



AWS デバイスの設定

この章は、次のセクションで構成されています。

- [AWS VPC 接続ログイン情報の更新](#) (1 ページ)
- [AWS Transit Gateway を使用して AWS VPC トンネルを監視する](#) (2 ページ)
- [サイト間 VPN トンネルの検索とフィルタ処理](#) (3 ページ)
- [AWS VPC トンネルに加えられた変更の履歴を表示する](#) (4 ページ)
- [セキュリティ ポリシー管理](#) (5 ページ)
- [仮想プライベートネットワークの管理](#) (9 ページ)
- [変更の読み取り、破棄、チェック、および展開](#) (17 ページ)
- [すべてのデバイス設定の読み取り](#) (19 ページ)
- [すべてのデバイスの構成変更のプレビューと展開](#) (20 ページ)
- [変更のデバイスへの展開](#) (21 ページ)
- [デバイス設定の一括展開](#) (22 ページ)
- [スケジュールされた自動展開](#) (23 ページ)
- [設定変更の確認](#) (25 ページ)
- [変更の破棄](#) (26 ページ)
- [デバイスのアウトオブバンド変更](#) (27 ページ)
- [Defense Orchestrator とデバイス間の設定を同期する](#) (27 ページ)
- [競合検出](#) (28 ページ)
- [デバイスからのアウトオブバンド変更の自動的な受け入れ](#) (29 ページ)
- [設定の競合の解決](#) (30 ページ)
- [デバイス変更のポーリングのスケジュール](#) (32 ページ)

AWS VPC 接続ログイン情報の更新

AWS VPC に接続するための新しいアクセスキーとシークレットアクセスキーを作成する場合は、CDO で接続ログイン情報を更新する必要があります。AWS コンソールでログイン情報を更新し、次の手順を使用して CDO コンソールからログイン情報を更新します。詳細については、『*Managing Access Keys for IAM Users*』

(https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html) または

『[Creating, Disabling, and Deleting Access Keys for Your AWS Account Root User](https://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html)』
(<https://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html>) を参照してください。

CDO からアクセスキーまたはシークレットアクセスキーを変更することはできません。この接続ログイン情報は、AWS コンソールまたは AWS CLI コンソールから手動で管理する必要があります。



(注) 複数の AWS VPC を CDO テナントに導入準備している場合は、一度に 1 つのデバイスのログイン情報を更新する必要があります。

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

ステップ 2 [デバイス] タブをクリックしてから、[AWS VPC] 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 AWS VPC を選択します。

[フィルタ機能](#)と[検索機能](#)を使用して、必要なデバイスを見つけることができます。

ステップ 4 [デバイスアクション (Device Action)] 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 AWS VPC への接続に使用する新しいアクセスキーとシークレットアクセスキーを入力します。

ステップ 6 [更新 (Update)] をクリックします。

(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、無効なユーザー名とパスワードの組み合わせを使用した可能性があります。[無効なログイン情報のトラブルシューティング](#)を参照してください。

関連情報

- [AWS VPC の導入準備](#)

AWS Transit Gateway を使用して AWS VPC トンネルを監視する

AWS Transit Gateway は、簡素化されたピアリング関係を可能にする中央ハブを介してエンタープライズ VPC を AWS VPC に接続するクラウドルータとして機能します。

CDO を使用すると、AWS Transit Gateway を使用してオンボードされた AWS VPC の接続ステータスを監視できます。



- (注) AWS Transit Gateway を使用して監視する上で、CDO に Secure Firewall Cloud Native (SFCN) VPC をオンボードする必要はありません。AWS VPC のオンボーディングについては、[AWS VPC の導入準備](#) を参照してください。

ステップ 1 CDO メニューバーで、[VPNとゼロトラスト (VPN and Zero Trust)] > [サイト間VPN (Site-to-Site VPN)] を選択します。

ステップ 2 [VPNトンネル (VPN Tunnels)] ページには、CDO テナントによって管理されるすべてのネットワークトンネルの接続ステータスが表示されます。VPN トンネルの接続ステータスは、[サイト間 VPN トンネルの検索とフィルタ処理](#) です。

ステップ 3 [アクション (Actions)] ペインの [接続の確認 (Check Connectivity)] リンクをクリックして、トンネルに対するリアルタイムの接続チェックをトリガーし、トンネルが現在[サイト間VPNトンネルの検索とフィルタ処理](#)かを識別できます。オンデマンド接続チェックリンクをクリックしない限り、すべてのオンボードデバイスで利用可能なすべてのトンネルでのチェックが 10 分ごとに実行されます。

- (注) VPN トンネルの接続がダウンすると、CDO から通知が表示されます。ただし、リンクが復旧した場合、通知プロンプトは表示されません。

Name	Status	Peer 1 Name	Peer 1 IP	Peer 2 Name	Peer 2 IP	Last active
VPN 1	Idle	abc-q1w2e3r4t5y6u7i8 AWS VPC	209.165.200.230	def-o9p0s1a2f3g4h5j6 Unknown	209.165.201.31	4/8/22 7:12 AM
VPN 1	Active	abc-q1w2e3r4t5y6u7i8 AWS VPC	209.165.202.148	def-o9p0s1a2f3g4h5j6 Unknown	209.165.201.31	5/10/22 2:32 PM

関連情報

- [AWS VPC の導入準備](#)

サイト間 VPN トンネルの検索とフィルタ処理

フィルタサイドバー を検索フィールドと組み合わせて使用して、VPN トンネル図に示されている VPN トンネルの検索を絞り込みます。

ステップ 1 メインのナビゲーションバーで、[VPN] > [サイト間VPN] に進みます。

ステップ 2 フィルタアイコン をクリックしてフィルタペインを開きます。

ステップ 3 これらのフィルタを使用して検索を絞り込みます。

AWS VPC トンネルに加えられた変更の履歴を表示する

- [デバイスによるフィルタ] : [デバイスによるフィルタ] をクリックし、[デバイスタイプ] タブを選択し、フィルタ処理によって検索するデバイスをオンにします。
- [デバイスの問題] : トンネルの各サイドでの問題検出の有無。問題のあるデバイスの例としては、関連するインターフェイス、ピア IP アドレス、またはアクセスリストの欠落、IKEv1 プロポーザルの不一致などがありますが、これらに限定されません（トンネルの問題の検出は、AWS VPC VPN トンネルではまだ使用できません）。
- [デバイス/サービス] : デバイスのタイプ別にフィルタ処理します。
- [ステータス] : トンネルのステータスは、アクティブまたはアイドルになります。
 - [アクティブ] : セッションが開かれ、ネットワークパケットが VPN トンネルを通過している、または正常なセッションが確立され、タイムアウトになっていない場合。アクティブであることは、トンネルがアクティブで関連していることを示します。
 - [アイドル] : CDO が該当のトンネル用のセッションが開かれていることを検出できない、トンネルが使用されていない、またはトンネルに問題がある場合。
- [導入準備済み] : デバイスは、CDO によって管理される場合と、CDO によって管理されない場合（管理対象外）があります。
- [デバイスタイプ] : トンネルの各サイドが実際のデバイス（接続されたデバイス）かモデルデバイスか。

ステップ 4 検索バーにデバイス名または IP アドレスを入力して、フィルタ処理された結果を検索することもできます。検索では大文字と小文字は区別されません。

AWS VPC トンネルに加えられた変更の履歴を表示する

AWS VPC トンネルに加えられた変更の履歴を表示するには :

ステップ 1 CDO メニューバーで、[ログの変更 (Change Log)] を選択します。

ステップ 2 [ログの変更 (Change Log)] ページで、フィルタアイコンをクリックし、[デバイス別のフィルタ処理 (Filter by device)] タブを選択して、[AWS VPC] をクリックします。

ステップ 3 履歴を確認する [AWS VPC] を選択し、[OK] をクリックします。

関連情報

- [変更ログ](#)

セキュリティ ポリシー管理

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

- [AWS VPC ポリシー \(5 ページ\)](#)

