



Cisco Defense Orchestrator を使用した AWS の管理

初版：2020年12月22日

最終更新：2022年4月20日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（ www.cisco.com/jp/go/safety_warning/ ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021–2022 Cisco Systems, Inc. All rights reserved.



Cisco Defense Orchestrator を使用した AWS の管理

- [Cisco Defense Orchestrator を使用した AWS の管理 \(iii ページ\)](#)

Cisco Defense Orchestrator を使用した AWS の管理

Cisco Defense Orchestrator を使用して AWS VPC の管理

CDO は、Amazon Web Services (AWS) 仮想プライベートクラウド (VPC) 向けの簡素化された管理インターフェイスを提供します。他のデバイスを管理するのと同じインターフェイスで、AWS VPC とそのコンポーネントを管理できます。

CDO を使用して、以下のタスクを実行できます。

- [AWS VPC の導入準備 \(95 ページ\)](#)
- [VPC の詳細を表示する](#)
- [セキュリティグループを操作する](#)
- [AWS オブジェクトを他の管理対象デバイスと共有する](#)
- [AWS のサイト間 VPN 接続を監視する](#)
- [AWS デバイスへの変更をモニタリングする](#)
- [AWS のサイト間 VPN トンネルを表示する](#)

以下は、CDO が将来サポートする予定の一般的な AWS の機能です。

- [セキュリティグループに対するロードバランサー \(エラスティック、ネットワーク、アプリケーションロードバランサー\) の関係を表示する](#)
- [セキュリティグループに対する自動スケーリンググループの関係を表示する](#)

セキュリティグループの以下の側面を CDO で管理することはできません。

- セキュリティグループを作成する。
- セキュリティグループをインスタンスにリンクする。
- セキュリティグループをロードバランサーに割り当てる。
- VPC ピアリング。

AWS VPC の導入準備

CDO の導入準備ウィザードを使用して、AWS VPC の導入準備を開始します。詳細については、[AWS VPC の導入準備](#)を参照してください。

AWS VPC にタグが含まれている場合、これらのタグは、デバイスの導入準備時に CDO にインポートされる点に注意してください。CDO はタグをラベルとして表示します。セキュリティクラウド オブジェクトやルールとは異なり、ラベルは AWS VPC に自動的に同期されません。詳細については、「[ラベルとフィルタ処理](#)」を参照してください。

CDO コンソールを介して、AWS VPC のログイン情報と権限を処理します。正しいログイン情報または権限がないと、CDO は AWS VPC と通信できません。詳細については、[AWS VPC 接続ログイン情報の更新 \(99 ページ\)](#) と「[IAM ユーザーのアクセス許可の変更](#)」を参照してください。

AWS VPC の詳細を表示する

AWS VPC が導入準備されると、AWS VPC の ID、リージョン、セキュリティグループ、セキュリティグループに割り当てられたルールとオブジェクトを表示できます。

セキュリティグループを操作する

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 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。AWS VPC を CDO に対して導入準備すると、セキュリティグループはセキュリティグループオブジェクトとして CDO に保存されます。

CDO を使用すると、以下のタスクを実行できます。

- [セキュリティグループルールの作成](#)
- [セキュリティグループのルールの設定変更の確認](#)、[セキュリティグループルールの編集](#)、[セキュリティグループルールの削除](#)

現時点では、VPC に新しいセキュリティグループを作成することはできません。

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を管理する](#)
- [AWS と他の管理対象デバイス間でオブジェクトを共有する](#)

AWS と他の管理対象デバイス間でオブジェクトを共有する

CDO は、ルールにおけるオブジェクトの使用をサポートしています。オブジェクトは値のコンテナです。たとえば、リソースの IP アドレスを含むネットワークオブジェクトを作成し、意味のある名前を付けることができます。その後、リソースのリテラル IP アドレスを使用するのではなく、ルールの送信元または接続先の一部としてアクセスルール内でそのオブジェクトを使用できます。また、そのオブジェクトを異なるルールで再利用することもできます。オブジェクトの値をいったん変更すると、そのオブジェクトを使用するすべてのルールが新しい値を使用し始めます。

AWS VPC の導入準備後、CDO は AWS の概念を、既存のセキュリティグループルールで見つかったセキュリティグループオブジェクト、ネットワークオブジェクト、およびサービスオブジェクトに変換します。

ネットワークオブジェクトとサービスオブジェクト（ポートオブジェクトと呼ばれることもある）は、AWS VPC と、CDO を使用して管理する他のデバイスとの間で共有できます。セキュリティグループオブジェクトは AWS に固有です。

詳細については、「[AWS と他の管理対象デバイス間でオブジェクトを共有する](#)」を参照してください。

AWS のサイト間 VPN 接続を監視する

AWS のサイト間 VPN は、AWS 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。詳細については、「[AWS のサイト間 VPN トンネルを表示する](#)」を参照してください。

AWS VPC および AWS セキュリティグループへの変更をモニタリングする

ログの変更

変更ログは、CDO で行われた構成変更を継続的にキャプチャします。この単一のビューには、サポートされているすべてのデバイスとサービスにわたる変更が含まれます。変更ログの機能の一部を次に示します。

- デバイス構成に加えられた変更の対照比較。
- すべての変更ログエントリの平易な英語のラベル。
- デバイスの導入準備と削除の記録。
- CDO の外部で発生するポリシー変更の競合の検出。
- インシデントの調査またはトラブルシューティング中に、誰が、何を、いつに回答可能。

変更リクエスト管理

変更リクエスト管理により、サードパーティのチケットシステムで開かれた変更リクエストとそのビジネス上の正当性を、変更ログのイベントに関連付けることができます。変更リクエスト管理を使用して、CDO で変更リクエストを作成し、作成した変更リクエストを一意の名前で識別し、変更の説明を入力して、変更リクエストを変更ログイベントに関連付けます。後から変更リクエスト名を変更ログで検索できます。

一般的な管理者タスクのサポート

CDO は、以下の AWS セキュリティグループの一般的な管理タスクをサポートしています。

- [デバイス設定の一括展開 \(120 ページ\)](#)
- [すべてのデバイス設定の読み取り \(117 ページ\)](#)
- [デバイスのアウトオブバンド変更](#)
- [競合検出](#)
- [設定の競合の解決](#)



第 1 章

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 \(2 ページ\)](#)
- [Secure Device Connector \(SDC\) \(3 ページ\)](#)
- [CDO へのサインイン \(30 ページ\)](#)
- [Cisco Secure Sign-On ID プロバイダーへの移行 \(32 ページ\)](#)
- [Cisco Secure Sign-On ダッシュボードからの CDO の起動 \(33 ページ\)](#)
- [テナントのネットワーク管理者の管理 \(34 ページ\)](#)
- [CDO でサポートされるソフトウェアとハードウェア \(34 ページ\)](#)
- [ブラウザ サポート \(35 ページ\)](#)
- [テナント管理 \(35 ページ\)](#)
- [ユーザ管理 \(53 ページ\)](#)
- [ユーザー管理の Active Directory グループ \(53 ページ\)](#)
- [新規 CDO ユーザーの作成 \(58 ページ\)](#)
- [ユーザの役割 \(65 ページ\)](#)
- [ユーザーロールのユーザーレコードの作成 \(70 ページ\)](#)
- [ユーザーロールのユーザーレコードの編集 \(71 ページ\)](#)
- [ユーザーロールのユーザーレコードの削除 \(72 ページ\)](#)
- [デバイスとサービスの管理 \(73 ページ\)](#)
- [\[インベントリ\] ページ情報の表示 \(80 ページ\)](#)
- [ラベルとフィルタ処理 \(81 ページ\)](#)
- [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 \(83 ページ\)](#)
- [検索 \(84 ページ\)](#)
- [一括コマンドラインインターフェイス \(84 ページ\)](#)
- [デバイスの管理用 CLI マクロ \(89 ページ\)](#)

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。

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。

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 に導入準備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 \(31 ページ\)](#) 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 にデバイスを導入準備する場合、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 に導入準備できます。

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。導入準備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 \(5 ページ\)](#)」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 \(6 ページ\)](#) および自身のVM上での[Secure Device Connector の展開 \(11 ページ\)](#) 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 \(149 ページ\)](#)
- [Secure Device Connector の更新 \(19 ページ\)](#)
- [Secure Device Connector の削除 \(16 ページ\)](#)

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 への導入準備を実行できます。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 の導入準備が可能になります。さまざまな導入準備方式の詳細については、「[FTD の導入準備](#)」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	導入準備方式	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 (Serial Number)	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 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、SSH および IOS デバイスはすべて、SDC を使用して CDO に導入準備できます。

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 \(20 ページ\)](#) 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 \(11 ページ\)](#) 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。

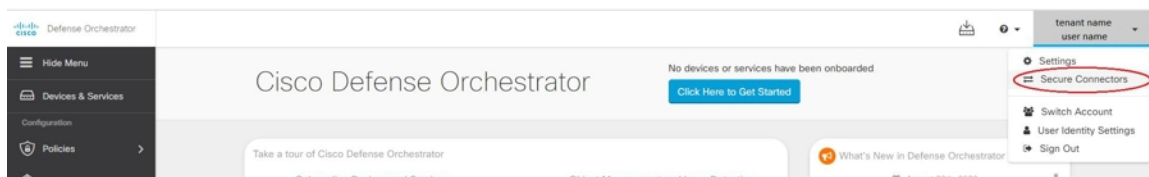
- CDO は、厳密な証明書チェックを必要とし、SDC とインターネットの間の Web/コンテンツプロキシ検査をサポートしていません。プロキシサーバーを使用している場合は、SDC と CDO の間のトラフィックの検査を無効にします。
- SDC には、TCP ポート 443 またはデバイス管理用に設定したポートでのインターネットへの完全なアウトバウンドアクセスが必要です。デバイスが CDO によって管理されている場合、このポートからのインバウンドトラフィックも許可する必要があります。
- 適切なネットワークアクセスを確保するため、「[Cisco Defense Orchestrator の管理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。
- 展開後 CDO で SDC ステータスがアクティブにならない
 - 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。
- 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。

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

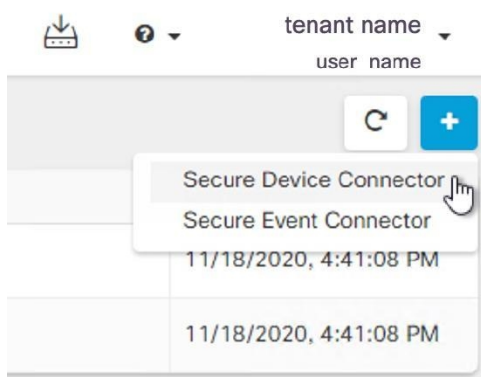
- インストールプロセス中に作成する root ユーザーと cdo ユーザーのパスワード。
 - 組織で使用する DNS サーバーの IP アドレス。
 - SDC アドレスが存在するネットワークのゲートウェイ IP アドレス。
 - タイムサーバーの FQDN または IP アドレス。
- SDC 仮想マシンは、セキュリティパッチを定期的にインストールするように設定されており、これを行うには、ポート 80 のアウトバウンドを開く必要があります。

ステップ 1 SDC を作成する CDO テナントにログインします。

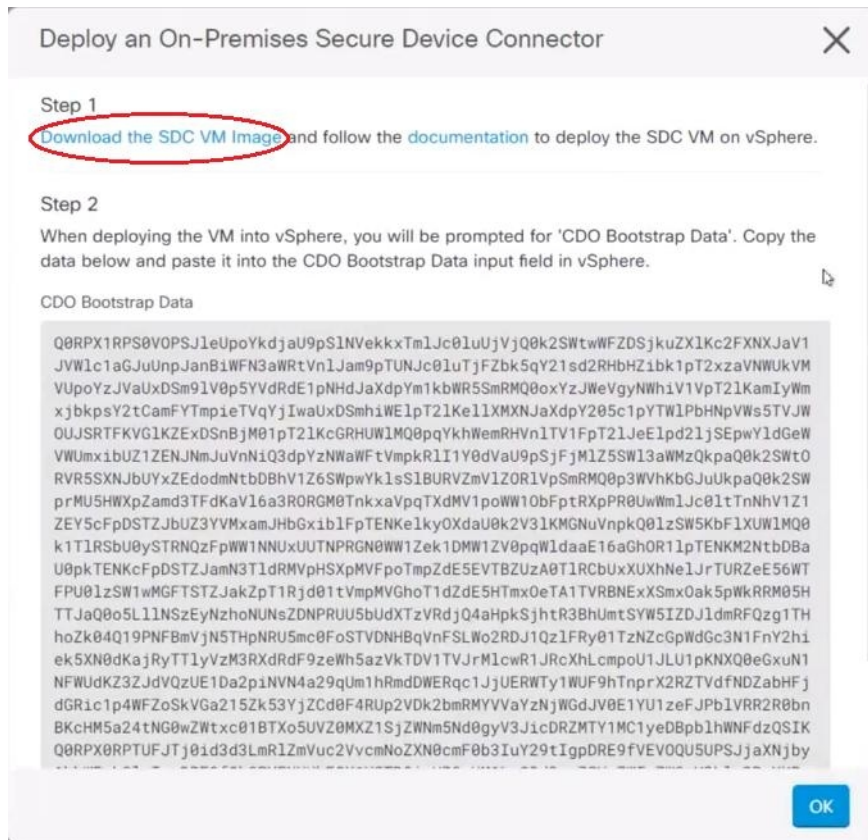
ステップ 2 [ユーザー (User)]メニューをクリックし、[セキュアコネクタ (Secure Connectors)]を選択します。



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。
- IP アドレス/CIDR
 - ゲートウェイ
 - DNS サーバー
 - NTP サーバーまたは FQDN
 - 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] を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。
- CDO にログインします。
  - 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。
  - [アクション] 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。
  - 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。

## Deploy an On-Premises Secure Device Connector



## Step 2

When deploying the VM into vSphere, you will be prompted for 'CDO Bootstrap Data'. Copy the data below and paste it into the CDO Bootstrap Data input field in vSphere.

## CDO Bootstrap Data

```
Q08RPX1RPS0V0PSJ1eUpoYkdjaU9pS1NVekkxTm1Jc01uUjVjQ0k2SWtwWFZDSjkuZX1Kc2FXNXJaV1
JWV1c1aGJuUnpJanB1WFN3aWRtVn1Jam9pTUNJc01uTjFZbk5qY21sd2RHbHZ1bk1pT2xzaVNWUkVM
VUpoYzJVaUxDSm91V0p5YVdRdE1pNHdJaXdpYm1kbWR5SsmRMQ00oxYzJWeVgyNWh1V1VpT21KamIyWm
xjbkpsY2tCamFYTmPieTVqYjIwaUxDSmh1WE1pT21Ke1lXMXNJaXdpY205c1pYTW1PbHNpVWs5TVJW
OUJSRTFKVGLKZExDSnBjM01pT21KcGRHUW1MQ0ppqYkhWemRHVn1TV1FpT21Je1pd21jSEpwYldGeW
VWUmxiBUZ1ZENJNmJuVnNiQ3dpYzNWaWftVmpkR1I1Y0dVaU9pSjFjM1Z5SW13aWMzQkpaQ0k2SWt0
RVR5SXNJbUyXZEdodmNtbDBhV1Z6SWpwYk1sS1BURVZmV1Z0R1VpSmRMQ0p3WVhKbGJuUkpaQ0k2SW
prMU5HWXpZamd3TFdKaV16a3R0RGM0TnkxaVpQTXdMV1poWW10bFptRxpPR0UwWm1Jc01tTnNhV1Z1
ZEY5cFpDSTZJbUz3YVMxamJHbGxiB1FpTENKe1ky0XdaU0k2V31KMGNUVnPkQ0lzSW5KbF1XUW1MQ0
k1T1RSBU0vSTRN0zFoWw1NNUxUUTNPRGN0Ww1Zek1DMW1ZV00dW1daaE16aGh0R11oTENKM2NtbDBa
Q08RPX0RPTUFJTj01d3d3LmR1ZmVuc2VvcMNoZXN0cmF0b3IuY29tIgpDRE9fVEV0QU5UPSjjaXNjby
1hbWFSbG1vIgpDRE9fQk9PVFNuUkFQX1VSTDB1aHR0cHM6Ly93d3cuZGVmZW5zZW9yY2h1c3RyYXRv
ci5jb20vc2RjL2Jvb3RzdHJhcC9jaXNjby1hbWFSbG1vL2Npc2NvLWFTYWxsaW8tU0RDIGo=
```

Copy bootstrap data

- 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] と入力します。
- 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 のトラブルシューティング \(149 ページ\)](#)
- [デバイスと SDC の接続に関するトラブルシューティング \(151 ページ\)](#)

## 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 に導入準備できます。

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 \(20 ページ\)](#) 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 \(6 ページ\)](#) 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 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。
- CentOS 7 ゲスト オペレーティング システム。
- 展開後 CDO で SDC ステータスがアクティブにならない
  - 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 10GB 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。
- 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。
- この手順を実行するユーザーは、Linux 環境の操作に親しんでおり、vi ビジュアルエディタを使用してファイルを編集している必要があります。

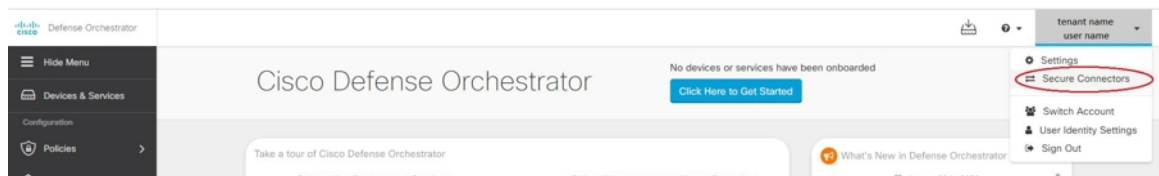
- オンプレミスの SDC を CentOS 仮想マシンにインストールする場合は、Yum セキュリティパッチを定期的にインストールすることをお勧めします。Yum の更新を取得するための設定に応じて、ポート 443 だけでなくポート 80 でもアウトバウンドアクセスを開く必要がある場合があります。また、更新をスケジュールするために yum-cron または crontab も設定する必要があります。セキュリティ運用チームと連携して、Yum の更新を取得するためにセキュリティポリシーを変更する必要があるかどうかを判断します。



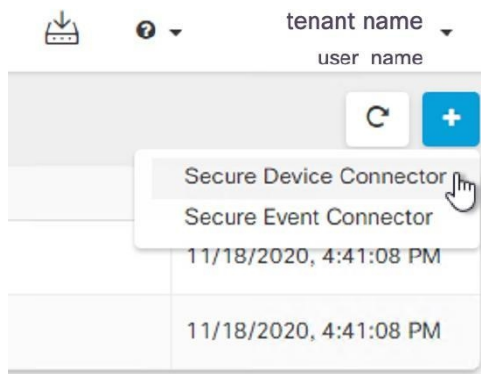
(注) 始める前に：手順内のコマンドは、コピーして端末ウィンドウに貼り付けるのではなく入力するようにしてください。一部のコマンドに含まれる「n ダッシュ」は、カットアンドペーストのプロセスで「m ダッシュ」として適用される場合があります、コマンドが失敗する原因となります。

**ステップ 1** SDC を作成する CDO テナントにログインします。

**ステップ 2** [ユーザー (User) ]メニューをクリックし、[セキュアコネクタ (Secure Connectors) ]を選択します。



**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@sdsc-vm ~]# grep docker /etc/group
docker:x:993:
[root@sdsc-vm ~]#
[root@sdsc-vm ~]# usermod -aG docker sdc
[root@sdsc-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@sdsc-vm ~]# cat /etc/docker/daemon.json
{
 "live-restore": true,
 "group": "docker"
}
[root@sdsc-vm ~]# systemctl restart docker
[root@sdsc-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@sdsc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdsc-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、暗号解読化して extractedbootstrapdata というファイルにエクスポートします。

