オブジェクト

オブジェクトは、1つ以上のセキュリティポリシーで使用できる情報のコンテナです。オブジェクトを使用すると、ポリシーの一貫性を簡単に維持できます。単一のオブジェクトを作成し、異なるポリシーを使用して、オブジェクトを変更すると、その変更がオブジェクトを使用するすべてのポリシーに伝播されます。オブジェクトを使用しない場合は、同じ変更が必要なすべてのポリシーを個別に変更する必要があります。

デバイスをオンボードすると、CDO はそのデバイスで使用されるすべてのオブジェクトを認識して保存し、[オブジェクト（Objects）] ページにリストします。[オブジェクト（Objects）] ページから、既存のオブジェクトを編集したり、セキュリティポリシーで使用する新しいオブジェクトを作成したりできます。

CDO は、複数のデバイスで使用されるオブジェクトを**共有オブジェクト**と呼び、[オブジェクト（Objects）] ページでこのバッジ でそれらを識別します。

共有オブジェクトが何らかの「問題」を引き起こし、複数のポリシーまたはデバイス間で完全に共有されなくなる場合があります。

- **重複オブジェクト**とは、同じデバイス上にある、名前は異なるが値は同じである2つ以上のオブジェクトです。通常、重複したオブジェクトは同じ目的を果たし、さまざまなポリシーによって使用されます。重複するオブジェクトは、この問題のアイコン で識別されます。
- **不整合オブジェクト**とは、2 つ以上のデバイス上にある、名前は同じだが値は異なるオブジェクトです。ユーザーは、さまざまな設定の中で、同じ名前と内容のオブジェクトを作成することがあります。これらのオブジェクトの値が時間の経過につれて相互に異なる値になり、不整合が生じます。不整合オブジェクトは、この問題のアイコン で識別されます。
- **未使用オブジェクト**は、デバイス構成に存在するものの、別のオブジェクト、アクセスリスト、NAT ルールによって参照されていないオブジェクトです。未使用オブジェクトは、この問題のアイコン で識別されます。

ルールやポリシーですぐに使用するためのオブジェクトを作成することもできます。ルールやポリシーに関連付けないオブジェクトを作成できます。関連付けられていないオブジェクトを

ルールまたはポリシーで使用すると、CDO ではそのコピーが作成され、そのコピーが使用されます。

[オブジェクト（Objects）]メニューに移動するか、ネットワークポリシーの詳細でオブジェクトを表示することにより、CDO によって管理されているオブジェクトを表示できます。

CDO を使用すると、サポートされているデバイス全体のネットワークオブジェクトとサービスオブジェクトを 1 つの場所から管理できます。CDO を使用すると、次の方法でオブジェクトを管理できます。

- さまざまな基準に基づいて、すべてのオブジェクトを検索してフィルタリングします。
- デバイス上の重複、未使用、および不整合のオブジェクトを見つけて、それらのオブジェクトの問題を統合、削除、または解決します。
- 関連付けられていないオブジェクトを見つけて、それらが未使用であれば削除します。
- デバイス間で共通の共有オブジェクトを検出します。
- 変更をコミットする前に、オブジェクトへの変更が一連のポリシーとデバイスに与える影響を評価します。
- 一連のオブジェクトとそれらの関係を、さまざまなポリシーやデバイスで比較します。
- デバイスが CDO にオンボードされた後、デバイスによって使用されているオブジェクトをキャプチャします。

オンボードされたデバイスからのオブジェクトの作成、編集、または読み取りで問題が発生した場合は、Cisco Defense Orchestrator のトラブルシューティングを参照してください。

• デバイス変更のポーリングのスケジュール （40 ページ）

オブジェクト

オブジェクトは、1つ以上のセキュリティポリシーで使用できる情報のコンテナです。オブジェクトを使用すると、ポリシーの一貫性を簡単に維持できます。単一のオブジェクトを作成し、異なるポリシーを使用して、オブジェクトを変更すると、その変更がオブジェクトを使用するすべてのポリシーに伝播されます。オブジェクトを使用しない場合は、同じ変更が必要なすべてのポリシーを個別に変更する必要があります。

デバイスをオンボードすると、CDO はそのデバイスで使用されるすべてのオブジェクトを認識して保存し、[オブジェクト（Objects）] ページにリストします。[オブジェクト（Objects）] ページから、既存のオブジェクトを編集したり、セキュリティポリシーで使用する新しいオブジェクトを作成したりできます。

CDO は、複数のデバイスで使用されるオブジェクトを**共有オブジェクト**と呼び、[オブジェクト（Objects）] ページでこのバッジ でそれらを識別します。

共有オブジェクトが何らかの「問題」を引き起こし、複数のポリシーまたはデバイス間で完全に共有されなくなる場合があります。

- **重複オブジェクト**とは、同じデバイス上にある、名前は異なるが値は同じである2つ以上のオブジェクトです。通常、重複したオブジェクトは同じ目的を果たし、さまざまなポリシーによって使用されます。重複するオブジェクトは、この問題のアイコン で識別されます。
- **不整合オブジェクト**とは、2 つ以上のデバイス上にある、名前は同じだが値は異なるオブジェクトです。ユーザーは、さまざまな設定の中で、同じ名前と内容のオブジェクトを作成することがあります。これらのオブジェクトの値が時間の経過につれて相互に異なる値になり、不整合が生じます。不整合オブジェクトは、この問題のアイコン で識別されます。
- **未使用オブジェクト**は、デバイス構成に存在するものの、別のオブジェクト、アクセスリスト、NAT ルールによって参照されていないオブジェクトです。未使用オブジェクトは、この問題のアイコン で識別されます。

ルールやポリシーですぐに使用するためのオブジェクトを作成することもできます。ルールやポリシーに関連付けないオブジェクトを作成できます。関連付けられていないオブジェクトをルールまたはポリシーで使用すると、CDO ではそのコピーが作成され、そのコピーが使用されます。

[オブジェクト（Objects）] メニューに移動するか、ネットワークポリシーの詳細でオブジェクトを表示することにより、CDO によって管理されているオブジェクトを表示できます。

CDO を使用すると、サポートされているデバイス全体のネットワークオブジェクトとサービスオブジェクトを 1 つの場所から管理できます。CDO を使用すると、次の方法でオブジェクトを管理できます。

- さまざまな基準に基づいて、すべてのオブジェクトを検索してフィルタリングします。

- デバイス上の重複、未使用、および不整合のオブジェクトを見つけて、それらのオブジェクトの問題を統合、削除、または解決します。
- 関連付けられていないオブジェクトを見つけて、それらが未使用であれば削除します。
- デバイス間で共通の共有オブジェクトを検出します。
- 変更をコミットする前に、オブジェクトへの変更が一連のポリシーとデバイスに与える影響を評価します。
- 一連のオブジェクトとそれらの関係を、さまざまなポリシーやデバイスで比較します。
- デバイスが CDO にオンボードされた後、デバイスによって使用されているオブジェクトをキャプチャします。

