Cisco Defense Orchestrator による ASA の管理

初版：2021 年 3 月 10 日

最終更新：2022 年 2 月 2 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/

目 次

Cisco Defense Orchestrator による ASA の管理

Cisco Defense Orchestrator による ASA の管理

Cisco Defense Orchestrator（CDO）はクラウドベースのマルチデバイスマネージャであり、すべての ASA デバイスのセキュリティポリシーを、シンプルで一貫性のあるセキュアな方法で管理できます。

このドキュメントの目的は、Cisco Defense Orchestrator（CDO）を初めて使用するお客様に、オブジェクトとポリシーの標準化、管理対象デバイスのアップグレード、VPN ポリシーの管理、リモートワーカーの監視に使用できる機能の概要を提供することです。このマニュアルでは、次のことを前提としています。

- 30 日間のトライアル用アカウントを作成している。または CDO を購入しており、シスコが CDO テナントを作成している。
- ユーザの役割新規 CDO テナントへの初回ログイン （33 ページ）ユーザーを設定している。
- すでに ASA が構成されており、企業で使用している。
- CDO で管理する ASA にインターネットから直接アクセスできない場合は、ネットワークに Secure Device Connector（SDC）を展開する必要があります。SDC は、CDO と ASA 間の通信を管理します。詳細については、CDO の VM イメージを使用した Secure Device Connector の展開 （7 ページ） または 自身の VM 上での Secure Device Connector の展開 （12 ページ） を参照してください。

このドキュメントでは、デバイスオーケストレーションアクティビティの概要に続いて、CDO の CLI インターフェイス、変更ログ、パブリック REST API を紹介し、CDO がデバイスに実行できるその他の管理機能の一部を紹介します。

Cisco Defense Orchestrator による ASA の管理

はじめに

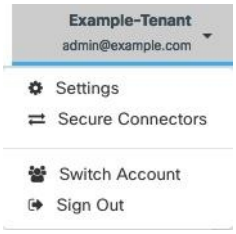
Secure Device Connector

デバイスのログイン情報を使用して CDO を ASA に接続する場合、CDO と ASA 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。デバイスのログイン情報を使用して、すべての ASA の CDO への導入準備を行うことができます。ASA と CDO 間の通信を SDC で管理しない場合で、デバイスにインターネットから直接アクセスできる場合は、ネットワークに SDC をインストールする必要はありません。Cloud Connector を使用して ASA の CDO への導入準備を行うことができます。

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、CDO テナントで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導入されている機能と、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。

SDC を表示するには：

1. CDO にログインします。
2. ユーザーメニューから、[セキュアコネクタ（Secure Connectors）] を選択します。



デバイスの導入準備

ASA の CDO への導入準備は、一括での ASA の導入準備、またはASA デバイスの導入準備実行できます。CDO でサポートされる ASA ソフトウェアおよびハードウェアの説明については、ASA サポート詳細 （37 ページ） を参照してください。

テナントに追加する CDO ユーザーを作成する

Cisco Defense Orchestrator（CDO）には、読み取り専用、編集専用、展開専用、管理者、および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。インターフェイスまたはドキュメントが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言及している場合、特定のテナントにおけるそのユーザーの権限レベルを説明しています。異なるタイプのユーザーに付与される権限については、ユーザの役割 （69 ページ）を参照してください。

テナントが作成された際、ネットワーク管理者ユーザーが自動的に割り当てられています。ネットワーク管理者は、テナントに他のユーザーを作成する権限を持ちます。これらの新しい

Cisco Defense Orchestrator による ASA の管理

ユーザーがテナントに接続するには、CDO のユーザーレコードと同じ E メールアドレスで Cisco Secure Sign-On アカウントを持っているか、それを作成する必要があります。CDO でユーザーレコードを作成するには、ユーザーロールのユーザーレコードの作成 （74 ページ） を参照してください。

ポリシー オーケストレーション

ポリシーオーケストレーションには、オブジェクトとポリシーのレビューが含まれます。ASA のポリシーを処理する際は、CDO では「アクセスグループ」が「アクセスポリシー」と呼ばれることに注意してください。ASA のアクセスポリシーを探すには、CDO メニューバーの [ポリシー] > [ASA アクセスポリシー] の順に移動します。

ネットワークオブジェクトの問題を解決する

年月が経つにつれて、使用されなくなったオブジェクト、他のオブジェクトと重複したオブジェクト、デバイス間で値が一致しないオブジェクトがセキュリティデバイスに存在している場合があります。オーケストレーションタスクの第一歩としてこれらのオブジェクトの問題を修正します。

以下の順序でオブジェクトの問題に対処します。初期の手順で行う作業により、後の手順で対処する必要がある問題の多くが解決される場合があります。

1. 未使用オブジェクトの問題の解決。未使用オブジェクト とは、デバイスに存在するが、別のオブジェクト、アクセスリスト、または NAT ルールによって参照されていないオブジェクトです。

2. 重複オブジェクトの問題の解決。重複オブジェクト とは、同じデバイス上にある、名前は異なるが値は同じである 2 つ以上のオブジェクトです。通常、重複したオブジェクトは誤って作成され、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。

3. 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 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。これはセキュリティ上の問題となる場合があります。古いリソースを保護するルールが設定されている可能性があります。

シャドウルールの修正

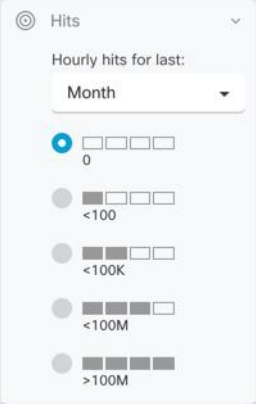
ネットワークオブジェクトの問題を解決したら、次にシャドウイングされたルールのネットワークポリシーを確認して修正します。**シャドウルール**は、ASA のアクセスポリシーページで

Cisco Defense Orchestrator による ASA の管理

半月のバッジ ◑ で示されます。アクセスポリシーのルールはリストで構成され、上から下に 1 つずつ評価されます。ネットワークトラフィックはポリシー内のシャドウルールより上位のルールと一致するため、ポリシー内のシャドウルールが一致することはありません。ヒットすることのないシャドウルールがある場合は、それを削除するか、ASA ネットワークポリシーの編集してルールを有効にします。

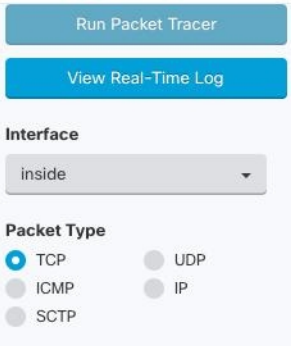
ポリシーのヒット率の評価

ポリシーのルールが実際にネットワークトラフィックを評価しているかどうかを判断します。CDO は、ポリシーのルールのヒット率データを毎時間収集します。デバイスが CDO によって管理されている時間が長いほど、特定のルールのヒット率データが持つ意味は大きくなります。特定の期間のヒット数で ASA アクセスポリシーをフィルタ処理して、ヒットしているかどうかを確認します。ヒットしていない場合は、ポリシーを作成し直すか削除することを検討してください。



ポリシーのトラブルシュート

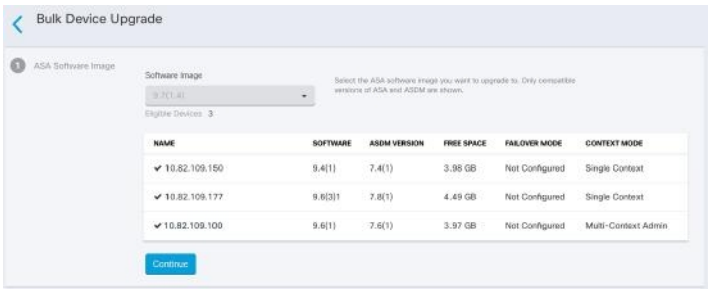
ASA パケットトレーサを使用して、模擬パケットに対するポリシーの適用をテストして、ルールによってアクセスが誤ってブロックまたは許可されていないかを判断できます。



ASA と ASDM のアップグレード

次に、ASA と ASDM を最新バージョンにアップグレードします。お客様は、CDO を使用して ASA をアップグレードすると、75% ～ 90% の時間を節約できると報告しています。

Cisco Defense Orchestrator による ASA の管理



CDO は、シングルコンテキストまたはマルチコンテキストモードで、個々の ASA または複数の ASA にインストールされている ASA および ASDM イメージをアップグレードできるウィザードを提供しています。CDO は、ASA および ASDM イメージのデータベースを維持します。

CDO は、必要なアップグレード互換性チェックをバックグラウンドで実行します。ウィザードは、互換性のある ASA および ASDM イメージを選択し、それらをインストールし、デバイスをリブートしてアップグレードを完了するプロセスを導きます。CDO で選択したイメージが ASA にコピーおよびインストールされているものであることを検証することにより、CDO はアップグレードプロセスを保護します。

CDO は定期的にデータベースを確認し、最新の ASA および ASDM イメージをデータベースに追加します。CDO は、一般に利用可能な（GA）イメージのみをサポートし、データベースにカスタムイメージを追加しません。リストに特定の GA イメージがない場合は、[サポートに連絡] ページから Cisco TAC にお問い合わせください。確立されたサポートチケット SLA によってリクエストを処理し、リストにない GA イメージをアップロードします。

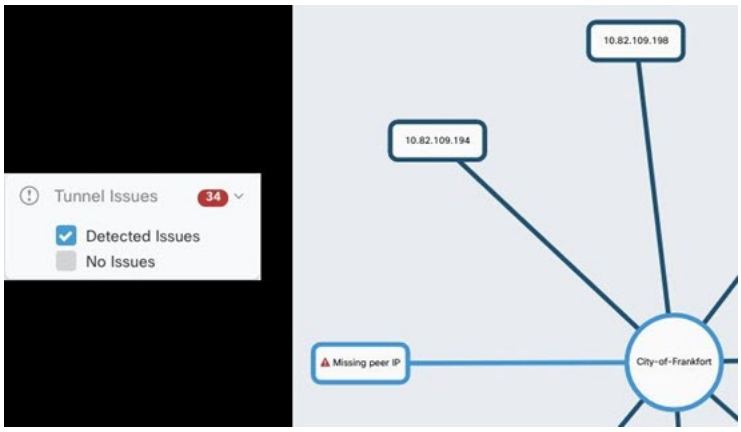
単一 ASA 上の ASA と ASDM イメージのアップグレード （124 ページ） を確認してから、独自のリポジトリからのイメージを含む複数の ASA のアップグレード （123 ページ） でASA のアップグレードについてさらに学習してください。

VPN 接続の監視と管理

サイト間 VPN の問題を確認する

CDO は、ネットワーク内の ASA デバイスに存在する VPN の問題を報告します。環境の表示方法は 2 つあります。VPN ピアのリストを示す表と、ハブ アンド スポーク トポロジで VPN 接続を示すマップです。サイドバーのフィルタを使用して、注意が必要な VPN トンネルを検索します。

Cisco Defense Orchestrator による ASA の管理



以下の方法で、CDO を使用して VPN トンネルを評価します。

- サイト間 VPN トンネルの接続の確認
- 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、または誤った構成のアクセスリストを見つける
- トンネル構成の問題を見つける

管理されていないサイト間 VPN ピアの導入準備を行う

CDO は、管理されていない VPN ピアも識別します。このようなデバイスを見つけたら、管理対象外 VPN ピアの導入準備 （206 ページ） を使用してデバイスの導入準備を行い、CDO で同様に管理します。

ASA リモートアクセス VPN のサポート

CDO を使用することで、リモートアクセス仮想プライベートネットワーク（RA VPN）構成を作成して、ユーザーが ASA 経由で接続中にエンタープライズリソースにセキュアにアクセスできるようになります。ASA の CDO への導入準備が行われると、ASDM または Cisco Security Manager（CSM）を使用して設定済みのすべての RA VPN 設定が CDO によって認識されるため、CDO で管理できるようになります。

AnyConnect はエンドポイントデバイスでサポートされている唯一のクライアントで、RA VPN 接続が可能です。

CDO は、ASA デバイスでの RA VPN 機能の次の側面をサポートします。

- SSL クライアントベースのリモートアクセス
- IPv4 および IPv6 のアドレッシング
- 複数の ASA デバイス間での共有 RA VPN 構成

Cisco Defense Orchestrator による ASA の管理

詳細については、ASA のリモートアクセス VPN を設定する （218 ページ）を参照してください。

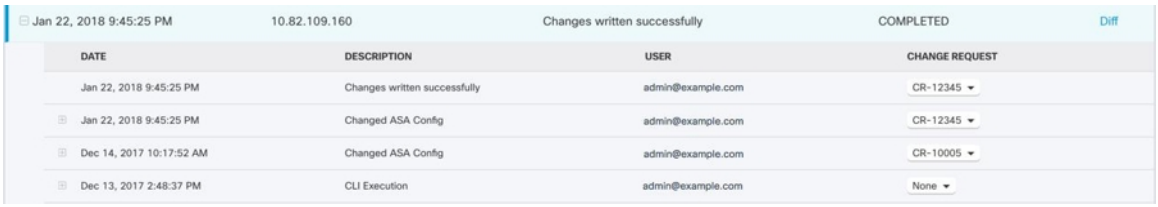
デバイス構成同期を監視する

CDO は、データベースに保存したデバイス構成と、ASA にインストールされている構成を定期的に比較します。CDO への導入準備がされた ASA は、引き続きデバイスの Adaptive Security Device Manager（ASDM）によって管理できます。そのため CDO はその構成がデバイスの構成と同じであることを確認し、相違点があれば警告します。[同期済み]、[非同期]、[競合検出] のデバイスの状態の詳細は、競合検出 （320 ページ） を参照してください。

変更ログで変更を追跡する

デバイスの構成に加えた変更は、変更ログ （325 ページ） に記録されます。変更ログには、CDO からデバイスに展開された変更、デバイスから CDO にインポートされた変更などの情報が表示されます。ここでは変更の「差分」、変更の時期、変更者といった変更内容も表示できます。

企業の追跡番号を使用する変更リクエスト管理して、加えた変更に適用することもできます。変更ログでは、そのカスタムラベル、日付範囲、特定のユーザー、変更タイプで変更のリストをフィルタ処理して、目的の変更を見つけることができます。



以前の構成を復元する

ASA に加えた変更を「元に戻す」必要がある場合、CDO を使用してデバイスを以前の構成に復元できます。詳細については、 ASA 設定の復元 （92 ページ）を参照してください。

コマンド ライン インターフェイスとコマンドマクロを使用してデバイスを管理する

CDO は、グラフィック ユーザー インターフェイス（GUI）とCDO コマンド ライン インターフェイスを使用する（CLI）の両方を提供する Web ベースの管理製品で、デバイスを 1 つずつまたは一括で管理できます。

ASA CLI のユーザーは、シスコの CLI ツールの追加機能を活用できます。SSH セッションでデバイスに接続するのではなく、CDO の CLI ツールを使用するべき理由は以下のとおりです。

- CDO は、コマンドに必要なユーザーモードを認識します。コマンドを実行するために権限レベルを上げたり下げたりする必要はありません。また、コマンドを実行するために特定のコマンドコンテキストを入力する必要もありません。
- CDO はコマンド履歴を保持しているため（）、リストから選択するだけで簡単にコマンドを再実行できます。

Cisco Defense Orchestrator による ASA の管理

- CLI アクションは変更ログに記録されるため、送信されたコマンドと実行されたアクションを確認できます。
- コマンドは一括モードで実行できるため、オブジェクトまたはポリシーを複数のデバイスに同時に展開できます。
- CDO は CLI マクロを提供します（）。. CLI マクロはすぐに実行可能なコマンドで、格納された状態からそのまま使用できます。または、CLI コマンドの「空白を埋めて」から実行することもできます。これらのコマンドを 1 つのデバイスで実行することも、コマンドを複数の ASA に同時に送信することもできます。
- CLI は、完全な ASA 構成ファイルを提供します。これを表示することも、上級ユーザーの場合は直接編集して変更を保存することもできます。CLI コマンドを実行して変更する必要はありません。

CDO パブリック API

CDO はパブリック API を公開しており、ドキュメント、例、実験用のプレイグラウンドを提供しています。パブリック API の目標は、通常は CDO UI で実行できる多くのことをコードで実行するためのシンプルで効果的な方法を提供することです。

この API を使用するには、GraphQL の知識が必要です。学ぶのは非常に簡単で、詳細で読みやすい公式ガイド（https://graphql.org/learn/）が提供されています。GraphQL を選択した理由は、柔軟で、厳密に型指定され、自動文書化されるためです。

完全なスキーマドキュメントを見つけるには、GraphQL Playground に移動し、ページの右側にある [ドキュメント] タブをクリックするだけです。

このリンクから、またはユーザーメニューから [</>CDO API] を選択して、CDO パブリック API を起動できます。

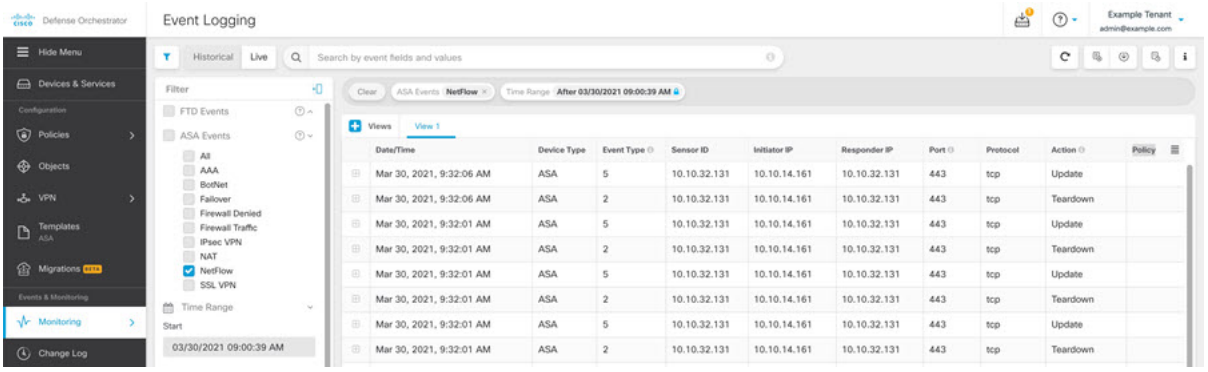
CDO と SecureX の統合

Cisco SecureX プラットフォームは、広範なシスコの統合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接続することで、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全体のセキュリティが強化されます。統合プラットフォームで技術を連携することで、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。詳細（SecureX と CDO （499 ページ））とハウツー（CDO の SecureX への追加 （501 ページ））もご覧ください。

Cisco Security Analytics and Logging

追加のライセンスを使用すると、Cisco Security Analytics and Logging （339 ページ） で Syslog イベントと Netflow Secure Event Logging（NSEL）イベントを ASA から Secure Event Connector （397 ページ）（SEC）に直接送信し、それから Cisco Cloud に転送できます。クラウドに転送されると、CDO の [イベントロギング] ページでこれらのイベントを表示できます。そこでイベントをフィルタ処理して確認することで、ネットワークでどのセキュリティルールがトリガーされているかを明確に把握できます。

Cisco Defense Orchestrator による ASA の管理



イベントのモニタリングに加えて、CDO から Secure Cloud Analytics ポータルを起動して、ログに記録されたイベントの動作分析を実行できます。

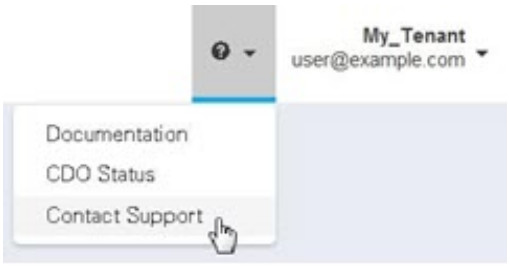
Cisco Security Analytics and Logging の導入方法の詳細は、ASA デバイスに安全なロギング分析（SaaS）を導入する （345 ページ） を参照してください。

次の作業

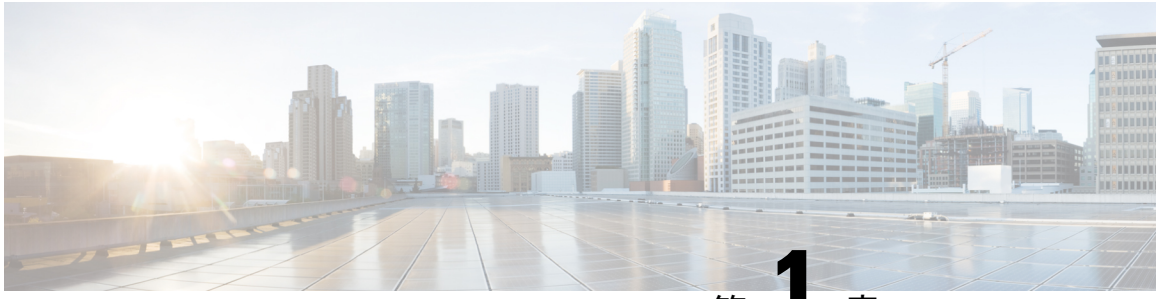
これで、ASA の導入準備とポリシーのオーケストレーションを開始できます。

サポートが必要な場合

CDO GUI のサポートメニューをクリックして、Cisco Defense Orchestrator サポートへの連絡したり、製品ドキュメントを読んだりできます。



Cisco Defense Orchestrator による ASA の管理



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

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（33 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 （7 ページ）および自身の VM 上での Secure Device Connector の展開 （12 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 （519 ページ）

• Secure Device Connector の更新 （21 ページ）
• Secure Device Connector の削除 （18 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	

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）
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。

ASA を SDC に接続する際の特別な考慮事項

具体的に述べると、ASA との接続に、SDC は ASDM で使用されるのと同じ安全な通信チャネルを使用します。

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、ASDM HTTP サーバーポートを 1024 以上の値に変更する必要があります。このポート番号は、CDO への ASA デバイスの導入準備に使用されるポート番号と同じものになることに注意してください。

ASA コマンドの例

次の例では、ASA 外部インターフェイスの名前が「outside」であり、ASA で AnyConnect クライアントが設定されているため、ASDM HTTP サーバーがポート 8443 でリッスンしていると想定しています。

外部インターフェイスを有効にするには、次のコマンドを入力します。

EMEA：

http 35.157.12.126 255.255.255.255 outside

http 35.157.12.15 255.255.255.255 outside

米国：

http 52.34.234.2 255.255.255.255 outside

http 52.36.70.147 255.255.255.255 outside

アジア - 太平洋 - 日本 - 中国地域：

http 54.199.195.111 255.255.255.255 outside

http 52.199.243.0 255.255.255.255 outside

AnyConnect VPN クライアントが使用されている場合に ASDM HTTP サーバーポートを有効にするには、次のコマンドを入力します。

http server enable 8443

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 （22 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 （12 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。

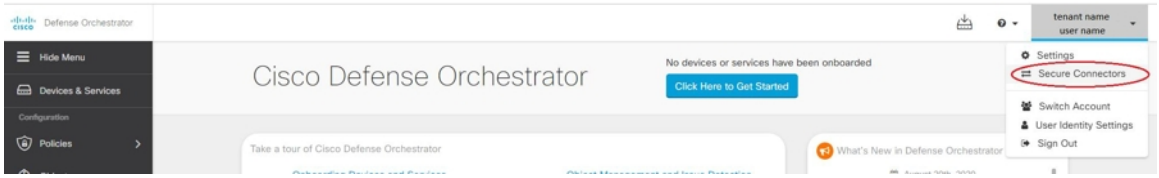
- CDO は、厳密な証明書チェックを必要とし、SDC とインターネットの間の Web/コンテンツプロキシ検査をサポートしていません。プロキシサーバーを使用している場合は、SDC と CDO の間のトラフィックの検査を無効にします。
- SDC には、TCP ポート 443 またはデバイス管理用に設定したポートでのインターネットへの完全なアウトバウンドアクセスが必要です。デバイスが CDO によって管理されている場合、このポートからのインバウンドトラフィックも許可する必要があります。
- 適切なネットワークアクセスを確保するため、「Cisco Defense Orchestrator の管理対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

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

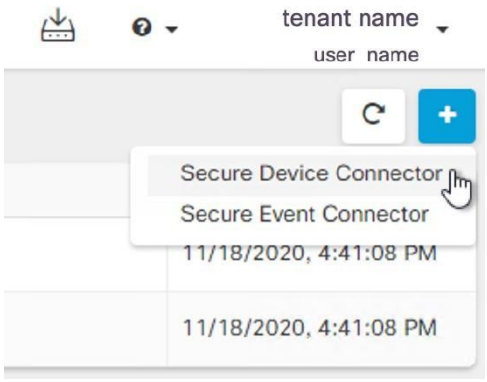
- Docker IP は、SDC の IP 範囲**および**デバイスの IP 範囲とは異なるサブネットにある必要があります。
- インストールを開始する前に、次の情報を収集します。
  - SDC に使用する静的 IP アドレス。
  - インストールプロセス中に作成する `root` ユーザーと `cdo` ユーザーのパスワード。
  - 組織で使用する DNS サーバーの IP アドレス。
  - SDC アドレスが存在するネットワークのゲートウェイ IP アドレス。
  - タイムサーバーの FQDN または IP アドレス。
- SDC仮想マシンは、セキュリティパッチを定期的にイン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

ステップ 1 SDC を作成する CDO テナントにログオンします。

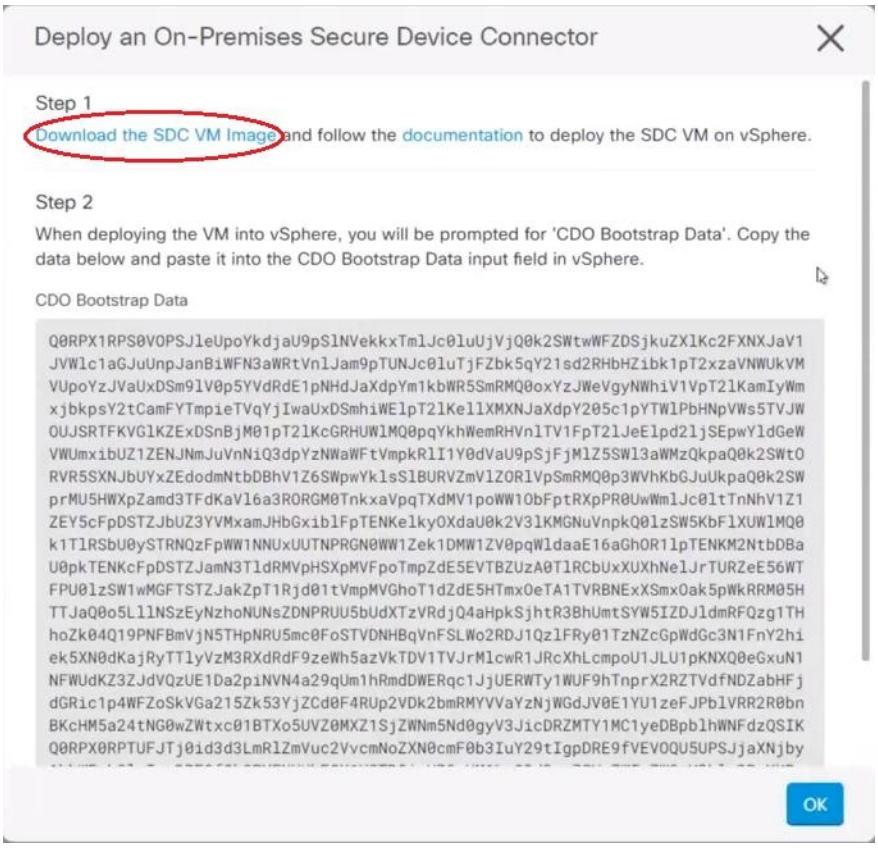
ステップ 2 [ユーザー（User）] メニューをクリックし、[セキュアコネクタ（Secure Connectors）] を選択します。



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。

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

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

ステップ 17 [これらの値は正しいですか？（はい/いいえ）（Are these values correct? (y/n)）]というプロンプトが表示されたら、[y] 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。

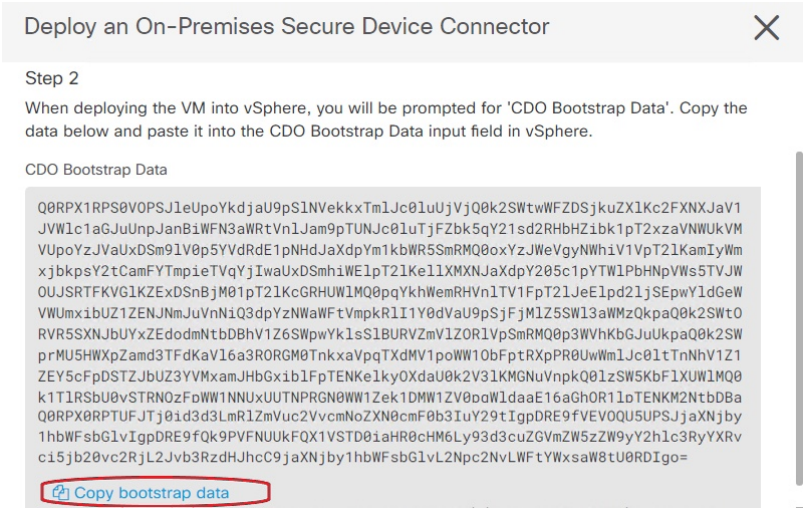
ステップ 22 プロンプトで、**sudo sdc-onboard bootstrap** と入力します。

```
[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。

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



ステップ 25 [これらの設定を更新しますか？（はい/いいえ）（Do you want to update these setting? (y/n)）] というプロンプトが表示されたら、[n] 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 のトラブルシュート （519 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 （521 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 （22 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 （7 ページ） を参照してください。

始める前に

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

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

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

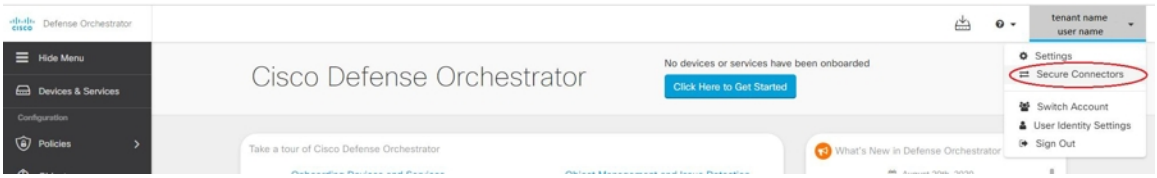
- VMware ESXi では、プロビジョニングの選択に応じて、仮想マシンをサポートするために 10 GB のディスク容量が必要です。これは、必要に応じてディスク領域を拡張できるように、パーティションで論理ボリューム管理（LVM）を使用していることを想定した値です。

- CDO コネクタと Secure Event Connector（SEC）の両方がインストールされている VM のシステム要件。
  - CPU：SEC 用に 4 つの CPU を追加します。
  - メモリ：SEC 用 8 GB のメモリを追加します。
- VM の CPU とメモリを更新したら、VM の電源を入れ、[セキュアコネクタ（Secure Connectors）] ページに SDC が「アクティブ」状態であることが示されていることを確認します。
- 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。

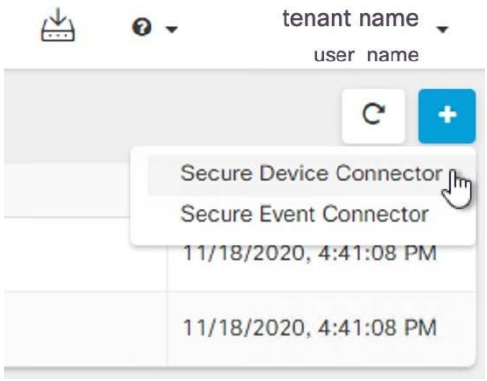
（注） **始める前に**：手順内のコマンドは、コピーして端末ウィンドウに貼り付けるのではなく入力するようにしてください。一部のコマンドに含まれる「n ダッシュ」は、カットアンドペーストのプロセスで「m ダッシュ」として適用される場合があり、コマンドが失敗する原因となります。

ステップ 1 SDC を作成する CDO テナントにログオンします。

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

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

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

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

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

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

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

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

ステップ 22 ブートストラップデータはbase64 でエンコードされていますので、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@sdc-vm ~]$ base64 -d /usr/local/cdo/bootstrapdata > /usr/local/cdo/extractedbootstrapdata
                [sdc@sdc-vm ~]$
```

catコマンドを実行して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@sdc-vm ~]$ cat /usr/local/cdo/extractedbootstrapdata
                CDO_TOKEN="<token string>"
                CDO_DOMAIN="www.defenseorchestrator.com"
                CDO_TENANT="<tenant-name>"

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

ステップ 23 以下のコマンドを実行して、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@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > sdcenv && source sdcenv
                [sdc@sdc-vm ~]$
```

ステップ 24 CDO からブートストラップバンドルをダウンロードします。

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

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

```
[sdc@sdc-vm ~]$ tar xzvf /usr/local/cdo/tenant-name-SDC
                <snipped - extracted files>
                [sdc@sdc-vm ~]$
                [sdc@sdc-vm ~]$ /usr/local/cdo/bootstrap/bootstrap.sh
                [2018-07-23 13:54:02] environment properly configured
                download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
                toolkit.sh
                common.sh
                [2018-07-23 13:54:04] startup new container
                Unable to find image 'ciscodefenseorchestrator/sdc_prod:latest' locally
                sha256:d98f17101db10e66db5b5d6afda1c95c29ea0004d9e4315508fd30579b275458: Pulling
from
                ciscodefenseorchestrator/sdc_prod
                08d48e6f1cff: Pull complete
                ebbd10b629b1: Pull complete
                d14d580ef2ed: Pull complete
                45421d451ab8: Pull complete
                <snipped - downloads>
                no crontab for sdc
```

すると、CDO で SDC が「アクティブ」と表示されるはずです。

次のタスク

- 「デバイス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 Event Connector をインストールする場合は、SDC 仮想マシンへの Secure Event Connector のインストール （398 ページ）に戻ります。
- テナントに **2 つ以上**の Secure Event Connector をインストールする場合は、「CDO イメージを使用して SEC をインストールする」に戻ります。

Secure Device Connector の削除

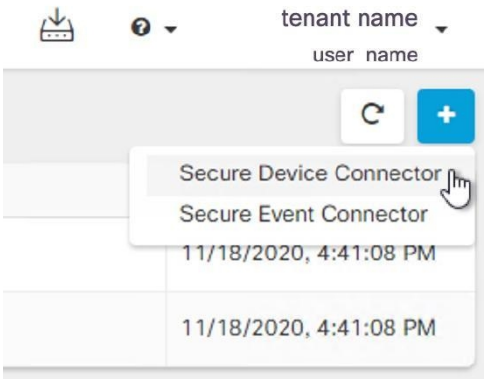
警告 この手順により、Secure Device Connector（SDC）が削除されます。この操作は元に戻せません。この操作を行った後は、新しい SDC をインストールしてデバイスを再接続するまで、その SDC に接続されているデバイスを管理できなくなります。デバイスを再接続するには、再接続が必要なデバイスごとに管理者ログイン情報を再入力する必要がある場合があります。

テナントから SDC を削除するには、次の手順を実行します。

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。
  - ある SDC から別の SDC への ASA の移動 （19 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 （22 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。

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。

デフォルトの Secure Device Connector の指定

すべてではありませんが、CDO によって管理される多くのデバイスは、Secure Device Connector（SDC）を介して CDO に接続します。SDC を介して CDO に接続するデバイスを導入準備すると、導入準備時に特に指定しない限り、デバイスはテナントのデフォルトの SDC に関連付けられます。

[セキュアコネクタ（Secure Connectors）] ページで、デフォルトで選択される SDC を指定できます。

ステップ 1 アカウントメニューから、[セキュアコネクタ（Secure Connectors）] を選択します。

ステップ 2 デフォルトにする SDC を選択します。

ステップ 3 [操作（Actions）] ウィンドウで、[デフォルトにする（Make Default）] をクリックします。[デフォルトにする（Make Default）] アクションが表示されない場合、その SDC はすでにデフォルトの SDC になっています。

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 （85 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 copyof this software and associated documentation files（the "Software"）, to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

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

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

==========

*** bluebird ***

The MIT License（MIT）

Copyright (c) 2013-2015 Petka Antonov

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

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

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

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

==========

* cheerio *

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

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

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

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

==========

* command-line-args *

The MIT License (MIT)

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

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

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

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

==========

* ip *

This software is licensed under the MIT License.

Copyright Fedor Indutny, 2012.

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

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

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

==========

*** json-buffer ***

Copyright (c) 2013 Dominic Tarr

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

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

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

==========

*** json-stable-stringify ***

This software is released under the MIT license:

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

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

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

==========

*** json-stringify-safe ***

The ISC License

Copyright (c) Isaac Z. Schlueter and Contributors

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

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

==========

*** lodash ***

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

Based on Underscore.js, copyright Jeremy Ashkenas,

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

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

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

documented below:

====

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

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

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

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

====

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

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

====

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

==========

*** log4js ***

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

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

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

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

==========

*** mkdirp ***

Copyright 2010 James Halliday (mail@substack.net)

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

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

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

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

==========

*** node-forge ***

New BSD License (3-clause)

Copyright (c) 2010, Digital Bazaar, Inc.

All rights reserved.

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

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

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

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

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

==========

*** request ***

Apache License

Version 2.0, January 2004

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

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

END OF TERMS AND CONDITIONS

==========

*** rimraf ***

The ISC License

Copyright (c) Isaac Z. Schlueter and Contributors

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

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

==========

*** uuid ***

Copyright (c) 2010-2012 Robert Kieffer

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

==========

*** validator ***

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

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

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

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

==========

*** when ***

Open Source Initiative OSI - The MIT License

CDO へのサインイン

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

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

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

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

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

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

CDO テナントが 2019 年 10 月 14 日以降に作成された場合は、「新規 CDO テナントへの初回ログイン （33 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 （34 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 （34 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 （63 ページ） に進みます。これは 4 段階のプロセスです。4 段階すべてを完了する必要があります。

ログインの失敗のトラブルシューティング

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

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

Cisco Secure Sign-On ID プロバイダーへの移行

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

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

（注）

- 独自のシングルサインオン ID プロバイダーを使用して CDO にサインインする場合、この Cisco Secure Sign-On および Duo への移行は影響しません。独自のサインオンソリューションを引き続き使用します。
- CDO の無料トライアル期間中であれば、この移行が適用されます。
- **2019 年 10 月 14 日以降に CDO テナントが作成されていた場合は**、この記事の代わりに 新規 CDO テナントへの初回ログイン （33 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 （63 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 （63 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を設定している場合は、オーセンティケータのロゴをクリックして [Duo Security] か [Google Authenticator] を選択します。

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

[ポータル（Portals）] ビューは、複数のテナントから統合された情報を取得して表示します。詳細については、マルチテナントポータルの管理 （52 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 （56 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：

- ASA サポート詳細 （37 ページ）
- ブラウザ サポート （38 ページ）

ASA サポート詳細

CDO は ASA 8.4 以降を実行中のすべてのプラットフォームを管理できます（「モデルごとの ASA と ASDM の互換性」を参照）。これには、CDO ではサポートされていない ASA サービスモジュール（ASASM）以外の ASAv インスタンスが含まれます。

CDO は、ASA 8.3 を実行している ASA の導入準備を行うことができますが、変更を展開したり、他の方法で管理したりすることはできません。サポートは「読み取り専用」です。

9.12 より前のバージョンからの ASA と ASDM のアップグレードの前提条件など、ASA の一部のバージョンをサポートしていない CDO 機能が存在する可能性があります。このような場合、CDO のドキュメントに、その機能の前提条件とともに例外となるバージョンが表示されます。

CDO は、ASA とは異なるオペレーティングシステムを実行する ASA FirePOWER モジュールの管理をサポートしていません。システムで ASA FirePOWER モジュールを引き続き使用できますが、Firepower Management Center または ASDM で個別に管理する必要があります。

ASA 5508-X および 5516-X を最新の ROMMON イメージにアップグレードすることをお勧めします。手順については、『Cisco ASA および Firepower Threat Defense 再イメージ化ガイド』を参照してください。それ以外の場合は、次の ASA ソフトウェアバージョンを使用してください。

- ASA 9.6(x) ～ 9.15(x)
- ASA 9.5(2)、9.5(3)

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
Umbrella 組織	Umbrella は、クラウドベースのセキュア インターネット ゲートウェイ（SIG）プラットフォームであり、定期的にクラウド経由で更新を受信します。詳細については、「顧客をシスコ セキュア インターネット ゲートウェイ（SIG）に安全に接続する」を参照してください。 Umbrella 組織に関連付けられる ASA デバイスは、バージョン 9.1.2 以降を実行している**必要**があります。

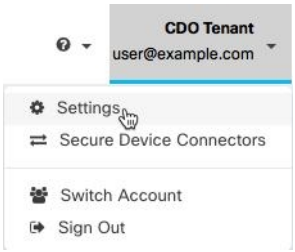
ブラウザ サポート

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

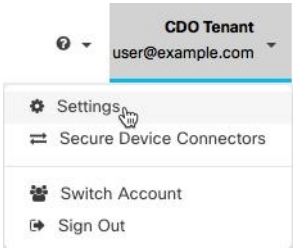
Cisco Defense Orchestrator（Defense Orchestrator）を使用すると、[設定] ページでテナントおよび個々のユーザーアカウントの特定の側面をカスタマイズできます。ユーザーメニューを開き、[設定（Settings）] をクリックして、[設定（Settings）] ページにアクセスします。



関連情報：

- 全般設定 （39 ページ）
- ユーザ管理
- ロギングの設定
- 通知設定 （43 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 （39 ページ）
- マイトークン（My Tokens）については、API トークン （48 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 （39 ページ）
  - シスコサポートによるテナントの表示の防止 （40 ページ）
  - 自動展開をスケジュールするオプションを有効にする （41 ページ）
  - デフォルトの競合検出間隔 （40 ページ）
  - Web 分析 （42 ページ）
  - テナント ID （42 ページ）
  - テナント名 （43 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。

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。

デフォルトの定期バックアップスケジュールの設定

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

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

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

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

ステップ 3 [**保存（Save**）] をクリックします。

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

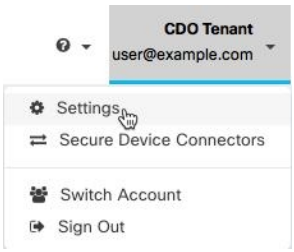
テナント名は、テナントも識別します。テナント名は組織名ではないことに注意してください。この情報は、Cisco Technical Assistance Center（TAC）に連絡する必要があるときに役立ちます。

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

サブスクライバ

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

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

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

CDO 通知の表示

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

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

サービス統合

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

CDO 通知用サービス統合の有効化

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

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

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

Webex チームの着信ウェブフック

始める前に

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

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

ステップ 1 Webex Teams アプリケーションを開きます。

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

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

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

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

ステップ 6 次を設定します。

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

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

ステップ 8 ウェブフック URL をコピーします。

ステップ 9 CDO にログインします。

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

ステップ 11 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 ヵ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 にない場合、CDO はランディングページを表示して、ユーザーにCDOの詳細を確認したり、無料試用版をリクエストしたりする機会を提供します。

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

同様に、IdP のアカウントを削除しても、CDO からユーザーレコードを削除したことにはなりません。ただし、IdP アカウントがなければ、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の管理

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

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

はじめる前に

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

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

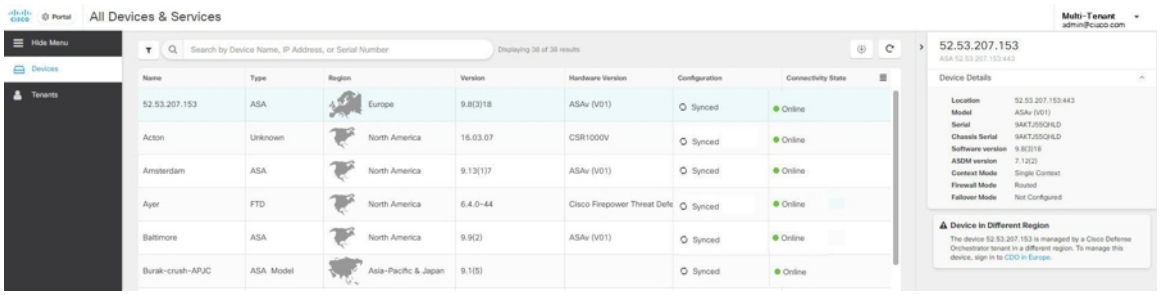
マルチテナントポータル

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。



- [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

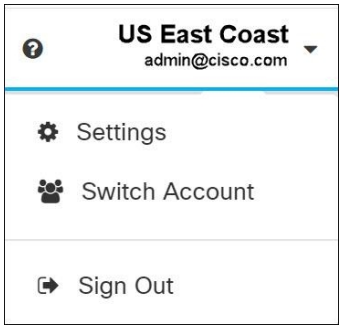
ステップ 1 ポータルに移動し、[テナント（Tenants）] タブをクリックします。

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。

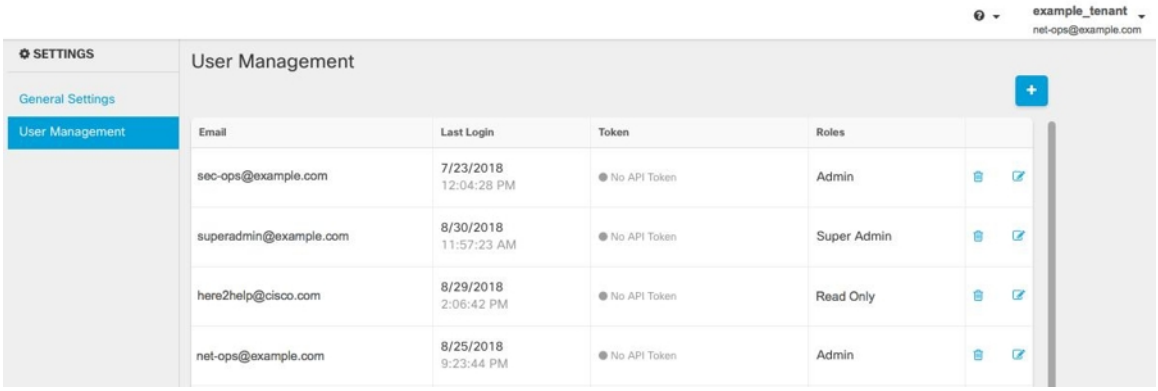
企業独自の IdP がない限り、Cisco Secure Sign-On はすべての CDO テナントの ID プロバイダーとなります。この記事の残りの部分は、ID プロバイダーとして Cisco Secure Sign-On を使用していることを前提としています。

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

テナントに関連付けられているユーザーレコードの表示

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 [ユーザー管理（User Management）] をクリックします。



（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 （39 ページ）ページでアカウント設定を指定します。

ユーザー管理の Active Directory グループ

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

[ユーザー管理（User Management）] ページから AD グループを追加、編集、または削除するには、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、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。

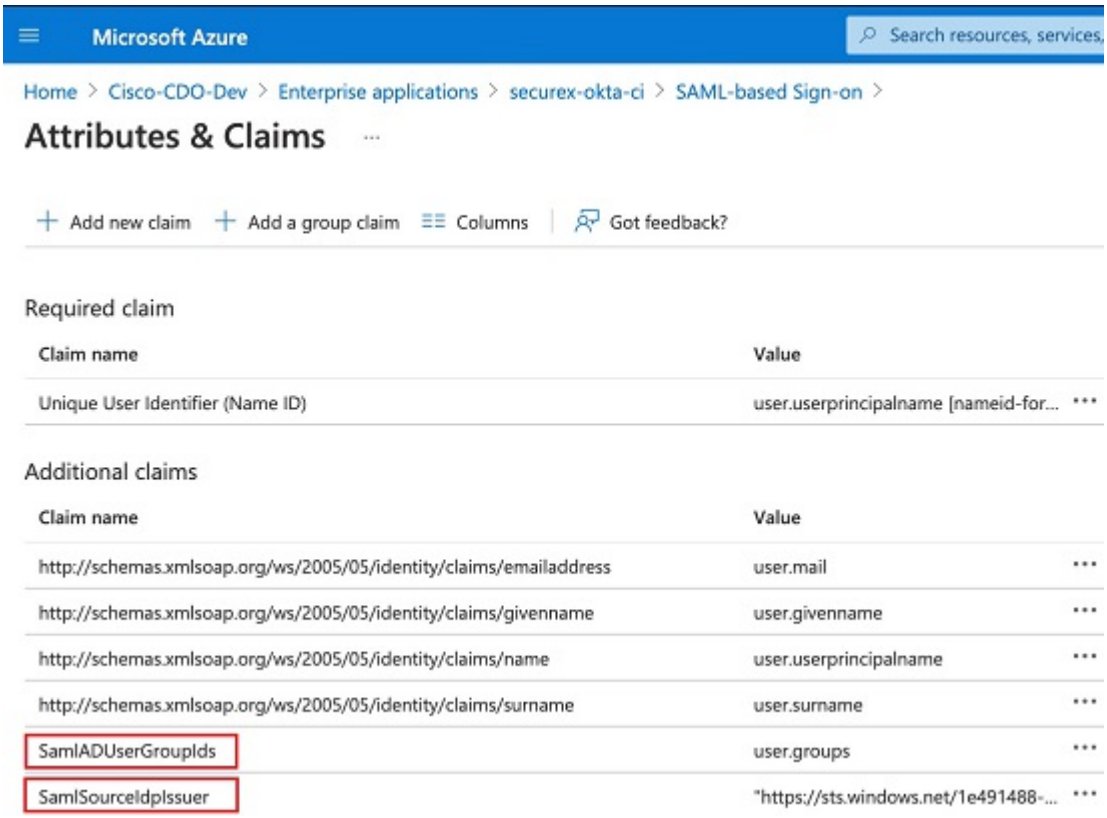
（注） ユーザーが、個別ユーザーであり、かつ同じテナントの AD グループにも属している場合は、個別ユーザーのユーザーロールが AD グループのユーザーロールよりも優先されます。

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。

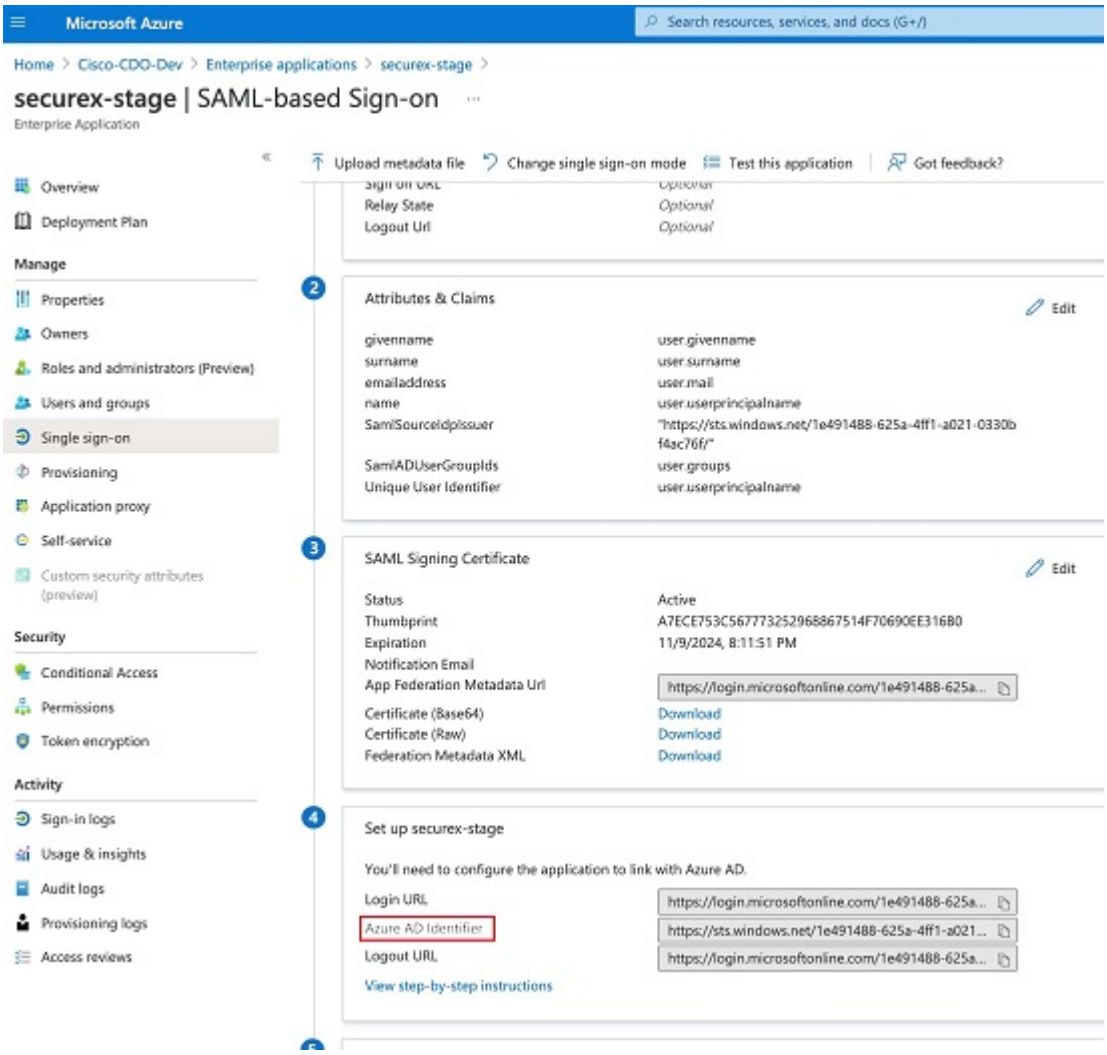
1. Cisco TAC でサポートケースを開き、次の情報を使用してカスタム AD IdP 統合を要求します。
   - CDO のテナント名と地域。
   - カスタムルーティングを定義するドメイン（例：@cisco.com、@myenterprise.com）。
   - .XML 形式の証明書とフェデレーションメタデータ。
2. AD に次のカスタム SAML 要求を追加します。これらの値では大文字と小文字が区別されます。
   - **SamlADUserGroupIds**：この属性は、ユーザーが AD 上で持つすべてのグループの関連付けを記述します。たとえば、次のスクリーンショット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

図 *1 : Active Directory* で定義されたカスタム要求



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

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



ユーザー管理用 Active Directory グループの追加

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できることに注意してください。CDO で AD グループ自体を編集することはできません。AD グループ内のユーザーのリストを編集するには、ADを使用する必要があります。

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 （34 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として Google オーセンティケータを設定します。

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

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

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

ヒント

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

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じ電子メールアドレスでユーザーレコードを作成する必要があります。

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

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

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

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

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

ユーザの役割

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

読み取り専用ロール

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

Read Only User. You cannot make configuration changes.

.

読み取り専用ロールを持つユーザーは、次のことを実行できます。

- CDO の任意のページまたは設定を確認する。
- 任意のページのコンテンツを検索およびフィルタリングする。

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

読み取り専用ユーザーは、次のことを実行**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 （33 ページ）を参照してください。

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

ユーザーロールのレコードの変更

ユーザーレコードは、現在記録されているユーザーのロールです。テナントに関連付けられているユーザーを調べることにより、各ユーザーがどのロールを使用しているかをレコードによって判断できます。ユーザーロールを変更すると、ユーザーレコードが変更されます。ユー

ザーのロールは、ユーザー管理テーブルでのロールによって識別されます。詳細については、「ユーザ管理」を参照してください。

ユーザーレコードを変更するには、ネットワーク管理者である必要があります。テナントにネットワーク管理者がいない場合は、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 （33 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 （69 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 （84 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 （88 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

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。

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 （80 ページ）
- CDO へのデバイス一括再接続 （83 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。

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。

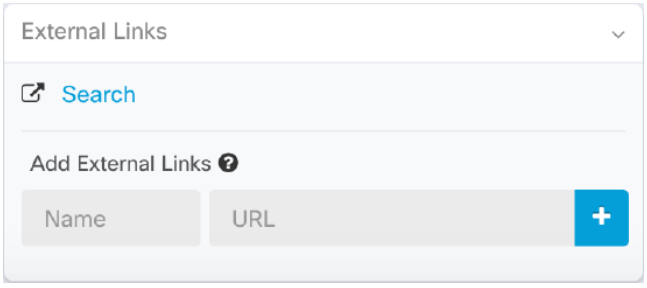
ステップ 4 必要なデバイスを選択して、強調表示します。

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（ASA の場合は Adaptive Security Device Manager（ASDM）。この機能を使用して、検索エンジン、ドキュメントリソース、企業 Wiki、または選択したその他の URL へのリンクを作成できます。必要な数の外部リンクをデバイスに関連付けることができます。同じリンクを同時に複数のデバイスに関連付けることもできます。



作成したリンクはどこにでも到達できますが、企業のセキュリティ要件は変わりません。たとえば、普段オンプレミスで、または VPN 接続を介して特定の URL にアクセスすることによって企業ネットワークに接続する必要がある場合、この要件は維持されます。企業が特定の URL をブロックしている場合、それらの URL は引き続きブロックされます。制限されていない URL は引き続き制限されません。

location 変数

URL に組み込むことができる {location} 変数が作成されました。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}
```

は ASA の ASDM 。

関連情報：

• デバイスノートを書く （84 ページ）
• デバイスとサービスのリストのエクスポート （79 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。

ASDM への外部リンクの作成

ASA の Adaptive Security Device Manager（ASDM）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 ASDM 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コマンドボタンのみ提供されることに注意してください。

ステップ 6 [通知（notifications）] タブで一括デバイス再接続アクションの進行状況を確認します。一括デバイス再接続ジョブのアクションがどのように成功または失敗したかについての詳細な情報が必要な場合は、青色の [レビュー（Review）] リンクをクリックして [ジョブ（Jobs）] ページ （336 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す。

- [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「group name:label」を使用して作成できます。たとえば、Region:East または Region:West などです。これらの 2 つのラベルを作成する場合、グループラベルは Region になり、そのグループの East または West から選択できます。

デバイスとオブジェクトにラベルを適用する

デバイスにラベルを適用するには、以下の手順を実行します。

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。

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。

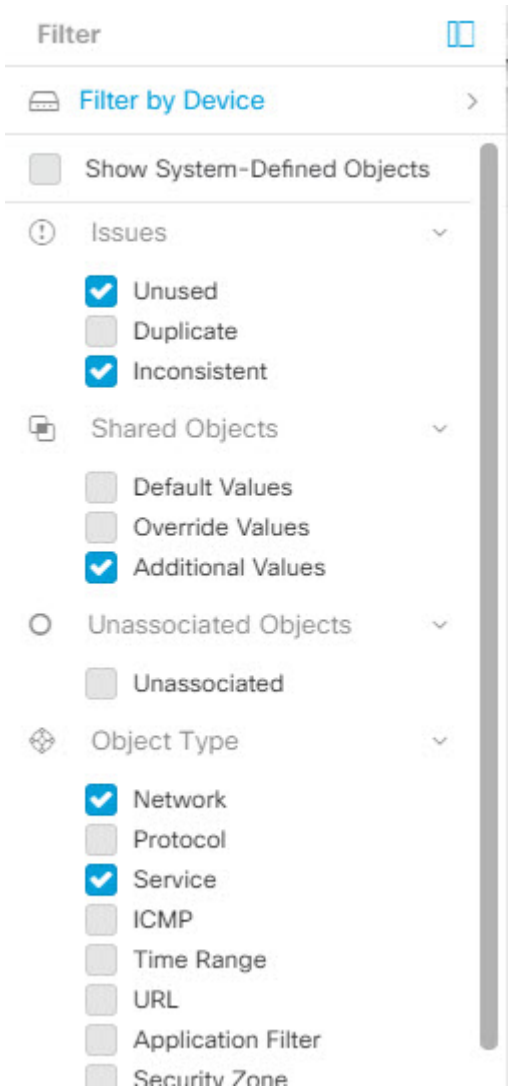
フィルタ処理するには、[デバイスとサービス（Devices and Services）] タブ、[ポリシー（Policies）] タブ、および [オブジェクト] タブの左側のペインで をクリックします。

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て、関連する結果を見つけるためのいくつかの潜在的な検索戦略を作成することができます。

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



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 （85 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。

CDO コマンド ライン インターフェイスを使用する

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

関連情報：

- 詳細な ASA CLI ドキュメントについては、ASA コマンド ライン インターフェイスのドキュメント （105 ページ） を参照してください。

コマンドの入力方法

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

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

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

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

このエラーメッセージを受信した場合、次の手順を実行します。

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

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

ステップ 3 [送信（Send）] をクリックします。

単一デバイスで CLI を使用する

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、デバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 コマンド ライン インターフェイスを使用して、管理するデバイスを選択します。

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

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

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

コマンド履歴での動作

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

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

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

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

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

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

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

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

- 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。

ASA デバイスの構成

ASA など、一部のタイプのデバイスは、構成を 1 つの構成ファイルに保存します。 これらのデバイスの場合、Cisco Defense Orchestrator でデバイス構成ファイルを表示し、デバイスに応じてさまざまな操作を実行できます。

デバイスの構成ファイルを表示する

ASA、Cisco Secure Firewall Cloud Native、SSH 管理対象デバイス、Cisco IOS を実行しているデバイスなど、構成全体を 1 つの構成ファイルに保存するデバイスの場合、CDO を使用して構成ファイルを表示できます。

（注） SSH 管理対象デバイスと Cisco IOS デバイスには読み取り専用の設定があります。

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（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 設定を表示するデバイスまたはモデルを選択します。

ステップ 5 右側の [管理（Management] ペインで、[設定（Configuration）] をクリックします。
完全な構成ファイルが表示されます。

関連情報：

- 完全なデバイス設定ファイルの編集

完全なデバイス設定ファイルの編集

ASA など、一部のタイプのデバイスは、設定を 1 つの構成ファイルに保存します。これらのデバイスの場合、CDO でデバイス構成ファイルを表示し、デバイスに応じてさまざまな操作を実行できます。

現在、CDO を使用して直接編集できるのは構成ファイルのみです。ASA

注意 この手順は、デバイスの構成ファイルのシンタックスに精通している上級ユーザーを対象としています。この手法では、Defense Orchestrator に保存されている構成ファイルのコピーに直接変更を加えます。

手順

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

ステップ 4 構成を編集するデバイスを選択します。

ステップ 5 右側の [管理] ペインで、[構成] をクリックします。

ステップ 6 [デバイスの構成] ページで、[編集] をクリックします。

ステップ 7 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 8 ファイルを編集し、変更を保存します。

ステップ 9 [デバイスとサービス] ページに戻り、変更をプレビューして展開します。

ASA 構成の比較

2 つの ASA の構成を比較するには、次の手順を実行します。

ステップ 1 ナビゲーションメニューで、[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 ASA 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 ASA モデルデバイスを見つけます。

ステップ 3 [ASA] タブをクリックします。

ステップ 4 比較するデバイスを見つけるためにデバイスリストをフィルタ処理します。

ステップ 5 2 つの ASA を選択します。それらのステータスは重要ではありません。Defense Orchestrator に保存されている ASA の構成を比較しようとしています。

ステップ 6 右側の [デバイスアクション] ペインで、[比較] をクリックします。

ステップ 7 [構成の比較（Comparing Configurations）] ダイアログで、[次へ] および [前へ（Previous）] をクリックして、構成ファイル内の青色で強調表示されている相違点をスキップします。

ASA 設定の復元

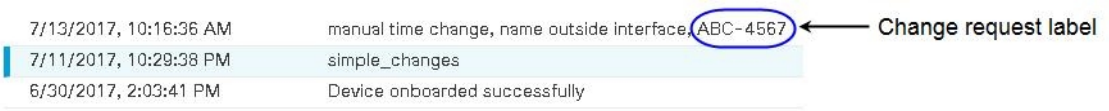
この手順では、Cisco Defense Orchestrator（CDO）を使用して ASA に行った設定変更を復元する方法について説明します。これは、予期しない結果や望ましくない結果をもたらした設定変更を削除する便利な方法です。

設定を復元する前に

設定を復元する前に、次の注意事項を確認してください。

- CDO は、復元することを選択した設定を、ASA に展開されている最後に認識された設定と比較します。ステージングされているが ASA のメモリに展開されていない設定とは比較しません。ASA に展開されていない変更がある場合に、以前の設定を復元すると、展開されていない変更は、復元プロセスによって上書きされて失われます。

- 過去の設定を復元すると、それまでに展開されたすべての設定変更が上書きされます。たとえば、以下のリストにある 2017 年 7 月 11 日の設定を復元すると、2017 年 7 月 13 日に行われた設定変更が上書きされます。



- 設定変更に最初に適用した変更リクエストラベルは、[設定の復元（Restore Configuration）] リストに表示されます。
- ASA は [同期（Synced）] または [非同期] の状態になっている可能性があるため、過去の設定を復元する前に、設定の競合を解決する必要があります。

設定の復元方法

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 [ASA] タブをクリックします。

ステップ 4 設定を復元する ASA を選択します。

ステップ 5 右側のペインで **[設定（Configuration）] > [設定の復元（Restore Configuration）]** を選択します。

ステップ 6 [設定の復元（Restore Configuration）] ペインで、復元する設定を選択します。たとえば、上の図では、2017 年 7 月 11 日の設定が選択され、強調表示されています。

ステップ 7 「CDO によって検証された最新の実行設定」と「*<date>* から選択された設定」を比較して、[<date> から選択された設定（Selected Configuration from *<date>*）] ウィンドウに表示されている設定を復元することを確認します。

ステップ 8 [復元（Restore）] をクリックします。これにより、CDO の設定がステージングされます。[デバイスとサービス] ページに、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 9 右側のペインで [変更の展開 ...（Deploy Changes...）] をクリックして変更を展開し、ASA を同期させます。

トラブルシューティング

保持したかったのに失ってしまった変更を回復するには、どうすればよいですか。

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 [ASA] タブをクリックします。
ステップ 4 必要なデバイスを選択します。
ステップ 5 右側のペインで [変更ログ] をクリックします。
ステップ 6 変更ログで変更を確認します。それらの記録から、失われた構成を再構築できる可能性があります。

CLI を使用した ASA の設定

CDO で提供される CLI インターフェイスで CLI コマンドを実行して、ASA デバイスを設定できます。このインターフェイスを使用するには、[デバイスとサービス]メニューでデバイスを選択し、[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。詳細については、「CDO コマンド ライン インターフェイスの使用」を参照してください。

新しいロギングサーバーの追加

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央 syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。

詳細については、実行している ASA バージョンの『CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide』に含まれる「Logging」の章にある「Monitoring」セクションを参照してください。

DNS サーバーの設定

DNS サーバーを設定して、ASA がホスト名を IP アドレスに解決できるようにする必要があります。また、アクセス ルールに完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを使用するように、DNS サーバーを設定する必要があります。

詳細については、実行している ASA バージョンの『CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide』に含まれる「Basic Settings」の章の「Configure the DNS Server」セクションを参照してください。

静的ルートとデフォルトルートの追加

接続されていないホストまたはネットワークにトラフィックをルーティングするには、スタティックルーティングとダイナミックルーティングのどちらかを使用して、ホストまたはネットワークへのルートを定義する必要があります。

詳細については、『CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide』の「Static and Default Routes」の章を参照してください。

インターフェイスの設定

CLI コマンドを使用して、管理インターフェイスとデータインターフェイスを設定できます。詳細については、『CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide』の「Basic Interface Configuration」の章を参照してください。

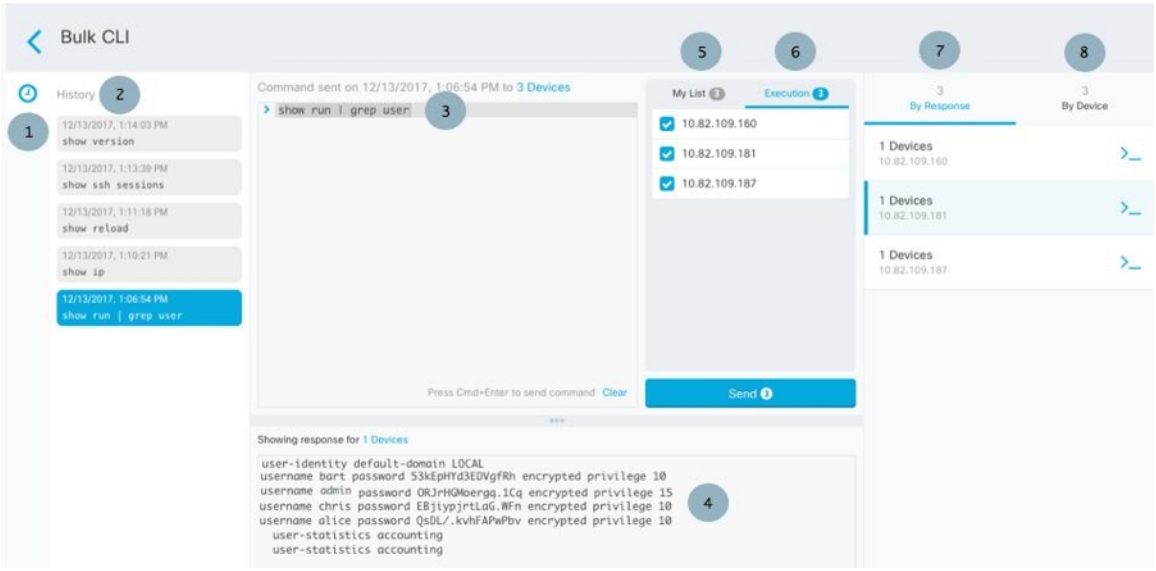
一括コマンド ライン インターフェイス

CDO では、コマンド ライン インターフェイス（CLI）を使用して ASA 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：

- 詳細な ASA CLI のドキュメントについては、ASA コマンド ライン インターフェイスのドキュメント （105 ページ）を参照してくださ
- 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。
4	応答ペイン。CDO は、コマンドに対するデバイスの応答と CDO メッセージを表示します。複数のデバイスの応答が同じだった場合、応答ペインに「X デバイスの応答を表示しています（Showing Responses for X devices）」というメッセージが表示されます。[Xデバイス（X Devices）] をクリックすると、コマンドに対して同じ応答を返したすべてのデバイスが CDO に表示されます。 （注） 次の 2 つの状況で「**完了しました（Done!）**」というメッセージが CDO に表示されます。 • 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。
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。

ケース	説明
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。ASA デバイスが同期されていない場合、そのデバイスで使用可能なコマンドは、`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、`dir`、`write`、`copy` だけです。

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。

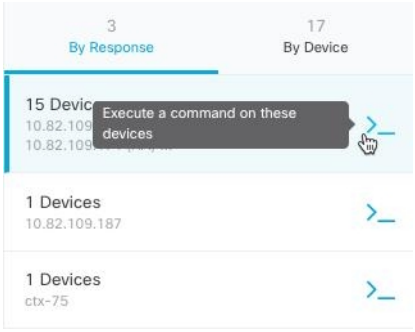
（注） 選択したデバイスのいずれかが同期されていない場合、次のコマンドのみが許可されます：`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、`dir`、`write`、`copy`

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。

ASA一括 CLI の使用例

次の例は、ASA デバイスに対して CDO の一括 CLI 機能を使用するときに発生する可能性のあるワークフローです。

ASA の実行構成ですべてのユーザーを表示し、いずれかのユーザーを削除する

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 [ASA] タブをクリックします。

ステップ 4 ユーザーを削除するデバイスのデバイスリストを検索およびフィルタ処理し、デバイスを選択します。

（注） 選択したデバイスが同期されていることを確認してください。デバイスが同期されていない場合、次のコマンドのみが許可されます。`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、`dir`、`copy`、および `write`。

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。CDO は、[マイリスト] ペインで選択したデバイスを一覧表示します。少数のデバイスにコマンドを送信する場合は、そのリストにあるデバイスのチェックを外します。

ステップ 6 コマンドペインで、`show run | grep user` と入力し、[送信（Send）] をクリックします。文字列 user を含む実行構成ファイルのすべての行が、応答ペインに表示されます。[実行（Execution）] タブが開き、コマンドが実行されたデバイスが表示されます。

ステップ 7 [応答別（By Response）] タブをクリックし、応答を確認して、削除するユーザーが含まれているデバイスを確認します。

ステップ 8 [マイリスト] タブをクリックし、ユーザーを削除するデバイスのリストを選択します。

ステップ 9 コマンドペインで、user コマンドの no 形式を入力して user2 を削除し、[送信（Send）] をクリックします。この例では、user2 を削除します。

```
no user user2 password reallyhardpassword privilege 10
```

ステップ 10 ユーザー名の検索に使用した、`show run | grep user` コマンドのインスタンスの履歴パネルを確認します。このコマンドを選択し、[実行（Execution）] リストでデバイスのリストを確認して、[送信（Send）] を選択します。指定したデバイスからユーザー名が削除されたことがわかります。

ステップ 11 実行構成から正しいユーザーを削除し、実行構成に残っているユーザーが正しいことを確認したら、次の手順を実行します。

1. 履歴ペインから `no user user2 password reallyhardpassword privilege 10` コマンドを選択します。
2. [デバイス別（By Device）] タブをクリックし、[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。
3. コマンドペインで、[クリア] をクリックしてコマンドペインをクリアします。
4. `deploy memory` コマンドを入力し、[送信（Send）] をクリックします。

選択した ASA 上のすべての SNMP 設定を見つける

この手順で、ASA の実行構成にあるすべての SNMP 構成エントリを表示できます。

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 [ASA] タブをクリックします。

ステップ 4 実行構成の SNMP 構成を分析するデバイスをフィルタ処理して検索し、それらを**選択**します。

（注） 選択したデバイスが同期されていることを確認してください。デバイスが同期されていない場合、次のコマンドのみが許可されます。`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、および `dir`。

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] をクリックします。選択したデバイスは [マイリスト] ペインに表示されます。少数のデバイスにコマンドを送信する場合は、そのリストにあるデバイスのチェックを外します。

ステップ 6 コマンドペインで、`show run | grep snmp` と入力し、[送信] をクリックします。文字列 snmp を含む実行構成ファイルのすべての行が、応答ペインに表示されます。[実行] タブが開き、コマンドが実行されたデバイスが表示されます。

ステップ 7 応答ペインでコマンド出力を確認します。

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 ASA 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。ASA 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） • 詳細な ASA CLI ドキュメントについては、ASA コマンドライン インターフェイスのドキュメント （105 ページ） を参照してください。

ステップ 2 ナビゲーションバーで、[デバイスとサービス] 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 マクロに一意の名前を指定します。必要に応じて、CLI マクロの説明とメモを入力します。

ステップ 8 [コマンド] 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。

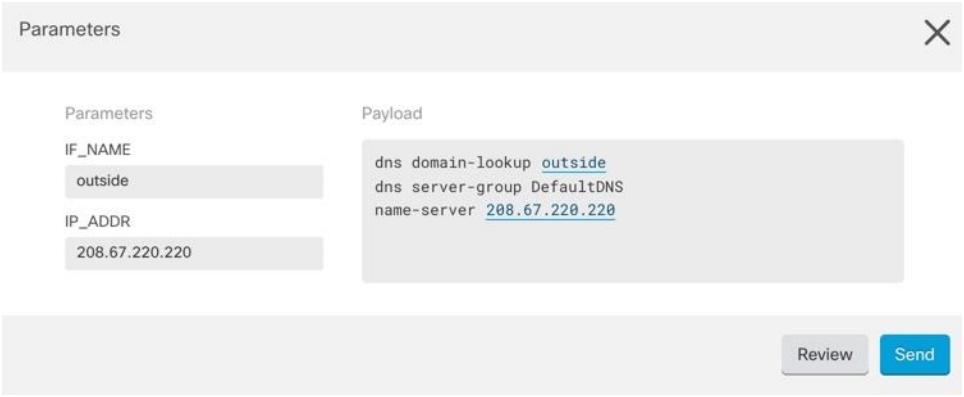
ステップ 5 コマンドパネルで、スター をクリックします。

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。

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



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

- ASA の場合は、実行構成が更新されます。

ステップ 10 コマンドを送信した後で、「一部のコマンドが実行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。

- [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 ASA 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。

ASA コマンド ライン インターフェイスのドキュメント

CDO は、ASA コマンドラインインターフェイスをすべてサポートしています。ユーザーが単一のデバイスおよび複数のデバイスに同時にコマンドを送信できるように、CDO ではターミナル型のインターフェイスを提供しています。ASA コマンドラインインターフェイスのドキュメントは豊富です。CDO ドキュメントでその一部を再作成するのではなく、Cisco.com の ASA CLI ドキュメントへのポインタを次に示します。

ASA CLI コンフィギュレーション ガイド

ASA バージョン 9.1 以降、ASA CLI コンフィギュレーション ガイドは 3 部に分かれています。

- CLI ブック 1：Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）
- CLI ブック 2: Cisco ASA シリーズ ファイアウォール CLI コンフィグレーションガイド
- CLI ブック 3：Cisco ASA シリーズ VPN CLI コンフィギュレーション ガイド

[サポート（Support）] > [製品カテゴリ（Products by Category）] > [セキュリティ（Security）] > [ファイアウォール（Firewalls）] > [ASA 5500] > [コンフィギュレーション（Configure）] > [コンフィギュレーションガイド（Configuration Guides）] に移動すると、Cisco.com の ASA CLI コンフィギュレーション ガイドにアクセスできます。https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

いくつかの特定の ASA CLI コンフィギュレーション ガイドのセクション

show コマンドと more コマンドの出力のフィルタリングCLI ブック 1：『Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）』の「show コマンドと more コマンドの出力のフィルタリング」では、正規表現を使用した show コマンド出力のフィルタ処理について学習できます。

ASA コマンドリファレンス

ASA コマンド リファレンス ガイドは、すべての ASA コマンドとそのオプションがアルファベット順でリストになっています。ASA コマンドリファレンスはバージョン固有ではありません。次の 4 部が公開されています。

- Cisco ASA シリーズ コマンド リファレンス、A ～ H コマンド
- Cisco ASA シリーズ コマンド リファレンス、I ～ R コマンド
- Cisco ASA シリーズ コマンド リファレンス、S コマンド
- Cisco ASA シリーズ コマンド リファレンス、T ～ Z コマンドおよび ASASM 用 IOS コマンド

[サポート（Support）] > [製品カテゴリ（Products by Category）] > [セキュリティ（Security）] > [ファイアウォール（Firewalls）] > [ASA 5500] > [リファレンスガイド（Reference Guides）] > [コマンドリファレンス（Command References）] に移動すると、Cisco.com の ASA コマンドリファレンスガイドにアクセスできます。https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html#anchor325

CLI コマンドの結果のエクスポート

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

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

CLI コマンドの結果のエクスポート

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

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
ステップ 3 適切なデバイスタイプのタブをクリックします。
ステップ 4 1 つまたは複数のデバイスを選択してハイライトします。
ステップ 5 デバイスの [デバイスアクション] ペインで、>_ [コマンド ライン インターフェイス（Command Line Interface）] をクリックします。
ステップ 6 [コマンドラインインターフェイス（Command Line Interface）] ペインでコマンドを入力し、[送信（Send）] をクリックしてデバイスに送ります。
ステップ 7 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。
ステップ 8 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。.csv ファイル上のコマンド出力を読み取る場合、すべてのセルを展開して、コマンドのすべての結果を表示します。

CLI マクロの結果のエクスポート

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

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ます。
ステップ 4 1 つまたは複数のデバイスを選択してハイライトします。
ステップ 5 デバイスの [デバイスアクション] ペインで、[>_コマンド ライン インターフェイス（>_Command Line Interface）] をクリックします。
ステップ 6 CLI ウィンドウの左側のペインで、CLI マクロのお気に入りを示す星を選択します。
ステップ 7 エクスポートするマクロコマンドをクリックします。適切なパラメータを入力し、[送信（Send）] をクリックします。
ステップ 8 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。
ステップ 9 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。.csv ファイル上のコマンド出力を読み取る場合、すべてのセルを展開して、コマンドのすべての結果を表示します。

CLI コマンド履歴のエクスポート

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

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] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
ステップ 3 適切なデバイスタイプのタブをクリックします。
ステップ 4 1 つまたは複数のデバイスを選択してハイライトします。
ステップ 5 デバイスの [デバイスアクション] ペインで、[>_コマンド ライン インターフェイス（>_Command Line Interface）] をクリックします。
ステップ 6 履歴ペインがまだ展開されていない場合は、[時計（Clock）] アイコン をクリックして展開します。
ステップ 7 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。
ステップ 8 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。.csv ファイル上のコマンド出力を読み取る場合、すべてのセルを展開して、コマンドのすべての結果を表示します。

関連情報：

- CDO コマンド ライン インターフェイスを使用する （88 ページ）
- 新規コマンドからの CLI マクロの作成
- CLI マクロの削除
- CLI マクロの編集
- CLI マクロの実行
- ASA一括 CLI の使用例
- ASA コマンド ライン インターフェイスのドキュメント
- 一括コマンド ライン インターフェイス

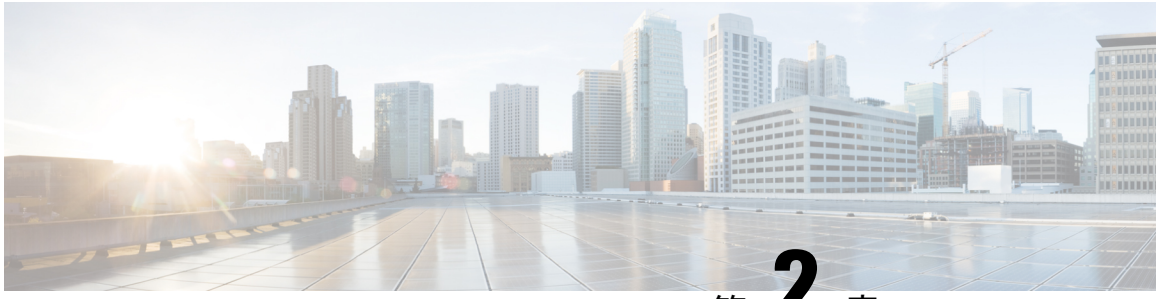
CLI マクロのリストをエクスポートする

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

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] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
ステップ 3 適切なデバイスタイプのタブをクリックします。
ステップ 4 1 つまたは複数のデバイスを選択してハイライトします。
ステップ 5 デバイスの [デバイスアクション] ペインで、[>_コマンド ライン インターフェイス] をクリックします。
ステップ 6 CLI ウィンドウの左側のペインで、CLI マクロのお気に入りを示す星を選択します。
ステップ 7 エクスポートするマクロコマンドをクリックします。適切なパラメータを入力し、[送信] をクリックします。

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

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



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。

ASA デバイスの導入準備

この手順を使用して、ASA モデルではなく単一のライブ ASA デバイスを CDO に導入準備します。複数の ASA を一度に導入準備する場合は、「一括での ASA の導入準備」を参照してください。

始める前に

デバイスの前提条件

- Cisco Defense Orchestrator の管理対象デバイスへの接続 （5 ページ）を確認してください。
- ASA の実行構成ファイルは 4.5 MB 未満である必要があります。実行構成ファイルのサイズを確認するには、「ASA 実行設定サイズを確認する」を参照してください。
- IP アドレッシング：各 ASA、ASAv、または ASA セキュリティコンテキストには一意の IP アドレスが必要であり、SDC は管理トラフィックを受信するように設定されたインターフェイスでその IP アドレスに接続する必要があります。

証明書の前提条件

ASA デバイスに互換性のある証明書が存在しない場合、デバイスの導入準備が失敗する可能性があります。次の要件が満たされていることを確認します。

- デバイスで TLS バージョン 1.0 以降を使用している。
- 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）。
- 証明書は、SHA-256 証明書であること。SHA1 証明書は受け入れられません。
- 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。

導入準備プロセス中に証明書エラーが発生した場合は、詳細について証明書エラーのため ASA の導入準備ができない （506 ページ）を参照してください。

オープン SSL 暗号の前提条件

互換性のある SSL 暗号スイートがデバイスにない場合、デバイスは Secure Device Connector（SDC）と正常に通信できません。次のいずれかの暗号スイートを使用します。

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA384

- ECDHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA256

ASA で使用する暗号スイートがこのリストにない場合、SDC はそれをサポートしていないため、ASA の暗号スイートの更新必要があります。

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 青色のプラスボタン  をクリックして、ASA を導入準備します。

ステップ 3 [ASA] タイルをクリックします。

ステップ 4 [デバイスの特定（Locate Device）] ステップで、次の手順を実行します。

1. [Secure Device Connector] ボタンをクリックし、ネットワークにインストールされている Secure Device Connector を選択します。SDC を使用しない場合、CDO は Cloud Connector を使用して ASA に接続できます。どちらを選択するかは、Cisco Defense Orchestrator の管理対象デバイスへの接続方法によって異なります。
2. デバイスに名前を付けます。
3. デバイスまたはサービスのロケーション（IP アドレス、FQDN、または URL）を入力します。デフォルトのポートは 443 です。
4. **[Next]** をクリックします。

ステップ 5 [ログイン情報（Credentials）] ステップで、CDO がデバイスへの接続に使用する、ASA 管理者または同様の最高特権の ASA ユーザーのユーザー名とパスワードを入力し、[次へ] をクリックします。

ステップ 6 （オプション）[完了（Done）] ステップで、デバイスのラベルを入力します。このラベルでデバイスのリストをフィルタリングできます。詳細については、ラベルとフィルタ処理に関するトピックを参照してください。

ステップ 7 デバイスまたはサービスにラベルを設定すると、[デバイスとサービス] リストに表示できます。

（注） 設定のサイズ、および他のデバイスまたはサービスの数によっては、設定の分析に時間がかかる場合があります

高可用性ペアの一部である ASA のオンボーディング

ハイアベイラビリティペアの一部である ASA を導入準備する場合は、ASA デバイスの導入準備 （111 ページ） を使用してペアのプライマリデバイスのみを導入準備します。

マルチコンテキストモードでの ASA の導入準備

マルチコンテキストモードについて

物理アプライアンスにインストールされている単一の ASA を、コンテキストと呼ばれる複数の論理デバイスに分割できます。マルチコンテキストモードで設定された ASA で使用される設定には、次の 3 種類があります。

- セキュリティコンテキスト
- 管理コンテキスト
- システム設定

セキュリティ コンテキストについて

各セキュリティコンテキストは、独自のセキュリティポリシー、インターフェイス、および管理者を持つ独立したデバイスとして機能します。複数のセキュリティコンテキストは、複数のスタンドアロンデバイスを持つことに似ています。セキュリティコンテキストは、プライベート クラウド インフラストラクチャにインストールされた仮想マシンイメージという意味での仮想 ASA ではありません。セキュリティコンテキストは、ハードウェアアプライアンスにインストールされた ASA で設定されます。各コンテキストは、そのアプライアンスの物理インターフェイスで設定されます。

マルチコンテキストモードの詳細については、ASA CLI および ASDM のコンフィギュレーション ガイド [英語] を参照してください。

CDO は、各セキュリティコンテキストを個別の ASA として導入準備し、個別の ASA であるかのように管理します。

管理コンテキストについて

管理コンテキストはセキュリティコンテキストと似ていますが、管理コンテキストにログインしたユーザーは、システム管理者権限を持つので、システムコンテキストや他のすべてのコンテキストにアクセスできる点が異なります。管理コンテキストは制限されていないため、通常のコンテキストとして使用できます。ただし、管理コンテキストにログインすると、すべてのコンテキストへの管理者特権が付与されるため、場合によっては、管理コンテキストへのアクセスを適切なユーザーに制限する必要があります。

CDO は、各管理コンテキストを個別の ASA として導入準備し、個別の ASA であるかのように管理します。CDO は、アプライアンスの ASA および ASDM ソフトウェアをアップグレードするときにも管理コンテキストを使用します。

システムの設定について

システム管理者は、各コンテキストコンフィギュレーションの場所、割り当てられたインターフェイス、およびその他のコンテキスト操作パラメータをシステム コンフィギュレーションに設定することで、コンテキストを追加および管理します。このコンフィギュレーションは、シ

ングルモードのコンフィギュレーション同様、スタートアップコンフィギュレーションです。システム コンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバーからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

CDO はシステム設定を導入準備しません。

セキュリティおよび管理コンテキストの導入準備の前提条件

セキュリティおよび管理コンテキストを導入準備するための前提条件は、他の ASA を導入準備する場合と同じです。前提条件のリストについては、ASA デバイスの導入準備 （111 ページ）を参照してください。

マルチコンテキストモードで ASA をサポートする Cisco アプライアンスについては、実行している ASA ソフトウェアバージョンの CLI ブック 1：Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）[英語] の「Multiple Context Mode」の章を参照してください。

シングル コンテキスト ファイアウォールとして実行されている ASA、およびマルチコンテキスト ファイアウォールの管理コンテキストでは、ASDM および CDO アクセスにさまざまなポート番号を使用できます。ただし、セキュリティコンテキストの場合、ASDM および CDO アクセスポートはポート 443 に固定されています。これは ASA の制限です。

ASA セキュリティおよび管理コンテキストの導入準備

セキュリティコンテキストまたは管理コンテキストを導入準備する方法は、他の ASA を導入準備する場合と同じです。導入準備の手順については、ASA デバイスの導入準備 （111 ページ）または一括での ASA の導入準備 （115 ページ）を参照してください。

セキュリティコンテキストのアップグレード

CDO は、マルチコンテキスト ASA の各セキュリティおよび管理コンテキストを個別の ASA として扱い、個別に導入準備します。ただし、マルチコンテキスト ASA のすべてのセキュリティおよび管理コンテキストは、アプライアンスにインストールされている同じバージョンの ASA ソフトウェアを実行します。

ASA のセキュリティコンテキストで使用される ASA および ASDM のバージョンをアップグレードするには、管理コンテキストを導入準備し、そのコンテキストでアップグレードを実行します。詳細については、単一 ASA 上の ASA と ASDM イメージのアップグレード （124 ページ）またはASA および ASDM の一括アップグレード （121 ページ） ASA および ASDM の一括アップグレード （121 ページ）を参照してください。

一括での ASA の導入準備

Cisco Defense Orchestrator（CDO）を使用すると、.csv ファイルですべての ASA に必要な情報を提供することで、ASA を一括で導入準備できます。ASA が導入準備されているときに、フィ

ルタペインを使用して、キューに入っている、ロードされている、完了している、または失敗した導入準備の試行を表示できます。

始める前に

- Cisco Defense Orchestrator の管理対象デバイスへの接続 （5 ページ）を確認してください。
- 導入準備する ASA の接続情報を含む .csv ファイルを準備します。1 つの ASA に関する情報を独自の行に追加します。行の先頭に # を使用して、コメントを示すことができます。
  - ASA の場所（IP アドレスまたは FQDN）
  - ASA 管理者ユーザー名
  - ASA 管理者パスワード
  - （任意）CDO のデバイス名
  - SDCName フィールドで、CDO を ASA に接続するために使用するネットワーク内の Secure Device Connector（SDC）の名前を指定します。SDC を使用して ASA を CDO に接続しない場合は、「none」と入力することもできます。デバイスを導入準備するときに、SDCName フィールドに「none」と指定すると、Cloud Connector を使用して ASA が導入準備されます。Cloud Connector を使用すると、SDC をインストールせずにデバイスを CDO に接続できます。どちらを選択するかは、Cisco Defense Orchestrator の管理対象デバイスへの接続方法によって異なります。
  - （任意）CDO のデバイスラベル
  - ラベルを 1 つ追加するには、ラベル名を最後の CSV フィールドに追加します。
  - デバイスに複数のラベルを追加するには、値を引用符で囲みます。例：`alpha,beta,gamma`。
  - カテゴリと選択肢のラベルを追加するには、2 つの値をコロン（:）で区切ります。例：`Rack:50`。

構成ファイルの例：

```
#Location,Username,Password,DeviceName,SDCName,DeviceLabel
192.168.3.2,admin,CDO123!,ASA3,sdc1,"HA-1,Rack:50"
192.168.4.2,admin,CDO123!,ASA4,sdc1,"HA-1,Rack:50"
ASA2.example.com,admin,CDO123!,ASA2,none,Rack:51
asav.virtual.io,admin,CDO123!,ASA-virtual,sdc3,Test
```

注意 CDO は .csv ファイル内のデータを検証しないため、エントリの正確性を保証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] をクリックします。

ステップ 2 青色のプラスボタン  をクリックして、ASA を導入準備します。

ステップ 3 [導入準備（Onboarding）] ページで、[複数のASA（Multiple ASAs）] タイルをクリックします。

ステップ 4 [参照] をクリックして、ASA エントリを含む .csv ファイルを見つけます。指定したデバイスは、導入準備の準備ができている [ASA一括導入準備（ASA Bulk Onboarding）] テーブルのキューに入れられました。

注意 導入準備プロセスが完了するまで、[ASA一括導入準備（ASA Bulk Onboarding）] ページから移動しないでください。移動すると、導入準備プロセスが停止します。

ステップ 5 [開始（Start）] をクリックします。[ASA一括導入準備（ASA Bulk Onboarding）] テーブルのステータス列に、導入準備プロセスの進行状況が表示されます。デバイスが正常に導入準備されると、ステータスが [完了（Complete）] に変わります。

次のタスク

一括導入準備を一時停止し、後で再開する必要がある場合は、一括導入準備を一時停止、再開する （117 ページ）を参照してください。

.

