Cisco Defense Orchestrator の基本

Cisco Defense Orchestrator（CDO）は、明確で簡潔なインターフェイスを通じてポリシーを管理するための独自のビューを提供します。CDO を初めて使用する場合の基本的な事柄について以下で取り上げます。

- CDO がデバイスを管理する方法 （2 ページ）
- CDO アカウントのリクエスト （8 ページ）
- Secure Device Connector（SDC） （9 ページ）
- CDO へのサインイン （37 ページ）
- Cisco Secure Sign-On ID プロバイダーへの移行 （39 ページ）
- Cisco Secure Sign-On ダッシュボードからの CDO の起動 （40 ページ）
- テナントのネットワーク管理者の管理 （41 ページ）
- CDO でサポートされるソフトウェアとハードウェア （42 ページ）
- ブラウザ サポート （44 ページ）
- テナント管理 （44 ページ）
- ユーザ管理 （63 ページ）
- ユーザー管理の Active Directory グループ （64 ページ）
- 新規 CDO ユーザーの作成 （69 ページ）
- ユーザの役割 （76 ページ）
- ユーザーロールのユーザーレコードの作成 （81 ページ）
- ユーザーロールのユーザーレコードの編集 （82 ページ）
- ユーザーロールのユーザーレコードの削除 （83 ページ）
- デバイスとサービスの管理 （84 ページ）
- [インベントリ（Inventory）] ページ情報の表示 （92 ページ）
- ラベルとフィルタ処理 （92 ページ）
- 同一 SDC を使用した CDO に接続するすべてのデバイスを見つける （95 ページ）
- 検索 （96 ページ）
- グローバル検索 （96 ページ）
- CDO コマンドライン インターフェイスの使用 （99 ページ）
- 一括コマンド ライン インターフェイス （101 ページ）
- デバイスの管理用 CLI マクロ （106 ページ）

• FTD コマンド ライン インターフェイスのドキュメント （111 ページ）
• CLI コマンドの結果のエクスポート （111 ページ）
• オブジェクト （114 ページ）
• ネットワーク オブジェクト （126 ページ）
• アプリケーション フィルタ オブジェクト （140 ページ）
• 地理位置情報オブジェクト （144 ページ）
• DNS グループオブジェクト （145 ページ）
• 証明書オブジェクト （147 ページ）
• IPsec プロポーザルの設定 （154 ページ）
• グローバル IKE ポリシーの設定 （157 ページ）
• RA VPN オブジェクト （162 ページ）
• セキュリティ ゾーン オブジェクト （163 ページ）
• サービス オブジェクト （165 ページ）
• セキュリティ グループ タグ グループ （168 ページ）
• Syslog サーバーオブジェクト （172 ページ）
• URL オブジェクト （175 ページ）

CDO がデバイスを管理する方法

CDO がサポートするデバイスを管理するには、CDO にデバイスへの https アクセス権が必要です。

そのデバイスがネットワークでどのように設定されているか、および SDC が存在する場所によって、これを行う方法は異なります。

クラウド SDC を使用するユーザーは、ネットワークの外部で管理アクセス権を利用できるようにする必要があります（適切なセクションへのリンク）。

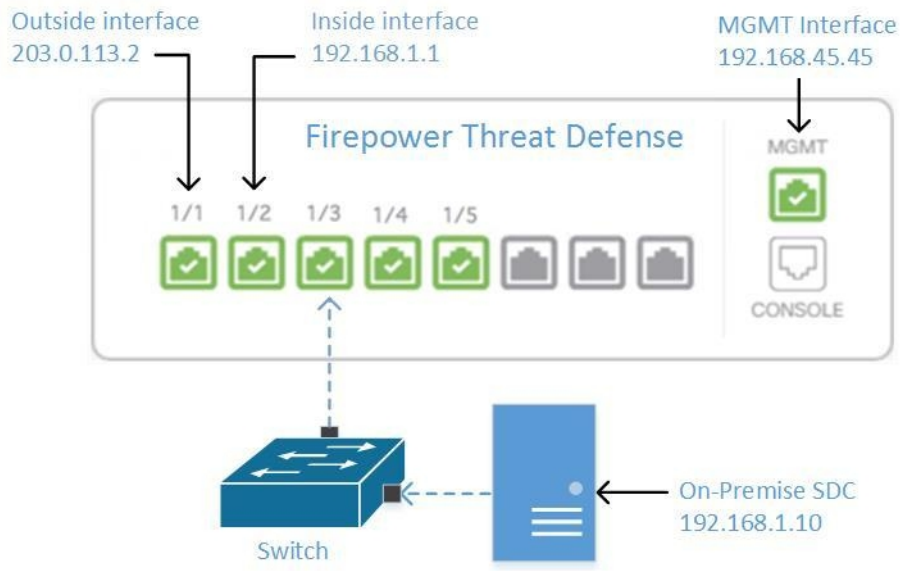
オンプレミス SDC を使用するユーザーは、内部または管理インターフェイス（編集済み）を使用できます。

ネットワーキング要件

内部インターフェイスからの FTD の管理

専用の MGMT インターフェイスに組織内でルーティングできないアドレスが割り当てられている場合は、内部インターフェイスを使用して Firepower Threat Defense（FTD）デバイスを管理することが望ましい場合があります。たとえば、データセンターまたはラボ内からしか到達できない場合などです。

図 *1* : *FTD* インターフェイスアドレス



リモートアクセス VPN の要件

CDO で管理する FTD がリモートアクセス VPN（RA VPN）接続を管理する場合、CDO は内部インターフェイスを使用して FTD デバイスを管理する必要があります。

次に行う作業：

FTD を設定する手順については、内部インターフェイスからの FTD の管理 （3 ページ） に進んでください。

内部インターフェイスからの FTD の管理

設定方法は次のとおりです。

- FTD が CDO にオンボードされていないことが前提です。
- データインターフェイスを内部インターフェイスとして設定します。
- MGMT トラフィック（HTTPS）を受信するように内部インターフェイスを設定します。
- SDC またはクラウドコネクタのアドレスが FTD の内部インターフェイスに到達できるようにします。

始める前に

この設定の前提条件を以下で確認してください。

- 内部インターフェイスからの FTD の管理 （2 ページ）
- Cisco Defense Orchestrator の管理対象デバイスへの接続 （10 ページ）

手順

ステップ 1 FDM にログインします。

ステップ 2 [システム設定（System Settings）] メニューで、[管理アクセス（Management Access）] をクリックします。

ステップ 3 [データインターフェース（Data Interfaces）] タブをクリックし、[データインターフェースの作成（Create Data Interface）] を選択します。

1. [インターフェース（Interface）] フィールドで、インターフェースのリストから「**inside**」という名前のインターフェースを選択します。
2. [プロトコル（pre-named）] フィールドがまだ選択されていない場合は、[HTTPS] を選択します。
3. [許可されたネットワーク（Allowed Networks）] フィールドで、組織内に配置され FTD の内部アドレスへのアクセスが許可されているネットワークを示すネットワークオブジェクトを選択します。SDC またはクラウドコネクタの IP アドレスは、FTD の内部アドレスへのアクセスが許可されているアドレス群の中にある必要があります。

   「FTD インターフェイスアドレス」図の中では、SDC の IP アドレス 192.168.1.10 が 192.168.1.1 に到達可能である必要があります。

ステップ 4 **変更を展開します**。これで、内部インターフェイスを使用してデバイスを管理できるようになりました。

次のタスク

Cloud Connector を使用している場合

上記の手順に加えて、以下の手順を実行します。

- 外部インターフェイス（203.0.113.2）から内部インターフェイス（192.168.1.1）への「NAT」を実行するステップを追加します。
- 上記の手順のステップ 3c の [許可ネットワーク（Allowed Network）] は、Cloud Connector のパブリック IP アドレスを含むネットワーク グループ オブジェクトになります。
- クラウドコネクタのパブリック IP アドレスから外部インターフェイス（203.0.113.2）へのアクセスを許可するアクセス制御ルールの作成ステップを追加します。

ヨーロッパ、中東、またはアフリカ（EMEA）地域のお客様が https://defenseorchestrator.eu/ で Defense Orchestrator に接続している場合、Cloud Connector のパブリック IP アドレスは、次のようになります。

- 35.157.12.126
- 35.157.12.15

アメリカ合衆国のお客様が https://defenseorchestrator.com/ で Defense Orchestrator に接続する場合、クラウドコネクタのパブリック IP アドレスは、次のようになります。

- 52.34.234.2
- 52.36.70.147

アジア - 太平洋 - 日本 - 中国（APJC）地域のお客様が https://www.apj.cdo.cisco.com/ で Defense Orchestrator に接続する場合は、次の IP アドレスからのインバウンドアクセスを許可します。

- 54.199.195.111
- 52.199.243.0

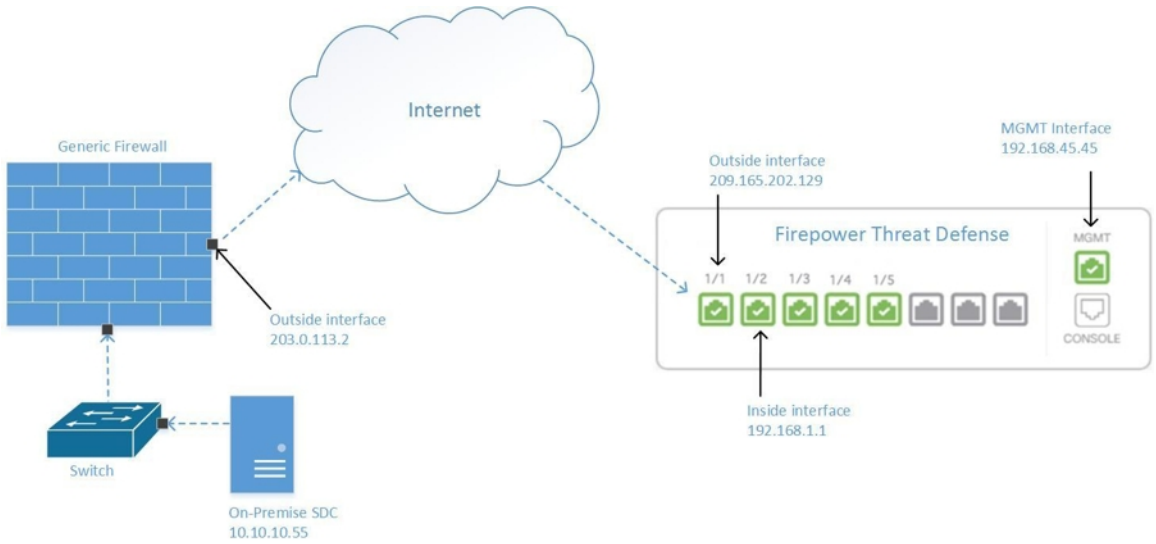
FTD の導入準備

CDO で FTD デバイスの導入準備をする際、登録トークンを使用した導入準備の方法をお勧めします。Cloud Connector から FTD への管理アクセスを許可するように内部インターフェイスを設定した後に、ユーザー名とパスワードを使用して FTD デバイスの導入準備をします。 詳細については、「ユーザー名、パスワード、および IP アドレスを使用した FTD の導入準備」を参照してください。内部インターフェイスの IP アドレスを使用して接続します。上記シナリオでは、そのアドレスは 192.168.1.1 です。

外部インターフェイスから FTD を管理する

分散拠点に 1 つのパブリック IP アドレスが割り当てられていて、CDO が別の場所にある Secure Device Connector（SDC）または Cloud Connector を使用して管理されている場合は、外部インターフェイスから Firepower Threat Defense（FTD）デバイスを管理することを推奨します。

図 *2*: 外部インターフェイスでの *FTD* の管理



この設定により、MGMT 物理インターフェイスがデバイスの管理インターフェイスでなくなるわけではありません。FTD の設置場所にいる場合は、MGMT インターフェイスのアドレスに接続して、FTD を直接管理できます。

リモートアクセス VPN の要件

CDO を使用して管理する FTD で、リモートアクセス VPN（RA VPN）接続を管理する場合、CDO は外部インターフェイスを使用して FTD デバイスを管理できません。代わりに、「内部インターフェイスからの FTD の管理」を参照してください。

次に行う作業：

FTD を設定する手順については、FTD の外部インターフェイスの管理 （6 ページ） に進んでください。

FTD の外部インターフェイスの管理

設定方法は次のとおりです。

1. FTD が CDO にオンボードされていないことが前提です。
2. データインターフェイスを外部インターフェイスとして設定します。
3. 外部インターフェイスで管理アクセスを設定します。
4. SDC または Cloud Connector のパブリック IP アドレス（ファイアウォールによる NAT 処理済み）が外部インターフェイスに到達できるようにします。

始める前に

この設定の前提条件を以下で確認してください。

- FTD の外部インターフェイスの管理 （6 ページ）
- Cisco Defense Orchestrator の管理対象デバイスへの接続 （10 ページ）

手順

ステップ 1 FDM にログインします。

ステップ 2 [システム設定（System Settings）] メニューで、[管理アクセス（Management Access）] をクリックします。

ステップ 3 [データインターフェース（Data Interfaces）] タブをクリックし、[データインターフェースの作成（Create Data Interface）] を選択します。

1. [インターフェイス（Interface）] フィールドで、インターフェイスのリストから「**outside**」という名前のインターフェイスを選択します。
2. [プロトコル（pre-named）] フィールドがまだ選択されていない場合は、[HTTPS] を選択します。CDO に必要なのは HTTPS アクセスのみです。
3. [許可ネットワーク（Allowed Networks）] フィールドで、ファイアウォールによる NAT 処理済みの SDC または Cloud Connector のパブリック方向 IP アドレスを含むホスト ネットワーク オブジェクトを作成します。

「外部インターフェイスからの FTD 管理」のネットワーク図では、SDC または Cloud Connector の IP アドレス 10.10.10.55 が 203.0.113.2 に NAT 処理されています。許可ネットワークの場合は、203.0.113.2 という値を使用してホスト ネットワーク オブジェクトを作成します。

ステップ 4 SDC または Cloud Connector のパブリック IP アドレスから FTD の外部インターフェイスへの管理トラフィック（HTTPS）を許可するアクセス コントロール ポリシーを、FDM で作成します。このシナリオでは、送信元アドレスは 203.0.113.2 で、送信元プロトコルは HTTPS です。また、宛先アドレスは 209.165.202.129 で、宛先プロトコルは HTTPS です。

ステップ 5 **変更を展開します**。これで、外部インターフェイスを使用してデバイスを管理できるようになります。

次のタスク

Cloud Connector を使用している場合

プロセスは非常によく似ていますが、次の 2 つの点が異なります。

- 上記の手順のステップ 3c の [許可ネットワーク（Allowed Network）] は、Cloud Connector のパブリック IP アドレスを含むネットワーク グループ オブジェクトになります。
  - **ヨーロッパ、中東、またはアフリカ（EMEA）地域**のお客様が https://defenseorchestrator.eu/ で Defense Orchestrator に接続している場合、Cloud Connector のパブリック IP アドレスは、次のようになります。
    - 35.157.12.126
    - 35.157.12.15
  - **アメリカ合衆国**のお客様が https://defenseorchestrator.com/ で CDO に接続している場合、Cloud Connector のパブリック IP アドレスは、次のようになります。
    - 52.34.234.2
    - 52.36.70.147
  - **アジア - 太平洋 - 日本 - 中国（APJC）**地域のお客様が https://www.apj.cdo.cisco.com/ で Defense Orchestrator に接続する場合は、次の IP アドレスからのインバウンドアクセスを許可します。
    - 54.199.195.111
    - 52.199.243.0
- 上記の手順のステップ 4 では、Cloud Connector のパブリック IP アドレスから外部インターフェイスへのアクセスを許可するアクセス制御ルールを作成します。

FTD デバイスを CDO にオンボーディングする際は、「登録トークンによるオンボーディング」の方法を推奨します。Cloud Connector からの管理アクセスを許可するように外部インターフェ

イスを設定した後に、FTD デバイスをオンボードします。外部インターフェイスの IP アドレスを使用して接続します。このシナリオでは、そのアドレスは 209.165.202.129 です。

CDO アカウントのリクエスト

CDO アカウントリクエストフォームに記入して、CDO アカウントをリクエストできます。リクエストフォームを使用して、30 日間の無料トライアルをリクエストするか、すでに支払い済みの CDO ライセンスの使用を開始できます。この記事では、フォームに記入する際に守る必要がある簡単な手順について詳しく説明します。

始める前に

CDO ライセンスを取得するか、既存のライセンスを確認します。

この情報を使用して、CDO ライセンスを購入するか、購入済みのライセンスを確認します。

- Enterprise License Agreement（ELA）をお持ちの場合は、そのバンドルの一部として購入したライセンスを確認してください。CDO ライセンスをすでに持っている可能性があります。CDO データシートの発注情報の表を参照して、ライセンス部品番号を確認してください。
- シスコパートナーを通じてライセンスを取得します。Cisco Commerce（CCW）を参照してください。
- Cisco Commerce（CCW）を使用して、シスコから直接 CDO ライセンスを購入します。
- CDO データシートを使用して、ライセンスの種類について学びます。

手順

ステップ 1 CDO をすでに購入している場合は、SO 番号と契約番号を取得します。

ステップ 2 CDO アカウントリクエストページに移動します。

ステップ 3 [はい（Yes）] をクリックして、連絡先情報をシスコと共有することに同意します。

ステップ 4 [会社と主要連絡先（Company and Primary Contact）] に、個人情報を入力します。

ステップ 5 [要件（Your Requirement）] 領域で、次のいずれかを選択します。

- [30日間の価値実証（30 Day Proof of Value）]：30 日間のカスタマートライアルのリクエスト。
- [CDOを購入済み（I Bought CDO Already）]：CDO の完全版をすでに購入していますが、アクセスできません。
- [パートナーアカウント（Partner Account）]：シスコパートナーのデモ目的で使用される永続的なアカウント。
- [内部アカウント（Internal Account）]：シスコの内部ユーザーに使用される永続的なアカウント。

ステップ 6 [SOと契約番号（Sales Order & Contract Number）] がわかっている場合は、詳細を入力します。CDO をすでに購入している場合は、SO と契約番号の詳細を受け取ります。

ステップ 7 CDO を展開するリージョンを選択します。

ステップ 8 [CDOのコアユースケース（Core Use Case(s) for CDO）] を提供すると、シスコが CDO の使用目的を理解するのに役立ちます。

ステップ 9 コストの見積もりが必要な場合は、CDO にオンボードするデバイスのタイプと数量を指定します。

ステップ 10 **Cisco Security Analytics and Logging** 機能を有効にすると、CDO はイベントログをデバイスから中央のログ管理システムに送信します。詳細については、Cisco Security Analytics and Logging を参照してください。

（注） この機能は、APJC リージョンでは使用できません。アクセスする必要がある場合は、テスト用に別のリージョンを選択してください。

ステップ 11 [調査を送信（Submit Survey）] をクリックします。CDO チームが 24 時間以内にリクエストを処理します。

その後の手順

次の手順が示された自動生成電子メールが届きます。

- Cisco Secure Sign-On にサインアップ：Cisco Secure Sign-On でアカウントを作成します。詳細については、新規 CDO テナントへの初回ログイン（38 ページ）を参照してください。
- Cisco Defense Orchestrator にアクセスします。アカウント作成時に通知されます。CDO にアクセスするには、Cisco Secure Sign-On にサインインし、リクエストしたリージョンで CDO を選択します。

Secure Device Connector（SDC）

デバイスのログイン情報を使用して CDO にデバイスをオンボーディングする場合、CDO は、そのデバイスと CDO 間の通信をプロキシするために、ネットワークに Secure Device Connector（SDC）をダウンロードして展開することがベストプラクティスだとみなします。ただし、必要に応じて、デバイスが CDO からの外部インターフェイスを介して直接通信を受信できるようにすることができます。適応型セキュリティアプライアンス（ASA）、Firepower Threat Defense デバイス（FTD）、Firepower Management Center（FMC）、 Secure Firewall Cloud Native デバイス、SSH および IOS デバイスはすべて、SDC を使用して CDO にオンボードできます。

SDC は、管理対象デバイスで実行する必要があるコマンドと、管理対象デバイスに送信する必要があるメッセージについて、CDO を監視します。SDC は、CDO に代わってこのコマンドを実行し、管理対象デバイスに代わって CDO にメッセージを送信し、管理対象デバイスからの応答を CDO に返します。

SDC は、AES-128-GCM over HTTPS（TLS 1.2）を使用して署名および暗号化された安全な通信メッセージを使用して、CDO と通信します。オンボードのデバイスとサービスのすべてのロ

グイン情報は、ブラウザから SDC に直接暗号化されるだけでなく、AES-128-GCM を使用して保存時にも暗号化されます。SDC だけがデバイスのログイン情報にアクセスできます。他の CDO サービスはログイン情報にアクセスできません。SDC と CDO 間の通信を許可する方法については、「Cisco Defense Orchestrator の管理対象デバイスへの接続 （10 ページ）」を参照してください。

SDC は、アプライアンスに、ハイパーバイザ上の仮想マシンとして、または AWS や Azure などのクラウド環境にインストールできます。CDO が提供する仮想マシンと SDC イメージを組み合わせて使用して SDC をインストールすることも、独自の仮想マシンを作成してその上に SDC をインストールすることもできます。SDC 仮想アプライアンスには CentOS オペレーティングシステムが含まれており、Docker コンテナ内で実行されます。

各 CDO テナントは、無制限の数の SDC を持つことができます。これらの SDC はテナント間で共有されず、1 つのテナント専用です。1 つの SDC が管理できるデバイスの数は、それらのデバイスに導入された機能と、設定ファイルのサイズによって異なります。ただし、展開を計画するために、1 つの SDC が約 500 台のデバイスをサポートすることを想定してください。

テナントに複数の SDC を展開すると、次の利点もあります。

- パフォーマンスを低下させることなく、CDO テナントでより多くのデバイスを管理できます。
- ネットワーク内の隔離されたネットワークセグメントに SDC を展開し、そのセグメント内のデバイスを同じ CDO テナントで引き続き管理できます。複数の SDC がない場合、これらの隔離されたネットワークセグメント内のデバイスを、異なる CDO テナントで管理する必要があります。

2 番目以降の SDC を展開する手順は、最初の SDC を展開する手順と同じです。テナントの最初の SDC には、テナントの名前と番号 1 が組み込まれており、CDO の [セキュアコネクタ（Secure Connectors）] ページに表示されます。追加の各 SDC には、順番に番号が付けられます。CDO の VM イメージを使用した Secure Device Connector の展開 （12 ページ）および自身の VM 上での Secure Device Connector の展開 （17 ページ）を参照してください。

関連情報：

- Cisco Defense Orchestrator の管理対象デバイスへの接続
- Secure Device Connector のトラブルシュート
- Secure Device Connector の更新 （26 ページ）
- Secure Device Connector の削除 （23 ページ）

Cisco Defense Orchestrator の管理対象デバイスへの接続

CDO は、Cloud Connector または Secure Device Connector（SDC）を介して管理対象デバイスに接続します。

インターネットからデバイスに直接アクセスできる場合は、Cloud Connectorを使用してデバイスに接続する必要があります。デバイスを設定できる場合は、クラウドリージョンの CDO IP アドレスからのポート 443 でのインバウンドアクセスを許可します。

インターネットからデバイスにアクセスできない場合は、ネットワークにオンプレミスのSDCを展開して、CDO がデバイスと通信できるようにすることができます。デバイスを設定できる場合は、ポート 443（またはデバイス管理用に設定したポート）での完全なインバウンドアクセスを許可する必要があります。

FTDは、インターネットから直接アクセスできるかどうかに関係なく、デバイスのログイン情報、登録キー、またはシリアル番号を使用して CDO へのオンボーディングを実行できます。FTDがインターネットに直接アクセスできないものの、インターネットに直接アクセスできるネットワーク上に存在する場合、FTD の一部として提供される Cisco Security Services Exchange（SSE）コネクタはSSEクラウドに到達できるため、FTDのオンボーディングが可能になります。さまざまなオンボーディング方式の詳細については、「FTDのオンボーディング」を参照してください。

表 *1 : CDO* をデバイスまたはサービスに接続するためのベストプラクティス

デバイスタイプまたはクラウドサービス	オンボーディング方式	クラウドコネクタ	Secure Device Connector（SDC）
Adaptive Security Appliance（ASA）[AdaptiveSecurityApplianceASA]	資格情報		X
Firepower Threat Defense（FTD）	資格情報		X
Firepower Threat Defense（FTD）	登録トークン	X	
Firepower Threat Defense（FTD）バージョン 6.7 以降	シリアル番号	X	
Firepower Management Center（FMC）	資格情報		X
Cisco IOS デバイス	資格情報		X
SSH アクセスのあるデバイス	資格情報		X
Meraki 組織	クラウドサービスからクラウドサービスへ	X	
Amazon Web Services（AWS）サービスまたはデバイス	クラウドサービスからクラウドサービスへ	X	

Cloud Connector を介したデバイスの CDO への接続

Cloud Connector を介して CDO をデバイスに直接接続する場合、EMEA、米国、または APJC 地域のさまざまなIPアドレスに、ポート443（またはデバイス管理用に設定したポート）でのインバウンドアクセスを許可する必要があります。

ヨーロッパ、中東、またはアフリカ（EMEA）地域のお客様で、https://defenseorchestrator.eu/ で Defense Orchestrator に接続している場合は、次の IP アドレスからのインバウンドアクセスを許可します。

- 35.157.12.126
- 35.157.12.15

米国地域のお客様で、https://defenseorchestrator.com で Defense Orchestrator に接続している場合は、次の IP アドレスからのインバウンドアクセスを許可します。

- 52.34.234.2
- 52.36.70.147

アジア - 太平洋 - 日本 - 中国（APJC）地域のお客様で、https://www.apj.cdo.cisco.com/ で Defense Orchestrator に接続している場合は、次の IP アドレスからのインバウンドアクセスを許可します。

- 54.199.195.111
- 52.199.243.0

SDC を使用したデバイスの CDO への接続

SDC を介してデバイスを CDO に接続する場合、CDO で管理するデバイスは、ポート 443（またはデバイス管理用に設定したポート）での完全なインバウンドアクセスを許可する必要があります。この許可は、管理アクセス制御ルールを使用して設定されます。

また、SDC が展開されている仮想マシンが、管理対象デバイスの管理インターフェイスにネットワーク接続されていることを確認する必要があります。

CDO の VM イメージを使用した Secure Device Connector の展開

デバイスのログイン情報を使用して CDO をデバイスに接続する場合、CDO とデバイス間の通信を管理するために、ネットワークに SDC をダウンロードして展開することがベストプラクティスです。通常、これらのデバイスは非境界ベースであり、パブリック IP アドレスを持たないか、外部インターフェイスに開かれたポートを持っています。適応型セキュリティアプライアンス（ASA）、Firepower Threat Defense デバイス（FTD）、Firepower Management Center（FMC）、 Secure Firewall Cloud Native デバイス、SSH および IOS デバイスはすべて、SDC を使用して CDO にオンボードできます。

SDC は、管理対象デバイスで実行する必要があるコマンドと、管理対象デバイスに送信する必要があるメッセージについて、CDO を監視します。SDC は、CDO に代わってこのコマンドを実行し、管理対象デバイスに代わって CDO にメッセージを送信し、管理対象デバイスからの応答を CDO に返します。

1 つの SDC が管理できるデバイスの数は、それらのデバイスに実装されている機能と、構成ファイルのサイズによって異なります。ただし、展開計画の目安として、1 つの SDC で約 500

台のデバイスをサポートできることを想定しています。詳細については、単一の CDO テナントで複数の SDC を使用する （27 ページ）を参照してください。

この手順では、CDO の VM イメージを使用してネットワークに SDC をインストールする方法について説明します。これは、SDC を作成するために推奨される、最も簡単で信頼できる方法です。作成した VM を使用して SDC を作成する必要がある場合は、自身の VM 上での Secure Device Connector の展開 （17 ページ）の手順に従います。

始める前に

SDC を展開する前に、次の前提条件を確認してください。

- CDO は、厳密な証明書チェックを必要とし、SDC とインターネットの間の Web/コンテンツプロキシ検査をサポートしていません。プロキシサーバーを使用している場合は、SDC と CDO の間のトラフィックの検査を無効にします。
- SDC には、TCP ポート 443 またはデバイス管理用に設定したポートでのインターネットへの完全なアウトバウンドアクセスが必要です。デバイスが CDO によって管理されている場合、このポートからのインバウンドトラフィックも許可する必要があります。
- 適切なネットワークアクセスを確保するため、「Cisco Defense Orchestrator の管理対象デバイスへの接続」を参照してください。
- CDO は、vSphere Web クライアントまたは ESXi Web クライアントを使用した SDC VM OVF イメージのインストールをサポートしています。
- CDO は、vSphere デスクトップクライアントを使用した SDC VM OVF イメージのインストールをサポートしていません。
- ESXi 5.1 ハイパーバイザ。
- Cent OS 7 ゲスト オペレーティング システム。
- SDC のみを持つ VM のシステム要件：
  - VMware ESXi ホストには 2 つの vCPU が必要です。
  - VMware ESXi ホストには 2 GB 以上のメモリが必要です。
  - VMware ESXi では、プロビジョニングの選択に応じて、仮想マシンをサポートするために 64 GB のディスク容量が必要です。
- テナント用の SDC と**単一**の SEC を備えた VM のシステム要件（SEC は Cisco Security Analytics and Logging で使用されるコンポーネント）：
  - VMware ESXi ホストには 6 つの vCPU が必要です。
  - VMware ESXi ホストには 10 GB 以上のメモリが必要です。
  - VMware ESXi では、プロビジョニングの選択に応じて、仮想マシンをサポートするために 64 GB のディスク容量が必要です。
- CDO コネクタとセキュア イベント コネクタ（SEC）を備えた VM のシステム要件：

- CPU：SEC 用に 4 つの CPU を追加します。
- メモリ：SEC 用 8 GB のメモリを追加します。

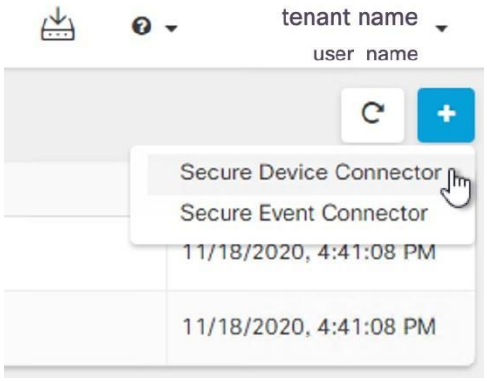
- Docker IP は、SDC の IP 範囲**および**デバイスの IP 範囲とは異なるサブネットにある必要があります。
- インストールを開始する前に、次の情報を収集します。
  - SDC に使用する静的 IP アドレス。
  - インストールプロセス中に作成する `root` ユーザーと `cdo` ユーザーのパスワード。
  - 組織で使用する DNS サーバーの IP アドレス。
  - SDC アドレスが存在するネットワークのゲートウェイ IP アドレス。
  - タイムサーバーの FQDN または IP アドレス。
- SDC 仮想マシンは、セキュリティパッチを定期的にインストールするように設定されており、これを行うには、ポート 80 のアウトバウンドを開く必要があります。

手順

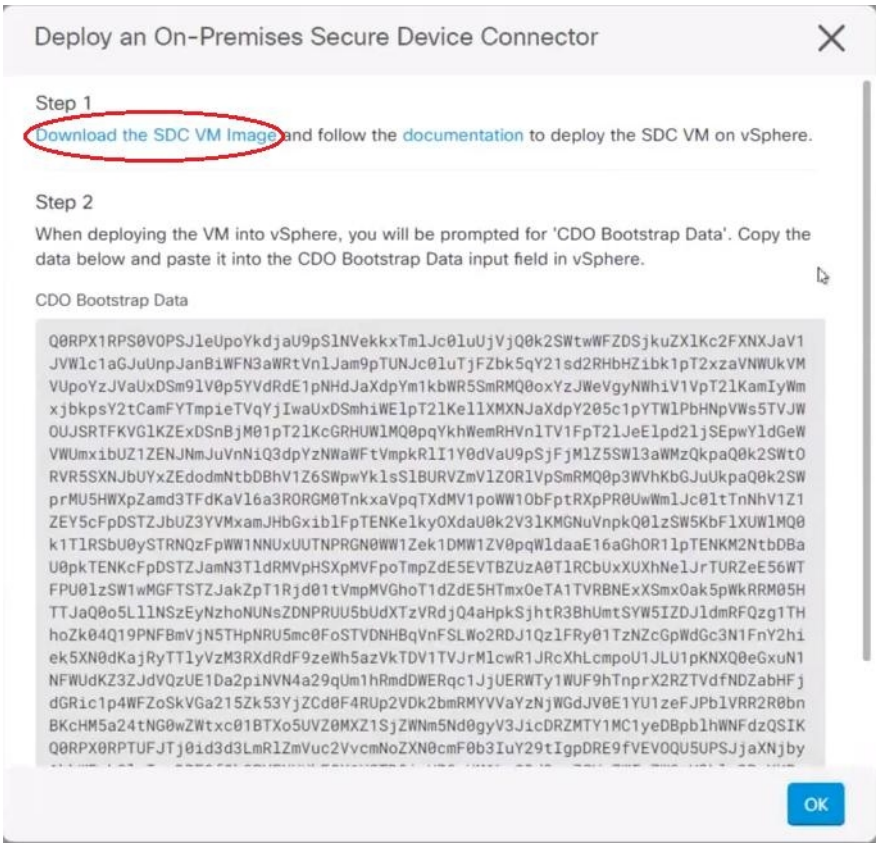
ステップ 1 SDC を作成する CDO テナントにログオンします。

ステップ 2 CDO メニューバーから**[管理（Admin）]** > **[セキュアコネクタ（Secure Connectors）]**に移動します。

ステップ 3 [セキュアコネクタ（Secure Connectors）] ページで、青いプラスボタンをクリックし、[Secure Device Connector] を選択します。



ステップ 4 手順 1 で [SDC VMイメージのダウンロード（Download the SDC VM image）] をクリックします。すると別のタブが表示されます。



ステップ 5 .zip ファイルからすべてのファイルを抽出します。これらは、次のようなものです。

- CDO-SDC-VM-ddd50fa.ovf
- CDO-SDC-VM-ddd50fa.mf
- CDO-SDC-VM-ddd50fa-disk1.vmdk

ステップ 6 vSphere Web クライアントを使用して、管理者として VMware サーバーにログオンします。

（注） ESXi Web クライアントは使用しないでください。

ステップ 7 プロンプトに従って、OVF テンプレートから Secure Device Connector 仮想マシンを展開します。

ステップ 8 セットアップが完了したら、SDC VM の電源を入れます。

ステップ 9 新しい SDC VM のコンソールを開きます。

ステップ 10 ユーザー名 **cdo** でログインします。デフォルトのパスワードは **adm123** です。

ステップ 11 プロンプトで、`sudo sdc-onboard setup` と入力します。

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

ステップ 12 パスワードのプロンプトが表示されたら、`adm123` と入力します。

ステップ 13 プロンプトに従って、`root` ユーザーの新しいパスワードを作成します。root ユーザーのパスワードを入力します。

ステップ 14 プロンプトに従って、**cdo** ユーザーの新しいパスワードを作成します。cdo ユーザーのパスワードを入力します。

ステップ 15 [接続する CDO ドメインを選択してください（Please choose the CDO domain you connect to）] というプロンプトが表示されたら、Cisco Defense Orchestrator のドメイン情報を入力します。

ステップ 16 プロンプトが表示されたら、SDC VM の次のドメイン情報を入力します。

a) IP アドレス/CIDR
b) ゲートウェイ
c) DNS サーバー
d) NTP サーバーまたは FQDN
e) Docker ブリッジ

または、Docker ブリッジが適用されない場合は Enter キーを押します。

ステップ 17 [これらの値は正しいですか？（はい/いいえ）（Are these values correct? (y/n)）]というプロンプトが表示されたら、**y** と入力してエントリを確認します。

ステップ 18 入力内容を確定します。

ステップ 19 [今すぐSDCを設定しますか？（はい/いいえ）（Would you like to setup the SDC now? (y/n)]というプロンプトが表示されたら、[n] を入力します。

