オンプレミス Firewall Management Center デバイスの設定

この章は、次のセクションで構成されています。

オンボード済みのオンプレミス Firewall Management Center の表示

オンボード済みの オンプレミス Firewall Management Center を表示するには、次の手順を実行します。

1. **[管理（Administration）] > [統合（Integrations）] > [Firewall Management Center]**
2. [FMC] タブをクリックします。

オンプレミス Firewall Management Center の高可用性ペアを表示する

高可用性ペアは **[Services]** ページに表示されます。ペアを展開すると、プライマリとセカンダリの オンプレミス Firewall Management Center ノードとその現在のステータスが表示されます。

アクティブな オンプレミス Firewall Management Center をクロス起動するには、次の手順を実行します。

1. **[Services]** ページで、対応する高可用性ペアを確認します。
2. 開きたいオプションを オンプレミス Firewall Management Center でクリックします。

[FMCクロス起動URLの確認（Verify FMC Cross Launch URL）] ウィンドウが表示されます。デフォルトでは、現在アクティブな オンプレミス Firewall Management Center のパブリック IP アドレスまたは FQDN が表示され、オンプレミス Firewall Management Center を開くのに使用されます。必要に応じて、スタンバイ オンプレミス Firewall Management Center の URL を指定して起動できます。

各 オンプレミス Firewall Management Center ノードにクロス起動 URL を追加します。ペアから起動すると、アクティブなノードのみが起動します。どのノードが現在アクティブであるかを確認する必要はありません。

特定の オンプレミス Firewall Management Center ノードをクロス起動するには、次の手順を実行します。

1. 高可用性ペアを展開し、起動するプライマリまたはセカンダリ オンプレミス Firewall Management Center ノードをクリックします。
2. [外部リンク（External Links）] ペインで、[FMCクロス起動URL（FMC Cross Launch URL）] をクリックして、選択した オンプレミス Firewall Management Center をクロス起動します。

   オンプレミス Firewall Management Center のパブリック IP アドレスまたは FQDN とポート番号を更新するには、**[FMC Cross Launch URL]** にカーソルを合わせて、編集アイコンをクリックします。

（注） オンプレミス Firewall Management Center（バージョン 7.4.x 以前）で高可用性を解除するか、ロールを切り替えた場合は、一度 SecureX との統合を無効化してから、セカンダリ オンプレミス Firewall Management Center で再度有効にする必要があります。このタスクを完了するには、セカンダリ オンプレミス Firewall Management Center に移動し、適切なオプションを選択します。

高可用性 オンプレミス Firewall Management Center ペアを解除すると、ペアを構成する Management Center が 2 つのスタンドアロン オンプレミス Firewall Management Center に変換されます。

オンプレミス Firewall Management Center 高可用性におけるクラウドリージョン同期の問題のトラブルシュート

問題

米国以外のリージョンで Security Cloud Control と統合された オンプレミス Firewall Management Center 高可用性（HA）ペアでスイッチオーバーが発生すると、次のクラウド接続の問題が発生します。

- 新しくアクティブになった オンプレミス Firewall Management Center は、本来設定された米国以外のリージョンではなく、米国リージョン（デフォルト）に自動的に接続します。

- [テナント（Tenant）] フィールドには、設定済みのテナントが表示される代わりに [なし（None）] と表示されます。
- クラウド統合エラーにより、Security Cloud Control に適切に接続できません。

シナリオ例

初期設定

- EU（欧州）リージョンの Security Cloud Control に接続するように設定された オンプレミス Firewall Management Center HA ペア
- オンプレミス Firewall Management Center プライマリ：アクティブ
- オンプレミス Firewall Management Center セカンダリ：スタンバイ

スイッチオーバーイベント後

- オンプレミス Firewall Management Center プライマリで障害が発生する
- オンプレミス Firewall Management Center セカンダリが新しいアクティブユニットになる
- オンプレミス Firewall Management Center セカンダリ（新しいアクティブ）が欧州リージョンではなく米国リージョン（デフォルト）に自動的に接続する
- [テナント（Tenant）] フィールドに [なし（None）] と表示される

（注）
- オンプレミス Firewall Management Center の HA ペアが Security Cloud Control で米国リージョンと統合されている場合、この手順は不要です。
- スイッチオーバーは、Firewall Threat Defense デバイスの設定、セキュリティポリシー、またはその他の オンプレミス Firewall Management Center 設定には影響しません。
- この手順はクラウド接続を復元するだけであり、管理対象デバイスへのポリシーの再展開は必要ありません。