一括導入準備を一時停止、再開する

導入準備プロセスを一時停止する必要がある場合は、[一時停止（Pause）]をクリックします。CDO は、導入準備を開始したデバイスの導入準備を終了します。一括導入準備プロセスを再開するには、[開始（Start）]をクリックします。CDOは、キューに入った次のデバイスの導入準備を開始します。

[一時停止（Pause）]をクリックしてこのページから移動した場合は、このページに戻って、最初から一括導入準備手順を最初から再度実行する必要があります。ただし、CDO は既に導入準備されたデバイスを認識し、このデバイスを新しい導入準備試行で「重複」としてマークし、リストをすばやく移動して、キューに入ったデバイスを導入準備します。

ASA モデルの作成とインポート

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 [ASA] タブをクリックします。

ステップ 4 ASA デバイスを選択し、左側のペインの [管理] で、[設定（Configuration）] をクリックします。

ステップ 5 [ダウンロード（Download）]をクリックしてデバイス設定をローカルコンピュータにダウンロードします。

ASA 設定のインポート

注意：導入準備する ASA 実行設定ファイルは 4.5 MB 未満である必要があります。導入準備する前に、設定ファイルのサイズを確認してください。

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 青いプラス（  ）ボタンをクリックして、設定をインポートします。

ステップ 3 [オフライン管理用設定のインポート（Import configuration for offline management）] をクリックします。

ステップ 4 [デバイスタイプ（Device Tipe）] で [ASA] を選択します。

ステップ 5 [参照] をクリックし、アップロードする設定ファイル（テキスト形式）を選択します。

ステップ 6 設定が確認されると、デバイスまたはサービスにラベルを設定するよう求められます。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。

ステップ 7 モデルデバイスにラベルを設定した後、[デバイスとサービス] リストで確認できます。

（注） 設定のサイズ、および他のデバイスまたはサービスの数によっては、設定の分析に時間がかかる場合があります

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。

オフライン管理用にデバイスの設定をインポートする

オフライン管理用にデバイスの設定をインポートすると、ネットワーク内の稼働中のデバイスを操作することなく、デバイスの設定を確認して最適化できます。CDO では、アップロードされたこれらの設定ファイルは「モデル」とも呼ばれます。

以下のデバイスの設定を CDO にインポートできます。

- 適応型セキュリティアプライアンス（ASA）。「ASA モデルの作成とインポート」を参照してください。
- Firepower Threat Defense（FTD）。
- Aggregation Services Routers（ASR）や Integrated Services Routers（ISR）などの Cisco IOS デバイス。

ASA と ASDM のアップグレードの前提条件

Cisco Defense Orchestrator（CDO）では、ASA および ASDM イメージのアップグレードに役立つウィザードが提供されます。個別の ASA、複数の ASA、アクティブ/スタンバイ構成の ASA、およびシングルコンテキストモードまたはマルチコンテキストモードで実行されている ASA にインストールされているイメージが対象です。

CDO は、アップグレード可能な ASA および ASDM イメージのリポジトリを保持します。CDO のイメージリポジトリからアップグレードイメージを選択すると、CDO は必要なすべてのアップグレード手順をバックグラウンドで実行します。このウィザードに従って、互換性のある ASA ソフトウェアおよび ASDM イメージを選択してインストールし、デバイスを再起動してアップグレードを完了するプロセスを実行できます。CDO で選択したイメージが ASA にコピーおよびインストールされているものであることを検証することにより、アップグレードプロセスを保護します。CDO は、定期的に ASA バイナリのインベントリを確認し、最新の ASA および ASDM イメージが利用可能になったときに、それらをリポジトリに追加します。これは、ASA にインターネットへのアウトバウンドアクセスがある場合に最適なオプションです。

CDO のイメージリポジトリには、一般的に利用可能な（GA）イメージのみが含まれています。リストに特定の GA イメージがない場合は、[サポートに連絡（Contact Support）] ページから Cisco TAC または電子メールサポートにお問い合わせください。確立されたサポートチケット SLA によってリクエストを処理し、リストにない GA イメージをアップロードします。

ASA にインターネットへのアウトバウンドアクセスがない場合は、必要な ASA イメージおよび ASDM イメージを Cisco.com からダウンロードして独自のリポジトリに保存し、アップグレードウィザードにそれらのイメージへのカスタム URL を入力できます。そうすると、CDO はそれらのイメージを使ってアップグレードを実行します。とはいえ、このケースでは、アップグレードするイメージを自分で決定することになります。CDO は、イメージの完全性チェックやディスク容量チェックを実施しません。FTP、TFTP、HTTP、HTTPS、SCP、および SMB のいずれかのプロトコルを使用して、リポジトリからイメージを取得できます。

設定要件

- ASA で DNS を有効にする必要があります。
- CDOのイメージリポジトリからアップグレードイメージを使用する場合、ASAはインターネットにアクセスできる必要があります。
- ASA は CDO に正常に導入準備されている必要があります。
- ASA で CDO に同期している必要があります。
- ASA はオンラインになっている必要があります。
- カスタム URL アップグレードの場合：『Cisco ASA Upgrade Guide』を使用して、使用している ASA と互換性のある ASA および ASDM のバージョンを確認してください。
- カスタム URL アップグレードの場合：イメージリポジトリに ASA イメージおよび ASDM イメージをダウンロードしてください。
- カスタム URL アップグレードの場合：ASA がイメージリポジトリにアクセスできることを確認してください。
- カスタムURLアップグレードの場合：ASAおよびASDMイメージ用にASAに十分なディスク容量があることを確認してください。
- カスタム URL アップグレードの場合：URL シンタックスの詳細については、「カスタム URL のアップグレード」を参照してください。

1000 および 2000 シリーズの設定の前提条件

- 2000 シリーズ デバイスの FXOS モードは、**アプライアンス**モードに設定する必要があります。詳細については、「アプライアンスまたはプラットフォームモードへの Firepower 2100 の設定」を参照してください。
- デバイスは、ASA バージョン 9.13(1) **以降**を実行している必要があります。
- ASA ソフトウェアをアップグレードする前に、FXOSバンドルをアップグレードする必要があります。詳細については、「Firepower 2100 ASA and FXOS Compatibility」を参照してください。

ASA を実行中の 4100 および 9300 シリーズ

CDO は、4100 または 9300 シリーズ デバイスのアップグレードをサポートしていません。これらのデバイスは CDO の外部でアップグレードする必要があります。

アップグレードのガイドライン

- CDOは、アクティブ/スタンバイ「フェールオーバー」ペアとして設定されたASAをアップグレードできます。CDO は、アクティブ/アクティブ「クラスタ化」ペアで設定された ASA をアップグレードできません。

ソフトウェアおよびハードウェア要件

アップグレード可能な ASA および ASDM の最小バージョン：

- ASA：ASA 9.1.2
- ASDM：最小バージョンなし

サポート対象のハードウェアバージョン

- 「CDO でサポートされるソフトウェアとハードウェア」を参照してください。

ASA および ASDM の一括アップグレード

ステップ 1 ASA および ASDM イメージのアップグレードに関するアップグレード要件と重要な情報については、「ASA と ASDM のアップグレードの前提条件」を参照してください。

（注） ASA 1000 または 2000 シリーズデバイスをアップグレードする場合は、「ASA と ASDM のアップグレードの前提条件」を必ずお読みください。

ステップ 2 （任意）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、変更リクエスト管理を作成して、このアクションによってアップグレードされたデバイスを変更ログで識別します。

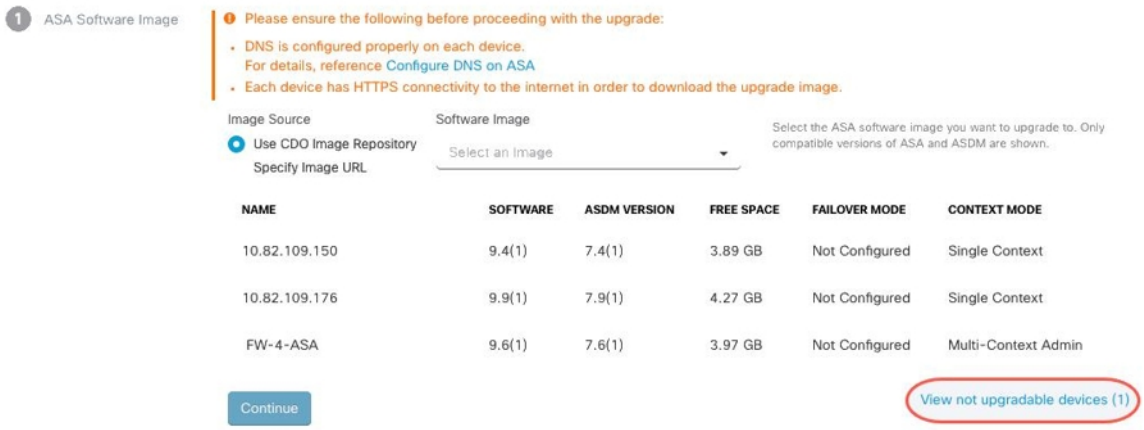
ステップ 3 [デバイス] タブをクリックします。

ステップ 4 フィルタを使用して、一括アップグレードに含めるデバイスのリストを絞り込みます。フィルタ （85 ページ）

ステップ 5 フィルタ処理されたデバイスのリストから、アップグレードするデバイスを選択します。

ステップ 6 [デバイスアクション（Device Actions）] ペインで、[アップグレード（Upgrade）] をクリックします。

ステップ 7 [デバイスの一括アップグレード（Bulk Device Upgrade）]ページに、アップグレード可能なデバイスが表示されます。選択したどのデバイスもアップグレードできない場合、CDO にはアップグレードできないデバイスのリンクが表示されます。



ステップ 8 ステップ 1 で、[CDOイメージリポジトリの使用（Use CDO Image Repository]）] をクリックしてアップグレードする ASA ソフトウェアイメージを選択し、[続行] をクリックします。

このリストは、選択したソフトウェアバージョンにアップグレードできる、選択した ASA の数を示しています。次の例では、すべてのデバイスをバージョン 9.9(1.2) にアップグレードでき、2 つのデバイスを

9.8(2)にアップグレードでき、1つのデバイスを9.6(1)にアップグレードできます。

選択したソフトウェアバージョンのいずれかが、選択したいずれのデバイスとも互換性がない場合、CDO は警告を表示します。次の例では、CDO は 10.82.109.176 デバイスを、すでに実行されているバージョンより前のバージョンにアップグレードできません。

NAME	SOFTWARE	ASDM VERSION	FREE SPACE	FAILOVER MODE	CONTEXT MODE
✔ 10.82.109.150	9.4(1)	7.4(1)	3.89 GB	Not Configured	Single Context
✔ FW-4-ASA	9.6(1)	7.6(1)	3.97 GB	Not Configured	Multi-Context Admin
✖ 10.82.109.176	9.9(1)	7.9(1)	4.27 GB	Not Configured	Single Context

ステップ 9 ステップ 2 で、アップグレードする ASDM イメージを選択します。アップグレード可能な ASA と互換性のある ASDM の選択肢のみが表示されます。

ステップ 10 ステップ 3 で、選択内容を確認し、ASA へのイメージのダウンロードのみを実行するか、あるいはイメージをコピーしてインストールしデバイスを再起動するかを決定します。

ステップ 11 準備ができたら、[アップグレードの実行（Perform Upgrade）] をクリックします。

（注） アップグレードが失敗すると、CDO からメッセージが表示されます。アップグレードの失敗は、多くの場合、ネットワークの問題によって ASA イメージと ASDM イメージの ASA への転送が阻害されることが原因です。

ステップ 12 後で CDO にアップグレードを実行させる場合は、[アップグレードのスケジュール設定（Schedule Upgrade）] チェックボックスをオンにします。フィールドをクリックして、将来の日時を選択します。日時の選択が完了したら、[アップグレードのスケジュール設定（Schedule Upgrade）] ボタンをクリックします。

ステップ 13 （マルチコンテキストモードの場合）管理コンテキストとセキュリティコンテキストが起動すると、セキュリティコンテキストに「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表示されることがあります。このメッセージが表示された場合は、すべてのセキュリティコンテキストの証明書を受け入れます。アップグレードによって生じる他のすべての変更も受け入れます。

ステップ 14 [通知（notifications）] タブで一括アップグレードアクションの進行状況を確認します。[ジョブ（Jobs）] ページ（336ページ）一括アップグレード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] ページに移動します。[ジョブ（Jobs）] ページ （336 ページ）

ステップ 15 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。

独自のリポジトリからのイメージを含む複数のASAのアップグレード

ステップ 1 ASA および ASDM イメージのアップグレードに関するアップグレード要件と重要な情報については、「ASA と ASDM のアップグレードの前提条件」を参照してください。

ステップ 2 （オプション）[デバイスとサービス] をクリックし、変更リクエスト管理を作成して、このアクションによってアップグレードされたデバイスを変更ログで識別します。

ステップ 3 [デバイス] タブをクリックします。

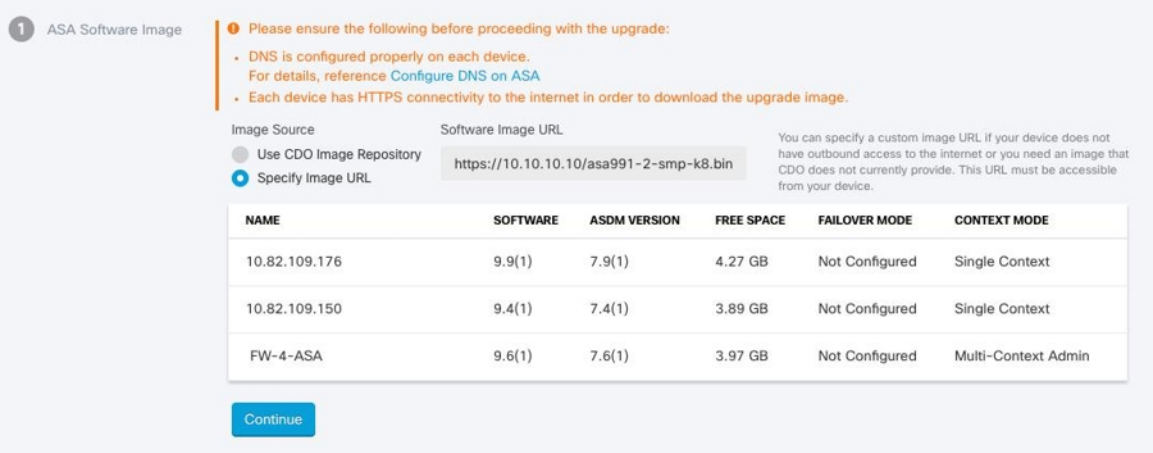
ステップ 4 フィルタ （85 ページ） を使用して、一括アップグレードに含めるデバイスのリストを絞り込みます。

ステップ 5 フィルタ処理されたデバイスのリストから、アップグレードするデバイスを選択します。

ステップ 6 [デバイスアクション（Device Actions）] ペインで、[アップグレード（Upgrade）] をクリックします。

ステップ 7 手順 1 で、[イメージURLの指定（Specify Image URL）] をクリックし、アップグレードする ASA イメージを [ソフトウェアイメージURL（Software Image URL）] フィールドで選択して、[続行] をクリックします。URL シンタックスの詳細については、「カスタム URL のアップグレード」を参照してください。

（注） 下の図は、[ソフトウェアイメージURL（Software Image URL）] フィールドに表示された HTTPS URL を示しています。FTP、TFTP、HTTP、HTTPS、SCP、および SMB のいずれかのプロトコルを使用して、リポジトリからイメージを取得できます。URL シンタックスの詳細については、「カスタム URL のアップグレード」を参照してください。



ステップ 8 手順 2 で、[イメージURLの指定（Specify Image URL）] をクリックし、アップグレードする ASDM イメージを [ソフトウェアイメージURL（Software Image URL）] フィールドで選択して、[続行] をクリックします。

ステップ 9 手順 3 で、選択内容を確認し、ASA へのイメージのダウンロードのみを実行するか、それともイメージをコピーしてインストールしデバイスを再起動するかを決定します。

ステップ 10 準備ができたら、[アップグレードの実行（Perform Upgrade）] をクリックします。

（注） アップグレードに失敗すると、CDO にメッセージが表示されます。アップグレードの失敗は、多くの場合、ネットワークの問題によって ASA イメージと ASDM イメージの ASA への転送が阻害されることが原因です。

ステップ 11 後で CDO にアップグレードを実行させる場合は、[アップグレードのスケジュール設定（Schedule Upgrade）] チェックボックスをオンにします。フィールドをクリックして、将来の日時を選択します。日時の選択が完了したら、[アップグレードのスケジュール設定（Schedule Upgrade）] ボタンをクリックします。

ステップ 12 （マルチコンテキストモードの場合）管理コンテキストとセキュリティコンテキストが起動すると、セキュリティコンテキストに「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表示されることがあります。そのメッセージが表示された場合は、すべてのセキュリティコンテキストの証明書を受け入れます。アップグレードによって生じる他のすべての変更も受け入れます。

ステップ 13 [ジョブ（Jobs）] ページで一括アップグレードアクションの進行状況を確認します。一括アップグレード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、青い [確認] リンクをクリックして [ジョブ（Jobs）] ページに移動します。

ステップ 14 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。

次のタスク

アップグレードに関する注意事項

- [デバイスとサービス] ページを開き、テーブルの [設定ステータス（Configuration Status）] 列を表示して、アップグレードのバッチの進行状況を監視することもできます。
- [デバイスとサービス] ページでデバイスを選択し、[アップグレード] ボタンをクリックすると、一括アップグレードに含まれていた単一のデバイスでの進行状況を表示できます。CDOに、該当するデバイスの [デバイスのアップグレード] ページが表示されます。

単一 ASA 上の ASA と ASDM イメージのアップグレード

単一の ASA 上で ASA および ASDM イメージをアップグレードするには、次の手順に従います。

ステップ 1 ASAおよびASDMイメージのアップグレードに関するアップグレード要件と重要な情報については、「ASA と ASDM のアップグレードの前提条件」を参照してください。

（注） ASA 1000 または 2000 シリーズ デバイスをアップグレードする場合は、「ASA と ASDM のアップグレードの前提条件」を必ずお読みください。

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

ステップ 3 [デバイス] タブをクリックします。

ステップ 4 （オプション）変更リクエスト管理を作成して、このアクションによってアップグレードされたデバイスを変更ログで識別します。

ステップ 5 アップグレードするデバイスを選択します。

ステップ 6 [デバイスアクション（Device Actions）] ペインで、[アップグレード（Upgrade）] をクリックします。

ステップ 7 [デバイスのアップグレード] ページで、ウィザードに表示される指示に従います。

1. 手順 1 で、[CDOイメージリポジトリの使用（Use CDO Image Repository]）] をクリックしてアップグレードする ASA ソフトウェアイメージを選択し、[続行] をクリックします。

   （注） ASA および ASDM を独自のリポジトリに保存されたイメージにアップグレードする場合、[メージURLの指定] を選択して、[ソフトウェアイメージのURL] フィールドに ASA または ASDM イメージの URL を入力します。FTP、TFTP、HTTP、HTTPS、SCP、および SMB のいずれかのプロトコルを使用して、リポジトリからイメージを取得できます。URL シンタックスの詳細については、「カスタム URL のアップグレード」を参照してください。

   （オプション）後で CDO にアップグレードを実行させる場合は、[アップグレードのスケジュール設定]チェックボックスをオンにします。フィールドをクリックして、将来の日時を選択します。日時の選択が完了したら、[アップグレードのスケジュール設定]ボタンをクリックします。

2. 手順 2 で、アップグレードする ASDM イメージを選択します。アップグレード可能な ASA と互換性のある ASDM の選択肢のみが表示されます。

3. 手順 3 で、選択内容を確認し、ASA へのイメージのダウンロードのみを実行するか、それともイメージをコピーしてインストールしデバイスを再起動するかを決定します。

ステップ 8 準備ができたら、[アップグレードの実行（Perform Upgrade）] をクリックします。

ステップ 9 （マルチコンテキストモードの場合）管理コンテキストとセキュリティコンテキストが起動すると、セキュリティコンテキストに「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表示されることがあります。このメッセージが表示された場合は、すべてのセキュリティコンテキストの証明書を受け入れます。アップグレードによって生じる他のすべての変更も受け入れます。デモを確認しますか？この手順のスクリーンキャストをご覧ください。

次のタスク

アップグレードに関する注意事項

- アップグレードするイメージを選択した後で気が変わった場合は、ソフトウェアイメージに関連付けられている [アップグレードをスキップ（Skip Upgrade）] チェックボックスをオンにします。イメージはデバイスにコピーされず、デバイスがイメージでアップグレードされることもありません。
- アップグレードの実行手順で、イメージを ASA にコピーすることだけを選択した場合は、後で [デバイスのアップグレード] ページに戻り、[今すぐアップグレード（Upgrade Now）] をクリックしてアップグレードを実行できます。コピータスクが完了すると、[デバイス

とサービス] ページにそのデバイスの「アップグレードの準備ができました」というメッセージが表示されます。

- イメージのコピー、インストール、デバイスの再起動のプロセス中は、デバイスでアクションを実行できません。イメージをインストールしてから再起動するデバイスは、[デバイスとサービス] ページで「アップグレード中」と表示されます。
- アップグレードプロセス中、つまりイメージのインストールおよびデバイスの再起動を行っている間は、デバイスでアクションを実行することはできません。
- イメージをデバイスにコピーすることのみを選択した場合、デバイス上でアクションを実行できます。イメージをコピーしているデバイスは、[デバイスとサービス] ページで [イメージをコピーしています] と表示されます。
- 自己署名証明書を持つデバイスをアップグレードすると、問題が発生する可能性があります。詳細については、「新規証明書の問題のトラブルシュート」を参照してください。

アクティブ/スタンバイペアの ASA と ASDM イメージのアップグレード

アクティブ/スタンバイ フェールオーバー モードで ASA のペアをアップグレードする前に、以下の前提条件を確認してください。ASA の設定方法、およびフェールオーバーモードでの動作方法についての詳細については、ASA のマニュアルの「Failover for High Availability」を参照してください。

デモを確認する場合は、この手順のスクリーンキャストをご覧ください。

前提条件

- ASA および ASDM イメージのアップグレードに関する要件と重要な情報については、「ASA と ASDM のアップグレードの前提条件」を参照してください。
- プライマリ（アクティブ）およびセカンダリ（スタンバイ）の ASA は、アクティブ/スタンバイ フェールオーバー モードで設定されています。
- プライマリ ASA は、アクティブ/スタンバイペアのアクティブデバイスです。プライマリ ASA が非アクティブの場合、CDO はアップグレードを実行しません。
- プライマリとセカンダリの ASA ソフトウェアバージョンは同じです。

ワークフロー

これは、CDO が ASA のアクティブ/スタンバイペアをアップグレードするプロセスです。

ステップ 1 CDO は、ASA および ASDM イメージを両方の ASA にダウンロードします。

（注） ユーザーは、ASA および ASDM イメージのダウンロードを選択できますが、すぐにはアップグレードできません。ASA および ASDM イメージが以前にダウンロードされている場合、CDO はそれらのイメージを再度ダウンロードせず、次の手順でアップグレードワークフローを続行します。

ステップ 2 CDO は、最初にセカンダリ ASA をアップグレードします。

ステップ 3 アップグレードが完了し、セカンダリ ASA が [スタンバイ準備完了（Standby-Ready）] 状態に戻ると、CDO はフェールオーバーを開始し、セカンダリ ASA がアクティブ ASA になります。

ステップ 4 CDO は、現在のスタンバイ ASA であるプライマリ ASA をアップグレードします。

ステップ 5 プライマリ ASA が [スタンバイ準備完了（Standby-Ready）] 状態に戻ると、CDO はフェールオーバーを開始し、プライマリ ASA がアクティブ ASA になります。

警告 自己署名証明書を持つデバイスをアップグレードすると、問題が発生する可能性があります。詳細については、「新規証明書の問題のトラブルシュート」を参照してください。

アクティブ/スタンバイペアの ASA と ASDM イメージのアップグレード

ステップ 1 CDO にログインします。

ステップ 2 [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] タブをクリックします。

ステップ 4 アップグレードするデバイスを選択します。

ステップ 5 [デバイスアクション] ペインで、[アップグレード] をクリックします。

デバイスのフェールオーバー モードがアクティブ/スタンバイであることに注意してください。

ステップ 6 [デバイスのアップグレード] ページで、ウィザードに表示される指示に従います。

（注） ASA および ASDM を独自のリポジトリに保存されたイメージにアップグレードする場合、[メージURLの指定] を選択して、[ソフトウェアイメージのURL] フィールドに ASA または ASDM イメージの URL を入力します。FTP、TFTP、HTTP、HTTPS、SCP、および SMB のいずれかのプロトコルを使用して、リポジトリからイメージを取得できます。URL シンタックスの詳細については、「カスタム URL のアップグレード」を参照してください。

カスタム URL のアップグレード

ASA を新しい ASA ソフトウェアおよび ASDM イメージでアップグレードする場合、Cisco Defense Orchestrator（CDO）のイメージリポジトリに格納されているイメージを使用するか、ユーザー独自のイメージリポジトリに格納されているイメージを使用することができます。ASA にインターネットへのアウトバウンドアクセスがない場合、ユーザー独自のイメージリポジトリを維持することが、CDO を使用して ASA をアップグレードするための最良のオプションです。

CDO は ASA の copy コマンドを使用してイメージを取得し、それを ASA のフラッシュドライブ（disk0:/）にコピーします。[イメージURLの指定（Specify Image URL）] フィールドに、copy コマンドの URL 部分を指定します。たとえば、copy コマンド全体が次のようになっているとします。

```
ciscoasa# copy ftp://admin:adminpass@10.10.10.10/asa991-smp-k8.bin disk:/0
```

この場合、[イメージURLの指定（Specify Image URL）] フィールドに

```
ftp://admin:adminpass@10.10.10.10/asa991-smp-k8.bin
```

と入力します。

CDO は、アップグレードイメージを取得する http、https、ftp、tftp、smb、および scp の各方式をサポートします。

URL 構文の例

ASA copy コマンドの URL 構文の例を次に示します。これらの URL の例では、以下を想定しています。

- **イメージリポジトリのアドレス**：10.10.10.10
- **イメージリポジトリにアクセスするためのユーザー名**：admin
- **パスワード**：adminpass
- **パス**：images/asa
- **イメージファイル名**：asa991-smp-k8.bin

```
http[s]:// [[ user [ : password ] @ ] server [ : port ] / [ path / ] filename ]
```

```
https://admin:adminpass@10.10.10.10:8080/images/asa/asa991-smp-k8.bin
HTTP[s] example without a username and password:
https://10.10.10.10:8080/images/asa/asa991-smp-k8.bin
```

ftp:// [[*user* [: *password*] **@**] *server* [: *port*] **/** [*path* **/**] *filename* [**;type=** *xx*]]
type は次のいずれかのキーワードになります。**ap**（ASCII パッシブモード）、**an**（ASCII通常モード）、**ip**（デフォルト：バイナリパッシブモード）、**in**（バイナリ通常モード）。

```
ftp://admin:adminpass@10.10.10.10:20/images/asa/asa991-smp-k8.bin
FTP example without a username and password:
ftp://10.10.10.10:20/images/asa/asa991-smp-k8.bin
```

tftp:// [[*user* [: *password*] **@**] *server* [: *port*] **/** [*path* **/**] *filename* [**;int=** *interface_name*]]

```
tftp://admin:adminpass@10.10.10.10/images/asa/asa991-smp-k8.bin outside
TFTP example without a username and password:
tftp://10.10.10.10/images/asa/asa991-smp-k8.bin outside
```

（注） パス名にスペースを含めることはできません。パス名がスペースを含む場合は、**copy tftp** コマンドの代わりに **tftp-server** コマンドでパスを設定します。**;int=** *interface* オプションは、ルートルックアップをバイパスし、常に指定したインターフェイスを使用して TFTP サーバーに到達します。

smb:/[[*path* **/**] *filename*]：UNIX サーバーのローカルファイルシステムを示します。

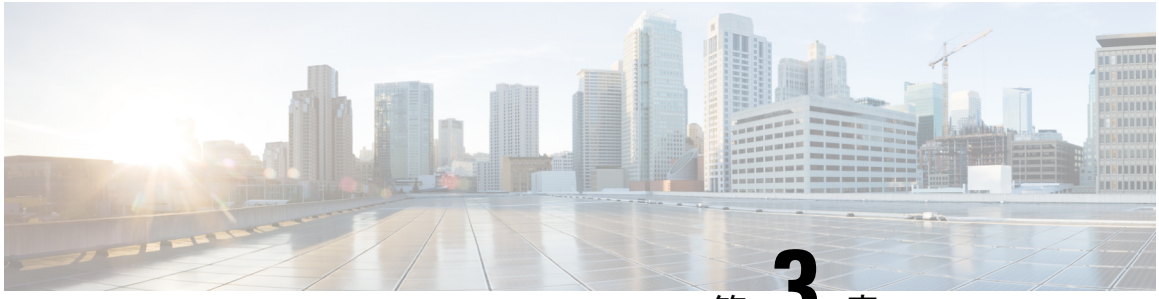
```
smb:/images/asa/asa991-smp-k8.bin
```

scp:// [[*user* [: *password*] **@**] *server* [**/** *path*] **/** *filename* [**;int=** *interface_name*]]]：**;int=** *interface* オプションはルートルックアップをバイパスし、常に指定したインターフェイスを使用してセキュアコピー（SCP）サーバーに到達します。

```
 scp://admin:adminpass@10.10.10.10:8080/images/asa/asa991-smp-k8.bin outside
SCP example without a username and password:
scp://10.10.10.10:8080/images/asa/asa991-smp-k8.bin outside
```

URL 構文を含む完全な copy コマンドについては、『Cisco ASA Series Command Reference, A - H Commands』ガイドを参照してください。

カスタム URL を使用した ASA および ASDM イメージのアップグレードの詳細については、「ASA と ASDM のアップグレードの前提条件」を参照してください。



第 3 章

ASA デバイスを設定する

この章は、次のセクションで構成されています。

ASA の接続ログイン情報の更新

ASA の導入準備プロセスで、CDO がデバイスに接続するために使用する必要があるユーザー名とパスワードを入力しました。これらのログイン情報がデバイスで変更された場合は、**ログイン情報の更新**のデバイスアクションを使用して、CDO でもログイン情報を更新します。この機能により、デバイスを再度導入準備することなく、CDO でログイン情報を更新できます。切り替えるユーザー名とパスワードの組み合わせは、ユーザーの ASA または認証、許可、およびアカウンティング（AAA）サーバーにすでに存在している必要があります。このプロセスは、Cisco Defense Orchestrator データベースにのみ影響します。ログイン情報の更新機能を使用しても、ASA の構成は変更されません。

ステップ 1 ナビゲーションバーで、[デバイスとサービス] 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、[ASA] 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 ASA を選択します。1 つ以上の ASA のログイン情報を一度に更新できます。

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] をクリックします。

ステップ 5 ASA を CDO に接続するために使用する Cloud Connector または Secure Device Connector（SDC）を選択します。

ステップ 6 ASA への接続に使用する新しいユーザー名とパスワードを入力します。

ステップ 7 ログイン情報が変更されると、CDO はデバイスを同期します。

（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] 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。使用するログイン情報が ASA または AAA サーバーに保存されていることを確認して、再試行してください。

ある SDC から別の SDC への ASA の移動

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 CDO メニューバーから、[デバイスとサービス] をクリックします。

ステップ 2 別の SDC に移動する ASA を選択します。

ステップ 3 [デバイスアクション] ウィンドウで、[ログイン情報の更新（Update Credentials）] をクリックします。

ステップ 4 [セキュアデバイスコネクタ（Secure Device Connector）] ボタンをクリックし、デバイスの移動先の SDC を選択します。

ステップ 5 ASA の導入準備に使用した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。これらの変更をデバイスに展開する必要はありません。

オブジェクト

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

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

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

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

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

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

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

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

導入準備されたデバイスからのオブジェクトの作成、編集、または読み取りで問題が発生した場合は、CDO のトラブルシューティング （535 ページ）を参照してください。

オブジェクト タイプ

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

表 *2*:適応型セキュリティアプライアンス（*ASA*）のオブジェクトタイプ

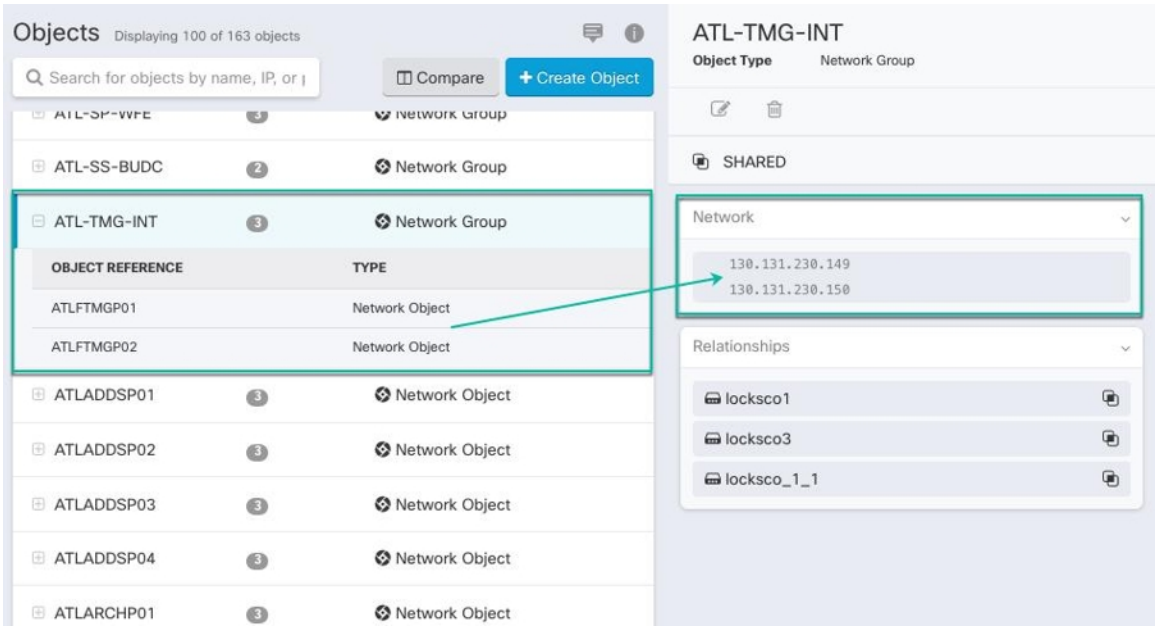
オブジェクト	説明
IP アドレスプールの作成	アドレスプールオブジェクトは、個々の IPv4 または IPv6 アドレス、または IP アドレス範囲と照合するように設定できます。
RA VPN AnyConnect クライアントプロファイルのアップロード	AnyConnect クライアント プロファイル オブジェクトは、ファイルオブジェクトで、通常はリモートアクセス VPN ポリシーの構成で使用するファイルを表します。このオブジェクトには、AnyConnect クライアントプロファイルと AnyConnect クライアント イメージ ファイルを含めることができます。
ネットワーク オブジェクト	ホストまたはネットワークのアドレスを定義するネットワーク グループおよびネットワーク オブジェクト（総称してネットワーク オブジェクトと呼ばれます）。
サービス オブジェクト	サービスオブジェクト、サービスグループ、ポートグループは、TCP/IP プロトコルスイートの一部が考慮されたプロトコルまたはポートを含む再利用可能なコンポーネントです。
ASA 時間範囲オブジェクト	時間範囲オブジェクトは、開始時刻、終了時刻、およびオプションの繰り返しエントリで構成される特定の時刻を定義します。これらのオブジェクトは、特定の機能またはアセットに時間ベースでアクセスするためにネットワークポリシーで使用されます。
トラストポイントのオブジェクト	トラストポイントを使用すると、ASA でデジタル証明書を管理および追跡できます。

共有オブジェクト

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

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

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



オブジェクトのオーバーライド

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

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

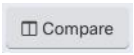
たとえば、各オフィスにプリンタサーバーがあり、プリンタ サーバー オブジェクト `print-server` を作成しているシナリオを考えてみましょう。ACL には、プリンタサーバーのインターネットへのアクセスを拒否するルールを設定しています。プリンタ サーバー オブジェクトには、オフィスごとに変更できるデフォルト値があります。これを行うには、オブジェクトのオーバーライドを使用し、すべての場所でルールと「printer-server」オブジェクトの一貫性を維持します（値は異なる場合があります）。

（注） 一貫性のないオブジェクトがある場合は、オーバーライドを使用してそれらを1つの共有オブジェクトに結合できます。詳細については、不整合オブジェクトの問題を解決する（542ページ）を参照してください。

オブジェクトの比較

ステップ1 [オブジェクト] ページを開きます。

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

ステップ3 [比較] 

ボタンをクリックします。

ステップ4 比較するオブジェクトを最大 3 つまで選択します。

ステップ5 画面の下部にオブジェクトを並べて表示します。

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

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

フィルタ

[インベントリ] 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。

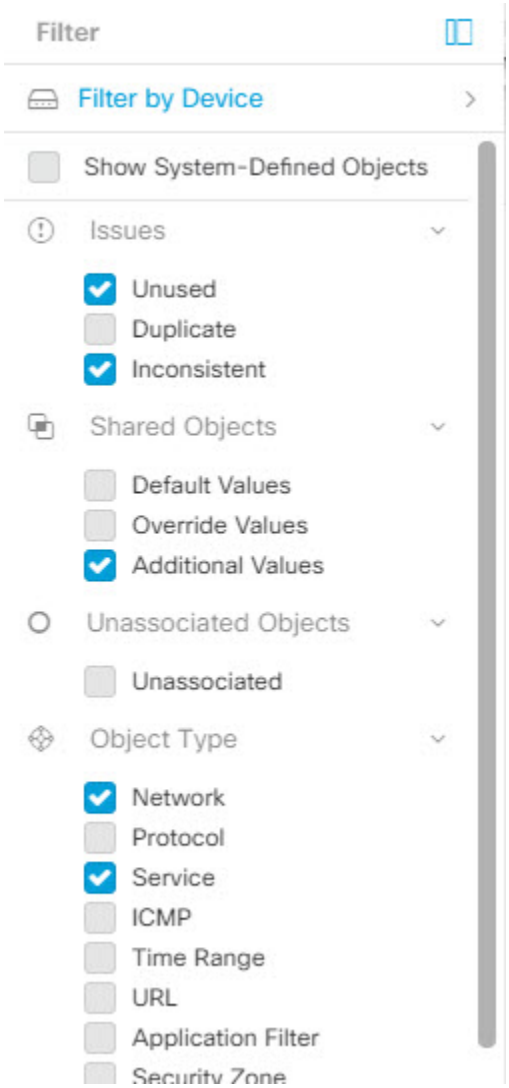
フィルタ処理するには、[デバイスとサービス（Devices and Services）] タブ、[ポリシー（Policies）] タブ、および [オブジェクト] タブの左側のペインで をクリックします。

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て、関連する結果を見つけるためのいくつかの潜在的な検索戦略を作成することができます。

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



オブジェクトフィルタ

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

- [すべてのオブジェクト]：このフィルタは、CDO で導入準備したすべてのデバイスから使用可能なすべてのオブジェクトを提供します。このフィルタは、すべてのオブジェクトを参照するために、または検索の開始点として、さらにサブフィルタを適用するために役立ちます。

- [共有オブジェクト]：このクイックフィルタは、複数のデバイスで共有されていることがCDO によって検出されたすべてのオブジェクトを表示します。
- [デバイスごとのオブジェクト]：特定のデバイスを選択して、選択したデバイスで見つかったオブジェクトを表示できます。

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

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

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

* **一貫性のない**オブジェクト AND

* **ネットワーク**オブジェクト OR **サービス**オブジェクト AND

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

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

システムオブジェクトを表示フィルタ

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

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

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

オブジェクトフィルタを設定する

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

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

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

ステップ 3 結果を特定のデバイスで見つかったものに限定したい場合：

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

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

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

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

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

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

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

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

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

フィルタ基準からデバイスを除外する場合

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

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

オブジェクトの無視の解除

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

ステップ 1 [オブジェクト] ページを開きます。

ステップ 2 オブジェクトフィルタ。

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

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

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

オブジェクトの削除

1 つのオブジェクトまたは複数のオブジェクトを削除できます。

1 つのオブジェクトの削除

1 つのオブジェクトを削除するには、次の手順を実行します。

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

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

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

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

ステップ 5 [OK] をクリックしてオブジェクトの削除を確認します。

ステップ 6 行った変更をすべてのデバイスの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グループの削除

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

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

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

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

ステップ 4 行った変更を今すぐ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。

ネットワーク オブジェクト

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

表 *3:* ネットワークオブジェクトで許可される値

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

表 *4:* ネットワークグループで許可される内容

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

ネットワークオブジェクトの表示

CDO を使用して作成するネットワークオブジェクトと、導入準備したデバイスの設定から CDO が認識するネットワークオブジェクトは、[オブジェクト] ページに表示されます。これらのネットワークオブジェクトには、それぞれのオブジェクトタイプのラベルが付けられていま

す。これにより、オブジェクトタイプでフィルタリングして、探しているオブジェクトをすばやく見つけることができます。

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

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

ASA ネットワークオブジェクトおよびネットワークグループの作成または編集

ASA ネットワークオブジェクトには、CIDR 表記で表現されたホスト名、IP アドレス、またはサブネットアドレスを含めることができます。**ネットワークグループ**は、アクセスルール、ネットワークポリシー、および NAT ルールで使用されるネットワークオブジェクト、ネットワークグループ、および IP アドレスの集合体です。CDO を使用して、ネットワークオブジェクトとネットワークグループを作成、読み取り、更新、および削除できます。

ネットワークオブジェクトに追加できる IP アドレス

デバイス タイプ（Device Type）	[IPv4 / IPv6]	シングル アドレス	アドレス範囲	部分修飾ドメイン名（PQDN）	CIDR 表記によるサブネット
ASA	IPv4	対応	対応	対応	対応

ASA ネットワークオブジェクトの作成

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

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

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

ステップ 4 オブジェクト名を入力します。

ステップ 5 [ネットワークオブジェクトの作成] を選択します。

ステップ 6 （任意）オブジェクトの説明を入力します。

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

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

ステップ 8 [追加（Add）] をクリックします。

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

ASA ネットワーク グループの作成

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

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

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

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

ステップ 4 [オブジェクト名（Object Name）] を入力します。

ステップ 5 [ネットワークグループの作成（Create a network group）] を選択します。

ステップ 6 （任意）オブジェクトの説明を入力します。

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

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

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

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

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

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

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

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

ステップ 12 すべてのデバイスの構成変更のプレビューと展開 （308 ページ）。

ASA ネットワークオブジェクトの編集

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

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

ステップ 3 ネットワークオブジェクトを選択し、[アクション] ペインで編集アイコン をクリックします。

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

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

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

ステップ 6 [確認（Confirm）] をクリックして、オブジェクトとその影響を受けるデバイスへの変更を確定します。

ASA ネットワークグループの編集

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

ステップ 2 オブジェクトフィルタと [検索] フィールドを使用して、編集するネットワークグループを見つけます。

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

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

1. オブジェクト名またはネットワークグループの横に表示される編集アイコン をクリックして、それらを変更します。
2. チェックマークをクリックして変更内容を保存します。

（注） 削除アイコンをクリックして、ネットワークグループから値を削除できます。

ステップ 5 ネットワークグループに新しいネットワークオブジェクトまたはネットワークグループを追加する場合は、次の手順を実行する必要があります。

1. [値（Values）]フィールドに、新しい値または既存のネットワークオブジェクトの名前を入力します。入力を開始すると、入力に一致するオブジェクト名または値がCDOによって表示されます。表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。
2. CDO で一致が検出された場合、既存のオブジェクトを選択するには、[追加] をクリックして、ネットワークオブジェクトまたはネットワークグループを新しいネットワークグループに追加します。
3. 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。
   - [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
   - [新しいオブジェクトとして追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。
   - [値の追加（Add Value）] をクリックして、オブジェクトを使用せずにインライン値を作成します。値を入力し、チェックマークをクリックして保存します。

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

ステップ 6 [保存（**Save**）] をクリックします。CDO は、変更の影響を受けるポリシーを表示します。

ステップ 7 [確認（Confirm）] をクリックして、オブジェクトとその影響を受けるデバイスへの変更を確定します。

ステップ 8 すべてのデバイスの構成変更のプレビューと展開 （308 ページ）。

共有ネットワークグループへの追加の値の追加

関連付けられたすべてのデバイスに存在する共有ネットワークグループ内の値は、「デフォルト値」と呼ばれます。CDO を使用すると、共有ネットワークグループに「追加の値」を追加し、それらの値をその共有ネットワークグループに関連付けられたいくつかのデバイスに割り当てることができます。CDOがデバイスに変更を展開するときに、内容が決定され、「デフォルト値」が共有ネットワークグループに関連付けられているすべてのデバイスにプッシュされ、「追加の値」が指定されたデバイスにのみプッシュされます。

たとえば、本社に 4 つの AD メインサーバーがあり、すべての拠点からアクセスできる必要があるシナリオを考えてみます。この状況で、すべての拠点で使用する「Active-Directory」という名前のオブジェクトグループを作成しました。ここで、ブランチオフィスの 1 つにさらに 2 つの AD サーバーを追加します。これを行うには、オブジェクトグループ「Active-Directory」で、ブランチオフィスに固有の追加値として詳細を追加します。これら2つのサーバーは、オブジェクト「Active-Directory」が一貫しているか、または共有されているかの判断には関与しません。したがって、4 つの AD メインサーバーはすべての拠点からアクセスできますが、ブ

ランチオフィス（2 つの追加サーバーがある）は 2 つの AD サーバーと 4 つの AD メインサーバーにアクセスできます。

（注） 一貫性のない共有ネットワークグループがある場合は、追加の値を使用してそれらを 1 つの共有ネットワークグループに結合できます。詳細については、「不整合オブジェクトの問題を解決する」を参照してください。

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

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、編集する共有ネットワークグループを見つけます。

ステップ 3 [アクション] ペインにある編集アイコン をクリックします。

- [デバイス] フィールドには、共有ネットワークグループが存在するデバイスが表示されます。
- [使用（Usage）] フィールドには、共有ネットワークグループに関連付けられたルールセットが表示されます。
- [デフォルト値（Default Values）] フィールドは、デフォルトのネットワークオブジェクトと、オブジェクトの作成時に指定された、共有ネットワークグループに関連付けられたオブジェクト値が示されます。このフィールドの横に、このデフォルト値を含むデバイスの数が表示され、クリックすると名前とデバイスタイプを表示できます。この値に関連付けられたルールセットも表示されます。

ステップ 4 [追加の値（Additional Values）] フィールドに、値または名前を入力します。 入力を開始すると、入力に一致するオブジェクト名または値が CDO によって表示されます。

ステップ 5 表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。

ステップ 6 CDO で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、ネットワークオブジェクトまたはネットワークグループを新しいネットワークグループに追加します。

ステップ 7 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

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

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

ステップ 8 [デバイス] 列で、新しく追加されたオブジェクトに関連付けられているセルをクリックし、[デバイスの追加（Add Devices）] をクリックします。

ステップ 9 必要なデバイスを選択し、[OK] をクリックします。

ステップ 10 [保存（Save）] をクリックします。CDO は、変更の影響を受けるデバイスを表示します。

ステップ 11 [確認（Confirm）] をクリックして、オブジェクトとその影響を受けるデバイスへの変更を確定します。

ステップ 12 すべてのデバイスの構成変更のプレビューと展開 （308 ページ）。

共有ネットワークグループの追加の値の編集

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

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、編集対象のオーバーライドがあるオブジェクトを見つけます。

ステップ 3 [アクション（Actions）] ペインにある編集アイコン をクリックします。

ステップ 4 オーバーライド値を変更します。

- 値を変更するには、編集アイコンをクリックします。
- [デバイス（Devices）] 列のセルをクリックして、新しいデバイスを割り当てます。すでに割り当てられているデバイスを選択し、[オーバーライドの削除（Remove Overrides）] をクリックすると、そのデバイスのオーバーライドを削除できます。
- [デフォルト値（Default Values）] の 矢印をクリックすると、共有ネットワークグループの追加値にできます。共有ネットワークグループに関連付けられているすべてのデバイスが、自動的に割り当てられます。
- [オーバーライド値（Override Values）] の 矢印をクリックすると、共有ネットワークグループのデフォルト値にできます。
- ネットワークグループからオブジェクトを削除するには、横にある削除アイコンをクリックします。

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

ステップ 6 [確認（Confirm）] をクリックして、オブジェクトとその影響を受けるデバイスへの変更を確定します。

ステップ 7 すべてのデバイスの構成変更のプレビューと展開 （308 ページ）。

トラストポイントのオブジェクト

CDO を使用して、デジタル証明書をトラストポイント オブジェクトとして追加し、1 つまたは複数の管理対象 ASA デバイスにインストールできます。単一のトラストポイント オブジェクトは、アイデンティティペア（ID 証明書と発行者の CA 証明書）、ID 証明書のみ、または CA 証明書のみを保持するコンテナです。

ASAデバイスには多くのトラストポイントを設定できます。サポートされている証明書形式はPKCS12、PEM、DERです。

PKCS12 を使用したID 証明書オブジェクトを追加する

この手順では、証明書ファイルをアップロードするか、既存の証明書テキストをテキストボックスに貼り付けることで、内部証明書アイデンティティまたは内部ID 証明書を作成します。必要な数のID 証明書を生成できます。

PKCS12 形式でエンコードされたファイルをアップロードできます。PKCS12 は、CA サーバー証明書、中間証明書、秘密キーを 1 つの暗号化されたファイルで保持する単一のファイルです。PKCS#12 ファイル、または PFX ファイルは、サーバー証明書、中間証明書、秘密キーが含まれる単一の暗号化ファイルです。復号のための [パスフレーズ（Passphrase）] 値を入力します。

ステップ 1 ナビゲーションバーで、[オブジェクト] > [ASA] > [トラストポイント] を選択します。

ステップ 2 証明書の [オブジェクト名] を入力します。名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 3 [証明書タイプ] ステップで、[ID 証明書] を選択します。

ステップ 4 [インポートタイプ] ステップで、[アップロード] を選択して証明書ファイルをアップロードします。

[登録] ステップは [端末] に設定されています。

ステップ 5 [証明書の内容] ステップで、PKCS12 形式の詳細を入力します。

PKCS#12 ファイル、または PFX ファイルは、サーバー証明書、中間証明書、秘密キーが含まれる単一の暗号化ファイルです。復号のための [パスフレーズ（Passphrase）] 値を入力します。

ステップ 6 [続行（Continue）] をクリックします。

ステップ 7 [詳細オプション] ステップでは、以下を設定できます。

[失効] タブでは、以下を設定できます。

- [証明書失効リスト（CRL）の有効化]：CRL の確認を有効にするにはオンにします。

  デフォルトでは、証明書からの失効リスト配布 URL を取得するために [証明書のCRL分散ポイントを使用する] チェックボックスがオンになっています。

  [キャッシュ更新時間（分）]：キャッシュの更新間隔を分単位で指定します。デフォルトは60分です。範囲は 1 ～ 1440 分です。CA から同じ CRL を何度も受け取る必要のないように、ASA では、取得した CRL をローカルで保存できます。これを CRL キャッシングと呼びます。CRL キャッシュの容量はプラットフォームによって異なり、すべてのコンテキストについて累積されます。新たに取得した CRL をキャッシュすることで、保存制限を超える可能性がある場合は、ASA により使用頻度が最も低い CRL が削除され、使用可能な空き容量が確保されます。

- [Online Certificate Status Protocol（OCSP）の有効化]：OCSP チェックを有効にするにはオンにします。

  [OCSP サーバ URL（OCSP Server URL）]：OCSP チェックを必須としている場合に、失効をチェックする OCSP サーバの URL。この URL は、**http://** で始まる必要があります。

  [ナンス拡張を無効化]：このチェックボックスをオンにすると、暗号化によって要求を応答にバインドし、リプレイアタックを回避します。このプロセスでは、要求と応答との間でそれぞれのナンス拡張

を照合し、両者が同一であることを確認することで、リプレイ アタックを防ぐことができます。ただし、事前に生成した応答には、各要求と一致するナンス拡張は含まれていません。そのため、使用している OCSP サーバーから、事前に生成した応答を送信する場合は、[ナンス拡張を無効化] チェックボックスをオフにしてください。

[評価の優先度]：CRL または OSCP で最初に証明書の失効ステータスを評価するかどうかを指定します。

- [失効情報に到達できない場合は証明書を有効と見なす]：失効情報に到達できない場合に証明書を有効な証明書と見なすには、このチェック ボックスをオンにします。

  失効チェックの詳細については、『 Cisco ASA Series General Operations ASDM Configuration、X.Y』ドキュメントの「基本設定」ブックの「デジタル証明書」の章を参照してください。

[その他] タブをクリックします。

- [検証にCA証明書を使用]：この CA によって検証できる接続のタイプを指定します。
  - [IPSecクライアント]：リモート SSL サーバーによって提示された証明書を検証します。
  - [SSLクライアント]：着信 SSL 接続によって提示された証明書を検証します。
  - [SSLサーバー]：着信 IPSec 接続によって提示された証明書を検証します。
- [ID 証明書の使用]：登録済み ID 証明書の使用方法を指定します。
  - [SSL & IPSec]：SSL & IPSec 接続の認証に使用します。
  - [コード署名者] ：コード署名者証明書は、関連付けられている秘密キーがデジタル署名の作成に使用される特殊な証明書です。コードの署名に使用される証明書は CA から取得され、署名されたコードそのものが証明書の発生元を示します。
- **その他のオプション**：
  - [基本制約拡張でCAフラグを有効化する]：この証明書で他の証明書に署名できるようにする場合はこのオプションをオンにします。基本制約の拡張によって、証明書のサブジェクトが認証局（CA）かどうかが識別されます。この場合、証明書を使用して他の証明書に署名することができます。CA フラグは、この拡張の一部です。証明書におけるこれらの項目のプレゼンス
  - [このCAが発行した証明書を受け入れる]：指定した CA の証明書を ASA で受け入れるようにするにはこのオプションを選択します。
  - [IPsecキーの使用状況を無視]：IPsec リモートクライアント証明書のキーの使用状況および拡張キーの用途拡張の値を検証しない場合は、このオプションを選択します。IPsec クライアント証明書のキーの使用状況チェックを行わないようにできます。デフォルトでは、このオプションはイネーブルになっていません。

ステップ 8 [追加（Add）] をクリックします。

自己署名済みID 証明書オブジェクトを作成する

この手順では、ウィザードに適切な証明書フィールド値を入力することにより、自己署名証明書を生成する手順を説明します。自己署名証明書は必要な数だけ生成できます。

自己署名済みID 証明書オブジェクトを作成するには、次の手順を実行します。

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] > [ASA] > [トラストポイント（Trustpoints）] を選択します。

ステップ 2 証明書の [オブジェクト名（Object Name）] を入力します。名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 3 [証明書タイプ] ステップで、[ID 証明書（Identity Certificate）] を選択します。

ステップ 4 [インポートタイプ] ステップで、[新規（New）] を選択して証明書ファイルをアップロードし、[続行] をクリックします。

ステップ 5 [登録] ステップで、[自己署名済み（Self-Signed）] を選択し、[続行] をクリックします。

証明書の内容のステップが表示されます。「証明書コンテンツに基づく自己署名済みCSR 証明書の生成」を読んで、生成されている自己署名付き証明書の CN および SANS コンテンツを理解してください。

ステップ 6 [証明書の内容（Certificate Contents）] の手順で、次の設定を行います。

- [国（C）（Country (C)）]：ドロップダウトリストから国コードを選択します。
- [都道府県（ST）（State or Province (ST)）]：証明書に含める都道府県または州。
- [地域または都市（L）（Locality or City (L)）]：都市の名前など、証明書に含める地域。
- [組織（O）（Organization (O)）]：証明書に含める組織または会社の名前。
- [組織単位（部門）（OU）（Organizational Unit (Department) ）]：証明書に含める組織単位の名前（部門名など）。
- [共通名（CN）（Common Name (CN)）]：証明書に含める X.500 共通名。これは、デバイスの名前、Web サイト、または他の文字列にできます。この要素は、通常は正常な接続のために必要です。たとえば、リモート アクセス VPN で使用する内部証明書に CN を含める必要があります。
- [電子メールアドレス（EA）（Email Address (EA)）]：ID 証明書に関連付けられている電子メールアドレス。
- [IPアドレス（IP Address）]：4 分割ドット付き 10 進表記の、ネットワーク上の ASA IP アドレス。
- [デバイスのFQDN（Device's FQDN）]：DNS ツリー階層内のノードの位置を示す完全修飾ドメイン名。
- [デバイスのシリアル番号を含める（Include Device's Serial Number）]：ASA のシリアル番号を証明書パラメータに追加するには、チェックボックスをオンにします。

a) [キー（Key）] タブをクリックします。

- **RSA** または **ECDSA** キーのタイプを選択します。

- [キーサイズ（Key Size）]：キーペアが存在しない場合は、必要なキーサイズ（係数）をビットで定義します。推奨されるキーのサイズは、RSA では 1024、ECDSA では 348 です。係数のサイズが大きくなるほど、キーがよりセキュアになります。ただし、係数のサイズが大きいキーほど、生成に時間がかかり（512 ビットより大きい場合は 1 分以上）、交換するときの処理にも時間がかかります。
- [続行（Continue）] をクリックします。

ステップ 7 [詳細オプション] ステップでは、以下の設定を行うことができます。

[失効] タブでは、以下の設定を行うことができます。

- [証明書失効リスト（CRL）の有効化）]：CRL の確認を有効にするにはオンにします。

  デフォルトでは、証明書からの失効リスト配布 URL を取得するために、[証明書からのCRL配布ポイントの使用] がオンになっています。

  [キャッシュ更新時間（分）]：キャッシュの更新間隔を分単位で指定します。デフォルトは 60 分です。範囲は 1 ～ 1440 分です。CA から同じ CRL を何度も受け取る必要のないように、ASA では、取得した CRL をローカルで保存できます。これを CRL キャッシングと呼びます。CRL キャッシュの容量はプラットフォームによって異なり、すべてのコンテキストについて累積されます。新たに取得した CRL をキャッシュすることで、保存制限を超える可能性がある場合は、ASA により使用頻度が最も低い CRL が削除され、使用可能な空き容量が確保されます。

- [Online Certificate Status Protocol（OCSP）の有効化]：OCSP チェックを有効にするにはオンにします。

  [OCSP サーバ URL（OCSP Server URL）]：OCSP チェックを必須としている場合に、失効をチェックする OCSP サーバの URL。この URL は、**`http://`** で始まる必要があります。

  [ナンス拡張子を無効化] ：このチェックボックスをオンにすると、暗号化によって要求を応答にバインドし、リプレイアタックを回避します。このプロセスでは、要求と応答との間でそれぞれのナンス拡張を照合し、両者が同一であることを確認することで、リプレイ アタックを防ぐことができます。使用している OCSP サーバーから、この一致するナンス拡張子を含まない事前に生成した応答を送信する場合は、[ナンス拡張子を無効化] チェックボックスをオフにしてください。

  [評価の優先度]：CRL または OSCP で最初に証明書の失効ステータスを評価するかどうかを指定します。

- [失効情報に到達できない場合は証明書を有効と見なす]：失効情報に到達できない場合に証明書を有効な証明書と見なすには、このチェックボックスをオンにします。

  失効チェックの詳細については、『Cisco ASA Series General Operations ASDM Configuration、XY』ドキュメントの「基本設定」ブックの「デジタル証明書」の章を参照してください。

[その他] タブをクリックします。

- [検証にCA証明書を使用（Use CA Certificate for the Validation of）]：この CA によって検証できる接続のタイプを指定します。
  - [IPSecクライアント]：リモート SSL サーバーによって提示された証明書を検証します。
  - [SSLクライアント]：着信 SSL 接続によって提示された証明書を検証します。

- [SSLサーバー]：着信 IPSec 接続によって提示された証明書を検証します。

- [ID証明書の使用]：登録済み ID 証明書の使用方法を指定します。
  - [SSL & IPSec]：SSL & IPSec 接続の認証に使用します。
  - [コード署名者]：コード署名者証明書は、関連付けられている秘密キーがデジタル署名の作成に使用される特殊な証明書です。コードの署名に使用される証明書は CA から取得され、署名されたコードそのものが証明書の発生元を示します。

- **その他のオプション**：
  - [基本制約拡張でCAフラグを有効化する]：この証明書で他の証明書に署名できるようにする場合はこのオプションをオンにします。基本制約の拡張によって、証明書のサブジェクトが認証局（CA）かどうかが識別されます。この場合、証明書を使用して他の証明書に署名することができます。CA フラグは、この拡張の一部です。証明書におけるこれらの項目の存在
  - [このCAが発行した証明書を受け入れる（Accept certificates issued by this CA）]：指定した CA の証明書を ASA で受け入れるようにするにはこのチェックボックスをオンにします。
  - [IPsecキーの使用状況を無視（Ignore IPsec Key Usage）]：IPsec リモートクライアント証明書のキーの使用状況および拡張キーの使用状況エクステンションの値を検証しない場合は、このオプションを選択します。IPsec クライアント証明書のキーの使用状況チェックを行わないようにできます。デフォルトでは、このオプションはイネーブルになっていません。

ステップ 8 [追加（Add）] をクリックします。

証明書署名要求（CSR）用 ID 証明書オブジェクトを追加する

証明書署名要求（CSR）を生成したり、指定されたCAからID証明書を取得したりするためには、認証局（CA）サーバー情報と登録パラメータが必要です。要求を生成するには、Rivest-Shamir-Adleman（RSA）または楕円曲線デジタル署名アルゴリズム（楕円曲線DSA）のいずれかのキータイプを選択する必要があります。

識別情報を提供し、オプションで CA から取得した CA 証明書をアップロードして、トラストポイント オブジェクトを作成します。

ステップ 1 ナビゲーションバーで、[オブジェクト] > [ASA] > [トラストポイント] を選択します。

ステップ 2 証明書の [オブジェクト名] を入力します。名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 3 [ID証明書] ステップで、[ID証明書] を選択します。

ステップ 4 [インポートタイプ] ステップで、[新規] を選択して証明書ファイルをアップロードし、[続行] をクリックします。

ステップ 5 [登録] ステップで、[手動] を選択します。

ステップ 6 （オプション）CA から取得した CA 証明書を貼り付けるか、アップロードできます。このフィールドは空のままにすることもできます。

ステップ 7 [続行（Continue）] をクリックします。

証明書の内容のステップが表示されます。「証明書コンテンツに基づく自己署名済み CSR 証明書の生成」を読んで、生成されている署名付き証明書の CN および SANS コンテンツを理解してください。

ステップ 8 [証明書の内容] の手順で、次の設定を行います。

- [国（C）]：ドロップダウトリストから国コードを選択します。
- [都道府県（ST）]：証明書に含める都道府県または州。
- [地域または都市（L）]：都市の名前など、証明書に含める地域。
- [組織（O）（Organization (O)）]：証明書に含める組織または会社の名前。
- [組織単位（部門）（OU）]：証明書に含める組織単位の名前（部門名など）。
- [共通名（CN）（Common Name (CN)）]：証明書に含める X.500 共通名。これは、デバイスの名前、Web サイト、または他の文字列にできます。この要素は、通常は正常な接続のために必要です。たとえば、リモート アクセス VPN で使用する内部証明書に CN を含める必要があります。
- [電子メールアドレス（EA）]：ID 証明書に関連付けられている電子メールアドレス。
- [IPアドレス]：4 分割ドット付き 10 進表記の、ネットワーク上の ASA IP アドレス。
- [サブジェクトの別名 （SAN）]：このフィールドは、「unstructuredName」として証明書のサブジェクト DN の一部にもなります。証明書が複数のドメインまたは IP アドレスに使用される場合は、このフィールドを使用することをお勧めします。
  - [デバイスのホスト名を使用]：デバイスのホスト名が使用されます。
  - [カスタム：デバイスのFQDN]：DNS ツリー階層内のノードの位置を示す明確なドメイン名。

    （注） CN と**カスタム FQDN** で指定する値は同じにすることを推奨します。

- [デバイスのシリアル番号を含める]：ASA のシリアル番号を証明書に含めるには、チェックボックスをオンにします。CA は、このシリアル番号を使用して、証明書を認証するか、またはあとで証明書を特定のデバイスに関連付けます。シリアル番号を含めるかどうか判断できない場合は、デバッグに役立つため、含めてください。

a) [キー] タブをクリックします。

- **RSA** または **ECDSA** キーのタイプを選択します。
- [キーサイズ]：キーペアが存在しない場合は、必要なキーサイズ（係数）をビット単位で定義します。推奨されるキーサイズは、RSA では 1024、ECDSA では 348 です。係数のサイズが大きくなるほど、キーがよりセキュアになります。ただし、係数のサイズが大きいキーほど、生成に時間がかかり（512 ビットより大きい場合は 1 分以上）、交換するときの処理にも時間がかかります。
- [続行（Continue）] をクリックします。

ステップ 9 [詳細オプション] ステップでは、以下を設定できます。

[失効] タブでは、以下を設定できます。

- [証明書失効リスト（CRL）の有効化）]：CRL の確認を有効にするにはオンにします。

  デフォルトでは、証明書からの失効リスト配布URLを取得するために、[証明書からのCRL配布ポイントの使用] がオンになっています。

  [キャッシュ更新時間（分）]：キャッシュの更新間隔を分単位で指定します。デフォルトは 60 分です。範囲は 1 ～ 1440 分です。CA から同じ CRL を何度も受け取る必要のないように、ASA では、取得した CRL をローカルで保存できます。これを CRL キャッシングと呼びます。CRL キャッシュの容量はプラットフォームによって異なり、すべてのコンテキストについて累積されます。新たに取得したCRLをキャッシュすることで、保存制限を超える可能性がある場合は、ASAにより使用頻度が最も低い CRL が削除され、使用可能な空き容量が確保されます。

- [Online Certificate Status Protocol（OCSP）の有効化]：OCSP チェックを有効にするにはオンにします。

  [OCSP サーバ URL（OCSP Server URL）]：OCSP チェックを必須としている場合に、失効をチェックする OCSP サーバの URL。この URL は、**http://** で始まる必要があります。

  [ナンス拡張子を無効化] ：このチェックボックスをオンにすると、暗号化によって要求を応答にバインドし、リプレイアタックを回避します。このプロセスでは、要求と応答との間でそれぞれのナンス拡張を照合し、両者が同一であることを確認することで、リプレイ アタックを防ぐことができます。使用している OCSP サーバーから、この一致するナンス拡張子を含まない事前に生成した応答を送信する場合は、[ナンス拡張子を無効化] チェックボックスをオフにしてください。

  [評価の優先度]：CRL または OSCP で最初に証明書の失効ステータスを評価するかどうかを指定します。

- [失効情報に到達できない場合は証明書を有効と見なす]：失効情報に到達できない場合に証明書を有効な証明書と見なすには、このチェックボックスをオンにします。

  失効チェックの詳細については、『Cisco ASA Series General Operations ASDM Configuration、XY』ドキュメントの「基本設定」ブックの「デジタル証明書」の章を参照してください。

[その他] タブをクリックします。

- [検証にCA 証明書を使用]：この CA によって検証できる接続のタイプを指定します。
  - [IPSecクライアント]：リモート SSL サーバーによって提示された証明書を検証します。
  - [SSLクライアント]：着信 SSL 接続によって提示された証明書を検証します。
  - [SSLサーバー]：着信 IPSec 接続によって提示された証明書を検証します。
- [ID証明書の使用]：登録済み ID 証明書の使用方法を指定します。
  - [SSL & IPSec]：SSL & IPSec 接続の認証に使用します。
  - [コード署名者]：コード署名者証明書は、関連付けられている秘密キーがデジタル署名の作成に使用される特殊な証明書です。コードの署名に使用される証明書は CA から取得され、署名されたコードそのものが証明書の発生元を示します。

- **その他のオプション**：
  - [基本制約拡張でCAフラグを有効化する]：この証明書で他の証明書に署名できるようにする場合はこのオプションをオンにします。基本制約の拡張によって、証明書のサブジェクトが認証局（CA）かどうかが識別されます。この場合、証明書を使用して他の証明書に署名することができます。CA フラグは、この拡張の一部です。証明書におけるこれらの項目のプレゼンス
  - [このCAが発行した証明書を受け入れる]：指定した CA の証明書を ASA で受け入れるようにするにはこのオプションを選択します。
  - [IPsecキーの使用状況を無視]：IPsec リモートクライアント証明書のキーの使用状況および拡張キーの用途拡張の値を検証しない場合は、このオプションを選択します。IPsec クライアント証明書のキーの使用状況チェックを行わないようにできます。デフォルトでは、このオプションはイネーブルになっていません。

ステップ 10 [追加（Add）] をクリックします。

これにより、トラストポイント証明書オブジェクトが作成されます。

信頼できる CA 証明書オブジェクトを追加する

外部の認証局から信頼できる CA 証明書を取得するか、自身の内部 CA を使用して（OpenSSL ツールを使用するなど）CA 証明書を作成します。次のサポートされている形式のいずれかでエンコードしたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] > [ASA] > [トラストポイント（Trustpoints）] を選択します。

ステップ 2 証明書の [オブジェクト名（Object Name）] を入力します。名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 3 [証明書タイプ] ステップで、[信頼できる CA 証明書（Trusted CA Certificate）] を選択します。

ステップ 4 [証明書の内容（Certificate Contents] ステップで、証明書の内容をテキストボックスに貼り付けるか、ウィザードの説明に従って CA 証明書ファイルをアップロードします。

ステップ 5 [続行（Continue）] をクリックします。ウィザードの手順が 4 に進みます。

証明書は、次のガイドラインに合致している必要があります。

- 証明書内のサーバ名は、サーバのホスト名または IP アドレスと一致している必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で ad.example.com を使用すると接続が失敗します。
- 証明書は PEM または DER 形式の X509 証明書である必要があります。

- 貼り付ける証明書は、BEGIN CERTIFICATE と END CERTIFICATE の行を含める必要があります。次に例を示します。

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

ステップ 6 [詳細オプション（Advanced Options）] ステップでは、以下を構成できます。

[失効] タブでは、以下の設定を行うことができます。

- [証明書失効リスト（CRL）の有効化）]：CRL の確認を有効にするにはオンにします。

  デフォルトでは、証明書からの失効リスト配布 URL を取得するために、[証明書からの CRL 分散ポイントの使用（Use CRL distribution point from the certificate）] がオンになっています。

  [キャッシュ更新時間（分）]：キャッシュの更新間隔を分単位で指定します。デフォルトは60分です。範囲は 1 ～ 1440 分です。CA から同じ CRL を何度も受け取る必要のないように、ASA では、取得した CRL をローカルで保存できます。これを CRL キャッシングと呼びます。CRL キャッシュの容量はプラットフォームによって異なり、すべてのコンテキストについて累積されます。新たに取得した CRL をキャッシュすることで、保存制限を超える可能性がある場合は、ASA により使用頻度が最も低い CRL が削除され、使用可能な空き容量が確保されます。

- [Online Certificate Status Protocol（OCSP）の有効化]：OCSP チェックを有効にするにはオンにします。

  [OCSP サーバ URL（OCSP Server URL）]：OCSP チェックを必須としている場合に、失効をチェックする OCSP サーバの URL。この URL は、**http://** で始まる必要があります。

  [ナンス拡張子を無効化] ：このチェックボックスをオンにすると、暗号化によって要求を応答にバインドし、リプレイアタックを回避します。このプロセスでは、要求と応答との間でそれぞれのナンス拡張を照合し、両者が同一であることを確認することで、リプレイ アタックを防ぐことができます。使用している OCSP サーバーから、この一致するナンス拡張子を含まない事前に生成した応答を送信する場合は、[ナンス拡張子を無効化] チェックボックスをオフにしてください。

  [評価の優先度]：CRL または OSCP で最初に証明書の失効ステータスを評価するかどうかを指定します。

- [失効情報に到達できない場合は証明書を有効と見なす]：失効情報に到達できない場合に証明書を有効な証明書と見なすには、このチェックボックスをオンにします。

  失効チェックの詳細については、『Cisco ASA Series General Operations ASDM Configuration、XY』ドキュメントの「基本設定」ブックの「デジタル証明書」の章を参照してください。

[その他] タブをクリックします。

- [検証にCA証明書を使用（Use CA Certificate for the Validation of）]：この CA によって検証できる接続のタイプを指定します。
  - [IPSecクライアント]：リモート SSL サーバーによって提示された証明書を検証します。
  - [SSLクライアント]：着信 SSL 接続によって提示された証明書を検証します。
  - [SSLサーバー]：着信 IPSec 接続によって提示された証明書を検証します。
- **その他のオプション**：
  - [このCAが発行した証明書を受け入れる（Accept certificates issued by this CA）]：指定した CA の証明書を ASA で受け入れるようにするにはこのチェックボックスをオンにします。
  - [このCAの下位CAが発行した証明書を受け入れる（Accept certificates issued by this CA）]：下位 CA の証明書を ASA で受け入れるようにするにはこのチェックボックスをオンにします。
  - [IPsecキーの使用状況を無視（Ignore IPsec Key Usage）]：IPsec リモートクライアント証明書のキーの使用状況および拡張キーの使用状況エクステンションの値を検証しない場合は、このオプションを選択します。IPsec クライアント証明書のキーの使用状況チェックを行わないようにできます。デフォルトでは、このオプションはイネーブルになっていません。

ステップ 7 [追加（Add）] をクリックします。

これにより、トラストポイント証明書オブジェクトが作成されます。

証明書コンテンツに基づく自己署名済み CSR 証明書の生成

自己署名証明書と CSR 証明書の CN と SANS の内容を理解する必要があります。内容は、作成時に指定したパラメータに基づいています。AnyConnect クライアントが組織の対象となる VPN ヘッドエンドに接続するには、パラメータを正確に設定する必要があります。

このセクションでは、指定されたパラメータに基づいて自己署名証明書と CSR 証明書の内容を理解できるように、さまざまなユースケースと例を示します。

ユースケース 1：異なる CN 値と FQDN 値

例：

- 共通名（CN）：mywebsite.com
- FQDN：mysan.com

表 *5:* 例：異なる *CN* 値と *FQDN* 値

	共通名	unstructuredName	SANS
自己署名	mywebsite.com	mysan.com	mysan.com

	共通名	unstructuredName	SANS
CSR	mywebsite.com	mysan.com	-

ユースケース 2：FQDN フィールドを [なし（None）] に設定

例：

- 共通名（CN）：mywebsite.com
- FQDN：なし（None）

表 *6*：例：*FQDN* フィールドを *[*なし（*None*）*]* に設定

	共通名	SANS
自己署名	ホスト名	-
CSR	mywebsite.com	-

ユースケース 3：FQDN なし（デフォルトの FQDN）

例：

- 共通名（CN）：mywebsite.com

表 *7*：例：*FQDN* なし（デフォルトの *FQDN*）

	共通名	unstructuredName	SANS
自己署名	mywebsite.com	ホスト名	-
CSR	mywebsite.com	ホスト名	ホスト名

ユースケース 4：FQDN で IP アドレスを指定する

例：

- 共通名（CN）：mywebsite.com
- FQDN：4.5.6.7

表 *8*：例：*FQDN* で *IP* アドレスを指定する

	共通名	unstructuredName	SANS
自己署名	mywebsite.com	4.5.6.7	-
CSR	mywebsite.com	4.5.6.7	4.5.6.7

ユースケース 5：IP アドレスを指定する

例：

- IP アドレス：4.5.6.7
- 共通名（CN）：mywebsite.com
- FQDN：fqdn.com

表 *9*：例：*IP* アドレスを指定する

	共通名	unstructuredAddress	unstructuredName	SANS
自己署名	mywebsite.com	4.5.6.7	fqdn.com	-
CSR	mywebsite.com	4.5.6.7	fqdn.com	fqdn.com

ユースケース 6：シリアル番号のチェックボックスがオン

例：

- シリアル番号：9AQXMWOKDT9

表 *10*：例：*IP* シリアル番号のチェックボックスがオン

	serialNumber	SANS
自己署名	9AQXMWOKDT9	-
CSR	9AQXMWOKDT9	fqdn.com

ユースケース 7：メールアドレスを指定する

例：

- EA：abc@xyz.com

表 *11*：例：メールアドレスを指定する

	unstructredName	emailAddress	SANS
自己署名	ホスト名	abc@xyz.com	ホスト名
CSR	ホスト名	abc@xyz.com	-

RA VPN オブジェクト

サービス オブジェクト

ASA サービスオブジェクト

ASA サービスオブジェクト、サービスグループ、およびポートグループは、IP プロトコルスイートの一部が考慮されたプロトコルまたはポートを含む再利用可能なコンポーネントです。サービスオブジェクトでは、単一のプロトコルを指定して、そのプロトコルを送信元ポート、宛先ポート、または送信元ポートと宛先ポートの両方に割り当てることができます。サービスグループには多くのサービスオブジェクトが含まれ、複数の種類のプロトコルを含めることができます。

ポートグループは、一種の ASA サービスオブジェクトです。ポートグループには、サービスタイプ（TCP や UDP など）と組み合わせるポートオブジェクト、およびポート番号またはポート番号の範囲が含まれます。その後、トラフィックの一致基準を定義するためにセキュリティポリシーでオブジェクトを使用できます。たとえば、これらをアクセス制御ルールで使用して、特定の範囲の TCP ポートへのトラフィックを許可できます。

詳細については、「ASA サービスオブジェクトの作成と編集」を参照してください。

プロトコルオブジェクト

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

ICMP オブジェクト

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

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

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

関連情報：

- オブジェクトの削除 （141 ページ）

ASA サービスオブジェクトの作成と編集

サービスオブジェクトでは、単一のプロトコルを指定して、そのプロトコルを送信元ポート、宛先ポート、または送信元ポートと宛先ポートの両方に割り当てることができます。

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

ステップ 2 **[オブジェクトの作成]** > **[ASA]** > **[サービス（Service）]** をクリックします。

ステップ 3 オブジェクト名を入力します。

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

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

- TCP、UDP、およびTCP-UDPサービスタイプの場合、送信元ポート、宛先ポート、または両方のポートを入力します。
  - 送信元ポート ID を使用すると、特定の番号のポートから発信されたトラフィックを照合できます。送信元ポートIDで、演算子（等しい、範囲、より小さい、より大きい、または等しくない）を選択し、適切なポート番号または範囲を指定します。
  - 宛先ポートIDを使用すると、特定の番号のポートに到着するトラフィックを照合できます。宛先ポートIDで、演算子（等しい、範囲、より小さい、より大きい、または等しくない）を選択し、適切なポート番号または範囲を指定します。
- **プロトコルサービスタイプの場合**、0 ～ 255 の範囲のプロトコル番号または、ip、tcp、udp、gre などの既知の名前を入力します。

ステップ 6 [追加（Add）] をクリックします。

例

- 着信 FTP トラフィックを識別するサービスオブジェクトは、TCP サービスタイプと 21 の宛先ポート範囲を持つオブジェクトです。
- 発信 DNS および DNS over TCP トラフィックを識別するサービスオブジェクトは、tcp-udb サービスタイプと 53 に等しい送信元ポートを持つオブジェクトです。

ASA サービスグループの作成

サービスグループは、1 つ以上のプロトコルを表す 1 つ以上のサービスオブジェクトで構成できます。

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

ステップ 2 **[オブジェクトの作成（Create Object）]** > **[ASA]** > **[サービス（Service）]** をクリックします。

ステップ 3 オブジェクト名を入力します。

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

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

ステップ 6 必要に応じて、追加の個別サービスタイプの値をサービスグループに追加します。

- **TCP、UDP、および TCP-UDP サービスタイプの場合、**送信元ポート、宛先ポート、または両方のポートを入力します。
  - 送信元ポート ID を使用すると、特定の番号のポートから発信されたトラフィックを照合できます。送信元ポート ID で、演算子（等しい、範囲、より小さい、より大きい、または等しくない）を選択し、適切なポート番号または範囲を指定します。
  - 宛先ポート ID を使用すると、特定の番号のポートに到着するトラフィックを照合できます。宛先ポート ID で、演算子（等しい、範囲、より小さい、より大きい、または等しくない）を選択し、適切なポート番号または範囲を指定します。
- **プロトコルサービスタイプの場合**、0 ～ 255 の範囲のプロトコル番号または、ip、tcp、udp、gre などの既知の名前を入力します。

ステップ 7 さらに個別のポート値を追加するには、[別の値を追加（Add Another Value）] をクリックして、ステップ 6 を繰り返します。

ステップ 8 サービスグループへのサービスオブジェクトとサービス値の追加が完了したら、[追加] をクリックします。

ASA サービスオブジェクトまたはサービスグループの編集

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

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

ステップ 3 詳細ペインで、[編集] をクリックします。

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

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 CDO は、変更の影響を受けるポリシーを表示します。[確認（Confirm）] をクリックして、オブジェクトとその影響を受けるポリシーへの変更を確定します。

ASA 時間範囲オブジェクト

時間範囲オブジェクトとは

時間範囲オブジェクトは、開始時刻、終了時刻、およびオプションの繰り返しエントリで構成される特定の時刻を定義します。これらのオブジェクトは、特定の機能またはアセットに時間ベースでアクセスするためにネットワークポリシーで使用されます。たとえば、勤務時間中にのみ特定のサーバーへのアクセスを許可するアクセスルールを作成できます。時間範囲を作成してもデバイスへのアクセスは制限されません。これらのオブジェクトに設定される時間は、デバイスのローカル時間であることに注意してください。

このオブジェクトには、絶対時間範囲または反復時間範囲を追加できます。反復時間範囲は、定期的な時間範囲と見なされます。

（注） 1 つの時間範囲に絶対（absolute）値と定期（periodic）値の両方が指定されている場合、periodic 値は absolute の開始時刻に到達した後にのみ評価され、absolute の終了時刻に到達した後は評価されません。

ASA の時間範囲オブジェクトの作成

ASA デバイスの時間範囲オブジェクトを作成するには、次の手順を使用します。

ステップ 1 左側のナビゲーションバーで、[オブジェクト] 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、オブジェクトを作成します。

ステップ 3 **[ASA]** > **[時間範囲]**をクリックします。

ステップ 4 オブジェクト名を入力します。

ステップ 5 時間範囲を定義します。

- [絶対時間範囲（Absolute Time Range）]：希望する時間範囲の開始時間と終了時間を入力します。このオブジェクトを数分、数時間、数日、または数週間かけて実行することを選択できます。時間範囲オブジェクトには、絶対時間範囲を 1 つだけ指定することができます。
- [定期的な時間範囲（Recurring Time Ranges）]： をクリックして、毎週繰り返される定期的な時間範囲を追加します。ドロップダウンメニューから [頻度（Frequency）]、時間範囲を有効にする [曜日（Days）]、[開始時間（Start）] と [終了時間（End）] を選択します。時間範囲オブジェクトは、複数の周期範囲を持つことができます。

（注） 時間範囲オブジェクトの開始時間と終了時間はオプションです。オブジェクトに開始時間が設定されていない場合、時間範囲はすぐに有効になります。オブジェクトに終了時間が設定されていない場合、時間範囲は無期限に続きます。

ステップ 6 [追加] をクリックしてオブジェクトを作成します。

ASA の時間範囲オブジェクトの編集

ASA デバイスの時間範囲オブジェクトを編集するには、次の手順を使用します。

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

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

ステップ 3 詳細ペインで、[編集（Edit）] をクリックします。

ステップ 4 必要に応じて値を編集し、[保存（Save）] をクリックします。

ステップ 5 オブジェクトが現在いずれかのポリシーで使用されている場合、CDO は変更の影響を受けるポリシーを表示します。[確認（Confirm）] をクリックして、オブジェクトとその影響を受けるポリシーへの変更を確定します。

ステップ 6 オブジェクトがデバイスのポリシーで使用されている場合は、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か、待機してから複数の変更を一度に展開します。

関連情報：

- オブジェクトの削除
- ASA レガシー ネットワーク ポリシー

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。

- ASA ポリシー（拡張アクセスリスト） （177 ページ）
- ネットワーク アドレス変換 （186 ページ）

ASA レガシー ネットワーク ポリシー

このセクションでは、Cisco Defense Orchestrator（CDO）によって管理されるすべてのデバイスで使用される、あらゆるネットワークポリシーのリストを表示するレガシー ネットワーク ポ

リシーページに関する情報を提供します。**[ポリシー]**>**[ASAポリシー]**を選択して、ネットワークポリシーページに移動します。

ネットワークポリシーは、ネットワークルールのコレクションです。各ネットワークルールは、送信元および接続先の IP アドレス、IP プロトコル、ポート番号、EtherType などの特性に基づいて、ネットワークトラフィックがネットワーク接続先に到達することを許可または阻止します。

CDO はネットワークポリシーを作成するときに、それを ASA インターフェイスに関連付け、ポリシーに 1 つのデフォルトルールを作成します。インターフェイスに関連付けられたネットワークポリシーは、ASA では「アクセスグループ」と呼ばれます。ポリシー名は、ASA のアクセス制御リスト（ACL）名に相当します。CDO が作成したデフォルトのルールと、このネットワークポリシーに追加する後続のルールは、ASA ではアクセス コントロール エントリ（ACE）と呼ばれます。

関連情報：

- レガシービューの ASA ネットワークポリシーの作成
- ASA ネットワークポリシーの編集
- ASA ネットワークポリシーのコピー
- ASA ネットワークポリシーの比較
- ASA ネットワークポリシーの削除
- ASA ネットワークポリシーとルールの検索とフィルタ処理
- 共有 ASA ネットワークポリシー
- アクセス コントロール エントリ（ACE）

レガシービューの ASA ネットワークポリシーの作成

ASA ネットワークポリシーを作成するには、次の手順を実行します。

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 3 [デバイス] フィルタをクリックして、ポリシーを保存するデバイスを検索します。

ステップ 4 ポリシーの名前を入力します。1 つのデバイスに同じ名前のネットワークポリシーを 2 つ持つことはできません。

ステップ 5 このポリシーを適用するインターフェイスを選択します。

ステップ 6 ポリシーがアウトバウンドトラフィック用か、インバウンドトラフィック用かを指定します。同じデバイス上の同じ方向の同じインターフェイスに対して 2 つのポリシーを持つことはできません。

ステップ 7 [保存（Save）] をクリックします。CDO は、ネットワークポリシーと、そのポリシーの単一の「permit ip any any」ルールを作成します。

ステップ 8 必要に応じて、ASA ネットワークポリシーの編集。

ステップ 9 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するか、待機してから複数の変更を同時に展開します。

ASA ネットワークポリシーの編集

Defense Orchestrator を使用すると、ポリシーの詳細ページからネットワークポリシーとポリシールールを編集できます。次の方法で ASA ポリシーを編集できます。

- ポリシーの名前変更
- ポリシーへのルールの追加
- ポリシー内でのルールの移動
- ポリシー間でのルールの移動
- ポリシーのルールの非アクティブ化
- ルールアクティビティのログ記録
- ポリシーの時間範囲の定義

ポリシーの名前変更

ステップ 1 **[ポリシー（Policies）] > [ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 名前を変更するネットワークポリシーを選択します。

ステップ 3 詳細ペインの名前変更アイコン をクリックします。

ステップ 4 ポリシー名を編集し、青色のチェックボックスをクリックして変更を保存します。

ポリシーへのルールの追加

ステップ 1 [ポリシー（Policies）] > [ASAポリシー（ASA Policies）] を選択します。

ステップ 2 編集するネットワークポリシーを選択します。

ステップ 3 [ポリシーの編集（Edit Policy）] をクリックします。

ステップ 4 詳細ペインで、編集ツールのツールバーの をクリックして、ネットワークポリシーにルールを追加します。ポリシーで強調表示されたルールの上に新しいルールが追加されます。ルールは、ルールのリスト内の位置によって、1 から最後の番号までの順に優先順位付けされます。

（注） 新しいルールには、デフォルトで [許可（Permit）] アクションが割り当てられます。

ステップ 5 [保存（**Save**）] をクリックします。Defense Orchestrator によって、変更の影響を受けるデバイスが特定されます。

ステップ 6 ポリシーの詳細ペインで [デバイス（Devices ）] フィールドを確認します。エントリの最適数を超えた場合、ASA がインストールされている ASA ハードウェアモデルに応じて、「ACE カウントが超過しました。最大エントリ 500 に対し1000 エントリが見つかりました」のような警告が表示されます。

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。

ポリシー内でのルールの移動

ステップ 1 [ポリシー（Policies）] > [ASAポリシー（ASA Policies）] を選択します。

ステップ 2 ネットワークポリシーを選択します。

ステップ 3 詳細ペインで、[ポリシーの編集（Edit Policy）] をクリックします。

ステップ 4 ルールテーブルでルールを選択し、[編集ツール（Edit Tools）] バーで [カット（cut）] をクリックします。

ステップ 5 カットしたルールの後に配置するルールを選択します。ルールは、ルールのリスト内の位置によって優先順位付けされます。ルールの位置が高いほど、優先順位は高くなります。

ステップ 6 [貼り付け（paste）] をクリックします。

ステップ 7 [保存（**Save**）] をクリックします。Defense Orchestrator によって、変更の影響を受けるデバイスが特定されます。

ステップ 8 行った変更を今すぐすべてのデバイスの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。

ポリシー間でのルールの移動

あるポリシーのルールをコピーして、別のポリシーに貼り付けることができます。

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 コピーするルールを含むネットワークポリシーを選択します。

ステップ 3 詳細ペインで、[ポリシーの編集（Edit Policy）] をクリックします。

ステップ 4 ルールテーブルでルールを選択し、[編集ツール（Edit Tools）] バーで [コピー] をクリックします。

ステップ 5 [ポリシー（Policies）] > [ASAポリシー（ASA Policies）] を選択します。

ステップ 6 ルールをコピーするネットワークポリシーを選択します。

ステップ 7 詳細ペインで、[ポリシーの編集（Edit Policy）] をクリックします。

ステップ 8 コピーしたルールの後に配置するルールを選択します。ルールは、ルールのリスト内の位置によって優先順位付けされます。ルールの位置が高いほど、優先順位は高くなります。

ステップ 9 [貼り付け（paste）] をクリックします。

ステップ 10 [**保存（Save）**] をクリックします。Defense Orchestrator によって、変更の影響を受けるデバイスが特定されます。

ステップ 11 行った変更を今すぐすべてのデバイスの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。

ポリシーのルールの非アクティブ化

ルールはデフォルトでアクティブです。ポリシー内の個々のルールを非アクティブ化できます。

ステップ 1 [ポリシー（Policies）] > [ASAポリシー（ASA Policies）] を選択します。

ステップ 2 非アクティブ化するルールを含むネットワークポリシーを選択します。

ステップ 3 詳細ペインで、[ポリシーの編集（Edit Policy）] をクリックします。

ステップ 4 非アクティブ化するルールを選択します。

ステップ 5 [アクティブ（Active）] 設定をスライドしてオフにします。 

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [**保存（Save）**] をクリックします。Defense Orchestrator によって、変更の影響を受けるデバイスが特定されます。

ステップ 8 行った変更を今すぐすべてのデバイスの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。

ルールアクティビティのログ記録

ネットワークポリシールールに起因するアクティビティは、デフォルトではログに記録されません。個別のルールについて、ロギングを有効化できます。

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 有効化するルールを含むネットワークポリシーを選択します。

ステップ 3 詳細ペインで、[ポリシーの編集（Edit Policy）] をクリックします。

ステップ 4 アクティビティをログ記録するルールを選択します。

ステップ 5 スライダをクリックしてログを有効化にします。 

ステップ 6 [Edit] をクリックします。

ステップ 7 ロギングレベルと、そのルールからのアクティビティが収集される頻度を選択します。次の表に、syslog メッセージの重大度の一覧を示します。

重大度	説明
emergencies	システムが使用不可能な状態です。
alert	すぐに措置する必要があります。
critical	深刻な状況です。
error	エラー状態です。
warning	警告状態です。
Notification（通告）	正常ですが、注意を必要とする状況です。
informational	情報メッセージです。
debugging	デバッグ メッセージです。
（注）	ASA は、重大度 0（緊急）の syslog メッセージを生成しません。

ステップ 8 ロギング間隔を変更することもできます。ロギング間隔は、間隔中にログがヒットされた回数を示します。ロギング間隔は、1 ～ 600（秒単位）で定義されます。デフォルトは 300 です。この値は、ドロップ統計情報の収集に使用するキャッシュから非アクティブなフローを削除するためのタイムアウト値としても使用されます。

ステップ 9 [**保存（Save）**] をクリックします。Defense Orchestrator によって、変更の影響を受けるデバイスが特定されます。

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。

ポリシーの時間範囲の定義

時間ベースの ASA ネットワークポリシーにより、時刻に基づいたネットワークとリソースへのアクセスが許可されます。時刻は、時間範囲オブジェクトによって定義されます。時間範囲オブジェクトには開始時間と終了時間があり、定期的なイベントとして定義することもできます。

時間範囲オブジェクトが ASA ですでに定義されている場合は、それらをネットワークポリシーに関連付けることができます。時間範囲オブジェクトが ASA にまだ存在しない場合は、Defense Orchestrator の CLI ツールを使用して作成するか、ASA で直接作成する必要があります。

次の手順に従って、ネットワークポリシーの時間範囲を追加します。

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 編集するネットワークポリシーを選択します。

ステップ 3 [ポリシーの編集（Edit Policy）] をクリックします。

ステップ 4 [ネットワークポリシー（Network Policy）] ボックスで、スライダをクリックして時間範囲を有効にします。

ステップ 5 時間範囲オブジェクトを**作成**するか、ドロップダウンリストから既存の時間範囲オブジェクトを**選択**します。

ステップ 6 [**保存（Save**）] をクリックします。

ステップ 7 [デバイスとサービス] ページに戻り、ポリシーを編集したデバイスを選択します。デバイスが同期されていないことがわかります。

ステップ 8 [プレビューして展開...（Preview and deploy..）] をクリックします。

ステップ 9 [デバイスの同期（Device Sync）] ボックスで、ポリシーを作成するコマンドとポリシーのルールを確認します。

ステップ 10 示された変更に問題がない場合は、[デバイスに変更を適用（Apply Changes to Device）] をクリックします。

ステップ 11 行った変更を今すぐすべてのデバイスの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。

ASA ネットワークポリシーのコピー

この手順を使用して、ある ASA から別の ASA にネットワークポリシーをコピーします。

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 コピーするポリシーを検索してフィルタリングします。

ステップ 3 コピーするネットワークポリシーの行で、[コピー] アイコンをクリックします。

ステップ 4 ポリシーをデバイスに追加します。

- **単一のインターフェイスに割り当てられたネットワークポリシーの場合**：[デバイスにポリシーを追加（Add Policy to Device）] ダイアログボックスで、ポリシーをコピーするデバイス、インターフェイス、およびトラフィックの方向を選択します。グローバルアクセスポリシーを別のデバイスにコピーする場合
- **グローバルポリシーの場合**：[デバイスにポリシーを追加（Add Policy to Device）] ダイアログボックスで、ポリシーをコピーするデバイスを選択し、[グローバル ポリシーとして作成（Create as a global policy）] をオンにします。ポリシーのインターフェイスまたは方向を選択できないことがわかります。グローバルポリシーは常にデバイス上のすべてのインターフェイスに割り当てられ、常にインバウンドトラフィックを評価します。

ステップ 5 [**保存（Save**）] をクリックします。

ステップ 6 行った変更を今すぐレビューして展開するか、待機して、複数の変更を同時に展開します。すべてのデバイスの構成変更のプレビューと展開 （308 ページ）

ASA ネットワークポリシーの比較

ステップ 1 ナビゲーションウィンドウで、[ポリシー（Policies）] > [ASAポリシー（ASA Policies）] を選択します。

ステップ 2 ビューアの右上隅にある [比較] をクリックします。

ステップ 3 比較するポリシーを 2 つまで選択します。

ステップ 4 ビューアの下部にある [比較の表示（View Comparison）] をクリックします。これにより、比較ビューアが表示されます。完了したら、[完了（Done）] をクリックし、[比較を完了（Done Comparing）] をクリックします。

ASA ネットワークポリシーの削除

ステップ 1 ナビゲーションバーで、[デバイスとサービス] 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 [ASA] タブをクリックし、ポリシーを削除する ASA を検索して選択します。

ステップ 4 [管理]ペインで、[構成] をクリックします。

ステップ 5 [編集（Edit）] をクリックします。

ステップ 6 デバイス構成で、ネットワークポリシーとルールを探します。

ネットワークポリシーは、ASA 構成ファイルではアクセスグループと呼ばれ、次のようなフォーマットになっています。

```
access-group <ポリシー名> <トラフィックの方向> interface <インターフェイス名>
```

アクセスグループエントリの例を以下に示します。

```
access-group abc-75-1-out out interface interface-1
```

ネットワークルールは、ASA 構成ファイルではアクセスリストと呼ばれ、次のような形式になっています。

```
access-list <ポリシー名> extended permit ip any any
```

アクセスリストエントリの例を以下に示します。

```
access-list abc-75-1-out extended permit ip any any
```

ステップ 7 ネットワークポリシーを含む行とネットワークルールを含む行をハイライトして削除します。

ステップ 8 変更を [保存（Save）] します。

ステップ 9 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。

ASA ネットワークポリシーとルールの検索とフィルタ処理

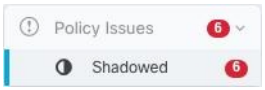
検索バーを使用して、ネットワークポリシーの名前およびポリシー内のルールに含まれる名前、キーワード、またはフレーズを検索します。検索では大文字と小文字が区別されません。

Filter

フィルタサイドバーを使用して、ネットワークポリシーの問題、共有ポリシー、および特定のデバイスのポリシーを見つけます。フィルタリングは。加算的ではなく、各フィルタ設定は互いに独立して機能します。

ポリシーの問題

CDO は、シャドウルールを含むネットワークポリシーを識別します。シャドウルールを含むポリシーの数は、[ポリシーの問題（Policy Issues）] フィルタに示されます。



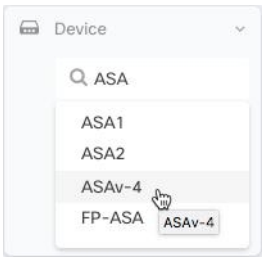
CDO は、ネットワークポリシーページのシャドウバッジ ◑ で、シャドウイングされたルールとそれらを含むネットワークポリシーをマークします。[シャドウイング済み（Shadowed）] をクリックして、シャドウイングされたルールを含むすべてのポリシーを表示します。詳細については、「シャドウイングされたルール」を参照してください。

Shared Policies

共有ポリシーは、複数のデバイスで検出されるポリシーです。共有ポリシーに加えられた変更は、そのポリシーが検出されたすべてのデバイスに影響します。次の例では、**inside-acl-in** ポリシーが 2 つのデバイスで共有されています。詳細については、「共有 ASA ネットワークポリシー」を参照してください。

