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 Management Center の表示

オンボードされた オンプレミス Management Center は、**[管理（Administration）] > [Firewall Management Center]** で確認できます。[FMC] タブをクリックします。

オンプレミス Management Center 高可用性ペアの表示

高可用性ペアは [サービス（Services）] ページに表示されます。ペアを展開すると、オンプレミス Management Center ノード（プライマリとセカンダリ）が現在のステータスとともに表示されます。

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

1. [サービス（Services）] ページで、対応する高可用性ペアを確認します。
2. 右側のペインで機能をクリックして、オンプレミス Management Center で開きます。

   [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 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 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 Management Center の URL を指定してクロス起動できます。

各 オンプレミス Management Center ノードにクロス起動 URL を追加できます。ペアからクロス起動する場合、アクティブなノードがクロス起動されるため、現在アクティブなノードを確認する必要はありません。

特定の オンプレミス 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 Management Center ノードをクリックします。
2. 右側の [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 Management Center をクロス起動します。

   オンプレミス 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クロス起動URL（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 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 Management Center で再度有効にする必要があります。これを行うには、セカンダリ オンプレミス Management Center に移動し、 次を選択します。

高可用性 オンプレミス 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 Management Center に変換されます。

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

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 左側のペインで、**[管理（Administration）] > [Firewall Management Center]** の順に選択して、[サービス（Services）] ページを表示します。

ステップ 2 すでに オンプレミス 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 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[アクション（Actions）]ペインから[設定（Settings）]を選択します。複数の オンプレミス Management Center を選択すると、[アクション（Actions）] ペインは表示されないので注意してください。

（注）
[設定（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 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、[ネットワークオブジェクトの自動同期を有効にする（Enable automatic sync of network objects）] トグルをオンにします。

（注）
- 選択した オンプレミス 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、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] トグルをオンにできません。.
- [ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] がオフの場合は、[ネットワークオブジェクトの自動同期を有効にする（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 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 Management Center からのオブジェクトの検出を開始します。このオブジェクトは、Security Cloud Control の管理対象であ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共有、管理、および使用できます。

Security Cloud Control で、オンプレミス 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 オンプレミス Management Center にプッシュすると、それまでオーバーライドが許可さ

れていなかった場合でも、以降は オンプレミス Management Center でこれらのオブジェクトのオーバーライドが許可されます。Security Cloud Control からオーバーライドが追加されると、[ネットワークオブジェクトの表示（View Network Object）] ウィンドウの [オーバーライドを許可（Allow Overrides）] チェックボックスが自動的にオンになります。

（注）
Security Cloud Control 内の既存のオブジェクトを オンプレミス Management Center に割り当てる場合は、オンプレミス 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 Management Center の競合検出の有効化 （13 ページ）

デバイス設定変更について

デバイスを管理するために、Security Cloud Control は、デバイスの設定のコピーを独自のデータベースに保存する必要があります。Security Cloud Control は、管理対象デバイスから設定を「読み取る」とき、デバイス設定のコピーを作成し、それを保存します。Security Cloud Control が最初にデバイスの設定のコピーを読み取って保存するのは、デバイスが導入準備されたときです。以下 の選択肢のように、さまざまな目的に応じて設定を読み取ります。

- [変更の破棄（Discard Changes）]：このアクションは、デバイスの設定ステータスが「未同期」の場合に使用できます。未同期の状態では、デバイスの設定に対する変更が Security Cloud Control で保留中になっています。このオプションを使用すると、保留中のすべての変更を取り消すことができます。保留中の変更は削除され、Security Cloud Control は設定のコピーをデバイスに保存されている設定のコピーで上書きします。
- [変更の確認（Check for Changes）]：このアクションは、デバイスの設定ステータスが同期済みの場合に使用できます。[変更の確認（Checking for Changes）] をクリックすると、Security Cloud Control は、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のコピーと比較するように指示します。違いがある場合、Security Cloud Control はデバイスに保存されているコピーでそのデバイスの設定のコピーをすぐに上書きします。
- [競合の確認（Review Conflict）] と [レビューなしで承認（Accept Without Review）]：デバイスで [競合検出（Conflict Detection）] を有効にすると、Security Cloud Control はデバイスに加えられた設定の変更を 10 分ごとにチェックします。https://docs.defenseorchestrator.com/Welcome_to_Cisco_Defense_Orchestrator/Basics_of_Cisco_Defense_Orchestrator/Synchronizing_Configurations_Between_Defense_Orchestrator_and_Device/0010_Conflict_Detectionデバイスに保存されている設定のコピーが変更された場合、Security Cloud Control は「競合が検出されました」という設定ステータスを表示して通知します。

