FAQ とサポート

この章は、次の項で構成されています。

Cisco Defense Orchestrator

Cisco Defense Orchestrator について

Cisco Defense Orchestrator（CDO）は、ネットワーク管理者がさまざまなセキュリティデバイス間で一貫したセキュリティポリシーを作成および維持できるクラウドベースのマルチデバイスマネージャです。

CDO を使用して、以下のデバイスを管理できます。

- Cisco Secure Firewall ASA
- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Cloud Native
- Cisco Umbrella
- Meraki
- Cisco IOS デバイス
- Amazon Web Services（AWS）インスタンス
- SSH 接続を使用して管理されるデバイス

CDO 管理者は、これらすべてのデバイスタイプを単一のインターフェイスで監視および保守できます。

デバイス

適応型セキュリティアプライアンス（ASA）とは何ですか。

Cisco ASA は、追加モジュールとの統合サービスに加え、高度なステートフル ファイアウォールおよび VPN コンセントレータ機能を 1 つのデバイスで提供します。ASA は、複数のセキュリティコンテキスト（仮想ファイアウォールに類似）、クラスタリング（複数のファイアウォールを 1 つのファイアウォールに統合）、トランスペアレント（レイヤ 2）ファイアウォールまたはルーテッド（レイヤ 3）ファイアウォール オペレーション、高度なインスペクションエンジン、IPsec VPN、SSL VPN、クライアントレス SSL VPN サポートなど、多数の高度な機能を含みます。ASA は、仮想マシンまたはサポートされているハードウェアにインストールできます。

ASA モデルとは何ですか。

ASA モデルは、CDO にオンボードされた ASA デバイスの実行コンフィギュレーション ファイルのコピーです。ASA モデルを使用すると、デバイス自体をオンボードせずに ASA デバイスの設定を分析することができます。

Firepower Threat Defense（FTD）とは何ですか。

シスコの次世代ファイアウォール ソフトウェア イメージです。Sourcefire 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を組み合わせることを目指しています。さまざまな Firepower ハードウェアデバイスまたは仮想マシンにインストールできます。これは、ASA FirePOWER モジュールとは異なります。詳細については、「ASA ソフトウェアおよびハードウェアサポート」を参照してください。

Firepower Device Manager（FDM）とは何ですか。

Firepower Device Manager は、FTD イメージとともに提供される Firepower Threat Defense 管理ソフトウェアです。FDM は、いっしょに提供される 1 つの FTD を管理するように設計されています。FDM は「ローカルデバイスマネージャ」と呼ばれる場合もあります。

Firepower とは何ですか。

Firepower は、次世代ファイアウォール ハードウェアおよびソフトウェアのグループを指す包括的な用語です。

デバイスが「同期済み（Synced）」であるのは、どのような場合ですか。

CDO の設定と、デバイスにローカルに保存されている設定が同じになっているときです。

デバイスが「非同期（Not Synced）」であるのは、どのような場合ですか。

CDO に保存されている設定が変更され、デバイスにローカルに保存されている設定と異なっているときです。

デバイスが「競合検出（Conflict Detected）」状態であるのは、どのような場合ですか。

デバイスの設定が CDO の外部（アウトオブバンド）で変更され、CDO に保存されている設定と異なっているときです。

アウトオブバンド変更とは何ですか。

CDO の外部でデバイスに変更が加えられることです。この変更は、CLI コマンドを使用するか、ASDM や FDM などのデバイス上のマネージャを使用して、デバイス上で直接行われたものです。アウトオブバンド変更が行われると、デバイスが「競合検出（Conflict Detected）」状態であると CDO が通知します。

変更をデバイスに展開するとは、どういう意味ですか。

デバイスを CDO にオンボードすると、CDO はその設定のコピーを保持します。CDO に変更を加えると、CDOは、デバイスの設定のコピーに変更を加えます。その変更をデバイスに「展開」すると、CDO は、加えた変更をデバイスの設定のコピーにコピーします。次のトピックを参照してください。