AWS VPC ポリシー

Cisco Defense Orchestrator (CDO) は、Amazon Web Services (AWS) アカウントに関連付けられた AWS 仮想プライベートクラウド (VPC) 全体でセキュリティポリシーの一貫性を維持する機能をユーザーに提供します。CDO を使用して、複数のデバイスタイプ間でオブジェクトを共有することもできます。詳細については、次のトピックを参照してください。

AWS VPC と CDO のセキュリティグループ

AWS VPC セキュリティグループルール

AWS セキュリティグループは、セキュリティグループに関連付けられているすべての AWS EC2 インスタンスおよびその他のエンティティへのインバウンドおよびアウトバウンドのネットワークトラフィックを管理するルールのコレクションです。

Amazon Web Services (AWS) コンソールと同様、CDO では各ルールが個別に表示されます。SDC がインターネットにアクセスできる限り、次の環境の AWS 仮想プライベートクラウド (VPC) ルールを作成および管理できます。

- 同じ AWS VPC 内の別のセキュリティグループとの間で情報を送受信できるセキュリティグループ。
- IPv4 または IPv6 アドレスとの間で送受信できるセキュリティグループ。

AWS セキュリティグループを含む CDO でルールを作成するときは、次の制限に注意してください。

- インバウンドトラフィックを許可するルールの場合、送信元は、同じ AWS VPC 内の 1 つ以上のセキュリティグループ オブジェクト、IPv4 または IPv6 CIDR ブロック、あるいは単一の IPv4 または IPv6 アドレスにできます。インバウンドルールには、宛先として 1 つのセキュリティグループ オブジェクトのみ設定できます。
- アウトバウンドトラフィックを許可するルールの場合、宛先は、同じ AWS VPC 内の 1 つ以上のセキュリティグループ オブジェクト、プレフィックスリスト ID、IPv4 または IPv6 CIDR ブロック、単一の IPv4 または IPv6 アドレスにできます。アウトバウンドルールには、送信元として 1 つのセキュリティグループ オブジェクトのみ設定できます。

- CDO は、複数のポートやサブネットなど、複数のエンティティを含むルールを、AWS VPC に展開する前に個別のルールに変換します。
- ルールを追加または削除すると、セキュリティグループに関連付けられているすべての AWS エンティティに変更が自動的に適用されます。
- 1 つの AWS セキュリティグループでホストできるのは、最大 60 のインバウンドルールと 60 のアウトバウンドルールに制限されています。この制限は、IPv4 ルールと IPv6 ルールに個別に適用されます。CDO で作成された追加のルールは、ルールの総数に含まれます。つまり、CDO への導入準備によって 60 のルールの制限を超えることはできません。



警告 既存のルールを編集すると、編集したルールが削除され、新しい詳細情報を使用して新しいルールが作成されます。そのため、そのルールに依存するトラフィックが、新しいルールが作成されるまでのごく短い間ドロップされます。まったく新しいルールを作成した場合、ドロップは発生しません。

AWS コンソールから作成できるルールのタイプの詳細情報が必要な場合は、[AWS セキュリティグループオブジェクト](#)を参照してください。AWS VPC に関連付けることができるオブジェクトの詳細については、[AWS セキュリティグループとクラウドセキュリティグループのオブジェクト](#)を参照してください。

関連情報

- [セキュリティグループルールの作成](#) (6 ページ)
- [セキュリティグループルールの編集](#) (8 ページ)
- [セキュリティグループルールの削除](#) (8 ページ)

セキュリティグループルールの作成



デフォルトでは、Amazon Web Services (AWS) の Virtual Private Cloud (VPC) はすべてのネットワークトラフィックをブロックします。つまり、トラフィックを許可するように自動的にルールが設定されます。このアクションは編集できません。



(注) 新しいセキュリティグループルールを作成する際、作成したルールをセキュリティグループに関連付ける必要があります。

AWS コンソールは、複数の送信元や宛先を含むルールをサポートしていません。つまり、複数のエンティティを含む単一のセキュリティグループルールを展開すると、CDO はそのルールを個別のルールに変換してから AWS VPC にデプロイします。たとえば、2 つのポート範囲から 1 つのクラウドセキュリティグループオブジェクトへのトラフィックを許可するインバウンドルールを作成すると、CDO はそれを次の 2 つの個別ルールに変換します。(1) 最初のポート範囲からセキュリティグループへのトラフィックを許可します。(2) 2 番目のポート範囲からセキュリティグループへのトラフィックを許可します。

セキュリティグループルールを作成するには、次の手順を実行します。

- ステップ 1** ナビゲーションウィンドウで、[デバイスとサービス (Devices & Services)] をクリックします。
- ステップ 2** [Template] タブをクリックします。
- ステップ 3** [AWS] タブをクリックし、アクセス コントロール ポリシーを編集する AWS VPC デバイステンプレートを選択します。
- ステップ 4** 右側の [管理] ペインで、[ポリシー] を選択します。
- 
- ステップ 5** ルールを追加するセキュリティグループの横にある青いプラスボタンをクリックします。
- 
- ステップ 6** [インバウンド (Inbound)] または [アウトバウンド (Outbound)] をクリックします。
- [インバウンド (Inbound)] ルール：送信元ネットワークには、1 つまたは複数の IPv4 アドレス、IPv6 アドレス、またはクラウドセキュリティグループ オブジェクトを含めることができます。宛先ネットワークは、単一のクラウドセキュリティグループ オブジェクトとして定義する **必要があります**。
 - [アウトバウンド (Outbound)] ルール：送信元ネットワークは、単一のクラウドセキュリティグループ オブジェクトとして定義する **必要があります**。宛先ネットワークには、1 つまたは複数の IPv4 アドレス、IPv6 アドレス、またはセキュリティグループ オブジェクトを含めることができます。
- ステップ 7** ルール名を入力します。英数字、スペース、および次の特殊文字を使用できます：+ . _ -
- ステップ 8** 次のタブ内の属性を任意に組み合わせて、トラフィック一致基準を定義します。
- [送信元 (Source)]：[送信元 (Source)] タブをクリックして、ネットワーク（ネットワークと大陸を含む）を追加または削除します。ポートまたはポート範囲を送信元として定義することはできません。
 - [接続先 (Destination)]：[接続先 (Destination)] タブをクリックして、ネットワーク（ネットワークと大陸を含む）またはネットワークトラフィック着信ポートを追加または削除します。デフォルト値は、[任意 (Any)] です。
- (注)：
ネットワークオブジェクトが定義されていない場合、AWS コンソールでは、IPv4 (0.0.0.0/0) と IPv6 (:::0/0) の 2 つのルールに変換されます。
- ステップ 9** [保存 (Save)] をクリックします。
- ステップ 10** 行った変更を今すぐ **すべてのデバイスの構成変更のプレビューと展開** か、待機してから複数の変更を一度に展開します。

注意 展開に失敗すると、CDO は AWS VPC の状態を展開を試みる前の状態に戻そうとします。これは「ベストエフォート」ベースで行われます。AWS は「状態」を維持しないため、このロールバックの試行は失敗する可能性があります。その場合、AWS マネジメントコンソールにログインし、AWS VPC を以前の設定に手動で戻して CDO に [変更の読み取り、破棄、チェック、および展開](#) 必要があります。


セキュリティグループルールの編集


この手順を使用して、CDO を使用して AWS VPC のアクセス制御ルールを編集します。

ステップ 1 [デバイスとサービス] 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 [AWS] タブをクリックし、アクセス コントロール ポリシーを編集する AWS VPC を選択します。

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

ステップ 5 既存のセキュリティグループルールを編集するには、ルールを選択し、[アクション (Actions)] ペインの編集アイコン  をクリックします。(単純な編集は、編集モードに移行せずにインラインで実行することも可能です。) ルールの制限と例外については、「[AWS VPC セキュリティグループルール](#)」を参照してください。

ステップ 6 [保存 (Save)] をクリックします。

ステップ 7 行った変更を今すぐ [すべてのデバイスの構成変更のプレビューと展開](#) か、待機してから複数の変更を一度に展開します。


注意 展開に失敗すると、CDO は AWS VPC の状態を展開を試みる前の状態に戻そうとします。これは「ベストエフォート」ベースで行われます。AWS は「状態」を維持しないため、このロールバックの試行は失敗する可能性があります。その場合、AWS マネジメントコンソールにログインし、AWS VPC を以前の設定に手動で戻し、AWS VPC デバイス設定と CDO の設定の間の変更をポーリングする必要があります。