問題の原因

クラウドリージョンおよびテナント設定は、HA ペアのアクティブな オンプレミス Firewall Management Center からスタンバイ状態の オンプレミス Firewall Management Center に自動的に同期されません。スイッチオーバー中に、スタンバイユニットがアクティブになります。ただし、以前に設定したリージョンは保持されず、デフォルト（米国リージョン）にリセットされます。

ソリューション

フェールオーバー後にクラウド接続を復元するには、新しくアクティブになったオンプレミス Firewall Management Center で次の手順を実行します。

1. スイッチオーバー後にアクティブになったオンプレミス Firewall Management Center にログインします。
2. [統合（Integrations）] > [（Security Cloud Control）] の順に選択します。

   [現在のクラウドリージョン（Current Cloud Region）] ドロップダウンリストが [米国リージョン（US Region）] に設定されます。
3. [Security Cloud Controlの無効化（Disable Security Cloud Control）] をクリックします。
4. [保存（Save）] をクリックします。
5. [現在のクラウドリージョン（Current Cloud Region）] ドロップダウンリストから、以前のアクティブな オンプレミス Firewall Management Center で設定したリージョンを選択します。
6. [Security Cloud Controlの有効化（Enable Security Cloud Control）] をクリックします。
7. [保存（Save）] をクリックします。

ネットワークオブジェクトの検出と管理オンプレミス Firewall Management Center

Security Cloud Control を使用して管理する オンプレミス Firewall Management Center があり、そのオブジェクトを共有および管理する場合は、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）]** > **[統合（Integrations）]** > **[Firewall Management Center]** の順に選択して、[Services] ページを表示します。

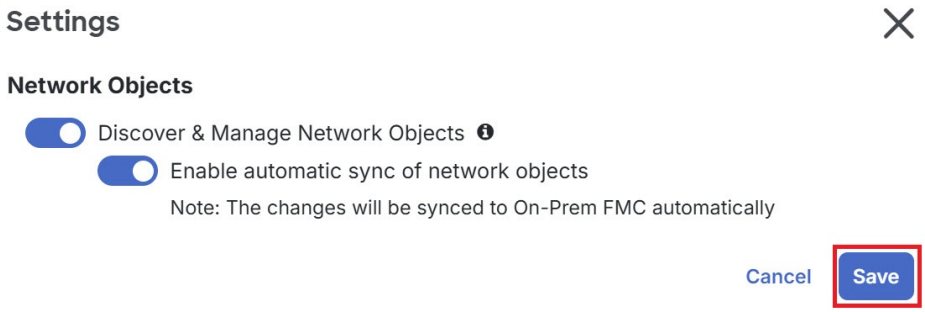
ステップ 2 すでに オンプレミス Firewall Management Center が Security Cloud Control にオンボード済みの場合は、それを選択します。

新たにオンプレミス Firewall Management Center をオンボードする場合は、「オンプレミス Firewall Management Center のオンボード」を参照してください。

ステップ 3 右側の [Actions] ペインから [Settings] を選択します。複数の オンプレミス Firewall Management Center を選択しても、**[Actions]** ペインは表示されません。

（注）
[Settings] を使用するには、管理者またはネットワーク管理者である必要があります。

ステップ 4 [ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] トグルボタンを有効にします。変更を オンプレミス Firewall Management Center と自動的に同期し、確認のためのステージングをしない場合は、**[Enable automatic sync of network objects]** トグルをオンにします。次に [Save] をクリックします。



（注）

- 選択した オンプレミス Firewall Management Center に 1 つ以上の子ドメインがある場合、または変更管理ワークフローが有効になっている場合は、[Discover & Manage Network Objects] トグルをオンにできません。
- [Discover & Manage Network Objects] がオフの場合は、[Enable automatic sync of network objects] トグルをオンにできません。

Security Cloud Control に新しい オンプレミス Firewall Management Center をオンボードするたびに、このトグルボタンを手動で有効にする必要があります。このオプションを有効にすると、Security Cloud Control はオンプレミス Firewall Management Center からオブジェクトを検出します。これらのオブジェクトを共有して管理し、Security Cloud Control によって管理される他のプラットフォーム間で一貫したオブジェクト定義を設定するために使用できます。

Security Cloud Control では、オンプレミス Firewall Management Center から検出されたオブジェクトにオーバーライドを追加し、変更をプッシュすると、以前はオーバーライドが許可されなかった場合でも、これらのオブジェクトをオーバーライドできるようになりました。**[View Network Object]** ウィンドウの **[Allow Overrides]** チェックボックスは、Security Cloud Control からオーバーライドを追加すると自動的に選択されます。

