートを使用せずに論理インターフェイスを作成できます。論理インターフェイスを作成するには、次の手順を実行します。

手順

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

ステップ 2 論理インターフェイスを追加するテンプレートの **Edit** (✎) アイコンをクリックします。

ステップ 3 **[インターフェイス（Interfaces）]** タブで、**[インターフェイスの追加（Add Interface）]**をクリックし、ドロップダウン リストから作成するインターフェイスのタイプを選択します。次のタイプのインターフェイスを作成できます。

- サブインターフェイス
- Ether チャネル インターフェイス
- ブリッジ グループ インターフェイス
- VLAN インターフェイス
- 仮想トンネルインターフェイス
- ループバック インターフェイス

詳細については、インターフェイスの概要と通常のファイアウォールインターフェイスを参照してください。

インターフェイスの編集

インターフェイスは、テンプレートを使用しない場合の Firewall Management Center と同じ方法で、編集できます。テンプレート変数を使用して、IPv4 および IPv6 アドレスを設定します。デバイステンプレートは、Firepower 1000、Cisco Secure Firewall 1200、 Firepower 2100、および Cisco Secure Firewall 3100 Firewall Threat Defense デバイスでサポートされている設定をサポートします。インターフェイスを編集するには、次の手順を実行します。

手順

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

ステップ 2 物理インターフェイスを編集するテンプレートの **Edit** (✎) アイコンをクリックします。

ステップ 3 **[インターフェイス（Interfaces）]** タブで、編集するインターフェイスの**編集**アイコンをクリックします。

ステップ 4 **[物理インターフェイスの編集（Edit Physical Interface）]** ウィンドウでは、次の設定を編集できます。

- 全般
- PoE
- IPv4
- IPv6
- パスモニタリング
- ハードウェア構成
- マネージャアクセス
- 拡張

（注）
変数を使用して、IPv4 および IPv6 アドレスを構成します。変数のテンプレート化の詳細については、テンプレート パラメータの構成を参照してください。

上記の設定の編集の詳細については、インターフェイスの概要および通常のファイアウォール インターフェイスを参照してください。

その他のデバイス設定の構成

テンプレートを使用せずに、Firewall Management Center で行うのと同じ方法で他のデバイス設定を構成します。

手順

ステップ 1 **Devices** > **Template Management**を選択します。
ステップ 2 設定を行うテンプレートの **Edit** (✎) アイコンをクリックします。
ステップ 3 ウィンドウ上部のタブをクリックして、次の設定を行います。

- インラインセット
- ルーティング
- DHCP
- VPN
- テンプレート設定

テンプレート設定の構成

これらは、テンプレートがデバイスに適用されたときにデバイスにコピーされるテンプレート固有の設定です。**[テンプレート設定（Template Settings）]** ウィンドウで、次のテンプレート設定を構成できます。

- 全般
  - 一般
  - ライセンス
  - [適用されたポリシー（Applied Policies）]
  - 詳細設定
  - 展開設定
- テンプレートパラメータ
  - 変数
  - [ネットワークオブジェクトのオーバーライド（Network object overrides）]
- モデルマッピング

全般設定の編集

[全般（General）] タイルには、次のフィールドが表示されます。

- **[テンプレート名（Template Name）]**：テンプレートの名前。
- **[パケットの転送（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管理センターに送信するかどうかを表示します。
- **[モード（Mode）]**：デバイスの管理インターフェイスのモードを表示します。ルーテッドなどです。
- **[構成（Configuration）]**：**[エクスポート（Export）]** をクリックして、テンプレート構成を SFO ファイルとしてエクスポートします。**[インポート（Import）]** をクリックして、必要なテンプレート設定を含む SFO ファイルをインポートします。
- **[データ インターフェイスによるデバイスの管理（Manage device by Data Interface）]**：ボタンを切り替えて、データインターフェイスを使用したデバイス管理を有効または無効にします。

デバイスの名前を編集し、パケット転送を有効または無効にするには、次の手順を実行します。

手順

ステップ 1 **[全般（General）]** タイルで **Edit** (✎) アイコンをクリックします。

ステップ 2 必要に応じて、**[テンプレート名（Template Name）]** を変更します。

ステップ 3 パケット データをイベントと一緒に Firewall 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。

ステップ 4 **[保存（Save）]** をクリックします。

ライセンスの編集

[ライセンス（License ）] タイルでは、テンプレートで使用されている設定に基づいて必要な**ライセンスタイプ**を確認できます。ここでライセンスを選択しても、デバイス上でそのライセンスは使用されません。ライセンスは、テンプレートをデバイスに適用した場合にのみ使用されます。

要件に応じてライセンス タイプを編集するには、次の手順を実行します。

手順

ステップ 1 **[ライセンス（License）]** タイルで **Edit** (✎) アイコンをクリックします。

ステップ 2 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 3 **[保存（Save）]** をクリックします。

適用されたポリシーの編集

[適用済みポリシー（Applied Policies）] タイルで、テンプレートに関連付けられているアクセス コントロール ポリシーを確認できます。

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。

要件に応じてポリシーの割り当てを編集するには、次の手順を実行します。

手順

ステップ 1 **[適用済みポリシー（Applied Policies）]** タイルで **Edit** (✎) アイコンをクリックします。

ステップ 2 ドロップダウン リスト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 3 **[保存（Save）]** をクリックします。

詳細設定の編集

[詳細設定（Advanced Settings）] タイルには、以下で説明する詳細構成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 *1 : [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）。
オブジェクトグループの検索	デバイスでのオブジェクトグループ検索の状態。動作中、Firewall 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るか、または Firewall Management Center にどのように表示されるかには影響しません。アクセスコントロールルールと接続を照合するときに、デバイスがアクセスコントロールルールを解釈して処理する方法のみに影響します。 （注） デフォルトでは、Firewall Management Center で初めて Firewall 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。

フィールド	説明
インターフェイス オブジェクトの最適化	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。

詳細設定を編集するには、次の手順を実行します。

手順

ステップ 1 **Edit** (✎) アイコンをクリックすると **[詳細設定（Advanced Settings）]** が開きます。

ステップ 2 要件に従って設定を変更できます。詳細については、次の項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
- オブジェクトグループ検索の構成
- インターフェイス オブジェクトの最適化の設定

ステップ 3 **[保存（Save）]** をクリックします。

展開設定の編集

[展開設定（Deployment Settings）] タイルには、以下の表に記載された情報が表示されます。

表 *2:* 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、Firewall Management Center 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。

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、Firewall Management Center 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（を参照）。

展開設定を編集するには、次の手順を実行します。

手順

ステップ 1 **[展開設定（Deplpyment Settings）]** タイルの **[編集（Edit）]** アイコンをクリックします。

ステップ 2 [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 3 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）]** をクリックしてから **[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。
- [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。

