オンボーディングされたデバイスの管理

この章では、オンボーディングされたデバイスのデバイス設定の管理について説明します。

Security Cloud Control のデバイスの IP アドレスの変更

IP アドレスを使用してデバイスを Security Cloud Control にオンボードすると、Security Cloud Control ではその IP アドレスがデータベースに保存され、デバイスとの通信に使用されます。デバイスの IP アドレスが変更された場合は、Security Cloud Control に保存されている IP アドレスを更新して、新しいアドレスに一致させることができます。Security Cloud Control でデバイスの IP アドレスを変更しても、デバイスの構成は変更されません。

Security Cloud Control でデバイスとの通信に使用する IP アドレスを変更するには、次の手順を実行します。

手順

ステップ 1 左側のペインで **Security Devices** 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。

フィルタ機能と検索機能を使用して、必要なデバイスを見つけることができます。

ステップ 4 IP アドレスを変更するデバイスを選択します。

ステップ 5 [デバイスの詳細（Device Details）]ペインの上で、デバイスの IP アドレスの横にある編集ボタンをクリックします。

ステップ 6 フィールドに新しい IP アドレスを入力し、青色のチェックボタンをクリックします。

デバイス自体は変更されないため、デバイスの [設定ステータス（Configuration Status）] には、引き続き [同期済み（Synced）] と表示されます。

関連情報：

- テナント間でのデバイスの移動 （9 ページ）
- Security Cloud Control へのデバイス一括再接続 （8 ページ）

Security Cloud Control でのデバイスの名前の変更

すべてのデバイス、モデル、テンプレート、およびサービスには、Security Cloud Control へのオンボード時または作成時に名前が付けられます。デバイス自体の設定を変更せずに、その名前を変更することができます。

手順

ステップ 1 左側のペインで **Security Devices** をクリックします。

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

ステップ 3 名前を変更するデバイスを選択します。

ステップ 4 [デバイスの詳細（Device Details）] ペインの上で、デバイス名の横にある編集ボタンをクリックします。

ステップ 5 フィールドに新しい名前を入力し、青色のチェックボタンをクリックします。

デバイス自体は変更されないため、デバイスの [設定ステータス（Configuration Status）] には、引き続き [同期済み（Synced）] と表示されます。

デバイスとサービスのリストのエクスポート

この記事では、デバイスとサービスのリストをコンマ区切り値（.csv）ファイルにエクスポートする方法について説明します。この形式にしたら、Microsoft Excel などのスプレッドシートアプリケーションでファイルを開いて、リスト内のアイテムを並べ替えたり、フィルタ処理したりできます。

エクスポートボタンは、デバイスとテンプレートタブで使用できます。選択したデバイスタイプタブで、デバイスの詳細をエクスポートすることもできます。

デバイスとサービスのリストをエクスポートする前に、フィルタペインを見て、エクスポートしたい情報が [セキュリティデバイス（Security Devices）] ページに表示されているかどうかを確認します。すべてのフィルタをクリアしてすべての管理対象デバイスとサービスを表示するか、情報をフィルタしてすべてのデバイスとサービスの一部を表示します。エクスポート機能は、[セキュリティデバイス（Security Devices）] ページに表示される内容をエクスポートします。

手順

ステップ 1 左側のペインで **Security Devices** 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タブをクリックして、そのタブのデバイスの詳細をエクスポートするか、[すべて（All）] をクリックしてすべてのデバイスから詳細をエクスポートします。

フィルタおよび検索機能を使用して、必要なデバイスを見つけることができます。

ステップ 4 [CSV にリストエクスポート（Export list to CSV）] をクリックします。

ステップ 5 プロンプトが表示されたら、.csv ファイルを保存します。

ステップ 6 スプレッドシート アプリケーションで .csv ファイルを開いて、結果を並べ替えたりフィルタリングしたりすることができます。

デバイス設定のエクスポート

一度にエクスポートできるデバイス設定は1つだけです。次の手順を使用して、デバイスの設定を JSON ファイルにエクスポートします。

手順

ステップ 1 左側のペインで **Security Devices** 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。