（注）
Security Cloud Control 内の既存のオブジェクトを オンプレミス Firewall Management Center に割り当てる場合は、オンプレミス Firewall Management Center を選択し、[アクション（Actions）] ペインで [オブジェクトの割り当て（Assign Objects）] をクリックします。

関連情報

- ネットワーク オブジェクト
- オンプレミス Firewall Management Center の設定のプレビューと展開
- オンプレミス Firewall Management Center の競合検出の有効化 （13 ページ）

設定変更の読み取り、破棄、および展開

すべてのデバイス設定の読み取り

Security Cloud Control の外部にあるデバイスの設定が変更された場合、Security Cloud Control に保存されているデバイスの設定と、当該デバイスの設定のローカルコピーは同じではなくなります。多くの場合、Security Cloud Control にあるデバイスの設定のコピーをデバイスに保存されている設定で上書きして、設定を再び同じにしたいと考えます。[すべて読み取り（Read All）] リンクを使用して、多くのデバイスでこのタスクを同時に実行できます。

Security Cloud Control によるデバイス設定の 2 つのコピーの管理方法の詳細については、「設定変更の読み取り、破棄、チェック、および展開」を参照してください。

[すべて読み取り（Read All）] をクリックした場合に、Security Cloud Control にあるデバイスの設定のコピーがデバイスの設定のコピーで上書きされる 3 つの設定ステータスを次に示します。

- [競合検出（Conflict Detected）]：競合検出が有効になっている場合、Security Cloud Control は、設定に加えられた変更について、管理するデバイスを 10 分ごとにポーリングします。Security Cloud Control がデバイスの設定が変更されたことを検出した場合、Security Cloud Control はデバイスの [競合検出（Conflict Detected）] 設定ステータスを表示します。
- [同期（Synced）]：デバイスが [同期（Synced）] 状態の場合に、[すべて読み取り（Read All）] をクリックすると、Security Cloud Control はすぐにデバイスをチェックして、設定に直接変更が加えられているかどうかを判断します。[すべて読み取り（Read All）] をクリックすると、Security Cloud Control はデバイスの設定のコピーを上書きすることを確認し、その後 Security Cloud Control が上書きを実行します。
- [未同期（Not Synced）]：デバイスが [未同期（Not Synced）] 状態の場合に、[すべて読み取り（Read All）] をクリックすると、Security Cloud Control は、Security Cloud Control を使用したデバイスの設定に対する保留中の変更があること、および[すべて読み取り（Read All）] 操作を続行すると保留中の変更が削除されてから、Security Cloud Control にある設定のコピーがデバイス上の設定で上書きされることを警告します。この [すべて読み取り（Read All）] は、[変更の破棄（Discard Changes）] と同様に機能します。設定変更の破棄 (9 ページ)

手順

ステップ 1 **セキュリティデバイス**を選択します。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 （任意）変更ログでこの一括アクションの結果を簡単に識別できるように、変更リクエストラベルを作成します。

ステップ 5 Security Cloud Control に保存する設定のデバイスを選択します。

Security Cloud Control では、選択したすべてのデバイスに適用できるアクションのコマンドボタンのみ提供されます。

選択したデバイスのいずれかについて、Security Cloud Control で設定変更がステージングされている場合、Security Cloud Control は警告を表示し、設定の一括読み取りアクションを続行するかどうかを尋ねられます。

ステップ 6 [すべて読み取り（Read All）] をクリックして続行します。

ステップ 7 設定の [すべて読み取り（Read All）] 操作の進行状況については、[通知（notifications）] タブで確認します。

ステップ 8 変更リクエストラベルを作成してアクティブ化した場合は、他の設定変更を誤ってこのイベントに関連付けないように、忘れずにラベルをクリアしてください。

関連情報

- 設定変更の読み取り、破棄、チェック、および展開
- 変更の破棄（Discard Changes）

すべてのデバイスの設定変更のプレビューと展開

組織上のデバイスに設定変更を加えたものの、その変更をまだ展開していない場合、Security Cloud Control は展開アイコン にオレンジ色のドットを表示して通知します。これらの変更の影響を受けるデバイスについては、[セキュリティデバイス（Security Devices）]ページに「未同期（Not Synced）」のステータスが表示されます。[展開（Deploy）] をクリックすると、保留中の変更があるデバイスを確認し、それらのデバイスに変更を展開できます。