セキュリティグループルールの削除

ステップ 1 [デバイスとサービス] ページを開きます。

ステップ 2 [デバイス] タブをクリックしてデバイスを見つけるか、[テンプレート] 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 [AWS] タブをクリックし、アクセス コントロール ポリシーを編集する AWS VPC を選択します。

ステップ 4 右側の [管理] ペインで、 [ポリシー] を選択します。

ステップ 5 不要になったセキュリティグループルールを削除するには、ルールを選択し、[アクション] ペインで削除アイコン  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、複数の変更を一度に待って展開します。[すべてのデバイスの構成変更のプレビューと展開 \(20 ページ\)](#)

注意 展開に失敗すると、CDO は AWS VPC の状態を展開を試みる前の状態に戻そうとします。これは「ベストエフォート」ベースで行われます。AWS は「状態」を維持しないため、このロールバックの試行は失敗する可能性があります。その場合、AWS 管理コンソールにログインし、AWS VPC を以前の構成に手動で戻し、AWS VPC デバイス構成と CDO の構成との間の変更をポーリングする必要があります。

仮想プライベートネットワークの管理

バーチャルプライベートネットワーク (VPN) 接続は、インターネットなどのパブリックネットワークを介してエンドポイント間の安全なトンネルを確立します。

このセクションは、デバイスのリモートアクセスおよびサイト間 VPN に適用されます。また、で VPN 接続を構築し、リモートでアクセスするために使用する SSL 標準についても説明します。

CDO は以下のタイプの VPN 接続をサポートします。

- [サイト間仮想プライベートネットワーク](#)

サイト間仮想プライベートネットワーク

サイト間 VPN トンネルは、地理的に異なる場所にあるネットワークを接続します。サイト間トンネルは、Internet Protocol Security (IPsec) プロトコルスイートとインターネットキーエクスチェンジバージョン 2 (IKEv2) を使用して構築されます。VPN 接続が確立されると、ローカルゲートウェイの背後にあるホストはセキュアな VPN トンネルを介して、リモートゲートウェイの背後にあるホストに接続することができます。

関連情報：

- [AWS サイト間仮想プライベートネットワークのモニタリング](#)

AWS サイト間仮想プライベートネットワークのモニタリング

CDO を使用すると、導入準備 AWS デバイスで既存のサイト間 VPN 設定を監視できます。サイト間の設定を変更または削除することはできません。

サイト間 VPN トンネルの接続の確認

[接続の確認 (Check Connectivity)] ボタンを使用して、トンネルに対するリアルタイムの接続確認をトリガーし、トンネルの現在の状態 (アクティブまたはアイドル) を確認します。[サイト間 VPN トンネルの検索とフィルタ処理 \(3 ページ\)](#) [オンデマンド接続確認 (on-demand

connectivity check)] ボタンをクリックしていない場合、導入準備されているすべてのデバイスで利用可能なすべてトンネルに対する確認が 1 時間に一度実行されます。



(注) • CDO は、トンネルがアクティブかアイドルかを判断するために、ASA および FTD で次の接続確認コマンドを実行します。

```
show vpn-sessiondb l2l sort ipaddress
```

• ASA モデルデバイストンネルは常に [アイドル (Idle)] と表示されます。

[VPN] ページからトンネル接続を確認するには、次の手順を実行します。

ステップ 1 メインのナビゲーションバーで、[VPN]>[サイト間VPN] をクリックします。

ステップ 2 サイト間 VPN トンネルのトンネルのリストを [サイト間 VPN トンネルの検索とフィルタ処理](#) して、選択します。

ステップ 3 右側の [アクション] ペインで、[接続の確認 (Check Connectivity)] をクリックします。

VPN の問題の特定

CDO は、ASA デバイスおよび FTD デバイスでの VPN の問題を特定できます（この機能は、AWS VPC サイト間 VPN トンネルではまだ利用できません）。この記事では次のことを説明します。

- [ピアが欠落している VPN トンネルを見つける](#)
- [暗号化キーの問題がある VPN ピアを見つける](#)
- [トンネルに対して定義された不完全な、または誤った設定のアクセスリストを見つける](#)
- [トンネル設定の問題を見つける](#)


[トンネル設定の問題の解決 \(12 ページ\)](#)

ピアが欠落している VPN トンネルを見つける

「Missing IP Peer」状態は、FTD デバイスよりも ASA デバイスで発生する可能性が高くなります。

ステップ 1 CDO ナビゲーションウィンドウで、[VPN]>[サイト間 VPN (Site-to-Site VPN)] をクリックして VPN ページを開きます。

ステップ 2 [テーブルビュー (Table View)] を選択します。

ステップ 3 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。

ステップ 4 検出された問題を確認します。

ステップ5 問題を報告している各デバイス▲を選択し、右側の [ピア (Peers)] ペインを確認します。1 つのピア名がリストされます。CDO は、他のピア名を「[Missing peer IP.]」として報告します。

暗号化キーの問題がある VPN ピアを見つける

このアプローチを使用して、以下のような暗号化キーの問題がある VPN ピアを見つけます。

- IKEv1 または IKEv2 キーが無効、欠落しているか、一致しない
- トンネルが古くなっているか、暗号化レベルが低い

ステップ1 CDO ナビゲーションバーで、[VPN]>[サイト間VPN] をクリックして VPN ページを開きます。 >

ステップ2 [テーブルビュー] を選択します。

ステップ3 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。

ステップ4 問題を報告している各デバイス▲を選択し、右側の [ピア] ペインを確認します。ピア情報には、両方のピアが表示されます。

ステップ5 いずれかのデバイスの [ピアの表示] をクリックします。

ステップ6 ダイアグラムビューで、問題を報告しているデバイスをダブルクリックします。

ステップ7 下部の [トンネルの詳細] パネルで [キー交換] をクリックします。両方のデバイスを表示して、そこでキーの問題を診断できます。

トンネルに対して定義された不完全な、または誤った設定のアクセスリストを見つける

「アクセスリストが不完全または正しく設定されていない」状態は、ASA デバイスでのみ発生する可能性があります。

ステップ1 CDO ナビゲーションバーで、[VPN]>[サイト間VPN] をクリックして VPN ページを開きます。 >

ステップ2 [テーブルビュー (Table View)] を選択します。

ステップ3 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。

ステップ4 問題を報告している各デバイス▲を選択し、右側の [ピア (Peers)] ペインを確認します。ピア情報には、両方のピアが表示されています。

ステップ5 いずれかのデバイスの [ピアの表示 (View Peers)] をクリックします。

ステップ6 ダイアグラムビューで、問題を報告しているデバイスをダブルクリックします。

ステップ7 下部の [トンネルの詳細] パネルで [トンネルの詳細] をクリックします。「ネットワークポリシー：不完全 (Network Policy: Incomplete) 」というメッセージが表示されます。


トンネル設定の問題を見つける

トンネル設定のエラーは、次のシナリオで FTD デバイスで発生する可能性があります。

- サイト間 VPN インターフェイスの IP アドレスが変更されたときの、「ピア IP アドレス値が変更されました (Peer IP Address Value has changed)」。
- VPN トンネルの IKE 値が他の VPN トンネルと一致しない場合、「IKE 値が一致しません (IKE value Mismatch)」というメッセージが表示されます。

ステップ 1 CDO ナビゲーションバーで、[VPN]>[サイト間VPN] をクリックして VPN ページを開きます。 >

ステップ 2 [テーブルビュー (Table View)] を選択します。

ステップ 3 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。

ステップ 4 [トンネルの問題 (Tunnel Issues)] で、[検出された問題 (Detected Issues)] をクリックして、エラーを報告している VPN 設定を表示します。問題を報告している (▲) 設定を表示できます。

ステップ 5 問題を報告している VPN 設定を選択します。

ステップ 6 右側の [ピア (Peers)] ペインに、問題のあるピアに ▲ アイコンが表示されます。▲ アイコンにカーソルを合わせると、問題と解決策が表示されます。

