Security Cloud Control でのデバイスのオンボーディング

ライブデバイスとモデルデバイスの両方を Security Cloud Control に導入準備できます。モデルデバイスはアップロードされた構成ファイルであり、Security Cloud Control を使用して表示および編集できます。

ほとんどのライブデバイスおよびサービスでは、Secure Device Connector が Security Cloud Control をデバイスまたはサービスに接続できるように、オープンな HTTPS 接続が必要となります。

この章は、次のセクションで構成されています。

- Security Cloud Control Firewall Management でサポートされるデバイス、ソフトウェア、ハードウェア （1 ページ）
- オンプレミス Firewall Management Center の Security Cloud Control へのオンボーディング （4 ページ）
- オンプレミス Firewall Management Center の Security Cloud Control からの削除 （13 ページ）

Security Cloud Control Firewall Management でサポートされるデバイス、ソフトウェア、ハードウェア

Security Cloud Control Firewall Management は、複数のセキュリティ プラットフォームにおけるセキュリティポリシーとデバイス設定を管理できるクラウドベースの管理ソリューションです。

このセクションでは、Security Cloud Control Firewall Management でファイアウォール、クラウド、SD-WAN、Cisco IOS、Cisco Umbrella、および管理センターの統合を管理するためにサポートされているデバイスタイプ、ソフトウェア、ハードウェア、および制約事項について説明します。

サポートの範囲

Security Cloud Control Firewall Management は、複数のセキュリティ プラットフォームにおけるセキュリティポリシーとデバイス設定を管理できるクラウドベースの管理ソリューションです。この情報ソースでは、次の管理エリアのサポートが特定されています。

- Cisco Secure Firewall ASA（オンプレミスと仮想）
- Cisco Secure Firewall Threat Defense（FTD）（オンプレミスと仮想）
- Cisco Catalyst SD-WAN Manager
- Cisco Secure Firewall Management Center（オンプレミス）
- Cisco Meraki MX
- Cisco IOS デバイス
- Cisco Umbrella
- AWS セキュリティグループ

Security Cloud Control Firewall Management のドキュメントでは、Security Cloud Control Firewall Management がサポートしているデバイス、ソフトウェア、およびハードウェアが特定されています。ソフトウェアのバージョンまたはデバイスタイプのサポートを明示的に記載していない場合、Security Cloud Control Firewall Management はそれをサポートしません。

Cisco Secure Firewall ASA

Cisco 適応型セキュリティアプライアンス（ASA）は、ファイアウォール、VPN、および侵入防御機能を統合したセキュリティデバイスです。Security Cloud Control は、ASA デバイスの管理をサポートし、設定管理を合理化する機能と、ネットワーク インフラストラクチャ全体での適合規格の遵守を支援する機能を提供します。

Cisco Secure Firewall Threat Defense

Cisco Cisco Secure Firewall Threat Defense は、従来のファイアウォール機能と高度な脅威防御機能を統合します。これには、侵入防御、アプリケーション制御、URL フィルタリング、高度なマルウェア防御などのセキュリティ機能が含まれます。

Cisco Secure Firewall Threat Defense デバイスは、ASA ハードウェアアプライアンス、Cisco ファイアウォール ハードウェア アプライアンス、および仮想環境に展開できます。Threat Defense デバイスは、Cisco Firewall Management Center、Security Cloud Control、Firewall Device Manager などの管理インターフェイスを介して管理できます。

Firewall Threat Defense は、従来のファイアウォール機能と高度な脅威防御機能を統合します。侵入防御、アプリケーション制御、URL フィルタリング、高度なマルウェア防御などを含む包括的なセキュリティ機能を提供します。FTD は、ASA ハードウェアアプライアンス、Cisco ファイアウォール ハードウェア アプライアンス、および仮想環境に展開できます。Threat Defense デバイスの管理は、Cisco Firewall Management Center、Security Cloud Control Firewall Management、Firewall Device Manager などのさまざまな管理インターフェイスを介して実行できます。

ソフトウェアおよびハードウェア互換性の詳細については、Cisco Secure Firewall Threat Defense 互換性ガイドを参照してください。

Firewall Device Manager は、Threat Defense デバイス管理用に明示的に設計された Web ベースの管理インターフェイスです。Threat Defense デバイスを設定およびモニターするためのシンプルなアプローチを提供するため、小規模な展開や、直感的なインターフェイスを求める組織に最適です。