ステップ 20 VM コンソールから自動的にログアウトします。

ステップ 21 SDC への SSH 接続を作成します。**cdo** としてログインし、パスワードを入力します。

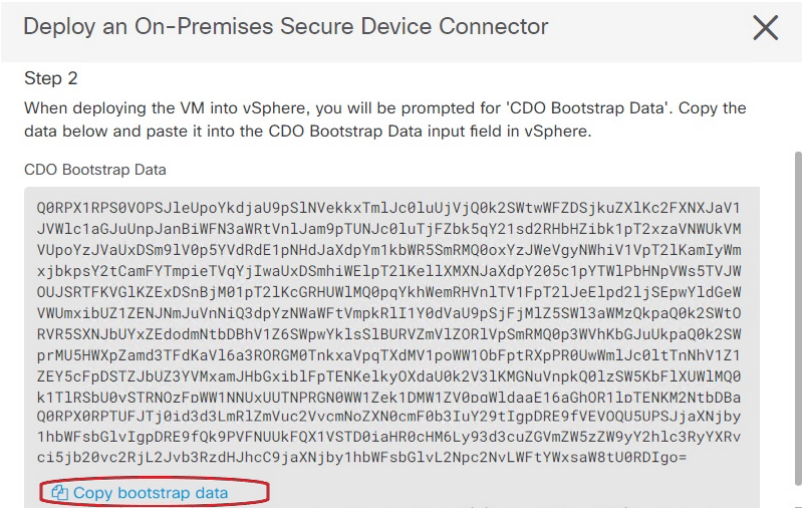
ステップ 22 プロンプトで、`sudo sdc-onboard bootstrap` と入力します。

```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

ステップ 23 [sudo] パスワードの入力を求められたら、ステップ 14 で作成した cdo パスワードを入力します。

ステップ 24 [CDOのセキュアコネクタページからブートストラップデータをコピーしてください（Please copy the bootstrap data form the Secure Connector Page of CDO）] というプロンプトが表示されたら、次の手順に従います。

1. CDO にログインします。
2. ユーザーメニューから、[セキュアコネクタ（Secure Connectors）] を選択します。
3. [アクション（Actions）]ペインで、[オンプレミスの Secure Device Connector の展開（Deploy an On-Premises Secure Device Connector）] をクリックします。
4. ダイアログボックスのステップ 2 で [ブートストラップデータをコピー（Copy the bootstrap data）] をクリックし、SSH ウィンドウに貼り付けます。



ステップ 25 [これらの設定を更新しますか？（はい/いいえ）（Do you want to update these setting? (y/n)）] というプロンプトが表示されたら、[n] を入力します。

ステップ 26 [Secure Device Connector] ページに戻ります。新しい SDC のステータスが [アクティブ（Active）] に変更されるまで、画面を更新します。

関連情報：

- Secure Device Connector のトラブルシュート
- デバイスと SDC の接続に関するトラブルシューティング

自身の VM 上での Secure Device Connector の展開

デバイスのログイン情報を使用して CDO をデバイスに接続する場合、CDO とデバイス間の通信を管理するために、ネットワークに Secure Device Connector（SDC）をダウンロードして展開することがベストプラクティスです。通常、これらのデバイスは非境界ベースであり、パブリック IP アドレスを持たないか、外部インターフェイスに開かれたポートを持っています。適応型セキュリティアプライアンス（ASA）、Firepower Threat Defense デバイス（FTD）、Firepower Management Center（FMC）、Secure Firewall Cloud Native デバイスはすべて、デバイスのログイン情報を使用して CDO にオンボードできます。

SDC は、管理対象デバイスで実行する必要があるコマンドと、管理対象デバイスに送信する必要があるメッセージについて、CDO を監視します。SDC は、CDO に代わってこのコマンドを実行し、管理対象デバイスに代わって CDO にメッセージを送信し、管理対象デバイスからの応答を CDO に返します。

1 つの SDC が管理できるデバイスの数は、それらのデバイスに実装されている機能と、構成ファイルのサイズによって異なります。ただし、展開計画の目安として、1 つの SDC で約 500 台のデバイスをサポートできることを想定しています。詳細については、単一の CDO テナントで複数の SDC を使用する （27 ページ）を参照してください。

この手順では、独自の仮想マシンイメージを使用してネットワークに SDC をインストールする方法について説明します。

（注） SDC をインストールするために推奨される、最も簡単で信頼できる方法は、CDO の SDC OVA イメージをダウンロードしてインストールすることです。手順については、CDO の VM イメージを使用した Secure Device Connector の展開 （12 ページ） を参照してください。

始める前に

- CDO は、厳密な証明書チェックを必要とし、SDC とインターネットの間の Web/コンテンツプロキシをサポートしていません。
- SDC には TCP ポート 443 でのインターネットへの完全なアウトバウンドアクセスが必要です。
- ネットワークのガイドラインについては、「Cisco Defense Orchestrator の管理対象デバイスへの接続」を参照してください。
- vCenter Web クライアントまたはr ESXi Web クライアントを使用してインストールされた VMware ESXi ホスト。

（注） vSphere デスクトップクライアントを使用したインストールはサポートしていません。

- ESXi 5.1 ハイパーバイザ。
- Cent OS 7 ゲスト オペレーティング システム。
- SDC のみを持つ VM のシステム要件：
  - VMware ESXi ホストには 2 つの CPU が必要です。
  - VMware ESXi ホストには 2 GB 以上のメモリが必要です。
  - VMware ESXi では、プロビジョニングの選択に応じて、仮想マシンをサポートするために 10 GB のディスク容量が必要です。これは、必要に応じてディスク領域を拡張できるように、パーティションで論理ボリューム管理（LVM）を使用していることを想定した値です。
- SDC と Secure Event Connector イメージの両方がインストールされている VM のシステム要件。SEC は、Cisco Security Analytics and Logging で使用されるコンポーネントです。
  - VMware ESXi ホストには 6 つの CPU が必要です。
  - VMware ESXi ホストには 10 GB 以上のメモリが必要です。

- VMware ESXi では、プロビジョニングの選択に応じて、仮想マシンをサポートするために 10 GB のディスク容量が必要です。これは、必要に応じてディスク領域を拡張できるように、パーティションで論理ボリューム管理（LVM）を使用していることを想定した値です。

- CDO コネクタと Secure Event Connector（SEC）の両方がインストールされている VM のシステム要件。
  - CPU：SEC 用に 4 つの CPU を追加します。
  - メモリ：SEC 用 8 GB のメモリを追加します。
- VM の CPU とメモリを更新したら、VM の電源を入れ、[セキュアコネクタ（Secure Connectors）] ページに SDC が「アクティブ」状態であることが示されていることを確認します。
- Linux 環境での操作や vi ビジュアルエディタを使用したファイル編集に慣れ親しんでいるユーザーがこの手順を実行してください。
- オンプレミスの SDC を CentOS 仮想マシンにインストールする場合は、Yum セキュリティパッチを定期的にインストールすることをお勧めします。Yum の更新を取得するための設定に応じて、ポート 443 だけでなくポート 80 でもアウトバウンドアクセスを開く必要がある場合があります。また、更新をスケジュールするために yum-cron または crontab も設定する必要があります。セキュリティ運用チームと連携して、Yum の更新を取得するためにセキュリティポリシーを変更する必要があるかどうかを判断します。

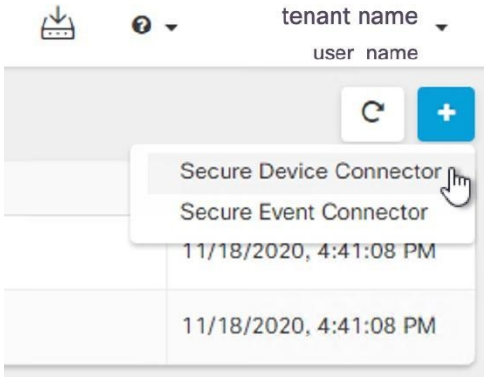
（注） **始める前に**：手順内のコマンドは、コピーして端末ウィンドウに貼り付けるのではなく入力するようにしてください。一部のコマンドに含まれる「n ダッシュ」は、カットアンドペーストのプロセスで「m ダッシュ」として適用される場合があり、コマンドが失敗する原因となります。

手順

ステップ 1 SDC を作成する CDO テナントにログオンします。

ステップ 2 CDO メニューバーから**[管理（Admin）]** > **[セキュアコネクタ（Secure Connectors）]**に移動します。

ステップ 3 [セキュアコネクタ（Secure Connectors）] ページで、青いプラスボタンをクリックし、[Secure Device Connector] を選択します。



ステップ 4 ウィンドウの手順 2 のブートストラップデータをメモ帳にコピーします。

ステップ 5 少なくとも次の RAM とディスク領域が SDC に割り当てられている **CentOS 7 仮想マシン**をインストールします。

- 8 GB の RAM
- 10 GB のディスクスペース

ステップ 6 インストールしたら、SDC の IP アドレス、サブネットマスク、ゲートウェイの指定など、ネットワークの基本設定を行います。

ステップ 7 DNS（ドメインネームサーバー）を設定します。

ステップ 8 NTP（ネットワーク タイム プロトコル）サーバーを設定します。

ステップ 9 SDC の CLI と簡単にやり取りできるように、CentOS に SSH サーバーをインストールします。

ステップ 10 Yum の更新を実行し、**open-vm-tools**、**nettools**、および **bind-utils** パッケージをインストールします。

```
[root@sdc-vm ~]# yum update -y
                 [root@sdc-vm ~]# yum install -y open-vm-tools net-tools bind-utils
```

ステップ 11 AWS CLI パッケージをインストールします。https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.htmlを参照してください。

（注） **--user** フラグは使用しないでください。

ステップ 12 Docker CE パッケージをインストールします。https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ceを参照してください。

（注） 「リポジトリを使用したインストール」方法を使用します。

ステップ 13 Docker サービスを開始し、起動時に開始できるようにします。

```
[root@sdc-vm ~]# systemctl start docker
[root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to
    /usr/lib/systemd/system/docker.service.
```

ステップ 14 「cdo」と「sdc」の 2 つのユーザーを作成します。cdo ユーザーは、管理機能を実行するためにログインするユーザーです（つまり root ユーザーを直接使用する必要はありません）。sdc ユーザーは、SDC docker コンテナを実行するユーザーです。

```
[root@sdc-vm ~]# useradd cdo
[root@sdc-vm ~]# useradd sdc -d /usr/local/cdo
```

ステップ 15 cdo ユーザーのパスワードを設定します。

```
[root@sdc-vm ~]# passwd cdo
Changing password for user cdo.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

ステップ 16 cdo ユーザーを「wheel」グループに追加し、管理者（sudo）権限を付与します。

```
[root@sdc-vm ~]# usermod -aG wheel cdo
[root@sdc-vm ~]#
```

ステップ 17 Docker がインストールされると、ユーザーグループが作成されます。CentOS/Docker のバージョンに応じて、「docker」または「dockerroot」と呼ばれます。/etc/group ファイルでどのグループが作成されたかを確認したら、sdc ユーザーをそのグループに追加します。

```
[root@sdc-vm ~]# grep docker /etc/group
 docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

ステップ 18 /etc/docker/daemon.json ファイルが存在しない場合は作成し、以下の内容を入力します。作成したら、docker デーモンを再起動します。

（注） 「group」キーに入力したグループ名が、前の手順の /etc/group ファイルで見つけたグループと一致していることを確認してください。

```
[root@sdc-vm ~]# cat /etc/docker/daemon.json
        {
           "live-restore": true,
           "group": "docker"
        }
        [root@sdc-vm ~]# systemctl restart docker
        [root@sdc-vm ~]#
```

ステップ 19 現在 vSphere コンソールセッションを使用している場合は、SSH に切り替えて、「cdo」ユーザーでログインします。ログインしたら、「sdc」ユーザーに切り替えます。パスワードの入力を求められたら、「cdo」ユーザーのパスワードを入力します。

```
[cdo@sdc-vm ~]$ sudo su sdc
              [sudo] password for cdo: <type password for cdo user>
              [sdc@sdc-vm ~]$
```

ステップ 20 ディレクトリを **/usr/local/cdo** に変更します。

ステップ 21 bootstrapdata という新しいファイルを作成し、[オンプレミスの Secure Device Connector の展開（Deploy an On-Premises Secure Device Connector）] ウィザードの手順2 のブートストラップデータを、このファイルに貼り付けます。[保存（Save）]をクリックしてファイルを保存します。[vi] または [nano] を使用してファイルを作成できます。

ステップ 22 ブートストラップデータは base64 でエンコードされていますので、復号化して extractedbootstrapdata というファイルにエクスポートします。

```
[sdc@sdc-vm ~]$ base64 -d /usr/local/cdo/bootstrapdata >
/usr/local/cdo/extractedbootstrapdata
             [sdc@sdc-vm ~]$
```

cat コマンドを実行して復号化したデータを表示します。コマンドおよび復号化したデータは次のようになります。

```
[sdc@sdc-vm ~]$ cat /usr/local/cdo/extractedbootstrapdata
              CDO_TOKEN="<token string>"
              CDO_DOMAIN="www.defenseorchestrator.com"
              CDO_TENANT="<tenant-name>"

CDO_BOOTSTRAP_URL="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"
```

ステップ 23 以下のコマンドを実行して、復号化したブートストラップデータの一部を環境変数にエクスポートします。

```
[sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > sdcenv && source sdcenv
             [sdc@sdc-vm ~]$
```

ステップ 24 CDO からブートストラップバンドルをダウンロードします。

```
[sdc@sdc-vm ~]$ curl -O -H "Authorization: Bearer $CDO_TOKEN" "$CDO_BOOTSTRAP_URL"
              100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
              [sdc@sdc-vm ~]$ ls -l /usr/local/cdo/*SDC
              -rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/cdo/tenant-name-SDC
```

ステップ 25 SDC tarball を展開し、bootstrap.sh ファイルを実行して SDC パッケージをインストールします。

```
[sdc@sdc-vm ~]$ tar xzvf /usr/local/cdo/tenant-name-SDC
              <snipped - extracted files>
              [sdc@sdc-vm ~]$
              [sdc@sdc-vm ~]$ /usr/local/cdo/bootstrap/bootstrap.sh
              [2018-07-23 13:54:02] environment properly configured
             download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar

              toolkit.sh
              common.sh
              [2018-07-23 13:54:04] startup new container
              Unable to find image 'ciscodefenseorchestrator/sdc_prod:latest' locally
              sha256:d98f17101db10e66db5b5d6afda1c95c29ea0004d9e4315508fd30579b275458:
 Pulling from
              ciscodefenseorchestrator/sdc_prod
              08d48e6f1cff: Pull complete
              ebbd10b629b1: Pull complete
              d14d580ef2ed: Pull complete
              45421d451ab8: Pull complete
              <snipped - downloads>
              no crontab for sdc
```

すると、CDO で SDC が「アクティブ」と表示されるはずです。

次のタスク

- 「デバイスおよびサービスのオンボード」に移動して、CDO で管理するデバイスをオンボードします。
- Secure Event Connector をインストールする場合は、SDC 仮想マシンへの Secure Event Connector のインストールに戻ります。
- テナントに **2 つ以上**の Secure Event Connector をインストールする場合は、「テナントに複数の SEC をインストールする」に戻ります。

Secure Device Connector の削除

警告 この手順により、Secure Device Connector（SDC）が削除されます。この操作は元に戻せません。この操作を行った後は、新しい SDC をインストールしてデバイスを再接続するまで、その SDC に接続されているデバイスを管理できなくなります。デバイスを再接続するには、再接続が必要なデバイスごとに管理者ログイン情報を再入力する必要がある場合があります。

テナントから SDC を削除するには、次の手順を実行します。

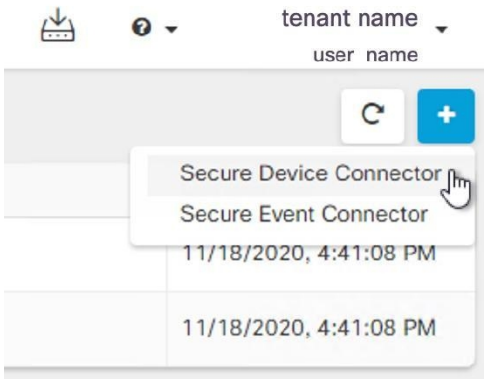
手順

ステップ 1 削除する SDC に接続されているデバイスをすべて削除します。

1. SDC で使用されるすべてのデバイスを特定するには、「同一 SDC を使用した CDO に接続するすべてのデバイスを見つける」を参照してください。同一 SDC を使用した CDO に接続するすべてのデバイスを見つける （27 ページ）
2. [インベントリ（Inventory）] ページで、識別したすべてのデバイスを選択します。
3. [デバイス アクション（Device Actions）] ウィンドウで [削除（Remove）] をクリックし、[OK] をクリックして操作を確定します。

ステップ 2 CDO メニューバーから**[管理（Admin）] > [セキュアコネクタ（Secure Connectors）]**に移動します。

ステップ 3 [セキュアコネクタ（Secure Connectors）] ページで、青いプラスボタンをクリックし、[Secure Device Connector] を選択します。



ステップ 4 [セキュアコネクタ（Secure Connectors）] テーブルで、削除する SDC を選択します。これで、デバイス数はゼロになっているはずです。

ステップ 5 操作ウィンドウで、[削除（Remove）] をクリックします。次の警告が表示されます。

警告 <sdc_name> を削除しようとしています。SDC の削除は元に戻せません。SDC を削除すると、デバイスをオンボーディングまたは再オンボーディングする前に、新しい SDC を作成してオンボーディングする必要があります。

現在オンボーディング済み のデバイスがあるため、SDC を削除するには、これらのデバイスを再接続し、新しい SDC を設定した後にログイン情報を再度入力する必要があります。

- ご質問や懸念事項がある場合は、[キャンセル（Cancel）] をクリックして、CDO サポートにお問い合わせください。
- 続行するには、下のテキストボックスに <sdc_name> を入力して、[OK] をクリックします。

ステップ 6 続行する場合は、警告メッセージに記載されている SDC の名前を確認ダイアログ ボックスに入力します。

ステップ 7 [OK] をクリックして、SDC の削除を確定します。

ある SDC から別の SDC への ASA の移動

CDO では、単一の CDO テナントで複数の SDC を使用する。次の手順を使用して、管理対象 ASA を、ある SDC から別の SDC に移動できます。

手順

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（Device）] タブをクリックしてから、[ASA] タブをクリックします。

ステップ 3 別の SDC に移動する 1 つ以上の ASA を選択します。

ステップ 4 [デバイスアクション（Device Actions）] ペインで、[資格情報の更新（Update Credentials）] をクリックします。

ステップ 5 [セキュアデバイスコネクタ（Secure Device Connector）] ボタンをクリックし、デバイスの移動先の SDC を選択します。

ステップ 6 CDO がデバイスにログインするために使用する管理者のユーザー名とパスワードを入力し、[更新（Update）] をクリックします。変更されていない限り、管理者のユーザー名とパスワードは、ASA のオンボードに使用したログイン情報と同じです。これらの変更をデバイスに展開する必要はありません。

（注） すべての ASA が同じログイン情報を使用している場合、複数の ASA を、ある SDC から別の SDC に一括で移動できます。複数の ASA のログイン情報が異なる場合、各 ASA をある SDC から別の SDC に 1つずつ移動する必要があります。

Firepower の接続ログイン情報の更新

Meraki ダッシュボードから新しい API キーを生成する場合は、CDO で接続ログイン情報を更新する必要があります。新しいキーを生成する詳細については、Meraki API キーの生成と取得を参照してください。CDO では、デバイス自体の接続ログイン情報を更新することはできません。必要に応じて、Meraki ダッシュボードで API キーを手動で更新できます。ログイン情報を更新して通信を再確立するには、CDO UI で API キーを手動で更新する必要があります。

（注） CDO がデバイスの同期に失敗した場合、CDO の接続ステータスに [無効なログイン情報（Invalid Credentials）] と表示されることがあります。その場合は、API キーを使用しようとした可能性があります。選択した Meraki MX の API キーが正しいことを確認します。

次の手順を使用して、Meraki MX デバイスのログイン情報を更新します。

手順

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（Device）] タブをクリックしてから、[Meraki] タブをクリックします。

ステップ 3 接続ログイン情報を更新する Meraki MX を選択します。

ステップ 4 [デバイスアクション（Device Actions）] ペインで、[ログイン情報の更新（Update Credentials）] をクリックします。

ステップ 5 CDO がデバイスにログインするために使用する **API キー**を入力し、[更新（Update）] をクリックします。この API キーは、変更されていない限り、Meraki MX のオンボードに使用したのと同じログイン情報です。これらの変更をデバイスに展開する必要はありません。

Secure Device Connector の名前変更

手順

ステップ 1 CDO メニューバーから [管理（Admin）] > [セキュアコネクタ（Secure Connectors）] に移動します。

ステップ 2 名前を変更する SDC を選択します。

ステップ 3 詳細ペインで、SDC の名前の横にある編集アイコン をクリックします。

ステップ 4 SDC の名前を変更します。

この新しい名前は、[インベントリ（Inventory）] ペインの Secure Device Connector フィルタなど、CDO インターフェイス内の SDC 名が表示される場所に表示されます。

Secure Device Connector の更新

この手順は、トラブルシューティング ツールとして使用してください。通常、SDC は自動的に更新されるため、この手順を使用する必要はありません。ただし、VM の時刻設定が正しくない場合、SDC は AWS への接続を確立して更新を受信できませんが、この手順により、SDC の更新が開始され、時刻同期の問題によるエラーが解決されます。

手順

ステップ 1 SDC に接続します。SSH を使用して接続するか、VMware Hypervisor のコンソールビューを使用できます。

ステップ 2 **cdo** ユーザーとして SDC にログインします。

ステップ 3 SDC ユーザーに切り替えて、SDC Docker コンテナを更新します。

```
[cdo@sdc-vm ~]$ sudo su sdc
                [sudo] password for cdo: <type password for cdo user>
                [sdc@sdc-vm ~]$
```

ステップ 4 SDC ツールキットをアップグレードします。

```
[cdo@sdc-vm ~]$ /usr/local/cdo/toolkit/toolkit.sh upgradeToolkit
                [sdc@sdc-vm ~]$
```

ステップ 5 SDC をアップグレードします。