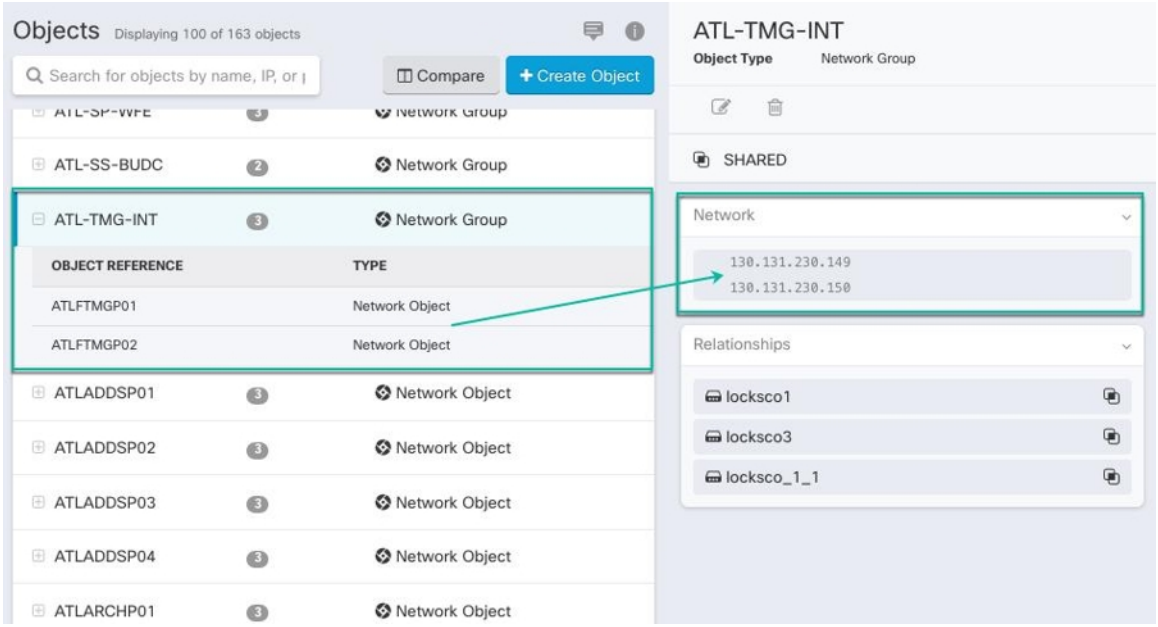
オンボードされたデバイスからのオブジェクトの作成、編集、または読み取りで問題が発生した場合は、Cisco Defense Orchestrator のトラブルシューティングを参照してください。

共有オブジェクト

Cisco Defense Orchestrator（CDO）では、複数のデバイス上の同じ名前と同じ内容のオブジェクトを共有オブジェクトと呼びます。共有オブジェクトはこのアイコンで識別されます。

これは、[オブジェクト（Objects）]ページに表示されます。共有オブジェクトを使用すると、1 か所でオブジェクトを変更でき、その変更がそのオブジェクトを使用する他のすべてのポリシーに影響するため、ポリシーの維持が容易になります。共有オブジェクトを使用しない場合は、同じ変更が必要なすべてのポリシーを個別に変更する必要があります。

共有オブジェクトを調査する場合、CDO ではオブジェクトの内容がオブジェクトテーブルに表示されます。共有オブジェクトの内容はまったく同じです。CDO では、オブジェクトの要素の結合された、つまり「フラット化された」ビューが詳細ペインに表示されます。詳細ペインでは、ネットワーク要素が単純なリストにフラット化されており、名前付きオブジェクトに直接関連付けられていないことに注意してください。

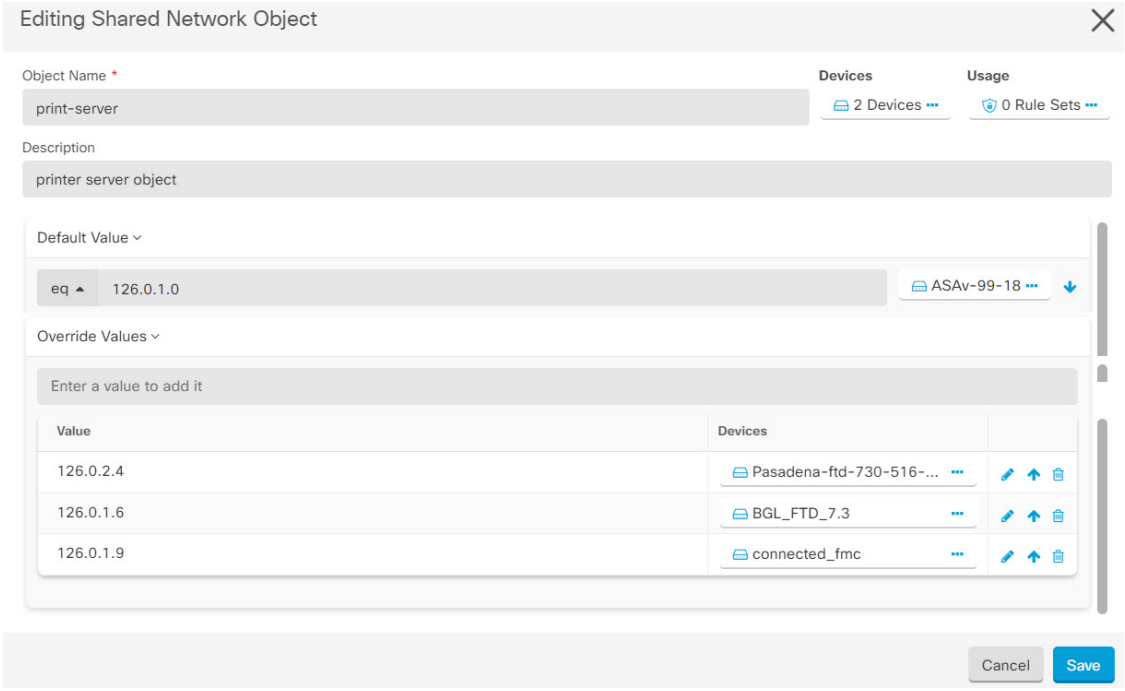


オブジェクトのオーバーライド

オブジェクトのオーバーライドを使用すると、特定のデバイス上の共有ネットワークオブジェクトの値をオーバーライドできます。CDO は、オーバーライドを構成するときに指定したデバイスに対応する値を使用します。これらのオブジェクトは、名前は同じで値が異なる複数のデバイス上にありますが、CDO は、これらの値がオーバーライドとして追加されただけでは、それらを**不整合オブジェクト**として識別しません。

ほとんどのデバイスに有効な定義を設定したオブジェクトを作成した後、異なる定義を必要とする少数のデバイスについて、オーバーライドを使用してオブジェクトに対する変更内容を指定できます。また、すべてのデバイスに対してオーバーライドする必要があるオブジェクトを作成し、そのオブジェクトを使用してすべてのデバイスに適用する単一のポリシーを作成することもできます。オブジェクト オーバーライドでは、デバイス全体で使用する共有ポリシーの小さなセットを作成し、個々のデバイスの必要に応じてポリシーを変更できます。

たとえば、各オフィスにプリンタサーバーがあり、プリンタ サーバー オブジェクト `print-server` を作成しているシナリオを考えてみましょう。ACL には、プリンタサーバーのインターネットへのアクセスを拒否するルールを設定しています。プリンタ サーバー オブジェクトには、オフィスごとに変更できるデフォルト値があります。これを行うには、オブジェクトのオーバーライドを使用し、すべての場所でルールと「printer-server」オブジェクトの一貫性を維持します（値は異なる場合があります）。



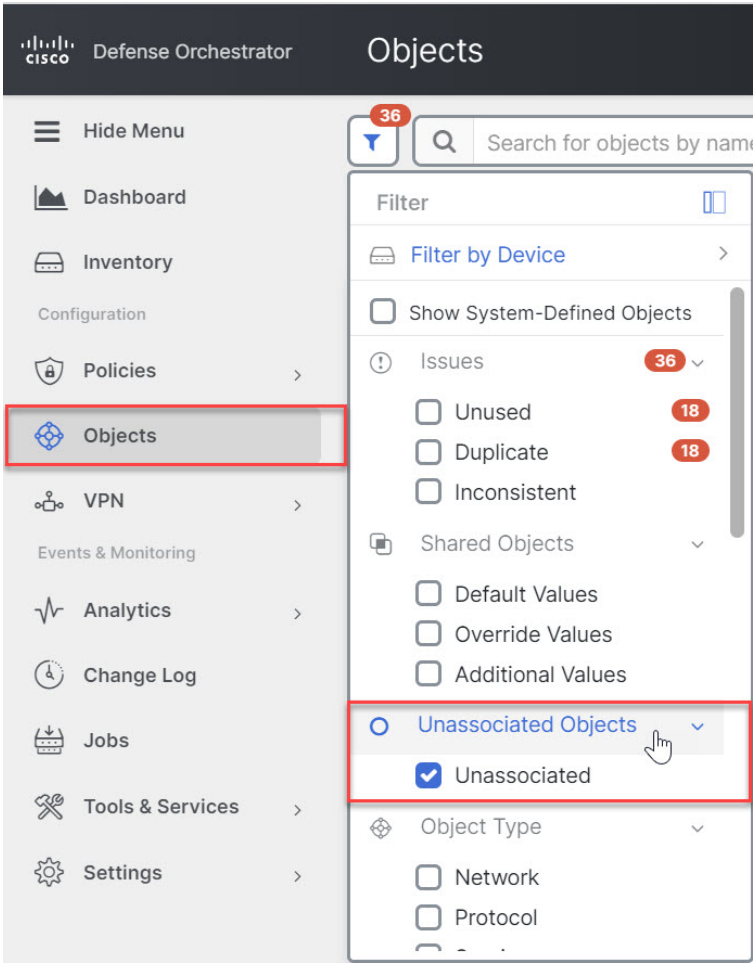
（注） 一貫性のないオブジェクトがある場合は、オーバーライドを使用してそれらを1つの共有オブジェクトに結合できます。詳細については、不整合オブジェクトの問題を解決するを参照してください。