FDM は、ネットワーク設定、アクセス コントロール ポリシー、NAT ルール、VPN 設定、モニタリング、および基本的なトラブルシューティングに関する基本的な設定機能を提供します。通常、Web ブラウザを介してアクセスする FDM は、FTD デバイスで直接使用できるため、追加の管理サーバーやアプライアンスは必要ありません。

Cisco Catalyst SD-WAN Manager

Security Cloud Control によって、Catalyst SD-WAN およびブランチ WAN の環境を中央管理できるようになり、組織がネットワーク全体でセキュリティポリシーを効率的に設定、監視、および適用できるようになります。この統合により、Catalyst SD-WAN Manager での高度なトラブルシューティング、ルールの最適化、および変更管理も容易になります。

ソフトウェアとハードウェアの互換性の詳細については、「Cisco Catalyst SD-WAN Device Compatibility」を参照してください。

Cisco Secure Firewall Management Center

Security Cloud Control Firewall Management は、セキュアな統合を確立し、セキュリティデバイスを検出し、一元化されたポリシー管理を有効にすることで、オンプレミスの Firewall Management Center の管理を簡素化します。ファイアウォールルール、VPN 設定、侵入防御ポリシーなどのセキュリティポリシーを、FMC 下にあるすべてのデバイスにわたって効率的に管理および展開できます。

Cisco Meraki MX

Cisco Meraki MX アプライアンスは、分散型展開用のエンタープライズグレード セキュリティおよび SD-WAN の次世代ファイアウォール アプライアンスです。Security Cloud Control Firewall Management は、Cisco Meraki MX デバイス上のレイヤ 3 ネットワークルールの管理をサポートします。

Cisco Meraki デバイスを Security Cloud Control Firewall Management にオンボーディングすると、Security Cloud Control Firewall Management は Cisco Meraki ダッシュボードと通信してそのデバイスを管理します。Security Cloud Control Firewall Management は設定リクエストを Cisco Meraki ダッシュボードに転送し、Cisco Muraki ダッシュボードが新しい設定をデバイスに適用します。

Cisco Meraki MX に関する Security Cloud Control Firewall Management のサポートには、ポリシーの一元管理、バックアップと復元、モニタリングとレポート、コンプライアンスチェック、自動化機能などがあります。

Cisco IOS デバイス

Cisco IOS ソフトウェアは、ルーティング、スイッチング、その他のネットワーキングプロトコルなどのネットワーク機能を管理します。Cisco IOS には、シスコのネットワークデバイスを設定および維持するための機能とコマンドが含まれています。

Cisco Umbrella

Security Cloud Control Firewall Management は、Cisco Umbrella と Cisco ASA の統合などの統合を介して Cisco Umbrella を管理します。この統合により、管理者はインターフェイスごとのポリシーを使用して、Cisco 適応型セキュリティアプライアンス（ASA）デバイスを Cisco Umbrella 設定に含めることができます。

この統合により、Cisco ASA デバイスが DNS クエリを Cisco Umbrella にリダイレクトすることが可能になり、Cisco Umbrella の DNS セキュリティ、Web フィルタリング、および脅威インテリジェンス機能を活用することも可能になります。

AWS セキュリティグループ

Security Cloud Control Firewall Management は、Amazon Web Services（AWS）仮想プライベートクラウド（VPC）向けの簡素化された管理インターフェイスを提供します。ソース連携機能には、AWS サイト間 VPN 接続のモニタリング、AWS デバイスへの変更の追跡、AWS サイト間 VPN トンネルの表示が含まれます。

オンプレミス Firewall Management Center の Security Cloud Control へのオンボーディング

Security Cloud Control では、2 つの方法で オンプレミス Firewall Management Center をオンボーディングできます。

- 推奨される方法（Secure Device Connector を使用しない直接オンボーディング）：Cisco Security Cloud と統合された オンプレミス Firewall Management Center 自動検出およびオンボーディング。ほとんどのクラウドアシスト機能は、オンプレミス Firewall Management Center が Secure Device Connector（SDC）を使用せずに直接オンボーディングされた場合にのみサポートされるため、この直接的な方法が推奨されます。直接オンボーディングでは、ゼロタッチプロビジョニング、一元化されたデバイスの可視性、ポリシーの最適化などのクラウドアシスト機能にフルアクセスできます。ほとんどのユースケースでは、この方法が推奨されます。オンプレミス Firewall Management Center と Cisco Security Cloud の統合の詳細については、「オンプレミス Firewall Management Center と Cisco Security Cloud の統合 （6 ページ）」を参照してください。
- 別の方法（SDC を使用）：SDC とともに オンプレミス Firewall Management Center ログイン情報を使用する方法もサポートされていますが、想定される対象は非常にまれなユースケースのみです。SDC を使用したオンボーディングでは、直接オンボーディングで利用できる多くのクラウドアシスト機能へのアクセスが制限されます。直接オンボーディングできない場合に、SDC を選択してください。