ステップ 4 管理接続が再確立されたことを確認します。

Firewall Management Center の接続状態ページで、管理接続の状態を確認します。**Devices** > **Device Management** ページに移動し、**[デバイス（Device）]** タブの **[管理（Management）]** エリアに移動します。次に、**[FMCアクセスの詳細（FMC Access Details）]** 画面で **[接続ステータス（Connection Status）]** をクリックします。

管理接続のステータスを表示するには、Firewall 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を参照してください。

テンプレート パラメータの構成

変数やネットワーク オブジェクトのオーバーライドなどのテンプレート パラメータを使用して、設定をテンプレート化できます。

サポートされる変数

デバイス テンプレートでは、次の変数タイプがサポートされています。

変数名	説明	タイプ
AS 番号	一意の自律システム（AS）番号を定義します。	Integer 例：2。
FQDN	完全修飾ドメイン名（FQDN）を定義します。	文字列 例：abc.example.com
IPv4ホスト	ホストの IPv4 アドレスを定義します。	文字列 例：209.165.201.8
IPv4 ネットワーク	IPv4 ネットワーク アドレス ブロックを定義します。	文字列 例：209.165.200.224/27
IPV4範囲	IPv4 アドレスの範囲を定義します。	文字列 例： 209.165.200.225-209.165.200.250
IPv6ホスト	ホストの IPv6 アドレスを定義します。	文字列 例：2001:DB8::1 となります。
IPv6 ネットワーク	IPv6 ネットワーク アドレス ブロックを定義します。	文字列 例：2001:DB8:0:CD30::/60
パスワード（Password）	パスワード文字列を定義します。	文字列 例：E28@2OiUrhx!
ルータ ID	ルータの識別子を定義します。	Integer 例：21
文字列	カスタム文字列を定義します。	文字列 例：testvalue2

変数を追加する

変数を追加するには、次の手順を実行します。

手順

ステップ 1 **Objects** > **Object Management**を選択します。

ステップ 2 オブジェクト タイプのリストから **[変数（Variable）]** を選択します。

ステップ 3 **[変数の追加（Add Variable）]** をクリックします。

ステップ 4 [Name] を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 ドロップダウンリストで **[変数タイプ（Variable Type）]** を選択します。

ステップ 6 （任意）[説明（Description）] を入力します。

ステップ 7 **[保存（Save）]** をクリックします。

サポートされるネットワーク オブジェクトのオーバーライド

次のネットワーク オブジェクトがサポートされています。

ネットワーク オブジェクト名	説明	タイプ
ネットワーク（Network）	アドレス ブロック（別名サブネット）。	文字列 例： IPv4 - 209.165.200.224/27 IPv6 - 2001:DB8::/48
ホスト	ホストの IP アドレス。	文字列 例： IPv4 - 209.165.200.225 IPv6 - 2001:DB8:1::1
範囲	IP アドレスの範囲。	文字列 例： IPv4 - 209.165.200.225-209.165.200.250 IPv6 - 2001:DB8::1 - 2001:DB8:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
[FQDN]	単独の完全修飾ドメイン名（FQDN）	文字列 例：abc.example.com

ネットワーク オブジェクトのオーバーライドの追加

ネットワーク オブジェクトのオーバーライドを追加するには、次の手順を実行します。

手順

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

ステップ 2 ネットワーク オブジェクト オーバーライドを追加するテンプレートの **Edit** (✎) アイコンをクリックします。

ステップ 3 **[テンプレートの設定（Template Settings）] > [テンプレートのパラメータ（Template Parameters）]**を選択します。

ステップ 4 **[ネットワーク オブジェクトのオーバーライド（Network Object Overrides）]** セクションで、**[ネットワーク オブジェクトのオーバーライドの追加または削除（Add or Remove Network Object Overrides）] を**クリックします。

ステップ 5 **[ネットワーク オブジェクトのオーバーライドの追加または削除（Add or Remove Network Object Overrides）]** ウィンドウで、**[使用可能なネットワーク（Available Networks）]** ウィンドウからネットワーク オブジェクト オーバーライドを作成するネットワーク オブジェクトを選択し、**[>]** ボタンをクリックします。

ステップ 6 **[保存（Save）]** をクリックします。

モデルマッピングの追加

モデルごとに、どのテンプレート インターフェイスがどのモデル インターフェイスに対応するかを指定できます。インターフェイス設定がマッピングされたすべてのモデルに有効である限り、テンプレートを1つ以上のモデルにマッピングできます。たとえば、テンプレートにスイッチポートと VLAN インターフェイスが含まれている場合、そのテンプレートは Firepower 1010 または Cisco Secure Firewall 1210/1220 にのみ適用できます。

モデル マッピングを追加するには、次の手順を実行します。

手順

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

ステップ 2 モデルマッピングを作成するテンプレートの**[モデル マッピングの追加（Add Model Mapping）]** をクリックします。または、テンプレートの **Edit** (✎) アイコンをクリックし、 **[テンプレートの設定（Template Settings）] > [モデル マッピング（Model Mapping）]**を選択することもできます。

ステップ 3 [モデルマッピングの追加（Add Model Mapping）] をクリックします。

ステップ 4 ドロップダウンリストから [デバイスモデル（Device Model）] を選択します。

ステップ 5 **[モデル インターフェイス（Model 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て、テンプレート インターフェイスをデバイス モデル インターフェイスにマッピングします。。

（注）

[マッピングのクリア（Clear Mapping）] をクリックして、定義したモデル マッピングを削除できます。**[マッピングのリセット（Reset Mappings）]** をクリックすると、スロットと、インターフェイス名のポートインデックス順に基づくデフォルトのインターフェイスマッピングに戻ります。

ステップ 6 **[Save（保存）]** をクリックします。インターフェイスのマッピングが、[モデルマッピング（Model Mapping）] ウィンドウにデバイスモデルおよびマッピングステータスとともに表示されます。

（注）
テンプレートの設定の中には、すべてのデバイスモデルでサポートされていない設定もあります。サポートされていない設定がある場合、その設定はデバイスには適用されません。こうした設定に関する詳細は、[デバイステンプレート適用レポート]で確認できます。

無効なモデル マッピング

テンプレートの設定の中には、すべてのデバイスモデルでサポートされていない設定もあります。サポートされていない設定がある場合、その設定はデバイスには適用されません。テンプレート設定を変更すると、有効なモデルマッピングが無効になる場合もあります。たとえば、テンプレートに新しいインターフェイスを追加して名前を割り当てる場合、新しいインターフェイスをデバイス モデルの適切なインターフェイスにマッピングする必要があります。