関連付けのないオブジェクト

ルールやポリシーですぐに使用するためのオブジェクトを作成できますが、ルールやポリシーに関連付けないオブジェクトを作成することもできます。関連付けられていないオブジェクトをルールまたはポリシーで使用すると、CDO ではそのコピーが作成され、そのコピーが使用されます。関連付けられていない元のオブジェクトは、夜間のメンテナンスジョブで削除されるか、ユーザーが削除するまで、使用可能な一連のオブジェクト内に残ります。

関連付けられていないオブジェクトはコピーとして CDO に残り、オブジェクトに関連付けられたルールまたはポリシーが誤って削除された場合にすべての設定が失われないようにします。

関連付けられていないオブジェクトを表示するには、[オブジェクト（Objects）] タブの左側のペインにある をクリックし、[関連付けなし（Unassociated）] チェックボックスをオンにします。



オブジェクトの比較

ステップ 1 左側の CDO ナビゲーションバーで、[オブジェクト（Objects）] をクリックして、オプションを選択します。

ステップ 2 ページのオブジェクトをフィルタ処理して、比較するオブジェクトを見つけます。

ステップ 3 [比較（Compare）] Compare ボタンをクリックします。

ステップ 4 比較するオブジェクトを最大 3 つまで選択します。

ステップ 5 画面の下部にオブジェクトを並べて表示します。

- [オブジェクトの詳細（Object Details）] タイトルバーの上下の矢印をクリックして、表示するオブジェクト詳細を調整します。
- [詳細（Details）] ボックスと [関係（Relationships）] ボックスを展開するか折りたたんで、表示する情報を調整します。

ステップ6 （オプション）[関係（Relationships）]ボックスには、オブジェクトの使用方法が表示されます。オブジェクトはデバイスまたはポリシーに関連付けられている場合があります。オブジェクトがデバイスに関連付けられている場合は、デバイス名をクリックしてから [構成の表示（View Configuration）] をクリックして、デバイスの構成を表示できます。CDOはデバイスの構成ファイルを表示し、そのオブジェクトのエントリをハイライトします。

フィルタ

[インベントリ（Inventory）]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およびオブジェクトを見つけることができます。

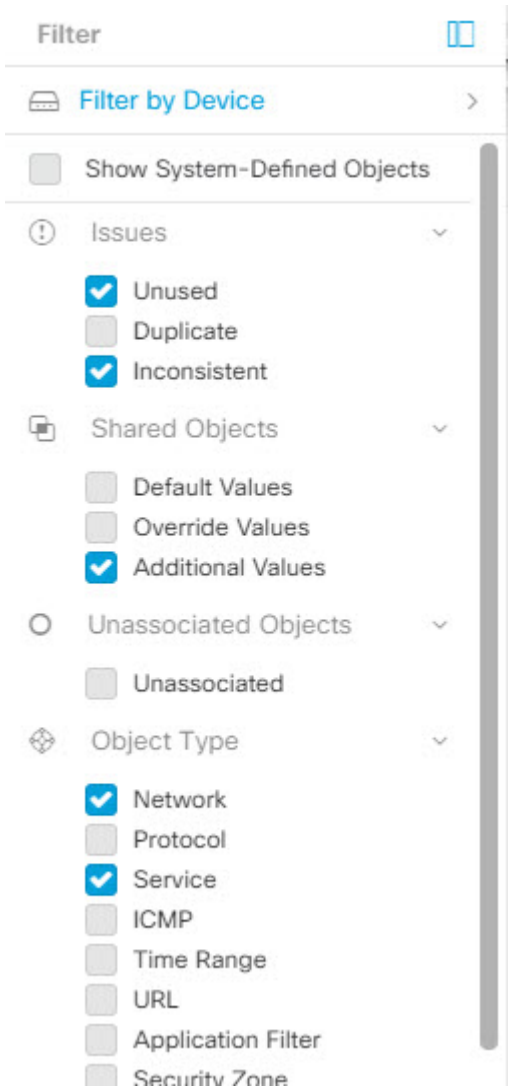
フィルタ処理するには、[デバイスとサービス（Devices and Services）] タブ、[ポリシー（Policies）] タブ、および [オブジェクト（Object）] タブの左側のペインで をクリックします。

インベントリフィルタでは、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。

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。

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（使用されている、または、不整合）があるオブジェクト、かつ、追加の値を持つ共有オブジェクト、かつ、特定のタイプ（ネットワーク、または、サービス）のオブジェクト」であるようなオブジェクトを検索するフィルタが適用されます。



オブジェクトフィルタ

フィルタ処理するには、[オブジェクト（Object）] タブの左側のペインで をクリックします。

- [すべてのオブジェクト（All Objects）] – このフィルタは、CDO にオンボーディングしたすべてのデバイスから使用可能なすべてのオブジェクトを提供します。このフィルタは、すべてのオブジェクトを参照するために、または検索の開始点としてや、さらにサブフィルタ適用するために役立ちます。
- [共有オブジェクト（Shared Objects）] – このクイックフィルタは、複数のデバイスで共有されていることが CDO によって検出されたすべてのオブジェクトを表示します。
- [デバイスごとのオブジェクト（Objects By Device）]–特定のデバイスを選択して、選択したデバイスで見つかったオブジェクトを表示できます。

サブフィルタ–各メインフィルタ内には、選択をさらに絞り込むために適用できるサブフィルタがあります。これらのサブフィルタは、オブジェクトタイプ（ネットワーク、サービス、プロトコルなど）に基づいています。

このフィルタバーで選択されたフィルタは、以下の条件に一致するオブジェクトを返します。

*****2つのデバイスのいずれかにあるオブジェクト（[デバイスでフィルタ処理（Filter by Device）]をクリックしてデバイスを指定します）。および

*** 一貫性のない**オブジェクト。および

*** ネットワーク**オブジェクトまたは**サービス**オブジェクト。 および

***** オブジェクトの命名規則に「**グループ**」という単語が含まれているオブジェクト。

[システムオブジェクトの表示（Show System Objects）] がオンになっているため、結果にはシステムオブジェクトとユーザー定義オブジェクトの両方が含まれます。

システムオブジェクトの表示フィルタ

一部のデバイスには、一般的なサービス用に事前定義されたオブジェクトがあります。これらのシステム オブジェクトは既に作成されており、ルールやポリシーで使用できるので便利です。オブジェクトテーブルには多くのシステムオブジェクトが含まれる場合があります。システムオブジェクトは編集または削除できません。

[システムオブジェクトを表示（Show System Objects）] はデフォルトで「**オフ**」です。オブジェクトテーブルにシステムオブジェクトを表示するには、フィルタバーで [システムオブジェクトを表示（Show System Objects）] をオンにします。オブジェクトテーブルでシステムオブジェクトを非表示にするには、フィルタバーで[システムオブジェクトを表示（Show System Objects）] をオフのままにします。

システムオブジェクトを非表示にすると、それらは検索およびフィルタ処理の結果に含まれなくなります。システムオブジェクトを表示すると、それらはオブジェクトの検索とフィルタ処理の結果に含まれます。

オブジェクトフィルタを設定する

条件を必要な数だけ設定してフィルタリングできます。フィルタリングするカテゴリが多いほど、予想される結果は少なくなります。

ステップ 1 左側のCDOナビゲーションバーで、[オブジェクト（Objects）] をクリックして、オプションを選択します。

ステップ 2 ページ上部のフィルタアイコン をクリックして、フィルタパネルを開きます。オブジェクトが誤って除外されないように、チェック付きのフィルタのチェックを外します。さらに、検索フィールドを見て、検索フィールドに入力された可能性のあるテキストを削除します。