- [競合の確認（Review Conflict）]：[競合の確認（Review Conflict）] をクリックすると、デバイスで直接行われた変更を確認し、それらを受け入れるか拒否するかを選択できます。
- [レビューなしで承認（Accept Without Review）]：このアクションにより、Security Cloud Control がもつ、デバイスの構成のコピーが、デバイスに保存されている構成の最新のコピーで上書きされます。Security Cloud Control では、上書きアクションを実行する前に、構成の 2 つのコピーの違いを確認するよう求められません。

[すべて読み取り（Read All）]：これは一括操作です。任意の状態にある複数のデバイスを選択し、[すべて読み取り（Read All）] をクリックして、Security Cloud Control に保存されているすべてのデバイスの設定を、デバイスに保存されている設定で上書きできます。

- [変更の展開（Deploy Changes）]：デバイスの設定に変更を加えると、Security Cloud Control では、加えた変更が独自のコピーに保存されます。これらの変更は、デバイスに展開されるまで Security Cloud Control で「保留」されています。デバイスの設定に変更があり、それがデバイスに展開されていない場合、デバイスは未同期構成状態になります。

  保留中の設定変更は、デバイスを通過するネットワークトラフィックには影響しません。変更は、Security Cloud Control がデバイスに展開した後にのみ影響を及ぼします。Security Cloud Control がデバイスの設定に変更を展開すると、変更された設定の要素のみが上書きされます。デバイスに保存されている構成ファイル全体を上書きすることはありません。展開は、1 つのデバイスに対して開始することも、複数のデバイスに対して同時に開始することもできます。
- [すべて破棄（Discard All）] は、[プレビューして展開...（Preview and Deploy..）] をクリックした後にのみ使用できるオプションです。。[プレビューして展開（Preview and Deploy）] をクリックすると、Security Cloud Control で保留中の変更のプレビューが Security Cloud Control に表示されます。[すべて破棄（Discard All）] をクリックすると、保留中のすべての変更が Security Cloud Control から削除され、選択したデバイスには何も展開されません。上述の [変更の破棄（Discard Changes）] とは異なり、保留中の変更を削除すると操作が終了します。

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、「デバイス設定変更について」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 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 （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 を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ることに注意してください。

ステップ 6 [すべて読み取り（Read All）] をクリックします。

ステップ 7 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。[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 8 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。一括操作の個々のアクションの成功または失敗に関する詳細を確認する場合は、青色の [レビュー（Review）] リンクをクリックすると、[ジョブ（Jobs）] ページに移動します。

ステップ 9 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

すべてのデバイスの設定変更のプレビューと展開

テナント上のデバイスに構成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に、

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は、[デバイスとサービス（Devices and Services）] 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。

（注） 作成および変更を行う新しい FDM または FTD ネットワークオブジェクトまたはグループごとに、Security Cloud Control は、Security Cloud Control によって管理されるすべての オンプレミス Management Centerに対してこのページにエントリを作成します。

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、単一の構成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 画面の右上で [デプロイ（Deploy）] アイコン 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 Changelog）] 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 （オプション）[保留中の変更があるデバイス（Devices with Pending Changes）] ページを離れずに、変更を追跡する変更リクエストを作成します。

ステップ 5 [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 6 （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。展開の結果を示す最近の「変更の展開（Deploy Changes）」ジョブが表示されます。

ステップ 7 変更リクエストラベルを作成し、それに関連付ける構成変更がない場合は、それをクリアします。

次のタスク

- オンプレミス Firewall Management Center の設定のプレビューと展開 （9 ページ）
- オンプレミス Firewall Management Center 設定変更の破棄 （10 ページ）