この展開方法は、サポートされているすべてのデバイスで使用できます。

この展開方法を使用して、単一の設定変更を展開することも、待機して複数の変更を一度に展開することもできます。

手順

ステップ 1 Security Cloud Control のメニューバーで、[展開（Deploy）] ボタン をクリックします。

ステップ 2 展開する変更があるデバイスを選択します。デバイスに黄色の三角の注意マークが付いている場合、そのデバイスに変更を展開することはできません。黄色の三角の注意マークにマウスのポインタを合わせると、そのデバイスに変更を展開できない理由を確認できます。

ステップ 3 （オプション）保留中の変更に関する詳細情報を表示する場合は、[詳細な変更ログを表示（View Detailed Change log）] リンクをクリックして、その変更に関連付けられた変更ログを開きます。[展開（Deploy）] アイコンをクリックして、[保留中の変更があるデバイス（Devices with Pending Changes）] ページに戻ります。

ステップ 4 [今すぐ展開（Deploy Now）] をクリックして、選択したデバイスに今すぐ変更を展開します。[ジョブ（Jobs）] トレイの [アクティブなジョブ（Active jobs）] インジケータに進行状況が表示されます。

ステップ 5 （オプション）展開が完了したら、Security Cloud Control ナビゲーションバーの [ジョブ（Jobs）] をクリックします。展開の結果は、最近の「変更の展開（Deploy Changes）」ジョブに表示されます。

ステップ 6 変更リクエストラベルを作成したときに、作成したラベルに関連付ける設定変更がない場合は、そのラベルをクリアします。

デバイス設定の一括展開

共有オブジェクトを編集するなどして複数のデバイスに変更を加えた場合、影響を受けるすべてのデバイスにそれらの変更を一度に適用できます。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 Security Cloud Control で設定を変更した、すべてのデバイスを選択します。これらのデバイスは、「未同期」ステータスが表示されているはずです。

ステップ 5 次のいずれかの方法を使用して、変更を展開します。

- 画面の右上にある ボタンをクリックして、[保留中の変更があるデバイス（Devices with Pending Changes）] ウィンドウを表示します。これにより、選択したデバイス上の保留中の変更を展開する前に確認することができます。変更を展開するには、[今すぐ展開（Deploy Now）] をクリックします。

  （注）
  [保留中の変更があるデバイス（Devices with Pending Changes）] 画面でデバイスの横に黄色の警告三角形が表示されている場合、そのデバイスに変更を展開することはできません。そのデバイスに変更を展開できない理由を確認するには、警告三角形の上にマウスカーソルを置きます。

- 詳細ペインで [すべて展開（Deploy All）] をクリックします。すべての警告を確認し、[OK] をクリックします。一括展開は、変更を確認せずにすぐに開始します。

ステップ 6 （任意）ナビゲーションバーの [ジョブ（Jobs）] アイコン  をクリックして、一括展開の結果を表示します。

オンプレミス Firewall Management Center 設定のプレビューと展開

値の変更やオブジェクトへのオーバーライドの追加など、オブジェクトに設定変更を加えた場合は、それらのすべての変更を一度に オンプレミス Firewall Management Center に展開できます。

（注） このタスクでは、設定の変更を オンプレミス Firewall Management Center にのみ展開します。これらの変更を Firewall Threat Defense デバイスに展開するには、オンプレミス Firewall Management Center から手動で変更を展開する必要があります。詳細については、『Cisco Secure Firewall Management Center Device Configuration Guide』の「Configuration Deployment」を参照してください。

手順

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

ステップ 2 [FMC] タブをクリックします。

ステップ 3 変更をプレビューして展開する オンプレミス Firewall Management Center を選択します。

（注）
Security Cloud Control は、オンプレミス Firewall Management Center が同期していないことを検出し、ステータスを [Not Synced] として表示します。

ステップ 4 右側の詳細ペインで [Preview and Deploy] をクリックします。

ステップ 5 警告を確認します。すぐに展開するには、**[Deploy Now]** をクリックします。確認後に続行しない場合は、**[Discard All]** をクリックします。

ステップ 6 または、画面の右上にある ダウンロード ボタンをクリックして、**[Devices with Pending Changes]** ウィンドウを表示できます。デバイスを選択し、展開する前に、選択したデバイス上の保留中の変更を確認します。

ステップ 7 変更を展開するには、[今すぐ展開（Deploy Now）] をクリックします。

設定変更の破棄

Security Cloud Control を使用してデバイスの構成に加えた、展開されていない構成変更のすべてを「元に戻す」場合は、[変更の破棄（Discard Changes）] をクリックします。[変更の破棄（Discard Changes）] をクリックすると、Security Cloud Control は、デバイスに保存されている構成でデバイスの構成のローカルコピーを完全に上書きします。