ステップ 3 結果を特定のデバイスで見つかったものに限定したい場合：

1. **[デバイスでフィルタ処理（Filter By Device）]** をクリックします。

2. すべてのデバイスを検索するか、デバイスタブをクリックして特定の種類のデバイスのみを検索します。
3. フィルタ条件に含めるデバイスのチェックボックスをオンにします。
4. [OK] をクリックします。

ステップ 4 検索結果にシステムオブジェクトを含めるには、[システムオブジェクトを表示（Show System Objects）] をオンにします。検索結果でシステムオブジェクトを除外するには、[システムオブジェクトを表示（Show System Objects）] をオフにします。

ステップ 5 [問題（Issues）] で、フィルタリングするオブジェクトの問題のチェックボックスをオンにします。複数の問題をオンにすると、オンにしたいずれかのカテゴリのオブジェクトがフィルタ結果に含まれます。

ステップ 6 問題があったが管理者によって無視されたオブジェクトを表示する場合は、[無視（Ignored）] の問題をチェックします。

ステップ 7 2つ以上のデバイス間で共有されるオブジェクトをフィルタリングする場合は、[共有オブジェクト（Shared Objects）] で必要なフィルタをオンにします。

- [デフォルト値（Default Values）]：デフォルト値のみを持つオブジェクトをフィルタリングします。
- [オーバーライド値（Override Values）]：オーバーライドされた値を持つオブジェクトをフィルタリングします。
- [追加の値（Additional Values）]：追加の値を持つオブジェクトをフィルタリングします。

ステップ 8 ルールまたはポリシーの一部ではないオブジェクトをフィルタリングする場合は、[関連付けなし（Unassociated）] をオンにします。

ステップ 9 フィルタリングする [オブジェクトタイプ（Object Types）] をオンにします。

ステップ 10 オブジェクト名、IP アドレス、またはポート番号を [オブジェクト（Objects）] 検索フィールドに追加して、フィルタリングされた結果の中から検索条件に一致するオブジェクトを見つけることもできます。

フィルタ基準からデバイスを除外する場合

デバイスをフィルタリング基準に追加すると、結果にはデバイス上のオブジェクトは表示されますが、それらのオブジェクトと他のデバイスとの関係は表示されません。たとえば、**ObjectA** が ASA1 と ASA2 の間で共有されている場合、オブジェクトをフィルタリングして ASA1 上の共有オブジェクトを検索すると、**ObjectA** は見つかりますが、[関係（Relationships）] ペインには、オブジェクトが ASA1 にあることだけが表示されます。

オブジェクトが関連するすべてのデバイスを表示するには、検索条件でデバイスを指定しないでください。他の条件でフィルタリングし、必要に応じて検索条件を追加します。CDO が識別するオブジェクトを選択し、[関係（Relationships）] ペインを調べます。そのオブジェクトに関連するすべてのデバイスとポリシーが表示されます。

オブジェクトの無視の解除

未使用、重複、不整合のオブジェクトを解決する方法の1つは、それらを無視することです。オブジェクトが未使用、重複、または不整合であっても、その状態には正当な理由があると判断し、オブジェクトの問題を未解決のままにすることを選択する場合もあります。将来のある時点で、これらの無視されたオブジェクトを解決することが必要になる場合があります。オブジェクトの問題を検索するときにCDOは無視されたオブジェクトを表示しないため、無視されたオブジェクトのオブジェクトリストをフィルタリングし、結果に基づいて操作する必要があります。

ステップ1 左側のCDOナビゲーションバーで、[オブジェクト（Objects）]をクリックして、オプションを選択します。

ステップ2 無視されたオブジェクトをフィルタリングして検索します。

ステップ3 [オブジェクト（Object）]テーブルで、無視を解除するオブジェクトをすべて選択します。一度に1つのオブジェクトの無視を解除できます。

ステップ4 詳細ペインで[無視の解除（Unignore）]をクリックします。

ステップ5 要求を確認します。これで、オブジェクトを問題でフィルタリングすると、以前は無視されていたオブジェクトが見つかるはずです。

オブジェクトの削除

1つのオブジェクトまたは複数のオブジェクトを削除できます。

1つのオブジェクトの削除

⚠

注意 クラウド提供型Firewall Management Centerがテナントにデプロイされている場合：

[]ページのネットワークオブジェクトおよびグループに加えた変更は、**[[オブジェクト（Objects）] > [その他のFTDオブジェクト（Other FTD Objects）]]**ページの対応するクラウド提供型Firewall Management Centerネットワークオブジェクトまたはグループに反映されます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

ステップ1 左側のCDOナビゲーションバーで、[オブジェクト（Objects）]を選択して、オプションを選択します。

ステップ2 オブジェクトフィルタと検索フィールドを使用して、削除するオブジェクトを見つけ、それを選択します。

ステップ3 [関係（Relationships）]ペインを確認します。オブジェクトがポリシーまたはオブジェクトグループで使用されている場合は、そのポリシーまたはグループから削除するまでオブジェクトを削除できません。

ステップ 4 [アクション（Actions）] ペインで、[削除（Remove）] アイコン をクリックします。

ステップ 5 [OK] をクリックしてオブジェクトの削除を確認します。

ステップ 6 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、待機してから複数の変更を一度に展開します。

未使用オブジェクトのグループの削除

デバイスをオンボードしてオブジェクトの問題解決に取り組むと、多くの未使用のオブジェクトが見つかります。一度に最大 50 個の未使用オブジェクトを削除できます。

ステップ 1 [問題（Issues）] フィルタを使用して、**未使用のオブジェクト**を見つけます。デバイスフィルタを使用する際に [デバイスなし（No Device）] を選択し、デバイスに関連付けられていないオブジェクトを検索することもできます。オブジェクトリストをフィルタリングすると、オブジェクトのチェックボックスが表示されます。

ステップ 2 オブジェクト テーブル ヘッダーの [すべて選択（Select all）] チェックボックスをオンにして、フィルタによって検出されオブジェクトテーブルに表示されるすべてのオブジェクトを選択するか、削除する個々のオブジェクトの個々のチェックボックスをオンにします。

ステップ 3 [アクション（Actions）] ペインで、[削除（Remove）] アイコン をクリックします。

ステップ 4 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

ネットワーク オブジェクト

1 つのネットワークオブジェクトには、ホスト名、ネットワーク IP アドレス、IP アドレスの範囲、完全修飾ドメイン名（FQDN）または CIDR 表記のサブネットワークのいずれか 1 つを入れることができます。[ネットワークグループ（Network groups）] は、ネットワークオブジェクトと、グループに追加するその他の個々のアドレスまたはサブネットワークのコレクションです。ネットワークオブジェクトとネットワークグループは、アクセスルール、ネットワークポリシー、および NAT ルールで使用されます。CDO を使用して、ネットワークオブジェクトとネットワークグループを作成、更新、および削除できます。

表 *1*: ネットワークオブジェクトで許可される値

デバイス タイプ（Device Type）	[IPv4 / IPv6]	シングル アドレス	アドレス範囲	完全修飾ドメイン名	CIDR 表記法によるサブネット
Meraki	IPv4	対応	対応	対応	対応

表 *2:* ネットワークグループで許可される内容

デバイス タイプ（**Device Type**）	**IP** 値	[ネットワーク オブジェクト（**Network Object**）]	ネットワーク グループ
Meraki	対応	対応	対応

製品間でのネットワークオブジェクトの再利用

クラウド提供型 Firewall Management Center とテナントにオンボーディングされている 1 つ以上の オンプレミス Management Center を含む Cisco Defense Orchestrator テナントがある場合は、次の手順を実行します。

Cisco Secure Firewall Threat Defense、FDM による管理脅威に対する防御、ASA、または Meraki ネットワークオブジェクトまたはグループを作成すると、そのオブジェクトのコピーが、クラウド提供型 Firewall Management Center の設定時に使用する [オブジェクト（Objects）] > [その他のFTDオブジェクト（Other FTD Objects）] ページのオブジェクトリストにも追加され、その逆も同様です。