詳細については、直接クラウド接続のインバウンドアクセスを許可を参照してください。

Security Cloud Control は、以下を可能にすることにより FMC を補完します。

- FMC を使用した共有オブジェクト管理による一貫性のあるポリシーの適用。

  詳細については、「Security Cloud Control を使用したオンプレミス Firewall Management Center の管理」の「**オブジェクト**」セクションを参照してください。

- Firewall Threat Defense デバイスのゼロタッチプロビジョニング。詳細については、「ゼロタッチ プロビジョニング を使用した オンプレミス Firewall Management Center へのデバイスのオンボーディング」を参照してください。

- セキュリティデバイスの一元化された可視性と管理。詳細については、「デバイスとサービスの管理」を参照してください。

- クラウド Cisco Secure Dynamic Attributes コネクタ（CSDC）およびクラウド提供型 Firewall Management Center との統合。詳細については、「Cisco Secure Dynamic Attributes Connector」を参照してください。

制限事項とガイドライン

- オンプレミス Firewall Management Center をオンボーディングすると、登録されているすべてのデバイスもオンボーディングされます。無効または到達不能なデバイスは、Security Cloud Control の [セキュリティデバイス（Security Devices）] ページに表示されることがありますが、管理やクエリは実行できません。

- オンボーディングでは、オンプレミス Firewall Management Center から Security Cloud Control または クラウド提供型 Firewall Management Center にポリシーがカスケード**されません**。Firewall Threat Defense デバイスを クラウド提供型 Firewall Management Center に移行するには、組み込みの [FTDからcdFMCへの移行（Migrate FTD to cdFMC）] 機能を使用します。詳細については、「Migrate Threat Defense to Cloud-delivered Firewall Management Center」を参照してください。

- 管理者レベルの権限を持つ Security Cloud Control 通信に特化した専用のユーザーを オンプレミス Firewall Management Center に作成することを推奨します。オンボーディング中に同じログイン情報で オンプレミス Firewall Management Center にログインすると、プロセスが失敗します。この推奨事項は、直接統合ではなく、ログイン情報ベースのオンボーディングにのみ適用されます。

- この専用ユーザーに対して、[ログイン失敗の最大回数（Maximum Number of Failed Logins）] をゼロに設定します。

- オンプレミス Firewall Management Center バージョン 7.4 以降の場合、スイッチオーバーによってクラウド接続が失われるときは、（バージョンに応じて）**SecureX**、**Security Cloud Control**、または **Cisco Security Cloud** を無効にしてから再度有効にして、接続を復元します。

Cisco Security Cloud に統合された オンプレミス Firewall Management Center の自動オンボーディング

自動検出およびオンボーディング機能は、Security Cloud Control ではデフォルトで有効になっています。バージョン7.2 以降を実行しており、Cisco Security Cloud と統合されているすべての オンプレミス Firewall Management Center は自動的に検出され、Security Cloud Control にオンボーディングされます。関連付けられた Firewall Threat Defense デバイスは Security Cloud Control にオンボードされています。

Security Cloud Control は オンプレミス Firewall Management Center の高可用性（HA）ペアもオンボードします。

始める前に

オンプレミス Firewall Management Center のポート 443 からのアウトバウンドトラフィックが許可されているかを確認します。

手順

ステップ 1 オンボードする オンプレミス Firewall Management Center を Cisco Security Cloud と統合し、Security Cloud Control テナントに登録します。詳細については、オンプレミス Firewall Management Center と Cisco Security Cloud の統合 （6 ページ）を参照してください。

ステップ 2 オンプレミス Firewall Management Center に登録されている Security Cloud Control テナントにログインします。

ステップ 3 の順に選択します。**[管理（Administration）] > [統合（Integrations）] > [Firewall Management Center]**

テナントに関連付けられているすべての オンプレミス Firewall Management Center が **FMC** タブに表示されます。詳細については、「オンボードされた オンプレミス Firewall Management Center を表示」を参照してください。