モデル マッピングは、次のいずれかの理由で無効になることもあります。

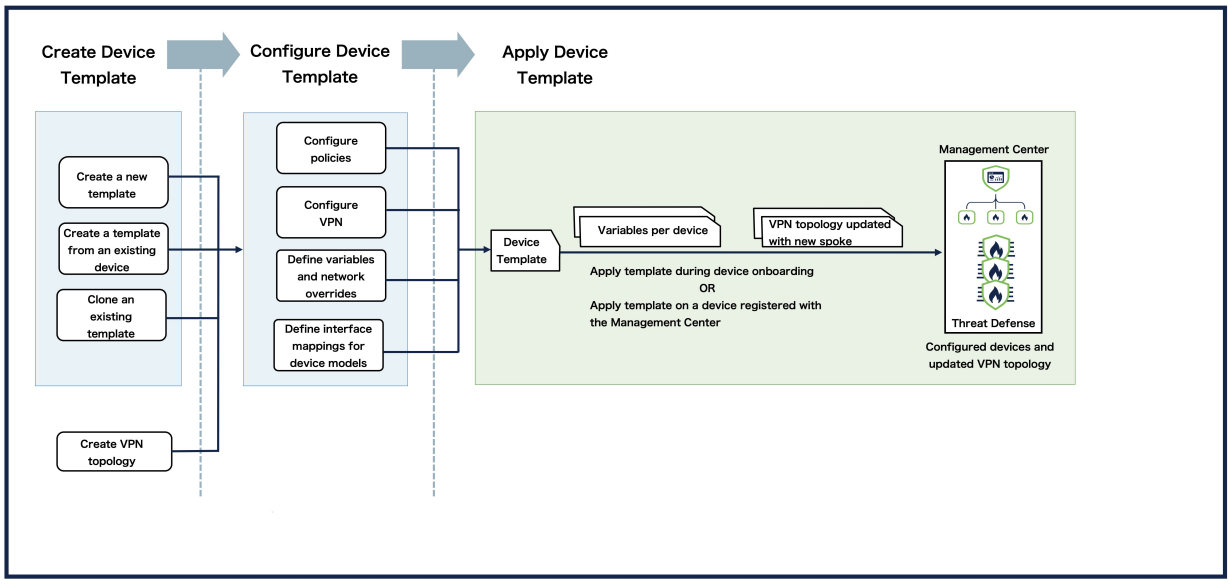
- 設定された VRF インスタンスの数が特定のモデルの制限を超えている。
- インターフェイスが互換性のないモデル、バージョン、またはインターフェイスにマッピングされている。詳細については、要件および前提条件を参照してください。
- インターフェイスの数がモデルの制限を超えている。
- マッピングされていたインターフェイスが削除された。
- 新しく追加された物理インターフェイスが、互換性のあるモデルのインターフェイスにマッピングされていない。
- モデルマッピングが、名前付きインターフェイスに対して行われていない。
- サブインターフェイス、PC インターフェイスなど、他の論理インターフェイスに関連するインターフェイスについては、モデルマッピングは行われません。
- 一部のデバイスモデルでサポートされていないポリシーまたは設定の変更。たとえば、インターフェイスのスイッチ ポート構成を有効にすること。

無効なモデルマッピングを含むテンプレートを保存することもできます。ただし、デバイスでテンプレートの適用を開始する前に、モデルマッピングを確認して修正する必要があります。

[マッピング ステータス（Mapping Status）] の **[無効（Invalid）]** にカーソルを合わせると、無効なマッピング ステータスの原因となったエラーを表示できます。デバイスでテンプレートの適用を開始する前にエラーを修正してください。

デバイス テンプレートでのサイト間 VPN 接続を設定する

サイト間 VPN 接続ワークフローを含むデバイス テンプレート



SD-WAN VPN 接続の設定

SD-WAN VPN 接続を設定し、デバイステンプレートを使用して SD-WAN トポロジにスポークを追加できます。

始める前に

- 少なくとも 1 つの SD-WAN トポロジ（**Devices** > **VPN** > **Site to Site**）を設定します。
- デバイス テンプレートを設定するための前提条件とデバイス テンプレートに関するガイドラインと制限事項を確認します。

手順

ステップ 1 **Devices** > **Template Management**を選択します。
ステップ 2 編集するデバイス テンプレートの横にある編集アイコンをクリックします。
ステップ 3 **[VPN]** タブをクリックします。
ステップ 4 **[VPN 接続の追加（Add VPN Connection）]** をクリックします。.

ステップ 5 **[VPN トポロジ（VPN Topology）]** ドロップダウン リストから SD-WAN トポロジを選択します。

[VPN 接続の追加（Add VPN Connection）] ダイアログボックスが表示され、次のパラメータを設定できます。

a) [VPNインターフェイス（VPN Interface）] ドロップダウンリストから、WAN 側またはインターネット側の物理インターフェイスを選択して、ハブとの VPN 接続を確立します。

このリストには、デバイステンプレートで構成されているすべてのインターフェイスが含まれています。

b) **[VPN インターフェイスからの IP アドレスを使用（Use IP Address from the VPN Interface）]**：このドロップダウン リストには、IP アドレス変数が自動入力されます。IPv6 アドレスの場合は、ドロップダウン リストから IPv6 アドレスを選択します。

c) **[ローカル トンネル（IKE）アイデンティティ（Local Tunnel (IKE) Identity）]** チェックボックスをオンにして、このデバイスからリモート ピアへの VPN トンネルの一意で設定可能なアイデンティティを有効にします。

d) **[アイデンティティ タイプ（Identity Type）]**：サポートされているアイデンティティ タイプはキー ID のみです。ドロップダウン リストからキー ID 変数を選択するか、 (+) をクリックして新しいキー ID 変数を作成します。

e) **[OK]** をクリックします。

VPN 接続は、**[サイト間 VPN 接続（Site-to-Site VPN Connections）]** テーブルで確認できます。

ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

1. デバイス テンプレートのスポークのルーティング ポリシーを設定します。
2. テンプレート インターフェイスをデバイス インターフェイスにマッピングします（モデル マッピング）。
3. テンプレートをデバイスに適用します。

ルートベースのサイト間 VPN 接続の設定

ルートベースのサイト間 VPN 接続を設定して、デバイス テンプレートを使用してルートベースのサイト間 VPN トポロジにスポークを追加できます。

始める前に

- 少なくとも 1 つのルートベースのサイト間 VPN トポロジ (**Devices** > **VPN** > **Site to Site**) を構成します。

- デバイス テンプレートを設定するための前提条件とデバイス テンプレートに関するガイドラインと制限事項を確認します。

手順

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

ステップ 2 編集するデバイス テンプレートの横にある編集アイコンをクリックします。

ステップ 3 **[VPN]** タブをクリックします。

ステップ 4 **[VPN 接続の追加（Add VPN Connection）]** をクリックします。.