いずれかのページのネットワークオブジェクトやグループに加えた変更は、両方のページのオブジェクトまたはグループインスタンスに適用されます。1 つのページからオブジェクトを削除すると、そのオブジェクトの対応するコピーも他のページから削除されます。

例外：

- 同じ名前のネットワークオブジェクトがすでにクラウド提供型 Firewall Management Center に存在する場合、新しい Cisco Secure Firewall Threat Defense、FDM による管理 脅威に対する防御、ASA、または Meraki ネットワークオブジェクトは、Cisco Defense Orchestrator の [オブジェクト（Objects）] > [他のFTDオブジェクト（Other FTD Objects）] ページには複製されません。
- オンプレミスの Cisco Secure Firewall Management Center によって管理される導入準備済み脅威に対する防御 デバイスのネットワークオブジェクトおよびグループは、[オブジェクト（Objects）] > [その他のFTDオブジェクト（Other FTD Objects）] ページでは複製されず、クラウド提供型 Firewall Management Center で使用できません。

  クラウド提供型 Firewall Management Center に移行したオンプレミスの Cisco Secure Firewall Management Center インスタンスの場合、ネットワークオブジェクトとグループは、FTD デバイスに展開されたポリシーで使用されていれば、CDO オブジェクトページに複製されることに注意してください。
- CDO と クラウド提供型 Firewall Management Center の間のネットワークオブジェクトの共有は、新しいテナントでは自動的に有効になりますが、既存のテナントでは要求する必要があります。ネットワークオブジェクトが クラウド提供型 Firewall Management Center と共有されていない場合は、TAC に連絡して、テナントで機能を有効にしてもらいます。

ネットワークオブジェクトの表示

CDO を使用して作成するネットワークオブジェクトと、オンボーディングしたデバイスの設定から CDO が認識するネットワークオブジェクトは、[オブジェクト（Objects）] ページに表示されます。これらのネットワークオブジェクトには、それぞれのオブジェクトタイプのラベルが付けられています。これにより、オブジェクトタイプでフィルタリングして、探しているオブジェクトをすばやく見つけることができます。

[オブジェクト（Objects）]ページでネットワークオブジェクトを選択すると、オブジェクトの値が [詳細（Detail）] ペインに表示されます。[関係（Relationships）] ペインには、オブジェクトがポリシーで使用されているかどうか、およびオブジェクトが保存されているデバイスが表示されます。

ネットワークグループをクリックすると、そのグループの内容が表示されます。ネットワークグループは、ネットワークオブジェクトによってグループに与えられたすべての値の集合体です。

Meraki デバイスに関連付けられるオブジェクト

Meraki デバイスで使用されるオブジェクトについて

Meraki ダッシュボードは、アウトバウンドアクセス制御ルールの送信元および宛先フィールドに指定された IP アドレス、プロトコル、またはポート範囲のグループを利用します。オンボーディングすると、CDO は、IP アドレスをネットワークオブジェクトに変換し、アプリケーションレイヤのプロトコル値をサービスオブジェクトまたはプロトコルオブジェクトに変換します。

CDO の 1 つのルールがダッシュボードで複数のルールに変換される可能性があります。たとえば、TCP プロトコルと UDP プロトコルの両方を含む ASA プロトコルグループを CDO の単一のアクセス制御ルールに追加すると、CDO は 1 つの CDO ルールをダッシュボード内の複数のルールに変換します。変換後のルールは、TCP プロトコルを含む 1 つのルールと UDP プロトコルを含む 1 つのルールになります。

Meraki ダッシュボードと CDO はどちらも CIDR サブネット表記をサポートしていることに注意してください。レイヤ 3 スイッチインターフェイスと MX デバイスレイアウトの詳細については、Meraki ナレッジベースを参照してください。

CDO の Meraki デバイスで使用できるオブジェクト

Cisco Defense Orchestrator（CDO）には、MX デバイス専用のオブジェクトはありません。代わりに、FTD、FDM および ASA オブジェクトを作成または共有し、デバイスに展開されるルールにこれらのオブジェクトを関連付けることができます。Meraki には FTD および ASA オブジェクトとの完全な互換性がないため、MX デバイスがオブジェクトを使用する方法に影響するいくつかの制限がある可能性があります。

FTD、FDM または ASA オブジェクトを MX デバイスに関連付けると、そのオブジェクトが共有されるようになることに注意してください。関連付けられたオブジェクトへの変更は、そのオブジェクトが共有されているすべてのデバイスに影響し、デバイスの設定ステータスには

[非同期（Not Synced）] と表示されます。詳細については、「共有オブジェクト」を参照してください。オブジェクトに影響する付加的なオブジェクト状態については、このページの下部に表示されている「**関連記事**」セクションを参照してください。

Meraki は、IPv6 アドレスまたは FQDN を含むオブジェクトをサポートしていません。

CDO のオブジェクト	Meraki との互換性あり
プロトコルオブジェクト	TCP、UDP、ICMP
ネットワーク オブジェクト	Yes
ネットワーク グループ	Yes
サービス オブジェクト	Yes
ASA サービスグループ	×
FTD サービスグループ	×

Meraki クラウドのローカル ネットワーク オブジェクトおよびオブジェクトグループ

ネットワークオブジェクトとオブジェクトグループを使用すると、Meraki デバイスのファイアウォールルールを簡単に管理できます。これらは、ファイアウォールルールなどのアクセスポリシーで使用できる IP サブネットおよび FQDN のラベルとして機能します。同じ IP サブネットや FQDN を使用する複数のアクセスポリシーを変更する必要がある場合は、ネットワークオブジェクトを変更して、すべてのポリシーに反映させるだけです。現時点では、ネットワークオブジェクトの作成と変更には、Meraki ダッシュボードを使用する必要があります。お使いの環境でネットワークオブジェクトを使って何ができるのかについては、Meraki の『ネットワークオブジェクトのハイライト』[英語] を参照してください。

（注） Meraki ネットワークオブジェクトやネットワーク オブジェクト グループを参照するデバイス設定が CDO UI にオンボードまたは同期されると、これらのオブジェクトは **FTD ネットワークオブジェクト**として表示されます。

これらのオブジェクトおよびオブジェクトグループは、**CDO** では読み取り専用になります。

CDO での Meraki ルールの表示

デバイスのポリシーページからオブジェクトを表示するか、デバイスに基づいてオブジェクトページをフィルタ処理できます。ポリシーページから、アクセス制御ルールの表示、編集、および並べ替えを実行できます。CDO は、Meraki ダッシュボードからのアウトバウンドルールをオブジェクトへのアクセス制御ルールに変換するため、Meraki ダッシュボードからのルールとプロトコルの表示が変更される場合があります。次の表は、CDO へのデバイスのオンボーディングを完了した後のプロトコルの新しい名前を示しています。

Meraki ダッシュボードでのルールまたはプロトコルのヘッダー	**CDO** でのルールまたはオブジェクトのヘッダー
ポリシー	操作
[ソースIP（Source IP）]	ネットワークオブジェクトまたはネットワークグループ
[宛先 IP アドレス（Destination IP）]	ネットワークオブジェクトまたはネットワークグループ
送信元ポート（Source Port）	ネットワークオブジェクトまたはネットワークグループ
[宛先ポート（Destination Port）]	ネットワークオブジェクトまたはネットワークグループ
レイヤ 3 アプリケーションプロトコル	ポート（プロトコルグループ、ポートグループ、またはサービスオブジェクト）

次の例は、Meraki ダッシュボードからのアウトバウンドルールがCDO でどのように表示されるかを示しています。

Meraki ローカル ネットワーク オブジェクトの作成

ローカルの Meraki ネットワークオブジェクトは、Cisco Merkai ダッシュボードで作成する必要があります。CDO にまだ導入準備されていない Meraki デバイスがある場合、既存のローカルオブジェクトはすべてデバイスに導入準備されます。**導入準備された** Meraki デバイスがある場合は、CDO でデバイスを同期して、新しい構成とローカルオブジェクトを読み取ります。

（注） Meraki ネットワークオブジェクトやネットワーク オブジェクト グループを参照するデバイス構成が CDO UI で導入準備または同期されると、これらのオブジェクトは **FTD ネットワーク** オブジェクトまたはオブジェクトグループとして表示されます。