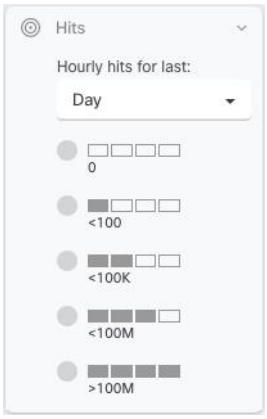
デバイス（Devices）

[デバイス] フィルタを展開し、[デバイスの検索（Search devices）] フィールドに名前または IP アドレスを入力して、ネットワークポリシーリストをデバイスでフィルタリングし、結果内で見つかったデバイスを選択します。



ヒット数（Hits）

このフィルタを使用して、指定された期間に何度もトリガーされたデバイスを対象にしてポリシーを特定します。



ヒットがゼロのネットワークポリシーを見つける

ヒットのないネットワークポリシーがある場合は、ネットワークポリシーを編集してより効果的にするか、単に削除することができます。

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 [フィルタ（Filter）] ペインで [すべて表示（Show All）] をクリックして、既存のフィルタをすべてクリアします。

ステップ 3 [ヒット（Hits）] フィルタを展開します。

ステップ 4 期間を選択します。

ステップ 5 0 ヒットを選択します。

ヒットがゼロのデバイス上のすべてのネットワークポリシーを見つける

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 [フィルタ（Filter）] ペインで [すべて表示（Show All）] をクリックして、既存のフィルタをすべてクリアします。

ステップ 3 [デバイス] フィルタを展開し、フィルタを適用するデバイスを選択します。
ステップ 4 [ヒット（Hits）] フィルタを展開します。
ステップ 5 期間を選択します。
ステップ 6 0 ヒットを選択します。

ネットワークポリシー内のルールがヒットする頻度の検索

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。
ステップ 2 [フィルタ（Filter）] ペインで [すべて表示（Show All）] をクリックして、既存のフィルタをすべてクリアします。
ステップ 3 1 つのデバイスで使用されるネットワークポリシーを選択します。
ステップ 4 ルールテーブルの [ヒット（Hits）] 列を調べて、ネットワークポリシーの各ルールがヒットしている頻度を確認します。
ステップ 5 ネットワークポリシーのルールが多すぎて結果を一目で確認できない場合は、[ヒット（Hits）] フィルタを展開します。
ステップ 6 期間を選択します。
ステップ 7 各種のヒットフィルタを選択して、各種のルールがどのカテゴリに分類されるかを確認します。

共有ネットワークポリシーがヒットする頻度の検索

ネットワークポリシーのヒット数は、個々のデバイスに対して計算されます。フィルタでデバイスを指定しないと、2 つ以上のデバイスで共有されている 1 つのネットワーク ポリシーのヒット率を表示できません。

ステップ 1 **[ポリシー（Policies）]** > **[ASAアクセスポリシー（ASA Access Policies）]**に移動します。
ステップ 2 ポリシーテーブルの上にある [クリア] をクリックして、既存のフィルタをクリアします。
ステップ 3 [共有ポリシー（Shared Policies）] フィルタを展開し、[共有（Shared）] をクリックします。
ステップ 4 共有されているネットワークポリシーを選択します。
ステップ 5 そのポリシーの詳細ペインで、そのネットワークポリシーを使用しているデバイスをメモしてから、ネットワーク ポリシー テーブルに戻ります。
ステップ 6 共有されているポリシーの名前を検索フィールドに入力します。
ステップ 7 [デバイス] フィルタを展開し、共有されているポリシーを使用しているいずれかのデバイスでフィルタします。
ステップ 8 [ヒット（Hits）] フィルタを展開します。
ステップ 9 期間を選択します。
ステップ 10 各種のヒットフィルタを選択して、ポリシーがどのカテゴリに分類されるのかを確認します。

ヒット率によるネットワークポリシーのフィルタ処理

ステップ 1 **[ポリシー（Policies）] > [ASAアクセスポリシー（ASA Access Policies）]** に移動します。

ステップ 2 ポリシーテーブルの上にある [クリア] をクリックして、既存のフィルタをクリアします。

ステップ 3 [ヒット（Hits）] フィルタを展開します。

ステップ 4 期間を選択します。

ステップ 5 異なるヒット率カテゴリを選択します。CDO は、指定したレートでヒットしているポリシーを表示します。ヒットレートの基準に一致する共有ネットワークポリシーがある場合、CDO は、共有ポリシーを使用するすべてのデバイスの行を表示します。

共有 ASA ネットワークポリシー

Cisco Defense Orchestrator（CDO）は、複数の ASA によって使用される同一のネットワークポリシーを見つけ、ネットワークポリシーページでそれらを識別します。共有ネットワークポリシーがある場合は、一度変更して、ポリシーを共有する他のデバイスに変更を配布できます。これにより、デバイス間でネットワークポリシーの一貫性が保たれます。

共有ネットワークポリシーの属性

ネットワーク ポリシー テーブルは、ネットワークポリシーを使用するデバイスの数を示します。複数のデバイスで使用されることを示すネットワークポリシーは、共有ポリシーです。共有ネットワークポリシーを検索するには、次の手順に従います。

ステップ 1 **[ポリシー（Policies）] > [ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 フィルタペインで、[すべて表示（Show All）] をクリックして、ページから過去のフィルタ条件または検索条件をクリアします。

ステップ 3 フィルタバーで、[共有ポリシー（Shared Policies）] を展開して [共有（Shared）] を選択します。

ステップ 4 検索バーにキーワードを入力して、さらに検索を絞り込みます。

ステップ 5 ネットワーク ポリシー テーブルから共有ネットワークポリシーを選択します。

（注） フィルタ条件と検索条件は組み合わせて使用されず、一度に1つしか使用できません。たとえば、「共有ポリシー（Shared Policies）」でフィルタリングすると、すべての共有ポリシーが表示されます。特定のデバイス名を検索に追加すると、ポリシーが共有されているかどうかに関係なく、そのデバイス名で使用されているすべてのネットワークポリシーが表示されます。

共有ネットワークポリシーの編集

ステップ 1 編集する共有 ASA ネットワークポリシー。

ステップ 2 共有ポリシーを選択します。CDO は、CDO 管理対象のどのデバイスがそのネットワークポリシーを使用するかを識別します。

ステップ 3 詳細ペインで、[ポリシーの編集（Edit Policy）] をクリックします。

ステップ 4 ポリシーのルールを編集します。

ステップ 5 [**保存（Save**）] をクリックします。

ステップ 6 [確認（Confirm）] で、変更の影響を受けるデバイスを確認します。

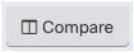
ステップ 7 [デバイスとサービス] ページを開いて、デバイスが同期されていないことを確認します。

ステップ 8 [変更を手動で展開...（Deploy Changes Manually...）] をクリックして、表示される指示に従って、ASA に保存されている設定を更新して変更を反映します。

共有ネットワークポリシーの比較

共有ネットワークポリシーを比較する目的は、少しだけ相違しているポリシーを探し、それらを再調整することです。ほとんど同じポリシーがいくつかある場合、それらは分岐したものであり、実際には同一のポリシーである可能性があります。ネットワークポリシーを再調整すると、CDO はポリシーを共有ポリシーとして認識します。ポリシーを変更する場合、そのポリシーを使用して他のデバイスに変更を配信できるようになります。

ステップ 1 比較する共有 ASA ネットワークポリシー。

ステップ 2 [比較] 

をクリックします。

ステップ 3 比較するネットワークポリシーを 2 つ選択し、[比較の表示（View Comparison）] をクリックします。

ステップ 4 違いをメモし、[比較を終了（Done Comparing）] をクリックします。

ステップ 5 ポリシーの 1 つを変更して他のポリシーと一致させる場合は、ネットワーク ポリシー テーブルからポリシーを選択し、詳細ペインで [ポリシーの編集（Edit Policy）] をクリックして編集します。

ASA ポリシー（拡張アクセスリスト）

Cisco Defense Orchestrator（CDO）は、ネットワークとアプリケーションのセキュリティポリシーをすべてのデバイスで一貫した状態に保つ機能をユーザーに提供します。この独自の機能により、複数のデバイスで同時にポリシーをシンプルかつ簡単に変更できます。

アクセス コントロール エントリ（ACE）

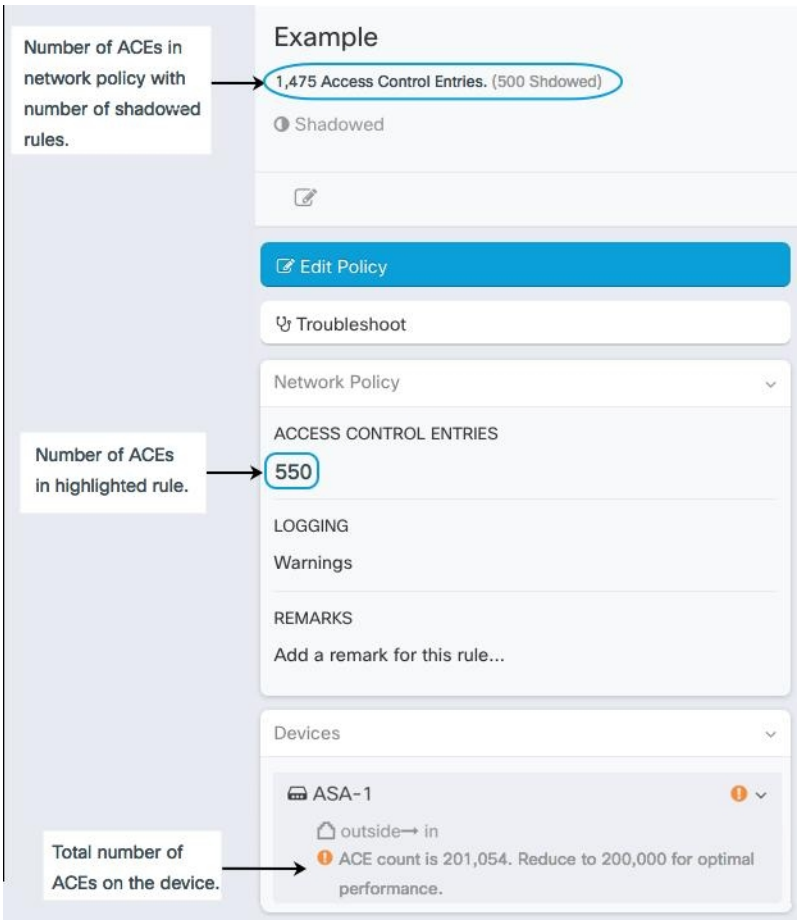
アクセス コントロール エントリについて、確認できるものと確認できないものについて考えてください。

確認できるものは、次のとおりです。CDO のユーザーインターフェイスに関しては、ネットワークポリシーに追加するルールは、ASA のアクセス コントロール エントリです。このルールでは、送信元アドレスと宛先アドレスの間、またはあるアドレスグループと別のアドレスグループの間で許可されるネットワークトラフィックを定義します。

確認できないものは、次のとおりです。ASA は、作成したネットワークルールを拡張して、そのネットワークルールによって暗示される送信元 IP アドレスと宛先 IP アドレスの可能なすべての組み合わせを考慮します。たとえば、1 つのネットワークオブジェクトの 3 つの IP アドレスが別のオブジェクトの 3 つの IP アドレスにアクセスすることを拒否するルールがある場合、ASA がメモリに格納する可能性のあるアクセス コントロール エントリは 9 つあります。

ASA が処理できる ACE の数にハードコードされた制限はありませんが、ACE の数が多すぎると、ASA のパフォーマンスが低下します。特定の ASA デバイスに予想される ACE エントリの最大数については、「Adaptive Security Appliance FAQ」 の表 4「Maximum Access Control Entries for Cisco ASA Models」を参照してください。

CDO は、すべてのネットワークポリシーから派生した ACE の総数を維持し、その ACE 数がアプライアンスで予想される ACE の最大制限数を超えると通知します。CDO が提供する情報は次のとおりです。



デバイス上の ACE 数の削減

予想される ACE の最大数を超えたデバイス上の ACE 数を減らすためのいくつかのアプローチを次に示します。

- 部分的なシャドウルールと完全なシャドウイングされたルールを持つポリシーを探します。必要に応じて、これらのルールを削除します。
- ネットワークポリシーをフィルタリングして、ヒットがゼロのデバイス上のすべてのネットワークポリシーを見つけるか、ヒットがゼロのネットワークポリシー内のルールがヒットする頻度の検索。該当する場合は、ヒットがゼロのポリシーまたはルールを削除します。
- 予想されるアクセス コントロール エントリ数を超えたASA ネットワークポリシーとルールの検索とフィルタ処理て、それらのポリシーを確認します。それらのポリシーの送信元と宛先のアドレス指定を、当初の計画どおりに広くする必要があるかどうかを検討してください。

ASA グローバルアクセスポリシーの設定

グローバルアクセスポリシーは、ASA のすべてのインターフェイスに適用されるネットワークポリシーです。これらのポリシーは、着信ネットワークトラフィックにのみ適用されます。一連のルールをすべての ASA インターフェイスに一様に適用する場合は、グローバルアクセスポリシーを作成します。

1 つの ASA に設定できるグローバルアクセスポリシーは 1 つだけです。他のポリシーと同様に、グローバルアクセスポリシーには複数のルールを割り当てることができます。

ASA グローバルアクセスポリシーは、特定のインターフェイスのネットワークポリシーの後、すべてのトラフィックの暗黙の拒否ルールの前に処理されます。ASA でのルール処理の順序は、次のとおりです。

1. インターフェイス アクセス規則。
2. ブリッジ グループ メンバーのインターフェイスでは、ブリッジ仮想インターフェイス（BVI）のアクセス ルール
3. グローバル アクセス ルール
4. 暗黙的な拒否

ASA グローバルアクセスポリシーの設定に関する制限事項

CDO では、ASA のグローバルアクセスポリシーを作成および編集できます。ただし、CDO に ASA を導入準備したときに ASA にグローバルアクセスポリシーが存在している場合、次の制限があります。

- ポリシーを編集することはできますが、デバイスごとに許可されるグローバルアクセスポリシーは 1 つしかないため、新しいポリシーを作成することはできません。
- ASA のグローバルアクセスポリシーに、CDO がサポートしていないルールが含まれている場合、そのポリシーを編集することはできません。
- ポリシーを削除するには、CLI インターフェイスを使用するか、デバイス構成ファイルを編集する必要があります。

グローバルアクセスポリシーの作成

ステップ 1 **[ポリシー（Policies）] > [ASAポリシー（ASA Policies）]** をクリックします。

ステップ 2 フィルタパネルで、ポリシーリストをフィルタ処理して、グローバルポリシーを追加するデバイスを見つけます。

ステップ 3 [ネットワークポリシー（Network Policies）] テーブルの [インターフェイス（Interfaces）] 列で、「グローバル（global）」というラベルの付いたポリシーがないことを確認します。

ステップ 4 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 5 [デバイス] ボタンをクリックし、グローバルポリシーを追加する ASA を選択します。[選択（Select）] をクリックします。

ステップ 6 ポリシーに名前を付け、[グローバルポリシーとして作成（Create as a global policy）] をオンにします。ポリシーのインターフェイスまたは方向を選択できないことがわかります。グローバルポリシーは常にデバイス上のすべてのインターフェイスに割り当てられ、常にインバウンドトラフィックを評価します。

ステップ 7 [保存（**Save**）] をクリックします。

ステップ 8 [ASAネットワークポリシーの編集（Edit an ASA Network Policy）] を使用して、新しいポリシーにルールを追加します。ASA ネットワークポリシーの編集 （167 ページ）

グローバルアクセスポリシーの編集

上記の構成の制限に留意し、[ASAネットワーク ポリシーの編集] を使用してグローバルアクセスポリシーを編集します。ASA ネットワークポリシーの編集 （167 ページ）

（注） [ポリシーの編集] ボタンが非アクティブになっているためにグローバルポリシーを編集できない場合は、ポリシーが ASA で作成され、CDO がサポートしていないオブジェクトを持つルールが含まれている可能性があります。これらのルールは、グローバル アクセス ポリシー テーブルでは表示されません。この場合、CDO の CLI ツールを使用して構成ファイルを編集する必要があります。これには CDO を使用して ASA の構成ファイルを編集するか、ASA で直接グローバルポリシーを編集します。

グローバルアクセスポリシーを別のデバイスにコピーする

[ASAネットワークポリシーのコピー] を使用して、グローバルアクセスポリシーを 1 つのデバイスから別のデバイスにコピーするか、グローバルアクセスポリシーを 1 つのデバイスから別のデバイスの単一のインターフェイスにコピーします。ASA ネットワークポリシーのコピー （171 ページ）

グローバルアクセスポリシーの削除

CDO のユーザーインターフェイスを使用してグローバルアクセスポリシーを削除することはできません。グローバルアクセスポリシーを削除するには、CDO の CLI ツールを使用してコマンドラインでグローバルアクセスポリシーを削除する必要があります。これには CDO を使用して ASA の構成ファイルを編集するか、ASA で直接グローバルポリシーを編集します。

ヒット率

CDO を使用すると、ポリシーの安全でスケーラブルなオーケストレーションに加えて、ポリシールールの結果を評価できるようになり、より正確なポリシー分析のためのシンプルな視覚

化と、根本原因への迅速で実行可能なピボットを、すべてクラウドから1つのペインで行うことが可能になります。ヒット率機能を使用すると、次のことが可能になります。

- 古く照合されないポリシールールを排除し、セキュリティ態勢を強化します。
- ボトルネックを即座に特定し、正確で効率的な優先順位付けを確実に実施することにより、ファイアウォールのパフォーマンスを最適化します（たとえば、トリガーされたポリシールールの優先順位が高くなります）。
- デバイスまたはポリシールールがリセットされた場合でも、設定されたデータ保持期間（1年）の間、ヒット率情報の履歴を維持します。
- 実用的な情報に基づいて、疑わしいシャドウおよび未使用のルールの検証を強化します。更新または削除についての疑問を解消します。
- 事前定義された時間間隔（日、週、月、年）と実際のヒットのスケール（ゼロ、>100、>100k など）を活用して、ポリシー全体のコンテキストでポリシールールの使用を視覚化し、ネットワークを通過するパケットへの影響を評価します。

ASA ポリシーのヒット率の表示

ステップ 1 CDO メニューバーから **[ポリシー（Policies）]** > **[ASAアクセスポリシー（ASA Access Policies）]** を選択します。

ステップ 2 フィルタアイコンをクリックして、開いた状態でピン留めします。

ステップ 3 [ヒット（Hits）]領域で、さまざまなヒットカウントフィルタをクリックして、他のポリシーよりもヒットの頻度が高いポリシーや低いポリシーを表示します。

ネットワークポリシールールのエクスポート

各 Access-Group または Crypto-Map の内容を .csv ファイルにエクスポートできます。この .csv には、各アクセス制御リスト（ACL）と、各 ACL について CDO が持つデータが表示されます。

ステップ 1 ナビゲーションウィンドウで、**[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 （任意）ASA ネットワークポリシーとルールの検索とフィルタ処理を使用して結果をフィルタ処理します。

ステップ 3 結果からネットワークポリシーを選択します。

ステップ 4 [CSVにエクスポート（Export to CSV）] 

をクリックします。

ステップ 5 CDO は、画面に表示されているルールを .csv ファイルにエクスポートします。

ASA ポリシー変更のデバイスへの適用

Cisco Defense Orchestrator（CDO）でセキュリティポリシーを変更すると、影響を受けるデバイスまたはサービスに変更がステージングされるため、設定が [非同期] になります。現在 [非同期] のデバイスやサービスで [デバイスに展開...（Deploy to Device...）] をクリックすると、ポリシーの変更を確認して適用することができます。

スクリプトによるデバイスの展開

ASAデバイスポリシー構成の変更が完了したら、変更を確認してデバイスに適用する必要があります。

ステップ 1 [デバイス] タブに移動し、[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、変更したデバイスをテーブルから選択します。構成ステータスには、デバイスにまだ適用されていない変更があることを示す [非同期] が表示されます。

ステップ 3 右側のサイドバーから [同期] をクリックし、デバイスと CDO 構成を同期済みステータスにするために、デバイスに適用するコマンドを生成します。

ステップ 4 プロンプトが表示されたら、[コマンドのダウンロード] をクリックして、コマンドのコピーをローカルにダウンロードします。これらのコマンドはテキストファイルに含まれており、適用する前に確認できます。必要に応じて変更を元に戻すためのコマンドも生成されます。

ステップ 5 CDOの外部で、標準プロトコルを使用してデバイスにログインし、ダウンロードしたコマンドを適用します。

ステップ 6 すべてのコマンドを入力したら、CDO に戻り、[デバイス] タブで変更されたデバイスを再度選択します。

ステップ 7 [更新] をクリックして、CDO との同期を確認します。

コマンドの一部が実行された場合、または追加のコマンドがアウトオブバンドで実行された場合、CDO は相違点を示すウィンドウを開いて相違点を示し、[競合検出] というステータスに更新することでユーザーに警告します。

ASA ポリシーのセキュリティグループタグ

アクセス制御ルール内で、セキュリティ グループ オブジェクト グループ（以下「SGT グループ」と呼ぶ）のセキュリティグループタグを使用する ASA を導入準備する場合、Cisco Defense Orchestrator では、これらの SGT グループを使用するルールを編集し、そのルールを持っているポリシーを管理できます。ただし、SGT グループを作成したり、CDO GUI を使用して編集したりすることはできません。SGT グループを作成または編集するには、ASA の Adaptive Security Device Manager（ASDM）、または CDO で使用可能なコマンド ライン インターフェイスを使用する必要があります。

CDO のオブジェクトページで SGT グループの詳細を読むと、それらのオブジェクトが編集不可のシステム提供オブジェクトとして識別されていることがわかります。

CDO管理者は、SGTグループを含むACLおよびASAポリシーで次のタスクを実行できます。

- CDO 管理者は、接続先および宛先セキュリティグループを除き、ACL のすべての側面を編集できます。
- SGT グループを含むポリシーを 1 つの ASA から別の ASA にコピーします。

コマンド ライン インターフェイスを使用して Cisco TrustSec を設定する手順の詳細については、お使いの ASA リリースの『ASA CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide』の「ASA and Cisco TrustSec」の章を参照してください。

シャドウイングされたルール

シャドウイングされたルールを含むネットワークポリシーは、ポリシーの少なくとも 1 つのルールがトリガーされることがないポリシーです。これは、それに先行するルールによって、シャドウイングされたルールによるパケットの評価が妨げられるためです。

たとえば、「example」ネットワークポリシーの次のネットワークオブジェクトとネットワークルールについて考えてみます。

```
object network 02-50
range 10.10.10.2 10.10.10.50
object network 02-100
range 10.10.10.2 10.10.10.100

access-list example extended deny ip any4 object 02-50
access-list example extended permit ip host 10.10.10.35 object 02-50
access-list example extended permit ip any4 object 02-100
```

次のルールによって評価されるトラフィックはありません

```
access-list example extended permit ip host 10.10.10.35 object 02-50
```

その理由は、先行するルール

```
access-list example extended deny ip any4 object 02-50
```

が、10.10.10.2 から 10.10.10.50 の範囲の任意アドレスから到達するすべて IPOv4 アドレスを拒否するためです。

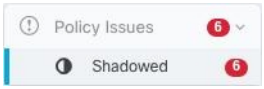
シャドウイングされたルールを持つネットワークポリシーを見つける

シャドウイングされたルールを持つネットワークポリシーを見つけるには、ネットワーク ポリシー フィルタを使用します。

ステップ 1 ナビゲーションウィンドウで、**[ポリシー]** > **[ASAポリシー]**を選択します。

ステップ 2 ASA アクセスポリシーテーブルの上部にあるフィルタアイコンをクリックします。

ステップ 3 [ポリシーの問題] フィルタで、[シャドウイング] をオンにして、シャドウイングされたルールを持つすべてのポリシーを表示します。



シャドウルールを使用した問題の解決

次に示すのは、CDO が前述の「例」のネットワークポリシーで説明されているルールを表示する方法です。

1 行目のルールは、ポリシー内の別のルールをシャドウしているため、シャドウ警告バッジ ⚠ のマークが付いています。2 行目のルールは、ポリシー内の別のルールによってシャドウされているため ◑ マークが付いています。2 行目のルールのアクションは、ポリシー内の別のルールによって完全にシャドウされているためグレー表示されています。CDO は、2 行目のルールをシャドウするポリシー内のルールを通知できます。

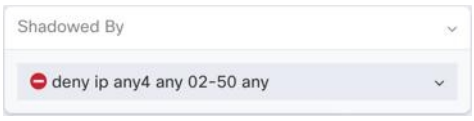
3 行目のルールは、時々のみトリガーできます。これは部分的なシャドウルールです。10.10.10.2 ～ 10.10.10.50 の範囲の IP アドレスに到達しようとする IPv4 アドレスからのネットワークトラフィックは、最初のルールによってすでに拒否されているため、評価されません。ただし、10.10.10.51 ～ 10.10.10.100 の範囲のアドレスに到達しようとする IPv4 アドレスは、最後のルールによって評価され、許可されます。

⚠

注意 CDO は、部分的なシャドウルールにシャドウ警告バッジ ⚠ を適用しません。

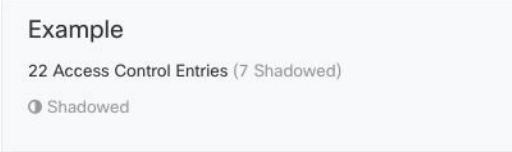
ステップ 1 ポリシーでシャドウルールを選択します。前述の例では、2 行目をクリックすることを意味します。

ステップ 2 ルールの詳細ペインで、[シャドウ基準（Shadowed By）] 領域を探します。この例では、2 行目のルールの [シャドウ基準（Shadowed By）] 領域は、1 行目のルールによってシャドウされていることを示しています。



ステップ 3 シャドウイングルールを確認します。広すぎる場合、シャドウルールを確認します。不要な場合、シャドウルールを編集するか、シャドウルールを削除します。

（注） シャドウルールを削除することで、ASA のアクセス コントロール エントリ（ACE）の数を減らすことができ、他の ACE で他のルールを作成するためのスペースが解放されます。CDO は、1 つのネットワークポリシーのすべてのルールから派生した ACE の数を計算し、ネットワークポリシーの詳細ペインの上部に合計を表示します。ネットワークポリシーのいずれかのルールがシャドウされている場合は、その数もリストされます。



CDO は、ネットワークポリシーの 1 つのルールから派生した ACE の数も表示し、その情報をネットワークポリシーの詳細ペインに表示します。リストの例を次に示します。

ステップ 4 ネットワークポリシーの詳細ペインの [デバイス（Devices）] 領域を調べて、ポリシーを使用するデバイスを特定します。

ステップ 5 [デバイスとサービス（Devices & Service）] ページを開き、ポリシー変更の影響を受けるデバイスに**変更を展開**し直します。

ネットワーク アドレス変換

IP ネットワーク内の各コンピュータおよびデバイスには、ホストを識別する固有の IP アドレスが割り当てられています。パブリック IPv4 アドレスが不足しているため、これらの IP アドレスの大部分はプライベートであり、企業のプライベートネットワークの外部にルーティングできません。RFC 1918 では、アドバタイズされない、内部で使用できるプライベート IP アドレスが次のように定義されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

ネットワーク アドレス変換（NAT）の主な機能の 1 つは、プライベート IP ネットワークがインターネットに接続できるようにすることです。NAT は、プライベート IP アドレスをパブリック IP に置き換え、内部プライベート ネットワーク内のプライベート アドレスをパブリック インターネットで使用可能な正式の、ルーティング可能なアドレスに変換します。このようにして、NAT はパブリック アドレスを節約します。これは、ネットワーク全体に対して 1 つのパ

ブリック アドレスだけを外部に最小限にアドバタイズするように NAT を設定できるためです。

NAT の他の機能は、次のとおりです。

- セキュリティ：内部アドレスを隠蔽し、直接攻撃を防止します。
- IP ルーティングソリューション：NAT を使用する際に、重複 IP アドレスが問題になりません。
- 柔軟性：外部で使用可能なパブリックアドレスに影響を与えずに、内部 IP アドレス方式を変更できます。たとえば、インターネットにアクセス可能なサーバーの場合、インターネット用に固定 IP アドレスを維持できますが、内部向けにサーバーのアドレスを変更することができます。
- IPv4 と IPv6（ルーテッドモードのみ）の間の変換：IPv4 ネットワークに IPv6 ネットワークを接続する場合は、NAT を使用すると、2 つのタイプのアドレス間で変換を行うことができます。

Cisco Defense Orchestrator を使用して、さまざまな使用例の NAT ルールを作成できます。NAT ルールウィザードまたは次のトピックを使用して、さまざまな NAT ルールを作成します。

NAT ルールの処理命令

ネットワーク オブジェクト NAT ルールおよび Twice NAT ルールは、3 セクションに分割される 1 つのテーブルに保存されます。最初にセクション 1 のルール、次にセクション 2、最後にセクション 3 というように、一致が見つかるまで順番に適用されます。たとえば、セクション 1 で一致が見つかった場合、セクション 2 とセクション 3 は評価されません。次の表に、各セクション内のルールの順序を示します。

表 *12 : NAT* ルール テーブル

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 1	Twice NAT（ASA） 手動 NAT（FTD）	設定に登場する順に、最初の一致ベースで適用されます。最初の一致が適用されるため、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、固有のルールを期待どおりに適用できない可能性があります。デフォルトでは、Twice NAT ルールはセクション 1 に追加されます。

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 2	ネットワークオブジェクト NAT（ASA） 自動 NAT（FTD）	セクション1で一致が見つからない場合、セクション2のルールが次の順序で適用されます。 **1.** スタティック ルール **2.** ダイナミック ルール **各ルールタイプでは、次の順序ガイドラインが使用されます。** **1.** 実際の IP アドレスの数量：小から大の順。たとえば、アドレスが 1 個のオブジェクトは、アドレスが 10 個のオブジェクトよりも先に評価されます。 **2.** 数量が同じ場合には、IP アドレス番号（最小から最大まで）が使用されます。たとえば、10.1.1.0 は、11.1.1.0 よりも先に評価されます。 **3.** 同じIPアドレスが使用される場合、ネットワーク オブジェクトの名前がアルファベット順で使用されます。たとえば、オブジェクト「Arlington」はオブジェクト「Detroit」の前に評価されます。
セクション 3	Twice NAT（ASA） 手動 NAT（FTD）	まだ一致が見つからない場合、セクション 3 のルールがコンフィギュレーションに登場する順に、最初の一致ベースで適用されます。このセクションには、最も一般的なルールを含める必要があります。このセクションにおいても、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、一般的なルールが適用されます。

たとえばセクション 2 のルールでは、ネットワーク オブジェクト内に定義されている次の IP アドレスがあるとします。

- 192.168.1.0/24（スタティック）
- 192.168.1.0/24（ダイナミック）
- 10.1.1.0/24（スタティック）
- 192.168.1.1/32（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト Detroit）

- 172.16.1.0/24（ダイナミック）（オブジェクト Arlington）

この結果、使用される順序は次のとおりです。

- 192.168.1.1/32（スタティック）
- 10.1.1.0/24（スタティック）
- 192.168.1.0/24（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト Arlington）
- 172.16.1.0/24（ダイナミック）（オブジェクト Detroit）
- 192.168.1.0/24（ダイナミック）

ネットワークアドレス変換ウィザード

ネットワークアドレス変換（NAT）ウィザードは、次のタイプのアクセスに使用するNATルールをデバイスで作成する際に役立ちます。

- **内部ユーザーのインターネットアクセスを有効にする**。この NAT ルールを使用して、内部ネットワーク上のユーザーがインターネットにアクセスできるようにすることができます。
- **内部サーバーをインターネットに公開する**。この NAT ルールを使用して、ネットワーク外のユーザーが内部 Web サーバーまたは電子メールサーバーにアクセスできるようにすることができます。

「内部ユーザーのインターネットアクセスを有効にする」ための前提条件

NAT ルールを作成する前に、次の情報を収集します。

- ユーザーに最も近いインターフェイス。通常これは「内部」インターフェイスと呼ばれます。
- インターネット接続に最も近いインターフェイス。通常これは「外部」インターフェイスと呼ばれます。
- 特定のユーザーのみにインターネットへのアクセスを許可する場合は、それらのユーザーのサブネットアドレスが必要です。

「内部サーバーをインターネットに公開する」ための前提条件

NAT ルールを作成する前に、次の情報を収集します。

- ユーザーに最も近いインターフェイス。通常これは「内部」インターフェイスと呼ばれます。

- インターネット接続に最も近いインターフェイス。通常これは「外部」インターフェイスと呼ばれます。
- インターネット側の IP アドレスに変換する、ネットワーク内のサーバーの IP アドレス。
- サーバーが使用するパブリック IP アドレス。

次の作業

NAT ウィザードを使用した NAT ルールの作成 （190 ページ） を参照してください。

NAT ウィザードを使用した NAT ルールの作成

始める前に

NAT ウィザードを使用して NAT ルールを作成するために必要な前提条件については、 ネットワークアドレス変換ウィザード （189 ページ）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（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 フィルタと検索を使用して、NAT ルールを作成するデバイスを見つけます。

ステップ 5 詳細パネルの [管理（Management）] 領域で、[NAT] NAT をクリックします。

ステップ 6 + > [NATウィザード（NAT Wizard）] をクリックします。

ステップ 7 NAT ウィザードの質問に回答し、画面の指示に従います。

- NAT ウィザードはネットワーク オブジェクト （142 ページ）を使用してルールを作成します。ドロップダウンメニューから既存のオブジェクトを選択するか、作成ボタン + Create... で新しいオブジェクトを作成します。
- NAT ルールを保存する前に、すべての IP アドレスをネットワークオブジェクトとして定義する必要があります。

ステップ 8 行った変更を今すぐすべてのデバイスの構成変更のプレビューと展開するか、待機してから複数の変更を同時に展開します。

NAT の一般的な使用例

Twice NAT と手動 NAT

「自動 NAT」とも呼ばれる「ネットワークオブジェクト NAT」を使用して達成できるいくつかの一般的なタスクを次に示します。

- 内部ネットワーク上のサーバーがパブリック IP アドレスを使用してインターネットに到達できるようにする （191 ページ）
- 内部ネットワーク上のユーザーが外部インターフェイスのパブリック IP アドレスを使用してインターネットにアクセスできるようにする （193 ページ）
- 内部ネットワーク上のサーバーをパブリック IP アドレスの特定のポートで使用できるようにする （194 ページ）
- プライベート IP アドレス範囲のパブリック IP アドレス範囲への変換 （199 ページ）

ネットワークオブジェクト NAT と自動 NAT

「手動 NAT」とも呼ばれる「Twice NAT」を使用して達成できる一般的なタスクを次に示します。

- 外部インターフェイスを通過する際に IP アドレスの範囲が変換されるのを防ぐ （201 ページ）

内部ネットワーク上のサーバーがパブリック IP アドレスを使用してインターネットに到達できるようにする

使用例

インターネットからアクセスする必要があるプライベート IP アドレスを持つサーバーがあり、1 つのパブリック IP アドレスからプライベート IP アドレスへの NAT に十分なパブリック IP アドレスがある場合は、この NAT 戦略を使用します。パブリック IP アドレスの数に限りがある場合は、「内部ネットワーク上のサーバーをパブリック IP アドレスの特定のポートで使用できるようにする」を参照してください（このソリューションの方が適している可能性があります）。

方法

サーバーは静的なプライベート IP アドレスを持ち、そのサーバーにネットワークの外部のユーザーがアクセスできる必要があります。静的プライベート IP アドレスを静的パブリック IP アドレスに変換するネットワークオブジェクト NAT ルールを作成します。その後、そのパブリック IP アドレスからのトラフィックがプライベート IP アドレスに到達できるようにするアクセスポリシーを作成します。最後に、これらの変更をデバイスに展開します。

始める前に

まず始めに、2 つのネットワークオブジェクトを作成します。一方のオブジェクトを「*servername*_inside」と名前を付け、もう一方のオブジェクトに「*servername*_outside」という名前を付けます。*servername*_inside ネットワークオブジェクトには、サーバーのプライベート IP アドレスが含まれている必要があります。*servername*_outside ネットワークオブジェクトには、サーバーのパブリック IP アドレスが含まれている必要があります。手順については、「ネットワーク オブジェクト」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（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 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理] ペインで [NAT] をクリックします。

ステップ 6  > [ネットワークオブジェクト NAT（Network Object NAT）] をクリックします。

ステップ 7 セクション 1の [タイプ] で、[静的（Static）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [内部（inside）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次のアクションを実行します。

1. [元のアドレス（Original Address）] メニューを展開し、[選択（Choose）] をクリックして、**servername_inside** オブジェクトを選択します。
2. [変換済みアドレス（Translated Address）] メニューを展開し、[選択]（Choose）] をクリックして、**servername_outside** オブジェクトを選択します。

ステップ 10 セクション 4 の [詳細（Advanced）] はスキップしてください。

ステップ 11 Firepower Threat Defense（FTD）の場合、セクション 5 の [名前（Name）] に NAT ルールの名前を入力します。

ステップ 12 [**保存（Save）**] をクリックします。

ステップ 13 ASA の場合はネットワークポリシールールを展開し、FTD の場合はアクセス コントロール ポリシールールを展開して、*servername*_inside から *servername*_outside へのトラフィックフローを可能にします。

ステップ 14 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。

ASA の保存済み構成ファイルのエントリ

この手順の結果として ASA の保存済み構成ファイル内に作成および表示されるエントリを次に示します。

（注） これは FTD デバイスには適用されません。

この手順によって作成されるオブジェクト：

```
object network servername_outside
host 209.165.1.29
object network servername_inside
host 10.1.2.29
```

この手順によって作成される *NAT* ルール：

```
object network servername_inside
 nat (inside,outside) static servername_outside
```

内部ネットワーク上のユーザーが外部インターフェイスのパブリック IP アドレスを使用してインターネットにアクセスできるようにする

使用例

外部インターフェイスのパブリックアドレスを共有することにより、プライベートネットワーク内のユーザーとコンピューターがインターネットに接続できるようにします。

方法

プライベートネットワーク上のすべてのユーザーがデバイスの外部インターフェイスのパブリック IP アドレスを共有できるようにするポートアドレス変換（PAT）ルールを作成します。

プライベートアドレスがパブリックアドレスとポート番号にマッピングされると、デバイスはそのマッピングを記録します。そのパブリック IP アドレスとポート宛の着信トラフィックを受信すると、デバイスはトラフィックを要求したプライベート IP アドレスにトラフィックを送り返します。

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（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 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理] ペインで [NAT] をクリックします。

ステップ 6  [ネットワークオブジェクトNAT] をクリックします。

ステップ 7 セクション 1 の [タイプ] で、[ダイナミック] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [任意（any）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次のアクションを実行します。

1. [元のアドレス（Original Address）] メニューを展開し、[選択（Choose）] をクリックして、ネットワーク構成に応じて [any-ipv4] オブジェクトまたは [any-ipv6] オブジェクトを選択します。
2. [変換済みアドレス（Translated Address）] メニューを展開し、利用可能なリストから [インターフェイス] を選択します。インターフェイスにより、外部インターフェイスのパブリックアドレスを使用することが示唆されています。

ステップ 10 Firepower Threat Defense（FTD）の場合、セクション 5 の [名前（Name）] に NAT ルールの名前を入力します。

ステップ 11 [保存（**Save**）] をクリックします。

ステップ 12 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。

ASA の保存済み構成ファイルのエントリ

この手順の結果として ASA の保存済み構成ファイル内に作成および表示されるエントリを次に示します。

（注） これは FTD デバイスには適用されません。

この手順によって作成されるオブジェクト：

```
object network any_network
subnet 0.0.0.0 0.0.0.0
```

この手順によって作成される *NAT* ルール：

```
object network any_network
nat (any,outside) dynamic interface
```

内部ネットワーク上のサーバーをパブリックIPアドレスの特定のポートで使用できるようにする

使用例

パブリック IP アドレスが 1 つしかない場合、または数が非常に限られている場合は、静的 IP アドレスとポートにバインドされた受信トラフィックを内部アドレスに変換するネットワークオブジェクト NAT ルールを作成できます。特定のケースの手順を提供していますが、これらはサポートされている他のアプリケーションのモデルとして使用できます。

前提条件

まず始めに、FTP、HTTP、および SMTP サーバーのネットワークオブジェクトを 1 つずつ、合計 3 つの個別のオブジェクトを作成します。この手順のために、これらのオブジェクトを **ftp-server-object**、**http-server-object**、および **smtp-server-object** と呼びます。手順については、

「ASA ネットワークオブジェクトおよびネットワークグループの作成または編集」「」を参照してください。

FTP サーバーへの NAT 着信 FTP トラフィック

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（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 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6 + > [ネットワークオブジェクトNAT] をクリックします。

ステップ 7 セクション 1 の [タイプ] で、[静的（Static）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [内部（inside）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次のアクションを実行します。

- [元のアドレス（Original Address）] メニューを展開し、[選択（Choose）] をクリックして、**ftp**-server-object を選択します。
- [変換済みアドレス（Translated Address）] メニューを展開し、[選択]（Choose）] をクリックして、[インターフェイス（Inerface）] を選択します。
- [ポート変換の使用（Use Port Translation）] にチェックを付けます。
- [tcp]、[ftp]、[ftp] を選択します。

ステップ 10 セクション 4 の [詳細（Advanced）] はスキップしてください。

ステップ 11 Firepower Threat Defense（FTD）の場合、セクション 5 の [名前（Name）] に NAT ルールの名前を入力します。

ステップ 12 [**保存（Save）**] をクリックします。NAT テーブルの NAT ルールの処理命令 に新しいルールが作成されます。

ステップ 13 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。

ASA の保存済み構成ファイルのエントリ

この手順の結果として ASA の保存済み構成ファイル内に作成および表示されるエントリを次に示します。

（注） これは FTD デバイスには適用されません。

この手順によって作成されるオブジェクト

```
object network ftp-object
host 10.1.2.27
```

この手順によって作成される *NAT* ルール

```
object network ftp-object
nat (inside,outside) static interface service tcp ftp ftp
```

HTTP サーバーへの NAT 着信 HTTP トラフィック

パブリック IP アドレスが 1 つしかない場合、または数が非常に限られている場合は、静的 IP アドレスとポートにバインドされた受信トラフィックを内部アドレスに変換するネットワークオブジェクト NAT ルールを作成できます。特定のケースの手順を提供していますが、これらはサポートされている他のアプリケーションのモデルとして使用できます。

始める前に

まず始めに、HTTP サーバーのネットワークオブジェクトを作成します。この手順のために、オブジェクトを **http-object** と呼びます。手順については、「ASA ネットワークオブジェクトおよびネットワークグループの作成または編集」「」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（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 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6 > [ネットワークオブジェクトNAT] をクリックします。

ステップ 7 セクション 1 の [タイプ] で、[静的（Static）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [内部（inside）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次のアクションを実行します。

- [オリジナルアドレス（Original Address）] メニューを展開し、[選択]（Choose）] をクリックして、**http** オブジェクトを選択します。

- [変換済みアドレス（Translated Address）] メニューを展開し、[選択]（Choose）] をクリックして、[インターフェイス（Inerface）] を選択します。
- [ポート変換の使用（Use Port Translation）] にチェックを付けます。
- **tcp**、**http**、http を選択します。

ステップ 10 セクション 4 の [詳細] はスキップしてください。

ステップ 11 Firepower Threat Defense（FTD）の場合、セクション 5 の [名前（Name）] に NAT ルールの名前を入力します。

ステップ 12 [**保存**（**Save**）] をクリックします。NAT テーブルの NAT ルールの処理命令 に新しいルールが作成されます。

ステップ 13 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、複数の変更を同時に展開します。

ASA の保存済み設定ファイルのエントリ

この手順の結果として ASA の保存済み設定ファイル内に作成および表示されるエントリを次に示します。

（注） これは FTD デバイスには適用されません。

この手順によって作成されるオブジェクト

```
object network http-object
host 10.1.2.28
```

この手順によって作成される *NAT* ルール

```
object network http-object
nat (inside,outside) static interface service tcp www www
```

SMTP サーバーへの NAT 着信 SMTP トラフィック

パブリック IP アドレスが 1 つしかない場合、または数が非常に限られている場合は、静的 IP アドレスとポートにバインドされた受信トラフィックを内部アドレスに変換するネットワークオブジェクト NAT ルールを作成できます。特定のケースの手順を提供していますが、これらはサポートされている他のアプリケーションのモデルとして使用できます。

始める前に

まず始めに、smtp サーバーのネットワークオブジェクトを作成します。この手順の説明では、オブジェクトを **smtp-object** と呼びます。手順については、「ASA ネットワークオブジェクトおよびネットワークグループの作成または編集」「」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（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 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6  > [ネットワークオブジェクトNAT] をクリックします。

ステップ 7 セクション 1 の [タイプ] で、[静的（Static）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [内部（inside）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次のアクションを実行します。

- [元のアドレス（Original Address）] メニューを展開し、[選択（Choose）] をクリックして、smtp-server-object を選択します。
- [変換済みアドレス（Translated Address）] メニューを展開し、[選択]（Choose）] をクリックして、[インターフェイス（Inerface）] を選択します。
- [ポート変換の使用（Use Port Translation）] にチェックを付けます。
- tcp、smtp、smtp を選択します。

ステップ 10 セクション 4 の [詳細（Advanced）] はスキップしてください。

ステップ 11 Firepower Threat Defense（FTD）の場合、セクション 5 の [名前（Name）] に NAT ルールの名前を入力します。

ステップ 12 [保存（**Save**）] をクリックします。NAT テーブルの NAT ルールの処理命令 に新しいルールが作成されます。

ステップ 13 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するか、待機してから複数の変更を同時に展開します。

ASA の保存済み構成ファイルのエントリ

この手順の結果として ASA の保存済み構成ファイル内に作成および表示されるエントリを次に示します。

（注） これは FTD デバイスには適用されません。

この手順によって作成されるオブジェクト

```
object network smtp-object
host 10.1.2.29
```

この手順によって作成される *NAT* ルール

```
object network smtp-object
nat (inside,outside) static interface service tcp smtp smtp
```

プライベート IP アドレス範囲のパブリック IP アドレス範囲への変換

使用例

特定のデバイスタイプまたはユーザータイプのグループがあり、IPアドレスを特定の範囲に変換して、受信側デバイス（トランザクションの反対側のデバイス）がトラフィックを許可する必要がある場合は、このアプローチを使用します。

内部アドレスのプールを外部アドレスのプールに変換

始める前に

変換するプライベート IP アドレスプールのネットワークオブジェクトを作成し、それらのプライベート IP アドレスの変換先となるパブリックアドレスプールのネットワークオブジェクトも作成します。

ASA の場合、「元のアドレス」プール（変換するプライベート IP アドレスプール）は、アドレス範囲を持つネットワークオブジェクト、サブネットを定義するネットワークオブジェクト、またはプール内のすべてのアドレスを含むネットワークグループにすることができます。FTDの場合、「元のアドレス」プールは、サブネットを定義するネットワークオブジェクト、またはプール内のすべてのアドレスを含むネットワークグループにすることができます。

（注） ASAの場合、「変換されたアドレス」のプールを定義するネットワークグループは、サブネットを定義するネットワークオブジェクトにすることはできません。

これらのアドレスプールを作成する場合は、「ASA ネットワークオブジェクトおよびネットワークグループの作成または編集」とを参照してください。

以下の手順のために、プライベートアドレスプールを **inside_pool**、パブリックアドレスプールを **outside_pool** と名付けました。

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 [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 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理] ペインで [NAT] をクリックします。

ステップ 6  > [ネットワークオブジェクトNAT] をクリックします。

ステップ 7 セクション 1 の [タイプ] で [ダイナミック] を選択し、[続行] をクリックします。

ステップ 8 セクション 2 の [インターフェイス] で、送信元インターフェイスを [内部] に設定し、接続先インターフェイスを [外部] に設定します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット] で、以下のタスクを実行します。

- [元アドレス] で、[選択] をクリックし、上記の前提条件セクションで作成した **inside_pool** ネットワークオブジェクト（またはネットワークグループ）を選択します。
- [変換されたアドレス] で、[選択] をクリックし、上記の前提条件セクションで作成した **outside_pool** ネットワークオブジェクト（またはネットワークグループ）を選択します。

ステップ 10 セクション 4 の [詳細] はスキップしてください。

ステップ 11 Firepower Threat Defense（FTD）の場合、セクション 5 の [名前] に NAT ルールの名前を入力します。

ステップ 12 [**保存**（**Save**）] をクリックします。

ステップ 13 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。

ASA の保存済み構成ファイルのエントリ

以下は、この手順の結果として ASA の保存済み構成ファイル内に表示されるエントリです。

（注） これは FTD デバイスには適用されません。

この手順によって作成されるオブジェクト

```
object network outside_pool
    range 209.165.1.1 209.165.1.255
object network inside_pool
    range 10.1.1.1 10.1.1.255
```

この手順によって作成される *NAT* ルール

```
object network inside_pool
nat (inside,outside) dynamic outside_pool
```

外部インターフェイスを通過する際にIPアドレスの範囲が変換されるのを防ぐ

使用例

この Twice NAT ユースケースを使用して、サイト間 VPN を有効にします。

方法

IP アドレスのプールをそれ自体に変換して、ネットワークのある場所の IP アドレスが変更されずに別の場所に届くようにします。

Twice NAT ルールの作成

始める前に

それ自体に変換する IP アドレスのプールを定義するネットワークオブジェクトまたはネットワークグループを作成します。 ASA の場合、アドレスの範囲は、IP アドレス範囲を使用するネットワークオブジェクト、サブネットを定義するネットワークオブジェクト、または範囲内のすべてのアドレスを含むネットワーク グループ オブジェクトによって定義できます。

ネットワークオブジェクトやネットワークグループを作成する場合は、『ASA ネットワークオブジェクトおよびネットワークグループの作成または編集』と『』を参照してください。

次の手順では、ネットワークオブジェクトまたはネットワークグループを Site-to-Site-PC-Pool と呼びます。

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（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 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6  > [Twice NAT] をクリックします。.

ステップ 7 セクション 1 の [タイプ] で、[静的（Static）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [内部（inside）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次の変更を行います。

- [元のアドレス（Original Address）] メニューを展開し、[選択（Choose）] をクリックして、前提条件セクションで作成した Site-to-Site-PC-Pool オブジェクトを選択します。

- [変換済みアドレス（Translated Address）] メニューを展開し、[選択（Choose）] をクリックして、前提条件セクションで作成した Site-to-Site-PC-Pool オブジェクトを選択します。

ステップ 10 セクション 4 の [詳細（Advanced）] はスキップしてください。

ステップ 11 Firepower Threat Defense（FTD）の場合、セクション 5 の [名前（Name）] に NAT ルールの名前を入力します。

ステップ 12 [**保存（Save**）] をクリックします。

ステップ 13 ASA の場合、クリプトマップを作成します。クリプトマップの作成方法の詳細については、『CLI ブック 3：Cisco ASA シリーズ VPN CLI コンフィギュレーション ガイド』の、「LAN-to-LAN IPsec VPN」の章を確認してください。

ステップ 14 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。

ASA の保存済み構成ファイルのエントリ

以下は、この手順の結果として ASA の保存済み構成ファイル内に作成および表示されるエントリです。

（注） これは FTD デバイスには適用されません。

この手順によって作成されるオブジェクト

```
object network Site-to-Site-PC-Pool
range 10.10.2.0 10.10.2.255
```

この手順によって作成される *NAT* ルール

```
nat (inside,outside) source static Site-to-Site-PC-Pool Site-to-Site-PC-Pool
```

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、適応型セキュリティアプライアンス（ASA）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、ASA 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
- リモートアクセス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。CDO に導入準備された ASA デバイスに存在するサイト間設定のみを監視できます。現在、CDO では、ASA デバイスでサイト間 VPN 設定を構成できません。ただし、デバイスが CDO に導入準備されている場合は、構成を監視できます。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：

- ASA 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

ASA 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 ASA デバイスで既存のサイト間 VPN 設定を監視できます。サイト間の設定は変更も削除もできません。

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 （207 ページ）[オンデマンド接続確認（on-demand connectivity check）] ボタンをクリックしていない場合、導入準備されているすべてのデバイスで利用可能なすべてトンネルに対する確認が 1 時間に一度実行されます。

（注）

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

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

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

[VPN] ページからトンネル接続を確認するには、次の手順を実行します。

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

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

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

VPN の問題の特定

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

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

トンネル設定の問題の解決 （206 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（Fnish）] 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 （308 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 （111 ページ）
- ASA デバイスの導入準備 （111 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。
  - [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。

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。

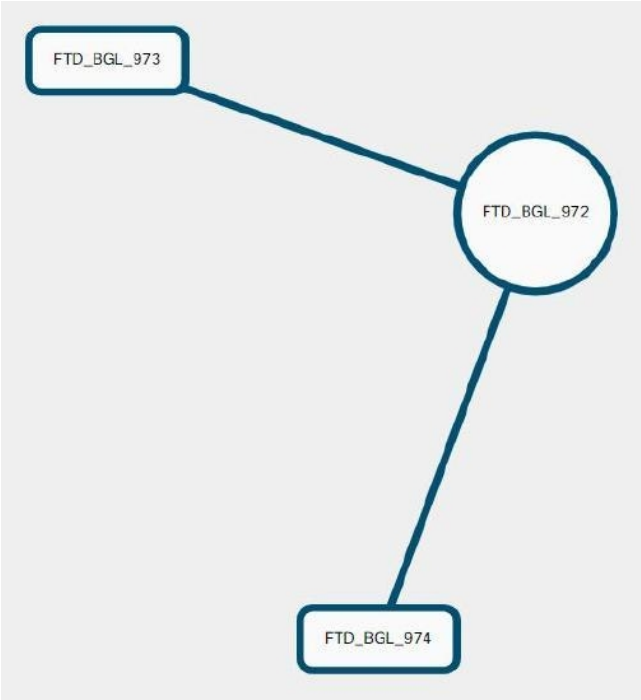
CDO がトンネルの両側を管理していない場合は、[導入準備デバイス（Onboard Device）] をクリックして、管理対象外のピアを導入準備するメインの導入準備ページを開くことができます。管理対象外 VPN ピアの導入準備 （206 ページ）CDO がトンネルの両側を管理する場合、[ピア2（Peer 2）] 列には管理対象デバイスの名前が含まれます。ただし、AWS VPC の場合、[ピア2（Peer 2）] 列には VPN ゲートウェイの IP アドレスが含まれています。

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。

リモートアクセス仮想プライベートネットワーク

リモートアクセス仮想プライベートネットワーク（RA VPN）では、各ユーザーがインターネットに接続されたコンピュータまたはその他のサポート対象の iOS または Android デバイスを使用して、離れた場所からネットワークに接続できます。これにより、モバイルワーカーが各自のホームネットワークや公共のWi-Fiネットワークから接続できるようになります。

RA VPN 設定は、次のコンポーネントで構成されています。

- 接続プロファイル：リモートアクセス VPN 接続プロファイルを作成すると、ホームネットワークなどの外部ネットワークからでも、ユーザーは内部ネットワークに接続できるようになります。異なる認証方式に対応するために、個別のプロファイルを作成します。接続プロファイルは、アイデンティティソースとグループポリシーで構成されます。

関連情報：

• ASA のリモートアクセス VPN を設定する （218 ページ）

リモートアクセス仮想プライベート ネットワーク セッションの監視

リモートアクセス仮想プライベートネットワーク（RA VPN）は、モバイルユーザーや在宅勤務者などのリモートユーザーにセキュアな接続を提供します。これらの接続をモニタリングすることで、接続とユーザーセッションのパフォーマンスの重要なインジケータを一目で把握できます。CDO リモートアクセス VPNのモニタリング機能を使用すると、リモートアクセス VPNの問題が存在するかどうか、および存在する場所を迅速に特定できます。この情報を利用し、ネットワーク管理ツールを使用して、ネットワークおよびユーザの問題を軽減したり、なくしたりすることが可能です。また、必要に応じてリモートアクセス VPN ユーザーをログアウトできます。

[リモートアクセス仮想プライベートモニタリング（Remote Access Virtual Private Monitoring）] ページには、[ライブ] と [履歴] の 2 つのビューがあります。テナント内のすべての 適応型セキュリティアプライアンス（ASA） VPN ヘッドエンドの AnyConnect リモートアクセス VPN セッションからリアルタイムデータまたは履歴データをモニタリングするために必要なビューを選択できます。

[リモートアクセス仮想プライベートモニタリング（Remote Access Virtual Private Monitoring）] ページには、各 RA VPN セッションからの次の情報が表示されます。

- RA VPN セッションからのライブデータと履歴データを提供します。
- CDO が管理するすべてのアクティブな VPN ヘッドエンドから一目でわかるビューを提供する直感的なグラフィカルビジュアルを表示します。
- ライブセッション画面には、CDO テナントで最も使用されているオペレーティングシステムと VPN 接続プロファイルが表示されます。また、平均セッション時間とアップロードおよびダウンロードされたデータも表示されます。
- ライブセッション画面には、RA VPN ヘッドエンドに接続されているユーザーの場所を可視化するためのインタラクティブなヒートマップが表示されます。
- 履歴セッション画面には、過去 24 時間、7 日間、および 30 日間にすべてのデバイスについて記録されたデータを示す棒グラフがプロットされます。
- デバイスの種類、セッションの長さ、アップロードとダウンロードのデータ範囲などの基準に基づいて検索を絞り込むための新しいフィルタリング機能を提供します。
- ユーザー名、ログイン時間、期間、およびセッションが非アクティブだった時間。
- エンタープライズ ネットワーク内で割り当てられた IP アドレスと、セッションが開始されたパブリック IP アドレス。
- セッションに関連付けられた接続プロファイルとグループポリシー情報。
- ユーザーセッションで使用される AnyConnect のバージョンとオペレーティングシステムのタイプ。
- セッションタイムアウトまでの残りのアイドル時間。

関連情報：

- AnyConnect リモートアクセス VPN ライブセッションのモニタリング （212 ページ）
- AnyConnect リモートアクセス VPN セッション履歴のモニターリング （214 ページ）
- リモートアクセス VPN セッションの検索とフィルタ処理
- リモートアクセス VPN モニタリングビューのカスタマイズ
- RA VPN セッションの CSV ファイルへのエクスポート
- ユーザーのすべてのアクティブな RA VPN セッションの切断

AnyConnect リモートアクセス VPN ライブセッションのモニタリング

デバイス上のアクティブな AnyConnect RA VPN セッションからのリアルタイムデータを監視できます。このデータは 10 分ごとに更新されます。画面の右隅に表示されるリロードアイコン をクリックすると、最新のデータを確認できます。

始める前に

- RA VPN ヘッドエンドを CDO に導入準備します。
- ライブデータを監視するデバイスの接続ステータスは、[インベントリ] ページで「オンライン」になっています。

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN] > [リモートアクセスVPNのモニタリング（Remote Access VPN Monitoring）]** をクリックします。

または、CDO ホームページで [アクティブリモートアクセスVPNセッションの表示（View Active Remote Access VPN Sessions）] をクリックするか、**[VPN] > [リモートアクセスVPN（Remote Access VPN）]** に移動して、右上隅の アイコンをクリックします。

ステップ 2 [ライブ] をクリックします。

CDO はデバイスからのライブ情報の取得を開始し、[リモートアクセスVPNのモニタリング（Remote Access VPN Monitoring）] ビューに RA VPN セッションを表示します。

（注） CDO がデバイスから情報を取得しないようにする場合は、[キャンセル] をクリックします。

ライブデータの表示

ライブデータは、ダッシュボードと表形式の両方で表示されます。

[ダッシュボード（Dashboard）] ビュー

ダッシュボードを表示するには、画面の右上隅に表示される [チャートビューの表示（Show Charts View）] アイコンをクリックする必要があります。

ダッシュボードには、CDO によって管理されるすべてのアクティブな VPN ヘッドエンドからの一目でわかるビューが表示されます。

- [内訳（すべてのデバイス）（Breakdown (All Devices)）]：ライブセッションの合計数が表示されます。また、4 つの弧の長さに分割された円グラフも表示されます。これは、セッション数が最も多い上位 3 つのデバイスの VPN セッションの割合を示しています。残りの弧の長さは、他のデバイスの総計を表します。
- CDO テナントで最も使用されているオペレーティングシステムと接続プロファイルが表示されます。
- 平均セッション時間とアップロードおよびダウンロードされたデータが表示されます。
- [国別のアクティブセッション（Active Sessions by Country）]：RA VPN ヘッドエンドに接続されているユーザーの場所を可視化するためのインタラクティブなヒートマップが表示されます。
  - ユーザーセッションがある国は、青の色合いで表示されます。
  - マップの下部にある凡例は、国のセッション数とその国の色に使用される青の色合いとの相関関係を示すスケールが表示されます。
  - 地図上にマウスポインタを合わせると、国名とアクティブなユーザーセッションの総数が表示されます。
  - テーブルにマウスポインタを合わせると、その国の場所とアクティブなユーザーセッションの総数が地図上に表示されます。

表形式のビュー

表形式のビューのみを表示するには、画面の右上隅に表示される [表形式のビューを表示（Show Tabular View）] アイコンをクリックする必要があります。

表形式のビューには、現在接続している VPN ユーザーの完全なリストが表示されます。

- [場所（Location）] 列には、パブリック IP アドレスを地理的に配置することにより、VPN ヘッドエンドに接続されているすべてのユーザーの場所が表示されます。行をクリックして、ユーザーの詳細を表示します。左ペインのロケーションリンクをクリックすると、ユーザーの場所が Google マップ上に表示されます。

重要 CDOは、ライブデータに標準フィルタを適用し、ダッシュボードにデータを表示します。ダッシュボードではカスタムフィルタはサポートされていないため、表形式のデータが表示されている場合にのみ、新しいフィルタを適用できます。新たに適用されたフィルタをクリアすると、ダッシュボードが再起動します（画面で[クリア]をクリックして、適用されたフィルタを手動で削除します）。標準フィルタは削除できません。

[RA VPNセッションの検索およびフィルタリング（Search and Filter RA VPN Sessions）] 機能を使用して、デバイスタイプ、セッションの長さ、アップロードおよびダウンロードのデータ範囲などの基準に基づいて検索を絞り込むことができます。リモートアクセス VPN セッションの検索とフィルタ処理 （215 ページ）一度に表示できる結果は最大 10,000 件です。

ステータス列の「アクティブ（Active）」ラベルの付いた緑色の点は、アクティブなVPNユーザーのセッションを示します。

AnyConnect リモートアクセス VPN セッション履歴のモニターリング

過去 3 ヵ月間に記録された AnyConnect リモートアクセス VPN セッションの履歴データをモニターリングできます。

始める前に

- RA VPN ヘッドエンドの CDO への導入準備をします。
- 履歴データを監視するデバイスの接続状態は、[インベントリ] ページで「オンライン」になっています。

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN] > [リモートアクセスVPNのモニターリング（Remote Access VPN Monitoring）]** をクリックします。

または、CDO ホームページで [アクティブリモートアクセスVPNセッションの表示（View Active Remote Access VPN Sessions）] をクリックするか、**[VPN] > [リモートアクセスVPN（Remote Access VPN）]**に移動して、右上隅の アイコンをクリックします。

ステップ 2 [履歴] をクリックします。

CDO には、過去 3 ヵ月間に記録された RA VPN セッションの履歴データが表示されます。

（注） CDOがデバイスから情報を取得しないようにする場合は、[キャンセル]（Cancel）]をクリックします。

履歴データの表示

履歴データは、ダッシュボードと表形式の両方で表示されます。

[ダッシュボード（Dashboard）] ビュー

ダッシュボードを表示するには、画面の右上隅に表示される [チャートビューの表示（Show Charts View）] アイコンをクリックする必要があります。表形式のビューとともに、ダッシュボードビューが表示されます。

ダッシュボードには、CDO によって管理されるすべてのアクティブな VPN ヘッドエンドからの一目でわかるビューが表示されます。過去 24 時間、7 日間、および 30 日間にすべてのデバイスで記録された VPN セッションを示す棒グラフが表示されます。ドロップダウンから期間を選択できます。個々のバーにカーソルを合わせると、日付とその日の合計セッション数が表示されます。

表形式のビュー

表形式のビューのみを表示するには、画面の右上隅に表示される [表形式のビューを表示（Show Tabular View）] アイコンをクリックする必要があります。表形式には、過去 3 ヵ月間に接続した VPN ユーザーの完全なリストが表示されます。

[場所（Location）] カラムには、パブリック IP アドレスを地理的に配置することにより、VPN ヘッドエンドに接続されているすべてのユーザーの場所が表示されます。行をクリックして、ユーザーの詳細を表示します。左ペインのロケーションリンクをクリックすると、ユーザーの場所が Google マップ上に表示されます。

重要 CDO は、履歴データに標準フィルタを適用し、ダッシュボードに表示します。ダッシュボードではカスタムフィルタはサポートされていないため、表形式のデータが表示されている場合にのみ、新しいフィルタを適用できます。新たに適用されたフィルタをクリアすると、ダッシュボードが再起動します（画面で [クリア] をクリックして、適用されたフィルタを手動で削除します）。標準フィルタは削除できません。

[RA VPNセッションの検索およびフィルタリング（Search and Filter RA VPN Sessions）]リモートアクセス VPN セッションの検索とフィルタ処理（215 ページ）機能を使用して、セッションの日と時間の範囲、セッションの長さ、アップロードおよびダウンロードのデータ範囲などの条件に基づいて検索を絞り込むことができます。一度に表示できる結果は最大 10,000 件です。

ステータス列の「アクティブ（Active）」ラベルの付いた緑色の点は、アクティブな VPN ユーザーのセッションを示します。

リモートアクセス VPN セッションの検索とフィルタ処理

検索（Search）

検索バー機能を使用して、RA VPN セッションを検索します。検索バーにデバイス名、IP アドレス、またはシリアル番号を入力し始めると、検索条件に一致する RA VPN セッションが表示されます。検索では大文字と小文字が区別されません。

Filter

フィルタサイドバーを使用して、セッション時間の範囲、セッションの長さ、アップロードおよびダウンロードのデータ範囲などの条件に基づいてRA VPNを特定できます。フィルタ機能は、ライブビューと履歴ビューの両方で使用できます。

- [デバイス]：1 つまたはすべてのデバイスを選択して、選択したデバイスからのセッションを表示します。
- [セッションの時間範囲（Sessions Time Range）]（履歴データにのみ適用）：指定した日時範囲のセッションの履歴を表示します。表示できるのは、過去 3 ヵ月間に記録されたデータのみです。
- [セッションの長さ（Sessions Length）]：指定されたセッションの継続時間に基づいてセッションを表示します。時間の単位（時間、分、または秒）を設定し、スライダを動かして、継続時間の最小長と最大長を指定します。表示されたフィールドで長さを指定することもできます。
- [アップロード（TX）（Upload (TX)）]：セキュリティで保護されたネットワークにアップロードまたは転送されたデータの指定量に基づいてセッションを表示します。単位（GB、MB、またはKB）を設定し、スライダを適宜動かして範囲を選択します。表示されるフィールドに値を指定することもできます。
- [ダウンロード（RX）（Download (RX)）]：セキュリティで保護されたネットワークからダウンロードまたは受信したデータの指定量に基づいてセッションを表示します。単位（GB、MB、または KB）を設定し、スライダを適宜動かして範囲を選択します。表示されるフィールドに値を指定することもできます。

リモートアクセス VPN モニタリングビューのカスタマイズ

ライブモードと履歴モードの両方のリモートアクセス VPN モニタリングビューを変更して、必要なビューに適用される列ヘッダーのみを含めることができます。列の右側にある列フィルタアイコン  をクリックし、必要な列を選択または選択解除します。

CDO に次回サインインしたとき、選択した内容が CDO に記憶されています。

RA VPN セッションの CSV ファイルへのエクスポート

1 つ以上のデバイスの RA VPN セッションをコンマ区切り値（.csv）ファイルにエクスポートできます。Microsoft Excel などのスプレッドシート アプリケーションで .csv ファイルを開いて、リストの項目を並べ替えたり、フィルタ処理したりできます。この情報は、RA VPN セッションの分析に役立ちます。セッションをエクスポートするたびに、CDO は new.csv ファイルを作成します。作成されるファイルの名前には日付と時刻が含まれます。

CDO は、最大 100,000 のアクティブセッションを CSV ファイルにエクスポートできます。すべてのデバイスからのセッションの合計数が上限を超えている場合は、[デバイス別表示（View By Device）] フィルタを使用して、個々のデバイスのレポートを生成できます。

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN]** > **[リモートアクセスVPNのモニタリング（Remote Access VPN Monitoring）]** をクリックします。

ステップ 2 [デバイス別表示（View By Devices）] 領域で、次のいずれかを選択します。

- [すべてのデバイス（All Devices）] は、その下に一覧表示されているすべてのデバイスからアクティブセッションをエクスポートします。
- セッションをエクスポートするデバイスをクリックします。

ステップ 3 右上隅の アイコンをクリックします。CDO は、画面に表示されているルールを .csv ファイルにエクスポートします。

ステップ 4 スプレッドシートアプリケーションで .csv ファイルを開いて、結果を並べ替えたりフィルタリングしたりすることができます。

ASA ユーザーのアクティブな RA VPN セッションの切断

ASA デバイス上のすべてのユーザーのアクティブな RA VPN セッションを終了できます。このタスクは、ライブモードと履歴モードの両方で実行できます。

CDO は、ユーザーが VPN セッションを表示および終了できるようにする VPN セッション マネージャー ユーザー ロールを提供します。詳細については、「ユーザの役割」を参照してください。

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN]** > **[リモートアクセスVPNのモニターリング（Remote Access VPN Monitoring）]** をクリックします。

ステップ 2 [デバイス別表示（View By Devices）] 領域で、デバイス上のすべてのアクティブなセッションを終了する ASA デバイスをクリックします。

ステップ 3 右上隅に表示される [すべてのセッションを終了（Terminate All Sessions）] をクリックします。

ステップ 4 [はい、すべてのセッションを終了します（Terminate All Sessions）] をクリックして、選択を確定します。

ユーザーのすべてのアクティブな *RA VPN* セッションの切断

CDO は、ユーザーを接続解除すると、ASA デバイス上のユーザーのアクティブな RA VPN セッションをすべて終了します。このタスクは、ライブモードと履歴モードの両方で実行できます。

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN]** > **[リモートアクセスVPNのモニターリング（Remote Access VPN Monitoring）]** をクリックします。

ステップ 2 セッションを切断するユーザーを検索します。[検索（Search）] バーに、検索条件を入力できます。

ステップ 3 アクティブなセッションをクリックし、右側の [アクション] ペインで、[このユーザーのすべてのRA VPN セッションを終了する（Terminate all RA VPN sessions for this user）] リンクをクリックします。

ASA のリモートアクセス VPN を設定する

ASACisco Secure Firewall Cloud Native は、ユーザーがプライベート接続と見なす TCP/IP ネットワーク（インターネットなど）全体でセキュアな接続を確立することにより、仮想プライベートネットワークを構築します。これによって、single-user-to-LAN 接続と LAN-to-LAN 接続を確立できます。

セキュアな接続はトンネルと呼ばれ、ASA はトンネリング プロトコルを使用して、セキュリティパラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを介したパケットの送受信、パケットのカプセル化解除を行います。ASA は、双方向トンネルのエンドポイントとして機能します。たとえば、プレーン パケットを受信してカプセル化し、それをトンネルのもう一方のエンドポイントに送信することができます。そのエンドポイントで、パケットはカプセル化を解除され、最終的な宛先に送信されます。また、セキュリティアプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。

CDO は、新しいリモートアクセス仮想プライベートネットワーク（RA VPN）を設定するための直感的なユーザーインターフェイスを提供します。また、CDO に導入準備された複数の適応型セキュリティアプライアンス（ASA）デバイスの RA VPN 接続をすばやく簡単に設定できます。

CDO を使用して、ASA デバイスで RA VPN 構成をゼロから設定できます。また、Adaptive Security Defense Manager（ASDM）や Cisco Security Manager（CSM）などの他の ASA 管理ツールを使用して構成済みの RA VPN 設定を管理することもできます。RA VPN 設定がすでにある ASA デバイスを導入準備すると、CDO は自動的に「デフォルトの RA VPN 構成」を作成し、ASA デバイスをこの構成に関連付けます。このデフォルト構成には、デバイスで定義されているすべての接続プロファイルオブジェクトを含めることができます。CDO に読み取られる RA VPN 属性を理解するには、「オンボーディング済み ASA デバイスの RA VPN 設定の読み取り」セクションを参照してください。それ以外の場合は、「ASA のエンドツーエンド リモート アクセス VPN 構成プロセス」で説明されている手順を実行してください。

関連情報：

- ASA のエンドツーエンド リモート アクセス VPN 設定プロセス
  - ASA のアイデンティティ ソースを設定する
    - ASA Active Directory レルム オブジェクトの作成または編集
    - ASA RADIUS サーバーオブジェクトまたはグループの作成または編集
  - 新規 ASA RA VPN グループポリシーの作成 （226 ページ）
  - ASA RA VPN 設定の作成 （235 ページ）
  - ASA RA VPN 接続プロファイルの設定 （239 ページ）

- オンボーディング済み ASA デバイスの RA VPN 設定の読み取り
- IP アドレスプールの作成
- NAT からの ASA リモート アクセス トラフィックの除外 （257 ページ）
- ASA のリモートアクセス VPN 設定の確認
- ASA のリモートアクセス VPN 設定の詳細表示

ASA のエンドツーエンド リモート アクセス VPN 設定プロセス

このセクションでは、CDO に導入準備された ASA デバイスでリモートアクセス仮想プライベートネットワーク（RA VPN）を設定するためのエンドツーエンドの手順について説明します。

クライアントのリモートアクセス VPN を有効化するには、いくつかの異なる項目を設定する必要があります。次の手順では、エンドツーエンドのプロセスについて説明します。

ステップ 1 リモート ユーザを認証する目的で使用されるアイデンティティ ソースを設定します。詳細については、「ASA のアイデンティティソースを設定する」を参照してください。

次のソースを使用して、RA VPN を使用してネットワークに接続しようとするユーザーを認証できます。さらに、クライアント証明書を単独で、またはアイデンティティソースと連携させて、認証に使用できます。

- Active Directory アイデンティティレルム：プライマリ認証ソースとして使用できます。ユーザ アカウントは Active Directory（AD）サーバで定義されます。「AD アイデンティティレルムの設定」を参照してください。「ASA Active Directory レルム オブジェクトの作成または編集」を参照してください。
- RADIUS サーバーグループ：プライマリまたはセカンダリ認証ソースとして使用でき、認可およびアカウンティングに使用できます。「ASA RADIUS サーバーオブジェクトまたはグループの作成または編集」を参照してください。
- ローカル ID ソース（ローカルユーザーデータベース）：プライマリソースまたはフォールバックソースとして使用できます。デバイスで直接ユーザを定義できます。外部サーバを使用することはできません。フォールバックソースとしてローカルデータベースを使用する場合は、必ず外部サーバーで定義したものと同じユーザー名/パスワードを定義します。注：ASA デバイスで直接ユーザーアカウントを作成できるのは、Adaptive Security Device Manager（ASDM）からのみです。『Cisco ASA Series Firewall ASDM Configuration Guide, XY』の「Objects for Access Control」の章の「Configure Local User Groups」セクションを参照してください

ステップ 2 （任意）新規 ASA RA VPN グループポリシーの作成 （226 ページ）。グループポリシーは、ユーザーに関連する属性を定義します。グループメンバーシップに基づいて、リソースへの差分アクセスを提供するためにグループポリシーを設定することができます。または、すべての接続でデフォルトポリシーを使用します。

ステップ 3 ASA RA VPN 設定の作成 （235 ページ）。

ステップ 4 ASA RA VPN 接続プロファイルの設定 （239 ページ）。

ステップ 5 （任意）NAT からの ASA リモート アクセス トラフィックの除外 （257 ページ）。

ステップ 6 CDO から ASA に設定変更を展開します。。

重要 Adaptive Security Device Manager（ASDM）などのローカルマネージャーを使用してリモートアクセス VPN の設定を変更すると、CDO では、そのデバイスの [設定ステータス（Configuration Status）] に [競合検出（Conflict Detected）] と表示されます。「デバイスのアウトオブバンド変更」を参照してください。この ASA で設定の競合の解決できます。

次のタスク

次の手順

RA VPN 設定が ASA デバイスにダウンロードされると、ユーザーは、インターネットに接続されているコンピュータやその他のサポートされている iOS または Android デバイスを使用して、リモートの場所からネットワークに接続できます。テナント内のすべての導入準備 ASA RA VPN ヘッドエンドから、ライブ AnyConnect リモートアクセス仮想プライベートネットワーク（RA VPN）セッションを監視できます。「リモートアクセス仮想プライベート ネットワーク セッションの監視」を参照してください。

ASA のアイデンティティ ソースを設定する

Microsoft Active Directory（AD）レルムや RADIUS サーバーなどのアイデンティティ ソースは、組織内のユーザーのユーザーアカウントを定義する AAA サーバーおよびデータベースです。この情報は、IP アドレスに関連付けられているユーザー ID の提供や、CDO へのリモートアクセス VPN 接続またはアクセスを認証するなど、さまざまな方法で利用できます。

[オブジェクト] > [オブジェクトの作成]（  ）> [アイデンティティ ソース] をクリックしてソースを作成します。アイデンティティ ソースを必要とするサービスを設定するときに、次のオブジェクトを使用します。適切なフィルタを適用して既存のソースを検索し、それらを管理できます。

ディレクトリ ベースの DN の決定

ディレクトリの各プロパティを設定する際、ユーザおよびグループに共通のベース識別名（DN）を指定する必要があります。ベースはディレクトリサーバー内で定義され、ネットワークごとに異なります。アイデンティティ ポリシーが正しく機能するには、適切なベースを入力する必要があります。ベースが誤っていると、ユーザ名またはグループ名が特定されず、アイデンティティに基づくポリシーが機能しなくなります。

（注） 正しいベースを取得するには、ディレクトリ サーバを担当する管理者に確認してください。

Active Directory の場合、ドメイン管理者として Active Directory サーバーにログインし、コマンドプロンプトで **dsquery** のコマンドを次のように使用することで、正しいベースを判別できます。

ユーザ検索ベース

dsquery user コマンドを入力し、ベース識別名を調べたい既知のユーザー名（一部または全体）を指定します。たとえば、次のコマンドでは、「John*」という部分名を使用して、「John」から始まるすべてのユーザーの情報を返します。

C:\Users\Administrator>dsquery user -name "John*"

"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"

ベース DN は「DC=csc-lab,DC=example,DC=com」となります。

グループ検索ベース

dsquery group コマンドを入力し、ベース識別名を調べたい既知のグループ名（一部または全部）を指定します。たとえば、次のコマンドは、Employees グループ名を使用して次に識別名を返します。

C:\>dsquery group -name "Employees"

"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"

グループのベース DN は、「DC=csc-lab,DC=example,DC=com」となります。

ADSI Edit プログラムを使用して、Active Directory 構造を参照することもできます（**[スタート（Start）] > [ファイル名を指定して実行（Run）] > [adsiedit.msc]**）。ADSI Edit で組織ユニット（OU）、グループ、ユーザーなどのオブジェクトを右クリックし、[プロパティ（Properties）] を選択すると、識別名が表示されます。DC 値の文字列を、ベースとしてコピーします。

正しいベースであることを確認するには、次の手順を実行します。

ステップ 1 ディレクトリ プロパティの [テスト接続（Test Connection）] ボタンをクリックし、接続を確認します。問題があった場合には修正して、ディレクトリ プロパティを保存します。

ステップ 2 変更をデバイスに適用します。

ステップ 3 アクセス ルールを作成して、[ユーザ（Users）] タブを選択し、ディレクトリから既知のユーザおよびグループ名の追加を試みます。ディレクトリを含むレルム内の一致ユーザ名およびグループ名を入力すると、入力中にオートコンプリートによる候補が表示されます。ドロップダウン リストに候補が表示される場合は、システムがディレクトリに適切に照会できたことを意味します。入力した文字列がユーザ名またはグループ名として表示されることが確かであるにもかかわらず、候補が表示されない場合は、対応する検索ベースを修正する必要があります。

次のタスク

詳細については、「ASA Active Directory レルム オブジェクトの作成または編集」を参照してください。

RADIUS サーバおよびグループ

RADIUS サーバーを使用して、管理ユーザーを認証および認可できます。RADIUS サーバを使用するように機能を設定する場合は、個別のサーバではなく RADIUS グループを選択します。RADIUS グループは、相互にコピーである RADIUS サーバの集合です。グループに複数のサー

バがある場合は、それらは、1 つのサーバが使用できなくなった場合に冗長性を提供する一連のバックアップサーバを形成します。ただし、サーバが1つしかない場合でも、機能のRADIUSサポートを設定するには、メンバーが 1 つのグループを作成する必要があります。

このソースは、以下の目的で使用できます。

- 認証、および許可、アカウンティングのアイデンティティソースとしてのリモートアクセス VPN。AD は RADIUS サーバーと組み合わせて使用できます。
- アイデンティティ ポリシー（リモート アクセス VPN ログインからユーザー アイデンティティを収集するためのパッシブ アイデンティティ ソースとして）。

詳細については、「ASA RADIUS サーバーオブジェクトまたはグループの作成または編集」を参照してください。

ASA Active Directory レルム オブジェクトの作成または編集

AD レルムオブジェクトなどの ID ソースオブジェクトを作成または編集すると、CDO は SDC を介して ASA デバイスに設定要求を送信します。次に ASA は、設定された AD レルムと通信します。

次の手順を使用して、オブジェクトを作成します。

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

ステップ 2 **[オブジェクトの作成]**（  ）**[RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）] > [アイデンティティ ソース（Identity Source 0]**をクリックします。

ステップ 3 オブジェクトの [オブジェクト名（Object Name）] を入力します。

ステップ 4 [デバイスタイプ（Device Tipe）] で [ASA] を選択します。

ステップ 5 ウィザードの最初の部分で、[IDソースタイプ（Identity Source Type）]として [Active Directoryレルム（Active Directory Realm）] を選択します。[続行（Continue）] をクリックします。

ステップ 6 基本レルムのプロパティを設定します。

- [ディレクトリユーザー名（Directory Username）]、[ディレクトリパスワード（Directory Password）]：取得するユーザー情報に対して適切な権限を持つユーザーの識別用ユーザー名とパスワード。Active Directory では、昇格されたユーザ特権は必要ありません。ドメイン内の任意のユーザを指定できます。ユーザー名は Administrator@example.com などの完全修飾名である必要があります（Administrator だけでなく）。

  （注） この情報から ldap-login-dn と ldap-login-password が生成されます。たとえば、Administrator@example.com は cn=administrator,cn=users,dc=example,dc=com に変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザーは、共通名の「users」フォルダの下で設定する必要があります。

- [ベース識別名（Base Distinguished Name）]：ユーザーおよびグループ情報、つまり、ユーザーとグループの共通の親を検索またはクエリするためのディレクトリツリー。例、cn=users,dc=example,dc=com。

ステップ 7 ディレクトリ サーバのプロパティを設定します。

- [ホスト名またはIPアドレス（Hostname/IP Address）]：ディレクトリ サーバのホスト名または IP アドレス。サーバに対して暗号化された接続を使用する場合、IP アドレスではなく、完全修飾ドメイン名を入力する必要があります。
- [ポート（Port）]：サーバとの通信に使用するポート番号。デフォルトは 389 です。暗号化方式として LDAPS を選択する場合は、ポート 636 を使用します。
- [暗号化（Encryption）]：ユーザーおよびグループ情報のダウンロードに暗号化接続を使用するには、[LDAPS] を選択し、SSL を使用して ASA と LDAP サーバー間の通信を保護します。LDAP over SSL が必要です。ポート 636 を使用します。

  デフォルトでは[なし（None）]になっており、ユーザおよびグループの情報がクリア テキストでダウンロードされます。

ステップ 8 （オプション）[テスト（Test）] ボタンを使用して、構成を検証します。

ステップ 9 （オプション）[別の構成を追加（Add another configuration）] をクリックして、複数の Active Directory（AD）サーバーを AD レルムに追加します。AD サーバーは互いの複製である必要があり、同じ AD ドメインをサポートする必要があります。したがって、ディレクトリ名、ディレクトリパスワード、ベース識別名などの基本的なレルムプロパティは、その AD レルムに関連付けられたすべての AD サーバーで同じである必要があります。

ステップ 10 [追加（Add）] をクリックします。

ASA Active Directory レルム オブジェクトの編集

アイデンティティ ソース オブジェクトの編集時にアイデンティティ ソース タイプを変更できないことに注意してください。正しいタイプの新しいオブジェクトを作成する必要があります。

ステップ 1 ナビゲーションバーで、[オブジェクト] をクリックします。

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

ステップ 3 編集するオブジェクトを選択します。

ステップ 4 詳細パネルの [操作（Actions）] ウィンドウにある編集アイコン をクリックします。

ステップ 5 ダイアログボックスの値を、上記の手順で作成したときと同じ方法で編集します。下に表示される設定バーを展開し、ホスト名/IP アドレスや暗号化情報を編集またはテストします。

ステップ 6 **[保存（Save）]** をクリックします。

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

ステップ 8 行った変更を今すぐCDO から ASA に設定変更を展開します。か、待機してから複数の変更を一度に展開します。

ASA RADIUS サーバーオブジェクトまたはグループの作成または編集

RADIUS サーバーオブジェクトや RADIUS サーバーオブジェクトのグループなどの ID ソースオブジェクトを作成または編集すると、CDO は SDC を介して設定要求を ASA デバイスに送信します。

RADIUS サーバーオブジェクトの作成

RADIUS サーバーは、AAA（認証、認可、アカウンティング）サービスを提供します。

次の手順を使用して、オブジェクトを作成します。

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

ステップ 2 **[オブジェクトの作成]**（  ）> **[RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）]** > **[アイデンティティ ソース]**をクリックします。

ステップ 3 オブジェクトの [オブジェクト名（Object name）] を入力します。

ステップ 4 [デバイスタイプ（Device Tipe）] で [ASA] を選択します。

ステップ 5 [アイデンティティ ソース タイプ（Identity Source Type）] として [RADIUSサーバーグループ（RADIUS Server Group）] を選択します。[続行（Continue）] をクリックします。

ステップ 6 次のプロパティを使用して ID ソース設定を編集します。

- [サーバー名またはIPアドレス（Server Name or IP Address）]：サーバーの完全修飾ホスト名（FQDN）または IP アドレス。
- [認証ポート（Authentication Port）]（オプション）：RADIUS 認証および承認が行われるポートです。デフォルトは 1812 です。
- [タイムアウト（Timeout）]：次のサーバーに要求を送信する前にサーバーからの応答を待機する時間の長さ（1 ～ 300 秒）。デフォルトは 10 秒です。
- [サーバー秘密キー（Server Secret Key）] の入力（オプション）：ASA デバイスと RADIUS サーバー間でデータを暗号化するために使用される共有秘密。キーは、大文字と小文字が区別される最大 64 文字の英数字文字列です。スペースは使用できません。キーは、英数字または下線で開始する必要があります。特殊文字 $ & - _ . + @ を使用できます。文字列は、RADIUS サーバーで設定された文字列と一致している必要があります。秘密キーを設定していない場合、接続は暗号化されません。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 行った変更を今すぐCDO から ASA に設定変更を展開します。か、待機してから複数の変更を一度に展開します。

RADIUS サーバーグループの作成

RADIUS サーバーグループには、1 つまたは複数の RADIUS サーバーオブジェクトが含まれています。グループ内のサーバーは、相互にコピーされる必要があります。グループ内のサーバーでバックアップサーバーのチェーンが形成されるため、最初のサーバーが利用できなった場合、システムはリスト上の次のサーバーを試すことができます。

次の手順を使用して、オブジェクトグループを作成します。

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

ステップ 2 **[オブジェクトの作成]**（  ）**[RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）] [アイデンティティソース（Identity Source 0]** をクリックします。

ステップ 3 オブジェクトの [オブジェクト名（Object name）] を入力します。

ステップ 4 [デバイスタイプ（Device Tipe）] で [ASA] を選択します。

ステップ 5 [アイデンティティ ソース タイプ（Identity Source Type）] として [RADIUSサーバーグループ（RADIUS Server Group）] を選択します。[続行（Continue）] をクリックします。

ステップ 6 次のプロパティを使用して ID ソース設定を編集します。

- [デッドタイム（Dead Time）]：失敗したサーバーは、すべてのサーバーが失敗した後にのみ再アクティブ化されます。デッドタイムは、最後のサーバーが失敗した後にすべてのサーバーを再アクティブ化するまで待機する時間の長さです。
- [最大失敗試行回数（Maximum Failed Attempts）]：次のサーバーを試行する前に、グループ内の RADIUS サーバーに送信されて失敗した要求の数（応答がなかった要求の数）。最大失敗試行回数を超えると、システムはそのサーバーを故障としてマークします。特定の機能について、ローカルデータベースを使用するフォールバック方式を設定していて、グループ内のすべてのサーバーが応答に失敗した場合、そのグループは非応答と見なされ、フォールバック方式が試行されます。サーバーグループはデッドタイムの間、非応答とマークされたままになるため、その期間内に追加の AAA 要求でサーバーグループへの接続は試行されず、フォールバック方式がすぐに使用されます。
- （任意）[ダイナミック認証/ポート（Dynamic Authorization/Port）]：RADIUS サーバーグループ向けの RADIUS ダイナミック認証または認可変更（CoA）サービスを有効にすると、そのグループは CoA 通知用に登録され、Cisco Identity Services Engine（ISE）からの CoA ポリシー更新を指定したポートでリッスンします。このサーバー グループを ISE と併せてリモート アクセス VPN で使用する場合にのみ動的認可をイネーブルにします。

ステップ 7 ドロップダウンメニューから、RADIUS サーバーをサポートする AD レルムを選択します。AD レルムをまだ作成していない場合は、ドロップダウンメニューの [作成（Create）] をクリックします。

ステップ 8 [RADIUSサーバーの追加（RADIUS SERVER Add）] ボタン  をクリックして、既存の RADIUS サーバーオブジェクトを追加します。必要に応じて、このウィンドウから新しい RADIUS サーバーオブジェクトを作成できます。

（注） リストの最初のサーバーは応答しなくなるまで使用されるため、作成したサーバーオブジェクトを優先して追加します。その後、ASA はデフォルトでリスト内の次のサーバーに設定されます。

ステップ 9 行った変更を今すぐCDO から ASA に設定変更を展開します。か、待機してから複数の変更を一度に展開します。

RADIUS サーバーオブジェクトまたはグループの編集

RADIUS サーバーオブジェクトまたは RADIUS サーバーグループを編集するには、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、[オブジェクト（Objects）] をクリックします。
ステップ 2 オブジェクトフィルタと [検索（search）] フィールドを使用して、編集するオブジェクトを見つけます。
ステップ 3 編集するオブジェクトを選択します。
ステップ 4 詳細パネルの [アクション] ペインにある [編集] アイコン をクリックします。
ステップ 5 前述の手順で作成したのと同じ方法で、ダイアログボックスの値を編集します。ホスト名/IP アドレスまたは暗号化情報を編集またはテストするには、設定バーを展開します。
ステップ 6 [保存（Save）] をクリックします。
ステップ 7 CDO は、変更の影響を受けるポリシーを表示します。[確認（Confirm）] をクリックして、オブジェクトとその影響を受けるポリシーへの変更を確定します。
ステップ 8 行った変更を今すぐCDO から ASA に設定変更を展開します。か、待機して、複数の変更を同時に展開します。

新規 *ASA RA VPN* グループポリシーの作成

グループポリシーは、リモートアクセス VPN ユーザーの一連のユーザー指向属性値ペアです。接続プロファイルでは、トンネル確立後、ユーザー接続の条件を設定するグループポリシーが使用されます。グループ ポリシーを使用すると、ユーザーまたはユーザーのグループに属性セット全体を適用できるので、ユーザーごとに各属性を個別に指定する必要がありません。

システムには、「DfltGrpPolicy」という名前のデフォルトグループポリシーがあります。必要なサービスを提供するために追加のグループポリシーを作成することができます。

（注） 不整合のあるグループ ポリシー オブジェクトを RA VPN 設定に追加することはできません。グループポリシーを RA VPN 設定に追加する前に、すべての不整合を解決してください。

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。
ステップ 2 青色のプラス ボタンをクリックします。
ステップ 3 **[RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）] > [RA VPNグループポリシー（RA VPN Group Policy）]** をクリックします。
ステップ 4 グループ ポリシーの名前を入力します。名前には最大 64 文字の長さを使用でき、スペースも使用できます。
ステップ 5 [デバイスタイプ] ドロップダウンで、[ASA] を選択します。
ステップ 6 次のいずれかを実行します。

- 必要なタブをクリックし、そのページで属性を設定します。

ステップ 7 [保存（Save）] をクリックしてグループポリシーを作成します。

ASA RA VPN グループポリシー属性

このセクションでは、ASA RA VPN グループポリシーに関連付けられた属性について説明します。

一般属性

グループポリシーの全般的な属性では、グループの名前およびその他の基本設定を定義します。

- [DNSサーバー（DNS Server）]：VPN接続時にドメイン名を解決するためのDNSサーバーのIPアドレスを入力します。コンマを使用してアドレスを区切ることができます。
- **Banner**：ユーザーのログイン時に表示するバナーテキストまたはウェルカムメッセージです。デフォルトでは、バナーは表示されません。最大文字数は496文字です。AnyConnectクライアントは、部分的なHTMLをサポートしています。リモートユーザーへバナーが適切に表示されることを確認するには、
タグを使用して改行を示します。
- [デフォルトドメイン（Default Domain）]：RA VPN内のユーザーのデフォルトドメインの名前。例、example.com。このドメインは、完全修飾されていないホスト名（たとえば、serverA.example.com ではなく serverA）に追加されます。

AnyConnect クライアント プロファイル

この機能は、ソフトウェアバージョン6.7以降のバージョンを実行しているFTDでサポートされています。

Cisco AnyConnect VPNクライアントは、さまざまな組み込みモジュールによって、強化されたセキュリティを提供します。これらのモジュールは、Webセキュリティ、エンドポイントフローに対するネットワークの可視性、オフネットワークローミング保護などのサービスを提供します。各クライアントモジュールには、要件に応じたカスタム設定のグループを含むクライアントプロファイルが含まれています。

VPN ユーザーが VPN AnyConnect クライアントソフトウェアをダウンロードするときに、クライアントにダウンロードする AnyConnect VPN プロファイルオブジェクトと AnyConnect モジュールを選択できます。

1. AnyConnect VPN プロファイルオブジェクトを選択または作成します。「RA VPN AnyConnect クライアントプロファイルのアップロード（260 ページ）」を参照してください。DART および Start Before Login モジュールを除き、AnyConnect VPN プロファイルオブジェクトを選択する必要があります。

2. [AnyConnectクライアントモジュールの追加（Add Any Connect Client Module）] をクリックします。

   次の AnyConnect モジュールはオプションであり、VPN AnyConnect クライアントソフトウェアとともに各モジュールがダウンロードされるように設定できます。

   - **AMP イネーブラ**：エンドポイント向けの高度なマルウェア防御（AMP）を導入します。
   - **DART**：システムログのスナップショットおよびその他の診断情報がキャプチャされて、.zip ファイルがデスクトップに作成されるため、トラブルシューティング情報を簡単に Cisco TAC に送信できます。
   - **フィードバック**：お客様が有効にして使用している機能とモジュールに関する情報を提供します。
   - **ISE ポスチャ**：OPSWAT ライブラリを使用してポスチャチェックを実行し、エンドポイントの適合性を評価します。
   - **Network Access Manager**：有線とワイヤレスの両方のネットワークにアクセスするための 802.1X（レイヤ 2）とデバイス認証を備えています。
   - **Network Visibility**：キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析に関して、企業内管理者の実行能力を向上させます。
   - **Start Before Login**：Windows のログインダイアログボックスが表示される前に AnyConnect を開始することにより、Windows にログインする前のユーザーを VPN 接続を介して企業インフラストラクチャに強制的に接続させます。
   - **Cisco Umbrella Roaming Security**：アクティブな VPN がないときに DNS レイヤセキュリティを提供します。
   - **Web セキュリティ**：定義されているセキュリティポリシーに基づいて、Web ページの要素を分析し、許容可能なコンテンツを許可し、悪意のあるコンテンツまたは許容できないコンテンツをブロックします。