オンプレミス Firewall Management Center と Cisco Security Cloud の統合

この手順は、オンプレミス Firewall Management Center と Cisco Security Cloud の統合方法を説明するものです。Cisco Security Cloud との統合を有効にすることで、Management Center が Cisco Cloud テナントに登録されます。

始める前に

オンプレミス Firewall Management Center のオンボーディング時：

- すでに Security Cloud Control テナントがある場合は、その既存のテナントに オンプレミス Firewall Management Center をアタッチするかどうかを確認するよう求められます。
- テナントまたはアカウントがない場合、オンプレミス Firewall Management Center 統合ウィザードはオンボーディングプロセスの登録タスク中に自動的に新しいテナントを作成しま

す。このテナントは、オンプレミス Firewall Management Center AI Assist 有効化専用に提供される無料階層です。後で変換が必要になるトライアルテナントを受信しないように、ウィザードでテナント作成を管理できるようにします。ウィザードはこのプロセスを管理して、シームレスなエクスペリエンスを提供します。

- クラウド提供型 Firewall Management Center を使用するか、Security Cloud Control を使用してファイアウォールを管理する場合は、基本ライセンスとデバイスの権限を購入する必要があります。詳細なライセンス情報および製品オプションについては、「Security Cloud Control ライセンスの概要」を参照してください。

手順

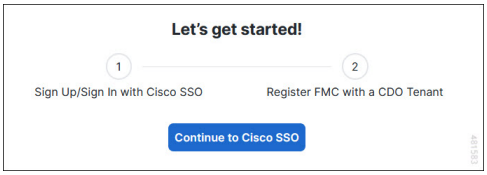
ステップ 1 オンプレミス Firewall Management Center のバージョンに基づいて、次の手順を実行します。

- オンプレミス Firewall Management Center バージョン 7.2 ～ 7.4.x の場合は、[SecureXの有効化（Enable SecureX）] をクリックします。
- オンプレミス Firewall Management Center バージョン 7.6 以降の場合は、[Cisco Security Cloud] をクリックします。
- オンプレミス Firewall Management Center バージョン 10.0 以降の場合は、**Security Cloud Control** をクリックします。

Security Cloud Control アカウントにログインするための別のブラウザタブが開きます。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。

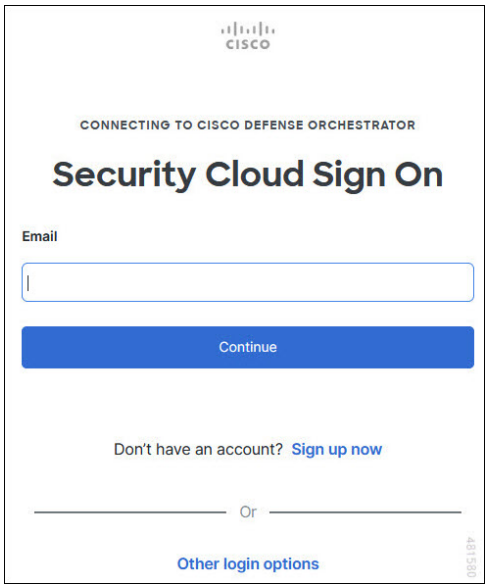
ステップ 2 [Cisco SSOに進む（Continue to Cisco SSO）] をクリックします。