これらのオブジェクトおよびオブジェクトグループは、**CDO** では読み取り専用になります。

始める前に

Merkai の**オープン ベータ ネットワーク オブジェクト**を有効にしていない場合は、Cisco Meraki ダッシュボードにログインし、**[組織]** > **[ポリシーオブジェクト]** に移動して、ローカルオブジェクトとオブジェクトグループに登録してアクセスします。

ステップ 1 Meraki ダッシュボードにログインし、ローカルオブジェクトまたはローカルオブジェクトグループを作成します。詳細については、『Network Objects Configuration Guide』を参照してください。

ステップ 2 CDO にログインします。

注：Meraki デバイスを CDO にまだ導入準備していない場合は、詳細について「CDO への MX デバイスのオンボード」を参照してください。デバイスを導入準備すると、既存のすべてのオブジェクトも導入準備されます。

ステップ 3 ナビゲーションウィンドウで、[インベントリ（Inventory）] をクリックします。

ステップ 4 Merkai デバイスを見つけて選択し、デバイスの行が強調表示されるようにします。デバイスのステータスは [競合が検出されました] になっています。右側のペインで、[競合の確認] を選択してデバイスの構成に追加された変更を確認するか、[確認せずに承認] を選択してすべての構成変更を承認します。

Merakiネットワークオブジェクトまたはネットワークグループの作成または編集

MX デバイスは Firepower および ASA **ネットワークオブジェクト**と同じ形式を使用し、CIDR 表記で表されたホスト名、IP アドレス、またはサブネットアドレスを含めることができます。**ネットワークグループ**は、ネットワークオブジェクトと、グループに追加するその他の個々のアドレスまたはサブネットのコレクションです。ネットワークオブジェクトとネットワークグループは、アクセスルールで使用されます。CDO を使用して、ネットワークオブジェクトとネットワークグループを作成、読み取り、更新、および削除できます。

ネットワークオブジェクトに追加できる IP アドレス

デバイス タイプ（Device Type）	[IPv4 / IPv6]	シングル アドレス	アドレス範囲	完全修飾ドメイン名	CIDR 表記法によるサブネット
MX	IPv4	対応	対応	×	対応

（注） クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

ネットワークオブジェクトまたはグループを [] ページに作成すると、オブジェクトのコピーが **[[オブジェクト（Objects）] > [その他の FTD オブジェクト（Other FTD Objects）]]** ページに自動的に追加されます。また、この逆も同様です。

注意 クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

[] ページのネットワークオブジェクトおよびグループに加えた変更は、**[[オブジェクト（Objects）] > [その他の FTD オブジェクト（Other FTD Objects）]]** ページの対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトまたはグループに反映されます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

Meraki ネットワークオブジェクトの作成

（注） クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

ネットワークオブジェクトまたはグループを []ページに作成すると、オブジェクトのコピーが **[[オブジェクト（Objects）] > [その他の FTD オブジェクト（Other FTD Objects）]]** ページに自動的に追加されます。また、この逆も同様です。

ステップ 1 左側の CDO ナビゲーションバーで、**[オブジェクト（Objects）] > [Meraki オブジェクト（Meraki Objects）]** をクリックします。

ステップ 2 をクリックしてから、**[FTD] > [ネットワーク（Network）]**または**[ASA] > [ネットワーク（Network）]** をクリックします。

ステップ 3 オブジェクト名を入力します。

ステップ 4 [ネットワークオブジェクトの作成（Create a network object）] を選択します。

ステップ 5 [値（Value）] セクションで、単一の IP アドレスまたは CIDR 表記で表されるサブネットアドレスを入力します。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

Meraki ネットワークグループの作成

ネットワークグループは、複数のネットワークオブジェクトまたは IP アドレスで構成されます。

ネットワークグループをネットワークオブジェクトで構成する場合は、上記の「ネットワークオブジェクトの作成」の手順を使用して、IP アドレスごとに個別のネットワークオブジェクトを作成します。

（注） クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

ネットワークオブジェクトまたはグループを [] ページに作成すると、オブジェクトのコピーが **[[オブジェクト（Objects）] > [その他の FTD オブジェクト（Other FTD Objects）]]** ページに自動的に追加されます。また、この逆も同様です。

ステップ 1 左側の CDO ナビゲーションバーで、**[オブジェクト（Objects）] > [Meraki オブジェクト（Meraki Objects）]** をクリックします。

ステップ 2 をクリックしてから、**[FTD] > [ネットワーク（Network）]** または **[ASA] > [ネットワーク（Network）]** のいずれかをクリックします。

ステップ 3 オブジェクト名を入力します。

ステップ 4 [ネットワークグループの作成（Create a network group）] を選択します。

ステップ 5 [オブジェクトの追加（Add Object）] をクリックし、リストからネットワークオブジェクトを選択して、[選択（Select）] をクリックします。必要なすべてのネットワークオブジェクトを追加するまで、この操作を繰り返します。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

Firepower ネットワークオブジェクトまたはネットワークグループの編集

注意 クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

[] ページのネットワークオブジェクトおよびグループに加えた変更は、**[[オブジェクト（Objects）] > [その他の FTD オブジェクト（Other FTD Objects）]]** ページの対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトまたはグループに反映されます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

ステップ 1 左側の CDO ナビゲーションバーで、**[オブジェクト（Objects）] > [Meraki オブジェクト（Meraki Objects）]** をクリックします。

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、編集するオブジェクトを見つけます。

ステップ 3 編集するオブジェクトを選択します。

ステップ 4 [詳細（details）] ペインの [編集（edit）] ボタン をクリックします。

ステップ 5 前述の手順で作成したのと同じ方法で、ダイアログボックスの値を編集します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 CDO は、変更の影響を受けるポリシーを表示します。[確認（Confirm）] をクリックして、オブジェクトとその影響を受けるポリシーへの変更を確定します。

ステップ 8 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

関連情報

- Meraki デバイスに関連付けられるオブジェクト
- Meraki サービスオブジェクトの作成または編集
- 未使用オブジェクトの問題の解決
- 重複オブジェクトの問題の解決
- ログの変更

ネットワークオブジェクトとグループの削除

クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

のページからネットワークオブジェクトまたはグループを削除すると、**[オブジェクト（Objects）] > [その他の FTD オブジェクト（Other FTD Objects）]** ページから重複するネットワークオブジェクトまたはグループが削除されます。その逆も同様です。

サービス オブジェクト

プロトコルオブジェクト

プロトコルオブジェクトは、使用頻度の低いプロトコルやレガシープロトコルを含むサービスオブジェクトの一種です。プロトコルオブジェクトは、名前とプロトコル番号で識別されます。CDO は、ASA および Firepower（FDM による管理 デバイス）設定でこれらのオブジェクトを認識し、これらに独自のフィルタ「プロトコル」を適用します。そのため、これらのオブジェクトを簡単に見つけることができます。

ICMP オブジェクト

Internet Control Message Protocol （ICMP）オブジェクトは、ICMP および IPv6-ICMP メッセージ専用のサービスオブジェクトです。CDO は、ASA および Firepower（FTD）がオンボードされたときにデバイスの設定でこれらのオブジェクトを認識し、これらに独自のフィルタ「ICMP」を適用します。そのため、これらのオブジェクトを簡単に見つけることができます。

CDO を使用して、ASA 設定から ICMP オブジェクトの名前を変更したり、ICMP オブジェクトを削除したりできます。CDO を使用して、Firepower 設定の ICMP および ICMPv6 オブジェクトを作成、更新、および削除できます。

（注） ICMPv6 プロトコルの場合、AWS は特定の引数の選択をサポートしていません。すべての ICMPv6 メッセージを許可するルールのみがサポートされます。

関連情報：

- オブジェクトの削除

Meraki サービスオブジェクトの作成または編集

サービスオブジェクトの概要

サービスオブジェクトは、TCP/IP プロトコルとポートを指定する再利用可能なコンポーネントです。CDO は、これらのオブジェクトをサービスオブジェクトとして分類します。MX デバイスに展開すると、CDO はオブジェクトをプロトコルまたはポート範囲に変換します。CDO が Meraki プロトコルをオブジェクトとして処理する方法の詳細については、 Meraki デバイスに関連付けられるオブジェクトを参照してください。