[変更の破棄（Discard Changes）] をクリックすると、デバイスの構成ステータスは [未同期（Not Synced）] 状態になります。変更を破棄すると、Security Cloud Control 上の構成のコピーは、デ

バイス上の構成のコピーと同じになり、Security Cloud Control の構成ステータスは [同期済み（Synced）] に戻ります。

デバイスの展開されていない構成変更のすべてを破棄する（つまり「元に戻す」）には、次の手順を実行します。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**セキュリティデバイス** を選択します。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 構成変更を実行中のデバイスを選択します。

ステップ 5 右側の [未同期（Not Synced）] ペインで [変更の破棄（Discard Changes）] をクリックします。

- FDM による管理 デバイスの場合は、Security Cloud Control で「Security Cloud Control 上の保留中の変更は破棄され、このデバイスに関する Security Cloud Control 構成は、デバイス上の現在実行中の構成に置き換えられます（Pending changes on CDO will be discarded and the CDO configuration for this device will be replaced with the configuration currently running on the device）」という警告メッセージが表示されます。[続行（Continue）] をクリックして変更を破棄します。
- Meraki デバイスの場合は、Security Cloud Control で変更がすぐに削除されます。
- AWS デバイスの場合は、Security Cloud Control で削除しようとしているものが表示されます。[同意する（Accept）] または [キャンセル（Cancel）] をクリックします。

オンプレミス Firewall Management Center 設定変更の破棄

Security Cloud Control で行ったすべての設定変更を元に戻す場合は、この手順を使用します。Security Cloud Control と オンプレミス Firewall Management Center の間で共有されているオブジェクトなども含まれます。これを実行すると、Security Cloud Control は、デバイスに保存されている設定で設定のローカルコピーを完全に上書きします。

手順

ステップ 1 **[管理（Administration）] > [統合（Integrations）] > [Firewall Management Center]**

ステップ 2 [FMC] タブをクリックします。

ステップ 3 変更を破棄する オンプレミス Firewall Management Center を選択します。

ステップ 4 [Not Synced] ペインで [Discard Changes] をクリックします。

[Discard Changes] をクリックすると、オンプレミス Firewall Management Center の設定ステータスは [Not Synced] 状態になります。変更を破棄した後、Security Cloud Control に保存されている設定コピーは オンプ

レミス Firewall Management Center の設定と一致します。Security Cloud Control のステータスは、[Synced] に戻ります。

デバイスのアウトオブバンド変更

アウトオブバンド変更とは、Security Cloud Control を使用せずにデバイス上で直接行われた変更を指します。アウトオブバンド変更は、SSH 接続を介してデバイスのコマンド ライン インターフェイスを使用して、または、ASA の場合は Adaptive Security Device Manager（ASDM）、FDM による管理 デバイスの場合は FDM、オンプレミス Firewall Management Center ユーザー インターフェイス上の オンプレミス Firewall Management Center などのローカルマネージャを使用して行うことができます。アウトオブバンド変更により、Security Cloud Control に保存されているデバイスの設定とデバイス自体に保存されている設定との間で競合が発生します。

デバイスでのアウトオブバンド変更の検出

ASA、FDM による管理デバイス、Cisco IOS デバイス、またはオンプレミス Firewall Management Center に対して競合検出が有効になっている場合、Security Cloud Control は 10 分ごとにデバイスをチェックし、Security Cloud Control の外部でデバイスの設定に直接加えられた新たな変更を検索します。

Security Cloud Control は、Security Cloud Control に保存されていないデバイスの設定に対する変更を検出した場合、そのデバイスの [設定ステータス（Configuration Status）] を [競合検出（Conflict Detected）] 状態に変更します。

Security Cloud Control が競合を検出した場合、次の 2 つの状態が考えられます。

- Security Cloud Control のデータベースに保存されていない設定変更が、デバイスに直接加えられています。
- FDM による管理 デバイスの場合、FDM による管理 デバイスに展開されていない「保留中」の設定変更がある可能性があります。
- オンプレミス Firewall Management Center の場合、たとえば、Security Cloud Control との同期が保留されている Security Cloud Control の外部で行われた変更や、オンプレミス Firewall Management Center への展開が保留されている Security Cloud Control で行われた変更がある可能性があります。

Security Cloud Control とデバイス間の設定を同期する

設定の競合について

[セキュリティデバイス（Security Devices）] ページで、デバイスまたはサービスのステータスが [同期済み（Synced）]、[未同期（Not Synced）]、または [競合検出（Conflict Detected）] になっていることがあります。Security Cloud Control を使用して管理する オンプレミス Firewall