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

cat コマンドを実行して暗号解読化したデータを表示します。コマンドおよび暗号解読化したデータは次のようになります。

```
[sdc@sdsc-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、暗号解読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@sdsc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > sdcenv && source sdcenv
[sdc@sdsc-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:d98f17101db10e66db5b5d6afdalc95c29ea0004d9e4315508fd30579b275458: 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が。

### 次のタスク

- 「[デバイスとサービスの導入準備](#)」に移動して、CDO で管理するデバイスを導入準備します。

## 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。

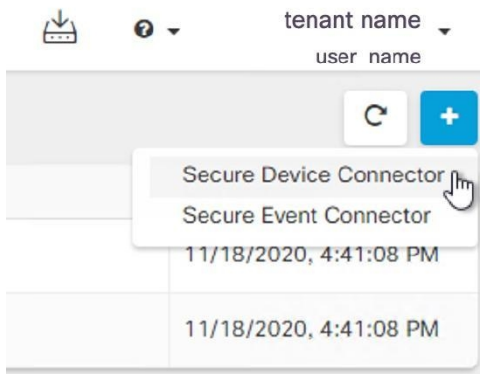
**ステップ 1** 削除する SDC に接続されているデバイスをすべて削除します。この操作は、次の 2 つの方法で実行できます。

- 一部のデバイスを別の SDC に移動するか、SDC から完全に切り離します。詳細については、次のトピックを参照してください。
  - [AWS VPC 接続ログイン情報の更新 \(99 ページ\)](#)



- 削除する SDC に接続されているすべてのデバイスを CDO から削除します。
  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 \(20 ページ\)](#)
  2. [デバイスとサービス] 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] 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** 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。



**ステップ 3** [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が。

**ステップ 4** [アクション] ペインで、[削除] 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。Secure Device Connector (SDC) の削除は元に戻せません。SDC を削除すると、デバイスを導入準備または再導入準備する前に、新しい SDC を作成して導入準備する必要があります。

現在導入準備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] 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 5** 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 6** [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。

- 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] 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 [Secure Device Connector] ボタンをクリックし、デバイスの移動先 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 の導入準備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。

- 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、[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] 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 の導入準備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

- ステップ1** [ユーザー (User) ] メニューから、[セキュアコネクタ (Secure Connectors) ] を選択します。
- 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、[デバイスとサービス] 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。

- 
- 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

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、[インベントリ] 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 フィルタ処理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] 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] メニューを展開します。 [フィルタ \(82 ページ\)](#)
  - ステップ 6 フィルタの [Secure Device Connector] セクションで、必要な SDC の名前をオンにします。インベントリテーブルには、フィルタでオンにした 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オンにします。
  - 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] 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 copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the right to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the 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 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 OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, 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 IN THE SOFTWARE.

---

---

\* bluebird \*

The MIT License (MIT)

Copyright (c) 2013-2015 Petka Antonov

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the right to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the 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 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 OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, 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 IN THE SOFTWARE.

---

---

\* cheerio \*

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

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the 'Software'), to deal in the Software without restriction, including without limitation the right to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the 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 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 OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, 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 IN THE 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 copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the right to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the 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 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 OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, 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 IN THE 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 copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the right to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the 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 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 OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, 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 IN THE SOFTWARE.**

---

---

**\* json-buffer \***

**Copyright (c) 2013 Dominic Tarr**

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the 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 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 OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, 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 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 of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the 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 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 OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, 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 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 any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN 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 many individuals. For exact contribution history, see the revision history available 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 obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the 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 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 OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, 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 IN THE SOFTWARE.

====

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

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

====

Files located in the `node_modules` and `vendor` directories are externally maintained libraries used by this software which have their own licenses; we recommend you read them, as their terms may differ from the terms 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 and limitations under the License.

---

---

**\* mkdirp \***

Copyright 2010 James Halliday ([mail@substack.net](mailto: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 copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the right to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the 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 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 OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, 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 IN THE 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 without modification, are permitted provided that the following conditions are met:

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

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

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

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL DIGITAL BAZAAR BE LIABLE FOR ANY DIRECT, 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 AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, 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 any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN 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 obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the 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 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 OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, 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 IN THE SOFTWARE.

---

---

**\* when \***

Open Source Initiative OSI - The MIT License

<http://www.opensource.org/licenses/mit-license.php>

Copyright (c) 2011 Brian Cavalier

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the 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 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 OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, 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 IN THE SOFTWARE.**

## 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せん。

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 \(31 ページ\)](#)」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 \(32 ページ\)](#)」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 Duo Security から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 \(32 ページ\)](#) 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 \(59 ページ\)](#) 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](https://defenseorchestrator.com) にアクセスするか、[CDO (EU)] をクリックして [defenseorchestrator.eu](https://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 \(31 ページ\)](#) 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 \(59 ページ\)](#)

## 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 (59 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

**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ーを設定している場合は、オーセンティケーター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 \(48 ページ\)](#) 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 \(53 ページ\)](#) 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：

- [クラウドデバイスのサポートの詳細 \(35 ページ\)](#)
- [ブラウザ サポート \(35 ページ\)](#)

## クラウドデバイスのサポートの詳細

次の表で、クラウドベースのデバイスのソフトウェアとデバイスタイプのサポートについて説明します。次の表の関連リンクで、デバイスタイプの導入準備と機能や特長に関する詳細な情報を確認してください。

| デバイスタイプ                 | 注記                                                                                                                                                                                 |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Amazon Web Services VPC | <p>AWS VPC は、AWS コンソールを介して更新を受信します。詳細については、<a href="#">Cisco Defense Orchestrator を使用した AWS の管理</a> (iii ページ) を参照してください。</p> <p>AWS VPC は、CDO に導入準備する前に AWS コンソールで起動する必要があります。</p> |

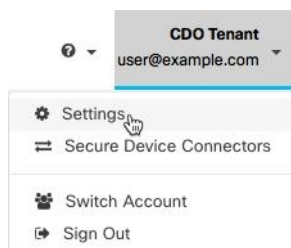
## ブラウザ サポート

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

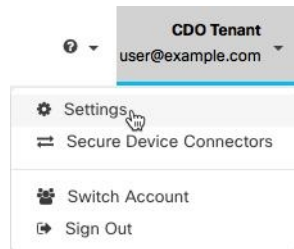
Cisco Defense Orchestrator (Defense Orchestrator) を使用すると、[設定] ページでテナントおよび個々のユーザーアカウントの特定の側面をカスタマイズできます。ユーザーメニューを開き、[設定 (Settings)] をクリックして、[設定 (Settings)] ページにアクセスします。



関連情報：

- [全般設定](#) (36 ページ)
- [ユーザ管理](#)
- [ロギングの設定](#)
- [通知設定](#) (39 ページ)

## 全般設定



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 \(36 ページ\)](#)
- マイトークン (My Tokens) については、[API トークン \(44 ページ\)](#) を参照してください。
- [テナント設定] 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 \(36 ページ\)](#)
  - [シスコサポートによるテナントの表示の防止 \(37 ページ\)](#)
  - [デフォルトの競合検出間隔 \(37 ページ\)](#)
  - [Web 分析 \(38 ページ\)](#)
  - [テナント ID \(39 ページ\)](#)
  - [テナント名 \(39 ページ\)](#)

## 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

変更リクエスト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。変更リクエストトラッキングを有効にするには、次の手順に従います。

**ステップ 1** ユーザーメニューから、[設定 (Settings)] を選択します。

**ステップ 2** ユーザーメニューで、[一般設定 (General Settings)] をクリックします。

**ステップ3** 変更リクエストトラッキング (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] の [変更リクエスト] ドロップダウンメニューに、[変更リクエスト] 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。

**ステップ1** ユーザーメニューから、[設定 (Settings) ] を選択します。

**ステップ2** [全般設定 (General Settings) ] をクリックします。

**ステップ3** [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。

**ステップ1** ユーザーメニューから、[設定 (Settings) ] を選択します。

**ステップ2** [全般設定 (General Settings) ] をクリックします。

**ステップ3** [デバイスの変更を自動承認するオプションの有効化] 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 が導入準備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、[デバイスとサービス] ページから利用できる [競合検出] オプションを介してオーバーライドできます。




## 自動展開をスケジュールするオプションを有効にする

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。

- 
- ステップ1 ユーザーメニューから、[設定 (Settings)] を選択します。
  - ステップ2 [全般設定 (General Settings)] をクリックします。
  - ステップ3 [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] 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] 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] 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。

- 
- ステップ1 ユーザーメニューから、[設定 (Settings)] を選択します。
  - ステップ2 [全般設定 (General Settings)] をクリックします。
  - ステップ3 [自動展開をスケジュールするオプションを有効にする] 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 分析を無効にしたり、その後に有効にするには、次の手順を実行します。

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

## 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

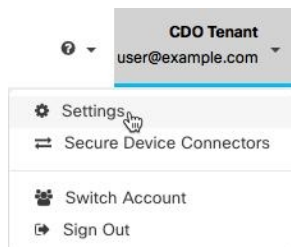
テナント名は、テナントも識別します。テナント名は組織名ではないことに注意してください。この情報は、Cisco Technical Assistance Center (TAC) に連絡する必要があるときに役立ちます。

## 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。

ユーザーメニューを開き、[設定] をクリックして、[設定] ページにアクセスします。



### 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。

- [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。
- [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。
- [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。

### 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。

### 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、チャン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。

**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。

## Slack 用の着信ウェブフック

- 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] 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せん。
- 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** 左側の [通知設定 (Notifications Settings)] タブを選択します。
- ステップ 12** [サービス通知 (Service Notifications)] 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、指定されたチャン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。

- 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 チャンネルを選択し、[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] 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** 左側の [通知設定 (Notifications Settings)] タブを選択します。
- ステップ 11** [サービス通知 (Service Notifications)] 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。

- 
- 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** 右上隅のユーザーメニューを開き、[設定] を選択します。
- ステップ 4** 左側の [通知設定 (Notifications Settings)] タブを選択します。

- ステップ5 [サービス通知 (Service Notifications)] までスクロールします。
- ステップ6 青色のプラスボタンをクリックします。
- ステップ7 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8 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9 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10 [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 ヶ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、[TAC でサポートチケットを開く](#)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明らかですが、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

---

**ステップ 1** ユーザーメニューから、[設定 (Settings)] を選択します。

**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。

---

**ステップ 1** ユーザーメニューから、[設定 (Settings)] を選択します。

**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

**ステップ 1** ユーザーメニューから、[設定 (Settings)] を選択します。

**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。

**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 がない場合、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 アカウントがなければ、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、ネットワーク管理者は 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、ネットワーク管理者が 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、ネットワーク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

マルチテナントポータルには、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が表示されます。[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、導入準備方式、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。

The screenshot shows the 'All Devices & Services' page in Cisco Defense Orchestrator. It features a table with columns for Name, Type, Region, Version, Hardware Version, Configuration, and Connectivity State. The table lists several devices, including ASA and FTD models. To the right, a detailed view for device '52.53.207.153' is shown, displaying its location, model, serial number, chassis serial, software version, ASDM version, context mode, firewall mode, and failover mode. A warning message at the bottom of the details panel states: 'Device in Different Region. The device 52.53.207.153 is managed by a Cisco Defense Orchestrator tenant in a different region. To manage this device, sign in to the CDO in Europe.'

- [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へのテナントの追加

ネットワーク管理者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 のみのユーザーの作成](#) 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次々と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。

**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] > [一般設定] > [マイトークン] をクリックします。

**ステップ 2** [API トークンを生成] 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] 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] 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

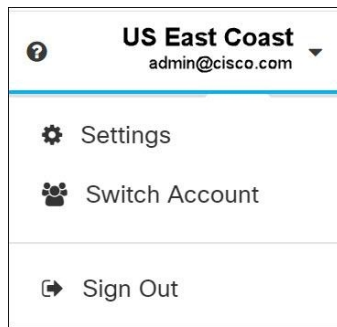
**ステップ 1** ポータルに移動し、[テナント (Tenants)] タブをクリックします。

**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] 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] をクリックして、[設定] 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で、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、将来的に有効にするには、次の手順に従います。

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ーをクリックします。

### [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。

---

**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。

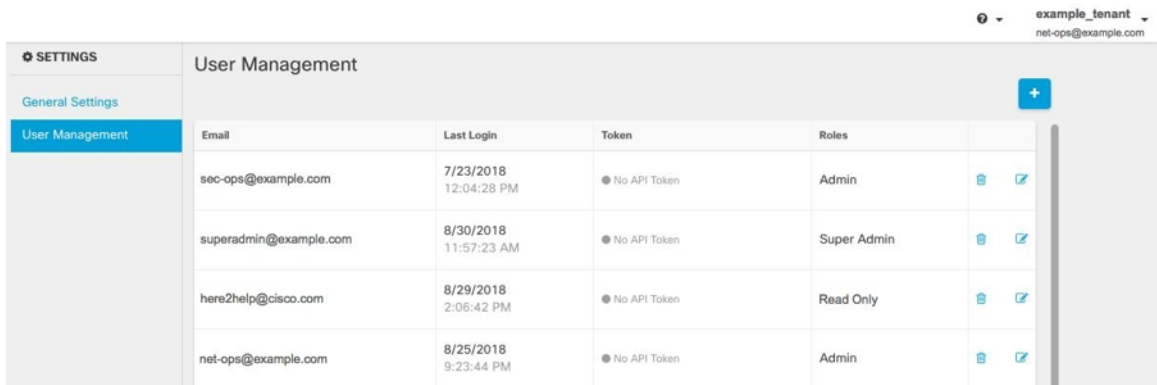
企業独自の IdP がない限り、Cisco Secure Sign-On はすべての CDO テナントの ID プロバイダーとなります。この記事の残りの部分は、ID プロバイダーとして Cisco Secure Sign-On を使用していることを前提としています。

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

**ステップ 1** ユーザーメニューから、[設定 (Settings)] を選択します。

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



| Email                  | Last Login               | Token        | Roles       |
|------------------------|--------------------------|--------------|-------------|
| sec-ops@example.com    | 7/23/2018<br>12:04:28 PM | No API Token | Admin       |
| superadmin@example.com | 8/30/2018<br>11:57:23 AM | No API Token | Super Admin |
| here2help@cisco.com    | 8/29/2018<br>2:06:42 PM  | No API Token | Read Only   |
| net-ops@example.com    | 8/25/2018<br>9:23:44 PM  | No API Token | Admin       |

(注) シスコのサポートがテナントにアクセスできないようにするには、[一般設定 (General Settings)] [全般設定 \(36 ページ\)](#) ページでアカウント設定を指定します。

## ユーザ管理の 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、SuperAdmin 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] タブ

[設定] 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] 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] 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 の複数のグループに属している場合があります、それらの各グループは、CDO において異なる CDO ロールで定義できます。ユーザーがログイン時に取得する最終的な権限は、そのユーザーが属している、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せん。
  - **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 1: *Active Directory* で定義されたカスタム要求

The screenshot shows the 'Attributes & Claims' configuration page in the Microsoft Azure portal. The breadcrumb navigation is: Home > Cisco-CDO-Dev > Enterprise applications > securex-okta-ci > SAML-based Sign-on > Attributes & Claims. Below the title, there are options to '+ Add new claim', '+ Add a group claim', 'Columns', and 'Got feedback?'. The page is divided into two sections: 'Required claim' and 'Additional claims'. The 'Required claim' section has a table with one row: 'Unique User Identifier (Name ID)' with the value 'user.userprincipalname [nameid-for-...]'. The 'Additional claims' section has a table with five rows. The first four rows are standard claims: 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress' (user.mail), 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname' (user.givenname), 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name' (user.userprincipalname), and 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname' (user.surname). The fifth row, 'SamlADUserGroupIds', and the sixth row, 'SamlSourceIdPIssuer', are highlighted with red boxes. The value for 'SamlADUserGroupIds' is 'user.groups' and for 'SamlSourceIdPIssuer' is 'https://sts.windows.net/1e491488-...'.

| Claim name                                                         | Value                                   |
|--------------------------------------------------------------------|-----------------------------------------|
| Unique User Identifier (Name ID)                                   | user.userprincipalname [nameid-for-...] |
| <b>Additional claims</b>                                           |                                         |
| Claim name                                                         | Value                                   |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress | user.mail                               |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname    | user.givenname                          |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name         | user.userprincipalname                  |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname      | user.surname                            |
| <b>SamlADUserGroupIds</b>                                          | user.groups                             |
| <b>SamlSourceIdPIssuer</b>                                         | "https://sts.windows.net/1e491488-..."  |

- **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 2: Azure Active Directory の識別子を見つける

The screenshot shows the Azure portal interface for configuring an enterprise application. The left sidebar contains navigation options like Overview, Deployment Plan, Manage, and Security. The main content area is titled 'securex-stage | SAML-based Sign-on'. It includes sections for 'Attributes & Claims', 'SAML Signing Certificate', and 'Set up securex-stage'. The 'Attributes & Claims' section lists various attributes and their corresponding values, such as 'givenname' and 'user.givenname'. The 'SAML Signing Certificate' section shows the status as 'Active' and provides download links for the certificate. The 'Set up securex-stage' section contains fields for 'Login URL', 'Azure AD Identifier', and 'Logout URL', with the 'Azure AD Identifier' field highlighted in red.

## ユーザー管理用 Active Directory グループの追加

ステップ 1 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] を選択します。

ステップ 3 [ユーザー管理 (User Management)] をクリックします。

ステップ 4 テーブルの上部にある [Active Directoryグループ] を選択します。

**ステップ5** 現在の AD グループがない場合は、[ADグループの追加] をクリックします。既存のエントリがある場合は、[追加] ボタンをクリックします。

**ステップ6** 次の情報を入力します。

- [グループ名]: 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してい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]: 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 からの AD 発行者の値を手動で入力します。
- [ロール]: 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]: 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7** [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す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。

**ステップ1** 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] を選択します。

**ステップ3** [ユーザー管理 (User Management)] をクリックします。

**ステップ4** テーブルの上部にある [Active Directoryグループ] を選択します。

**ステップ5** 編集する AD グループを特定し、[編集] アイコンを選択します。

**ステップ6** 次の値を変更します。

- [グループ名]: 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]: 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 からの AD 発行者の値を手動で入力します。
- [ロール]: 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]：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

---

- ステップ 1 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 (Settings)] を選択します。
- ステップ 3 [ユーザー管理 (User Management)] をクリックします。
- ステップ 4 テーブルの上にある [Active Directoryグループ] を選択します。
- ステップ 5 削除する AD グループを特定します。
- ステップ 6 [削除 (Delete)] アイコンを選択します。
- ステップ 7 [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（32 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 セキュリティのインストール。** 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。

### 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ーとして Google オーセンティケーターを設定します。

1. Google オーセンティケーター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ー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化したり

## 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一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。

**ステップ 1** CDO にログインします。

**ステップ 2** ユーザーメニューで、[設定 (Settings)] をクリックします。

**ステップ 3** [ユーザー管理 (User Management)] をクリックします。

**ステップ 4** 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 5** 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 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。

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

**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ーを設定している場合は、オーセンティケーター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、次のことを実行できません。

- 任意のページで作成、更新、設定、または削除する。
- デバイスを導入準備する。
- 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、インターフェイス、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。
- デバイスを導入準備する。
- 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設定するか、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設定するか、手動で開始する。
- 変更リクエスト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 バージョンと Snort 3 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。
- デバイスを導入準備する。
- 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。
- デバイスを導入準備する。
- 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**。

- 任意のページでの作成、更新、設定、または削除。
- デバイスのオンボーディング。
- 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 ユーザーレコードの作成。
- ユーザーロールの変更。
- ポリシーへのアクセスルールのアタッチまたはデタッチ。

## 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。
- デバイスの導入準備。
- CDO の任意のページまたは任意の設定を表示する。
- 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注意を表示する。

- 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

ネットワーク管理者ユーザーは、CDO のあらゆる側面に完全にアクセスできます。ネットワーク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) ネットワーク管理者は 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 \(31 ページ\)](#) 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

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ない場合は、[TACでサポートチケットを開く](#)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。

**ステップ 1** CDO にログインします。

**ステップ 2** ユーザーメニューで、[設定 (Settings)] をクリックします。

**ステップ 3** [ユーザー管理 (User Management)] をクリックします。

**ステップ 4** 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 5** 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 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** [v] をクリックします。

- (注) ネットワーク管理者は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 \(31 ページ\)](#) を参照してください。

## API のみのユーザーの作成

- ステップ 1** CDO にログインします。
- ステップ 2** ユーザーメニューで、[設定] をクリックします。
- ステップ 3** [ユーザー管理 (User Management)] をクリックします。
- ステップ 4** 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 5** [APIのみのユーザー] チェックボックスを選択します。
- ステップ 6** [ユーザー名] 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 7** 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 8** [OK] をクリックします。
- ステップ 9** [ユーザー管理] タブをクリックします。
- ステップ 10** 新しい API のみのユーザーの [トークン] 列で、[APIトークンの生成] 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、ネットワーク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。

- ステップ 1** CDO にログインします。
- ステップ 2** ユーザーメニューで、[設定] をクリックします。
- ステップ 3** [ユーザー管理 (User Management)] をクリックします。
- ステップ 4** ユーザーの行にある [編集] アイコンをクリックします。
- ステップ 5** [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 \(65 ページ\)](#) を選択します。
- ステップ 6** 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 7** [v] をクリックします。
- ステップ 8** 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。

- ステップ 1 CDO にログインします。
- ステップ 2 ユーザーメニューで、[設定 (Settings)] をクリックします。
- ステップ 3 [ユーザー管理 (User Management)] をクリックします。
- ステップ 4 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 5 [OK] をクリックします。
- ステップ 6 [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] 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導入準備します。
- 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。
- 導入準備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。「[\[インベントリ\] ページ情報の表示 \(80 ページ\)](#)」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 \(84 ページ\)](#)」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) に導入準備すると、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

## CDO のデバイスの名前を変更する

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。

**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] 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。

Nashua Building 1   
ASA 10.86.118.4:443 

**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] と表示されます。

## 関連情報：

- [デバイスの外部リンク \(76 ページ\)](#)
- [CDO へのデバイス一括再接続 \(79 ページ\)](#)

## 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 での導入準備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。

**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] 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。

Nashua Building 1 

**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。

デバイス自体には変更が加えられないため、デバイスの [設定ステータス (Configuration Status) ]には引き続き [同期済み] 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、リスト内の項目を並べ替えたり、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、情報をフィルタ処理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できる内容をエクスポートします。

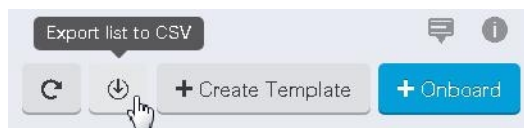
**ステップ 1** CDO ナビゲーションバーで、[インベントリ] をクリックします。

**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** 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] 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にリストをエクスポート] 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処理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。

- 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** 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** 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] 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 (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} 変数が作成されました。この変数には、デバイスの IP アドレスが入力されます。たとえば、

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

。

関連情報：

- [デバイスノートを書く \(80 ページ\)](#)
- [デバイスとサービスのリストのエクスポート \(75 ページ\)](#)

## デバイスからの外部リンクの作成

---

- 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** 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] 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。
- 

## への外部リンクの作成

を CDO から直接開く便利な方法を次に示します。

---

- 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。
- [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** 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

---

**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** 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] 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。

- 次の文字列を [URL] フィールドに入力します。

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

{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

---

**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

- 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

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。

- 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。

[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 Command 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 (139 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。

**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** 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] ペインで、[ノート] をクリックします。 ■ [Notes](#)。

**ステップ 6** 右側のエディタボタンをクリックして、デフォルト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] 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] ページ情報の表示

[インベントリ] ページには、すべての物理および仮想導入準備デバイスと、導入準備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] 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] ページには、次の詳細情報が表示されます。

- [デバイス] タブには、CDO に導入準備されているすべてのライブデバイスが表示されません。

- [テンプレート] 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。導入準備中または導入準備後のいつでも、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「groupname: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。

- 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] 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 [オブジェクト] 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** 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] 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。


## AWS VPC のラベルとタグ

AWS VPC を CDO に導入準備すると、CDO はすべての AWS VPC タグを設定の一部として読み取ります。つまりこれらのタグは、AWS からコピーされ、CDO のデータベースに保存されます。これらのタグは CDO ラベルとして表され、他のデバイスタイプのラベルと同様に [デバイスとサービス] ページで表示されます。CDO で既存のラベルを削除したり新しいラベルを作

成した場合、これらの変更は AWS VPC に同期されません。AWS コンソールを使用して、同じ変更を手動で行う必要があります。AWS VPC が導入準備された後に AWS コンソールで作成または変更された VPC タグは、CDO の設定のコピーに保存されず、アウトオブバンドの変更として検出されません。

## フィルタ

[インベントリ] ページと [オブジェクト] ページのさまざまなフィルタを使用して、探しているデバイスおよびオブジェクトを見つけることができます。

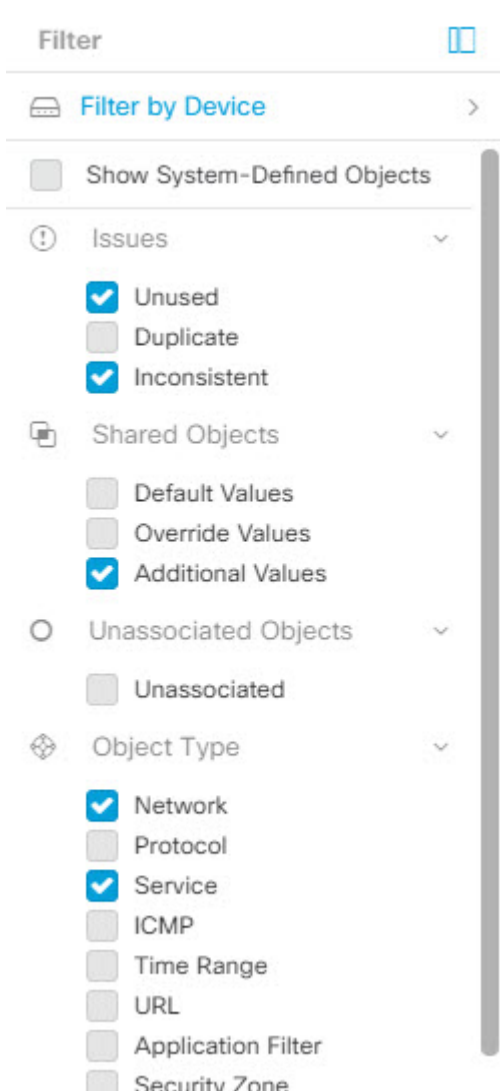
フィルタ処理するには、[デバイスとサービス (Devices and Services)] タブ、[ポリシー (Policies)] タブ、および [オブジェクト] タブの左側のペインで  をクリックします。

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

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

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


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



## 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

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、[インベントリ] 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** フィルタ処理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] 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] メニューを展開します。 [フィルタ \(82 ページ\)](#)
- ステップ 6** フィルタの [Secure Device Connector] セクションで、必要な SDC の名前をオンにします。インベントリテーブルには、フィルタでオンにした 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オンにします。
- 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] 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] 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。

- 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。

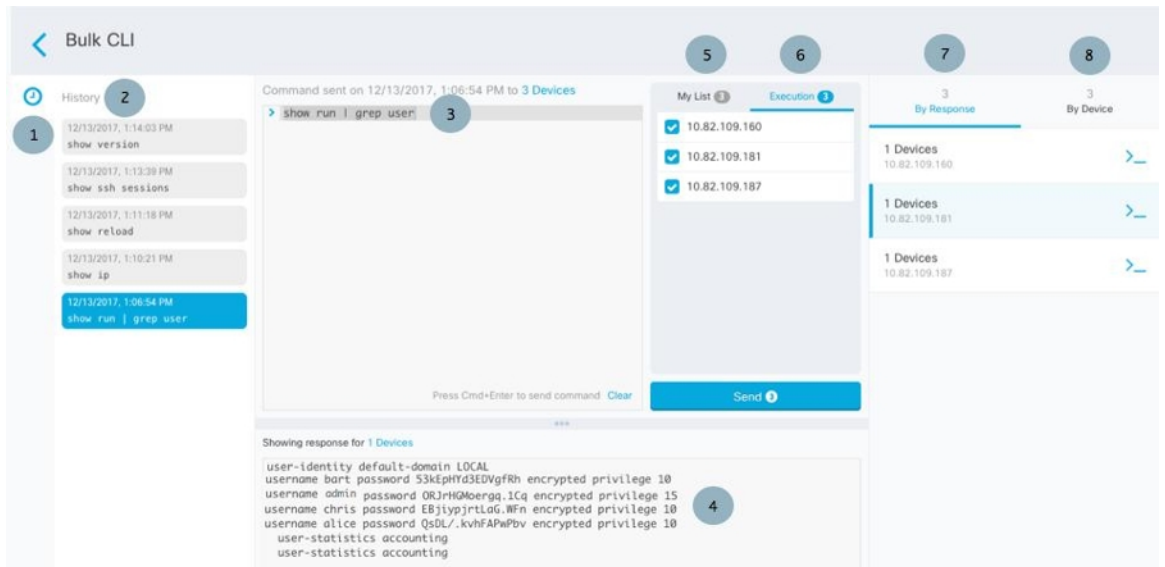
## 一括コマンドラインインターフェイス

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>

## 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。

- コマンドがエラーなしで正常に実行された後。
- 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   | <p>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。</p> <p>(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。</p> <ul style="list-style-type: none"> <li>• コマンドがエラーなしで正常に実行された後。</li> <li>• 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。</li> </ul> |
| 5   | [マイリスト] タブには、[インベントリ] 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

- 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。

- 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、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] 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。

- 
- 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] 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、実行構成がスタートアップ 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。

- 
- 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] 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] 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構成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。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 に導入準備された後にのみ、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

**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)


**ステップ 2** 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 3** [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 4** 適切なデバイスタイプのタブをクリックし、オンラインで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] 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] フィールドに完全な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。

**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** マクロに一意的な名前を指定します。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] 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

**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。