図 *1 : Cisco Security Cloud* のウェルカムページ



ステップ 3 Security Cloud Control アカウントにログインします。

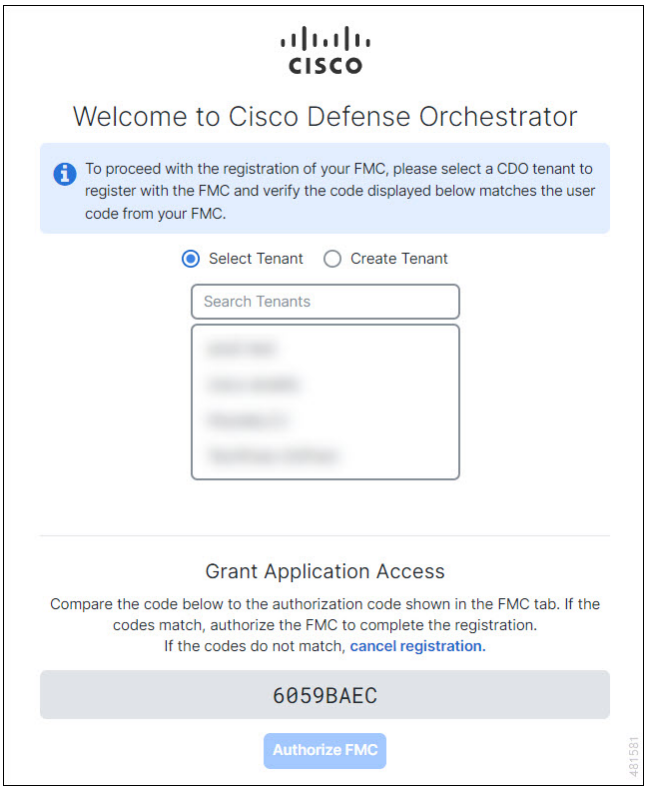
図 2 : Cisco Security Cloud Sign On



Security Cloud Control にログインするための Security Cloud Sign On アカウントがなく、アカウントを作成する場合は、[Security Cloud Sign On] ページで [今すぐ登録（Sign up now）] をクリックします。「Create a New Cisco Security Cloud Sign On Account」を参照してください。

ステップ 4 この統合に使用する Security Cloud Control テナントを選択します。オンプレミス Firewall Management Center と管理対象デバイスは、ここで選択した Security Cloud Control テナントにオンボーディングされます。

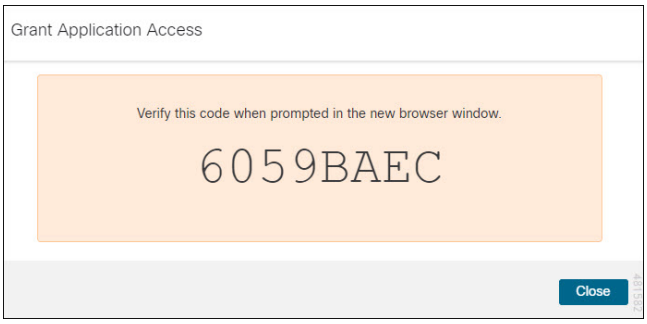
図 *3 : Security Cloud Control* テナントを選択します。



Security Cloud Control テナントがまだない場合、またはこの統合に新しいテナントを使用する場合は、新しいテナントを作成します。

ステップ 5 Security Cloud Control ログインページに表示されるコードが、オンプレミス Firewall Management Center で提供されるコードと一致することを確認します。

図 *4 :* オンプレミス *Firewall Management Center* の確認コード



ステップ 6 [FMCの許可（Authorize FMC）] をクリックします。

ステップ 7 オンプレミス Firewall Management Center UI で [保存（Save）] をクリックして、設定を保存します。

[通知（Notifications）] > [タスク（Tasks）] を選択すると、タスクの進行状況を表示できます。

登録タスクが完了するまでに最大90秒かかる場合があります。登録タスクの進行中にオンプレミスFirewall Management Centerを使用する必要がある場合は、新しいウィンドウでオンプレミスFirewall Management Centerを開きます。

Cisco Security Cloudからのオンプレミスfmcの自動オンボード

自動オンボーディング機能を無効にすると、Cisco Security Cloudテナントから新しいオンプレミスFirewall Management Centerが自動的に追加されなくなります。

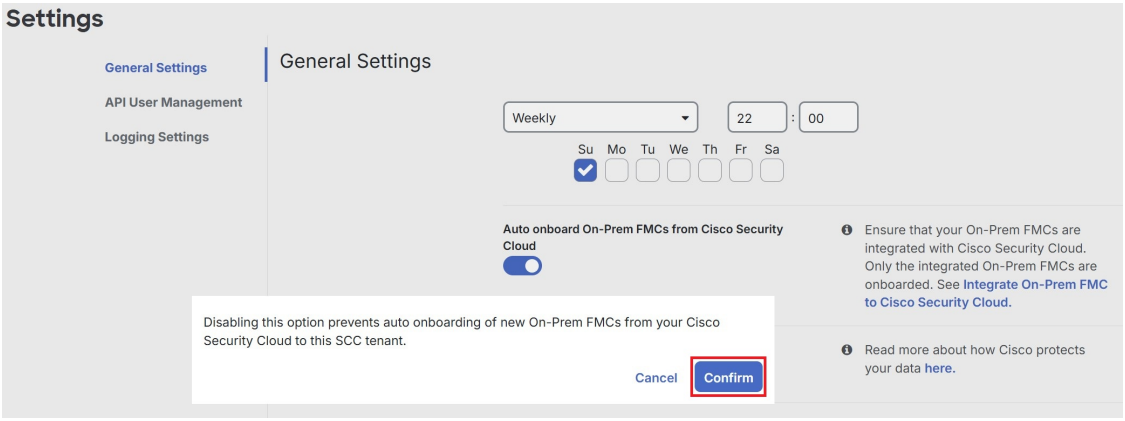
（注） ネットワーク管理者または管理者のみが、Security Cloud Controlでこの機能を有効または無効にできます。