サービスオブジェクトの作成

ステップ 1 左側の CDO ナビゲーションバーで、**[オブジェクト（Objects）] > [Meraki オブジェクト（Meraki Objects）]** をクリックします。

ステップ 2 + をクリックしてから、**[FTD] > [サービス（Service）]** または **[ASA] > [サービス（Service）]** をクリックします。

ステップ 3 オブジェクト名と説明を入力します。

ステップ 4 [サービスオブジェクトの作成（Create a service object）] を選択します。

ステップ 5 [サービスタイプ（Service Type）] ボタンをクリックし、オブジェクトを作成するプロトコルを選択します。

ステップ 6 次のいずれかのアクションを実行して、プロトコルを識別する情報を入力します。

- TCP または UDP ポートの特定のポート番号を入力します。
- ICMP または ICMPv6 メッセージタイプを選択します。
- 「その他」のサービスタイプを選択した場合は、リストから TCP/IP プロトコルの 1 つを選択します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

サービスグループを作成する

ステップ 1 左側の CDO ナビゲーションバーで、**[オブジェクト（Objects）] > [Meraki オブジェクト（Meraki Objects）]** をクリックします。

ステップ 2  をクリックしてから、**[FTD] > [サービス（Service）]** をクリックします。

（注） Meraki は ASA サービスグループをサポートしていません。

ステップ 3 オブジェクト名と説明を入力します。

ステップ 4 [サービスグループの作成（Create a service group）] を選択します。

ステップ 5 [オブジェクトの追加（Add Object）] をクリックし、オブジェクトを選択して [選択（Select）] をクリックすることで既存のオブジェクトを追加します。このステップを繰り返してさらにオブジェクトを追加します。

ステップ 6 サービスオブジェクトとサービス値のサービスグループへの追加が完了したら、[追加（Add）] をクリックします。

ステップ 7 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

サービスオブジェクトまたはサービスグループの編集

ステップ 1 左側の CDO ナビゲーションバーで、**[オブジェクト（Objects）] > [Meraki オブジェクト（Meraki Objects）]** をクリックします。

ステップ 2 オブジェクトをフィルタリングして編集するオブジェクトを見つけ、オブジェクトテーブルでオブジェクトを選択します。

ステップ 3 詳細ペインで、[編集（Edit）]  をクリックします。

ステップ 4 前述の手順で作成したのと同じ方法で、ダイアログボックスの値を編集します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 CDO は、変更の影響を受けるポリシーを表示します。[確認（Confirm）] をクリックして、オブジェクトとその影響を受けるポリシーへの変更を確定します。これで、オブジェクトを Meraki ポリシーで使用する準備ができました。

ステップ 7 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

関連情報

- Meraki デバイスに関連付けられるオブジェクト
- 未使用オブジェクトの問題の解決
- 重複オブジェクトの問題の解決

- ログの変更

セキュリティ ポリシー管理

セキュリティポリシーは、目的の宛先へのトラフィックを許可するか、セキュリティ脅威が特定された場合にトラフィックをドロップすることを最終的な目標として、ネットワークトラフィックを検査します。CDOを使用して、さまざまな種類のデバイスでセキュリティポリシーを設定できます。

- Meraki アクセスコントロールポリシー （24 ページ）

Meraki アクセスコントロールポリシー

Meraki MX デバイスは、CDO にオンボーディングする前に Meraki ダッシュボードによって管理されていた可能性があり、デバイスにはすでにいくつかのアウトバウンドルールが設定されている可能性があります。これらのルールは、CDO でアクセスコントロールルールとして表示されます。これらのルールを変更し、アクセスコントロールポリシー内に追加のルールを作成できます。アクセスコントロールポリシーをカスタマイズするには、オブジェクトを作成してアタッチします。詳しくは下の関連記事をご覧ください。

（注） Meraki アクセスコントロールポリシーのアクションは、デフォルトで [許可（Allow）] です。このアクションを変更することはできません。

CDO を使用して Meraki アクセス コントロール ポリシーを編集するには、次の手順を使用します。

ステップ 1 [デバイスとサービス（Devices & Services）] ページを開きます。

ステップ 2 [テンプレート（Templates）] タブをクリックします。

ステップ 3 [Meraki] タブをクリックし、アクセス コントロール ポリシーを編集する Meraki MX デバイステンプレートを選択します。

ステップ 4 右側の [管理（Management）] ペインで、[ポリシー（Policy）] を選択します。

ステップ 5 次のいずれかを実行します。

- 新しいルールを作成するには、青色のプラスボタン をクリックします。
- 既存のルールを編集するには、ルールを選択し、[アクション（Actions）] ペインの編集ボタン をクリックします。(単純な編集は、編集モードに移行せずにインラインで実行することも可能です。)
- 不要になったルールを削除するには、ルールを選択し、[アクション（Actions）] ペインで削除ボタン をクリックします。

- ポリシー内でルールを移動させるには、アクセス コントロール テーブルでルールを選択し、ルールの行の最後にある上下の矢印をクリックしてルールを移動します。

ステップ 6 [順序（Order）]フィールドで、ポリシー内のルールの位置を選択します。ネットワークトラフィックは、ルールのリストに照らして 1 から最後の番号までの順に評価されます。

ルールは最初に一致したものから順に適用されるため、限定的なトラフィック一致基準を持つルールは、同じトラフィックに適用され、汎用的な基準を持つルールよりも上に置く必要があります。

デフォルトでは、ルールはリストの最後に追加されます。ルールの順序を後で変更する場合、このオプションを編集します。

ステップ 7 ルール名を入力します。英数字、スペース、および次の特殊文字を使用できます：+ . _ -

注：アクセスコントロールルールの [名前（Name）] は CDO のルール名として使用されます。一方、[備考（Remark）] フィールドは Meraki ダッシュボードのルール名として扱われます。この 2 つのフィールドは互いに依存していません。

ステップ 8 ネットワークトラフィックがルールに一致する場合に適用するアクションを選択します。

- [ブロック（Block）]：トラフィックを無条件でドロップします。トラフィックのインスペクションは実行されません。
- [許可（Allow）]：ポリシーで侵入およびその他のインスペクション設定の対象となるトラフィックを許可します。

（注） ルールアクションのみを設定または変更できます。デフォルトポリシーのアクションを CDO から変更することはできません。

ステップ 9 次のタブ内の属性を任意に組み合わせて、トラフィック一致基準を定義します。

- [送信元（Source）]：[送信元（Source）] タブをクリックして、ネットワーク（ネットワークと大陸を含む）またはネットワークトラフィック発信元ポートを追加または削除します。デフォルト値は、[任意（Any）] です。
- [接続先（Destination）]：[接続先（Destination）] タブをクリックして、ネットワーク（ネットワークと大陸を含む）またはネットワークトラフィック着信ポートを追加または削除します。デフォルト値は、[任意（Any）] です。

（注） 送信元および接続先のネットワークは、設定されたいずれかの VLAN サブネット内にある必要があります。または、VLAN サブネットが手動で設定されていない場合は、デフォルトの VPN サブネット内にある必要があります。無効な送信元または接続先ネットワークを含むルールの展開は失敗します。

ステップ 10 [保存（Save）] をクリックします。

ステップ 11 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

次のタスク

関連記事：

- Meraki デバイスに関連付けられるオブジェクト
- Meraki サービスオブジェクトの作成または編集
- Meraki ネットワークオブジェクトまたはネットワークグループの作成または編集

Meraki テンプレート

Merakiテンプレートは、複数のサイト/ネットワークで共有されるネットワーク設定です。個々のサイトネットワークはテンプレートネットワークにバインドできるため、1 つのテンプレートを変更すると、バインドされたすべてのネットワークに影響します。 CDO では、バインドされたネットワークはバインドされたデバイスとして表示されます。この設定は、異なる場所にある複数のネットワークに 1 つのポリシーを適用する場合に最適です。1 つのテンプレートに対して複数のネットワークを設定するには、「設定テンプレートを使用した複数のネットワークの管理」を参照してください。Meraki テンプレートの詳細、ネットワークでのテンプレートの使用を計画する方法、およびテンプレートネットワークのセットアップ方法の詳細については、『Meraki Templates Best Practices』を参照してください。