ステップ 5 **[VPN トポロジ（VPN Topology）]** ドロップダウン リストからルートベースのサイト間 VPN トポロジを選択します。

[VPN 接続の追加（Add VPN Connection）] ダイアログボックスが表示され、次のパラメータを設定できます。

a) **[仮想トンネル インターフェイス（VTI）（Virtual Tunnel Interface (VTI)）]** ドロップダウンリストから VTI インターフェイスを選択するか、 (+) をクリックして新しい VTI を作成します。

VTIは、ルートベースのVPNトンネルを確立するために使用される仮想インターフェイスです。VTI のルーティング ポリシーを設定して、VPNトンネルをセットアップする必要があります。このリストには、デバイステンプレートに設定されているすべての VTI が含まれています。VTI の詳細については、VTI インターフェイスの追加を参照してください

b) **[パブリック IP アドレスを使用（Use Public IP Address）]** チェックボックスをオンにして、トンネル送信元 IP アドレスを上書きし、VTI のパブリック IP アドレス変数を設定します。(+) をクリックして、新しいパブリック IP アドレス変数を作成します。

この IP アドレスが、VPNトンネルの送信元IPアドレスになります。デフォルトでは、これがVPNインターフェイスのIPアドレスです。ただし、デバイスがNATの背後にある場合、VPNインターフェイスにはプライベートアドレスがありますが、NAT後のパブリックIPアドレスを設定する必要があります。

c) **[ローカル トンネル（IKE）アイデンティティ（Local Tunnel (IKE) Identity）]** チェックボックスをオンにして、このデバイスからリモート ピアへの VPN トンネルの一意で設定可能なアイデンティティを有効にします。

d) **[アイデンティティ タイプ（Identity Type）]** : サポートされるアイデンティティ タイプは Key ID のみです。ドロップダウン リストからキー ID 変数を選択するか、 (+) をクリックして新しいキー ID 変数を作成します。

e) （オプション） **[セカンダリ VPN トンネルの有効化（Enable Secondary VPN Tunnel）]** チェックボックスをオンにして、セカンダリ VPN トンネルのパラメータを設定します。

f) **[OK]** をクリックします。

VPN 接続は、**[サイト間 VPN 接続（Site-to-Site VPN Connections）]** テーブルで確認できます。

ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

1. デバイス テンプレートのスポークのルーティング ポリシーを設定します。
2. テンプレート インターフェイスをデバイス インターフェイスにマッピングします（モデル マッピング）。
3. テンプレートをデバイスに適用します。

ポリシーベースのサイト間 VPN 接続の設定

ポリシーベースのサイト間 VPN 接続を設定して、デバイス テンプレートを使用してスポークをポリシーベースのサイト間 VPN トポロジに追加できます。

始める前に

- 少なくとも 1 つのポリシーベースのサイト間 VPN を構成します（**Devices** > **VPN** > **Site to Site**）。
- デバイス テンプレートを設定するための前提条件とデバイス テンプレートに関するガイドラインと制限事項を確認します。

手順

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

ステップ 2 編集するデバイス テンプレートの横にある編集アイコンをクリックします。

ステップ 3 **[VPN]** タブをクリックします。

ステップ 4 **[VPN 接続の追加（Add VPN Connection）]** をクリックします。.

ステップ 5 **[VPN トポロジ（VPN Topology）]** ドロップダウン リストから、ポリシーベースのサイト間 VPN トポロジを選択します。

[VPN 接続の追加（Add VPN Connection）] ダイアログボックスが表示され、次のパラメータを設定できます。

a) [VPNインターフェイス（VPN Interface）] ドロップダウンリストから、WAN 側またはインターネット側の物理インターフェイスを選択して、ハブとの VPN 接続を確立します。

このリストには、デバイステンプレートで構成されているすべてのインターフェイスが含まれています。

次のいずれかを実行して、VPN インターフェイスの IP アドレスを設定します。

- VPN インターフェイスの IP アドレスを使用するには、**[`VPN インターフェイスからの IP アドレスを使用（Use IP Address from the VPN Interface]** オプションボタンをクリックします。

  IP アドレスは自動的に入力されます。IPv6 アドレスの場合は、ドロップダウン リストから IPv6 アドレスを選択します。

- **[パブリック IP アドレスを使用（Use Public IP Address）]** オプションボタンをクリックして、VPN インターフェイスのパブリック IP アドレスを設定します。

  ドロップダウンリストから IP アドレス変数を選択するか、 (+) をクリックして IP アドレス変数を追加します。

b) **[ローカル トンネル（IKE）アイデンティティ（Local Tunnel (IKE) Identity）]** チェックボックスをオンにして、このデバイスからリモート ピアへの VPN トンネルの一意で設定可能なアイデンティティを有効にします。

c) **[アイデンティティ タイプ（Identity Type）]**：サポートされるアイデンティティ タイプは Key ID のみです。ドロップダウンリストからキー ID 変数を選択するか、 (+) をクリックして新しいキー ID 変数を追加します。

d) **保護されたネットワーク**： (+) をクリックして、VPN 接続に保護されたネットワークを構成します。

   次のいずれかを実行します。

   - 保護されたネットワークを選択し、 **[OK]**をクリックします。
   - **[追加（Add）]**をクリックしてネットワークオブジェクトを追加し、**[保存（Save）]** をクリックします。

     保護されるネットワーク オブジェクトを作成する場合は、次の点に注意してください。

     - **[ホスト（Host）]** または **[ネットワーク（Network）]** ラジオ ボタンをクリックします。
     - **[AAA オーバーライドを許可（Allow AAA Override）]**チェックボックスをオンにします。

e) **[OK]** をクリックします。

   VPN 接続は、**[サイト間 VPN 接続（Site-to-Site VPN Connections）]** テーブルで確認できます。

ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

1. デバイスにテンプレートを適用する前に、保護ネットワークにデバイス固有の値を設定するには、**[テンプレート設定（Template Settings）] > [テンプレート パラメータ（Template Parameter）] > [ネットワーク オブジェクトのオーバーライドの追加（Add Network Objects Overrides）]** でこれらのオブジェクトを追加することに注意してください。
2. テンプレート インターフェイスをデバイス インターフェイスにマッピングします（モデル マッピング）。
3. テンプレートをデバイスに適用します。