手順

ステップ1 **[管理（Administration）]** > **[一般設定（General Settings）]** を選択します。

ステップ2 [Cisco Security Cloudオンプレミスfmcの自動オンボード（Auto onboard On-Prem FMCs from Cisco Security Cloud）] トグルボタンをオフにして、オンプレミスFirewall Management Centerの自動オンボーディングを無効にします。

ステップ3 [確認（Confirm）] をクリックします。



ログイン情報を使用したSecurityCloudControlへのオンプレミスFirewall Management Centerのオンボーディング

ログイン情報を使用してオンプレミスFirewall Management CenterのSecurity Cloud Controlへの導入準備を行うには、次の手順に従います。

始める前に

次の前提条件を満たす必要があります。

- **Cloud Secure Device Connector（SDC）の場合**：オンプレミス Firewall Management Center のポート 443 でのインバウンドトラフィックを許可します。

  SDCは、ポート443でのインバウンドトラフィックを許可することにより、オンプレミス Firewall Management Center に到達します。

  Security Cloud Control と SDC の両方がクラウドでホストされます。

- **オンプレミスの Secure Device Connector（SDC）の場合**：SDC のポート 443 でのアウトバウンド接続を許可します。

  SDC は Security Cloud Control への接続を必要とするため、SDC から Security Cloud Control へのアウトバウンドトラフィックを許可する必要があります。オンプレミス Firewall Management Center での追加のポート設定は必要ありません。

手順

ステップ 1 **[管理（Administration）]** > **[一般設定（General Settings）]** を選択します。

ステップ 2 + をクリックして オンプレミス Firewall Management Center をオンボーディングします。

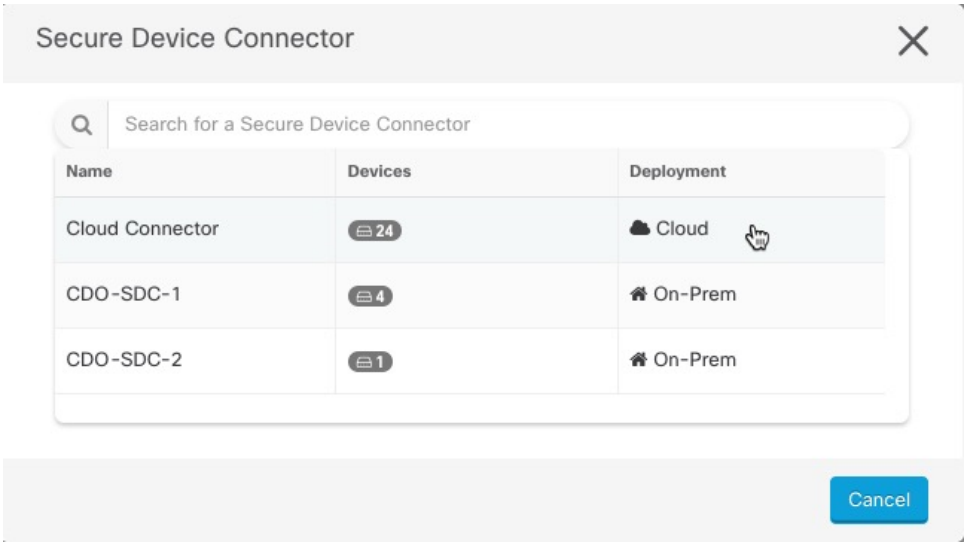
ステップ 3 [Firewall Management Center] をクリックします。

ステップ 4 [ログイン情報を使用] カードを選択します。

ステップ 5 [Secure Device Connector] ボタンをクリックし、ネットワークにインストールされている SDC を選択します。

SDC を使用しない場合、Security Cloud Control は Cloud Connector を使用して オンプレミス Firewall Management Center に接続できます。どちらを選択するかは、Security Cloud Control を管理対象デバイスに接続する方法によって異なります。

図 *5 : Secure Device Connector* の選択



ステップ 6 デバイス名を入力して、**[Next]** をクリックします。

ステップ 7 オンプレミス Firewall Management Center へのアクセスに使用するアカウントログイン情報の [ユーザー名（Username）] と [パスワード（Password）] を入力します。[次へ（Next）] をクリックします。