```
[cdo@sdc-vm ~]$ /usr/local/cdo/toolkit/toolkit.sh upgradeSDC
                [sdc@sdc-vm ~]$
```

単一の CDO テナントで複数の SDC を使用する

テナントに複数の SDC を展開すると、パフォーマンスを低下させることなく、より多くのデバイスを管理できます。1 つの SDC が管理できるデバイスの数は、それらのデバイスに実装されている機能と、構成ファイルのサイズによって異なります。

テナントにインストールできる SDC の数に制限はありません。各 SDC は 1 つのネットワークセグメントを管理できます。これらの SDC は、それらのネットワークセグメント内のデバイスを同一の CDO テナントに接続します。複数の SDC がない場合、隔離されたネットワークセグメント内のデバイスを、異なる CDO テナントで管理する必要があります。

2 番目以降の SDC を展開する手順は、最初の SDC を展開する手順と同じです。CDO の VM イメージを使用した Secure Device Connector の展開か、自身の VM 上での Secure Device Connector の展開ことができます。テナントの最初の SDC には、テナントの名前と番号 1 が組み込まれています。追加の各 SDC には、順番に番号が付けられます。

同一 SDC を使用した CDO に接続するすべてのデバイスを見つける

次の手順に従って、同じ SDC を使用して CDO に接続するすべてのデバイスを識別します。

手順

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 フィルタ基準がすでに指定されている場合は、インベントリテーブルの上部にある [クリア（Clear）] ボタンをクリックして、CDO で管理しているすべてのデバイスとサービスを表示します。

ステップ 5 フィルタボタン をクリックして、[フィルタ（Filter）] メニューを展開します。フィルタ（93 ページ）

ステップ 6 フィルタの [Secure Device Connector] セクションで、必要な SDC の名前をクリックします。インベントリテーブルには、フィルタでチェックした SDC を使用して CDO に接続しているデバイスのみが表示されます。

ステップ 7 （オプション）検索をさらに絞り込むには、フィルタメニューで追加のフィルタをチェックします。

ステップ 8 （オプション）完了したら、インベントリテーブルの上部にある [クリア（Clear）] ボタンをクリックして、CDO で管理しているすべてのデバイスとサービスを表示します。

Secure Device Connector オープンソースおよびサードパーティライセンス属性

==========

*** amqplib ***

amqplib copyright (c) 2013, 2014

Michael Bridgen <mikeb@squaremobius.net>

This package, "amqplib", is licensed under the MIT License. A copy maybe found in the file LICENSE-MIT in this directory, or downloaded from

http://opensource.org/licenses/MIT

==========

*** async ***

Copyright (c) 2010-2016 Caolan McMahon

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files（the "Software"）, to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** bluebird ***

The MIT License（MIT）

Copyright (c) 2013-2015 Petka Antonov

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files（the "Software"）, to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF

MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** cheerio ***

Copyright (c) 2012 Matt Mueller <mattmuelle@gmail.com>

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the 'Software'), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED 'AS IS', WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** command-line-args ***

The MIT License (MIT)

Copyright (c) 2015 Lloyd Brookes <75pound@gmail.com>

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files（the "Software"）, to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** ip ***

This software is licensed under the MIT License.

Copyright Fedor Indutny, 2012.

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files（the "Software"）, to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** json-buffer ***

Copyright (c) 2013 Dominic Tarr

Permission is hereby granted, free of charge,to any person obtaining a copy of this software andassociated documentation files (the "Software"), todeal in the Software without restriction, includingwithout limitation the rights to use, copy, modify,merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whomthe Software is furnished to do so,subject to the following conditions:

The above copyright notice and this permission noticeshall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIESOF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FORANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THESOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

*** json-stable-stringify ***

This software is released under the MIT license:

Permission is hereby granted, free of charge, to any person obtaining a copy ofthis software and associated documentation files (the "Software"), to deal inthe Software without restriction, including without limitation the rights touse, copy, modify, merge, publish, distribute, sublicense, and/or sell copies ofthe Software, and to permit persons to whom the Software is furnished to do so,subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESSFOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS ORCOPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHERIN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR INCONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

*** json-stringify-safe ***

The ISC License

Copyright (c) Isaac Z. Schlueter and Contributors

Permission to use, copy, modify, and/or distribute this software for anypurpose with or without fee is hereby granted, provided that the abovecopyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIESWITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OFMERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FORANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGESWHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN ANACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF ORIN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

==========

*** lodash ***

Copyright JS Foundation and other contributors <https://js.foundation/>

Based on Underscore.js, copyright Jeremy Ashkenas,

DocumentCloud and Investigative Reporters & Editors<http://underscorejs.org/>

This software consists of voluntary contributions made by manyindividuals. For exact contribution history, see the revision historyavailable at https://github.com/lodash/lodash

The following license applies to all parts of this software except as

documented below:

====

Permission is hereby granted, free of charge, to any person obtaininga copy of this software and associated documentation files（the"Software"）, to deal in the Software without restriction, includingwithout limitation the rights to use, copy, modify, merge, publish,distribute, sublicense, and/or sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

The above copyright notice and this permission notice shall beincluded in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OFMERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE

ANDNONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BELIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTIONOF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTIONWITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

====

Copyright and related rights for sample code are waived via CC0. Samplecode is defined as all source code displayed within the prose of thedocumentation.

CC0: http://creativecommons.org/publicdomain/zero/1.0/

====

Files located in the node_modules and vendor directories are externallymaintained libraries used by this software which have their ownlicenses; we recommend you read them, as their terms may differ from theterms above.

==========

*** log4js ***

Copyright 2015 Gareth Jones (with contributions from many other people)

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions andlimitations under the License.

==========

*** mkdirp ***

Copyright 2010 James Halliday (mail@substack.net)

This project is free software released under the MIT/X11 license:

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files（the "Software"）, to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** node-forge ***

New BSD License (3-clause)

Copyright (c) 2010, Digital Bazaar, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or withoutmodification, are permitted provided that the following conditions are met:

*** Redistributions of source code must retain the above copyrightnotice, this list of conditions and the following disclaimer.**

*** Redistributions in binary form must reproduce the above copyrightnotice, this list of conditions and the following disclaimer in thedocumentation and/or other materials provided with the distribution.**

*** Neither the name of Digital Bazaar, Inc. nor thenames of its contributors may be used to endorse or promote productsderived from this software without specific prior written permission.**

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" ANDANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIEDWARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AREDISCLAIMED. IN NO EVENT SHALL DIGITAL BAZAAR BE LIABLE FOR ANYDIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED ANDON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THISSOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

*** request ***

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

==========

*** rimraf ***

The ISC License

Copyright (c) Isaac Z. Schlueter and Contributors

Permission to use, copy, modify, and/or distribute this software for anypurpose with or without fee is hereby granted, provided that the abovecopyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIESWITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OFMERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FORANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGESWHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN ANACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF ORIN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

==========

*** uuid ***

Copyright (c) 2010-2012 Robert Kieffer

MIT License - http://opensource.org/licenses/mit-license.php

==========

*** validator ***

Copyright (c) 2016 Chris O'Hara <cohara87@gmail.com>

Permission is hereby granted, free of charge, to any person obtaininga copy of this software and associated documentation files（the"Software"）, to deal in the Software without restriction, includingwithout limitation the rights to use, copy, modify, merge, publish,distribute, sublicense, and/or sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

The above copyright notice and this permission notice shall beincluded in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OFMERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE ANDNONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BELIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTIONOF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTIONWITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

*** when ***

Open Source Initiative OSI - The MIT License

CDO へのサインイン

Cisco Defense Orchestrator（CDO）にログインするには、SAML 2.0 準拠の ID プロバイダー（IdP）、多要素認証プロバイダー、および ユーザ管理を持つアカウントが必要です。

IdP アカウントにはユーザーのログイン情報が含まれており、IdP はそのログイン情報に基づいてユーザーを認証します。多要素認証では、アイデンティティセキュリティの付加的なレイヤが提供されます。CDO ユーザーレコードには、主にユーザー名、ユーザーが関連付けられる CDO テナント、ユーザーのロールが含まれます。ユーザーがログインすると、CDO は IdP のユーザー ID を CDO のテナントの既存ユーザーレコードにマッピングします。CDO が一致するレコードを見つけた場合に、該当するユーザーはそのテナントへのログインを許可されます。

お客様の企業に独自のシングルサインオン ID プロバイダーがない限り、ID プロバイダーは Cisco Secure Sign-on です。Cisco Secure Sign-On は、多要素認証に Duo を使用します。顧客は、必要に応じてSAML シングルサインオンと Cisco Defense Orchestrator の統合できます。

Cisco Defense Orchestrator（CDO）にログインするには、まず Cisco Secure Sign-On でアカウントを作成し、Duo Security を使用して多要素認証（MFA）を設定し、テナントのネットワーク管理者に CDO レコードの作成を依頼する必要があります。

2019 年 10 月 14 日、CDO は、既存のすべてのテナントを、ID プロバイダーとして Cisco Secure Sign-On を使用し、MFA に Duo を使用するように変換しました。

（注）

- 独自のシングルサインオン ID プロバイダーを使用して CDO にサインインする場合、Cisco Secure Sign-On および Duo への移行の影響はありません。独自のサインオンソリューションを引き続き使用できます。
- CDO の無料試用期間中であれば、この移行の影響はあります。

CDO テナントが 2019 年 10 月 14 日以降に作成された場合は、「新規 CDO テナントへの初回ログイン （38 ページ）」を参照してください。

2019 年 10 月 14 日より前に CDO テナントが存在していた場合は、「Cisco Secure Sign-On ID プロバイダーへの移行 （39 ページ）」を参照してください。

新規 CDO テナントへの初回ログイン

Cisco Defense Orchestrator（CDO）は、Cisco Secure Sign-On をアイデンティティ プロバイダーとして使用し、多要素認証（MFA）に Duo を使用します。**CDO にログインするには、まず Cisco Secure Sign-On でアカウントを作成し、Duo を使用して MFA を設定する必要があります。**

CDO には MFA が必要です。MFA は、ユーザーアイデンティティを保護するためのセキュリティを強化します。MFA の一種である二要素認証では、CDO にログインするユーザーの ID を確認するために、2 つのコンポーネントまたは要素が必要です。最初の要素はユーザー名とパスワードで、2 番目の要素はオンデマンドで生成されるワンタイムパスワード（OTP）です。

重要 **2019 年 10 月 14 日より前に CDO テナントが存在していた場合は、**この項目の代わりに Cisco Secure Sign-On ID プロバイダーへの移行 （39 ページ） をログイン手順として使用してください。

はじめる前に

Duo Security のインストール。Duo Security アプリケーションを携帯電話にインストールすることをお勧めします。Duo のインストールについてご質問がある場合は、『Duo Guide to Two Factor Authentication：Enrollment Guide』を参照してください。

時刻の同期。モバイルデバイスを使用してワンタイムパスワードを生成します。OTP は時間ベースであるため、デバイスのクロックがリアルタイムと同期していることが重要です。デバイスのクロックが自動的に、または手動で正しい時刻に設定されていることを確認します。

次の手順

新規 Cisco Secure Sign-On アカウントの作成と Duo 多要素認証の設定 （70 ページ） に進みます。これは 4 段階のプロセスです。4 段階すべてを完了する必要があります。

ログインの失敗のトラブルシューティング

正しくない CDO リージョンに誤ってログインしているため、ログインに失敗する

適切な CDO リージョンにログインしていることを確認してください。
https://sign-on.security.cisco.com にログインすると、アクセスするリージョンを選択できます。[CDO] タイルをクリックして defenseorchestrator.com にアクセスするか、[CDO (EU)] をクリックして defenseorchestrator.eu にアクセスします。

Cisco Secure Sign-On ID プロバイダーへの移行

2019 年 10 月 14 日時点で、Cisco Defense Orchestrator（CDO）では、すべてのテナントが ID プロバイダーとして Cisco Secure Sign-On に変換されており、多要素認証（MFA）には Duo を使用しています。**CDO にログインするには、まず Cisco Secure Sign-On でアカウントをアクティブ化し、Duo を使用して MFA を設定する必要があります。**

CDO には MFA が必要です。MFA は、ユーザーアイデンティティを保護するためのセキュリティを強化します。MFA の一種である二要素認証では、CDO にログインするユーザーの ID を確認するために、2 つのコンポーネントまたは要素が必要です。最初の要素はユーザー名とパスワードで、2 番目の要素はオンデマンドで生成されるワンタイムパスワード（OTP）です。

（注）

- 独自のシングルサインオン ID プロバイダーを使用して CDO にサインインする場合、この Cisco Secure Sign-On および Duo への移行は影響しません。独自のサインオンソリューションを引き続き使用します。
- CDO の無料トライアル期間中であれば、この移行が適用されます。
- **2019 年 10 月 14 日以降に CDO テナントが作成されていた場合は、**この記事の代わりに 新規 CDO テナントへの初回ログイン （38 ページ） をログイン手順として使用してください。

はじめる前に

移行する前に、次の手順を実行することを強くお勧めします。

- **Duo Security のインストール。**Duo Security アプリケーションを携帯電話にインストールすることをお勧めします。Duo のインストールについてご質問がある場合は、『Duo Guide to Two Factor Authentication：Enrollment Guide』を参照してください。
- **時刻の同期。**モバイルデバイスを使用してワンタイムパスワードを生成します。OTP は時間ベースであるため、デバイスのクロックがリアルタイムと同期していることが重要です。デバイスのクロックが自動的に、または手動で正しい時刻に設定されていることを確認します。

- 新しい Cisco Secure Sign-On アカウントを作成し、Duo 多要素認証を設定します。これは 4 段階のプロセスです。4 段階すべてを完了する必要があります。

次の作業

新規 Cisco Secure Sign-On アカウントの作成と Duo 多要素認証の設定 （70 ページ）

移行後のログイン失敗のトラブルシューティング

ユーザー名またはパスワードが正しくないため、CDO へのログインに失敗する

解決法 CDO にログインしようとして、正しいユーザー名とパスワードを使用しているにもかかわらずログインに失敗する場合、または「パスワードを忘れた場合」を試しても有効なパスワードを回復できない場合は、新しい Cisco Secure Sign-On アカウントを作成せずにログインを試みた可能性があります。新規 Cisco Secure Sign-On アカウントの作成と Duo 多要素認証の設定 （70 ページ） の手順に従って、新しい Cisco Secure Sign-On アカウントにサインアップする必要があります。

Cisco Secure Sign-On ダッシュボードへのログインは成功するが、CDO を起動できない

解決法 CDO アカウントとは異なるユーザー名で Cisco Secure Sign-On アカウントを作成している可能性があります。CDO と Cisco Secure Sign-On の間でユーザー情報を標準化するには、Cisco Technical Assistance Center（TAC）に連絡してください。http://cdo.support@cisco.com

保存したブックマークを使用したログインに失敗する

解決法 ブラウザに保存された古いブックマークを使用してログインしようとしているかもしれません。ブックマークが https://cdo.onelogin.com を指している可能性があります。

解決法 https://sign-on.security.cisco.com にログインします。

- **解決法** Cisco Secure Sign-On アカウントをまだ作成していない場合は、新規 Cisco Secure Sign-On アカウントの作成と Duo 多要素認証の設定します。
- **解決法** 新しいアカウントを作成している場合は、ダッシュボードで Cisco Defense Orchestrator（米国）、Cisco Defense Orchestrator（欧州）、または Cisco Defense Orchestrator（アジア太平洋/日本/中国）に対応する CDO タイルをクリックします。
- **解決法** https://sign-on.security.cisco.com を指すようにブックマークを更新します。

Cisco Secure Sign-On ダッシュボードからの CDO の起動

手順

ステップ 1 Cisco Secure Sign-on ダッシュボードで適切な [CDO] ボタンをクリックします。[CDO] タイルをクリックすると https://defenseorchestrator.com に移動し、[CDO（EU）] タイルをクリックすると https://defenseorchestrator.eu に移動します。

ステップ 2 両方のオーセンティケータを設定している場合は、オーセンティケータのロゴをクリックして [Duo Security] か [Google Authenticator] を選択します。

- 既存のテナントにすでにユーザーレコードがある場合は、そのテナントにログインします。
- 複数のポータルにすでにユーザーレコードがある場合は、接続するポータルを選択できます。
- すでに複数のテナントにユーザーレコードがある場合は、接続先の CDO テナントを選択できます。
- 既存のテナントにユーザーレコードがない場合は、CDO の詳細を確認するか、またはトライアルアカウントを要求できます。

[ポータル（Portals）] ビューは、複数のテナントから統合された情報を取得して表示します。詳細については、マルチテナントポータルの管理 （58 ページ）を参照してください。

[テナント（Tenant）] ビューには、ユーザーレコードがある一部のテナントが表示されます。

テナントのネットワーク管理者の管理

テナントのネットワーク管理者の数を制限することを、ベストプラクティスとしてお勧めします。ネットワーク管理者権限を持つユーザーを決定し、[ユーザー管理（User Management）] ユーザ管理 （63 ページ）を確認して、他のユーザーの役割を「管理者」に変更します。

CDO でサポートされるソフトウェアとハードウェア

CDO のドキュメントでは、サポートするソフトウェアとデバイスについて説明しています。CDO がサポートしていないソフトウェアやデバイスについては触れていません。ソフトウェアのバージョンまたはデバイスタイプのサポートを明示的に記載していない場合、それはサポートされません。

関連情報：

- Firepower Threat Defense のサポートの詳細 （42 ページ）
- ブラウザ サポート （44 ページ）

Firepower Threat Defense のサポートの詳細

Firepower Threat Defense（FTD）は、シスコの次世代ファイアウォールです。次世代ファイアウォールサービスと ASA プラットフォームの長所が融合されており、さまざまな ASA および Firepower ハードウェアデバイスや仮想マシンにインストールできます。

サポートしている機能の詳細については、『Managing FTD with Cisco Defense Orchestrator』[英語] を参照してください。導入の前提条件と要件の詳細については、「FTD デバイスの導入準備」を参照してください。

（注） Snort 3 は、バージョン 6.7 以降を実行している FTD デバイスで使用できます。Snort 2 と Snort 3 は自由に切り替えることができますが、互換性がない設定のリスクがあることに注意してください。Snort 3、サポートされているデバイスとソフトウェア、および制限の詳細については、「Snort 3.0 へのアップグレード」を参照してください。

CDO でサポートされる Firepower Threat Defense ハードウェアおよびソフトウェアイメージ

次の表の CDO 列は、CDO がサポートする Firepower Threat Defense ソフトウェアのバージョンとハードウェア プラットフォームを示しています。

表 *2: FTD* マネージャとバージョン別のハードウェア

デバイスのプラットフォーム	デバイスバージョン：**FMC** 管理対象	デバイスバージョン：**FDM** 管理対象	デバイスバージョン：**CDO** 管理対象
Firepower 1010、1120、1140	6.4.0 以降	6.4.0 以降	6.4.0 以降
Firepower 1150	6.5.0 以降	6.5.0 以降	6.5.0 以降
Firepower 2110、2120、2130、2140	6.2.1 以降	6.2.1 以降	6.4.0 以降

デバイスのプラットフォーム	デバイスバージョン：FMC 管理対象	デバイスバージョン：FDM 管理対象	デバイスバージョン：CDO 管理対象
Secure Firewall 3110、3120、3130、3140	7.1.0+	7.1.0+	7.1.0+
Firepower 4110、4120、4140	6.0.1 以降	6.5.0 以降	6.5.0 以降
Firepower 4150	6.1.0 以降	6.5.0 以降	6.5.0 以降
Firepower 4115、4125、4145	6.4.0 以降	6.5.0 以降	6.5.0 以降
Firepower 4112	6.6.0 +	6.6.0 +	6.6.0 +
Firepower 9300：SM-24、SM-36、SM-44	6.0.1 以降	6.5.0 以降	6.5.0 以降
Firepower 9300：SM-40、SM-48、SM-56	6.4.0 以降	6.5.0 以降	6.5.0 以降
ISA 3000	6.2.3 以降	6.2.3 以降	6.4.0 以降
ASA 5506-X、5506H-X、5506W-X	6.0.1 ～ 6.2.3	6.1.0 ー 6.2.3	—
ASA 5508-X、5516-X	6.0.1 ～ 7.0.x	6.4.0 ～ 7.0.x	6.4.0 ～ 7.0.x
ASA 5512-X	6.0.1 ～ 6.2.3	6.1.0 ー 6.2.3	—
ASA 5515-X	6.0.1 ー 6.4.0	6.1.0 ー 6.4.0	6.4.0
ASA 5525-X、5545-X、5555-X	6.0.1 ー 6.6.x	6.1.0 ー 6.6.x	6.4.0 ～ 6.6.x

CDO でサポートされる Firepower Threat Defense 仮想マシンプラットフォームおよびソフトウェアイメージ

次の表の CDO 列は、CDO がサポートする Firepower Threat Defense ソフトウェアのバージョンと仮想デバイスプラットフォームを示しています。

表 *3 : FTDv* マネージャとバージョン別

デバイスのプラットフォーム	デバイスバージョン：FMC 管理対象	デバイスバージョン：FDM 管理対象	デバイスバージョン：CDO 管理対象
AWS 用 FTDv	6.0.1 以降	6.6.0 +	6.6.0 +
Azure 用 FTDv	6.2.0 以降	6.5.0 以降	6.5.0 以降

デバイスのプラットフォーム	デバイスバージョン：**FMC** 管理対象	デバイスバージョン：**FDM** 管理対象	デバイスバージョン：**CDO** 管理対象
GCP 用 FTDv	6.7.0 以降	—	—
HyperFlex 用 FTDv	7.0.0 以降	7.0.0 以降	7.0.0 以降
KVM 用 FTDv	6.1.0 以降	6.2.3 以降	6.4.0 以降
Nutanix 用FTDv	7.0.0 以降	7.0.0 以降	7.0.0 以降
OCI 用 FTDv	6.7.0 以降	—	—
OpenStack 用 FTDv	7.0.0 以降	—	—
FTDv VMware の場合	6.0.1 以降	6.2.2 以降	6.4.0 以降

CDO を使用した Firepower デバイスインターフェイスの管理の詳細については、「Firepower インターフェイス設定に関する注意事項と制約事項」を参照してください。

ASA FirePOWER サービスモジュール

CDO は ASA FirePOWER サービスモジュールをサポートしてい**ません**。

ブラウザ サポート

CDO は、次のブラウザの最新バージョンをサポートしています。

- Google Chrome
- Mozilla Firefox

テナント管理

Cisco Defense Orchestrator（Defense Orchestrator）を使用すると、[設定（Settings）] ページでテナントおよび個々のユーザーアカウントの特定の側面をカスタマイズできます。CDO メニューバーから**[管理（Admin）] > [全般設定（General Settings）]**に移動します。

関連情報：

- 全般設定 （45 ページ）
- ユーザ管理
- ロギングの設定
- 通知設定 （49 ページ）

全般設定

CDO メニューバーから**[管理（Admin）] > [全般設定（General Settings）]**に移動します。

一般的な CDO 設定に関する次のトピックを参照してください。

- ユーザー設定 （45 ページ）
- マイトークン（My Tokens）については、API トークン （55 ページ）を参照してください。
- [テナント設定（Tenant Settings）] については、以下を参照してください。
  - 変更リクエストのトラッキングの有効化 （45 ページ）
  - シスコサポートによるテナントの表示の防止 （46 ページ）
  - 自動展開をスケジュールするオプションを有効にする （47 ページ）
  - デフォルトの競合検出間隔 （46 ページ）
  - Web 分析 （48 ページ）
  - デフォルトの定期バックアップスケジュールの設定 （48 ページ）
  - テナント ID （49 ページ）
  - テナント名 （49 ページ）

ユーザー設定

CDO UI で表示する言語を選択します。この選択は、この変更を行うユーザーにのみ影響します。

マイトークン

詳細については、「API トークン」を参照してください。

テナント設定

変更リクエストのトラッキングの有効化

変更要求トラッキングの有効化は、テナントのすべてのユーザーに影響を及ぼします。変更要求トラッキングを有効にするには、次の手順に従います。

手順

ステップ 1 CDO メニューバーから [管理（Admin）] > [全般設定（General Settings）] に移動します。

ステップ 2 [変更要求トラッキング（Change Request Tracking）] の下のスライダをクリックします。

確認が完了すると、Defense Orchestrator インターフェイスの左下隅と、[変更ログ（Change Log）] の [変更要求（Change Request）] ドロップダウンメニューに、[変更要求（Change Request）] ツールバーが表示されます。

シスコサポートによるテナントの表示の防止

シスコサポートは、ユーザーをテナントに関連付けて、サポートチケットを解決したり、複数の顧客に影響する問題を積極的に修正したりします。ただし、必要に応じて、アカウント設定を変更して、シスコサポートがテナントにアクセスしないようにすることができます。これを行うには、[シスコサポートがこのテナントを表示できないようにする（Prevent Cisco support from viewing this tenant）] の下にあるボタンをスライドして、緑色のチェックマークを表示します。

Cisco サポートにテナントを表示させないようにするには、次の手順に従います。

手順

ステップ 1 CDO メニューバーから**[管理（Admin）] > [全般設定（General Settings）]**に移動します。

ステップ 2 [シスコサポートがこのテナントを表示できないようにする（Prevent Cisco support from viewing this tenant）] の下のスライダーをクリックします。

デバイスの変更を自動承認するオプションの有効化

デバイスの変更の自動承認を有効にすると、Defense Orchestrator はデバイスで直接行われた変更を自動的に承認できます。このオプションを無効のままにするか、後で無効にする場合は、変更を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。

デバイスの変更の自動承認を有効にするには、次の手順に従います。

手順

ステップ 1 CDO メニューバーから**[管理（Admin）] > [全般設定（General Settings）]**に移動します。

ステップ 2 [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）] の下にあるスライダをクリックします。

デフォルトの競合検出間隔

この間隔で、CDO がオンボードデバイスの変更をポーリングする頻度が決まります。この選択は、このテナントで管理されるすべてのデバイスに影響し、いつでも変更できます。

（注） この選択は、1 つまたは複数のデバイスを選択した後、[インベントリ（Inventory）] ページから利用できる [競合検出（Conflict Detection）] オプションを介してオーバーライドできます。

このオプションを設定し、競合検出の新しい間隔を選択するには、次の手順に従います。

手順

ステップ 1 CDO メニューバーから**[管理（Admin）] > [全般設定（General Settings）]**に移動します。

ステップ 2 [デフォルトの競合検出間隔（Default Conflict Detection Interval）] のドロップダウンメニューをクリックし、時間の値を選択します。

自動展開をスケジュールするオプションを有効にする

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。有効にすると、一回限りまたは繰り返しの自動展開をスケジュールできます。自動展開をスケジュールするには、「自動展開のスケジュール」を参照してください。

デバイスの Defense Orchestrator で行われた変更は、デバイス自体 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ないことに注意してください。デバイスが [競合検出（Conflict Detected）] または [非同期（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。

[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。

重要 Defense Orchestrator UI 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**。

自動展開をスケジュールするオプションを有効にするには、次の手順に従います。

手順

ステップ 1 CDO メニューバーから**[管理（Admin）] > [全般設定（General Settings）]**に移動します。

ステップ 2 [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）] の下のスライダをクリックします。

Web 分析

Web分析により、ページのヒット数に基づいて匿名の製品使用情報がシスコに提供されます。情報には、表示したページ、ページで費やした時間、ブラウザのバージョン、製品バージョン、デバイスのホスト名などが含まれます。この情報は、シスコが機能の使用状況パターンを確認し、製品を改善するのに使用されます。すべての使用状況データは匿名で、センシティブデータは送信されません。

Web 分析はデフォルトで有効になっています。Web 分析を無効にする、または今後有効にするには、次の手順に従います。

手順

ステップ 1 CDO メニューバーから**[管理（Admin）]** > **[全般設定（General Settings）]**に移動します。

ステップ 2 [Web 分析（Web Analytics）] の下にあるスライダをクリックします。

デフォルトの定期バックアップスケジュールの設定

デバイス間でバックアップスケジュールの一貫性を保つために、この設定を使用して、独自のデフォルト バックアップ スケジュールを設定できます。特定のデバイスのバックアップをスケジュールするときは、デフォルト設定を使用することも、変更することもできます。デフォルトの定期バックアップスケジュールを変更しても、既存のスケジュールされたバックアップまたは定期バックアップスケジュールは変更されません。

手順

ステップ 1 [頻度（Frequency）] フィールドで、 [日次（Daily）]、[週次（Weekly）]、または [月次（Monthly）] を選択します。

ステップ 2 バックアップを実行する時間を 24 時間制で選択します。協定世界時（UTC）で時間をスケジュールすることに注意してください。

- 週次バックアップの場合：バックアップを実行する曜日をチェックします。
- 月次バックアップの場合：[日付（Days of Month）] フィールドをクリックして、バックアップをスケジュールする日付を追加します。注：31 日を入力しても、その月に 31 日が含まれていない場合、バックアップは行われません。スケジュールしたバックアップの時間に名前と説明を付けます。

ステップ 3 [保存（Save）] をクリックします。

詳細については、「単一FTDの定期バックアップスケジュールの設定」を参照してください。

テナント ID

テナント ID によってテナントが識別されます。この情報は、Cisco Technical Assistance Center（TAC）に連絡する必要があるときに役立ちます。

テナント名

テナント名は、テナントも識別します。テナント名は組織名ではないことに注意してください。この情報は、Cisco Technical Assistance Center（TAC）に連絡する必要があるときに役立ちます。

通知設定

テナントに関連付けられたデバイスで特定のアクションが発生するたびに、CDOから電子メール通知を受け取るように登録できます。それらの通知はテナントに関連付けられたすべてのデバイスに適用されますが、すべてのデバイスタイプが使用可能なすべてのオプションをサポートしているわけではありません。また、以下にリストされている CDO 通知に加えられた変更は、リアルタイムで自動的に更新され、展開を必要としないことに注意してください。

CDOからの電子メール通知には、アクションのタイプと影響を受けるデバイスが示されます。デバイスの現在の状態とアクションの内容の詳細については、CDO にログインし、影響を受けるデバイスの変更ログを調べることをお勧めします。

CDO メニューバーから**[管理（Admin）]** > **[通知設定（Notification Settings）]**に移動します。

デバイスワークフローのアラートの送信

（注） これらの設定を変更するか、手動で通知を登録するには、**ネットワーク管理者**ユーザーロールが必要です。詳細については、「ユーザの役割」を参照してください。

通知が必要なすべてのデバイス ワークフロー シナリオを必ず確認してください。次のいずれかのアクションについて、[デバイスワークフロー（Device Workflow）] を手動で確認します。

- [展開（Deployments）]：このアクションには、SSH または IOS デバイスの統合インスタンスは含まれません。
- [バックアップ（Backups）]：このアクションは FTD デバイスにのみ適用されます。
- [アップグレード（Upgrades）]：このアクションは、ASA および FTD デバイスにのみ適用されます。
- [FTDマネージャの変更（Change FTD Manager）]：このアクションは、FTD

  デバイスマネージャを FMC から CDO に変更すると適用されます。

デバイスイベントのアラートの送信

（注） これらの設定を変更するか、手動で通知を登録するには、**ネットワーク管理者**ユーザーロールが必要です。詳細については、「ユーザの役割」を参照してください。

通知が必要なすべてのデバイス ワークフロー シナリオを必ず確認してください。次のいずれかのアクションについて、[デバイスイベント（Device Events）] を手動で確認します。

- [オフラインになる（Went offline）]：このアクションは、テナントに関連付けられているすべてのデバイスに適用されます。
- [オンラインに戻る（Back online）]：このアクションは、テナントに関連付けられているすべてのデバイスに適用されます。
- [競合検出（Conflict detected）]：このアクションは、テナントに関連付けられているすべてのデバイスに適用されます。
- [HA状態の変更（HA state changed）]：このアクションは、HA またはフェールオーバーペア内のデバイス、現在の状態、および変更前の状態を示します。このアクションは、テナントに関連付けられたすべての HA およびフェールオーバー設定に適用されます。
- [サイト間セッションの切断（Site-to-Site session disconnected）]：このアクションは、テナントで設定されているすべてのサイト間 VPN の設定に適用されます。

サブスクライバ

[アラートを受信するために登録（Subscribe to receive alerts）] トグルを有効にして、テナントログインに関連付けられた電子メールを通知リストに追加します。メーラーリストからメールを削除するには、トグルの選択を解除してグレー表示にします。

特定のユーザーロールは、この設定ページのサブスクリプションアクションへのアクセスが制限されていることに注意してください。**ネットワーク管理者**ユーザーロールを持つユーザーは、電子メールエントリを追加または削除できます。自分以外のユーザーまたは代替の電子メール連絡先を登録済みユーザーのリストに追加するには、  をクリックして電子メールを手動で入力します。

警告 ユーザーを手動で追加する場合は、正しい電子メールアドレスを入力してください。CDO は、テナントに関連付けられている既知のユーザーの電子メールアドレスをチェックしません。

CDO 通知の表示

通知アイコン  をクリックして、テナントで発生した最新のアラートを表示します。CDO UI の通知は、30 日後に通知リストから削除されます。

（注） [アラートの送信時期（Send Alerts When）] セクションでの選択は、CDO UI に表示される通知のタイプに影響します。

サービス統合

メッセージングアプリで着信ウェブフックを有効にし、アプリダッシュボードで直接 CDO 通知を受信します。CDO でこのオプションを有効にするには、選択したアプリで着信ウェブフックを手動で許可し、ウェブフック URL を取得する必要があります。詳細については、「CDO 通知用サービス統合の有効化」を参照してください。

CDO 通知用サービス統合の有効化

サービス統合を有効にして、指定されたメッセージングアプリケーションまたはサービスを介して CDO 通知を転送します。通知を受信するには、メッセージング アプリケーションから Webhook URL を生成し、CDO の [通知設定（Notification Settings）] ページでその Webhook を CDO に指定する必要があります。

CDO は、サービス統合として Cisco Webex と Slack をネイティブにサポートしています。これらのサービスに送信されるメッセージは、チャネルと自動ボット用に特別にフォーマットされています。

（注） [通知設定（Notification Settings）] ページで選択した通知は、メッセージング アプリケーションに転送されるイベントです。

Webex チームの着信ウェブフック

始める前に

CDO通知は、指定されたワークスペースに表示されるか、自動ボットとしてプライベートメッセージに表示されます。Webex Teams がウェブフックを処理する方法の詳細については、『Webex for Developers』を参照してください。

次の手順を使用して、Webex Teams の着信ウェブフックを許可します。

手順

ステップ 1 Webex Teams アプリケーションを開きます。

ステップ 2 ウィンドウの左下隅にある [アプリ（Apps）] アイコンをクリックします。このアクションにより、推奨ブラウザの新しいタブで Cisco Webex App Hub が開きます。

ステップ 3 検索バーを使用して、[着信ウェブフック（Incoming Webhooks）] を探します。

ステップ 4 [接続（Connect）] を選択します。このアクションにより、OAuth 承認が開かれ、アプリケーションが新しいタブに表示されるようになります。

ステップ 5 [許可（Accept）] を選択します。タブが自動的にアプリケーションの設定ページにリダイレクトされます。

ステップ 6 次を設定します。

- [ウェブフック名（Webhook name）]：このアプリケーションによって提供されるメッセージを識別するための名前を指定します。
- [スペースの選択（Select a space）]：ドロップダウンメニューを使用して [スペース（Space）] を選択します。スペースは Webex Teams に既に存在している必要があります。スペースが存在しない場合は、Webex Teams で新しいスペースを作成できます。アプリケーションの設定ページを更新すると新しいスペースが表示されます。

ステップ 7 [追加（Add）] を選択します。選択した Webex スペースに、アプリケーションが追加されたという通知が送信されます。

ステップ 8 ウェブフック URL をコピーします。

ステップ 9 CDO にログインします。

ステップ 10 右上隅のユーザーメニューを開き、[設定（Settings）] を選択します。

ステップ 11 CDO メニューバーから**[管理（Admin）] > [通知設定（Notification Settings）]**に移動します。

ステップ 12 [サービス統合（Service Integrations）] までスクロールします。

ステップ 13 青色のプラスボタンをクリックします。

ステップ 14 名前を入力します。 この名前は、設定されたサービス統合として CDO に表示されます。設定されたサービスに転送されるイベントには表示されません。

ステップ 15 ドロップダウンメニューを展開し、サービスタイプとして Webex を選択します。

ステップ 16 サービスから生成したウェブフック URL を貼り付けます。

ステップ 17 [OK] をクリックします。

Slack 用の着信ウェブフック

CDO 通知は、指定されたチャネルに表示されるか、自動ボットとしてプライベートメッセージに表示されます。Slack による着信ウェブフックの処理方法の詳細については、「Slack Apps」を参照してください。

次の手順を使用して、Slack の着信ウェブフックを許可します。

手順

ステップ 1 Slack アカウントにログインします。

ステップ 2 左側のパネルで、一番下までスクロールして [アプリの追加（Add Apps）] を選択します。

ステップ 3 [着信ウェブフック（Incoming Webhooks）] のアプリケーション ディレクトリを検索し、アプリを見つけます。[追加（Add）] を選択します。

ステップ 4 Slack ワークスペースの管理者ではない場合、組織の管理者にリクエストを送信し、アプリが自分のアカウントに追加されるのを待つ必要があります。[設定のリクエスト（Request

Configuration）] を選択します。オプションのメッセージを入力し、[リクエストの送信（Submit Request）] を選択します。

ステップ 5 ワークスペースで着信ウェブフックアプリが有効になったら、Slack の設定ページを更新し、[新しいウェブフックをワークスペースに追加（Add New Webhook to Workspace）] を選択します。

ステップ 6 ドロップダウンメニューを使用して、CDO 通知を表示する Slack チャネルを選択し、[承認（Authorize）] を選択します。リクエストが有効になるのを待っている間にこのページから移動した場合は、Slack にログインして、左上隅にあるワークスペース名を選択します。ドロップダウンメニューから [ワークスペースのカスタマイズ（Customize Workspace）] を選択し、[アプリの設定（Configure Apps）] を選択します。**[管理（Manage）]**>**[カスタム統合（Custom Integrations）]** に移動します。[着信ウェブフック（Incoming Webhooks）] を選択してアプリのランディングページを開き、タブから [設定（Settings）] を選択します。このアプリが有効になっているワークスペース内のすべてのユーザーが一覧表示されます。ユーザーはアカウントの設定の表示と編集のみできます。ワークスペース名を選択して設定を編集し、次に進みます。

ステップ 7 Slack の設定ページから、アプリの設定ページにリダイレクトされます。ウェブフック URL を見つけてコピーします。

ステップ 8 CDO にログインします。

ステップ 9 右上隅のユーザーメニューを開き、[設定（Settings）] を選択します。

ステップ 10 CDO メニューバーから**[管理（Admin）]** > **[通知設定（Notification Settings）]**に移動します。

ステップ 11 [サービス統合（Service Integrations）] までスクロールします。

ステップ 12 青色のプラスボタンをクリックします。

ステップ 13 名前を入力します。 この名前は、設定されたサービス統合として CDO に表示されます。設定されたサービスに転送されるイベントには表示されません。

ステップ 14 ドロップダウンメニューを展開し、サービスタイプとして [Slack] を選択します。

ステップ 15 サービスから生成したウェブフック URL を貼り付けます。

ステップ 16 [OK] をクリックします。

カスタム統合用の着信ウェブフック

始める前に

COD は、カスタム統合用にメッセージをフォーマットしません。カスタムサービスまたはアプリケーションの統合を選択した場合、CDO は JSON メッセージを送信します。