- すべてのデバイスの設定変更のプレビューと展開
- Defense Orchestrator から FTD への設定変更の展開

現在、どの ASA コマンドがサポートされていますか。

すべてのコマンドです。ASA CLI を使用するには、[デバイスアクション（Device Actions）] の [コマンドラインインターフェイス（Command Line Interface）] をクリックしてください。

デバイスの管理に関して規模の制約はありますか。

CDO のクラウドアーキテクチャにより、数千台のデバイスにまで規模を拡張できます。

CDO は、Cisco サービス統合型ルータおよびアグリゲーション サービス ルータを管理できますか。

CDO では ISR および ASR 用のモデルデバイスを作成して、その設定をインポートできます。次に、インポートされた設定に基づいてテンプレートを作成し、その設定を標準の設定としてエクスポートできます。この標準の設定を、ISR および ASR の新規または既存のデバイスに展開して、セキュリティの一貫性を確保できます。

CDO は SMA を管理できますか。

いいえ、現時点では、CDO は SMA を管理しません。

Secure Firewall Cloud Native（SFCN）とは何ですか。

セキュリティ

CDO は安全ですか?

CDO は、次の機能を通じて顧客データのエンドツーエンドのセキュリティを実現します。

- 新規 CDO テナントへの初回ログイン
- API およびデータベース操作の認証呼び出し
- 転送中および保存中のデータ分離
- 役割分担

CDO では、ユーザーがクラウドポータルに接続するために多要素認証が必要です。多要素認証は、顧客の ID を保護するために必要な重要な機能です。

すべてのデータは、転送中も保存中も暗号化されます。顧客構内のデバイスと CDO からの通信は SSL で暗号化され、顧客テナントのデータボリュームはすべて暗号化されます。

CDO のマルチテナント アーキテクチャは、テナントデータを分離し、データベースとアプリケーション サーバー間のトラフィックを暗号化します。CDO へのアクセス権が認証されると、ユーザーにトークンが送られます。このトークンは、キー管理サービスからキーを取得するために使用され、このキーはデータベースへのトラフィックを暗号化するために使用されます。

CDO はお客様に価値を素早く提供すると同時に、お客様のクレデンシャルの安全性を確保します。これは、クラウドまたはお客様自身のネットワーク（ロードマップ）に「Secure Data Connector」を展開することによって実現されます。Secure Data Connector は、インバウンドおよびアウトバウンドトラフィックを制御して、クレデンシャルデータが顧客構内から離れることがないようにします。

CDO に初めてログインしたときに、「OTP を検証できませんでした」というエラーが表示されました。

デスクトップまたはモバイルデバイスの時計がワールドタイムサーバーと同期していることを確認します。時計が 1 分以上ずれていると、誤った OTP が生成される可能性があります。

デバイスは Cisco Defense Orchestrator クラウドプラットフォームに直接接続されるのですか？

はい。保護された接続は、デバイスと CDO プラットフォーム間のプロキシとして使用される CDO SDC を使用して実行されます。セキュリティを最優先に設計された CDO アーキテクチャにより、デバイスとの間を行き来するデータを完全に分離できます。

パブリック IP アドレスを持たないデバイスを接続するにはどうすればよいですか？

ネットワーク内に展開でき、外部ポートを開く必要がないCDO Secure Device Connector（SDC）を利用できます。SDC が展開されると、内部（インターネットでルーティングできない）IP アドレスを持つデバイスをオンボードできます。

SDC には追加のコストやライセンスが必要ですか？

番号

CDO で現在サポートされている仮想プライベートネットワークのタイプは？

ASA のお客様の場合、CDO は IPsec サイト間 VPN トンネル管理のみをサポートします。新着情報ページの更新情報を定期的にご確認ください。

トンネルステータスはどのように確認できますか？状態オプション

CDO はトンネル接続チェックを 1 時間ごとに自動的に実行しますが、トンネルを選択して接続チェックを要求することで、アドホックの VPN トンネル接続チェックを実行できます。結果の処理には数秒かかる場合があります。