次のステップ: [トンネル設定の問題の解決](#)。

トンネル設定の問題の解決

この手順では、次のトンネル設定の問題を解決を試みます。

- サイト間 VPN インターフェイスの IP アドレスが変更されたときの、「ピア IP アドレス値が変更されました (Peer IP Address Value has changed)」。
- VPN トンネルの IKE 値が他の VPN トンネルと一致しない場合、「IKE 値が一致しません (IKE value Mismatch)」というメッセージが表示されます。

詳細については、「[トンネル設定の問題を見つける](#)」を参照してください。

ステップ 1 CDO の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、問題を報告している VPN 設定に関連付けられているデバイスを選択します。

ステップ 4 [\[競合検出 \(Conflict Detected\)\] ステータスの解決](#)。

ステップ 5 CDO ナビゲーションウィンドウで、[VPN]>[サイト間VPN] をクリックして VPN ページを開きます。

ステップ 6 この問題を報告している VPN 設定を選択します。

ステップ 7 [アクション] ペインで、[編集] アイコンをクリックします。

ステップ 8 各手順で [次へ] をクリックして、最後に手順 4 で [完了 (Finish)] ボタンをクリックします。

ステップ 9 [すべてのデバイスの構成変更のプレビューと展開 \(20 ページ\)](#)。

管理対象外 VPN ピアの導入準備

ピアの1つが導入準備されると、CDOはサイト間VPNトンネルを検出します。2番目のピアがCDOによって管理されていない場合は、VPNトンネルのリストをフィルタリングして、管理されていないデバイスを見つけて導入準備することができます。

ステップ1 メインナビゲーションバーで、[VPN]>[サイト間VPN]を選択してVPNページを開きます。

ステップ2 [テーブルビュー (Table View)]を選択します。

ステップ3  をクリックしてフィルタパネルを開きます。

ステップ4 [管理対象外 (Unmanaged)] にチェックを入れます。


ステップ5 結果から管理対象外のデバイスを選択します。

ステップ6 右側の[ピア (Peers)] ペインで、[デバイスの導入準備 (Onboard Device)] をクリックし、画面の指示に従います。


関連情報：

- [デバイスとサービスの導入準備](#)
- [AWS VPC の導入準備](#)

サイト間VPNトンネルの検索とフィルタ処理

フィルタサイドバー  を検索フィールドと組み合わせて使用して、VPNトンネル図に示されているVPNトンネルの検索を絞り込みます。

ステップ1 メインのナビゲーションバーで、[VPN]>[サイト間VPN]に進みます。

ステップ2 フィルタアイコン  をクリックしてフィルタペインを開きます。

ステップ3 これらのフィルタを使用して検索を絞り込みます。

- [デバイスによるフィルタ]: [デバイスによるフィルタ] をクリックし、[デバイスタイプ] タブを選択し、フィルタ処理によって検索するデバイスをオンにします。
- [デバイスの問題]: トンネルの各サイドでの問題検出の有無。問題のあるデバイスの例としては、関連するインターフェイス、ピアIPアドレス、またはアクセスリストの欠落、IKEv1プロポーザルの不一致などがありますが、これらに限定されません (トンネルの問題の検出は、AWS VPC VPN トンネルではまだ使用できません)。
- [デバイス/サービス]: デバイスのタイプ別にフィルタ処理します。
- [ステータス]: トンネルのステータスは、アクティブまたはアイドルになります。
 - [アクティブ]: セッションが開かれ、ネットワークパケットがVPNトンネルを通過している、または正常なセッションが確立され、タイムアウトになっていない場合。アクティブであることは、トンネルがアクティブで関連していることを示します。

AWS のサイト間 VPN トンネルを表示する

- [アイドル]: CDO が該当のトンネル用のセッションが開かれていることを検出できない、トンネルが使用されていない、またはトンネルに問題がある場合。
- [導入準備済み]: デバイスは、CDO によって管理される場合と、CDO によって管理されない場合（管理対象外）があります。
- [デバイスタイプ]: トンネルの各サイドが実際のデバイス（接続されたデバイス）かモデルデバイスか。

ステップ 4 検索バーにデバイス名または IP アドレスを入力して、フィルタ処理された結果を検索することもできます。検索では大文字と小文字は区別されません。

AWS のサイト間 VPN トンネルを表示する

AWS サイト間 VPN は、仮想プライベートクラウド（VPC）をセキュアなトンネルを介してエンタープライズ ネットワークに接続します。

すべてのサイト間 VPN 設定は、AWS 管理コンソールで行われます。VPC を導入準備すると、CDO は AWS VPC によって維持されているサイト間 VPN 接続を表示し、それらを [VPN トンネル (VPN Tunnels)] ページに表示するため、その他すべてのサイト間接続とともにそれらを管理できるようにします。ネットワークから VPC への各 VPN 接続は、2 つの個別の VPN トンネルで構成されています。

CDO の [VPN トンネル (VPN Tunnels)] ページでは、[サイト間 VPN トンネル情報の表示](#)したり、[サイト間 VPN トンネルの検索とフィルタ処理](#)したりできます。また、[管理対象外 VPN ピアの導入準備](#)できます。

CDO は 10 分ごとに AWS 管理コンソールをポーリングして、サイト間 VPN 設定の変更を確認します。変更があったことを CDO が検出すると、その設定内の変更をポーリングし、変更をデータベースに保存します。CDO 管理者は、CDO で新しい設定を表示できます。

Amazon Web Services (AWS) 参考資料

[AWS 仮想プライベートネットワークのドキュメント](#)

サイト間 VPN トンネルの IKE オブジェクトの詳細の表示

選択したトンネルのピア/デバイスで設定されている IKE オブジェクトの詳細を表示できます。それらの詳細は、IKE ポリシーオブジェクトの優先順位に基づいた階層のツリー構造に表示されます。



(注) エクストラネットデバイスには、IKE オブジェクトの詳細が表示されません。

ステップ 1 左側の CDO ナビゲーションバーで、[VPN] > [サイト間VPN] をクリックします。

ステップ 2 [VPN トンネル (VPN Tunnels)] ページで、ピアを接続する VPN トンネルの名前をクリックします。

ステップ3 右側の [関係] で、詳細を表示するオブジェクトを展開します。

サイト間 VPN トンネルが最後に正常に確立された日を表示する

ステップ1 [サイト間 VPN トンネル情報の表示](#)。

ステップ2 [トンネルの詳細] ペインをクリックします。

ステップ3 [最終アクティブ確認日 (Last Seen Active)] フィールドを表示します。

サイト間 VPN トンネル情報の表示

サイト間 VPN テーブルビューは、CDO に導入準備されたすべてのデバイスで使用可能なすべてのサイト間 VPN トンネルの完全なリストです。トンネルは、このリストに 1 つだけ存在します。表にリストされているトンネルをクリックすると、右側のサイドバーにオプションが表示され、トンネルのピアに直接移動して詳細に調査できます。

CDO がトンネルの両側を管理していない場合は、[導入準備デバイス (Onboard Device)] をクリックして、管理対象外のピアを導入準備するメインの導入準備ページを開くことができます。[管理対象外 VPN ピアの導入準備 \(13 ページ\)](#) CDO がトンネルの両側を管理する場合、[ピア2 (Peer 2)] 列には管理対象デバイスの名前が含まれます。ただし、AWS VPC の場合、[ピア2 (Peer 2)] 列には VPN ゲートウェイの IP アドレスが含まれています。