ステップ 8 デバイスをオンボーディングした後、オンプレミス Firewall Management Center にラベルを追加するか、[Go to Services] をクリックしてオンボーディングされたデバイスのページを表示できます。デバイスが正常な場合、FMC には **[Synced]** ステータスが表示されます。

（注）
オンプレミス Firewall Management Center によって管理されるデバイスには、自動的に「<*fmcname*>_<*manageddevicename*>」という名前が付けられます。

Security Cloud Control を オンプレミス Firewall Management Center にリダイレクトする

オンプレミス Firewall Management Center を Security Cloud Control にオンボードしたら、オンプレミス Firewall Management Center UI で管理インターフェイスのホスト名を更新して FQDN を含めます。管理インターフェイスのホスト名を更新しないと、Security Cloud Control からクロス起動できません。

この手順を使用して、管理インターフェイスのホスト名を更新し、Security Cloud Control からオンプレミス Firewall Management Center にリダイレクトします。

手順

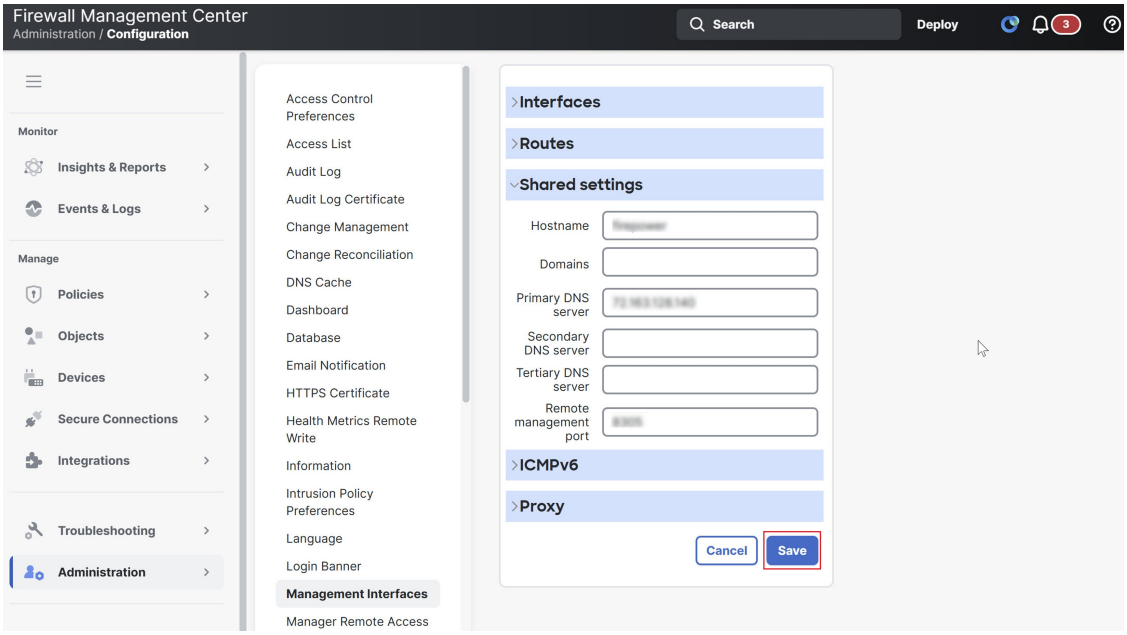
ステップ 1 オンプレミス Firewall Management Center UI にログインします。

ステップ 2 **[管理（Administration）] > [設定（Configuration）]** の順に選択します。

ステップ 3 [管理インターフェイス（Management Interfaces）] タブをクリックします。

ステップ 4 [共有設定（Shared Settings）] の下で、[ホスト名（Hostname）] フィールドを見つけ、Firewall Management Center の FQDN を入力します。

ステップ 5 [保存（Save）] をクリックします。



（注）
場合によっては、Security Cloud Control からログアウトしてから、[Firepower Management Centerでデバイスを管理（Manage Devices in Firepower Management Center）] をクリックし、オンプレミス Firewall Management Center UI にクロス起動する必要があります。