3. [クライアントモジュール（Client Module）] リストで [AnyConnect] モジュールを選択します。

4. [プロファイル（Profile）] リストで、AnyConnect クライアントプロファイルを含むプロファイルオブジェクトを選択または作成します。

5. [モジュールのダウンロードを有効化（Enable Module Download）] をオンにすると、エンドポイントでプロファイルとともにクライアントモジュールをダウンロードできます。オフの場合、エンドポイントはクライアントプロファイルだけをダウンロードできます。

セッション設定属性

グループポリシーのセッションの設定は、VPN を通じて接続できる時間と、接続を確立できる個別の接続数を制御します。

- [最大接続時間（Maximum Connection Time）]：ユーザーがログアウト、再接続せずに VPN に接続したままにできる最大時間（分）で、1 ～ 4473924 または空白で指定します。デフォルトは無制限（空白）ですが、その場合でもアイドル タイムアウトは適用されます。
- [接続時間のアラート間隔（Connection Time Alert Interval）]：最大接続時間を指定した場合、アラート間隔は、次回の自動切断についてユーザーに警告を表示する最大時間に達するまでの時間を定義します。ユーザーは、接続を終了し、再接続してタイマーを再起動することを選択できます。デフォルトは 1 分です。1 ～ 30 分を指定できます。
- [アイドルタイム（Idle Time）]：VPN 接続が自動的に閉じられる前にアイドル状態になる時間（分）で、1 ～ 35791394 で指定します。指定した時間、接続で通信アクティビティがない場合、システムは接続を停止します。デフォルトは 30 分です。
- [アイドル時間のアラート間隔（Idle Time Alert Interval）]：アイドルセッションが原因の次回の自動切断について、ユーザーに警告を表示するアイドル時間に達するまでの時間。アクティビティがあるとタイマーがリセットされます。デフォルトは 1 分です。1 ～ 30 分を指定できます。
- [ユーザーあたりの同時ログイン数（Simultaneous Login Per User）]：ユーザーに許可する同時接続の最大数。デフォルトは 3 です。1 ～ 2147483647 個の接続を指定できます。多数の同時接続を許可するとセキュリティの低下を招き、パフォーマンスに影響を及ぼす可能性があります。

アドレス割り当て属性

グループポリシーのアドレスの割り当て属性は、グループの IP アドレスプールを定義します。ここで定義されているプールで、このグループを使用するすべての接続プロファイルで定義済みのプールがオーバーライドされます。接続プロファイルで定義済みのプールを使用する場合は、これらの設定を空白のままにします。

- [IPv4アドレスプール]、[IPv6アドレスプール]：これらのオプションは、リモートエンドポイントのアドレスプールを定義します。クライアントには、VPN 接続のために使用する IP バージョンに基づき、これらのプールからアドレスが割り当てられます。サポートする IP タイプごとにサブネットを定義する IP アドレスプールを選択します。当該 IP バージョンをサポートしない場合は、リストを空のままにします。たとえば、IPv4 プールを「10.100.10.0/24」と定義できます。アドレス プールは、外部インターフェイスの IP アドレスと同じサブネット上に存在することはできません。新しい IP アドレスプールの作成を作成するには、次の手順を実行します。ローカルアドレスの割り当てに使用する最大 6 個のアドレスプールのリストを指定できます。プールの指定順序は重要です。システムで

は、プールの表示順に従いプールからアドレスが割り当てられます。**注**：同じグループポリシーで IPv4 と IPv6 両方のアドレスプールを設定できます。同じグループ ポリシーに両方のバージョンの IP アドレスが設定されている場合、IPv4 に設定されたクライアントは IPv4 アドレス、IPv6 に設定されたクライアントは IPv6 アドレスを取得し、IPv4 アドレスと IPv6 アドレス両方に設定されたクライアントは IPv4 アドレスと IPv6 アドレス両方を取得します。

- [DHCPスコープ]：接続プロファイルのアドレスプールにDHCPサーバーを設定した場合、DHCP スコープはこのグループのプールに使用するサブネットを識別します。DHCP サーバーには、そのスコープによって識別される同じプール内のアドレスも設定されている必要があります。スコープを使用すると、この特定のグループに使用するDHCPサーバーで定義されているアドレスプールのサブセットを選択できます。ネットワーク スコープを定義しない場合、DHCP サーバーはアドレス プールの設定順にプール内を探して IP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。スコープを指定するには、ネットワーク番号のホストアドレスを含むネットワークオブジェクトを入力します。たとえば、192.168.5.0/24 サブネットプールのアドレスを使用するように DHCP サーバーに指示するには、ホストアドレスとして 192.168.5.0 を指定するネットワークオブジェクトを入力します。DHCP は IPv4 アドレス指定にのみ使用することができます。

スプリット トンネリング属性

グループポリシーのスプリットトンネリング属性は、システムが内部ネットワーク用のトラフィックと外部方向トラフィックを処理する方法を定義します。スプリットトンネリングは、VPN トンネル（暗号化）と VPN トンネル外の残りのネットワークトラフィック（非暗号化、つまりクリアテキスト）を介して一部のネットワークトラフィックを誘導します。

通常、リモートアクセス VPN では、VPN ユーザーに自社のデバイスを介してインターネットにアクセスさせます。ただし、RA VPN に接続している VPN ユーザーに、外部ネットワークへのアクセスを許可することができます。この技術は、スプリットトンネリングまたはヘアピニングと呼ばれます。スプリットトンネルでは、セキュアトンネル経由のリモートネットワークへの VPN 接続が可能ですが、VPN トンネル外のネットワークにも接続できます。スプリットトンネリングは、FTDデバイスのネットワーク負荷を軽減し、外部インターフェイスの帯域幅を拡大します。

はじめる前に

IPv4ネットワーク用とIPv6ネットワーク用のスプリットトンネルポリシーを作成する場合は、指定するアクセスリストが両方のプロトコルで使用されます。したがって、アクセスリストには、IPv4 トラフィックと IPv6 トラフィックの両方のアクセス コントロール エントリ（ACE）が含まれている必要があります。

ASA デバイスが CDO に導入準備されると、CDO はデバイスに関連付けられた拡張 ACL を読み取ります。詳細については、「Group Policy」を参照してください。新しい ACL を作成する場合は、「ASA ポリシー（拡張アクセスリスト）」を参照して作成してください。

（注） 作成する ACL の送信元ネットワークとして、スプリットトンネリング用のネットワークを指定していることを確認してください。

- [IPv4スプリットトンネリング（IPv4 Split Tunneling）]、[IPv6スプリットトンネリング（IPv6 Split Tunneling）]：トラフィックが IPv4 または IPv6 アドレスを使用するかどうかに基づいて、さまざまなオプションを指定できますが、それぞれのオプションは同じです。スプリットトンネリングを有効にする場合は、ネットワークオブジェクトを選択する必要があるいずれかのオプションを指定します。
  - [トンネル経由のトラフィックをすべて許可する（Allow all traffic over tunnel）]：スプリットトンネリングを行いません。ユーザーが RA VPN 接続を行うと、そのユーザーのトラフィックはすべて保護されたトンネルを通過します。これがデフォルトです。最も安全なオプションであるとも考えられます。
  - [トンネル経由の指定されたトラフィックを許可する（Allow specified traffic over the tunnel）]：送信元ネットワークを定義する拡張アクセスリストを選択します。これらの送信元からのトラフィックはすべて、保護されたトンネルを通過します。その他すべての送信元からのトラフィックは、クライアントによって、トンネル外の接続（ローカル Wi-Fi やネットワーク接続など）にルーティングされます。
  - [以下に指定したネットワークを除外する（Exclude networks specified below）]：送信元ネットワークを定義するネットワークオブジェクトを選択します。クライアントは、指定された送信元からのトラフィックをトンネル外の接続にルーティングします。他の送信元からのトラフィックはトンネルを通過します。
  - [ネットワークリスト（Network List）]：IPv4 と IPv6 ネットワークの両方を持つことができる拡張 ACL ネットワークを選択します。
- [スプリットDNS（Split DNS）]：クライアントが、そのクライアントで設定されている DNS サーバーに他の DNS 要求を送信することを許可しながら、セキュアな接続を介して一部の DNS 要求を送信するようにシステムを設定できます。次の DNS 動作を設定できます。
  - [スプリットトンネルポリシーに従ってDNS要求を送信する（Send DNS Request as per split tunnel policy）]：このオプションを選択すると、スプリット トンネル オプションが定義されている場合と同じ方法で DNS 要求が処理されます。スプリットトンネリングを有効にすると、DNS 要求は宛先アドレスに基づいて送信されます。スプリットトンネリングを有効にしていない場合、DNS 要求はすべて保護された接続を介します。
  - [常にトンネル経由でDNS要求を送信する（Always send DNS requests over tunnel）]：スプリットトンネリングを有効にするが、すべての DNS 要求を保護された接続を介して、グループで定義された DNS サーバーに送信する場合は、このオプションを選択します。

- [指定したドメインのみをトンネル経由で送信（Send only specified domains over tunnel）]：保護された DNS サーバーが特定のドメインのアドレスだけを解決するようにする場合は、このオプションを選択します。次に、ドメインを指定します。ドメイン名はコンマで区切ります。例：example.com, example1.com。内部 DNS サーバーが内部ドメインの名前を解決し、外部 DNS サーバーが他のすべてのインターネットトラフィックを処理するようにする場合は、このオプションを使用します。

AnyConnect 属性

グループポリシーの AnyConnect 属性は、AnyConnect クライアントでリモートアクセス VPN 接続に使用されるいくつかの SSL および接続設定を定義します。

- **SSL 設定**
  - [Datagram Transport Layer Security（DTLS）の有効化（Enable Datagram Transport Layer Security (DTLS)）]：AnyConnect クライアントが SSL トンネルと DTLS トンネルの 2 つのトンネルを同時に使用することを許可するかどうかを指定します。DTLS によって、一部の SSL 接続に関連する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。DTLS をイネーブルにしない場合、SSL VPN 接続を確立している AnyConnect クライアント ユーザーは SSL トンネルのみで接続します。
  - [DTLS圧縮（DTLS Compression）]：LZS を使用してこのグループの Datagram Transport Layer Security（DTLS）接続を圧縮するかどうかを指定します。[DTLS圧縮（DTLS Compression）] はデフォルトで無効になっています。
  - [SSL圧縮（SSL Compression）]：データ圧縮を有効にするかどうかを指定します。有効にする場合、使用するデータ圧縮の方法は（[圧縮（Deflate）] または [LZS]）です。[SSL圧縮（SSL Compression）] はデフォルトで無効になっています。データ圧縮により、伝送速度は上がりますが、各ユーザーセッションのメモリ要件と CPU 使用率も高くなるため、SSL 圧縮はデバイスの全体的なスループットを低下させます。
  - [SSLキーの再生成方法（SSL Rekey Method）]、[SSLキーの再生成間隔（SSL Rekey Interval）]：クライアントは、暗号キーと初期化ベクトルを再ネゴシエーションしながら VPN 接続キーを再生成して、接続のセキュリティを強化します。[なし（None）] を選択して、キーの再生成を無効にします。キーの再生成を有効にするには、新しいトンネルを作成するたびに [新しいトンネル（New Tunnel）] を選択します（[既存のトンネル（Existing Tunnel）] オプションは、[新しいトンネル（New Tunnel）] と同じアクションになります）。キーの再生成を有効にする場合は、キーの再生成間隔も設定します。デフォルトは 4 分です。間隔は、4 ～ 10080 分（1 週間）の範囲で設定できます。
- **接続の設定**
  - [DF（Don't Fragment）ビットを無視する（Ignore the DF (Don't Fragment) bit）]：フラグメント化が必要なパケットの Don't Fragment（DF）ビットを無視するかどうかを指定します。DF ビットが設定されているパケットの強制フラグメンテーションを許可し、

それらのパケットがトンネルを通過できるようにするには、このオプションを選択します。

- [Client Bypass Protocol]：セキュアゲートウェイによる（IPv6 トラフィックだけを予期しているときの）IPv4 トラフィックの管理方法や、（IPv4 トラフィックだけを予期しているときの）IPv6 トラフィックの管理方法を設定できます。

  AnyConnect クライアントがヘッドエンドに VPN 接続するときに、ヘッドエンドは IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ヘッドエンドが AnyConnect 接続に IPv4 アドレスのみ、または IPv6 アドレスのみを割り当てた場合、ヘッドエンドが IP アドレスを割り当てなかったネットワークトラフィックについて、Client Bypass Protocol によってそのトラフィックをドロップさせるか（デフォルト、無効、オフ）、またはヘッドエンドをバイパスしてクライアントからの暗号化なし、つまり「クリアテキスト」としての送信を許可するか（有効、オン）を設定できます。

  たとえば、セキュア ゲートウェイが AnyConnect 接続に IPv4 アドレスだけを割り当て、エンドポイントがデュアルスタックされていると想定してください。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアント バイパス プロトコルが無効の場合は、IPv6 トラフィックがドロップされますが、クライアント バイパス プロトコルが有効の場合は、IPv6 トラフィックはクライアントからクリア テキストとして送信されます。

- [MTU]：Cisco AnyConnect VPN Client によって確立された SSL VPN 接続の最大伝送ユニット（MTU）サイズ。デフォルトは 1406 バイトで、範囲は 576 ー 1462 バイトです。

  - [AnyConnectとVPNゲートウェイ間のキープアライブメッセージ（Keepalive Messages Between AnyConnect and VPN Gateway）]：トンネルでのデータの送受信にピアを使用できることを示すために、ピア間でキープアライブメッセージを交換するかどうかを指定します。キープアライブ メッセージは、設定された間隔で送信されます。デフォルトの間隔は 20 秒、有効な範囲は 15 ～ 600 秒です。

  - [ゲートウェイ側の間隔でのDPD（DPD on Gateway Side Interval）]、[クライアント側の間隔でのDPD（DPD on Client Side Interval）]：ピアが応答しなくなったときに VPN ゲートウェイまたは VPN クライアントによる迅速な検出を確実に実行するには、Dead Peer Detection（DPD; デッドピア検出）を有効にします。ゲートウェイまたはクライアント DPD を個別に有効にすることができます。DPD メッセージのデフォルトの送信間隔は 30 秒です。間隔は、5～3600 秒にすることができます。

トラフィック フィルタ属性

グループポリシーのトラフィックフィルタ属性は、グループに割り当てられているユーザーに適用する制限を定義します。アクセス コントロール ポリシー ルールを作成する代わりにこれらの属性を使用することで、ホストまたはサブネットアドレスとプロトコル、または VLAN に基づいて、RA VPN ユーザーのアクセスを特定のリソースに制限できます。デフォルトで

は、RA VPN ユーザーは、保護されたネットワーク上の宛先へのアクセスがグループポリシーによって制限されることはありません。

- [アクセスリストフィルタ（Access List Filter）]：拡張アクセス制御リスト（ACL）を使用してアクセスを制限します。Smart CLI 拡張 ACL オブジェクトを選択します。拡張 ACL では、送信元アドレス、宛先アドレス、およびプロトコル（IP や TCP など）に基づいてフィルタリングできます。ACL はトップダウン方式で最初に一致したものから評価されるため、具体的なルールはより一般的なルールの前に配置してください。ACL の末尾には、暗黙的な「deny any」があるため、いくつかのサブネットへのアクセスを拒否しながら、他のすべてのアクセスを許可する場合は、ACL の最後に「permit any」ルールを含めてください。拡張 ACL スマート CLI オブジェクトを編集しながらネットワークオブジェクトを作成することはできないため、グループポリシーを編集する前に、ACL を作成する必要があります。そうしないと、単純にオブジェクトを作成し、後でもう一度ネットワークオブジェクトを作成し、その後で必要なすべてのアクセス制御エントリを作成する必要があります。ACL を作成するには、FDM にログインして、**[デバイス]** > **[詳細設定（Advanced Configuration）]** > **[スマートCLI（Smart CLI）]** > **[オブジェクト]** に移動し、オブジェクトを作成して、オブジェクトタイプとして [拡張アクセスリスト（Extended Access List）] を選択します。

- [VPNをVLANに制限（Restrict Access to VLAN）]：「VLAN マッピング」とも呼ばれるこの属性で、このグループポリシーが適用されるセッションの出力 VLAN インターフェイスを指定します。システムは、このグループからのトラフィックすべてを、選択した VLAN に転送します。この属性を使用して VLAN をグループ ポリシーに割り当て、アクセス コントロールを簡素化します。この属性に値を割り当てる方法は、ACL を使用してセッションのトラフィックをフィルタリングする方法の代替方法です。デバイスのサブインターフェイスで定義されている VLAN 番号を指定していることを確認します。値の範囲は 1 ～ 4094 です。

Windows ブラウザ プロキシ属性

グループポリシーの Windows ブラウザプロキシ属性は、ユーザーのブラウザで定義されたプロキシが動作しているかどうか、およびその動作方法を判断します。

[VPNセッション中のブラウザプロキシ（Browser Proxy During VPN Session）] に対して次のいずれかの値を選択できます。

- [エンドポイント設定のまま（No change in endpoint settings）]：HTTP のブラウザプロキシを設定するかどうかをユーザーが決定できます。設定されている場合、そのプロキシが使用されます。

- [ブラウザプロキシの無効化（Disable browser proxy）]：ブラウザに定義されているプロキシ（ある場合）を使用しません。どのブラウザ接続もプロキシを経由しません。

- [自動検出設定（Auto detect settings）]：クライアントデバイスのブラウザでの自動プロキシサーバー検出の使用を有効にします。

- [カスタム設定を使用（Use custom settings）]：HTTP トラフィックに対してすべてのクライアントデバイスで使用する必要があるプロキシを定義します。次を設定します。

- [プロキシサーバーのIPまたはホスト名（Proxy Server IP or Hostname）]、[ポート]：プロキシサーバーの IP アドレスまたはホスト名、およびプロキシサーバーが使用するプロキシ接続のポート。ホストとポートを組み合わせた文字数が 100 文字を超えることはできません。
- [ブラウザプロキシ免除リスト（Browser Proxy Exemption List）]：免除リストにあるホスト/ポートへの接続はプロキシを経由しません。プロキシを使用すべきでない宛先のすべてのホスト/ポート値を追加します。例：www.example.com ポート 80。[プロキシ例外の追加（Add proxy exception）] をクリックしてリストに項目を追加します。項目を削除するには、ごみ箱アイコンをクリックします。すべてのアドレスとポートを合わせたプロキシ例外リスト全体で、255 文字を超えることはできません。

ASA RA VPN 設定の作成

CDO を使用して、1 つ以上の適応型セキュリティアプライアンス（ASA）デバイスを RA VPN 設定ウィザードに追加し、デバイスに関連付けられた VPN インターフェイス、アクセス制御、および NAT 免除設定ができます。したがって、各 RA VPN 設定には、RA VPN 設定に関連付けられた複数の ASA デバイス間で共有される接続プロファイルとグループポリシーを含めることができます。さらに、接続プロファイルとグループポリシーを作成して、設定を拡張できます。

RA VPN 設定がすでになされている ASA デバイス、または RA VPN 設定のない新しいデバイスを導入準備できます。「ASA デバイスの導入準備（111 ページ）」を参照してください。RA VPN 設定がすでにある ASA デバイスを導入準備すると、CDO は自動的に「デフォルトの RA VPN 設定」を作成し、ASA デバイスをこの設定に関連付けます。このデフォルト設定には、デバイスで定義されているすべての接続プロファイルオブジェクトを含めることができます。詳細については、「オンボーディング済み ASA デバイスの RA VPN 設定の読み取り」を参照してください。CDO では、デフォルトの設定を削除できます。

重要

- 同じリモートアクセス VPN 設定に ASA と FTD を追加することは許可されていません。
- ASA デバイスは、1 つ以上の RA VPN 設定を持つことはできません。

始める前に

ASA デバイスを RA VPN 設定に追加する前に、ASA デバイスで次の前提条件が満たされている必要があります。

- ライセンス要件

  輸出規制されている機能に対して、デバイスを有効にする必要があります。

  ASA デバイスのライセンスの概要を表示するには、ASA コマンドライン インターフェイスで show license summary コマンドを実行します。CDO ASA CLI インターフェイスを使用するには、「CDO コマンドライン インターフェイスを使用する」を参照してください。

  - ライセンスの概要で有効になっている輸出規制機能の例：

```
Registration: Status: REGISTERED Smart Account: Cisco SVS temp-request access
licensing@cisco.com Export-Controlled Functionality: ALLOWED

Last Renewal Attempt: None

Next Renewal Attempt: Jun 08 2021 09:46:22 UTC
```

VPN 設定を作成または編集するには、[エクスポート制御機能（Export-Controlled Functionality）] プロパティを [許可（Allowed）] ステータスにする必要があります。

このプロパティが [許可しない（Not Allowed）] ステータスの場合、VPN 設定を作成または変更する際に CDO がエラーメッセージ（「エクスポートに準拠していないデバイスには RA VPN を設定できません」）を表示し、デバイスの RA VPN 設定を許可しません。

- デバイスのID 証明書

  証明書は、クライアントと ASA デバイス間の接続を認証するために必要です。VPN 設定を開始する前に、ID 証明書が ASA デバイスにすでにあることを確認してください。

  証明書がデバイスにあるかどうかを確認するには、ASA コマンド ライン インターフェイスで **show crypto CA Certificates** コマンドを実行します。CDO ASA CLI インターフェイスを使用するには、「CDO コマンド ライン インターフェイスを使用する」を参照してください。

  ID 証明書がない場合、または新しい証明書に登録する場合は、CDO を使用してそれらを ASA にインストールします。ASA 証明書管理を参照してください。

  リモートアクセス VPN コンテキストでのデジタル証明書の使用については、リモートアクセス VPN 認証ベースの認証 （256 ページ）で説明されています。

- 外部インターフェイス

  外部インターフェイスが、ASA デバイスですでに設定されている必要があります。**インターフェイスを設定するには、ASDM または ASA CLI を使用する必要があります。**ASDM を使用したインターフェイスの設定については、『Cisco ASA Series General Operations CLI Configuration Guide, XY』の「Interfaces」ブックを参照してください。

- AnyConnect パッケージをダウンロードして、リモートサーバーにアップロードします。その後、RA VPN ウィザードまたは ASA ファイル管理ウィザードを使用して、AnyConnect ソフトウェアパッケージをサーバーから ASA にアップロードします。手順については、「ASA デバイス上の AnyConnect ソフトウェアパッケージの管理」を参照してください。

- 保留中の設定展開はありません。

- 認証にローカルデータベースを使用している場合、ASDM または ASA CLI を使用して、ローカルデータベースにユーザーアカウントを追加します。

  ASDM を使用してユーザーアカウントを追加するには、『Cisco ASA Series VPN CLI Configuration Guide, X.Y』の「AAA Servers and the Local Database」ブックの「Add a User Account to the Local Database」セクションを参照してください。

  ASA CLI を使用してユーザーアカウントを追加するには、**username[***username***] password [***password***] privilege [***priv_level***]** コマンドを実行します。

- ASA の変更は CDO に同期されます。
  1. 左側の CDO 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、同期する 1 つ以上の ASA デバイスを検索します。
  2. 1 つ以上のデバイスを選択し、[変更の確認（Check for changes）] をクリックします。CDO は 1 つ以上の FTD デバイスと通信して、変更を同期します。
- RA VPN 設定グループポリシーのオブジェクトは一貫しています。
  - 一貫性のないすべてのグループポリシーのオブジェクトは RA VPN 設定に追加できないため、それらが解決されていることを確認します。問題に対処するか、一貫性のないグループポリシーのオブジェクトを [オブジェクト] ページから削除します。詳細については、「重複オブジェクトの問題の解決」および「不整合オブジェクトの問題を解決する」を参照してください。

ステップ 1 ASA デバイスの導入準備 （111 ページ）。

ステップ 2 左側の CDO ナビゲーションバーで、 **[VPN]** > **[リモートアクセスVPNの設定（Remote Access VPN Configuration）]**をクリックします。

ステップ 3 青いプラス  ボタンをクリックして、新しい RA VPN 設定を作成します。

ステップ 4 リモートアクセス VPN の設定の名前を入力します。

ステップ 5 青いプラス  ボタンをクリックして、ASA デバイスを設定に追加します。

デバイスの詳細を追加し、デバイスに関連付けられたネットワークトラフィック関連の権限を設定できます。

1. 次のデバイスの詳細を提供します。
   - [デバイス]：追加する ASA デバイスを選択し、[選択（Select）] をクリックします。**重要**：同じリモートアクセス VPN 設定に ASA と FTD を追加することはできません。
   - [デバイス ID 証明書（Certificate of Device Identity）]：デバイスのアイデンティティを確立するために使用する内部証明書を選択します。内部証明書は、AnyConnect クライアントがデバイスへの接続を行うときにデバイスのアイデンティティを確立します。クライアントはこの証明書を承認して、セキュアな VPN 接続を完了させる必要があります。
   - [外部インターフェイス（Outside Interface）]：リモートアクセス VPN 接続を確立するときにユーザーが接続するインターフェイスを選択します。これは通常外部（インターネットに接続された）インターフェイスですが、デバイスとこの接続プロファイルがサポートしているエンドユーザー間のインターフェイスのいずれかを選択します。

     注目 エクスポートに準拠していないデバイスの RA VPN 設定を作成または変更することはできません。輸出規制機能が有効になっている ASA デバイスのライセンスを取得して、再試行する必要があります。

2. [続行] をクリックして、トラフィックの権限を設定します。

   - [暗号解読されたトラフィック（sysopt permit-vpn）に対するバイパスアクセス コントロール ポリシー（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）]：デフォルトでは、暗号解読されたトラフィックは、アクセス コントロール ポリシーのインスペクションの対象になります。このオプション[複合されたトラフィックのバイパス（bypasses the decrypted traffic）]オプションを有効にすると、アクセス コントロール ポリシーのインスペクションがバイパスされますが、AAA サーバーからダウンロードされた VPN フィルタ ACL と認証 ACL は、VPN トラフィックに引き続き適用されます。

     このオプションを選択すると、システムによりグローバル設定である sysopt connection permit-vpn コマンドが設定されることに注意してください。これは、サイト間 VPN 接続の動作にも影響を及ぼします。

     このオプションを選択しない場合、外部ユーザーがリモートアクセス VPN アドレスプール内の IP アドレスをスプーフィングし、ネットワークにアクセスするおそれがあります。この理由は、アドレスプールに内部リソースへのアクセスを許可するアクセス制御ルールを作成する必要があるためです。アクセス制御ルールを使用する場合は、送信元 IP アドレスだけではなく、ユーザーの仕様を使用してアクセスを制御することを検討してください。

     このオプションを選択することの欠点は、VPN トラフィックが検査されないことです。つまり、侵入およびファイル保護、URL フィルタリング、またはその他の高度な機能がトラフィックに適用されません。つまり、このトラフィックに対する接続イベントは生成されず、VPN 接続は統計ダッシュボードには反映されません。

   - [NAT免除（NAT Exempt）]：NAT 免除を使用すると、アドレスは変換から除外され、変換済みのホストとリモートホストの両方が保護されたホストとの接続を開始できるようになります。リモートアクセス VPN エンドポイントとの入出力トラフィックに対する NAT 変換を免除するには、NAT 免除を設定します。NAT からの ASA リモート アクセス トラフィックの除外 （257 ページ）を参照してください。

3. [OK] をクリックします。

   [検出されたAnyConnectパッケージ（AnyConnect Packages Detected）]には、デバイスですでに使用可能な AnyConnect パッケージが表示されます。

   RA VPN ウィザードから AnyConnect パッケージを ASA にアップロードするには、次の 2 つのオプションがあります。

   - （オプション 1）：CDO のリポジトリからパッケージを選択します。ASA はインターネットにアクセスできる必要があります。
   - （オプション 2）：AnyConnect パッケージがプリロードされている ftp/http/https/scp/smb/tftp URL の場所を指定します。

   手順については、「ASA デバイス上の AnyConnect ソフトウェアパッケージの管理」を参照してください。

   （注） 注:既存のパッケージを置き換える場合は、「ASA デバイス上の AnyConnect ソフトウェアパッケージの管理」を参照してください。

ステップ 6 [OK] をクリックします。

ASA VPN 設定が作成されます。

ASA RA VPN 構成の変更

既存の RA VPN 構成の名前とデバイスの詳細を変更できます。

ステップ 1 変更する構成を選択し、[アクション] の下で [編集] をクリックします。

- 必要に応じて名前を変更します。
- 青色のプラス  ボタンをクリックして、新しいデバイスを追加します。
- をクリックして、ASA デバイスで次の手順を実行します。
  - [編集] をクリックして、既存の RA VPN 構成を変更します。
  - [削除] をクリックして、RA VPN 構成から ASA デバイスを削除します。グループポリシーを除き、そのデバイスに関連付けられているすべての接続プロファイルと RA VPN 設定が削除されます。グループポリシーは、オブジェクトページから明示的に削除できます。

    （注） 構成を使用しているデバイスがその ASA だけの場合は、ASA を削除できません。代わりに、RA VPN 構成を削除できます。

ステップ 2 CDO から ASA に設定変更を展開します。

次のタスク

構成またはデバイスの名前を入力して、リモートアクセス VPN 構成を検索することもできます。

関連情報：

- ASA RA VPN 接続プロファイルの設定 （239 ページ）。

ASA RA VPN 接続プロファイルの設定

リモートアクセスVPN接続プロファイルの定義する接続特性では、外部ユーザーがAnyConnectクライアントを使用してシステムにVPN接続することを許可します。各プロファイルは、ユーザーの認証に使用される AAA サーバーと証明書、ユーザーの IP アドレスを割り当てるためのアドレスプール、およびさまざまなユーザー関連の属性を定義するグループポリシーを定義します。

異なるユーザーグループに異なるサービスを提供する必要がある場合、または異なる認証ソースがある場合は、RA VPN 設定内に複数のプロファイルを作成できます。たとえば、自分の組

織が異なる認証サーバーを使用する別の組織とマージする場合、別の組織の認証サーバーを使用する新しいグループのプロファイルを作成できます。

RA VPN 接続プロファイルを作成すると、ユーザーは、ホームネットワークなどの外部ネットワークから内部ネットワークに接続できるようになります。異なる認証方式に対応するために、個別のプロファイルを作成します。

始める前に

ASA RA VPN 設定の作成 （235 ページ）。

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN]** > **[リモートアクセスVPNの設定（Remote Access VPN Configuration）]** をクリックします。VPN 設定をクリックして、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報を表示できます。

（注） デバイスに割り当てられているグループポリシーを確認するには、[アクション] で [グループポリシー（Group Policies）] をクリックします。接続プロファイルに割り当てられたグループポリシーは、リストに自動的に追加され、削除できません。

必要なグループポリシーがまだ存在しない場合は、  をクリックしてリストから選択します。必要なサービスを提供するために追加のグループポリシーを作成することができます。「新規 ASA RA VPN グループポリシーの作成 （226 ページ）」を参照してください。

ステップ 2 接続プロファイルをクリックし、右側のサイドバーの [アクション] で [接続プロファイルの追加（Add Connection Profile）] をクリックします。

ステップ 3 基本接続の属性を設定します。

- [接続プロファイル名（Connection Profile Name）]：スペースを含めずに最大 50 文字で、この接続の名前を指定します。例、MainOffice。

  （注） ここで入力する名前が、AnyConnect クライアントの接続リストに表示されます。ユーザーにとって意味のある名前を選択します。

- [グループエイリアス（Group Alias）]、[グループURL（Group URL）]：エイリアスには特定の接続プロファイルの代替名または URL が含まれます。VPN ユーザーは、 ASA デバイスへの接続時に、接続リストの AnyConnect クライアントでエイリアス名を選択できます。接続プロファイル名はグループのエイリアスとして自動的に追加されます。グループ URL のリストも設定できます。このリストは、リモートアクセス VPN 接続を開始するときにエンドポイントが選択できるリストです。ユーザーがグループ URL を使用して接続すると、システムはその URL に一致する接続プロファイルを自動的に使用します。この URL は、AnyConnect クライアントをまだインストールしていないクライアントによって使用されます。グループエイリアスと URL を必要な数だけ追加します。これらのエイリアスと URL は、デバイスで定義されているすべての接続プロファイルで一意である必要があります。グループ URL は https:// で始まる必要があります。

- たとえば、エイリアスは Contractor、グループ URL は https://ravpn.example.com/contractor のように指定できます。AnyConnect クライアントをインストールすると、ユーザーは単純に AnyConnect VPN の接続ドロップダウンリストでグループエイリアスを選択します。

ステップ 4 プライマリ アイデンティティ ソース、および必要に応じてセカンダリ ソースを設定します。これらのオプションにより、リモートアクセス VPN 接続を有効にするための、デバイスへのユーザー認証方法が決定されます。最も簡単なアプローチは、AAA のみを使用し、AD レルムを選択するか、または LocalIdentitySource を使用する方法です。[認証タイプ] として次のアプローチを使用できます。

- [AAAのみ（AAA Only）]：ユーザー名とパスワードに基づいてユーザーを認証および認可します。詳細は、接続プロファイルのための AAA の設定 （241 ページ）を参照してください。
- [クライアント証明書のみ]：クライアント デバイス ID 証明書に基づいてユーザーを認証します。詳細については、「接続プロファイルの証明書認証の設定」を参照してください。
- [AAAおよびクライアント認証（AAA and Client Certificate）]：ユーザー名/パスワードと、クライアント デバイス ID 証明書の両方を使用します。

ステップ 5 クライアントのアドレスプールを設定します。アドレスプールは、リモートクライアントが VPN 接続を確立するときに、システムがリモートクライアントに割り当てることができる IP アドレスを定義します。詳細については、「クライアントアドレスプール割り当ての設定」を参照してください。

ステップ 6 [続行（Continue）] をクリックします。

ステップ 7 リストからこのプロファイルに対して使用する [グループポリシー（Group Policy）] を選択し、[選択（Select）] をクリックします。

グループポリシーは、トンネル確立後のユーザー接続の期間を設定します。システムには、「DfltGrpPolicy」という名前のデフォルトグループポリシーがあります。必要なサービスを提供するために追加のグループポリシーを作成することができます。「新規 ASA RA VPN グループポリシーの作成（226 ページ）」を参照してください。

ステップ 8 [続行（Continue）] をクリックします。

ステップ 9 サマリーを確認します。最初に、サマリーが正しいことを確認します。AnyConnect ソフトウェアをインストールし、VPN 接続を完了できることをテストするために、エンドユーザーが最初に行う必要がある内容を確認できます。 をクリックしてこれらの手順をクリップボードにコピーし、ユーザーに配布します。

ステップ 10 [完了（Done）] をクリックします。

ステップ 11 「ASA のエンドツーエンド リモート アクセス VPN 設定プロセス」のステップ 5 を実行します。

接続プロファイルのための AAA の設定

認証、許可、およびアカウンティング（AAA） サーバーは、ユーザー名とパスワードを使用して、ユーザーのリモートアクセス VPN へのアクセスを許可するかどうかを判断します。RADIUS サーバーを使用する場合は、認証されたユーザー間で許可レベルを区別して、保護されたリソースへの差別化されたアクセスを提供できます。使用状況を追跡するために RADIUS アカウンティングサービスを使用することもできます。

AAA を設定する場合は、プライマリ アイデンティティ ソースを設定する必要があります。セカンダリ ソースとフォールバック ソースはオプションです。RSA トークンや DUO などを使用する二重認証を実装する場合は、セカンダリ ソースを使用します。

プライマリ アイデンティティ ソースのオプション

- [ユーザー認証用のプライマリアイデンティティソース]：認証はユーザーを特定する方法です。アクセスが許可されるには、ユーザーは通常、有効なユーザー名と有効なパスワードを入力する必要があります。プライマリ アイデンティティ ソースはリモートユーザーを認証する目的で使用されます。VPN接続を完了するには、エンドユーザーがこのソースか任意のフォールバックソースで定義されている必要があります。次のいずれかを選択します。
  - Active Directory（AD）のアイデンティ レルム。
  - RADIUS サーバーグループ。
  - LocalIdentitySource（ローカル ユーザー データベース）：デバイスで直接ユーザーを定義できます。外部サーバーを使用することはできません。

    ASA のアイデンティティソースを設定するをクリックすると、新しいアイデンティティソースを作成できます。

- [フォールバックローカルアイデンティティソース]：プライマリソースが外部サーバーの場合、プライマリサーバーが使用できない場合のフォールバックとしてLocalIdentitySourceを選択できます。フォールバック ソースとしてローカルデータベースを使用する場合は、必ず外部サーバで定義したものと同じローカル ユーザ名/パスワードを定義します。
- [削除オプション]：レルムとは管理ドメインのことです。次のオプションを有効にすると、ユーザー名だけに基づいて認証できます。これらのオプションを任意に組み合わせて有効にできます。ただし、サーバーが区切り文字を解析できない場合は、両方のチェックボックスをオンにする必要があります。
  - [ユーザー名からアイデンティティソースサーバーを削除]：ユーザー名を AAA サーバーに渡す前に、ユーザー名からアイデンティティソース名を削除するかどうか。たとえば、このオプションを選択してユーザーが「username」として domain\username に入ると、ユーザー名からドメインが削除され、認証用の AAA サーバーに送信されます。デフォルトでは、このオプションはオフになります。
  - [ユーザー名からグループを削除]：ユーザー名をAAAサーバーに渡す前に、ユーザー名からグループを削除するかどうか。このオプションは、username@domain形式で指定された名前に適用されます。選択すると、domainと@記号が削除されます。デフォルトでは、このオプションはオフになります。

セカンダリ アイデンティティ ソース

- [ユーザー承認用のセカンダリアイデンティティソース]：オプションの 2 番目のアイデンティティソースです。ユーザーがプライマリソースで正常に認証されると、セカンダリソースでの認証が求められます。AD レルム、RADIUS サーバーグループ、またはローカル アイデンティティ ソースを選択することができます。
- [詳細オプション]：[詳細] リンクをクリックし、次のオプションを設定します。

- [セカンダリ用フォールバックローカルアイデンティティソース（Fallback Local Identity Source for Secondary）]：セカンダリソースが外部サーバーの場合、セカンダリサーバーが使用できない場合のフォールバックとしてLocalIdentitySourceを選択できます。フォールバックソースとしてローカルデータベースを使用する場合は、必ずセカンダリ外部サーバーで定義したものと同じローカルユーザー名/パスワードを定義します。
- [セカンダリログインにプライマリユーザー名を使用]：デフォルトでは、セカンダリアイデンティティ ソースを使用する場合、セカンダリ ソースに対してユーザー名とパスワードの両方が求められます。このオプションを選択すると、システムはセカンダリパスワードの入力のみを求め、プライマリ アイデンティティ ソースに対して認証されたものと同じユーザー名をセカンダリソースに対して使用します。プライマリとセカンダリの両方のアイデンティティソースで同じユーザー名を設定する場合は、このオプションを選択します。
  - [セッションサーバーのユーザー名]：認証に成功すると、ユーザー名はイベントと統計ダッシュボードに表示されます。ユーザー名はユーザーベースまたはグループベースのSSL暗号解読化およびアクセス制御ルールに一致するものを判断するために使用され、アカウンティングに使用されます。2つの認証ソースを使用しているため、ユーザーアイデンティティとして、プライマリまたはセカンダリのどちらのユーザー名を使用するのかシステムに通知する必要があります。デフォルトでは、プライマリ名が使用されます。
  - [パスワードタイプ]：セカンダリサーバーのパスワードを取得する方法。デフォルトは[プロンプト（Prompt）]で、ユーザーはパスワードの入力が求められることを意味します。プライマリサーバーへのユーザー認証時に入力したパスワードを自動的に使用するには、[プライマリアイデンティティソースのパスワード（Primary Identity Source Password）]を選択します。すべてのユーザーに同じパスワードを使用するには[共通パスワード]を選択し、[共通パスワード]フィールドにそのパスワードを入力します。
- [承認サーバー]：リモートアクセスVPNユーザーを認証するように設定されたRADIUSサーバーグループです。認証の完了後、認可によって、認証済みの各ユーザーが使用できるサービスおよびコマンドが制御されます。認可は、ユーザーが実行を認可されていることを示す属性のセット、実際の機能、および制限事項をアセンブルすることによって機能します。認可を使用しない場合は、認証が単独で、認証済みのすべてのユーザーに対して同じアクセス権を提供します。

  システムがグループポリシーで定義されているものと重複する認可属性をRADIUSサーバーから取得した場合、RADIUS属性は、グループポリシー属性をオーバーライドすることに注意してください。

  [RADIUSサーバーグループの作成（Create RADIUS Server Group）]をクリックして、新しいサーバーグループを作成できます。ASA RADIUS サーバーオブジェクトまたはグループの作成または編集 （224 ページ）
- [アカウンティングサーバー]：（オプション）リモートアクセスVPNセッションへのアカウンティングに使用するRADIUSサーバーグループ。アカウンティングは、ユーザーがアクセスしているサービスや、ユーザーが消費しているネットワークリソース

の数を追跡します。ASA デバイスは、RADIUS サーバーにユーザーアクティビティを報告します。アカウンティング情報には、セッションの開始時刻と停止時刻、ユーザー名、セッションごとのデバイスを通過したバイト数、使用されたサービス、および各セッションの時間が含まれています。これらのデータは、ネットワーク管理、クライアントへの課金、または監査のために後で分析できます。アカウンティングは、単独で使用するか、認証および認可とともに使用することができます。

[RADIUSサーバーグループの作成（Create RADIUS Server Group）] をクリックして、新しいサーバーグループを作成できます。ASA RADIUS サーバーオブジェクトまたはグループの作成または編集 （224 ページ）

接続プロファイルのための証明書認証の設定

（注） このセクションは、**認証タイプ**が **AAA のみ**の場合には適用されません。

リモート アクセス VPN 接続を認証するために、クライアント デバイスにインストールされた証明書を使用することができます。

クライアント証明書を使用していても、セカンダリ アイデンティティ ソース、フォールバック ソース、および認証およびアカウンティングサーバーを引き続き設定できます。これらは AAA オプションです。詳細については ASA RA VPN 接続プロファイルの設定 （239 ページ）を参照してください。

次に、証明書固有の属性を示します。これらの属性は、プライマリ アイデンティティ ソースとセカンダリ アイデンティティ ソースに対して個別に設定できます。セカンダリ ソースの設定はオプションです。

- [証明書のユーザー名]：次のいずれかを選択します。
  - [マップ固有フィールド]：証明書の要素を [プライマリフィールド] および [セカンダリフィールド] の順番で使用します。デフォルトは CN（共通名）と OU（組織単位）です。組織に適したオプションを選択します。これらのフィールドを組み合わせてユーザー名が提供され、このユーザー名がイベント、ダッシュボード、さらに SSL 暗号解読とアクセス制御ルールでのマッチング目的に使用されます。
  - [DN（識別名）全体をユーザー名として使用]：システムが自動的に DN フィールドからユーザー名を導出します。
- [詳細オプション]：（[認証タイプ] が [クライアント証明書のみ] の場合には適用されません）：[詳細] リンクをクリックし、次のオプションを設定します。
  - [ユーザーログインウィンドウの証明書からユーザー名を事前入力]：ユーザーに認証を要求するときに、取得したユーザー名をユーザー名フィールドに入力するかどうか。

- [ログインウィンドウでユーザー名を非表示にする]：[事前入力] オプションを選択すると、ユーザー名を非表示にできます。これは、ユーザーがパスワードプロンプトでユーザー名を編集できないことを意味します。

クライアントアドレスプール割り当ての設定

リモートアクセス VPN に接続するエンドポイントにシステムが IP アドレスを提供するための方法が必要です。AAA サーバーは、これらのアドレス、DHCP サーバー、グループポリシーで設定されている IP アドレスプール、または接続プロファイルで設定された IP アドレスプールを提供できます。システムは、この順序でこれらのリソースを試行し、使用可能なアドレスを取得すると停止し、次にアドレスをクライアントに割り当てます。このように、同時接続数が異常な場合のフェールセーフを作成するために複数のオプションを設定できます。

接続プロファイルのアドレスプールを設定するには、次の方法の 1 つ以上を使用します。

- [IPv4アドレスプール] および [IPv4アドレスプール]：まず、サブネットを指定する最大 6 つのネットワークオブジェクトを作成します。IPv4 と IPv6 に別々のプールを設定できます。次に、グループポリシーまたは接続プロファイルの [IPv4アドレスプール] および [IPv6アドレスプール] オプションで、これらのオブジェクトを選択します。IPv4 と IPv6 の両方を設定する必要はありません。サポートするアドレス方式を設定してください。また、グループポリシーと接続プロファイルの両方でプールを設定する必要もありません。グループポリシーは接続プロファイル設定をオーバーライドします。そのため、グループポリシーでプールを設定する場合は、接続プロファイルのオプションを空白のままにしてください。プールはリストの順序で使用されることに注意してください。新しい IPv4 または IPV6 アドレスプールを作成するには、「IP アドレスプールの作成」を参照してください。
- [DHCPサーバー]：まず、1 つ以上の IPv4 アドレス範囲を持つ RA VPN の DHCP サーバーを設定します（DHCP を使用して IPv6 プールを設定することはできません）。次に、DHCP サーバーの IP アドレスを使用してホスト ネットワーク オブジェクトを作成します。その後、このオブジェクトは接続プロファイルの [DHCPサーバー（DHCP Servers）] 属性で選択できます。複数の DHCP サーバーを設定することができます。DHCP サーバーに複数のアドレスプールがある場合、[DHCPスコープ] 属性を接続プロファイルにアタッチする新規 ASA RA VPN グループポリシーの作成で使用して、使用するプールを選択することができます。プールのネットワークアドレスを使用して、ホスト ネットワーク オブジェクトを作成します。たとえば、DHCP プールに 192.168.15.0/24 および 192.168.16.0/24 が含まれている場合、DHCP スコープを 192.168.16.0 に設定すると、192.168.16.0/24 サブネットからのアドレスが必ず選択されるようになります。

関連情報：

ASA のエンドツーエンド リモート アクセス VPN 設定プロセス

ASA デバイス上の *AnyConnect* ソフトウェアパッケージの管理

次のいずれかの手順を実行して、リモートアクセス VPN ウィザードを使用して AnyConnect パッケージをアップロードできます。

- CDO リポジトリからパッケージをアップロードします。

- HTTP、HTTPS、TFTP、FTP、SMB、または SCP プロトコルを使用して、サーバーからパッケージをアップロードします。

CDO リポジトリから AnyConnect パッケージをアップロードする

リモートアクセス VPN 設定ウィザードには、CDO リポジトリからオペレーティングシステムごとに AnyConnect パッケージが表示されるため、選択してデバイスにアップロードできます。デバイスがインターネットにアクセスでき、DNS が適切に設定されていることを確認してください。

（注） 目的のパッケージが表示されたリストにない場合、またはデバイスがインターネットにアクセスできない場合は、AnyConnect パッケージがプリロードされているサーバーを使用してパッケージをアップロードできます。

ステップ 1 オペレーティングシステムに対応するフィールドをクリックし、AnyConnect パッケージを選択します。

ステップ 2 をクリックして、パッケージをアップロードします。チェックサムが一致しない場合、AnyConnect パッケージのアップロードは失敗します。失敗の詳細については、デバイスの [ワークフロー（workflow）] タブで確認できます。

サーバーから ASA への AnyConnect パッケージのアップロード

AnyConnect クライアント ソフトウェア パッケージをコンピュータにダウンロードし、ASA からアクセス可能なリモートサーバーにそれをアップロードします。その後、RA VPN ウィザードまたは ASA ファイル管理ウィザードを使用して、そのサーバーから ASA に AnyConnect ソフトウェアパッケージをアップロードします。ドメイン名を使用する URL 用に、デバイスで DNS を正しく設定する必要があります。

ASA RA VPN ウィザードは、HTTP、HTTPS、TFTP、FTP、SMB、SCP プロトコルを使用したパッケージのアップロードをサポートしています。

ファイルのアップロード時にサポートされているプロトコルの構文:

プロトコル（Protocol）	構文	例
HTTP	http://[[パス/]ファイル名]	http://www.geonames.org/data-sources.html
HTTPS	https://[[パス/]ファイル名]	https://docs.aws.amazon.com/amazon/tagging.html
TFTP	tftp://[[パス/]ファイル名]	tftp://10.10.16.6/ftd/components.html
FTP	ftp://[[ユーザー[:パスワード]@]サーバー[:ポート]/[パス/]ファイル名]	[illegible]
SMB	smb://[[パス/]ファイル名]	smb://10.10.32.145//sambashare/hello.txt

プロトコル（Protocol）	構文	例
SCP	scp://[[ユーザー[:パスワード]@]サーバー[/パス]/ファイル名]	scp://rootcisco123@10.10.10.166//root/events_send.py

始める前に

必要なオペレーティングシステム用の「AnyConnect ヘッドエンド展開パッケージ」をダウンロードしていることを確認してください。最新の機能、バグ修正、セキュリティパッチを確保するには、常に最新の AnyConnect バージョンをダウンロードする必要があります。デバイスのパッケージは定期的に更新してください。

重要 ASA ファイル管理ウィザードを使用してパッケージをアップロードすることを選択した場合、パッケージのダウンロード後に名前を変更しないでください。

（注） オペレーティングシステム（OS）（Windows、Mac、Linux）ごとに 1 つの AnyConnect をアップロードできます。1 つの OS タイプに対して複数のバージョンをアップロードすることはできません。

ステップ 1 https://software.cisco.com/download/home/283000185 から AnyConnect パッケージをダウンロードします。

- EULA に同意し、K9（暗号化されたイメージ）の権限を持っていることを確認してください。
- オペレーティングシステムの「AnyConnect ヘッドエンド展開パッケージ」を選択します。パッケージ名は「anyconnect-win-4.7.04056-webdeploy-k9.pkg」のようになります。Windows、macOS、Linux のそれぞれに個別のヘッドエンドパッケージがあります。

ステップ 2 AnyConnect パッケージをリモートサーバーにアップロードします。ASA デバイスとサーバーからのネットワークルートがあることを確認します。

ASA RA VPN ウィザードは、HTTP、HTTPS、TFTP、FTP、SMB、SCP プロトコルを使用したパッケージのアップロードをサポートしています。

重要 AnyConnect パッケージを HTTPS サーバーにアップロードする場合は、以下の手順を実行してください。

- そのサーバーの信頼できる CA 証明書を ASA デバイスにアップロードします。
- 信頼できる CA 証明書を HTTPS サーバーにインストールします。

ステップ 3 リモートサーバーの URL は、認証を求めない直接リンクである必要があります。URL が事前認証されている場合は、RA VPN ウィザードの URL を指定してファイルをダウンロードできます。

ステップ 4 リモートサーバーの IP アドレスが NAT 処理されている場合は、リモートサーバーのロケーションの NAT 処理済みパブリック IP アドレスを指定する必要があります。

AnyConnect パッケージの ASA へのアップロード

RA VPN ウィザードまたは ASA ファイル管理ウィザードを使用して、AnyConnect ソフトウェアパッケージを ASA にアップロードできます。

HTTP または HTTPS サーバーから ASA デバイスに新しい AnyConnect パッケージをアップロードするには、次の手順を使用します。

ステップ 1 [検出されたAnyConnectパッケージ（AnyConnect Packages Detected）] で、Windows、Mac、Linux のエンドポイントに対して別々のパッケージをアップロードできます。

ステップ 2 対応するプラットフォームフィールドで、Windows、Mac、および Linux と互換性のある AnyConnect パッケージが事前にアップロードされているサーバーのパスを指定します。サーバーパスの例：
'http://<ip_address>:port_number/<folder_name>/anyconnect-win-4.8.01090-webdeploy-k9.pkg',
'https://<ip_address>:port_number/<folder_name>/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'

ステップ 3 をクリックして、パッケージをアップロードします。CDO は、パスが到達可能であり、指定されたファイル名が有効なパッケージかどうかを検証します。検証が成功すると、AnyConnect パッケージの名前が表示されます。RA VPN 設定に ASA デバイスを追加して、AnyConnect パッケージをそれらにアップロードできます。

ステップ 4 [OK] をクリックします。AnyConnect パッケージが RA VPN 設定に追加されます。

ステップ 5 ステップ 5 から、「ASA RA VPN 設定の作成」に進みます。

次のタスク

VPN 接続を完了するには、ユーザーは AnyConnect クライアントソフトウェアをワークステーションにインストールする必要があります。詳細については、「ユーザーが AnyConnect クライアントソフトウェアを ASA にインストールする方法」を参照してください。

ファイル管理ウィザードを使用した AnyConnect パッケージのアップロード

ファイル管理ウィザードを使用して、HTTP、HTTPS、TFTP、FTP、SMB、または SCP サーバーから単一または複数の ASA デバイスに AnyConnect パッケージをアップロードします。AnyConnect パッケージを複数の ASA デバイスに同時にプッシュする場合は、一括アップロードが便利です。詳細については、「ASA ファイルの管理」を参照してください。

重要 ASA ファイル管理ウィザードを使用してパッケージをアップロードすることを選択した場合、パッケージのダウンロード後に名前を変更しないでください。

アップロードが完了したら、ASA RA VPN 設定ウィザードを開き、パッケージが自動検出されることを確認します。1 つの OS バージョンに対して複数のパッケージをアップロードする場

合、ウィザードではそれらのパッケージがドロップダウンリストに表示され、そのリストの中から 1 つを選択できます。次に、RA VPN 設定を作成してデバイスに展開できます。

既存の AnyConnect パッケージの置換

AnyConnect パッケージがデバイスにすでに存在している場合、これらは RA VPN ウィザードに表示されます。オペレーティングシステムで利用可能なすべての AnyConnect パッケージが、ドロップダウンリストに表示されます。既存のパッケージをリストから選択して、新しいパッケージと置き換えることができます。ただし、新しいパッケージをリストに追加することはできません。

（注） 既存のパッケージを新しいパッケージに置き換える場合は、新しい AnyConnect パッケージが、ASA が到達できるネットワーク上のサーバーにすでにアップロードされていることを確認してください。

ステップ 1 左側の CDO ナビゲーションバーで、**[VPN]** > **[リモートアクセスVPN（Remote Access VPN）]**をクリックします。

ステップ 2 変更する RA VPN 設定を選択し、[アクション] で [編集] をクリックします。

ステップ 3 [検出された AnyConnect パッケージ（AnyConnect Packages Detected）] で、既存の AnyConnect パッケージの横に表示される アイコンをクリックします。オペレーティングシステムに複数のバージョンの AnyConnect パッケージがある場合は、置き換えるパッケージをリストから選択して [編集] をクリックします。既存のパッケージが対応するフィールドから消去されます。

ステップ 4 新しい AnyConnect パッケージがプリロードされているサーバーのパスを指定し、 をクリックしてパッケージをアップロードします。

ステップ 5 [OK] をクリックします。新しい AnyConnect パッケージが RA VPN 設定に追加されます。

ステップ 6 ステップ 6 から、「ASA RA VPN 設定の作成 （235 ページ）」に進みます。

AnyConnect パッケージの削除

ステップ 1 左側の CDO ナビゲーションバーで、**[VPN]** > **[リモートアクセスVPN（Remote Access VPN）]**をクリックします。

ステップ 2 変更する RA VPN 設定を選択し、[アクション] で [編集] をクリックします。

ステップ 3 [検出されたAnyConnectパッケージ（AnyConnect Packages Detected）] で、削除する AnyConnect パッケージの横に表示される アイコンをクリックします。オペレーティングシステムに複数のバージョンの AnyConnect パッケージがある場合は、リストから削除するパッケージを選択します。既存のパッケージが対応するフィールドから消去されます。

（注） [キャンセル（Cancel）] をクリックすると削除操作を停止し、既存のパッケージが保持されます。

ステップ 4 [OK] をクリックします。 デバイスの [設定ステータス（Configuration Status）] は [未同期（Not Synced）] となります。

（注） この段階で削除アクションを取り消す場合は、[デバイスとサービス（Device & Services）] ページに移動し、[変更の破棄（Discard Changes）] をクリックして、既存の AnyConnect パッケージを保持します。

ステップ 5 CDO から ASA に設定変更を展開します。。

オンボーディング済み ASA デバイスの RA VPN 設定の読み取り

RA VPN 設定がすでに存在する ASDM 管理対象 ASA デバイスを導入準備すると、既存のリモートアクセス VPN 設定が検出されて表示されます。CDO は自動的に「デフォルトの RA VPN 設定」を作成し、ASA デバイスをこの設定に関連付けます。CDO では読み取られないか、サポートされていない RA VPN 設定がいくつかありますが、これらは、CDO コマンドライン インターフェイスで設定できます。

（注） このセクションでは、CDO でサポートされている設定またはサポートされていない設定についてすべては網羅していません。最も一般的に使用される設定のみを説明します。

導入準備した ASA の RA VPN 設定を表示するには、次の手順を実行します。

ステップ 1 CDO インターフェイスで、**[VPN] > [リモートアクセスVPNの設定（Remote Access VPN Configuration）]** に移動します。

ステップ 2 導入準備した ASA デバイスに対応する RA VPN 設定をクリックします。CDO は自動的に「Default_RA_VPN_Configuration」を作成し、ASA デバイスをこの設定に関連付けます。デフォルト設定は削除できます。CDO で読み取られる ASA RA VPN 設定は、次のように分類されます。

- デバイス設定
- 接続プロファイル
- グループ ポリシー

デバイス設定

導入準備されている ASA デバイスに関連付けられている RA VPN 設定が **Default_RA_VPN_Configuration** に表示されます。この設定をクリックして、この設定に関連付けられている ASA デバイス（右側の [デバイス] ペインにあります）の名前 を表示する必要があります。編集ボタンをクリックして、ASA デバイスに存在する AnyConnect パッケージを表示することもできます。

接続プロファイル

CDO は、ASA デバイスの [AnyConnectクライアントVPNアクセス（AnyConnect Client VPN Access）] で定義された接続プロファイルをサポートしており、読み取ります。[クライアントレスSSL VPNアクセス（Clientless SSL VPN Access）] 設定はサポートしていません。

接続プロファイルの属性を確認するには、次の手順を実行します。

ステップ 1 **Default_RA_VPN_Configuration** を展開します。

ステップ 2 必要な接続プロファイルの 1 つをクリックし、[編集] をクリックします。

すべての基本および高度な ASA RA VPN 属性は、[CDO RA VPN] 設定ページの [接続プロファイル名と詳細（Connection Profile name and details）] に表示されます。

（注） デフォルトの設定を削除できます（デフォルトの RA VPN 設定を選択し、右側の [アクション] ペインで [削除] をクリックします）。

プライマリ アイデンティティ ソース

- CDO は、**接続エイリアス**属性と**グループ URL 属性**を**グループエイリアス**および**グループ URL** として読み取ります。

（注）
- SAML、複数の証明書と AAA、および複数の証明書を使用して設定された接続プロファイルは読み取られません。
- インターフェイスとサーバーグループを持つ認証サーバーグループはサポートされていません。

- CDO は、**プライマリ アイデンティティ ソース**で、「AAA」、「AAA と証明書」、「証明書のみ」の認証方式で設定された AnyConnect 接続プロファイルをサポートします。
- **AAA サーバーグループ**は、[プライマリ アイデンティティ ソース] で**ユーザー認証用のプライマリ アイデンティティ ソース**として CDO で読み取られます（この属性は、[認証タイプ] として [AAA] または [AAAとクライアント証明書] を選択することで表示できます）。
  - **AAA サーバーグループ**が LOCAL 以外に設定されている場合、CDO はこの属性を読み取り、[プライマリ アイデンティティ ソース] の下の [フォールバック ローカル アイデンティティ ソース] フィールドに表示します（認証タイプとして [AAA] を選択すると、この属性が表示されます）。

    CDO で読み取られるサーバーグループ属性の詳細については、「AAA サーバグループ」を参照してください。

セカンダリ アイデンティティ ソース

[セカンダリ アイデンティティ ソース] には、ASA デバイスのセカンダリ認証属性が表示されます。これらの属性を表示するには、認証タイプとして [AAA] または [AAAとクライアント証明書] を選択し、[セカンダリ アイデンティティ ソースの表示] をクリックします。

- [ユーザー認証用セカンダリ アイデンティティ ソース] に、セカンダリ認証の**サーバーグループ**属性が表示されます。
  - **サーバーグループ**が LOCAL 以外に設定されている場合、CDO はこの属性を読み取り、[セカンダリ アイデンティティ ソース] の下の [セカンダリ用フォールバック ローカル アイデンティティ ソース] フィールドに表示します。
- CDOは、**属性サーバー**および**インターフェイス固有の承認サーバーグループ**属性をサポートしていません。

CDO で読み取られるサーバーグループ属性の詳細については、「AAA サーバグループ」を参照してください。

承認サーバー

- [承認サーバー] には承認**サーバーグループ**の属性が表示されます。
- CDO は、インターフェイスとサーバーグループを持つ承認サーバーグループをサポートしていません。

CDO で読み取られる RADIUS サーバーグループ属性の詳細については、「RADIUS サーバグループ」を参照してください。

アカウンティングサーバー

アカウンティングサーバーは、アカウンティング **サーバー グループ**属性を表示します。CDO で読み取られるサーバーグループ属性の詳細については、「RADIUS サーバグループ」を参照してください。

クライアントアドレスプールの割り当て

CDO は、**クライアントアドレス割り当て属性（DHCP サーバー、クライアントアドレスプール、クライアント IPv6 アドレスプール**）をオブジェクトとして読み取ります（これらの属性は「**クライアントアドレスプールの割り当て**」で確認できます）。DHCP サーバーの詳細はリテラルとして読み取られます。

（注） CDO は、特定のインターフェイスに割り当てられた IP アドレスプールをサポートしていません。ただし、これらの属性はASA コマンドライン インターフェイス（CLI）で確認できます。

AAA サーバグループ

CDO は、LDAP サーバーグループとそれに関連付けられた LDAP サーバーを、[Active Directory レルム（Active Directory Realm）] オブジェクトとして表します。Active Directory（AD）の場合、レルムは Active Directory ドメインに相当します。CDO は、既に存在する AD レルムオブジェクトの AD パスワードを読み取ります。

ステップ 1 [オブジェクト] で、[Active Directoryレルム（Active Directory レルム）] フィルタを適用して、このオブジェクトを表示できます。

ステップ 2 必要な Active Directory レルムオブジェクトを選択して、[編集] をクリックして詳細を表示します。

次のタスク

AD レルムには、関連付けられた AD サーバーとその設定が含まれていることがわかります。AD レルムに対して複数の Active Directory（AD）サーバーが存在する場合、AD サーバーは相互に複製されていて、同じ AD ドメインをサポートする必要があります。したがって、ディレクトリ名、ディレクトリパスワード、ベース識別名などの基本的なレルムプロパティは、その AD レルムに関連付けられたすべての AD サーバーで同じである必要があります。これらのプロパティが同じでない場合、CDO は Active Directory レルムオブジェクトに警告メッセージを表示します。これらのプロパティを修正して、AD サーバー全体で一貫性を持たせる必要があります。この警告に対処せずに続行すると、CDO はいずれかの AD サーバープロパティを使用し、そのレルムオブジェクト内の他のサーバーに適用します。

RADIUS サーバグループ

ASA デバイスの AAA RADIUS サーバーグループ属性は、CDO では RADIUS サーバー グループ オブジェクトとして読み取られます。

ステップ 1 [オブジェクト] で RADIUS サーバーグループフィルターを適用して、このオブジェクトを表示できます。

ステップ 2 必要なオブジェクトを選択して、[編集] をクリックして詳細を表示します。

- ASA での [ダイナミック認証の有効化（Enable dynamic authorization）]は、CDO では [ダイナミック認証（RA VPNの場合のみ）（Dynamic Authorization (for RA VPN only)）] として読み取られます。
- [再アクティブ化モード（Reactivation Mode）] の [枯渇（Depletion）] オプションは CDO で読み取られるため、枯渇時間に関連する [デッドタイム値（Dead Time）] も CDO で読み取られます。ただし、[時間指定（Timed）] 属性は CDO で読み取られません。
- CDO は、[アカウンティングモード（Accounting Mode）]、[時間指定（Timed）]、[中間アカウンティングアップデートの有効化（Enable interim accounting update）]、[中間アカウンティングアップデートの有効化（Enable interim accounting update）]、および [認可専用モードの使用（Use authorization only mode）] をサポートしていません。

RADIUS サーバ

CDO が ASA から Radius サーバーを読み取ると、「Radius サーバーグループの名前_サーバー名または IPアドレス」という名前を指定する Radius サーバーオブジェクトが作成されます。

ステップ 1 [オブジェクト] で [RADIUSサーバー（RADIUS Server）] フィルタを適用して、このオブジェクトを表示できます。

ステップ 2 必要なオブジェクトを選択して、[編集（Edit）] をクリックして詳細を表示します。

Group Policy

[グループポリシー（Group Policy）] セクションでドロップダウンをクリックして、デバイスに関連付けられたグループポリシーを表示します。

注目 CDOは、トンネリングプロトコルでSSL VPNクライアントとして設定されたグループポリシーを読み取ります。

CDOは、ASAで設定されたグループポリシー属性の大部分を読み取ります。情報は、RA VPNグループポリシーウィザードの複数のタブにわたって表示されます。ASAデバイスから読み取られたグループポリシーの詳細を表示するには、次を実行する必要があります。

ステップ 1 CDO ナビゲーションバーで、[オブジェクト] をクリックし、[RA VPNグループポリシー（RA VPN Group Policy）] でフィルタリングします。

ステップ 2 そのデバイスに関連付けられているグループポリシーを選択し、[編集] をクリックします。

次のタスク

（注） CDO は、ASA デバイスのスプリットトンネリングで定義されている標準アクセス制御リスト（ACL）をサポートしていません。CDO は拡張アクセス制御リスト（ACL）をサポートし、ASA ポリシーの ACL として読み取ります。詳細については、「ASA RA VPN グループポリシー属性」を参照してください。ポリシーを表示するには、ナビゲーションバーで [ポリシー（Policies）] > [ASAアクセスポリシー（ASA Access Policies）] をクリックします。

拡張 ACL を選択するには、次の手順を実行します。

- [スプリットトンネリング（Split Tunneling）] タブをクリックします。
- ASA のトラフィックが IPv4 または IPv6 アドレスのどちらを使用するかに基づいて、対応するドロップダウンリストから [トンネル経由の指定したトラフィックを許可する（Allow specified traffic over tunnel）] または [以下に指定したネットワークを除外する（Exclude

networks specified below）] を選択します。ASA からインポートされた拡張 ACL を選択します。

IP アドレスプールの作成

ASA の IPv4 および IPv6 IP アドレスプールを設定して、VPN 接続を使用してネットワークにリモート接続しているクライアントにそれらを割り当てることができます。プールの指定順序は重要です。接続プロファイルまたはグループ ポリシーに複数のアドレス プールを設定すると、ASA は追加された順でそれらのプールを使用します。

IPv4 アドレスプールを定義するには、IP アドレス範囲を指定します。IPv4 アドレスプールの例は、10.10.147.100 - 10.10.147.177 です。

IPv6 アドレスプールを設定するには、開始 IP アドレス範囲、アドレスプレフィックス、プールに設定できるアドレス数を指定します。IPv6 アドレスプールの例は、2001:DB8:1::1 です。

ローカルでないサブネットのアドレスを割り当てる場合は、そのようなネットワーク用のルートの追加が容易になるように、サブネットの境界を担当するプールを追加することをお勧めします。

IP アドレスプールを作成するには、次の手順を実行します。

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

ステップ 2 青いプラスボタン  をクリックし、**[ASA] > [アドレスプール]**を選択します。

ステップ 3 [IPアドレスプールの作成（Create IP Address Pool）] ダイアログボックスで、次の情報を入力します。

- [オブジェクト名] : アドレスプールの名前を入力します。最大 64 文字を指定できます。
- [IPv4アドレスプール] : このラジオボタンを選択して、IPv4 アドレスプールを設定します。
  - [IPv4アドレス範囲（IPv4 Address Range）] : 設定された各プールで使用可能な最初の IP アドレスと最後の IP アドレスを入力します。たとえば、10.10.147.100 - 10.10.147.177 です。
  - [マスク（Mask）] : この IP アドレスプールが常駐するサブネットを指定します。
- [IPv6アドレスプール] : このラジオボタンを選択して、IPv4 アドレスプールを設定します。
  - [IPv6 アドレス（IPv6 Address）] : 設定されたプールで使用できる最初の IP アドレスとビットのプレフィックス長を、 <address>/<prefix> 形式で入力します。たとえば、2001:DB8:1::1/3 です。
  - [アドレスの数（Number of Addresses）] : IP アドレスから始まる、プールにある IPv6 アドレスの数を指定します。

ステップ 4 [保存（Save）] をクリックします。

リモートアクセス VPN 認証ベースの認証

リモートアクセス VPN は、次のシナリオでセキュアゲートウェイおよび AnyConnect クライアント（エンドポイント）を認証するためにデジタル証明書を使用します。

重要 CDO は、VPN ヘッドエンド（ASA ）へのデジタル証明書のインストールを処理します。AnyConnect クライアントデバイスへの証明書のインストールは処理されません。これは、組織の管理者が処理する必要があります。

- VPN ヘッドエンドデバイス（ASA ）を識別して認証します。

  VPN ヘッドエンドは、AnyConnect クライアントが VPN 接続を要求するときに、VPN ヘッドエンド自体を識別して認証するための ID 証明書を必要とします。CDO を使用して、デバイスに ID 証明書をインストールする必要があります。「PKCS12 を使用した ID 証明書をインストールする」または「証明書とキー」を参照してください。AnyConnect クライアントに発行元の CA 証明書をインストールすることは、必須ではありません。

  CDO からリモートアクセス VPN 構成を作成するときに、登録済み ID 証明書をデバイスの外部インターフェイスに割り当て、構成をデバイスにダウンロードします。ID 証明書は、デバイスの外部インターフェイスで完全に機能するようになります。

  AnyConnect クライアントが VPN への接続を試みると、デバイスは、その ID 証明書を AnyConnect クライアントに提示することにより、それ自体を認証します。AnyConnect クライアントは、信頼できる CA 証明書を使用してこの ID 証明書を検証し、その証明書を信頼することによってデバイスを信頼します。AnyConnect クライアントに CA 証明書がインストールされていない場合、プロンプトが表示されたときに、ユーザーがデバイスを手動で信頼する必要があります。

- AnyConnect クライアントを識別して認証します。

  （注） これは、RA VPN 構成の接続プロファイルで認証方式として「クライアント証明書のみ」または「AAA とクライアント証明書」を使用する場合に適用されます。「AAA のみ」には適用されません。

  デバイスが信頼されると、AnyConnect クライアントは、VPN 接続を完了するためにそれ自体を認証する必要があります。AnyConnect クライアントに ID 証明書をインストールし、CDO を使用して、信頼できる CA 証明書をデバイスにインストールする必要があります。これらの証明書は、同じ認証局によって発行される必要があります。「ASA の信頼できる証明書をインストールする」を参照してください。

  AnyConnect クライアントが ID 証明書を提示し、デバイスは、この証明書を信頼できる CA 証明書で検証して、VPN 接続を確立します。

NAT からの ASA リモート アクセス トラフィックの除外

リモートアクセス VPN エンドポイントとの入出力トラフィックに対する NAT 変換を免除するには、NAT 免除を設定します。VPN トラフィックを NAT 免除にしない場合は、外部および内部インターフェイスに対する既存の NAT ルールが RA VPN アドレス プールに適用されないことを確認してください。NAT 免除 ルールは特定の送信元/宛先インターフェイスとネットワークの組み合わせに対する手動スタティック アイデンティティ NAT ルールですが、NAT ポリシーには反映されず、非表示になります。NAT 免除を有効にした場合、以下も設定する必要があります。

- [内部インターフェイス（Inside Interfaces）]：リモートユーザーがアクセスする内部ネットワークのインターフェイスを選択します。これらのインターフェイスには NAT ルールが作成されます。
- [内部ネットワーク（Inside Networks）]：リモートユーザーがアクセスする内部ネットワークを表すネットワークオブジェクトを選択します。ネットワークリストには、サポートしているアドレス プールと同じ IP タイプを含める必要があります。

始める前に

デバイスの接続プロファイルおよびグループポリシーで使用されるローカル IP アドレスプールの設定に一致する ASA ネットワークオブジェクトを作成します。それらのネットワークオブジェクトは、NAT ルールを設定するときに、宛先アドレスおよび変換されたアドレスとして割り当てる必要があります。「ASA ネットワークオブジェクトの作成（143 ページ）」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 [デバイスとサービス] フィルタと [検索] フィールドを使用して、NAT ルールを作成する ASA デバイスを見つけます。

ステップ 3 詳細パネルの [管理] 領域で、[NAT] NAT をクリックします。

ステップ 4 + > [Twice NAT] をクリックします。

1. セクション 1 で、[静的（Static）] を選択します。 [続行（Continue）] をクリックします。
2. セクション 2 で、[送信元インターフェイス（Source Interface）] で [any] および [宛先インターフェイス（Destination Interface）] で [any] を選択します。[続行] をクリックします。
3. セクション 3 で、[送信元の元のアドレス（Source Original Address）] で [any] および [送信元の変換後アドレス（Source Translated Address）] で [any] を選択します。
4. [宛先を使用（Use Destination）] を選択します。
    1. [宛先の元のアドレス（Destination Original Address）] と [送信元の変換後アドレス（Source Translated Address）]：ドロップダウンで [選択（Choose）] をクリックし、ローカル IP アドレスプールの設定に一致するネットワークオブジェクトを選択します。次の例では、「IPV4_Object」は、ASA（BGL_ASA1_SH）デバイスの接続プロファイルおよびグループポリシー設定で使用される IPv4

アドレスプールオブジェクトと同じ設定を持つネットワークオブジェクトです。

2. [着信パケットのプロキシARPの無効化（Disable proxy ARP for incoming packets）] を選択します。
3. [保存（Save）] をクリックします。
4. プロセス（ステップ 4 から）を繰り返して、IP アドレスプールに相当する他のネットワークオブジェクトごとに同等のルールを作成します。

ステップ 5 CDO から ASA に設定変更を展開します。。

ユーザーが AnyConnect クライアントソフトウェアを ASA にインストールする方法

VPN 接続を完了するには、ユーザは AnyConnect クライアント ソフトウェアをインストールする必要があります。既存のソフトウェア配布方式を使用して、ソフトウェアを直接インストールできます。または、ASA デバイスから AnyConnect クライアントを直接インストールすることもできます。

（注） ソフトウェアをインストールするには、ユーザにワークステーションでの管理者権限が必要です。

ソフトウェアの最初のインストールを ASA デバイスからユーザーに行ってもらう場合、以下の手順を実行するようにユーザーに指示します。

（注） Android および iOS のユーザは、適切な App Store から AnyConnect をダウンロードする必要があります。

ステップ 1 Web ブラウザを使用して、**https://***ravpn-address* を開きます。*ravpn-address* は、VPN 接続を許可する外部インターフェイスの IP アドレスまたはホスト名です。このインターフェイスは、リモート アクセス VPN を設定する際に指定します。ログインを指示するメッセージがユーザに示されます。

ステップ 2 サイトにログインします。ユーザは、リモート アクセス VPN 用に設定されたディレクトリ サーバを使用して認証されます。続行するには、ログインが正常に行われる必要があります。ログインが成功すると、システムは、必要となる AnyConnect クライアントのバージョンがインストールされているかを確認します。AnyConnect クライアントがユーザーのコンピュータにないか、下位のバージョンである場合、システムは自動的に AnyConnect ソフトウェアのインストールを開始します。インストールが終了すると、AnyConnect がリモートアクセス VPN 接続を完了します。

導入準備済み ASA のリモートアクセス VPN 設定の変更

ASA デバイスが CDO に導入準備されると、導入準備された ASA デバイスから既存のリモートアクセス VPN 設定を検出して表示します。詳細については、オンボーディング済み ASA デバイスの RA VPN 設定の読み取り （250 ページ）を参照してください。

これらの設定を変更して、新しい設定をデバイスにダウンロードできます。

- ASA RA VPN 構成の変更
- ASA 接続プロファイルの変更

リモートアクセス *VPN* 設定の変更

ステップ 1 左側の CDO ナビゲーションバーで、[VPN] > [リモートアクセスVPNの設定（Remote Access VPN Configuration）] をクリックします。

ステップ 2 グループポリシーを VPN 設定に追加または削除する場合は、導入準備の ASA デバイスに関連付けられている VPN 設定をクリックします。左側の [操作（Actions）] ウィンドウで、[グループポリシー（Group Policies）] をクリックします。

a) 青い [+] アイコンをクリックして選択を設定し、[選択（Select）] をクリックします。
b) [保存（Save）] をクリックします。新しい新規 ASA RA VPN グループポリシーの作成を作成することもできます。

ステップ 3 [VPN設定（VPN configuration）] をクリックし、左側の [操作（Actions）] ウィンドウで [編集] をクリックします。

ウィザードには、設定に関連付けられている ASA デバイスが一覧表示されます。

a) 作成時と同じ方法で、次の詳細を変更できます。

- RA VPN 設定の名前を変更します。
- デバイスの詳細が表示されている行に表示される 3 つのドットをクリックし、[編集] をクリックします。

詳細については、ASA RA VPN 設定の作成 （235 ページ）を参照してください。

ステップ 4 [OK] をクリックします。

ステップ 5 すべてのデバイスの構成変更のプレビューと展開 （308 ページ）

ASA 接続プロファイルの変更

ステップ 1 左側の CDO ナビゲーションバーで、[VPN] > [リモートアクセスVPNの設定（Remote Access VPN Configuration）] をクリックします。

ステップ 2 導入準備の ASA デバイスに関連付けられている VPN 設定を展開し、接続プロファイルを選択します。

ステップ 3 左側の [アクション] ペインで、[編集] をクリックします。

ステップ 4 作成時と同じ方法で値を編集し、[完了（Done）] をクリックします。

詳細については、「ASA RA VPN 接続プロファイルの設定 （239 ページ）」を参照してください。

ステップ 5 すべてのデバイスの構成変更のプレビューと展開 （308 ページ）

RA VPN AnyConnect クライアントプロファイルのアップロード

リモートアクセス VPN AnyConnect クライアントプロファイルは、ファイルに保存されている設定パラメータのグループです。AnyConnect クライアントプロファイルにはさまざまな種類があり、コアクライアント VPN 機能とオプション クライアント モジュールであるネットワーク アクセス マネージャ、AMP イネーブラ、ISE ポスチャ、ネットワークの可視性、カスタマー フィードバック エクスペリエンス プロファイル、Umbrella ローミングセキュリティ、Web セキュリティの構成設定が含まれています。

CDO では、後でグループポリシーで使用できるオブジェクトとしてこれらのプロファイルをアップロードできます。

- [AnyConnect VPNプロファイル（AnyConnect VPN Profile）]：AnyConnect クライアントプロファイルは、VPN AnyConnect クライアントソフトウェアとともにクライアントにダウンロードされます。これらのプロファイルでは、多くのクライアント関連オプション（スタートアップ時の自動接続、自動再接続など）や、エンドユーザーが AnyConnect クライアントの設定および詳細設定からオプションを変更できるかどうかを定義します。CDO は XML ファイル形式をサポートしています。
- [AMPイネーブラサービスプロファイル（AMP Enabler Service Profile）]：このプロファイルは AnyConnect AMP イネーブラに使用されます。リモートアクセス VPN ユーザーが VPN に接続すると、AMP イネーブラがこのプロファイルと共に FTD からエンドポイントにプッシュされます。CDO は、XML および ASP ファイル形式をサポートしています。
- [フィードバックプロファイル（Feedback Profile）]：カスタマー エクスペリエンス フィードバック プロファイルを追加し、このタイプを選択すると、顧客が有効にして使用している機能およびモジュールに関する情報を受信できます。CDO は FSP ファイル形式をサポートしています。

- [ISEポスチャプロファイル（ISE Posture Profile）]：AnyConnect ISE ポスチャモジュールのプロファイルファイルを追加する場合は、このオプションを選択します。CDO は、XML および ISP ファイル形式をサポートしています。
- [ネットワークアクセスマネージャサービスプロファイル（Network Access Manager Service Profile）]：ネットワーク アクセス マネージャのプロファイルエディタを使用して、NAM プロファイルファイルを設定および追加します。CDO は、XML および NSP ファイル形式をサポートしています。
- [ネットワーク可視性サービスプロファイル（Network Visibility Service Profile）]：AnyConnect Network Visibility Module のプロファイルファイル。NVM プロファイルエディタを使用してプロファイルを作成できます。CDO は、XML および NVMSP ファイル形式をサポートしています。
- [Umbrellaローミングセキュリティプロファイル（Umbrella Roaming Security Profile）]：Umbrella ローミング セキュリティ モジュールを展開する場合は、このファイルタイプを選択する必要があります。CDO は、XML および JSON ファイル形式をサポートしています。
- [Webセキュリティサービスプロファイル（Web Security Service Profile）]：Web セキュリティモジュールのプロファイルファイルを追加するときに、このファイルタイプを選択します。CDO は、XML、WSO、および WSP ファイル形式をサポートします。

始める前に

適切な GUI ベースの AnyConnect プロファイルエディタを使用して、必要なプロファイルを作成します。AnyConnect セキュア モビリティ クライアント カテゴリの Cisco Software Download Center からプロファイルエディタをダウンロードし、AnyConnect の「プロファイルエディタ - Windows/スタンドアロンインストーラ（MSI）」をインストールできます。プロファイルエディタのインストーラには、スタンドアロンバージョンのプロファイルエディタが含まれています。このインストールファイルは Windows 専用で、ファイル名は anyconnect-profileeditor-win-<version>-k9.msi です。ここで、<version> は AnyConnect のバージョンです。たとえば、anyconnect-profileeditor-win-4.3.04027-k9.msi のような名前になります。プロファイル エディタをインストールする前に、Java JRE（1.6 以降）もインストールする必要があります。

このパッケージには、Umbrella ローミング セキュリティ プロファイル エディタを除き、モジュールの作成に必要なすべてのプロファイルエディタが含まれています。詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』の該当するリリースの「*AnyConnect* プロファイルエディタ」の章を参照してください。Umbrella ダッシュボードから Umbrella ローミング セキュリティ プロファイルを個別にダウンロードします。詳細については、『Cisco Umbrella User Guide』の「Umbrella ローミングセキュリティ」章の「Umbrella ダッシュボードから AnyConnect ローミング セキュリティ プロファイルをダウンロードする」セクションを参照してください。

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

ステップ 2 青色のプラス ボタンをクリックします。

ステップ 3 **[RA VPNオブジェクト（ASA & FTD）（RA VPN Objects (ASA & FTD)）] > [AnyConnectクライアントプロファイル（AnyConnect Client Profile）]**をクリックします。

ステップ 4 [オブジェクト名] フィールドに、AnyConnect クライアントプロファイルの名前を入力します。

ステップ 5 [参照] をクリックし、プロファイルエディタを使って作成したファイルを選択します。

ステップ 6 [開く（Open）] をクリックしてプロファイルをアップロードします。

ステップ 7 [追加] をクリックしてオブジェクトを追加します。

関連情報：

- RA VPN グループポリシーウィンドウで、クライアントモジュールを AnyConnect VPN プロファイルに関連付けます。「新規 ASA RA VPN グループポリシーの作成」を参照してください。

（注） クライアントモジュールの関連付けは、すべての ASA バージョン、およびソフトウェアバージョン 6.7 以降を実行している FTD でサポートされています。

ASA のリモートアクセス VPN 設定の確認

リモートアクセス VPN を設定し、設定をデバイスに展開した後で、リモート接続できることを確認します。

ステップ 1 外部ネットワークから、AnyConnect クライアントを使用して VPN 接続を確立します。Web ブラウザを使用して、**https://***ravpn-address* を開きます。*ravpn-address* は、VPN 接続を許可する外部インターフェイスの IP アドレスまたはホスト名です。必要に応じて、クライアントソフトウェアをインストールし、接続を完了します。「ユーザーが AnyConnect クライアントソフトウェアを ASA にインストールする方法」を参照してください。グループ URL を設定した場合は、グループ URL も試してください。

ステップ 2 [デバイスとサービス] ページで、確認するデバイス（FTD または ASA）を選択し、[デバイスアクション] の下の [コマンドラインインターフェイス（Command Line Interface）] をクリックします。

ステップ 3 **show vpn-sessiondb** コマンドを使用して、現在の VPN セッションに関する概要情報を表示します。

ステップ 4 統計情報では、アクティブな AnyConnect クライアント セッション、および累積セッション数、ピーク同時セッション数、非アクティブ セッション数の情報が示されます。次は、コマンドからの出力例です。

```
> show vpn-sessiondb
--------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
AnyConnect Client           :      1 :         49 :           3 :        0
  SSL/TLS/DTLS              :      1 :         49 :           3 :        0
Clientless VPN              :      0 :          1 :           1
  Browser                   :      0 :          1 :           1
--------------------------------------------------------------------------


  Total Active and Inactive    :      1             Total Cumulative :     50
  Device Total VPN Capacity    :  10000
  Device Load                  :     0%
  --------------------------------------------------------------------------

  --------------------------------------------------------------------------
  Tunnels Summary
  --------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ----------------------------------------------
  Clientless                 :      0 :          1 :               1
  AnyConnect-Parent          :      1 :         49 :               3
  SSL-Tunnel                 :      1 :         46 :               3
  DTLS-Tunnel                :      1 :         46 :               3
  --------------------------------------------------------------------------
  Totals                     :      3 :        142
  --------------------------------------------------------------------------

  --------------------------------------------------------------------------
  IPv6 Usage Summary
  --------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ----------------------------------------------
  AnyConnect SSL/TLS/DTLS    :        :           :
    Tunneled IPv6            :      1 :         20 :           2
  --------------------------------------------------------------------------
```

ステップ 5 **show vpn-sessiondb anyconnect** コマンドを使用して、現在の AnyConnect VPN セッションに関する詳細情報を表示します。詳細情報には、使用されている暗号化、送信バイト数と受信バイト数などの統計情報が含まれます。VPN 接続を使用する場合、このコマンドを再発行すると送信バイト数と受信バイト数が変わるのがわかります。

ステップ 6 **show vpn-sessiondb anyconnect** コマンドを使用して、現在の AnyConnect VPN セッションに関する詳細情報を表示します。詳細情報には、使用されている暗号化、送信バイト数と受信バイト数などの統計情報が含