デバイス名とそのピアの片方の IP アドレスに基づいてトンネルを検索できますか？

はい。名前とピア IP アドレスの両方で利用可能なフィルタ機能と検索機能を使用して、特定の VPN トンネルの詳細を検索してピボットします。

トラブルシューティング

CDOから管理対象デバイスへのデバイス構成の完全な展開を実行しているときに、「変更をデバイスに展開できません」という警告が表示されます。解決するにはどうすればよいですか？

完全な構成（CDO でサポートされているコマンドを超えて実行された変更）をデバイスに展開するときにエラーが発生した場合は、[変更の確認（Check for changes）] をクリックして、デバイスから使用可能な最新の構成をプルします。これによって問題が解決されたら、CDO で引き続き変更を加えて展開することができます。問題が解決しない場合は、[サポートに連絡（Contact Support ）] ページから Cisco TAC に連絡してください。

帯域外の問題（CDO の外部で、デバイスに対して直接実行された変更）を解決しているときに、CDOに存在する構成をデバイスの構成と比較すると、CDOは、私が追加または変更していない追加のメタデータを提示します。どうしてですか。

CDO がその機能を拡張すると、デバイスの構成から追加情報が収集され、ポリシーとデバイス管理の分析を改善するために必要なすべてのデータを充実させて維持します。これらは管理対象デバイスで発生した変更ではなく、既存の情報です。[競合が検出されました（Conflict Detected）] の状態の解決は、デバイスからの変更を確認し、発生した変更を確認することで簡単に解決できます。

CDO が私の証明書を拒否するのはなぜですか？

「新しい証明書の解決」を参照してください。

ロータッチプロビジョニングで使用される用語と定義

- **要求（Claimed）**：CDO でシリアル番号のオンボーディングのコンテキストで使用されます。シリアル番号が CDO テナントにオンボードされている場合、そのデバイスは「要求」されています。
- **パーク（Parked）**：CDO でシリアル番号のオンボーディングのコンテキストで使用されます。デバイスが Cisco Cloud に接続されていて、CDO テナントがそのデバイスのシリアル番号を要求していない場合、そのデバイスは「パーク」されています。
- **初期プロビジョニング（Initial provisioning）**：初期 FTD セットアップのコンテキストで使用されます。このフェーズでは、デバイスの EULA を受け入れ、新しいパスワードを作成し、管理 IP アドレス、FQDN、および DNS サーバーを設定し、FDM を使用してデバイスをローカルで管理することを選択します。
- **ロータッチプロビジョニング（Low-touch provisioning）**：FTD を工場からお客様のサイト（通常は分散拠点）に出荷するプロセスであり、サイトの従業員が FTD をネットワークに接続し、デバイスを Cisco Cloud に接続します。その時点で、シリアル番号がすでに「要求」されている場合、デバイスは CDO テナントにオンボードされます。また、FTD は、CDO テナントが要求するまで Cisco Cloud に「パーク」されます。
- **シリアル番号のオンボーディング（Serial number onboarding）**：すでに設定（インストールおよびセットアップ）されているシリアル番号を使用して FTD をオンボーディングするプロセスです。

ポリシーの最適化

2 つ以上のアクセスリスト（同じアクセスグループ内）で相互にシャドウイングしているケースを特定するにはどうすればよいですか。

Cisco Defense Orchestrator のネットワークポリシー管理（NPM）を使用することで、ルールセット内で上位のルールが別のルールをシャドウイングしている場合に、ユーザーを特定して警告できます。ユーザーは、すべてのネットワークポリシー間を移動するか、フィルタ処理を実行してすべてのシャドウ問題を特定できます。

（注） CDO は、完全にシャドウされたルールのみをサポートします。

接続性

Secure Device Connector により IP アドレスが変更されましたが、これは CDO 内に反映されませんでした。変更を反映するにはどうすればよいですか。