フィルタ機能と検索機能を使用して、必要なデバイスを見つけることができます。

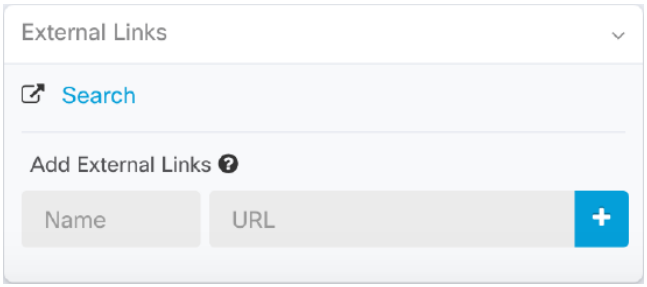
ステップ 4 必要なデバイスを選択して、強調表示します。

ステップ 5 [アクション（Actions）] ペインで、[設定のエクスポート（Export Configuration）] を選択します。

ステップ 6 [確認（Confirm）] を選択して、設定を JSON ファイルとして保存します。

デバイスの外部リンク

外部リソースへのハイパーリンクを作成し、Security Cloud Control で管理するデバイスに関連付けることができます。この機能を使用して、いずれかのデバイスのローカルマネージャへの便利なリンクを作成できます（Adaptive Security Device Manager (ASDM))。この機能を使用して、検索エンジン、ドキュメントリソース、企業 wiki、または選択したその他の URL へのリンクを作成できます。必要な数の外部リンクをデバイスに関連付けることができます。同じリンクを同時に複数のデバイスに関連付けることもできます。



作成したリンクはどこにでも到達できますが、企業のセキュリティ要件は変わりません。たとえば、普段オンプレミスで、または VPN 接続を介して特定の URL にアクセスすることによって企業ネットワークに接続する必要がある場合、この要件は維持されます。企業が特定の URL

をブロックしている場合、それらのURLは引き続きブロックされます。制限されていないURLは引き続き制限されません。

location変数

URL に組み込むことができる {location} 変数を作成しました。この変数には、デバイスの IP アドレスが入力されます。次に例を示します。

```
https://{location}
```

または FDM 管理対象デバイスの FDM に到達します。

関連情報：

- デバイスノートを書く （9 ページ）
- デバイスとサービスのリストのエクスポート （3 ページ）

デバイスからの外部リンクの作成

手順

ステップ 1 左側のペインで **Security Devices** 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 デバイスまたはモデルを選択します。

フィルタ機能と検索機能を使用して、必要なデバイスを見つけることができます。

ステップ 5 右側の詳細ペインから、[外部リンク（External Links）] セクションに移動します。

ステップ 6 リンクの名前を入力します。

ステップ 7 [URL] フィールドにリンクの URL を入力します。完全な URL を指定する必要があります。たとえばシスコの場合、http://www.cisco.com と入力します。

ステップ 8 [+] をクリックして、リンクとデバイスを関連付けます。

FDM への外部リンクの作成

FDM 管理対象デバイスの Firepower Device Manager（FDM）を Security Cloud Control から直接開く便利な方法を次に示します。

手順

ステップ 1 左側のペインで **Security Devices** 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。

フィルタ機能と検索機能を使用して、必要なデバイスを見つけることができます。

ステップ 4 デバイスまたはモデルを選択します。

ステップ 5 右側の詳細ペインから、[外部リンク（External Links）] セクションに移動します。

ステップ 6 FDM などのリンクの名前を入力します。

ステップ 7 https://{location} を [URL] フィールドに入力します。{location} 変数には、デバイスの IP アドレスが入力されます。

ステップ 8 [+] ボックスをクリックします。

複数デバイスの外部リンクの作成

手順

ステップ 1 左側のペインで **Security Devices** 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。

フィルタ機能と検索機能を使用して、必要なデバイスを見つけることができます。

ステップ 4 複数のデバイスまたはモデルを選択します。

ステップ 5 右側の詳細ペインから、[外部リンク（External Links）] セクションに移動します。

ステップ 6 リンクの名前を入力します。

ステップ 7 次のいずれかの方法を使用して、アクセスする URL を入力します。

- 以下をURL フィールドに入力します。

  ```
  https://{location}
  ```

  URL フィールドに入力します。{location} 変数には、デバイスの IP アドレスが入力されます。入力後、デバイスの ASDM への自動リンクが作成されます。

- [URL] フィールドにリンクの URL を入力します。完全な URL を指定する必要があります。たとえばシスコの場合、http://www.cisco.com と入力します。

ステップ 8 [+] をクリックして、リンクとデバイスを関連付けます。

外部リンクの編集または削除

手順

ステップ 1 左側のペインで **Security Devices** 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。

フィルタ機能と検索機能を使用して、必要なデバイスを見つけることができます。

ステップ 4 デバイスまたはモデルを選択します。

ステップ 5 右側の詳細ペインから、[外部リンク（External Links）] セクションに移動します。

ステップ 6 リンク名の上にカーソルを置くと、編集アイコンと削除アイコンが表示されます。

ステップ 7 該当するアイコンをクリックし、外部リンクを編集または削除して、アクションを確認します。

複数のデバイスへの外部リンクの編集または削除

手順

ステップ 1 左側のペインで **Security Devices** 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。