着信ウェブフックを有効にしてウェブフック URL を生成する方法については、サービスのマニュアルを参照してください。ウェブフック URL を取得したら、以下の手順を使用してウェブフックを有効にします。

手順

ステップ 1 選択したカスタムサービスまたはアプリケーションからウェブフック URL を生成してコピーします。

ステップ 2 CDO にログインします。

ステップ 3 CDO メニューバーから**[管理（Admin）]** > **[通知設定（Notification Settings）]**に移動します。

ステップ 4 [サービス統合（Service Integrations）] までスクロールします。

ステップ 5 青色のプラスボタンをクリックします。

ステップ 6 名前を入力します。 この名前は、設定されたサービス統合として CDO に表示されます。設定されたサービスに転送されるイベントには表示されません。

ステップ 7 ドロップダウンメニューを展開し、[サービスタイプ（Service Type）] として [カスタム（Custom）] を選択します。

ステップ 8 サービスから生成したウェブフック URL を貼り付けます。

ステップ 9 [OK] をクリックします。

ロギングの設定

毎月のイベントロギングの制限と、制限がリセットされるまでの残り日数を表示します。保存されたロギングは、Cisco Cloud が受信した圧縮されたイベントデータを表すことに注意してください。

[使用履歴の表示（View Historical Usage）] をクリックして、過去 12 か月間にテナントで受信されたすべてのロギングを表示します。

追加のストレージをリクエストするために使用できるリンクもあります。

SAML シングルサインオンと Cisco Defense Orchestrator の統合

Cisco Defense Orchestrator（CDO）は、Cisco Secure Sign-On を SAML シングル サインオン アイデンティティ プロバイダーとして使用し、多要素認証（MFA）に Duo Security を使用します。これは、CDO で推奨される認証方法です。

ただし、顧客が独自の SAML シングルサインオン IdP ソリューションと CDO を統合したい場合、IdP が SAML 2.0 および ID プロバイダーが開始するワークフローをサポートしている限り、それも可能です。

独自の SAML ソリューションを統合する場合は、Cisco Defense Orchestrator サポートにお問い合わせください。

API トークン

開発者は、CDO REST API 呼び出しを行うときに CDO API トークンを使用します。呼び出しを成功させるには、API トークンを REST API 認証ヘッダーに挿入する必要があります。API トークンは、有効期限のない「長期的な」アクセストークンですが、更新したり、取り消したりできます。

CDO 内から API トークンを生成できます。生成されたトークンは、生成直後に、[一般設定（General Settings）] ページが開いている間のみ表示されます。CDO で別のページを開いてから [一般設定（General Settings）] ページに戻ると、トークンが発行されたことはわかりますが、トークンは表示されなくなります。

個々のユーザーは、特定のテナントに対して独自のトークンを作成できます。あるユーザーが別のユーザーに代わってトークンを生成することはできません。トークンはアカウントとテナントのペアに固有であり、他のユーザーとテナントの組み合わせには使用できません。

API トークン形式とクレーム

API トークンは JSON Web トークン（JWT）です。JWT トークン形式の詳細については、「Introduction to JSON Web Tokens」を参照してください。

CDO API トークンは、次の一連のクレームを提供します。

- **id**：ユーザー/デバイス uid
- **parentId**：テナント uid
- **ver**：公開キーのバージョン（初期バージョンは 0、例：**cdo_jwt_sig_pub_key.0**）
- **subscriptions**：SSE サブスクリプション（任意）
- **client_id**：「**api-client**」
- **jti**：トークン id

トークンの管理

API トークンの生成

手順

ステップ 1 CDO メニューバーから**[管理（Admin）] > [全般設定（General Settings）]**に移動します。

ステップ 2 [マイトークン（My Tokens）] で、[APIトークンの生成（Generate API Token）] をクリックします。

ステップ 3 機密データを維持するための企業のベストプラクティスに従って、トークンを安全な場所に保存します。

API トークンの確認

API トークンに有効期限はありませんが、ユーザーは、トークンが紛失した場合、侵害された場合、または企業のセキュリティガイドラインに準拠させる場合、API トークンの更新を選択できます。

手順

ステップ 1 CDO メニューバーから**[管理（Admin）] > [全般設定（General Settings）]**に移動します。

ステップ 2 [マイトークン（My Tokens）] で、[更新（Renew）] をクリックします。 Defense Orchestrator によって新しいトークンが生成されます。

ステップ 3 機密データを維持するための企業のベストプラクティスに従って、新しいトークンを安全な場所に保存します。

API トークンの取り消し

手順

ステップ 1 CDO メニューバーから**[管理（Admin）] > [全般設定（General Settings）]**に移動します。

ステップ 2 [マイトークン（My Tokens）] で、[取り消し（Revoke）] をクリックします。 Defense Orchestrator によりトークンが取り消されます。

アイデンティティ プロバイダーアカウントと Defense Orchestrator ユーザーレコードとの関係

Cisco Defense Orchestrator（CDO）にログインするには、SAML 2.0 準拠の ID プロバイダー（IdP）、多要素認証プロバイダー、および CDO のユーザーレコードを持つアカウントが必要です。IdP アカウントにはユーザーのログイン情報が含まれており、IdP はそのログイン情報に基づいてユーザーを認証します。多要素認証では、アイデンティティセキュリティの付加的なレイヤが提供されます。CDO ユーザーレコードには、主にユーザー名、ユーザーが関連付けられる CDO テナント、ユーザーのロールが含まれます。ユーザーがログインすると、CDO は IdP のユーザー ID を CDO のテナントの既存ユーザーレコードにマッピングします。CDO が一致するレコードを見つけた場合に、該当するユーザーはそのテナントへのログインを許可されます。

お客様の企業に独自のシングルサインオン ID プロバイダーがない限り、ID プロバイダーは Cisco Secure Sign-on です。Cisco Secure Sign-On は、多要素認証に Duo を使用します。顧客は、必要に応じてSAML シングルサインオンと Cisco Defense Orchestrator の統合できます。

ログインのワークフロー

ここでは、IdP アカウントが、CDO ユーザーにログインするために CDO ユーザーレコードとどのようにやり取りするかについて簡単に説明します。

手順

ステップ 1 ユーザーは、認証のために Cisco Secure Sign-On（https://sign-on.security.cisco.com）などの SAML 2.0 準拠のアイデンティティ プロバイダー (IdP) にログインして、CDO へのアクセスを要求します。

ステップ 2 IdP は、ユーザーが本物であるという SAML アサーションを発行し、ポータルには、ユーザーがアクセスできるアプリケーション（https://defenseorchestrator.com や https://defenseorchestrator.eu、https://www.apj.cdo.cisco.com/ を表すタイルなど）が表示されます。

ステップ 3 CDO は SAML アサーションを検証し、ユーザー名を抽出して、そのユーザー名に対応するテナントの中からユーザーレコードを見つけようとします。

- ユーザーが CDO 上の 1 つのテナントにユーザーレコードを持っている場合、CDO はそのユーザーにテナントへのアクセスを許可し、ユーザーロールによって実行できるアクションが決まります。
- ユーザーが複数のテナントにユーザーレコードを持っている場合、CDO は認証されたユーザーに、選択できるテナントのリストを提示します。ユーザーがテナントを選択すると、テナントへのアクセスが許可されます。その特定のテナントでのユーザーロールによって、実行できるアクションが決まります。
- 認証されたユーザーとテナントのユーザーレコードとのマッピングが CDO にない場合、CDO はランディングページを表示して、ユーザーに CDO の詳細を確認したり、無料試用版をリクエストしたりする機会を提供します。

CDO でユーザーレコードを作成しても IdP にアカウントは作成されず、IdP でアカウントを作成しても CDO にユーザーレコードは作成されません。

同様に、IdP のアカウントを削除しても、CDO からユーザーレコードを削除したことにはなりません。ただし、IdP アカウントがないと、CDO に対してユーザーを認証する方法はありません。CDO ユーザーレコードの削除は、IdP アカウントを削除したことを意味するものではありません。ただし、CDO ユーザーレコードがなければ、認証されたユーザーが CDO テナントにアクセスする方法はありません。

このアーキテクチャの影響

Cisco Secure Sign-On を使用する顧客

お客様が CDO の Cisco Secure Sign-On ID プロバイダーを使用している場合、スーパー管理者は CDO でユーザーレコードを作成でき、ユーザーは CDO に自己登録できます。2 つのユー

ザー名が一致し、ユーザーが正しく認証されている場合、ユーザーは CDO にログインできます。

ユーザーが CDO にアクセスできないようにする必要がある場合は、スーパー管理者が CDO ユーザーのユーザーレコードを削除するだけで済みます。Cisco Secure Sign-On アカウントは引き続き存在し、スーパー管理者がユーザーを復元したい場合は、Cisco Secure Sign-On で使用していたものと同じユーザー名で新しい CDO ユーザーレコードを作成することができます。

お客様が CDO の問題に遭遇し、テクニカル アシスタンス センター（TAC）を呼び出す必要が生じた場合、お客様が TAC エンジニアのユーザーレコードを作成することで、TAC エンジニアがテナントを調査し、お客様に情報と提案を報告できるようになります。

独自のアイデンティティ プロバイダーをもつ顧客

SAML シングルサインオンと Cisco Defense Orchestrator の統合は、アイデンティティ プロバイダーアカウントと CDO アカウントの両方を制御します。このようなお客様は、CDO でアイデンティティ プロバイダーのアカウントとユーザーレコードを作成および管理できます。

ユーザーが CDO にアクセスできないようにする必要がある場合は、お客様は IdP アカウント、CDO ユーザーレコード、またはその両方を削除できます。

Cisco TAC からの支援が必要な場合は、お客様は読み取り専用ロールを持つアイデンティティ プロバイダー アカウントと CDO ユーザーレコードの両方を、TAC エンジニア用に作成できます。TAC エンジニアは、お客様の CDO テナントにアクセスして調査し、情報と提案をお客様に報告することができます。

シスコ マネージドサービス プロバイダー

シスコ マネージドサービス プロバイダー（MSP）は、CDO の Cisco Secure Sign-On IdP を使用している場合、Cisco Secure Sign-On に自己登録できます。 MSP のお客様は CDO にそれぞれのユーザーレコードを作成できるため、MSP はお客様のテナントを管理できます。もちろん、お客様は MSP のレコードの削除を完全に制御できます（削除を選択した場合）。

関連項目

- 全般設定
- ユーザ管理
- ユーザの役割

マルチテナントポータルの管理

CDO マルチテナント ポータル ビューには、複数のテナントにまたがるすべてのデバイスから取得された情報が表示されます。このマルチテナントポータルには、デバイスのステータス、デバイスで実行中のソフトウェアバージョンなどが表示されます。

（注） マルチテナントポータルから、複数のリージョンにテナントを追加したり、追加したテナントの管理対象デバイスを表示したりできますが、テナントの編集やデバイスの設定はできません。

はじめる前に

マルチテナントポータルは、テナントでこの機能が有効になっている場合にのみ使用できます。テナントでマルチテナントポータルを有効にするには、Cisco TAC でサポートチケットを開きます。サポートチケットが解決され、ポータルが作成されると、ポータルで**ネットワーク管理者**のロールを持つユーザーが、テナントを追加できるようになります。

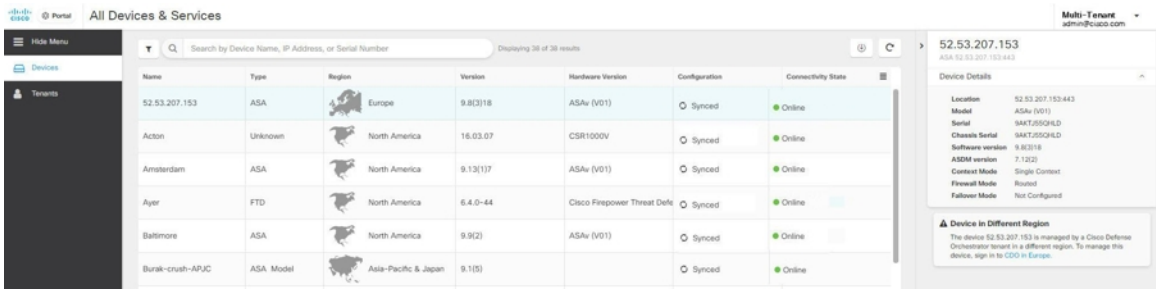
発生する可能性のある特定のブラウザ関連の問題を回避するために、Webブラウザからキャッシュと Cookie をクリアすることをお勧めします。

マルチテナントポータル

ポータルには、次のメニューが用意されています。

- [デバイス（Device）] :
  - ポータルに追加されたテナントに存在するすべてのデバイスを表示します。[フィルタ（Filter）] と [検索（Search）] フィールドを使用して、表示するデバイスを検索できます。デバイスをクリックすると、デバイスのステータス、オンボーディング方式、ファイアウォールモード、フェールオーバーモード、ソフトウェアバージョンなどを表示できます。
  - インターフェイスには、テーブルに表示するデバイスプロパティを選択またはクリアする際に使用できる列ピッカー ≣ があります。「AnyConnect リモートアクセス VPN」を除き、他のすべてのデバイスプロパティがデフォルトで選択されています。テーブルをカスタマイズすると、CDO に次回サインインしたとき、選択した内容が CDO で保持されています。
  - デバイスをクリックすると、右側にその詳細が表示されます。
  - ポータルの情報は、コンマ区切り値（CSV）ファイルにエクスポート ⏻ できます。この情報は、デバイスを分析したり、アクセス権のないユーザーに送信したりするのに役立ちます。データをエクスポートするたびに、CDO では新しい .csv ファイルが作成されます。作成されるファイル名には日付と時刻が含まれます。
  - デバイスを管理する CDO テナントからのみデバイスを管理できます。マルチテナントポータルには、CDO テナントページに移動するための [デバイスの管理（Manage Devices）] リンクが用意されています。そのテナントのアカウントを持っており、テナントとポータルが同じリージョン内にある場合、デバイスにこのリンクが表示されます。テナントにアクセスする権限がない場合は、[デバイスの管理（Manage Devices）] リンクは表示されません。組織のネットワーク管理者に連絡して許可を得ることができます。

（注） デバイスを管理しているテナントが別のリージョン内にある場合は、そのリージョンの CDO にサインインするためのリンクが表示されます。そのリージョン内の CDO またはそのリージョン内のテナントにアクセスする権限のない場合は、デバイスを管理できません。



- [テナント（Tenants）]：
  - ポータルに追加されたテナントが表示されます。
  - ネットワーク管理者ユーザーがポータルにテナントを追加できます。
  - をクリックすると、CDO テナントのメインページが表示されます。

マルチテナントポータルにテナントを追加する

Super Admin ロールを持つユーザーは、ポータルにテナントを追加できます。複数のリージョンにまたがってテナントを追加できます。たとえば、ヨーロッパリージョンから米国リージョンにテナントを追加したり、米国リージョンからヨーロッパリージョンに追加したりできます。

重要 テナントに API のみのユーザーを作成するし、CDO への認証用に API トークンを生成することをお勧めします。

（注） ポータルに複数のテナントを追加する場合は、各テナントから API トークンを生成し、テキストファイルに貼り付けます。これにより、複数のテナントをポータルに簡単に追加できます。トークンを生成するために毎回テナントを切り替える必要はありません。

手順

ステップ 1 テナントページに移動し、アカウントメニューから [設定（Settings）] > [一般設定（General Settings）] > [マイトークン（My Tokens）] をクリックします。 > >

ステップ 2 [APIトークンを生成（Generate API Token）] をクリックしてコピーします。

ステップ 3 ポータルに移動し、[テナント（Tenants）] タブをクリックします。

ステップ 4 右側の+テナント追加ボタンをクリックします。

ステップ 5 トークンを貼り付けて、[保存（Save）] をクリックします。

マルチテナントポータルからのテナントの削除

手順

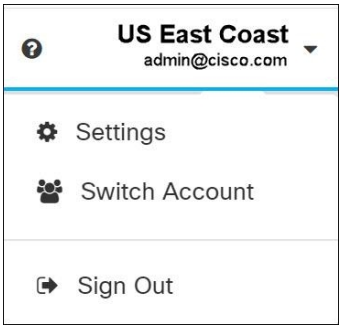
ステップ 1 ポータルに移動し、[テナント（Tenants）] タブをクリックします。

ステップ 2 右側に表示される対応する削除アイコンをクリックして、必要なテナントを削除します。

ステップ 3 [削除（Remove）]をクリックします。関連付けられたデバイスもポータルから削除されます。

Manage-Tenant ポータルの設定

Cisco Defense Orchestrator（Defense Orchestrator）を使用して、[設定（Settings）] ページのマルチテナントポータルと個々のユーザーアカウントの特定の部分をカスタマイズできます。[ユーザーメニュー（user menu）] を開き、[設定（Settings）] をクリックして、[設定（Settings）] ページにアクセスします。



設定

全般設定

Web分析により、ページのヒット数に基づく匿名の製品使用情報がシスコに提供されます。情報には、表示したページ、ページで費やした時間、ブラウザのバージョン、製品バージョン、デバイスのホスト名などが含まれます。この情報は、シスコが機能の使用状況パターンを確認

し、製品を改善するのに使用されます。すべての使用状況データは匿名化されており、機密データは送信されません。

Web 分析はデフォルトで有効になっています。Web 分析を無効にする場合や、後から有効にする場合は、次の手順を実行します。

1. ユーザーメニューから、[設定（Settings）] を選択します。
2. [全般設定（General Settings）] をクリックします。
3. [Web 分析（Web Analytics）] の下にあるスライダをクリックします。

[ユーザー管理（User Management）]

マルチテナントポータルに関連付けられているすべてのユーザーレコードは、[ユーザー管理（User Management）] 画面で確認できます。ユーザーアカウントは追加、編集または削除できます。詳細については、「ユーザ管理」を参照してください。

アカウントの切り替え

複数のポータルアカウントがある場合、CDO からサインアウトせずに、異なるポータルアカウント間やテナントアカウント間で切り替えることができます。

手順

ステップ 1 マルチテナントポータルで、右上隅に表示されるアカウントメニューをクリックします。
ステップ 2 [アカウントの切り替え（Switch Account）] をクリックします。
ステップ 3 表示するポータルまたはテナントを選択します。

Cisco Success Network

Cisco Success Network はユーザ対応のクラウドサービスです。Cisco Success Network を有効にすると、デバイスと Cisco Cloud 間にセキュアな接続が確立され、使用状況に関する情報と統計情報がストリーミングされます。テレメトリをストリーミングすることによって、デバイスからの対象のデータを選択してそれを構造化形式でリモートの管理ステーションに送信するメカニズムが提供されるため、次のメリットが得られます。

- ネットワーク内の製品の有効性を向上させるために、利用可能な未使用の機能について通知します。
- 製品に利用可能な、追加のテクニカル サポート サービスとモニターリングについて通知します。
- シスコ製品の改善に役立ちます。

デバイスは常にセキュアな接続を確立および維持し、Cisco Success Network に登録できるようにします。デバイスを登録した後で Cisco Success Network の設定を変更できます。

（注）

- Firepower Threat Defense ハイアベイラビリティペアでは、アクティブデバイスを選択すると、スタンバイデバイスの Cisco Success Network 設定を上書きします。
- CDO は Cisco Success Network 設定を管理しません。設定の管理とテレメトリ情報の提供は、Firepower Device Manager（FDM）ユーザーインターフェイスが行います。

Cisco Success Network の有効化または無効化

システムの初期設定時に、Cisco Smart Software Manager にデバイスを登録するように求められます。登録せずに 90 日間の評価ライセンスを使用する場合、評価期間の終了前にデバイスを登録する必要があります。デバイスを登録するには、（[スマートライセンス（Smart Licensing）] ページで）Cisco Smart Software Manager にデバイスを登録するか、または登録キーを入力して Cisco Defense Orchestrator に登録します。

デバイスを登録すると、バーチャル アカウントからデバイスにライセンスが割り当てられます。デバイスを登録すると、有効にしているすべてのオプション ライセンスも登録されます。

この接続は、Cisco Success Network を無効にすることでいつでも無効にできますが、このオプションは FDM UI からのみ無効にできます。無効にすると、デバイスがクラウドから切断されます。切断しても更新の受信やスマート ライセンス機能の操作には影響せず、正常に動作を継続します。詳細については、『Firepower Device Manager コンフィギュレーション ガイド、バージョン 6.4.0 以降』の「システム管理」の章の「**Cisco Success Network への接続**」セクションを参照してください。

ユーザ管理

CDO でユーザーレコードを作成または編集する前に、「アイデンティティ プロバイダー アカウントと Defense Orchestrator ユーザーレコードとの関係」を読んで、ID プロバイダー（IdP）アカウントとユーザーレコードがどのように相互作用するかを学習してください。CDO ユーザーは、認証されて CDO テナントにアクセスできるように、CDO レコードと対応する IdP アカウントが必要です。

企業独自の IdP がない限り、Cisco Secure Sign-On はすべての CDO テナントの ID プロバイダーとなります。この記事の残りの部分は、ID プロバイダーとして Cisco Secure Sign-On を使用していることを前提としています。

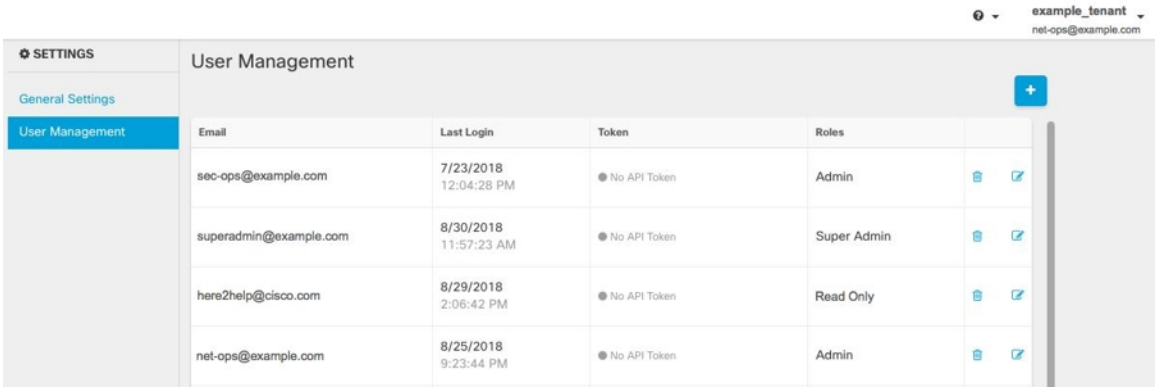
テナントに関連付けられているすべてのユーザーレコードは、**ユーザー管理**画面で確認できます。サポートチケットを解決するために一時的にアカウントに関連付けられたシスコ サポート エンジニアも対象となります。

テナントに関連付けられているユーザーレコードの表示

手順

ステップ 1 CDO メニューバーから**[管理（Admin）]**>**[ユーザー管理（User Management）]**に移動します。

ステップ 2 [ユーザー管理（User Management）] をクリックします。



（注） シスコのサポートチームがテナントにアクセスできないようにするには、[全般設定（General Settings）]全般設定 （45 ページ）ページでアカウント設定を行います。

ユーザー管理の Active Directory グループ

多数のユーザーが頻繁に入れ替わるテナントの場合、個々のユーザーを CDO に追加する代わりに、CDO を Active Directory（AD）グループにマッピングして、ユーザーリストとユーザーロールをより簡単に管理できます。新しいユーザーの追加や既存のユーザーの削除といったユーザーの変更はすべて、Active Directory で実行できるようになり、CDO で実行する必要がなくなります。

[ユーザー管理（User Management）]ページから AD グループを追加、編集、または削除するには、**ネットワーク管理者**のユーザーロールが必要です。詳細については、「ユーザの役割」を参照してください。

[Active Directoryグループ（Active Directory Groups）] タブ

[設定（Settings）] ページの [ユーザー管理（User Management）] セクションには、現在 CDO にマッピングされている Active Directory グループのタブがあります。最も重要な点として、このページには、AD マネージャで割り当てられた AD グループのロールが表示されます。

AD グループに含まれているユーザーは、[Active Directoryグループ（Active Directory Groups）] タブまたは [ユーザー（Users）] タブに個別に表示されません。

[Audit Logs] タブ

[設定（Settings）] ページの [ユーザー管理（User Management）] セクションには、監査ログのタブがあります。この新しいセクションには、CDO アカウントにアクセスしたすべてのユーザーの最終ログイン時刻と、最終ログイン時に保持していた各ユーザーのロールが表示されます。これには、明示的なユーザーログインと AD グループログインの両方が含まれます。

マルチロールユーザー

CDO の IAM 機能が拡張され、ユーザーが複数のロールを持つことができるようになりました。

ユーザーは、AD の複数のグループの一部になることができ、それらの各グループは、異なる CDO ロールを持つ CDO で定義できます。ユーザーがログイン時に取得する最終的なアクセス許可は、そのユーザーが属する CDO で定義されているすべての AD グループのロールの組み合わせです。たとえば、ユーザーが 2 つの AD グループに属しており、両方のグループが 2 つの異なるロール（編集専用とデプロイ専用など）で CDO に追加されている場合、ユーザーは編集専用とデプロイ専用の両方の権限を持ちます。これは、任意の数のグループとロールに適用されます。

AD グループのマッピングを CDO で定義する必要があるのは 1 回だけであり、ユーザーのアクセスと権限の管理は、その後、異なるグループ間でユーザーを追加、削除、または移動することによって AD で排他的に実行できます。

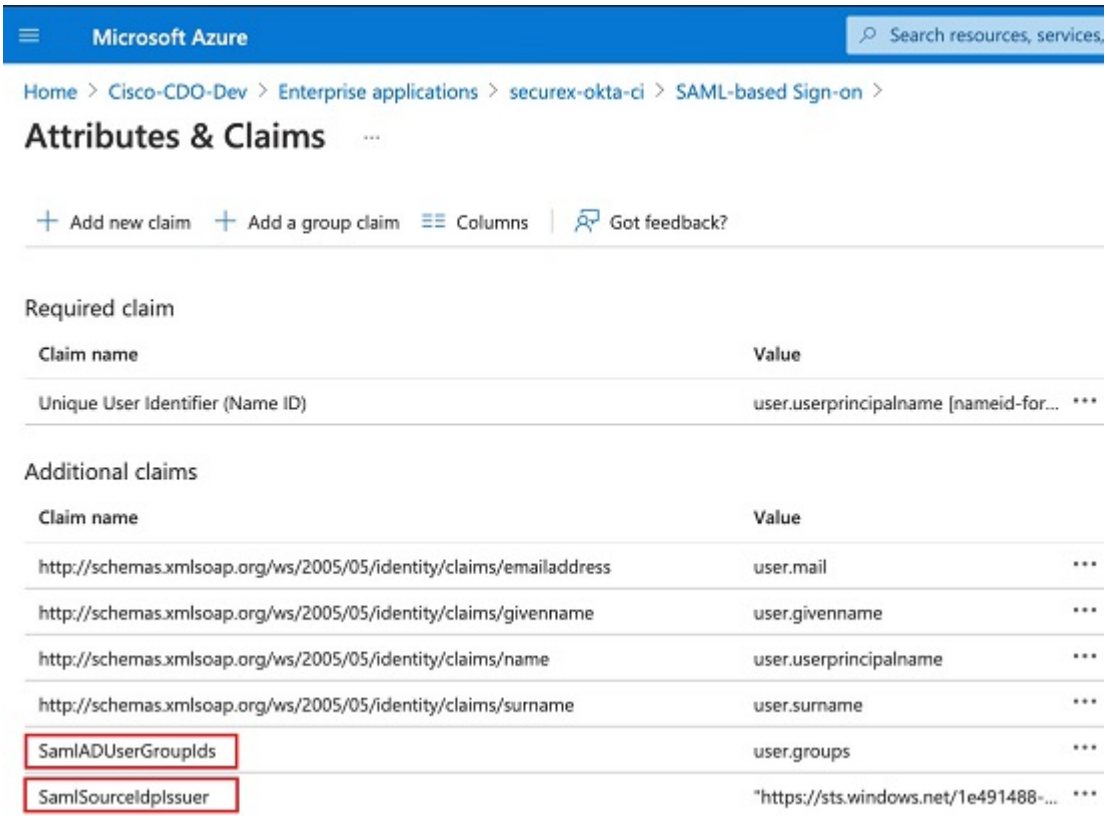
（注） ユーザーが、個別ユーザーであり、かつ同じテナントの AD グループにも属している場合は、個別ユーザーのユーザーロールが AD グループのユーザーロールよりも優先されます。

はじめる前に

AD グループマッピングをユーザー管理形式として CDO に追加する前に、AD を SecureX と統合する必要があります。AD の ID プロバイダー（IdP）がまだ統合されていない場合は、次の操作を実行する必要があります。

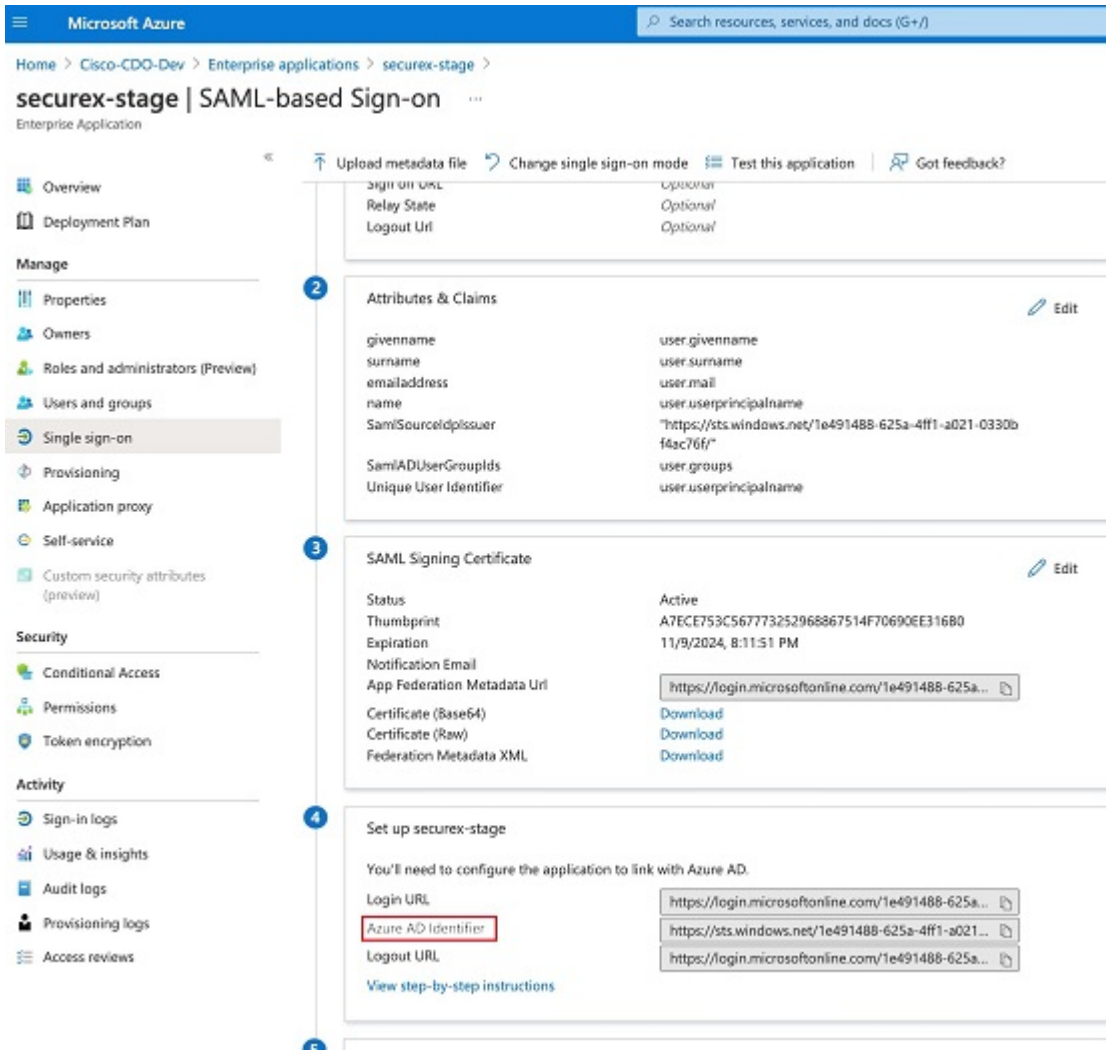
1. Cisco TAC でサポートケースを開き、次の情報を使用してカスタム AD IdP 統合を要求します。
   - CDO のテナント名と地域。
   - カスタムルーティングを定義するドメイン（例：@cisco.com、@myenterprise.com）。
   - .XML 形式の証明書とフェデレーションメタデータ。
2. AD に次のカスタム SAML 要求を追加します。これらの値では大文字と小文字が区別されます。
   - **SamlADUserGroupIds**：この属性は、ユーザーが AD 上で持つすべてのグループの関連付けを記述します。たとえば、次のスクリーンショットに示すように、Azure で [+ グループ要求の追加（+ Add groups claim）] を選択します。

図 *3 : Active Directory* で定義されたカスタム要求



- **SamlSourceIdpIssuer**：この属性は、ADインスタンスを一意に識別します。たとえば、次のスクリーンショットに示すように、Azure で [+グループ要求の追加（+ Add a group claim）] を選択し、スクロールして Azure AD 識別子を見つけます。

図 *4 : Azure Active Directory* の識別子を見つける



ユーザー管理用 Active Directory グループの追加

手順

ステップ 1 CDO にログインします。

ステップ 2 CDO メニューバーから**[管理（Admin）]**>**[ユーザー管理（User Management）]**に移動します。

ステップ 3 テーブルの上にある [Active Directoryグループ（Active Directory Groups）] を選択します。

ステップ 4 現在の AD グループがない場合は、[ADグループの追加（Add AD group）] をクリックします。既存のエントリがある場合は、[追加（Add）] ボタンをクリックします。

ステップ 5 次の情報を入力します。

- [グループ名（Group Name）]：一意の名前を入力します。この名前は、AD のグループ名と一致する必要はありません。CDO は、このフィールドで特殊文字をサポートしていません。
- [グループ ID（Group ID）]：AD からのグループ ID を手動で入力します。これは、AD アプリケーションにおいて「オブジェクト ID」という別名で呼ばれる場合があります。
- [AD 発行者（AD Issuer）]：AD からの AD 発行者の値を手動で入力します。
- [ロール（Role）]：この AD グループに含まれるすべてのユーザーのロールが決まります。詳細については、「ユーザーロール」を参照してください。
- （オプション）[注記（Notes）]：この AD グループに適用される注記を追加します。

ステップ 6 **[OK]** を選択します。

ユーザー管理用 Active Directory グループの編集

始める前に

CDO で AD グループのユーザー管理を編集する場合は、CDO が AD グループを制限する方法だけを変更できることに注意してください。CDO で AD グループ自体を編集することはできません。AD グループ内のユーザーのリストを編集するには、AD を使用する必要があります。

手順

ステップ 1 CDO にログインします。

ステップ 2 CDO メニューバーから**[管理（Admin）]**>**[ユーザー管理（User Management）]**に移動します。

ステップ 3 テーブルの上にある [Active Directoryグループ（Active Directory Groups）] を選択します。

ステップ 4 編集する AD グループを特定し、[編集（Edit）] アイコンを選択します。

ステップ 5 次の値を変更します。

- [グループ名（Group Name）]：一意の名前を入力します。CDO は、このフィールドで特殊文字をサポートしていません。
- [グループ ID（Group ID）]：AD からのグループ ID を手動で入力します。これは、AD アプリケーションにおいて「オブジェクト ID」という別名で呼ばれる場合があります。
- [AD 発行者（AD Issuer）]：AD からの AD 発行者の値を手動で入力します。
- [ロール（Role）]：この AD グループに含まれるすべてのユーザーのロールが決まります。詳細については、「ユーザーロール」を参照してください。

- [注記（Notes）]：この AD グループに適用される注記を追加します。

ユーザー管理用 Active Directory グループの削除

手順

ステップ 1 CDO にログインします。
ステップ 2 CDO メニューバーから**[管理（Admin）]**>**[ユーザー管理（User Management）]**に移動します。
ステップ 3 テーブルの上にある [Active Directoryグループ（Active Directory Groups）] を選択します。
ステップ 4 削除する AD グループを特定します。
ステップ 5 [削除（Delete）] アイコンを選択します。
ステップ 6 [OK] をクリックして、AD グループを削除することを確認します。

新規 CDO ユーザーの作成

次の 2 つのタスクは、新しい CDO ユーザーを作成するために必要です。順番に実行する必要はありません。

- 新規ユーザー向け Cisco Secure Sign-On アカウントの作成
- CDO ユーザー名での CDO ユーザーレコードの作成

これらのタスクが完了すると、ユーザーは 新規ユーザーが Cisco Secure Sign-On ダッシュボードから CDO を開くことができます。

新規ユーザー向け Cisco Secure Sign-On アカウントの作成

Cisco Secure Sign-on アカウントの作成は、新しいユーザーが自分でいつでも行うことができます。割り当てられるテナントの名前を把握しておく必要はありません。

CDO へのログインについて

Cisco Defense Orchestrator（CDO）は、Cisco Secure Sign-On をアイデンティティ プロバイダーとして使用し、多要素認証（MFA）に Duo を使用します。**CDO にログインするには、まず Cisco Secure Sign-On でアカウントを作成し、Duo を使用して MFA を設定する必要があります。**

CDO には MFA が必要です。MFA は、ユーザーアイデンティティを保護するためのセキュリティを強化します。MFA の一種である二要素認証では、CDO にログインするユーザーの ID

を確認するために、2 つのコンポーネントまたは要素が必要です。最初の要素はユーザー名とパスワードで、2番目の要素はオンデマンドで生成されるワンタイムパスワード（OTP）です。

重要 **2019 年 10 月 14 日より前に CDO テナントが存在していた場合は**、この項目の代わりに「Cisco Secure Sign-On ID プロバイダーへの移行 （39 ページ）」をログイン手順として使用してください。

ログインする前に

Duo Security のインストール。Duo Security アプリケーションを携帯電話にインストールすることをお勧めします。Duo のインストールについてご質問がある場合は、『Duo Guide to Two Factor Authentication：Enrollment Guide』を参照してください。

時刻の同期。モバイルデバイスを使用してワンタイムパスワードを生成します。OTP は時間ベースであるため、デバイスのクロックがリアルタイムと同期していることが重要です。デバイスのクロックが自動的に、または手動で正しい時刻に設定されていることを確認します。

新規 Cisco Secure Sign-On アカウントの作成と Duo 多要素認証の設定

最初のサインオンワークフローは 4 段階のプロセスです。4 段階すべてを完了する必要があります。

手順

ステップ 1 新しい Cisco Secure Sign-On アカウントにサインアップする

1. https://sign-on.security.cisco.com にアクセスします。
2. [サインイン（Sign In）] 画面の下部にある [サインアップ（Sign up）] をクリックします。

3. [アカウントの作成（Create Account）]ダイアログのフィールドに入力し、[登録（Register）]をクリックします。

次にいくつかのヒントを示します。

- [E メール（Email）]：CDO へのログインに最終的に使用する電子メールアドレスを入力します。
- [組織（Organization）]：会社を表す名前を追加します。

4. [登録（Register）]をクリックすると、登録したアドレスに確認メールが送信されます。電子メールを開き、[アカウントの有効化（Activate Account）] をクリックします。

ステップ 2 Duo を使用して多要素認証をセットアップする

多要素認証をセットアップするときは、モバイルデバイスを使用することをお勧めします。

1. [多要素認証の設定（Set up multi-factor authentication）] 画面で、[要素の設定（Configure factor）] をクリックします。
2. [セットアップの開始（Start setup）]をクリックし、プロンプトに従ってモバイルデバイスを選択して、そのモバイルデバイスとアカウントのペアリングを確認します。

   詳細については、『Duo Guide to Two Factor Authentication：Enrollment Guide』を参照してください。デバイスにDuoアプリケーションがすでにインストールされている場合は、このアカウントのアクティベーションコードが送信されます。Duo は 1 台のデバイスで複数のアカウントをサポートします。
3. ウィザードの最後で、[ログインを続行する（Continue to Login）] をクリックします。
4. 二要素認証を使用して Cisco Secure Sign-On にログインします。

ステップ 3 （任意）追加のオーセンティケータとして Google オーセンティケータを設定します。

1. Googleオーセンティケータとペアリングするモバイルデバイスを選択し、[次へ（Next）] をクリックします。
2. セットアップウィザードのプロンプトに従って、Google オーセンティケータをセットアップします。

ステップ 4 Cisco Secure Sign-On アカウントのアカウントリカバリのオプションを設定する

1. SMS を使用してアカウントをリセットするための予備の電話番号を選択します。
2. セキュリティイメージを選択します。
3. [マイアカウントの作成（Create My Account）] をクリックします。これで、Cisco Security Sign-On ダッシュボードに CDO アプリケーションのタイルが表示されます。他のアプリケーションタイルも表示される場合があります。

ヒント

ダッシュボード上でタイルをドラッグして並べ替えたり、タブを作成してタイルをグループ

CDO ユーザー名での CDO ユーザーレコードの作成

「ネットワーク管理者（Super Admin）」権限を持つCDOユーザーのみがCDOユーザーレコードを作成できます。ネットワーク管理者は、上記の**CDO ユーザー名の作成**タスクで指定したものと同じ電子メールアドレスでユーザーレコードを作成する必要があります。

次の手順を使用して、適切なユーザーロールを持つユーザーレコードを作成します。

手順

ステップ 1 CDO にログインします。

ステップ 2 CDO メニューバーから**[管理（Admin）]**>**[ユーザー管理（User Management）]**に移動します。

ステップ 3 青いプラスボタン  をクリックして、新しいユーザーをテナントに追加します。

ステップ 4 ユーザーの電子メールアドレスを入力します。

（注） ユーザーの電子メールアドレスは、Cisco Secure Log-On アカウントの電子メールアドレスに対応している必要があります。

ステップ 5 ドロップダウンメニューからユーザーのユーザの役割を選択します。

ステップ 6 [OK] をクリックします。

新規ユーザーが Cisco Secure Sign-On ダッシュボードから CDO を開く

手順

ステップ 1 Cisco Secure Sign-on ダッシュボードで適切な [CDO] タイルをクリックします。[CDO] タイルをクリックすると https://defenseorchestrator.com に移動し、[CDO（EU）] タイルをクリックすると https://defenseorchestrator.eu に移動します。

ステップ 2 両方のオーセンティケータを設定している場合は、オーセンティケータのロゴをクリックして [Duo Security] か [Google Authenticator] を選択します。

- 既存のテナントにすでにユーザーレコードがある場合は、そのテナントにログインします。
- 複数のポータルにすでにユーザーレコードがある場合は、接続するポータルを選択できます。

- すでに複数のテナントにユーザーレコードがある場合は、接続先の CDO テナントを選択できます。
- 既存のテナントにユーザーレコードがない場合は、CDO の詳細を確認するか、またはトライアルアカウントを要求できます。

[ポータル（Portals）] ビューは、複数のテナントから統合された情報を取得して表示します。詳細については、「マルチテナントポータルの管理」を参照してください。

[テナント（Tenant）] ビューには、ユーザーレコードがある一部のテナントが表示されます。

ユーザの役割

Cisco Defense Orchestrator（CDO）には、読み取り専用、編集専用、展開専用、管理者、ネットワーク管理者など、さまざまなユーザーロールがあります。ユーザーロールは、各テナントのユーザーごとに設定されます。1 人の CDO ユーザーが複数のテナントにアクセスできる場合、ユーザー ID は同じでも、テナントごとにロールが異なる場合があります。ユーザーは、あるテナントで読み取り専用ロールを持ち、別のテナントでネットワーク管理者ロールを持つ場合があります。インターフェイスまたはマニュアルで読み取り専用ユーザー、管理者ユーザー、ネットワーク管理者ユーザーについて言及されている場合、特定のテナントにおけるそのユーザーの権限レベルが説明されています。

読み取り専用ロール

読み取り専用ロールが割り当てられたユーザーには、すべてのページに次の青いバナーが表示されます。

Read Only User. You cannot make configuration changes.

。

読み取り専用ロールを持つユーザーは、次のことを実行できます。

- CDO の任意のページまたは設定を確認する。
- 任意のページのコンテンツを検索およびフィルタリングする。
- デバイス設定を比較し、変更ログを表示し、VPN マッピングを確認する。
- 任意のページの設定またはオブジェクトに関するすべての警告を表示する。
- 独自の API トークンを生成する、更新する、取り消す。読み取り専用ユーザーは、自分のトークンを取り消すと、再作成できないことに注意してください。
- インターフェイスからサポートに連絡し、変更ログをエクスポートする。

読み取り専用ユーザーは、次の操作を実行**できません**。

- 任意のページで作成、更新、設定、または削除する。
- デバイスをオンボーディングする。
- オブジェクトやポリシーなどの作成に必要なタスクのステップスルーはできるが保存はできない。
- CDO ユーザーレコードを作成する。
- ユーザーロールを変更する。
- アクセスルールをポリシーにアタッチまたはデタッチする。

編集専用ロール

編集専用ロールを持つユーザーは、次の操作を実行できます。

- オブジェクト、ポリシー、ルールセット、インターフェース、VPNなどを含むがこれらに限定されないデバイス構成を編集および保存する。
- **構成の読み取り**アクションによって行われた構成の変更を許可する。
- 変更リクエスト管理アクションを利用する。

編集専用ユーザーは、次の操作を実行**できません**。

- 1 つまたは複数のデバイスに変更を展開する。
- 段階的な変更または OOB によって検出された変更を破棄する。
- AnyConnect パッケージをアップロードする、またはこれらの設定を構成する。
- デバイスのイメージアップグレードをスケジュールする、または手動で開始する。

- セキュリティデータベースのアップグレードをスケジュールする、または手動で開始する。
- Snort 2 と Snort 3 のバージョンを手動で切り替える。
- テンプレートを作成します。
- 既存の OOB 変更の設定を変更する。
- システム管理設定を編集する。
- デバイスをオンボーディングする。
- デバイスを削除する。
- VPN セッションまたはユーザーセッションを削除する。
- CDO ユーザーレコードを作成する。
- ユーザーロールを変更する。

展開専用ロール

展開専用ロールを持つユーザーは、次の操作を実行できます。

- 段階的な変更を単一のデバイスまたは複数のデバイスに展開する。
- ASA デバイスの設定変更を元に戻すか、復元する。
- デバイスのイメージアップグレードをスケジュールする、または手動で開始する。
- セキュリティデータベースのアップグレードをスケジュールする、または手動で開始する。
- 変更要求管理アクションを使用する。

展開専用ユーザーは、次の操作を実行**できません**。

- Snort 2 と Snort 3 のバージョンを手動で切り替える。
- テンプレートを作成します。
- 既存の OOB 変更の設定を変更する。
- システム管理設定を編集する。
- デバイスをオンボーディングする。
- デバイスを削除する。
- VPN セッションまたはユーザーセッションを削除する。
- 任意のページで作成、更新、設定、または削除する。
- デバイスをオンボーディングする。

- オブジェクトやポリシーなどの作成に必要なタスクのステップスルーはできるが保存はできない。
- CDO ユーザーレコードを作成する。
- ユーザーロールを変更する。
- アクセスルールをポリシーにアタッチまたはデタッチする。

VPN セッションマネージャロール

VPN セッションマネージャロールは、サイト間 VPN 接続ではなく、リモートアクセス VPN 接続を監視する管理者向けに設計されています。

VPN セッションマネージャロールを持つユーザーは、次のことができます。

- CDO の任意のページまたは設定を確認する。
- 任意のページのコンテンツを検索およびフィルタリングする。
- デバイス設定を比較し、変更ログを表示し、RA VPN マッピングを確認する。
- 任意のページの設定またはオブジェクトに関するすべての警告を表示する。
- 独自の API トークンを生成する、更新する、取り消す。VPN セッションマネージャのユーザーは、自分のトークンを取り消すと、再作成できないことに注意してください。
- インターフェイスからサポートに連絡し、変更ログをエクスポートする。
- 既存の RA VPN セッションを終了する。

VPN セッションマネージャのユーザーは、次のことは**できません**。

- 任意のページで作成、更新、設定、または削除する。
- デバイスをオンボーディングする。
- オブジェクトやポリシーなどの作成に必要なタスクのステップスルーはできるが保存はできない。
- CDO ユーザーレコードを作成する。
- ユーザーロールを変更する。
- アクセスルールをポリシーにアタッチまたはデタッチする。

Admin ロール

管理者ユーザーは、CDO のあらゆる側面に完全にアクセスできます。管理者ユーザーは次のことができます。

- CDO の任意のオブジェクトを作成、読み取り、更新、削除し、設定を行う。

- デバイスのオンボーディング。
- CDO の任意のページまたは設定を確認する。
- 任意のページのコンテンツを検索およびフィルタリングする。
- デバイス設定を比較し、変更ログを表示し、VPN マッピングを確認する。
- 任意のページの設定またはオブジェクトに関するすべての警告を表示する。
- 独自の API トークンを生成する、更新する、取り消す。トークンが取り消された場合は、インターフェイスを介してサポートに連絡し、変更ログをエクスポートできます。

管理者ユーザーは次のことを**実行できません**。

- CDO ユーザーレコードを作成する。
- ユーザーロールを変更する。

ネットワーク管理者ロール

スーパー管理者ユーザーは、CDO のあらゆる側面に完全にアクセスできます。スーパー管理者は次のことができます。

- ユーザーロールを変更する。
- ユーザーレコードを作成する。

（注） スーパー管理者は CDO ユーザーレコードを作成できますが、そのユーザーレコードだけではユーザーがテナントにログインするには不十分です。テナントが使用する ID プロバイダーのアカウントも必要になります。お客様の企業に独自のシングルサインオン ID プロバイダーがない限り、ID プロバイダーは Cisco Secure Sign-on です。ユーザーは Cisco Secure Sign-On アカウントに自己登録することができます。詳細については、新規 CDO テナントへの初回ログイン （38 ページ）を参照してください。

- CDO の任意のオブジェクトを作成、読み取り、更新、削除し、設定を行う。
- デバイスのオンボーディング。
- CDO の任意のページまたは設定を確認する。
- 任意のページのコンテンツを検索およびフィルタリングする。
- デバイス設定を比較し、変更ログを表示し、VPN マッピングを確認する。
- 任意のページの設定またはオブジェクトに関するすべての警告を表示する。
- 独自の API トークンを生成する、更新する、取り消す。トークンが取り消された場合は、次のことができます。

- インターフェイスからサポートに連絡し、変更ログをエクスポートする。

ユーザーロールのレコードの変更

ユーザーレコードは、現在記録されているユーザーのロールです。テナントに関連付けられているユーザーを調べることにより、各ユーザーがどのロールを使用しているかをレコードによって判断できます。ユーザーロールを変更すると、ユーザーレコードが変更されます。ユーザーのロールは、ユーザー管理テーブルでのロールによって識別されます。詳細については、「ユーザ管理」を参照してください。

ユーザーレコードを変更するには、ネットワーク管理者である必要があります。テナントにネットワーク管理者がいない場合は、Defense Orchestrator サポートまでお問い合わせください。

ユーザーロールのユーザーレコードの作成

CDO ユーザーは、認証されて CDO テナントにアクセスできるように、CDO レコードと対応する IdP アカウントが必要です。この手順では、Cisco Secure Sign-On のユーザーアカウントではなく、ユーザーの CDO ユーザーレコードを作成します。ユーザーが Cisco Secure Sign-On にアカウントを持っていない場合、https://sign-on.security.cisco.com に移動し、サインイン画面の下部にある [サインアップ（Sign up）] をクリックして、自己登録できます。

（注） このタスクを実行するには、CDO でネットワーク管理者ロールのロールが必要です。

ユーザーレコードの作成

次の手順を使用して、適切なユーザーロールを持つユーザーレコードを作成します。

手順

ステップ 1 CDO にログインします。

ステップ 2 CDO メニューバーから**[管理（Admin）]**>**[ユーザー管理（User Management）]**に移動します。

ステップ 3 青いプラスボタン  をクリックして、新しいユーザーをテナントに追加します。

ステップ 4 ユーザーの電子メールアドレスを入力します。

（注） ユーザーの電子メールアドレスは、Cisco Secure Log-On アカウントの電子メールアドレスに対応している必要があります。

ステップ 5 ドロップダウンメニューからユーザーのユーザの役割を選択します。

ステップ 6 [v] をクリックします。

（注） スーパー管理者は CDO ユーザーレコードを作成できますが、そのユーザーレコードだけではユーザーがテナントにログインするには不十分です。テナントが使用する ID プロバイダーのアカウントも必要になります。お客様の企業に独自のシングルサインオン ID プロバイダーがない限り、ID プロバイダーは Cisco Secure Sign-on です。ユーザーは Cisco Secure Sign-On アカウントに自己登録することができます。詳細については、新規 CDO テナントへの初回ログイン （38 ページ）を参照してください。

API のみのユーザーを作成する

手順

ステップ 1 CDO にログインします。

ステップ 2 CDO メニューバーから**[管理（Admin）]**>**[ユーザー管理（User Management）]**に移動します。

ステップ 3 青いプラスボタン  をクリックして、新しいユーザーをテナントに追加します。

ステップ 4 [APIのみのユーザー（API Only User）] チェックボックスを選択します。

ステップ 5 [ユーザー名（Username）] フィールドに ユーザー名を入力し、[OK] をクリックします。

重要 ユーザー名に E メールアドレスを使用したり、「@」文字を含めることはできません。「@yourtenant」サフィックスがユーザー名に自動的に追加されるためです。

ステップ 6 ドロップダウンメニューからユーザーのユーザの役割を選択します。

ステップ 7 [OK] をクリックします。

ステップ 8 [ユーザー管理（User Management）] タブをクリックします。

ステップ 9 新しい API のみのユーザーの [トークン（Token）] 列で、[API トークンの生成（Generate API Token）] をクリックして API トークンを取得します。

ユーザーロールのユーザーレコードの編集

このタスクを実行するには、ネットワーク管理者のロールが必要です。ログインしている CDO ユーザーのロールをネットワーク管理者が変更する場合、そのロールが変更されると、そのユーザーはセッションから自動的にログアウトされます。ユーザーが再度ログインすると、ユーザーは新しいロールを担います。

（注） このタスクを実行するには、CDO でネットワーク管理者ロールのロールが必要です。

注意 ユーザーレコードのロールを変更すると、ユーザーレコードに関連付けられたAPIトークンがある場合はそれが削除されます。ユーザーロールが変更されたら、ユーザーは新しいAPIトークンを生成する必要があります。

ユーザーロールの編集

（注） CDOユーザーがログインしていて、スーパー管理者がそのロールを変更した場合、変更を有効にするには、そのユーザーがログアウトして再度ログインする必要があります。

ユーザーレコードで定義されたロールを編集するには、次の手順に従います。

手順

ステップ1 CDOにログインします。

ステップ2 CDOメニューバーから**[管理（Admin）]**>**[ユーザー管理（User Management）]**に移動します。

ステップ3 ユーザーの行にある [編集（Edit）] アイコンをクリックします。

ステップ4 [ロール（Rple)] ドロップダウンメニューからユーザーの新しい [ロール（Rple)]ユーザの役割（76 ページ）を選択します。

ステップ5 ユーザーレコードに、ユーザーに関連付けられたAPIトークンがあることが示されている場合は、ユーザーのロールを変更し、結果としてAPIトークンを削除することを確認する必要があります。」

ステップ6 [v] をクリックします。

ステップ7 CDOがAPIトークンを削除した場合、ユーザーに連絡し、新しいAPIトークンを作成できることを知らせます。

ユーザーロールのユーザーレコードの削除

CDOのユーザーレコードを削除すると、ユーザーレコードのCisco Secure Sign-Onアカウントとのマッピングが壊れ、関連付けられたユーザーがCDOにログインできなくなります。ユーザーレコードを削除すると、そのユーザーレコードに関連付けられているAPIトークンも削除されます（存在する場合）。CDOのユーザーレコードを削除しても、Cisco Secure Sign-Onのユーザーの IdPアカウントは削除されません。

（注） このタスクを実行するには、CDOでネットワーク管理者ロールのロールが必要です。

ユーザーレコードの削除

ユーザーレコードに定義されているロールを削除するには、次の手順を実行します。

手順

ステップ 1 CDO にログインします。
ステップ 2 CDO メニューバーから**[管理（Admin）]**>**[ユーザー管理（User Management）]**に移動します。
ステップ 3 削除するユーザーの行のごみ箱アイコン をクリックします。
ステップ 4 [OK] をクリックします。
ステップ 5 [OK] をクリックして、テナントからアカウントを削除することを確認します。

デバイスとサービスの管理

Cisco Defense Orchestrator（CDO）は、サポートされているデバイスとサービスを表示、管理、フィルタリング、および評価する機能を提供します。[インベントリ（Inventory）] ページから、次の操作を実行できます。

- CDO 管理用のデバイスとサービスをオンボーディングします。
- 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。[インベントリ（Inventory）] ページ情報の表示 （92 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。
- 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。検索（96 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。

CDO のデバイスの IP アドレスを変更する

IP アドレスを使用してデバイスを Cisco Defense Orchestrator（CDO）にオンボードすると、CDO 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、CDO 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。CDO 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。

CDO 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 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。

フィルタと検索を使用して、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：

- デバイスの外部リンク （87 ページ）
- CDO へのデバイス一括再接続 （91 ページ）

CDO のデバイスの名前を変更する

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、CDO で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 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（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インベントリテーブル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、インベントリテーブル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 CDO 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 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。

フィルタと検索を使用して、必要なデバイスを見つけることができます。

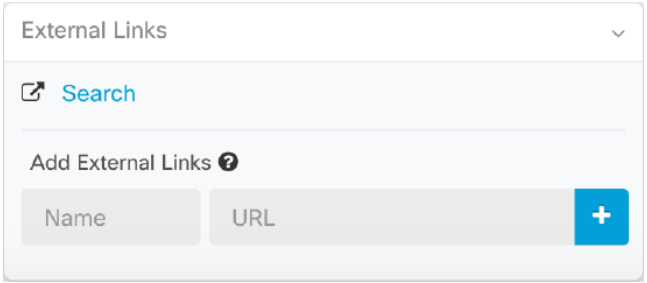
ステップ 4 必要なデバイスを選択して、強調表示します。

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、CDO 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 FTD の FDM に到達します。

関連情報：

- デバイスノートを書く （91 ページ）
- デバイスとサービスのリストのエクスポート （86 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 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 デバイスまたはモデルを選択します。

フィルタと検索を使用して、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

、FTD の Firepower Device Manager（FDM）を CDO 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 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。

フィルタと検索を使用して、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 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。

フィルタと検索を使用して、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。

- Enter