デバイス テンプレートを使用したデバイスの登録とルートベースの VPN トポロジへの追加

このセクションでは、デバイステンプレートを使用してデバイスを登録し、デバイスをルートベースの VPN トポロジに追加する手順について説明します。

はじめる前に

ルートベースの VPN トポロジがあることを確認します。

手順	タスク	GUI パス	詳細情報
1	デバイス テンプレートを作成します。	**Devices** > **Template Management**、および **[デバイス テンプレートの追加（Add Device Templates）]** をクリックします。	デバイステンプレートの新規作成 （11 ページ）
2	インターフェイス テンプレートを設定します。	**Devices** > **Template Management**、および **[インターフェイス（Interfaces）]** をクリックします。	インターフェイスの編集（15 ページ）

手順	タスク	GUI パス	詳細情報
3	テンプレートでルートベースの VPN 接続を設定します。	**Devices** > **Template Management**、**[VPN]** > **[VPN 接続の追加（Add VPN Connection）]** をクリックします。	ルートベースのサイト間 VPN 接続の設定 （27 ページ）
4	テンプレートでルーティング ポリシーを設定します。	**Devices** > **Template Management**、および **[ルーティング（Routing）]** をクリックします。	—
5	テンプレートにデバイス モデルのモデル マッピングを追加します。	**Devices** > **Template Management**、**[テンプレート設定（Template 設定）]** > **[モデル マッピング（Model Mapping）]** をクリックします。	モデルマッピングの追加（24 ページ）
6	デバイス テンプレートを使用してデバイスを登録します。	**Devices** > **Device Management**、および **[追加（Add）]** > **[デバイス（ウィザード）（Device (Wizard)）]** をクリックします。	登録キーを使用したデバイスの追加：デバイス テンプレート
7	VPN トポロジのハブに設定を展開します。	**Deploy**	—

デュアル ISP 展開での SD-WAN トポロジへのデバイスの追加

このセクションでは、デバイステンプレートを使用してデュアル ISP 展開で SD-WAN トポロジにデバイスを追加する手順について説明します。

はじめる前に

同じハブをもつ 2 つの SD-WAN VPN トポロジがあることを確認します。SD-WAN トポロジの設定の詳細については、SD-WAN ウィザードを使用した SD-WAN トポロジの設定を参照してください。

手順	タスク	GUI パス	詳細情報
1	デバイステンプレートを作成します。	**Devices** > **Template Management**	デバイステンプレートの新規作成 （11 ページ）
2	物理インターフェイステンプレートを追加します。 デフォルトでは、テンプレートに外部インターフェイスは 1 つだけあります。外部インターフェイスの名前を変更します（例：ISP1、ISP2）。	**Devices** > **Template Management**、**[インターフェイス（Interfaces）]** > **[物理インターフェイスの追加（Add Physical Interface）]** をクリックします。	物理インターフェイスの追加 （14 ページ）
3	ISP1 インターフェイスを使用して SD-WAN VPN 接続を設定します。	**Devices** > **Template Management**、**[VPN]** > **[VPN 接続の追加（Add VPN Connection）]** をクリックします。	SD-WAN VPN 接続の設定 （26 ページ）
4	ISP2 インターフェイスを使用して SD-WAN VPN 接続を設定します。		

手順	タスク	GUI パス	詳細情報
5	ISP1 および ISP2 インターフェイスから SD-WAN ハブ ネットワークにスタティック ルートを追加します。	**Devices** > **Template Management**、**[ルーティング（Routing）]** > **[スタティック ルート（Static Route）]** の順にクリックします。	-
6	ECMP ゾーンに ISP1 インターフェイスと ISP2 インターフェイスを追加します。	**Devices** > **Template Management**、**[ルーティング（Routing）]** > **[ECMP]** をクリックします。	-
7	ネットワークオブジェクトのオーバーライドを設定します。	**Devices** > **Template Management**、**[テンプレート設定（Template Settings）]** > **[テンプレート パラメータ（Template Parameters）]** > **[ネットワーク オブジェクト オーバーライドの追加（Add Network Objects Overrides）]** をクリックします。	ネットワーク オブジェクトのオーバーライドの追加 （23 ページ）

手順	タスク	GUI パス	詳細情報
8	テンプレートインターフェイスをデバイスモデルインターフェイスにマッピングします（モデルマッピング）。	**Devices** > **Template Management**、**[テンプレート設定（Template 設定）]** > **[モデルマッピング（Model Mapping）]** をクリックします。	モデルマッピングの追加（24 ページ）
9	テンプレートをデバイスに適用します。	**Devices** > **Template Management**	テンプレートの適用（38 ページ）
10	設定をデバイスに展開します。	**Deploy**	—
11	SD-WAN トポロジのハブに設定を展開します。	**Deploy**	—

SD-WAN ウィザードを使用したデュアル ISP 展開の詳細については、SD-WAN ウィザードを使用したデュアル ISP 展開の構成例を参照してください。

データインターフェイスを使用して管理される Firewall Threat Defense デバイスのテンプレートの設定

Firewall Management Center 接続用のデータインターフェイスを使用して管理される Firewall Threat Defense デバイスに適用するテンプレートを設定する場合は、デバイスの接続パラメータがテンプレートと一致するようにしてください。一致させることで、テンプレートの適用後に Threat Defense デバイスが Firewall Management Center との接続を失うことがなくなります。データインターフェイスを使用して管理されている Firewall Threat Defense デバイスに設定したテンプレートは、データインターフェイスで管理されていないデバイスには適用できません。

接続パラメータのリストを以下に示します。

- Firewall Threat Defense デバイスの管理に使用されるデータインターフェイス。たとえば、**Ethernet1/1** などです。
- インターフェイスの名前。たとえば、**outside** などです。
- データインターフェイスに設定された IP アドレス。たとえば、DHCP、静的 IP などです。
- データインターフェイスに設定されたルート。ルートには、デフォルトまたは特定のルートを設定でき、Firewall Threat Defense デバイスと Firewall Management Center 間の接続に使用されるデータインターフェイスに定義されます。

- データインターフェイスの DDNS ホスト名設定。

テンプレートの接続パラメータがデバイスの接続パラメータと一致しない場合、テンプレートがデバイスに正常に適用されていることを確認するために実行されるテンプレート有効性検査は失敗します。この場合、テンプレートはデバイスに適用されません。テンプレート有効性検査では、IP アドレスや DDNS ホスト名などの一部のパラメータを完全一致させることはありません。ただし、展開後に Firewall Threat Defense デバイスと Firewall Management Center 間の接続を維持するために、それらのパラメータを設定してください。

次に、データインターフェイスを使用して Firewall Threat Defense デバイスを管理するために必要な設定が正しいことを保証するために実行されるテンプレート有効性検査のリストを示します。