CDO 内で新しい Secure Device Connector（SDC）を取得して更新するには、次のコマンドを使用してコンテナを再起動する必要があります。

```
 Stop Docker deamon>#service docker stop
Change IP address
Start Docker deamon >#service docker start
Restart container on the SDC virtual appliance >bash-4.2$ ./cdo/toolkit/toolkit.sh
restartSDC <tenant-name>
```

CDO がデバイス（FTD または ASA）を管理するために使用する IP アドレスが変更された場合はどうなりますか。

デバイスの IP アドレスが何らかの理由で変更された場合、それが静的 IP アドレスの変更であるか、DHCP による IP アドレスの変更であるかにかかわらず、CDO がデバイスへの接続に使用する IP アドレスを変更して（CDO のデバイスの IP アドレスを変更するを参照）、デバイスを再接続できます（CDO へのデバイス一括再接続を参照）。デバイスを再接続するときに、デバイスの新しい IP アドレスの入力と、認証の資格情報の再入力を求められます。

ASA を CDO に接続するには、どのようなネットワークが必要ですか。

- ASDM イメージが存在し、ASA に対して有効になっている。
- 52.25.109.29、52.34.234.2、52.36.70.147 へのパブリック インターフェイス アクセス。
- ASA の HTTPS ポートは 443、または 1024 以上の値に設定する必要があります。たとえば、ポート 636 に設定することはできません。
- 管理下の ASA も AnyConnect VPN クライアント接続を受け入れるように設定されている場合は、ASA HTTPS ポートを 1024 以上の値に変更する必要があります。

Cisco Defense Orchestrator サポートへの連絡

この章は、次のセクションで構成されています。

ワークフローのエクスポート

サポートチケットを開く前に、問題が発生しているデバイスのワークフローをエクスポートすることを強くお勧めします。この追加情報は、サポートチームがトラブルシューティング作業を迅速に特定して修正するのに役立ちます。

ワークフローをエクスポートするには、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、[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、トラブルシューティングが必要なデバイスを選択します。

フィルタまたは**検索バー**を使用して、トラブルシューティングが必要なデバイスを見つけます。デバイスを選択して強調表示します。

ステップ 4 [デバイスアクション（Device Actions）] ペインで、[ワークフロー（Workflows）] を選択します。

ステップ 5 ページ右上のイベントテーブルの上にある [エクスポート（Export）] ボタンをクリックします。ファイルは、**.json** ファイルとしてローカルに自動的に保存されます。このファイルを、TAC で開いた電子メールまたはチケットに添付します。

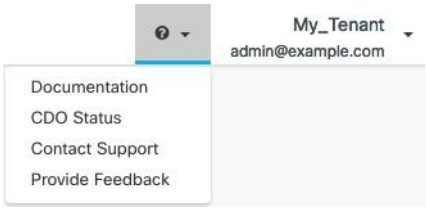
TAC でサポートチケットを開く

CDO インターフェイスを使用して、Cisco Technical Assistance Center（TAC）でサポートチケットを開くことができます。

手順

ステップ 1 CDO にログインします。

ステップ 2 テナント名とアカウント名の横にある [ヘルプ（help）] ボタンをクリックし、[サポートに連絡（Contact Support）] を選択します。