テーブルビューでサイト間 VPN 接続を表示するには、次の手順を実行します。

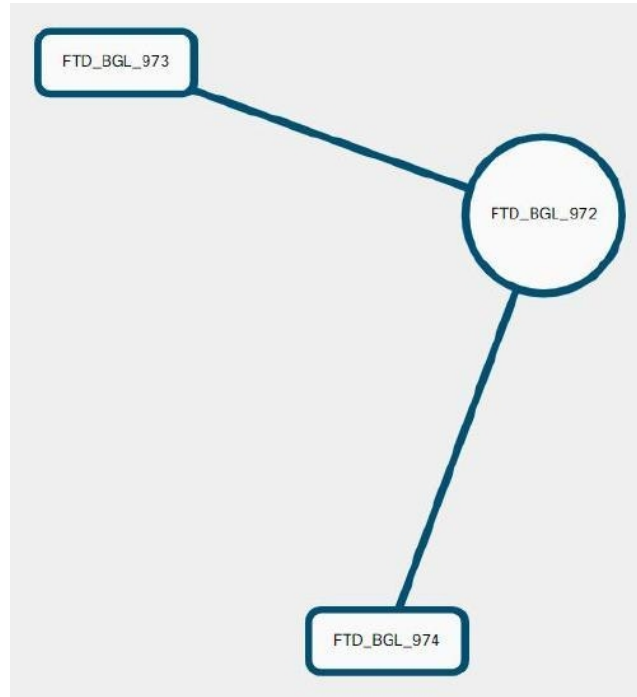
ステップ1 メインのナビゲーションバーで、[VPN] > [サイト間VPN] をクリックします。

ステップ2 [テーブルビュー] ボタンをクリックします。

ステップ3 「[サイト間 VPN トンネルの検索とフィルタ処理](#)」を使用して特定のトンネルを見つけるか、グローバルビューのグラフィックを拡大して、探している VPN ゲートウェイとそのピアを見つけます。

サイト間 VPN のグローバル表示

これは、グローバルビューの例です。この図では、「FTD_BGL_972」に FTD_BGL_973 デバイスおよび FTD_BGL_974 デバイスとのサイト間接続があります。



ステップ 1 メインのナビゲーションバーで、[VPN]>[サイト間VPN] をクリックします。

ステップ 2 [グローバルビュー (Global view)] ボタンをクリックします。

ステップ 3 「[サイト間 VPN トンネルの検索とフィルタ処理](#)」を使用して特定のトンネルを見つけるか、グローバルビューのグラフィックを拡大して、探している VPN ゲートウェイとそのピアを見つけます。

ステップ 4 グローバルビューに表示されているピアのいずれかを選択します。

ステップ 5 [詳細の表示 (View Details)] をクリックします。

ステップ 6 VPN トンネルのもう一方の端をクリックすると、CDO は、その接続のトンネルの詳細、NAT 情報、およびキー交換情報を表示します。

- [トンネルの詳細]: トンネルの名前と接続情報が表示されます。[更新]アイコンをクリックすると、トンネルの接続情報が更新されます。
- [AWS接続固有のトンネルの詳細 (Tunnel Details specific to AWS connections)]: AWS サイト間接続のトンネルの詳細は、他の接続の場合と若干異なります。AWS VPC から VPN ゲートウェイへの接続ごとに、AWS は 2 つの VPN トンネルを作成します。これは、ハイアベイラビリティを実現するためです。
 - トンネルの名前は、VPN ゲートウェイが接続されている VPC の名前を表します。トンネルの名前に含まれている IP アドレスは、VPN ゲートウェイが VPC として認識している IP アドレスです。

- CDO 接続の状態が「active」の場合、AWS トンネルの状態は「Up」です。CDO 接続の状態が「inactive」の場合、AWS トンネルの状態は「Down」です。
- [NAT情報 (NAT Information)]: 使用されている NAT ルールのタイプ、元のパケットの情報、および変換されたパケットの情報が表示され、そのトンネルの NAT ルールを確認できる NAT テーブルへのリンクが提供されます (AWS VPC サイト間 VPN ではまだ利用できません)。
- [キー交換]: トンネルで使用されている暗号キーと、キー交換の問題が表示されます (AWS VPC サイト間 VPN ではまだ利用できません)。

トンネルペイン

[トンネル (Tunnels)] ペインには、特定の VPN ゲートウェイに関連付けられているすべてのトンネルのリストが表示されます。VPN ゲートウェイと AWS VPC のサイト間 VPN 接続の場合、[トンネル (Tunnels)] ペインには、VPN ゲートウェイから VPC へのすべてのトンネルが表示されます。VPN ゲートウェイと AWS VPC のサイト間 VPN 接続にはそれぞれ 2 つのトンネルがあるため、他のデバイスで通常表示される 2 倍の数のトンネルが表示されます。

VPN ゲートウェイの詳細

VPN ゲートウェイに接続されているピア数と、VPN ゲートウェイの IP アドレスが表示されます。これは、[VPN トンネル (VPN Tunnels)] ページにのみ表示されます。

[ピア (Peers)] ペイン

サイト間 VPN ピアのペアを選択すると、ペアリングされた 2 つのデバイスのリストが [ピア (Peers)] ペインに表示され、いずれかのデバイスで [ピアの表示] をクリックできます。[ピアの表示 (View Peers)] をクリックすると、そのデバイスが関連付けられている他のサイト間ピアが表示されます。これは、テーブルビューとグローバルビューに表示されます。

変更の読み取り、破棄、チェック、および展開

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

- [変更の破棄 (Discard Changes)] は、デバイスの設定ステータスが「未同期」の場合に使用できます。未同期の状態では、デバイスの設定に対する変更が CDO で保留中になっています。このオプションを使用すると、保留中のすべての変更を取り消すことができます。保留中の変更は削除され、CDO は設定のコピーをデバイスに保存されている設定のコピーで上書きします。

- [変更の確認 (Check for Changes)]。このアクションは、デバイスの設定ステータスが同期済みの場合に使用できます。[変更の確認 (Checking for Changes)] をクリックすると、CDO は、デバイスの設定のコピーを、デバイスに保存されている設定のコピーと比較するように指示します。違いがある場合、CDO はデバイスに保存されているコピーでそのデバイスの設定のコピーをすぐに上書きします。
- [競合の確認 (Review Conflict)] と [レビューなしで承認 (Accept Without Review)]。デバイスで [競合検出] を有効にすると、CDO はデバイスに加えられた設定の変更を 10 分ごとにチェックします。https://docs.defenseorchestrator.com/Welcome_to_Cisco_Defense_Orchestrator/Basics_of_Cisco_Defense_Orchestrator/Synchronizing_Configurations_Between_Defense_Orchestrator_and_Device/0010_Conflict_Detection デバイスに保存されている設定のコピーが変更された場合、CDO は「競合が検出されました」という設定ステータスを表示して通知します。
 - [競合の確認 (Review Conflict)]。[競合の確認 (Review Conflict)] をクリックすると、デバイスで直接行われた変更を確認し、それらを受け入れるか拒否するかを選択できます。
 - [レビューなしで承認 (Accept Without Review)]。このアクションは、デバイスの設定の CDO のコピーを、デバイスに保存されている設定のコピーで上書きします。CDO は、上書きアクションを実行する前に、設定の 2 つのコピーの違いを確認するように求めません。

[すべて読み取り (Read All)] は一括操作です。任意の状態の複数のデバイスを選択し、[すべて読み取り (Read All)] をクリックして、CDO に保存されているすべてのデバイスの設定を、デバイスに保存されている設定で上書きすることができます。

変更の配置

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

保留中の設定変更は、デバイスを通過するネットワークトラフィックには影響しません。変更は、CDO がデバイスに展開した後にのみ影響を及ぼします。CDO がデバイスの設定に変更を展開すると、変更された設定の要素のみが上書きされます。デバイスに保存されている構成ファイル全体を上書きすることはありません。展開は、1 つのデバイスに対して開始することも、複数のデバイスに対して同時に開始することもできます。

[すべて破棄] は、[プレビューして展開... (Preview and Deploy..)] をクリックした後にのみ使用できるオプションです。[プレビューして展開 (Preview and Deploy)] をクリックすると、CDO で保留中の変更のプレビューが CDO に表示されます。[すべて破棄] をクリックすると、保留中のすべての変更が CDO から削除され、選択したデバイスには何も展開されません。上述の [変更の破棄 (Discard Changes)] とは異なり、保留中の変更を削除すると操作が終了します。

すべてのデバイス設定の読み取り

Cisco Defense Orchestrator (CDO) の外部にあるデバイスの設定が変更された場合、CDO に保存されているデバイスの設定と、当該デバイスの設定のローカルコピーは同じではなくなります。多くの場合、CDO にあるデバイスの設定のコピーをデバイスに保存されている設定で上書きして、設定を再び同じにしたいと考えます。[すべて読み取り (Read All)] リンクを使用して、多くのデバイスでこのタスクを同時に実行できます。