まれます。VPN接続を使用する場合、このコマンドを再発行すると送信バイト数と受信バイト数が変わるのがわかります。

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : User1                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone : 0
```

ASA のリモートアクセス VPN 設定の詳細表示

ステップ 1 左側の CDO ナビゲーションバーで、**[VPN]** > **[リモートアクセスVPNの設定（Remote Access VPN Configuration）]**をクリックします。

ステップ 2 表示されたVPN設定オブジェクトをクリックします。グループには、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報が表示されます。

- RA VPN 設定を展開して、それらに関連付けられているすべての接続プロファイルを表示します。
  - 追加 + ボタンをクリックして新しい接続プロファイルを追加します。
  - 表示ボタン（  ）をクリックして、接続プロファイルの概要と接続手順を開きます。[アクション（Actions）] で、[編集（Edit）] をクリックして変更を変更できます。
- [アクション（Actions）] で次のオプションのいずれかをクリックすると、追加のタスクを実行できます。
  - グループポリシーを割り当て/追加するには、[グループポリシー（Group Policies）] をクリックします。
  - 不要になった設定オブジェクトまたは接続プロファイルをクリックし、[削除（Remove）] をクリックして削除します。

ASA のテンプレート

テンプレートを使用すると、汎用のデバイス/サービス構成を構築できるため、その構成をグループ化された他の構成に適用できます。これらのテンプレートにより、グループ化された多くの実装に影響を与えるための変更を一箇所で行うことができます。

ASA テンプレートパラメータ

新しいテンプレートを作成する際、特定のデバイスをモデルにしたいことがあります。CDO には、テンプレートがモデル化されたデバイスの設定内にあるテキストの選択されたフィールドに基づいてテンプレートパラメータを設定する機能があります。パラメータは、作成するか、既存のパラメータから設定する、またはテンプレート パラメータ ビュー内で検索することができます。

（注） ASAテンプレートの設定をインポートすることを選択した場合、設定はJSON形式である必要があります。

新規パラメータの作成

ステップ 1 既存のデバイスが導入準備された状態で、CDO の上部にある [テンプレート] タブに移動します。
ステップ 2 [新しいテンプレート（New Template）] または [テンプレートの管理（Manage Templates）] を選択します。
ステップ 3 必要な設定を選択してパラメータを作成します。
ステップ 4 画面上部にある [名前（Name）] フィールドに入力することによってテンプレートに名前を付けます。
ステップ 5 パラメータを追加する目的のテキストフィールドを選択します。
ステップ 6 パラメータに説明を付け、値と必要な注記を追加します。
ステップ 7 [名前（Name）] フィールドの横にある [保存（Save）] をクリックしてパラメータを保存します。
ステップ 8 その後、[テンプレートの確認（Review Template）] をクリックして、テンプレートを確認することができます。

これで、今後このテンプレートを使用して導入準備されるすべてのデバイスに適用されるパラメータが作成され、保存されました。

新規 ASA、ISR、ASR テンプレートの作成

基本設定

既知のASA、ISR、またはASRの基本設定から始めます。目的の設定を選択して、テンプレートのパラメータ化を開始します。パラメータ化には、構成ファイル内のフィールドまたは属性の選択と、構成ファイルのインスタンス化で選択される値のリストの識別が含まれます。

（注） ASAテンプレートの設定をインポートすることを選択した場合、設定はJSON形式である必要があります。

パラメータの追加

基本設定を選択すると、パラメータ化プロセスを開始できます。設定エディタから、パラメータ化する目的のフィールドを選択します。選択した文字列は二重括弧で囲まれています。左ペインから、パラメータの名前を変更したり、説明を追加したり、複数の値を追加したりできます。[カスタム値を許可（Allow Custom Value）] を選択すると、インスタンス化時にカスタム値を設定できます。それ以外の場合は、識別された値のみ選択できます。

パラメータ化が完了したら、テンプレートの名前を指定し、[保存（Save）] をクリックします。

パラメータ化の詳細については、ASA テンプレートパラメータを参照してください。

レビュー

テンプレートを保存したら、[レビュー（Review）] をクリックしてレビュープロセスに移動します。レビューでは、パラメータ化された値を含め、テンプレートをそのままエクスポートできます。これは必ずしも有効な設定ではありませんが、CDO に保存されているテンプレートを確認する手段が提供されます。必要に応じて、[編集] をクリックしてテンプレートを編集することもできます。[差分（Diff）] ボタンを使用すると、保存されたテンプレートと最新の編集との違いが表示されます。

テンプレートからの ASA 設定の生成

テンプレートからの設定の作成

テンプレートからカスタム設定を生成するプロセスを開始するには、[テンプレートから設定（Config from Template）] ボタンをします。使用可能なテンプレートが一覧表示されます。該当するテンプレートを選択して、[テンプレートの選択（Choose Template）] をクリックします。

ほとんどの場合、テンプレートには、設定をカスタマイズするために [エクスポート（Export）] で設定する必要があるパラメータ化された値が含まれます。左側のペインから、この設定に必要な各パラメータと値を選択します。値がエディターに示されるので注目してください。これらは、エクスポート時にパラメータを置き換える値です。すべてのパラメータ値を設定したら、[エクスポート（Export）] ボタンをクリックして設定をエクスポートし、ダウンロードします。テンプレートにパラメータ化された値が含まれていない場合は、[エクスポート（Export）] ボタンをクリックして設定をそのままエクスポートします。

ASA テンプレートの管理

[テンプレートの管理（Manage Templates）] ビューでは、既存のすべてのテンプレートを可視化し、それらを編集および削除することができます。パラメータ化と値の構成は、テンプレートの編集中に変更できます。その方法は、既存のテンプレートにマウスのカーソルを合わせて、[編集] を選択して変更を加えるだけです。

テンプレートの編集

編集ビューでは、次の作業を実行できます。

- エディタのテキストをダブルクリックまたは強調表示して、パラメータを追加します。
- 説明のテキストボックスに入力して、パラメータを説明します。その後に、[値の追加（Add Value）] をクリックします。
- 値を指定し、注記を入力します。[追加（Add）] をクリックします。
- 完了したら、[Save] をクリックします。
- ここで、[テンプレートの確認（Review Template）] をクリックして、テンプレートを確認することができます。
  - [差分（Diff）] をクリックして、ファイルを比較することができます。
  - テンプレートをエクスポートするには、[Export（エクスポート）] をクリックします。

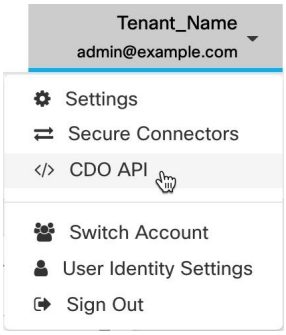
CDO パブリック API

CDO はパブリック API を公開しており、ドキュメント、例、試してみるためのプレイグラウンドを提供しています。パブリック API の目標は、通常は CDO UI で実行できる多くのことをコードで実行するためのシンプルで効果的な方法を提供することです。

この API を使用するには、GraphQL の知識が必要です。詳細でありながら読みやすい公式ガイド（https://graphql.org/learn/）が提供されています。

完全なスキーマドキュメントを見つけるには、GraphQL Playground に移動し、ページの右側にある [ドキュメント（docs）] タブをクリックしてください。

ユーザーメニューから選択して、CDO パブリック API を起動できます。



API トークン

開発者は、CDO REST API 呼び出しを行うときに CDO API トークンを使用します。呼び出しを成功させるには、API トークンを REST API 認証ヘッダーに挿入する必要があります。API

トークンは、有効期限のない「長期的な」アクセストークンですが、更新したり、取り消したりできます。

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

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

API トークン形式とクレーム

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

CDO API トークンは、次の一連のクレームを提供します。

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

ASA 証明書の管理

デジタル証明書は、デバイスや個々のユーザーの認証に使用されるデジタル ID を提供します。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザーまたはデバイスを識別する情報が含まれます。デジタル証明書には、ユーザーまたはデバイスの公開キーのコピーも含まれています。デジタル証明書の詳細については、『Cisco ASA Series General Operations ASDM Configuration, X.Y』ドキュメントの「Basic Settings」ブックの「Digital Certificates」の章を参照してください。

認証局（CA）は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザーのアイデンティティを保証する、信頼できる機関です。CA はID 証明書も発行します。

- **ID 証明書**：ID 証明書は、特定のシステムまたはホストの証明書です。これらは OpenSSL ツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名証明書を生成することもできます。CA は、特定のシステムまたはホストの証明書である ID 証明書を発行します。
- **信頼できる認証局（CA）証明書**：信頼できる CA 証明書は、システムで他の証明書への署名に使用できる証明書です。これらの証明書は、基本制約拡張と CA フラグに関して内

部アイデンティティ証明書と異なります。これらはCA 証明書では有効ですが、アイデンティティ証明書では無効です。信頼できる CA 証明書は自己署名され、ルート証明書と呼ばれます。

リモートアクセス VPN は、セキュリティで保護された VPN 接続を確立するために、セキュアゲートウェイおよび AnyConnect クライアント（エンドポイント）を認証するためのデジタル証明書を使用します。詳細については、「リモートアクセス VPN 認証ベースの認証」を参照してください。

証明書のインストールに関するガイドライン

ASA での証明書のインストールに関する以下のガイドラインをお読みください。

- 証明書は、1 つの ASA デバイスに、または複数の ASA デバイスに同時にインストールできます。
- 証明書は一度に 1 つだけインストールできます。
- 証明書は、ライブ ASA デバイスにのみインストールできます。モーダルデバイスにはインストールできません。
- 証明書は、 Secure Firewall Cloud Native デバイスにインストールできません。

ASA 証明書のインストール

デジタル証明書をトラストポイントのオブジェクトとしてアップロードし、CDO によって管理される ASA デバイスにインストールする必要があります。

（注） ASAデバイスにアウトオブバンドの変更がなく、ステージングされたすべての変更が展開されていることを確認します。

CDO でサポートされているデジタル証明書と形式を次に示します。

- ID 証明書は、次の方法を使用してインストールできます。
  - PKCS12 ファイルのインポート。
  - 自己署名証明書。
  - 証明書署名要求（CSR）のインポート。
- 信頼できる CA 証明書は、PEM または DER 形式を使用してインストールできます。

CDO を使用して ASA に証明書をインストールする手順を示すスクリーンキャストをご覧ください。インストールされている証明書を変更、エクスポート、および削除する手順も示しています。

サポートされている証明書形式

- PKCS12：PKCS#12、P12、または PFX 形式は、サーバー証明書、あらゆる中間証明書、および秘密キーを 1 つの暗号化可能ファイルに格納するためのバイナリ形式です。PFX ファイルには通常、**.pfx** や **.p12** などの拡張子が付いています。
- PEM：PEM（元は「Privacy Enhanced Mail」）ファイルには ASCII（または Base64）エンコードデータが含まれており、証明書ファイルは .pem、.crt、.cer、または .key 形式にすることができます。これらは Base64 でエンコードされた ASCII ファイルで、「-----BEGIN CERTIFICATE-----」および「-----END CERTIFICATE-----」ステートメントが含まれています。
- DER：DER（Distinguished Encoding Rule）形式は、ASCII PEM 形式ではなく、シンプルなバイナリ形式の証明書です。**.der** ファイル拡張子が付いている場合もありますが、**.cer** ファイル拡張子が付いていることが多いため、DER の.cer ファイルと PEM の .cer ファイルを区別する唯一の方法は、テキストエディタで開いて、 BEGIN/END ステートメントの有無を確認することです。PEM とは異なり、DER でエンコードされたファイルには、 -----BEGIN CERTIFICATE----- などのプレーン テキスト ステートメントは含まれません。

トラストポイント画面

ASA デバイスを CDO に導入準備した後、[デバイスとサービス] タブで ASA デバイスを選択し、左側の [管理] ペインで [トラストポイント] をクリックします。

[トラストポイント] タブに、デバイスにインストール済みの証明書が表示されます。

- [インストール済み（Installed）] ステータスは、対応する証明書がデバイスに正常にインストールされたことを示します。
- 「不明（Unknown）」ステータスは、対応する証明書に情報がなにも含まれていないことを示します。このような証明書は削除して、正しい情報を含む証明書を再度アップロードする必要があります。CDO は、すべての不明な証明書を信頼できる CA 証明書として検出します。
- [インストール済み（Installed）] と表示されている行をクリックして、右側のペインに証明書の詳細を表示します。[詳細（More）] をクリックして、選択した証明書の詳細を表示します。
- インストールされたID 証明書は、PKCS12 または PEM 形式でエクスポートして、他の ASA デバイスにインポートできます。「ID 証明書のエクスポート」を参照してください。
- インストールされた証明書で変更できるのは、詳細設定のみです。
  - [編集] をクリックして、詳細設定を変更します。
  - 変更を加えたら、[送信（Send）] をクリックして、更新された証明書をインストールします。

PKCS12 を使用した ID 証明書のインストール

PKCS12 形式用に作成された既存のトラストポイントオブジェクトを選択して、ASA デバイスにインストールできます。インストールウィザードから新しいトラストポイントオブジェクトを作成し、ASA デバイスに証明書をインストールすることもできます。

始める前に

- 「証明書のインストールに関するガイドライン」を読みます。
- ASA は [同期（Synced）] 状態で [オンライン] である必要があります。

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

ステップ 2 単一の ASA デバイスに ID 証明書をインストールするには、次の手順を実行します。

a) [デバイス] タブをクリックします。
b) [ASA] タブをクリックして、ASA デバイスを選択します。
c) 右側の [管理] ペインで、[トラストポイント] をクリックします。
d) [Install（インストール）] をクリックします。

（注） 複数の ASA デバイスに証明書をインストールすることもできます。複数の ASA デバイスを選択し、右側の [デバイスアクション（Devices Action）] で [証明書のインストール（Install Certificate）] をクリックします。

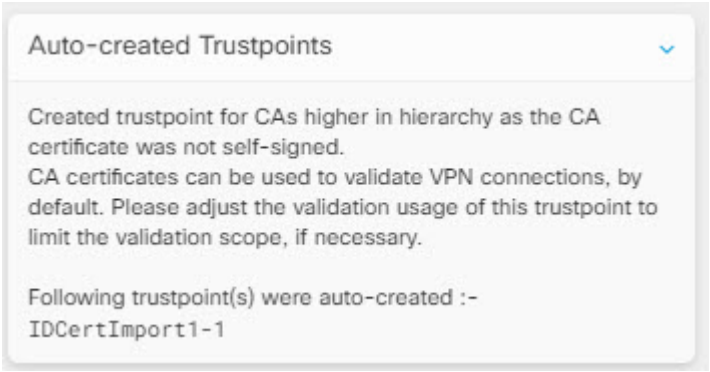
ステップ 3 [インストールするトラストポイント証明書の選択（Select Trustpoint Certificate to Install）] で、次のいずれかをクリックします。

- [作成（Create）]：新しいトラストポイント オブジェクトを追加します。詳細については、「PKCS12 を使用したID 証明書オブジェクトを追加する」を参照してください。
- [選択（Choose）]：PKCS タイプの証明書登録オブジェクトを選択します。

ステップ 4 [送信（Send）] をクリックします。

ASA デバイスに証明書がインストールされます。

（注） 中間CAがインストールされているASAにPKCS12証明書をインポートする場合、まだインストールされていないすべての中間 CA 証明書について、トラストポイント オブジェクトが自動的に作成されてデバイスにインストールされます。ID 証明書をクリックすると、次の例のようなメッセージが右側のペインに表示されます。



自己署名登録を使用した証明書のインストール

自己署名証明書用に作成された既存のトラストポイント オブジェクトを選択して、ASA デバイスにインストールできます。インストールウィザードから新しいトラストポイントオブジェクトを作成し、ASA デバイスに証明書をインストールすることもできます。

始める前に

- 証明書のインストールに関するガイドラインを読みます。
- ASA は「同期」状態で「オンライン」である必要があります。

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 単一の ASA デバイスに ID 証明書をインストールするには、次の手順を実行します。

a) [デバイス] タブをクリックします。
b) [ASA] タブをクリックして、ASA デバイスを選択します。
c) 右側の [管理（Management）] ペインで、[トラストポイント（Trustpoints）] をクリックします。
d) [Install（インストール）] をクリックします。

（注） 複数の ASA デバイスに署名付き証明書をインストールすることもできます。複数の ASA デバイスを選択し、右側の [デバイスアクション（Devices Action）] で [証明書のインストール（Install Certificate）] をクリックします。

ステップ 3 [インストールするトラストポイント証明書の選択（Select Trustpoint Certificate to Install）] で、次のいずれかをクリックします。

- [作成（Create）]：新しいトラストポイント オブジェクトを追加します。詳細については、「PKCS12 を使用したID 証明書オブジェクトを追加する」を参照してください。
- [選択（Choose）]：自己署名タイプの証明書登録オブジェクトを選択します。

ステップ 4 [送信（Send）] をクリックします。

自己署名登録タイプのトラストポイントの場合は、[発行元の共通名（Issuer Common Name ）] ステータスが常に ASA デバイスとなります。これは、管理対象デバイス自体が独自の CA として機能し、独自のID 証明書を生成するために CA 証明書を必要としないためです。

証明書署名要求（CSR）の管理

最初に CSR リクエストを生成し、信頼できる認証局（CA）によって署名されたこのリクエストを取得する必要があります。次に、CA によって発行された署名付き ID 証明書を ASA デバイスにインストールできます。

- 証明書のインストールに関するガイドラインを読みます。
- ASA は「同期」状態で「オンライン」である必要があります。

次の図は、CSR を生成し、認証された発行済み証明書を ASA にインストールするワークフローを示しています。

CSR リクエストの生成

ステップ 1 ナビゲーションバーで、[デバイスとサービス（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 [ASA] タブをクリックして、ASA デバイスを選択します。

ステップ 4 単一の ASA デバイスに ID 証明書をインストールするには、次の手順を実行します。

ステップ 5 [Install（インストール）] をクリックします。

ステップ 6 [インストールするトラストポイント証明書の選択（Select Trustpoint Certificate to Install）] で、次のいずれかをクリックします。

- [作成（Create）]：新しいトラストポイント CSR オブジェクトを追加します。詳細については、証明書署名要求（CSR）用 ID 証明書オブジェクトを追加する （153 ページ）を参照してください。
- [選択（Choose）]：作成済みの CSR リクエストトラストポイントを選択します。

ステップ 7 [送信（Send）] をクリックします。

未署名の証明書署名要求（CSR）が生成されます。

ステップ 8 コピーアイコン copy_icon.png をクリックして、CSR の詳細をコピーします。CSR リクエストは「.csr」ファイル形式でもダウンロードできます。

ステップ 9 [OK] をクリックします。

ステップ 10 証明書に署名するために、証明書署名要求（CSR）を認証局に送信します。

認証局によって発行された署名済みID 証明書のインストール

CA が署名付き証明書を発行したら、それを ASA デバイスにインストールします。

ステップ 1 [トラストポイント（Trustpoint ）] 画面で、[ステータス（Status）] が [署名付き証明書のインストールを待機中（Awaiting Signed Certificate Install）] の CSR 要求をクリックし、右側の [アクション（Actions）] ペインで [認証済みID証明書のインストール（Install Certified ID Certificate）] をクリックします。

ステップ 2 CAから受信した署名付き証明書をアップロードします。ファイルをドラッグアンドドロップするか、その内容を所定のフィールドに貼り付けることができます。トラストポイントコマンドは、選択したトラストポイントに基づいて生成されます。

ステップ 3 [送信（Send）] をクリックします。

これにより、署名付きID証明書がASAデバイスにインストールされます。証明書をインストールすると、変更がすぐにデバイスに展開されます。

（注） 複数の ASA デバイスに証明書をインストールすることもできます。複数の ASA デバイスを選択し、右側の [デバイスアクション（Devices Action）] で [証明書のインストール（Install Certificate）] をクリックします。

ASA の信頼できる証明書をインストールする

始める前に

- 証明書のインストールに関するガイドラインを読みます。
- ASA は「同期済み」状態で「オンライン」である必要があります。

ステップ 1 ナビゲーションメニューで、[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 [ASA] タブをクリックして、ASA デバイスを選択します。

ステップ 4 単一の ASA デバイスにID 証明書をインストールするには、次の手順を実行します。

a) ASA デバイスを選択し、右側の [管理] ペインで [トラストポイント] をクリックします。

b) [Install（インストール）] をクリックします。

（注） 複数の ASA デバイスに証明書をインストールすることもできます。複数の ASA デバイスを選択し、右側の [デバイスアクション] で [証明書のインストール] をクリックします。

ステップ 5 [インストールするトラストポイント証明書の選択] で、次のいずれかをクリックします。

- [作成]：新しいトラストポイント オブジェクトを追加します。詳細については、信頼できる CA 証明書オブジェクトを追加する （156 ページ）を参照してください。
- [選択] ：信頼された証明機関オブジェクトを選択します。

ステップ 6 [送信（Send）] をクリックします。

これにより、信頼できる CA ファイルが ASA デバイスにインストールされます。

ID 証明書のエクスポート

キーペアと、トラストポイントに関連付けられている発行済み証明書は、PKCS12 形式または PEM 形式でエクスポートおよびインポートできます。この形式は、異なる ASA 上のトラストポイント コンフィギュレーションを手動でコピーする場合に便利です。

手順の概要

1. ナビゲーションメニューで、[デバイスとサービス（Devices & Services）] をクリックします。
2. [デバイス] タブをクリックします。
3. [ASA] をクリックします。
4. ASA デバイスを選択し、右側の [管理] で [トラストポイント] をクリックします。
5. ID 証明書をクリックして証明書コンフィギュレーションをエクスポートします。または、検索フィールドに名前を入力することにより、証明書を検索することもできます。
6. 右側の [操作（Actions）] ペインで [証明書のエクスポート（Export Certificate）] をクリックします。
7. [PKCS12 形式（PKCS12 Format）] または [PEM 形式（PEM Format）] をクリックすることにより、証明書の形式を選択します。
8. PKCS12 ファイルをエクスポート用に暗号化するために使用する暗号化パスフレーズを入力します。
9. 暗号化パスフレーズを確認のために再入力します。
10. [エクスポート（Export）] をクリックして、証明書コンフィギュレーションをエクスポートします。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	ナビゲーションメニューで、[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	[ASA] をクリックします。	
ステップ 4	ASA デバイスを選択し、右側の [管理] で [トラストポイント] をクリックします。	
ステップ 5	ID 証明書をクリックして証明書コンフィギュレーションをエクスポートします。または、検索フィールドに名前を入力することにより、証明書を検索することもできます。	
ステップ 6	右側の [操作（Actions）] ペインで [証明書のエクスポート（Export Certificate）] をクリックします。	
ステップ 7	[PKCS12 形式（PKCS12 Format）] または [PEM 形式（PEM Format）] をクリックすることにより、証明書の形式を選択します。	
ステップ 8	PKCS12 ファイルをエクスポート用に暗号化するために使用する暗号化パスフレーズを入力します。	
ステップ 9	暗号化パスフレーズを確認のために再入力します。	

	コマンドまたはアクション	目的
ステップ 10	[エクスポート（Export）] をクリックして、証明書コンフィギュレーションをエクスポートします。	情報ダイアログボックスが表示され、証明書コンフィギュレーション ファイルが指定の場所に正常にエクスポートされたことが示されます。

インストールされた証明書の編集

インストールされている証明書の詳細オプションのみを変更できます。

ステップ 1 ナビゲーションメニューで、[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 [ASA] タブをクリックします。
ステップ 4 ASA デバイスを選択し、右側の [管理] で [トラストポイント] をクリックします。
ステップ 5 変更する証明書をクリックし、右側の [アクション] ペインで [編集] をクリックします。
ステップ 6 該当するパラメータを変更し、[保存（Save）] をクリックします。

ASA から既存証明書を削除する

証明書は 1 つずつ削除できます。証明書を削除すると、復元できなくなります。

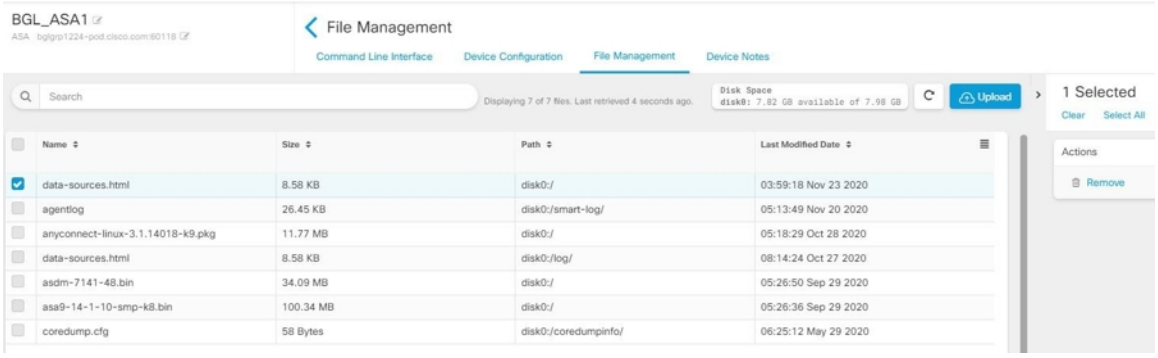
ステップ 1 ナビゲーションメニューで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 ASA デバイスを選択し、右側の [管理（Management）] で [トラストポイント（Trustpoints）] をクリックします。
ステップ 3 変更する証明書をクリックし、右側の [アクション] ペインで [削除] をクリックします。
ステップ 4 [OK] をクリックして、選択した証明書を削除します。

ASA ファイルの管理

CDO は、ASA デバイスのフラッシュ（disk0）スペースに存在するファイルの表示、アップロード、または削除などの基本的なファイル管理タスクを実行するために役立つファイル管理ツールを提供します。

（注） disk1 に存在するファイルを管理することはできません。

[ファイル管理（File Management）]画面には、デバイスのフラッシュ（disk0）に存在するすべてのファイルが一覧表示されます。ファイルのアップロードが成功したら、更新のアイコンをクリックしてファイルを表示することができます。デフォルトでは、この画面は 10 分ごとに自動的に更新されます。[ディスク容量（Disk Space）] フィールドには、disk0 ディレクトリのディスク容量が表示されます。



AnyConnect イメージは、単一または複数の ASA デバイスにアップロードできます。アップロードが成功すると、AnyConnect イメージは、選択した ASA デバイスの RA VPN 設定に関連付けられます。これにより、容易に、新しくリリースされた AnyConnect パッケージを複数の ASA デバイスに同時にアップロードできます。

フラッシュシステムへのファイルのアップロード

CDO は、リモートサーバーからの URL ベースのファイルアップロードのみをサポートしています。ファイルをアップロードするためにサポートされているプロトコルは、HTTP、HTTPS、TFTP、FTP、SMB、および SCP です。AnyConnect ソフトウェアイメージ、DAP.xml、data.xml、ホストスキャンイメージファイルなどの任意のファイルを単一または複数の ASA デバイスにアップロードできます。

（注） リモートサーバーの URL パスが無効である場合または何らかの問題が発生した問題、CDO は、選択された ASA デバイスにファイルをアップロードしません。詳細については、そのデバイスの [ワークフロー（Workflows）] に移動してください。

デバイスがハイアベイラビリティ用に設定されている場合、CDO は、まずファイルをスタンバイデバイスにアップロードし、そのアップロードが成功した後にのみ、アクティブデバイスにファイルがアップロードされます。ファイル削除プロセスでも同じ動作が適用されます。

ファイルのアップロード時にサポートされているプロトコルの構文:

プロトコル（Protocol）	構文	例
HTTP	http://[[path/]filename]	http://www.geonames.org/data-sources.html
HTTPS	https://[[path/]filename]	https://docs.aws.amazon.com/amazov/tagging.html
TFTP	tftp://[[path/]filename]	tftp://10.10.16.6/ftd/components.html

プロトコル（Protocol）	構文	例
FTP	ftp://[[user[:password]@]server[:port]/[path/]filename]	[illegible]
SMB	smb://[[path/]filename]	smb://10.10.32.145//sambashare/hello.txt
SCP	scp://[[user[:password]@]server[/path]/filename]	scp://rootcisco123@10.10.10.166//root/events_send.py

はじめる前に

- ASA デバイスからリモートサーバーにアクセスできることを確認します。
- ファイルがすでにリモートサーバーにアップロードされていることを確認します。
- ASA デバイスからそのサーバーへのネットワークルートがあることを確認します。
- URL で FQDN が使用されている場合は、DNS が設定されていることを確認します。
- リモートサーバーの URL は、認証を求めない直接リンクである必要があります。
- リモートサーバーの IP アドレスが NAT 処理されている場合は、リモートサーバーのロケーションの NAT 処理済みパブリック IP アドレスを指定する必要があります。

（注） フェールオーバーでピアとして設定されている ASA にファイルをアップロードすると、CDO はフェールオーバーペアの他のピアの新しいファイルを確認せず、デバイスのステータスは **[未同期（Not Synced）]** に変わります。CDO が両方のデバイスのファイルを認識できるようにするには、変更を**両方**のデバイスに手動で展開する必要があります。

単一の ASA デバイスへのファイルのアップロード

単一の ASA デバイスにファイルをアップロードするには、こ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 [ASA] タブをクリックして、ASA デバイスを選択します。

ステップ 4 右側の [管理] ペインで、[ファイル管理（File Management）] をクリックします。使用可能なディスクスペースと ASA デバイスに存在するファイルが表示されます。

ステップ 5 右側の [アップロード] ボタンをクリックします。

ステップ 6 **URL リンク**で、ファイルが事前にアップロードされているサーバーのパスを指定します。[接続先パス（Destination Path）] フィールドには、**disk0** ディレクトリにアップロードされるファイルの名前が表示されます。disk0 内の特定のディレクトリにファイルをアップロードする場合は、このフィールドでその名前を指定します。たとえば、dap.xml ファイルを「DAPFiles」ディレクトリにアップロードする場合は、フィールドで「**disk0:/**DAPFiles/dap.xml」と指定します。

（注） CDO ASA CLI インターフェイスで **dir** コマンドを実行すると、disk0 フォルダに存在するディレクトリが表示されます。

ステップ 7 指定したサーバーパスが AnyConnect ファイルを指している場合、[ファイルを RA VPN 設定に関連付ける（Associate file with RA VPN Configuration）] チェックボックスがオンになります。**注**：このチェック ボックスは、正しい命名規則（「anyconnect-win-xxx.pkg」、「anyconnect-linux-xxx.pkg」、または「anyconnect-mac-xxx.pkg」形式）に従う AnyConnect ファイル名に対してのみ有効です。このチェックボックスを選択すると、アップロードが成功した後、CDO は AnyConnect ファイルを選択した ASA デバイスの RA VPN 設定に関連付けます。

ステップ 8 [アップロード（Upload）] をクリックします。CDO がファイルをデバイスにアップロードします。

ステップ 9 手順 5 で AnyConnect パッケージの RA VPN 設定との関連付けを選択した場合は、CDO から ASA に設定変更を展開します。。

次のタスク

設定の変更をデバイスに展開する必要はありません。

複数の ASA デバイスへのファイルのアップロード

複数の ASA デバイスにファイルを同時にアップロードするには、こ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 [ASA] タブをクリックし、複数の ASA デバイスを選択して一括アップロードを実行します。

ステップ 4 右側の [デバイスアクション] ペインで、[ファイルのアップロード（Upload File）] をクリックします。注：[ファイルのアップロード（Upload File）] リンクは、ASA デバイスがオンラインの場合に表示されます。

ステップ 5 [URL リンク（URL link）]で、ファイルが事前にアップロードされているサーバーのパスを指定します。[接続先パス（Destination Path）] フィールドには、**disk0** ディレクトリにアップロードされるファイルの名前が表示されます。disk0 内の特定のディレクトリにファイルをアップロードする場合は、このフィールドでその名前を指定します。たとえば、dap.xml ファイルを「DAPFiles」ディレクトリにアップロードする場合は、フィールドで「**disk0:**/DAPFiles/dap.xml」と指定します。

（注） CDO ASA CLI インターフェイスで **dir** コマンドを実行すると、disk0 フォルダに存在するディレクトリが表示されます。

ステップ 6 指定したサーバーパスが AnyConnect ファイルを指している場合、[ファイルをRA VPN設定に関連付ける（Associate file with RA VPN Configuration）] チェックボックスがオンになります。

（注） このチェック ボックスは、正しい命名規則（「anyconnect-win-xxx.pkg」、「anyconnect-linux-xxx.pkg」、または「anyconnect-mac-xxx.pkg」形式）に従う AnyConnect ファイル名に対してのみ有効です。このチェックボックスを選択すると、アップロードが成功した後、CDO は AnyConnect ファイルを選択した ASA デバイスの RA VPN 設定に関連付けます。

ステップ 7 [アップロード（Upload）] をクリックします。

ステップ 8 手順 4 で AnyConnect パッケージの RA VPN 設定との関連付けを選択した場合は、CDO から ASA に設定変更を展開します。。

次のタスク

個々のデバイスのファイルのアップロードの進行状況を表示できます。ASA デバイスを選択し、右側の [管理] ペインで [ファイル管理（File Management）] をクリックします。ファイルのアップロードが進行中の場合は、操作が完了するまで待ちます。

設定の変更をデバイスに展開する必要はありません。

ASA からのファイルの削除

RA VPN 設定に関連付けられた AnyConnect ファイルを削除することはできません。対応する RA VPN 設定から AnyConnect ファイルの関連付けを解除してから、ファイル管理ツールからファイルを削除する必要があります。

（注） フェールオーバーでピアとして設定されている ASA にファイルをアップロードすると、CDO はフェールオーバーペアの他のピアの新しいファイルを確認せず、デバイスのステータスは **[未同期（Not Synced）]** に変わります。CDO が両方のデバイスのファイルを認識できるようにするには、変更を**両方**のデバイスに手動で展開する必要があります。

remove の操作は、選択したファイルをフラッシュメモリから完全に削除します。ファイルの削除時に確認を求めるメッセージが表示されます。選択した ASA デバイスからファイルを削除するには、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 [ASA] タブをクリックして、ASA デバイスを選択します。

ステップ 4 右側の [管理] ペインで、[ファイル管理（File Management）] をクリックします。

ステップ 5 削除するファイルを選択し、右側の [アクション] で [削除] をクリックします。最大 25 個のファイルを選択できます。CDO が一部のファイルの削除に失敗した場合は、デバイスの**ワークフロー**を表示して、削除されたファイルと保持されたファイルを確認できます。

ステップ 6 AnyConnect パッケージの削除を選択した場合は、CDO から ASA に設定変更を展開します。。

ASA の高可用性を管理する

アクティブ-アクティブ フェールオーバー モードの ASA に加えられた設定変更

Cisco Defense Orchestrator（CDO）が ASA の実行構成を CDO でステージングされた構成で変更する場合、または CDO の構成を ASA に保存されている構成で変更する場合、CDO は、設定の変更部分が CDO GUI で管理可能な場合、構成ファイルの関連する行のみを変更しようとします。CDO GUI を使用して目的の構成変更を行うことができない場合、CDO は構成ファイル全体を上書きして変更を加えようとします。

2 つの例を示します。

- ネットワークオブジェクトは、CDO GUI を使用して作成または変更が可能です。CDO がその変更を ASA の設定に展開する必要がある場合、変更が発生したときに ASA の実行構成ファイルの関連する行が上書きされます。
- CDO GUI を使用して新しい ASA ユーザーを作成することはできません。ASA の ASDM または CLI を使用して新しいユーザーが ASA に追加された場合、そのアウトオブバンド変更が受け入れられ、CDO が保存されているコンフィギュレーション ファイルを更新すると、CDO は CDO にステージングされているその ASA のコンフィギュレーション ファイル全体を上書きしようとします。

ASA がアクティブ-アクティブ フェールオーバー モードで設定されている場合、これらのルールは適用されません。CDO がアクティブ-アクティブ フェールオーバー モードで設定された ASA を管理する場合、CDO は常に、すべての設定変更をそれ自体から ASA に展開したり、すべての設定変更を ASA からそれ自体に読み込むとは限りません。これに該当する 2 つの例を次に示します。

- CDO が CDO GUI でサポートしていない、CDO で行われた ASA の設定ファイルへの変更は、ASA に展開できません。また、CDO がサポートしていない設定ファイルに加えられた変更と、CDO がサポートしている設定ファイルに加えられた変更の組み合わせは、ASA に展開できません。どちらの場合も、「CDO は現時点でフェールオーバーモードのデバイスの完全な構成の置き換えをサポートしていません。[キャンセル]をクリックして、デバイスに手動で変更を適用してください。」というエラーメッセージを受け取ります。CDO インターフェイスのメッセージとともに、無効になっている [構成の置換（Replace Configuration）] ボタンが表示されます。
- アクティブ-アクティブ フェールオーバー モードで設定された ASA に加えられたアウトオブバンド変更は、CDO によって拒否されません。ASA の実行構成にアウトオブバンド変更を加えると、ASA は[デバイスとサービス]ページで「競合が検出されました（Conflict Detected）」とマークされます。競合を確認して拒否しようとすると、CDO はそのアクションをブロックします。「CDO は、このデバイスのアウトオブバンド変更の拒否をサポートしていません。このデバイスは、サポートされていないソフトウェアバージョンを実行しているか、アクティブ/アクティブ フェールオーバー ペアのメンバーです。[続行]

をクリックして、アウトオブバンド変更を受け入れてください。」というエラーメッセージを受け取ります。

⚠

注意 ASA からのアウトオブバンド変更を受け入れることにした場合、CDO でステージングされていて、まだ ASA に展開されていない設定変更はすべて上書きされ、失われます。

変更が CDO GUI でサポートされている場合、CDO は、フェールオーバーモードの ASA に加えられた設定変更をサポートします。

関連情報：

ASA での DNS の設定

次の手順を使用して、各 ASA でドメインネームサーバー（DNS）を設定します。

前提条件

- ASA はインターネットにアクセスできる必要があります。
- 開始する前に、次の情報を収集します。
  - DNS サーバーに到達できる ASA インターフェイスの名前。たとえば、inside、outside、dmz。
  - 組織で使用する DNS サーバーの IP アドレス。独自の DNS サーバーを保持していない場合は、Cisco Umbrella を使用できます。Cisco Umbrella の IP アドレスは 208.67.220.220 です。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス] 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 [ASA] タブをクリックし、DNS を設定するすべての ASA を選択します。
ステップ 4 右側の操作ウィンドウで、[コマンド ライン インターフェイス] を選択します。
ステップ 5 CLI マクロのお気に入りの星をクリックします。
ステップ 6 [マクロ] パネルで [DNSの設定] マクロを選択します。
ステップ 7 [>_パラメータを表示] を選択し、パラメータ列に以下のパラメータの値を入力します。

- IF_Name：DNS サーバーに到達できる ASA インターフェイスの名前。
- IP_ADDR： 組織で使用する DNS サーバーの IP アドレス。

ステップ 8 [デバイスに送信] をクリックします。

CDO コマンド ライン インターフェイスを使用する

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

関連情報：

- 詳細な ASA CLI ドキュメントについては、ASA コマンド ライン インターフェイスのドキュメント （105 ページ） を参照してください。

コマンドの入力方法

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

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

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

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

このエラーメッセージを受信した場合、次の手順を実行します。

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

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

ステップ 3 [送信（Send）] をクリックします。

単一デバイスで CLI を使用する

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、デバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 コマンド ライン インターフェイスを使用して、管理するデバイスを選択します。

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

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

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

コマンド履歴での動作

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

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

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

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

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

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

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

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

- 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。

ASA デバイスの構成

ASA など、一部のタイプのデバイスは、構成を 1 つの構成ファイルに保存します。 これらのデバイスの場合、Cisco Defense Orchestrator でデバイス構成ファイルを表示し、デバイスに応じてさまざまな操作を実行できます。

デバイスの構成ファイルを表示する

ASA、Cisco Secure Firewall Cloud Native、SSH 管理対象デバイス、Cisco IOS を実行しているデバイスなど、構成全体を 1 つの構成ファイルに保存するデバイスの場合、CDO を使用して構成ファイルを表示できます。

（注） SSH 管理対象デバイスと Cisco IOS デバイスには読み取り専用の設定があります。

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（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 設定を表示するデバイスまたはモデルを選択します。

ステップ 5 右側の [管理（Management] ペインで、[設定（Configuration）] をクリックします。
完全な構成ファイルが表示されます。

関連情報：

- 完全なデバイス設定ファイルの編集

完全なデバイス設定ファイルの編集

ASA など、一部のタイプのデバイスは、設定を1つの構成ファイルに保存します。これらのデバイスの場合、CDO でデバイス構成ファイルを表示し、デバイスに応じてさまざまな操作を実行できます。

現在、CDO を使用して直接編集できるのは構成ファイルのみです。ASA

⚠

注意 この手順は、デバイスの構成ファイルのシンタックスに精通している上級ユーザーを対象としています。この手法では、Defense Orchestrator に保存されている構成ファイルのコピーに直接変更を加えます。

手順

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

ステップ 4 構成を編集するデバイスを選択します。

ステップ 5 右側の [管理] ペインで、[構成] をクリックします。

ステップ 6 [デバイスの構成] ページで、[編集] をクリックします。

ステップ 7 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 8 ファイルを編集し、変更を保存します。

ステップ 9 [デバイスとサービス] ページに戻り、変更をプレビューして展開します。

ASA 構成の比較

2 つの ASA の構成を比較するには、次の手順を実行します。

ステップ 1 ナビゲーションメニューで、[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 ASA 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 ASA モデルデバイスを見つけます。

ステップ 3 [ASA] タブをクリックします。

ステップ 4 比較するデバイスを見つけるためにデバイスリストをフィルタ処理します。

ステップ 5 2 つの ASA を選択します。それらのステータスは重要ではありません。Defense Orchestrator に保存されている ASA の構成を比較しようとしています。

ステップ 6 右側の [デバイスアクション] ペインで、[比較] をクリックします。

ステップ 7 [構成の比較（Comparing Configurations）] ダイアログで、[次へ] および [前へ（Previous）] をクリックして、構成ファイル内の青色で強調表示されている相違点をスキップします。

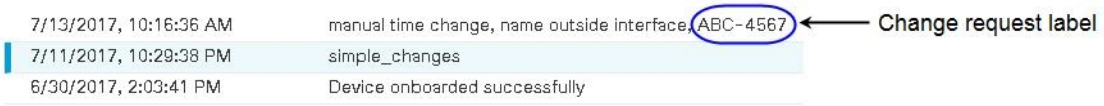
ASA 設定の復元

この手順では、Cisco Defense Orchestrator（CDO）を使用して ASA に行った設定変更を復元する方法について説明します。これは、予期しない結果や望ましくない結果をもたらした設定変更を削除する便利な方法です。

設定を復元する前に

設定を復元する前に、次の注意事項を確認してください。

- CDO は、復元することを選択した設定を、ASA に展開されている最後に認識された設定と比較します。ステージングされているが ASA のメモリに展開されていない設定とは比較しません。ASA に展開されていない変更がある場合に、以前の設定を復元すると、展開されていない変更は、復元プロセスによって上書きされて失われます。
- 過去の設定を復元すると、それまでに展開されたすべての設定変更が上書きされます。たとえば、以下のリストにある 2017 年 7 月 11 日の設定を復元すると、2017 年 7 月 13 日に行われた設定変更が上書きされます。



- 設定変更に最初に適用した変更リクエストラベルは、[設定の復元（Restore Configuration）] リストに表示されます。
- ASA は [同期（Synced）] または [非同期] の状態になっている可能性があるため、過去の設定を復元する前に、設定の競合を解決する必要があります。

設定の復元方法

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 [ASA] タブをクリックします。

ステップ 4 設定を復元する ASA を選択します。

ステップ 5 右側のペインで **[設定（Configuration）]** > **[設定の復元（Restore Configuration）]** を選択します。

ステップ 6 [設定の復元（Restore Configuration）]ペインで、復元する設定を選択します。たとえば、上の図では、2017 年 7 月 11 日の設定が選択され、強調表示されています。

ステップ 7 「CDO によって検証された最新の実行設定」と「*<date>* から選択された設定」を比較して、[<date> から選択された設定（Selected Configuration from *<date>*）] ウィンドウに表示されている設定を復元することを確認します。

ステップ 8 [復元（Restore）]をクリックします。これにより、CDO の設定がステージングされます。[デバイスとサービス] ページに、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 9 右側のペインで [変更の展開 ...（Deploy Changes...）] をクリックして変更を展開し、ASA を同期させます。

トラブルシューティング

保持したかったのに失ってしまった変更を回復するには、どうすればよいですか。

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 [ASA] タブをクリックします。

ステップ 4 必要なデバイスを選択します。

ステップ 5 右側のペインで [変更ログ] をクリックします。

ステップ 6 変更ログで変更を確認します。それらの記録から、失われた構成を再構築できる可能性があります。

CLI を使用した ASA の設定

CDO で提供される CLI インターフェイスで CLI コマンドを実行して、ASA デバイスを設定できます。このインターフェイスを使用するには、[デバイスとサービス] メニューでデバイスを選択し、[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。詳細については、「CDO コマンド ライン インターフェイスの使用」を参照してください。

新しいロギングサーバーの追加

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央 syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。

詳細については、実行している ASA バージョンの『CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide』に含まれる「Logging」の章にある「Monitoring」セクションを参照してください。

DNS サーバーの設定

DNS サーバーを設定して、ASA がホスト名を IP アドレスに解決できるようにする必要があります。また、アクセスルールに完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを使用するように、DNS サーバーを設定する必要があります。

詳細については、実行している ASA バージョンの『CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide』に含まれる「Basic Settings」の章の「Configure the DNS Server」セクションを参照してください。

静的ルートとデフォルトルートの追加

接続されていないホストまたはネットワークにトラフィックをルーティングするには、スタティックルーティングとダイナミックルーティングのどちらかを使用して、ホストまたはネットワークへのルートを定義する必要があります。

詳細については、『CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide』の「Static and Default Routes」の章を参照してください。

インターフェイスの設定

CLI コマンドを使用して、管理インターフェイスとデータインターフェイスを設定できます。詳細については、『CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide』の「Basic Interface Configuration」の章を参照してください。

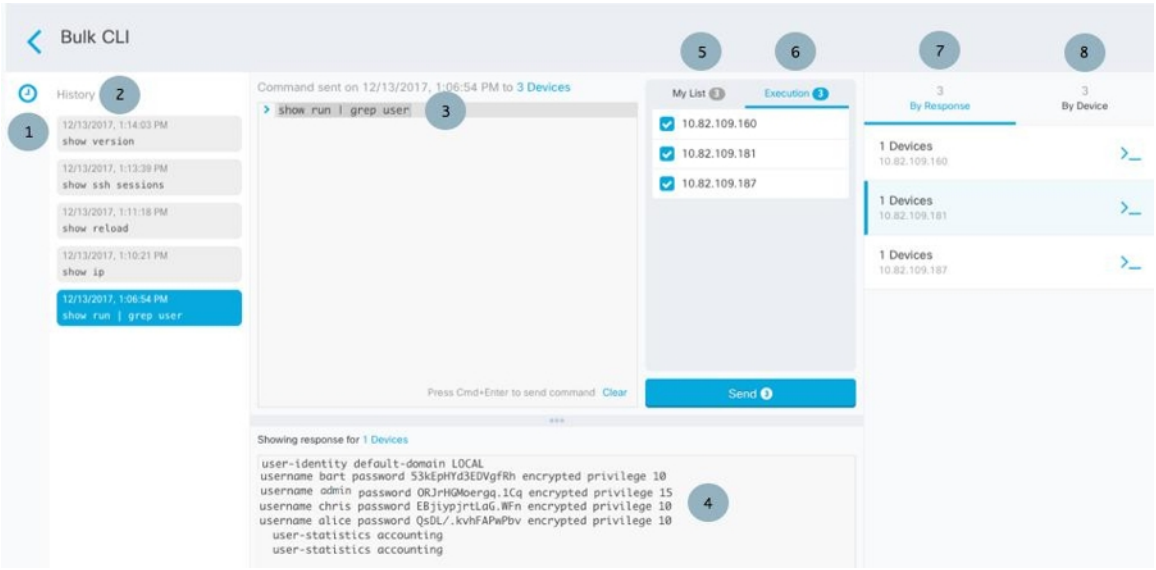
一括コマンド ライン インターフェイス

CDO では、コマンド ライン インターフェイス（CLI）を使用して ASA 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：

- 詳細な ASA CLI のドキュメントについては、ASA コマンド ライン インターフェイスのドキュメント （105 ページ）を参照してくださ
- 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	応答ペイン。CDO は、コマンドに対するデバイスの応答と CDO メッセージを表示します。複数のデバイスの応答が同じだった場合、応答ペインに「X デバイスの応答を表示しています（Showing Responses for X devices）」というメッセージが表示されます。[Xデバイス（X Devices）] をクリックすると、コマンドに対して同じ応答を返したすべてのデバイスが CDO に表示されます。 （注） 次の 2 つの状況で「**完了しました（Done!）**」というメッセージが CDO に表示されます。 • 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。
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。ASA デバイスが同期されていない場合、そのデバイスで使用可能なコマンドは、`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、`dir`、`write`、`copy` だけです。

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。

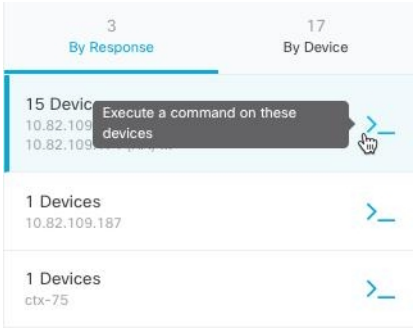
（注） 選択したデバイスのいずれかが同期されていない場合、次のコマンドのみが許可されます：`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、`dir`、`write`、`copy`

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。

ASA一括 CLI の使用例

次の例は、ASA デバイスに対して CDO の一括 CLI 機能を使用するときに発生する可能性のあるワークフローです。

ASA の実行構成ですべてのユーザーを表示し、いずれかのユーザーを削除する

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 [ASA] タブをクリックします。

ステップ 4 ユーザーを削除するデバイスのデバイスリストを検索およびフィルタ処理し、デバイスを選択します。

（注） 選択したデバイスが同期されていることを確認してください。デバイスが同期されていない場合、次のコマンドのみが許可されます。`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、`dir`、`copy`、および `write`。

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。CDO は、[マイリスト] ペインで選択したデバイスを一覧表示します。少数のデバイスにコマンドを送信する場合は、そのリストにあるデバイスのチェックを外します。

ステップ 6 コマンドペインで、`show run | grep user` と入力し、[送信（Send）] をクリックします。文字列 user を含む実行構成ファイルのすべての行が、応答ペインに表示されます。[実行（Execution）] タブが開き、コマンドが実行されたデバイスが表示されます。

ステップ 7 [応答別（By Response）] タブをクリックし、応答を確認して、削除するユーザーが含まれているデバイスを確認します。

ステップ 8 [マイリスト] タブをクリックし、ユーザーを削除するデバイスのリストを選択します。

ステップ 9 コマンドペインで、user コマンドの no 形式を入力して user2 を削除し、[送信（Send）] をクリックします。この例では、user2 を削除します。

```
no user user2 password reallyhardpassword privilege 10
```

ステップ 10 ユーザー名の検索に使用した、`show run | grep user` コマンドのインスタンスの履歴パネルを確認します。このコマンドを選択し、[実行（Execution）] リストでデバイスのリストを確認して、[送信（Send）] を選択します。指定したデバイスからユーザー名が削除されたことがわかります。

ステップ 11 実行構成から正しいユーザーを削除し、実行構成に残っているユーザーが正しいことを確認したら、次の手順を実行します。

1. 履歴ペインから `no user user2 password reallyhardpassword privilege 10` コマンドを選択します。
2. [デバイス別（By Device）] タブをクリックし、[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。
3. コマンドペインで、[クリア] をクリックしてコマンドペインをクリアします。
4. `deploy memory` コマンドを入力し、[送信（Send）] をクリックします。

選択した ASA 上のすべての SNMP 設定を見つける

この手順で、ASA の実行構成にあるすべての SNMP 構成エントリを表示できます。

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 [ASA] タブをクリックします。

ステップ 4 実行構成の SNMP 構成を分析するデバイスをフィルタ処理して検索し、それらを**選択**します。

（注） 選択したデバイスが同期されていることを確認してください。デバイスが同期されていない場合、次のコマンドのみが許可されます。`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、および `dir`。

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] をクリックします。選択したデバイスは [マイリスト] ペインに表示されます。少数のデバイスにコマンドを送信する場合は、そのリストにあるデバイスのチェックを外します。

ステップ 6 コマンドペインで、`show run | grep snmp` と入力し、[送信] をクリックします。文字列 snmp を含む実行構成ファイルのすべての行が、応答ペインに表示されます。[実行] タブが開き、コマンドが実行されたデバイスが表示されます。

ステップ 7 応答ペインでコマンド出力を確認します。

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 ASA 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。ASA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）
- 詳細な ASA CLI ドキュメントについては、ASA コマンドライン インターフェイスのドキュメント （105 ページ） を参照してください。

ステップ 2 ナビゲーションバーで、[デバイスとサービス] 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 マクロに一意の名前を指定します。必要に応じて、CLI マクロの説明とメモを入力します。

ステップ 8 [コマンド] 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。

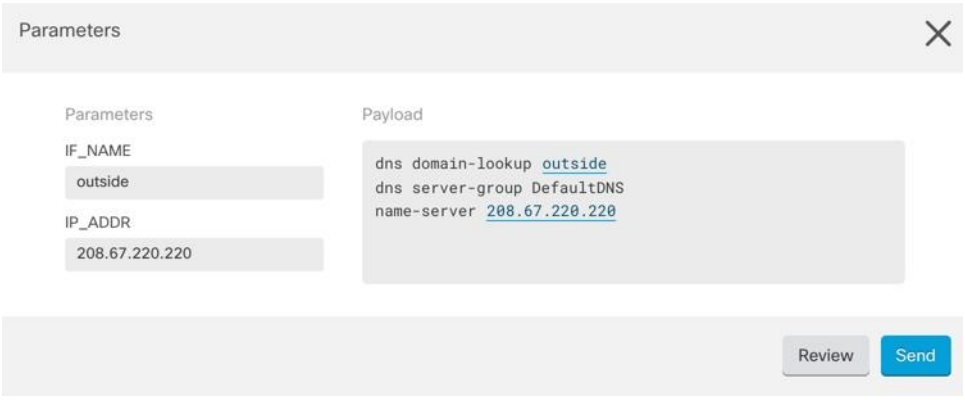
ステップ 5 コマンドパネルで、スター をクリックします。

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。

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



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

- ASA の場合は、実行構成が更新されます。

ステップ 10 コマンドを送信した後で、「一部のコマンドが実行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。

- [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 ASA 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。

ASA コマンド ライン インターフェイスのドキュメント

CDO は、ASA コマンドラインインターフェイスをすべてサポートしています。ユーザーが単一のデバイスおよび複数のデバイスに同時にコマンドを送信できるように、CDO ではターミナル型のインターフェイスを提供しています。ASA コマンドラインインターフェイスのドキュメントは豊富です。CDO ドキュメントでその一部を再作成するのではなく、Cisco.com の ASA CLI ドキュメントへのポインタを次に示します。

ASA CLI コンフィギュレーション ガイド

ASA バージョン 9.1 以降、ASA CLI コンフィギュレーション ガイドは 3 部に分かれています。

- CLI ブック 1：Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）
- CLI ブック 2: Cisco ASA シリーズ ファイアウォール CLI コンフィグレーションガイド
- CLI ブック 3：Cisco ASA シリーズ VPN CLI コンフィギュレーション ガイド

[サポート（Support）] > [製品カテゴリ（Products by Category）] > [セキュリティ（Security）] >[ファイアウォール（Firewalls）] > [ASA 5500] > [コンフィギュレーション（Configure）] > [コンフィギュレーションガイド（Configuration Guides）] に移動すると、Cisco.com の ASA CLI コンフィギュレーション ガイドにアクセスできます。https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

いくつかの特定の ASA CLI コンフィギュレーション ガイドのセクション

show コマンドと more コマンドの出力のフィルタリングCLI ブック 1：『Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）』の「show コマンドと more コマンドの出力のフィルタリング」では、正規表現を使用した show コマンド出力のフィルタ処理について学習できます。

ASA コマンドリファレンス

ASA コマンド リファレンス ガイドは、すべての ASA コマンドとそのオプションがアルファベット順でリストになっています。ASA コマンドリファレンスはバージョン固有ではありません。次の 4 部が公開されています。

- Cisco ASA シリーズ コマンド リファレンス、A ～ H コマンド
- Cisco ASA シリーズ コマンド リファレンス、I ～ R コマンド
- Cisco ASA シリーズ コマンド リファレンス、S コマンド

- Cisco ASA シリーズ コマンド リファレンス、T ～ Z コマンドおよび ASASM 用 IOS コマンド

[サポート（Support）] > [製品カテゴリ（Products by Category）] > [セキュリティ（Security）] > [ファイアウォール（Firewalls）] > [ASA 5500] > [リファレンスガイド（Reference Guides）] > [コマンドリファレンス（Command References）] に移動すると、Cisco.com の ASA コマンドリファレンスガイドにアクセスできます。https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html#anchor325

CLI コマンドの結果のエクスポート

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

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

CLI コマンドの結果のエクスポート

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

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

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 1 つまたは複数のデバイスを選択してハイライトします。

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

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

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

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

CLI マクロの結果のエクスポート

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

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ます。

ステップ 4 1 つまたは複数のデバイスを選択してハイライトします。

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

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

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

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

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

CLI コマンド履歴のエクスポート

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

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] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 1 つまたは複数のデバイスを選択してハイライトします。

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

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

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

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

関連情報：

- CDO コマンド ライン インターフェイスを使用する （88 ページ）

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

CLI マクロのリストをエクスポートする

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

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] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
ステップ 3 適切なデバイスタイプのタブをクリックします。
ステップ 4 1 つまたは複数のデバイスを選択してハイライトします。
ステップ 5 デバイスの [デバイスアクション] ペインで、[>_コマンド ライン インターフェイス] をクリックします。
ステップ 6 CLI ウィンドウの左側のペインで、CLI マクロのお気に入りを示す星を選択します。
ステップ 7 エクスポートするマクロコマンドをクリックします。適切なパラメータを入力し、[送信] をクリックします。
ステップ 8 入力されたコマンドのウィンドウの右側でエクスポートアイコン をクリックします。
ステップ 9 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。

変更の読み取り、破棄、チェック、および展開

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

- [変更の破棄（Discard Changes）] は、デバイスの設定ステータスが「未同期」の場合に使用できます。未同期の状態では、デバイスの設定に対する変更が CDO で保留中になっています。このオプションを使用すると、保留中のすべての変更を取り消すことができま

す。保留中の変更は削除され、CDO は設定のコピーをデバイスに保存されている設定のコピーで上書きします。

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

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

変更の配置

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

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

（注） 展開や繰り返しの展開をスケジュールできます。詳細については、自動展開のスケジュール（315 ページ）を参照してください。

[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）] をクリックしすると、CDO はすぐにデバイスをチェックして、設定に直接変更が加えられているかどうかを判断します。[すべて読み取り（Read All）] をクリックすると、CDO はデバイスの設定のコピーを上書きすることを確認し、上書きを実行します。
- [非同期]：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（318 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 （336 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

ASA から CDO への設定変更の読み取り

Cisco Defense Orchestrator が ASA の設定を「読み取る」理由

ASA を管理するために、CDO には、ASA の実行構成ファイルの独自のコピーが保存されている必要があります。CDO が最初にデバイスの構成ファイル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。その後、CDO が ASA から設定を読み取るときに、[変更の確認（Check for Changes）]、[レビューなしで承認（Accept Without Review）]、または [設定の読み取り（Read Configuration）] のいずれかを選択します。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。

CDO は、次の状況でも ASA の設定を読み取る必要があります。

- ASA への設定変更の展開に失敗し、デバイスの状態がリストにないか、[非同期] になっている場合。
- デバイスの導入準備が失敗し、デバイスの状態が [設定なし（No Config）] になっている場合。
- CDO の外部でデバイス設定を変更したが、その変更はポーリングまたは検出されていないため、デバイスの状態が [同期（Synced）] または [競合検出（Conflict Detected）] になっている場合。

このような場合、CDO は、デバイスに保存されている最後に認識された設定のコピーを必要とします。

ASA での構成変更の読み取り

ASA での構成変更の読み取りが求められたら、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 CDO が最近導入準備に失敗したデバイス、または CDO が変更の展開に失敗したデバイスを選択します。
ステップ 5 右側の [同期済み] ペインで [構成の読み取り（Read Configuration）] をクリックします。このオプションを実行すると、現在 CDO に保存されている構成が上書きされます。

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
- CDO から ASA に設定変更を展開します。 （309 ページ）
- ASA に展開後の変更ログエントリ （327 ページ）

CDO から ASA に設定変更を展開します。

CDO が ASA に変更を展開する理由

Cisco Defense Orchestrator（CDO）を使用してデバイスの設定を管理および変更すると、加えた変更が CDO により構成ファイルの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「ステージング」されたと見なされます。ステージングされた設定変更は、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。CDO がデバイスに変更を「展開」した後にのみ、デバイスを通過するトラフィックに影響を与えます。

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。

ASA には、「実行構成」とも呼ばれる「実行」構成ファイルと、「スタートアップ コンフィギュレーション」とも呼ばれる「起動」構成ファイルがあります。実行コンフィグレーションファイルに保存されている構成は、ASA を通過するトラフィックに適用されます。実行コンフィグレーションに変更を加え、それらの変更がもたらす動作に問題がないことを確認したら、それらをスタートアップ コンフィギュレーションに展開できます。ASA が再起動されるたびに、スタートアップコンフィギュレーションが構成の開始点として使用されます。実行コンフィギュレーシに加えた変更で、スタートアップコンフィギュレーションに保存されていないものは、ASA の再起動後にすべて失われます。

CDO から ASA に変更を展開すると、それらの変更が実行構成ファイルに書き込まれます。これらの変更によってもたらされる動作に問題がなければ、それらの変更をスタートアップ コンフィギュレーション ファイルに展開できます。

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。単一のデバイスに対して、個別の展開や繰り返しの展開をスケジュールできます。

一部の変更は ASA に直接展開される

CDO で CDO コマンド ライン インターフェイスを使用する デバイスの管理用 CLI マクロを使用して ASA に変更を加えた場合、それらの変更は CDO で「ステージング」されません。それらは、ASA の実行構成に直接展開されます。このように変更を加えると、デバイスは CDO と「同期」状態が維持されます。

設定変更の展開について

このセクションでは、ASA 構成ファイルを変更するために、CDO の CLI インターフェイスまたは CLI マクロインターフェイスを使用せずに、CDO の GUI を使用しているか、[デバイス設定（Device Configuration）] ページを編集していることを前提としています。

ASA 設定の更新は、2 段階のプロセスです。

ステップ 1 次のいずれかの方法を使用して、CDO で変更を加えます。

- CDO GUI
- [デバイス設定（Device Configuration）] ページのデバイス設定

ステップ 2 変更を加えたら、[デバイスとサービス] ページに戻り、[プレビューと展開（Preview and Deploy...）] でデバイスへの変更をプレビューして展開します。

次のタスク

CDO が ASA の実行構成を CDO でステージングされた設定で更新する場合、または ASA に保存されている実行構成で CDO 上の設定を変更する場合、CDO は、設定の変更部分が CDO GUI で管理可能な場合、構成ファイルの関連する行のみを変更しようとします。CDO GUI を使用して目的の構成変更を行うことができない場合、CDO は構成ファイル全体を上書きして変更を加えようとします。

2 つの例を示します。

- ネットワークオブジェクトは、CDO GUI を使用して作成または変更が可能です。CDO がその変更を ASA の設定に展開する必要がある場合、変更が発生したときに ASA の実行構成ファイルの関連する行が上書きされます。
- 新しいローカル ASA ユーザーは CDO GUI を使用して作成することはできませんが、[デバイスの設定（Device Configuration）] ページで ASA の設定を編集することで作成できます。[デバイスの設定（Device Configuration）] ページでユーザーを追加し、その変更を ASA に展開すると、CDO は実行構成ファイル全体を上書きして、その変更を ASA の実行構成ファイルに保存しようとします。

CDO GUIを使用して行った設定変更の展開

ステップ 1 CDO GUI を使用して構成を変更し、変更を保存すると、その変更は CDO に保存されたバージョンの ASA の実行構成ファイルに保存されます。

ステップ 2 [デバイスとサービス] ページでデバイスに戻ります。

ステップ 3 [デバイス]_タブをクリックします。デバイスが「未同期」になっていることがわかります。

ステップ 4 次のいずれかの方法を使用して、変更を展開します。

- 画面右上の [展開（Deploy）] アイコン をクリックします。これにより、デバイスに加えた変更を展開する前に確認することができます。変更を加えたデバイスを確認し、デバイスを展開して変更を確認し、[今すぐ展開（Deploy Now）] をクリックして変更を展開します。

  （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、変更を展開することはできません。警告の三角形にマウスを合わせると、デバイスに変更を展開できない理由が表示されます。

- [未同期（Not Synced）] ウィンドウで、[プレビューして展開...（Preview and Deploy...）] をクリックします。

  1. ASA コンフィギュレーション ファイルを変更するコマンドを確認します。
  2. コマンドに問題がない場合は、[リカバリプリファレンスの設定（Configuration Recovery Preference）] を選択します。

     （注） [通知を受け取り、設定を手動で復元します。（Let me know and I will restore the configuration manually）] を選択した場合、続行する前に、[手動同期手順の表示（View Manual Synchronization Instructions）] をクリックします。

3. [デバイスに変更を適用する（Apply Changes to Device）] をクリックします。
4. [OK] をクリックして成功メッセージを確認します。

自動展開をスケジュール設定する

自動展開のスケジュールことにより、単一のデバイスまたは保留中の変更があるすべてのデバイスへの展開をスケジュールするようにテナントを設定することもできます。

CDO の CLI インターフェイスを使用した設定変更の展開

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 設定を編集するデバイスを選択します。

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

ステップ 6 コマンド ライン インターフェイス テーブルにコマンドがある場合は、[クリア] をクリックしてそれらを削除します。

ステップ 7 コマンドラインインターフェイスの表の上部のボックスにあるコマンドプロンプトに、コマンドを入力します。各コマンドを個別の行に入力するか、構成ファイルのセクションをコマンドとして入力することにより、1 つのコマンドを実行したり、複数のコマンドを一括で実行したりできます。コマンド ライン インターフェイス テーブルに入力できるコマンドの例を次に示します。

ネットワークオブジェクト「albany」を作成する単一のコマンド

```
object network albany
host 209.165.30.2
```

一緒に送信される複数のコマンド：

```
object network albany
host 209.165.30.2
object network boston
host 209.165.40.2
object network cambridge
host 209.165.50.2
```

コマンドとして入力された実行構成ファイルのセクション：

```
interface GigabitEthernet0/5
 nameif guest
 security-level 0
 no ip address
```

（注） CDO では、EXEC モード、特権 EXEC モード、およびグローバル コンフィギュレーション モードの間を移動する必要はありません。入力したコマンドは適切なコンテキストで解釈されます。

ステップ 8 コマンドを入力したら、[送信（Send）] をクリックします。CDO が ASA の実行中の構成ファイルへの変更を正常に展開すると、[完了（Done!）] というメッセージが表示されます。

ステップ 9 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。

- [ディスクに展開（Deploy 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、ASA 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。

デバイス設定の編集による設定変更の展開

注意 この手順は、ASA 設定ファイルの構文に精通している上級ユーザーを対象としています。この手法では、CDO に保存されている実行設定ファイルに直接変更を加えます。

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] 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 設定を編集するデバイスを選択します。

ステップ 5 [アクション] ペインで、[設定の表示（View Configuration）] をクリックします。

ステップ 6 [編集（Edit）] をクリックします。

ステップ 7 実行中の設定に変更を加えて**保存**します。

ステップ 8 [デバイスとサービス（Devices & Services）] ページに戻ります。[未同期（Not Synced）] ウィンドウで、[プレビューして展開...（Preview and Deploy...）] をクリックします。

ステップ 9 [デバイスの同期（Device Sync）] ウィンドウで、変更を確認します。

ステップ 10 変更の種類に応じて、[変更の置換（Replace Configuration）] または [変更のデバイスへの適用（Apply Changes to Device）] をクリックします。

複数デバイス上の共有オブジェクトの設定変更の展開

この手順は、2 つ以上のデバイスで共有されているポリシーまたはオブジェクトに変更を加える場合に使用します。多くのデバイスで使用されている共通ポリシーを変更できます。

ステップ 1 編集する共有オブジェクトを含む [ポリシー（Policies）] ページまたは [オブジェクト] ページを開いて編集します。

ステップ 2 共有デバイスリストを確認し、挙げられているすべてのデバイスに変更を加えることを確認します。

ステップ 3 [確認（Confirm）] をクリックします。

ステップ 4 [**保存**（**Save**）] をクリックします。

ステップ 5 [展開] アイコンをクリックして、すべてのデバイスの構成変更のプレビューと展開します。

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。

関連情報：

- 自動展開のスケジュール （315 ページ）

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（41 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。

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

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

自動展開のスケジュール

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

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

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

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 1 つ以上のデバイスを選択します。

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

ステップ 6 展開をいつ実行するかを選択します。

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

ステップ 7 [保存（Save）] をクリックします。

スケジュールされた展開の編集

スケジュールされた展開を編集するには、次の手順に従います。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
ステップ 3 適切なデバイスタイプのタブをクリックします。
ステップ 4 1 つ以上のデバイスを選択します。
ステップ 5 [デバイスの詳細] ペインで、[スケジュールされた展開（Scheduled Deployments）] タブを見つけて、[編集] をクリックします。

ステップ 6 スケジュールされた展開の繰り返し回数、日付、または時刻を編集します。
ステップ 7 [保存（Save）] をクリックします。

スケジュールされた展開の削除

スケジュールされた展開を削除するには、次の手順に従います。

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

ステップ 1 ナビゲーションバーで、[デバイスとサービス] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
ステップ 3 適切なデバイスタイプのタブをクリックします。
ステップ 4 1 つ以上のデバイスを選択します。

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

次のタスク

- 変更の読み取り、破棄、チェック、および展開
- すべてのデバイス設定の読み取り （306 ページ）
- CDO から ASA に設定変更を展開します。 （309 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 （308 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。

- 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。

- ASA 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（323 ページ）を参照してください。

競合検出の有効化

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

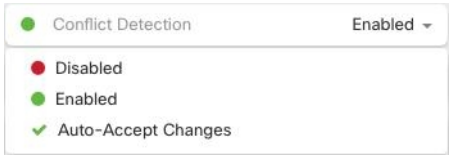
ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブを選択します。

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

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



デバイスからのアウトオブバンド変更の自動的な受け入れ

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

変更の自動受け入れ機能は、競合検出のための強化機能です。デバイスで変更の自動受け入れを有効にしている場合、CDO は 10 分ごとに変更をチェックして、デバイスの設定に対してア

ウトオブバンドの変更が行われたかどうかを確認します。設定が変更されていた場合、CDO は、プロンプトを表示することなく、デバイスの設定のローカルバージョンを自動的に更新します。

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

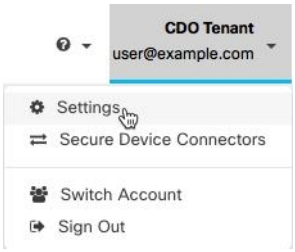
変更の自動受け入れを使用するには、最初に、テナントが [デバイスとサービス] ページの [競合検出] メニューで自動受け入れオプションを表示できるようにします。次に、個々のデバイスでの変更の自動受け入れを有効にします。

CDO でアウトオブバンドの変更を検出するものの、変更を手動で受け入れたり拒否したりするオプションを選択する場合は、代わりに 競合検出 （320 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。

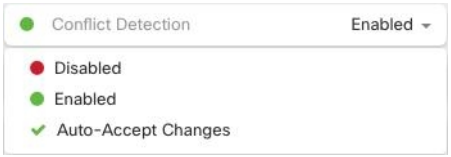
ステップ 2 ユーザーメニューから [設定] をクリックして、[設定] ページにアクセスします。



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 （320 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 （320 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 （40 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。

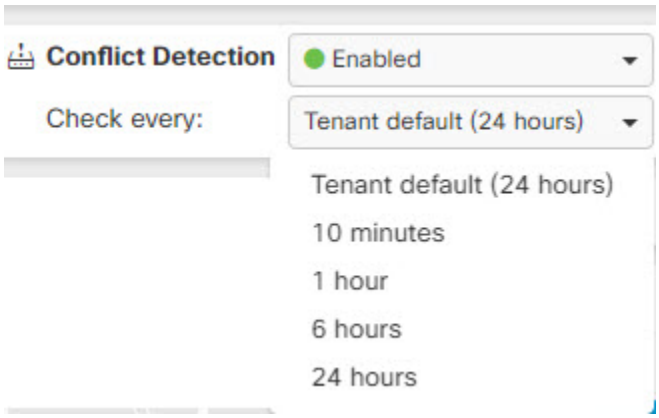
ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

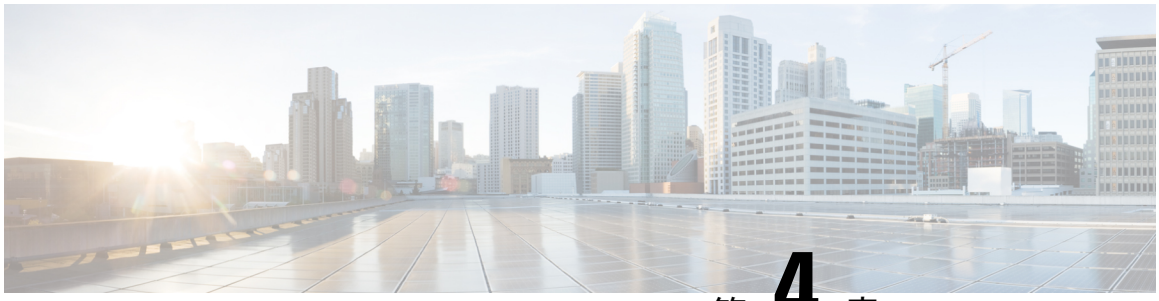
ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

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

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、いつに関する問に回答可能。
- 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 （330 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。

次の画像は、ASA の**アクティブ**な変更ログエントリです。左側のタイムスタンプの横にある白い円に注意してください。

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。

ASA 変更ログの詳細

ASA 変更ログのエントリの説明については、次の記事を参照してください。

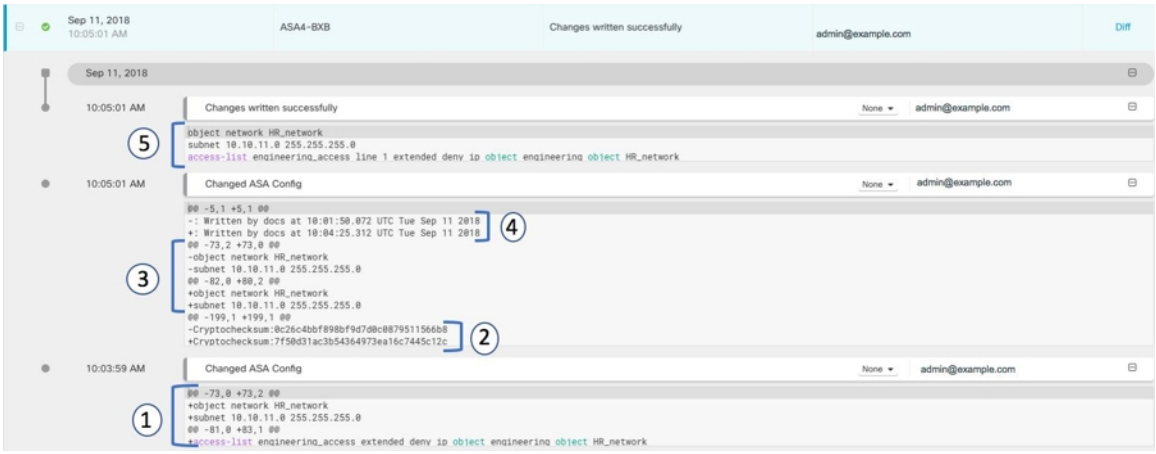
- ASA に展開後の変更ログエントリ （327 ページ）
- ASA から変更を読み取った後の変更ログエントリ （329 ページ）
- 変更ログの差分の表示 （330 ページ）

ASA に展開後の変更ログエントリ

変更ログエントリの説明は次のとおりです。エントリの左上にあるチェックマークの付いた緑色の円は、変更ログが完了したことを示しています。変更ログには、新しいものから古い順にエントリが表示されます。エントリ内の変更は新しいものから古い順に並べ替えられます。

変更ログエントリの行にある青色の [差分（Diff）] リンクをクリックすると、実行コンフィギュレーション ファイルのコンテキストで変更が並べて表示されるため、変更を対比できます。変更ログの差分の表示 （330 ページ）

以下のさまざまな変更の説明を参照してください。

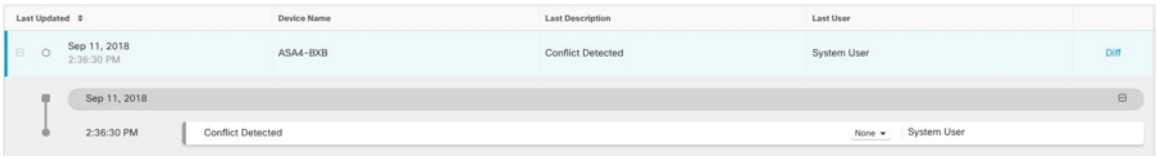


図の番号	説明
1	これは、2018 年 9 月 11 日の午前 10:03:59 に admin@example.com が行った変更です。 **1.** 「HR_network」オブジェクトが追加されました。 **2.** 初期ネットワークアドレス（10.10.11.0）とサブネットマスク（255.255.255.0）が HR_network オブジェクトに追加されました。 **3.** 「engineering」ネットワークのアドレスが「HR_network」に到達することを拒否するルールが「engineering_access」ネットワークポリシーに追加されました。
2	実行構成ファイルのチェックサムが ASA によって再計算され、変更されました。古い値が削除され、新しい値が追加されました。
3	ASA は、Defense Orchestrator が配置した場所とは異なる実行構成ファイル内の場所にオブジェクトを移動します。 （注） この種のエントリが常に表示されるとは限りません。
4	実行構成ファイルが最後に更新されたときのレコード。古いタイムスタンプが削除され、新しいタイムスタンプが追加されています。この変更は、ASA によって行われました。

図の番号	説明
5	これらは、設定を変更するために Defense Orchestrator から ASA に送信されるコマンドです。

ASA から変更を読み取った後の変更ログエントリ

Cisco Defense Orchestrator（CDO）は、管理対象の ASA で変更を検出すると、変更ログエントリを開き、設定の競合が検出された時刻を記録します。これは、CDO が競合を検出したときに表示される可能性のある変更ログエントリの種類です。



変更を受け入れるか、変更を確認して受け入れると、その変更が変更ログエントリに追加され、エントリが完了します。

このエントリには、[競合検出（Conflict Detected）]の変更と、エンジニアリング ネットワークのアドレスが HR_network に到達しないようにするルールの削除が表示されます。変更ログエントリには、「Successfully imported out-of-band changes」というメッセージとともに変更も表示されます。管理者がアウトオブバンド変更を拒否した場合、変更ログには、拒否された内容とともに「Successfully rejected out-of-band changes on the device」というメッセージが表示されます。アウトオブバンド変更とは、CDO を使用せずに ASA デバイスに直接加えられる変更を指します。

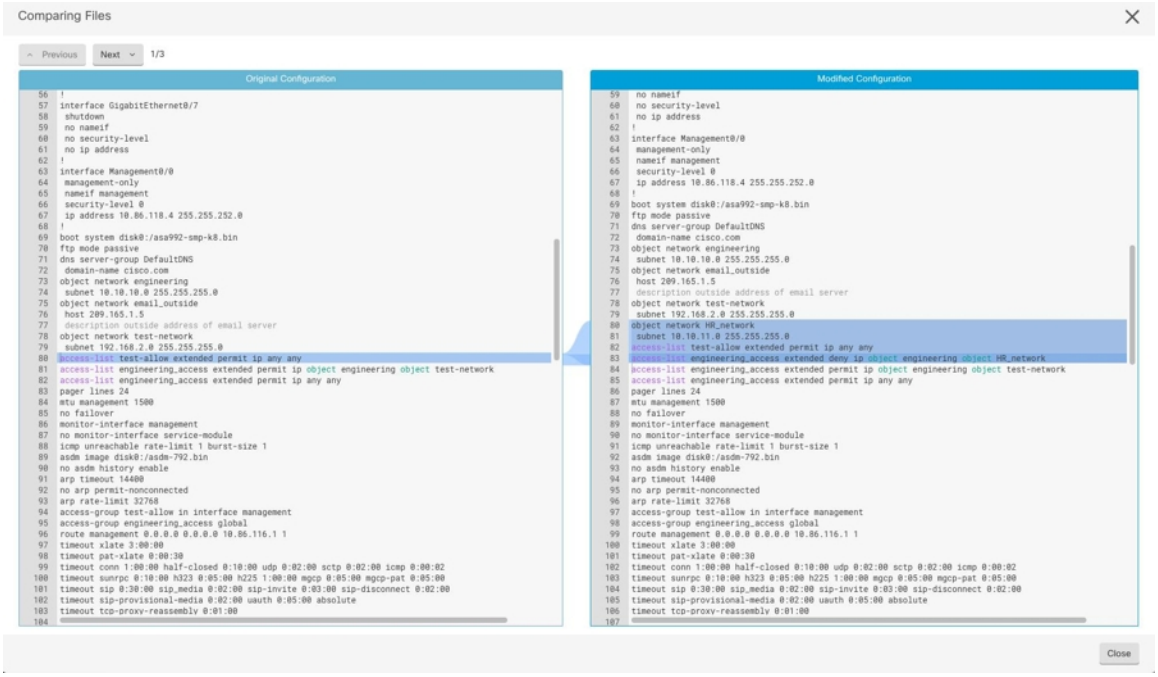
関連項目

- 変更ログ （325 ページ）
- ASA に展開後の変更ログエントリ （327 ページ）
- 変更ログの差分の表示 （330 ページ）
- 変更の読み取り、破棄、チェック、および展開

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）] 列の参照点をとなります。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 （325 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グ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グイベントの検索

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グイベントを検索します。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の部分一致の結果が、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、変更ログ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、変更ログイベントを関連付けます。

1. 変更リクエストの作成 （332 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 （333 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 （332 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 （332 ページ）。
4. 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グ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、どの変更ログ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グイベントを検索するには、次の手順に従います。

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。
2. 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グイベントを検索します。

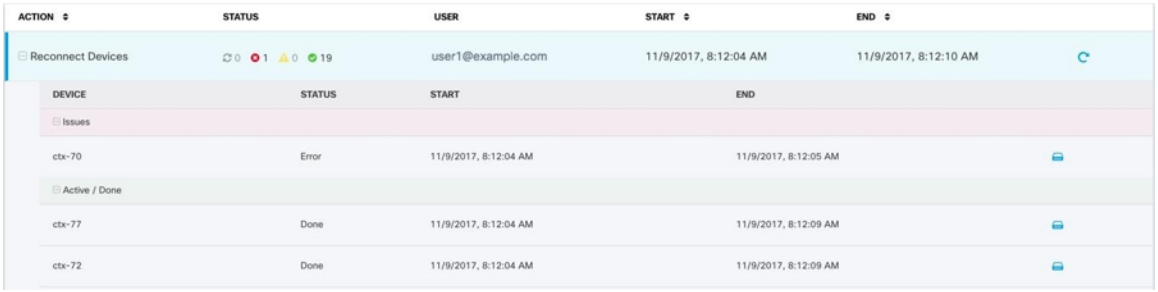
- [変更ログ] 検索フィールドに、変更リクエストの正確な名前を入力して、その変更リクエストに関連付けられた変更ログイベントを検索します。CDOは、完全に一致する変更ログイベントを強調表示します。
- フィルタ変更リクエスト（333ページ）を実行して変更ログイベントを検索します。

3. 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グイベントを見つけます。

[ジョブ（Jobs）] ページ

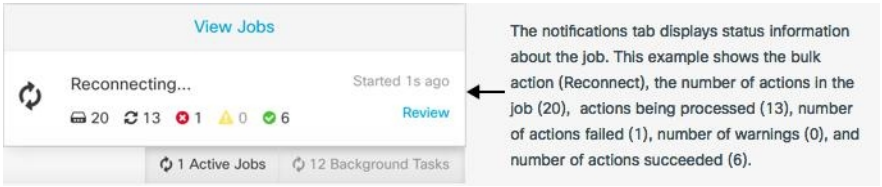
[ジョブ]ページには、一括操作のステータスに関する情報が表示されます。一括操作には、複数のデバイスの再接続、複数のデバイスからの設定の読み取り、複数のデバイスの同時アップグレードなどがあります。ジョブテーブルの色分けされた行は、成功または失敗した個々のアクションを示します。

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。



[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、**[モニターリング（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。

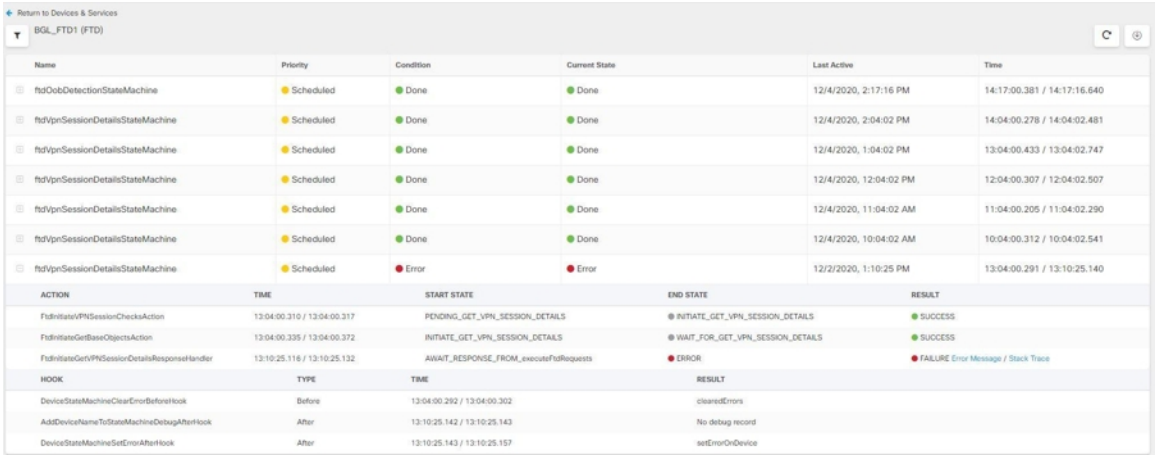
[ワークフロー（Workflows）] ページ

[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。

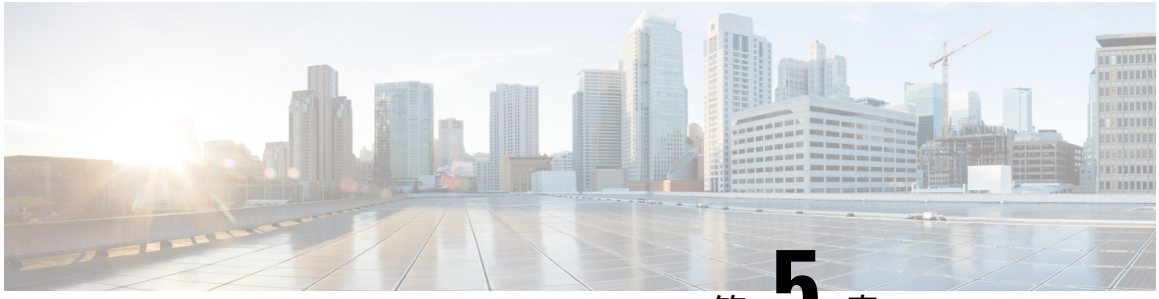


ワークフロー情報のダウンロード

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

Cisco Security Analytics and Logging

Security Analytics and Logging（SaaS）について

Cisco Security Analytics and Logging（SAL）を使用すると、すべての Firepower Threat Defense（FTD）デバイスからの接続イベント、侵入イベント、ファイルイベント、マルウェアイベント、およびセキュリティ インテリジェンス イベント、および ASA からのすべての syslog イベントと NetFlow Secure Event Logging（NSEL）イベントをキャプチャし、Cisco Defense Orchestrator（CDO）の 1 か所で表示できます。イベントは Cisco Cloud に保存され、CDO の [イベントロギング（Event Logging ）] ページから表示できます。このページでイベントをフィルタリングして確認し、ネットワークでトリガーされているセキュリティルールを明確に理解できます。

これらのイベントをキャプチャ後、追加のライセンスを使用して、CDO から、プロビジョニングされた Cisco Secure Cloud Analytics ポータルをクロス起動できます。Cisco Secure Cloud Analytics は、イベントとネットワークフローデータの動作分析を実行することでネットワークの状態を追跡する Software as a Service（SaaS）ソリューションです。ファイアウォールイベントとネットワークフローデータを含め、ネットワークトラフィックに関する情報を送信元から収集することによって、トラフィックに関する観測内容が作成され、トラフィックパターンに基づいてネットワークエンティティのロールが自動的に識別されます。Cisco Secure Cloud Analytics は、この情報を他の脅威インテリジェンス（Talos など）のソースと組み合わせて使用してアラートを生成します。このアラートは、本質的に悪意のある可能性がある動作の存在を示す警告を構成します。Cisco Secure Cloud Analytics は、このアラートとともに、ネットワークおよびホストの可視性と、収集したコンテキスト情報を提供します。このコンテキスト情報により、アラートを調査して悪意のある動作の原因を特定するためのより優れた基盤が得られます。

用語に関する注 : このドキュメントでは、Cisco Security Analytics and Logging が Cisco Secure Cloud Analytics ポータル（Software as a Service（SaaS）製品）で使用されている場合、この統合は Cisco Security Analytics and Logging（SaaS）または SAL（SaaS）と呼ばれています。

ASA の Security Analytics and Logging（SAL SaaS）について

Security Analytics and Logging（SaaS）を使用すると、すべての syslog イベントと NetFlow Secure Event Logging（NSEL）を ASA からキャプチャし、Cisco Defense Orchestrator（CDO）の 1 か所で表示できます。

イベントは Cisco Cloud に保存され、CDO の [イベントロギング（Event Logging ）] ページから確認できます。このページでイベントをフィルタリングして確認し、ネットワークでトリガー

されているセキュリティルールを明確に理解できます。それらの機能は、**Logging and Troubleshooting** パッケージで提供されます。

Logging Analytics and Detection パッケージ（旧 **Firewall Analytics and Logging** パッケージ）を使用すると、システムは Cisco Secure Cloud Analytics 動的エンティティモデリングを FTD イベントに適用し、行動モデリング分析を使用して Cisco Secure Cloud Analytics の観測値とアラートを生成できます。**Total Network Analytics and Monitoring** パッケージを使用すると、システムは FTD イベントとネットワークトラフィックの両方に動的エンティティモデリングを適用し、観測値とアラートを生成します。Cisco Single Sign-On を使用して、プロビジョニングされた Cisco Secure Cloud Analytics ポータルを CDO からクロス起動できます。

CDO イベントビューアでの ASA イベントの表示方法

Syslog イベントと NSEL イベントは、ロギングが ASA で有効になっていて、ネットワークトラフィックがアクセス制御ルールの基準に一致するときに生成されます。イベントが Cisco Cloud に保存されたら、CDO で表示できます。

複数の Secure Event Connector（SEC）をインストールし、任意のデバイスでルールによって生成されたイベントを、syslog サーバーであるかのように任意の SEC に送信できます。SEC はイベントを Cisco Cloud に転送します。同じイベントをすべての SEC に転送しないでください。Cisco Cloud に送信されるイベントを複製すると、日次取り込み率が不必要に高くなります。

Syslog および NSEL イベントが Secure Event Connector を介して ASA から Cisco Cloud に送信される方法

Logging and Troubleshooting の基本ライセンスでは、ASA イベントが Cisco Cloud に到達する方法は次のとおりです。

1. ユーザー名とパスワードを使用して、ASA を CDO に導入準備します。
2. ASA を設定して、syslog および NSEL イベントを、syslog サーバーであるかのいように任意の SEC に転送し、デバイスでのロギングを有効にします。
3. SEC は、イベントが保存されている Cisco Cloud にイベントを転送します。
4. CDO は、設定したフィルタに基づいて、Cisco Cloud からのイベントをイベントビューアに表示します。

Logging Analytics and Detection または **Total Network Analytics and Monitoring** ライセンスでは、次のことも発生します。

1. Cisco Secure Cloud Analytics は、Cisco Cloud に保存されている ASA syslog イベントに分析を適用します。
2. 生成された観測値とアラートには、CDO ポータルに関連付けられた Cisco Secure Cloud Analytics ポータルからアクセスできます。
3. CDO ポータルから、Cisco Secure Cloud Analytics ポータルをクロス起動して、観察値とアラートを確認できます。

ソリューションで使用されるコンポーネント

Secure Device Connector（SDC）：SDC は CDO を ASA に接続します。ASA のログイン情報は SDC に保存されます。詳細については、Secure Device Connector（SDC）（3 ページ）を参照してください。

Secure Event Connector（SEC）：SEC は、ASA からイベントを受信し、Cisco Cloud に転送するアプリケーションです。Cisco Cloud に転送されたイベントは、CDO の [イベントロギング] ページで確認したり、Cisco Secure Cloud Analytics で分析したりできます。使用環境に応じて、SEC は Secure Device Connector（ある場合）にインストールされます。または、ネットワーク内で維持する独自の CDO コネクタ仮想マシンにインストールされます。詳細については、Secure Event Connector（397 ページ）を参照してください。

適応型セキュリティアプライアンス（ASA）：ASA はアドオン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。

Cisco Secure Cloud Analytics は、動的エンティティモデリングを ASA イベントに適用し、この情報に基づいて検出を生成します。これにより、ネットワークから収集されたテレメトリの詳細な分析が可能になり、ネットワークトラフィックの傾向を特定し、異常な動作を調べることができます。**Logging Analytics and Detection** または **Total Network Analytics and Monitoring** ライセンスをお持ちの場合は、このサービスを利用できます。

ライセンシング

このソリューションを設定するには、次のアカウントとライセンスが必要です。

- **Cisco Defense Orchestrator**。CDO テナントが必要です。
- **Secure Device Connector**。Secure Device Connector 用の個別のライセンスはありません。
- **Secure Event Connector**。Secure Event Connector 用の個別のライセンスはありません。
- **Secure Logging Analytics（SaaS）**。「Security Analytics and Logging ライセンスの表」を参照してください。
- **適応型セキュリティアプライアンス（ASA）**。基本ライセンス以上。

Security Analytics and Logging ライセンス

Security Analytics and Logging（SaaS）を実装するには、次のいずれかのライセンスを購入する必要があります。

ライセンス名	提供される機能	利用可能なライセンス期間	機能の前提条件
Logging and Troubleshooting	• ライブフィードと履歴ビューの両方で、CDO 内の ASA イベントとイベントの詳細を表示します。	• 1 年 • 3 年 • 5 年	• CDO • ソフトウェアバージョン 9.6 以降を実行しているオンプレミスの ASA 展開。 • ASA イベントを Cisco Cloud に渡すための 1 つ以上の SEC の展開。
Logging Analytics and Detection（旧 **Firewall Analytics and Monitoring**）	**Logging and Troubleshooting** の機能に加えて、以下の機能 • 動的エンティティモデリングと行動分析をイベントに適用します。 • イベントデータに基づいて Cisco Secure Cloud Analytics でアラートを開き、CDO イベントビューアからクロス起動します。	• 1 年 • 3 年 • 5 年	• CDO • ソフトウェアバージョン 9.6 以降を実行しているオンプレミスの ASA 展開 • ASA イベントを Cisco Cloud に渡すための 1 つ以上の SEC の展開。 • 新たにプロビジョニングされたか、または既存の Cisco Secure Cloud Analytics ポータル。

ライセンス名	提供される機能	利用可能なライセンス期間	機能の前提条件
Total Network Analytics and Monitoring	**Logging Analytics and Detection** の機能に加えて、以下の機能 • 動的エンティティモデリングと行動分析を ASA イベント、オンプレミスのネットワークトラフィック、およびクラウドベースのネットワークトラフィックに適用します。 • ASA イベントデータ、Cisco Secure Cloud Analytics センサーによって収集されたオンプレミスのネットワークトラフィックのフローデータ、および Cisco Secure Cloud Analytics に渡されるクラウドベースのネットワークトラフィックの組み合わせに基づいて、Cisco Secure Cloud Analytics でアラートを開き、CDO イベントビューアからクロス起動します。	• 1 年 • 3 年 • 5 年	• CDO • ソフトウェアバージョン 9.6 以降を実行しているオンプレミスの ASA 展開 • イベントを Cisco Cloud に渡すための 1 つ以上の SEC の展開。 • ネットワークトラフィックのフローデータをクラウドに渡すための少なくとも 1 つの Cisco Secure Cloud Analytics センサーバージョン 4.1 以降の展開、または、ネットワークトラフィックのフローデータを Cisco Secure Cloud Analytics に渡すためのクラウドベースと統合された Cisco Secure Cloud Analytics の展開。 • 新たにプロビジョニングされたか、または既存の Cisco Secure Cloud Analytics ポータル。

データプラン

Cisco Cloud が導入準備された ASA から毎日受け取るイベント数を反映したデータプランを購入する必要があります。これは「日次取り込み率」と呼ばれます。Logging Volume Estimator

ツールを使用して、日次取り込み率を推定でき、率が変化すると、データプランを更新できます。

データプランは、1 GB の日次ボリューム単位で、1 年、3 年、または 5 年の期間で利用できます。データプランの詳細については、Secure Logging Analytics（SaaS）発注ガイド [英語] を参照してください。

（注） Security Analytics and Logging ライセンスとデータプランがある場合、その後は別のライセンスを取得するだけで済み、別のデータプランを取得する必要はありません。ネットワークトラフィックのスループットが変化した場合は、別のデータプランを取得するだけで済み、別の Security Analytics and Logging ライセンスを取得する必要はありません。

30 日間の無料トライアル

CDO にログインし、**[モニタリング（Monitoring）]** > **[イベントロギング（Event Logging）]** タブに移動して、30 日間のリスクフリーのトライアルをリクエストできます。30 日間のトライアルが終了したら、Secure Logging Analytics（SaaS）発注ガイド [英語] の手順に従って、Cisco Commerce Workspace（CCW）からサービスを継続するために必要なイベントデータボリュームを注文できます。

次のステップ

「ASA デバイスに安全なロギング分析（SaaS）を導入する」に移動します。

ASA デバイスに安全なロギング分析（SaaS）を導入する

はじめる前に

- 「ASA の Security Analytics and Logging（SAL SaaS）について」で以下について確認してください。
  - Cisco Cloud へのイベントの送信方法
  - ソリューションに含まれるアプリケーション
  - 必要なライセンス
  - 必要なデータプラン
- すでにマネージドサービスプロバイダーまたは CDO セールス担当者に問い合わせて CDO テナントを作成しました。
- Secure Device Connector（SDC） （3 ページ）を確認してください。SDC を使用して CDO を ASA に接続することは「ベストプラクティス」と考えられますが、必須ではありません。

- ネットワークで SDC を展開する場合、次のいずれかの方法を使用してインストールできます。
  - 「CDO の VM イメージを使用した Secure Device Connector の展開」を使用して、CDO の準備された VM イメージを使用して SDC をインストールします。これが推奨される最も簡単な SDC の展開方法です。
  - 「自身の VM 上での Secure Device Connector の展開」を使用します。
- Secure Event Connector をインストールする、任意の ASA から、テナントに導入準備された任意の SEC にイベントを送信できます。
- アカウントのユーザー向けに新規 Cisco Secure Sign-On アカウントの作成と Duo 多要素認証の設定しました。

Cisco Security Analytics and Logging（SaaS）の導入と Secure Event Connector を介した Cisco Cloud へのイベント送信のワークフロー

1. 上の「はじめる前に」を参照し、環境が適切に設定されていることを確認してください。
2. ユーザー名とパスワードを使用して ASA デバイスの導入準備 （111 ページ） を行います。
3. コマンド ライン インターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信
4. CDO マクロを使用して ASA デバイスの NSEL を設定する
5. CDO にイベントが表示されていることを確認します。ナビゲーションバーから、[モニターリング（Monitoring）] > [イベントロギング（Event Logging）] を選択します。ライブイベントを表示するには、[ライブ] タブをクリックします。
6. [Firewall Analytics and Monitoring] ライセンスや [Total Network Analytics and Monitoring] ライセンスがある場合は、次のセクション「**Cisco Secure Cloud Analytics を使用したイベントの分析**」に進みます。

Cisco Secure Cloud Analytics を使用したイベントの分析

[Firewall Analytics and Monitoring] ライセンスや [Total Network Analytics and Monitoring] ライセンスがある場合は、先行するステップに加えて、次の手順を実行します。

1. Cisco Secure Cloud Analytics ポータルのプロビジョニング （418 ページ）。
2. [Total Network Analytics and Monitoring] ライセンスを購入した場合は、1 つ以上の Secure Cloud Analytics センサーを内部ネットワークに展開します。「総合的なネットワーク分析およびレポーティングのための Cisco Secure Cloud Analytics センサーの展開 （420 ページ）」を参照してください。
3. Cisco シングルサインオンのログイン情報に関連付ける Secure Cloud Analytics ユーザーアカウントを作成するようにユーザーに勧めます。「Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （421 ページ）」を参照してください。

4. CDO から Secure Cloud Analytics をクロス起動し、FTD イベントから生成される Secure Cloud Analytics アラートをモニターします。「Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （421 ページ）」を参照してください。

CDO からのクロス起動による Cisco Secure Cloud Analytics アラートの確認

[Firewall Analytics and Monitoring] ライセンスまたは [Total Network Analytics and Monitoring] ライセンスにより、CDO から Secure Cloud Analytics をクロス起動して、FTD イベントから生成されるアラートを確認できます。

詳細については、次の項目を参照してください。

- CDO へのサインイン
- Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （421 ページ）
- Cisco Secure Cloud Analytics とダイナミック エンティティ モデリング
- ファイアウォールイベントに基づくアラートの使用

Secure Event Connector に関する問題のトラブルシューティング

ステータス情報とロギング情報の収集については、次のトラブルシューティングトピックを使用してください。

- SEC オンボーディング失敗のトラブルシューティング
- イベントロギングのトラブルシューティング ログ ファイル
- Secure Event Connector の状態を把握するためのヘルスチェックの使用

ワークフロー

「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」では、Cisco Security Analytics and Logging から生成されたイベントを使用して、ユーザーがネットワークリソースにアクセスできなかった原因を特定する方法について説明しています。

「ファイアウォールイベントに基づくアラートの使用」も参照してください。

CDO マクロを使用した Cisco Cloud への ASA Syslog イベントの送信

「コマンドライン インターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信」で説明されているすべてのコマンドを使用する CDO マクロを作成し、同じバッチのすべての ASA でそのマクロを実行することにより、すべての ASA を設定してイベントを Cisco Cloud に送信します。

CDO のマクロツールを使用すると、CLI コマンドのリストを作成し、コマンドシンタックスの要素をパラメータに変換してから、コマンドのリストを保存して、複数回使用できるようにすることができます。マクロは、一度に複数のデバイスで実行することもできます。

実証済みのマクロを使用すると、デバイス間の設定の一貫性が促進され、コマンド ライン インターフェイスの使用時に発生する可能性のあるシンタックスエラーが防止されます。

先に進む前に、以下のトピックを参照して、マクロの使用方法を把握してください。この記事では、最終的なマクロの作成についてのみ説明します。

- デバイスの管理用 CLI マクロ
- 新規コマンドからの CLI マクロの作成
- CLI マクロの実行
- CLI マクロの編集
- CLI マクロの削除

ASA セキュリティ分析とロギング（SaaS）マクロを作成する

次の手順では、ASA CLI コマンドとマクロ形式の 2 種類の形式があります。ASA CLI コマンドは、ASA の構文表記法に従うように記述されています。マクロの表記法については、「新規コマンドからの CLI マクロの作成」で説明されています。

開始する前に、マクロを作成しながらコマンドの説明を読むことができるように、別ウィンドウで「コマンド ライン インターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信」を開き、この手順と並行して読めるようにしてください。

（注） ASA にロギング設定がすでに存在する場合、CDO からマクロを実行しても、最初に既存のログ設定がすべてクリアされるわけではありません。その代わり、CDO マクロで定義された設定は、既存の設定があればそれにマージされます。

ステップ 1 プレーンテキストエディタを開き、以下の手順とオプションに基づいて、マクロに変換するコマンドのリストを作成します。CDO は、マクロに記述された順序でコマンドを実行します。一部のコマンドには、{{parameters}} に変換する値が含まれます。これは、マクロの実行時に入力することになります。

ステップ 2 SEC が syslog サーバーであるかのように、SEC にメッセージを送信するように ASA を設定します。

logging host コマンドを使用して、メッセージ送信先の syslog サーバーとして SEC を指定します。テナントに導入準備した SEC のいずれかにイベントを送信できます。

logging host コマンドは、イベント送信先の TCP または UDP ポートを指定します。どのポートを使用するかを判断するには、「Secure Logging Analytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。

logging host*interface_nameSEC_IP_address* { **tcp/port** | **udp/port** }

syslog イベントを SEC に送信するために使用するプロトコルに応じて、このコマンドを 2 つの異なるマクロのいずれかに変換します。

logging host {{interface_name}} {{SEC_ip_address}} tcp/{{port_number}}

logging host {{interface_name}} {{SEC_ip_address}} udp/{{port)_number}}

（任意）TCP を使用する場合、次のコマンドをマクロのコマンドリストに追加できます。パラメータは必要としません。

logging permit-hostdown

ステップ 3　syslog サーバに送信する syslog メッセージを指定します。

logging trap コマンドを使用して、syslog サーバーに送信する syslog メッセージを指定します。

logging trap {*severity_level* | *message_list*}

SEC に送信されるイベントを重大度レベルで定義する場合は、コマンドを次のマクロに変換します。

logging trap {{severity_level}}

メッセージリストの一部であるイベントのみを SEC に送信する場合は、コマンドを次のマクロに変換します。

logging trap {{message_list_name}}

前のステップで **logging trap message_list** コマンドを選択した場合は、メッセージリスト内で syslog を定義する必要があります。マクロを作成しながらコマンドの説明を読むことができるように、「カスタムイベント リストの作成」を開いておきます。次のコマンドで開始します。

logging list*name* {**level***level* [**class***message_class*] | **message***start_id* [*-end_id*]}

次に、これを次のバリエーションに分割します。

logging list {{message_list_name}} level {{security_level}}

logging list {{message_list_name}} level {{security_level}} class {{message_class}}

logging list {{message_list_name}} message {{syslog_range_or_number}}

最後のバリエーションでは、メッセージパラメータ{{syslog_range_or_number}} は、単一の syslog ID（106023）または範囲（302013-302018）として入力できます。メッセージリストを作成するには、1 つまたは複数のコマンドバリエーションを任意の行数で使用します。単一のマクロでは、同じ名前のすべてのパラメータが、入力した同じ値を使用することに注意してください。CDO は、空のパラメータを含むマクロを実行しません。

重要　マクロでは、**logging list** コマンドは **logging trap** コマンドの前に置く必要があります。最初にリストを定義すると、**logging trap** コマンドでそれを使用できます。下のサンプルマクロを参照してください。

ステップ 4　（任意）**syslog timestamp** を追加します。 ASA 上の syslog メッセージから生じたメッセージに日付と時刻を追加する場合は、このコマンドを追加します。タイムスタンプの値は **SyslogTimestamp** フィールドに表示されます。このコマンドをコマンドのリストに追加します。パラメータは必要としません。

logging timestamp

（注） バージョン 9.10(1) 以降、ASA は、イベントの syslog で RFC 5424 に従ってタイムスタンプを有効にするオプションを提供します。このオプションを有効にすると、Syslog メッセージのすべてのタイムスタンプには、RFC 5424 形式に従って時刻が表示されます。次に、RFC 5424 形式の出力例を示します。

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol
from src interface :src IP/src port to dest IP/dest port
```

.