  ```
  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 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。

フィルタと検索を使用して、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 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。

フィルタと検索を使用して、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。

デバイスの CDO への再接続

手順

例：

CDO へのデバイス一括再接続

CDO を使用すると、管理者は複数の管理対象デバイスを CDO に同時に再接続を試みることができます。CDO 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、CDO 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、CDO 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、CDO 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、CDO 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 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。

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。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 [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 [ジョブ（Jobs）] ページに移動します。

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。

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 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 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。

[インベントリ（Inventory）] ページ情報の表示

[インベントリ（Inventory）] 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。検索機能を使用するか、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。

[インベントリ（Inventory）] ページには、次の詳細情報が表示されます。

- [デバイス（Devices）] タブには、CDO 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。
- [テンプレート（Templates）] には、ライブデバイスから、または CDO にインポートされた構成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。

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、そのラベルごとに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。

ラベルグループは、次の構文「group name:label」を使用して作成できます。たとえば、Region:East または Region:West などです。これらの 2 つのラベルを作成する場合、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 デバイスにラベルを追加するには、左側の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。オブジェクトにラベルを追加するには、左側のナビゲーションウィンドウでで [オブジェクト（Objects）] 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 生成された表で 1 つ以上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 [グループとラベルの追加（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 6 青色の + アイコンをクリックします。

フィルタ

[インベントリ（Inventory）] ページおよび [オブジェクト（Objects）] ページの各種フィルタを使用して、目的のデバイスや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、およびラベルを指定して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。

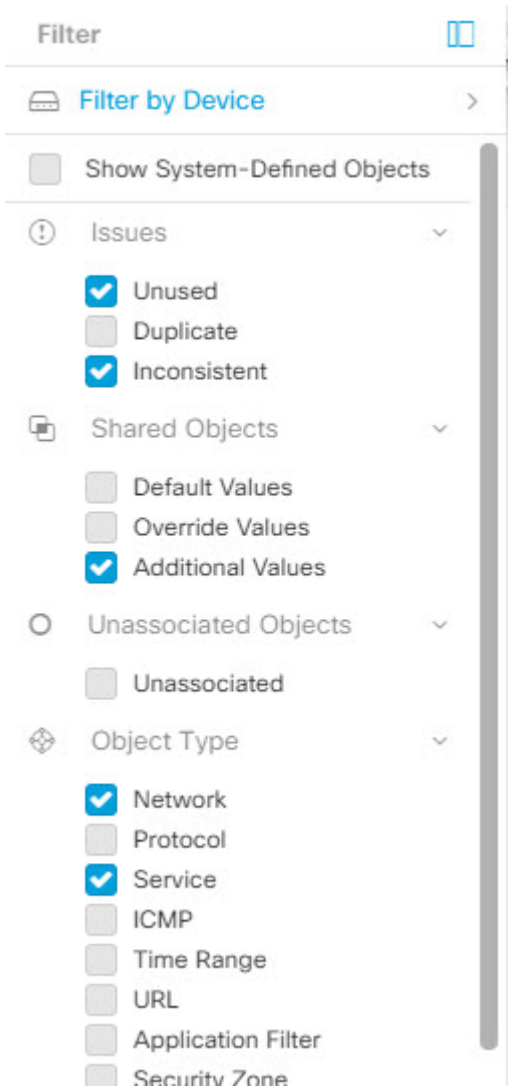
（注） [FTD] タブを開くと、フィルタペインでフィルタを使用できます。これにより、CDO からデバイスにアクセスするために使用されている管理アプリケーションに基づいて FTD デバイスが表示されます。

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

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、検索用語を組み合わせて、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できます。

次の例では、「問題（使用済みまたは不整合）があるオブジェクト、追加の値を持つ共有オブジェクト、特定タイプ（ネットワークまたはサービス）のオブジェクト」のすべての条件を満たすオブジェクトを検索するフィルタが適用されます。



同一 SDC を使用した CDO に接続するすべてのデバイスを見つける

次の手順に従って、同じ SDC を使用して CDO に接続するすべてのデバイスを識別します。

手順

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 フィルタ基準がすでに指定されている場合は、インベントリテーブルの上部にある [クリア（Clear）] ボタンをクリックして、CDO で管理しているすべてのデバイスとサービスを表示します。

ステップ 5 フィルタボタン をクリックして、[フィルタ（Filter）] メニューを展開します。フィルタ（93 ページ）

ステップ 6 フィルタの [Secure Device Connector] セクションで、必要な SDC の名前をクリックします。インベントリテーブルには、フィルタでチェックした SDC を使用して CDO に接続しているデバイスのみが表示されます。

ステップ 7 （オプション）検索をさらに絞り込むには、フィルタメニューで追加のフィルタをチェックします。

ステップ 8 （オプション）完了したら、インベントリテーブルの上部にある [クリア（Clear）] ボタンをクリックして、CDO で管理しているすべてのデバイスとサービスを表示します。

検索

CDO は、デバイス、オブジェクト、およびアクセス グループを簡単に検索できる強力な検索機能を提供します。[デバイスとサービス（Devices & Service）] 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。

同様に、[オブジェクト（Objects）] スペースの検索バーを使用して、オブジェクト名の一部、または IP アドレス、ポート、名前付きアドレス、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。

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、CDO 内で使用可能なオンボーディング済みデバイスと関連オブジェクトを検索できます。さらに、検索結果からデバイスとオブジェクトのページに直接移動できます。

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。このプロセスでは、システム内のすべてのデバイスとオブジェクトがスキャンされます。インデックス作成を呼び出した後にのみ、それらが検索インデックスに表示されます。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 （97 ページ）を参照してください。

- インデックス増分作成：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は、大文字と小文字が区別されません。デバイス名の一部、URL、IP アドレス、IP アドレス範囲、名前が付けられたデバイスやオブジェクト、オブジェクトのコンテンツなどを使用して検索を実行できます。

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（デバイスまたはオブジェクト）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、その項目の情報が右側のペインに表示されます。リストをスクロールして検索結果の項目をクリックすると、対応する情報を表示したり、対応するページに移動したりできます。

（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。
- CDO 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 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 CDO にログインします。

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

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、CDO テナントの既存のインデックスがクリアされます。

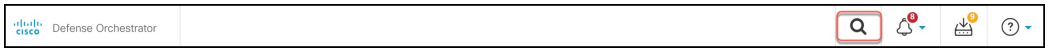
ステップ 4 ここをクリックして、グローバル検索ワークフローを表示します。

グローバル検索の実行

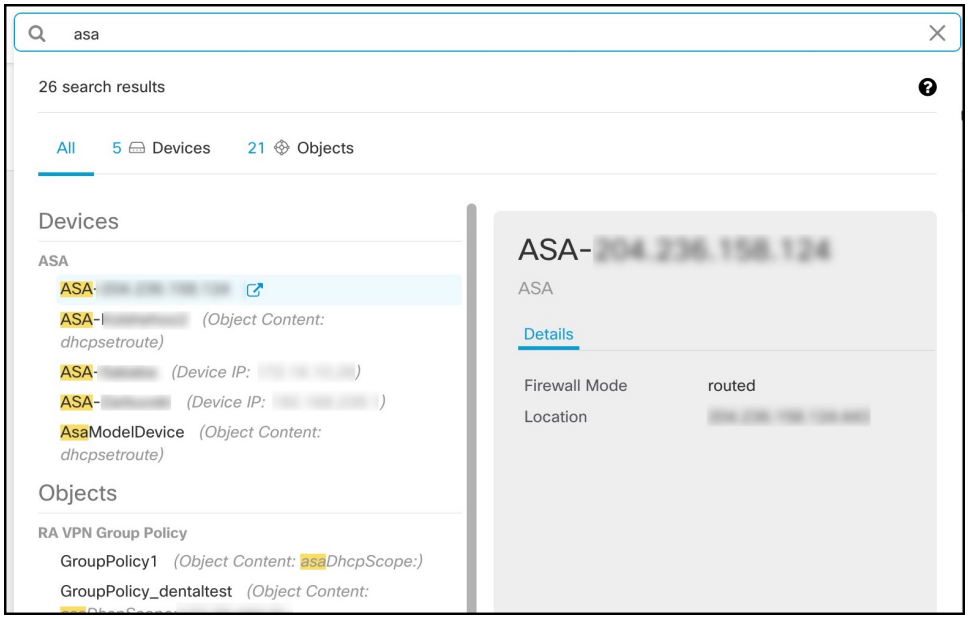
手順

ステップ 1 CDO にログインします。

ステップ 2 CDO ページの右上隅にある検索アイコンをクリックし、表示される検索フィールドに検索文字列を入力します。



検索文字列の入力を開始すると、検索候補が一覧表示されます。検索結果は、[すべて（All）]、[デバイス（Devices）]、および[オブジェクト（Objects）]の 3 つのタブの下に表示されます。



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やオブジェクトのページに移動します。

ステップ 4 [X] をクリックして検索バーを閉じます。

CDO コマンドライン インターフェイスの使用

CDO では、コマンドライン インターフェイス（CLI）を使用して FTD デバイスを管理できます。コマンドは、単一のデバイスに送信することも、複数のデバイスに同時に送信することも可能です。ここでは、CLI コマンドを単一の デバイスに送信する方法について説明します。

関連情報：

- FTD SSH CLI ドキュメントについては、『Cisco Firepower Threat Defense Command Reference』を参照してください。FTD デバイスの CLI 機能は制限されていることに注意してください。FTD デバイスでは、`show`、`ping`、`traceroute`、`packet-tracer`、`failover`、および `shutdown` コマンドのみ使用できます。

コマンドの入力方法

1 つのコマンドを 1 行に入力することも、複数のコマンドを複数の行に連続して入力することも可能で、CDO は、入力されたコマンドをバッチとして順番に実行します。次の ASA の例では、3つのネットワークオブジェクトと、それらのネットワークオブジェクトを含むネットワーク オブジェクト グループを作成するコマンドのバッチを送信します。

[ASAデバイスコマンドの入力（Entering ASA device Commands）]：CDO は、グローバル コンフィギュレーション モードでコマンドの実行を開始します。

[FTDデバイスコマンドの入力（Entering FTD device Commands）]：CLI コンソールは基本 FTD CLI を使用します。CLI コンソールを使用して、診断 CLI、エキスパート モード、および FXOS CLI（FXOS を使用するモデル）に入ることはできません。このような他の CLI モードに入る必要がある場合は、SSH を使用します。

長いコマンド：非常に長いコマンドを入力すると、CDO は、コマンドを複数のコマンドに分割して、すべてのコマンドを ASA API に対して実行できるようにします。コマンドの適切な区切りを CDO が判断できない場合、コマンドのリストをどこで区切るかのヒントを求めるプロンプトが表示されます。次に例を示します。

```
Error: CDO attempted to execute a portion of this command with a length that exceeded
600 characters. You can give a hint to CDO at where a proper command separation point
is by breaking up your list of commands with an additional empty line between them.
```

このエラーメッセージを受信した場合、次の手順を実行します。

手順

ステップ 1 CLI 履歴ペインでエラーの原因となったコマンドをクリックします。CDO は、コマンドボックスにコマンドの長いリストを入力します。

ステップ 2 関連するコマンドのグループの後に空行を挿入して、コマンドの長いリストを編集します。たとえば、上記の例のように、ネットワークオブジェクトのリストを定義し、それらをグループに追加した後に空の行を追加します。この作業を、コマンドリストのいくつかの箇所で実行することになる場合があります。

ステップ 3 [送信（Send）] をクリックします。

単一デバイスで CLI を使用する

手順

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 [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 コマンド ライン インターフェイスを使用して、管理するデバイスを選択します。

ステップ 5 デバイスの [デバイスアクション（Device Actions）] ペインで、[>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 6 上部の「コマンドペイン」にコマンドを入力し、[送信（Send）] をクリックします。コマンドに対するデバイスの応答は、「応答ペイン」の下に表示されます。

（注） 選択したデバイスが同期されていない場合、次のコマンドのみが許可されます：`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、`dir`、`write`、`copy`

コマンド履歴での動作

CLI コマンドを送信すると、CDO はそのコマンドを [コマンド ラインインターフェイス（Command Line Interface）] ページの履歴ペインに記録します。履歴ペインに保存されたコマンドは、再実行することも、コマンドをテンプレートとして使用することもできます。

手順

ステップ 1 [デバイスとサービス（Devices & Services）] ページで、設定するデバイスを選択します。

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 [>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 5 履歴ペインがまだ展開されていない場合は、時計アイコン をクリックして展開します。

ステップ 6 [履歴（History）] ペインで変更または再送信するコマンドを選択します。

ステップ 7 コマンドをそのまま再利用するか、コマンドペインでコマンドを編集し、[送信（Send）] をクリックします。CDO は、応答ペインにコマンドの結果を表示します。

（注） 次の 2 つの状況で「完了しました（Done!）」というメッセージが CDO の応答ペインに表示されます。

- OpenStack の導入要件
- コマンドの返すべき結果が何もなかった場合。たとえば、特定の設定エントリを検索する正規表現を含む show コマンドを発行したとします。この正規表現の条件に合致する設定エントリがなかった場合、CDO は「完了しました（Done!）」を返します。

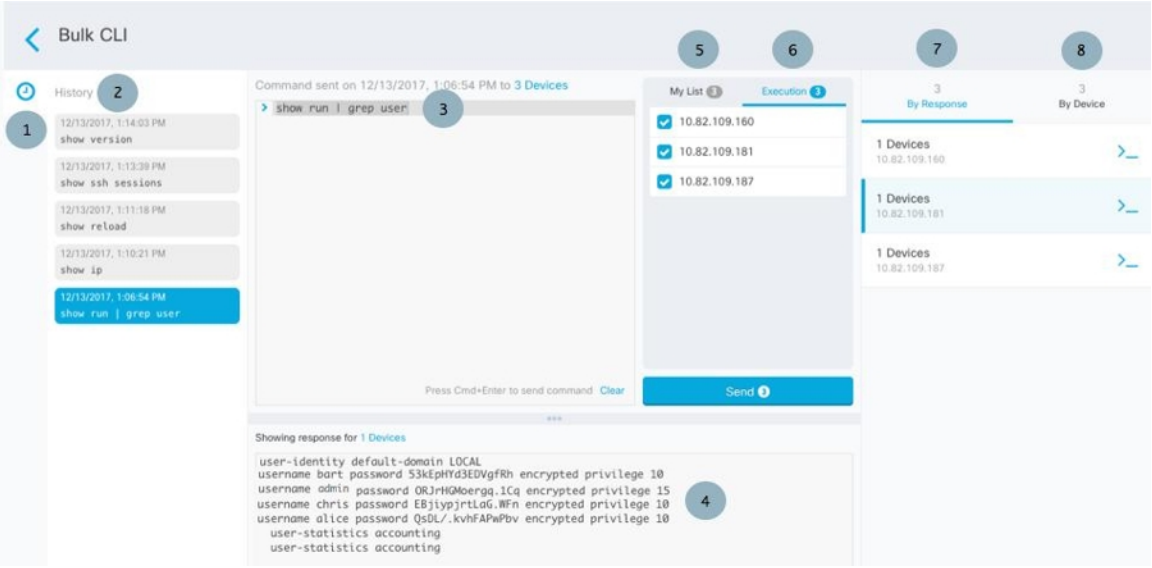
一括コマンド ライン インターフェイス

CDO では、コマンドライン インターフェイス（CLI）を使用して FTD デバイスを管理できます。コマンドは、単一のデバイスに送信することも、同じ種類の複数のデバイスに同時に送信することも可能です。この項目では、CLI コマンドを複数のデバイスに一度に送信する方法について説明します。

関連情報：

- Cisco IOS CLI のドキュメントについては、お使いの IOS バージョンの「Networking Software（IOS & NX-OS）」を参照してください。https://www.cisco.com/c/en/us/support/ios-nx-os-software/index.html
- FTD については、CDO はベース FTD CLI のみをサポートします。FTD デバイスでは、`show`、`ping`、`traceroute`、`packet-tracer`、`failover`、および `shutdown` コマンドのみ使用できます。FTD SSH CLI ドキュメントについては、『Cisco Firepower Threat Defense Command Reference』を参照してください。

一括 CLI インターフェイス



（注） 次の 2 つの状況で「**完了しました（Done!）**」というメッセージが CDO に表示されます。

- OpenStack の導入要件
- コマンドの返すべき結果が何もなかった場合。たとえば、特定の設定エントリを検索する正規表現を含む show コマンドを発行したとします。この正規表現の条件に合致する設定エントリがなかった場合、CDO は「**完了しました（Done!）**」を返します。

ケース	説明
1	コマンド履歴ペインを展開したり折りたたんだりするには、時計アイコンをクリックします。
2	コマンド履歴。コマンドを送信すると、CDO はこの履歴ペインにコマンドを記録するので、コマンドをもう一度選択し、再度実行できます。
3	コマンドペイン。このペインのプロンプトにコマンドを入力します。

ケース	説明
4	応答ペイン。CDO は、コマンドに対するデバイスの応答と CDO メッセージを表示します。複数のデバイスの応答が同じだった場合、応答ペインに「X デバイスの応答を表示しています（Showing Responses for X devices）」というメッセージが表示されます。[Xデバイス（X Devices）] をクリックすると、コマンドに対して同じ応答を返したすべてのデバイスが CDO に表示されます。 （注） 次の 2 つの状況で「**完了しました（Done!）**」というメッセージが CDO に表示されます。 • OpenStack の導入要件 • コマンドの返すべき結果が何もなかった場合。たとえば、特定の設定エントリを検索する正規表現を含む show コマンドを発行したとします。この正規表現の条件に合致する設定エントリがなかった場合、CDO は「**完了しました（Done!）**」を返します。
5	[マイリスト（My List）] タブには、[インベントリ（Inventory）] テーブルから選択したデバイスが表示されます。このタブで、コマンドを送信するデバイスを含めたり除外したりすることができます。
[6]	上の図で強調表示されている [実行（Execution）] タブには、履歴ペインで選択されているコマンドの対象デバイスが表示されます。この例では、履歴ペインで show run | grep user コマンドが選択され、[実行（Execution）] タブに、10.82.109.160、10.82.109.181、および 10.82.10.9.187 に送信されたことが表示されます。
7	[応答別（By Response）] タブをクリックすると、コマンドによって生成された応答のリストが表示されます。同一の応答は 1 行にグループ化されます。[応答別] タブで行を選択すると、CDO はそのコマンドへの応答を応答ペインに表示します。
8	[デバイス別（By Device）] タブをクリックすると、各デバイスからの個別の応答が表示されます。リスト内のいずれかのデバイスをクリックすると、特定のデバイスからのコマンドへの応答を表示できます。

コマンドの一括送信

手順

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 CLI を使用して管理するデバイスを特定して、それらを選択します。

ステップ 5 詳細ペインで、>_ [コマンド ライン インターフェイス（Command Line Interface）] をクリックします。

ステップ 6 コマンドペインにコマンドを入力して、[送信（Send）] をクリックします。コマンド出力が応答ペインに表示されます。コマンドは変更ログに記録され、CDO はコマンドを [一括CLI（Bulk CLI）] ウィンドウの [履歴（History）] ペインに記録します。

（注） 選択したデバイスが到達可能で同期されていることを確認してください。

一括コマンド履歴での動作

一括 CLI コマンドを送信すると、CDO はそのコマンドを一括 CLI インターフェイスページの履歴ペインに記録します。履歴ペインに保存されたコマンドは、再実行することも、コマンドをテンプレートとして使用することもできます。履歴ペインのコマンドは、それらが実行された元のデバイスに関連付けられています。

手順

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、設定するデバイスを選択します。

ステップ 4 [コマンドラインインターフェイス（Command Line Interface）] をクリックします。

ステップ 5 [履歴（History）] ペインで変更または再送信するコマンドを選択します。選択したコマンドは特定のデバイスに関連付けられており、最初のステップで選択したものとは限らないことに注意してください。

ステップ 6 [マイリスト（My List）] タブを見て、送信しようとしているコマンドが対象のデバイスに送信されることを確認します。

ステップ 7 コマンドペインでコマンドを編集し、[送信（Send）] をクリックします。CDO は、応答ペインにコマンドの結果を表示します。

（注） 選択したデバイスのいずれかが同期されていない場合、次のコマンドのみが許可されます：`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、`dir`、`write`、`copy`

一括コマンドフィルタでの動作

一括 CLI コマンドを実行後、[応答別（By Response）] フィルタと [デバイス別（By Device）] フィルタを使用して、デバイスの設定を続行できます。

応答別フィルタ

一括コマンドの実行後、CDO は [応答別（By Response）] タブに、コマンドを送信したデバイスから返された応答のリストを入力します。同じ応答のデバイスは1行にまとめられます。[応答別（By Response）] タブの行をクリックすると、応答ペインにデバイスからの応答が表示されます。応答ペインに複数のデバイスの応答が表示される場合、「Xデバイスの応答を表示しています（Showing Responses for X devices）」というメッセージが表示されます。[Xデバイス（X Devices）] をクリックすると、コマンドに対して同じ応答を返したすべてのデバイスが CDO に表示されます。

コマンド応答に関連付けられたデバイスのリストにコマンドを送信するには、次の手順に従います。

手順

ステップ 1 [応答別（By Response）] タブの行にあるコマンドシンボルをクリックします。

ステップ 2 コマンドペインでコマンドを確認し、[送信（Send）] をクリックしてコマンドを再送信するか、[クリア（Clear）] をクリックしてコマンドペインをクリアし、新しいコマンドを入力してデバイスに送信してから、[送信（Send）] をクリックします。

ステップ 3 コマンドから受け取った応答を確認します。

ステップ 4 選択したデバイスの実行コンフィギュレーションファイルに変更が反映されていることが確実な場合は、コマンドペインに「deploy memory」と入力し、[送信（Send）] をクリックします。この操作により、実行コンフィギュレーションがスタートアップコンフィギュレーションに保存されます。

デバイス別フィルタ

一括コマンドの実行後、CDO は [実行（Execution）] タブと [デバイス別（By Device）] タブに、コマンドを送信したデバイスのリストを入力します。[デバイス別（By Device）] タブの行をクリックすると、各デバイスの応答が表示されます。

同じデバイスリストでコマンドを実行するには、次の手順に従います。

手順

ステップ 1 [デバイス別（By Device）] タブをクリックします。

ステップ 2 [>_これらのデバイスでコマンドを実行（>_Execute a command on these devices）] をクリックします。

ステップ 3 [クリア（Clear）] をクリックしてコマンドペインをクリアし、新しいコマンドを入力します。

ステップ 4 [マイリスト（My List）] ペインで、リスト内の個々のデバイスを選択または選択解除して、コマンドを送信するデバイスのリストを指定します。

ステップ 5 [送信（Send）] をクリックします。コマンドへの応答が応答ペインに表示されます。応答ペインに複数のデバイスの応答が表示される場合、「X デバイスの応答を表示しています（Showing Responses for X devices）」というメッセージが表示されます。[X デバイス（X Devices）] をクリックすると、コマンドに対して同じ応答を返したすべてのデバイスが CDO に表示されます。

ステップ 6 選択したデバイスの実行コンフィギュレーションファイルに変更が反映されていることが確実な場合は、コマンドペインに「deploy memory」と入力し、[送信（Send）] をクリックします。

デバイスの管理用 CLI マクロ

CLI マクロは、すぐに使用できる完全な形式の CLI コマンド、または実行前に変更できる CLI コマンドのテンプレートです。すべてのマクロは、1 つ以上の FTD デバイスで同時に実行できます。

テンプレートに似た CLI マクロを使用して、複数のデバイスで同じコマンドを同時に実行します。CLI マクロは、デバイスの設定と管理の一貫性を促進します。完全な形式の CLI マクロを使用して、デバイスに関する情報を取得します。FTD デバイスですぐに使用できるさまざまな CLI マクロがあります。

頻繁に実行するタスクを監視するための CLI マクロを作成できます。詳細については、「新規コマンドからの CLI マクロの作成」を参照してください。

CLI マクロは、システム定義またはユーザー定義です。システム定義マクロは CDO によって提供され、編集も削除もできません。ユーザー定義マクロはユーザーが作成し、編集または削除できます。

（注） デバイスが CDO にオンボードされた後にのみ、デバイスのマクロを作成できます。

例として ASA を使用すると、いずれかの ASA で特定のユーザーを検索する場合は、次のコマンドを実行できます。

```
show running-config | grep username
```

このコマンドを実行すると、検索しているユーザーのユーザー名が username に置き換わります。このコマンドからマクロを作成するには、同じコマンドを使用して、username を中括弧で囲みます。

```
> show running-config | grep {{username}}
```

パラメータには任意の名前を付けることができ、そのパラメータ名で同じマクロを作成することもできます。

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

パラメータ名は説明的な名前にでき、英数字と下線を使用する必要があります。この場合、コマンドシンタックスは次のようになります。

```
show running-config | grep
```

コマンドの一部として、コマンドの送信先のデバイスに適した CLI シンタックスを使用する必要があります。

新規コマンドからの CLI マクロの作成

手順

ステップ 1 CLI マクロを作成する前に CDO のコマンド ライン インターフェイスでコマンドをテストして、コマンドの構文が正しく、信頼できる結果が返されることを確認します

（注）
- FTD デバイスの場合、CDO は FDM の CLI コンソールで実行できるコマンド（`show`、`ping`、`traceroute`、`packet-tracer`、`failover`、`reboot`、`shutdown`）のみをサポートします。これらのコマンドの構文の完全な説明については、『Cisco Firepower Threat Defense コマンドリファレンス』を参照してください。

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（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、オンラインかつ同期されているデバイスを選択します。

ステップ 5 [>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 6 CLI マクロのお気に入りのスター をクリックして、すでに存在するマクロを確認します。

ステップ 7 プラスボタン をクリックします。

ステップ 8 マクロに一意の名前を指定します。必要に応じて、CLI マクロの説明とメモを入力します。

ステップ 9 [コマンド（Command）] フィールドにコマンドを入力します。

ステップ 10 コマンドの実行時に変更したいコマンドの部分を、中括弧で囲まれたパラメータ名に置き換えます。

ステップ 11 [作成（Create）] をクリックします。作成したマクロは、最初に指定したデバイスだけでなく、そのタイプのすべてのデバイスで使用できます。

コマンドを実行するには、『CLI マクロの実行』を参照してください。

CLI 履歴または既存の CLI マクロからの CLI マクロの作成

この手順では、すでに実行したコマンド、別のユーザー定義マクロ、またはシステム定義マクロからユーザー定義マクロを作成します。

手順

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。

（注） CLI 履歴からユーザー定義マクロを作成する場合は、コマンドを実行したデバイスを選択します。CLI マクロは、同じアカウントのデバイス間で共有されますが、CLI 履歴は共有されません。

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、オンラインかつ同期されているデバイスを選択します。

ステップ 4 [>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 5 CLI マクロを作成するコマンドを見つけて選択します。次のいずれかの方法を使用してください。

- クロック をクリックして、そのデバイスで実行したコマンドを表示します。マクロに変換するコマンドを選択すると、コマンドペインにそのコマンドが表示されます。
- CLI マクロのお気に入りのスター をクリックして、すでに存在するマクロを確認します。変更するユーザー定義またはシステム定義の CLI マクロを選択します。コマンドがコマンドペインに表示されます。