CDO によるデバイス設定の 2 つのコピーの管理方法の詳細については、「[変更の読み取り、破棄、チェック、および展開](#)」を参照してください。

[すべて読み取り (Read All)] をクリックした場合に、CDO にあるデバイスの設定のコピーがデバイスの設定のコピーで上書きされる 3 つの設定ステータスを次に示します。

- [競合検出 (Conflict Detected)] : 競合検出が有効になっている場合、CDO は、設定に加えられた変更について、管理するデバイスを 10 分ごとにポーリングします。CDO は、デバイスの設定が変更されたことを検出した場合、デバイスの [競合検出 (Conflict Detected)] 設定ステータスを表示します。
- [同期 (Synced)] : デバイスが [同期 (Synced)] 状態の場合に、[すべて読み取り (Read All)] をクリックすると、CDO はすぐにデバイスをチェックして、設定に直接変更が加えられているかどうかを判断します。[すべて読み取り (Read All)] をクリックすると、CDO はデバイスの設定のコピーを上書きすることを確認し、上書きを実行します。
- [非同期] : デバイスが [非同期] 状態の場合に、[すべて読み取り (Read All)] をクリックすると、CDO を使用したデバイスの設定に対する保留中の変更があること、および [すべて読み取り (Read All)] 操作を続行すると保留中の変更が削除されてから、CDO にある設定のコピーがデバイス上の設定で上書きされることが警告されます。この [すべて読み取り (Read All)] は、[変更の破棄 (Discard Changes)] と同様に機能します。[変更の破棄 \(26 ページ\)](#)

-
- 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** (任意) 変更ログでこの一括アクションの結果を簡単に識別できるように、[変更リクエストラベル](#)を作成します。
 - ステップ 5** CDO を保存する設定のデバイスを選択します。CDO では、選択したすべてのデバイスに適用できるアクションのコマンドボタンのみ提供されることに注意してください。
 - ステップ 6** [すべて読み取り (Read All)] をクリックします。
 - ステップ 7** 選択したデバイスのいずれかについて、CDO で設定変更がステージングされている場合、CDO は警告を表示し、設定の一括読み取りアクションを続行するかどうかを尋ねられます。[すべて読み取り (Read All)] をクリックして続行します。

- ステップ 8** 設定の [すべて読み取り (Read All)] 操作の進行状況については、[通知 (notifications)] タブで確認します。一括操作の個々のアクションの成功または失敗に関する詳細を確認する場合は、青色の [レビュー (Review)] リンクをクリックすると、[ジョブ] ページに移動します。[ジョブ (Jobs)] ページ
- ステップ 9** 変更リクエストラベルを作成してアクティブ化した場合は、他の設定変更を誤ってこのイベントに関連付けないように、忘れずにラベルをクリアしてください。

関連情報

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

すべてのデバイスの構成変更のプレビューと展開

テナント上のデバイスに構成変更を加えたものの、その変更をまだ展開していない場合に、CDO は展開アイコンにオレンジ色のドットを表示して通知します。




これらの変更の影響を受けるデバイスには、[デバイスとサービス] ページに [非同期] のステータスが表示されます。[展開] をクリックすると、保留中の変更があるデバイスを確認し、それらのデバイスに変更を展開できます。

この展開方法は、サポートされているすべてのデバイスで使用できます。


この展開方法を使用して、単一の構成変更を展開することも、待機して複数の変更を一度に展開することもできます。

手順の概要

1. 画面の右上隅で [展開] アイコン  をクリックします。
2. 展開する変更があるデバイスを選択します。デバイスに黄色の三角の注意マークが付いている場合、そのデバイスに変更を展開することはできません。黄色の三角の注意マークにマウスを合わせると、そのデバイスに変更を展開できない理由を確認できます。
3. デバイスを選択したら、右側のパネルでデバイスを拡大し、具体的な変更をプレビューできます。
4. (オプション) 保留中の変更に関する詳細情報を表示する場合は、[詳細な変更ログを表示] リンクをクリックして、その変更に関連付けられた変更ログを開きます。[展開] アイコンをクリックして、[保留中の変更があるデバイス] ページに戻ります。
5. (オプション) [保留中の変更があるデバイス] ページを離れずに、変更を追跡する [変更リクエスト](#) を作成します。
6. [今すぐ展開] をクリックして、選択したデバイスに今すぐ変更を展開します。[ジョブ] トレイの [アクティブなジョブ] インジケータに進行状況が表示されます。

7. (オプション) 展開が完了したら、CDO ナビゲーションバーの [ジョブ] をクリックします。展開の結果を示す最近の「変更の展開」ジョブが表示されます。
8. 変更リクエストラベルを作成し、それに関連付ける構成変更がない場合は、それをクリアします。

手順の詳細


- ステップ 1** 画面の右上隅で [展開] アイコン  をクリックします。
- ステップ 2** 展開する変更があるデバイスを選択します。デバイスに黄色の三角の注意マークが付いている場合、そのデバイスに変更を展開することはできません。黄色の三角の注意マークにマウスを合わせると、そのデバイスに変更を展開できない理由を確認できます。
- ステップ 3** デバイスを選択したら、右側のパネルでデバイスを拡大し、具体的な変更をプレビューできます。
- ステップ 4** (オプション) 保留中の変更に関する詳細情報を表示する場合は、[詳細な変更ログを表示] リンクをクリックして、その変更に関連付けられた変更ログを開きます。[展開] アイコンをクリックして、[保留中の変更があるデバイス] ページに戻ります。
- ステップ 5** (オプション) [保留中の変更があるデバイス] ページを離れずに、変更を追跡する [変更リクエストを作成](#) します。
- ステップ 6** [今すぐ展開] をクリックして、選択したデバイスに今すぐ変更を展開します。[ジョブ] トレイの [アクティブなジョブ] インジケータに進行状況が表示されます。
- ステップ 7** (オプション) 展開が完了したら、CDO ナビゲーションバーの [ジョブ] をクリックします。展開の結果を示す最近の「変更の展開」ジョブが表示されます。
- ステップ 8** 変更リクエストラベルを作成し、それに関連付ける構成変更がない場合は、それをクリアします。

次のタスク

- [スケジュールされた自動展開](#)

変更のデバイスへの展開

- ステップ 1** CDO を使用してデバイスの設定を変更して保存すると、その変更はデバイスの設定の CDO インスタンスに保存されます。
- ステップ 2** ナビゲーションバーで、[デバイスとサービス (Devices & Services)] をクリックします。
- ステップ 3** [デバイス] タブをクリックします。
- ステップ 4** 適切なデバイスタイプのタブをクリックします。変更を加えたデバイスの設定ステータスが [非同期] と表示されます。
- ステップ 5** 次のいずれかの方法を使用して、変更を展開します。

- デバイスを選択し、右側の [非同期] ペインで [プレビューして展開 (Preview and Deploy)] をクリックします。[保留中の変更 (Pending Changes)] 画面で、変更を確認します。保留中のバージョンに問題がなければ、[今すぐ展開 (Deploy Now)] をクリックします。変更が正常に展開されたら、[変更ログ](#)を表示して、展開の結果を確認できます。
- 画面右上の [展開] アイコン  をクリックします。詳細については、[すべてのデバイスの構成変更のプレビューと展開 \(20 ページ\)](#) を参照してください。

変更をキャンセルする

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


変更の破棄

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


デバイス設定の一括展開


共有オブジェクトを編集するなどして複数のデバイスに変更を加えた場合、影響を受けるすべてのデバイスにそれらの変更を一度に適用できます。

- ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス (Devices & Services)] をクリックします。
- ステップ 2 [デバイス] タブをクリックします。
- ステップ 3 適切なデバイスタイプのタブをクリックします。
- ステップ 4 CDO で設定を変更した、すべてのデバイスを選択します。これらのデバイスは、「未同期」ステータスが表示されているはずですが。
- ステップ 5 次のいずれかの方法を使用して、変更を展開します。

- 画面右上の [展開] ボタン  をクリックします。これにより、選択したデバイス上の保留中の変更を展開する前に確認することができます。変更を展開するには、[今すぐ展開 (Deploy Now)] をクリックします。