フィルタ機能と検索機能を使用して、必要なデバイスを見つけることができます。

ステップ 4 複数のデバイスまたはモデルを選択します。

ステップ 5 右側の詳細ペインから、[外部リンク（External Links）] セクションに移動します。

ステップ 6 リンク名の上にカーソルを置くと、編集アイコンと削除アイコンが表示されます。

ステップ 7 該当するアイコンをクリックし、外部リンクを編集または削除して、アクションを確認します。

Security Cloud Control へのデバイス一括再接続

Security Cloud Control を使用すると、管理者は複数の管理対象デバイスを Security Cloud Control に同時に再接続を試みることができます。Security Cloud Control が管理するデバイスが「到達不能」とマークされている場合、Security Cloud Control は帯域外構成の変更を検出したり、デバイスを管理したりできなくなります。切断については、さまざまな原因が考えられます。デバイスの再接続を試みることは、Security Cloud Control によるデバイスの管理を復元するための簡単な最初のステップです。

（注） 新しい証明書を持つデバイスを再接続する場合、Security Cloud Control は、デバイス上の新しい証明書を自動的に確認して受け入れ、それらとの再接続を続行します。ただし、再接続するデバイスが 1 つだけの場合、Security Cloud Control は、それとの再接続を続行するために、証明書を手動で確認して受け入れることを求めます。

手順

ステップ 1 左側のペインで **Security Devices** 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。

フィルタを使用して、接続ステータスが「到達不能」であるデバイスを見つけてください。

ステップ 4 フィルタ処理の結果から、再接続を試みるデバイスを選択します。

ステップ 5 [再接続（Reconnect）] をクリックします。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 [通知（notifications）] タブで一括デバイス再接続アクションの進行状況を確認します。一括デバイス再接続ジョブのアクションがどのように成功または失敗したかについての詳細な情報が必要な場合は、青色の [レビュー（Review）] リンクをクリックして Security Cloud Control でのジョブのモニタリング に移動します。

ヒント
デバイスの証明書またはログイン情報が変更されたために再接続に失敗した場合は、それらのデバイスに個別に再接続して、新しいログイン情報を追加し、新しい証明書を受け入れる必要があります。

テナント間でのデバイスの移動

デバイスを Security Cloud Control テナントに導入準備すると、そのデバイスは、別の Security Cloud Control テナントに移行できません。デバイスを新しいテナントに移動させる場合は、古いテナントからデバイスを削除して、新しいテナントに導入準備し直す必要があります。

デバイス証明書の有効期限の検出

管理証明書は Security Cloud Control から FDM-managed および ASA デバイスへのアクセスに使用されますが、Security Cloud Control から ASA、FDM-managed、および FTD デバイスの仮想プライベートネットワーク機能を使用するには Cisco Secure Client（旧称 AnyConnect）が必要です。

Security Cloud Control は、これらの証明書の有効期限ステータスをアクティブにモニターし、証明書の期限日が近づくと、または期限切れになるとユーザーに通知します。これにより、証明書の期限切れによるデバイス操作の中断を回避できます。対応する証明書を更新して、この問題に対処する必要があります。

管理証明書の有効期限チェックは ASA および FDM 管理対象デバイスに適用され、Secure Client 証明書の有効期限チェックは ASA、FDM-managed、および FTD デバイスに適用されます。

証明書の有効期限通知の表示

右上隅の [通知（Notifications）]（  ）アイコンをクリックして、テナントで発生した最新のアラート、またはテナントにオンボード済みのデバイスに影響を及ぼすアラートを表示します。[優先順位：高（High Priority）] セクションには、証明書の有効期限通知が表示されます。

これらの通知は、証明書の期限日の 30 日前、14 日前、および 7 日前に送信され、その後は証明書が期限切れになるか、有効な証明書で更新されるまで毎日送信されます。ユーザー設定ページの [通知設定（Notification Settings）] セクションで、これらの通知を電子メールで受信するように登録することもできます。詳細については、「ユーザー通知設定」を参照してください。

デバイスノートを書く

以下の手順で、デバイス用に単一のプレーンテキストのノートファイルを作成します。

手順

ステップ 1 左側のペインで **Security Devices** 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 ノートを作成するデバイスまたはモデルを選択します。