ステップ 6 コマンドがコマンドペインに表示された状態で、CLI マクロの金色の星 をクリックします。このコマンドが、新しい CLI マクロの基礎になります。

ステップ 7 マクロに一意の名前を指定します。必要に応じて、CLI マクロの説明とメモを入力します。

ステップ 8 [コマンド（Command）] フィールドのコマンドを確認し、必要な変更を加えます。

ステップ 9 コマンドの実行時に変更したいコマンドの部分を、中括弧で囲まれたパラメータ名に置き換えます。

ステップ 10 [作成（Create）]をクリックします。作成したマクロは、最初に指定したデバイスだけでなく、そのタイプのすべてのデバイスで使用できます。

コマンドを実行するには、CLI マクロの実行を参照してください。

CLI マクロの実行

手順

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、1 つ以上のデバイスを選択します。

ステップ 4 [>_ コマンド ライン インターフェイス（>_Command Line Interface）] をクリックします。

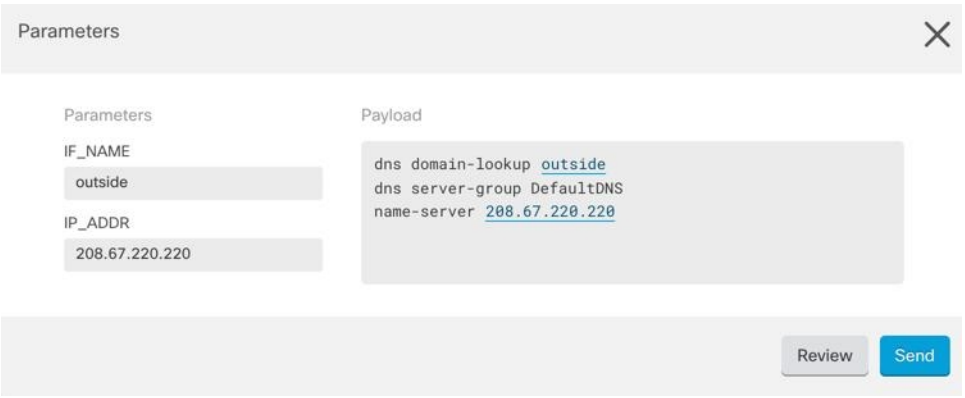
ステップ 5 コマンドパネルで、スター ★ をクリックします。

ステップ 6 コマンドパネルから CLI マクロを選択します。

ステップ 7 次のいずれかの方法でマクロを実行します。

- 定義するパラメータがマクロに含まれていない場合は、[送信（Send）] をクリックします。コマンドへの応答が応答ペインに表示されます。これで完了です。
- マクロにパラメータが含まれている場合（下の Configure DNS マクロなど）、[>_ パラメータの表示（>_ View Parameters）] をクリックします。

ステップ 8 [パラメータ（Parameters）] ペインで、パラメータの値を [パラメータ（Parameters）] の各フィールドに入力します。



ステップ 9 [送信（Send）] をクリックします。CDO が正常にコマンドを送信し、デバイスの構成を更新すると、「完了」というメッセージが表示されます。

- FTD の場合は、デバイスのアクティブな構成が更新されます。

ステップ 10 コマンドを送信した後で、「一部のコマンドが実行コンフィギュレーションに変更を加えた可能性があります」というメッセージが 2 つのリンクとともに表示されることがあります。

- [ディスクへの書き込み（Write to Disk）] をクリックすると、このコマンドによって加えられた変更と、実行コンフィギュレーションのその他の変更がデバイスのスタートアップ構成に保存されます。
- [取り消す（Dismiss）] をクリックすると、メッセージが取り消されます。

CLI マクロの編集

ユーザー定義の CLI マクロは編集できますが、システム定義のマクロは編集できません。CLI マクロを編集すると、すべての FTD デバイスでマクロが変更されます。マクロは特定のデバイス固有のものではありません。

手順

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 デバイスを選択します。
ステップ 5 [コマンドラインインターフェイス（Command Line Interface）] をクリックします。
ステップ 6 編集するユーザー定義マクロを選択します。
ステップ 7 マクロラベルの編集アイコンをクリックします。
ステップ 8 [マクロの編集（Edit Macro）] ダイアログボックスで CLI マクロを編集します。
ステップ 9 [保存（Save）] をクリックします。

CLI マクロの実行方法については、「CLI マクロの実行」を参照してください。

CLI マクロの削除

ユーザー定義の CLI マクロは削除できますが、システム定義のマクロは削除できません。CLI マクロを削除すると、すべてのデバイスでマクロが削除されます。マクロは特定のデバイス固有のものではありません。

手順

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 デバイスを選択します。
ステップ 5 [コマンド ライン インターフェイス（Command Line Interface）] をクリックします。
ステップ 6 削除するユーザー定義 CLI マクロを選択します。
ステップ 7 CLI マクロラベルのゴミ箱アイコン をクリックします。
ステップ 8 CLI マクロを削除することを確認します。

FTD コマンド ライン インターフェイスのドキュメント

CDO は、FTD コマンド ライン インターフェイスの一部をサポートしています。ユーザーが単一のデバイスおよび複数のデバイスにコマンドアンドレスポンス形式で同時にコマンドを送信できるように、CDO ではターミナル型のインターフェイスを提供しています。CDO でサポートされていないコマンドについては PuTTy や SSH クライアントなどのデバイス GUI ターミナルを使用してデバイスにアクセスし、『FTD CLI リファレンス』ドキュメントでさらに多くのコマンドを参照してください。

CLI コマンドの結果のエクスポート

スタンドアロンデバイスまたは複数のデバイスに発行された CLI コマンドの結果をコンマ区切り値（.csv）ファイルにエクスポートして、必要に応じて情報をフィルタリングおよび並べ替えることができます。単一のデバイスまたは多数のデバイスの CLI 結果を一度にエクスポートできます。エクスポートされた情報には、次のものが含まれます。

- Device
- 日付（Date）
- User
- コマンド
- 出力

CLI コマンドの結果のエクスポート

コマンドウィンドウで実行したコマンドの結果を .csv ファイルにエクスポートできます。

手順

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 つまたは複数のデバイスを選択してハイライトします。

ステップ 5 デバイスの [デバイスアクション（Device Actions）] ペインで、>_ [コマンドラインインターフェイス（Command Line Interface）] をクリックします。

ステップ 6 [コマンドラインインターフェイス（Command Line Interface）] ペインでコマンドを入力し、[送信（Send）] をクリックしてデバイスに送ります。

ステップ 7 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。

ステップ 8 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。.csv ファイル上のコマンド出力を読み取る場合、すべてのセルを展開して、コマンドのすべての結果を表示します。

CLI マクロの結果のエクスポート

コマンドウィンドウで実行されたマクロの結果をエクスポートできます。次の手順で、1 つまたは複数のデバイスで実行された CLI マクロの結果を .csv ファイルにエクスポートします。

手順

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 [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 つまたは複数のデバイスを選択してハイライトします。

ステップ 5 デバイスの [デバイスアクション（Device Actions）] ペインで、>_ [コマンドラインインターフェイス（Command Line Interface）] をクリックします。

ステップ 6 CLI ウィンドウの左側のペインで、CLI マクロのお気に入りを示す星を選択します。

ステップ 7 エクスポートするマクロコマンドをクリックします。適切なパラメータを入力し、[送信（Send）] をクリックします。

ステップ 8 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。

ステップ 9 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。.csv ファイル上のコマンド出力を読み取る場合、すべてのセルを展開して、コマンドのすべての結果を表示します。

CLI コマンド履歴のエクスポート

次の手順を使用して、1 つまたは複数のデバイスの CLI 履歴を .csv ファイルにエクスポートします。

手順

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 1 つまたは複数のデバイスを選択してハイライトします。

ステップ 5 デバイスの [デバイスアクション（Device Actions）] ペインで、[>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 6 履歴ペインがまだ展開されていない場合は、[時計（Clock）] アイコン をクリックして展開します。

ステップ 7 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。

ステップ 8 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。.csv ファイル上のコマンド出力を読み取る場合、すべてのセルを展開して、コマンドのすべての結果を表示します。

関連情報：

- CDO コマンドライン インターフェイスの使用 （99 ページ）
- 新規コマンドからの CLI マクロの作成
- CLI マクロの削除
- CLI マクロの編集
- CLI マクロの実行
- FTD コマンド ライン インターフェイスのドキュメント
- 一括コマンド ライン インターフェイス

CLI マクロのリストをエクスポートする

コマンドウィンドウで実行されたマクロのみをエクスポートできます。次の手順で、1 つまたは複数のデバイスの CLI マクロを .csv ファイルにエクスポートします。

手順

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 1 つまたは複数のデバイスを選択してハイライトします。

ステップ 5 デバイスの[デバイスアクション]ペインで、[>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 6 CLI ウィンドウの左側のペインで、CLI マクロのお気に入りを示す星を選択します。

ステップ 7 エクスポートするマクロコマンドをクリックします。適切なパラメータを入力し、[送信（Send）] をクリックします。

ステップ 8 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。

ステップ 9 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。

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 では、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はそのコピーを作成し、そのコピーを使用します。

[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オブジェクトフィルタします。
- 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、CDO のトラブルシューティングを参照してください。

オブジェクト タイプ

以下の表では、デバイス用に作成し、CDO を使用して管理できるオブジェクトについて説明します。

表 *4 : Firepower Threat Defense*（*FTD*）オブジェクトタイプ

オブジェクト	説明
アプリケーション フィルタ オブジェクト	アプリケーション フィルタ オブジェクトは、IP 接続で使用されるアプリケーション、あるいはタイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性によってアプリケーションを定義するフィルタを定義します。ポートの仕様を使用する代わりに、これらのオブジェクトをポリシーで使用し、トラフィックを制御できます。

オブジェクト	説明
AnyConnect クライアント プロファイル	AnyConnect クライアント プロファイル オブジェクトは、通常はリモートアクセス VPN ポリシーの構成で使用するファイルオブジェクトおよび表明ファイルです。このオブジェクトには、AnyConnect クライアントプロファイルと AnyConnect クライアントイメージファイルを含めることができます。
証明書オブジェクト	デジタル証明書は、認証に使用されるデジタル ID を提供します。証明書は、SSL（セキュア ソケット レイヤ）、TLS（Transport Layer Security）、およびDTLS（データグラム TLS）接続（HTTPS や LDAPS など）に使用されます。
DNS グループオブジェクト	www.example.com などの完全修飾ドメイン名（FQDN）を IP アドレスに解決するのには、DNS サーバーが必要です。管理インターフェイスとデータインターフェイスに異なる DNS グループオブジェクトを構成できます。
Firepower 地理位置情報フィルタオブジェクトの作成と編集	地理位置情報オブジェクトは、トラフィックの送信元または接続先であるデバイスをホストする国と大陸を定義します。IP アドレスを使用する代わりに、これらのオブジェクトをポリシーで使用してトラフィックを制御できます。
FTD IKEv1 ポリシーの作成または編集	IKEv1 ポリシーオブジェクトには、VPN 接続を定義する際に IKEv1 ポリシーに必要なパラメータが含まれています。
IKEv2 ポリシー	IKEv2 ポリシーオブジェクトには、VPN 接続を定義する際に IKEv2 ポリシーに必要なパラメータが含まれています。
IKEv1 IPSec プロポーザル	IPsec プロポーザル オブジェクトは、IKE フェーズ 1 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルでは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。

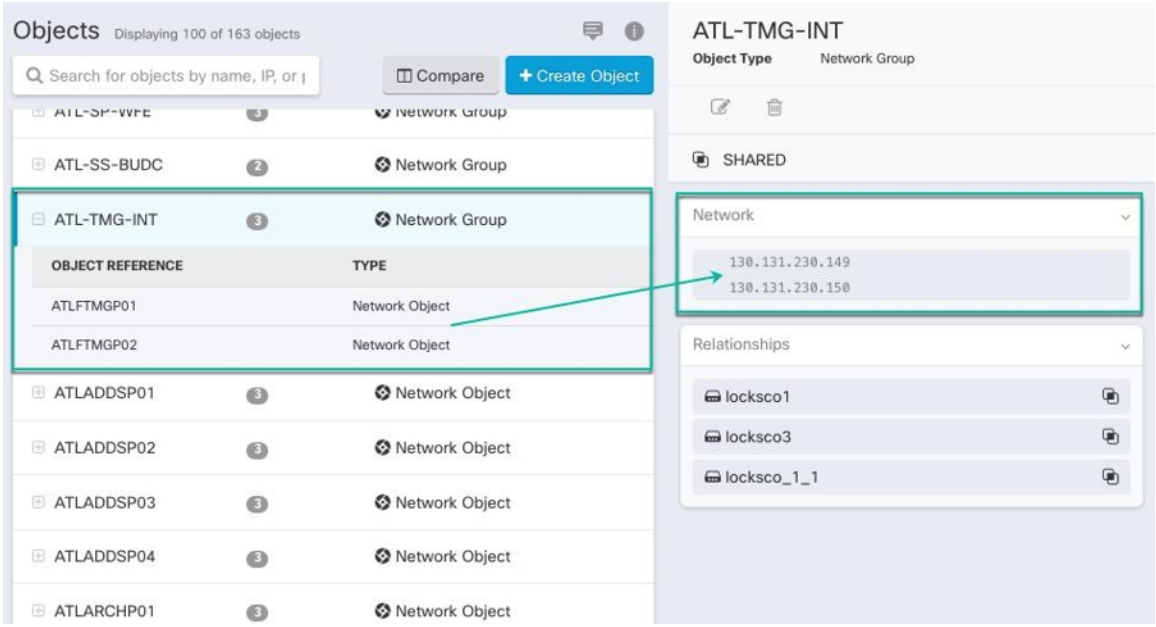
オブジェクト	説明
IKEv2 IPSec プロポーザル	IPsec プロポーザル オブジェクトは、IKE フェーズ 2 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルでは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。
ネットワーク オブジェクト	ホストまたはネットワークのアドレスを定義するネットワーク グループおよびネットワーク オブジェクト（総称してネットワーク オブジェクトと呼ばれます）。
セキュリティ ゾーン オブジェクト	セキュリティ ゾーンとはインターフェイスのグループ分けです。ゾーンは、トラフィックの管理と分類に役立つようにネットワークをセグメントに分割します。
サービス オブジェクト	サービスオブジェクト、サービスグループ、ポートグループは、TCP/IP プロトコルスイートの一部が考慮されたプロトコルまたはポートを含む再利用可能なコンポーネントです。
FTD SGT グループの作成	SGT ダイナミックオブジェクトは、ISE によって割り当てられた SGT に基づいて送信元または宛先アドレスを識別し、着信トラフィックと照合できます。
Syslog サーバーオブジェクト	syslog サーバーのオブジェクトはコネクション型メッセージまたは診断システム ログ（syslog）メッセージを受信できるサーバーを指定します。
URL オブジェクト	URL オブジェクトとグループ（URL オブジェクトと総称する）を使用して、Web リクエストの URL または IP アドレスを定義します。これらのオブジェクトを使用して、アクセス制御ポリシーに手動の URL フィルタリング、またはセキュリティ インテリジェンス ポリシーにブロッキングを実装できます。

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） CDO を使用すると、ルールセット内のルールに関連付けられたオブジェクトを上書きできます。新しいオブジェクトをルールに追加する場合、デバイスをルールセットに接続して変更を保存しないと、オブジェクトを上書きできません。詳細については、「FTD のルールセットの設定」を参照してください。

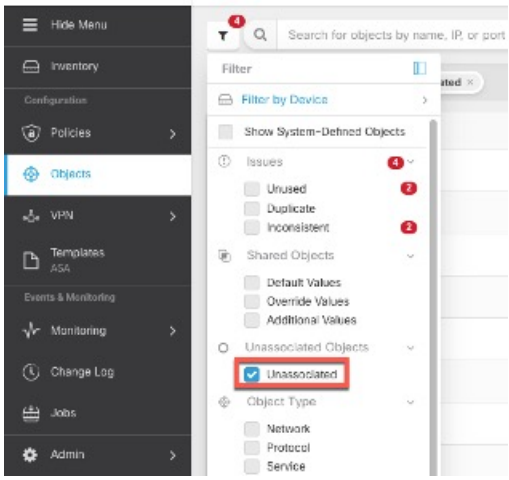
（注） 一貫性のないオブジェクトがある場合は、オーバーライドを使用してそれらを 1 つの共有オブジェクトに結合できます。詳細については、不整合オブジェクトの問題を解決するを参照してください。

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 はそのコピーを作成し、そのコピーを使用します。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 ジョブによって削除されるか、ユーザーが削除するまで、使用可能なオブジェクトのリストに残ります。

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 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

手順

ステップ 1 [オブジェクト（Objects）] ページを開きます。

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）] ページおよび [オブジェクト（Objects）] ページの各種フィルタを使用して、目的のデバイスや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、およびラベルを指定して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。

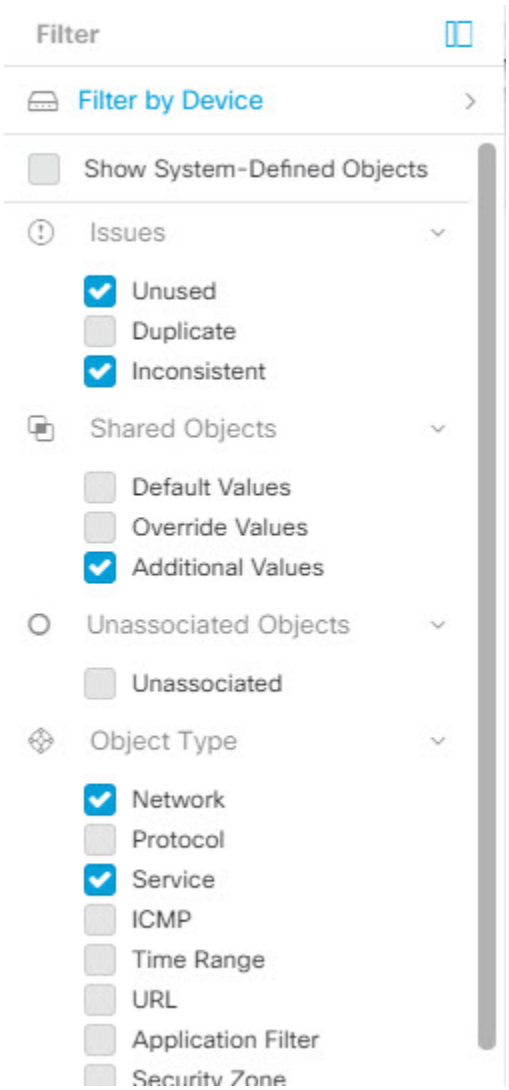
（注） [FTD] タブを開くと、フィルタペインでフィルタを使用できます。これにより、CDO からデバイスにアクセスするために使用されている管理アプリケーションに基づいて FTD デバイスが表示されます。

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

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、検索用語を組み合わせて、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できます。

次の例では、「問題（使用済みまたは不整合）があるオブジェクト、追加の値を持つ共有オブジェクト、特定タイプ（ネットワークまたはサービス）のオブジェクト」のすべての条件を満たす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、フィルターバーで [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、フィルターバーで [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。

手順

ステップ 1 ナビゲーションバーで [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

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。

手順

ステップ 1 [オブジェクト（Objects）] ページを開きます。

ステップ 2 オブジェクトフィルタ。

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

1 つのオブジェクトを削除するには、次の手順を実行します。

手順

ステップ 1 [オブジェクト（Objects）] タブをクリックして、[オブジェクト（Objects）] ページを開きます。

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 行った変更をレビューして展開するか、複数の変更を後から一度に展開します。

未使用の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。

手順

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処理すると、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チェックボックスを個別にオンにします。

ステップ 3 操作ウィンドウで、削除アイコン をクリックします。

ステップ 4 行った変更を今すぐレビューして展開するか、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**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集合体です。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 *5:* 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	[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
FTD	IPv4 と IPv6	対応	対応	対応	対応

表 *6:* 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	IP 値	ネットワークオブジェクト	ネットワークグループ
FTD	×	対応	対応

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。

関連情報：

- 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作成または編集

ASA ネットワークオブジェクトおよびネットワークグループの作成または編集

ASA ネットワークオブジェクトには、CIDR 表記で表現されたホスト名、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、アクセスルール、ネットワークポリシー、および NAT ルールで使用されるネットワークオブジェクト、ネットワークグループ、および IP アドレスの集合体です。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	[IPv4 / IPv6]	シングル アドレス	アドレス範囲	部分修飾ドメイン名（PQDN）	CIDR 表記法によるサブネット
ASA	IPv4	対応	対応	対応	対応

ASA ネットワークオブジェクトの作成

手順

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

ステップ 2 青色のプラスボタン  をクリックして、オブジェクトを作成します。

ステップ 3 **[ASA] > [ネットワーク（Network）]** をクリックします。

ステップ 4 オブジェクト名を入力します。

ステップ 5 [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 6 （任意）オブジェクトの説明を入力します。

ステップ 7 [値（Value）] セクションで、次のいずれかの方法で IP アドレス情報を追加します。

- [eq] を選択し、単一の IP アドレス、CIDR 表記を使用したサブネットアドレス、または部分修飾ドメイン名（PQDN）を入力します。
- [範囲（range）] を選択し、IP アドレスの範囲を入力します。範囲の開始アドレスと終了アドレスをスペースで区切って入力します。例：10.1.1.1 10.1.1.255。

ステップ 8 [追加（Add）] をクリックします。

重要 新たに作成されたネットワークオブジェクトは、ルールやポリシーの一部ではないため、いずれの ASA デバイスにも関連付けられていません。それらのオブジェクトを表示するには、オブジェクトフィルタで [関連付けなし（Unassociated）] オブジェクトカテゴリを選択します。詳細については、「オブジェクトフィルタ」を参照してください。デバイスのルールやポリシーに関連付けられていないオブジェクトを使用すると、そのオブジェクトはそのデバイスに関連付けられます。

ASA ネットワーク グループの作成

[ネットワークグループ（Network Group）] には、IP アドレス値、ネットワークオブジェクト、およびネットワークグループを含めることができます。新しい [ネットワークグループ（Network Group）] を作成するときに、名前、IP アドレス、IP アドレス範囲、または FQDN で既存のオブジェクトを検索し、[ネットワークグループ（Network Group）] に追加できます。オブジェクトが存在しない場合は、同じインターフェイスでそのオブジェクトをすぐに作成し、[ネットワークグループ（Network Group）] に追加できます。

手順

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

ステップ 2 青色のプラスボタン  をクリックして、オブジェクトを作成します。

ステップ 3 **[ASA]** > **[ネットワーク（Network）]** をクリックします。

ステップ 4 [オブジェクト名（Object Name）] を入力します。

ステップ 5 [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 6 （任意）オブジェクトの説明を入力します。

ステップ 7 [値（Values）] フィールドに、値またはオブジェクト名を入力します。入力を開始すると、入力に一致するオブジェクト名または値が CDO によって表示されます。

ステップ 8 表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。

ステップ 9 CDO で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、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を新しいネットワークグループに追加します。

ステップ 10 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

- [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
- [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。
- [値の追加（Add Value）] をクリックして、オブジェクトを使用せずにインライン値を作成します。値を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

（注） 編集アイコンをクリックして、詳細を変更できます。削除ボタンをクリックしても、オブジェクト自体は削除されず、代わりに、ネットワークグループから削除されます。

ステップ 11 必要なオブジェクトを追加したら、[保存（Save）] をクリックして新しいネットワークグループを作成します。

ステップ 12 すべてのデバイスの設定変更のプレビューと展開。

ASA ネットワークオブジェクトの編集

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（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 ネットワークオブジェクトを選択し、[アクション（Actions）] ペインで編集アイコン をクリックします。

ステップ 4 ダイアログボックスの値を、上記の手順で作成したときと同じ方法で編集します。

（注） ネットワークグループからオブジェクトを削除するには、横にある削除アイコンをクリックします。

ステップ 5 [保存（Save）] をクリックします。CDO は、変更の影響を受けるデバイスを表示します。

ステップ 6 [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デバイスへの変更を確定します。

ASA ネットワークグループの編集

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（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（Search）] フィールドを使用して、編集するネットワークグループを見つけます。

ステップ 3 ネットワークグループを選択し、[アクション（Actions）] ペインで編集アイコン をクリックします。

ステップ 4 ネットワークグループにすでに追加されているオブジェクトまたはネットワークグループを変更する場合は、次の手順を実行します。

1. オブジェクト名またはネットワークグループの横に表示される編集アイコン をクリックして、それらを変更します。
2. チェックマークをクリックして変更内容を保存します。

（注） 削除アイコンをクリックして、ネットワークグループから値を削除できます。

ステップ 5 ネットワークグループに新しい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を追加する場合は、次の手順を実行する必要があります。

1. [値（Values）] フィールドに、新しい値または既存のネットワークオブジェクトの名前を入力します。入力を開始すると、入力に一致するオブジェクト名または値が CDO によって表示されます。表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。
2. CDO で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、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を新しいネットワークグループに追加します。
3. 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

- [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
- [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。
- [値の追加（Add Value）] をクリックして、オブジェクトを使用せずにインライン値を作成します。値を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

ステップ 6 [保存（Save）] をクリックします。CDO は、変更の影響を受けるポリシーを表示します。

ステップ 7 [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デバイスへの変更を確定します。

ステップ 8 すべてのデバイスの設定変更のプレビューと展開。

共有ネットワークグループへの追加の値の追加

関連付けられたすべてのデバイスに存在する共有ネットワークグループ内の値は、「デフォルト値」と呼ばれます。CDO を使用すると、共有ネットワークグループに「追加の値」を追加し、それらの値をその共有ネットワークグループに関連付けられたいくつかのデバイスに割り当てることができます。CDO がデバイスに変更を展開するときに、内容が決定され、「デフォルト値」が共有ネットワークグループに関連付けられているすべてのデバイスにプッシュされ、「追加の値」が指定されたデバイスにのみプッシュされます。

たとえば、本社に 4 つの AD メインサーバーがあり、すべての拠点からアクセスできる必要があるシナリオを考えてみます。この状況で、すべての拠点で使用する「Active-Directory」という名前のオブジェクトグループを作成しました。ここで、ブランチオフィスの 1 つにさらに 2 つの AD サーバーを追加します。これを行うには、オブジェクトグループ「Active-Directory」で、ブランチオフィスに固有の追加値として詳細を追加します。これら 2 つのサーバーは、オブジェクト「Active-Directory」が一貫しているか、または共有されているかの判断には関与しません。したがって、4 つの AD メインサーバーはすべての拠点からアクセスできますが、ブランチオフィス（2 つの追加サーバーがある）は 2 つの AD サーバーと 4 つの AD メインサーバーにアクセスできます。

（注） 一貫性のない共有ネットワークグループがある場合は、追加の値を使用してそれらを 1 つの共有ネットワークグループに結合できます。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。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（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、編集する共有ネットワークグループを見つけます。

ステップ 3 [アクション（Actions）] ペインにある編集アイコン をクリックします。

- [デバイス（Devices）] フィールドには、共有ネットワークグループが存在するデバイスが表示されます。
- [使用（Usage）] フィールドには、共有ネットワークグループに関連付けられたルールセットが表示されます。
- [デフォルト値] フィールドは、デフォルトのネットワークオブジェクトと、オブジェクトの作成時に指定された、共有ネットワークグループに関連付けられたオブジェクト値が示されます。このフィールドの横に、このデフォルト値を含むデバイスの数が表示され、クリックすると名前とデバイスタイプを表示できます。この値に関連付けられたルールセットも表示されます。

ステップ 4 [追加の値（Additional Values）] フィールドに、値または名前を入力します。 入力を開始すると、入力に一致するオブジェクト名または値が CDO によって表示されます。

ステップ 5 表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。

ステップ 6 CDO で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、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を新しいネットワークグループに追加します。

ステップ 7 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

- [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
- [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。
- [値の追加（Add Value）] をクリックして、オブジェクトを使用せずにインライン値を作成します。値を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

ステップ 8 [デバイス（Devices）] 列で、新しく追加されたオブジェクトに関連付けられているセルをクリックし、[デバイスの追加（Add Devices）] をクリックします。

ステップ 9 必要なデバイスを選択し、[OK] をクリックします。

ステップ 10 [保存（Save）] をクリックします。CDO は、変更の影響を受けるデバイスを表示します。

ステップ 11 [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デバイスへの変更を確定します。

ステップ 12 すべてのデバイスの設定変更のプレビューと展開。

共有ネットワークグループの追加の値の編集

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（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、編集対象のオーバーライドがあるオブジェクトを見つけます。

ステップ 3 [アクション（Actions）] ペインにある編集アイコン をクリックします。

ステップ 4 オーバーライド値を変更します。

- 値を変更するには、編集アイコンをクリックします。
- [デバイス（Devices）]列のセルをクリックして、新しいデバイスを割り当てます。すでに割り当てられているデバイスを選択し、[オーバーライドの削除（Remove Overrides）] をクリックすると、そのデバイスのオーバーライドを削除できます。
- [デフォルト値（Default Values）] の 矢印をクリックすると、共有ネットワークグループの追加値にできます。共有ネットワークグループに関連付けられているすべてのデバイスが、自動的に割り当てられます。
- [オーバーライド値（Override Values）] の 矢印をクリックすると、共有ネットワークグループのデフォルト値にできます。
- ネットワークグループからオブジェクトを削除するには、横にある削除アイコンをクリックします。

ステップ 5 [保存（Save）] をクリックします。CDO は、変更の影響を受けるデバイスを表示します。

ステップ 6 [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デバイスへの変更を確定します。

ステップ 7 すべてのデバイスの設定変更のプレビューと展開。

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作成または編集

Firepower ネットワークオブジェクトには、CIDR 表記で表現されたホスト名、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、アクセスルール、ネットワークポリシー、およびNATルールで使用されるネットワークオブジェクトとネットワークグループの集合体です。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。

表 *7:* 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	[IPv4 / IPv6]	シングル アドレス	アドレス範囲	部分修飾ドメイン名（PQDN）	CIDR 表記によるサブネット
Firepower	[IPv4 / IPv6]	対応	対応	対応	対応

関連情報

- Firepower ネットワークオブジェクトの作成 （134 ページ）
- Firepower ネットワークオブジェクトの編集 （136 ページ）
- 共有ネットワークグループへの追加の値の追加 （137 ページ）
- 共有ネットワークグループの追加の値の編集 （139 ページ）

Firepower ネットワークオブジェクトの作成

手順

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）] をクリックします。

ステップ 2 青色のプラスボタン をクリックして、オブジェクトを作成します。

ステップ 3 **[FTD]** > **[ネットワーク（Network）]** をクリックします。

ステップ 4 [オブジェクト名（Object Name）] を入力します。

ステップ 5 [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 6 [値（Value）] セクションで、次の手順を実行します。

- [eq] を選択し、単一の IP アドレス、CIDR 表記で表されるサブネットアドレス、または部分修飾ドメイン名（PQDN）を入力します。
- [範囲（range）] を選択し、IP アドレスの範囲を入力します。

ステップ 7 [追加（Add）] をクリックします。

注意 : 新たに作成されたネットワークオブジェクトは、ルールやポリシーの一部ではないため、いずれの FTD デバイスにも関連付けられていません。それらのオブジェクトを表示するには、オブジェクトフィルタで [関連付けなし（Unassociated）] オブジェクトカテゴリを選択します。詳細については、「オブジェクトフィルタを設定する」を参照してください。デバイスのルールやポリシーに関連付けられていないオブジェクトを使用すると、そのオブジェクトはそのデバイスに関連付けられます。

Firepower ネットワークグループの作成

[ネットワークグループ（Network Group）] には、ネットワークオブジェクトとネットワークグループを含めることができます。新しい [ネットワークグループ（Network Group）] を作成すると、名前、IP アドレス、IP アドレス範囲、または FQDN で既存のオブジェクトを検索し、[ネットワークグループ（Network Group）] に追加できます。オブジェクトが存在しない場合は、同じインターフェイスでそのオブジェクトをすぐに作成し、[ネットワークグループ（Network Group）] に追加できます。

手順

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）] をクリックします。

ステップ 2 青色のプラスボタン をクリックして、オブジェクトを作成します。

ステップ 3 **[FTD] > [ネットワーク（Network）]** をクリックします。

ステップ 4 [オブジェクト名（Object Name）] を入力します。

ステップ 5 [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 6 [値（Values）] フィールドに、値または名前を入力します。入力を開始すると、入力に一致するオブジェクト名または値が CDO によって表示されます。

ステップ 7 表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。

ステップ 8 CDO で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、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を新しいネットワークグループに追加します。

ステップ 9 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

- [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
- [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

注：編集アイコンをクリックして、詳細を変更できます。削除ボタンをクリックしても、オブジェクト自体は削除されず、代わりに、ネットワークグループから削除されます。

ステップ 10 必要なオブジェクトを追加したら、[保存（Save）] をクリックして新しいネットワークグループを作成します。

ステップ 11 すべてのデバイスの設定変更をプレビューして展開します。

Firepower ネットワークオブジェクトの編集

手順

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）] をクリックします。

ステップ 2 オブジェクトフィルタと [検索（search）] 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 ネットワークオブジェクトを選択し、[アクション（Actions）] ペインで編集アイコン をクリックします。

ステップ 4 「Firepower ネットワークグループの作成」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。注：ネットワークグループからオブジェクトを削除するには、横にある削除アイコンをクリックします。

ステップ 5 [保存（Save）] をクリックします。CDO は、変更の影響を受けるデバイスを表示します。

ステップ 6 [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デバイスへの変更を確定します。

Firepower ネットワークグループの編集

手順

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）] をクリックします。

ステップ 2 オブジェクトフィルタと [検索（Search）] フィールドを使用して、編集するネットワークグループを見つけます。

ステップ 3 ネットワークグループを選択し、[アクション（Actions）] ペインで編集アイコン をクリックします。

ステップ 4 オブジェクトの名前と説明を必要に応じて変更します。

ステップ 5 ネットワークグループにすでに追加されているオブジェクトまたはネットワークグループを変更する場合は、次の手順を実行します。

1. オブジェクト名またはネットワークグループの横に表示される編集アイコン をクリックして、それらを変更します。
2. チェックマークをクリックして変更内容を保存します。**注**：削除アイコンをクリックして、ネットワークグループから値を削除できます。

ステップ 6 ネットワークグループに新しい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を追加する場合は、次の手順を実行する必要があります。

1. [値（Values）] フィールドに、新しい値または既存のネットワークオブジェクトの名前を入力します。入力を開始すると、入力に一致するオブジェクト名または値が CDO によって表示されます。表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。
2. CDO で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、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を新しいネットワークグループに追加します。
3. 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。
   - [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
   - [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

ステップ 7 [保存（Save）] をクリックします。CDO は、変更の影響を受けるポリシーを表示します。

ステップ 8 [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デバイスへの変更を確定します。

ステップ 9 すべてのデバイスの設定変更をプレビューして展開します。

共有ネットワークグループへの追加の値の追加

関連付けられたすべてのデバイスに存在する共有ネットワークグループ内の値は、「デフォルト値」と呼ばれます。CDO を使用すると、共有ネットワークグループに「追加の値」を追加し、それらの値をその共有ネットワークグループに関連付けられたいくつかのデバイスに割り当てることができます。CDO がデバイスに変更を展開するときに、内容が決定され、「デフォルト値」が共有ネットワークグループに関連付けられているすべてのデバイスにプッシュされ、「追加の値」が指定されたデバイスにのみプッシュされます。

たとえば、本社に 4 つの AD メインサーバーがあり、すべての拠点からアクセスできる必要があるシナリオを考えてみます。この状況で、すべての拠点で使用する「Active-Directory」とい

う名前のオブジェクトグループを作成しました。ここで、ブランチオフィスの 1 つにさらに 2 つの AD サーバーを追加します。これを行うには、オブジェクトグループ「Active-Directory」で、ブランチオフィスに固有の追加値として詳細を追加します。これら2つのサーバーは、オブジェクト「Active-Directory」が一貫しているか、または共有されているかの判断には関与しません。したがって、4 つの AD メインサーバーはすべての拠点からアクセスできますが、ブランチオフィス（2 つの追加サーバーがある）は 2 つの AD サーバーと 4 つの AD メインサーバーにアクセスできます。

（注） 一貫性のない共有ネットワークグループがある場合は、追加の値を使用してそれらを1つの共有ネットワークグループに結合できます。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。

手順

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、編集する共有ネットワークグループを見つけます。

ステップ 3 [アクション（Actions）] ペインにある編集アイコン をクリックします。

- [デバイス（Devices）]フィールドには、共有ネットワークグループが存在するデバイスが表示されます。
- [使用（Usage）]フィールドには、共有ネットワークグループに関連付けられたルールセットが表示されます。
- [デフォルト値]フィールドは、デフォルトのネットワークオブジェクトと、オブジェクトの作成時に指定された、共有ネットワークグループに関連付けられたオブジェクト値が示されます。このフィールドの横に、このデフォルト値を含むデバイスの数が表示され、クリックすると名前とデバイスタイプを表示できます。この値に関連付けられたルールセットも表示されます。

ステップ 4 [追加の値（Additional Values）] フィールドに、値または名前を入力します。入力を開始すると、入力に一致するオブジェクト名または値が CDO によって表示されます。

ステップ 5 表示されている既存のオブジェクトの1つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。

ステップ 6 CDO で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）]をクリックして、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を新しいネットワークグループに追加します。