(注) [保留中の変更があるデバイス] 画面でデバイスの横に黄色の警告三角形が表示されている場合、そのデバイスに変更を展開することはできません。そのデバイスに変更を展開できない理由を確認するには、警告三角形の上にマウスカーソルを置きます。

- 詳細ペインで[すべて展開 (Deploy All)]  をクリックします。すべての警告を確認し、[OK] をクリックします。一括展開は、変更を確認せずにすぐに開始します。

ステップ 6 (任意) ナビゲーションバーの [ジョブ] アイコン  をクリックして、一括展開の結果を表示します。

スケジュールされた自動展開

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

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

CDO に [変更の読み取り](#)、[破棄](#)、[チェック](#)、および [展開](#) 変更がデバイスに直接加えられた場合、その競合が解決されるまで、展開スケジュールはスキップされます。[ジョブ] 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] をオフにすると、スケジュールされたすべての展開が削除されます。



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



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

自動展開のスケジュール

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



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

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

ステップ2 [デバイス] タブをクリックします。

ステップ3 適切なデバイスタイプのタブをクリックします。

ステップ4 1つ以上のデバイスを選択します。

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

ステップ6 展開をいつ実行するかを選択します。

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

ステップ7 [保存 (Save)] をクリックします。

スケジュールされた展開の編集

スケジュールされた展開を編集するには、次の手順に従います。

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

ステップ2 [デバイス] タブをクリックします。

ステップ3 適切なデバイスタイプのタブをクリックします。

ステップ4 1つ以上のデバイスを選択します。

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



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

ステップ7 [保存 (Save)] をクリックします。

スケジュールされた展開の削除

スケジュールされた展開を削除するには、次の手順に従います。




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

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

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 1 つ以上のデバイスを選択します。

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

次のタスク

- [変更の読み取り、破棄、チェック、および展開](#)
- [すべてのデバイス設定の読み取り \(19 ページ\)](#)
- [すべてのデバイスの構成変更のプレビューと展開 \(20 ページ\)](#)

設定変更の確認

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

変更を確認するには、次の手順を実行します。

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

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 設定がデバイス上で直接変更された可能性があるデバイスを選択します。

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

ステップ 6 次の動作は、デバイスによって若干異なります。

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

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

- [OK] をクリックして、先へ進みます。デバイスの設定で、CDO に保存されている設定が上書きされます。
 - 操作をキャンセルするには、[キャンセル] をクリックします。
- デバイスの場合：
1. 提示された2つの設定を比較します。[続行 (Continue)] をクリックします。最後に認識されたデバイス設定 (**Last Known Device Configuration**) というラベルの付いた設定は、CDO に保存されている設定です。デバイスで検出 (**Found on Device**) というラベルの付いた設定は、ASA に保存されている設定です。
 2. 次のいずれかを選択します。
 1. [拒否 (Reject)] : アウトオブバンド変更を拒否して、「最後に認識されたデバイス設定 (Last Known Device Configuration)」を維持します。
 2. [承認 (Accept)] : アウトオブバンド変更を承認して、CDO に保存されているデバイスの設定を、デバイスで見つかった設定で上書きします。
 3. [続行 (Continue)] をクリックします。

変更の破棄

CDOを使用してデバイスの構成に加えた、展開されていない構成変更のすべてを「元に戻す」場合は、[変更の破棄 (Discard Changes)] をクリックします。[変更の破棄 (Discard Changes)] をクリックすると、CDO は、デバイスに保存されている構成でデバイスの構成のローカルコピーを完全に上書きします。

[変更の破棄 (Discard Changes)] をクリックすると、デバイスの構成ステータスは [非同期] 状態になります。変更を破棄すると、CDO 上の構成のコピーは、デバイス上の構成のコピーと同じになり、CDO の構成ステータスは [同期済み] に戻ります。

デバイスの展開されていない構成変更のすべてを破棄する（つまり「元に戻す」）には、次の手順を実行します。

- ステップ1 ナビゲーションバーで、[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 構成変更を実行中のデバイスを選択します。
- ステップ5 右側の [非同期] ペインで [変更の破棄 (Discard Changes)] をクリックします。

- FTD デバイスの場合は、「Pending changes on CDO will be discarded and the CDO configuration for this device will be replaced with the configuration currently running on the device (CDO 上の保留中の変更は破棄され、このデバイスに関する CDO 構成は、デバイス上の現在実行中の構成に置き換えられます)」という警告メッセージが表示されます。[続行] をクリックして変更を破棄します。
- Meraki デバイスの場合は、変更がすぐに削除されます。
- AWS デバイスの場合は、削除しようとしているものが表示されます。[同意する (Accept)] または [キャンセル] をクリックします。

デバイスのアウトオブバンド変更

アウトオブバンド変更とは、CDO を使用せずにデバイス上で直接行われた変更を指します。アウトオブバンド変更は、SSH 接続を介してデバイスのコマンドライン インターフェイスを使用して、または、ASA の場合は Adaptive Security Device Manager (ASDM) 、FTD の場合は FDM などのローカルマネージャを使用して行うことができます。アウトオブバンド変更により、CDO に保存されているデバイスの設定とデバイス自体に保存されている設定との間で競合が発生します。

デバイスでのアウトオブバンド変更の検出

ASA、FTD、または Cisco IOS デバイスに対して競合検出が有効になっている場合、CDO は 10 分ごとにデバイスをチェックし、CDO の外部でデバイスの設定に直接加えられた新たな変更を検索します。

CDO は、CDO に保存されていないデバイスの設定に対する変更を検出した場合、そのデバイスの [設定ステータス (Configuration Status)] を [競合検出 (Conflict Detected)] 状態に変更します。

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

- CDO のデータベースに保存されていない設定変更が、デバイスに直接加えられています。
- FTD の場合、展開されていない「保留中」の設定変更がある可能性があります。

Defense Orchestrator とデバイス間の設定を同期する

設定の競合について

[デバイスとサービス] ページで、デバイスまたはサービスのステータスが [同期済み]、[未同期 (Not Synced)]、または [競合が検出されました (Conflict Detected)] になっていることがあります。

- デバイスが [同期済み] の場合、Cisco Defense Orchestrator (CDO) の設定と、デバイスにローカルに保存されている設定は同じです。
- デバイスが [未同期 (Not Synced)] の場合、CDO に保存された設定が変更され、デバイスにローカルに保存されている設定とは異なっています。CDO からデバイスに変更を展開すると、CDO のバージョンに一致するようにデバイスの設定が変更されます。
- CDO の外部でデバイスに加えられた変更は、**アウトオブバンドの変更**と呼ばれます。デバイスの競合検出が有効になっている場合、アウトオブバンドの変更が行われると、デバイスのステータスが [競合が検出されました (Conflict Detected)] に変わります。アウトオブバンドの変更を受け入れると、CDO の設定がデバイスの設定と一致するように変更されます。

競合検出

競合検出が有効になっている場合、Cisco Defense Orchestrator (CDO) はデフォルトの間隔でデバイスをポーリングして、CDO の外部でデバイスの構成が変更されたかどうかを判断します。変更が行われたことを検出すると、CDO はデバイスの構成ステータスを [競合が検出されました] に変更します。CDO の外部でデバイスに加えられた変更は、「アウトオブバンド」の変更と呼ばれます。

このオプションを有効にすると、デバイスごとに競合または OOB 変更を検出する頻度を設定できます。詳細については、[デバイス変更のポーリングのスケジュール \(32 ページ\)](#) を参照してください。

競合検出の有効化

競合検出を有効にすると、Defense Orchestrator の外部でデバイスに変更が加えられた場合に警告が表示されます。

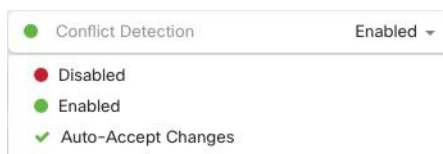
ステップ 1 ナビゲーションバーで、[デバイスとサービス (Devices & Services)] をクリックします。

