

デバイス設定の管理

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 が管理対象デバイスから設定を読み取ると、設定をコピーして保存します。

Security Cloud Control はデバイスが導入されたときに、デバイスの設定のコピーを読み取って保存します。これらのアクションにはそれぞれ特定の目的があります。

- [変更の破棄（Discard Changes）]：このアクションは、デバイス設定のステータスが [未同期（Not Synced）] の場合に使用できます。[未同期（Not Synced）] の状態では、デバイス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、デバイス設定のステータスが [同期済み（Synced）] 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、そのデバイス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。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）]：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するには、[競合の確認（Review Conflict）] をクリックします。

  - [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 のデバイス設定のコピーが、デバイスに保存されている最新の設定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 2 つの設定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 はその変更を自らの設定のコピーに保存します。これらの変更は、デバイスに展開するまで Security Cloud Control で [保留中（Pending）] のままです。展開されていない保留中の変更がある場合、デバイスの設定状態は [未同期（Not Synced）] になります。

  保留中の設定変更は、ネットワークトラフィックには影響しません。これらは、Security Cloud Control がデバイスに展開した後にのみ有効になります。

  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。デバイス構成ファイル全体が上書きされることはありません。1つまたは複数のデバイスに変更を同時に展開できます。

- [すべて破棄（Discard All）]：このオプションは、[プレビューして展開...（Preview and Deploy...）] をクリックした後に表示されます。[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、保留中の変更すべてを、選択したデバイスに展開せずに Security Cloud Control から削除できます。[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。

- 設定変更の読み取り、破棄、および展開 （2 ページ）
- Security Cloud Control とデバイス間の設定を同期する （12 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。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

ステップ 3 [デバイス] タブをクリックします。

ステップ 4 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 5 （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 6 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。

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 7 [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 **[Read All]** 操作の進行状況については、[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 **[Review]** リンクをクリックすると、[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。

すべてのデバイスの設定変更のプレビューと展開

Security Cloud Control は、組織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、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

の影響を受ける各デバイスについて、[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できます。または、待機して複数の変更を一度に展開することもできます。

このデプロイメントメソッドは、Security Cloud Control Firewall Management が Security Cloud Control にオンボードされている場合にのみ使用できます。

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。黄色の三角の注意マークにマウスのポインタを合わせて、理由を確認します。

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、**[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 [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、[プラットフォーム（Platform）] メニューで [ファイアウォール（Firewall）]をクリックし、**[イベントとログ（Events & Logs）]**>**[イベント（Events）]**>**[ジョブ（Jobs）]** の順に選択します。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。

デバイスへの変更の展開

Procedure

ステップ 1 Security Cloud Control を使用してデバイスの設定を変更して保存すると、その変更はデバイスの設定の Security Cloud Control インスタンスに保存されます。

ステップ 2 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 3 **セキュリティデバイス**を選択します。

ステップ 4 [デバイス] タブをクリックします。

ステップ 5 適切なデバイスタイプのタブをクリックします。変更を加えると、デバイスの設定ステータスに [未同期（Not synced）] と表示されます。

ステップ 6 次のいずれかの方法を使用して、変更を展開します。

- デバイスを選択し、[未同期（Not Synced）] ペインで [プレビューして展開（Preview and Deploy）] をクリックします。[保留中の変更（Pending Changes）] 画面で、変更を確認します。保留中のバージョンに問題がなければ、[今すぐ展開（Deploy Now）] をクリックします。

  変更が正常に展開されたら、変更ログを表示して、展開の結果を確認できます。

- [展開（Deploy）] アイコン をクリックします。詳細については、すべてのデバイスの設定変更のプレビューと展開, on page 3を参照してください。

変更をキャンセルする

Security Cloud Control からデバイスに変更を展開するときに [キャンセル（Cancel）] をクリックすると、行った変更はデバイスに展開されません。プロセスはキャンセルされます。行った変更はまだ Security Cloud Control で保留中であり、最終的に FDM による管理 デバイスに展開する前に編集を加えることができます。

変更の破棄

変更をプレビューしているときに [すべて破棄（Discard all）] をクリックすると、自分が行った変更と、他のユーザーが行ったもののデバイスに展開しなかったその他の変更が削除されます。Security Cloud Control は、保留中の構成を、変更が行われる前の最後の読み取りまたは展開された構成に戻します。

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。

Procedure

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。

Note [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。

スケジュールされた自動展開について

Security Cloud Control を使用すると、CDO が管理する 1 つ以上のデバイスの構成を変更し、都合のよいタイミングでそれらのデバイスに変更を展開するようにスケジュールできます。

[設定（Settings）] ページの [テナント設定（Tenant Settings）] タブで 自動展開をスケジュールするオプションを有効にする をした場合のみ、展開をスケジュールできます。このオプションを有効にすると、展開スケジュールを作成、編集、削除できます。展開スケジュールによって、Security Cloud Control に保存されたすべてのステージング済みの変更が、設定した日時に展開されます。[ジョブ] ページから、展開スケジュールを表示および削除することもできます。