ステップ 7 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

- [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
- [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

ステップ 8 [デバイス（Devices）] 列で、新しく追加されたオブジェクトに関連付けられているセルをクリックし、[デバイスの追加（Add Devices）] をクリックします。

ステップ 9 必要なデバイスを選択し、[OK] をクリックします。

ステップ 10 [保存（Save）] をクリックします。CDO は、変更の影響を受けるデバイスを表示します。

ステップ 11 [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デバイスへの変更を確定します。

ステップ 12 すべてのデバイスの設定変更をプレビューして展開します。

共有ネットワークグループの追加の値の編集

手順

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、編集対象のオーバーライドがあるオブジェクトを見つけます。

ステップ 3 [アクション（Actions）] ペインにある編集アイコン をクリックします。

ステップ 4 オーバーライド値を変更します。

- 値を変更するには、編集アイコンをクリックします。
- [デバイス（Devices）] 列のセルをクリックして、新しいデバイスを割り当てます。すでに割り当てられているデバイスを選択し、[オーバーライドの削除（Remove Overrides）] をクリックすると、そのデバイスのオーバーライドを削除できます。
- [デフォルト値（Default Values）] の 矢印をクリックすると、共有ネットワークグループの追加値にできます。共有ネットワークグループに関連付けられているすべてのデバイスが、自動的に割り当てられます。
- [オーバーライド値（Override Values）] の 矢印をクリックすると、共有ネットワークグループのデフォルト値にできます。
- ネットワークグループからオブジェクトを削除するには、横にある削除アイコンをクリックします。

ステップ 5 [保存（Save）] をクリックします。CDO は、変更の影響を受けるデバイスを表示します。

ステップ 6 [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デバイスへの変更を確定します。

ステップ 7 すべてのデバイスの設定変更をプレビューして展開します。

アプリケーション フィルタ オブジェクト

アプリケーション フィルタ オブジェクトは、Firepower デバイスによって使用されます。アプリケーション フィルタ オブジェクトは、IP 接続で使用されるアプリケーション、あるいはタイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性によってアプリケーションを定義するフィルタを定義します。ポートの仕様を使用する代わりに、これらのオブジェクトをポリシーで使用し、トラフィックを制御できます。

個々のアプリケーションを指定することはできますが、アプリケーションフィルタはポリシーの作成や管理を簡素化します。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックする、アクセス コントロール ルールを作成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとすると、セッションがブロックされます。

アプリケーション フィルタ オブジェクトを使用せず、ポリシーのアプリケーションとアプリケーション フィルタを直接選択できます。ただし、同じアプリケーションまたはフィルタ グループに対して複数のポリシーを作成する場合にはオブジェクトが便利です。システムには、事前に定義されたいくつかのアプリケーションフィルタが含まれていて、これらは編集または削除できません。

（注） シスコは、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にアプリケーションディテクタを更新し追加しています。そのため、手動でルールを更新することなく、高リスクのアプリケーションをブロックするルールを新しいアプリケーションに自動的に適用できます。

（注） FDM 管理の FTD デバイスが CDO にオンボードされると、アクセスルールまたは SSL 復号化で定義されたルールを変更することなく、アプリケーションフィルタがアプリケーションフィルタ オブジェクトに変換されます。設定が変更されたため、デバイスの設定ステータスが [非同期（Not Synced）] に変更されるので、CDO から設定を展開する必要があります。一般に、FDMは、フィルタを手動で保存するまで、アプリケーションフィルタをアプリケーションフィルタ オブジェクトに変換しません。

関連情報：

- Firepower アプリケーション フィルタ オブジェクトの作成と編集

• オブジェクトの削除

Firepower アプリケーション フィルタ オブジェクトの作成と編集

アプリケーション フィルタ オブジェクトを使用すると、厳選されたアプリケーションまたはフィルタによって識別されるアプリケーションのグループを対象にできます。このアプリケーション フィルタ オブジェクトは、ポリシーで使用できます。

Firepower アプリケーション フィルタ オブジェクトの作成

アプリケーション フィルタ オブジェクトを作成するには、次の手順を実行します。

手順

ステップ 1 [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

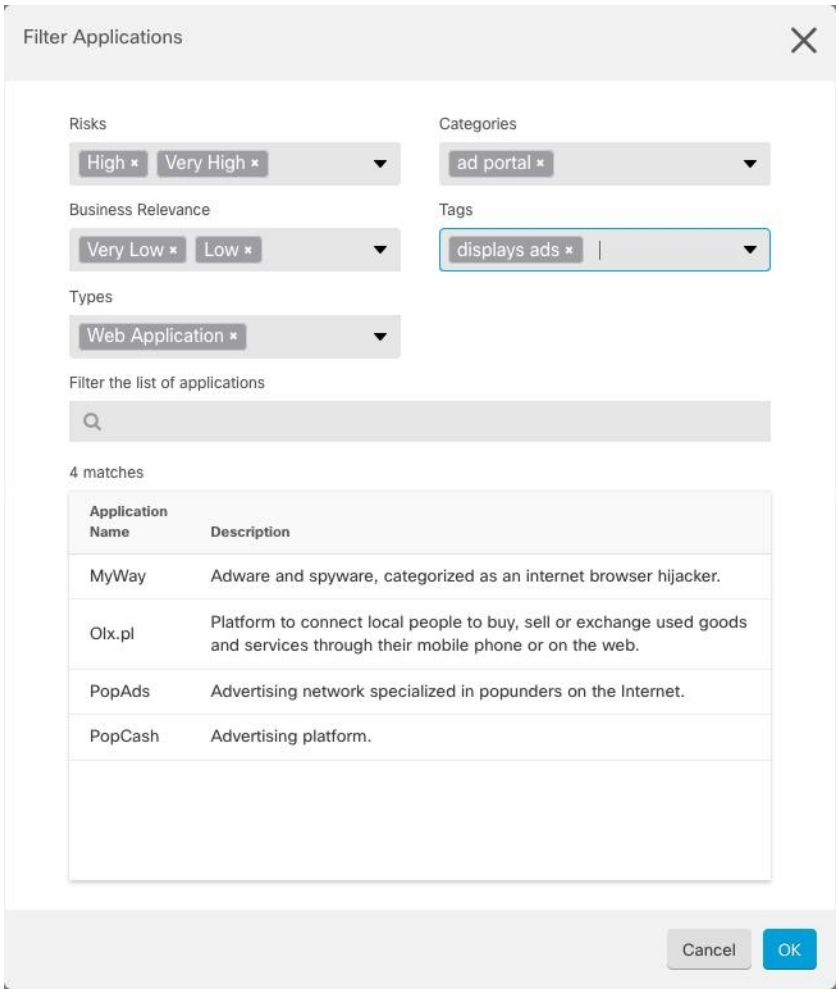
ステップ 2 [オブジェクトの作成（Create Object）] > [FTD] > [アプリケーションサービス（Application Service）] をクリックします。

ステップ 3 そのオブジェクトの**オブジェクト名**を入力し、任意で**説明**を入力します。

ステップ 4 [フィルタの追加（Add Filter）] をクリックし、オブジェクトに追加するアプリケーションとフィルタを選択します。

最初のリストには、継続的にスクロールするリストでアプリケーションが表示されます。[フィルタの詳細設定（Advanced Filter）] をクリックすると、フィルタ オプションが表示され、アプリケーションを容易に選択できます。選択したら、[追加（Add）] をクリックします。このプロセスを繰り返して、アプリケーションやフィルタを追加できます。

（注） 1 つのフィルタ条件内での複数の選択は OR 関係にあります。たとえば、リスクが「高（High）」または（OR）「非常に高い（Very High）」となります。フィルタ間の関係は「論理積（AND）」であるため、リスクが「高（High）」または（OR）「非常に高い（Very High）」であり、かつ（AND）ビジネスとの関連性が「低（Low）」または（OR）「非常に低い（Very Low）」となります。フィルタを選択すると、ディスプレイに表示されるアプリケーションが更新され、条件を満たすものだけが表示されます。これらのフィルタを使用すると、個別に追加するアプリケーションを容易に見つけたり、ルールに追加する目的のフィルタを選択していることを確認したりできます。



[リスク（Risks）]：アプリケーションが組織のセキュリティポリシーに反する可能性がある目的のために使用される確率（「非常に低い」から「非常に高い」まで）。

[ビジネスとの関連性（Business Relevance）]：アプリケーションが、娯楽とは逆に、組織の事業運営の文脈内で使用される確率（「非常に低い」から「非常に高い」まで）。

[タイプ（Types）]：アプリケーションのタイプ。

- [アプリケーションプロトコル（Application Protocol）]：HTTP や SSH などのホスト間の通信を表すアプリケーションプロトコル。
- [クライアントプロトコル（Client Protocol）]：Web ブラウザや電子メールクライアントなどのホスト上で動作しているソフトウェアを表すクライアント。
- [Webアプリケーション（Web Application）]：HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの Web アプリケーション。

[カテゴリ（Categories）]：アプリケーションの最も重要な機能を説明する一般分類。

[タグ（Tags）]：カテゴリに似た、アプリケーションに関する追加情報。

暗号化されたトラフィックの場合、システムは[SSL Protocol]とタグ付けされたアプリケーションだけを使用して、トラフィックを識別およびフィルタリングできます。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。また、システムは、復号されたトラフィック（暗号化された、または暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションに[復号されたトラフィック（decrypted traffic）]タグを割り当てます。

[アプリケーションリスト（Applications List）]（画面下部）：上記のリストのオプションからフィルタを選択するとこのリストが更新されるため、現在のフィルタに一致するアプリケーションを確認できます。ルールにフィルタ条件を追加するときに、フィルタが目的のアプリケーションを対象としていることを確認するためにこのリストを使用します。特定のアプリケーションまたは複数のアプリケーションをオブジェクトに追加するには、フィルタ処理されたリストからそれらを選択します。アプリケーションを選択すると、フィルタは適用されなくなります。フィルタ自体をオブジェクトにする場合は、リストからアプリケーションを選択しないでください。その後、そのオブジェクトは、常に、フィルタによって識別されたアプリケーションを表します。

ステップ 5 [OK] をクリックして変更を保存します。

Firepower アプリケーション フィルタ オブジェクトの編集

手順

ステップ 1 [オブジェクト（Objects）] タブをクリックして、[オブジェクト（Objects）] ページを開きます。

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 詳細パネルの [アクション（Actions）] ペインにある編集アイコン 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。

関連情報：

- オブジェクト
- オブジェクトフィルタ
- オブジェクトの削除

地理位置情報オブジェクト

地理位置情報オブジェクトは、トラフィックの送信元または接続先であるデバイスをホストする国と大陸を定義します。IPアドレスを使用する代わりに、これらのオブジェクトをポリシーで使用してトラフィックを制御できます。たとえば、地理的な場所を使用して、使用されている可能性のある IP アドレスすべてを把握する必要なしに、特定の国へのアクセスを簡単に制限できます。

通常は、地理位置情報オブジェクトを使用せずに、地理的な場所をポリシーで直接選択できます。とはいえ、同じ国や大陸のグループのために複数のポリシーを作成する場合、オブジェクトが便利です。

地理位置情報データベースの更新

常に最新の地理位置情報データを使用してトラフィックをフィルタ処理できるように、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。現時点で、これは Cisco Defense Orchestrator を使用して実行できるタスクではありません。GeoDB とその更新方法の詳細については、デバイスが実行しているバージョンの『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の次のセクションを参照してください。

- システム データベースとフィードの更新
- システム データベースの更新

Firepower 地理位置情報フィルタオブジェクトの作成と編集

地理位置情報オブジェクトは、オブジェクトページで単独で作成するか、セキュリティポリシーの作成時に作成することができます。この手順では、オブジェクトページから地理位置情報オブジェクトを作成します。

地理位置情報オブジェクトを作成するには、次の手順を実行します。

手順

ステップ 1 [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

ステップ 2 **[オブジェクトの作成（Create Object）]** > **[FTD]** > **[地理位置情報（Geolocation）]** をクリックします。

ステップ 3 そのオブジェクトの**オブジェクト名**を入力し、任意で**説明**を入力します。

ステップ 4 フィルタバーで、国または地域の名前の入力を開始すると、一致する可能性のあるもののリストが表示されます。

ステップ 5 オブジェクトに追加する 1 つまたは複数の国や地域のチェックボックスをオンにします。

ステップ 6 [追加（Add）] をクリックします。

オブジェクトを追加する方法：地理位置情報

手順

ステップ 1 [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。
ステップ 2 フィルタパネルと検索フィールドを使用して、オブジェクトを見つけます。
ステップ 3 [アクション（Actions）] ペインで、[編集（Edit）] をクリックします。
ステップ 4 オブジェクト名を変更したり、オブジェクトに国や地域を追加または削除したりできます。
ステップ 5 [保存（Save）] をクリックします。
ステップ 6 影響を受けるデバイスがある場合は通知されます。[確認（Confirm）] をクリックします。
ステップ 7 デバイスまたはポリシーが影響を受けた場合は、[デバイスとサービス（Devices & Services）] ページを開き、変更をプレビューしてデバイスに展開します。

DNS グループオブジェクト

ドメインネームシステム（DNS）グループは、DNS サーバーおよび関連付けられているいくつかの属性のリストを定義します。www.example.com などの完全修飾ドメイン名（FQDN）を IP アドレスに解決するのには、DNS サーバーが必要です。管理インターフェイスとデータインターフェイスに異なる DNS グループオブジェクトを構成できます。

新しい DNS グループオブジェクトを作成する前に、FTD デバイスに DNS サーバーが構成されている必要があります。CDO の Firepower Threat Defense デバイス設定に DNS サーバーを追加するか、FDM で DNS サーバーを作成してから、FDM 構成を CDO に同期することができます。FDM で DNS サーバー設定を作成または変更するには、『Cisco Firepower Device Manager 構成ガイド』バージョン 6.4 以降の「**データおよび管理インターフェイスの DNS の構成**」を参照してください。またはそれ以降。

DNS グループオブジェクトの作成

CDO で新しい DNS グループオブジェクトを作成するには、次の手順を使用します。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。
ステップ 2 青色のプラスボタン  をクリックして、オブジェクトを作成します。
ステップ 3 C**[FTD] > [DNS グループ（DNS Group）]**をクリックします。
ステップ 4 [オブジェクト名（Object Name）] を入力します。
ステップ 5 （任意）説明を追加します。

ステップ 6 [DNSサーバー（DNS server）] の IPアドレスを入力します最大 6 台の DNS サーバーを追加できます。[DNS サーバーの追加（Add DNS Server）] をクリックします。サーバーアドレスを削除する場合は、削除アイコンをクリックします。

（注） リストは優先順です。リストの最初のサーバが常に使用されます。後続のサーバは、上位のサーバから応答が受信されない場合にのみ使用されます。最大 6 台のサーバーを追加できますが、リストされている最初の 3 台のサーバーのみが管理インターフェイスに使用されます。

ステップ 7 [ドメイン検索名（Domain Search Name）] を入力します。このドメインは、完全修飾されていないホスト名（たとえば、serverA.example.com ではなく serverA）に追加されます。

ステップ 8 [再試行（Retries）] の回数を入力します。システムが応答を受信しない場合に DNS サーバーのリストを再試行する回数です（0 ～ 10）。デフォルトは 2 です。この設定は、データインターフェイスのみで使用される DNS グループに適用されます。

ステップ 9 [タイムアウト（Timeout）] の値を入力します。次の DNS サーバーを試行する前に待機する秒数です（1 ～ 30）。デフォルト値は 2 秒です。システムがサーバーのリストを再試行するたびに、このタイムアウトは 2 倍になります。この設定は、データインターフェイスのみで使用される DNS グループに適用されます。

ステップ 10 [追加（Add）] をクリックします。

DNS グループオブジェクトの編集

CDO または FDM で作成された DNS グループオブジェクトを編集できます。次の手順を使用して、既存の DNS グループオブジェクトを編集します。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（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（search）] フィールドを使用して、編集する **DNS グループオブジェクト**を見つけます。

ステップ 3 オブジェクトを選択し、[アクション（Actions）] ペインで編集アイコン をクリックします。

ステップ 4 次のエントリのいずれかを編集します。

- オブジェクト名。
- [説明（Description）]
- DNS サーバー。このリストから DNS サーバーを編集、追加、または削除できます。
- ドメイン検索名。
- リトライ。

- タイムアウト。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 すべてのデバイスの設定変更をプレビューして展開します。

DNS グループオブジェクトの削除

CDO から DNS グループオブジェクトを削除するには、次の手順を使用します。

手順

ステップ 1 ナビゲーションバーで、[オブジェクト（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（search）] フィールドを使用して、編集する **DNS グループオブジェクト**を見つけます。

ステップ 3 オブジェクトを選択し、[削除（remove）] アイコン をクリックします。

ステップ 4 DNS グループオブジェクトを削除することを確認し、[Ok] をクリックします。

ステップ 5 すべてのデバイスの設定変更をプレビューして展開します。

DNS サーバー グループ オブジェクトを FTD DNS サーバーとして追加

DNS グループオブジェクトは、[データインターフェイス（Data Interface）] または [管理インターフェイス（Management Interface）] の優先 DNS グループとして追加できます。詳細については、「FTD の設定」を参照してください。

証明書オブジェクト

デジタル証明書は、認証に使用されるデジタル ID を提供します。証明書は、SSL（セキュアソケット レイヤ）、TLS（Transport Layer Security）、および DTLS（データグラム TLS）接続（HTTPS や LDAPS など）に使用されます。

デバイスが実行しているバージョンについては、『Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用』の「再利用可能なオブジェクト」の章にある「**証明書について**」および「**証明書の設定**」以降のセクションを参照してください。

証明書について

デジタル証明書は、認証に使用されるデジタルIDを提供します。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザーまたはデバイスを識別する情報が含まれます。デジタル証明書には、ユーザまたはデバイスの公開キーのコピーも含まれて

います。証明書は、SSL（セキュア ソケット レイヤ）、TLS（Transport Layer Security）、および DTLS（データグラム TLS）接続（HTTPS や LDAPS など）に使用されます。

次のタイプの証明書を作成できます。

- **内部証明書**：内部 ID 証明書は、特定のシステムまたはホストの証明書です。これらは OpenSSL ツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名証明書を生成することもできます。

  システムには、そのまま、または置き換えて使用できる事前定義された内部証明書（**DefaultInternalCertificate** および **DefaultWebServerCertificate**）が付属します。

- **内部認証局（CA）証明書**：内部 CA 証明書は、他の証明書の署名にシステムが使用できる証明書です。これらの証明書は、基本制約拡張と CA フラグに関して内部アイデンティティ証明書と異なります。これらは CA 証明書では有効ですが、アイデンティティ証明書では無効です。これらは OpenSSL ツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名内部 CA 証明書を生成することもできます。自己署名内部 CA 証明書を設定する場合は、CA はデバイス自体で稼働します。

  システムには、そのまま、または置き換えて使用できる事前定義された内部 CA 証明書（**NGFW-Default-InternalCA**）が付属します。

- **信頼できる認証局（CA）証明書**：信頼できる CA 証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。別の CA 証明書により発行される証明書は、下位証明書と呼ばれます。

  認証局（CA）は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザーのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。CA は、信頼できるサード パーティ（VeriSign など）の場合もあれば、組織内に設置したプライベート CA（インハウス CA）の場合もあります。CA は、証明書要求の管理とデジタル証明書の発行を行います。

  システムには、第三者証明機関からの多数の信頼できる CA の証明書も含まれています。これらは再署名の復号アクションのために SSL 復号化ポリシーが使用します。

詳細については、デバイスが実行しているバージョンの Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）[英語] の「Reusable Objects」の章にある「Certificate Types Used by Feature」を参照してください。https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html

各機能で使用される証明書タイプ

各機能に適したタイプの証明書を作成する必要があります。次の機能は、証明書が必要です。

アイデンティティ ポリシー（キャプティブ ポータル）：内部証明書

（オプション）キャプティブ ポータルはアイデンティティ ポリシーで使用されます。この証明書は、ユーザーが自身を証明し、自分のユーザー名に関連付けられた IP アドレスを取得す

ることを目的として、デバイスへの認証の際に承認する必要があります。証明書を提示しないと、デバイスは自動生成された証明書を使用します。

SSL 復号ポリシー：内部、内部 CA、および信頼できる CA 証明書。

（必須）SSL 復号ポリシーは、以下の目的のため証明書を使用します。

- 内部証明書は既知のキー復号ルールに使用されます。
- 内部 CA 証明書は、クライアントと FTD デバイス間のセッションを作成するときに、再署名の復号ルールに使用されます。
- 信頼できる CA 証明書
  - この証明書は、FTDデバイスとサーバー間のセッションを作成するときに、再署名の復号ルールに間接的に使用されます。その他の証明書とは異なり、これらの証明書はSSL復号ポリシーで直接設定しません。これらは単にシステムにアップロードする必要があります。システムには多数の信用できる CA 証明書が含まれるため、追加の証明書をアップロードする必要はないことがあります。
  - Active Directory レルムオブジェクトを作成し、暗号化を使用するようにディレクトリサーバーを設定する場合。

証明書の設定

アイデンティティポリシーまたは SSL 復号化ポリシーで使用される証明書は、PEM または DER 形式の X509 証明書である必要があります。OpenSSL を使用して必要に応じて証明書を生成したり、信頼できる認証局から取得したり、または自己署名証明書を作成したりできます。

以下の手順を使用して、証明書オブジェクトを構成します。

- 内部および内部 CA 証明書のアップロード
- 信頼できる CA 証明書のアップロード
- 自己署名内部および内部 CA 証明書の生成
- 証明書を表示または編集するには、証明書の編集アイコンまたは表示アイコンをクリックします。
- 証明書を削除するには、その証明書のごみ箱アイコン（削除アイコン）をクリックします。「オブジェクトの削除」を参照してください。

内部および内部 CA 証明書のアップロード

内部 ID 証明書は、特定のシステムまたはホストの証明書です。これらは OpenSSL ツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名証明書を生成することもできます。

内部認証局（CA）証明書（内部 CA 証明書）は、他の証明書の署名にシステムが使用できる証明書です。これらの証明書は、基本制約拡張と CA フラグに関して内部アイデンティティ証明書と異なります。これらは CA 証明書では有効ですが、アイデンティティ証明書では無効です。これらは OpenSSL ツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名内部 CA 証明書を生成することもできます。自己署名内部 CA 証明書を設定する場合は、CA はデバイス自体で稼働します。

これらの証明書を使用する機能の詳細については、「各機能で使用される証明書タイプ」を参照してください。

手順

この手順では、証明書ファイルをアップロードするか、既存の証明書のテキストをテキストボックスに貼り付けて、内部証明書または内部 CA 証明書を作成します。自己署名証明書を生成する場合は、「自己署名内部および内部 CA 証明書の生成」を参照してください。

内部証明書または内部 CA 証明書オブジェクトを作成する場合、または新しい証明書オブジェクトをポリシーに追加する場合は、次の手順に従います。

手順

ステップ 1 次のいずれかを実行します。

- [オブジェクト（Objects）] ページで証明書オブジェクトを作成します。
  1. ナビゲーションバーで、[オブジェクト（Objects）] を選択します。
  2. プラスボタン  をクリックして、**[FTD]** > **[証明書（Certificate）]** を選択します。
- ポリシーに新しい証明書オブジェクトを追加するときに、[新しいオブジェクトの作成（Create New Object）] をクリックします。

ステップ 2 [Name] に証明書の名前を入力します。名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 3 ステップ 1 で、[内部証明書（Internal Certificate）] または [内部CA（Internal CA）] を選択します。