ステップ 5 右側の [管理（Management）] ペインで、[ノート（Notes）] をクリックします。 Notes。

ステップ 6 右側のエディター ボタンをクリックして、既定のテキストエディタ（Vim または Emacs テキストエディタ）を選択します。

ステップ 7 [ノート（Notes）] ページを編集します。

ステップ 8 [保存（Save）] をクリックします。
ノートはタブに保存されます。

Security Cloud Control からデバイスを削除

Security Cloud Control からデバイスを削除するには、次の手順を使用します。

手順

ステップ 1 Security Cloud Control にログインします。

ステップ 2 左側のペインで **Security Devices** をクリックします。

ステップ 3 削除するデバイスを見つけ、そのデバイスの行でデバイスをチェックして選択します。

ステップ 4 右側にある [デバイスアクション（Device Actions）] パネルで、[削除（Remove）] を選択します。

ステップ 5 プロンプトが表示されたら、[OK] を選択して、選択したデバイスの削除を確認します。[キャンセル（Cancel）] を選択して、デバイスをオンボードしたままにします。

HA ペアの両方のデバイスを同時に削除する必要があることに注意してください。FDM-managed 個々のピアではなく、FDM-managed HA ペア名をクリックします。

セキュリティデバイスの管理

Security Cloud Control を使用すると、[Security Devices] ページでオンボード済みのデバイスを表示、管理、フィルタ処理、および評価できます。**[Security Devices]** ページから次のことができます。

- Security Cloud Control 管理用のデバイスとサービスをオンボードします。
- 管理対象のデバイスとサービスの設定状態と接続状態を表示します。

- オンボードしたデバイスとテンプレートを個別のタブに分類して表示します。セキュリティデバイスの概要 （13 ページ）を参照してください。
- 個々のデバイスとサービスを評価し、アクションを実行します。
- デバイスとサービスに固有の情報を表示し、問題を解決します。
- 次によって管理される脅威防御デバイスの正常性ステータスを表示します。
  - Cloud-Delivered Firewall Management Center
  - on-premises Firewall Management Center

  Cloud-Delivered Firewall Management Center によって管理される脅威防御デバイスの場合は、クラスタ内のデバイスのノードステータスも表示できます。
- 名前、タイプ、IPアドレス、モデル名、シリアル番号またはラベルで、デバイスまたはテンプレートを検索します。検索では大文字と小文字が区別されません。複数の検索条件を入力すると、少なくとも 1 つの条件に一致するデバイスとサービスが表示されます。ページレベルの検索 （17 ページ）を参照してください。
- デバイス タイプ、ハードウェアとソフトウェアのバージョン、Snort バージョン、設定ステータス、接続状態、競合検出、Secure Device Connector、およびラベルで、デバイスまたはテンプレートのフィルタを絞り込みます。「フィルタ」を参照してください。
- デバイスの削除

Security Cloud Control によって管理される Firewall Threat Defense デバイスのバックアップ

Security Cloud Control 管理対象 Firewall Threat Defense デバイスタイプをバックアップする方法については、以下を参考にしてください。

Cloud-Delivered Firewall Management Center によって管理される Firewall Threat Defense デバイスのバックアップ

- Security Cloud Control 左ペインで、**Administration** > **Firewall Management Center** を選択します。
- **[FMC]** タブで **[Cloud-delivered FMC]** を選択します。
- 右側のペインで **[Device]** をクリックして、Cloud-Delivered Firewall Management Center に移動します。
- 引き続き「クラウド提供型 Firewall Management Center からの Threat Defense デバイスのバックアップ」の手順に従います。

Security Cloud Control にオンボーディング済みの On-Premises Firewall Management Center によって管理される Firewall Threat Defense デバイスのバックアップ

- Security Cloud Control 左ペインで、**Administration** > **Firewall Management Center** を選択します。
- バックアップする On-Premises Firewall Management Center の Firewall Threat Defense デバイスを選択します。
- 右側のペインで **[FMC Cross Launch URL]** をクリックして on-premises Firewall Management Center に移動するか、on-premises Firewall Management Center に手動でログインします。
- 引き続き『*Cisco Secure Firewall Management Center Administration Guide*』の「Back Up the Management Center」の指示に従ってください。

Security Cloud Control にオンボーディング済みの Firewall Device Manager によって管理される Firewall Threat Defense デバイスのバックアップ

「FDM 管理対象デバイスのバックアップ」の手順に従います。

Security Cloud Control を介した Firewall Threat Defense デバイスの管理

始める前に

Security Cloud Control は、ハードウェア形式と仮想形式の両方で Firewall Threat Defense デバイスを管理するための統合インターフェイスを提供します。

次の 3 つの管理アプリケーションに関連付けられている Firewall Threat Defense デバイスは、Cisco Security Cloud Control プラットフォームで管理できます。

- セキュア Firewall Device Manager
- Secure Firewall Management Center
- セキュア Cloud-Delivered Firewall Management Center