- デバイスへのマネージャアクセスが管理インターフェイスにより設定されているテンプレートを、デバイスへのマネージャアクセスがデータインターフェイスにより設定されているデバイスに適用することはできません。
- デバイスへのマネージャアクセスがデータインターフェイスにより設定されているテンプレートを、デバイスへのマネージャアクセスが管理インターフェイスにより設定されているデバイスに適用することはできません。
- デバイスへのマネージャアクセスが単一の WAN データインターフェイスにより設定されているテンプレートを、デバイスへのマネージャアクセスがデュアル WAN データインターフェイスにより設定されているデバイスに適用することはできません。
- いずれかの接続パラメータが一致しない場合、デバイスへのマネージャアクセスがデータインターフェイスにより設定されているテンプレートを、デバイスへのマネージャアクセスがデータインターフェイスにより設定されているデバイスに適用することはできません。

次の手順を実行して、データインターフェイスを使用して Firewall Threat Defense デバイスを管理するようにテンプレートを設定します。

手順

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

ステップ 2 データインターフェイスを使用して Firewall Threat Defense デバイスを管理するように設定するテンプレートの **Edit** (✎) アイコンをクリックします。

ステップ 3 [テンプレート設定（Template Settings）] タブをクリックします。

ステップ 4 [全般（General）] タイルで、[データインターフェイスでデバイスを管理（Manage device by Data Interface）] ボタンを切り替えます。

ステップ 5 マネージャアクセスのデータインターフェイスを選択するよう求めるポップアップが表示されます。[OK] をクリックします。

ステップ 6 [インターフェイス（Interfaces）] タブをクリックします。

ステップ 7 マネージャアクセスに使用するデータインターフェイスの [編集（Edit）] アイコンをクリックします。多くの場合、最初のデータインターフェイスである Ethernet1/1（外部インターフェイス）がマネージャアクセスに使用されます。

ステップ 8 [物理インターフェイスの編集（Edit Physical Interface）] ウィンドウで、[マネージャアクセス（Manager Access）] タブをクリックします。

ステップ 9 [管理アクセスの有効化（Enable management access）] チェックボックスをオンにします。

ステップ 10 [OK] をクリックします。マネージャアクセス用に選択したインターフェイスが、[マネージャアクセス（Manager Access）] のマーク付きで表示されます。

ステップ 11 [DHCP] タブをクリックします。

ステップ 12 [DDNS更新方法（DDNS Update Methods）] タブをクリックします。

ステップ 13 [+追加（+Add）] をクリックして、DDNS 更新方法を追加します。

ステップ 14 [DDNS更新方法の追加（Add DDNS Update Method）] ウィンドウで、[方式名（Method Name）] を入力し、[FMCのみ（FMC only）] を選択します。

ステップ 15 要件に応じて [更新間隔（Update Interval）] を設定します。

ステップ 16 [OK] をクリックします。作成した方法が [DDNS更新方法（DDNS Update Methods）] テーブルに表示されます。

ステップ 17 [DDNSインターフェイス設定（DDNS Interface Settings）] タブをクリックします。

ステップ 18 動的 DNS 設定を追加する場合は、[+追加（+Add）] をクリックします。

ステップ 19 [動的DNSの追加（Add Dynamic DNS）] 設定画面で、次のフィールドの値を選択します。

- [インターフェイス（Interface）]：マネージャアクセスが有効なインターフェイスを選択します。
- [方式名（Method Name）]：作成した方法を選択します。
- [ホスト名（Host Name）]：ホスト名の変数を選択します。

このウィンドウの残りのフィールドは編集しないでください。

ステップ 20 [OK] をクリックします。[DDNSインターフェイス設定（DDNS Interface Settings）] テーブルに、作成したエントリが入力されます。

ステップ 21 テンプレートでマネージャアクセス用に設定されたデータインターフェイスが、デバイスでマネージャアクセス用に選択されたデータインターフェイスと一致するようにモデルマッピングを設定するには、[テンプレート設定（Template Settings）] タブをクリックし、[モデルマッピング（Model Mapping）] をクリックします。

ステップ 22 [モデルマッピングの追加（Add Model Mapping）] をクリックします。

ステップ 23 ドロップダウンリストから [デバイスモデル（Device Model）] を選択します。

ステップ 24 [モデルインターフェイス（Model 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て、テンプレートでマネージャアクセス用に設定されたデータインターフェイスをデバイスの適切なデータインターフェイスにマッピングします。

ステップ 25 **[Save（保存）]** をクリックします。インターフェイスのマッピングが、[モデルマッピング（Model Mapping）] ウィンドウにデバイスモデルおよびマッピングステータスとともに表示さ

れます。これで、データインターフェイスを使用して管理されているデバイスにテンプレートが適用できるようになりました。

デバイスでのテンプレートの使用

Firewall Management Centerでデバイスを登録すると、初期設定と互換性のあるテンプレートを選択できます。また、Firewall Management Centerにすでに登録されているデバイスにテンプレートを適用できます。

シリアル番号とデバイステンプレートを使用した Management Center へのデバイスの追加

デバイス テンプレートと次のオプションを使用して、デバイスを Firewall Management Center に追加できます。

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

（注） テンプレート設定に関連する変更管理チケットは、対応する変更をテンプレート アプリケーション ワークフローに組み込むために承認される必要があります。テンプレートの適用時には、承認済みのテンプレート設定のみが使用されます。

既存のデバイスへのテンプレートの適用

既存のデバイスにテンプレートを適用または再適用できます。

テンプレートの適用

すでにFirewall Management Centerに登録されているデバイスにテンプレートを適用できます。デバイスでテンプレートを適用すると、既存の設定がクリアされ、テンプレートからの設定が適用されます。ただし、Firewall Threat Defense HA フェールオーバー設定はクリアされません。

テンプレートを適用すると、Firewall Management Center でのみデバイス設定が変更されます。Firewall Threat Defense へのこれらのデバイス設定の変更は、明示的に展開する必要があります。適用した設定変更をロールバックすることはできません。ただし、必要な構成を含む別のテンプレートを適用することはできます。

（注） テンプレート設定に関連する変更管理チケットは、対応する変更をテンプレート アプリケーション ワークフローに組み込むために承認される必要があります。テンプレートの適用時には、承認済みのテンプレート設定のみが使用されます。