ステップ 5 **（任意）非 EMBLEM 形式の syslog メッセージにデバイス ID を含めます。**マクロを作成しながらコマンドの説明を読むことができるように、「非 EMBLEM 形式の syslog メッセージにデバイス ID を含める」を開いておきます。次は、マクロのベースとなる CLI コマンドです。

logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string***text*}

次に、これを次のバリエーションに分割します。

logging device-id cluster-id

logging device-id context-name

logging device-id hostname

logging device-id ipaddress {{interface_name}} **system**

logging device-id string {{text_16_char_or_less}}

ステップ 6 **ロギングを有効にします。**次のコマンドをそのままマクロに追加します。パラメータはありません。

logging enable

ステップ 7 マクロの最終行に **write memory を追加しないでください。**その代わりに、 **show running-config logging** コマンドを追加して、ロギングコマンドを ASA のスタートアップコンフィギュレーションにコミットする前に、入力したロギングコマンドの結果を確認します。

show running-config logging

ステップ 8 設定の変更が行われたことを確認したら、**write memory** コマンド用に別のマクロを作成して、または CDO の一括 CLI インターフェイスを使用して、設定したすべてのデバイスにマクロを使用してコマンドを発行できます。

write memory

ステップ 9 **（任意）アクセス制御ルール「許可」イベントのロギングを有効化します。**コマンド ライン インターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信手順で説明されているこのステップは、このマクロには含まれていません。代わりに CDO GUI で実行されます。

ステップ 10 マクロを保存します。

例

1 つのマクロに結合されるコマンドのリストのサンプルを次に示します。

```
logging host {{interface_name}} {{SEC_ip_address}} {{tcp_or_udp}}/{{port_number}}
```

```
logging permit-hostdown
logging list {{message_list_name}} level {{security_level}}
logging list {{message_list_name}} message {{syslog_range_or_number_1}}
logging list {{message_list_name}} message {{syslog_range_or_number_2}}
logging trap {{message_list_name}}
logging device-id cluster-id
logging enable
show running-config logging
```

（注） 特定のさまざまな syslog ID または範囲を追加するための logging list コマンドがいくつかあります。{{syslog_range_or_number_X}} パラメータには、数値またはその他の差別化要因が必要です。そうしないと、マクロが入力されたときにそれらの値はすべて同じになります。また、すべてのパラメータに値が指定されていない場合には、CDO はマクロを実行しないことに注意してください。そのため、マクロには実行するコマンドのみが含まれるようにしてください。すべての syslog ID を同じリストに含める必要があるため、event_list_name は各行で同じままです。

次のタスク

マクロの実行

ASA セキュリティ分析とロギングマクロを作成して保存したら、マクロを実行して ASA syslog イベントを Cisco Cloud に送信します。

コマンドラインインターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信

この手順では、ASA の syslog イベントを Secure Event Connector（SEC）に転送してから、ロギングを有効にする方法について説明します。以下の手順では、ワークフローの完了に必要な事柄のみを説明します。ASA でロギングを設定できるすべての方法の広範な説明については、『ASDM ブック 1：Cisco ASA シリーズ ASDM コンフィギュレーション ガイド（一般的な操作）』または『CLI ブック 1：Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）』のいずれかのモニターリングに関する章を参照してください。

ASA コマンドのサポート制限

CDO では、次の syslog コマンドまたはメッセージの形式はまだサポートされていません。

- syslog の EMBLEM 形式
- Secure Syslog

ASA の CDO コマンド ライン インターフェイス

この手順に含まれるすべてのタスクでは、ASA の CDO のコマンド ライン インターフェイスで作業します。コマンド ライン インターフェイスのページを開くには、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] 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、ロギングを有効にする ASA を選択します。

ステップ 4 右側の [デバイスアクション] ペインで、[>_コマンドラインインターフェイス（>_ Command Line Interface）] をクリックします。

ステップ 5 [コマンド ライン インターフェイス（Command Line Interface）] タブをクリックします。プロンプトで以下に説明するコマンドを入力する準備ができました。

すべてのコマンドを入力したら、[送信（Send）] をクリックします。CDO の CLI インターフェイスは ASA への直接接続なので、コマンドはデバイスの実行構成に即座に書き込まれます。ASA のスタートアップ コンフィギュレーションに変更を書き込むには、さらに `write memory` コマンドを発行する必要があります。

ASA syslog イベントの Secure Event Connector への転送

導入準備した Secure Event Connector（SEC）の 1 つに ASA syslog イベントを転送し、ログを有効にするには、次の手順で以下のタスクを完了する必要があります。

ステップ 1 SEC が syslog サーバーであるかのように、SEC にメッセージを送信するように ASA を設定します。

ステップ 2 すべてのログの重大度レベル、または SEC に送信する syslog イベントのリストを決定します。

ステップ 3 ロギングを有効にします。

ステップ 4 ASA のスタートアップ コンフィギュレーションに変更を保存します。

CLI を使用した Cisco Cloud への ASA Syslog イベントの送信

ステップ 1 **SEC が syslog サーバーであるかのように、SEC にメッセージを送信するように ASA を設定する**

ASA から Cisco Cloud に syslog イベントを送信する場合、ユーザーは SEC が外部の syslog サーバーであるかのように SEC に転送し、SEC はメッセージを Cisco Cloud に転送します。

syslog メッセージを SEC に送信するには、次の手順を実行します。

1. TCP または UDP を使用して、SEC が syslog サーバーであるかのように、SEC にメッセージを送信するように ASA を設定します。SEC は、IPv4 アドレスまたは IPv6 アドレスを使用できます。TCP ポートと UDP ポートのいずれかにイベントを送信します。どのポートを使用するかを判断するには、「Secure Logging Analytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。

   logging host コマンドシンタックスの例を次に示します。

   logging host *interface_name SEC_IP_address* [[**tcp/port**] | [**udp/port**]]

   例：

   ```
    > logging host mgmt 192.168.1.5 tcp/10125
   > logging host mgmt 192.168.1.5 udp/10025
   > logging host mgmt 2002::1:1 tcp/10125
   > logging host mgmt 2002::1:1 udp/10025
   ```

   - **interface_name** 引数は、syslog サーバーへのメッセージの送信元である ASA インターフェイスを指定します。SDC との通信にすでに使用されているのと同じ ASA インターフェイスを介して、syslog メッセージを SDC に送信するのが「ベストプラクティス」です。
   - **SEC_IP_address** 引数には、SEC がインストールされている VM の IP アドレスが含まれている必要があります。
   - キーワードと引数のペア **tcp/port** または **udp/port** は、TCP プロトコルと関連するポート、または UDP プロトコルと関連するポートのいずれかを使用して、syslog メッセージが送信されるように指定します。UDP または TCP のいずれかを使用して syslog サーバにデータを送信するようにASA を設定することはできますが、両方を使用するように設定することはできません。プロトコルを指定しない場合、デフォルトのプロトコルは UDP です。

     TCP を指定すると、ASA は syslog サーバーの障害を検出し、セキュリティ保護として ASA 経由の新しい接続をブロックします。TCP syslog サーバーへの接続の状態に関係なく新しい接続を許可するには、手順 b を参照してください。UDP を指定すると、syslog サーバーが動作しているかどうかにかかわらず、ASA は引き続き新しい接続を許可します。有効なポート値

     （注） ASA メッセージを 2 台の別個の syslog サーバーに送信する場合は、もう一方の syslog サーバーの適切なインターフェイス、IP アドレス、プロトコル、およびポートを使用して、2 番目の logging host コマンドを実行できます。

2. （オプション）TCP 経由で SEC にイベントを送信し、SEC がダウンしているものの、ASA のログキューがいっぱいである場合、新しい接続はブロックされます。新しい接続は、syslog サーバーがバックアップされ、ログ キューがいっぱいでなくなった後に再度許可されます。TCP syslog サーバーへの接続の状態に関係なく新しい接続を許可するには、次のコマンドを使用して、TCP 接続された syslog サーバーがダウンしたときに新しい接続をブロックする機能を無効にします。

   logging permit-hostdown

   例：

   ```
    > logging permit-hostdown
   ```

ステップ 2 次のコマンドを使用して、**syslog サーバーに送信する syslog メッセージを指定します。**

logging trap { severity_level | message_list }

例：

```
> logging trap 3
> logging trap asa_syslogs_to_cloud
```

重大度として、値（1 ～ 7）または名前を指定できます。たとえば重大度を 3 に設定すると、ASAは、重大度が 3、2、および 1 の syslog メッセージを送信します。

message_list 引数は、カスタムイベントリストを作成した場合、そのリストの名前に置き換えられます。カスタムイベントリストの指定に必要な操作は、そのリストにある syslog メッセージを Secure Event Connector に送信することだけです。上記の例では、asa_syslogs_to_cloud がイベントリストの名前です。

message_list を使用すると、Cisco Cloud に送信する syslog メッセージを明確に指定できるため、費用を節約できます。

message_list を作成するには、カスタム イベント リストの作成を参照してください。データの取り込みとストレージのコストの詳細については、「データストレージプラン」を参照してください。

ステップ 3 （オプション）syslog タイムスタンプの追加

logging timestamp コマンドを使用して、ASA での syslog メッセージの発信日時をメッセージに追加します。タイムスタンプの値は **SyslogTimestamp** フィールドに表示されます。

例：

```
> logging timestamp
```

（注） バージョン 9.10(1) 以降、ASA は、イベントの syslog で RFC 5424 に従ってタイムスタンプを有効にするオプションを提供します。このオプションを有効にすると、Syslog メッセージのすべてのタイムスタンプには、RFC 5424 形式に従って時刻が表示されます。次に、RFC 5424 形式の出力例を示します。

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol from
 src interface :src IP/src port to dest IP/dest port.
```

ステップ 4 （オプション）非 EMBLEM 形式の Syslog メッセージにデバイス ID を含める

デバイス ID は、特定の ASA から送信されたすべての syslog メッセージを簡単に区別できるように、syslog メッセージに挿入できる識別子です。詳細については、「非 EMBLEM 形式の syslog メッセージにデバイス ID を含める」を参照してください。

ステップ 5 （オプション）アクセス制御ルール「許可」イベントのロギングの有効化

アクセス制御ルールによってリソースへのアクセスが拒否されると、イベントが自動的にログに記録されます。アクセス制御ルールによってリソースへのアクセスが許可されたときに生成されたイベントもログに記録する場合は、アクセス制御ルールのロギングをオンにして、重大度タイプを設定する必要があります。個々のネットワークアクセス制御ルールのロギングをオンにする方法については、「ルールアクティビティのログ記録」を参照してください。

（注） アクセス制御ルール「許可」イベントでのロギングを有効にすると、購入したデータプランはイベントの毎日の取り込み率に基づいているため、データの消費量が増大します。

ステップ 6 ロギングの有効化

コマンドプロンプトで、「logging enable」と入力します。ASA では、個々のルールではなく、デバイス全体に対してロギングが有効になります。

例：

```
> logging enable
```

（注）　現時点では、CDO はセキュアロギングの有効化をサポートしていません。

ステップ 7　スタートアップ コンフィギュレーションへの変更の保存

コマンドプロンプトで、「write memory」と入力します。ASA では、個々のルールではなく、デバイス全体に対してロギングが有効になります。

例：

```
> write memory
```

関連情報：

- SDC 仮想マシンへの Secure Event Connector のインストール （398 ページ）
- CDO イメージを使用して SEC をインストールする

カスタム イベント リストの作成

ASA syslog イベントを Cisco Cloud に送信するときに、次のいずれかの方法を使用してカスタムイベントリストを作成します。

- コマンド ライン インターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信
- CDO マクロを使用した Cisco Cloud への ASA Syslog イベントの送信

次の 3 つの基準に基づいて、message_list とも呼ばれるイベントリストを作成できます。

- イベント クラス
- 重大度
- メッセージ ID

特定のロギングの宛先（syslog サーバーや Secure Event Connector など）に送信するカスタムイベントリストを作成するには、次の手順を実行します。

ステップ 1　[デバイスとサービス] ページで、[デバイス] タブをクリックします。

ステップ 2　適切なタブをクリックして、syslog メッセージをカスタムイベントリストに含める ASA を選択します。

ステップ 3　[デバイスアクション] ペインで、[>_コマンド ライン インターフェイス（>_ Command Line Interface）] をクリックします。

ステップ 4　次のコマンドシンタックスを使用して、**logging list** コマンドを ASA に発行します。

logging list *name* { **level** *level* [**class** *message_class*] | **message** *start_id* [*-end_id*] }

name 引数には、リストの名前を指定します。キーワードと引数のペア **level** *level* により、重大度が指定されます。キーワードと引数のペア **class** *message_class* により、特定のメッセージクラスが指定されます。キーワードと引数のペア **message** *start_id* [*-end_id*] により、個々の syslog メッセージ番号または番号の範囲が指定されます。

（注） 重大度の名前を syslog メッセージ リストの名前として使用しないでください。使用禁止の名前には、emergencies、alert、critical、error、warning、notification、informational、および debugging が含まれます。同様に、イベント リスト名の先頭にこれらの単語の最初の 3 文字は使用しないでください。たとえば、「err」で始まるイベントリスト名は使用しないでください。

- **重大度に基づいてイベントリストに syslog メッセージを追加します。**たとえば重大度を 3 に設定すると、ASAは、重大度が 3、2、および 1 の syslog メッセージを送信します。

  例：

  ```
  > logging list asa_syslogs_to_cloud level 3
  ```

- **他の基準に基づいて syslog メッセージをイベントリストに追加します。**

  前回の手順で使用したものと同じコマンドを入力し、既存のメッセージ リストの名前と追加基準を指定します。リストに追加する基準ごとに、新しいコマンドを入力します。たとえば、リストに追加される syslog メッセージの基準として、次の基準を指定できます。

  - ID が 302013 ～ 302018 の範囲の syslog メッセージ。
  - 重大度が critical 以上（emergency、alert、または critical）のすべての syslog メッセージ。
  - 重大度が warning 以上（emergency、alert、critical、error、または warning）のすべての HA クラス syslog メッセージ。

    例：

    ```
    > logging list asa_syslogs_to_cloud message 302013-302018
    > logging list asa_syslogs_to_cloud level critical
    > logging list asa_syslogs_to_cloud level warning class ha
    ```

    （注） syslogメッセージは、これらの条件のいずれかを満たす場合にログに記録されます。syslog メッセージが複数の条件を満たす場合、そのメッセージは一度だけログに記録されます。

ステップ 5 スタートアップ コンフィギュレーションへの変更の保存

コマンドプロンプトで、「**write memory**」と入力します。

例：

```
> write memory
```

非 EMBLEM 形式の syslog メッセージにデバイス ID を含める

非 EMBLEM 形式の syslog メッセージにデバイス ID を含めるように ASA を設定できます。syslog メッセージに対して指定できるデバイス ID のタイプは 1 つだけです。この手順は、次の手順によって参照されます。

- コマンドライン インターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信
- CDO マクロを使用した Cisco Cloud への ASA Syslog イベントの送信

このデバイス ID は、[イベントロギング] ページに表示される syslog イベントの SensorID フィールドに反映されます。

ステップ 1 デバイス ID を割り当てる syslog メッセージが属す ASA を選択します。

ステップ 2 [デバイスアクション] ペインで、[>_コマンドラインインターフェイス（>_ Command Line Interface）] をクリックします。

ステップ 3 次のコマンドシンタックスを使用して、デバイスに **logging device-id** コマンドを発行します。

logging device-id { **cluster-id** | **context-name** | **hostname** | **ipaddress***interface_name* [**system**] | **string***text* }

例：

```
> logging device-id hostname
> logging device-id context-name
> logging device-id string Cambridge
```

context-name キーワードは、現在のコンテキストの名前を装置 ID として使用することを示します（マルチ コンテキスト モードにだけ適用されます）。マルチ コンテキスト モードの管理コンテキストでデバイス ID のロギングをイネーブルにすると、そのシステム実行スペースで生成されるメッセージは**システム**のデバイス ID を使用し、管理コンテキストで生成されるメッセージは管理コンテキストの名前をデバイス ID として使用します。

（注） ASA クラスタでは、選択したインターフェイスのプライマリユニットの IP アドレスが常に使用されます。

Cluster-id キーワードは、デバイス ID として、クラスタの個別の ASA ユニットのブート設定に一意の名前を指定します。

hostname キーワードは、ASA のホスト名をデバイス ID として使用することを指定します。

ipaddress *interface_name* キーワード引数のペアは、*interface_name* として指定されたインターフェイスの IP アドレスをデバイス ID として使用することを指定します。**ipaddress** キーワードを使用すると、syslog メッセージの送信元となるインターフェイスに関係なく、そのデバイス ID は指定された ASA のインターフェイス IP アドレスとなります。クラスタ環境では、**system** キーワードは、デバイス ID がインターフェイスのシステム IP アドレスとなることを指定します。このキーワードにより、デバイスから送信されるすべての syslog メッセージに単一の一貫したデバイス ID を指定できます。

string *text* キーワード引数のペアは、テキスト文字列をデバイス ID として使用することを指定します。文字列の長さは、最大で 16 文字です。

空白スペースを入れたり、次の文字を使用したりすることはできません。

- &（アンパサンド）
- '（一重引用符）
- "（二重引用符）
- <（小なり記号）
- >（大なり記号）
- ?（疑問符）

ステップ 4　スタートアップ コンフィギュレーションへの変更の保存

コマンドプロンプトで、**write memory** と入力します。

例：

```
> write memory
```

ASA デバイス向け NetFlow Secure Event Logging（NSEL）

ASA からの基本的な Syslog メッセージには、ASA によって報告されたイベントが脅威を示しているかどうかを Secure Cloud Analytics が判断するために必要な多くのデータが不足しています。Netflow Secure Event Logging（NSEL）は、そのデータを Secure Cloud Analytics に提供します。

「フローは、ネットワークデバイスを通過する、いくつかの共通プロパティを持つ一方向のパケットシーケンスとして定義されます。これらの収集されたフローは、外部デバイスである NetFlow コレクタにエクスポートされます。ネットワークフローは非常に細分化されています。たとえば、フローレコードには IP アドレス、パケット数とバイト数、タイムスタンプ、サービスのタイプ（ToS）、アプリケーションポート、入出力インターフェイスなどの詳細が含まれます。」[1]

Cisco ASA では、NetFlow バージョン 9 サービスがサポートされています。ASA の NSEL の導入は、フロー内の重要なイベントを示すレコードだけをエクスポートするステートフルな IP フローのトラッキング方式を提供します。ステートフル フロー トラッキングでは、追跡されるフローは一連のステートの変更を通過します。

このドキュメントでは、CDO マクロを使用して ASA に NetFlow を設定するための簡単なアプローチについて説明します。『Cisco NetFlow Implementation Guide』には、ASA に NetFlow を設定することに関する非常に詳細な説明が記載されており、このコンテンツに付随する貴重なリソースとなっています。

次の作業

「CDO マクロを使用して ASA デバイスの NSEL を設定する」に進みます。

関連記事

1. （『Cisco Systems NetFlow サービス エクスポート バージョン 9』。インターネット技術特別委員会、ネットワーク ワーキング グループ、Request for Comments（RFC）：3954、2004 年 10 月、B. Claise 編集。https://www.ietf.org/rfc/rfc3954.txt）

CDO マクロを使用して ASA デバイスの NSEL を設定する

ASA は、NetFlow Secure Event Logging（NSEL）を使用して詳細な接続イベントデータをレポートします。この接続イベントデータ（双方向フロー統計を含む）に Stealthwatch Cloud 分析を適用できます。この手順では、ASA デバイスで NSEL を設定し、NSEL イベントをフローコレクタに送信する方法について説明します。このケースでは、フローコレクタは Secure Event Connector（SEC）です。

この手順では、**Configure NSEL** マクロを参照します。

```
 flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate {{timeout_rate_in_mins}}
flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
flow-export active refresh-interval {{refresh_interval_in_mins}}
class-map {{flow_export_class_name}}
     match {{add_this_traffic_to_class_map}}
policy-map {{global_policy_map_name}}
     class {{flow_export_class_name}}
          flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}
service-policy {{global_policy_map_name}} global
logging flow-export-syslogs disable
show run flow-export
show run policy-map {{global_policy_map_name}}
show run class-map {{flow_export_class_name}}
```

クラスマップの一般名、グローバルポリシーに追加されたクラスマップなど、すべてのデフォルト値が入力された Configure NSEL マクロの例を次に示します。これらの手順を完了すると、マクロは次のようになります。

```
 flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate 60
flow-export delay flow-create 55
flow-export active refresh-interval 1
class-map flow_export_class_map
     match any
policy-map global_policy
     class flow_export_class_map
          flow-export event-type all destination {{SEC_IPv4_address}}
logging flow-export-syslogs disable
show run flow-export
show run policy-map global_policy
show run class-map flow_export_class_map
```

はじめる前に

次の情報を用意します。

- CDO マクロを初めて使用する場合は、次のトピックをお読みください。
  - デバイスの管理用 CLI マクロ （101 ページ）
    - CLI マクロの編集 （104 ページ）
    - CLI マクロの実行 （103 ページ）

- ASA からデータを受け取る SEC の IPv4 アドレス
- SEC にデータを送信する ASA のインターフェイス
- NetFlow イベントの転送に使用する UDP ポート番号「Secure Logging Analytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索 （396 ページ）」を参照してください。
- ASA グローバルポリシーの名前を決定する （367 ページ）

ワークフロー

CDO マクロを使用して ASA デバイスの NSEL を設定するには、次のワークフローに従います。各手順に従う必要があります。

1. [NSELの設定（Configuring NSEL）] マクロを開く （360 ページ）。
2. NSEL メッセージの宛先と SEC に送信される間隔の定義 （361 ページ）。
3. SEC に送信される NSEL イベントを定義するクラスマップの作成 （362 ページ）。
4. NSEL イベントのポリシーマップの定義 （363 ページ）。
5. 冗長な Syslog メッセージの無効化 （364 ページ）。
6. マクロのレビューと送信 （365 ページ）。

次の作業

[NSELの設定（Configuring NSEL）] マクロを開く （360 ページ）に移動して、前述のワークフローを開始します。

[NSELの設定（Configuring NSEL）] マクロを開く

始める前に

これは長いワークフローの最初の部分です。開始する前に CDO マクロを使用して ASA デバイスの NSEL を設定する （359 ページ） を参照してください。

ステップ 1 [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。

ステップ 2 適切なデバイスタイプのタブをクリックし、NetFlow セキュアイベントロギング（NSEL）を設定する ASA を選択します。

ステップ 3 [デバイスアクション] ペインで、[コマンドライン インターフェイス（Command Line Interface）] をクリックします。

ステップ 4 マクロスター  をクリックして、使用可能なマクロのリストを表示します。

ステップ 5 マクロのリストから、[NSELの設定（Configuring NSEL）] を選択します。

ステップ 6 [マクロ（Macro）] ボックスで、[パラメータの表示（View Parameters）] をクリックします。

次のタスク

NSEL メッセージの宛先と SEC に送信される間隔の定義 （361 ページ） に進みます。

NSEL メッセージの宛先と SEC に送信される間隔の定義

NSEL メッセージは、テナントに導入準備した SEC のいずれかに送信できます。以下の手順では、このセクションのマクロを参照しています。

flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}

flow-export template timeout-rate {{timeout_rate_in_mins}}

flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

flow-export active refresh-interval {{refresh_interval_in_mins}}

始める前に

この手順は、より大きなワークフローの一部です。始める前にCDO マクロを使用して ASA デバイスの NSEL を設定する （359 ページ）を参照してください。

ステップ 1 **flow-export destination** コマンドは、NetFlow パケットの送信先のコレクタを定義します。この場合、SEC に送信します。次のパラメータのフィールドに入力します。

- **{{interface}}**：NetFlow イベントの送信元である ASA のインターフェイス名を入力します。
- **{{SEC_IPv4_address}}**：SEC の IPv4 アドレスを入力します。SEC はフローコレクタとして機能します。
- **{{SEC_NetFlow_port}}**：NetFlow パケットが送信された SEC の UDP ポート番号を入力します。

ステップ 2 **flow-export template timeout-rate** コマンドは、テンプレートレコードがすべての設定された出力先に送信される間隔を指定します。

- **{{timeout_rate_in_mins}}**：テンプレートが再送信されるまでの分数を入力します。60 分の値を使用することをお勧めします。SEC はテンプレートを処理しません。数字を大きくすると、SEC へのトラフィックが減少します。

ステップ 3 **flow-export delay flow-create** コマンドは、flow-create イベントの送信を指定した秒数遅らせます。この値は、推奨されるアクティブタイムアウト値と一致し、ASA からエクスポートされるフローイベントの数を減らします。この場合、NSEL イベントが最初に CDO に表示されるのは、接続の終了時または接続の作成

から 55 秒以内のいずれか早い方となると考えてください。このコマンドが設定されていない場合は、遅延はなく、flow-create イベントはフローが作成された時点でエクスポートされます。

- **{{delay_flow_create_rate_in_secs}}**：flow-create イベントの送信間の遅延秒数を入力します。55 秒の値を使用することをお勧めします。

ステップ 4 **flow-export active refresh-interval** コマンドは、長時間フローのステータスの更新が ASA から送信される頻度を定義します。有効な値は 1 ～ 60 分です。[フロー更新間隔（Flow Update Interval）] フィールドで、**flow-export active refresh-interval** を **flow-export delay flow-create interval** よりも少なくとも 5 秒長く設定すると、flow-update イベントが flow-creation イベントの前に表示されなくなります。

- **{{refresh_interval_in_mins}}**：**値を 1 分にすることをお勧めします。**有効な値は 1 ～ 60 分です。

次のタスク

SEC に送信される NSEL イベントを定義するクラスマップの作成 （362 ページ） に進みます。

SEC に送信される NSEL イベントを定義するクラスマップの作成

マクロ内の次のコマンドは、クラス内のすべての NSEL イベントをグループ化し、そのクラスを Secure Event Connector（SEC）にエクスポートします。以下の手順では、このセクションのマクロを参照しています。

```
class-map {{flow_export_class_name}}
match {{add_this_traffic_to_class_map}}
```

始める前に

この手順は、より大きなワークフローの一部です。始める前にCDO マクロを使用して ASA デバイスの NSEL を設定する （359 ページ）を参照してください。

ステップ 1 **class-map** コマンドは、SEC にエクスポートされる NSEL トラフィックを識別するクラスマップに名前を付けます。

- **{{flow-export-class-name}}**：クラスマップの名前を入力します。名前の長さは最大 40 文字です。名前「class-default」と、「_internal」または「_default」で始まる名前はすべて予約されています。すべてのタイプのクラスマップで同じ名前空間が使用されるため、別のタイプのクラスマップですでに使用されている名前は再度使用できません。

ステップ 2 クラスマップに関連付けられる（一致する）トラフィックを識別します。**{{add_this_traffic_to_class_map}}** の値として、次のいずれかのオプションを選択します。

- **{{add_this_traffic_to_class_map}}** フィールドに **any** と入力します。NSEL トラフィックのすべてのトラフィックタイプが監視されます。**値「any」を使用することをお勧めします。**
- **{{add_this_traffic_to_class_map}}** フィールドに **access-list *name-of-access-list*** と入力します。作成したアクセスリストに関連付けられたすべてのトラフィックが関連付けられます。詳細については、Cisco

ASA NetFlow 実装ガイド [英語] の「Configure Flow-Export Actions Through Modular Policy Framework」を参照してください。

次のタスク

NSEL イベントのポリシーマップの定義 （363 ページ）に進みます。

NSEL イベントのポリシーマップの定義

このタスクでは、前のタスクで作成したクラスに NetFlow エクスポートアクションを割り当て、そのクラスを新しいポリシーマップに割り当てます。以下の手順では、このセクションのマクロを参照しています。

policy-map {{global_policy_map_name}}

class {{flow_export_class_name}}

flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}

始める前に

この手順は、より大きなワークフローの一部です。始める前にCDO マクロを使用して ASA デバイスの NSEL を設定する （359 ページ）を参照してください。

ステップ 1 **policy-map** コマンドは、ポリシーマップを作成します。次のタスクでは、このポリシーマップをグローバルポリシーに関連付けます。

- **{{global_policy_map_name}}**：ポリシーマップの名前を入力します。ファイアウォールの既存のグローバルポリシーがある場合は、その名前を使用することをお勧めします。グローバルポリシーのデフォルト名は **global_policy** です。ASA グローバルポリシーの名前を決定する新しいポリシーマップを作成し、『Cisco ASA NetFlow 実装ガイド』の「モジュラ ポリシー フレームワークを使用した flow-export アクションの設定」に従ってグローバルに適用すると、残りの検査ポリシーは非アクティブ化されます。

ステップ 2 **class** コマンドでは、SEC に送信される NSEL イベントを定義するクラスマップの作成 （362 ページ）で作成したクラスマップの名前が継承されます。

ステップ 3 **flow-export event-type** {{event-type}} **destination** {{IPv4_address}} コマンドは、フローコレクタ（この場合は SEC）に送信する必要があるイベントタイプを定義します。

- **{{event-type}}**：event_type キーワードは、フィルタリングされるサポートされているイベントの名前です。値「all」を使用することをお勧めします。
- **{{SEC_IPv4_address}}**：これは SEC の IPv4 アドレスです。その値は、NSEL メッセージの宛先と SEC に送信される間隔の定義 （361 ページ）で入力した値から継承されます。

次のタスク

冗長な Syslog メッセージの無効化 （364 ページ） に進みます。

冗長な Syslog メッセージの無効化

以下の手順では、このセクションのマクロを参照しています。コマンドを変更する必要はありません。

logging flow-export-syslogs disable

NetFlow でフロー情報をエクスポートできるようにすると、次の表に記載されている syslog メッセージが冗長になります。パフォーマンスの向上のためには、同じ情報が NetFlow を通してエクスポートされるため、冗長な syslog メッセージをディセーブルにすることをお勧めします。

（注） NSEL メッセージと syslog メッセージの両方がイネーブルにされている場合、2 つのロギングタイプ間が時系列順になる保証はありません。

syslog メッセージ	説明	NSEL イベント ID	NSEL 拡張イベント ID
106100	アクセス制御ルール（ACL）が発生するたびに生成されます。	1：フローが作成されました（ACL がフローを許可した場合）。 3：フローが拒否されました（ACL がフローを拒否した場合）。	0：ACL がフローを許可した場合。 1001：入力 ACL によってフローが拒否されました。 1002：出力 ACL によってフローが拒否されました。
106015	最初のパケットが SYN パケットではなかったため、TCP フローが拒否されました。	3：フローが拒否されました。	1004：最初のパケットが TCP SYN パケットではなかったため、フローが拒否されました。
106023	**access-group** コマンドによってインターフェイスに接続された ACL によってフローが拒否された場合。	3：フローが拒否されました。	1001：入力 ACL によってフローが拒否されました。 1002：出力 ACL によってフローが拒否されました。

syslog メッセージ	説明	NSEL イベント ID	NSEL 拡張イベント ID
302013、302015、302017、302020	TCP、UDP、GRE、および ICMP 接続の作成。	1：フローが作成されました。	0：無視します。
302014、302016、302018、302021	TCP、UDP、GRE、および ICMP 接続のティアダウン。	2：フローが削除されました。	0：無視します。 > 2000：フローが切断されました。
313001	デバイスへの ICMP パケットが拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。
313008	デバイスへの ICMP v6 パケットが拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。
710003	デバイスインターフェイスへの接続の試行が拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。

冗長なsyslogメッセージを無効にしない場合は、このマクロを編集して、次の行のみを削除できます。

logging flow-export-syslogs disable

後に NetFlow 関連の Syslog メッセージの無効化と再有効化の手順を実行することで、個別の syslog メッセージを有効化または無効化できます。

マクロのレビューと送信

始める前に

この手順は、より大きなワークフローの一部です。始める前に、「CDO マクロを使用して ASA デバイスの NSEL を設定する （359 ページ）」を参照してください。

ステップ 1 マクロのフィールドに入力したら、[確認] をクリックして、コマンドを ASA への送信前に確認します。

ステップ 2 コマンドへの応答に問題がなければ、[送信（Send）] をクリックします。

ステップ 3 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。

- [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。

CDO マクロを使用して ASA デバイスの NSEL を設定する （359 ページ） で説明されているワークフローが完了しました。

ASA から NetFlow Secure Event Logging（NSEL）構成を削除する

この手順では、Secure Event Connector（SEC）を NSEL フローコレクタとして指定する ASA で NetFlow Secure Event Logging（NSEL）の構成を削除する方法について説明します。この手順では、「CDO マクロを使用して ASA デバイスの NSEL を設定する」で説明されているマクロを元に戻します。

この手順では、このマクロを **DELETE NSEL** と呼びます。

```
policy-map {{flow_export_policy_name}}
no class {{flow_export_class_name}}
no class-map {{flow_export_class_name}}
no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}
no flow-export template timeout-rate {{timeout_rate_in_mins}}
no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
no flow-export active refresh-interval {{refresh_interval_in_mins}}
logging flow-export-syslogs enable
show run flow-export
show run policy-map {{flow_export_policy_name}}
show run class-map {{flow_export_class_name}}
```

DELETE-NSEL マクロを開く

ステップ 1 [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。

ステップ 2 適切なデバイスタイプのタブをクリックし、NetFlow セキュアイベントロギング（NSEL）の設定を削除する ASA を選択します。

ステップ 3 [デバイスアクション] ペインで、[コマンド ライン インターフェイス（Command Line Interface）] をクリックします。

ステップ 4 マクロスター  Macros をクリックして、使用可能なマクロのリストを表示します。

ステップ 5 マクロのリストで、[DELETE-NSEL] を選択します。

ステップ 6 [マクロ（Macro）] ボックスで、[パラメータの表示（View Parameters）] をクリックします。

マクロに値を入力して No コマンドを完成させる

ASA CLI では、コマンドの「no」形式を使用してそのコマンドを削除します。マクロのフィールドに入力して、コマンドの「no」形式を完成させます。

ステップ 1 policy-map {{flow_export_policy_name}}

- **{{flow_export_policy_name}}**：policy-map 名の値を入力します。

ステップ 2 no class {{flow_export_class_name}}

- **{{flow_export_class_name}}**：class-map 名の値を入力します。

ステップ 3 no class-map {{flow_export_class_name}}

- **{{flow_export_class_name}}**：class-map 名の値は、上記の手順から継承されます。

ステップ 4 no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}

- **{{interface}}**：NetFlow イベントの送信元である ASA のインターフェイス名を入力します。
- **{{IPv4_address}}**：SEC の IPv4 アドレスを入力します。SEC はフローコレクタとして機能します。
- **{{NetFlow_port}}**：NetFlow パケットが送信された SEC の UDP ポート番号を入力します。

ステップ 5 no flow-export template timeout-rate {{timeout_rate_in_mins}}

- **{{timeout_rate_in_mins}}**：flow-export template のタイムアウトレートを入力します。

ステップ 6 no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

- **{{delay_flow_create_rate_in_secs}}**：flow-export delay flow-create のレートを入力します。

ステップ 7 no flow-export active refresh-interval {{refresh_interval_in_mins}}

- **{{refresh_interval_in_mins}}**：flow-export active refresh-interval の間隔を入力します。

ASA グローバルポリシーの名前を決定する

ASA のグローバルポリシーの名前を決定するには、次の手順に従います。

ステップ 1 [デバイスとサービス] ページで、グローバルポリシーの名前を検索するデバイスを選択します。
ステップ 2 [デバイスアクション] ペインで、[>_コマンドリファレンス（>_Command Reference）] を選択します。
ステップ 3 コマンド ライン インターフェイス ウィンドウのプロンプトで、次のように入力します。

show running-config service-policy

以下の例の出力では、global_policy はグローバルポリシーの名前です。

例：

> **show running-config service-policy**

service-policy global_policy global

NSEL データフローのトラブルシューティング

CDO マクロを使用して ASA デバイスの NSEL を設定するしたら、次の手順を使用して、NSEL イベントが ASA から Cisco Cloud に送信されていること、および Cisco Cloud がそれらのイベントを受信していることを確認します。

NSEL イベントを Secure Event Connector（SEC）に送信してから Cisco Cloud に送信するように ASA を設定すると、データはすぐには流れないことに注意してください。ASA で NSEL 関連のトラフィックが生成されていると仮定すると、最初の NSEL パケットが到着するまでに数分かかることがあります。

（注） このワークフローは、「flow-export counters」コマンドと「capture」コマンドを単純に使用して NSEL データフローをトラブルシューティングする方法を示しています。これらのコマンドの使用法の詳細については、CLI ブック 1：Cisco ASA シリーズ CLI コンフィギュレーションガイド（一般的な操作）[英語] および Cisco ASA NetFlow 実装ガイド [英語] の「Monitoring NSEL」を参照してください。

次のタスクを実行します。

- NetFlow パケットが SEC に送信されていることを確認する
- NetFlow パケットが Cisco Cloud 受信されていることを確認する

NSEL イベントが SEC に送信されたことを確認する

次の 2 つのコマンドのいずれかを使用して、NSEL パケットが SEC に送信されていることを確認します。

- flow-export counters
- capture

「flow-export counters」コマンドは、送信中の flow-export パケットと NSEL エラーをチェックするために使用します。

- ASA が NSEL イベントを SEC に送信するように設定されていることを確認してください。「CDO マクロを使用して ASA デバイスの NSEL を設定する」を参照してください。
- SEC IP アドレスは、NSEL イベントのフローコレクタアドレスです。テナントに複数の SEC を導入準備している場合は、正しい IP アドレスを使用していることを確認してください。
- NetFlow イベントの転送に使用する UDP ポート番号を検索します。「Secure Logging Analytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。
- ASA でそこから NSEL イベントを送信するための推奨インターフェイスは管理インターフェイスです。お使いのインターフェイスとは異なる場合があります。

CDO の一括コマンドライン インターフェイスを使用して、NSEL に設定した ASA にこれらのコマンドを送信します。

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 [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] タブをクリックし、NSEL イベントを SEC に送信するように設定した ASA を選択します。

ステップ 4 右側の [デバイスアクション（Device Actions）] ペインで、[コマンド ライン インターフェイス（Command Line Interface）] をクリックします。

ステップ 5 `clear flow-export counters` コマンドを実行して、フローエクスポートカウンタをリセットします。これにより、エクスポートフローカウンタがクリアされてゼロになるため、新しいイベントの発生を簡単に知ることができます。

例：

```
> clear flow-export counters

Done!
```

ステップ 6 show flow-export counters コマンドを実行して、NSEL パケットの宛先、送信されたパケットの数、およびエラーを確認します。

例：

```
>show flow-export counters

destination: management 209.165.200.225 10425

Statistics:

packets sent 25000

エラー：

block allocation errors 0

invalid interface 0

template send failure 0

no route to collector 0

source port allocation 0
```

上記の出力では、宛先行は、NSEL イベントの送信元の ASA のインターフェイス、SEC の IP アドレス、SEC のポート 10425 を示しています。また、25000 のパケットが送信されたことも示しています。

エラーがなく、パケットが送信されている場合は、以下の「NetFlow パケットが Cisco Cloud 受信されていることを確認する」にスキップしてください。

エラーの説明：

- [ブロック割り当てエラー（block allocation errors）]：ブロック割り当てエラーを受け取った場合、ASA によってフローエクスポーターにメモリが割り当てられていません。

- 回復処置：Cisco Technical Assistance Center（TAC）に連絡してください。

- [無効なインターフェイス（invalid interface）]：NSELイベントをSECに送信しようとしていますが、フローエクスポート用に定義したインターフェイスがそれを行うように設定されていないことを示します。
  - 回復処置：NSEL の設定時に選択したインターフェイスを確認します。管理インターフェイスを使用することをお勧めします。お使いのインターフェイスが異なる場合があります。

- [テンプレート送信失敗（template send failure）]：NSEL を定義するためのテンプレートが正しく解析されませんでした。
  - 回復処置：Cisco Defense Orchestrator サポートへの連絡

- [コレクタへのルートがない（no route to collector）]：ASA から SEC へのネットワークルートがないことを示します。
  - 回復処置：
    - NSEL を設定したときに SEC に使用した IP アドレスが正しいことを確認してください。
    - SEC のステータスがアクティブで、最近のハートビートが送信されていることを確認します。「SDC に到達不能 （519 ページ）」を参照してください。
    - Secure Device Connector のステータスがアクティブで、最近のハートビートが送信されていることを確認します。

- [送信元ポートの割り当て（source port allocation）]：ASAにポート不良がある可能性を示しています。

「capture」コマンドを使用して、ASAからSECに送信されたNSELパケットをキャプチャする

- ASA が NSEL イベントを SEC に送信するように設定されていることを確認してください。「CDO マクロを使用して ASA デバイスの NSEL を設定する」を参照してください。
- SEC IP アドレスは、NSEL イベントのフローコレクタアドレスです。テナントに複数の SEC を導入準備している場合は、正しい IP アドレスを使用していることを確認してください。
- NetFlowイベントの転送に使用するUDPポート番号を検索します。「Secure Logging Analytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。
- ASA でそこから NSEL イベントを送信するための推奨インターフェイスは管理インターフェイスです。お使いのインターフェイスとは異なる場合があります。

CDO のCDO コマンドライン インターフェイスを使用するを使用して、NSEL に設定した ASA にこれらのコマンドを送信します。

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] 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] タブをクリックし、NSEL イベントを SEC に送信するように設定した ASA を選択します。

ステップ 4 右側の [デバイスアクション] ペインで、[コマンドライン インターフェイス（Command Line Interface）] をクリックします。

ステップ 5 コマンドウィンドウで、以下の [キャプチャ（capture）] コマンドを実行します。

>**capture***capture_name***interface***interface_name* **match udp any host** *IP_of_SEC***eq***NetFlow_port*

引数の説明

- *capture_name* は、パケットキャプチャの名前です。
- *interface_name* は、NSEL パケットが ASA から送信されるインターフェイスの名前です。
- *IP_of_SEC* は、SEC VM の IP アドレスです。
- *NetFlow_port* は、NSEL イベントが送信されるポートです。

これにより、パケットキャプチャが開始されます。

ステップ 6 キャプチャされたパケットを表示するには、**show capture** コマンドを実行します。

> show capture*capture_name*

ここで、*capture_name* は、前の手順で定義したパケットキャプチャの名前です。

キャプチャの時刻、パケットの送信元の IP アドレス、IP アドレス、およびパケットの送信先ポートを示す出力の例を次に示します。この例では、192.168.25.4 は SEC の IP アドレスであり、ポート 10425 は NSEL イベントを受信する SEC 上のポートです。

6 パケットがキャプチャされました

```
1: 14:23:51.706308 192.168.0.169.16431 > 192.168.25.4.10425: udp 476
2: 14:23:53.923017 192.168.0.169.16431 > 192.168.25.4.10425: udp 248
3: 14:24:07.411904 192.168.0.169.16431 > 192.168.25.4.10425: udp 1436
4: 14:24:07.411920 192.168.0.169.16431 > 192.168.25.4.10425: udp 1276
5: 14:24:21.021208 192.168.0.169.16431 > 192.168.25.4.10425: udp 112
6: 14:24:27.444755 192.168.0.169.16431 > 192.168.25.4.10425: udp 196
```

ステップ 7 パケットキャプチャを手動で停止するには、**capture stop** コマンドを実行します。

> capture *capture_name***stop**

ここで、*capture_name* は、前の手順で定義したパケットキャプチャの名前です。

NetFlow パケットが Cisco Cloud 受信されていることを確認する

はじめる前に

ASA から NSEL イベントが送信されていることを確認します。

ライブ NSEL イベントの確認

ライブイベントと履歴イベントの両方を確認します。

この手順では、過去 1 時間以内に Cisco Cloud が受信した NSEL イベントをフィルタ処理します。

ステップ 1 CDO の左側のメニューバーで、**[モニターリング（Monitoring）]** > **[イベントロギング]** を選択します。
ステップ 2 [ライブ（Live）] タブをクリックします。
ステップ 3 イベントフィルタを開いた状態でピン留めします。
ステップ 4 [ASAイベント（ASA Event）] セクションで、[NetFlow] がオンになっていることを確認します。
ステップ 5 [センサーID] フィールドで、NSEL イベントを送信するために設定した ASA の IPアドレスを入力します。
ステップ 6 フィルタの一番下の [NetFlowイベントを含める（Include NetFlow Events）] がオンになっていることを確認します。

NSEL のイベント履歴の確認

この手順では、指定した時間枠内に Cisco Cloud が受信した NSEL イベントをフィルタリングします。

ステップ 1 CDO で、左側のメニューバーにある **[モニタリング（Monitoring）]** > **[イベントロギング]** を選択します。
ステップ 2 [履歴（Historic）] タブをクリックします。
ステップ 3 イベントフィルタを開いた状態でピン留めします。
ステップ 4 [ASAイベント（ASA Event）] セクションで、[NetFlow] がオンになっていることを確認します。
ステップ 5 CDO が NSEL イベントを受信したことがあるかどうかを確認するために、時間を十分にさかのぼって [開始時刻（Start time）] を設定します。
ステップ 6 [センサーID] フィールドで、NSEL イベントを送信するために設定した ASA の IPアドレスを入力します。
ステップ 7 フィルタの一番下の [NetFlowイベントを含める（Include NetFlow Events）] がオンになっていることを確認します。

ASA イベント タイプ

イベントロギングページでのイベントの検索とフィルタリング場合、イベントタイプのリストから選択できますこれらのイベントタイプは、syslog ID のグループを表します。次の表は、どの ASA イベントタイプにどの syslog ID が含まれるかを示しています。特定の syslog ID の詳細については、『Cisco ASA シリーズ Syslog メッセージガイド』で検索できます。

一部の syslog イベントには、追加の属性「EventName」があります。属性:値のペアでフィルタ処理することにより、EventName 属性を使用してイベントテーブルをフィルタ処理し、イベントを見つけることができます。「Syslog イベントの EventName 属性」を参照してください。

ASA デバイス向け NetFlow Secure Event Logging（NSEL） は、syslog イベントとは異なります。NetFlow フィルタは、NSEL レコードになったすべての NetFlow イベント ID を検索します。これらの NetFlow イベント ID は、『Cisco ASA NetFlow 実装ガイド』で定義されています。

フィルタ名（Filter Name）	対応する Syslog イベントまたは NetFlow イベント
AAA	109001-109035 113001-113027
BotNet	338001-338310
フェールオーバー	101001-101005、102001、103001-103007、104001-104004、105001-105048 210001-210022 311001-311004 709001-709007
Firewall Denied	106001、106007、106012、106013、106015、106016、106017、106020、106021、106022、106023、106025、106027 Firewall Denied イベントは NetFlow に含まれている場合があり、syslog ID だけでなく NetFlow イベント ID と共に報告される場合もあります。

フィルタ名（Filter Name）	対応する Syslog イベントまたは NetFlow イベント
Firewall Traffic	106001-106100、108001-108007、110002-110003 201002-201013、209003-209005、215001 302002-302304、302022-302027、303002-303005、313001-313008、317001-317006、324000-324301、337001-337009 400001-400050、401001-401005、406001-406003、407001-407003、408001-408003、415001-415020、416001、418001-418002、419001-419003、424001-424002、431001-431002、450001 500001-500005、508001-508002 607001-607003、608001-608005、609001-609002、616001 703001-703003、726001 Firewall Traffic イベントは NetFlow に含まれている場合があり、syslog ID だけでなく NetFlow イベント ID と共に報告される場合もあります。
IPSec VPN	402001-402148、602102-602305、702304-702307
NAT	201002-201013、202001-202011、305005-305012
SSL VPN	716001-716060、722001-722053、723001-723014、724001-724004、725001-725015
NetFlow	0、1、2、3、5

関連情報：

- 一部の Syslog メッセージの EventGroup および EventGroupDefinition 属性 （443 ページ）
- Syslog イベントの EventName 属性

解析済みの ASA Syslog イベント

解析済みの syslog イベントは、他の syslog イベントよりも多くのイベント属性を含んでおり、特定の解析済みフィールドの検索を可能にします。SEC は、指定したすべての ASA イベントを Cisco Cloud に転送しますが、解析されるのは以下の表の syslog メッセージのみです。すべての解析済みの Syslog イベントは、識別しやすいように EventType が斜体で表示されます。

syslog ID	syslog カテゴリ	syslog メッセージの目的
106015	ファイアウォール	州外 TCP の拒否を表します。
106023	ファイアウォール	実際の IP パケットが ACL によって拒否されました。このメッセージは、ACL に対して **log** オプションをイネーブルにしていない場合でも表示されます。
106100	アクセスリスト/ユーザーセッション	パケットは ACL によって許可または拒否されました。
113019	ユーザー認証（User Authentication）	クリティカルな AnyConnect
302013、302015、302017、302020	ユーザ セッション	TCP、UDP、GRE、および ICMP 接続作成の接続開始 syslog と接続終了 syslog。
302014, 302016, 302018, 302021	ユーザ セッション	TCP、UDP、GRE、および ICMP 接続作成の接続開始 syslog と接続終了 syslog。
302020 ～ 302021	ユーザ セッション	ICMP セッションの確立と解除。
305006	ユーザーセッション/NAT および PAT	NAT 接続の失敗
305011 ～ 305014	ユーザーセッション/NAT および PAT	NAT 確立/解除関連
313001、313008	IP スタック	ボックスへの接続が拒否されたことを表します。
414004	システム（System）	クリティカルな AnyConnect
609001 ～ 609002	ファイアウォール	ネットワーク状態コンテナは、ゾーンに接続されたホスト **ip-address** 用に予約済み/削除済みでした。
710002、710004、710005	ユーザ セッション	ボックスへの接続の失敗
710003	ユーザ セッション	ボックスへの接続が拒否されたことを表します。

syslog ID	syslog カテゴリ	syslog メッセージの目的
746012、746013	ユーザ セッション	クリティカルな AnyConnect

syslog の詳細な説明については、『Cisco ASA Series Syslog Messages』を参照してください。

関連情報：

- コマンドライン インターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信
- イベントロギングページでのイベントの検索とフィルタリング

Cisco Secure Firewall Cloud Native 向け Secure Logging and Analytics（SaaS）

Secure Analytics and Logging（SaaS）を使用すると、Cisco Secure Firewall Cloud Native からすべての syslog イベントと NetFlow Secure Event Logging（NSEL）をキャプチャし、Cisco Defense Orchestrator（CDO）の 1 か所で表示できます。

イベントは Cisco Cloud に保存され、CDO の [イベントロギング（Event Logging）] ページから確認できます。このページでイベントをフィルタリングして確認し、ネットワークでトリガーされているセキュリティルールを明確に理解できます。それらの機能は、**Logging and Troubleshooting** パッケージで提供されます。

Logging Analytics and Detection パッケージ（旧 **Firewall Analytics and Logging** パッケージ）を使用すると、システムは Cisco Secure Cloud Analytics 動的エンティティモデリングを FTD イベントに適用し、行動モデリング分析を使用して Cisco Secure Cloud Analytics の観測値とアラートを生成できます。**Total Network Analytics and Monitoring** パッケージを使用すると、システムは FTD イベントとネットワークトラフィックの両方に動的エンティティモデリングを適用し、観測値とアラートを生成します。Cisco Single Sign-On を使用して、CDO から、プロビジョニングされた Secure Cloud Analytics ポータルを相互起動できます。

CDO イベントビューアでの Cisco Secure Firewall Cloud Native イベントの表示方法

Syslog イベントと NSEL イベントは、ロギングが Cisco Secure Firewall Cloud Native で有効になっていて、ネットワークトラフィックがアクセス制御ルールの基準に一致するときに生成されます。イベントが Cisco Cloud に保存されたら、CDO で表示できます。

複数の Secure Event Connector（SEC）をインストールし、任意のデバイスでルールによって生成されたイベントを、syslog サーバーであるかのように任意の SEC に送信できます。SEC はイベントを Cisco Cloud に転送します。同じイベントをすべての SEC に転送しないでください。Cisco Cloud に送信されるイベントを複製すると、日次取り込み率が不必要に高くなります。

Syslog および NSEL イベントが Secure Event Connector を介して Cisco Secure Firewall Cloud Native から Cisco Cloud に送信される方法

Logging and Troubleshooting の基本ライセンスでは、Cisco Secure Firewall Cloud Native イベントが Cisco Cloud に到達する方法は次のとおりです。

1. クラスタエンドポイント、名前空間、およびトークンを使用して、Cisco Secure Firewall Cloud Native を CDO に導入準備します。.
2. Cisco Secure Firewall Cloud Native を設定して、syslog および NSEL イベントを、syslog サーバーであるかのように任意の SEC に転送し、デバイスでのロギングを有効にします。
3. SEC は、イベントが保存されている Cisco Cloud にイベントを転送します。
4. CDO は、設定したフィルタに基づいて、Cisco Cloud からのイベントをイベントビューアに表示します。

Logging Analytics and Detection または **Total Network Analytics and Monitoring** ライセンスでは、次のことも発生します。

1. Cisco Secure Cloud Analytics は、Cisco Cloud に保存されている Cisco Secure Firewall Cloud Native syslog イベントに分析を適用します。
2. 生成された観測値とアラートには、CDO ポータルに関連付けられた Cisco Secure Cloud Analytics ポータルからアクセスできます。
3. CDO ポータルから、Cisco Secure Cloud Analytics ポータルをクロス起動して、観察値とアラートを確認できます。

ソリューションで使用されるコンポーネント

Secure Device Connector（SDC）：SDC は、CDO を Cisco Secure Firewall Cloud Native に接続します。Cisco Secure Firewall Cloud Native のログイン情報は SDC に保存されます。詳細については、Secure Device Connector（SDC） （3 ページ）を参照してください。

Secure Event Connector（SEC）：SEC は、Cisco Secure Firewall Cloud Native からイベントを受信し、Cisco Cloud に転送するアプリケーションです。Cisco Cloud に転送されたイベントは、CDO の [イベントロギング] ページで確認したり、Cisco Secure Cloud Analytics で分析したりできます。使用環境に応じて、SEC は Secure Device Connector（ある場合）にインストールされます。または、ネットワーク内で維持する独自の CDO コネクタ仮想マシンにインストールされます。詳細については、Secure Event Connector （397 ページ）を参照してください。

Cisco Secure Firewall Cloud Native：Cisco Secure Firewall Cloud Native は、Kubernetes（K8s）オーケストレーションを使用して、シスコの業界をリードするセキュリティをクラウド ネイティブ フォーム ファクタ（CNFW）にシームレスに拡張し、拡張性と管理性を実現します。Amazon Elastic Kubernetes Service（Amazon EKS）を使用すると、AWS クラウドで Kubernetes アプリケーションを柔軟に開始、実行、スケーリングできます。Amazon EKS は、可用性が高く安全なクラスタを提供し、パッチ適用、ノードのプロビジョニング、更新などの主要なタスクを自動化するのに役立ちます。

Cisco Secure Cloud Analytics は動的エンティティモデリングを Cisco Secure Firewall Cloud Native イベントに適用し、この情報に基づいて検出を生成します。これにより、ネットワークから収集されたテレメトリの詳細な分析が可能になり、ネットワークトラフィックの傾向を特定し、異常な動作を調べることができます。**Logging Analytics and Detection** または **Total Network Analytics and Monitoring** ライセンスをお持ちの場合は、このサービスを利用できます。

ライセンシング

このソリューションを設定するには、次のアカウントとライセンスが必要です。

- **Cisco Defense Orchestrator**。CDO テナントが必要です。
- **Secure Device Connector**。Secure Device Connector 用の個別のライセンスはありません。
- **Secure Event Connector**。Secure Event Connector 用の個別のライセンスはありません。
- **Secure Logging Analytics（SaaS）**。「Security Analytics and Logging ライセンスの表」を参照してください。
- **Cisco Secure Firewall Cloud Native**。基本ライセンス以上。

Security Analytics and Logging ライセンス

Security Analytics and Logging（SaaS）を実装するには、次のいずれかのライセンスを購入する必要があります。

ライセンス名	提供される機能	利用可能なライセンス期間	機能の前提条件
Logging and Troubleshooting	• ライブフィードと履歴ビューの両方で、CDO 内の Cisco Secure Firewall Cloud Native イベントとイベントの詳細を表示します。	• 1 年 • 3 年 • 5 年	• CDO • ソフトウェアバージョン 9.6 以降を実行しているオンプレミスの Cisco Secure Firewall Cloud Native 展開。 • Cisco Secure Firewall Cloud Native イベントを Cisco Cloud に渡すための 1 つ以上の SEC の展開。

ライセンス名	提供される機能	利用可能なライセンス期間	機能の前提条件
Logging Analytics and Detection（旧 **Firewall Analytics and Monitoring**）	**Logging and Troubleshooting** の機能に加えて、以下の機能 • 動的エンティティモデリングと行動分析をイベントに適用します。 • イベントデータに基づいて Cisco Secure Cloud Analytics でアラートを開き、CDO イベントビューアからクロス起動します。	• 1 年 • 3 年 • 5 年	• CDO • ソフトウェアバージョン 9.6 以降を実行しているオンプレミスの Cisco Secure Firewall Cloud Native 展開。 • Cisco Secure Firewall Cloud Native イベントを Cisco Cloud に渡すための 1 つ以上の SEC の展開。 • 新たにプロビジョニングされたか、または既存の Cisco Secure Cloud Analytics ポータル。

ライセンス名	提供される機能	利用可能なライセンス期間	機能の前提条件
Total Network Analytics and Monitoring	**Logging Analytics and Detection** の機能に加えて、以下の機能 • 動的エンティティモデリングと行動分析を Cisco Secure Firewall Cloud Native イベント、オンプレミスのネットワークトラフィック、およびクラウドベースのネットワークトラフィックに適用します。 • Cisco Secure Firewall Cloud Native イベントデータ、Cisco Secure Cloud Analytics センサーによって収集されたオンプレミスのネットワークトラフィックのフローデータ、および Cisco Secure Cloud Analytics に渡されるクラウドベースのネットワークトラフィックの組み合わせに基づいて、Cisco Secure Cloud Analytics でアラートを開き、CDO イベントビューアからクロス起動します。	• 1 年 • 3 年 • 5 年	• CDO • ソフトウェアバージョン 9.6 以降を実行しているオンプレミスの Cisco Secure Firewall Cloud Native 展開。 • イベントを Cisco Cloud に渡すための 1 つ以上の SEC の展開。 • ネットワークトラフィックのフローデータをクラウドに渡すための少なくとも 1 つの Cisco Secure Cloud Analytics センサーバージョン 4.1 以降の展開、または、ネットワークトラフィックのフローデータを Cisco Secure Cloud Analytics に渡すためのクラウドベースと統合された Cisco Secure Cloud Analytics の展開。 • 新たにプロビジョニングされたか、または既存の Cisco Secure Cloud Analytics ポータル。

データプラン

導入準備された Cisco Secure Firewall Cloud Native から Cisco Cloud が毎日受け取るイベント数を反映したデータプランを購入する必要があります。これは「日次取り込み率」と呼ばれます。Logging Volume Estimator ツールを使用して、日次取り込み率を推定でき、率が変化すると、データプランを更新できます。

データプランは、1 GB の日次ボリューム単位で、1 年、3 年、または 5 年の期間で利用できます。データプランの詳細については、Secure Logging Analytics（SaaS）発注ガイド [英語] を参照してください。

（注） Security Analytics and Logging ライセンスとデータプランがある場合、その後は別のライセンスを取得するだけで済み、別のデータプランを取得する必要はありません。ネットワークトラフィックのスループットが変化した場合は、別のデータプランを取得するだけで済み、別の Security Analytics and Logging ライセンスを取得する必要はありません。

30 日間の無料トライアル

CDO にログインし、**[モニタリング（Monitoring）]** > **[イベントロギング]** タブに移動して、30 日間のリスクフリーのトライアルをリクエストできます。30 日間のトライアルが終了したら、Secure Logging Analytics（SaaS）発注ガイド [英語] の手順に従って、Cisco Commerce Workspace（CCW）からサービスを継続するために必要なイベントデータボリュームを注文できます。

次のステップ

に進みます。 Secure Firewall Cloud Native のセキュアロギング分析（SaaS）の導入 （381 ページ）

Secure Firewall Cloud Native のセキュアロギング分析（SaaS）の導入

はじめる前に

- 「Cisco Secure Firewall Cloud Native 向け Secure Logging and Analytics（SaaS） （376 ページ）」を参照して、次の点を確認してください。
  - Cisco Cloud へのイベントの送信方法
  - ソリューションに含まれるアプリケーション
  - 必要なライセンス
  - 必要なデータプラン
- すでにマネージドサービス プロバイダーまたは CDO セールス担当者に問い合わせて CDO テナントを作成しました。

- を確認してください。SDC を使用して CDO を Secure Firewall Cloud Native に接続することは「ベストプラクティス」と考えられますが、必須ではありません。

  Secure Device Connector（SDC） （3 ページ）を確認してください。SDC を使用して CDO を Secure Firewall Cloud Native に接続することは「ベストプラクティス」と考えられますが、必須ではありません。
- ネットワークで SDC を展開する場合、次のいずれかの方法を使用してインストールできます。
  - 「CDO の VM イメージを使用した Secure Device Connector の展開 （7 ページ）」を参照し、CDO で準備した VM イメージを使用して SDC をインストールします。これが推奨される最も簡単な SDC の展開方法です。
  - 自身の VM 上での Secure Device Connector の展開 （12 ページ） を使用します。
- Secure Event Connector をインストールする、任意の Secure Firewall Cloud Native から、テナントに導入準備された任意の SEC にイベントを送信できます。
- アカウントのユーザー向けに新規 Cisco Secure Sign-On アカウントの作成と Duo 多要素認証の設定しました。

Cisco Security Analytics and Logging（SaaS）の展開と Secure Event Connector を介した Cisco Cloud へのイベント送信のワークフロー

1. 上の「はじめる前に」を参照し、環境が適切に構成されていることを確認してください。
2. クラスタエンドポイント、名前空間、およびトークンを使用して、Secure Firewall Cloud Native デバイスを導入準備します。
3. Secure Firewall Cloud Native Syslog イベントの Cisco Cloud への送信 （384 ページ）。
4. Cisco Secure Firewall Cloud Native デバイス向け NSEL の設定 （387 ページ）。
5. CDOにイベントが表示されていることを確認します。ナビゲーションバーから、[モニターリング（Monitoring）] > [イベントロギング（Event Logging）] を選択します。ライブイベントを表示するには、[ライブ] タブをクリックします。
6. [Firewall Analytics and Monitoring] ライセンスや [Total Network Analytics and Monitoring] ライセンスがある場合は、次のセクション「**Cisco Secure Cloud Analytics を使用したイベントの分析**」に進みます。

Cisco Secure Cloud Analytics を使用したイベントの分析

[Firewall Analytics and Monitoring] ライセンスや [Total Network Analytics and Monitoring] ライセンスがある場合は、先行するステップに加えて、次の手順を実行します。

1. Cisco Secure Cloud Analytics ポータルのプロビジョニング （418 ページ）。
2. [Total Network Analytics and Monitoring] ライセンスを購入した場合は、1 つ以上の Secure Cloud Analytics センサーを内部ネットワークに展開します。「総合的なネットワーク分析

およびレポーティングのための Cisco Secure Cloud Analytics センサーの展開 （420 ページ）」を参照してください。

3. Cisco Single Sign-On ログイン情報に関連付ける Secure Cloud Analytics ユーザーアカウントを作成するようにユーザーに勧めます。「Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （421 ページ）」を参照してください。

4. CDO から Secure Cloud Analytics をクロス起動し、FTD イベントから生成される Secure Cloud Analytics アラートをモニタします。「Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （421 ページ）」を参照してください。

CDO からのクロス起動による Cisco Secure Cloud Analytics アラートの確認

Firewall Analytics and Monitoring ライセンスまたは **Total Network Analytics and Monitoring** ライセンスにより、CDO から Secure Cloud Analytics をクロス起動して、FTD イベントから生成されるアラートをモニタできます。

詳細については、次の項目を参照してください。

- CDO へのサインイン
- Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （421 ページ）
- Cisco Secure Cloud Analytics とダイナミック エンティティ モデリング
- ファイアウォールイベントに基づくアラートの使用

Secure Event Connector に関する問題のトラブルシューティング

ステータス情報とロギング情報の収集については、次のトラブルシューティングトピックを使用してください。

- SEC オンボーディング失敗のトラブルシューティング
- イベントロギングのトラブルシューティング ログ ファイル
- Secure Event Connector の状態を把握するためのヘルスチェックの使用

ワークフロー

「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」では、Cisco Security Analytics and Logging から生成されたイベントを使用して、ユーザーがネットワークリソースにアクセスできなかった原因を特定する方法について説明しています。

「ファイアウォールイベントに基づくアラートの使用」も参照してください。

Secure Firewall Cloud Native Syslog イベントの Cisco Cloud への送信

この手順では、Secure Firewall Cloud Native の syslog イベントを Secure Event Connector（SEC）に転送してから、ロギングを有効にする方法について説明します。以下の手順では、ワークフローの完了に必要な事柄のみを説明します。

（注） コマンドは、ファイアウォールの構成ファイルに入力する必要があります。

始める前に

注目 この手順は、デバイスの構成ファイルのシンタックスに精通している上級ユーザーを対象としています。この手法では、Defense Orchestrator に保存されている構成ファイルのコピーに直接変更を加えます。そのため、変更を加える前に、既存のデバイス設定をバックアップすることをお勧めします。必要に応じて、バックアップ設定を復元できます。

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。
2. [デバイス] タブをクリックします。
3. 適切なデバイスタイプタブをクリックし、設定を変更する Secure Firewall Cloud Native デバイスを選択します。
4. 右側の [管理（Management] ペインで、[設定（Configuration）] をクリックします。
5. [ダウンロード（Download）] をクリックします。

ステップ 1 [デバイスの設定（Device Configuration）] タブで、[編集] をクリックします。

ステップ 2 構成ファイルで、「snmp-server-config」に先立つ任意の場所に新しいCRDエントリを作成し、以下で説明するコマンドを入力します。

コマンド

```
########## CRD ### name: entry-name, order: order-number, generation: 1 ##########
           logging enable
           logging timestamp
           logging trap {severity_level | message_list}
           logging list name {level level [class message_class] | message start_id[-end_id]}
           logging host interface_name SEC_IP_address [[tcp/port] | [udp/port]]
           logging host interface_name SEC_IP_address [[tcp/port] | [udp/port]]
           logging permit-hostdown
```

例

```
########## CRD ### name: syslog-events, order: 4, generation: 3 ##########
           logging enable
           logging timestamp
           logging list sfcn_syslogs_to_cloud level critical
           logging list sfcn_syslogs_to_cloud level warnings class ha
```

```
logging list sfcn_syslogs_to_cloud message 302013-302018
logging trap sfcn_syslogs_to_cloud
logging host outside 192.168.1.5 17/10125
logging host outside 192.168.1.5 6/10025
logging permit-hostdown
```

- **entry-name**：CRD エントリの名前を指定します。名前に下線「_」を使用しないでください。
- **order-number**：コマンドを任意の順に実行する順序を指定します。構成ファイルで使用されている最大の番号の前にある一意の番号である必要があります。
- **logging enable**：個々のルールではなく、デバイス全体に対してロギングが有効になります。注：現時点では、CDO はセキュアロギングの有効化をサポートしていません。
- **logging timestamp**：logging timestamp コマンドを使用して、syslog メッセージがファイアウォールで発信された日付と時刻をメッセージに追加します。タイムスタンプの値は、SyslogTimestamp フィールドに表示されます。
- **logging trap** {severity_level | message_list}：

  次のコマンドを使用して、syslog サーバーに送信する syslog メッセージを指定します。

  例：

  ```
  logging trap 3
            logging trap sfcn_syslogs_to_cloud
  ```

  重大度として、値（1 ～ 7）または名前を指定できます。たとえば重大度を 3 に設定すると、SFCN は、重大度が 3、2、および 1 の syslog メッセージを送信します。

  message_list 引数は、カスタムイベントリストを作成した場合、そのリストの名前に置き換えられます。カスタムイベントリストの指定に必要な操作は、そのリストにある syslog メッセージを Secure Event Connector に送信することだけです。上記の例では、sfcn_syslogs_to_cloud がイベントリストの名前です。

  message_list を使用すると、Cisco Cloud に送信する syslog メッセージを明確に指定できるため、費用を節約できます。

- **logging list** *name* {**level** *level* [class message_class] | **message** start_id[-end_id]}

  このコマンドシンタックスを使用して、ファイアウォールに **logging list** コマンドを発行します。

  name 引数には、リストの名前を指定します。level level キーワードと引数のペアは、重大度を指定します。キーワードと引数のペア **class** *message_class* により、特定のメッセージクラスが指定されます。キーワードと引数のペア **message** start_id [-end_id] により、個々の syslog メッセージ番号または番号の範囲が指定されます。

  他の基準に基づいて syslog メッセージをイベントリストに追加します。

  前回の手順で使用したものと同じコマンドを入力し、既存のメッセージリストの名前と追加基準を指定します。リストに追加する基準ごとに、新しいコマンドを入力します。たとえば、リストに追加される syslog メッセージの基準として、次の基準を指定できます。

  - ID が 302013 ～ 302018 の範囲の syslog メッセージ。
  - 重大度が critical 以上（emergency、alert、または critical）のすべての syslog メッセージ。

- 重大度が warning 以上（emergency、alert、critical、error、または warning）のすべての HA クラス syslog メッセージ。

（注） syslog メッセージは、これらの条件のいずれかを満たす場合にログに記録されます。syslog メッセージが複数の条件を満たす場合、そのメッセージは一度だけログに記録されます。

- **logging host** interface_name SEC_IP_address [[tcp/port] | [udp/port]]
- **logging host** interface_name SEC_IP_address [[tcp/port] | [udp/port]]

TCP または UDP を使用して、SEC が syslog サーバーであるかのように、SEC にメッセージを送信するように Secure Firewall Cloud Native を設定します。SEC は、IPv4 アドレスまたは IPv6 アドレスを使用できます。TCP ポートと UDP ポートのいずれかにイベントを送信します。どのポートを使用するかを判断するには、「Cisco Security Analytics and Logging に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。

logging host interface_name SEC_IP_address [[tcp/port] | [udp/port]]

logging host コマンドシンタックスの例を次に示します。

```
logging host outside 192.168.1.5 tcp/10125
          logging host outside 192.168.1.5 udp/10025
          logging host outside 2002::1:1 tcp/10125
          logging host outside 2002::1:1 udp/10025
```

interface_name 引数は、syslog サーバーへのメッセージの送信元である Secure Firewall Cloud Native インターフェイスを指定します。SDC との通信に使用されるのと同じ Secure Firewall Cloud Native インターフェイスから、SEC に syslog メッセージを送信するのが「ベストプラクティス」です。

SEC_IP_address 引数には、SEC がインストールされている VM の IP アドレスが含まれている必要があります。

キーワードと引数のペア **tcp/port** または **udp/port** は、TCP プロトコルと関連するポート、または UDP プロトコルと関連するポートのいずれかを使用して、syslog メッセージが送信されるように設定します。UDP または TCP のいずれかを使用して syslog サーバーにデータを送信するように Secure Firewall Cloud Native を設定することはできますが、両方を使用するように設定することはできません。プロトコルを指定しない場合、デフォルトのプロトコルは UDP です。

TCP を指定すると、Secure Firewall Cloud Native は syslog サーバーの障害を検出し、セキュリティ保護として、Secure Firewall Cloud Native 経由の新しい接続をブロックします。TCP syslog サーバーへの接続の状態に関係なく新しい接続を許可するには、手順 b を参照してください。UDP を指定すると、syslog サーバーが動作しているかどうかにかかわらず、Secure Firewall Cloud Native は引き続き新しい接続を許可します。

（注） Secure Firewall Cloud Native メッセージを 2 台の別個の syslog サーバーに送信する場合は、もう一方の syslog サーバーの適切なインターフェイス、IP アドレス、プロトコル、およびポートを使用して、2 番目の logging host コマンドを実行できます。

- **logging permit-hostdown**

  （オプション）TCP 経由で SEC にイベントを送信し、SEC がダウンしているものの、Secure Firewall Cloud Native のログキューがいっぱいである場合、新しい接続はブロックされます。新しい接続は、syslog サーバーがバック アップされ、ログ キューがいっぱいでなくなった後に再度許可されます。

TCP syslog サーバーへの接続の状態に関係なく新しい接続を許可するには、このコマンドを使用して、TCP 接続された syslog サーバーがダウンしたときに新しい接続をブロックする機能を無効にします。

ステップ 3 [保存（**Save**）] をクリックします。

ステップ 4 すべてのデバイスの構成変更のプレビューと展開。

Cisco Secure Firewall Cloud Native デバイス向け NetFlow セキュアイベントロギング（NSEL）

Secure Firewall Cloud Native からの基本的な Syslog メッセージには、 Secure Firewall Cloud Native によって報告されたイベントが脅威を示しているかどうかを Cloud Cisco Secure Cloud Analytics が判断するために必要な多くのデータが不足しています。Netflow Secure Event Logging（NSEL）は、そのデータを Secure Cloud Analytics に提供します。

「フローは、ネットワークデバイスを通過する、いくつかの共通プロパティを持つ一方向のパケットシーケンスとして定義されます。これらの収集されたフローは、外部デバイスである NetFlow コレクタにエクスポートされます。ネットワークフローは非常に細分化されています。たとえば、フローレコードには IP アドレス、パケット数とバイト数、タイムスタンプ、タイプオブサービス（ToS）、アプリケーションポート、入出力インターフェイスなどの詳細が含まれます。」1

Secure Firewall Cloud Native では、NetFlow バージョン 9 サービスがサポートされています。Secure Firewall Cloud Native の NSEL を実装することで、フロー内の重要なイベントを示すレコードだけをエクスポートする、ステートフルな IP フローのトラッキング方式が可能となります。ステートフル フロー トラッキングでは、追跡されるフローは一連のステートの変更を通過します。

このドキュメントでは、 構成ファイル内の一連のコマンドを使用して、Secure Firewall Cloud Native デバイスに NetFlow を設定する簡単な方法について説明します。『Cisco NetFlow Implementation Guide』には、Secure Firewall Cloud Native に NetFlow を設定することに関する非常に詳細な説明が記載されており、このコンテンツに付随する貴重なリソースとなっています。

Cisco Secure Firewall Cloud Native デバイス向け NSEL の設定

Secure Firewall Cloud Native デバイスは、NetFlow Secure Event Logging（NSEL）を使用して詳細な接続イベントデータをレポートします。この接続イベントデータ（双方向フロー統計を含む）に Cisco Secure Cloud Analytics を適用できます。この手順では、Secure Firewall Cloud Native デバイスで NSEL を設定し、それらの NSEL イベントをフローコレクタに送信する方法について説明します。このケースでは、フローコレクタは Secure Event Connector（SEC）です。

この手順では、ファイアウォールの構成ファイルに入力する一連のコマンドに言及します。

ステップ 1 [デバイスの設定（Device Configuration）] タブで、[編集（Edit）] をクリックします。

ステップ 2 構成ファイルで、「snmp-server-config」に先立つ任意の場所に新しいCRDエントリを作成し、以下で説明するコマンドを入力します。

コマンド

```
########## CRD ### name: entry-name, order: order-number, generation: 1 ##########
flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
    flow-export template timeout-rate {{timeout_rate_in_mins}}
    flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
    flow-export active refresh-interval {{refresh_interval_in_mins}}
    class-map {{flow_export_class_name}}
         match {{add_this_traffic_to_class_map}}
    policy-map {{global_policy_map_name}}
         class {{flow_export_class_name}}
              flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}
    service-policy {{global_policy_map_name}} global
    logging flow-export-syslogs disable
    show run flow-export
    show run policy-map {{global_policy_map_name}}
    show run class-map {{flow_export_class_name}}
```

クラスマップの一般名、および global_policy に追加されたクラスマップなど、すべてのデフォルト値が入力された例を次に示します。