Management Center のステータスを確認するには、**[管理（Administration）] > [統合（Integrations）] > [Firewall Management Center]** に移動します。

- デバイスが [同期済み（Synced）] の場合、Security Cloud Control の設定と、デバイスにローカルに保存されている設定は同じです。
- デバイスが [未同期（Not Synced）] の場合、Security Cloud Control に保存された設定が変更され、デバイスにローカルに保存されている設定とは異なっています。Security Cloud Control からデバイスに変更を展開すると、Security Cloud Control のバージョンに一致するようにデバイスの設定が変更されます。
- Security Cloud Control の外部でデバイスに加えられた変更は、**アウトオブバンドの変更**と呼ばれます。デバイスの競合検出が有効になっている場合、アウトオブバンドの変更が行われると、デバイスのステータスが [競合が検出されました（Conflict Detected）] に変わります。アウトオブバンドの変更を受け入れると、Security Cloud Control の設定がデバイスの設定と一致するように変更されます。

競合検出

競合検出が有効になっている場合、Security Cloud Control はデフォルトの間隔でデバイスをポーリングして、Security Cloud Control の外部でデバイスの構成が変更されたかどうかを判断します。変更が行われたことを検出すると、Security Cloud Control はデバイスの構成ステータスを [競合検出（Conflict Detected）] に変更します。Security Cloud Control の外部でデバイスに加えられた変更は、「アウトオブバンドの」変更と呼ばれます。

Security Cloud Control によって管理されているオンプレミス Firewall Management Center で、ステージングされた変更があり、デバイスが [未同期（Not Synced）] 状態の場合、Security Cloud Control はデバイスのポーリングを停止して変更を確認します。Security Cloud Control との同期が保留されている Security Cloud Control の外部で行われた変更と、オンプレミス Firewall Management Center への展開が保留されている Security Cloud Control で行われた変更がある場合、Security Cloud Control は オンプレミス Firewall Management Centerが [競合検出（Conflict Detected）] 状態であることを宣言します。

このオプションを有効にすると、デバイスごとに競合または OOB 変更を検出する頻度を設定できます。詳細については、デバイス変更のポーリングのスケジュール （17 ページ）を参照してください。

競合検出の有効化

競合検出を有効にすると、Security Cloud Control の外部でデバイスに変更が加えられた場合に警告が表示されます。

手順

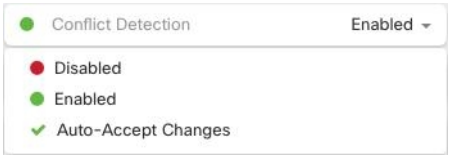
ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブを選択します。

ステップ 4 競合検出を有効にする 1 台または複数のデバイスを選択します。

ステップ 5 デバイステーブルの右側にある [競合検出（Conflict Detection）] ボックスで、リストから [有効（Enabled）] を選択します。



オンプレミス Firewall Management Center の競合検出の有効化

オンプレミス Firewall Management Center の競合検出を有効にすると、Security Cloud Control との同期が保留されている Security Cloud Control の外部で行われた変更と、Security Cloud Control で行われた変更がオンプレミス オンプレミス Firewall Management Center への展開が保留されている場合に、その情報を把握できます。

手順

ステップ 1 **[管理（Administration）] > [統合（Integrations）] > [Firewall Management Center]**。

ステップ 2 リストから、競合検出を有効にする オンプレミス Firewall Management Center を選択します。

ステップ 3 右側のペインの [競合検出（Conflict Detection）] ボックスで、リストから [有効（Enabled）] を選択します。

（注）
Security Cloud Control によって管理される他のデバイスとは異なり、オンプレミス Firewall Management Center では、競合検出を有効または無効にできます。変更の自動承認は選択できません。

デバイスからのアウトオブバンド変更の自動的な受け入れ

変更の自動的な受け入れを有効にすることで、管理対象デバイスに直接加えられた変更を自動的に受け入れるように Security Cloud Control を設定できます。Security Cloud Control を使用せずにデバイスに直接加えられた変更は、アウトオブバンド変更と呼ばれます。アウトオブバンドの変更により、Security Cloud Control に保存されているデバイスの設定とデバイス自体に保存されている設定との間で競合が発生します。

変更の自動受け入れ機能は、競合検出のための強化機能です。デバイスで変更の自動受け入れを有効にしている場合、Security Cloud Control は 10 分ごとに変更をチェックして、デバイスの設定に対してアウトオブバンドの変更が行われたかどうかを確認します。設定が変更されていた場合、Security Cloud Control は、プロンプトを表示することなく、デバイスの設定のローカルバージョンを自動的に更新します。