ステップ 4 ステップ 2 で、[アップロード（Upload）] を選択して証明書ファイルをアップロードします。

ステップ 5 ステップ 3 で、[サーバー証明書（Server Certificate）] 領域で、証明書の内容をテキストボックスに貼り付けるか、ウィザードの説明に従って証明書ファイルをアップロードします。証明書をテキストボックスに貼り付ける場合、証明書に BEGIN CERTIFICATE と END CERTIFICATE の行を含める必要があります。次に例を示します。

```
-----BEGIN CERTIFICATE-----
 MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0
(...5 lines removed...)
shGJDReRYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxwCUn
```

```
RV7LRfQGFYd76V/5uor4Wx2ZCjqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
vlk3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

ステップ 6 ステップ 3 で、[証明書キー（Certificate Key）] 領域で、キーの内容を [証明書キー（Certificate Key）] テキストボックスに貼り付けるか、ウィザードの説明に従ってキーファイルをアップロードします。キーをテキストボックスに貼り付ける場合、キーには BEGIN PRIVATE KEY または BEGIN RSA PRIVATE KEY、および END PRIVATE KEY または END PRIVATE KEY 行が含まれている必要があります。

（注） キーは暗号化できません。

ステップ 7 [追加（Add）] をクリックします。

信頼できる CA 証明書のアップロード

信頼できる認証局（CA）の証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。別の CA 証明書により発行される証明書は、下位証明書と呼ばれます。

これらの証明書を使用する機能の詳細については、「各機能で使用される証明書タイプ」を参照してください。

外部の認証局から信頼できる CA 証明書を取得するか、自身の内部 CA を使用して（OpenSSL ツールを使用するなど）CA 証明書を作成します。その後、次の手順を使用して証明書をアップロードします。

手順

手順

ステップ 1 次のどちらかを実行します。

- [オブジェクト（Objects）] ページで証明書オブジェクトを作成します。
  1. ナビゲーションバーで、[オブジェクト（Objects）] を選択します。
  2. プラスボタン  をクリックして、**[FTD]** > **[証明書（Certificate）]** を選択します。
- ポリシーに新しい証明書オブジェクトを追加するときに、[新しいオブジェクトの作成（Create New Object）] をクリックします。

ステップ 2 [Name] に証明書の名前を入力します。名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 3 手順 1 では、[外部CA証明書（External CA Certificate）] を選択し、[続行（Continue）] をクリックします。ウィザードの手順が 3 に進みます。

ステップ 4 手順 3 では、[証明書の内容（Certificate Contents）] 領域にあるテキストボックスに証明書の内容を貼り付けるか、ウィザードの説明に従って証明書ファイルをアップロードします。

証明書は、次のガイドラインに合致している必要があります。

- 証明書内のサーバ名は、サーバのホスト名または IP アドレスと一致している必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で ad.example.com を使用すると接続が失敗します。
- 証明書は PEM または DER 形式の X509 証明書である必要があります。
- 貼り付ける証明書は、BEGIN CERTIFICATE と END CERTIFICATE の行を含める必要があります。次に例を示します。

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

ステップ 5 [追加（Add）] をクリックします。

自己署名内部および内部 CA 証明書の生成

内部 ID 証明書は、特定のシステムまたはホストの証明書です。これらは OpenSSL ツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名証明書を生成することもできます。

内部認証局（CA）証明書（内部 CA 証明書）は、他の証明書の署名にシステムが使用できる証明書です。これらの証明書は、基本制約拡張と CA フラグに関して内部アイデンティティ証明書と異なります。これらは CA 証明書では有効ですが、アイデンティティ証明書では無効です。これらは OpenSSL ツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名内部 CA 証明書を生成することもできます。自己署名内部 CA 証明書を設定する場合は、CA はデバイス自体で稼働します。

また、これらの証明書は、OpenSSL を使用して作成することも、信頼できる CA から取得してアップロードすることもできます。詳細は「内部および内部 CA 証明書のアップロード」を参照してください。

これらの証明書を使用する機能の詳細については、各機能で使用される証明書タイプを参照してください。

（注） 新しい自己署名証明書は5年の有効期間で生成されます。期限が切れる前に必ず証明書を交換してください。

警告 自己署名証明書を持つデバイスをアップグレードすると、問題が発生する可能性があります。詳細については、「新しい証明書の検出」を参照してください。

手順

この手順では、ウィザードに適切な証明書フィールド値を入力することにより、自己署名証明書を生成します。証明書ファイルをアップロードして内部または内部CA証明書を作成する場合は、「内部および内部 CA 証明書のアップロード」を参照してください。

自己署名証明書を生成するには、次の手順を実行します。

手順

ステップ 1 次のいずれかを実行します。

- [オブジェクト（Objects）] ページで証明書オブジェクトを作成します。
  1. ナビゲーションバーで、[オブジェクト（Objects）] を選択します。
  2. プラスボタン をクリックして、**[FTD]** > **[証明書（Certificate）]** を選択します。
- ポリシーに新しい証明書オブジェクトを追加するときに、[新しいオブジェクトの作成（Create New Object）] をクリックします。

ステップ 2 [Name] に証明書の名前を入力します。名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 3 ステップ 1 で、[内部証明書（Internal Certificate）] または [内部CA（Internal CA）] を選択します。

ステップ 4 ステップ 2 で、[自己署名（Self-Signed）] を選択して、この手順で自己署名証明書を作成します。

ステップ 5 証明書の件名および発行者の情報については、次の少なくとも 1 つを設定します。

- [国（C）（Country (C)）]：ドロップダウトリストから国コードを選択します。
- [都道府県（ST）（State or Province (ST)）]：証明書に含める都道府県。
- [地域または都市（L）（Locality or City (L)）]：都市の名前など、証明書に含める地域。
- [組織（O）（Organization (O)）]：証明書に含める組織または会社の名前。

- [組織単位（部門）（OU）（Organizational Unit (Department)）]：証明書に含める組織単位の名前（部門名など）。
- [共通名（CN）（Common Name (CN)）]：証明書に含める X.500 共通名。これは、デバイスの名前、Webサイト、または他の文字列にできます。この要素は、通常は正常な接続のために必要です。たとえば、リモート アクセス VPN で使用する内部証明書に CN を含める必要があります。

ステップ 6 [追加（Add）] をクリックします。

IPsec プロポーザルの設定

IPsec は、VPN を設定する場合の最も安全な方法の 1 つです。IPsec では、IP パケット レベルでのデータ暗号化が提供され、標準規格に準拠した堅牢なセキュリティ ソリューションが提供されます。IPsec では、データはトンネルを介してパブリック ネットワーク経由で送信されます。トンネルとは、2つのピア間のセキュアで論理的な通信パスです。IPsecトンネルを通過するトラフィックは、トランスフォーム セットと呼ばれるセキュリティ プロトコルとアルゴリズムの組み合わせによって保護されます。IPsec Security Association（SA：セキュリティ アソシエーション）のネゴシエーション中に、ピアでは、両方のピアに共通するトランスフォーム セットが検索されます。

IKE バージョン（IKEv1 または IKEv2）に基づいて、別個の IPsec プロポーザル オブジェクトがあります。

- IKEv1 IPsec プロポーザルを作成する場合、IPSec が動作するモードを選択し、必要な暗号化タイプおよび認証タイプを定義します。アルゴリズムには単一のオプションを選択できます。VPN で複数の組み合わせをサポートするには、複数の IKEv1 IPsec プロポーザル オブジェクトを作成して選択します。
- IKEv2 IPsec プロポーザルを作成する際に、VPN で許可するすべての暗号化アルゴリズムとハッシュ アルゴリズムを選択できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、マッチが見つかるまでピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを個別に送信することなく、許可されるすべての組み合わせを伝送するために単一のプロポーザルを送信できます。

カプセル化セキュリティ プロトコル（ESP）は、IKEv1 と IKEv2 IPsec プロポーザルの両方に使用されます。これは認証、暗号化、およびアンチリプレイ サービスを提供します。ESP は、IP プロトコル タイプ 50 です。

（注） IPsec トンネルで暗号化と認証の両方を使用することを推奨します。

次に、各 IKE バージョンの IPsec プロポーザルの設定方法を説明します。

• IPsec プロポーザルオブジェクトの管理
• IKEv2 IPsec プロポーザルオブジェクトの管理

IPsec プロポーザルオブジェクトの管理

IPsec プロポーザル オブジェクトは、IKE フェーズ 2 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。IKEv1 と IKEv2 に対して、異なるオブジェクトがあります。現在、Cisco Defense Orchestrator（CDO）は IKEv1 IPsec プロポーザルオブジェクトをサポートしています。

カプセル化セキュリティ プロトコル（ESP）は、IKEv1 と IKEv2 IPsec プロポーザルの両方に使用されます。このプロトコルにより、認証、暗号化、およびアンチリプレイサービスが実現します。ESP は、IP プロトコル タイプ 50 です。

（注） IPsec トンネルで暗号化と認証の両方を使用することを推奨します。

関連トピック

IKEv1 IPSec プロポーザルオブジェクトの作成または編集

FTD IKEv1 IPSec プロポーザルオブジェクトの作成または編集

定義済みの複数の IKEv1 IPsec プロポーザルがあります。その他のセキュリティ設定の組み合わせを実装する新しいプロポーザルを作成することもできます。システム定義オブジェクトの編集や削除はできません。

次の手順では、[オブジェクト（Objects）]ページから直接オブジェクトを作成および編集する方法について説明します。サイト間 VPN 接続の IKEv1 IPSec 設定を編集している間に、オブジェクトリストに表示される [新規IKEv1プロポーザルの作成（Create New IKEv1 Proposal）] リンクをクリックして、IKEv1 IPSec プロポーザルオブジェクトを作成することもできます。

手順

ステップ 1 ナビゲーションバーで [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

ステップ 2 次のいずれかの操作を実行します。

- 青色のプラスボタン  をクリックし、[FTD] > [IKEv1 IPSecプロポーザル（IKEv1 IPsec Proposal）] を選択して新しいオブジェクトを作成します。
- オブジェクトページで、編集する IPSec プロポーザルを選択し、右側の [アクション（Actions）] ペインで [編集（Edit）] をクリックします。

ステップ 3 新しいオブジェクトのオブジェクト名を入力します。

ステップ 4 IKEv1 IPSec プロポーザルオブジェクトが動作するモードを選択します。

- トンネルモードでは IP パケット全体がカプセル化されます。IPSec ヘッダーが、元の IP ヘッダーと新しい IP ヘッダーとの間に追加されます。これがデフォルトです。トンネルモードは、ファイアウォールの背後にあるホストとの間で送受信されるトラフィックをファイアウォールが保護する場合に使用します。トンネルモードは、インターネットなどの非信頼ネットワークを介して接続されている 2 つのファイアウォール（またはその他のセキュリティ ゲートウェイ）間で通常の IPSec が実装される標準の方法です。
- トランスポートモードでは IP パケットの上位層プロトコルだけがカプセル化されます。IPSec ヘッダーは、IP ヘッダーと上位層プロトコル ヘッダー（TCP など）との間に挿入されます。トランスポート モードでは、送信元ホストと宛先ホストの両方が IPSec をサポートしている必要があります。また、トランスポート モードは、トンネルの宛先ピアが IP パケットの最終宛先である場合にだけ使用されます。一般的に、トランスポート モードは、レイヤ 2 またはレイヤ 3 のトンネリング プロトコル（GRE、L2TP、DLSW など）を保護する場合にだけ使用されます。

ステップ 5 このプロポーザルの [ESP暗号化（ESP Encryption）]（カプセル化セキュリティプロトコル暗号化）アルゴリズムを選択します。オプションの説明については、使用する暗号化アルゴリズムの決定を参照してください。

ステップ 6 認証に使用する [ESPハッシュ（ESP Hash）] または整合性アルゴリズムを選択します。オプションの説明については、使用するハッシュ アルゴリズムの決定を参照してください。

ステップ 7 [追加（Add）] をクリックします。

IKEv2 IPsec プロポーザルオブジェクトの管理

IPsec プロポーザル オブジェクトは、IKE フェーズ 2 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルでは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。

IKEv2 IPsec プロポーザルを作成する際に、VPN で許可するすべての暗号化アルゴリズムとハッシュ アルゴリズムを選択できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、マッチが見つかるまでピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを個別に送信することなく、許可されるすべての組み合わせを伝送するために単一のプロポーザルを送信できます。

関連トピック

IKEv2 IPSec プロポーザルオブジェクトの作成または編集

FTD IKEv2 IPSec プロポーザルオブジェクトの作成または編集

定義済みの複数の IKEv2 IPsec プロポーザルがあります。その他のセキュリティ設定の組み合わせを実装する新しいプロポーザルを作成することもできます。システム定義オブジェクトの編集や削除はできません。

次の手順では、[オブジェクト（Objects）]ページから直接オブジェクトを作成および編集する方法について説明します。VPN 接続の IKEv2 IPsec 設定を編集している間に、オブジェクトリストに表示される [新規IPsecプロポーザルの作成（Create New IPsec Proposal）] リンクをクリックして、IKEv2 IPsec プロポーザル オブジェクトを作成することもできます。

手順

ステップ 1 ナビゲーションバーで [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

ステップ 2 次のいずれかの操作を実行します。

- 青色のプラスボタン  をクリックし、[FTD] > [IKEv2 IPSecプロポーザル（IKEv2 IPsec Proposal）] を選択して新しいオブジェクトを作成します。
- オブジェクトページで、編集する IPSec プロポーザルを選択し、右側の [アクション（Actions）] ペインで [編集（Edit）] をクリックします。

ステップ 3 新しいオブジェクトのオブジェクト名を入力します。

ステップ 4 IKEv2 IPsec プロポーザルオブジェクトの設定：

- [暗号化（Encryption）]：このプロポーザルのカプセル化セキュリティプロトコル（ESP）暗号化アルゴリズム。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、使用する暗号化アルゴリズムの決定を参照してください。
- [整合性ハッシュ（Integrity Hash）]：認証に使用するハッシュまたは整合性アルゴリズム。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、使用するハッシュアルゴリズムの決定を参照してください。

ステップ 5 [追加（Add）] をクリックします。

グローバル IKE ポリシーの設定

Internet Key Exchange（IKE、インターネット キー エクスチェンジ）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA、セキュリティアソシエーション）の自動的な確立に使用されるキー管理プロトコルです。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティアソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec

などの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKEプロポーザルは、2つのピア間のネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKEポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。

IKE ポリシー オブジェクトはこれらのネゴシエーションに対して IKE プロポーザルを定義します。有効にするオブジェクトは、ピアが VPN 接続をネゴシエートするときに使用するものであり、接続ごとに異なるIKEポリシーを指定することはできません。各オブジェクトの相対的な優先順位は、これらの中でどのポリシーを最初に試行するかを決定します。数が小さいほど、優先順位が高くなります。ネゴシエーションで両方のピアがサポートできるポリシーを見つけられなければ、接続は確立されません。

IKE グローバル ポリシーを定義するには、各 IKE バージョンを有効にするオブジェクトを選択します。事前定義されたオブジェクトが要件を満たさない場合、セキュリティ ポリシーを適用する新しいポリシーを作成します。

次に、オブジェクト ページでグローバル ポリシーを設定する方法について説明します。VPN 接続を編集しているときに IKE ポリシー設定の [編集（Edit）] をクリックすることで、ポリシーの有効化、無効化および作成が行えます。

次に、各バージョンの IKE ポリシーの設定方法を説明します。

- IKEv1 ポリシーの管理
- IKEv2 ポリシーの管理

IKEv1 ポリシーの管理

IKEv1 ポリシーを作成および編集する方法について説明します。

IKEv1 ポリシーについて

インターネット キー エクスチェンジ（IKE）バージョン 1 ポリシー オブジェクトには、VPN 接続を定義する際に必要な IKEv1 ポリシーが含まれています。IKE は、IPsec ベースの通信の管理を簡易化するキー管理プロトコルです。IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec セキュリティ アソシエーション（SA）の自動確立に使用されます。

複数の事前定義された IKEv1 ポリシーが存在します。必要に適したポリシーがあれば、[状態（State）] トグルをクリックして有効にします。セキュリティ設定の他の組み合わせを実装する新しいポリシーも作成できます。システム定義オブジェクトは、編集または削除できません。

関連トピック

IKEv1 ポリシーの作成または編集

FTD IKEv1 ポリシーの作成または編集

次に、オブジェクトページからオブジェクトを直接作成および編集する方法について説明します。サイト間 VPN 接続での IKE 設定の編集時に、オブジェクトリストに表示される [新しいIKEv1 ポリシーの作成（Create New IKEv1 Policy）] リンクをクリックして、IKEv1 ポリシーを作成することもできます。

手順

ステップ 1 ナビゲーションバーで [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

ステップ 2 次のいずれかの操作を実行します。

- 青いプラスボタン  をクリックし、[FTD] > [IKEv1ポリシー（IKEv1 Policy）] を選択して、新しい IKEv1 ポリシーを作成します。
- オブジェクトのページで、編集する IKEv1 ポリシーを選択し、右側の [操作（Actions）] ウィンドウで [編集（Edit）] をクリックします。

ステップ 3 [オブジェクト名（Object Name）] を 128 文字以内で入力します。

ステップ 4 IKEv1 プロパティを設定します。

- [優先順位（Priority）]：IKE ポリシーの相対的優先順位（1 ～ 65,535）。このプライオリティによって、共通のセキュリティアソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。リモート IPsec ピアが、最も高いプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティで定義されているパラメータの使用を試行します。値が小さいほど、プライオリティが高くなります。
- [暗号化（Encryption）]：フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 セキュリティ アソシエーション（SA）の確立に使用される暗号化アルゴリズム。オプションの説明については、「使用する暗号化アルゴリズムの決定」を参照してください。
- [Diffie-Hellmanグループ（Diffie-Hellman Group）]：2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。オプションの説明については、「使用する Diffie-Hellman 係数グループの決定」を参照してください。
- [ライフタイム（Lifetime）]：セキュリティアソシエーション（SA）のライフタイム（120 ～ 2147483647 までの秒数、または空白）。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。デフォルトは 86400 です。無期

限のライフタイムを指定するには、値を入力しません（フィールドを空白のままにします）。

- [認証（Authentication）]：2 つのピア間で使用される認証方式。詳細については、使用する認証方式の決定を参照してください。
  - [事前共有キー（Preshared Key）]：各デバイスで定義されている事前共有キーを使用します。事前共有キーを使用すると、秘密鍵を 2 つのピア間で共有し、認証フェーズ中に IKE で使用できます。ピアに同じ事前共有キーが設定されていない場合は、IKE SA を確立できません。
  - [証明書（Certificate）]：ピアのデバイス ID 証明書を使用して相互に識別します。認証局に各ピアを登録することによって、これらの証明書を取得する必要があります。また、各ピアでアイデンティティ証明書の署名に使用された、信頼できる CA ルート証明書および中間 CA 証明書もアップロードする必要があります。ピアは、同じ CA または別の CA に登録できます。どちらのピアにも自己署名証明書を使用することはできません。
- [ハッシュ（Hash）]：メッセージの整合性の確保に使用されるメッセージダイジェストを作成するためのハッシュ アルゴリズム。オプションの説明については、VPN で使用される暗号化アルゴリズムとハッシュアルゴリズムを参照してください。

ステップ 5 [追加（Add）] をクリックします。

IKEv2 ポリシーの管理

IKEv2 ポリシーを作成および編集する方法について説明します。

IKEv2 ポリシーについて

インターネット キー エクスチェンジ（IKE）バージョン 2 ポリシー オブジェクトには、VPN 接続を定義する際に必要な IKEv2 ポリシーが含まれています。IKE は、IPsec ベースの通信の管理を簡易化するキー管理プロトコルです。IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec セキュリティ アソシエーション（SA）の自動確立に使用されます。

複数の事前定義された IKEv2 ポリシーがあります。必要に適したポリシーがあれば、[状態（State）] トグルをクリックして有効にします。セキュリティ設定の他の組み合わせを実装する新しいポリシーも作成できます。システム定義オブジェクトは、編集または削除できません。

関連トピック

IKEv2 ポリシーの作成または編集

FTD IKEv2 ポリシーの作成または編集

次に、オブジェクトページからオブジェクトを直接作成および編集する方法について説明します。サイト間 VPN 接続での IKE 設定の編集時に、オブジェクトリストに表示される [新しいIKEv2ポリシーの作成（Create New IKEv2 Policy）] リンクをクリックして、IKEv2 ポリシーを作成することもできます。

手順

ステップ 1 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、[オブジェクト（Objects）] ページを表示します。

ステップ 2 次のいずれかの操作を実行します。

- 青いプラスボタン  をクリックし、[FTD]>[IKEv2 ポリシー] を選択して、新しい IKEv2 ポリシーを作成します。
- オブジェクトページで、編集する IKEv2 ポリシーを選択し、右側の [アクション（Actions）] ペインで [編集（Edit）] をクリックします。

ステップ 3 [オブジェクト名（Object Name）] を 128 文字以内で入力します。

ステップ 4 IKEv2 プロパティを設定します。

- [優先順位（Priority）]：IKE ポリシーの相対的優先順位（1 ～ 65,535）。このプライオリティによって、共通のセキュリティアソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。リモート IPsec ピアが、最も高いプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティで定義されているパラメータの使用を試行します。値が小さいほど、プライオリティが高くなります。
- [状態（State）]：IKE ポリシーが有効か無効かを示します。トグルをクリックして状態を変更します。IKE ネゴシエーション中には、有効なポリシーのみが使用されます。
- [暗号化（Encryption）]：フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 セキュリティ アソシエーション（SA）の確立に使用される暗号化アルゴリズム。有効にするすべてのアルゴリズムを選択します。ただし、同じポリシーに混合モード（AES-GCM）と通常モードのオプションを含めることはできません（通常モードでは整合性ハッシュを選択する必要がありますが、混合モードでは個別の整合性ハッシュの選択は禁止されています）。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、使用する暗号化アルゴリズムの決定を参照してください。
- [Diffie-Hellmanグループ（Diffie-Hellman Group）]：2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。許可するすべてのアルゴリズムを選択します。システムは、最も強いグループから始めて最も弱いグループに至るまで、適合する

ものが確認できるまでピアとネゴシエートします。オプションの説明については、使用する Diffie-Hellman 係数グループの決定を参照してください。

- [整合性ハッシュ（Integrity Hash）]：メッセージの整合性の確保に使用されるメッセージダイジェストを作成するためのハッシュアルゴリズムの整合性部分。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。整合性ハッシュは、AES-GCM 暗号化オプションでは使用されません。オプションの説明については、VPN で使用される暗号化アルゴリズムとハッシュアルゴリズムを参照してください。
- [擬似ランダム関数（PRF）ハッシュ（Pseudo-Random Function（PRF）Hash）]：ハッシュアルゴリズムの疑似ランダム関数（PRF）部分。このアルゴリズムは IKEv2 トンネル暗号化に必要なキー関連情報とハッシュ操作を取得するために使用されます。IKEv1 では、整合性と PRF アルゴリズムは別ですが、IKEv2 では、これらの要素に異なるアルゴリズムを指定できます。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、VPN で使用される暗号化アルゴリズムとハッシュアルゴリズムを参照してください。
- [ライフタイム（Lifetime）]：セキュリティアソシエーション（SA）のライフタイム（120 ～ 2147483647 までの秒数、または空白）。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティアソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。デフォルトは 86400 です。無期限のライフタイムを指定するには、値を入力しません（フィールドを空白のままにします）。

ステップ 5 [追加（Add）] をクリックします。

RA VPN オブジェクト

AnyConnectクライアント プロファイル オブジェクト

AnyConnect クライアント プロファイル オブジェクトの作成および編集

手順

テキスト作成中

セキュリティ ゾーン オブジェクト

セキュリティ ゾーンとはインターフェイスのグループ分けです。ゾーンは、トラフィックの管理と分類に役立つようにネットワークをセグメントに分割します。複数のゾーンを定義できますが、所与のインターフェイスは単一のゾーンの中にのみ存在できます。

Firepower システムでは、初期設定中に次のゾーンが作成され、Defense Orchestrator のオブジェクトページに表示されます。ゾーンを編集してインターフェイスを追加または削除したり、使用しなくなったゾーンを削除したりできます。

- **inside_zone**：内部インターフェイスが含まれます。このゾーンは、内部ネットワークを表します。
- **outside_zone**：外部インターフェイスが含まれます。このゾーンは、インターネットなどの制御不可能な外部ネットワークを表すことを目的としています。

通常、ネットワーク内で果たす役割によって、インターフェイスをグループ化します。たとえば、インターネットに接続するインターフェイスを **outside_zone** セキュリティゾーンに配置し、内部ネットワークに接続するすべてのインターフェイスを **inside_zone** セキュリティゾーンに配置できます。次に、外部ゾーンから来て内部ゾーンへ向かうトラフィックにアクセスコントロール ルールを適用できます。

ゾーンを作成する前に、ネットワークに適用するアクセス ルールや他のポリシーを検討してください。たとえば、すべての内部インターフェイスを同じゾーンに配置する必要はありません。4 つの内部ネットワークがあり、1 つだけ他の 3 つとは異なる処理をしたい場合、1 つではなく 2 つのゾーンを作成できます。パブリック Web サーバへの外部アクセスを許可するインターフェイスがある場合、そのインターフェイスに別のゾーンを使用できます。

関連情報：

- Firepower セキュリティ ゾーン オブジェクトの作成または編集
- Firepower インターフェイスをセキュリティゾーンに割り当てる
- オブジェクトの削除

Firepower セキュリティ ゾーン オブジェクトの作成または編集

セキュリティ ゾーンとはインターフェイスのグループ分けです。ゾーンは、トラフィックの管理と分類に役立つようにネットワークをセグメントに分割します。複数のゾーンを定義できますが、所与のインターフェイスは単一のゾーンの中にのみ存在できます。詳細については、「セキュリティ ゾーン オブジェクト」を参照してください。

セキュリティ ゾーン オブジェクトは、デバイスのルールで使用されない限り、そのデバイスに関連付けられません。

セキュリティ ゾーン オブジェクトの作成

セキュリティ ゾーン オブジェクトを作成するには、以下の手順に従ってください。

手順

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

ステップ 2 青いプラスボタン  をクリックし、FTD セキュリティゾーンを選択してオブジェクトを作成します。 >

ステップ 3 オブジェクトに名前を付け、任意で説明を入力します。

ステップ 4 セキュリティゾーンに含めるインターフェイスを選択します。

ステップ 5 [追加（Add）] をクリックします。

セキュリティ ゾーン オブジェクトの編集

FTD をオンボーディングすると、少なくとも 2 つのセキュリティゾーンがすでに存在することがわかります。1 つは inside_zone で、もう 1 つは outside_zone です。これらのゾーンは編集または削除できます。セキュリティゾーン オブジェクトを編集するには、次の手順に従います。

手順

ステップ 1 編集するオブジェクトを見つけます。

- オブジェクトの名前がわかっている場合は、[オブジェクト（Objects）] ページで検索できます。
  - リストをセキュリティゾーンでフィルタリングします。
  - オブジェクトの名前を検索フィールドに入力します。
  - オブジェクトを選択します。
- オブジェクトがデバイスに関連付けられていることがわかっている場合は、[デバイスとサービス（Devices & Services）] ページから検索を開始できます。
  - 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。
  - [デバイス] タブをクリックします。
  - 適切なタブをクリックします。
  - デバイスフィルタと検索バーを使用して、デバイスを見つけます。
  - デバイスを選択します。

- 右側の [管理（Management）] ペインで、  [オブジェクト（Objects）] をクリックします。
- オブジェクトフィルタ と検索バーを使用して、探しているオブジェクトを見つけます。

（注） 作成したセキュリティ ゾーン オブジェクトがデバイスのポリシーに含まれるルールに関連付けられていない場合、そのオブジェクトは「関連付けられていない」と見なされ、デバイスの検索結果に表示されません。

ステップ 2 オブジェクトを選択します。

ステップ 3 右側の [操作（Actions）] ウィンドウで [編集（Edit）] アイコン をクリックします。

ステップ 4 オブジェクトの属性を編集した後、[保存（Save）] をクリックします。

ステップ 5 [保存（Save）] をクリックすると、加えた変更が他のデバイスにどのように影響するかを説明するメッセージが表示されます。[確認（Confirm）] をクリックして変更を確定するか、[キャンセル（Cancel）] をクリックして変更を取り消します。

サービス オブジェクト

Firepower サービスオブジェクト

FTD サービスオブジェクト、サービスグループ、およびポートグループは、IP プロトコルスイートの一部が考慮されたプロトコルまたはポートを含む再利用可能なコンポーネントです。

FTD サービスグループは、サービスオブジェクトのコレクションです。1 つのサービスグループには、1 つ以上のプロトコルのオブジェクトを含めることができます。その後、トラフィックの一致基準を定義するためのセキュリティポリシーでオブジェクトを使用して、たとえばアクセス ルールを使用して特定の TCP ポートへのトラフィックを許可できます。システムには、一般的なサービス向けの複数の事前定義されたオブジェクトが含まれています。これらのオブジェクトはポリシーで使用できます。ただし、システムで定義されたオブジェクトは編集または削除ができません。

Firepower Defense Manager および Firepower Management Center では、サービスオブジェクトをポートオブジェクトとして、およびサービスグループとポートグループとして参照します。

詳細については、「Firepower サービスオブジェクトの作成および編集」を参照してください。

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（FTD）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（Protocols"）」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。

詳細については、「Firepower サービスオブジェクトの作成および編集」を参照してください。

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。

詳細については、「Firepower サービスオブジェクトの作成および編集」を参照してください。

関連情報：

- オブジェクトの削除 （125 ページ）

Firepower サービスオブジェクトの作成および編集

Firepower サービスオブジェクトを作成するには、次の手順を実行します。

Firepower Threat Defense（FTD）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。Firepower Defense Manager および Firepower Management Center では、それらのオブジェクトを「ポートオブジェクト」と呼びます。

手順

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

ステップ 2 右側の青色のボタン をクリックしてオブジェクトを作成し、**[FTD]**>**[サービス（Service）]** を選択します。

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 次の手順に従い、プロトコルを設定します。

- **TCP**、**UDP**
  - [eq] を選択し、ポート番号またはプロトコル名を入力します。たとえば、ポート番号として 80 を入力したり、プロトコル名として HTTP を入力したりできます。
  - [範囲（range）] を選択して、ポート番号の範囲を入力することもできます（例、1 65535 （すべてのポートをカバーする場合））。
- **ICMP**、**IPv6-ICMP**：ICMP タイプを選択します。タイプをすべての ICMP メッセージに適用するには、[任意（Any）] を選択します。タイプとコードについての詳細は、次のページを参照してください。
  - [ICMP]：http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - [ICMPv6]：http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- [その他（Other）]：目的のプロトコルを選択します。

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レビューして展開するか、待機してから複数の変更を一度に展開します。

Firepower サービスグループの作成

サービスグループは、1 つ以上のプロトコルを表す 1 つ以上のサービスオブジェクトで構成できます。サービスオブジェクトは、グループに追加する前に作成する必要があります。Firepower Defense Manager および Firepower Management Center では、それらのオブジェクトを「ポートオブジェクト」と呼びます。

手順

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

ステップ 2 右側の青いボタン をクリックしてオブジェクトを作成し、[FTD] > [サービス（Service）] を選択します。

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）] をクリックして、オブジェクトをグループに追加します。

- 上記の「Firepower サービスオブジェクトの作成および編集」で行ったように、[作成（Create）] をクリックして新しいオブジェクトを作成します。
- [選択（Choose）] をクリックして、既存のサービスオブジェクトをグループに追加します。この手順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 サービスグループへのサービスオブジェクト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レビューして展開するか、待機してから複数の変更を一度に展開します。

Firepower サービスオブジェクトまたはサービスグループの編集

手順

ステップ 1 左側のメインナビゲーションバーで、[オブジェクト（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 [アクション（Actions）] 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。

ステップ 7 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

セキュリティ グループ タグ グループ

FTD セキュリティグループタグ

セキュリティグループタグについて

Cisco TrustSec ネットワークでトラフィックを分類するために Cisco Identity Services Engine（ISE）を使用して**セキュリティグループタグ**（SGT）を定義して使用する場合は、一致基準として SGT を使用するアクセス制御ルールを作成できます。これにより、IP アドレスではなく、セキュリティ グループ メンバーシップに基づいてアクセスをブロックまたは許可することができます。

ISE で SGT を作成し、各タグにホストまたはネットワークの IP アドレスを割り当てることができます。ユーザー アカウントに SGT を割り当てた場合、SGT はユーザーのトラフィックに割り当てられます。ISE サーバーに接続するように FTD を構成して SGT をした後、CDO で SGT グループを作成し、それらに関するアクセスコントロールルールを構築できます。SGT を FTD デバイスに関連付ける前に、ISE の SGT 交換プロトコル（SXP）マッピングを構成する必要があることに注意してください。詳細は、現在実行しているバージョンの『Cisco Identity Services Engine 管理者ガイド』の「**セキュリティグループタグ交換プロトコル**」を参照してください。

FTD は、アクセス制御ルールのトラフィック一致基準として SGT を評価するときに、次の優先順位を使用します。

1. パケット内で定義されている送信元SGT（存在する場合）。宛先の照合は、この手法では行われません。SGTがパケットに含まれるようにするには、ネットワーク内のスイッチとルータがそれらを追加するように設定されている必要があります。このメソッドの実装方法については、ISE のマニュアルを参照してください。
2. ISEセッションディレクトリからダウンロードされるユーザーセッションに割り当てられた SGT。この種の SGT 照合では、セッションディレクトリ情報をリッスンするオプションを有効にする必要がありますが、このオプションは最初に ISE アイデンティティソースを作成するときにデフォルトでオンになっています。SGTは、送信元または宛先と照合することができます。必須ではありませんが、通常は ISE アイデンティティソースを AD レルムとともに使用してパッシブ認証アイデンティティルールを設定し、ユーザ ID 情報を収集します。
3. SXP を使用してダウンロードされた SGT-to-IP アドレス マッピング。IP アドレスが SGT の範囲内にある場合、トラフィックはSGTを使用するアクセス制御ルールと一致します。SGT は、送信元または宛先と照合することができます。

（注） ISE から取得した情報をアクセス制御ルールで直接使用することはできません。代わりにウンロードした SGT 情報を参照する SGT グループを作成する必要があります。SGT グルは複数の SGT を参照できます。そのため、必要に応じて、関連するタグのコレクションづいてポリシーを適用できます。

バージョン サポート

CDO は現在、バージョン 6.5 以降を実行している FTD で SGT および SGT グループをサポートしています。FDM では、バージョン 6.5 以降で ISE サーバを構成して接続できますが、バージョン 6.7 までは FDM UI からの SGT 構成をサポートしていません。

これは、バージョン 6.5 以降を実行している FTD は SGT の SXP マッピングをダウンロードできますが、オブジェクトまたはアクセスコントロールルールに手動で追加できないことを意味します。バージョン 6.5 またはバージョン 6.6 を実行しているデバイスの SGT に変更を加えるには、ISE UI を使用する必要があります。ただし、バージョン 6.5 を実行しているデバイスが CDO にオンボーディングされている場合は、デバイスに関連付けられている現在の SGT を表示し、SGT グループを作成できます。

CDO の SGT

セキュリティグループタグ

SGT は、CDO では読み取り専用です。CDO で SGT を作成または編集することはできません。SGT を作成するには、現在実行しているバージョンの『Cisco Identity Services Engine 管理者ガイド』を参照してください。https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html

SGT グループ

（注） FDM では、SGT のグループを SGT 動的オブジェクトと呼びます。CDO では、これらのタグのリストは現在 SGT グループと呼ばれています。FDM または ISE UI を参照せずに、CDO で SGT グループを作成できます。

SGT グループを使用して、ISE によって割り当てられた SGT に基づいて送信元または宛先アドレスを識別します。その後、トラフィックの一致基準を定義するためにアクセス制御ルールでオブジェクトを使用できます。ISE から取得した情報をアクセス制御ルールで直接使用することはできません。代わりに、ダウンロードした SGT 情報を参照する SGT グループを作成する必要があります。

SGT グループは複数の SGT を参照できます。そのため、必要に応じて、関連するタグのコレクションに基づいてポリシーを適用できます。

CDO で SGT グループを作成するには、少なくとも 1 つの構成済み SGT と、使用するデバイスの FDM コンソール用に構成された ISE サーバーからの SGT マッピングが必要です。複数の FTD が同じ ISE サーバに関連付けられている場合、SGT または SGT グループを複数のデバイスに適用できます。デバイスが ISE サーバに関連付けられていない場合、アクセスコントロールルールに SGT オブジェクトを含めたり、そのデバイス構成に SGT グループを適用したりすることはできません。

ルール内の SGT グループ

SGT グループをアクセスコントロールルールに追加できます。それらは、送信元または宛先のネットワークオブジェクトとして表示されます。ネットワークがルールでどのように機能するかの詳細は、『FTD アクセスコントロールルールの送信元および接続先の条件』を参照してください。

[オブジェクト（Objects）] ページから SGT グループを作成できます。詳細については、FTD SGT グループの作成 （170 ページ）を参照してください。

FTD SGT グループの作成

アクセス制御ルールに使用できる SGT グループを作成するには、次の手順を実行します。

始める前に

セキュリティグループタグ（SGT）グループを作成する前に、次の構成または環境を設定しておく必要があります。

- FTD デバイスは、少なくともバージョン 6.5 を実行している必要があります。
- SXP マッピングを登録して変更を展開できるように ISE アイデンティティソースを設定する必要があります。SXP マッピングの管理については、使用しているバージョン（バージョン 6.7 以降）用の『Firepower Device Manager Configuration Guide』[英語] の「**Configure Security Groups and SXP Publishing in ISE**」を参照してください。

- すべての SGT は ISE で作成する必要があります。SGT の作成については、現在実行しているバージョンの『Cisco Identity Services Engine コンフィギュレーション ガイド』を参照してください。

手順

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）] をクリックします。

ステップ 2 青色のプラスボタン  をクリックして、オブジェクトを作成します。

ステップ 3 [FTD] > [ネットワーク（Network）] をクリックします。

ステップ 4 [オブジェクト名（Object Name）] を入力します。

ステップ 5 （任意）説明を追加します。

ステップ 6 [SGT] をクリックし、ドロップダウンメニューを使用して、グループに含めるすべての SGT のチェックボックスをオンにします。SGT 名順にリストをソートできます。

ステップ 7 [保存（Save）] をクリックします。

（注） CDO で SGT を作成したり編集したりすることはできません。SGT グループへの追加やグループからの削除のみを実行できます。SGT を作成または編集するには、現在実行しているバージョンの『Cisco Identity Services Engine Configuration Guide』を参照してください。

FTD SGT グループの編集

SGT グループを編集するには、次の手順を使用します。

手順

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 SGT グループを見つけます。

ステップ 3 SGT グループを選択し、[操作（Actions）] ウィンドウで編集アイコン  をクリックします。

ステップ 4 SGT グループを変更します。グループに関連付けられた名前、説明、または SGT を編集します。

ステップ 5 [保存（Save）] をクリックします。

（注） CDO で SGT を作成したり編集したりすることはできません。SGT グループへの追加やグループからの削除のみを実行できます。SGT を作成または編集するには、現在実行しているバージョンの『Cisco Identity Services Engine Configuration Guide』を参照してください。

FTD SGT グループのアクセス制御ルールへの追加

SGT グループをアクセス制御ルールに追加するには、次の手順を実行します。

手順

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（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 [FTD] タブをクリックして、SGT グループを追加するデバイスを選択します。

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

ステップ 5 [送信元（Source）] オブジェクトまたは [宛先（Destination）] オブジェクトの青いプラスボタン  をクリックし、[SGTグループ（SGT Groups）] を選択します。

ステップ 6 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 SGT グループを見つけます。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 すべてのデバイスの設定変更をプレビューして展開します。

（注） 追加のSGTグループを作成する必要がある場合は、[新しいオブジェクトを作成（Create New Object）] をクリックします。「FTD SGT グループの作成」に記載されている必須情報を入力し、SGT グループをルールに**追加**します。

Syslog サーバーオブジェクト

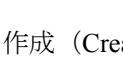
FTD ではイベントを保存するための容量が制限されています。イベントのストレージを最大化するために、外部サーバーを構成できます。システムログ（syslog）サーバーのオブジェクトはコネクション型メッセージまたは診断 syslog メッセージを受信できるサーバーを指定します。syslog サーバーにログ収集と分析のための設定がある場合は、Defense Orchestrator を使用してオブジェクトを作成してそれらを定義し、関連ポリシーでこのオブジェクトを使用します。

Syslog サーバーオブジェクトの作成および編集

新しい syslog サーバーオブジェクトを作成するには、次の手順を実行します。

手順

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

ステップ 2 新しいオブジェクトを作成するには、[オブジェクトの作成（Create Object）] ボタン  をクリックします。

ステップ 3 FTD オブジェクトタイプの下で [Syslog サーバ（Syslog Server）] を選択します。

ステップ 4 syslog サーバーオブジェクトのプロパティを設定します。

- [IPアドレス（IP Address）]：syslog サーバーの IP アドレスを入力します。
- [プロトコルタイプ（Protocol Type）]：syslog サーバーがメッセージの受信に使用するプロトコルを選択します。[TCP] を選択すると、システムは syslog サーバーが利用できない場合を認識して、サーバーが再度利用可能になるまでイベントの送信を停止できます。
- [ポート番号（Port Number）]：syslog に使用する有効なポート番号を入力します。syslog サーバーがデフォルトのポートを使用している場合は、デフォルトの UDP ポートとして 514 を入力するか、デフォルトの TCP ポートとして 1470 を入力します。サーバーがデフォルトのポートを使用していない場合は、正しいポート番号を入力します。1025 ～ 65535 の範囲のポートを使用してください。
- [インターフェイスの選択（Select an interface）]：診断 syslog メッセージの送信に使用するインターフェイスを選択します。接続および侵入イベントでは常に管理インターフェイスを使用します。インターフェイスの選択によって、syslog メッセージに関連付けられる IP アドレスが決まります。以下にリストされているオプションで選択できるのは 1 つだけです。両方を選択することはできません。次のオプションのいずれかを選択します。
  - [データインターフェイス（Data Interface）]：選択したデータ インターフェイスを診断 syslog メッセージに使用します。生成されたリストからインターフェイスを選択します。サーバーがブリッジグループのメンバーインターフェイスを介してアクセスできる場合、ブリッジグループインターフェイス（BVI）を選択します。診断インターフェイス（物理的な管理インターフェイス）経由でアクセスできる場合は、このオプションではなく [管理インターフェイス（Management Interface）] を選択することを推奨します。パッシブインターフェイスを選択することはできません。データインターフェイスで通信する場合、接続および侵入の syslog メッセージでは、送信元 IP アドレスが管理インターフェイスかゲートウェイ インターフェイスで使用されます。
  - [管理インターフェイス（Management Interface）]：すべてのタイプの syslog メッセージに仮想管理インターフェイスを使用します。データ インターフェイスで通信する場合、送信元 IP アドレスが管理インターフェイスかゲートウェイ インターフェイスで使用されます。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

Syslog サーバーオブジェクトの編集

既存の syslog サーバーオブジェクトを編集するには、次の手順を実行します。

手順

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

ステップ 2 対象の syslog サーバーオブジェクトを見つけて選択します。オブジェクトリストは、syslog サーバーオブジェクトタイプでフィルタリング できます。

ステップ 3 [アクション（Actions）] ペインで、[編集（Edit）] をクリックします。

ステップ 4 必要な編集を行って、[保存（Save）] をクリックします。

ステップ 5 行った変更を確認します。

ステップ 6 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

関連情報：

- オブジェクトの削除

Secure Logging Analytics（SaaS）の Syslog サーバーオブジェクトの作成

イベントを送信する Secure Event Connector（SEC）の IP アドレス、TCP ポート、または UDP ポートを使用して、syslog サーバーオブジェクトを作成します。テナントにオンボーディングした SEC ごとに 1 つの syslog オブジェクトを作成しますが、1 つのルールから 1 つの SEC を表す 1 つの syslog オブジェクトのみにイベントを送信します。

前提条件

このタスクは、より大きなワークフローの一部です。開始する前に「FTD デバイスに安全なロギング分析（SaaS）を導入する」を参照してください。

手順

手順

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

ステップ 2 新しいオブジェクトを作成するには、[オブジェクトの作成（Create Object）] ボタン  をクリックします。

ステップ 3 FTD オブジェクトタイプの下で [Syslog サーバー（Syslog Server）] を選択します。

ステップ 4 syslog サーバーオブジェクトのプロパティを設定します。SEC のこれらのプロパティを見つけるには、アカウントメニューをクリックし、[セキュア コネクタ（Secure Connectors）] をクリックします。次に、syslog オブジェクトを設定する Secure Event Connector を選択し、右側の [詳細（Details）] ペインを調べます。

- [IP アドレス（IP Address）]：SEC の IP アドレスを入力します。
- [プロトコルタイプ（Protocol Type）]：TCP または UDP を選択します。
- [ポート番号（Port Number）]：TCP を選択した場合はポート 10125、UDP を選択した場合は 10025 を入力します。
- [インターフェイスの選択（Select an interface）]：SEC に到達するように設定されたインターフェイスを選択します。

（注） FTD は IP アドレスごとに 1 つの syslog オブジェクトをサポートするため、TCP と UDP のどちらを使用するかを選択する必要があります。

ステップ 5 [追加（Add）] をクリックします。

次のタスク

セキュアロギング分析（SaaS）を導入し、Secure Event Connector を介して Cisco Cloud にイベントを送信するための既存の CDO カスタマーワークフローのステップ 3 に進みます。

URL オブジェクト

URL オブジェクトと URL グループは、Firepower デバイスによって使用されます。URL オブジェクトとグループ（URL オブジェクトと総称する）を使用して、Web リクエストの URL または IP アドレスを定義します。これらのオブジェクトを使用して、アクセス制御ポリシーに手動の URL フィルタリング、またはセキュリティ インテリジェンス ポリシーにブロッキングを実装できます。URL オブジェクトは単一の URL または IP アドレスを定義するのに対して、URL グループは複数の URL または IP アドレスを定義します。

はじめる前に

URL オブジェクトを作成する場合は、次の点に注意してください。

- パスを含めない（つまり、URL に / の文字がない）場合、一致はサーバーのホスト名のみに基づきます。ホスト名は、:// の区切り記号の後、またはホスト名のドットの後に来る場合、一致とみなされます。たとえば、ign.com は ign.com および www.ign.com と一致するが、verisign.com とは一致しません。

- 1 つ以上の / を含める場合、サーバ名、パス、およびクエリ パラメータを含む文字列の部分一致には URL 文字列全体が使用されます。ただし、サーバは再構成することができ、ページは新しいパスに移動できるため、個々の Web ページまたはサイトの一部をブロックまたは許可するのに手動の URL フィルタリングは使用しないことをお勧めします。文字列の部分一致も予期しない一致となる可能性があり、URL オブジェクトに含める文字列が意図しないサーバ上のパスやクエリ パラメータ内の文字列とも一致することがあります。
- システムは、暗号化プロトコル（HTTP と HTTPS）を無視します。つまり、ある Web サイトをブロックした場合、アプリケーション条件で特定のプロトコルを対象にしない限り、その Web サイトに向かう HTTP トラフィックと HTTPS トラフィックの両方がブロックされます。URL オブジェクトを作成する場合は、オブジェクトの作成時にプロトコルを指定する必要はありません。たとえば、http://example.com の代わりに example.com を使用します。
- アクセス コントロール ルールで URL オブジェクトを使用して HTTPS トラフィックを照合することを計画している場合は、トラフィックの暗号化に使用される公開キー証明書内でサブジェクトの共通名を使用するオブジェクトを作成します。なお、システムはサブジェクトの共通名に含まれるドメインを無視するため、サブドメイン情報は含めないでください。たとえば、www.example.com ではなく、example.com を使用します。

  ただし、証明書のサブジェクト共通名が Web サイトのドメイン名とはまったく関係ない場合があることをご了承ください。たとえば、youtube.com の証明書のサブジェクト共通名は *.google.com です（当然、これは随時変更される可能性があります）。SSL 復号ポリシーを使用して HTTPS トラフィックを復号し、URL フィルタリング ルールが復号されたトラフィックで動作するようにすると、より一貫性のある結果が得られるようになります。

（注） 証明書情報を利用できないためにブラウザが TLS セッションを再開した場合、URL オブジェクトは HTTPS トラフィックと一致しません。このため、慎重に URL オブジェクトを設定した場合でも、HTTPS 接続では一貫性のない結果が得られることがあります。

FTD URL オブジェクトの作成または編集

Firepower Threat Defense（FTD）URL オブジェクトは、URL または IP アドレスを指定する再利用可能なコンポーネントです。Firepower Defense Manager および Firepower Management Center では、これらのオブジェクトは「URL オブジェクト」とも呼ばれます。

Firepower URL オブジェクトを作成するには、次の手順を実行します。

手順

ステップ 1 [オブジェクト（Objects）] タブをクリックして、[オブジェクト（Objects）] ページを開きます。

ステップ 2 **[オブジェクトの作成（Create Object）]** > **[FTD]** > **[URL]**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 [URLオブジェクトの作成（Create a URL object）] を選択します。

ステップ 5 オブジェクトに固有の URL または IP 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。

Firepower URL グループの作成

URL グループは、1 つ以上の URL または IP アドレスを表す 1 つ以上の URL オブジェクトで構成できます。Firepower Defense Manager および Firepower Management Center では、これらのオブジェクトは「URL オブジェクト」とも呼ばれます。

手順

ステップ 1 [オブジェクト（Objects）] タブをクリックして、[オブジェクト（Objects）] ページを開きます。

ステップ 2 **[オブジェクトの作成（Create Object）]** > **[FTD]** > **[URL]**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 [URLグループの作成（Create a URL 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 URL グループへの URL オブジェクトの追加が完了したら、[追加（Add）] をクリックします。

Firepower URL オブジェクトまたは URL グループの編集

手順

ステップ 1 [オブジェクト（Objects）] タブをクリックして、[オブジェクト（Objects）] ページを開きます。

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、編集する  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。