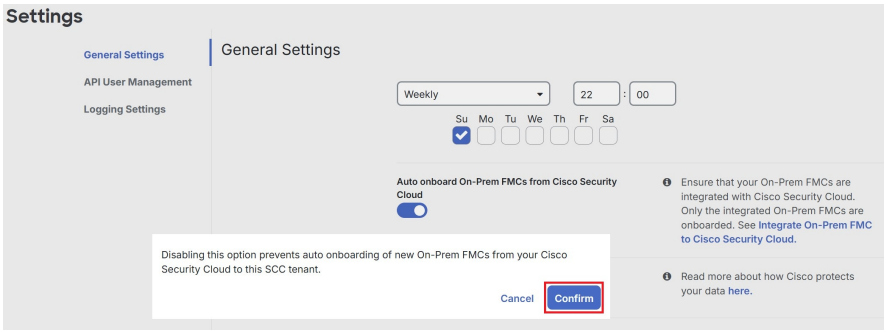
オンプレミス Firewall Management Center の Security Cloud Control からの削除

Security Cloud Control から オンプレミス Firewall Management Center を削除すると、その オンプレミス Firewall Management Center によって管理されているすべてのデバイスも削除されます。

始める前に

自動オンボーディング機能を使用してオンボードされた1つまたは複数のオンプレミスFirewall Management Centerを削除するには、まず自動オンボーディングオプションを無効にします。

1. **[管理（Administration）]** > **[一般設定（General Settings）]** を選択します。
2. [テナント設定（Tenant Settings）] セクションで、[Cisco Security Cloudに統合されたオンプレミスFMCの自動オンボード（Auto onboard On-Prem FMCs integrated to Cisco Security Cloud）] を無効化します。



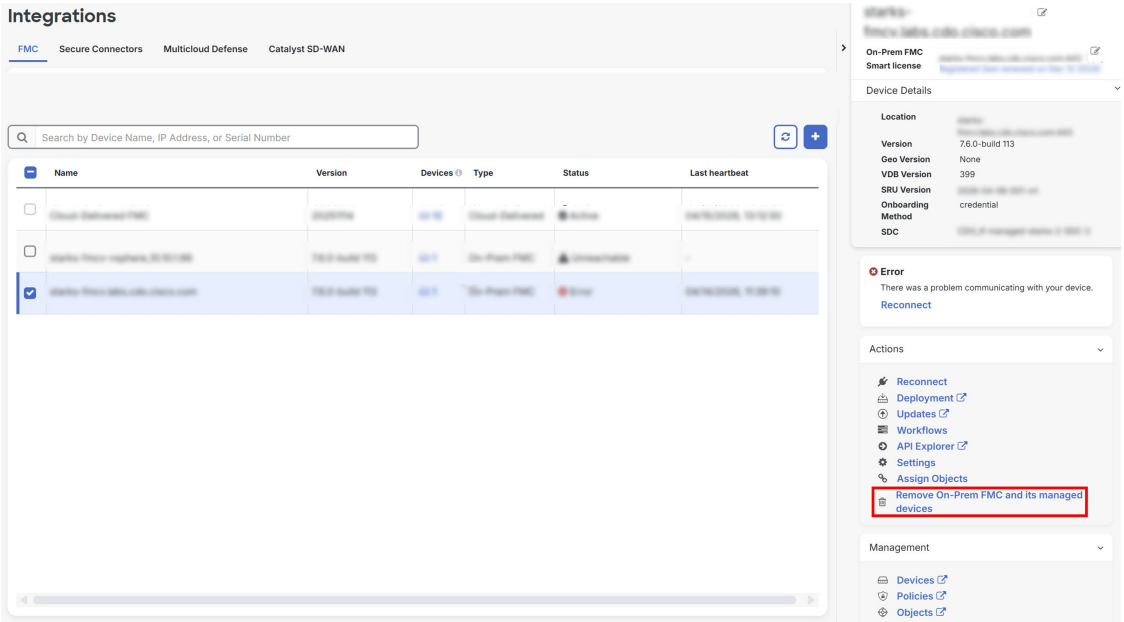
手順

ステップ 1 **[管理（Administration）]** > **[統合（Integrations）]** > **[Firewall Management Center]** を選択します。

ステップ 2 [FMC] タブをクリックします。

ステップ 3 削除する オンプレミス Firewall Management Center を選択します。

ステップ 4 [Device Actions] ペインで、[Remove On-Prem FMC and its managed devices] をクリックします。



ステップ 5 [OK] をクリックして、オンプレミス Firewall Management Center とその管理対象デバイスをテナントから削除することを確認します。

ステップ 6 ブラウザを更新して、デバイスの更新リストを表示します。

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。