Security Cloud Control で行われたいずれかの設定変更がデバイスにまだ展開されていない場合、Security Cloud Control は設定変更を自動的に**受け入れません**。画面上のプロンプトに従って、次のアクションを決定します。

変更の自動承認を使用するには、最初に、[セキュリティデバイス（Security Devices）] ページの [競合検出（Conflict Detection）] メニューで自動承認オプションをテナントが表示できるようにします。次に、個々のデバイスでの変更の自動承認を有効にします。オンプレミス Firewall Management Center の場合は、[サービス（Services）] ページから **[管理（Administration）]** > **[統合（Integrations）]** > **[Firewall Management Center]** に移動し、[FMC] を選択します。

Security Cloud Control でアウトオブバンドの変更を検出するものの、変更を手動で受け入れたり拒否したりするオプションを選択する場合は、代わりに 競合検出 （12 ページ） を有効にします。

自動承認変更の設定

手順

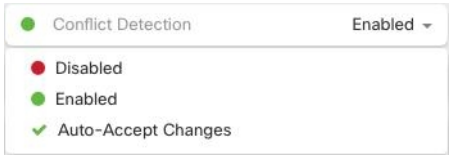
ステップ 1 管理者またはネットワーク管理者権限を持つアカウントを使用して Security Cloud Control にログインします。

ステップ 2 **[管理（Administration）]** > **[一般設定（General Settings）]** の順に選択します。

ステップ 3 [テナント設定（Tenant Settings）] エリアで、[デバイスの変更を自動承認するオプションの有効化（Enable the Option to Auto-accept Device Changes）] のトグルをクリックします。[セキュリティデバイス（Security Devices）] ページの [競合検出（Conflict Detection）] メニューに [変更の自動承認（Auto-Accept Changes）] メニューオプションが表示されます。

ステップ 4 左側のペインで**セキュリティデバイス**をクリックして、アウトオブバンドの変更を自動承認するデバイスを選択します。

ステップ 5 [競合の検出（Devices & Services）] メニューで、ドロップダウンメニューから [変更の自動承認（Auto-Accept Changes）] を選択します。



テナント上のすべてのデバイスの自動承認変更の無効化

手順

ステップ 1 [管理者（Admin）] または [ネットワーク管理者（Super Admin）] 権限を持つアカウントを使用して Security Cloud Control にログインします。

ステップ 2 **[管理（Administration）] > [一般設定（General Settings）]** の順に選択します。

ステップ 3 [テナント設定（Tenant Settings）] 領域で、トグルを左にスライドして灰色の X を表示し、[デバイスの変更を自動承認するオプションを有効にする（Enable the option to auto-accept device changes）] を無効にします。これにより、競合検出メニューの [変更の自動承認（Auto-Accept Changes）] オプションが無効になり、テナント上のすべてのデバイスでこの機能が無効になります。

（注）
[自動承認（Auto-Accept）] を無効にした場合、Security Cloud Control で承認する前に、各デバイスの競合を確認する必要があります。これまで変更の自動承認が設定されていたデバイスも対象になります。

設定の競合の解決

このセクションでは、デバイスで発生する設定の競合の解決に関する情報を提供します。

未同期ステータスの解決

次の手順を使用して、「未同期」の設定ステータスのデバイスを解決します。

手順

ステップ 1 ナビゲーションバーで **セキュリティデバイス** をクリックします。

（注）
オンプレミス Firewall Management Center の場合は、**[管理（Administration）] > [統合（Integrations）] > [Firewall Management Center]** をクリックして、[未同期（Not Synced）] 状態の FMC を選択し、ステップ 5 から続行します。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 未同期と報告されたデバイスを選択します。

ステップ 5 右側の [未同期（Not synced）] パネルで、次のいずれかを選択します。

- [プレビューして展開...（Preview and Deploy..）]：設定の変更を Security Cloud Control からデバイスにプッシュする場合は、今行った変更をプレビューして展開するか、待ってから一度に複数の変更を展開します。
- [変更の破棄（Discard Changes）]：設定の変更を Security Cloud Control からデバイスに**プッシュしない**場合、または Security Cloud Control で開始した設定の変更を「元に戻す」場合。このオプションは、Security Cloud Control に保存されている設定を、デバイスに保存されている実行構成で上書きします。

競合検出ステータスの解決

Security Cloud Control を使用すると、ライブデバイスごとに競合検出を有効化または無効化できます。競合検出 （12 ページ） が有効になっていて、Security Cloud Control を使用せずにデバイスの設定に変更が加えられた場合、デバイスの設定ステータスには [競合検出（Conflict Detected）] と表示されます。