```
★ Using Macro: Configure DNS
> dns domain-lookup {{IF_NAME}}
 dns server-group DefaultDNS
 name-server {{IP_ADDR}}
```

**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。

Parameters
✕

| Parameters                                                                  | Payload                                                                                                   |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| IF_NAME<br><input style="width: 100%;" type="text" value="outside"/>        | <pre>dns domain-lookup <u>outside</u> dns server-group DefaultDNS name-server <u>208.67.220.220</u></pre> |
| IP_ADDR<br><input style="width: 100%;" type="text" value="208.67.220.220"/> |                                                                                                           |

**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、「Done!」というメッセージが表示されます。

**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構成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。

⚠ Some commands may have made changes to the running config
Write to Disk
Dismiss

- [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、実行構成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。

**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。

---

- 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。
-





## 第 2 章

# デバイスとサービスの導入準備

ライブデバイスとモデルデバイスの両方を CDO に対して導入準備できます。モデルデバイスはアップロードされた構成ファイルであり、CDO を使用して閲覧および編集できます。

ほとんどのライブデバイスおよびサービスでは、Secure Device Connector が CDO をデバイスまたはサービスに接続できるように、オープンな HTTPS 接続が必要となります。

SDC とそのステータスの詳細については、[Secure Device Connector \(SDC\) \(3 ページ\)](#) を参照してください。

この章は、次のセクションで構成されています。

- [AWS VPC の導入準備 \(95 ページ\)](#)
- [CDO からのデバイスの削除 \(97 ページ\)](#)

## AWS VPC の導入準備

AWS VPC を CDO に対して導入準備するには、以下の手順に従います。

始める前に



- (注) CDO は、ピアリングされた AWS VPC をサポートしていません。ピア VPC で定義されたセキュリティグループを参照する、ピアリングされた VPC を導入準備しようとすると、導入準備プロセスは失敗します。

Amazon Web Service (AWS) 仮想プライベートクラウド (VPC) を CDO に対して導入準備する前に、以下の前提条件を確認してください。

- CDO を AWS VPC に接続するために必要なネットワーク要件を [Cisco Defense Orchestrator の管理対象デバイスへの接続 \(5 ページ\)](#) で確認します。
- AWS VPC を導入準備するには、AWS VPC のアクセスキーとシークレットアクセスキーが必要です。これらはいずれもアイデンティティとアクセス管理 (IAM) コンソールを使



用して生成されます。詳細については、「セキュリティログイン情報の理解と取得」(<https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html>)を参照してください。

- CDO が AWS VPC と通信できるように権限を設定します。詳細は、「IAM ユーザーの権限の変更」([https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_users\\_change-permissions.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_change-permissions.html))を参照してください必要な権限については、以下の例を参照してください。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ec2:AuthorizeSecurityGroupEgress",
 "ec2:AuthorizeSecurityGroupIngress",
 "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
 "ec2:DescribeInstances",
 "ec2:DescribeVpnConnections",
 "ec2:DescribeRegions",
 "ec2:DescribeSecurityGroups",
 "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
 "ec2:RevokeSecurityGroupIngress",
 "ec2:DescribeVpcs",
 "ec2:RevokeSecurityGroupEgress",
 "sts:GetCallerIdentity",
 "ec2:DescribeSubnets",
 "ec2:DescribeVpnGateways"
],
 "Resource": "*"
 }
]
}
```

**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] 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て、デバイスの導入準備を開始します。



**ステップ 3** [AWS VPC] をクリックします。

**ステップ 4** AWS アカウントに接続するためのアクセスキー ID とシークレットアクセスキーのログイン情報を入力します。生成された名前のリストは、ログイン情報を入力した AWS VPC から取得されます。

**ステップ 5** [接続 (Connect)] をクリックします。

**ステップ 6** ドロップダウンメニューから [リージョン] を選択します。VPC のローカルであるリージョンを選択する必要があります。

**ステップ 7** [選択 (Select)] をクリックします。

**ステップ 8** ドロップダウンメニューを使用して、正しい AWS 名を選択します。生成された名前のリストは、ログイン情報を入力した AWS VPC から取得されます。ドロップダウンメニューから目的の AWS VPC を選択します。AWS VPC ID の名前は一意であり、2 つ以上のインスタンスが同じ ID を持つことはできません。

**ステップ 9** [選択 (Select)] をクリックします。

- ステップ 10** CDO UI で表示する名前を入力します。
- ステップ 11** [続行 (Continue) ] をクリックします。
- ステップ 12** (オプション) デバイスのラベルを入力します。AWS VPC のラベルを作成する場合、テーブルはデバイスに自動的に同期されません。AWS コンソールで、ラベルをタグとして手動で再作成する必要があります。詳細については、[AWS VPC のラベルとタグ \(81 ページ\)](#) を参照してください。
- ステップ 13** [続行 (Continue) ] をクリックします。
- ステップ 14** [デバイスとサービス] ページに戻ります。デバイスが正常に導入準備されると、構成ステータスが [同期済み]、接続状態が [オンライン] と表示されます。

---

**関連情報 :**

- [AWS VPC 接続ログイン情報の更新 \(99 ページ\)](#)
- [AWS VPC ポリシー \(103 ページ\)](#)
- [AWS VPC と CDO のセキュリティグループ](#)
- [AWS とその他の管理対象デバイス間でオブジェクトを共有する](#)

## CDO からのデバイスの削除

CDO からデバイスを削除するには、次の手順を使用します。

- 
- ステップ 1** CDO にログインします。
- ステップ 2** [インベントリ] ページに移動します。
- ステップ 3** 削除するデバイスを見つけ、そのデバイスの行でデバイスをチェックして選択します。
- ステップ 4** 右側にある [デバイスアクション] パネルで、[削除] を選択します。
- ステップ 5** プロンプトが表示されたら、[OK] を選択して、選択したデバイスの削除を確認します。[キャンセル] を選択して、デバイスを導入準備したままにします。
-





## 第 3 章

# 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](#) (99 ページ)
- [AWS Transit Gateway を使用して AWS VPC トンネルを監視する](#) (100 ページ)
- [サイト間 VPN トンネルの検索とフィルタ処理](#) (101 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](#) (102 ページ)
- [セキュリティ ポリシー管理](#) (103 ページ)
- [仮想プライベートネットワークの管理](#) (107 ページ)
- [変更の読み取り、破棄、チェック、および展開](#) (115 ページ)
- [すべてのデバイス設定の読み取り](#) (117 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](#) (118 ページ)
- [変更のデバイスへの展開](#) (119 ページ)
- [デバイス設定の一括展開](#) (120 ページ)
- [スケジュールされた自動展開](#) (121 ページ)
- [設定変更の確認](#) (123 ページ)
- [変更の破棄](#) (124 ページ)
- [デバイスのアウトオブバンド変更](#) (125 ページ)
- [Defense Orchestrator とデバイス間の設定を同期する](#) (125 ページ)
- [競合検出](#) (126 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](#) (127 ページ)
- [設定の競合の解決](#) (128 ページ)
- [デバイス変更のポーリングのスケジュール](#) (130 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](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>) 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](#) 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 \(164 ページ\)](#) を参照してください。

#### 関連情報

- [AWS VPC の導入準備 \(95 ページ\)](#)

## 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 \(95 ページ\)](#) 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<br>AWS VPC | 209.165.200.230 | def-o9p0s1a2f3g4h5j6<br>Unknown | 209.165.201.31 | 4/8/22 7:12 AM  |
| VPN 1 | Active | abc-q1w2e3r4t5y6u7i8<br>AWS VPC | 209.165.202.148 | def-o9p0s1d2f3g4h5j6<br>Unknown | 209.165.201.31 | 5/10/22 2:32 PM |


## 関連情報

- [AWS VPC の導入準備 \(95 ページ\)](#)

# 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 \(131 ページ\)](#)

# 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 \(103 ページ\)](#)

## 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 \(104 ページ\)](#)
- [セキュリティグループルールの編集 \(106 ページ\)](#)
- [セキュリティグループルールの削除 \(106 ページ\)](#)

## 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 \(118 ページ\)](#)

**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 \(101 ページ\)](#) [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の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 \(110 ページ\)](#)

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 \(118 ページ\)](#)。



## 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 \(95 ページ\)](#)
- [AWS VPC の導入準備 \(95 ページ\)](#)

## 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 \(111 ページ\)](#) 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。

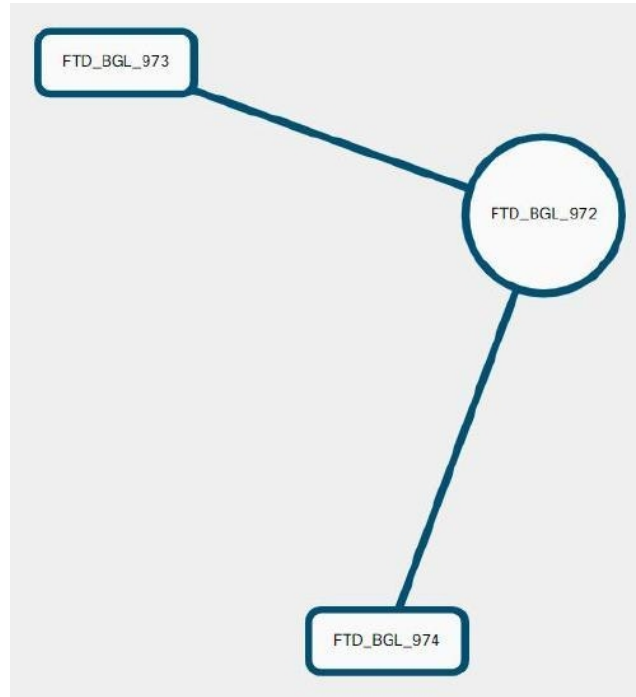
**ステップ 2** [テーブルビュー] ボタンをクリックします。

**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](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 \(124 ページ\)](#)