手順

ステップ 1 Security Cloud Control プラットフォームにログインします。

ステップ 2 左側のペインで、[セキュリティデバイス（Security Devices）] をクリックします。

ステップ 3 [FTD] タブをクリックします。

ステップ 4 左上隅にある  をクリックします。

[Devices/Services] の下で、フィルタペインは Security Cloud Control からアクセスされる管理アプリケーションに基づいて Firewall Threat Defense デバイスを表示するフィルタを提供します。

- **FDM**：Firewall Device Manager で管理されている Firewall Threat Defense デバイス
- **FMC-FTD**：Firewall Management Center によって管理される Firewall Threat Defense デバイス
- **FTD**：Cloud-Delivered Firewall Management Center によって管理される Firewall Threat Defense デバイス

ステップ 5 管理アプリケーションの Firewall Threat Defense デバイスを表示するには、対応するチェックボックスをオンにします。

セキュリティデバイスの概要

[Security Devices] ページには、すべての物理および仮想オンボードデバイスと、オンボードデバイスから作成されたテンプレートが表示されます。[インベントリ（Inventory）] ページでは、デバイスとテンプレートがそれぞれのタイプに基づいて分類され、各デバイスタイプ専用の対応するタブに表示されます。

[Security Devices] ページで、次の詳細を確認できます。

- [Devices] タブには、Security Cloud Control にオンボードされているすべてのライブデバイスが表示されます。
- [Templates] タブには、ライブデバイスから、または Security Cloud Control にインポートされた設定ファイルから作成されたすべてのテンプレートデバイスが表示されます。

セキュリティデバイスのフィルタ

[Filter] パネルには、**[Security Devices]** ページで結果を絞り込み、特定の属性に基づいてデバイスを検索するための複数のオプションがあり、**デバイス/サービス、ハードウェアバージョン、デバイスのサポート終了、ソフトウェアバージョン、Snortバージョン、設定ステータス、接続の状態、競合検出、正常性ステータス、Secure Device Connector、およびラベル** に基づいてデバイスを検索できます。

ハードウェアのサポート終了（EoL）フィルタ

[Hardware End-of-Life (EoL)] フィルタを使用すると、ハードウェアサポートの最終日に近づいているデバイス、または最終日に達したデバイスを特定できます。この日付以降、Cisco はソフトウェアアップデート、セキュリティパッチ、またはテクニカルサポートを提供しません。これにより、運用上およびセキュリティ上のリスクが生じる可能性があります。

（注） [Hardware End-of-Life (EoL)] フィルタは現在、on-premises Firewall Management Center および Cloud-Delivered Firewall Management Center によって管理される Firewall Threat Defense デバイスと、ASA デバイスをサポートしています。

手順

1. **[Devices]** タブで、フィルタアイコンをクリックします。
2. 使用可能なフィルタのリストから、**[Device End-of-Life]** で、**[Hardware End-of-Life]** を選択します。

   このリストには、ハードウェアのサポート終了が近づいている、またはハードウェアのサポート終了に達したすべてのデバイスが表示されるようになりました。
3. 右側のペインで詳細情報を表示するデバイスを選択します。
4. **[Device End of Life]** セクションまで下にスクロールすると、次の詳細が表示されます。
   - 正確なサポート終了日。
   - サポート終了日までの残り期間
5. **[Know more]** をクリックします。

   次の情報を含む詳細ページを表示できます。
   - Cisco の推奨交換デバイスと製品仕様の両方に、公式データシートを表示するためのリンクが含まれています。
   - [Contact Cisco page] ページを介してリクエストを送信するためのガイダンス、および Cisco の専門家に直接連絡するオプション。
   - Cisco の製品再利用プログラムに関する情報。
6. **[Export]** をクリックすると、デバイスレポートが CSV 形式でダウンロードされ、オフラインで分析できます。

Security Cloud Control ラベルとフィルタ処理

ラベルは、デバイスまたはオブジェクトをグループ化するために使用されます。オンボーディング中またはオンボーディング後のいつでも、1 つ以上のデバイスにラベルを適用できます。ラベルをオブジェクトに適用するには、まずラベルを作成します。デバイスまたはオブジェクトにラベルを適用したら、対応するラベルを使用して、デバイステーブルまたはオブジェクトテーブルの内容をフィルタリングできます。

（注） デバイスに適用されたラベルは、その関連オブジェクトには拡張されません。また、共有オブジェクトに適用されたラベルは、その関連オブジェクトには拡張されません。

構文 group name:label を使用してラベルグループを作成できます。たとえば、Region:East または Region:West です。これらの 2 つのラベルを作成した場合、グループラベルは Region になり、そのグループの East または West から選択できます。