Meraki テンプレートは、Meraki デバイスと同じように機能します。CDO にオンボーディングする前に、Meraki ダッシュボードを使用してテンプレートを設定する必要があります。テンプレートを CDO にオンボーディングすると、既存のルールまたは IP のグループが CDO に変更の読み取り、破棄、チェック、および展開、オブジェクトに変換されます。同期が完了すると、[インベントリ（Inventory）] ページの [デバイスの詳細（Device Details）] ペインに、テンプレート名と、テンプレートに関連付けられているネットワーク（バインドされたデバイスとして表示される）の数が表示されます。つまり、テンプレートに関連付けられたポリシーとバインドされたネットワークを CDO から管理および変更/展開することも可能ということです。詳細については、『Onboard Meraki Templates to Defense Orchestrator』を参照してください。

関連情報

- CDO と Meraki の通信方法
- Meraki デバイスに関連付けられるオブジェクト
- 変更の読み取り、破棄、チェック、および展開

変更の読み取り、破棄、チェック、および展開

デバイスを管理するために、CDO 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。CDO 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。CDO 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）] 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 CDO 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、CDO 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、CDO 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、CDO 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、CDO 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、CDO 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、CDO 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。CDO 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）] 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、CDO 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。

変更の配置

デバイスの設定に変更を加えると、CDO 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 CDO 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、CDO がデバイスに展開した後にのみ影響を及ぼします。CDO 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、CDOで保留中の変更のプレビューがCDO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 CDO 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

Cisco Defense Orchestrator（CDO）の外部にあるデバイスの設定が変更された場合、CDO 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、CDO 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。

CDO 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、「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、CDO 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、CDO 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。CDO は、デバイスの設定が変更されたことを検出した場合、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）] をクリックしすると、CDO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、CDO はデバイスの設定のコピーを上書きすることを確認し、上書きを実行します。
- [非同期（Not Synced）]：デバイスが [非同期（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、CDO 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、CDO 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が警告されます。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。変更の破棄 （35 ページ）

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] 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 CDO を保存する設定のデバイスを選択します。CDO 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、CDO で設定変更がステージングされている場合、CDO 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。 [ジョブ（Jobs）] ページ

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

- 変更の読み取り、破棄、チェック、および展開
- 変更の破棄
- 設定変更の確認

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、CDO 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「非同期（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。

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 デバイスを選択したら、右側のパネルにデバイスを拡大し、具体的な変更をプレビューできます。

ステップ 4 （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 5 （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 6 [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 7 （オプション）展開が完了したら、CDO 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 8 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

- スケジュールされた自動展開

変更のデバイスへの展開

ステップ 1 CDO 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 CDO インスタンスに保存されます。

ステップ 2 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

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。変更を加えたデバイスの設定ステータスが [非同期（Not Synced）] と表示されます。

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。

- デバイスを選択し、右側の [非同期（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。

- 画面右上の [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 （29 ページ）を参照してください。

変更をキャンセルする

CDO 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CDO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。CDO は、保留中の構成を、変更が行われる前に最後に読み取られた構成またはデプロイ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。

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] 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 CDO 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。

- 画面右上の [展開（Deploy）] ボタン をクリックします。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。

スケジュールされた自動展開

CDO 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、CDO 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。

CDOに変更の読み取り、破棄、チェック、および展開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。

注意 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。

（注） 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。

（注） 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。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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、[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。

ステップ1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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、[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。

（注） 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。

ステップ1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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。

次のタスク

- 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 （28 ページ）
- すべてのデバイスの設定変更のプレビューと展開 （29 ページ）

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、CDO 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。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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 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、CDO 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：

1. 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、CDO 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。
2. 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、CDO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。

3. [続行（Continue）] をクリックします。

変更の破棄

CDO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、CDO 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 [非同期（Not Synced）] 状態になります。変更を破棄すると、CDO 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、CDO 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。

ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）]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 [非同期（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、CDO で「CDO 上の保留中の変更は破棄され、このデバイスに関する CDO 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、CDO で変更がすぐに削除されます。
- AWS デバイスの場合は、CDO 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、CDO 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 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、CDO 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、または Cisco IOS デバイスに対して競合検出が有効になっている場合、CDO は 10 分ごとにデバイスをチェックし、CDO 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。

CDO は、CDO 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。

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

- CDO 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。

Defense Orchestrator とデバイス間の設定を同期する

設定の競合について

[デバイスとサービス（Devices & Services）] 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 [競合が検出されました（Conflict Detected）] になっていることがあります。

- デバイスが [同期済み（Synced）] の場合、Cisco Defense Orchestrator（CDO）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、CDO 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。CDO からデバイスに変更を展開すると、CDO 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。
- CDO 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、CDO 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、Cisco Defense Orchestrator（CDO）はデフォルトの間隔でデバイスをポーリングして、CDO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、CDO 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。CDO 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。

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 （40 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、Defense Orchestrator 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。

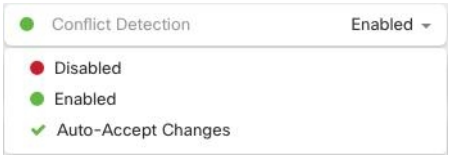
ステップ 1 ナビゲーションバーで、[インベントリ（Inventory）] をクリックします。

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。



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 Cisco Defense Orchestrator（CDO）を設定できます。CDO 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、CDO 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、CDO 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、CDO 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。

CDO 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、CDO 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。

変更の自動受け入れを使用するには、最初に、テナントが [インベントリ（Inventory）] ページの [競合検出（Conflict Detection）] メニューで自動受け入れ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受け入れを有効にします。

CDO 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 （37 ページ） を有効にします。

自動承認変更の設定

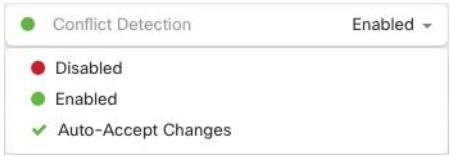
ステップ 1 管理者またはスーパー管理者権限を持つアカウントを使用して CDO にログインします。

ステップ 2 CDO メニューから **[設定（Settings）] > [全般設定（General Settings）]** に移動します

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。この操作により、[インベントリ（Inventory）] 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るようになります。

ステップ 4 [インベントリ] ページを開き、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

ステップ 1 管理者またはスーパー管理者権限を持つアカウントを使用して CDO にログインします。

ステップ 2 CDO メニューから **[設定（Settings）] > [全般設定（General Settings）]** に移動します

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、CDO 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。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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 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 CDO 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 CDO からデバイスにプッシュ**したくない**場合、または CDO 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、CDO 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中の設定で上書きします。

[競合検出（Conflict Detected）] ステータスの解決

CDO 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 （37 ページ） が有効になっていて、CDO 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。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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、CDO 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、CDO 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） CDO 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 CDO 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 （37 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、CDO はデフォルトの間隔でデバイスをポーリングして、CDO 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。CDO 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） [デバイスとサービス（Devices & Services）] ページでデバイスごとの間隔をカスタマイズすると、[全般設定（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で選択したポーリング間隔が上書きされます。

[デバイスとサービス（Conflict Detection）] 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 CDO 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。

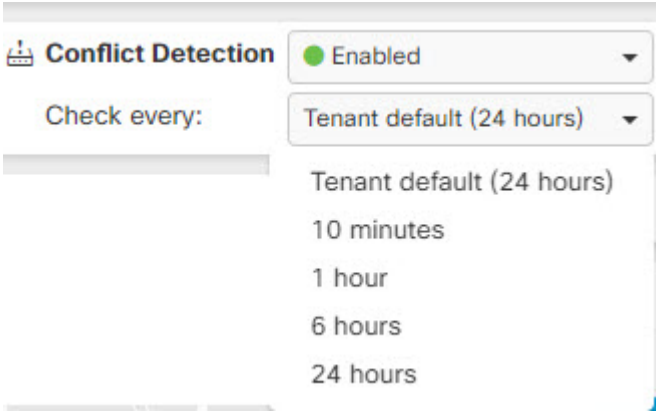
ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

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。