- 
- 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、[変更リクエスト管理](#)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、[ジョブ (Jobs)] ページで確認します。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 (139 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 [変更リクエスト管理](#) 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 [変更リクエスト管理](#) 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 \(118 ページ\)](#) 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。
- 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 \(38 ページ\)](#) 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せん。



(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 \(117 ページ\)](#)
- [すべてのデバイスの構成変更のプレビューと展開 \(118 ページ\)](#)

## 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 \(130 ページ\)](#) 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。

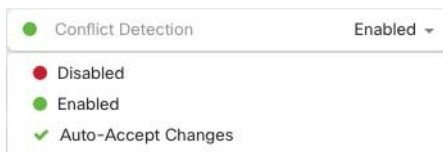
**ステップ 1** ナビゲーションバーで、[デバイスとサービス (Devices & Services)] をクリックします。

**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。

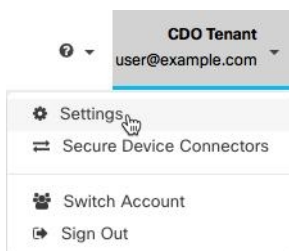
変更の自動受け入れを使用するには、最初に、テナントが [デバイスとサービス] ページの [競合検出] メニューで自動受け入れオプションを表示できるようにします。次に、個々のデバイスでの変更の自動受け入れを有効にします。

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 \(126 ページ\)](#) 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。

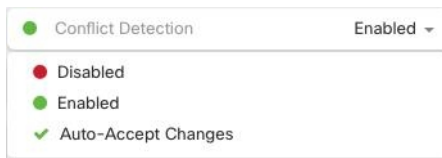


**ステップ 3** [テナント設定] エリアで、[デバイスの変更を自動承認するオプションの有効化] のトグルをクリックします。これにより、[デバイスとサービス] ページの [競合検出] メニューに [変更の自動承認] メニューオプションが表示されるようになります。

**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 \(126 ページ\)](#) 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 \(126 ページ\)](#) 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。

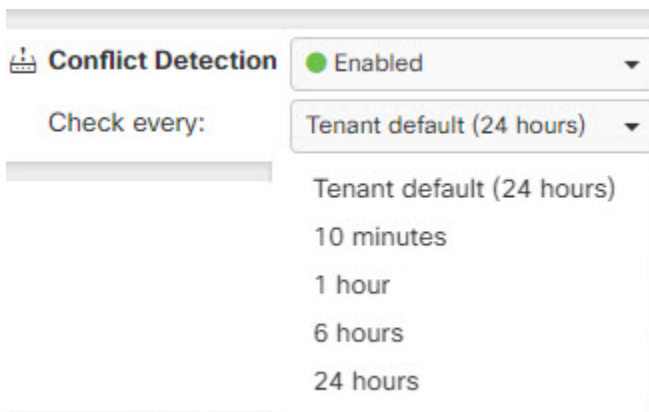
デバイスでこの間隔が選択されていない場合は、間隔は「テナントのデフォルト」に自動的に設定されます。



(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 \(37 ページ\)](#) 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。





## 第 4 章

# モニタリングとレポート

CDO の監視およびレポート機能は、既存のポリシーの影響とその結果として生じるセキュリティ態勢に関する貴重なインサイトをもたらします。

この章は、次のセクションで構成されています。

- [変更ログ \(131 ページ\)](#)
- [変更ログの差分の表示 \(133 ページ\)](#)
- [変更ログを CSV ファイルにエクスポートする \(134 ページ\)](#)
- [変更リクエスト管理 \(135 ページ\)](#)
- [\[ジョブ \(Jobs\) \] ページ \(139 ページ\)](#)
- [\[ワークフロー \(Workflows\) \] ページ \(141 ページ\)](#)

## 変更ログ

### 変更ログについて

変更ログは、CDOで行われた設定変更を継続的にキャプチャします。この単一のビューには、サポートされているすべてのデバイスとサービスにわたる変更が含まれます。変更ログの機能の一部を次に示します。

- デバイス構成に加えられた変更の対照比較。
- すべての変更ログエントリの平易な英語のラベル。
- デバイスの導入準備と削除の記録。
- CDO の外部で発生するポリシー変更の競合の検出。
- インシデントの調査またはトラブルシューティング中に、誰が、何を、いつに関する間に回答可能。
- 完全な変更ログまたは一部のみを CSV ファイルとしてダウンロード可能。

## 変更ログの容量

CDO は、変更ログの情報を 1 年間保持します。1 年以上前の情報は削除されます。

CDO がデータベースに保存する変更ログ情報と、変更ログをエクスポートしたときに表示される情報には違いがあります。詳細については、[変更ログを CSV ファイルにエクスポートする \(134 ページ\)](#) を参照してください。

## [変更ログ] ページの変更ログエントリ


変更ログエントリには、単一のデバイス設定への変更、デバイスで実行されたアクション、または CDO の外部でデバイスに加えられた変更が反映されます。

- 設定の変更を含む変更ログエントリの場合、行の任意の場所をクリックして変更を展開できます。
- 競合として検出された CDO の外部で行われたアウトオブバンド変更の場合、**システムユーザー**は最後のユーザーとして報告されます。
- CDO 上のデバイスの設定がデバイス上の設定と同期された後、またはデバイスが CDO から削除されたときに、CDO は変更ログエントリを閉じます。設定は、デバイスから CDO に設定を「読み取った」後に、または CDO からデバイスに設定を展開することによって同期されます。
- CDO は、既存のエントリを閉じた直後に新しい変更ログエントリを作成します。追加の設定変更は、開いている変更ログエントリに追加されます。
- デバイスに対する読み取り、展開、および削除アクションのイベントが表示されます。これらのアクションで、デバイスの変更ログが閉じられます。
- CDO が（読み取りまたは展開によって）デバイスの設定と同期されると、または CDO がデバイスを管理しなくなると、変更ログは閉じられます。
- CDO の外部でデバイスに変更が加えられた場合、[競合検出 (Conflict Detected)] エントリが変更ログに書き込まれます。

## アクティブおよび完了した変更ログエントリ

変更ログには、**アクティブ**または**完了**のステータスがあります。CDO を使用してデバイスの設定を変更すると、変更は**アクティブ**な変更ログエントリに記録されます。デバイスから CDO への設定の読み取り、CDO からデバイスへの変更の展開、CDO からのデバイスの削除が完了するか、または実行構成ファイルを更新する CLI コマンドを実行すると、アクティブな変更ログが完了し、将来の変更のために新しいログが作成されます。

## 変更ログでのエントリの検索

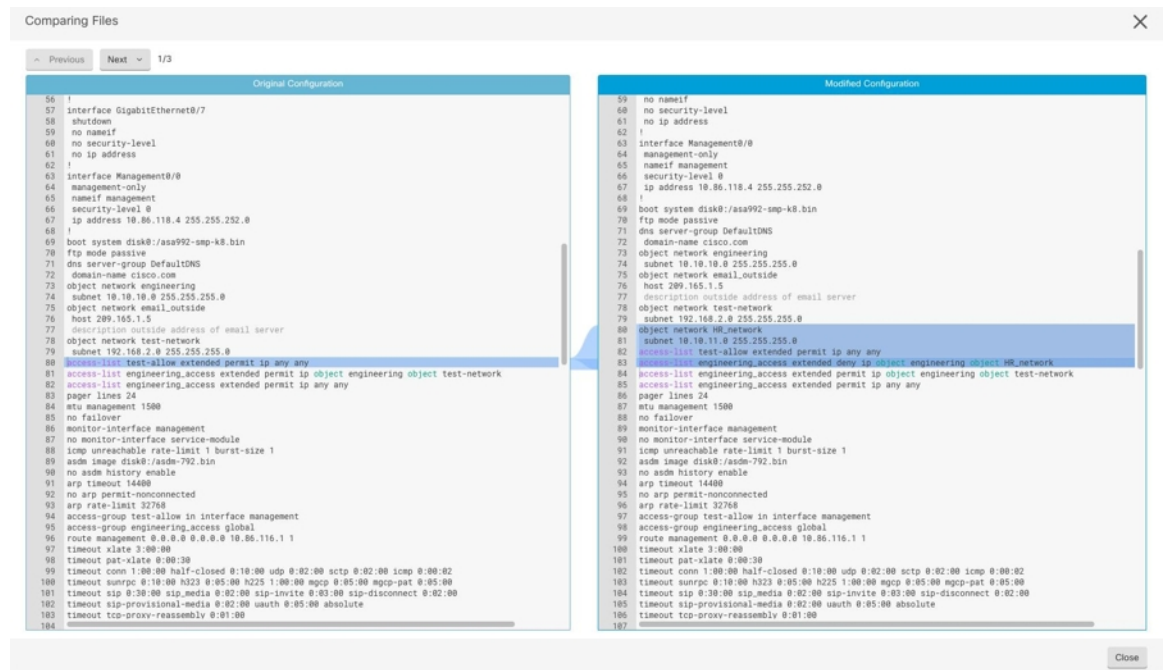
変更ログイベントは検索およびフィルタリングできます。検索バーを使用して、キーワードに一致するイベントを検索します。フィルタ  を使用して、指定したすべての条件を満たすエントリを検索します。また、変更ログをフィルタリングし、[検索] フィールドにキーワードを

追加して、操作を組み合わせることで、フィルタリングされた結果内のエントリを検索できます。

## 変更ログの差分の表示

変更ログにある青色の [差分 (Diff)] リンクをクリックすると、デバイスの実行構成ファイル内の変更が並べて表示されるため、変更を対比できます。2つのバージョンの違いがわかります。

次の図では、[元の設定 (Original Configuration)] は変更が ASA に書き込まれる前の実行構成ファイルであり、[変更された設定 (Modified Configuration)] 列は変更が書き込まれた後の実行構成ファイルを示しています。この場合、[元の設定 (Original Configuration)] 列は、実際には変更されていない実行構成ファイルの行を強調表示しますが、[変更された設定 (Modified Configuration)] 列の参照点となります。左から右の列に向かって線をたどると、HR\_network オブジェクトの追加と、「engineering」ネットワークのアドレスが「HR\_network」ネットワークのアドレスに到達することを防止するアクセスルールを確認できます。[前へ (Previous)] および [次へ] ボタンを使用して、ファイル内の変更を確認します。



### 関連項目

- [変更ログ \(131 ページ\)](#)



## 変更ログを CSV ファイルにエクスポートする

CDO 変更ログのすべてまたは一部をコンマ区切り値 (.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処理および並べ替えることができます。


変更ログを .csv ファイルにエクスポートするには、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、[変更ログ] をクリックします。

**ステップ 2** 次のいずれかのアクションを実行して、エクスポートする変更を見つけます。

- フィルタフィールドと検索フィールドを使用して、エクスポート対象を正確に見つけます。たとえば、デバイスでフィルタ処理して、選択した1つまたは複数のデバイスの変更のみを表示します。
- 変更ログのすべてのフィルタおよび検索条件をクリアします。これにより、変更ログ全体をエクスポートできます。

(注) CDO は 1 年間の変更ログデータを保存することに注意してください。最大限の 1 年間分の変更ログ履歴をダウンロードするよりも、変更ログの内容をフィルタ処理し、その結果を .csv ファイルとしてダウンロードする方がよい場合があります。

**ステップ 3** 変更ログの右上にある青色のエクスポートボタン  をクリックします。

**ステップ 4** .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。

## CDO の変更ログのキャパシティとエクスポートした変更ログのサイズの差異

CDO の変更ログページからエクスポートする情報は、CDO がデータベースに保存する変更ログ情報とは異なります。

すべての変更ログについて、CDO はデバイスの設定の 2 つのコピーを保存します。クローズされた変更ログの場合は「開始」設定と「終了」設定のいずれかとなり、オープンな変更ログの場合は「最新」設定となります。これにより、CDO は設定の違いを並べて表示できます。さらに、CDO は、変更を行ったユーザー名、変更が行われた時刻、およびその他の詳細とともに、すべてのステップの「変更イベント」を追跡して保存します。

ただし、変更ログをエクスポートする場合、エクスポートには設定の 2 つの完全なコピーは含まれません。これには「変更イベント」のみが含まれるため、エクスポートファイルは変更ログ CDO ストアよりもはるかに小さくなります。

CDO は最大 1 年分の変更ログ情報を保存し、この情報には設定の 2 つのコピーが含まれます。

## 変更リクエスト管理

変更リクエスト管理により、サードパーティのチケットシステムで開かれた変更リクエストとそのビジネス上の正当性を、変更ログのイベントに関連付けることができます。変更リクエスト管理を使用して、CDO で変更リクエストを作成し、作成した変更リクエストを一意の名前で識別し、変更の説明を入力して、変更リクエストを変更ログイベントに関連付けます。後で変更リクエスト名を変更ログで検索できます。



- (注) CDO の変更リクエストトラッキングへの参照も表示される場合があります。変更リクエストトラッキングと変更リクエスト管理は、同じ機能を参照します。

## 変更リクエスト管理の有効化

変更リクエスト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。変更リクエストトラッキングを有効にするには、次の手順に従います。

**ステップ 1** ユーザーメニューから、[設定 (Settings)] を選択します。

**ステップ 2** ユーザーメニューで、[一般設定 (General Settings)] をクリックします。

**ステップ 3** [変更リクエストトラッキング (Change Request Tracking)] 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] の [変更リクエスト] ドロップダウンメニューに、[変更リクエスト] ツールバーが表示されます。

## 変更リクエストの作成

**ステップ 1** 任意の CDO ページから、ページの左下隅にある変更リクエストツールバーの青色の [+] ボタンをクリックします。

**ステップ 2** 変更リクエストに名前を付け、説明を入力します。変更リクエスト名に、組織が実装する変更リクエスト ID を反映させます。説明フィールドを使用して、変更の目的を記述します。

(注) 作成した変更リクエストの名前は変更できません。

**ステップ 3** 変更リクエストを保存します。



- (注) CDO は変更リクエストを保存し、その変更リクエストを無効にするか、変更リクエストツールバーの変更リクエスト情報をクリアするまで、すべての新しい変更をその変更リクエスト名に関連付けます。

---

## 変更リクエストと変更ロギイベントの関連付け

---

- ステップ1** ナビゲーションウィンドウで、[変更ログ (Change Log)] をクリックします。
- ステップ2** 変更ログを展開して、変更リクエストに関連付けるイベントを表示します。
- ステップ3** [変更リクエスト] 列で、イベントのドロップダウンメニューをクリックします。最新の変更リクエストが変更リクエストリストの一番上に表示されることに注意してください。
- ステップ4** 変更リクエストの名前をクリックし、[選択 (Select)] をクリックします。
- 

---

## 変更リクエストがある変更ロギイベントの検索

---

- ステップ1** ナビゲーションウィンドウで、[変更ログ] をクリックします。
- ステップ2** [変更ログ (Change Log)] 検索フィールドに、変更リクエストの正確な名前を入力して、その変更リクエストに関連付けられた変更ロギイベントを検索します。CDO は、完全に一致する変更ロギイベントを強調表示します。
- 

---

## 変更リクエストの検索

---

- ステップ1** 変更リクエストツールバーの変更リクエストメニューをクリックします。
- ステップ2** 検索する変更リクエスト名またはキーワードの入力を開始します。名前フィールドと説明フィールド両方で部分一致の結果が、変更リクエストのリストに表示されるようになります。
- 

---

## フィルタ変更リクエスト

フィルタトレイには、変更ロギイベントの検索に使用できる変更リクエストフィルタがあります。

---

- ステップ1** [変更ログ] ページの左側にあるフィルタトレイで、[変更リクエスト (Change Requests)] 領域を探します。

- ステップ2** フィルタを展開し、[検索 (search)] フィールドに変更リクエストの名前の入力を開始します。[検索 (Search)] フィールドの下に、部分一致が表示され始めます。
- ステップ3** 変更リクエスト名を選択し、対応するチェックボックスをオンにすると、[変更ログ] テーブルに一致したものが表示されます。CDO は、完全に一致する変更ログイベントを強調表示します。

---

## 変更リクエストツールバーのクリア

変更リクエストツールバーをクリアすると、変更ログイベントが既存の変更リクエストに自動的に関連付けられることを防ぐことができます。

- ステップ1** 変更リクエストツールバーの変更リクエストメニューを選択します。
- ステップ2** [クリア (Clear)] をクリックします。変更リクエストメニューが [なし] に変わります。

---

## 変更ログイベントと関連付けられた変更リクエストのクリア

- ステップ1** ナビゲーションウィンドウで、[変更ログ] をクリックします。
- ステップ2** 変更ログを拡大して、変更リクエストとの関連付けを解除するイベントを表示します。
- ステップ3** [変更リクエスト] 列で、イベントのドロップダウンメニューをクリックします。
- ステップ4** [クリア (Clear)] をクリックします。

---

## 変更リクエストの削除

変更リクエストを削除するときは、変更ログからではなく、変更リクエストリストから削除します。

- ステップ1** 変更リクエストツールバーの変更リクエストメニューをクリックします。
- ステップ2** 変更リクエスト名をクリックします。
- ステップ3** その行の [削除 (delete)] アイコンをクリックします。
- ステップ4** 緑色のチェックマークをクリックして、変更リクエストを削除することを確認します。

---

## 変更リクエスト管理の無効化

変更リクエスト管理を無効にすると、アカウントのすべてのユーザーに影響します。変更リクエスト管理を無効にするには、次の手順に従います。

**ステップ1** ユーザー名のメニューから、[設定] を選択します。

**ステップ2** [変更リクエストのトラッキング (Change Request Tracking)] の下にあるボタンをスライドして、灰色の X を表示します。

## 使用例

これらのユースケースは、上記の手順に従って変更リクエスト管理を前もって有効にしていることを前提としています。

### 外部システムで維持されているチケットを解決するために行われたファイアウォールの変更を追跡する

このユースケースでは、ユーザーがファイアウォールの変更を行って、外部システムで維持されているチケットを解決します。ユーザーは、ファイアウォールの変更に起因する変更ログイベントを変更リクエストに関連付けたいと考えています。次の手順に従って変更リクエストを作成し、変更ログイベントに関連付けます。

1. [変更リクエストの作成 \(135 ページ\)](#)。変更リクエストの名前として、外部システムからのチケット名または番号を使用します。説明フィールドを使用して、変更の理由やその他の関連情報を追加します。
2. 新しい変更リクエストが変更リクエストツールバーに表示されていることを確認します。
3. ファイアウォールを変更します。
4. ナビゲーションウィンドウで[変更ログ]をクリックし、新しい変更リクエストに関連付けられている変更ログイベントを見つけます。
5. 完了したら、[変更リクエストツールバーのクリア \(137 ページ\)](#) を実行します。

### ファイアウォールの変更が行われた後、個々の変更ログイベントを手動で更新する

このユースケースでは、ユーザーがファイアウォールの変更を行って外部システムで維持されているチケットを解決しましたが、変更リクエスト管理機能を使用して変更リクエストを変更ログイベントに関連付けるのを忘れていました。ユーザーは、変更ログに戻って、チケット番号で変更ログイベントを更新したいと考えています。変更リクエストを変更ログイベントに関連付けるには、次の手順に従います。