既存のデバイスにテンプレートを適用するには、次の手順を実行します。

手順

ステップ 1 **[テンプレート管理（Template Management）]** ウィンドウからテンプレートを適用するには、**Devices** > **Template Management** を選択します。

a) 適用するテンプレートの横にある **More** (⋮) アイコンをクリックし、**[適用（Apply）]**をクリックします。

b) **[デバイス（Device）]** ドロップダウン リストから、テンプレートを適用するデバイスを選択します。

c) **[確認（Confirm）]** をクリックして、デバイスへのテンプレートの適用を開始します。

ステップ 2 （任意）**[関連付けられたデバイス（Associated Devices）]** ウィンドウからテンプレートを適用するには、**[デバイス（Devices）] > [テンプレート管理（Template Management）]** を選択します。

a) デバイスに適用するテンプレートの **Edit** (✎) アイコンをクリックします。

b) **[関連付けたデバイス（Associated Devices）]** をクリックします。

c) **[関連付けられたデバイス（Associated Devices）]** ウィンドウで、**[テンプレートの適用（Apply Template）]**をクリックします。

d) **[デバイス（Device）]** ドロップダウンリストから、テンプレートを適用するデバイスを選択します。

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

f) **[適用（Apply）]** をクリックして、デバイスにテンプレートの適用を開始します。

テンプレートの再適用

デバイスまたはテンプレートに変更を加えた結果、設定が同期しなくなった場合は、テンプレートを再適用して、設定をテンプレートと同期させることができます。

デバイスにテンプレートを再適用するには、次の手順を実行します。

手順

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

ステップ 2 デバイスに再適用するテンプレートの **Edit** (✎) アイコンをクリックします。

ステップ 3 **[関連付けたデバイス（Associated Devices）]** をクリックします。

ステップ 4 **[関連付けたデバイス（Associated Devices）]** ウィンドウで、テンプレートを再適用するデバイスの **[テンプレートの再適用（Reapply Template）]** をクリックします。

（注）
テンプレート内の関連付けられているすべてのデバイスにテンプレートを再適用する場合は、**[一括再適用（Bulk Reapply）]** をクリックし、 **[確認（Confirm）]**をクリックします。

ステップ 5 **[テンプレートの再適用（Reapply template）]** ウィンドウでは、自動入力された **変数** と **ネットワークオブジェクトのオーバーライド** 値を再利用したり、新しい値を入力したりできます。

ステップ 6 **[確認（Confirm）]** をクリックして、デバイスでのテンプレートの再適用を開始します。

デバイス テンプレートのモニタリング

[関連デバイス（Associated Devices）] ウィンドウに一覧表示されているデバイスと、 **[テンプレート適用レポート（Template Apply Report）]** を表示することにより、テンプレートの適用をモニターおよび確認できます。

関連デバイスの表示

テンプレートに関連付けられているデバイスが **[関連デバイス（Associated Devices）]** ウィンドウに表示されます。各デバイス行には、**[デバイス名（Device Name）]**、**[同期ステータス（Sync Status）]**、**[テンプレート アプリケーション ステータス（Template Application Status）]**、および **[適用されたデータ（Applied Date）]** が表示されます。 **[テンプレートの再適用（Reapply template）]** をクリックして、テンプレートを再適用することもできます。**変数の概要** アイコンをクリックしてテンプレート内の変数の概要を表示し、 **Report** (📋) アイコンをクリックしてデバイステンプレート適用レポートをダウンロードします。**Delete** (🗑) アイコンをクリックして、デバイスからテンプレートを削除します。

[関連デバイス（Associated Devices）] ウィンドウからデバイスにテンプレートを適用する場合は、 **[テンプレートの適用（Apply Template）]** をクリックします。テンプレート内の関連付けられているすべてのデバイスにテンプレートを再適用する場合は、**[一括再適用（Bulk Reapply）]** をクリックし、 **[確認（Confirm）]**をクリックします。

[同期ステータス（Sync Status）] は、**[同期（Sync）]** または **[非同期（Out-of-Sync）]** のいずれかになります。ステータスが **[同期（Sync）]**と表示されている場合は、テンプレートとデバイスの設定が同一または同期していることを示します。ステータスが **[非同期（Out-of-Sync）]**として表示されている場合は、テンプレートが最後に適用された後で、デバイスまたはテンプレートのいずれかの設定に変更があったことを示します。

デバイスとテンプレートの関連付けは、次の条件によって変更されません。

- デバイスの保留中の構成変更：デバイスに適用する必要がある保留中の構成変更がある場合、**同期ステータス**は変更されません。
- 保留中の構成変更のデバイスへの展開：保留中の構成変更がデバイスに展開された後、**同期ステータス**は変更されません。

次の表は、発生する可能性がある**同期**および**非同期**シナリオを示しています。

デバイスでのテンプレートの適用後に変更されるデバイス設定	デバイスへのテンプレートの適用後に変更されるテンプレート設定	アソシエーションの状態
いいえ	非対応	同期しています
はい	いいえ	同期しない
非対応	○	同期しない
はい	はい	同期しない

テンプレート適用レポートの生成

テンプレート適用レポートの PDF は、テンプレートを適用するタスクが完了した後に生成されます。このレポートは、デバイスでのテンプレートの適用が成功した場合と失敗した場合の両方について生成されます。このレポートをアクセスするには、**[通知（Notifications）]** をクリックし、その後に **[タスク（Tasks）]** タブをクリックします。

テンプレート適用レポートには、次の詳細が含まれています。

- テンプレート名
- デバイスのモデル名。
- テンプレートの適用元のドメイン
- 開始時間と終了時間
- デバイスでのテンプレートのアプリケーションのステータス
- インターフェイス マッピング情報
- 変数値

互換性のないデバイス モデルまたはバージョンが原因で、デバイスに適用されない設定がテンプレートに含まれている場合があります。このレポートには、そのような設定に関する詳細も含まれています。このレポートには、テンプレートの適用が失敗したときに発生したエラーも含まれます。デバイスでのテンプレートの適用は、次のいずれかの理由で失敗することがあります。

- 使用されているデバイス モデルにモデル マッピングが存在しない。

- 変数およびネットワーク オブジェクト オーバーライドに使用される値が、ルーティング ポリシーまたはインターフェイス設定ルールに従わない。（たとえば、2 つの IPv4 アドレス インターフェイス変数に同じ IPv4 アドレスが使用されている場合です）。
- テンプレートの適用や変更など、実行中の他のタスクによりデバイスまたはテンプレートがロックされている。

監査ログ

デバイス テンプレートのアプリケーション、設定の更新、デバイス テンプレートの作成、および削除に関連するログは、監査ログに記録されます。デバイステンプレートの監査ログは、デバイスにテンプレートを適用するタスクの開始時と終了時の両方でログに追加されます。

また、監査差分ファイルも生成され、デバイスでのテンプレートの適用中に行われた設定の変更を表示できるようになります。差分ファイルを表示するには、次の手順を実行します。

手順

ステップ 1 **System** (⚙) > **Monitoring** > **Audit**を選択します。

ステップ 2 デバイス テンプレートのログは、サブシステムの **Devices** > **Template Management** でログに記録されます。**[差分（diff）]** アイコンをクリックして、デバイスでのテンプレートの適用中に行われた設定の変更を表示する新しいウィンドウを開きます。