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選択します。

ステップ 4 競合検出を有効にする 1 台または複数のデバイスを選択します。

ステップ 5 デバイステーブルの右側にある [競合検出] ボックスで、リストから [有効 (Enabled)] を選択します。



デバイスからのアウトオブバンド変更の自動的な受け入れ

変更の自動的な受け入れを有効にすることで、管理対象デバイスに直接加えられた変更を自動的に受け入れるように Cisco Defense Orchestrator (CDO) を設定できます。CDO を使用せずにデバイスに直接加えられた変更は、アウトオブバンド変更と呼ばれます。アウトオブバンドの変更により、CDO に保存されているデバイスの設定とデバイス自体に保存されている設定との間で競合が発生します。

変更の自動受け入れ機能は、競合検出のための強化機能です。デバイスで変更の自動受け入れを有効にしている場合、CDO は 10 分ごとに変更をチェックして、デバイスの設定に対してアウトオブバンドの変更が行われたかどうかを確認します。設定が変更されていた場合、CDO は、プロンプトを表示することなく、デバイスの設定のローカルバージョンを自動的に更新します。

CDO で行われたいずれかの設定変更がデバイスにまだ展開されていない場合、CDO は設定変更を自動的に受け入れません。画面上のプロンプトに従って、次のアクションを決定します。

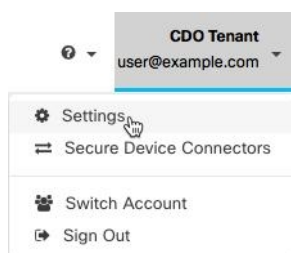
変更の自動受け入れを使用するには、最初に、テナントが [デバイスとサービス] ページの [競合検出] メニューで自動受け入れオプションを表示できるようにします。次に、個々のデバイスでの変更の自動受け入れを有効にします。

CDO でアウトオブバンドの変更を検出するものの、変更を手動で受け入れたり拒否したりするオプションを選択する場合は、代わりに [競合検出 \(28 ページ\)](#) を有効にします。

自動承認変更の設定

ステップ 1 管理者または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。

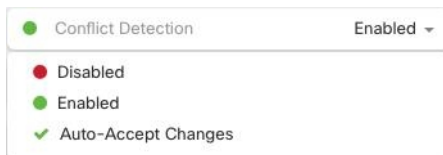
ステップ 2 ユーザーメニューから [設定] をクリックして、[設定] ページにアクセスします。



ステップ 3 [テナント設定] エリアで、[デバイスの変更を自動承認するオプションの有効化] のトグルをクリックします。これにより、[デバイスとサービス] ページの [競合検出] メニューに [変更の自動承認] メニューオプションが表示されるようになります。

ステップ 4 [デバイスとサービス] ページを開き、アウトオブバンドの変更を自動承認するデバイスを選択します。

ステップ 5 [競合検出] メニューで、ドロップダウンメニューから [変更の自動承認] を選択します。



テナント上のすべてのデバイスの自動承認変更の無効化

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

ステップ 2 ユーザーメニューから [設定] をクリックして、[設定] ページにアクセスします。

ステップ 3 [テナント設定] 領域で、トグルを左にスライドして灰色の X を表示し、[デバイスの変更を自動承認するオプションを有効にする (Enable the option to auto-accept device changes)] を無効にします。これにより、競合検出メニューの [変更の自動承認] オプションが無効になり、テナント上のすべてのデバイスでこの機能が無効になります。

(注) [自動承認 (Auto-Accept)] を無効にした場合、CDO で承認する前に、各デバイスの競合を確認する必要があります。これまで変更の自動承認が設定されていたデバイスも対象になります。

設定の競合の解決

このセクションでは、デバイスで発生する設定の競合の解決に関する情報を提供します。

「未同期」ステータスの解決

次の手順を使用して、「未同期」の設定ステータスのデバイスを解決します。

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

ステップ 2 [デバイス (Devices)] タブをクリックしてデバイスを見つけるか、[テンプレート (Templates)] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 未同期と報告されたデバイスを選択します。

ステップ 5 右側の [未同期 (Not synced)] パネルで、次のいずれかを選択します。

- [プレビューして展開... (Preview and Deploy..)] : 設定の変更を CDO からデバイスにプッシュする場合は、今行った変更を [すべてのデバイスの構成変更のプレビューと展開](#) か、待ってから一度に複数の変更を展開します。

- [変更の破棄 (Discard Changes)] : 設定の変更を CDO からデバイスにプッシュしたくない場合、または CDO で開始した設定の変更を「元に戻す」場合。このオプションは、CDO に保存されている設定を、デバイスに保存されている実行中の設定で上書きします。

[競合検出 (Conflict Detected)] ステータスの解決

CDO を使用すると、ライブデバイスごとに競合検出を有効化または無効化できます。[競合検出 \(28 ページ\)](#) が有効になっていて、CDO を使用せずにデバイスの設定に変更が加えられた場合、デバイスの設定ステータスには [競合検出 (Conflict Detected)] と表示されます。

[競合検出 (Conflict Detected)] ステータスを解決するには、次の手順に従います。

- ステップ 1** ナビゲーションバーで、[デバイスとサービス (Devices & Services)] をクリックします。
- ステップ 2** [デバイス] タブをクリックして、デバイスを見つけます。
- ステップ 3** 適切なデバイスタイプのタブをクリックします。
- ステップ 4** 競合を報告しているデバイスを選択し、右側の詳細ペインで [競合の確認 (Review Conflict)] をクリックします。
- ステップ 5** [デバイスの同期 (Device Sync)] ページで、強調表示されている相違点を確認して、2 つの設定を比較します。
 - 「最後に認識されたデバイス設定 (Last Known Device Configuration)」というラベルの付いたパネルは、CDO に保存されているデバイス設定です。
 - 「デバイスで検出 (Found on Device)」というラベルの付いたパネルは、ASA の実行構成に保存されている設定です。
- ステップ 6** 次のいずれかを選択して、競合を解決します。
 - [デバイスの変更を承認 (Accept Device changes)] : 設定と、CDO に保存されている保留中の変更がデバイスの実行構成で上書きされます。
 - (注) CDO はコマンドライン インターフェイス以外での Cisco IOS デバイスへの変更の展開をサポートしていないため、競合を解決する際の Cisco IOS デバイスの唯一の選択肢は [レビューなしで承認 (Accept Without Review)] です。
 - [デバイスの変更を拒否 (Reject Device Changes)] : デバイスに保存されている設定を CDO に保存されている設定で上書きします。
 - (注) 拒否または承認されたすべての設定変更は、変更ログに記録されます。

デバイス変更のポーリングのスケジュール

競合検出 (28 ページ) を有効にしている場合、または [設定] ページで [デバイスの変更を自動承認するオプションの有効化] オプションを有効にしている場合、CDO はデフォルトの間隔でデバイスをポーリングして、CDO の外部でデバイスの設定に変更が加えられたかどうかを判断します。CDO による変更のポーリング間隔は、デバイスごとにカスタマイズできます。ポーリング間隔の変更は、複数のデバイスに適用できます。

デバイスでこの間隔が選択されていない場合は、間隔は「テナントのデフォルト」に自動的に設定されます。



(注) [デバイスとサービス] ページでデバイスごとの間隔をカスタマイズすると、[全般設定 (General Settings)] ページの [デフォルトの競合検出間隔 (Default Conflict Detection Interval)] **デフォルトの競合検出間隔** で選択したポーリング間隔が上書きされます。

[デバイスとサービス (Conflict Detection)] ページで [競合検出] を有効にするか、[設定] ページで [デバイスの変更を自動承認するオプションの有効化] オプションを有効にしたら、次の手順に従い CDO によるデバイスのポーリング間隔をスケジュールします。

- ステップ 1 ナビゲーションバーで、[デバイスとサービス (Devices & Services)] をクリックします。
- ステップ 2 [デバイス (Devices)] タブをクリックして、デバイスを見つけます。
- ステップ 3 適切なデバイスタイプのタブをクリックします。
- ステップ 4 競合検出を有効にする 1 台または複数のデバイスを選択します。
- ステップ 5 [競合検出] と同じ領域で、[チェック間隔 (Check every)] のドロップダウンメニューをクリックし、目的のポーリング間隔を選択します。