1. [変更リクエストの作成 \(135 ページ\)](#)。変更リクエストの名前として、外部システムからのチケット名または番号を使用します。説明フィールドを使用して、変更の理由やその他の関連情報を追加します。
2. ナビゲーションウィンドウで[変更ログ]をクリックし、ファイアウォールの変更に関連付けられている変更ログイベントを検索します。
3. [変更リクエストと変更ログイベントの関連付け \(136 ページ\)](#)。

- 完了したら、変更リクエストツールバーをクリアします。

#### 変更リクエストに関連付けられた変更ロギイベントを検索する

このユースケースでは、ユーザーは、外部システムで維持されているチケットを解決するために行われた作業の結果として、どの変更ロギイベントが変更ログに記録されたかを知りたいと考えています。変更リクエストに関連付けられている変更ロギイベントを検索するには、次の手順に従います。

- ナビゲーションウィンドウで、[変更ログ] をクリックします。
- 次のいずれかの方法を使用して、変更リクエストに関連付けられた変更ロギイベントを検索します。
  - [変更ログ] 検索フィールドに、変更リクエストの正確な名前を入力して、その変更リクエストに関連付けられた変更ロギイベントを検索します。CDOは、完全に一致する変更ロギイベントを強調表示します。
  - [フィルタ変更リクエスト \(136 ページ\)](#) を実行して変更ロギイベントを検索します。
- 各変更ログを表示して、関連する変更リクエストを示す強調表示された変更ロギイベントを見つけます。

## [ジョブ (Jobs) ] ページ

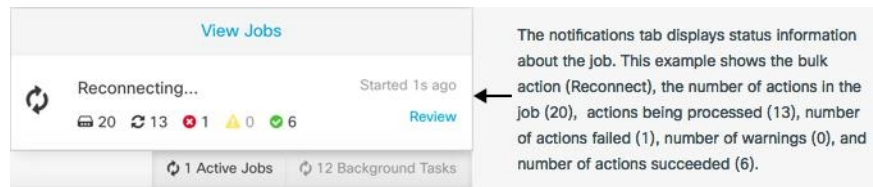
[ジョブ] ページには、一括操作のステータスに関する情報が表示されます。一括操作には、複数のデバイスの再接続、複数のデバイスからの設定の読み取り、複数のデバイスの同時アップグレードなどがあります。ジョブテーブルの色分けされた行は、成功または失敗した個々のアクションを示します。

表の1行は、1回の一括操作を表します。この1回の一括操作は、たとえば、20台のデバイスを再接続する試みだった可能性があります。[ジョブ] ページの行を展開すると、一括操作の影響を受ける各デバイスの結果が表示されます。

| ACTION            | STATUS   | USER                  | START                 | END                   |
|-------------------|----------|-----------------------|-----------------------|-----------------------|
| Reconnect Devices | 0 1 0 19 | user1@example.com     | 11/9/2017, 8:12:04 AM | 11/9/2017, 8:12:10 AM |
| DEVICE            | STATUS   | START                 | END                   |                       |
| Issues            |          |                       |                       |                       |
| ctx-70            | Error    | 11/9/2017, 8:12:04 AM | 11/9/2017, 8:12:05 AM |                       |
| Active / Done     |          |                       |                       |                       |
| ctx-77            | Done     | 11/9/2017, 8:12:04 AM | 11/9/2017, 8:12:09 AM |                       |
| ctx-72            | Done     | 11/9/2017, 8:12:04 AM | 11/9/2017, 8:12:09 AM |                       |

[ジョブ] ページには、次の3つの方法でアクセスできます。

- 通知タブで、通知行の [確認] リンクをクリックします。[ジョブ] ページにリダイレクトされ、その通知に対応する特定のジョブが表示されます。



- [通知 (Notifications) ] タブの上部にある [ジョブを表示 (View jobs) ] リンクをクリックすると、[ジョブ] ページに移動します。
- CDO のメニューから、[モニタリング (Monitoring) ] > [ジョブ] を選択します。この表には、CDO で実行される一括操作の完全なリストが示されます。


### フィルタリングと検索

[ジョブ] ページでは、操作タイプ、操作を実行したユーザー、および操作ステータスによってフィルター処理および検索を実行できます。

## いずれかのアクションに失敗した一括操作の再開

ジョブのページを確認して、一括操作で1つ以上のアクションに失敗したことがわかった場合は、必要な修正を行った後に一括操作を再実行できます。CDO は、失敗したアクションのみでジョブを再実行します。一括操作を再実行するには、次の手順に従います。

**ステップ1** アクションの失敗を示すジョブページの行を選択します。

**ステップ2** 再開  アイコンをクリックします。

## 一括操作のキャンセル

複数のデバイスで実行したアクティブな一括操作をキャンセルできるようになりました。たとえば、4台の管理対象デバイスを再接続しようとして、3台のデバイスが正常に再接続したが、4台目のデバイスは再接続に成功も失敗もしていないとします。

一括操作をキャンセルするには、次の手順を実行します。

**ステップ1** CDO ナビゲーションメニューで、[ジョブ] をクリックします。

**ステップ2** まだ実行中の一括操作を見つけて、ジョブの行の右側にある [キャンセル] リンクをクリックします。

一括操作のいずれかの部分が成功した場合、それらの操作は元に戻されません。まだ実行中の操作はすべてキャンセルされます。

## [ワークフロー (Workflows) ] ページ

[ワークフロー (Workflows) ] ページでは、デバイス、Secure Device Connector (SDC)、または Secure Event Connector (SEC) と通信するとき、およびルールセットの変更をデバイスに適用するときに、CDOが実行するすべてのプロセスを監視できます。CDOは、各ステップのワークフローテーブルにエントリを作成し、その結果をこのページに表示します。エントリには、CDOによって実行されるアクションについての情報のみが含まれており、CDOがデータをやり取りしているデバイスについての情報は含まれません。

CDOは、デバイスでのタスクの実行に失敗するとエラーを報告します。[ワークフロー (Workflows) ] ページに移動して、エラーが発生したステップとエラーの詳細を確認できます。

このページにアクセスして、エラーを特定してトラブルシューティングしたり、TACに要求された情報をTACと共有したりすることができます。

[ワークフロー (Workflows) ] ページに移動するには、[デバイスとサービス] ページで、[デバイス] タブをクリックします。適切なデバイスタイプタブをクリックしてデバイスを特定し、必要なデバイスを選択します。右側のペインの[デバイスとアクション (Devices and Actions) ] で、[ワークフロー (Workflows) ] をクリックします。次の図は、[ワークフロー (Workflows) ] テーブルのエントリが表示された [ワークフロー (Workflows) ] ページを示しています。

| Name                             | Priority  | Condition | Current State | Last Active            | Time                        |
|----------------------------------|-----------|-----------|---------------|------------------------|-----------------------------|
| ftdObjDetectorStateMachine       | Scheduled | Done      | Done          | 12/4/2020, 2:17:16 PM  | 14:17:00.381 / 14:17:16.640 |
| ftdVpnSessionDetailsStateMachine | Scheduled | Done      | Done          | 12/4/2020, 2:04:02 PM  | 14:04:00.278 / 14:04:02.481 |
| ftdVpnSessionDetailsStateMachine | Scheduled | Done      | Done          | 12/4/2020, 1:04:02 PM  | 13:04:00.433 / 13:04:02.747 |
| ftdVpnSessionDetailsStateMachine | Scheduled | Done      | Done          | 12/4/2020, 12:04:02 PM | 12:04:00.307 / 12:04:02.507 |
| ftdVpnSessionDetailsStateMachine | Scheduled | Done      | Done          | 12/4/2020, 11:04:02 AM | 11:04:00.205 / 11:04:02.290 |
| ftdVpnSessionDetailsStateMachine | Scheduled | Done      | Done          | 12/4/2020, 10:04:02 AM | 10:04:00.312 / 10:04:02.541 |
| ftdVpnSessionDetailsStateMachine | Scheduled | Error     | Error         | 12/2/2020, 1:10:25 PM  | 13:04:00.291 / 13:10:25.140 |

| ACTION                                         | TIME                        | START STATE                            | END STATE                          | RESULT                              |
|------------------------------------------------|-----------------------------|----------------------------------------|------------------------------------|-------------------------------------|
| ftdInitiateVpnSessionCheckAction               | 13:04:00.310 / 13:04:00.317 | PENDING_GET_VPN_SESSION_DETAILS        | @ INITIATE_GET_VPN_SESSION_DETAILS | SUCCESS                             |
| ftdInitiateGetBaseObjectsAction                | 13:04:00.335 / 13:04:00.372 | INITIATE_GET_VPN_SESSION_DETAILS       | @ WAIT_FOR_GET_VPN_SESSION_DETAILS | SUCCESS                             |
| ftdInitiateGetVpnSessionDetailsResponseHandler | 13:10:25.116 / 13:10:25.132 | AWAIT_RESPONSE_FROM_execoutFtdRequests | ERROR                              | FAILURE Error Message / Stack Trace |

| HOOK                                      | TYPE   | TIME                        | RESULT           |
|-------------------------------------------|--------|-----------------------------|------------------|
| DeviceStateMachineClearErrorBeforeHook    | Before | 13:04:00.292 / 13:04:00.302 | clearErrors      |
| AddDeviceNameToStateMachineDebugAfterHook | After  | 13:10:25.142 / 13:10:25.143 | No debug record  |
| DeviceStateMachineSetErrorAfterHook       | After  | 13:10:25.143 / 13:10:25.157 | setErrorOnDevice |

### ワークフロー情報のダウンロード

完全なワークフロー情報をJSONファイルにダウンロードして、TACチームから詳細な分析情報を求められたときに提供できます。この情報をダウンロードするには、デバイスを選択してその [ワークフロー (Workflows) ] ページに移動し、右上隅に表示されるエクスポートボタン をクリックします。

### スタックトレースの生成

解決できないエラーがある場合、TACからスタックトレースのコピーを求められる場合があります。エラーのスタックトレースを収集するには、[スタックトレース (Stack Trace) ] リンク

をクリックし、[スタックトレースのコピー (Copy Stacktrace) ] をクリックして、画面に表示されるスタックをクリップボードにコピーします。



## 第 5 章

# CDO と SecureX を統合する

- [SecureX と CDO \(143 ページ\)](#)

## SecureX と CDO

Cisco SecureX プラットフォームは、広範なシスコの統合型セキュリティポートフォリオとお客様のインフラストラクチャをつなぐことで、一貫した操作性を提供します。これにより可視性が統一され、自動化が実現し、ネットワーク、エンドポイント、クラウド、およびアプリケーションの全体でセキュリティが強化されます。統合プラットフォームでの接続技術により、SecureX は測定可能な分析情報、望ましい成果、比類のないチーム間のコラボレーションを実現します。SecureX の概要とこのプラットフォームが提供する機能の詳細については、「[SecureX について](#)」を参照してください。

SecureX に CDO テナントへのアクセスを許可すると、デバイスの合計数、エラーのあるデバイス、競合のあるデバイス、現在同期していないデバイスの数など、デバイスイベントの概要が表示されます。イベントの概要には、現在適用されているポリシーとそれらのポリシーに関連付けられているオブジェクトの集計を示す 2 番目のウィンドウも表示されます。ポリシーはデバイスタイプによって定義され、オブジェクトはオブジェクトタイプによって識別されます。

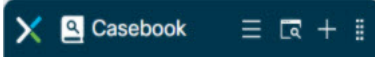
CDO モジュールを SecureX ダッシュボードに追加するには、複数の手順が必要です。詳細については、「[CDO の SecureX への追加](#)」を参照してください。



**警告** CDO アカウントと SecureX アカウントをまだマージしていない場合、導入準備されたすべてのデバイスのイベントを表示できないことがあります。SecureX で CDO モジュールを作成する前に、アカウントをマージすることを強くお勧めします。詳細については、「[CDO アカウントと SecureX アカウントのマージ](#)」を参照してください。



### SecureX のリボン

SecureX のリボンは、SecureX アカウントを作成するかどうかにかかわらず、CDO で使用できます。ページの下部にある SecureX タブ  をクリックして、リボンを展開します。

リボンを使用するには、SecureX アカウントを検証する必要があります。SecureX へのアクセスに使用するのと同じ認証ログインを使用することを強くお勧めします。リボンが認証されると、CDO から直接 SecureX 機能を利用できるようになります。

詳細については、[SecureX リボンのドキュメント](#)を参照してください。

### SecureX のトラブルシューティング

このエクスペリエンスには 2 つの製品が関係します。発生する可能性のある問題の特定、解決、または問い合わせに役立つ「[SecureX のトラブルシューティング \(176 ページ\)](#)」を参照してください。

#### 関連情報：

- [SecureX について](#)
- [CDO アカウントと SecureX アカウントのマージ](#)
- [CDO の SecureX の接続 \(145 ページ\)](#)
- [CDO の SecureX の切断 \(146 ページ\)](#)
- [CDO の SecureX への追加](#)
- [SecureX のトラブルシューティング \(176 ページ\)](#)

## CDO アカウントと SecureX アカウントのマージ

SecureX または Cisco Threat Response (CTR) アカウントをすでにお持ちの場合、デバイスを SecureX に登録するには、CDO アカウントと SecureX/CTR アカウントをマージする必要があります。アカウントは、SecureX ポータルにマージできます。CDO モジュールを作成する前に、アカウントをマージすることを強く推奨します。アカウントがマージされるまで、デバイスのイベントを SecureX で表示したり、他の SecureX 機能を利用したりすることはできません。

手順については、SecureX の「[アカウントのマージ](#)」を参照してください。



(注) 複数の地域クラウドに異なるアカウントがある場合は、地域クラウドごとに個別にアカウントをマージする必要があります。

#### 関連情報：

- [SecureX と CDO](#)

- [CDO の SecureX への追加](#)
- [SecureX のトラブルシューティング](#)

## CDO の SecureX への追加

SecureX が登録済みデバイスにアクセスできるようにし、CDO モジュールを SecureX ダッシュボードに追加して、セキュリティポートフォリオ内の他のシスコプラットフォームとともにデバイスポリシーとオブジェクトの概要を表示します。

### はじめる前に

CDO で SecureX を接続する前に、次のアクション項目を確認することを強くお勧めします。

- SecureX アカウントの管理者以上である必要があります。
- CDO テナントの SuperAdmin ユーザーロールを保有している必要があります。
- テナントの通信を容易にするために、Security Service Exchange (SSE) でテナントアカウントをマージします。詳細については、「[CDO アカウントと SecureX アカウントのマージ](#)」を参照してください。
- まだマージしていない場合は、Cisco Secure Sign-On を SAML シングルサインオン ID プロバイダー (IdP) として設定し、Duo Security を多要素認証 (MFA) 用に設定します。CDO と SecureX では、認証方式として多要素認証が使用されます。詳細については、「[SAML シングルサインオンと Cisco Defense Orchestrator の統合](#)」を参照してください。



(注) 注：複数のテナントがある場合は、SecureX でテナントごとに 1 つのモジュールを作成する必要があります。各テナントには、承認用の一意の API トークンが必要です。

## CDO の SecureX の接続

SecureX アカウントと CDO アカウントをマージした後、2 つのプラットフォーム間の通信を認可し、CDO モジュールが SecureX ダッシュボードに追加されるように手動で有効にする必要があります。CDO UI を介して SecureX に接続し、デバイスのポリシー、イベントタイプ、オブジェクトなどの概要を、セキュリティポートフォリオに含まれる他のシスコプラットフォームとともに表示します。



(注) SecureX ダッシュボードで CDO モジュールがすでに設定されている場合、[テナントを SecureX に接続 (Connect Tenant to SecureX)] オプションにより、重複した CDO モジュールが作成されます。この問題が発生した場合は、「[SecureX のトラブルシューティング](#)」詳細を参照してください。

次の手順を使用して、CDO から API トークンを取得し、CDO モジュールを SecureX に追加します。

- 
- ステップ 1 CDO にログインします。
  - ステップ 2 右上隅のユーザーメニューから、[設定] を選択します。
  - ステップ 3 ウィンドウの左側にある [全般設定 (General Settings) ] タブを選択します。
  - ステップ 4 [テナント設定] セクションを見つけて、[SecureX の接続 (Connect SecureX) ] をクリックします。ブラウザウィンドウが SecureX のログインページにリダイレクトします。CDO テナントに関連付ける組織のログイン情報を使用して SecureX にログインします。
  - ステップ 5 SecureX に正常にログインすると、ブラウザは自動的に CDO にリダイレクトします。[全般設定 (General Settings) ] ページの [ユーザー管理 (User Management) ] タブに、SecureX へのログインに使用した組織の名称を含む新しいユーザーが表示されます。このユーザーは読み取り専用で、SecureX にデータを送信するためにのみ使用されます。
- 

## CDO の SecureX の切断

CDO と SecureX 組織の間の通信リクエストを切断することができます。このオプションでは、SecureX の組織は削除されませんが、CDO から読み取り専用 API ユーザーが削除され、SecureX 組織に関連付けられていたテナントがイベントレポートの送信を停止します。


なお、これにより、CDO の SecureX リボンからテナントがログアウトしたり、リボンが無効になることはありません。リボンからログアウトするには、[Support Case Manager](#) でケースを開いてリボンのログインを手動でリセットする必要があります。このリクエストにより、テナントがリボンからログアウトします。

- 
- ステップ 1 CDO にログインします。
  - ステップ 2 右上隅のユーザーメニューから、[設定] を選択します。
  - ステップ 3 ウィンドウの左側にある [全般設定 (General Settings) ] タブを選択します。
  - ステップ 4 [テナント設定] セクションを見つけて、[SecureX の切断 (Disconnect SecureX) ] をクリックします。[全般設定 (General Settings) ] ページの [ユーザー管理 (User Management) ] タブで、SecureX にデータを送信するために作成された読み取り専用ユーザーが削除されます。
- 

## CDO タイルの SecureX への追加

CDO モジュールを有効にしたら、CDO タイルを SecureX ダッシュボードに追加できます。製品のモジュールは、CDO からのステータス情報にアクセスし、選択可能な 2 つのタイルを介してダッシュボードにデータを報告します。

次の手順を使用して、CDO タイルを SecureX ダッシュボードに追加します。

**ステップ 1** SecureX の [ダッシュボード (Dashboard) ] タブ  で、[新しいダッシュボード (New Dashboard) ] をクリックします。SecureX ダッシュボードに初めてアクセスする場合は、[タイルの追加 (Add Tiles) ] をクリックすることもできます。

**ステップ 2** (任意) ダッシュボードの名前を変更します。

**ヒント** 複数のテナントがある場合は、この名前変更オプションを使用して、CDO タイルが関連付けられているテナントを識別します。

**ステップ 3** [使用可能なタイル (Available Tiles) ] のリストから CDO を選択し、オプションを展開して使用可能なタイルを表示します。ダッシュボードに含めるタイルをすべて選択します。

- [CDO デバイスの概要 (CDO Device Summary) ] : このタイルには、CDO テナントに現在導入準備されているすべてのデバイスとそのステータスの一覧が表示されます。
- [CDO オブジェクトとポリシー (CDO Objects and Policies) ] : このタイルには、デバイスに現在適用されているすべてのポリシーと、それらのポリシーに関連付けられているオブジェクトの一覧が表示されます。

(注) CDO の一覧が表示されない場合、SecureX には CDO からの有効な API トークンが保存されていません。詳細については、[CDO タイルの SecureX への追加](#) ことに関するトピックを参照してください。

**ステップ 4** [保存 (Save) ] をクリックします。

**関連情報 :**

- [CDO アカウントと SecureX アカウントのマージ](#)
- [SecureX のトラブルシューティング](#)





## 第 6 章

# トラブルシューティング

この章は、次のセクションで構成されています。

- [Secure Device Connector のトラブルシューティング](#) (149 ページ)
- [CDO のトラブルシューティング](#) (153 ページ)
- [デバイスの接続状態](#) (162 ページ)
- [SecureX のトラブルシューティング](#) (176 ページ)