デバイス テンプレートのトラブルシューティング

初期のトラブルシューティング

初期のトラブルシューティングでは、テンプレート適用レポートの情報と、エラーが発生したときに Firewall Management Center UI に表示される通知を確認することをお勧めします。Firewall Management Center ログ ファイルには、詳細なデバッグおよびトラブルシューティングの情報も含まれています。

初期トラブルシューティングについては、以下の手順に従ってください。

1. **[テンプレート適用レポート（Template Apply Report）]** に記載されているエラーを確認します。詳細については、テンプレート適用レポートを参照してください。
2. 変数値を確認し、重複や非互換性を確認します。
3. モデル マッピングをチェックして、正しいモデル マッピングが存在するかどうかを確認します。適宜、マッピングを削除または追加します。
4. Firewall Management Center 監査ログを参照して、他の問題を見つけて解決します。

次のエラー シナリオを考えてみましょう。デバイス テンプレートで、内部インターフェイスが静的 IPv4 変数（*$insideIPv4*）を使用して設定されている。

BGP IPv4 アドレスが、IPv4 BGP ネイバーで設定されている。

重複する IPv4 アドレスが BGP ネイバーとインターフェイスに対して設定されている。

上記の問題により、デバイステンプレートの適用が失敗し、エラーが表示されます。

このエラーをトラブルシューティングするには、UI に表示される通知からエラーを特定します。

```
IP Address 192.168.10.1 same as ip address of interface - 'inside'(Ethernet1/1)
```

詳細については、 **テンプレート適用レポート** を参照してください。

変数に正しい値を入力し、テンプレートを再度適用して、デバイスにテンプレートが正常に適用されるようにします。

デバイス登録のトラブルシューティング

- 問題：管理者パスワードが正しくないか、登録時に指定されていない

  シナリオ：管理者パスワードがデバイスで設定されておらず、登録時に管理者パスワードを指定していない場合、Firewall Threat Defense デバイスのプロビジョニングは失敗します。このようなシナリオでは、*[プロビジョニング エラー（Provision Error）]* と **[パスワードの入力（Enter Password）]** リンクが表示されます。

  回避策：**[パスワードの入力（Enter Password）]** をクリックして新しいパスワードを入力し、**[保存（Save）]**をクリックします。**[確認して続行（Confirm and Proceed）]** をクリックして、オンボーディングを再度トリガーします。

- 管理者パスワードがデバイスですでに設定されている場合、登録時に別の管理者パスワードを指定すると、デバイスのプロビジョニングは失敗します。

- 問題：Firewall Management Center でのデバイス登録が失敗している

  回避策：既存のデバイス登録のトラブルシューティング手順に従います。詳細については、Firepower デバイス登録の設定、検証、およびトラブルシューティングを参照してください。

- 問題：一括登録要求が Firewall Management Centerで失敗している

  シナリオ：一括登録要求は、次のいくつかのシナリオが原因で失敗する可能性があります。

  - この操作を実行するために必要な権限がない。
  - リクエスト ドメインからのテンプレートが得られていない
  - 無効な CSV ファイルがアップロードされた

  回避策：VMS 共有ログ ファイルと USM 共有ログ ファイルでこれらのエラーのログを確認できます。エラーを修正し、登録を再度開始します。

- 問題：デバイスとの通信の失敗などの一般的なエラーが原因で、 Security Cloud Control でデバイスのプロビジョニングが失敗している

  回避策：[プロビジョニング エラー（Provision Error）] で [再試行（Retry）] をクリックして、 Security Cloud Control のオンボーディングを再度トリガーします。エラーの詳細とトラブルシューティング情報については、Security Cloud Control ワークフローも参照できます。

Cisco Security Cloud の統合のトラブルシューティング

問題：Cisco Security Cloud の統合が失敗している

回避策：Cisco Security Cloud 統合のトラブルシューティング手順に従います。詳細については、Cisco Security Cloud の統合を参照してください。

ネットワーク テンプレート設定の問題のトラブルシューティング

問題：デバイス テンプレートの設定ミスにより、登録後の展開に失敗する

回避策：初期のトラブルシューティングについては、次の手順に従います。

1. [テンプレート適用レポート（Template Apply Report）] に記載されているエラーを確認します。
2. 変数値を確認し、重複や非互換性を確認します。
3. モデル マッピングをチェックして、正しいモデル マッピングが存在するかどうかを確認します。適宜、マッピングを削除または追加します。
4. Firewall Management Center 監査ログを参照して、他の問題を見つけて解決します。

Security Cloud Control の問題のトラブルシューティング

- 問題：シリアル番号を持つデバイスがすでに要求されている

  回避策：シリアル番号を確認し、オンボーディングを再開します。

- 問題：Security Cloud Control がデバイスを要求できない

  回避策：Security Cloud Control **[セキュリティ デバイス（Security Devices）]** ウィンドウでデバイスを選択してエラーの詳細を表示します。VMS 共有ログ ファイルと USM 共有ログ ファイルで、デバイス要求の問題に関連するログを確認できます。**[再試行]** をクリックして、登録を再度開始します。

- 問題：Firewall Management Center と Security Cloud Control間の通信障害

  シナリオ： Firewall Management Center と Security Cloud Control 間の通信障害により、ゼロタッチプロビジョニング（ZTP）のデバイス登録要求中に障害が発生する可能性があります。

  回避策：ZTP デバイスのステータスを更新し、ZTP 登録を再試行して、ZTP デバイスを削除します。認証デーモンのログで、 Firewall Management Center と Security Cloud Control 間

の通信障害に関するログを確認できます。ZTP に関連する操作の失敗については、VMS 共有ログファイルと USM 共有ログファイルでログを確認できます。

デバイステンプレートを使用したデバイス管理の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
デバイステンプレートを使用したデバイス管理	7.6.0	7.4.1	デバイステンプレートを使用すると、事前にプロビジョニングされた初期デバイス設定を使用して、複数のブランチデバイスを展開できます。デバイステンプレートを使用して、複数のデバイスの一括ゼロタッチプロビジョニングを実行し、異なるインターフェイス設定を持つ複数のデバイスに Day 2 設定変更を適用し、既存のデバイスから設定パラメータを製できます。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [追加（Add）] > [デバイス（ウィザード）（Device (Wizard)）]** • **[デバイス（Devices）] > [テンプレート管理（Template Management）] > [デバイステンプレートの追加（Add Device Template）]** • **[デバイス（Devices）] > [テンプレート管理（Template Management）] > [モデルマッピングの追加（Add Model Mapping）]** • **[デバイス（Devices）] > [テンプレート管理（Template Management）] > [テンプレートの編集（Edit a template）] > [テンプレート設定（Template Settings）]** • **[統合（Integration）] > [Cisco Security Cloud]**

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。