```
########## CRD ### name: nsel-config, order: 5, generation: 1 ##########
    flow-export destination outside {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
    flow-export template timeout-rate 60
    flow-export delay flow-create 55
    flow-export active refresh-interval 1
    class-map flow_export_class_map
         match any
    policy-map global_policy
         class flow_export_class_map
              flow-export event-type all destination {{SEC_IPv4_address}}
    service-policy global_policy global
    logging flow-export-syslogs disable
    show run flow-export
    show run policy-map global_policy
    show run class-map flow_export_class_map
```

ステップ 3 [保存（Save）] をクリックします。

ステップ 4

NSEL メッセージの宛先と SEC に送信される間隔の定義

NSELメッセージは、テナントに導入準備したSECのいずれかに送信できます。以下の手順では、このセクションのマクロを参照しています。

flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}

flow-export template timeout-rate {{timeout_rate_in_mins}}

flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

flow-export active refresh-interval {{refresh_interval_in_mins}}

始める前に

この手順は、より大きなワークフローの一部です。始める前にCDO マクロを使用して ASA デバイスの NSEL を設定する （359 ページ）を参照してください。

ステップ 1 **flow-export destination** コマンドは、NetFlow パケットの送信先のコレクタを定義します。この場合、SEC に送信します。次のパラメータのフィールドに入力します。

- **{{interface}}**：NetFlow イベントの送信元である ASA のインターフェイス名を入力します。
- **{{SEC_IPv4_address}}**：SEC の IPv4 アドレスを入力します。SEC はフローコレクタとして機能します。
- **{{SEC_NetFlow_port}}**：NetFlow パケットが送信された SEC の UDP ポート番号を入力します。

ステップ 2 **flow-export template timeout-rate** コマンドは、テンプレートレコードがすべての設定された出力先に送信される間隔を指定します。

- **{{timeout_rate_in_mins}}**：テンプレートが再送信されるまでの分数を入力します。60 分の値を使用することをお勧めします。SEC はテンプレートを処理しません。数字を大きくすると、SEC へのトラフィックが減少します。

ステップ 3 **flow-export delay flow-create** コマンドは、flow-create イベントの送信を指定した秒数遅らせます。この値は、推奨されるアクティブタイムアウト値と一致し、ASA からエクスポートされるフローイベントの数を減らします。この場合、NSEL イベントが最初に CDO に表示されるのは、接続の終了時または接続の作成から 55 秒以内のいずれか早い方となると考えてください。このコマンドが設定されていない場合は、遅延はなく、flow-create イベントはフローが作成された時点でエクスポートされます。

- **{{delay_flow_create_rate_in_secs}}**：flow-create イベントの送信間の遅延秒数を入力します。55 秒の値を使用することをお勧めします。

ステップ 4 **flow-export active refresh-interval** コマンドは、長時間フローのステータスの更新が ASA から送信される頻度を定義します。有効な値は 1 ～ 60 分です。[フロー更新間隔（Flow Update Interval）] フィールドで、**flow-export active refresh-interval** を **flow-export delay flow-create interval** よりも少なくとも 5 秒長く設定すると、flow-update イベントが flow-creation イベントの前に表示されなくなります。

- **{{refresh_interval_in_mins}}**：**値を 1 分にすることをお勧めします。**有効な値は 1 ～ 60 分です。

次のタスク

SEC に送信される NSEL イベントを定義するクラスマップの作成 （362 ページ） に進みます。

SEC に送信される NSEL イベントを定義するクラスマップの作成

マクロ内の次のコマンドは、クラス内のすべてのNSELイベントをグループ化し、そのクラスを Secure Event Connector（SEC）にエクスポートします。以下の手順では、このセクションのマクロを参照しています。

class-map {{flow_export_class_name}}

match {{add_this_traffic_to_class_map}}

始める前に

この手順は、より大きなワークフローの一部です。始める前にCDO マクロを使用して ASA デバイスの NSEL を設定する （359 ページ）を参照してください。

ステップ 1 **class-map** コマンドは、SEC にエクスポートされる NSEL トラフィックを識別するクラスマップに名前を付けます。

- **{{flow-export-class-name}}**：クラスマップの名前を入力します。名前の長さは最大 40 文字です。名前「class-default」と、「_internal」または「_default」で始まる名前はすべて予約されています。すべてのタイプのクラスマップで同じ名前空間が使用されるため、別のタイプのクラスマップですでに使用されている名前は再度使用できません。

ステップ 2 クラスマップに関連付けられる（一致する）トラフィックを識別します。**{{add_this_traffic_to_class_map}}** の値として、次のいずれかのオプションを選択します。

- **{{add_this_traffic_to_class_map}}** フィールドに **any** と入力します。NSEL トラフィックのすべてのトラフィックタイプが監視されます。**値「any」を使用することをお勧めします。**
- **{{add_this_traffic_to_class_map}}** フィールドに **access-list *name-of-access-list*** と入力します。作成したアクセスリストに関連付けられたすべてのトラフィックが関連付けられます。詳細については、Cisco ASA NetFlow 実装ガイド [英語] の「Configure Flow-Export Actions Through Modular Policy Framework」を参照してください。

次のタスク

NSEL イベントのポリシーマップの定義 （363 ページ）に進みます。

NSEL イベントのポリシーマップの定義

このタスクでは、前のタスクで作成したクラスに NetFlow エクスポートアクションを割り当て、そのクラスを新しいポリシーマップに割り当てます。以下の手順では、このセクションのマクロを参照しています。

policy-map {{global_policy_map_name}}

class {{flow_export_class_name}}

flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}

始める前に

この手順は、より大きなワークフローの一部です。始める前にCDO マクロを使用して ASA デバイスの NSEL を設定する （359 ページ）を参照してください。

ステップ 1 **policy-map** コマンドは、ポリシーマップを作成します。次のタスクでは、このポリシーマップをグローバルポリシーに関連付けます。

- **{{global_policy_map_name}}**：ポリシーマップの名前を入力します。ファイアウォールの既存のグローバルポリシーがある場合は、その名前を使用することをお勧めします。グローバルポリシーのデフォルト名は **global_policy** です。ASA グローバルポリシーの名前を決定する新しいポリシーマップを作成し、『Cisco ASA NetFlow 実装ガイド』の「モジュラ ポリシー フレームワークを使用した flow-export アクションの設定」に従ってグローバルに適用すると、残りの検査ポリシーは非アクティブ化されます。

ステップ 2 **class** コマンドでは、SEC に送信される NSEL イベントを定義するクラスマップの作成 （362 ページ）で作成したクラスマップの名前が継承されます。

ステップ 3 **flow-export event-type** {{event-type}} **destination** {{IPv4_address}} コマンドは、フローコレクタ（この場合は SEC）に送信する必要があるイベントタイプを定義します。

- **{{event-type}}**：event_type キーワードは、フィルタリングされるサポートされているイベントの名前です。値「all」を使用することをお勧めします。
- **{{SEC_IPv4_address}}**：これは SEC の IPv4 アドレスです。その値は、NSEL メッセージの宛先と SEC に送信される間隔の定義 （361 ページ）で入力した値から継承されます。

次のタスク

冗長な Syslog メッセージの無効化 （364 ページ） に進みます。

冗長な Syslog メッセージの無効化

以下の手順では、このセクションのマクロを参照しています。コマンドを変更する必要はありません。

logging flow-export-syslogs disable

NetFlow でフロー情報をエクスポートできるようにすると、次の表に記載されている syslog メッセージが冗長になります。パフォーマンスの向上のためには、同じ情報が NetFlow を通してエクスポートされるため、冗長な syslog メッセージをディセーブルにすることをお勧めします。

（注） NSEL メッセージと syslog メッセージの両方がイネーブルにされている場合、2 つのロギングタイプ間が時系列順になる保証はありません。

syslog メッセージ	説明	NSEL イベント ID	NSEL 拡張イベント ID
106100	アクセス制御ルール（ACL）が発生するたびに生成されます。	1：フローが作成されました（ACLがフローを許可した場合）。 3：フローが拒否されました（ACLがフローを拒否した場合）。	0：ACL がフローを許可した場合。 1001：入力 ACL によってフローが拒否されました。 1002：出力 ACL によってフローが拒否されました。
106015	最初のパケットがSYNパケットではなかったため、TCPフローが拒否されました。	3：フローが拒否されました。	1004：最初のパケットが TCP SYN パケットではなかったため、フローが拒否されました。
106023	**access-group** コマンドによってインターフェイスに接続されたACLによってフローが拒否された場合。	3：フローが拒否されました。	1001：入力 ACL によってフローが拒否されました。 1002：出力 ACL によってフローが拒否されました。
302013、302015、302017、302020	TCP、UDP、GRE、および ICMP 接続の作成。	1：フローが作成されました。	0：無視します。
302014、302016、302018、302021	TCP、UDP、GRE、およびICMP接続のティアダウン。	2：フローが削除されました。	0：無視します。 > 2000：フローが切断されました。
313001	デバイスへの ICMP パケットが拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。
313008	デバイスへの ICMP v6 パケットが拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。
710003	デバイスインターフェイスへの接続の試行が拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。

冗長なsyslogメッセージを無効にしない場合は、このマクロを編集して、次の行のみを削除できます。

logging flow-export-syslogs disable

後に NetFlow 関連の Syslog メッセージの無効化と再有効化の手順を実行することで、個別の syslog メッセージを有効化または無効化できます。

ASA グローバルポリシーの名前を決定する

ASA のグローバルポリシーの名前を決定するには、次の手順に従います。

ステップ 1 [デバイスとサービス] ページで、グローバルポリシーの名前を検索するデバイスを選択します。

ステップ 2 [デバイスアクション] ペインで、[>_コマンドリファレンス（>_Command Reference）] を選択します。

ステップ 3 コマンド ライン インターフェイス ウィンドウのプロンプトで、次のように入力します。

show running-config service-policy

以下の例の出力では、global_policy はグローバルポリシーの名前です。

例：

> **show running-config service-policy**

service-policy global_policy global

ASA イベント タイプ

イベントロギングページでのイベントの検索とフィルタリング場合、イベントタイプのリストから選択できますこれらのイベントタイプは、syslog ID のグループを表します。次の表は、どの ASA イベントタイプにどの syslog ID が含まれるかを示しています。特定の syslog ID の詳細については、『Cisco ASA シリーズ Syslog メッセージガイド』で検索できます。

一部の syslog イベントには、追加の属性「EventName」があります。属性:値のペアでフィルタ処理することにより、EventName 属性を使用してイベントテーブルをフィルタ処理し、イベントを見つけることができます。「Syslog イベントの EventName 属性」を参照してください。

ASA デバイス向け NetFlow Secure Event Logging（NSEL） は、syslog イベントとは異なります。NetFlow フィルタは、NSEL レコードになったすべての NetFlow イベント ID を検索します。これらの NetFlow イベント ID は、『Cisco ASA NetFlow 実装ガイド』で定義されています。

フィルタ名（**Filter Name**）	対応する **Syslog** イベントまたは **NetFlow** イベント
AAA	109001-109035 113001-113027
BotNet	338001-338310

フィルタ名（**Filter Name**）	対応する **Syslog** イベントまたは **NetFlow** イベント
フェールオーバー	101001-101005、102001、103001-103007、104001-104004、105001-105048 210001-210022 311001-311004 709001-709007
Firewall Denied	106001、106007、106012、106013、106015、106016、106017、106020、106021、106022、106023、106025、106027 Firewall Denied イベントは NetFlow に含まれている場合があり、syslog ID だけでなく NetFlow イベント ID と共に報告される場合もあります。
Firewall Traffic	106001-106100、108001-108007、110002-110003 201002-201013、209003-209005、215001 302002-302304、302022-302027、303002-303005、313001-313008、317001-317006、324000-324301、337001-337009 400001-400050、401001-401005、406001-406003、407001-407003、408001-408003、415001-415020、416001、418001-418002、419001-419003、424001-424002、431001-431002、450001 500001-500005、508001-508002 607001-607003、608001-608005、609001-609002、616001 703001-703003、726001 Firewall Traffic イベントは NetFlow に含まれている場合があり、syslog ID だけでなく NetFlow イベント ID と共に報告される場合もあります。
IPSec VPN	402001-402148、602102-602305、702304-702307
NAT	201002-201013、202001-202011、305005-305012
SSL VPN	716001-716060、722001-722053、723001-723014、724001-724004、725001-725015

フィルタ名（Filter Name）	対応する Syslog イベントまたは NetFlow イベント
NetFlow	0、1、2、3、5

関連情報：

- 一部の Syslog メッセージの EventGroup および EventGroupDefinition 属性 （443 ページ）
- Syslog イベントの EventName 属性

解析済みの ASA Syslog イベント

解析済みの syslog イベントは、他の syslog イベントよりも多くのイベント属性を含んでおり、特定の解析済みフィールドの検索を可能にします。SEC は、指定したすべての ASA イベントを Cisco Cloud に転送しますが、解析されるのは以下の表の syslog メッセージのみです。すべての解析済みの Syslog イベントは、識別しやすいように EventType が斜体で表示されます。

syslog ID	syslog カテゴリ	syslog メッセージの目的
106015	ファイアウォール	州外 TCP の拒否を表します。
106023	ファイアウォール	実際の IP パケットが ACL によって拒否されました。このメッセージは、ACL に対して **log** オプションをイネーブルにしていない場合でも表示されます。
106100	アクセスリスト/ユーザーセッション	パケットは ACL によって許可または拒否されました。
113019	ユーザー認証（User Authentication）	クリティカルな AnyConnect
302013、302015、302017、302020	ユーザ セッション	TCP、UDP、GRE、および ICMP 接続作成の接続開始 syslog と接続終了 syslog。
302014, 302016, 302018, 302021	ユーザ セッション	TCP、UDP、GRE、および ICMP 接続作成の接続開始 syslog と接続終了 syslog。
302020 ～ 302021	ユーザ セッション	ICMP セッションの確立と解除。
305006	ユーザーセッション/NAT および PAT	NAT 接続の失敗

syslog ID	syslog カテゴリ	syslog メッセージの目的
305011 ～ 305014	ユーザーセッション/NAT および PAT	NAT 確立/解除関連
313001、313008	IP スタック	ボックスへの接続が拒否されたことを表します。
414004	システム（System）	クリティカルな AnyConnect
609001 ～ 609002	ファイアウォール	ネットワーク状態コンテナは、ゾーンに接続されたホスト **ip-address** 用に予約済み/削除済みでした。
710002、710004、710005	ユーザ セッション	ボックスへの接続の失敗
710003	ユーザ セッション	ボックスへの接続が拒否されたことを表します。
746012、746013	ユーザ セッション	クリティカルな AnyConnect

syslog の詳細な説明については、『Cisco ASA Series Syslog Messages』を参照してください。

関連情報：

- コマンドライン インターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信
- イベントロギングページでのイベントの検索とフィルタリング

SecureLoggingAnalytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索

Secure Logging Analytics（SaaS）を使用すると、ご使用の ASA デバイスまたは FTD デバイスから、Secure Event Connector（SEC）上の特定の UDP、TCP、または NSEL ポートにイベントを送信できます。その後、SEC はそれらのイベントを Cisco Cloud に転送します。

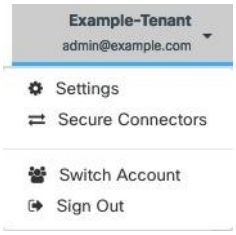
まだ使用されていないポートの場合、SEC はそれらのポートを使用してイベントを受信できるようにします。Secure Logging Analytics（SaaS）のマニュアルでは、機能を設定するときにポートを使用することが推奨されています。

- TCP：10125
- UDP：10025
- NSEL：10425

すでに使用されているポートの場合は、Secure Logging Analytics（SaaS）を設定する前に、SEC デバイスの詳細を調べて、イベントの受信に実際に使用しているポートを特定します。

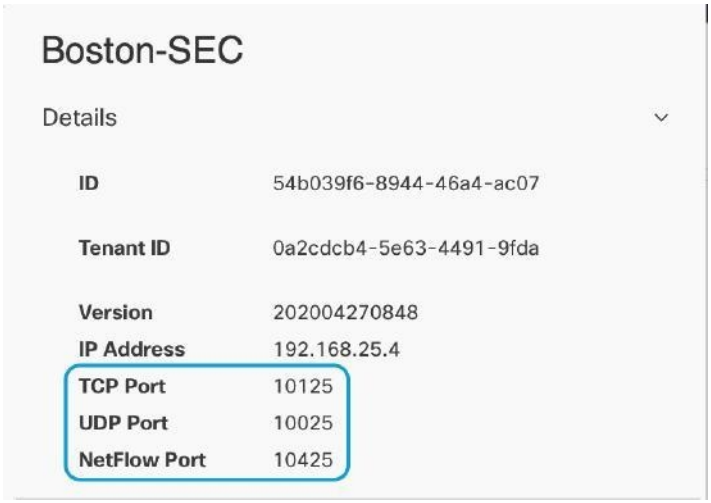
SEC が使用するポート番号を見つけるには、次の手順を実行します。

ステップ 1 CDO の任意のページで [アカウント（Account）] メニューを開き、[セキュアコネクタ（Secure Connectors）] を選択します。



ステップ 2 [セキュアコネクタ（Secure Connectors）] ページで、イベントを送信する SEC を選択します。

ステップ 3 [詳細] ペインに、イベントの送信先となる TCP、UDP、および NetFlow（NSEL）ポートが表示されます。



Secure Event Connector

Secure Event Connector（SEC）は、Security Analytics and Logging SaaS ソリューションのコンポーネントです。ASA や FTD デバイスからイベントを受信し、Cisco Cloud に転送します。イベントは CDO の [イベントロギング] ページに表示されます。管理者はこのページまたは Cisco Secure Cloud を使用してイベントを分析できます。

SEC は、ネットワークに展開された Secure Device Connector、またはネットワークに展開された独自の CDO コネクタ仮想マシンにインストールします。

Secure Event Connector ID

Cisco Technical Assistance Center（TAC）などの CDO サポートと連携する場合、SEC の ID が必要になる場合があります。この ID は、CDO の [セキュアコネクタ（Secure Connectors）] ページで確認できます。SEC ID を確認するには、次の手順を実行します。

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. 確認する SEC をクリックします。
3. SEC ID は、[詳細] ペインの [テナントID（ Tenant ID）] の上に表示されている ID です。

関連情報：

- ASA の Security Analytics and Logging（SAL SaaS）について
- SDC 仮想マシンへの Secure Event Connector のインストール （398 ページ）
- VM イメージを使用した SEC のインストール
- VM イメージを使用した SEC のインストール
- Secure Event Connector の削除
- Cisco Security Analytics and Logging（SaaS）をプロビジョニング解除する

Secure Event Connector をインストールする

Secure Event Connector（SEC）は、SDC の有無にかかわらず、テナントにインストールできます。

SEC は Secure Device Connector（あれば）と同じ仮想マシンにインストールすることも、ネットワーク内で維持管理している独自の CDO コネクタ仮想マシンにインストールすることもできます。

各インストールケースについて説明している次のトピックを参照してください。

- VM イメージを使用した SEC のインストール （408 ページ）
- CDO イメージを使用して SEC をインストールする （402 ページ）

SDC 仮想マシンへの Secure Event Connector のインストール

Secure Event Connector（SEC）は、ASA および FTD デバイスからイベントを受信し、それらをシスコクラウドに転送します。CDO は [イベントロギング] ページにイベントを表示し、管理者はそこで、または Cisco Secure Cloud Analytics を使用してイベントを分析できます。

SEC は Secure Device Connector（あれば）と同じ仮想マシンにインストールすることも、ネットワーク内で維持管理している独自の CDO コネクタ仮想マシンにインストールすることもできます。

この記事では、SDC と同じ仮想マシンに SEC をインストールする方法について説明します。他にも SEC をインストールする場合は、CDO イメージを使用して SEC をインストールする（402 ページ）または VM イメージを使用した SEC のインストール（408 ページ）を参照してください。

始める前に

- Cisco Security and Analytics Logging の **Logging and Troubleshooting** ライセンスを購入します。または、Cisco Security and Analytics を最初に試す場合は、CDO にログインし、メインナビゲーションバーで [モニタリング（Monitoring）] > [イベントロギング] を選択し、[トライアルのリクエスト（Request Trial）] をクリックします。また、**Logging Analytics and Detection** および **Total Network Analytics and Monitoring** ライセンスを購入して、Secure Cloud Analytics をイベントに適用することもできます。
- SDC がインストールされていることを確認します。SDC をインストールする必要がある場合は、次のいずれかの手順に従います。
  - CDO の VM イメージを使用した Secure Device Connector の展開
  - 自身の VM 上での Secure Device Connector の展開

（注） オンプレミスの SDC を独自の VM にインストールした場合は、イベントが到達できるようにするために作成した VM にインストールされた SDC および CDO コネクタの追加設定が必要です。

- SDC が CDO と通信していることを確認します。
  1. CDO で開いている任意のページから、ページの右上隅にあるユーザー名の下にあるメニューをクリックして、Secure Connectors のページを開きます。
  2. SEC をインストールする前に、SDC の最後のハートビートが 10 分以内であったこと、および SDC のステータスがアクティブであることを確認してください。
- システム要件：SDC を実行している仮想マシンに追加の CPU とメモリを割り当てます。
  - CPU：SEC 用に**追加**の 4 つの CPU を割り当て、CPU の合計が 6 つとなるようにします。
  - メモリ：SEC 用に**追加**の 8 GB のメモリを割り当てて、メモリの合計が 10 GB となるようにします。

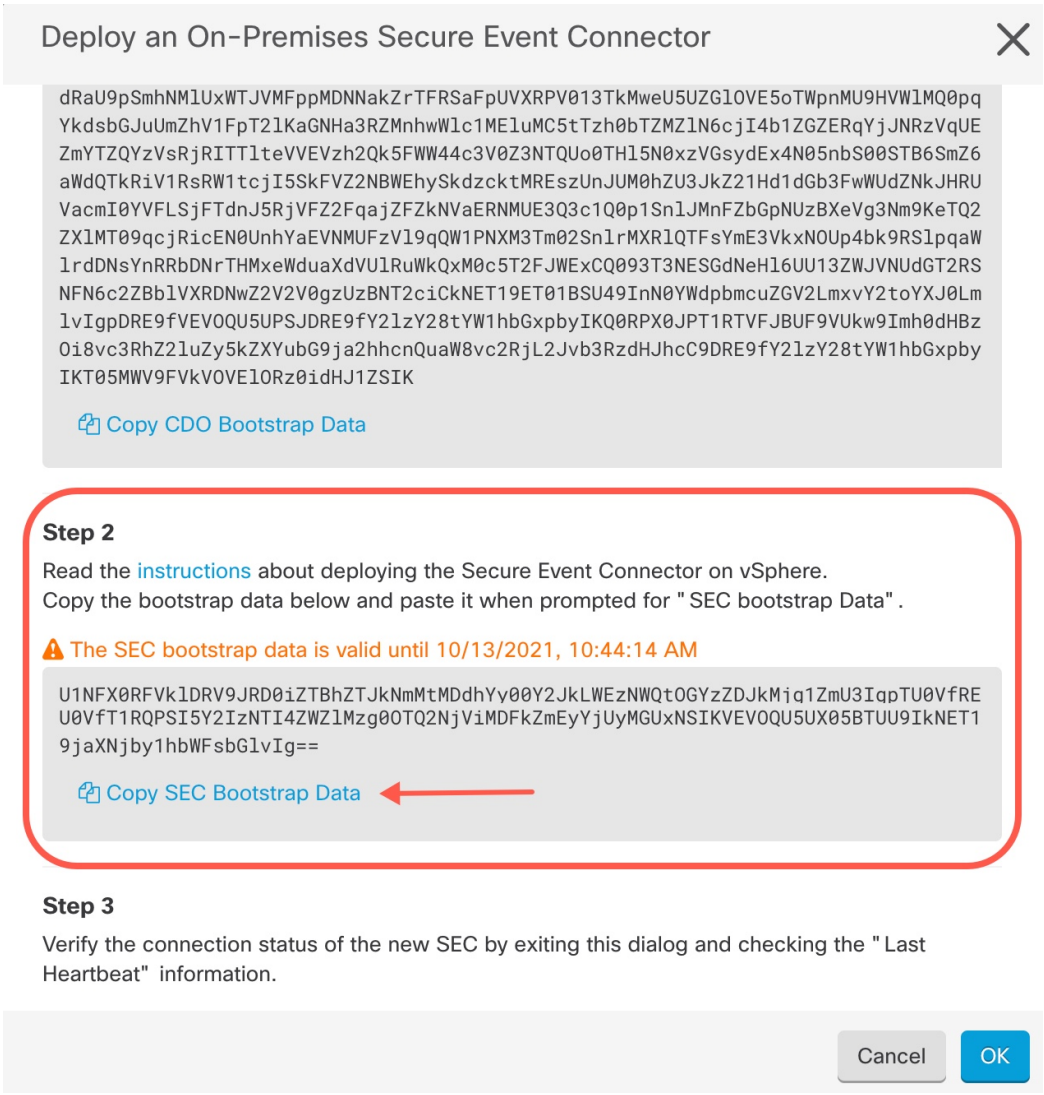
    SEC に対応するように VM の CPU とメモリを更新したら、VM の電源を入れ、[セキュアコネクタ（Secure Connectors）] ページに SDC が「アクティブ」状態であることが示されていることを確認します。

ステップ 1 CDO 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 青色のプラスボタンをクリックし、[Secure Event Connector] をクリックします。

ステップ 4 ウィザードのステップ 1 をスキップして、ステップ 2 に進みます。ウィザードのステップ 2で、 [SECブートストラップデータのコピー（Copy SEC bootstrap data）] のリンクをクリックします。



ステップ 5 ターミナルウィンドウを開き、SDC に「cdo」ユーザーとしてログインします。

ステップ 6 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。これらのコマンドの例を次に示します。

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

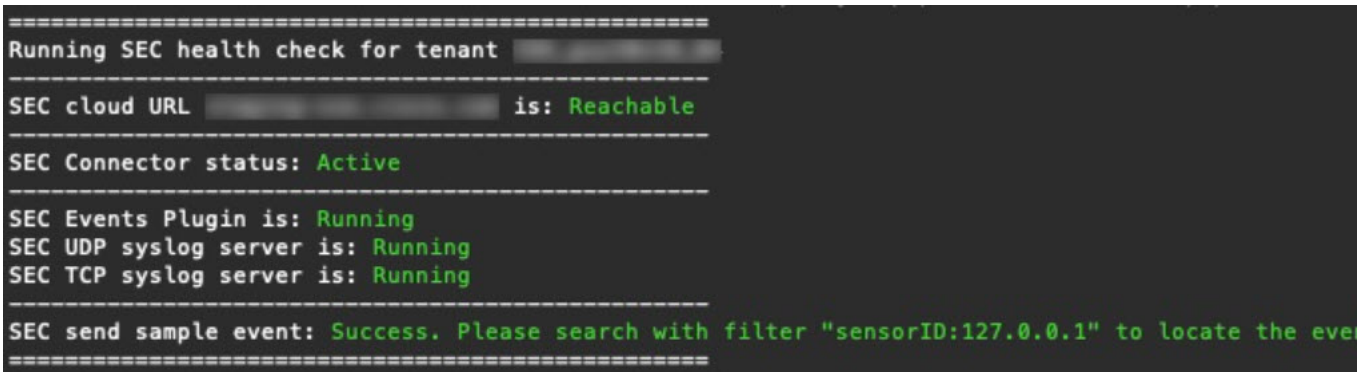
ステップ 7 プロンプトで、**sec.sh setup** スクリプトを実行します。

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

ステップ 8 プロンプトの最後に、手順4でコピーしたブートストラップデータを貼り付けて、**Enter** キーを押します。

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC がオンボーディングされると、sec.sh は、SEC のヘルスをチェックするスクリプトを実行します。すべてのヘルスチェックが「正常」の場合、ヘルスチェックはサンプルイベントをイベントログに送信します。このサンプルイベントは、「sec-health-check」という名前のポリシーとしてイベントログに表示されます。



登録に失敗したことやSECの導入準備に失敗したことを示すメッセージを受け取った場合は、「SEC オンボーディング失敗のトラブルシューティング」を参照してください。

ステップ 9 SDC と SEC が実行されている VM に追加の構成が必要かどうかを判断します。

- SDC を独自の仮想マシンにインストールした場合は、作成した VM にインストールされた SDC および CDO コネクタの追加設定 （413 ページ） を続行します。
- CDO イメージを使用して SDC をインストールした場合は、「次に行う作業」に進みます。

次のタスク

ASA デバイスに安全なロギング分析（SaaS）を導入する （345 ページ） に戻ります。

関連情報：

- Secure Device Connector のトラブルシュート （519 ページ）
- Secure Event Connector のトラブルシューティング
- SEC オンボーディング失敗のトラブルシューティング
- Secure Event Connector の登録失敗のトラブルシューティング （527 ページ）

CDO イメージを使用して SEC をインストールする

Secure Event Connector（SEC）は、ASA と FTD からのイベントを Cisco Cloud に転送するため、ライセンスに応じて、[イベントロギング] ページでイベントを表示し、Stealthwatch Cloud で調査できます。

テナントに複数の Secure Event Connector（SEC）をインストールし、インストールした任意の SEC に ASA および FTD からイベントを送信できます。複数の SEC を使用すると、さまざまな場所に SEC をインストールし、Cisco Cloud にイベントを送信する作業を分散できます。

SEC のインストールは、2 つの部分からなるプロセスです。

1. CDO VM イメージを使用して Secure Event Connector をサポートするための CDO コネクタのインストール （402 ページ） インストールする SEC ごとに 1 つの CDO コネクタが必要です。CDO コネクタは、Secure Device Connector（SDC）とは異なります。
2. CDO コネクタ仮想マシンへの Secure Event Connector のインストール （414 ページ）。

（注） 独自の VM を作成して CDO コネクタを作成する場合は、「作成した VM にインストールされた SDC および CDO コネクタの追加設定」を参照してください。

次に行う作業：

CDO VM イメージを使用して Secure Event Connector をサポートするための CDO コネクタのインストール （402 ページ） に進みます。

CDO VM イメージを使用して Secure Event Connector をサポートするための CDO コネクタのインストール

始める前に

- Cisco Security and Analytics Logging と **Logging and Troubleshooting** ライセンスに加えて、**Logging Analytics and Detection** と **Total Network Analytics and Monitoring** ライセンスを購入すると、イベントに Stealthwatch Cloud 分析を適用できます。

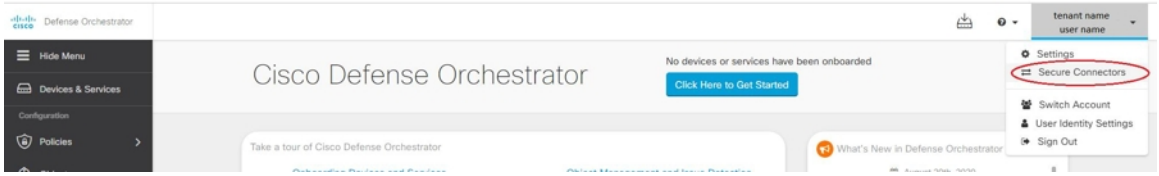
  Security Analytics and Logging のトライアル版をリクエストする場合は、CDO にログインし、メインナビゲーションバーで **[モニタリング（Monitoring）][イベントロギング]** を選択し、[トライアルのリクエスト（Request Trial）] をクリックします。

- CDO は、厳密な証明書チェックを必要とし、CDO コネクタ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、CDO コネクタと CDO の間のトラフィックの検査を無効にします。
- **このプロセスでインストールされる CDO コネクタには 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。**
- **CDO コネクタで適切なネットワークアクセスを確保するには、「**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。**

- 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 CDO コネクタ 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、VM vSphere デスクトップクライアントを使用した CDO コネクタ 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。
- CDO コネクタと SEC のみをホストすることを目的した VM のシステム要件は以下のとおりです。
  - VMware ESXi ホストには 4 つの vCPU が必要です。
  - VMware ESXi ホストには 8 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 64GB のディスク容量が必要です。
- インストールを開始する前に、次の情報を収集します。
  - CDO コネクタ VM に使用する静的 IP アドレス。
  - インストールプロセス中に作成する **root** ユーザーと **cdo** ユーザーのパスワード。
  - 組織で使用する DNS サーバーの IP アドレス。
  - SDC アドレスが存在するネットワークのゲートウェイ IP アドレス。
  - タイムサーバーの FQDN または IP アドレス。
- CDO Connector 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 CDO コネクタを作成する CDO テナントにログオンします。

ステップ 2 [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 3 青色のプラスボタンをクリックし、[Secure Event Connector] をクリックします。

ステップ 4 手順 1 で [CDOコネクタVMイメージのダウンロード（Download the CDO Connector VM image）] をクリックします。これは、SEC をインストールする特別なイメージです。最新のイメージを確実に使用するために、常に CDO コネクタ VM をダウンロードしてください。

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） VM vSphere デスクトップ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 テンプレートからオンプレミスの CDO コネクタ仮想マシンを展開します（テンプレートを展開するには、.ovf、.mf、および .vdk ファイルが必要です）。

ステップ 8 セットアップが完了したら、VM の電源を入れます。

ステップ 9 新しい CDO コネクタ VM のコンソールを開きます。

ステップ 10 **cdo** ユーザーとしてログインします。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 プロンプトで、cdo ユーザーのデフォルトのパスワード（`adm123`）を入力します。

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。

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。

ステップ 15 プロンプトに従って、Cisco Defense Orchestrator ドメイン情報を入力します。

ステップ 16 CDO コネクタ VM に使用する静的 IP アドレスを入力します。

ステップ 17 CDO コネクタ VM がインストールされているネットワークのゲートウェイ IP アドレスを入力します。

ステップ 18 CDO コネクタの NTP サーバーのアドレスまたは FQDN を入力します。

ステップ 19 プロンプトで、Docker ブリッジの情報を入力するか、該当しない場合は空白のままにして、Enter キーを押します。

ステップ 20 入力内容を確定します。

ステップ 21 「Would you like to setup the SDC now?」というプロンプトで、**n** を入力します。

ステップ 22 **cdo** ユーザーとしてログインして、CDO コネクタへの SSH 接続を作成します。

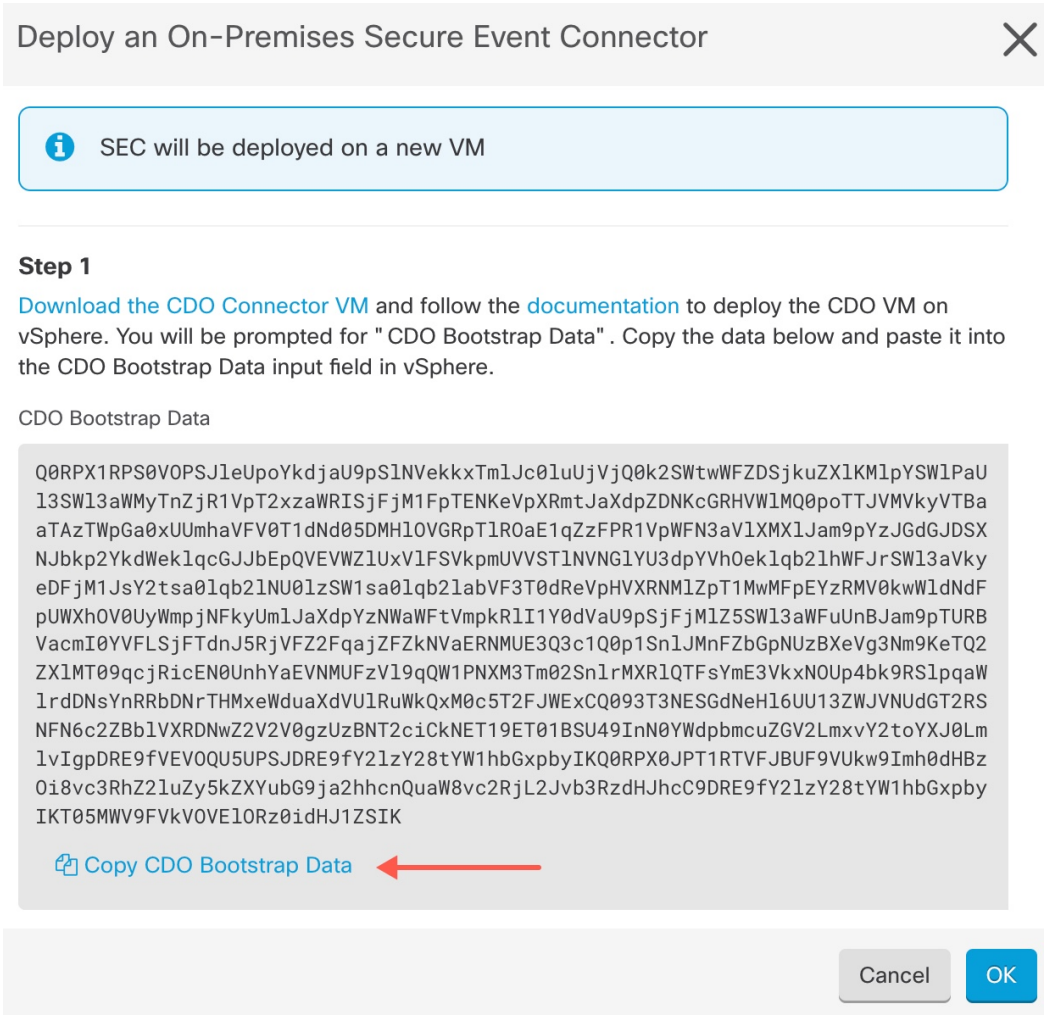
ステップ 23 プロンプトで、**`sudo sdc-onboard bootstrap`** と入力します。

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

ステップ 24 プロンプトで、cdo ユーザーのパスワードを入力します。

ステップ 25 プロンプトで、CDO に戻り、CDO ブートストラップデータをコピーして、SSH セッションに貼り付けます。CDO ブートストラップデータをコピーするには、次の手順を実行します。

1. CDO にログインします。
2. ユーザーメニューから、[セキュアコネクタ（Secure Connectors）] を選択します。
3. 導入準備を開始した Secure Event Connector を選択します。ステータスが「Onboarding」と表示されます。
4. [アクション] ペインで、[オンプレミスのSecure Event Connectorの展開（Deploy an On-Premises Secure Event Connector）] をクリックします。
5. ダイアログボックスのステップ 1 で、CDO ブートストラップデータをコピーします。



ステップ 26 「Would you like to update these settings?」というプロンプトで、**n** を入力します。

ステップ 27 CDO の [オンプレミスのSecure Event Connectorの展開（Deploy an On-Premises Secure Event Connector）] ダイアログに戻り、[OK] をクリックします。[セキュアコネクタ（Secure Connectors）] ページで、Secure Event Connector が黄色の導入準備状態であることを確認できます。

次のタスク

CDO コネクタ VM への Secure Event Connector のインストール （406 ページ） に進みます。

CDO コネクタ VM への Secure Event Connector のインストール

始める前に

CDO VM イメージを使用して Secure Event Connector をサポートするための CDO コネクタのインストール （402 ページ） に記載があるように、CDO コネクタ VM がインストールされている必要があります。

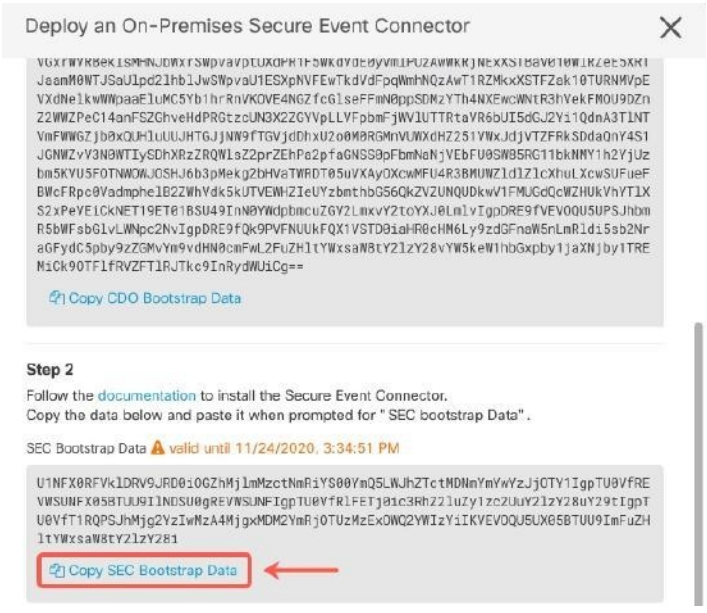
ステップ 1 CDO にログインします。

ステップ 2 [ユーザー（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 上記で導入準備した CDO コネクタを選択します。セキュアコネクタテーブルでは、これはセキュアイベントコネクタと呼ばれ、「導入準備」ステータスのままである必要があります。

ステップ 4 右側の [アクション] ペインで、[オンプレミスのSecure Event Connectorの展開（Deploy an On-Premises Secure Event Connector）] をクリックします。

ステップ 5 ウィザードの**ステップ 2**で、 [SECブートストラップデータのコピー（Copy SEC bootstrap data）] のリンクをクリックします。



ステップ 6 CDO コネクタへの SSH 接続を作成し、**cdo** ユーザーとしてログインします。

ステップ 7 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。これらのコマンドの例を次に示します。

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

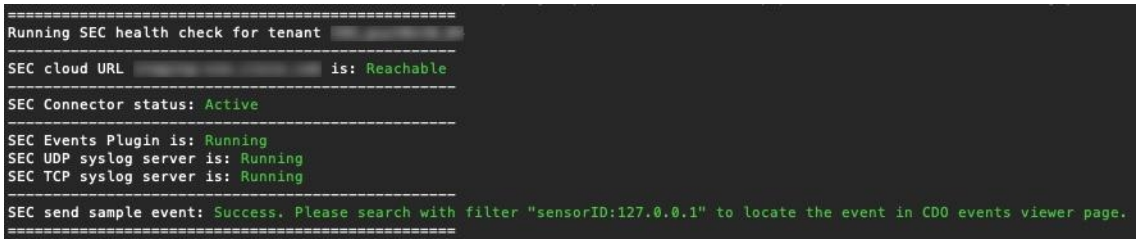
ステップ 8 プロンプトで、sec.sh セットアップスクリプトを実行します。

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

ステップ 9 プロンプトの最後に、手順 4 でコピーしたブートストラップデータを貼り付けて、**Enter** キーを押します。

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
 RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC がオンボーディングされると、sec.sh は、SEC のヘルスをチェックするスクリプトを実行します。すべてのヘルスチェックが「正常」の場合、ヘルスチェックはサンプルイベントをイベントログに送信します。このサンプルイベントは、「sec-health-check」という名前のポリシーとしてイベントログに表示されます。



登録に失敗したことや SEC の導入準備に失敗したことを示すメッセージを受け取った場合は、次を参照してください： SEC オンボーディング失敗のトラブルシューティング （523 ページ）

成功メッセージを受け取った場合は、CDO に戻り、[オンプレミス セキュア イベント コネクタの展開（Deploy an ON-Premise Secure Event Connector）] ダイアログボックスで [完了（Done）] をクリックします。

ステップ 10 「**次のステップ**」に進みます。 "

次のタスク

ASA デバイスに安全なロギング分析（SaaS）を導入する （345 ページ） に戻ります。

関連情報：

- Secure Device Connector のトラブルシュート （519 ページ）
- Secure Event Connector のトラブルシューティング （523 ページ）
- SEC オンボーディング失敗のトラブルシューティング （523 ページ）

VM イメージを使用した SEC のインストール

Secure Event Connector（SEC）は、ASA と FTD からのイベントを Cisco Cloud に転送するため、ライセンスに応じて、[イベントロギング] ページでイベントを表示し、Stealthwatch Cloud で調査できます。

テナントに複数の Secure Event Connector（SEC）をインストールし、インストールした任意の SEC に ASA および FTD からイベントを送信できます。複数の SEC を使用すると、さまざまなリージョンに SEC をインストールし、Cisco Cloud にイベントを送信する作業を分散できます。

独自の VM イメージを使用した複数の SEC のインストールは、3 つの部分からなるプロセスです。次の各手順を実行する必要があります。

1. VM イメージを使用して SEC をサポートするための CDO コネクタのインストール （408 ページ）
2. 作成した VM にインストールされた SDC および CDO コネクタの追加設定 （413 ページ）を使用して、VM の追加の設定手順をいくつか実行します。
3. CDO コネクタ仮想マシンへの Secure Event Connector のインストール

（注） CDO コネクタに CDO VM イメージを使用する方法は、CDO コネクタをインストールする最も簡単で正確な推奨される方法です。その方法を使用する場合は、CDO イメージを使用して SEC をインストールする （402 ページ）を参照してください。

次に行う作業：

VM イメージを使用して SEC をサポートするための CDO コネクタのインストール （408 ページ）に進みます。

VM イメージを使用して SEC をサポートするための CDO コネクタのインストール

CDO コネクタ VM は、SEC をインストールする仮想マシンです。CDO コネクタの唯一の目的は、Cisco Security Analytics and Logging（SaaS）のお客様向けに SEC をサポートすることです。

始める前に

- Cisco Security and Analytics Logging と **Logging and Troubleshooting** ライセンスに加えて、**Logging Analytics and Detection** と **Total Network Analytics and Monitoring** ライセンスを購入すると、イベントに Secure Cloud Analytics を適用できます。

  Security Analytics and Logging のトライアル版をリクエストする場合は、CDO にログインし、メインナビゲーションバーで **[モニタリング（Monitoring）][イベントロギング（Event Logging）]** を選択し、[トライアルのリクエスト（Request Trial）] をクリックします。

- CDO は、厳密な証明書チェックを必要とし、CDO コネクタとインターネット間の Web プロキシやコンテンツプロキシをサポートしていません。
- **CDO コネクタには 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。**
- **CDO コネクタで適切なネットワークアクセスを確保するには、「Cisco Defense Orchestrator の管理対象デバイスへの接続」を参照してください。**
- vCenter Web クライアントまたはr ESXi Web クライアントを使用してインストールされた VMware ESXi ホスト。

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

- ESXi 5.1 ハイパーバイザ。
- Cent OS 7 ゲスト オペレーティング システム。
- CDO コネクタと SEC のみをホストするための VM のシステム要件は以下のとおりです。
  - CPU：SEC 用に 4 つの CPU を割り当てます。
  - メモリ：SEC 用に 8 GB のメモリを割り当てます。
  - ディスク領域：64 GB
- この手順を実行するユーザーは、Linux 環境の操作と **vi** ビジュアルエディタによるファイルの編集に慣れている必要があります。
- CDO コネクタを 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。
- インストールを開始する前に、次の情報を収集します。
  - CDO コネクタに使用する静的 IP アドレス。
  - インストールプロセス中に作成する **root** ユーザーと **cdo** ユーザーのパスワード。
  - 組織で使用する DNS サーバーの IP アドレス。
  - CDO コネクタアドレスが存在するネットワークゲートウェイの IP アドレス。
  - タイムサーバーの FQDN または IP アドレス。
- CDO Connector 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。

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

ステップ 1 [Secure Device Connector] ページで、青いプラスボタン  をクリックし、[Secure Event Connector] を選択します。

ステップ 2 表示されたリンクを使用して、[オンプレミスのSecure Event Connectorの展開（Deploy an On-Premises Secure Event Connector）] ウィンドウの手順 2 で SEC ブートストラップデータをコピーします。

ステップ 3 少なくともこの手順の前提条件に記載されているメモリ、CPU、およびディスク容量を備えた CentOS 7 仮想マシン（http://isoredirect.centos.org/centos/7/isos/x86_64/CentOS-7-x86_64-Minimal-1804.iso）をインストールします。

ステップ 4 インストールしたら、CDO コネクタの 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 5 DNS（ドメインネームサーバー）を設定します。

ステップ 6 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 7 CDO コネクタの 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 8 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 9 **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）。

（注） `--user` フラグは使用しないでください。

ステップ 10 **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）。

（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 11 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 12 **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、CDO コネクタの 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 13 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 14 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 15 Docker がインストールされると、ユーザーグループが作成されます。CentOS/Docker のバージョンに応じて、「docker」または「dockerroot」と呼ばれます。/etc/group ファイルでどのグループが作成されたかを確認したら、sdc ユーザーをそのグループに追加します。

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

ステップ 16 `/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、ステップ 15と一致していることを確認してください。

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

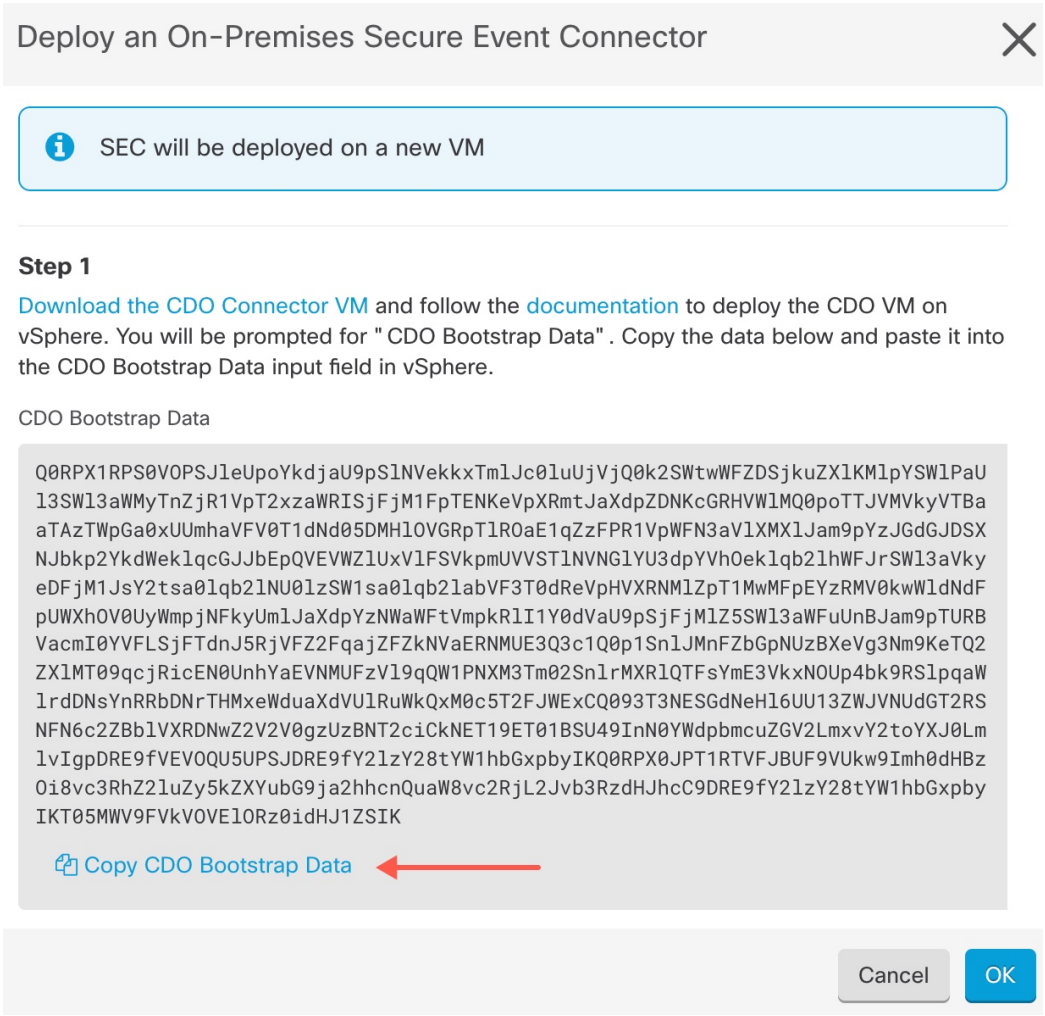
ステップ 17 現在 vSphere コンソールセッションを使用している場合は、SSH に切り替えて、**cdo** ユーザーでログインします。ログインしたら、**sdc** ユーザーに切り替えます。パスワードの入力を求められたら、**cdo** ユーザーのパスワードを入力します。

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

ステップ 18 ディレクトリを **/usr/local/cdo** に変更します。

ステップ 19 **bootstrapdata** という新しいファイルを作成し、展開ウィザードの手順1 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 20 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@sdc-vm ~]$ base64 -d /usr/local/cdo/bootstrapdata > /usr/local/cdo/extractedbootstrapdata
[sdc@sdc-vm ~]$
```

catコマンドを実行して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@sdc-vm ~]$ cat /usr/local/cdo/extractedbootstrapdata
CDO_TOKEN="<token string>"
CDO_DOMAIN="www.defenseorchestrator.com"
CDO_TENANT="<tenant-name>"
CDO_BOOTSTRAP_URL="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"

ONLY_EVENTING="true"
```

ステップ 21 以下のコマンドを実行して、暗号解読化したブートストラップデータの一部を環境変数にエクスポートします。

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

ステップ 22 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 23 CDO コネクタ tarball を展開し、bootstrap_sec_only.sh ファイルを実行して CDO コネクタ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_sec_only.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
es_toolkit.sh
sec.sh
healthcheck.sh
troubleshoot.sh
no crontab for sdc
-bash-4.2$ crontab -l
*/5 * * * * /usr/local/cdo/toolkit/es_toolkit.sh upgradeEventing 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
0 2 * * * sleep 30 && /usr/local/cdo/toolkit/es_toolkit.sh es_maintenance 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
You have new mail in /var/spool/mail/sdc
```

次のタスク

作成した VM にインストールされた SDC および CDO コネクタの追加設定 （413 ページ） に進みます。

作成した VM にインストールされた SDC および CDO コネクタの追加設定

CDO コネクタを独自の CentOS 7 仮想マシンにインストールした場合は、イベントが SEC に到達できるように、次の付加的な設定手順の**いずれか**を実行する必要があります。

- CentOS 7 VM での firewalld サービスの無効化この設定は、シスコが提供する SDC VM の設定と一致します。
- firewalld サービスの実行を許可し、ファイアウォールルールを追加して、イベントトラフィックが SEC に到達できるようにします。 （414 ページ）。この手順では、インバウンドイベント トラフィックを許可するためのより詳細なアプローチが示されます。

CentOS 7 VM での firewalld サービスの無効化

1. SDC VM の CLI に「cdo」ユーザーとしてログインします。

2. firewalld サービスを停止してから、続く VM の再起動時に無効のままになっていることを確認します。プロンプトが表示されたら、**cdo** ユーザーのパスワードを入力します。

```
[cdo@SDC-VM ~]$ sudo systemctl stop firewalld
cdo@SDC-VM ~]$ sudo systemctl disable firewalld
```

3. Docker サービスを再起動して、Docker 固有のエントリをローカルファイアウォールに再挿入します。

```
[cdo@SDC-VM ~]$ sudo systemctl restart docker
```

4. CDO コネクタ仮想マシンへの Secure Event Connector のインストール （414 ページ）に進みます。

firewalld サービスの実行を許可し、ファイアウォールルールを追加して、イベントトラフィックが SEC に到達できるようにします。

1. SDC VM の CLI に「cdo」ユーザーとしてログインします。
2. ローカル ファイアウォール ルールを追加して、設定した TCP、UDP、または NSEL ポートから SEC への着信トラフィックを許可します。SEC で使用されるポートについては、「Secure Logging Analytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。プロンプトが表示されたら、**cdo** ユーザーのパスワードを入力します。コマンドの例を次に示します。別のポート値の指定が必要になる場合があります。

```
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10125/tcp
cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10025/udp
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10425/udp
```

3. firewalld サービスを再起動して、新しいローカルファイアウォールルールをアクティブかつ持続的なものにします。

```
[cdo@SDC-VM ~]$ sudo systemctl restart firewalld
```

4. CDO コネクタ仮想マシンへの Secure Event Connector のインストール （414 ページ） に進みます。

CDO コネクタ仮想マシンへの Secure Event Connector のインストール

始める前に

次の 2 つのタスクを実行します。

- VM イメージを使用して SEC をサポートするための CDO コネクタのインストール （408 ページ）
- 作成した VM にインストールされた SDC および CDO コネクタの追加設定 （413 ページ）

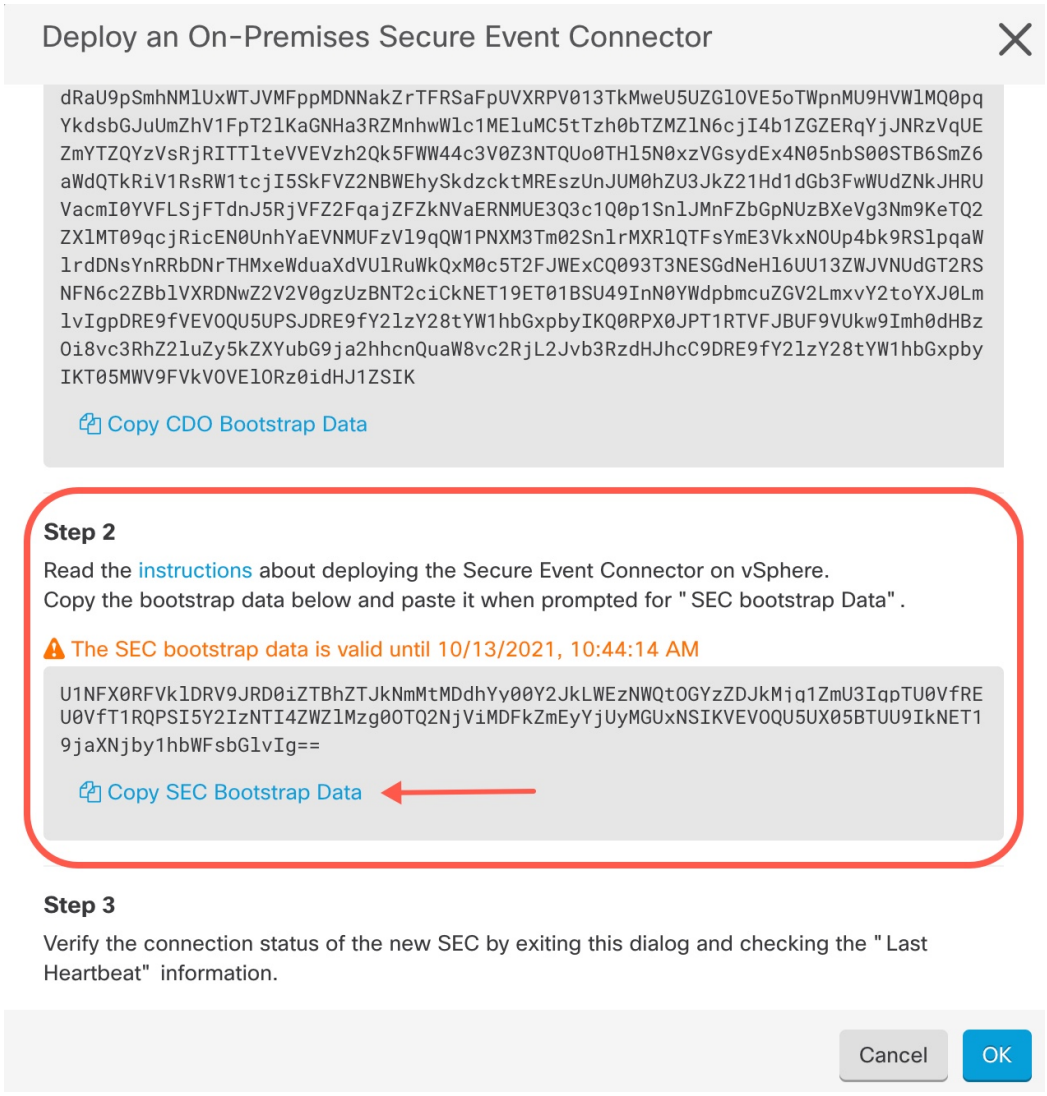
ステップ 1 CDO にログインします。

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 上記の前提条件の手順を使用してインストールした CDO コネクタを選択します。[セキュアコネクタ（Secure Connectors）] テーブルでは、「Secure Event Connector」と呼ばれます。

ステップ 4 右側の [アクション] ペインで、[オンプレミスのSecure Event Connectorの展開（Deploy an On-Premises Secure Event Connector）] をクリックします。

ステップ 5 ウィザードの**ステップ 2**で、[SECブートストラップデータのコピー（Copy SEC bootstrap data）] のリンクをクリックします。



ステップ 6 SSH を使用してセキュアコネクタに接続し、**cdo** ユーザーとしてログインします。

ステップ 7 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。これらのコマンドの例を次に示します。

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

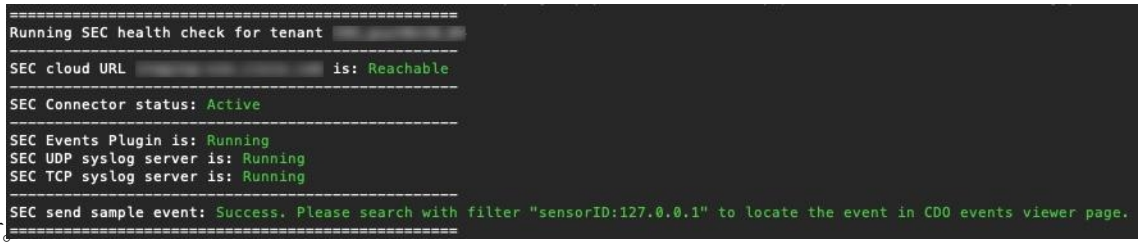
ステップ 8 プロンプトで、sec.sh セットアップスクリプトを実行します。

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

ステップ 9 プロンプトの最後に、手順 4 でコピーしたブートストラップデータを貼り付けて、**Enter** キーを押します。

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
 KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC がオンボーディングされると、sec.sh は、SEC のヘルスをチェックするスクリプトを実行します。すべてのヘルスチェックが「正常」の場合、ヘルスチェックはサンプルイベントをイベントログに送信します。このサンプルイベントは、「sec-health-check」という名前のポリシーとしてイベントログに表示されます。



登録に失敗したことや SEC の導入準備に失敗したことを示すメッセージを受け取った場合は、「Secure Event Connector のトラブルシューティング」を参照してください。

成功メッセージを受け取った場合は、[オンプレミスのSecure Event Connectorの展開（Deploy an ON-Premise Secure Event Connector）] ダイアログボックスで [完了（Done）] をクリックします。VM イメージへの SEC のインストールは完了です。

ステップ 10 「**次の作業**」に進みます。

次のタスク

この手順に戻って、SAL SaaS の実装を続行します：ASA デバイスに安全なロギング分析（SaaS）を導入する （345 ページ）

関連情報：

- Secure Device Connector のトラブルシュート （519 ページ）
- Secure Event Connector のトラブルシューティング
- SEC オンボーディング失敗のトラブルシューティング
- Secure Event Connector の登録失敗のトラブルシューティング

Cisco Security Analytics and Logging（SaaS）をプロビジョニング解除する

Cisco Security Analytics and Logging（SaaS）の有料ライセンスの有効期限が切れた場合、90 日間の猶予期間があります。この猶予期間中に有料ライセンスを更新した場合は、サービスが中断されません。

更新せずに 90 日間の猶予期間が経過すると、お客様のデータはすべて消去されます。[イベントロギング] ページから ASA や FTD イベントを表示することも、ダイナミック エンティティ モデリングの動作分析を ASA、FTD イベント、およびネットワークフローデータに適用することもできなくなります。

Secure Event Connector の削除

警告：この手順により、Secure Event Connector が Secure Device Connector から削除されます。これを行うと、Secure Logging Analytics（SaaS）を使用できなくなります。この操作は元に戻せません。質問や懸念事項がある場合は、このアクションを実行する前に Cisco Defense Orchestrator サポートへの連絡。

Secure Device Connector から Secure Event Connector を削除するには、次の 2 段階のプロセスを実行します。

1. CDO からの SEC の削除。
2. SDC からの SEC ファイルの削除。

次に行う作業：CDO からの SEC の削除を続行します。

CDO からの SEC の削除

始める前に

Secure Event Connector の削除 （417 ページ）を参照してください。

ステップ 1 CDO にログインします。

ステップ 2 アカウントメニューから、[セキュアコネクタ（Secure Connectors）] を選択します。

ステップ 3 デバイスタイプが [Secure Event Connector] の行を選択します。

警告 ：慎重に操作してください。Secure Device Connector を選択しないでください。

ステップ 4 [アクション] ペインで、[削除] をクリックします。

ステップ 5 [OK] をクリックして、Secure Event Connector を削除することを確認します。

次のタスク

SDC からの SEC ファイルの削除 （417 ページ） に進みます。

SDC からの SEC ファイルの削除

この項目は、SDC から Secure Event Connector を削除する 2 つの部分から成る手順の 2 番目の部分です。開始する前に「Secure Event Connector の削除 （417 ページ）」を参照してください。

ステップ 1 仮想マシンのハイパーバイザを開き、SDC のコンソールセッションを開始します。

ステップ 2 SDC ユーザーに切り替えます。

```
[cdo@tenant toolkit]$sudo su sdc
```

ステップ 3 プロンプトで、次のいずれかのコマンドを入力します。

- 独自のテナントのみを管理している場合：

```
[sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove
```

- 複数のテナントを管理する場合は、テナント名の先頭に CDO_ を追加してください。次に例を示します。

```
[sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove CDO_[tenant_name]
```

ステップ 4 SEC ファイルの削除を確定します。

Cisco Secure Cloud Analytics ポータルのプロビジョニング

必要なライセンス：**Logging Analytics and Detection** または **Total Network Analytics and Monitoring**

Logging Analytics and Detection ライセンスまたは **Total Network Analytics and Monitoring** ライセンスを購入した場合、Secure Event Connector（SEC）を展開して設定した後、Secure Cloud Analytics ポータルを CDO ポータルに関連付けて、Secure Cloud Analytics アラートを表示する必要があります。ライセンスを購入すると、既存の Secure Cloud Analytics ポータルがある場合は、Secure Cloud Analytics ポータル名を指定して、すぐに CDO ポータルに関連付けることができます。

それ以外の場合は、CDO UI から新しい Secure Cloud Analytics ポータルをリクエストできます。Secure Cloud Analytics アラートに初めてアクセスすると、システムに Secure Cloud Analytics ポータルを要求するページが表示されます。このポータルを要求するユーザーには、ポータルの管理者権限が付与されます。

ステップ 1 CDO で、**[モニタリング（Monitoring）]**>**[セキュリティ分析（Security Analytics）]** を選択し、新しいウィンドウで Secure Cloud Analytics UI を開きます。

ステップ 2 [無料トライアルを開始（Start Free Trial）] をクリックして、Secure Cloud Analytics ポータルをプロビジョニングし、CDO ポータルに関連付けます。

（注） ポータルを要求した後、プロビジョニングに数時間かかる場合があります。

次の手順に進む前に、ポータルがプロビジョニングされていることを確認してください。

1. CDO で、**[モニタリング（Monitoring）]** > **[セキュリティ分析（Security Analytics）]** を選択し、新しいウィンドウで Secure Cloud Analytics UI を開きます。
2. 次の選択肢があります。
   - Secure Cloud Analytics ポータルを要求したものの、まだポータルのプロビジョニング中であることがシステムに表示されている場合は、しばらく待ってから、後でアラートへのアクセスを試行してください。
   - Secure Cloud Analytics ポータルがプロビジョニング済みの場合は、[ユーザー名（Username）] と [パスワード（Password）] を入力し、[サインイン（Sign in）] をクリックします。

（注） 管理者ユーザーは、Secure Cloud Analytis ポータル内でアカウントを作成するように他のユーザーを招待できます。詳細については、Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （421 ページ）を参照してください。

次のタスク

- **Logging Analytics and Detection** ライセンスを購入した場合、設定は完了しています。Secure Cloud Analytics ポータル UI から CDO 統合のステータスやセンサーの正常性のステータスを表示する場合は、「Cisco Secure Cloud Analytics でのセンサーの正常性と CDO 統合ステータスの確認 （419 ページ）」で詳細を参照してください。Secure Cloud Analytics ポータルでアラートを操作する場合は、「Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （421 ページ）」および「ファイアウォールイベントに基づくアラートの使用」を参照してください。
- **Total Network Analytics and Monitoring** ライセンスを購入した場合は、1 つ以上の Secure Cloud Analytics センサーを内部ネットワークに展開して、ネットワークフローデータをクラウドに渡します。クラウドベースのネットワークフローデータを監視する場合は、フローデータを Secure Cloud Analytics に渡すようにクラウドベースの展開を設定します。詳細については、総合的なネットワーク分析およびレポーティングのための Cisco Secure Cloud Analytics センサーの展開 （420 ページ）を参照してください。

Cisco Secure Cloud Analytics でのセンサーの正常性と CDO 統合ステータスの確認

Sensor Status

必要なライセンス：Logging Analytics and Detection または **Total Network Analytics and Monitoring**

Cisco Secure Cloud Analytics Web UI では、[センサーリスト（Sensor List）] ページで CDO 統合ステータスと設定済みセンサーを確認できます。CDO 統合は、読み取り専用の接続イベントセンサーです。Stelathwatch Cloud のメインメニューには、センサーの全体的な正常性が示されます。

- 緑色の雲のアイコン（）：すべてのセンサーと CDO（設定されている場合）との接続が確立されています。
- 黄色の雲のアイコン（）：一部のセンサー、または CDO（設定されている場合）との接続が確立されており、1 つ以上のセンサーが正しく設定されていません。
- 赤色の雲のアイコン（）：設定されているすべてのセンサーと CDO（設定されている場合）との接続が失われています。

センサーまたは CDO 統合ごとに、緑色のアイコンは接続が確立されていることを示し、赤色のアイコンは接続が失われていることを示します。

ステップ 1 1. Cisco Secure Cloud Analytics ポータル UI で、[設定]（）> [センサー（Sensors）] を選択します。

ステップ 2 [センサーリスト（Sensor List）] を選択します。

総合的なネットワーク分析およびレポーティングのための Cisco Secure Cloud Analytics センサーの展開

Secure Cloud Analytics センサーの概要と展開

必要なライセンス：Total Network Analytics and Monitoring

Total Network Analytics and Monitoring ライセンスを取得している場合は、Secure Cloud Analytics ポータルをプロビジョニングした後に、次のことができます。

- オンプレミスネットワーク内に Secure Cloud Analytics センサーを展開し、ネットワークフローデータを分析のためにクラウドに渡すように設定します。
- フローデータを分析のために Secure Cloud Analytics に渡すようにクラウドベースの展開を設定します。

ネットワーク境界のファイアウォールが内部ネットワークと外部ネットワークの間のトラフィックに関する情報を収集する一方で、Secure Cloud Analytics センサーは内部ネットワーク内のトラフィックに関する情報を収集します。

（注） FTD デバイスは、NetFlow データを渡すように設定できます。センサーを展開するときは、イベント情報を CDO に渡すように設定されている FTD デバイスからの NetFlow データを渡すようにセンサーを設定しないでください。

センサーの展開手順と推奨事項については、Secure Cloud Analytics センサーのインストールガイドを参照してください。

クラウドベース展開の設定手順と推奨事項については、Secure Cloud Analytics パブリック クラウド モニタリング ガイドを参照してください。

（注） Secure Cloud Analytics ポータルの UI で手順を確認して、センサーとクラウドベース展開を設定することもできます。

Secure Cloud Analytics の詳細については、Secure Cloud Analytics 無料試用ガイドを参照してください。

次の手順

- 「Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （421 ページ）」に進みます。

Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示

必要なライセンス：Logging Analytics and Detection または **Total Network Analytics and Monitoring**

[イベントロギング] ページでファイアウォールイベントを確認できますが、CDO ポータル UI から Cisco Secure Cloud Analytics アラートを確認することはできません。[セキュリティ分析（Security Analytics）] メニューオプションを使用して CDO から Secure Cloud Analytics ポータルをクロス起動し、ファイアウォール イベント データ（および [Total Network Analytics and Monitoring] を有効にしている場合はネットワークフローデータ）から生成されたアラートを表示できます。[セキュリティ分析（Security Analytics）] メニューオプションには、1 つ以上のワークフローステータスが開いている場合、開いているワークフローステータスの Secure Cloud Analytics アラートの数を示すバッジが表示されます。

Security Analytics and Logging ライセンスを使用して Secure Cloud Analytics アラートを生成し、新しい Secure Cloud Analytics ポータルをプロビジョニングした場合は、CDO にログインしてから、Cisco Secure Sign-On を使用して Secure Cloud Analytics をクロス起動します。URL を使用して Secure Cloud Analytics ポータルに直接アクセスすることもできます。

詳細については、『Cisco SecureX sign-on』を参照してください。

Cisco Secure Cloud Analytics ポータルへに参加するようユーザーを招待する

Cisco Secure Cloud Analytics ポータルのプロビジョニングをリクエストする最初のユーザーには、Cisco Secure Cloud Analytics ポータルの管理者権限があります。そのユーザーは、他のユーザーを電子メールで招待してポータルに参加させることができます。招待されたユーザーは、Cisco Secure Sign-On のログイン情報を持っていない場合、招待メールのリンクを使用して作成できます。ユーザーは、CDO から Cisco Secure Cloud Analytics へのクロス起動中に、Cisco Secure Sign-On のログイン情報を使用してログインできます。

電子メールで他のユーザーを Cisco Secure Cloud Analytics ポータルに招待するには、次の手順を実行します。

ステップ 1 Cisco Secure Cloud Analytics ポータルに管理者としてログインします。
ステップ 2 **[設定]** > **[アカウント管理（Account Management）]** > **[ユーザー管理（User Management）]** を選択します。
ステップ 3 [電子メール（Email）] アドレスを入力します。
ステップ 4 [招待（Invite）] をクリックします。

CDO から Secure Cloud Analytics をクロス起動する

CDO からのセキュリティアラートを表示するには以下を実行します。

ステップ 1 CDO ポータルにログインします。
ステップ 2 ナビゲーションバーから **[モニタリング]** > **[セキュリティ分析]**を選択します。
ステップ 3 Secure Cloud Analytics インターフェイスで **[監視]** > **[アラート]**を選択します。

Cisco Secure Cloud Analytics とダイナミック エンティティ モデリング

必要なライセンス：**Logging Analytics and Detection** または **Total Network Analytics and Monitoring**

Secure Cloud Analytics は、オンプレミスおよびクラウドベースのネットワーク展開をモニターする Software as a Service（SaaS）ソリューションです。ファイアウォールイベントとネットワークフローデータを含め、ネットワークトラフィックに関する情報をソースから収集することによって、トラフィックに関する観測内容が作成され、トラフィックパターンに基づいてネットワークエンティティのロールが自動的に識別されます。Secure Cloud Analytics は、この情報を他の脅威インテリジェンス（Talos など）のソースと組み合わせて使用してアラートを

生成します。このアラートは、本質的に悪意のある可能性がある動作の存在を示す警告を構成します。Secure Cloud Analytics は、このアラートとともに、ネットワークおよびホストの可視性と、収集したコンテキスト情報を提供します。このコンテキスト情報により、アラートを調査して悪意のある動作の原因を特定するためのより優れた基盤が得られます。

ダイナミック エンティティ モデリング

ダイナミック エンティティ モデリングは、ファイアウォールイベントとネットワークフローデータの動作分析を実行することにより、ネットワークの状態を追跡します。Secure Cloud Analyticsのコンテキストにおいて、エンティティとは、ネットワーク上のホストやエンドポイントといった、何らかの経時的に追跡できるものです。ダイナミック エンティティ モデリングは、ネットワークで送信されるトラフィックと実行されるアクティビティに基づいて、エンティティに関する情報を収集します。**Logging Analytics and Detection** ライセンスと統合されたSecure Cloud Analytics は、エンティティが通常送信するトラフィックのタイプを判別するために、ファイアウォールイベントやその他のトラフィック情報から引き出すことができます。**Total Network Analytics and Monitoring** ライセンスを購入すると、Secure Cloud Analytics は、エンティティトラフィックのモデル化にNetFlowおよびその他のトラフィック情報を含めることもできます。各エンティティの最新のモデルを維持するため、Secure Cloud Analytics では、エンティティがトラフィックを送信し続け、場合によっては異なるトラフィックを送信する可能性があるため、これらのモデルを徐々に更新します。この情報から、Secure Cloud Analytics は以下を識別します。

- エンティティのロール：これは、エンティティが通常行うことの記述子です。たとえば、エンティティが、一般に電子メールサーバーに関連付けられるトラフィックを送信する場合、Secure Cloud Analytics は、そのエンティティに電子メールサーバーロールを割り当てます。エンティティは複数のロールを実行する場合があるため、ロールとエンティティの関係は多対 1 である可能性があります。
- エンティティの観測内容：これは、ネットワーク上でのエンティティの動作に関する事実（外部 IP アドレスとのハートビート接続、別のエンティティとの間で確立されたリモートアクセスセッションなど）です。CDO と統合すると、ファイアウォールイベントからこれらの事実を取得できます。**Total Network Analytics and Monitoring** ライセンスも購入すると、システムはNetFlowから事実を取得し、ファイアウォールイベントとNetFlowの両方から観測内容を生成することもできます。観測内容それ自体は、それらが表すものの事実を超えた意味を持ちません。一般的なお客様は、何千もの観測内容と少数のアラートを持つ可能性があります。

アラートと分析

ロール、観測内容、およびその他の脅威インテリジェンスの組み合わせに基づいてSecure Cloud Analyticsが生成するアラートは、潜在的な悪意のある動作をシステムによって識別されたものとして表す実用的な項目です。1 つのアラートが複数の観測内容を表す場合があることに注意してください。ファイアウォールが同じ接続とエンティティに関連する複数の接続イベントをログに記録する場合、アラートが 1 つだけになる可能性があります。

上記の例で言えば、新しい内部デバイスの観測内容だけでは、潜在的な悪意のある動作は構成されません。ただし、時間の経過とともに、エンティティがドメインコントローラと一致する

トラフィックを送信する場合、システムではそのエンティティにドメイン コントローラ ロールが割り当てられます。その後、そのエンティティが、以前に接続を確立していない外部サーバーへの接続を確立し、異常なポートを使用して大量のデータを転送すると、システムは、[新しい大規模接続（外部）（New Large Connection (External)）] 観測内容と [例外ドメインコントローラ（Exceptional Domain Controller）] 観測内容をログに記録します。その外部サーバーが Talos ウォッチリストに登録されているものと識別された場合、これらすべての情報の組み合わせにより Secure Cloud Analytics はこのエンティティの動作に関するアラートを生成し、悪意のある動作を調査して対処するように促します。

Secure Cloud Analytics の Web ポータル UI でアラートを開くと、システムがアラートを生成した原因となっている観測内容を確認できます。これらの観測内容から、関連するエンティティに関する追加のコンテキスト（それらが送信したトラフィック、外部脅威インテリジェンス（利用可能な場合）など）も確認できます。また、エンティティが関係性を持っていたその他の観測内容やアラートを確認したり、この動作が他の潜在的に悪意のある動作に結び付いているかどうかを判断することもできます。

Secure Cloud Analytics でアラートを表示して閉じる場合、Secure Cloud Analytics UI からのトラフィックを許可またはブロックできないことに注意してください。デバイスをアクティブモードで展開した場合、ファイアウォール アクセス コントロール ルールを、トラフィックを許可またはブロックするように更新する必要があり、ファイアウォールがパッシブモードで展開されている場合は、ファイアウォールアクセスコントロールルールを更新する必要があります。

ファイアウォールイベントに基づくアラートの使用

必要なライセンス：Logging Analytics and Detection または **Total Network Analytics and Monitoring**

アラートのワークフロー

アラートのワークフローは、そのステータスに基づいて異なります。システムによってアラートが生成される場合、そのデフォルト ステータスは [オープン（Open）] であり、ユーザーは割り当てられません。アラートのサマリーを表示すると、デフォルトでは、当面注意が必要なすべてのオープン アラートが表示されます。

注：**Total Network Analytics and Monitoring** ライセンスを持っている場合、アラートは、NetFlow から生成された観測結果、ファイアウォールイベントから生成された観測結果、または両方のデータソースからの観測結果に基づいて生成できます。

アラートのサマリーを確認する際は、初期トリアージとして、アラートにステータスを割り当て、タグ付けし、更新することができます。フィルタ機能と検索機能を使用して、特定のアラートを検索したり、さまざまなステータスのアラートを表示したり、さまざまなタグや割り当て対象を関連付けたりすることができます。アラートのステータスは[スヌーズ（Snoozed）] に設定できます。この場合、そのアラートはスヌーズ期間が経過するまでオープンアラートのリストに表示されません。アラートから [スヌーズ（Snoozed）] ステータスを削除して、再びオープンアラートとして表示されるようにすることもできます。アラートを確認する際は、それらのアラートをそのユーザー自身またはシステム内の別のユーザーに割り当てることができ

ます。ユーザーは、自分のユーザー名に割り当てられているすべてのアラートを検索できます。

アラートのサマリーから、アラートの詳細ページを表示できます。このページでは、このアラートを生成させた、裏付けとなる観測内容に関する追加のコンテキストと、このアラートに関連するエンティティに関する追加のコンテキストを確認できます。この情報は、ネットワーク上の問題をさらに調査して悪意のある動作を潜在的に解決するために実際の問題を特定する上で役立ちます。

CDO の Stealthwatch Cloud Web ポータル UI 内やネットワーク上で調査しているときに、発見した内容を説明するコメントをアラートと一緒に残すことができます。これは、将来参照できる調査の記録を作成するために役立ちます。

分析が完了したら、ステータスを[クローズ（Closed）]に更新できます。これにより、デフォルトではオープンアラートとして表示されなくなります。将来、状況が変わった場合は、クローズ アラートのステータスを再度オープンにすることもできます。

ここでは、特定のアラートを調査する方法に関する一般的なガイドラインと推奨事項を示します。Stealthwatch Cloud はアラートをログに記録するときに追加のコンテキストを提供するため、このコンテキストを参照しながら調査を進めることができます。

これらの手順は、総合的または包括的であることを意図したものではありません。これらは単にアラートの調査を開始するための一般的な枠組みを提供するためのものです。

一般に、次の手順でアラートを確認できます。

1. オープンアラートのトリアージ （425 ページ）
2. 後で分析するためにアラートをスヌーズする （426 ページ）
3. 詳細な調査のためのアラートの更新 （427 ページ）
4. アラートの確認と調査の開始 （427 ページ）
5. エンティティとユーザーの調査 （429 ページ）
6. Secure Cloud Analytics を使用して問題を修復する （430 ページ）
7. アラートの更新とクローズ （431 ページ）

オープンアラートのトリアージ

特に複数の調査が必要な場合は、オープンアラートのトリアージを行います。

- CDO から SWC へのクロス起動とアラート表示の詳細については、「Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示」を参照してください。

次の質問に答えてください。

- このアラート タイプを優先度の高いものとして設定しましたか。
- 影響を受けるサブネットに高い機密性を設定しましたか。

- この異常な動作はネットワーク上の新しいエンティティによるものですか。
- エンティティの通常のロールは何ですか。また、このアラートの動作はそのロールにどのように適合しますか。
- これは、このエンティティの通常の動作からの例外的な逸脱ですか。
- ユーザーが関与している場合、これはユーザーの予想される動作ですか、それとも例外的な動作ですか。
- 保護されたデータや機密データが侵害を受けるリスクがありますか。
- この動作の継続を許可すると、ネットワークへの影響はどの程度深刻になりますか。
- 外部エンティティとの通信がある場合、それらのエンティティは過去にネットワーク上の他のエンティティとの接続を確立しましたか。

これが優先順位の高いアラートである場合は、調査を進める前に、インターネットからエンティティを隔離するか、隔離しないときは接続を切断することを検討してください。

後で分析するためにアラートをスヌーズする

他のアラートと比較して優先度が低いときに、アラートをスヌーズします。たとえば、組織が電子メールサーバーをFTPサーバーとして再利用する場合、緊急プロファイルアラートが生成されます（エンティティの現在のトラフィックが、以前には一致しなかった動作プロファイルと一致することを示します）。これは想定される動作であるため、このアラートをスヌーズして、後日再検討できます。スヌーズされたアラートは、オープンアラートと一緒に表示されません。これらのスヌーズされたアラートを確認するには、特別にフィルタリングする必要があります。

アラートをスヌーズする：

ステップ1 [アラートを閉じる（Close Alert）] をクリックします。

ステップ2 [このアラートをスヌーズ（Snooze this alert）] ペインで、ドロップダウンからスヌーズ期間を選択します。

ステップ3 [保存（**Save**）] をクリックします。

次のタスク

スヌーズしたアラートを確認する準備ができたら、アラートのスヌーズを解除できます。これにより、ステータスが[オープン（Open）]に設定され、他のオープンアラートとともにアラートが表示されます。

スヌーズしたアラートのスヌーズを解除する：

- スヌーズしたアラートから、[アラートのスヌーズ解除（Unsnooze Alert）] をクリックします。

詳細な調査のためのアラートの更新

アラートの詳細情報を確認します。

ステップ 1 **[モニター（Monitor）]** > **[アラート（Alerts）]** を選択します。

ステップ 2 アラートタイプ名をクリックします。

次のタスク

初期トリアージと優先順位付けに基づいて、アラートを割り当て、タグを付けます。

1. [担当者（Assignee）] ドロップダウンからユーザーを選択してアラートを割り当てます。これにより、ユーザーが調査を開始できるようになります。
2. [タグ（Tags）] ドロップダウンから 1 つ以上のタグを選択して、アラートにタグを追加することにより、将来の識別のためにアラートをより適切に分類したり、アラートの長期的なパターンの確立を試みることができます。
3. 必要に応じて、**このアラートに関するコメント**を入力し、[コメント（Comment）]をクリックすることにより、最初の調査結果を追跡するためのコメントを残し、アラートに割り当てられた担当者を支援することができます。アラートは、システムコメントとユーザーコメントの両方を追跡します。

アラートの確認と調査の開始

割り当てられたアラートを確認する場合は、アラートの詳細を確認して、Stealthwatch Cloud がアラートを生成した理由を把握してください。裏付けとなる観測内容を確認し、これらの観測内容がソースエンティティに対して持つ意味を理解します。

アラートがファイアウォールイベントに基づいて生成された場合、ファイアウォールの展開がこのアラートのソースであることはシステムに認識されません。

このソースエンティティの一般的な動作やパターンを理解するために、サポートされている観測内容をすべて表示し、このアクティビティがより長いトレンドの一部である可能性があるかどうかを確認します。

手順の概要

1. アラートの詳細で、観測タイプの横にある矢印アイコン（  ）をクリックして、そのタイプの記録されたすべての観測内容を表示します。
2. [ネットワークのすべての観測内容（All Observations for Network）] の横にある矢印アイコン（  ）をクリックして、このアラートのソースエンティティの記録された観測内容をすべて表示します。

手順の詳細

ステップ 1 アラートの詳細で、観測タイプの横にある矢印アイコン（）をクリックして、そのタイプの記録されたすべての観測内容を表示します。

ステップ 2 [ネットワークのすべての観測内容（All Observations for Network）] の横にある矢印アイコン（）をクリックして、このアラートのソースエンティティの記録された観測内容をすべて表示します。

観測内容に対して追加の分析を実行する場合は、サポートされている観測内容をコンマ区切り値ファイルでダウンロードします。

- アラートの詳細の [サポートされている観測内容（Supporting Observations）] ペインで、[CSV] をクリックします。

観測内容から、ソースエンティティの動作が悪意のある動作を示しているか判断します。ソースエンティティが複数の外部エンティティとの接続を確立している場合は、それらのエンティティが何らかの関連性を持つかどうか（それらのすべてが類似の地理位置情報を持っているか、それらの IP アドレスが同じサブネットからのものであるかなど）を確認します。

ソースエンティティの IP アドレスまたはホスト名から、ソースエンティティに関連する追加コンテキスト（関与している可能性がある他のアラートや観測内容、デバイス自体に関する情報、送信しているセッショントラフィックのタイプなど）を表示します。

- エンティティに関連するすべてのアラートを表示するには、IPアドレスまたはホスト名のドロップダウンから [アラート（Alerts）] を選択します。
- エンティティに関連するすべての観測内容を表示するには、IPアドレスまたはホスト名のドロップダウンから [観測内容（Observations）] を選択します。
- デバイスに関する情報を表示するには、IPアドレスまたはホスト名のドロップダウンから [デバイス] を選択します。
- このエンティティに関連するセッショントラフィックを表示するには、IPアドレスまたはホスト名のドロップダウンから [セッショントラフィック（Session Traffic）] を選択します。
- IP アドレスまたはホスト名をコピーするには、IP アドレスまたはホスト名のドロップダウンから [コピー] を選択します。

Stealthwatch Cloud のソースエンティティは常にネットワークの内部にあることに注意してください。この点を、接続を開始したエンティティを示し、ネットワークの内部または外部にある可能性がある、ファイアウォールイベントのイニシエータ IP と比較してください。

観測内容から、他の外部エンティティに関する情報を調べます。地理位置情報を調査し、いずれかの地理位置情報データまたは Umbrella データによって悪意のあるエンティティが特定されるかどうかを確認します。これらのエンティティによって生成されたトラフィックを表示します。Talos、AbuseIPDB、または Google にこれらのエンティティに関する情報があるかどうかを確認します。複数の日にわたる IP アドレスを見つけて、外部エンティティがネットワー

ク上のエンティティと確立した他のタイプの接続を確認します。必要に応じて、それらの内部エンティティを見つけ、侵害または意図しない動作の証拠があるかどうかを判断します。

ソースエンティティが接続を確立した外部エンティティの IP アドレスまたはホスト名のコンテキストを確認します。

- このエンティティの最近のトラフィック情報を表示するには、IPアドレスまたはホスト名のドロップダウンから [IPトラフィック（IP Traffic）] を選択します。
- このエンティティの最近のセッショントラフィック情報を表示するには、IPアドレスまたはホスト名のドロップダウンから [セッショントラフィック（Session Traffic）] を選択します。
- AbuseIPDB の Web サイト上でこのエンティティに関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから [AbuseIPDB] を選択します。
- Cisco Umbrella の Web サイト上でこのエンティティに関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから [Cisco Umbrella] を選択します。
- Google でこの IP アドレスを検索するには、IP アドレスまたはホスト名のドロップダウンから [Google検索（Google Search）] を選択します。
- Talos の Web サイト上でこの情報に関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから [Talos Intelligence] を選択します。
- このエンティティをウォッチリストに追加するには、IPアドレスまたはホスト名のドロップダウンから [IPをウォッチリストに追加（Add IP to watchlist）] を選択します。
- 前月のこのエンティティのトラフィックを検索するには、IPアドレスまたはホスト名のドロップダウンから [複数日のIPを検索（Find IP on multiple days）] を選択します。
- IP アドレスまたはホスト名をコピーするには、IP アドレスまたはホスト名のドロップダウンから [コピー（Copy）] を選択します。

Stealthwatch Cloud の接続エンティティは、常にネットワークの外部にあることに注意してください。この点を、接続要求に応答したエンティティを示し、ネットワークの内部または外部にある可能性がある、ファイアウォールイベントのレスポンダ IP と比較してください。

調査結果に関するコメントを残します。

- [アラートの詳細（ alert detail）] で、[このアラートに関するコメント（Comment on this alert）] を入力し、[コメント（Comment）] をクリックします。

エンティティとユーザーの調査

Stealthwatch Cloud ポータル UI でアラートを確認した後、ソースエンティティ、このアラートに関係している可能性のあるユーザー、およびその他の関連エンティティに対して、追加の調査を直接実行できます。

- ソースエンティティがネットワーク上のどこ（物理的またはクラウド上）にあるかを特定し、直接アクセスします。このエンティティのログファイルを見つけます。それがネット

ワーク上の物理エンティティである場合は、デバイスにアクセスしてログ情報を確認し、この動作の原因となっているものに関する情報があるかどうかを確認します。それが仮想エンティティである場合またはクラウドに保存されている場合は、ログにアクセスして、このエンティティに関連するエントリを検索します。不正なログイン、承認されていない設定変更などに関する詳細について、ログを調査します。

- エンティティを調査します。マルウェアまたはエンティティ自体にある脆弱性を特定できるかどうかを判断してください。デバイスの物理的な変更（組織によって承認されていない USB スティックなど）を含め、何らかの悪意のある変更があったかどうかを確認します。
- ネットワーク上のユーザーまたはネットワーク外のユーザーによる関与があったかどうかを確認します。可能であれば、何をしていたのかをユーザーに尋ねてください。ユーザーに尋ねることができない場合は、そのユーザーがアクセス権を持っていたと考えられるかどうかと、この動作を促す状況（解雇された従業員が退社する前に外部サーバーにファイルをアップロードするなど）が発生したかどうかを確認します。

調査結果に関するコメントを残します。

- [アラートの詳細（ alert detail）] で、[このアラートに関するコメント（Comment on this alert）] を入力し、[コメント（Comment）] をクリックします。

Secure Cloud Analytics を使用して問題を修復する

悪意のある動作によってアラートが発生した場合は、悪意のある動作を修正します。次に例を示します。

- 悪意のあるエンティティまたはユーザーがネットワーク外からのログインを試みた場合は、ファイアウォールルールとファイアウォール構成を更新して、それらのエンティティまたはユーザーがネットワークにアクセスできないようにします。
- エンティティが許可されていないドメインまたは悪意のあるドメインにアクセスを試みた場合は、影響を受けるエンティティを調べて、マルウェアが原因かどうかを判断します。悪意のある DNS リダイレクトがある場合は、ネットワーク上の他のエンティティが影響を受けているかどうか、またはボットネットの一部であるかどうかを判断します。これがユーザーによる意図である場合は、ファイアウォール設定のテストなど、正当な理由があるかどうかを判断します。ファイアウォールルールとファイアウォール構成を更新して、ドメインへのそれ以上のアクセスを防止します。
- エンティティが過去のエンティティモデルの動作と異なる動作を示している場合は、動作の変更が意図されたものかどうかを判断します。意図されたものでない場合は、変更の責任がネットワーク上の承認ユーザーにあるかどうかを調べます。ネットワークの外部にあるエンティティが関係している場合は、ファイアウォールルールとファイアウォール構成を更新して意図せぬ動作に対処します。
- 脆弱性またはエクスプロイトを特定した場合は、影響を受けるエンティティを更新したり、それらにパッチを適用して脆弱性を削除するか、ファイアウォール構成を更新して許可されていないアクセスを防止します。ネットワーク上の他のエンティティが同様に影響

を受ける可能性があるかどうかを判断し、それらのエンティティに同じ更新またはパッチを適用します。現時点で脆弱性またはエクスプロイトを修正する手段がない場合は、該当するベンダーに連絡し、それらを通知してください。

- マルウェアを特定した場合は、エンティティを隔離してマルウェアを削除します。ファイアウォールファイルおよびマルウェアイベントを確認してネットワーク上の他のエンティティが危険にさらされているかどうかを判断し、エンティティを検疫および更新して、このマルウェアが広がることを防止します。このマルウェアまたはこのマルウェアの原因となったエンティティに関する情報によってセキュリティ情報を更新してください。ファイアウォールのアクセス制御およびファイルとマルウェアルールを更新して、今後このマルウェアがネットワークに感染するのを防ぎます。必要に応じてベンダーに通知してください。
- 悪意のある動作によってデータが漏洩した場合は、許可されていないソースに送信されたデータの性質を確認します。不正なデータ漏洩に関する組織の規定に従ってください。ファイアウォール構成を更新して、このソースによる今後のデータ漏洩の試みを防ぎます。

アラートの更新とクローズ

調査結果に基づいてタグを追加します。

ステップ 1 Secure Cloud Analytics ポータルの UI で、**[監視]** > **[アラート]**を選択します。

ステップ 2 ドロップダウンから 1 つ以上の**タグ**を選択します。

調査結果と実行された修正手順を説明する最終コメントを追加します。

- アラートの詳細で、[このアラートに関するコメント] を入力し、[コメント] をクリックします。

アラートのステータスをクローズにして、役立つものかどうかが分かるようにマークします。

1. アラートの詳細から、[アラートを閉じる] をクリックします。
2. アラートが役立った場合は [はい] を、アラートが役立たなかった場合は [いいえ] を選択します。これはアラートが悪意のある動作に起因するかどうかではなく、単にアラートが組織にとって有用であったかどうかを意味する点に注意してください。
3. [保存（**Save**）] をクリックします。

次のタスク

クローズしたアラートの再オープン

クローズしたアラートに関連する追加情報を検出した場合、またはそのアラートに関連するコメントを追加する場合は、そのアラートを再度開いてステータスを [オープン（Open）] に変更できます。その後、必要に応じてアラートを変更し、追加調査が完了したら再度閉じます。

クローズしたアラートを再オープンします。

- クローズしたアラートの詳細から、[アラートを再オープン] をクリックします。

アラートの優先順位を変更する

必要なライセンス：**Logging Analytics and Detection** または **Total Network Analytics and Monitoring**

アラートタイプにはデフォルトの優先順位が設定されています。これは、このタイプのアラートを生成するシステムの機密性に影響します。アラートの優先順位は、シスコのインテリジェンスおよびその他の要因に基づいて、[低] または [通常] にデフォルト設定されます。ネットワーク環境に基づいて、関心のある特定のアラートを強調するために、アラートタイプの優先順位を変更することができます。アラートタイプの優先順位は、[低]、[通常]、または [高] に設定できます。

- **[モニター]** > **[アラート]** を選択します。
- 設定のドロップダウンアイコン（）をクリックし、[アラートのタイプと優先順位] を選択します。
- アラートタイプの横にある編集のアイコン（）をクリックし、[低]、[中]、または [高] を選択して優先順位を変更します。

ライブイベントを表示する

[ライブ]イベントページには、入力したイベントロギングページでのイベントの検索とフィルタリングに一致する、直近 500 件のイベントが表示されます。[ライブ] ページに最大数である 500 のイベントが表示されており、さらに表示されるイベントが追加されると、CDO は最新のライブイベントを表示し、最も古いライブイベントを [履歴] イベントページに転送します。これにより、ライブイベントの総数が 500 に維持されます。この転送には、約 1 分を要します。フィルタリング基準を追加しない場合は、イベントを記録するように設定されたルールによって生成された最新の 500 のライブイベントがすべて表示されます。

イベントのタイムスタンプは、イベントを表示している CDO 管理者の現地時間で表示されます。

ライブイベントが再生中か一時停止中かにかかわらず、フィルタリング基準を変更すると、イベント画面がクリアされ、収集プロセスが再開されます。

CDO イベントビューアでライブイベントを表示するには、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、**[モニターリング（Monitoring）]>[イベントロギング]** をクリックします。
ステップ 2 [ライブ] タブをクリックします。

次のタスク

次の関連情報を参照して、イベントを再生および一時停止する方法を確認します。

関連情報：

- ライブイベントの再生/一時停止 （433 ページ）
- 履歴イベントの表示 （434 ページ）
- イベントビューのカスタマイズ （434 ページ）

ライブイベントの再生/一時停止

ライブイベントがストリーミング中に「再生」 または「一時停止」 できます。ライブイベントが「再生中」の場合、CDO は、イベントビューアで指定されたフィルタ処理基準に一致するイベントを受信順に表示します。イベントが一時停止された場合、ライブイベントの再生を再開するまで、CDO はライブイベントページを更新しません。イベントの再生を再開すると、CDO は、イベントの再生を再開した時点からライブページへのイベントの入力を開始します。見逃したイベントが遡って再生されることはありません。

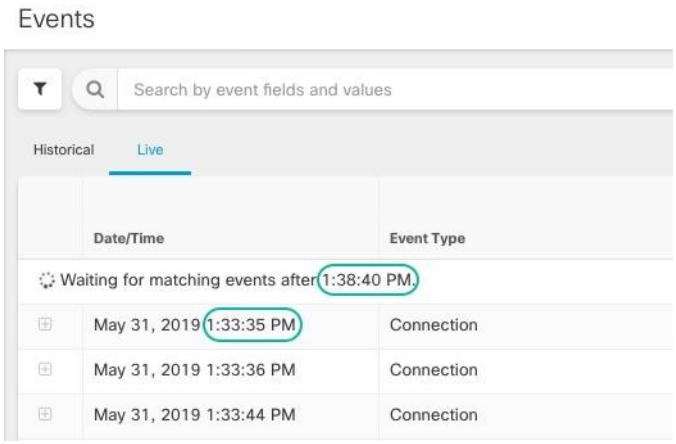
ライブイベントのストリーミングを再生または一時停止したかどうかにかかわらず、CDO が受信したすべてのイベントを表示するには、[履歴] タブをクリックします。

ライブイベントの自動一時停止

イベントを約 5 分間連続して表示した後、CDO は、ライブイベントのストリーミングを一時停止しようとしていることを警告します。その時点で、リンクをクリックしてライブイベントのストリーミングをさらに5分間継続するか、ストリーミングを停止することができます。準備ができたら、ライブイベントのストリーミングを再開できます。

イベントの受信とレポート

Secure Event Connector（SEC）がイベントを受信してから、CDO がライブイベントビューアにイベントを投稿するまでに、わずかに遅れが生じる場合があります。ライブページで遅延を確認できます。イベントのタイムスタンプは、SEC がイベントを受信した時刻です。



履歴イベントの表示

[ライブ]イベントページには、入力したイベントロギングページでのイベントの検索とフィルタリングに一致する、直近 500 件のイベントが表示されます。直近の 500 件より古いイベントは、[履歴] イベントテーブルに転送されます。この転送には、約 1 分を要します。その後、保存したすべてのイベントをフィルタリングして、探しているイベントを見つけることができます。

履歴イベントを表示するには、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、[モニターリング（Monitoring）] > [イベントロギング] をクリックします。

ステップ 2 [履歴（Historic）] タブをクリックします。デフォルトでは、[履歴] イベントテーブルを開くと、フィルタは過去 1 時間以内に収集されたイベントを表示するように設定されています。

イベントの属性は、Firepower Device Manager（FDM）または Adaptive Security Device Manager（ASDM）によって報告されるものとほぼ同じです。

- Firepower Threat Defense イベント属性の完全な説明については、『Cisco Firepower Threat Defense Syslog メッセージ』を参照してください。
- ASA イベント属性の詳細については、『Cisco ASA シリーズ Syslog メッセージ』を参照してください。

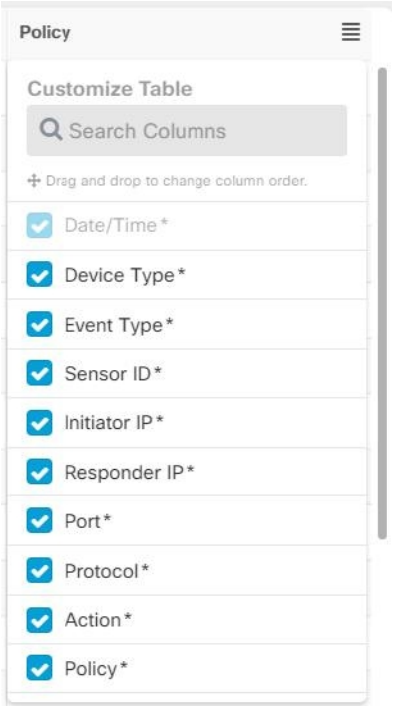
イベントビューのカスタマイズ

[イベントロギング]ページに加えられた変更は、このページから移動して後で戻ったときに備えて自動的に保存されます。

（注） ライブイベントと履歴イベントビューの設定は同じです。イベントビューをカスタマイズすると、変更はライブビューと履歴ビューの両方に適用されます。

列

ライブイベントと履歴イベントの両方のイベントビューを変更して、必要なビューに適用される列ヘッダーのみを含めることができます。列の右側にある列フィルタアイコン をクリックし、必要な列を選択または選択解除します。



アスタリスクの付いた列は、デフォルトでイベントテーブル内に含まれますが、いつでも削除できます。検索バーを使用して、追加する列のキーワードを手動で検索します。

順序

[イベント（Events）] ビューの列を並べ替えることができます。列の右側にある列フィルタアイコン をクリックして、選択した列のリストを展開し、列を目的の順序に手動でドラッグアンドドロップします。ドロップダウンメニューのリストの上部にある列がイベントビューの左端の列です。

関連情報：

- イベントロギングページでのイベントの検索とフィルタリング
- Security Analytics and Logging のイベント属性

イベントロギングページの列の表示および非表示

[イベントロギング] ページには、設定済み ASA および FTD デバイスから Cisco Cloud に送信された ASA および FTD Syslog イベントと、ASANetFlow セキュアイベントロギング（NSEL）イベントが表示されます。

テーブルで表示/非表示ウィジェットを使用して、[イベントロギング]ページの列を表示したり非表示にしたりできます。

ステップ 1 CDO のナビゲーションバーから、**[モニタリング]** > **[イベントロギング]**を選択します。

ステップ 2 テーブルの右端までスクロールし、[列の表示/非表示] ボタン ≡ をクリックします。

ステップ 3 表示する列のチェックボックスをオンにし、非表示にする列のチェックボックスをオフにします。

ステップ 4 [列の表示/非表示] ドロップダウンメニューの列名にマウスカーソルを合わせ、灰色の **+** をクリックして列の順序を変更します。

列が再び表示されるか非表示にされるまで、表示するように選択した列がテナントにログインしている他のユーザーにも表示されます。

以下の表は列ヘッダーについて説明しています。

カラム ヘッダ	説明
Date/Time	デバイスがイベントを生成した時間。時間はコンピュータのローカル時間で表示されます。
デバイスタイプ（Device Type）	ASA（適応型セキュリティアプライアンス） または FTD（Firepower Threat Defense）

カラム ヘッダ	説明

イベント タイプ（Event Type）	この複合列には、以下のいずれかを含めることができます。
	• **FTD イベントタイプ**
	  • 接続：アクセス制御ルールからの接続イベントを表示します。
	  • ファイル：アクセス制御ルールのファイルポリシーによってレポートされたイベントを表示します。
	  • 侵入：アクセス制御ルールの侵入ポリシーによってレポートされたイベントを表示します。
	  • マルウェア：アクセス制御ルールのマルウェアポリシーによって報告されたイベントを表示します。
	• ASA **イベントタイプ**：これらのイベントタイプは、syslog または NetFlow イベントのグループを表します。syslog ID または NetFlow ID が含まれているグループの詳細については、「ASA イベントタイプ」を参照してください。
	  • 解析されたイベント：解析された syslog イベントには、他の syslog イベントよりも多くのイベント属性が含まれており、CDO はそれらの属性に基づいて検索結果をより迅速に返すことができます。解析されたイベントはフィルタ処理カテゴリではありませんが、解析されたイベント ID は、[イベントタイプ] 列に斜体で表示されます。斜体で表示されていないイベント ID は解析されていません。
	  • ASANetFlow イベント ID：ASA からのすべての Netflow（NSEL）イベントがここに表示されます。

カラム ヘッダ	説明
センサー ID（Sensor ID）	センサー ID は、イベントを Secure Event Connector に送信する IP アドレスです。これは通常、Firepower Threat Defense または ASA の管理インターフェイスです。
[イニシエータ IP（Initiator IP）]	これは、ネットワークトラフィックの送信元の IP アドレスです。イニシエータ アドレス フィールドの値は、イベントの詳細の InitiatorIP フィールドの値に対応します。10.10.10.100 などの単一のアドレス、または 10.10.10.0/24 などの CIDR 表記で定義されたネットワークを入力できます。
レスポンダ IP（Responder IP）	これは、パケットの宛先 IP アドレスです。宛先アドレスフィールドの値は、イベントの詳細の ResponderIP フィールドの値に対応します。10.10.10.100 などの単一のアドレス、または 10.10.10.0/24 などの CIDR 表記で定義されたネットワークを入力できます。
ポート（Port）	セッション**レスポンダ**が使用するポートまたは ICMP コードです。宛先ポートの値は、イベントの詳細の **ResponderPort** の値に対応します
プロトコル（Protocol）	これは、イベントのプロトコルを表します。

カラム ヘッダ	説明
操作	ルールによって定義されたセキュリティアクションを指定します。入力する値は、検索対象と完全に一致する必要がありますが、大文字小文字は関係ありません。各イベントタイプ（接続、ファイル、侵入、マルウェア、syslog、および NetFlow）に異なる値を入力します。 • 接続イベントタイプの場合、フィルタは AC_RuleAction 属性で一致を検索します。それらの値は、Allow、Block、Trust のいずれかです。 • ファイルイベントタイプの場合、フィルタは FileAction 属性で一致を検索します。それらの値は、Allow、Block、Trust のいずれかです。 • 侵入イベントタイプの場合、フィルタは InLineResult 属性で一致を検索します。それらの値は、Allowed、Blocked、Trusted のいずれかです。 • マルウェアイベントタイプの場合、フィルタは FileAction 属性で一致を検索します。それらの値は、クラウド ルックアップ タイムアウトである可能性があります。 • syslog および NetFlow イベントタイプの場合、フィルタは Action 属性で一致を検索します。
ポリシー	イベントをトリガーしたポリシーの名前です。ASA と FTD デバイスでは名前が異なります。

関連情報：

イベントロギングページでのイベントの検索とフィルタリング （475 ページ）

カスタマイズ可能なイベントフィルタ

Secure Logging Analytics（SaaS）のお客様は、頻繁に使用するカスタムフィルタを作成して保存できます。

フィルタの要素は、設定時にフィルタのタブに保存されます。[イベントロギング]ページに戻るたびに、これらの検索機能を使用できます。テナントの他の CDO ユーザーは使用できません。複数のテナントを管理している場合、別のテナントでは使用できません。

（注） フィルタのタブで作業しているときにフィルタ条件を変更すると、加えられた変更はカスタムフィルタのタブに自動的に保存されることに注意してください。

ステップ 1 メインメニューから、**[モニタリング（Monitoring）]** > **[イベントロギング]** を選択します。

ステップ 2 値の [検索（Search）] フィールドをクリアします。

ステップ 3 イベントテーブルの上にある青いプラスボタンをクリックして、[表示（View）] タブを追加します。フィルタ表示には、名前を付けるまで、[表示1（View 1）]、[表示2（View 2）]、[表示3（View 3）] のようにラベルが付けられます。

ステップ 4 ビューのタブを選択します。

ステップ 5 フィルタバーを開き、カスタムフィルタに必要なフィルタ属性を選択します。「イベントロギングページでのイベントの検索とフィルタリング （475 ページ）」を参照してください。カスタムフィルタにはフィルタ属性のみが保存されることに注意してください。

ステップ 6 [イベントロギング] テーブルに表示する列をカスタマイズします。列の表示と非表示については、「イベントロギングページの列の表示および非表示 （436 ページ）」を参照してください。

ステップ 7 [表示X（View X）] ラベルの付いたフィルタタブをダブルクリックし、名前を変更します。

ステップ 8 （オプション）カスタムフィルタを作成したので、[検索（Search）] フィールドに検索条件を追加することにより、カスタムフィルタを変更せずに、[イベントロギング]ページに表示される結果を微調整できます。「イベントロギングページでのイベントの検索とフィルタリング （475 ページ）」を参照してください。

ステップ 9 （オプション）カスタムフィルタの結果を .csv.gz ファイルにダウンロードして、さらに並べ替えと分析を行います。[イベントのダウンロード（Downloading Events）]イベントのダウンロード （440 ページ）を参照してください。

イベントのダウンロード

[イベントログ（Event Logging）] ページの [履歴（Historical）] タブに表示されるイベントを、CDO からダウンロードできます。イベントダウンロードのいくつかの機能を次に示します。

- CDOがイベントを .csv ファイルに追加し、.gz 形式で圧縮します。
- 1 つの .csv ファイルに、最大約 50 GB の圧縮情報を収容できます。
- ダウンロード可能なファイルの生成は並行して実行できます。

- 作成された .csv.gz ファイルは Cisco Cloud に保存され、そこから直接ダウンロードされます。これらのファイルは、CDO/Secure Cloud Analytics サーバーリソースを消費しません。
- 作成されたダウンロード可能な .csv.gz ファイルは 7 日間保存され、その後削除されます。
- 進行中のジョブは手動でキャンセルできます。

[イベントログ（Event Logging）] ページに表示されるイベントのダウンロードは、次の 2 段階のプロセスです。

ステップ 1 .CSV.GZ ファイルの生成。（これは、GNU Gzip 形式を使用して圧縮されたカンマ区切り値のファイルです。GNU Gzip の詳細については、https://www.gnu.org/software/gzip/を参照してください）。

ステップ 2 .CSV.GZ ファイルのダウンロード。

次のタスク

.CSV.GZ ファイルの内容 （442 ページ）について学ぶ

.CSV.GZ ファイルの生成

ステップ 1 CDO のメニューバーから、**[モニタリング（Monitoring）]** > **[イベントロギング（Event Logging）]** を選択します。

ステップ 2 そのビューがまだ表示されていない場合は、[履歴] タブをクリックします。

ステップ 3 イベントフィルタと検索フィールドを使用して、ダウンロードするイベントを見つけます。そのフィルタリングと検索の結果に一致し、指定した時間範囲内に発生したイベントが、.csv.gz ファイルに含まれます。

ステップ 4 [.CSVの生成（Generate .CSV）] ボタンをクリックします。

ステップ 5 CDO がイベントを検出する時間範囲を選択します。

ステップ 6 わかりやすいファイル名を入力します。

ステップ 7 [.CSVの生成（Generate .CSV）] をクリックします。[ダウンロードおよび生成したファイル（Downloaded Generated Files）] ボタンをクリックすると、生成したファイルを見つけることができます。

（注） 実行中の .CSV ファイルの生成をキャンセルする場合は、[ダウンロードおよび生成したファイル（Downloaded Generated Files）] ボタンをクリックし、実行中のジョブを見つけて、[キャンセル] をクリックします。

.CSV.GZ ファイルのダウンロード

ステップ 1 CDO のメニューバーから、**[モニターリング（Monitoring）]** > **[イベントロギング]** を選択します。

ステップ 2 [生成されたファイルのダウンロード（Download Generated Files）] ボタンをクリックします。

ステップ 3 生成されたファイルを選択し、[ダウンロード（Download）] をクリックします。ファイルは圧縮形式であることに注意してください。

ステップ 4 ファイルを保存する場所を選択します。

.CSV.GZ ファイルの内容

.csv.gz フィールドの列には、イベントの展開された行に含まれるフィールドが反映されます。タイムスタンプ、FirstPacketSecond、および LastPacketSecond は、**協定世界時（UTC）**の秒単位で .csv ファイルに記録されます。

Security Analytics and Logging のイベント属性

イベント属性の説明

CDO によって使用されるイベント属性の説明は、Firepower Device Manager（FDM）および Adaptive Security Device Manager（ASDM）によって報告されるものとほぼ同じです。

- 適応型セキュリティアプライアンス（ASA）イベント属性の詳細については、「Cisco ASA シリーズ Syslog メッセージ」を参照してください。

一部の ASA syslog イベントは「解析」され、その他には、属性値ペアを使用してイベントログテーブルの内容をフィルタリングするときに使用できる追加の属性があります。syslog イベントのその他の重要な属性については、次の追加トピックを参照してください。