## Secure Device Connector のトラブルシューティング

オンプレミスの Secure Device Connector (SDC) のトラブルシューティングを行うには、以下のトピックを参照してください。

これらのシナリオのいずれにも当てはまらない場合は、[TAC でサポートチケットを開く](#)。

### SDC に到達不能

CDO からの 2 回のハートビート要求に連続して応答しなかった場合、SDC の状態は [到達不能 (Unreachable)] になります。SDC に到達不能な場合、テナントは、導入準備したどのデバイスとも通信できません。

CDO は、次の方法で SDC に到達不能であることを示します。

- 「一部の Secure Device Connector (SDC) に到達できません。該当する SDC に関連付けられたデバイスとは通信できません (Some Secure Device Connectors (SDC) are unreachable. You will not be able to communicate with devices associated with these SDCs)」というメッセージが CDO のホームページに表示されます。
- [セキュアコネクタ (Secure Connectors)] ページの SDC のステータスが [到達不能 (Unreachable)] になります。

この問題を解決するには、まず SDC とテナントの再接続を試行してください。

1. SDC 仮想マシンが実行中で、地域の CDO IP アドレスに到達できることを確認します。  
「[Cisco Defense Orchestrator の管理対象デバイスへの接続 \(5 ページ\)](#)」を参照してください。
2. ハートビートを手動で要求して、CDO と SDC の再接続を試行します。SDC がハートビート要求に応答すると、[アクティブ (Active)] ステータスに戻ります。ハートビートを手動で要求するには、次の手順に従います。
  1. 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。
  2. 到達不能な SDC をクリックします。
  3. [操作 (Actions)] ウィンドウで、[ハートビートの要求 (Request heartbeat)] をクリックします。
  4. [再接続 (Reconnect)] をクリックします。
3. SDC を手動でテナントに再接続しようとしても、SDC が [アクティブ (Active)] ステータスに戻らない場合は、「[展開後 CDO で SDC ステータスがアクティブにならない \(150 ページ\)](#)」の指示に従ってください。

## 展開後 CDO で SDC ステータスがアクティブにならない

展開して約 10 分たっても SDC がアクティブになったことを CDO が示さない場合は、SDC の展開時に作成した cdo ユーザーおよびパスワードにより、SSH を使用して SDC VM に接続します。

---

**ステップ 1** /opt/cdo/configure.log を確認します。ここには、入力した SDC の構成設定と、それらが正常に適用されたかどうかを示されます。セットアッププロセスでエラーが発生している場合または値が正しく入力されていない場合は、`sdc-onboard setup` を再度実行します。

- a) `[cdo@localhost cdo]$` プロンプトで、`sudo sdc-onboard setup` と入力します。
- b) cdo ユーザーのパスワードを入力します。
- c) プロンプトに従います。セットアップスクリプトの指示に従って、セットアップウィザードで行ったすべての設定手順を確認し、入力した値を変更することができます。

**ステップ 2** ログを確認し、`sudo sdc-onboard setup` を実行しても、SDC がアクティブになったことを CDO が示さない場合は、[Cisco Defense Orchestrator サポートへの連絡](#)。

---

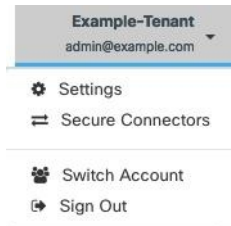
## SDC の変更した IP アドレスが CDO に反映されない

SDC の IP アドレスを変更した場合、GMT の午前 3 時以降まで変更は CDO に反映されません。

## デバイスと SDC の接続に関するトラブルシューティング

このツールを使用して、Secure Device Connector (SDC) を介した CDO からデバイスへの接続をテストします。デバイスが導入準備に失敗した場合、または導入準備の前に CDO がデバイスに到達できるかどうかを判断する場合は、この接続をテストすることができます。

**ステップ 1** [アカウント (Account) ]メニューをクリックし、[セキュアコネクタ (Secure Connectors) ]を選択します。



**ステップ 2** SDC を選択します。

**ステップ 3** 右側の [トラブルシューティング (Troubleshooting) ] ペインで、[デバイスの接続 (Device Connectivity) ] をクリックします。

**ステップ 4** トラブルシューティングまたは接続しようとしているデバイスの有効な IP アドレスまたは FQDN とポート番号を入力し、[実行 (Go) ] をクリックします。CDO は次の検証を実行します。

- a) [DNS 解決 (DNS Resolution) ] : IP アドレスの代わりに FQDN を指定すると、SDC がドメイン名を解決でき、IP アドレスを取得できることを確認します。
- b) [接続テスト (Connection Test) ] : デバイスが到達可能であることを確認します。
- c) [TLS サポート (TLS support) ] : デバイスと SDC の両方がサポートする TLS バージョンと暗号を検出します。
  - [サポートされていない暗号 (Unsupported Cipher) ] : デバイスと SDC の両方でサポートされている TLS バージョンがない場合、CDO は、SDC ではなくデバイスでサポートされている TLS バージョンと暗号についてもテストします。
- d) SSL 証明書 : トラブルシューティングでは、証明書情報が提供されます。

**ステップ 5** デバイスの導入準備またはデバイスへの接続の問題が解消しない場合は、[Cisco Defense Orchestrator サポートへの連絡](#)。

## Secure Device Connector に影響を与えるコンテナ特権昇格の脆弱性 : cisco-sa-20190215-runc

Cisco Product Security Incident Response Team (PSIRT) は、Docker の重大度の高い脆弱性について説明するセキュリティアドバイザリ [cisco-sa-20190215-runc](#) を公開しました。脆弱性の完全な説明については、[PSIRT チームのアドバイザリ全体をお読みください](#)。

この脆弱性は、すべての CDO ユーザーに影響します。



- CDO のクラウド展開された Secure Device Connector (SDC) を使用しているお客様は、CDO 運用チームによってすでに修復手順が実行されているため、何もする必要はありません。
- オンプレミスで展開された SDC を使用しているお客様は、最新の Docker バージョンを使用するように SDC ホストをアップグレードする必要があります。アップグレードするには、次の手順を使用します。
  - [CDO 標準の SDC ホストの更新 \(152 ページ\)](#)
  - [カスタム SDC ホストを更新する \(153 ページ\)](#)
  - [バグトラッキング \(153 ページ\)](#)

## CDO 標準の SDC ホストの更新

CDO の VM イメージを使用した Secure Device Connector の展開した場合は、次の手順を使用します。

**ステップ 1** SSH またはハイパーバイザコンソールを使用して SDC ホストに接続します。

**ステップ 2** 次のコマンドを実行して、Docker サービスのバージョンを確認します。

```
docker version
```

**ステップ 3** 最新の仮想マシン (VM) のいずれかを実行している場合、次のような出力が表示されます。

```
> docker version
Client:
 Version: 18.06.1-ce
 API version: 1.38
 Go version: go1.10.3
 Git commit: e68fc7a
 Built: Tue Aug 21 17:23:03 2018
 OS/Arch: linux/amd64
 Experimental: false
```

ここで古いバージョンが表示される可能性があります。

**ステップ 4** 次のコマンドを実行して Docker を更新し、サービスを再起動します。

```
> sudo yum update docker-ce
> sudo service docker restart
```

(注) Docker サービスの再起動中、CDO とデバイス間の接続が短時間停止します。

**ステップ 5** docker version コマンドを再度実行します。次の出力が表示されます。

```
> docker version
Client:
 Version: 18.09.2
 API version: 1.39
 Go version: go1.10.6
 Git commit: 6247962
 Built: Sun Feb XX 04:13:27 2019
 OS/Arch: linux/amd64
 Experimental: false
```

**ステップ 6** これで追加されました。パッチが適用された最新バージョンの Docker にアップグレードされました。

## カスタム SDC ホストを更新する

独自の SDC ホストを作成している場合は、Docker のインストール方法に基づいた更新手順に従う必要があります。CentOS、yum、Docker-ce（コミュニティ版）を使用した場合は、前述の手順で動作します。

Docker-ee（エンタープライズ版）をインストールした場合、または別の方法を使用して Docker をインストールした場合は、Docker の修正バージョンが異なる場合があります。正しいインストールバージョンは、Docker のページ（[Docker Security Update and Container Security Best Practices](#)）で確認できます。

## バグトラッキング

シスコでは、この脆弱性を引き続き評価し、追加情報が利用可能になりしだい、アドバイザリを更新します。アドバイザリに最終とマーキングされた後は、詳細については次の関連 Cisco Bug を参照してください。

[CSCvo33929-CVE-2019-5736](#) : runC コンテナのブレイクアウト

# CDO のトラブルシューティング

## 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。

## 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](#)（59 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。

## アクセスと証明書のトラブルシューティング

### 新規フィンガープリントを検出状態の解決

**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** [新しいフィンガープリントを検出] 状態のデバイスを選択します。

**ステップ 5** [新しいフィンガープリントを検出] ペインで [フィンガープリントの確認] をクリックします。

**ステップ 6** フィンガープリントを確認して承認するように求められたら、以下の手順を実行します。

1. [フィンガープリントのダウンロード] をクリックして確認します。
2. フィンガープリントに問題がなければ [承認] をクリックします。問題がある場合は、[キャンセル] をクリックします。

**ステップ 7** 新しいフィンガープリントの問題を解決した後、デバイスの接続状態が [オンライン] と表示され、構成ステータスが [非同期] または [競合検出] と表示される場合があります。[構成の競合の解決] を確認し、CDO とデバイス間の構成の差異を確認して解決します。 [設定の競合の解決 \(128 ページ\)](#)

## Security and Analytics Logging イベントを使用したネットワーク問題のトラブルシューティング

これは、イベントビューアを使用してネットワークの問題をトラブルシューティングするための基本的なフレームワークです。

このシナリオでは、ネットワーク運用チームが、ユーザーがネットワーク上のリソースにアクセスできないという報告を受け取ったと想定しています。問題とその場所を報告しているユーザーに基づいて、ネットワーク運用チームは、どのファイアウォールがユーザーによるリソースへのアクセスを制御しているかを把握しています。



(注) また、このシナリオでは、ネットワークトラフィックを管理するファイアウォールが FTD デバイスであると想定しています。Security Analytics and Logging は、他のデバイスタイプからロギング情報を収集しません。

- ステップ 1 ナビゲーションウィンドウで、[モニタリング]>[イベントロギング]をクリックします。
- ステップ 2 [履歴] タブをクリックします。
- ステップ 3 [時間範囲] によるイベントのフィルタ処理を開始します。デフォルトでは、[履歴] タブには過去 1 時間のイベントが表示されます。それが正しい時間範囲である場合は、現在の日付と時刻を [終了] 時刻として入力します。それが正しい時間範囲でない場合は、報告された問題の時間を含む開始時間と終了時間を入力します。
- ステップ 4 [センサーID] フィールドに、ユーザーのアクセスを制御していると考えられるファイアウォールの IP アドレスを入力します。ファイアウォールが複数の可能性がある場合は、検索バーで属性:値のペアを使用してイベントをフィルタ処理します。2つのエントリを作成し、それらを OR ステートメントで結合します。  
例: SensorID:192.168.10.2 OR SensorID:192.168.20.2。
- ステップ 5 イベントフィルタバーの [送信元IP] フィールドにユーザーの IP アドレスを入力します。
- ステップ 6 ユーザーがリソースにアクセスできない場合は、そのリソースの IP アドレスを [接続先IP] フィールドに入力します。
- ステップ 7 結果に表示されるイベントを展開し、その詳細を確認します。以下に表示される詳細の一部を示します。
  - **AC\_RuleAction** : ルールがトリガーされたときに実行されたアクション (許可、信頼、ブロック)。
  - **FirewallPolicy** : イベントをトリガーしたルールが存在するポリシー。
  - **FirewallRule** : イベントをトリガーしたルールの名前。値が Default Action の場合、イベントをトリガーしたのはポリシーのデフォルトアクションであり、ポリシー内のルールの 1 つではありません。
  - **UserName** : イニシエータの IP アドレスに関連づけられたユーザー。イニシエータ IP アドレスは送信元 IP アドレスと同じです。
- ステップ 8 ルールのアクションがアクセスを妨げている場合は、[FirewallRule] フィールドと [FirewallPolicy] フィールドを確認して、アクセスをブロックしているポリシー内のルールを特定します。

## SSL 暗号解読の問題のトラブルシューティング

復号再署名がブラウザでは機能するがアプリでは機能しないWebサイトの処理（SSLまたは認証局ピンング）

スマートフォンおよびその他のデバイス用の一部のアプリケーションでは「SSL（または認証局）ピンング」と呼ばれる手法が使用されます。SSLピンング手法では、元のサーバー証明書のハッシュがアプリケーション自体の内部に埋め込まれます。その結果、アプリケーションが再署名された証明書を Firepower Threat Defense デバイスから受け取ると、ハッシュ検証に失敗し、接続が中断されます。

Webサイトのアプリケーションを使用してそのサイトに接続することができないにもかかわらず、Webブラウザを使用する場合は、接続に失敗したアプリケーションを使用したデバイス上のブラウザでも接続できるというのが主な症状です。たとえば、FacebookのiOSまたはAndroidアプリケーションを使用すると接続に失敗しますが、SafariまたはChromeで <https://www.facebook.com> を指定すると接続に成功します。

SSLピンングは特に中間者攻撃を回避するために使用されるため、回避策はありません。次のいずれかの選択肢を使用する必要があります。

### 詳細の表示

サイトがブラウザでは機能するのに同じデバイス上のアプリケーションでは機能しない場合は、ほぼ確実にSSLピンングによるものと考えられます。ただし、詳しく調べる必要がある場合は、ブラウザのテストに加えて、接続イベントを使用してSSLピンングを識別できます。

アプリケーションは、次の2つの方法でハッシュ検証の失敗に対処する場合があります。

- グループ1のアプリケーション（Facebookなど）は、サーバからSH、CERT、SHDメッセージを受け取るとすぐにSSLALERTメッセージを送信します。アラートは、通常、SSLピンングを示す「Unknown CA (48)」アラートです。アラートメッセージの後にTCPリセットが送信されます。イベントの詳細情報で次のような症状が見られます。
  - SSL フロー フラグには ALERT\_SEEN が含まれます。
  - SSL フロー フラグには APP\_DATA\_C2S または APP\_DATA\_S2C は含まれません。
  - SSL フロー メッセージは、通常、CLIENT\_HELLO、SERVER\_HELLO、SERVER\_CERTIFICATE、SERVER\_KEY\_EXCHANGE、SERVER\_HELLO\_DONE です。
- グループ2のアプリケーション（Dropboxなど）はアラートを送信しません。代わりに、ハンドシェイクが完了するまで待ってからTCPリセットを送信します。イベントで次のような症状が見られます。
  - SSL フロー フラグには ALERT\_SEEN、APP\_DATA\_C2S または APP\_DATA\_S2C は含まれません。
  - SSL フロー メッセージは、通常、CLIENT\_HELLO、SERVER\_HELLO、SERVER\_CERTIFICATE、SERVER\_KEY\_EXCHANGE、SERVER\_HELLO\_DONE、CLIENT\_KEY\_EXCHANGE、CLIENT\_CHANGE\_CIPHER\_SPEC、CLIENT\_FINISHED、SERVER\_CHANGE\_CIPHER\_SPEC、SERVER\_FINISHED です。

## 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 (59 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。


## オブジェクトのトラブルシューティング

### 重複オブジェクトの問題の解決

重複オブジェクト<sup>④</sup>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誤って作成され、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。重複オブジェクトの問題を解決した後、CDO は、影響を受けるすべてのオブジェクト参照を残されたオブジェクト名で更新します。

重複オブジェクトの問題を解決するには以下の手順を実行します。

- ステップ 1** [オブジェクト]ページを開き、オブジェクトを [フィルタ処理](#) して、重複オブジェクトの問題を見つけます。
- ステップ 2** 結果の中から1つを選択します。オブジェクトの詳細パネルに、該当する重複の数を示す [重複] フィールドが表示されます。

 DUPLICATE **2** [Resolve](#) | [Ignore](#)

**ステップ3** [解決 (Resolve)] をクリックします。CDO は、重複オブジェクトを比較できるように表示します。


**ステップ4** 比較するオブジェクトを2つ選択します。

**ステップ5** 以下のオプションがあります。

- オブジェクトの1つを別のオブジェクトで置き換える場合は、保持するオブジェクトで[選択]をクリックし、[解決] をクリックして影響を受けるデバイスとネットワークポリシーを確認し、変更の問題がなければ[確認] をクリックします。CDO は、選択したオブジェクトに置き換えて保持し、重複を削除します。
- リストにあるオブジェクトを無視する場合は、[無視] をクリックします。オブジェクトを無視すると、CDO が表示する重複オブジェクトのリストから削除されます。
- オブジェクトを保持するものの、重複オブジェクトの検索で CDO がそれを検出しないようにするには、[すべて無視] をクリックします。

**ステップ6** 重複オブジェクトの問題が解決したら、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。

## 未使用オブジェクトの問題の解決

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。

関連情報：


- [デバイスとサービスのリストのエクスポート \(75 ページ\)](#)
- [CDO へのデバイス一括再接続 \(79 ページ\)](#)

## 未使用オブジェクトの問題の解決

**ステップ1** メニューバーで[オブジェクト] をクリックし、オブジェクトを[フィルタ処理](#)して、未使用のオブジェクトの問題を見つけます。

**ステップ2** 1つ以上の未使用のオブジェクトを選択します。



**ステップ3** 以下のオプションがあります。

- 操作ウィンドウで [削除]  をクリックして、未使用のオブジェクトを CDO から削除します。
- [問題] ペインで、[無視] をクリックします。オブジェクトを無視すると、CDO は未使用のオブジェクトの結果にそのオブジェクトを表示しなくなります。



**ステップ4** 未使用のオブジェクトを削除した場合は、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 \(118 ページ\)](#)か、待機してから複数の変更を一度に展開します。

- (注) 未使用のオブジェクトの問題を一括で解決するには、「[オブジェクトの問題を一度に解決する](#)」を参照してください。

## 未使用オブジェクトの一括削除

- ステップ 1** [オブジェクト] ページを開き、オブジェクトを[フィルタ処理](#)して、未使用オブジェクトの問題を見つけます。
- ステップ 2** 削除する未使用のオブジェクトを選択します。
- ページ上のすべてのオブジェクトを選択するには、オブジェクトテーブルのヘッダー行にあるチェックボックスをクリックします。
  - オブジェクトテーブルで未使用のオブジェクトを個別に選択します。
- ステップ 3** 右側の [アクション] ペインで [削除]  をクリックして、CDO で選択した未使用のオブジェクトをすべて削除します。99 個のオブジェクトを同時に削除できます。
- ステップ 4** [OK] をクリックして、未使用のオブジェクトを削除することを確認します。
- ステップ 5** これらの変更の展開には、つぎの 2 つの方法があります。
- 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。
  - [デバイスとサービス] ページを開き、変更の影響を受けたデバイスを特定します。変更の影響を受けるすべてのデバイスを選択し、[管理] ペインで [すべて展開 (Deploy All)]  をクリックします。警告を読み、適切なアクションを実行します。

## 不整合オブジェクトの問題を解決する

不整合オブジェクト  INCONSISTENT  [Resolve](#) | [Ignore](#) 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。ユーザーが異なる構成の中で、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。

**注：**不整合オブジェクトの問題を一括で解決するには、「[オブジェクトの問題を一度に解決する](#)」を参照してください。

不整合オブジェクトに対して次のことを実行できます。

- [無視] : CDO は、オブジェクト間の不整合を無視し、それらの値を保持します。このオブジェクトは、不整合カテゴリに表示されなくなります。
- [マージ (Merge)] : CDO は、選択されているすべてのオブジェクトとその値を 1 つのオブジェクトグループに結合します。