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 の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 Management Center に展開できます。

（注） このタスクは、設定変更をオンプレミス Management Center にプッシュするだけです。オンプレミス Management Center の脅威に対する防御デバイスにこれらの変更を手動で展開してください。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 ナビゲーションウィンドウで、**[管理（Administration）] > [Firewall Management Center]** をクリックし、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 Management Center が同期していないことを検出し、ステータスを [未同期（Not Synced）] として表示します。

ステップ 2 右側の詳細ペインで [プレビューと展開（Preview and Deploy）] をクリックします。

ステップ 3 すべての警告を確認し、[今すぐ展開（Deploy Now）] をクリックします。展開は、変更を確認せずにすぐに開始します。プレビュー後に展開を続行しない場合は、[すべて破棄（Discard All）] をクリックします。

ステップ 4 または、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）] ウィンドウを表示することもできます。目的のデバイスを選択し、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します。

ステップ 5 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 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 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 と オンプレミス Management Center の間で共有されているオブジェクトなど、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。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する点に注意してください。

手順

ステップ 1 左側のペインで、**[管理（Administration）]** > **[Firewall Management Center]** をクリックします。

ステップ 2 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 3 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。

[変更の破棄（Discard Changes）] をクリックすると、オンプレミス Management Center の設定ステータスは [未同期（Not Synced）] 状態になります。変更を破棄すると、Security Cloud Control 上の設定のコピーは、

オンプレミス Management Center 上の設定のコピーと同じになり、Security Cloud Control の設定ステータスは [同期済み（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、**[ツールとサービス（Tools & Services）]** > **[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 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 Management Centerが [競合検出（Conflict Detected）] 状態であることを宣言します。

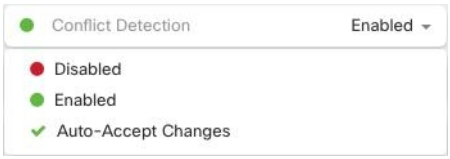
このオプションを有効にすると、デバイスごとに競合または OOB 変更を検出する頻度を設定できます。詳細については、デバイス変更のポーリングのスケジュール （17 ページ）を参照してください。

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 Management Center の競合検出の有効化

オンプレミス 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、オンプレミス 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に、その情報を把握できます。

手順

ステップ 1 ナビゲーションバーで、**[管理（Administration）] > [Firewall Management Center]** をクリックします。
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 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 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、テナントが[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 Management Center の場合は、[サービス（Services）] ページから **[ツールとサービス（Tools and Services）]** > **[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

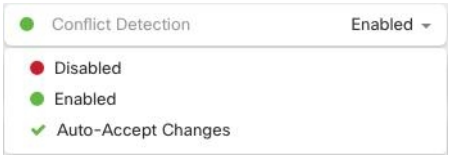
ステップ 1 管理者またはネットワーク管理者権限を持つアカウントを使用して Security Cloud Control にログインします。

ステップ 2 左側のペインで **[管理（Administration）]** > **[一般設定（General Settings）]** をクリックします。

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 左側のペインで **[管理（Administration）] > [一般設定（General Settings）]** をクリックします。

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）]** > **[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、今行った変更をすべてのデバイスの設定変更のプレビューと展開か、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）]** > **[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

[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

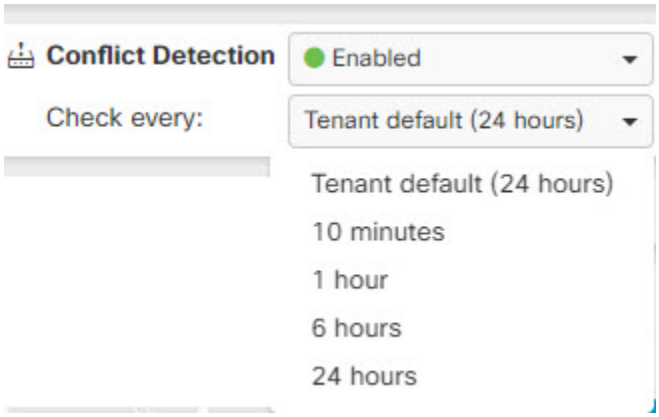
ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

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。



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。