デバイスとオブジェクトにラベルを適用する

デバイスにラベルを適用するには、以下の手順を実行します。

手順

ステップ 1 左側のペインで **Security Devices** をクリックします。

ステップ 2 左側のペインで [オブジェクト（Objects）] をクリックします。

ステップ 3 [Devices] タブをクリックしてデバイスを見つけるか、[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 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 1 つ以上のデバイスを選択します。

ステップ 6 右側の [Add Groups and Labels] フィールドで、デバイスのラベルを指定します。

ステップ 7  アイコンをクリックします。

フィルタ

[セキュリティデバイス（Security Devices）] ページと [オブジェクト（Objects）] ページのさまざまなフィルタを使用して、探しているデバイスやオブジェクトを検索できます。

フィルタ処理するには、[セキュリティデバイス（Security Devices）] タブ、[ポリシー（Policies）] タブ、および [オブジェクト（Objects）] タブの左側のペインで  をクリックします。

セキュリティ デバイス フィルタでは、デバイスタイプ、ハードウェアとソフトウェアのバージョン、Snort バージョン、設定ステータス、接続状態、競合検出、Secure Device Connector、およびラベルでフィルタ処理できます。フィルタを適用して、選択したデバイスタイプのタブ内のデバイスを見つけることができます。フィルタを使用して、選択したデバイスタイプのタブ内のデバイスを見つけることができます。

（注） [FTD] タブを開くと、フィルタペインでフィルタを使用できます。これにより、Security Cloud Control からデバイスにアクセスするために使用されている管理アプリケーションに基づいて FDM-managed デバイスが表示されます。

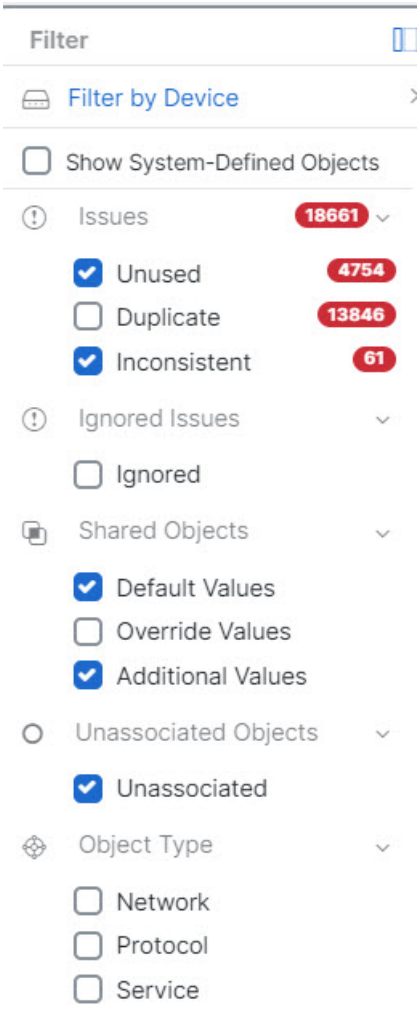
- FDM：FTD API または FDM を使用して管理されるデバイス。
- FMC-FTD：Firepower Management Center を使用して管理されるデバイス。
- FTD：FTD 管理を使用して管理されるデバイス。

オブジェクトフィルタを使用すると、デバイス、問題タイプ、共有オブジェクト、関連付けのないオブジェクト、およびオブジェクトタイプでフィルタ処理できます。結果にシステムオブジェクトを含めるかどうかを選択できます。検索フィールドを使用して、特定の名前、IP アドレス、またはポート番号を含むフィルタ結果内のオブジェクトを検索することもできます。

オブジェクトタイプフィルタを使用すると、ネットワークオブジェクト、ネットワークグループ、URL オブジェクト、URL グループ、サービスオブジェクト、サービスグループなどのタイプによってオブジェクトをフィルタ処理できます。共有オブジェクトフィルタを使用すると、デフォルト値またはオーバーライド値を持つオブジェクトをフィルタ処理できます。

デバイスとオブジェクトをフィルタ処理する場合、検索語を組み合わせて、関連する結果を見つけるためのいくつかの潜在的な検索戦略を作成することができます。

次の例では、「問題（使用されていない、または、不整合）、かつ、共有オブジェクト（デフォルト値、または、追加の値を持つ）かつ、関連付けられていないオブジェクト」を検索するフィルタが適用されます。



Security Cloud Control の検索機能の使用

Security Cloud Control プラットフォームにはきわめて効率的な検索機能があり、必要なものが簡単に見つかります。各ページの検索バーはそのページの内容に合わせてカスタマイズされたものであり、一方グローバル検索では、テナント全体を包括的に検索できます。この検索機能により、必要な情報をすばやく見つけられるため、時間と手間を省けます。