- [名前の変更 (Rename)] : CDO で、不整合オブジェクトの一つの名前を変更し、新しい名前を付けることができます。
- [共有ネットワークオブジェクトのオーバーライドへの変換 (Convert Shared Network Objects to Overrides)] : CDO で、不整合のある共有オブジェクトを (オーバーライドの有無にかかわらず)、オーバーライドのある単一の共有オブジェクトに結合できます。不整合オブジェクトの最も一般的なデフォルト値が、新しく形成されるオブジェクトのデフォルトとして設定されます。



(注) 共通のデフォルト値が複数ある場合は、そのうちの一つがデフォルトとして選択されます。残りのデフォルト値とオーバーライド値は、そのオブジェクトのオーバーライドとして設定されます。

- [共有ネットワークグループの追加の値への変換 (Convert Shared Network Group to Additional Values)] : CDO で、不整合のある共有ネットワークグループを、追加の値のある単一の共有ネットワークグループに結合できます。この機能の基準は、「変換される不整合ネットワークグループに、同じ値を持つ少なくとも1つの共通オブジェクトが必要である」というものです。この基準に一致するすべてのデフォルト値がデフォルト値になり、残りのオブジェクトは、新しく形成されるネットワークグループの追加の値として割り当てられます。

たとえば、不整合のある2つの共有ネットワークグループがあるとします。1つ目のネットワークグループ「shared\_network\_group」は、「object\_1」(192.0.2.x)と「object\_2」(192.0.2.y)で形成されています。また、追加の値「object\_3」(192.0.2.a)も含まれています。2つ目のネットワークグループ「shared\_network\_group」は、「object\_1」(192.0.2.x)と追加の値「object\_4」(192.0.2.b)で形成されます。共有ネットワークグループを追加の値に変換すると、新しく形成されるグループ「shared\_network\_group」には、デフォルト値として「object\_1」(192.0.2.x)と「object\_2」(192.0.2.y)が含まれ、追加の値として「object\_3」(192.0.2.a)と「object\_4」(192.0.2.b)が含まれます。



(注) 新しいネットワークオブジェクトを作成すると、CDOは、その値を同じ名前の既存の共有ネットワークオブジェクトへのオーバーライドとして自動的に割り当てます。これは、新しいデバイスがCDOに導入準備される場合にも当てはまります。

自動割り当ては、次の条件が満たされている場合にのみ発生します。

1. 新しいネットワークオブジェクトがデバイスに割り当てられる必要があります。
2. テナントには、同じ名前とタイプの共有オブジェクトが1つだけ存在する必要があります。
3. 共有オブジェクトには、すでにオーバーライドが含まれている必要があります。

不整合オブジェクトの問題を解決するには、次の手順を実行します。

**ステップ 1** [オブジェクト] ページを開き、オブジェクトを **フィルタ処理** して、不整合オブジェクトの問題を見つけます。

**ステップ 2** 不整合オブジェクトを選択します。オブジェクトの詳細パネルに、該当するオブジェクトの数を示す [不整合 (INCONSISTENT) ] フィールドが表示されます。



**ステップ 3** [解決 (Resolve) ] をクリックします。CDO は、不整合オブジェクトを比較できるように表示します。

**ステップ 4** 以下のオプションがあります。

• [すべて無視 (Ignore All) ] :

1. 提示されるオブジェクトを比較し、いずれかのオブジェクトで [無視] をクリックします。または、すべてのオブジェクトを無視するために、[すべて無視 (Ignore All) ] をクリックします。
2. [OK] をクリックして確認します。

• [オブジェクトをマージして解決 (Resolve by merging objects) ] :

1. [Xつのオブジェクトをマージして解決 (Resolve by Merging X Objects) ] をクリックします。
2. [確認 (Confirm) ] をクリックします。

• [名前の変更 (Rename) ] :

1. [名前の変更 (Rename) ] をクリックします。
2. 該当するネットワークポリシーおよびデバイスへの変更を保存し、[確認 (Confirm) ] をクリックします。

• [オーバーライドへの変換 (Convert to Overrides) ] (不整合のある共有オブジェクトの場合) : 共有オブジェクトをオーバーライドと比較する場合、比較パネルには、[不整合のある値 (Inconsistent Values) ] フィールドのデフォルト値のみが表示されます。

1. [オーバーライドへの変換 (Convert to Overrides) ] をクリックします。すべての不整合オブジェクトは、オーバーライドを持つ単一の共有オブジェクトに変換されます。
2. [確認 (Confirm) ] をクリックします。[共有オブジェクトの編集 (Edit Shared Object) ] をクリックすると、新しく形成されたオブジェクトの詳細が表示されます。上向き矢印と下向き矢印を使用して、デフォルトとオーバーライドの間で値を移動することができます。

• [追加の値への変換 (Convert to Additional Values) ] (不整合のあるネットワークグループの場合) :

1. [追加の値への変換 (Convert to Additional Values) ] をクリックします。すべての不整合オブジェクトは、追加の値を持つ単一の共有オブジェクトに変換されます。
2. 該当するネットワークポリシーおよびデバイスへの変更を保存し、[確認 (Confirm) ] をクリックします。

**ステップ 5** 不整合を解決したら、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。

## オブジェクトの問題を一度に解決する

未使用オブジェクトの問題の解決、重複オブジェクトの問題の解決、不整合オブジェクトの問題を解決する (159 ページ) の問題のあるオブジェクトを解決する方法の1つは、それらを見捨てることです。オブジェクトに複数の問題がある場合でも、複数のオブジェクトを選択して見捨てるできます。たとえば、オブジェクトに一貫性がなく、さらに未使用の場合、一度に見捨てる問題タイプは1つだけです。



**重要** 後でオブジェクトが別の問題タイプに関連付けられた場合も、実行した見捨てるアクションは、その時に選択した問題にのみ影響します。たとえば、重複していたためにオブジェクトを見捨てるし、後でそのオブジェクトが不整合としてマークされた場合、そのオブジェクトを重複オブジェクトとして見捨てるしても、不整合のオブジェクトとして見捨てるわけではありません。

問題を一括で見捨てるには、以下の手順に従ってください。

**ステップ 1** [オブジェクト] ページを開きます。検索を絞り込むために、オブジェクトの問題をフィルタ処理できます。

**ステップ 2** オブジェクトテーブルで、見捨てるすべての該当するオブジェクトを選択します。問題ペインでは、問題タイプごとにオブジェクトがグループ化されます。

| Issues       |            |
|--------------|------------|
| Duplicate    | Ignore (4) |
| Inconsistent | Ignore (2) |
| Unused       | Ignore (1) |

**ステップ 3** [見捨てる] をクリックして、問題をタイプ別に見捨てるします。問題タイプごとに個別に見捨てる必要があります。

**ステップ 4** [OK] をクリックして、それらのオブジェクトを見捨てることを確認します。

## デバイスの接続状態

CDO テナントに導入準備されたデバイスの接続状態を表示できます。このトピックは、さまざまな接続状態を理解するのに役立ちます。[デバイスとサービス] ページの [接続 (Connectivity)] カラムに、デバイスの接続状態が表示されます。

デバイスの接続状態が「オンライン」の場合、デバイスの電源がオンになっていて、CDO に接続されていることを意味します。以下の表に記載されているその他の状態は、通常、さまざまな理由でデバイスに問題が発生した場合になります。この表は、このような問題から回復する方法を示しています。接続障害の原因となっている問題が複数ある可能性があります。再接

続を試みると、CDO は、再接続を実行する前に、まずこれらの問題をすべて解決するように求めます。

| デバイスの接続状態                | 考えられる原因                                                                   | 解像度                                               |
|--------------------------|---------------------------------------------------------------------------|---------------------------------------------------|
| オンライン (Online)           | デバイスの電源が入っていて、CDO に接続されています。                                              | NA                                                |
| オフライン                    | デバイスの電源が切れているか、ネットワーク接続が失われています。                                          | デバイスがオフラインかどうかを確認します。                             |
| Insufficient licenses    | デバイスに十分なライセンスがありません。                                                      | <a href="#">ライセンス不足のトラブルシューティング (163 ページ)</a>     |
| クレデンシャルが無効である            | CDO がデバイスに接続するために使用するユーザー名とパスワードの組み合わせが正しくありません。                          | <a href="#">無効なログイン情報のトラブルシューティング (164 ページ)</a>   |
| New Certificate Detected | このデバイスの証明書が変更されました。デバイスが自己署名証明書を使用している場合、これはデバイスの電源を再投入したために発生した可能性があります。 | <a href="#">新規証明書の問題のトラブルシューティング (165 ページ)</a>    |
| オンボーディングエラー              | CDO が導入準備時にデバイスとの接続を失った可能性があります。                                          | <a href="#">オンボーディングエラーのトラブルシューティング (174 ページ)</a> |

## ライセンス不足のトラブルシューティング

デバイスの接続ステータスに[ライセンスが不足しています (Insufficient License) ]と表示される場合は、以下の手順を実行します。

- デバイスがライセンスを取得するまでしばらく待ちます。通常、Cisco Smart Software Manager が新しいライセンスをデバイスに適用するには時間がかかります。
- デバイスのステータスが変わらない場合は、CDO からサインアウトしてから再度サインインすることで CDO ポータルを更新して、ライセンスサーバーとデバイスとの間のネットワーク通信の不具合を解決します。
- ポータルを更新してもデバイスのステータスが変更されない場合は、次の手順を実行します。

- 
- ステップ 1 [Cisco Smart Software Manager](#) から新しいトークンを生成し、コピーします。詳細については、[スマートライセンスの生成](#)に関するビデオをご覧ください。
  - ステップ 2 CDO のナビゲーションバーで、[デバイスとサービス] ページをクリックします。
  - 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、ステータスが [ライセンスが不足しています (Insufficient License) ] 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、[ライセンスが不足しています (Insufficient License) ] に表示される [ライセンスの管理 (Manage Licenses) ] をクリックします。[ライセンスの管理 (Manage Licenses) ] ウィンドウが表示されます。
  - ステップ 6 [アクティブ化 (Activate) ] フィールドで、新しいトークンを貼り付けて [デバイスの登録 (Register Device) ] をクリックします。  
トークンがデバイスに正常に適用されると、接続状態が [オンライン] に変わります。
- 

## 無効なログイン情報のトラブルシューティング

無効なログイン情報によるデバイスの切断を解決するには、次の手順を実行します。

- 
- 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] 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、ステータスが [無効なログイン情報] のデバイスを選択します。
  - ステップ 4 [デバイスの詳細] ペインで、[無効なログイン情報] に表示される [再接続] をクリックします。CDO がデバイスとの再接続を試行します。
  - ステップ 5 デバイスの新しいユーザー名とパスワードの入力を求められたら、
  - ステップ 6 [続行 (Continue) ] をクリックします。
  - ステップ 7 デバイスがオンラインになり、使用できる状態になったら、[閉じる] をクリックします。
  - ステップ 8 CDO がデバイスへの接続に間違ったログイン情報を使用しようとしたため、デバイスへの接続に CDO が使用するユーザー名とパスワードの組み合わせが、デバイス上で直接変更された可能性があります。デバイスは「オンライン」ですが、構成ステータスは [競合が検出されました] であることがわかります。[構成の競合の解決] を使用して、CDO とデバイス間の構成の差異を確認して解決します。[設定の競合の解決 \(128 ページ\)](#)
-

## 新規証明書の問題のトラブルシューティング

### CDO での証明書の使用

CDO は、デバイスに接続するときに証明書の有効性をチェックします。具体的には、CDO は次のことを要求します。

1. デバイスで TLS バージョン 1.0 以降を使用している。
2. デバイスにより提示される証明書が有効期限内であり、発効日が過去の日付である（すなわち、すでに有効になっており、後日に有効化されるようにスケジュールされていない）。
3. 証明書は、SHA-256 証明書であること。SHA-1 証明書は受け入れられません。
4. 次のいずれかが該当すること。
  - デバイスは自己署名証明書を使用し、その証明書は認可されたユーザーにより信頼された最新の証明書と同じである。
  - デバイスは、信頼できる認証局（CA）が署名した証明書を使用し、提示されたリーフ証明書から関連 CA にリンクしている証明書チェーンを形成している。

これらは、ブラウザとは異なる CDO の証明書の使用方法です。

- 自己署名証明書の場合、CDO は、デバイスの導入準備または再接続時に、ドメイン名チェックを無効にして、代わりに、その証明書が承認ユーザーによって信頼された証明書と完全に一致することをチェックします。
- CDO は、まだ内部 CA をサポートしていません。現時点では、内部 CA によって署名された証明書をチェックする方法はありません。

ASA デバイスの証明書チェックを、デバイスごとに無効にすることができます。ASA の証明書を CDO が信頼できない場合、そのデバイスの証明書チェックを無効にするオプションがあります。デバイスの証明書チェックの無効化を試みても依然としてデバイスを導入準備できない場合は、デバイスに関して指定した IP アドレスおよびポートが正しくないか到達可能ではない可能性があります。証明書チェックをグローバルに無効にする方法、またはサポートされている証明書を持つデバイスの証明書チェックを無効にする方法はありません。非 ASA デバイスの証明書チェックを無効にする方法はありません。

デバイスの証明書チェックを無効にしても、CDO は、引き続き TLS を使用してデバイスに接続しますが、接続の確立に使用される証明書を検証しません。つまり、パッシブ中間者攻撃者は接続を盗聴できませんが、アクティブ中間攻撃者は、無効な証明書を CDO に提供することによって、接続を傍受する可能性があります。

### 証明書の問題の特定

いくつかの理由で CDO がデバイスを導入準備できない場合があります。UI に「CDO cannot connect to the device using the certificate presented」というメッセージが表示される場合は、証明書に問題があります。このメッセージが UI に表示されない場合は、問題が接続の問題（デバ

イスに到達できない) またはその他のネットワークエラーに関連している可能性が高くなります。

CDO が特定の証明書を拒否する理由を判断するには、SDC ホスト、または関連デバイスに到達できる別のホストで、**openssl** コマンドラインツールを使用します。次のコマンドを使用して、デバイスによって提示された証明書を示すファイルを作成します。

```
openssl s_client -showcerts -connect <host>:<port> && <filename>.txt
```

このコマンドでは、対話型セッションが開始されるため、数秒後に **Ctrl+C** キーを押して終了する必要があります。

次のような出力を含むファイルが作成されます。

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = *.google.com
verify return:1 CONNECTED(00000003)

Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
 i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMakGA1UE
...lots of base64...
tzw9TylihJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
 i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTA1VT
...lots of base64...
tzw9TylihJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
 i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTA1VT
...lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----

Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2

No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits

SSL handshake has read 4575 bytes and written 434 bytes

New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
 Protocol : TLSv1.2
 Cipher : ECDHE-RSA-AES128-GCM-SHA256
```

```

Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB
Session-ID-ctx:
Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

Key-Arg : None
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 100800 (seconds)
TLS session ticket:
0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de z.T..H~v0s...@[.
0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c .S..A6f>[5...o].
0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6 K..o....1[.eo..
0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28 q=.S.)A.....3(
0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36 ..n....c...c.d.6
0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d "...Y...!\...R(E.
0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d r..#...|....+.B.
0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de #5m.}.9...I.....
0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45 ...^E.|.k.x.I..E
0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63 n.$..E.A....J.6.c
00a0 - 72 a4 ad
00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)

```

この出力では、最初に、**確認リターン (verify return)** コードが示されている最後の行に注目してください。証明書に関する問題が存在する場合、このリターンコードはゼロ以外になり、エラーの説明が表示されます。

この証明書エラーコードのリストを展開して、一般的なエラーとその修正方法を確認してください。

0 X509\_V\_OK : 操作が成功しました。

2 X509\_V\_ERR\_UNABLE\_TO\_GET\_ISSUER\_CERT : 信頼できない証明書の発行者証明書が見つかりませんでした。

3 X509\_V\_ERR\_UNABLE\_TO\_GET\_CRL : 証明書の CRL が見つかりませんでした。

4 X509\_V\_ERR\_UNABLE\_TO\_DECRYPT\_CERT\_SIGNATURE : 証明書の署名を暗号解読できませんでした。これは、実際の署名値が、期待値と一致しないのではなく、判別できなかったことを意味します。これは、RSA キーについてのみ意味を持ちます。

5 X509\_V\_ERR\_UNABLE\_TO\_DECRYPT\_CRL\_SIGNATURE : CRL の署名を暗号解読できませんでした。これは、実際の署名値が、期待値と一致しないのではなく、判別できなかったことを意味します。未使用。

6 X509\_V\_ERR\_UNABLE\_TO\_DECODE\_ISSUER\_PUBLIC\_KEY : 証明書 SubjectPublicKeyInfo の公開キーを読み取れませんでした。

7 X509\_V\_ERR\_CERT\_SIGNATURE\_FAILURE : 証明書の署名が無効です。

8 X509\_V\_ERR\_CRL\_SIGNATURE\_FAILURE : 証明書の署名が無効です。

9 X509\_V\_ERR\_CERT\_NOT\_YET\_VALID : 証明書がまだ有効ではありません (notBefore の日付が現在時刻より後です)。詳細については、この後の「**確認リターンコード : 9 (証明書がまだ有効ではありません)**」を参照してください。



10 X509\_V\_ERR\_CERT\_HAS\_EXPIRED : 証明書の有効期限が切れています (notAfter の日付が現在時刻より前です)。詳細については、この後の「[確認リターンコード：10 \(証明書の有効期限が切れています\)](#)」を参照してください。

11 X509\_V\_ERR\_CRL\_NOT\_YET\_VALID : CRL がまだ有効ではありません。

12 X509\_V\_ERR\_CRL\_HAS\_EXPIRED : CRL の有効期限が切れています。

13 X509\_V\_ERR\_ERROR\_IN\_CERT\_NOT\_BEFORE\_FIELD : 証明書の notBefore フィールドに無効な時刻が含まれています。

14 X509\_V\_ERR\_ERROR\_IN\_CERT\_NOT\_AFTER\_FIELD : 証明書の notAfter フィールドに無効な時刻が含まれています。

15 X509\_V\_ERR\_ERROR\_IN\_CRL\_LAST\_UPDATE\_FIELD : CRL の lastUpdate フィールドに無効な時刻が含まれています。

16 X509\_V\_ERR\_ERROR\_IN\_CRL\_NEXT\_UPDATE\_FIELD : CRL の nextUpdate フィールドに無効な時刻が含まれています。

17 X509\_V\_ERR\_OUT\_OF\_MEM : メモリを割り当てようとしてエラーが発生しました。これは決して発生しないはずの問題です。

18 X509\_V\_ERR\_DEPTH\_ZERO\_SELF\_SIGNED\_CERT : 渡された証明書は自己署名済みであり、信頼できる証明書のリストに同じ証明書が見つかりません。

19 X509\_V\_ERR\_SELF\_SIGNED\_CERT\_IN\_CHAIN : 信頼できない証明書を使用して証明書チェーンを構築できましたが、ルートがローカルで見つかりませんでした。

20 X509\_V\_ERR\_UNABLE\_TO\_GET\_ISSUER\_CERT\_LOCALLY : ローカルでルックアップされた証明書の発行者証明書が見つかりませんでした。これは、通常、信頼できる証明書のリストが完全ではないことを意味します。

21 X509\_V\_ERR\_UNABLE\_TO\_VERIFY\_LEAF\_SIGNATURE : チェーンに証明書が1つしか含まれておらず、それが自己署名済みでないため、署名を検証できませんでした。詳細については、この後の「[確認リターンコード：21 \(最初の証明書を検証できません\)](#)」を参照してください。詳細については、この後の「[確認リターンコード：21 \(最初の証明書を検証できません\)](#)」を参照してください。

22 X509\_V\_ERR\_CERT\_CHAIN\_TOO\_LONG : 証明書チェーンの長さが、指定された最大深度を超えています。未使用。

23 X509\_V\_ERR\_CERT\_REVOKED : 証明書が失効しています。

24 X509\_V\_ERR\_INVALID\_CA : CA 証明書が無効です。CA ではないか、その拡張領域が、提供された目的と一致していません。

25 X509\_V\_ERR\_PATH\_LENGTH\_EXCEEDED : basicConstraints の pathlength パラメータを超えています。

26 X509\_V\_ERR\_INVALID\_PURPOSE : 提供された証明書を、指定された目的に使用できません。

27 X509\_V\_ERR\_CERT\_UNTRUSTED : ルート CA が、指定された目的に関して信頼できるものとしてマークされていません。

- 28 X509\_V\_ERR\_CERT\_REJECTED : ルート CA が、指定された目的を拒否するようにマークされています。
- 29 X509\_V\_ERR\_SUBJECT\_ISSUER\_MISMATCH : 件名が現在の証明書の発行者名と一致しないため、現在の候補発行者証明書が拒否されました。-issuer\_checks オプションが設定されている場合にのみ表示されます。
- 30 X509\_V\_ERR\_AKID\_SKID\_MISMATCH : 件名キー識別子が存在し、現在の証明書の認証局キー識別子と一致しないため、現在の候補発行者証明書が拒否されました。-issuer\_checks オプションが設定されている場合にのみ表示されます。
- 31 X509\_V\_ERR\_AKID\_ISSUER\_SERIAL\_MISMATCH : 発行者名とシリアル番号が存在し、現在の証明書の認証局キー識別子と一致しないため、現在の候補発行者証明書が拒否されました。-issuer\_checks オプションが設定されている場合にのみ表示されます。
- 32 X509\_V\_ERR\_KEYUSAGE\_NO\_CERTSIGN : keyUsage 拡張領域が証明書の署名を許可していないため、現在の候補発行者証明書が拒否されました。
- 50 X509\_V\_ERR\_APPLICATION\_VERIFICATION : アプリケーション固有のエラーです。未使用。

#### 「New Certificate Detected」メッセージ

自己署名証明書を持つデバイスをアップグレードして、アップグレードプロセス後に新しい証明書が生成された場合、CDO で、[設定 (Configuration)] ステータスと [接続 (Connectivity)] ステータスの両方として、「新しい証明書が検出されました (New Certificate Detected)」というメッセージが生成されることがあります。このデバイスを引き続き CDO から管理するには、この問題を手動で確認して解決する必要があります。証明書が同期されて、デバイスの状態が正常になったら、このデバイスを管理できます。



- (注) 複数の管理対象デバイスを CDO に同時に **CDO へのデバイス一括再接続** すると、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。

新しい証明書を解決するには、次の手順を使用します。

1. [デバイスとサービス (Device & Services)] ページに移動します。
2. フィルタを使用して、接続ステータスまたは設定ステータスが [新しい証明書が検出されました (New Certificate Detected)] であるデバイスを表示し、必要なデバイスを選択します。
3. [アクション] ペインで、[証明書の確認 (Review Certificate)] をクリックします。CDO では、確認のために証明書をダウンロードし、新しい証明書を受け入れることができます。
4. [デバイス同期 (Device Sync)] ウィンドウで [承認 (Accept)] をクリックするか、[デバイスへの再接続 (Reconnecting to Device)] ウィンドウで [続行] をクリックします。

CDO は、デバイスを新しい自己署名証明書と自動的に同期します。同期されたデバイスを表示するには、[デバイスとサービス] ページを手動で更新する必要がある場合があります。

### 証明書エラーコード

#### 確認リターンコード:0 (OK) (ただし、CDO は証明書エラーを返します)

CDO は、証明書を取得すると、「https://<device\_ip>:<port>」への GET コールを実行することにより、デバイスの URL への接続を試みます。これが機能しない場合、CDO は証明書エラーを表示します。証明書が有効である (openssl が 0 つまり OK を返します) ことがわかった場合、接続しようとしているポートで別のサービスがリスンしている可能性があります。この場合、次のコマンドを使用できます。