ステップ 3 [サポートケースマネージャ（Support Case Manager）] をクリックします。

ステップ 4 青色の [新しいケースを開く（Open New Case）] ボタンをクリックします。

ステップ 5 [ケースをオープン（Open Case）] をクリックします。

ステップ 6 [リクエストタイプ（Request Type）] を選択します。

ステップ 7 [サービス契約による製品の検索（Find Product by Service Agreement）] 行を展開します。

ステップ 8 すべてのフィールドに入力します。多くのフィールドは明らかで説明するまでもありませんが、追加の情報を以下に記載します。

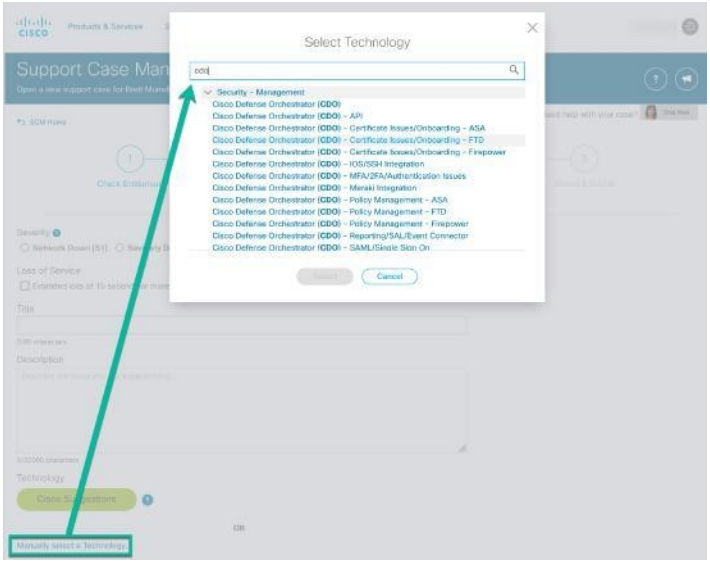
- [製品名（PID）（Product Name (PID)）]：この番号がわからない場合は、『Cisco Defense Orchestrator データシート』を参照してください。
- [製品の説明（Product Description）]：PID の説明です。
- [サイト名（Site Name）]：サイト名を入力します。シスコパートナーがお客様に代わってケースを開いている場合は、お客様の名前を入力します。
- [サービス契約（Service Contract）]：サービス契約番号を入力します。
  - **重要**：ケースを Cisco.com アカウントに関連付けるには、契約番号を Cisco.com プロファイルに関連付ける必要があります。契約番号を Cisco.com プロファイルに関連付けるには、次の手順を実行します。
    1. Cisco Profile Manager を開きます。
    2. [アクセス管理（Access Management）] タブをクリックします。
    3. [アクセス権の追加（Add Access）] をクリックします。
    4. [Cisco.comのTACおよびRMAケース作成、ソフトウェアダウンロード、サポートツール、および権限付きコンテンツ（TAC and RMA case creation, Software Download, support tools, and entitled content on Cisco.com）] を選択し、[実行（Go）] をクリックします。
    5. 指定されたスペースにサービス契約番号を入力し、[送信（Submit）] をクリックします。サービス契約の関連付けが完了したことが電子メールで通知されます。サービス契約の関連付けは、完了までに最長 6 時間かかる場合があります。

重要　重要：以下のリンクのいずれにもアクセスできない場合は、シスコ認定のパートナーや再販業者、シスコのアカウント担当者、または社内でシスコサービスの契約情報を管理する担当者にお問い合わせください。

ステップ 9　[次へ（Next）] をクリックします。

ステップ 10　[問題の説明（Describe Problem）] 画面を下にスクロールして [テクノロジーを手動で選択（Manually select a Technology）] をクリックし、検索フィールドに CDO と入力します。

ステップ 11　リクエストに最も一致するカテゴリを選択し、[選択（Select）] をクリックします。



ステップ 12 サービスリクエストの残りの部分をすべて入力し、[送信（Submit）] をクリックします。

CDO サービスステータスページ

CDO ではお客様向けのサービスステータスページが維持管理されています。このページには、CDO サービスの稼働状況やサービス中断の発生状況が表示されます。稼働時間情報を日次、週次、または月次のグラフで表示できます。

CDO の任意のページのヘルプメニューで **[CDOステータス（CDO Status）]** をクリックすると、CDO ステータスページにアクセスできます。

ステータスページで、[更新をサブスクライブ（Subscribe to Updates）] をクリックすると、CDO サービスがダウンした場合に通知を受け取ることができます。