ページレベルの検索

ページレベルの検索では、[セキュリティデバイス（Security Devices）]、[ポリシー（Policies）]、[オブジェクト（Objects）]、[VPN]、[変更ログ（Change Log）]、および[ジョブ（Jobs）]ページで特定の項目を検索できます。

- [セキュリティデバイス（Security Devices）]スペースでは、検索バーに入力を開始するだけで、検索条件に一致するデバイスが表示されます。デバイスの名前の一部、IP アドレ

ス、または物理デバイスのシリアル番号を入力して、デバイスを見つけることができます。

- [ポリシー（Policies）]スペースでは、名前、コンポーネント、または使用されているオブジェクトでポリシーを検索できます。
- [オブジェクト（Objects）] スペースでは、オブジェクト名の一部、または IP アドレス、ポート、プロトコルの一部を入力してオブジェクトを検索できます。
- [VPN] スペースでは、VPN ポリシーで使用されるトンネル名、デバイス名、および IP アドレスで検索できます。
- [変更ログ（Change log）] スペースでは、イベント、デバイス名、またはアクションに基づいてログを検索できます。

手順

ステップ 1 インターフェイスの上部近くにある検索バーに移動します。

ステップ 2 検索バーに検索条件を入力すると、対応する結果が表示されます。

グローバル検索

グローバル検索機能を使用すると、Security Cloud Control の管理対象のデバイスをすばやく見つけてナビゲートできます。

すべての検索結果は、選択したインデックス作成オプションに基づいています。インデックス作成オプションは次のとおりです。

- フルインデックス作成：フルインデックス作成プロセスを呼び出す必要があります。このプロセスは、システム内のすべてのデバイスとオブジェクトをスキャンし、インデックス作成を呼び出した後にのみ、それらを検索インデックスに表示します。フルインデックス作成を呼び出すには、管理者権限が必要です。

  詳細については、「フルインデックス作成の開始」を参照してください。

- 増分インデックス作成：イベントベースのインデックス作成プロセスで、デバイスまたはオブジェクトが追加、変更、または削除されるたびに検索インデックスが自動的に更新されます。

検索フィールドに入力する情報では、大文字と小文字が区別されません。次のエンティティを使用して、グローバル検索を実行できます。

- [デバイス名（Device Name）]：部分的なデバイス名、URL、IP アドレス、または範囲をサポートします。

- [オブジェクトタイプ（Object Types）]：オブジェクト名、オブジェクトの説明、および構成された値をサポートします。
- [ポリシータイプ（Policy Types）]：ポリシー名、ポリシーの説明、ルール名、およびルールコメントをサポートします。

  Security Cloud Control で管理されるクラウド提供型 Firewall Management Center とオンプレミス FMC は、次のポリシータイプをサポートします。

  - アクセス コントロール ポリシー（Access Control Policy）
  - プレフィルタポリシー（Prefilter Policy）
  - Threat Defense NAT ポリシー

検索式を入力すると、インターフェイスに検索結果の表示が開始され、検索を実行するために Enter キーを押す必要はありません。

検索結果には、検索文字列に一致するすべてのデバイスとオブジェクトが表示されます。検索文字列がデバイスやオブジェクト以外と一致する場合、結果はカテゴリ（Devices、Objects、および connected_fmc）の下に表示されます。

デフォルトでは、検索結果の最初の項目が強調表示され、その項目の関連情報が右側のペインに表示されます。検索結果をスクロールして項目をクリックすると、対応する情報を表示できます。項目の横にある矢印アイコンをクリックして、対応するページに移動できます。

（注）
- グローバル検索では、重複する検索結果は表示されません。オブジェクトの場合、共有オブジェクトの UID は、オブジェクトビューに移動するために使用されます。
- Security Cloud Control からデバイスを削除すると、関連するすべてのオブジェクトがグローバル検索インデックスから削除されます。
- ポリシーからオブジェクトを削除し、デバイスを保持した状態でフルインデックス作成を開始すると、削除したオブジェクトはデバイスに関連付けられているため、グローバル検索インデックスに残ります。

フルインデックス作成の開始

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Administration** > **General Settings** をクリックします。