Security Cloud Control に読み取られていないデバイスに直接変更が加えられた場合、その競合が解決されるまで、展開スケジュールはスキップされます。[ジョブ（Jobs）] ページには、スケジュールされた展開が失敗したインスタンスが一覧表示されます。[自動展開をスケジュールするオプションを有効にする（Enable the Option to Schedule Automatic Deployments）] をオフにすると、スケジュールされたすべての展開が削除されます。

Caution 複数のデバイスの新しい展開をスケジュールし、それらのデバイスの一部に展開が既にスケジュールされている場合、既存の展開スケジュールが新しい展開スケジュールで上書きされます。

Note 展開スケジュールを作成すると、スケジュールはデバイスのタイムゾーンではなく現地時間で作成されます。展開スケジュールは、サマータイムに合わせて自動的に調整されません。

自動展開をスケジュールするオプションを有効にする

自動展開をスケジュールするオプションを有効にすると、都合のよい日時に将来の展開をスケジュールできます。このオプションを有効にすると、単一の自動展開をスケジュールしたり、定期的な自動展開を設定したりできます。

デバイスの Security Cloud Control で行われた変更は、 に保留中の変更がある場合、デバイスに自動的に展開されません。デバイスが [競合検出（Conflict Detected）] または [未同期（Not Synced）] など、[同期（Synced）] 状態でない場合、スケジュールされた展開は実行されません。[ジョブ（Jobs）] ページには、スケジュールされた展開が失敗したインスタンスが一覧表示されます。

[Enable the Option to Schedule Automatic Deployments] をオフにすると、スケジュールされたすべての展開が削除されます。



Important Security Cloud Control を使用して、スケジュールされた展開をデバイスに対して複数作成する場合、新しい展開によって既存の展開が上書きされます。API を使用してデバイスのスケジュールされた展開を複数作成する場合は、新しい展開をスケジュールする前に、既存の展開を**削除する必要**があります。

スケジュールされた自動展開を有効にするには、次の手順を実行します。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **管理（Administration）** > **一般設定（General Settings）** を選択します。

ステップ 3 **[Enable the option to schedule automatic deployments]** トグルボタンをオンにして、有効にします。

自動展開のスケジュール

展開スケジュールは、単一のイベントまたは繰り返し行われるイベントにすることができます。繰り返し行われる自動展開は、繰り返し行われる展開をメンテナンス期間に合わせるための便利な方法です。次の手順に従って、単一のデバイスに対して 1 回限りまたは繰り返し行われる展開をスケジュールします。



Important この手順は、Cisco ASA および FDM-managed デバイスにのみ適用されます。

[on-premises Firewall Management Center] または [Cloud-Delivered Firewall Management Center] によって管理される [Cisco Secure Firewall Threat Defense] デバイスの展開をスケジュールするには、「スケジュール」を参照してください。

Note 既存の展開がスケジュールされているデバイスへの展開をスケジュールすると、新しくスケジュールされた展開によって既存の展開が上書きされます。

Procedure

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 1 つ以上のデバイスを選択します。

ステップ 5 [デバイスの詳細（Device Details）] ペインで、[スケジュールされた展開（ Scheduled Deployments）] タブを見つけて、[スケジュール（Schedule）] をクリックします。

ステップ 6 展開をいつ実行するかを選択します。

- 1 回限りの展開の場合は、[1回限り（Once on）] オプションをクリックして、カレンダーから日付と時刻を選択します。
- 繰り返し展開する場合は、[定期（Every）] オプションをクリックします。日に 1 回と週に 1 回のいずれかの展開を選択できます。展開を実行する [曜日（Day）] と [時刻（Time）] を選択します。

ステップ 7 [保存（Save）] をクリックします。

スケジュールされた展開の編集

スケジュールされた展開を編集するには、次の手順に従います。

Procedure

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 1 つ以上のデバイスを選択します。

ステップ 5 [デバイスの詳細（Device Details）] ペインで、[スケジュールされた展開（ Scheduled Deployments）] タブを見つけて、[編集（Edit）] をクリックします。



ステップ 6 スケジュールされた展開の繰り返し回数、日付、または時刻を編集します。

ステップ 7 [保存（Save）] をクリックします。

スケジュールされた展開の削除

スケジュールされた展開を削除するには、次の手順に従います。

Note 複数のデバイスの展開をスケジュールしてから、一部のデバイスのスケジュールを変更または削除した場合は、残りのデバイスの元のスケジュールされた展開が保持されます。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] 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 1 つ以上のデバイスを選択します。
ステップ 5 [デバイスの詳細（Device Details）] ペインで、[スケジュールされた展開（Scheduled Deployments）] タブを見つけて、[削除（Delete）] をクリックします。