```
curl -k -u <username>:<password>
https://<device_id>:<device_port>/admin/exec/show%20version
```

これにより、次のように、ASA と確実に通信しているかどうかを確認することができ、HTTPS サーバーが ASA の正しいポートで動作しているかどうかをチェックすることもできます。

```
show asp table socket
```

| Protocol | Socket   | State  | Local Address   | Foreign Address |
|----------|----------|--------|-----------------|-----------------|
| SSL      | 00019b98 | LISTEN | 192.168.1.5:443 | 0.0.0.0:*       |
| SSL      | 00029e18 | LISTEN | 192.168.2.5:443 | 0.0.0.0:*       |
| TCP      | 00032208 | LISTEN | 192.168.1.5:22  | 0.0.0.0:*       |

#### 確認リターンコード : 9 (証明書がまだ有効ではありません)

このエラーは、提供された証明書の発行日が将来の日付であるため、クライアントがそれを有効なものとして扱わないことを意味します。これは、証明書の不完全な作成が原因である可能性があります。また、自己署名証明書の場合は、証明書生成時のデバイスの時刻が間違っていたことが原因である可能性があります。

エラーには、証明書の notBefore の日付が含まれた行があります。

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=9:certificate is not yet valid
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

このエラーから、証明書がいつ有効になるかを判別できます。

### 修復

証明書の notBefore の日付は過去の日付である必要があります。notBefore の日付をより早い日付にして証明書を再発行できます。この問題は、クライアントまたは発行デバイスのいずれかで時刻が正しく設定されていない場合にも発生する可能性があります。

#### 確認リターンコード : 10 (証明書の有効期限が切れています)

このエラーは、提供された証明書の少なくとも1つの期限が切れていることを意味します。エラーには、証明書の `notBefore` の日付が含まれた行があります。

```
error 10 at 0 depth lookup:certificate has expired
```

この有効期限は、証明書の本文に含まれています。

### 修復

証明書が本当に期限切れの場合、唯一の修復方法は、別の証明書を取得することです。証明書の有効期限が将来の日付であるのに、`openssl` が期限切れであると主張する場合は、コンピュータの日付と時刻をチェックしてください。たとえば、証明書が 2020 年に期限切れになるように設定されているのに、コンピュータの日付が 2021 年になっている場合、そのコンピュータは証明書を期限切れとして扱います。

### 確認リターンコード：21（最初の証明書を検証できません）

このエラーは、証明書チェーンに問題があることと、デバイスによって提示された証明書を信頼できることを `openssl` が検証できないことを示しています。ここで、上記の例の証明書チェーンを調べて、証明書チェーンがどのように機能するのかを見てみましょう。

```

Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2

-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
...lots of base64...
tzw9TyIimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqsMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
...lots of base64...
tzw9TyIimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDervmMA0GCSqGSIb3DQEBCQUAME4xCzAJBgNVBAYTAlVT
...lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1B0oa+Y7mHyhD8S
-----END CERTIFICATE-----
```

証明書チェーンとは、サーバーによって提示される証明書のリストです。このリストは、サーバー自体の証明書から始まり、そのサーバーの証明書を認証局の最上位の証明書に結び付ける、段階的により上位の中間証明書が含まれます。各証明書には、その件名（「s:」で始まる行）とその発行者（「i:」で始まる行）のリストが示されています。

件名は、証明書によって識別されるエンティティです。これには、組織名が含まれており、場合によっては証明書の発行先エンティティの共通名も含まれます。

発行者は、証明書を発行したエンティティです。これには、組織フィールドも含まれており、場合によっては共通名も含まれます。

サーバーは、信頼できる認証局によって直接発行された証明書を持っている場合、証明書チェーンに他の証明書を含める必要がありません。次のような1つの証明書が表示されます。

```
--- Certificate chain 0 s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com
i:/C=US/O=Trusted Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
...lots of base64...
tzw9TylihnhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE----- ---
```

この証明書を提供すると、`openssl` は、**\*.example.com** の ExampleCo 証明書が、`openssl` の組み込み信頼ストアに存在する信頼できる認証局の証明書によって正しく署名されていることを検証します。その検証の後に、`openssl` は、デバイスに正常に接続します。

ただし、ほとんどのサーバーには、信頼できる CA によって直接署名された証明書がありません。代わりに、最初の例のように、サーバーの証明書は1つ以上の中間証明書によって署名されており、最上位の中間証明書が、信頼できる CA によって署名された証明書を持ちます。`OpenSSL` は、デフォルトでは、これらの中間 CA を信頼せず、信頼できる CA で終わる完全な証明書チェーンが提供されている場合にのみ、それらを検証できます。

中間認証局によって署名された証明書を持つサーバーが、信頼できる CA に結び付けられたすべての証明書（すべての中間証明書を含む）を提供することが非常に重要です。このチェーン全体が提供されない場合、`openssl` からの出力は次のようになります。

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1
```

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1
```

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1
```

```
CONNECTED(00000003)
```

```

Certificate chain
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
-----BEGIN CERTIFICATE-----
...lots of b64...
-----END CERTIFICATE-----

```

```
Server certificate
subject=/OU=Example Unit/CN=example.com
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734

```

```
No client certificate CA names sent

```

```
SSL handshake has read 1509 bytes and written 573 bytes

New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C

Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)

```

この出力は、サーバーが1つの証明書のみを提供しており、提供された証明書が信頼されたルート認証局ではなく中間認証局によって署名されていることを示しています。この出力には、特性検証エラーも示されています。

### 修復

この問題は、デバイスによって提示された証明書の設定が間違っているために発生します。この問題を修正して CDO またはその他のプログラムがデバイスに安全に接続できるようにする唯一の方法は、正しい証明書チェーンをデバイスにロードして、接続しているクライアントに完全な証明書チェーンを提示することです。

中間 CA をトラストポイントに含めるには、次のいずれか（CSR が ASA で生成されたかどうかに応じて）のリンク先に記載されている手順に従ってください。

- <https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc13>
- <https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc15>

## 新しい証明書が検出されました

自己署名証明書を持つデバイスをアップグレードして、アップグレードプロセス後に新しい証明書が生成された場合、CDO は、[設定 (Configuration)] ステータスおよび [接続 (Connectivity)] の両方のステータスとして、「新しい証明書が検出されました (New Certificate Detected)」メッセージを生成する場合があります。このデバイスを CDO から管理する前に、この問題を手動で確認して解決する必要があります。証明書が同期されて、デバイスの状態が正常になったら、このデバイスを管理できます。



(注) 複数の管理対象デバイスを同時に [CDO へのデバイス一括再接続](#)すると、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。

新しい証明書を解決するには、次の手順を使用します。

- 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 フィルタを使用して、接続ステータスまたは設定ステータスが [新しい証明書が検出されました (New Certificate Detected)] であるデバイスを表示し、必要なデバイスを選択します。
- ステップ 5 [アクション] ペインで、[証明書の確認 (Review Certificate)] をクリックします。CDO では、確認のために証明書をダウンロードし、新しい証明書を受け入れることができます。
- ステップ 6 [デバイス同期 (Device Sync)] ウィンドウで [承認 (Accept)] をクリックするか、[デバイスへの再接続 (Reconnecting to Device)] ウィンドウで [続行] をクリックします。

CDO は、デバイスを新しい自己署名証明書と自動的に同期します。同期されたデバイスを表示するには、[デバイスとサービス] ページを手動で更新する必要がある場合があります。

## オンボーディングエラーのトラブルシュート

デバイスの導入準備エラーは、さまざまな理由で発生する可能性があります。  
次の操作を実行できます。

- ステップ 1 [インベントリ] ページで [デバイス] タブをクリックします。
- ステップ 2 適切なデバイスタイプのタブをクリックし、エラーが発生しているデバイスを選択します。場合によっては、右側にエラーの説明が表示されます。説明に記載されている必要なアクションを実行します。  
または
- ステップ 3 CDO からデバイスインスタンスを削除し、デバイスの導入準備を再試行します。

## [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 \(126 ページ\)](#) 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。
- 

## 「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。

## SecureX のトラブルシューティング

SecureX と組み合わせて CDO を使用しようとする、エラーや警告が表示されたり、問題が発生したりする場合があります。SecureX UI に表示される問題については、SecureX のマニュアルを参照する必要があります。詳細については、SecureX の [Support](#) を参照してください。

CDO 内の SecureX リボン機能、または SecureX リボンへのテナントアクセシビリティに関するケースを開くには、[Cisco Defense Orchestrator サポートへの連絡](#)を参照してください。テナント ID の入力を求められる場合があります。

### SecureX UI のトラブルシューティング

#### SecureX ダッシュボードに重複した CDO モジュールが表示される

SecureX では、単一製品の複数のモジュールを手動で設定できます。たとえば、複数の CDO テナントがある場合、テナントごとに 1 つの CDO モジュールを作成できます。重複モジュールは、同じ CDO テナントからの 2 つの異なる API トークンがあることを意味します。この冗長性により、混乱が生じ、ダッシュボードが乱雑になる可能性があります。

SecureX で CDO モジュールを手動で設定し、CDO の [一般設定 (General Settings)] ページで [SecureX に接続 (Connect SecureX)] を選択した場合、1 つのテナントが SecureX に複数のモジュールを持つ可能性があります。

回避策として、SecureX から元の CDO モジュールを削除し、複製したモジュールで CDO のパフォーマンスの監視を続けることをお勧めします。このモジュールは、より安全で、SecureX リボンと互換性のある、より堅牢な API トークンを使用して生成されます。

### CDO UI のトラブルシューティング

SecureX 内の CDO モジュールに関するケースを開く場合、詳細については、SecureX の [Terms, Privacy, Support](#) の「サポート」セクションを参照してください。

#### OAuth エラー

メッセージ「ユーザーは必要なすべてのスコープまたは十分な権限を持っていないようです (The user does not seem to have all the required scopes or sufficient privilege)」が表示されて、OAuth エラーが発生する場合があります。この問題が発生した場合は、次の可能性を検討してください。

- アカウントがアクティブ化されていない可能性。<https://visibility.test.iroh.site/> を参照し、登録したメールアドレスを使用して、アカウントがアクティブ化されているか確認します。アカウントがアクティブ化されていない場合、CDO アカウントは SecureX とマージされない可能性があります。この問題を解決するには、Cisco TAC に連絡する必要があります。詳細については、[Cisco Defense Orchestrator サポートへの連絡](#) を参照してください。

#### 組織の間違ったログイン情報で SecureX にログインしている

[一般設定 (General Settings)] ページの [テナント設定] セクションで [SecureX に接続 (Connect SecureX)] オプションを使用して CDO イベントを SecureX に送信することを選択したが、間違ったログイン情報を使用して SecureX にログインした場合、間違ったテナントからのイベントが SecureX ダッシュボードに表示されることがあります。

回避策として、CDO の [一般設定 (General Settings)] ページで [SecureX の切断 (Disconnect SecureX)] をクリックします。SecureX 組織、つまり SecureX ダッシュボードとの情報の送受信に使用される読み取り専用 API ユーザーが終了します。

次に、[テナントを SecureX に接続 (Connect Tenant to SecureX)] を再度有効にし、SecureX へのログインを求められたら、正しい組織のログイン情報を使用する必要があります。

#### 間違ったアカウントでリボンにログインしている

現時点では、間違ったアカウント情報でリボンにログインすると、リボンからログアウトできません。リボンのログインを手動でリセットするには、[Support Case Manager](#) でケースを開く必要があります。

#### SecureX リボンを起動できない

適切なスコープにアクセスできない可能性があります。この問題を解決するには、Cisco TAC に連絡する必要があります。詳細については、[Cisco Defense Orchestrator サポートへの連絡](#) を参照してください。

SecureX リボンの動作の詳細については、[SecureX ribbon documentation](#) を参照してください。





## 第 7 章

# 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](#) (179 ページ)
- [デバイス \(Devices\)](#) (180 ページ)
- [セキュリティ](#) (181 ページ)
- [トラブルシューティング](#) (183 ページ)
- [ロータッチプロビジョニングで使用される用語と定義](#) (183 ページ)
- [ポリシーの最適化](#) (184 ページ)
- [接続性](#) (184 ページ)
- [Cisco Defense Orchestrator サポートへの連絡](#) (185 ページ)

## 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 (Devices)

**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 に導入準備された ASA デバイスの実行構成ファイルのコピーです。ASA モデルを使用すると、デバイス自体を導入準備せずに ASA デバイスの設定を分析することができます。

**デバイスが「同期済み」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 に導入準備すると、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構成変更のプレビューと展開 \(118 ページ\)](#)

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] 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 \(31 ページ\)](#)
- 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 \(SDC\)](#) (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導入準備できます。

**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？

「[新規証明書の問題のトラブルシューティング](#)」を参照してください。

## ロータ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 でシリアル番号の導入準備のコンテキストで使用されます。シリアル番号が CDO テナントに導入準備されている場合、そのデバイスは「要求」されています。
- **パーク（Parked）**：CDO でシリアル番号の導入準備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 テナントに導入準備されます。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。



- シリアル番号の導入準備 (**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 を導入準備するプロセスです。

## 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が発生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することができます。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、完全にシャドウイング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 daemon>#service docker stop
Change IP address
Start Docker daemon >#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 \(73 ページ\)](#) 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 \(79 ページ\)](#) 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。

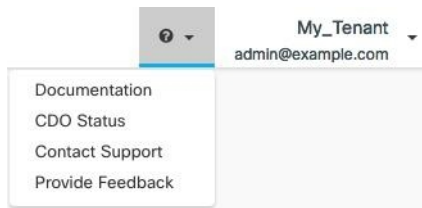
ワークフローをエクスポートするには、次の手順を使用します。

- 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 (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] 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。

- 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。

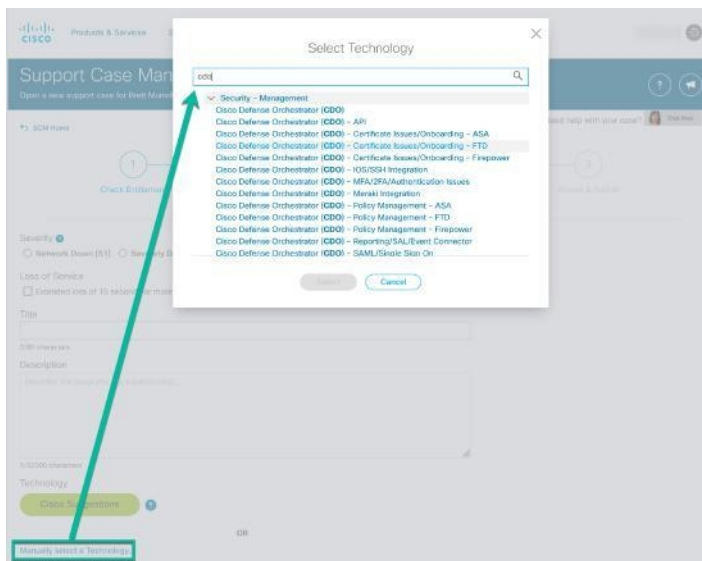
- [製品名 (PID) (Product Name (PID)) ] : この番号がわからない場合は、『[Cisco Defense Orchestrator データシート](#)』を参照してください。
- [製品の説明 (Product Description) ] : PID の説明です。
- [サイト名 (Site Name) ] : サイト名を入力します。シスコパートナーがお客様に代わってケースを開いている場合は、お客様の名前を入力します。
- [サービス契約 (Service Contract) ] : サービス契約番号を入力します。
  - **重要** : ケースを Cisco.com 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 は顧客向けのサービスステータスページを維持しており、このページには、CDO サービスが稼働しているかどうかと、サービスの中断があったかどうかが表示されます。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 \(Subscribe to Updates\) \]](#) をクリックして、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。