ステップ 3 グローバル検索で、[フルインデックス作成の開始（Initiate Full Indexing）] をクリックしてインデックス作成をトリガーします。

（注）
フルインデックスの作成を開始すると、Security Cloud Control テナントの既存のインデックスがクリアされます。

ステップ 4 ここをクリックして、グローバル検索ワークフローを表示します。

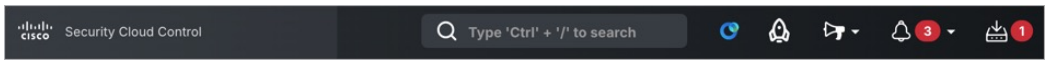
グローバル検索の実行

手順

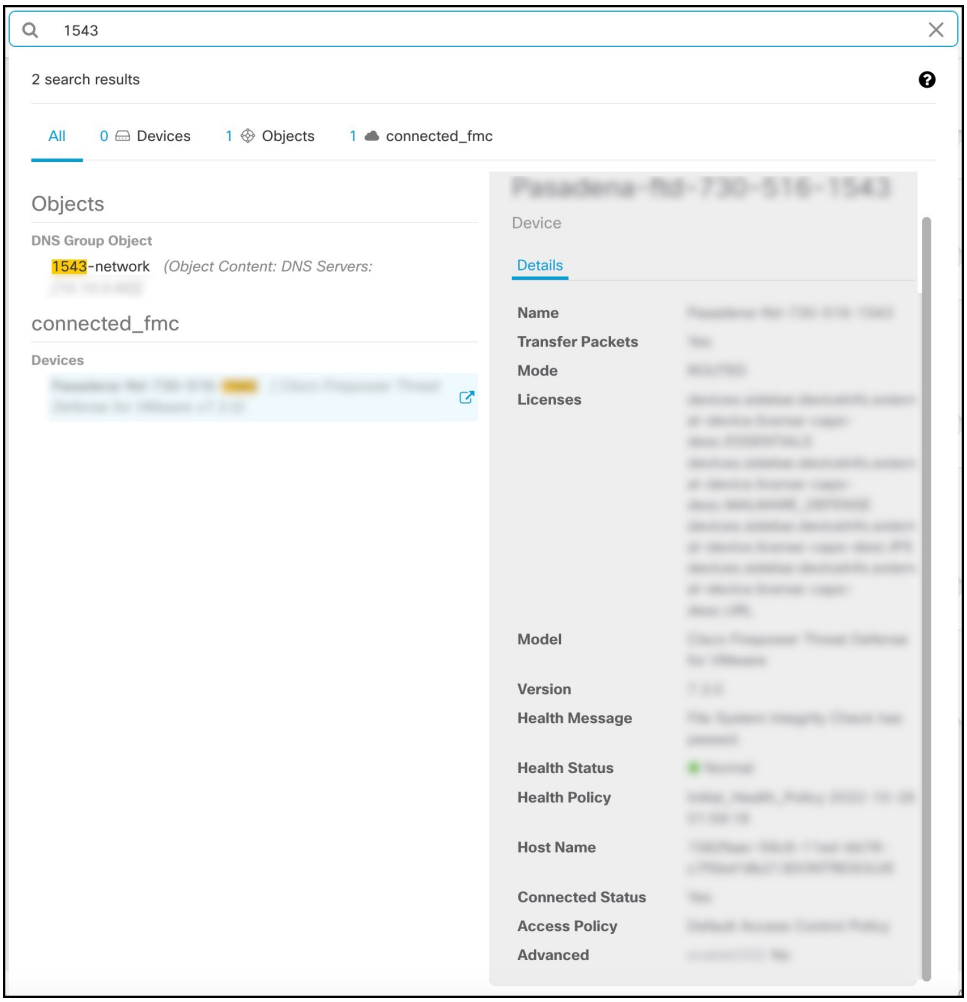
ステップ 1 Security Cloud Control にログインします。

ステップ 2 Security Cloud Control ページにある検索アイコンをクリックし、表示される [Search] フィールドに検索文字列を入力します。

または、Windows の場合は **Ctrl** キーを押しながら / キーを押す、Mac の場合は **Command** キーを押しながら / キーを押して検索バーを開くこともできます。



検索文字列の入力を開始すると、可能性のある項目のリストが表示されます。検索結果は、[すべて（All）]、[デバイス（Devices）]、[オブジェクト（Objects）]、[ポリシー（Policies）]、および Cloud-Delivered Firewall Management Center の 4 つのカテゴリの下に表示されます。右ペインには、選択した検索結果の情報が表示されます。



ステップ 3 検索結果からデバイスまたはオブジェクトを選択し、矢印アイコンをクリックして、検索結果から対象のデバイスおよびオブジェクトのページに移動します。検索結果からオブジェクトを選択し、矢印アイコンをクリックして、検索結果から対象のページに移動します。

（注）
Cloud-Delivered Firewall Management Center でデバイスの検索結果を選択すると、Security Cloud Control 内の Cloud-Delivered Firewall Management Center ユーザーインターフェイスに移動できます。

ステップ 4 [X] をクリックして検索バーを閉じます。

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。