- 設定変更の読み取り、破棄、チェック、および展開
- すべてのデバイス設定の読み取り, on page 2
- すべてのデバイスの設定変更のプレビューと展開, on page 3

設定変更の確認

[変更の確認（Check for Changes）] をクリックして、デバイスの設定がデバイス上で直接変更されているか、Security Cloud Control に保存されている設定のコピーと異なっているかどうかを確認します。このオプションは、デバイスが [同期（Synced）] 状態のときに表示されます。

変更を確認するには、次の手順を実行します。

Procedure

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 設定がデバイス上で直接変更された可能性があるデバイスを選択します。

ステップ 5 右側の [同期（Synced）] ペインで [変更の確認（Check for Changes）] をクリックします。

ステップ 6 次の動作は、デバイスによって若干異なります。

- Meraki デバイスの場合、デバイスの設定に変更があった場合、次のメッセージが表示されます。

```
Reading the policy from the device. If there are active deployments on the device, reading will
start after they are finished.
```

  - [OK] をクリックして、先へ進みます。デバイスの設定で、Security Cloud Control に保存されている設定が上書きされます。
  - 操作をキャンセルするには、[キャンセル（Cancel）] をクリックします。

- デバイスの場合：

a. 提示された 2 つの設定を比較します。[続行（Continue）] をクリックします。**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設定は、Security Cloud Control に保存されている設定です。[デバイスで検出（Found on Device）] というラベルの付いた設定は、ASA に保存されている設定です。

b. 次のいずれかを選択します。

1. [拒否（Reject）] : アウトオブバンド変更を拒否して、「最後に認識されたデバイス設定（Last Known Device Configuration）」を維持します。
2. [承認（Accept）] : アウトオブバンド変更を承認して、Security Cloud Control に保存されているデバイスの設定を、デバイスで見つかった設定で上書きします。

c. [続行（Continue）] 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。

Procedure

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。

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, on page 17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。

Procedure

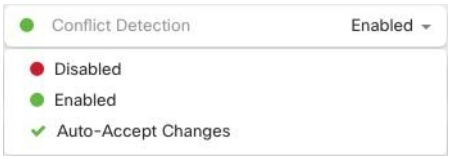
ステップ 1 **セキュリティデバイス**を選択します。

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。



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。

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, on page 12 を有効にします。

自動承認変更の設定

Procedure

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。

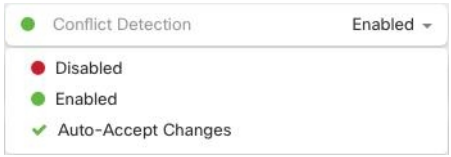
ステップ 2 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 3 **管理（Administration）** > **一般設定（General Settings）** の順に選択します。

ステップ 4 [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 5 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 6 [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

Procedure

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 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 3 **管理（Administration）** > **一般設定（General Settings）** の順に選択します。

ステップ 4 [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。

Note [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

ここでは、デバイスで発生する設定の競合を解決する方法について説明します。

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。

Procedure

ステップ 1 **セキュリティデバイス**を選択します。

Note 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, on page 12 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。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

Note 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 3 [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 4 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 5 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 6 [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 7 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。

Note 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。

Note 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, on page 12 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。デバイスごとに、Security Cloud Control が変更をポーリングする頻度を設定できます。このカスタマイズは複数のデバイスに適用できます。

この間隔が設定されていないデバイスについては、間隔が「テナントのデフォルト」に自動的に設定されます。

Note [セキュリティデバイス（Security Devices）] ページでデバイスごとのカスタム間隔を設定すると、[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）]デフォルトの競合検出間隔の設定で選択したポーリング間隔が上書きされます。

[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できます。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

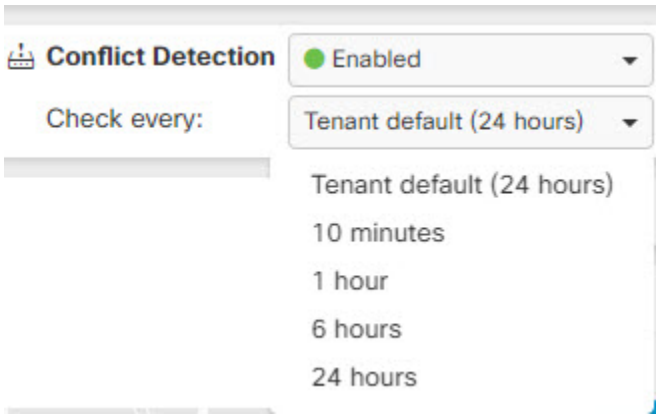
ステップ 2 **セキュリティデバイス**を選択します。

ステップ 3 [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 4 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 5 競合検出を有効にするデバイスを選択します。

ステップ 6 [競合検出（Conflict Detection）] の横にある [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。