[競合検出（Conflict Detected）] ステータスを解決するには、次の手順に従います。

手順

ステップ 1 ナビゲーションバーで **セキュリティデバイス** をクリックします。

（注）
オンプレミス Firewall Management Center の場合は、**[管理（Administration）]** > **[統合（Integrations）]** > **[Firewall Management Center]** をクリックして、[未同期（Not Synced）] 状態の FMC を選択し、ステップ 5 から続行します。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 競合を報告しているデバイスを選択し、右側の詳細ペインで [競合の確認（Review Conflict）] をクリックします。

ステップ 5 [デバイスの同期（Device Sync）] ページで、強調表示されている相違点を確認して、2 つの設定を比較します。

- 「最後に認識されたデバイス設定（Last Known Device Configuration）」というラベルの付いたパネルは、Security Cloud Control に保存されているデバイス設定です。
- [デバイスで検出（Found on Device）] というラベルの付いたパネルは、ASA の実行コンフィギュレーションに保存されている設定です。

ステップ 6 次のいずれかを選択して、競合を解決します。

- [デバイスの変更を承認（Accept Device changes）]：設定と、Security Cloud Control に保存されている保留中の変更がデバイスの実行コンフィギュレーションで上書きされます。

  （注）
  Security Cloud Control はコマンド ライン インターフェイス以外での Cisco IOS デバイスへの変更の展開をサポートしていないため、競合を解決する際の Cisco IOS デバイスの唯一の選択肢は [レビューなしで承認（Accept Without Review）] です。

- [デバイスの変更を拒否（Reject Device Changes）]：デバイスに保存されている設定を Security Cloud Control に保存されている設定で上書きします。

（注）

拒否または承認されたすべての設定変更は、変更ログに記録されます。

デバイス変更のポーリングのスケジュール

競合検出 （12 ページ） を有効にしている場合、または [設定（Settings）] ページで [デバイスの変更を自動承認するオプションの有効化（Enable the Option to Auto-accept Device Changes）] オプションを有効にしている場合、Security Cloud Control はデフォルトの間隔でデバイスをポーリングして、Security Cloud Control の外部でデバイスの設定に変更が加えられたかどうかを判断します。Security Cloud Control による変更のポーリング間隔は、デバイスごとにカスタマイズできます。ポーリング間隔の変更は、複数のデバイスに適用できます。

デバイスでこの間隔が選択されていない場合は、間隔は「テナントのデフォルト」に自動的に設定されます。

（注） [セキュリティデバイス（Security Devices）] ページでデバイスごとの間隔をカスタマイズすると、[一般設定（General Settings）] ページの [デフォルトの競合検出間隔（Default Conflict Detection Interval）] で選択したポーリング間隔がオーバーライドされます。デフォルトの競合検出間隔の設定

[セキュリティデバイス（Security Devices）] ページで [競合検出（Conflict Detection）] を有効にするか、[設定（Settings）] ページで [デバイスの変更を自動承認するオプションの有効化（Enable the Option to Auto-accept Device Changes）] オプションを有効にしたら、次の手順に従い Security Cloud Control によるデバイスのポーリング間隔をスケジュールします。

手順

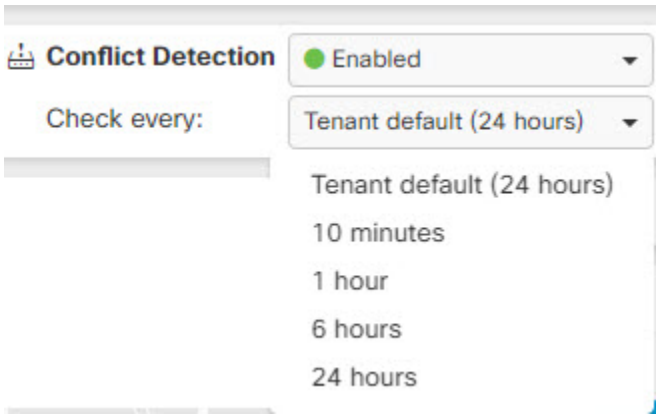
ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 競合検出を有効にする 1 台または複数のデバイスを選択します。

ステップ 5 [競合検出（Conflict Detection）] と同じ領域で、[チェック間隔（Check every）] のドロップダウンメニューをクリックし、目的のポーリング間隔を選択します。


Conflict Detection
Enabled
Check every:
Tenant default (24 hours)
Tenant default (24 hours)
10 minutes
1 hour
6 hours
24 hours

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。