- 解析済みの ASA Syslog イベント
- 一部の Syslog メッセージの EventGroup および EventGroupDefinition 属性
- Syslog イベントの EventName 属性
- Syslog イベントの時間属性

一部の Syslog メッセージの EventGroup および EventGroupDefinition 属性

一部の syslog イベントには、追加の属性「EventGroup」および「EventGroupDefinition」があります。属性:値のペアでフィルタ処理することにより、これらの追加属性を使用してイベントテーブルをフィルタ処理し、イベントを見つけることができます。たとえば、イベントロギングテーブルの [検索（search）] フィールドに「`apfw:415*`」と入力して、アプリケーション ファイアウォール イベントをフィルタできます。

syslog メッセージのクラスおよび関連付けられているメッセージ ID 番号

EventGroup	EventGroupDefinition	Syslog メッセージ ID 番号（最初の 3 桁）
aaa/auth	ユーザ認証	109、113
acl/session	アクセスリスト/ユーザーセッション	106
apfw	アプリケーション ファイアウォール	415
bridge	トランスペアレント ファイアウォール	110、220
ca	PKI 証明機関	717
citrix	Citrix クライアント	723
clst	クラスタリング	747
cmgr	カード管理	323
config	コマンド インターフェイス	111、112、208、308
csd	セキュアなデスクトップ	724
cts	Cisco TrustSec	776
dap	ダイナミック アクセス ポリシー	734
eap、eapoudp	ネットワーク アドミッション コントロール用の EAP または EAPoUDP	333、334
eigrp	EIGRP ルーティング	336
email	電子メール プロキシ	719
ipaa/envmon	環境モニタリング	735
ha	フェールオーバー	101、102、103、104、105、210、311、709

EventGroup	EventGroupDefinition	Syslog メッセージ ID 番号（最初の 3 桁）
idfw	Identity-Based ファイアウォール	746
ids	侵入検知システム	733
ids/ips	侵入検知システム/侵入防御システム	400
ikev2	IKEv2 ツールキット	750、751、752
ip	IP スタック	209、215、313、317、408
ipaa	IP アドレスの割り当て	735
ips	侵入防御システム	401、420
ipv6	IPv6	325
l4tm	ブロックリスト、許可リスト、グレーリスト	338
lic	ライセンシング	444
mdm-proxy	MDM プロキシ	802
nac	ネットワーク アドミッション コントロール	731、732
vpn/nap	IKE と IPsec /ネットワーク アクセス ポイント	713
np	ネットワーク プロセッサ	319
ospf	OSPF ルーティング	318、409、503、613
passwd	パスワードの暗号化	742
pp	Phone Proxy	337
rip	RIP ルーティング	107、312
rm	Resource Manager	321
sch	Smart Call Home	120
session	ユーザ セッション	108、201、202、204、302、303、304、314、405、406、407、500、502、607、608、609、616、620、703、710
session/natpat	ユーザーセッション/NAT および PAT	305
snmp	SNMP	212

EventGroup	EventGroupDefinition	Syslog メッセージ ID 番号（最初の 3 桁）
ssafe	ScanSafe	775
ssl/np ssl	SSL スタック/NP SSL	725
svc	SSL VPN クライアント	722
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711、741
tre	トランザクション ルール エンジン	780
ucime	UC-IME	339
tag-switching	サービス タグ スイッチング	779
td	脅威の検出	733
vm	VLAN マッピング	730
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN クライアント	611
vpnfo	VPN フェールオーバー	720
vpnlb	VPN ロード バランシング	718
vxlan	VXLAN	778
webfo	WebVPN フェールオーバー	721
webvpn	WebVPN および AnyConnect クライアント	716
session/natpat	ユーザーセッション/NAT および PAT	305

Syslog イベントの EventName 属性

一部の syslog イベントには、付加的な属性「EventName」が含まれます。EventName 属性を使用して、属性と値のペアでフィルタリングすることにより、イベントテーブルをフィルタリングしてイベントを見つけることができます。たとえば、[イベントロギング] テーブルの検索フィールドに「**EventName:"Denied IP Packet"**」と入力することで、「Denied IP packet」のイベントをフィルタリングできます。

Syslog イベント ID とイベント名のテーブル

- AAA Syslog イベント ID とイベント名
- ボットネット Syslog イベント ID とイベント名
- フェールオーバー Syslog イベント ID とイベント名
- ファイアウォール拒否 Syslog イベント ID とイベント名
- ファイアウォール トラフィック Syslog イベント ID とイベント名
- アイデンティティ ベース ファイアウォール Syslog イベント ID とイベント名
- IPSec Syslog イベント ID とイベント名
- NAT Syslog イベント ID とイベント名
- SSL VPN Syslog イベント ID とイベント名

AAA Syslog イベント ID とイベント名

EventID	EventName
109001	AAA Begin
109002	AAA Failed
109003	AAA Server Failed
109005	Authentication Success
109006	認証に失敗
109007	Authorization Success
109008	「許可に失敗しました（Authorization Failed）」
109010	AAA Pending
109011	AAA Session Started
109012	AAA Session Ended
109013	AAA
109014	AAA Failed
109016	AAA ACL not found
109017	AAA Limit Reach
109018	AAA ACL Empty
109019	AAA ACL error

EventID	EventName
109020	AAA ACL error
109021	AAA error
109022	AAA HTTP limit reached
109023	AAA auth required
109024	「許可に失敗しました（Authorization Failed）」
109025	「許可に失敗しました（Authorization Failed）」
109026	AAA error
109027	AAA Server error
109028	AAA Bypassed
109029	AAA ACL error
109030	AAA ACL error
109031	認証に失敗
109032	AAA ACL error
109033	認証に失敗
109034	認証に失敗
109035	AAA Limit Reach
113001	AAA Session limit reach
113003	AAA overridden
113004	AAA Successful
113005	Authorization Rejected
113006	AAA user locked
113007	AAA User unlocked
113008	AAA successful
113009	AAA retrieved
113010	AAA Challenge received
113011	AAA retrieved

EventID	EventName
113012	認証成功
113013	AAA error
113014	AAA error
113015	認証を却下
113016	AAA Rejected
113017	AAA Rejected
113018	AAA ACL error
113019	AAA Disconnected
113020	AAA error
113021	AAA Logging Fail
113022	AAA Failed
113023	AAA reactivated
113024	AAA Client certification
113025	AAA Authentication fail
113026	AAA error
113027	AAA error

ボットネット Syslog イベント ID とイベント名

EventID	EventName
338001	Botnet Source Block List
338002	Botnet Destination Block List
338003	Botnet Source Block List
338004	Botnet Destination Block List
338101	Botnet Source Allow List
338102	Botnet destination Allow List
338202	Botnet destination Grey
338203	Botnet Source Grey
338204	Botnet Destination Grey

EventID	EventName
338301	Botnet DNS Intercepted
338302	Botnet DNS
338303	Botnet DNS
338304	Botnet Download successful
338305	Botnet Download failed
338306	Botnet Authentication failed
338307	Botnet Decrypt failed
338308	Botnet Client
338309	Botnet Client
338310	Botnet dyn filter failed

フェールオーバー Syslog イベント ID とイベント名

EventID	EventName
101001	Failover Cable OK
101002	Failover Cable BAD
101003	Failover Cable not connected
101004	Failover Cable not connected
101005	Failover Cable reading error
102001	Failover Power failure
103001	No response from failover mate
103002	Failover mate interface OK
103003	Failover mate interface BAD
103004	Failover mate reports failure
103005	Failover mate reports self failure
103006	Failover version incompatible
103007	Failover version difference
104001	Failover role switch
104002	Failover role switch

EventID	EventName
104003	Failover unit failed
104004	Failover unit OK
106100	Permit/Denied by ACL
210001	Stateful Failover error
210002	Stateful Failover error
210003	Stateful Failover error
210005	Stateful Failover error
210006	Stateful Failover error
210007	Stateful Failover error
210008	Stateful Failover error
210010	Stateful Failover error
210020	Stateful Failover error
210021	Stateful Failover error
210022	Stateful Failover error
311001	Stateful Failover update
311002	Stateful Failover update
311003	Stateful Failover update
311004	Stateful Failover update
418001	Denied Packet to Management
709001	Failover replication error
709002	Failover replication error
709003	Failover replication start
709004	Failover replication complete
709005	Failover receive replication start
709006	Failover receive replication complete
709007	Failover replication failure
710003	Denied access to Device

ファイアウォール拒否 Syslog イベント ID とイベント名

EventID	EventName
106001	Denied by Security Policy
106002	Outbound Deny
106006	Denied by Security Policy
106007	Denied Inbound UDP
106008	Denied by Security Policy
106010	Denied by Security Policy
106011	Denied Inbound
106012	Denied due to Bad IP option
106013	Dropped Ping to PAT IP
106014	Denied Inbound ICMP
106015	Denied by Security Policy
106016	Denied IP Spoof
106017	Denied due to Land Attack
106018	Denied outbound ICMP
106020	Denied IP Packet
106021	Denied TCP
106022	Denied Spoof packet
106023	Denied IP Packet
106025	Dropped Packet failed to Detect context
106026	Dropped Packet failed to Detect context
106027	Dropped Packet failed to Detect context
106100	Permit/Denied by ACL
418001	Denied Packet to Management
710003	Denied access to Device

ファイアウォール トラフィック Syslog イベント ID とイベント名

EventID	EventName
108001	Inspect SMTP

EventID	EventName
108002	Inspect SMTP
108003	Inspect ESMTP Dropped
108004	Inspect ESMTP
108005	Inspect ESMTP
108006	Inspect ESMTP Violation
108007	Inspect ESMTP
110002	No Router found
110003	Failed to Find Next hop
209003	Fragment Limit Reach
209004	Fragment invalid Length
209005	Fragment IP discard
302003	H245 Connection Start
302004	H323 Connection start
302009	Restart TCP
302010	Connection USAGE
302012	H225 CALL SIGNAL CONN
302013	Built TCP
302014	Teardown TCP
302015	Built UDP
302016	Teardown UDP
302017	Built GRE
302018	Teardown GRE
302019	H323 Failed
302020	Built ICMP
302021	Teardown ICMP
302022	Built TCP Stub
302023	Teardown TCP Stub
302024	Built UDP Stub

EventID	EventName
302025	Teardown UDP Stub
302026	Built ICMP Stub
302027	Teardown ICMP Stub
302033	Connection H323
302034	H323 Connection Failed
302035	Built SCTP
302036	Teardown SCTP
303002	FTP file download/upload
303003	Inspect FTP Dropped
303004	Inspect FTP Dropped
303005	Inspect FTP reset
313001	ICMP Denied
313004	ICMP Drop
313005	ICMP Error Msg Drop
313008	ICMP ipv6 Denied
324000	GTP Pkt Drop
324001	GTP Pkt Error
324002	メモリ エラー
324003	GTP Pkt Drop
324004	GTP Version Not Supported
324005	GTP Tunnel Failed
324006	GTP Tunnel Failed
324007	GTP Tunnel Failed
337001	Phone Proxy SRTP Failed
337002	Phone Proxy SRTP Failed
337003	Phone Proxy SRTP Auth Fail
337004	Phone Proxy SRTP Auth Fail
337005	Phone Proxy SRTP no Media Session

EventID	EventName
337006	Phone Proxy TFTP Unable to Create File
337007	Phone Proxy TFTP Unable to Find File
337008	Phone Proxy Call Failed
337009	Phone Proxy Unable to Create Phone Entry
400000	IPS IP options-Bad Option List
400001	IPS IP options-Record Packet Route
400002	IPS IP options-Timestamp
400003	IPS IP options-Security
400004	IPS IP options-Loose Source Route
400005	IPS IP options-SATNET ID
400006	IPS IP options-Strict Source Route
400007	IPS IP Fragment Attack
400008	IPS IP Impossible Packet
400009	IPS IP Fragments Overlap
400010	IPS ICMP Echo Reply
400011	IPS ICMP Host Unreachable
400012	IPS ICMP Source Quench
400013	IPS ICMP Redirect
400014	IPS ICMP Echo Request
400015	IPS ICMP Time Exceeded for a Datagram
400017	IPS ICMP Timestamp Request
400018	IPS ICMP Timestamp Reply
400019	IPS ICMP Information Request
400020	IPS ICMP Information Reply
400021	IPS ICMP Address Mask Request
400022	IPS ICMP Address Mask Reply
400023	IPS Fragmented ICMP Traffic
400024	IPS Large ICMP Traffic

EventID	EventName
400025	IPS Ping of Death Attack
400026	IPS TCP NULL flags
400027	IPS TCP SYN+FIN flags
400028	IPS TCP FIN only flags
400029	IPS FTP Improper Address Specified
400030	IPS FTP Improper Port Specified
400031	IPS UDP Bomb attack
400032	IPS UDP Snork attack
400033	IPS UDP Chargen DoS attack
400034	IPS DNS HINFO Request
400035	IPS DNS Zone Transfer
400036	IPS DNS Zone Transfer from High Port
400037	IPS DNS Request for All Records
400038	IPS RPC Port Registration
400039	IPS RPC Port Unregistration
400040	IPS RPC Dump
400041	IPS Proxied RPC Request
400042	IPS YP server Portmap Request
400043	IPS YP bind Portmap Request
400044	IPS YP password Portmap Request
400045	IPS YP update Portmap Request
400046	IPS YP transfer Portmap Request
400047	IPS Mount Portmap Request
400048	IPS Remote execution Portmap Request
400049	IPS Remote execution Attempt
400050	IPS Statd Buffer Overflow
406001	Inspect FTP Dropped
406002	Inspect FTP Dropped

EventID	EventName
407001	Host Limit Reach
407002	Embryonic limit Reached
407003	Established limit Reached
415001	Inspect Http Header Field Count
415002	Inspect Http Header Field Length
415003	Inspect Http body Length
415004	Inspect Http content-type
415005	Inspect Http URL length
415006	Inspect Http URL Match
415007	Inspect Http Body Match
415008	Inspect Http Header match
415009	Inspect Http Method match
415010	Inspect transfer encode match
415011	Inspect Http Protocol Violation
415012	Inspect Http Content-type
415013	Inspect Http Malformed
415014	Inspect Http Mime-Type
415015	Inspect Http Transfer-encoding
415016	Inspect Http Unanswered
415017	Inspect Http Argument match
415018	Inspect Http Header length
415019	Inspect Http status Matched
415020	Inspect Http non-ASCII
416001	Inspect SNMP dropped
419001	Dropped packet
419002	Duplicate TCP SYN
419003	Packet modified
424001	Denied Packet

EventID	EventName
424002	Dropped Packet
431001	Dropped RTP
431002	Dropped RTCP
500001	Inspect ActiveX
500002	Inspect Java
500003	Inspect TCP Header
500004	Inspect TCP Header
500005	Inspect Connection Terminated
508001	Inspect DCERPC Dropped
508002	Inspect DCERPC Dropped
509001	Prevented No Forward Cmd
607001	Inspect SIP
607002	Inspect SIP
607003	Inspect SIP
608001	Inspect Skinny
608002	Inspect Skinny dropped
608003	Inspect Skinny dropped
608004	Inspect Skinny dropped
608005	Inspect Skinny dropped
609001	Built Local-Host
609002	Teardown Local Host
703001	H225 Unsupported Version
703002	H225 Connection
726001	Inspect Instant Message

アイデンティティ ベース ファイアウォール Syslog イベント ID とイベント名

EventID	EventName
746001	Import started

EventID	EventName
746002	Import complete
746003	Import failed
746004	Exceed user group limit
746005	AD Agent down
746006	AD Agent out of sync
746007	Netbios response failed
746008	Netbios started
746009	Netbios stopped
746010	Import user failed
746011	Exceed user limit
746012	User IP add
746013	User IP delete
746014	FQDN Obsolete
746015	FQDN resolved
746016	DNS lookup failed
746017	Import user issued
746018	Import user done
746019	Update AD Agent failed

IPSec Syslog イベント ID とイベント名

EventID	EventName
402114	Invalid SPI received
402115	Unexpected protocol received
402116	Packet doesn't match identity
402117	Non-IPSEC packet received
402118	Invalid fragment offset
402119	Anti-Replay check failure
402120	Authentication failure（認証失敗）
402121	Packet dropped
426101	cLACP Port Bundle

EventID	EventName
426102	cLACP Port Standby
426103	cLACP Port Moved To Bundle From Standby
426104	cLACP Port Unbundled
602103	Path MTU updated
602104	Path MTU exceeded
602303	New SA created
602304	SA deleted
702305	SA expiration - Sequence rollover
702307	SA expiration - Data rollover

NAT Syslog イベント ID とイベント名

EventID	EventName
201002	Max connection Exceeded for host
201003	Embryonic limit exceed
201004	UDP connection limit exceed
201005	FTP connection failed
201006	RCMD connection failed
201008	New connection Disallowed
201009	Connection Limit exceed
201010	Embryonic Connection limit exceeded
201011	接続制限の超過
201012	Per-client embryonic connection limit exceeded
201013	Per-client connection limit exceeded
202001	Global NAT exhausted
202005	Embryonic connection error
202011	Connection limit exceeded
305005	No NAT group found
305006	Translation failed
305007	Connection dropped
305008	NAT allocation issue
305009	NAT Created
305010	NAT teardown

EventID	EventName
305011	PAT created
305012	PAT teardown
305013	Connection denied

SSL VPN Syslog イベント ID とイベント名

EventID	EventName
716001	WebVPN Session Started
716002	WebVPN Session Terminated
716003	WebVPN User URL access
716004	WebVPN User URL access denied
716005	WebVPN ACL error
716006	WebVPN User Disabled
716007	WebVPN Unable to Create
716008	WebVPN Debug
716009	WebVPN ACL error
716010	WebVPN User access network
716011	WebVPN User access
716012	WebVPN User Directory access
716013	WebVPN User file access
716014	WebVPN User file access
716015	WebVPN User file access
716016	WebVPN User file access
716017	WebVPN User file access
716018	WebVPN User file access
716019	WebVPN User file access
716020	WebVPN User file access
716021	WebVPN user access file denied
716022	WebVPN Unable to connect proxy
716023	WebVPN session limit reached
716024	WebVPN User access error
716025	WebVPN User access error
716026	WebVPN User access error
716027	WebVPN User access error

EventID	EventName
716028	WebVPN User access error
716029	WebVPN User access error
716030	WebVPN User access error
716031	WebVPN User access error
716032	WebVPN User access error
716033	WebVPN User access error
716034	WebVPN User access error
716035	WebVPN User access error
716036	WebVPN User login successful
716037	WebVPN User login failed
716038	WebVPN User Authentication Successful
716039	WebVPN User Authentication Rejected
716040	WebVPN User logging denied
716041	WebVPN ACL hit count
716042	WebVPN ACL hit
716043	WebVPN Port forwarding
716044	WebVPN Bad Parameter
716045	WebVPN Invalid Parameter
716046	WebVPN connection terminated
716047	WebVPN ACL usage
716048	WebVPN memory issue
716049	WebVPN Empty SVC ACL
716050	WebVPN ACL error
716051	WebVPN ACL error
716052	WebVPN Session Terminated
716053	WebVPN SSO Server added
716054	WebVPN SSO Server deleted
716055	WebVPN Authentication Successful
716056	WebVPN Authentication Failed
716057	WebVPN Session terminated
716058	WebVPN Session lost
716059	WebVPN Session resumed

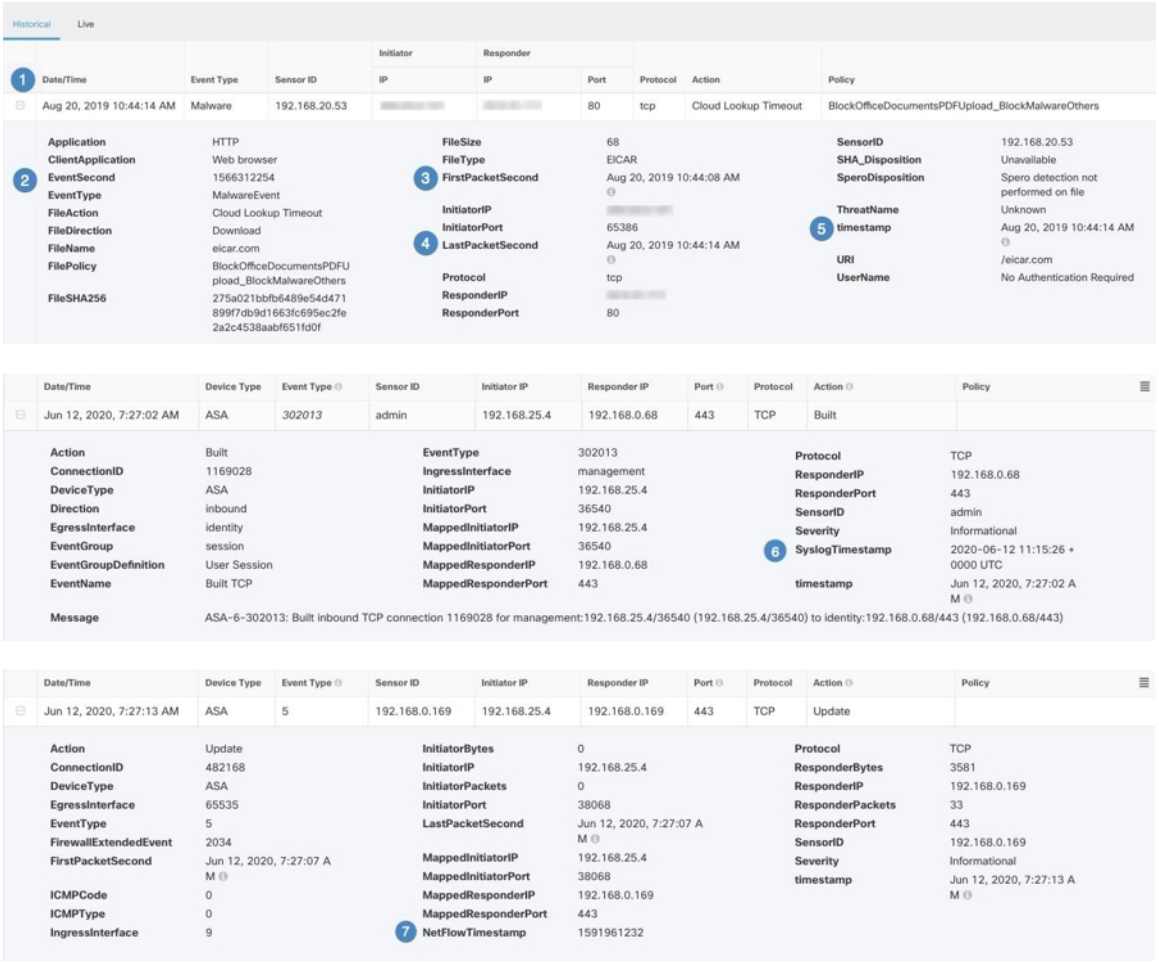
EventID	EventName
716060	WebVPN Session Terminated
722001	WebVPN SVC Connect request error
722002	WebVPN SVC Connect request error
722003	WebVPN SVC Connect request error
722004	WebVPN SVC Connect request error
722005	WebVPN SVC Connect update issue
722006	WebVPN SVC Invalid address
722007	WebVPN SVC Message
722008	WebVPN SVC Message
722009	WebVPN SVC Message
722010	WebVPN SVC Message
722011	WebVPN SVC Message
722012	WebVPN SVC Message
722013	WebVPN SVC Message
722014	WebVPN SVC Message
722015	WebVPN SVC invalid frame
722016	WebVPN SVC invalid frame
722017	WebVPN SVC invalid frame
722018	WebVPN SVC invalid frame
722019	WebVPN SVC Not Enough Data
722020	WebVPN SVC no address
722021	WebVPN Memory issue
722022	WebVPN SVC connection established
722023	WebVPN SVC connection terminated
722024	WebVPN Compression Enabled
722025	WebVPN Compression Disabled
722026	WebVPN Compression reset
722027	WebVPN Decompression reset
722028	WebVPN Connection Closed
722029	WebVPN SVC Session terminated
722030	WebVPN SVC Session terminated
722031	WebVPN SVC Session terminated

EventID	EventName
722032	WebVPN SVC connection Replacement
722033	WebVPN SVC Connection established
722034	WebVPN SVC New connection
722035	WebVPN Received Large packet
722036	WebVPN transmitting Large packet
722037	WebVPN SVC connection closed
722038	WebVPN SVC session terminated
722039	WebVPN SVC invalid ACL
722040	WebVPN SVC invalid ACL
722041	WebVPN SVC IPv6 not available
722042	WebVPN invalid protocol
722043	WebVPN DTLS disabled
722044	WebVPN unable to request address
722045	WebVPN Connection terminated
722046	WebVPN Session terminated
722047	WebVPN Tunnel terminated
722048	WebVPN Tunnel terminated
722049	WebVPN Session terminated
722050	WebVPN Session terminated
722051	WebVPN address assigned
722053	WebVPN Unknown client
723001	WebVPN Citrix connection Up
723002	WebVPN Citrix connection Down
723003	WebVPN Citrix no memory issue
723004	WebVPN Citrix bad flow control
723005	WebVPN Citrix no channel
723006	WebVPN Citrix SOCKS error
723007	WebVPN Citrix connection list broken
723008	WebVPN Citrix invalid SOCKS
723009	WebVPN Citrix invalid connection
723010	WebVPN Citrix invalid connection
723011	WebVPN citrix Bad SOCKS

EventID	EventName
723012	WebVPN Citrix Bad SOCKS
723013	WebVPN Citrix invalid connection
723014	WebVPN Citrix connected to Server
724001	WebVPN Session not allowed
724002	WebVPN Session terminated
724003	WebVPN CSD
724004	WebVPN CSD
725001	SSL handshake Started
725002	SSL Handshake completed
725003	SSL Client session resume
725004	SSL Client request Authentication
725005	SSL Server request authentication
725006	SSL Handshake failed
725007	SSL Session terminated
725008	SSL Client Cipher
725009	SSL Server Cipher
725010	SSL Cipher
725011	SSL Device choose Cipher
725012	SSL Device choose Cipher
725013	SSL Server choose cipher
725014	SSL LIB error
725015	SSL client certificate failed

Syslog イベントの時間属性

[イベントロギング]ページのさまざまなタイムスタンプの目的を理解すると、関心のあるイベントをフィルタリングして見つけるのに役立ちます。



番号	ラベル	説明
1	日時	Secure Event Connector（SEC）がイベントを処理した時刻。これは、ファイアウォールでそのトラフィックが検査された時刻と同じではない場合があります。タイムスタンプと同じ値。
2	EventSecond	LastPacketSecond と同じです。

番号	ラベル	説明
3	FirstPacketSecond	接続が開かれた時刻。この時点で、ファイアウォールはパケットを検査します。 FirstPacketSecond の値は、LastPacketSecond から ConnectionDuration を差し引いて計算されます。 接続の開始時にログに記録される接続イベントの場合、FirstPacketSecond、LastPacketSecond、および EventSecond の値はすべて同じになります。
4	LastPacketSecond	接続が閉じた時刻。接続の最後に記録される接続イベントの場合、LastPacketSecond と EventSecond は等しくなります。
5	timestamp	Secure Event Connector（SEC）がイベントを処理した時刻。これは、ファイアウォールでそのトラフィックが検査された時刻と同じではない場合があります。[日時（Date/Time）] と同じ値。
[6]	syslog タイムスタンプ	「ロギングタイムスタンプ」が使用されている場合、syslog の開始時刻を表します。syslog にこの情報がない場合、SEC がイベントを受信した時刻が反映されます。
7	NetflowTimeStamp	ASA で、NetFlow パケットを埋めてフローコレクタに送信するのに十分なフローレコード/イベントの収集が終了した時刻。

Cisco Secure Cloud Analytics とダイナミック エンティティ モデリング

必要なライセンス：Logging Analytics and Detection または **Total Network Analytics and Monitoring**

Secure Cloud Analytics は、オンプレミスおよびクラウドベースのネットワーク展開をモニターする Software as a Service（SaaS）ソリューションです。ファイアウォールイベントとネットワークフローデータを含め、ネットワークトラフィックに関する情報をソースから収集することによって、トラフィックに関する観測内容が作成され、トラフィックパターンに基づいてネットワークエンティティのロールが自動的に識別されます。Secure Cloud Analytics は、この情報を他の脅威インテリジェンス（Talos など）のソースと組み合わせて使用してアラートを生成します。このアラートは、本質的に悪意のある可能性がある動作の存在を示す警告を構成します。Secure Cloud Analytics は、このアラートとともに、ネットワークおよびホストの可視性と、収集したコンテキスト情報を提供します。このコンテキスト情報により、アラートを調査して悪意のある動作の原因を特定するためのより優れた基盤が得られます。

ダイナミック エンティティ モデリング

ダイナミック エンティティ モデリングは、ファイアウォールイベントとネットワークフローデータの動作分析を実行することにより、ネットワークの状態を追跡します。Secure Cloud Analytics のコンテキストにおいて、エンティティとは、ネットワーク上のホストやエンドポイントといった、何らかの経時的に追跡できるものです。ダイナミック エンティティ モデリングは、ネットワークで送信されるトラフィックと実行されるアクティビティに基づいて、エンティティに関する情報を収集します。**Logging Analytics and Detection** ライセンスと統合された Secure Cloud Analytics は、エンティティが通常送信するトラフィックのタイプを判別するために、ファイアウォールイベントやその他のトラフィック情報から引き出すことができます。**Total Network Analytics and Monitoring** ライセンスを購入すると、Secure Cloud Analytics は、エンティティトラフィックのモデル化に NetFlow およびその他のトラフィック情報を含めることもできます。各エンティティの最新のモデルを維持するため、Secure Cloud Analytics では、エンティティがトラフィックを送信し続け、場合によっては異なるトラフィックを送信する可能性があるため、これらのモデルを徐々に更新します。この情報から、Secure Cloud Analytics は以下を識別します。

- エンティティのロール：これは、エンティティが通常行うことの記述子です。たとえば、エンティティが、一般に電子メールサーバーに関連付けられるトラフィックを送信する場合、Secure Cloud Analytics は、そのエンティティに電子メールサーバーロールを割り当てます。エンティティは複数のロールを実行する場合があるため、ロールとエンティティの関係は多対 1 である可能性があります。
- エンティティの観測内容：これは、ネットワーク上でのエンティティの動作に関する事実（外部 IP アドレスとのハートビート接続、別のエンティティとの間で確立されたリモートアクセスセッションなど）です。CDO と統合すると、ファイアウォールイベントからこれらの事実を取得できます。**Total Network Analytics and Monitoring** ライセンスも購入すると、システムは NetFlow から事実を取得し、ファイアウォールイベントと NetFlow の両方から観測内容を生成することもできます。観測内容それ自体は、それらが表すものの事実を超えた意味を持ちません。一般的なお客様は、何千もの観測内容と少数のアラートを持つ可能性があります。

アラートと分析

ロール、観測内容、およびその他の脅威インテリジェンスの組み合わせに基づいてSecure Cloud Analyticsが生成するアラートは、潜在的な悪意のある動作をシステムによって識別されたものとして表す実用的な項目です。1 つのアラートが複数の観測内容を表す場合があることに注意してください。ファイアウォールが同じ接続とエンティティに関連する複数の接続イベントをログに記録する場合、アラートが 1 つだけになる可能性があります。

上記の例で言えば、新しい内部デバイスの観測内容だけでは、潜在的な悪意のある動作は構成されません。ただし、時間の経過とともに、エンティティがドメイン コントローラと一致するトラフィックを送信する場合、システムではそのエンティティにドメイン コントローラ ロールが割り当てられます。その後、そのエンティティが、以前に接続を確立していない外部サーバーへの接続を確立し、異常なポートを使用して大量のデータを転送すると、システムは、[新しい大規模接続（外部）（New Large Connection (External)）] 観測内容と [例外ドメインコントローラ（Exceptional Domain Controller）] 観測内容をログに記録します。その外部サーバーがTalos ウォッチリストに登録されているものと識別された場合、これらすべての情報の組み合わせによりSecure Cloud Analyticsはこのエンティティの動作に関するアラートを生成し、悪意のある動作を調査して対処するように促します。

Secure Cloud Analytics の Web ポータル UI でアラートを開くと、システムがアラートを生成した原因となっている観測内容を確認できます。これらの観測内容から、関連するエンティティに関する追加のコンテキスト（それらが送信したトラフィック、外部脅威インテリジェンス（利用可能な場合）など）も確認できます。また、エンティティが関係性を持っていたその他の観測内容やアラートを確認したり、この動作が他の潜在的に悪意のある動作に結び付いているかどうかを判断することもできます。

Secure Cloud Analytics でアラートを表示して閉じる場合、Secure Cloud Analytics UI からのトラフィックを許可またはブロックできないことに注意してください。デバイスをアクティブモードで展開した場合、ファイアウォール アクセス コントロール ルールを、トラフィックを許可またはブロックするように更新する必要があり、ファイアウォールがパッシブモードで展開されている場合は、ファイアウォールアクセスコントロールルールを更新する必要があります。

ファイアウォールイベントに基づくアラートの使用

必要なライセンス：Logging Analytics and Detection または **Total Network Analytics and Monitoring**

アラートのワークフロー

アラートのワークフローは、そのステータスに基づいて異なります。システムによってアラートが生成される場合、そのデフォルト ステータスは [オープン（Open）] であり、ユーザーは割り当てられません。アラートのサマリーを表示すると、デフォルトでは、当面注意が必要なすべてのオープン アラートが表示されます。

注：**Total Network Analytics and Monitoring** ライセンスを持っている場合、アラートは、NetFlow から生成された観測結果、ファイアウォールイベントから生成された観測結果、または両方のデータソースからの観測結果に基づいて生成できます。

アラートのサマリーを確認する際は、初期トリアージとして、アラートにステータスを割り当て、タグ付けし、更新することができます。フィルタ機能と検索機能を使用して、特定のアラートを検索したり、さまざまなステータスのアラートを表示したり、さまざまなタグや割り当て対象を関連付けたりすることができます。アラートのステータスは[スヌーズ（Snoozed）]に設定できます。この場合、そのアラートはスヌーズ期間が経過するまでオープンアラートのリストに表示されません。アラートから [スヌーズ（Snoozed）] ステータスを削除して、再びオープンアラートとして表示されるようにすることもできます。アラートを確認する際は、それらのアラートをそのユーザー自身またはシステム内の別のユーザーに割り当てることができます。ユーザーは、自分のユーザー名に割り当てられているすべてのアラートを検索できます。

アラートのサマリーから、アラートの詳細ページを表示できます。このページでは、このアラートを生成させた、裏付けとなる観測内容に関する追加のコンテキストと、このアラートに関連するエンティティに関する追加のコンテキストを確認できます。この情報は、ネットワーク上の問題をさらに調査して悪意のある動作を潜在的に解決するために実際の問題を特定する上で役立ちます。

CDO の Stealthwatch Cloud Web ポータル UI 内やネットワーク上で調査しているときに、発見した内容を説明するコメントをアラートと一緒に残すことができます。これは、将来参照できる調査の記録を作成するために役立ちます。

分析が完了したら、ステータスを[クローズ（Closed）]に更新できます。これにより、デフォルトではオープンアラートとして表示されなくなります。将来、状況が変わった場合は、クローズ アラートのステータスを再度オープンにすることもできます。

ここでは、特定のアラートを調査する方法に関する一般的なガイドラインと推奨事項を示します。Stealthwatch Cloud はアラートをログに記録するときに追加のコンテキストを提供するため、このコンテキストを参照しながら調査を進めることができます。

これらの手順は、総合的または包括的であることを意図したものではありません。これらは単にアラートの調査を開始するための一般的な枠組みを提供するためのものです。

一般に、次の手順でアラートを確認できます。

1. オープンアラートのトリアージ （425 ページ）
2. 後で分析するためにアラートをスヌーズする （426 ページ）
3. 詳細な調査のためのアラートの更新 （427 ページ）
4. アラートの確認と調査の開始 （427 ページ）
5. エンティティとユーザーの調査 （429 ページ）
6. Secure Cloud Analytics を使用して問題を修復する （430 ページ）
7. アラートの更新とクローズ （431 ページ）

オープンアラートのトリアージ

特に複数の調査が必要な場合は、オープンアラートのトリアージを行います。

- CDO から SWC へのクロス起動とアラート表示の詳細については、「Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示」を参照してください。

次の質問に答えてください。

- このアラート タイプを優先度の高いものとして設定しましたか。
- 影響を受けるサブネットに高い機密性を設定しましたか。
- この異常な動作はネットワーク上の新しいエンティティによるものですか。
- エンティティの通常のロールは何ですか。また、このアラートの動作はそのロールにどのように適合しますか。
- これは、このエンティティの通常の動作からの例外的な逸脱ですか。
- ユーザーが関与している場合、これはユーザーの予想される動作ですか、それとも例外的な動作ですか。
- 保護されたデータや機密データが侵害を受けるリスクがありますか。
- この動作の継続を許可すると、ネットワークへの影響はどの程度深刻になりますか。
- 外部エンティティとの通信がある場合、それらのエンティティは過去にネットワーク上の他のエンティティとの接続を確立しましたか。

これが優先順位の高いアラートである場合は、調査を進める前に、インターネットからエンティティを隔離するか、隔離しないときは接続を切断することを検討してください。

後で分析するためにアラートをスヌーズする

他のアラートと比較して優先度が低いときに、アラートをスヌーズします。たとえば、組織が電子メールサーバーをFTPサーバーとして再利用する場合、緊急プロファイルアラートが生成されます（エンティティの現在のトラフィックが、以前には一致しなかった動作プロファイルと一致することを示します）。これは想定される動作であるため、このアラートをスヌーズして、後日再検討できます。スヌーズされたアラートは、オープンアラートと一緒に表示されません。これらのスヌーズされたアラートを確認するには、特別にフィルタリングする必要があります。

アラートをスヌーズする：

ステップ 1 [アラートを閉じる（Close Alert）] をクリックします。
ステップ 2 [このアラートをスヌーズ（Snooze this alert）] ペインで、ドロップダウンからスヌーズ期間を選択します。
ステップ 3 [保存（**Save**）] をクリックします。

次のタスク

スヌーズしたアラートを確認する準備ができたら、アラートのスヌーズを解除できます。これにより、ステータスが[オープン（Open）]に設定され、他のオープンアラートとともにアラートが表示されます。

スヌーズしたアラートのスヌーズを解除する：

- スヌーズしたアラートから、[アラートのスヌーズ解除（Unsnooze Alert）]をクリックします。

詳細な調査のためのアラートの更新

アラートの詳細情報を確認します。

ステップ 1 **[モニター（Monitor）]** > **[アラート（Alerts）]** を選択します。

ステップ 2 アラートタイプ名をクリックします。

次のタスク

初期トリアージと優先順位付けに基づいて、アラートを割り当て、タグを付けます。

1. [担当者（Assignee）] ドロップダウンからユーザーを選択してアラートを割り当てます。これにより、ユーザーが調査を開始できるようになります。
2. [タグ（Tags）] ドロップダウンから 1 つ以上のタグを選択して、アラートにタグを追加することにより、将来の識別のためにアラートをより適切に分類したり、アラートの長期的なパターンの確立を試みることができます。
3. 必要に応じて、**このアラートに関するコメント**を入力し、[コメント（Comment）]をクリックすることにより、最初の調査結果を追跡するためのコメントを残し、アラートに割り当てられた担当者を支援することができます。アラートは、システムコメントとユーザーコメントの両方を追跡します。

アラートの確認と調査の開始

割り当てられたアラートを確認する場合は、アラートの詳細を確認して、Stealthwatch Cloud がアラートを生成した理由を把握してください。裏付けとなる観測内容を確認し、これらの観測内容がソースエンティティに対して持つ意味を理解します。

アラートがファイアウォールイベントに基づいて生成された場合、ファイアウォールの展開がこのアラートのソースであることはシステムに認識されません。

このソースエンティティの一般的な動作やパターンを理解するために、サポートされている観測内容をすべて表示し、このアクティビティがより長いトレンドの一部である可能性があるかどうかを確認します。

手順の概要

1. アラートの詳細で、観測タイプの横にある矢印アイコン（）をクリックして、そのタイプの記録されたすべての観測内容を表示します。
2. [ネットワークのすべての観測内容（All Observations for Network）] の横にある矢印アイコン（）をクリックして、このアラートのソースエンティティの記録された観測内容をすべて表示します。

手順の詳細

ステップ 1 アラートの詳細で、観測タイプの横にある矢印アイコン（）をクリックして、そのタイプの記録されたすべての観測内容を表示します。

ステップ 2 [ネットワークのすべての観測内容（All Observations for Network）] の横にある矢印アイコン（）をクリックして、このアラートのソースエンティティの記録された観測内容をすべて表示します。

観測内容に対して追加の分析を実行する場合は、サポートされている観測内容をコンマ区切り値ファイルでダウンロードします。

- アラートの詳細の [サポートされている観測内容（Supporting Observations）] ペインで、[CSV] をクリックします。

観測内容から、ソースエンティティの動作が悪意のある動作を示しているか判断します。ソースエンティティが複数の外部エンティティとの接続を確立している場合は、それらのエンティティが何らかの関連性を持つかどうか（それらのすべてが類似の地理位置情報を持っているか、それらの IP アドレスが同じサブネットからのものであるかなど）を確認します。

ソースエンティティの IP アドレスまたはホスト名から、ソースエンティティに関連する追加コンテキスト（関与している可能性がある他のアラートや観測内容、デバイス自体に関する情報、送信しているセッショントラフィックのタイプなど）を表示します。

- エンティティに関連するすべてのアラートを表示するには、IPアドレスまたはホスト名のドロップダウンから [アラート（Alerts）] を選択します。
- エンティティに関連するすべての観測内容を表示するには、IPアドレスまたはホスト名のドロップダウンから [観測内容（Observations）] を選択します。
- デバイスに関する情報を表示するには、IPアドレスまたはホスト名のドロップダウンから [デバイス] を選択します。
- このエンティティに関連するセッショントラフィックを表示するには、IPアドレスまたはホスト名のドロップダウンから [セッショントラフィック（Session Traffic）] を選択します。
- IP アドレスまたはホスト名をコピーするには、IP アドレスまたはホスト名のドロップダウンから [コピー] を選択します。

Stealthwatch Cloud のソースエンティティは常にネットワークの内部にあることに注意してください。この点を、接続を開始したエンティティを示し、ネットワークの内部または外部にある可能性がある、ファイアウォールイベントのイニシエータ IP と比較してください。

観測内容から、他の外部エンティティに関する情報を調べます。地理位置情報を調査し、いずれかの地理位置情報データまたは Umbrella データによって悪意のあるエンティティが特定されるかどうかを確認します。これらのエンティティによって生成されたトラフィックを表示します。Talos、AbuseIPDB、または Google にこれらのエンティティに関する情報があるかどうかを確認します。複数の日にわたる IP アドレスを見つけて、外部エンティティがネットワーク上のエンティティと確立した他のタイプの接続を確認します。必要に応じて、それらの内部エンティティを見つけ、侵害または意図しない動作の証拠があるかどうかを判断します。

ソースエンティティが接続を確立した外部エンティティの IP アドレスまたはホスト名のコンテキストを確認します。

- このエンティティの最近のトラフィック情報を表示するには、IPアドレスまたはホスト名のドロップダウンから [IPトラフィック（IP Traffic）] を選択します。
- このエンティティの最近のセッショントラフィック情報を表示するには、IPアドレスまたはホスト名のドロップダウンから [セッショントラフィック（Session Traffic）] を選択します。
- AbuseIPDB の Web サイト上でこのエンティティに関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから [AbuseIPDB] を選択します。
- Cisco Umbrella の Web サイト上でこのエンティティに関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから [Cisco Umbrella] を選択します。
- Google でこの IP アドレスを検索するには、IP アドレスまたはホスト名のドロップダウンから [Google検索（Google Search）] を選択します。
- Talos の Web サイト上でこの情報に関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから [Talos Intelligence] を選択します。
- このエンティティをウォッチリストに追加するには、IPアドレスまたはホスト名のドロップダウンから [IPをウォッチリストに追加（Add IP to watchlist）] を選択します。
- 前月のこのエンティティのトラフィックを検索するには、IPアドレスまたはホスト名のドロップダウンから [複数日のIPを検索（Find IP on multiple days）] を選択します。
- IP アドレスまたはホスト名をコピーするには、IP アドレスまたはホスト名のドロップダウンから [コピー（Copy）] を選択します。

Stealthwatch Cloud の接続エンティティは、常にネットワークの外部にあることに注意してください。この点を、接続要求に応答したエンティティを示し、ネットワークの内部または外部にある可能性がある、ファイアウォールイベントのレスポンダ IP と比較してください。

調査結果に関するコメントを残します。

- [アラートの詳細（ alert detail）] で、[このアラートに関するコメント（Comment on this alert）] を入力し、[コメント（Comment）] をクリックします。

エンティティとユーザーの調査

Stealthwatch Cloud ポータル UI でアラートを確認した後、ソースエンティティ、このアラートに関係している可能性のあるユーザー、およびその他の関連エンティティに対して、追加の調査を直接実行できます。

- ソースエンティティがネットワーク上のどこ（物理的またはクラウド上）にあるかを特定し、直接アクセスします。このエンティティのログファイルを見つけます。それがネットワーク上の物理エンティティである場合は、デバイスにアクセスしてログ情報を確認し、この動作の原因となっているものに関する情報があるかどうかを確認します。それが仮想エンティティである場合またはクラウドに保存されている場合は、ログにアクセスして、このエンティティに関連するエントリを検索します。不正なログイン、承認されていない設定変更などに関する詳細について、ログを調査します。
- エンティティを調査します。マルウェアまたはエンティティ自体にある脆弱性を特定できるかどうかを判断してください。デバイスの物理的な変更（組織によって承認されていない USB スティックなど）を含め、何らかの悪意のある変更があったかどうかを確認します。
- ネットワーク上のユーザーまたはネットワーク外のユーザーによる関与があったかどうかを確認します。可能であれば、何をしていたのかをユーザーに尋ねてください。ユーザーに尋ねることができない場合は、そのユーザーがアクセス権を持っていたと考えられるかどうかと、この動作を促す状況（解雇された従業員が退社する前に外部サーバーにファイルをアップロードするなど）が発生したかどうかを確認します。

調査結果に関するコメントを残します。

- [アラートの詳細（ alert detail）] で、[このアラートに関するコメント（Comment on this alert）] を入力し、[コメント（Comment）] をクリックします。

アラートの更新とクローズ

調査結果に基づいてタグを追加します。

ステップ 1 Secure Cloud Analytics ポータルの UI で、**[監視]** > **[アラート]**を選択します。

ステップ 2 ドロップダウンから 1 つ以上の**タグ**を選択します。

調査結果と実行された修正手順を説明する最終コメントを追加します。

- アラートの詳細で、[このアラートに関するコメント] を入力し、[コメント] をクリックします。

アラートのステータスをクローズにして、役立つものかどうかが分かるようにマークします。

1. アラートの詳細から、[アラートを閉じる] をクリックします。

2. アラートが役立った場合は[はい]を、アラートが役立たなかった場合は[いいえ]を選択します。これはアラートが悪意のある動作に起因するかどうかではなく、単にアラートが組織にとって有用であったかどうかを意味する点に注意してください。
3. [保存（**Save**）]をクリックします。

次のタスク

クローズしたアラートの再オープン

クローズしたアラートに関連する追加情報を検出した場合、またはそのアラートに関連するコメントを追加する場合は、そのアラートを再度開いてステータスを[オープン（Open）]に変更できます。その後、必要に応じてアラートを変更し、追加調査が完了したら再度閉じます。

クローズしたアラートを再オープンします。

- クローズしたアラートの詳細から、[アラートを再オープン]をクリックします。

アラートの優先順位を変更する

必要なライセンス：**Logging Analytics and Detection** または **Total Network Analytics and Monitoring**

アラートタイプにはデフォルトの優先順位が設定されています。これは、このタイプのアラートを生成するシステムの機密性に影響します。アラートの優先順位は、シスコのインテリジェンスおよびその他の要因に基づいて、[低]または[通常]にデフォルト設定されます。ネットワーク環境に基づいて、関心のある特定のアラートを強調するために、アラートタイプの優先順位を変更することができます。アラートタイプの優先順位は、[低]、[通常]、または[高]に設定できます。

- **[モニター]** > **[アラート]** を選択します。
- 設定のドロップダウンアイコン（）をクリックし、[アラートのタイプと優先順位]を選択します。
- アラートタイプの横にある編集のアイコン（）をクリックし、[低]、[中]、または[高]を選択して優先順位を変更します。

イベントロギングページでのイベントの検索とフィルタリング

特定のイベントの履歴イベントテーブルとライブイベントテーブルの検索とフィルタ処理は、CDOで他の情報を検索してフィルタ処理する場合と同様に機能します。フィルタ条件を追加すると、CDOは[イベント（Events）]ページに表示される内容を制限し始めます。検索フィールドに検索条件を入力して、特定の値を持つイベントを検索することもできます。フィルタリ

ングと検索のメカニズムを組み合わせると、検索はイベントのフィルタリング後に表示される結果の中から、入力した値を見つけようとします。

ライブイベントのフィルタリングは、履歴イベントの場合と同じように機能しますが、ライブイベントは時刻でフィルタリングできない点が異なります。

次のフィルタリング方法について説明します。

- ライブまたは履歴イベントのフィルタ処理 （476 ページ）
- NetFlow イベントのみフィルタ処理 （478 ページ）
- ASA または FTD Syslog イベントをフィルタリングするが、ASA NetFlow イベントはフィルタリングしない （478 ページ）
- フィルタ要素の結合 （479 ページ）

ライブまたは履歴イベントのフィルタ処理

この手順では、イベントフィルタリングを使用して、[イベントロギング]ページでイベントのサブセットを表示する方法について説明します。特定のフィルタ条件を繰り返し使用する場合は、カスタマイズしたフィルタを作成して保存できます。詳細については、「カスタマイズ可能なイベントフィルタ」を参照してください。

ステップ 1 ナビゲーションバーで、**[モニタリング（Monitoring）] > [イベントロギング]** をクリックします。

ステップ 2 [履歴] タブまたは [ライブ] タブをクリックします。

ステップ 3 フィルタボタン をクリックします。フィルタリング列は、ピンアイコン をクリックして開いた状態でピン留めできます。

ステップ 4 保存されているフィルタ要素がない [表示（View）] タブをクリックします。

ステップ 5 フィルタリングするイベントの詳細を選択します。

- **FTD イベントタイプ**
  - 接続：アクセス制御ルールからの接続イベントを表示します。
  - ファイル：アクセス制御ルールのファイルポリシーによって報告されたイベントを表示します。
  - 侵入：アクセス制御ルールの侵入ポリシーによって報告されたイベントを表示します。
  - マルウェア：アクセス制御ルールのマルウェアポリシーによって報告されたイベントを表示します。
- ASA **イベントタイプ**：これらのイベントタイプは、syslog または NetFlow イベントのグループを表します。syslog ID または NetFlow ID が含まれているグループの詳細については、「ASA イベント タイプ」を参照してください。

- 解析されたイベント：解析された syslog イベントには、他の syslog イベントよりも多くのイベント属性が含まれており、CDO はそれらの属性に基づいて検索結果をより迅速に返すことができます。解析済みの ASA Syslog イベント （374 ページ）解析されたイベントはフィルタリングカテゴリではありませんが、解析されたイベント ID は、[イベントタイプ（Event Types）] 列に斜体で表示されます。斜体で表示されていないイベント ID は解析されていません。

- **時間範囲**：[開始時刻（Start time）] または [終了時刻（End time）] フィールドをクリックして、表示する期間の開始時刻と終了時刻を選択します。タイムスタンプは、コンピュータのローカル時間で表示されます。
- **アクション**：ルールによって定義されたセキュリティアクションを指定します。入力する値は、検索対象と完全に一致する必要がありますが、大文字小文字は関係ありません。各イベントタイプ（接続、ファイル、侵入、マルウェア、syslog、および NetFlow）に異なる値を入力します。
  - 接続イベントタイプの場合、フィルタは AC_RuleAction 属性で一致を検索します。それらの値は、Allow、Block、Trust の可能性があります。
  - ファイルイベントタイプの場合、フィルタは FileAction 属性で一致を検索します。それらの値は、Allow、Block、Trust の可能性があります。
  - 侵入イベントタイプの場合、フィルタは InLineResult 属性で一致を検索します。それらの値は、Allowed、Blocked、Trusted の可能性があります。
  - マルウェアイベントタイプの場合、フィルタは FileAction 属性で一致を検索します。それらの値は、クラウド ルックアップ タイムアウトである可能性があります。
  - syslog および NetFlow イベントタイプの場合、フィルタは Action 属性で一致を検索します。
- **センサー ID**：センサー ID は、イベントが Secure Event Connector に送信される管理 IP アドレスです。Firepower Threat Defense（FTD）デバイスの場合、センサー ID は通常、デバイスの管理インターフェイスの IP アドレスです。
- **IP アドレス**
  - **イニシエータ**：ネットワークトラフィックの送信元の IP アドレスです。イニシエータ アドレス フィールドの値は、イベントの詳細の InitiatorIP フィールドの値に対応します。10.10.10.100 などの単一のアドレス、または 10.10.10.0/24 などの CIDR 表記で定義されたネットワークを入力できます。
  - **レスポンダ**：パケットの宛先 IP アドレスです。宛先アドレスフィールドの値は、イベントの詳細の ResponderIP フィールドの値に対応します。10.10.10.100 などの単一のアドレス、または 10.10.10.0/24 などの CIDR 表記で定義されたネットワークを入力できます。
- **ポート**
  - **イニシエータ**：セッションイニシエータが使用するポートまたは ICMP タイプ。送信元ポートの値は、イベントの詳細の InitiatorPort の値に対応します（範囲の追加：開始ポートと終了ポートと、イニシエータとレスポンダの間または両方のスペース）。

- **レスポンダ**：セッションレスポンダが使用するポートまたは ICMP コード。宛先ポートの値は、イベントの詳細の ResponderPort の値に対応します

- **NetFlow**：ASA デバイス向け NetFlow Secure Event Logging（NSEL） イベントは、syslog イベントとは異なります。NetFlow フィルタは、NSEL レコードになったすべての NetFlow イベント ID を検索します。これらの「NetFlow イベント ID」は、Cisco ASA NetFlow 実装ガイド [英語] で定義されています。

ステップ 6 （任意）[表示（View）] タブの側をクリックして、フィルタをカスタムフィルタとして保存します。

ステップ 7 （任意）さらに分析するために、イベントを .CSV.GZ ファイルにダウンロードできます。「イベントのダウンロード」を参照してください。

NetFlow イベントのみフィルタ処理

この手順では、ASA NetFlow イベントのみを検索します。

ステップ 1 CDO メニューバーから、**[モニターリング（Monitoring）]** > **[イベントロギング]** を選択します。.

ステップ 2 フィルタアイコン をクリックして、開いた状態でフィルタをピン留めします。

ステップ 3 [Netflow] ASA イベントフィルタをオンにします。

ステップ 4 他のすべての ASA イベントフィルタをオフにします。

[イベントロギング] テーブルには、ASA NetFlow イベントのみが表示されます。

ASA または FTD Syslog イベントをフィルタリングするが、ASA NetFlow イベントはフィルタリングしない

この手順では、syslog イベントのみを検索します。

ステップ 1 CDO メニューバーから、**[モニタリング（Monitoring）]** > **[イベントロギング]** を選択します。

ステップ 2 フィルタアイコン をクリックして、開いた状態でフィルタをピン留めします。

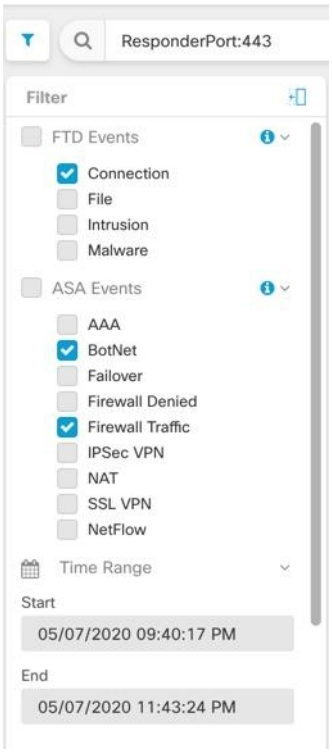
ステップ 3 フィルタバーの一番下までスクロールし、[NetFlowイベントを含める（Include NetFlow Events）] フィルタが**オフ**になっていることを確認します。

ステップ 4 [ASAイベント（ASA Events）] フィルタツリーまでスクロールして戻り、[NetFlow] ボックスが**オフ**になっていることを確認します。

ステップ 5 ASA または FTD フィルタ条件の残りを選択します。

フィルタ要素の結合

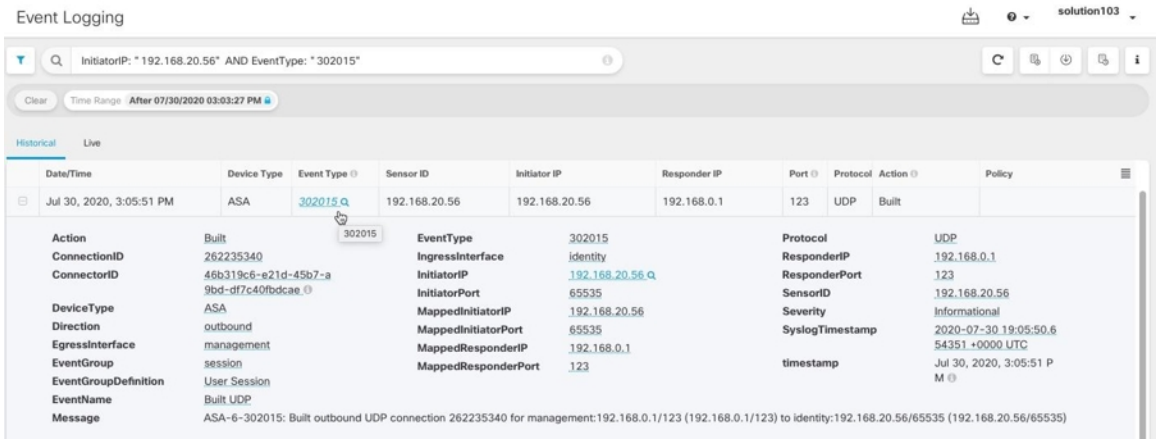
イベントのフィルタリングは、通常、CDO の標準フィルタリングルールに従います。フィルタリングカテゴリには「AND」が適用され、カテゴリ内の値は「OR」が適用されます。フィルタ処理をユーザー独自の検索条件と組み合わせることもできます。ただし、イベントフィルタの場合は、デバイスイベントフィルタにも「OR」が適用されます。たとえば、フィルタで次の値が選択されているとします。



このフィルタを使用すると、CDO では、FTD の接続イベント **OR** ASA ボットネットイベント **OR** ファイアウォール トラフィック イベント、**AND** 時間範囲内の 2 つの時間の間に発生したイベント **AND** ResponderPort 443 も含むイベントが表示されます。時間範囲内の履歴イベントでフィルタ処理できます。ライブイベントページには常に最新のイベントが表示されます。

特定の属性：値ペアの検索

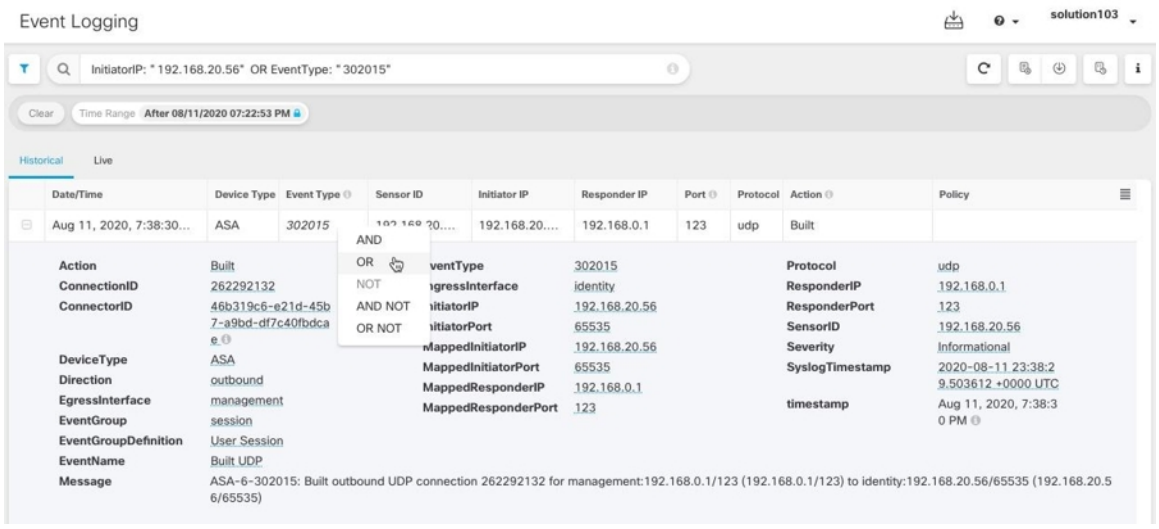
検索フィールドにイベント属性と値を入力することで、ライブイベントや過去のイベントを検索できます。これを行う最も簡単な方法は、イベントロギングテーブルで、検索する属性をクリックすることです。CDO により、その属性が検索フィールドに入力されます。クリックできるイベントは、マウスカーソルを合わせると青色になります。次に例を示します。



この例では、イニシエータ IP の値である 192.168.20.56 にマウスカーソルを合わせてクリックすることにより、検索が開始されています。イニシエータ IP とその値が検索文字列に追加されています。次に、イベントタイプの値である 302015 にマウスカーソルを合わせてクリックし、検索文字列に追加されています。このとき、CDO によって AND が追加されています。そのため、この検索の結果は、192.168.20.56 から開始されたイベント AND イベントタイプが 302015 のイベントのリストになります。

上の例で、値 302015 の横にある虫眼鏡に注目してください。この虫眼鏡にマウスカーソルを合わせ、AND、OR、AND NOT、OR NOT 演算子を選択して、検索に追加する値とともに指定することもできます。次の例では「OR」が選択されています。この検索の結果は、192.168.20.56 から開始されたイベント OR イベントタイプが 302015 のイベントのリストになります。

検索フィールドが空のときにテーブルの値を右クリックした場合は、他の値がないため、「NOT」しか使用できないことに注意してください。



マウスカーソルを合わせると青色で強調表示される値は、検索文字列に追加できます。

AND、OR、NOT、AND NOT、OR NOT フィルタ処理演算子

検索文字列で使用される「AND」、「OR」、「NOT」、「AND NOT」、および「OR NOT」の動作は次のとおりです。

AND

すべての属性を含むイベントを検索するには、フィルタ文字列で AND 演算子を使用します。AND 演算子は、検索文字列の先頭では使用できません。

たとえば、次の検索文字列では、TCP プロトコルを含んだ、「かつ」イニシエータ IP アドレス（InitiatorIP）10.10.10.43 から開始された、「かつ」イニシエータポート（InitiatorPort）59614 から送信されたイベントが検索されます。AND ステートメントを追加するたびに、基準を満たすイベントの数が少なくなることが予期されます。

```
Protocol: "tcp" AND InitiatorIP: "10.10.10.43" AND InitiatorPort: "59614"
```

OR

いずれかの属性を含むイベントを検索するには、フィルタ文字列で OR 演算子を使用します。OR 演算子は、検索文字列の先頭では使用できません。

たとえば、次の検索文字列では、TCP プロトコルを含んだ、「または」イニシエータ IP アドレス（InitiatorIP）10.10.10.43 から開始された、「または」イニシエータポート（InitiatorPort）59614 から送信されたイベントがイベントビューアに表示されます。OR ステートメントを追加するたびに、基準を満たすイベントの数が多くなることが予期されます。

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR InitiatorPort: "59614"
```

NOT

特定の属性を持つイベントを除外するには、検索文字列の先頭でのみ、これを使用します。たとえば、次の検索文字列では、InitiatorIP が 192.168.25.3 のイベントが結果から除外されます。

```
 NOT InitiatorIP: "192.168.25.3"
```

AND NOT

特定の属性を含むイベントを除外するには、フィルタ文字列で AND NOT 演算子を使用します。AND NOT 演算子は、検索文字列の先頭では使用できません。

たとえば、次のフィルタ文字列では、イニシエータ IP アドレス（InitiatorIP）が 192.168.25.3 のイベントが表示されますが、それらのうち、レスポンダ IP アドレス（ResponderIP）が 10.10.10.1 のものは表示されません。

```
 InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

NOT と AND NOT を組み合わせて、複数の属性を除外することもできます。たとえば、次のフィルタ文字列では、InitiatorIP が 192.168.25.3 のイベントと ResponderIP が 10.10.10.1 のイベントが除外されます。

```
NOT InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

OR NOT

特定の要素を除外する検索結果を含めるには、フィルタ文字列で OR NOT 演算子を使用します。OR NOT 演算子は、検索文字列の先頭では使用できません。

たとえば、次の検索文字列では、プロトコル（Protocol）が TCP のイベント、「または」InitiatorIP が 10.10.10.43 のイベント、「または」InitiatorPort が 59614 ではないイベントが検索されます。

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR NOT InitiatorPort: "59614"
```

これは、(Protocol: "tcp") OR (InitiatorIP: "10.10.10.43") OR (NOT InitiatorPort: "59614") の検索と考えることもできます。

ワイルドカード検索

アスタリスク（*）を「属性：値」ペア検索の「値」フィールドでワイルドカードとして使用して、イベント内の結果を検索することができます。たとえば、次のフィルタ文字列では、

```
URL:*feedback*
```

属性フィールドが「URL」のイベントの文字列が検索され、「feedback」という文字列が含まれているイベントが表示されます。

関連情報：

- イベントのダウンロード
- イベントロギングページの列の表示および非表示
- Security Analytics and Logging のイベント属性

データストレージプラン

Cisco Cloud が導入準備された ASA および FTD から毎日受け取るイベント数を反映したデータストレージプランを購入する必要があります。これは「日次取り込み率」と呼ばれます。データプランは整数量の GB/日で、1 年、3 年、5 年単位でご利用いただけます。取り込み率を判断する最善の方法は、購入する前に Secure Logging Analytics（SaaS）の無料トライアルに参加することです。これにより、イベントボリュームを適切に見積ることができます。

お客様は、自動的に 90 日間のローリングデータストレージを受け取ります。つまり、最新の 90 日間のイベントが Cisco Cloud に保存され、91 日目に削除されます。

お客様は、デフォルトの 90 日間を超える追加のイベント保持にアップグレードしたり、既存のサブスクリプションの発注変更によって日単位のボリューム（GB/日）を追加したりすることができます。課金は、サブスクリプション期間の残りの部分についてのみ日割り計算で行われます。

データ プランの詳細については、『Secure Logging Analytics （SaaS）発注ガイド』を参照してください。

（注） Security Analytics and Logging のライセンスとデータプランをお持ちの場合は、その後は別の Security Analytics and Logging ライセンスを取得するだけで、別のデータプランを取得する必要はありません。ネットワークトラフィックのスループットが変化した場合は、別のデータプランを取得するだけで済み、別の Security Analytics and Logging ライセンスを取得する必要はありません。

割り当てに対してどのデータがカウントされますか？

Secure Event Connector に送信されたイベントはすべて、Secure Logging Analytics（SaaS）クラウドに蓄積され、データ割り当てに対してカウントされます。

イベントビューアに表示される内容をフィルタ処理しても、Secure Logging Analytics（SaaS）クラウドに保存されるイベントの数は減りません。イベントビューアに表示されるイベントの数が減るだけです。

イベントは Secure Logging Analytics（SaaS）クラウドに 90 日間保存され、その後消去されます。

ストレージの割り当てをすぐに使い果たしてしまいます。どうすればよいでしょうか？

この問題に対処するには、2 通りのアプローチがあります。

- より多くのストレージをリクエストする。必要なストレージ量の見積りが少なすぎる可能性があります。
- イベントを記録するルールの数を減らす。SSL ポリシールール、セキュリティ インテリジェンス ルール、アクセス制御ルール、侵入ポリシー、ファイルおよびマルウェアポリシーからのイベントをログに記録できます。現在何をログに記録していかを調べてください。考えているほど多くのルールとポリシーからのイベントをログに記録する必要がありますか？

イベントストレージ期間の延長およびイベントストレージ容量の増加

Secure Analytics and Logging のお客様は、これらのライセンシングのいずれかを購入すると、90 日間のイベントストレージを受け取ります。

- **Logging and Troubleshooting**
- **Logging Analytics and Detection**
- **Total Network Analytics and Monitoring**

ライセンスを最初に購入するとき、またはライセンスの有効期間中いつでも、ライセンスをアップグレードして、1 年、2 年、または 3 年分のローリング イベント ストレージを持つことを選択できます。

Security Analytics and Logging のライセンスを初めて購入する際、ストレージ容量をアップグレードするか尋ねられます。「はい」と答えると、購入する PID のリストに追加の製品識別子（PID）が追加されます。

ライセンス期間の途中で、ローリング イベント ストレージを拡張するか、イベントクラウドストレージの量を増やすことを決めた場合、次の手順を実行できます。

ステップ 1 Cisco Commerce のアカウントにログインします。

ステップ 2 自分の Cisco Defense Orchestrator PID を選択します。

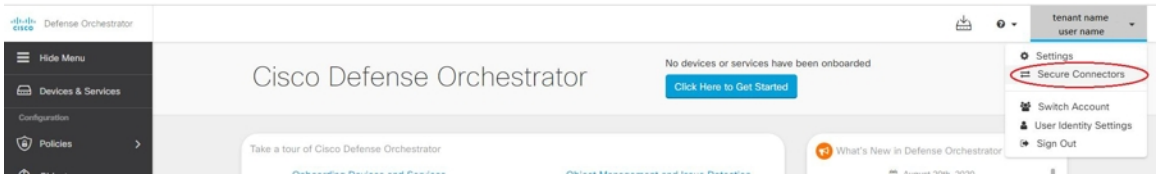
ステップ 3 プロンプトに従って、ストレージ容量の長さまたは容量をアップグレードします。

増加したコストは、既存のライセンスの残りの期間に基づいて比例配分されます。詳細な手順については、Secure Logging Analytics（SaaS）発注ガイド [英語] を参照してください。

セキュリティ分析およびロギングデータプランの使用状況の表示

毎月のロギング制限、使用したストレージ量、いつ使用期間がゼロにリセットされるかを表示するには、次の手順を実行します。

ステップ 1 アカウントメニューをクリックし、[設定] を選択します。



ステップ 2 [ロギングの設定（Logging Settings）] をクリックします。

ステップ 3 [使用履歴の表示（View Historical Usage）] をクリックして、過去 12 ヵ月のストレージ使用状況を表示することもできます。

SecureLoggingAnalytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索

Secure Logging Analytics（SaaS）を使用すると、ご使用の ASA デバイスまたは FTD デバイスから、Secure Event Connector（SEC）上の特定の UDP、TCP、または NSEL ポートにイベントを送信できます。その後、SEC はそれらのイベントを Cisco Cloud に転送します。

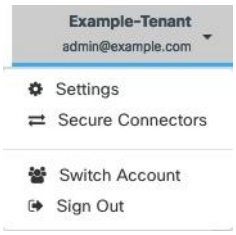
まだ使用されていないポートの場合、SECはそれらのポートを使用してイベントを受信できるようにします。Secure Logging Analytics（SaaS）のマニュアルでは、機能を設定するときにポートを使用することが推奨されています。

- TCP：10125
- UDP：10025
- NSEL：10425

すでに使用されているポートの場合は、Secure Logging Analytics（SaaS）を設定する前に、SECデバイスの詳細を調べて、イベントの受信に実際に使用しているポートを特定します。

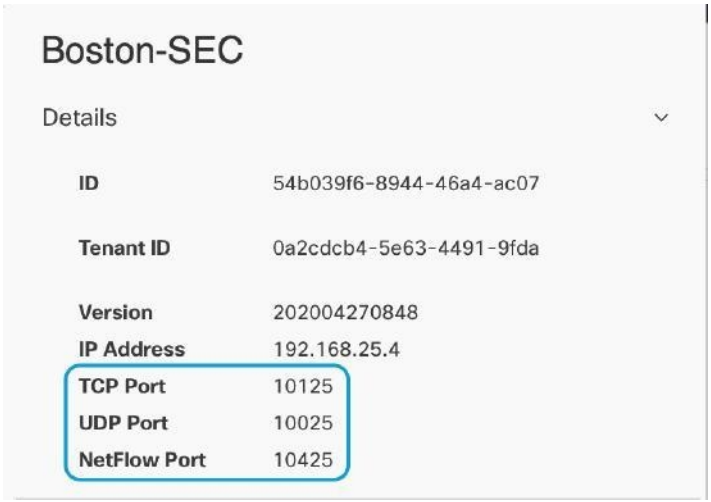
SEC が使用するポート番号を見つけるには、次の手順を実行します。

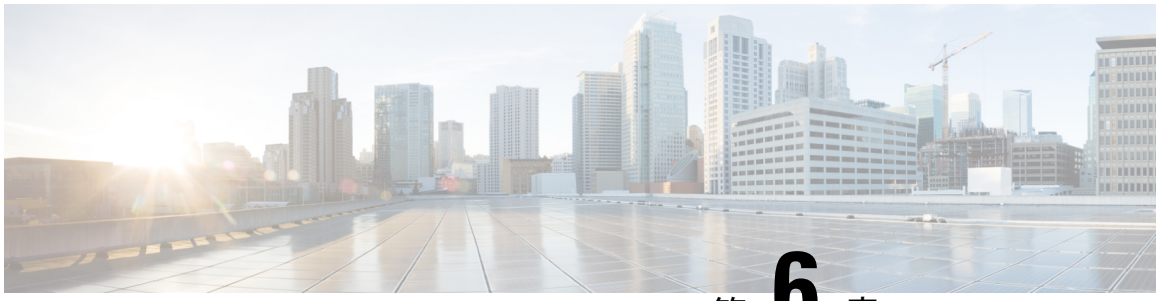
ステップ 1 CDO の任意のページで[アカウント（Account）]メニューを開き、[セキュアコネクタ（Secure Connectors）]を選択します。



ステップ 2 [セキュアコネクタ（Secure Connectors）]ページで、イベントを送信する SEC を選択します。

ステップ 3 [詳細]ペインに、イベントの送信先となる TCP、UDP、および NetFlow（NSEL）ポートが表示されます。





第 6 章

顧客をシスコ セキュア インターネット ゲートウェイ（SIG）に安全に接続する

Cisco Defense Orchestrator で Umbrella を管理する

Umbrella は、シスコのクラウドベース Secure Internet Gateway（SIG）プラットフォームです。インターネットベースの脅威に対する防御を複数のレベルで提供します。Umbrellaは、セキュア Web ゲートウェイ、ファイアウォール、DNS レイヤセキュリティ、およびクラウド アクセス セキュリティ ブローカ（CASB）機能を統合して、システムを脅威から保護します。SIG およびDNS 保護を利用することにより、ASA デバイスは、デバイスのローカル DNS インスペクションポリシーと Umbrella クラウドベースの DNS インスペクションポリシーの両方を使用して保護されます。Umbrellaは、着信トラフィックを検査および検出するいくつかの方法を提供することにより、ASA デバイスを FTD 次世代ファイアウォール（NGFW）に匹敵するものにします。

現時点では、CDO は Umbrella 組織との ASA の統合のみをサポートしています。

SASE を使用したブリッジの構築

セキュアアクセス サービスエッジ（SASE）は、ネットワーキング機能とセキュリティ機能を単一のサービスに統合する先進的なフレームワークであり、クラウドエッジで動作して保護と優れたパフォーマンスを実現します。この取り組みにより、場所に関係なくサービスを安全かつ確実に統合する方法が提供され、組織の規模にかかわりなくネットワークを制御および管理できるようになります。複雑さが軽減され、管理が俊敏になれば、展開がシンプル、スケーラブルかつ安全になります。

Umbrella 組織とは

Umbrella 組織は、1 つのライセンスキーに関連付けられたさまざまなユーザーロールを持つユーザーのグループです。 1 人のユーザーが複数の Umbrella 組織にアクセスできます。すべ

ての Umbrella 組織は、Umbrella の個別のインスタンスであり、独自のダッシュボードを持ちます。組織は名前と組織 ID によって識別されます。組織 ID により組織が識別され、仮想アプライアンスなどのコンポーネントの展開に使用されます。また、サポートに組織 ID が必要となる場合があります。

SIG トンネルとは

セキュア インターネット ゲートウェイ（SIG）トンネルは、ASA と Umbrella の間で生成される SIG IPSec（インターネット プロトコル セキュリティ）トンネルのインスタンスであり、インターネットに向かうすべてのトラフィックは Umbrella SIG に転送され、検査およびフィルタリングされます。このソリューションは、セキュリティの中央管理を実現するため、ネットワーク管理者は各ブランチのセキュリティ設定を個別に管理する必要がありません。

トンネルが設定されている Umbrella 組織を導入準備すると、これらのトンネルは CDO のサイト間 VPN ページに一覧表示されます。CDO UI から Umbrella 組織の SASE トンネルを作成するには、「Cisco Umbrella 用の SASE トンネルの設定」を参照してください。

（注） Umbrella 組織とそのピアデバイスを導入準備した場合、サイト間 VPN ページで、その組織に関連付けられているトンネルに接続するすべてのデバイスが 1 つのエントリにまとめられます。[トンネル（Tunnels）]ページを手動で更新し、Umbrella ダッシュボードから加えられた変更を読み取るには、「Umbrella のトンネル設定の読み取り」を参照してください。

CDO と Umbrella の通信方法

Umbrella 組織と、その組織に関連付けられている ASA デバイスを導入準備する必要があります。

ASA デバイスが Umbrella クラウドに関連付けられている場合、その接続には、デバイスとクラウドの間に安全な接続を作成するためのサイト間 VPN SIG トンネルが必要です。CDO は、Umbrella 組織と ASA デバイスの両方と通信します。このデュアル通信方式により、CDO は設定の変更またはトンネルの変更を即座に検出し、Umbrella、ASA、およびトンネルのアウトオブバンドの変更、エラー、または異常な状態について時を移さず警告します。

Umbrella 組織を CDO に導入準備する場合、組織の API キーと秘密を使用して導入準備します。どちらも組織とその組織に関連付けられている ASA デバイスに固有のものを使用します。CDO は Umbrella API を使用して Umbrella クラウドと通信し、組織の導入準備に使用された API キーと秘密を使用して、ASA デバイスに関する情報を要求および送信します。このレベルの通信で、ASA と Umbrella クラウドの間に存在する SIG トンネルが危険にさらされることはありません。

Umbrella 組織が導入準備されると、[デバイスとサービス]ページに、組織に関連付けられている検出済みの ASA デバイスが「ピア」として表示され、デバイスが CDO に導入準備されているかどうかが示されます。ピアデバイスがまだ導入準備されていない場合は、[デバイスの導入準備] をクリックして、そのページから直接導入準備することも可能です。Umbrella 組織に関連付けられている ASA デバイスが CDO に導入準備されると、[デバイスとサービス] ページにその関係が表示され、[VPN トンネル（VPN Tunnels）] ページにデバイスと組織間のトンネルが表示されます。組織に関連付けられている ASA デバイスが CDO に導入準備されていない

場合、デバイスに関連付けられているトンネルが [VPNトンネル（VPN Tunnels）] に表示されるので、このページから直接デバイスを導入準備することができます。

CDO から Umbrella クラウドへのアクセス方法

Umbrella 組織が CDO に正常に導入準備されると、CDO UI から組織のダッシュボードまたは [Umbrellaトンネル（Umbrella Tunnels）] ページをクロス起動できます。

CDO UI から Umbrella クラウドにアクセスするには、「Umbrella ダッシュボードのクロス起動（493 ページ）」と「[Cisco Umbrellaトンネル（Umbrella Tunnels）] ページのクロス起動（494 ページ）」を参照してください。

前提条件

サポート対象ハードウェアおよびソフトウェア

Umbrella 組織はクラウドベースであるため、バージョンがありません。Umbrella 組織を CDO に導入準備する際、その組織を関連付けることができるのは 1 台の ASA デバイスのみであることに注意してください。

Umbrella 統合の場合、CDO は 9.1.2 以降を実行する ASA デバイスをサポートします。CDO がサポートする ASA デバイスモデルとソフトウェアのリストについては、「クラウドデバイスのサポートの詳細（37 ページ）」を参照してください。

ライセンス要件

Umbrella 組織を CDO に正常に導入準備するには、次のいずれかのライセンスパッケージを選択する必要があります。

- Umbrella SIG Essentials
- SIG Advantage

オンボーディング

Umbrella アカウントを正常に管理するには、Umbrella 組織のオンボーディングとそれに関連付けられている ASA デバイスの導入準備の両方を導入準備する必要があります。Umbrella 組織を導入準備すると、CDO は組織に関連付けられた既存の ASA トンネルを読み取り、これらのトンネルと、作成して組織に関連付けた追加のトンネルの正常性ステータスを監視します。Umbrella 組織を導入準備する前に、一般的なデバイス要件と導入準備の前提条件を確認してください。

Umbrella 組織に関連付けられた ASA デバイスを導入準備する前に、その組織を導入準備した場合は、[サイト間VPN] ページから ASA ピアを表示して、VPN ページからデバイスを導入準備できます。

（注） フェールオーバー用に設定された ASA ペアがある場合は、2 つのピアのうちアクティブデバイス**のみ**を導入準備する必要があります。アクティブデバイスとスタンバイデバイスの両方を CDO に導入準備すると、Umbrella ですでに設定されている SASE トンネルと重複するトンネル情報が生成される場合があります。

ネットワークのモニタリング

CDO は、セキュリティポリシーの影響を要約したレポートを発行し、セキュリティポリシーによってトリガーされた重要なイベントの表示方法を提供します。また CDO は、デバイスに加えた変更をログに記録し、それらの変更にラベルを付ける方法を提供します。これにより、CDO で確定した操作をヘルプチケットやその他の操作要求に関連付けることができます。

ログの変更

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おける変更が含まれます。Umbrella はクラウドベースの製品であるため、変更は即座に展開されます。

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、いつを回答。
- 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。

（注） Umbrella 組織に関連付けられた SASE トンネルを作成、編集、または削除すると、Umbrella 組織とそれに関連付けられている ASA デバイスの要求と設定の変更が表示されることに注意してください。

Umbrella ドキュメント

- Umbrella ヘルプ
- Umbrella と Cisco ASA の設定
- トンネル経由での Cisco Umbrella への接続
- Cisco Umbrella API

Umbrella 組織の導入準備

Umbrella ライセンス要件

Cisco Umbrella 組織を CDO に正常に導入準備するには、Cisco Umbrella ダッシュボードから次のいずれかのライセンスパッケージを選択する必要があります。

- Umbrella SIG Essentials
- SIG Advantage

現在有効になっているライセンスを確認するには、Cisco Umbrella ダッシュボードにログインし、**[管理（Admin）]** > **[ライセンス（Licensing）]**に移動します。

Umbrella 組織 ID

組織を CDO に正常に導入準備するには、Umrbrella 組織 ID の場所を特定し、それをログイン資格情報とともに使用する必要があります。

ステップ 1 Cisco Umbrella ダッシュボードにアクセスして、組織にログインします。

ステップ 2 ページの URL には数字の ID が含まれています。たとえば、https://dashboard.umbrella.com/o/**123456**/#/overview の組織 ID は **123456** です。

ステップ 3 URL から組織 ID をコピーします。使用する準備ができるまで、一時的にメモに貼り付けることをお勧めします。

API キーと秘密の生成

Umbrella 組織を CDO に導入準備する前に、新しい API キーを生成し、**API キー**と対応する**シークレット**の**両方**を取得します。API キーをすでに持っているものの、シークレットを保存していない場合は、**[管理（Admin）]** > **[API キー（API Keys）]** 画面に移動し、[更新] をクリックしてキーとシークレットを更新します。それ以外の場合は、次の手順を使用して新しい API キーを作成します。

始める前に

Umbrella からの管理 API キーは、次の Umbrella サービスに使用されます。

- ネットワークおよびドメイン
- ネットワークトンネル
- ユーザおよびロール
- 接続先リスト
- サービス プロバイダー

これらのサービスへの CDO アクセスを許可せずに Umbrella 組織を導入準備することはできません。

ステップ 1 Cisco Umbrella ダッシュボードにアクセスして、組織にログインします。

ステップ 2 Umbrella ダッシュボードの左側のナビゲーションウィンドウで [管理（Admin）] をクリックし、[APIキー（API Keys）] を選択します。

ステップ 3 [API キーの作成（Create API Key）] をクリックします。

ステップ 4 [Umbrella管理（Umbrella Management）] を選択します。**[Next]** をクリックします。

ステップ 5 API キーと対応するシークレットをコピーします。使用する準備ができるまで、一時的にメモに貼り付けることをお勧めします。

Umbrella 組織のオンボーディング

Umbrella 組織を CDO に導入準備するには、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 青いプラスボタンをクリックして、デバイスのオンボーディングを開始します。

ステップ 3 [Umbrella組織（Umbrella Organization）] をクリックします。

ステップ 4 Umbrella ダッシュボードから生成した Umbrella ネットワークデバイスの [APIキー（API Key）] と [秘密（Secret）] を入力します。

ステップ 5 **[Next]** をクリックします。

ステップ 6 正しい組織名と組織 ID が表示されていることを確認してください。

ステップ 7 **[Next]** をクリックします。

ステップ 8 （オプション）デバイスに固有の [ラベル（Labels）] を追加します。後で、このラベルでデバイスのリストをフィルタリングできます。

ステップ 9 [ダッシュボードとサービスに移動（Go to Dashboard & Services）] をクリックします。

Umbrella 組織の CDO への再接続

警告 保存されているログイン情報が無効である場合、CDO は、Umbrella 組織への設定変更の展開や Umbrella 組織からの設定変更の読み取りを正常に実行できませんが、その組織に関連付けられた ASA デバイスへの設定変更の展開やそれらのデバイスからの設定変更の読み取りは正常に実行できます。そのため、ログイン情報が更新および検証されると、問題が発生する可能性があります。設定変更を展開する前に、組織のログイン情報を更新することをお勧めします。

Umbrella組織のAPIキーとシークレットが更新されたか、タイムアウトした場合は、デバイスを CDO に手動で再接続する必要があります。再接続するには、次の手順を実行します。

ステップ 1 Umbrella ダッシュボードに移動します。左側のナビゲーションウィンドウで [管理（Admin）] をクリックし、既存の Umbrella 管理の **API キー**を選択します。

ステップ 2 [更新（Refresh）] をクリックします。API キーとシークレットを更新することを確認します。

ステップ 3 API キーと対応するシークレットをコピーします。

ステップ 4 CDO にログインします。

ステップ 5 [デバイスとサービス（Devices & Services）] ページに移動します。

ステップ 6 フィルタまたは検索バーを使用して Umbrella 組織を見つけます。

ステップ 7 [デバイスアクション] ペインで、[再接続（Reconnect）] をクリックします。CDO は、保存されている API キーとシークレットが無効になっていることを確認します。

ステップ 8 API キーとシークレットを適切なポップアップウィンドウに貼り付けます。

ステップ 9 [続行（Continue）] をクリックします。

ステップ 10 新しいキーとシークレットが有効であることを CDO が確認したら、[閉じる（Close）] をクリックします。

Umbrella ダッシュボードのクロス起動

ASA デバイスと Cisco Umbrella 組織が CDO に正常に導入準備されると、CDO UI から組織のダッシュボードをクロス起動できます。

次の手順を使用して、デバイスの Cisco Umbrella ダッシュボードをクロス起動します。

ステップ 1 CDO にログインします。

ステップ 2 [デバイスとサービス（Devices & Services）] をクリックします。

ステップ 3 Cisco Umbrella 組織を検索またはフィルタリングします。フィルタ （85 ページ）

ステップ 4 [管理] ペインで [Cisco Umbrella組織の管理（Manage Umbrella Organization）] をクリックします。CDO が新しいタブをブラウザで起動し、選択した組織に関連付けられた Cisco Umbrella ダッシュボードが開きます。

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。

Umbrella 組織の設定

Umbrella のトンネル設定の読み取り

Umbrella 組織が CDO に導入準備されると、CDO に手動で Umbrella からトンネル設定を要求および更新させることができます。これには、追加、削除、または変更されたトンネルが含まれます。

警告 Umbrella 組織の資格情報が無効と見なされているときにトンネルが CDO から削除された場合、または組織を導入準備してから変更された場合、CDO は、組織に関連付けられた ASA デバイスにのみトンネル設定を展開できます。ログイン情報の更新時に、CDO は Umbrella の設定を読み取り、削除されたすべてのトンネルを再度追加します。Umbrella 組織に存在するものの、いずれの ASA デバイスにも存在しないトンネルがあると、同期の問題が発生し、ASA デバイスが組織のピアとして表示されない場合があります。

ステップ 1 CDO にログインします。
ステップ 2 [デバイスとサービス（Devices & Services）] ページで、[デバイス（Devices）] タブをクリックします。
ステップ 3 [SFCN] タブをクリックします。
ステップ 4 Umbrella 組織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、[トンネルの読み取り（Read Tunnels）] を選択します。

[Cisco Umbrella トンネル（Umbrella Tunnels）] ページのクロス起動

ASA デバイスと Cisco Umbrella 組織が CDO に正常に導入準備されると、CDO UI からトンネルの Cisco Umbrella ダッシュボードをクロス起動できます。

次の手順を使用して、デバイスの [Cisco Umbrella トンネル（Umbrella Tunnels）] ページをクロス起動します。

ステップ 1 CDO にログインします。
ステップ 2 [VPN] ウィンドウに移動します。[サイト間VPN] を選択します。
ステップ 3 目的のトンネルを選択して強調表示します。

ステップ 4 [アクション] ペインで、[Cisco Umbrellaのトンネルの管理（Manage Tunnel in Umbrella）] をクリックします。CDO により、ブラウザで新しいタブが起動され、[トンネル（Tunnels）] の概要ページが開きます。

Cisco Umbrella 用の SASE トンネルの設定

次の手順を使用して、Cisco Umbrella 組織の SASE トンネルを作成します。

始める前に

トンネルを作成する Cisco Umbrella 組織と ASA デバイスは、すでに CDO に導入準備されている必要があることに注意してください。

展開したトンネルに関連付けられた ASA または Cisco Umbrella 組織が異常な状態になっている場合、CDOはトンネルを正常に展開できないことがあります。問題が発生した場合は、Cisco TAC にお問い合わせください。

ステップ 1 CDO にログインします。

ステップ 2 [VPN] ウィンドウに移動します。[サイト間VPN] を選択します。

ステップ 3 青色のプラスボタンをクリックし、[SASEトンネルの作成（Create SASE Tunnel）] を選択します。

ステップ 4 Cisco Umbrella ピア情報を入力します。

- [Cisco Umbrellaの選択（Select Umbrella）]：選択した **Cisco Umbrella** 組織を選択します。
- [データセンター（Datacenter）]：ヘッドエンドデータセンターを選択します。Cisco Umbrella 組織に関連付けられている ASA に地理的に近いデータセンターを選択することをお勧めします。

ステップ 5 ASA ピア情報を入力します。

- [ASAデバイスの選択（Select ASA Device）]：ドロップダウンリストから Cisco Umbrella 組織に関連付けられている ASA デバイスを選択し、[選択（Select）] をクリックします。
- [パブリックインターフェイス（Public Facing Interface）]：静的でパブリックにルーティング可能な IPv4 アドレスを選択します。使用されるアドレスは、NAT には使用しないでください。
- [LANアドレス（LAN Address）]：LAN サブネットを制御する LAN インターフェースを選択します。LAN 用に少なくとも 1 つのインターフェースを選択する必要があります。
- [仮想トンネルインターフェイス（Virtual Tunnel Interface）]：Cisco Umbrella 組織と ASA ピアデバイスを選択すると、このフィールドは自動的に入力されます。必要に応じて、新しい VTI として使用される IP アドレスを手動で入力できます。

ステップ 6 Cisco Umbrella 組織と ASA ピアデバイスを選択すると、[パスフレーズ（Passphrase）] が自動的に入力されます。[確認パスフレーズ（Confirm Passphrase）] も自動的に入力されます。必要に応じて、これらのフィールドに手動で入力できます。

ステップ 7 （任意）ポップアップウィンドウの下部にある [変更をASAにすぐに展開（Deploy changes to ASA immediately）] トグルは、デフォルトで有効になっています。有効になっている場合、SASE トンネル設定は、トンネル設定で選択されたASAピアにすぐに展開されます。変更をステージングして後で展開する場合は、オプションを手動で無効に切り替えます。

ステップ 8 [展開（Deploy）] をクリックします。必要に応じて、[展開してもう 1 つ作成（Deploy and Create Another）] をクリックして、この SASE トンネルを同時に展開し、別のトンネルを作成します。展開されたトンネルは [VPNトンネル（VPN Tunnels）] ページに表示されます。[展開して別のSASEトンネルを作成（Deploy and Create Another SASE tunnel）] を選択した場合、CDO は Cisco Umbrella 組織の選択と [変更をASAにすぐに展開（Deploy changes to ASA immediately）] トグル設定の両方を保存し、これらの選択を次のトンネル設定に自動的に適用します。展開する前に、これらの選択を手動で変更できます。

SASE トンネルの編集

次の手順を使用して、既存の SASE トンネルを変更します。

ステップ 1 CDO にログインします。

ステップ 2 [VPN] ウィンドウに移動します。[サイト間VPN] を選択します。

ステップ 3 変更するトンネルを選択します。

ステップ 4 [アクション] ペインで、[編集] を選択します。

ステップ 5 SASE トンネルの次のフィールドを編集します。

- [名前（Name）]：CDO および Cisco Umbrella ダッシュボードに表示される SASE トンネルの名前を変更します。
- [Cisco Umbrellaピアのデータセンター（Umbrella Peer's Datacenter）]：ドロップダウンメニューから新しいヘッドエンドデータセンターを選択します。
- [ASAピアのパブリックインターフェイス（ASA Peer's Public Facing Interface）]ドロップダウンメニューから新しい IPv4 アドレスを選択します。
- [ASAピアのLANインターフェイス（ASA Peer's LAN Interfaces）]：ドロップダウンメニューから 1 つ以上の新しい LAN インターフェイスを選択します。
- [ASA仮想トンネルインターフェイス（VTI）アドレス（ASA Virtual Tunnel Interface (VTI) Address）]：VTI を手動で編集します。
- [パスフレーズ（Passphrase）]：トンネルのパスフレーズを手動で変更します。
- [パスフレーズの確認（Confirm Passphrase）]：このエントリを手動で変更してパスフレーズと照合し、新しい値を確認します。

ステップ 6 （任意）ポップアップウィンドウの下部にある [変更をASAにすぐに展開（Deploy changes to ASA immediately）] トグルは、デフォルトで有効になっています。有効になっている場合、SASE トンネル設定は、トンネル設定で選択されたASAピアにすぐに展開されます。変更をステージングして後で展開する場

合は、オプションを手動で無効に切り替えます。変更をステージングして後で展開することを選択した場合、[インベントリ] ページの ASA ピアステータスは [Deploy Pending（展開保留中）] と表示されます。

ステップ 7 [更新の保存（Save Updates）] を選択します。

Umbrella からの SASE トンネルの削除

CDO UI を使って SASE トンネルを削除するには、次の手順を使用します。

始める前に

SASE トンネルを削除するには、それに関連付けられている ASA が CDO で同期済みのステータスになっている必要があります。デバイスが正常でない場合は、トンネルを削除できません。

CDO から SASE トンネルを削除すると、トンネルは、関連付けられている ASA デバイスと Umbrella 組織の両方から削除されることに注意してください。

警告 Umbrella 組織のログイン情報が無効と見なされているときに CDO からトンネルを削除した場合や、組織を導入準備した後に変更した場合、CDO は、組織に関連付けられた ASA デバイスにのみトンネル設定を展開できます。ログイン情報の更新時に、CDO は Umbrella の設定を読み取り、削除されたすべてのトンネルを再度追加します。Umbrella 組織に存在するものの、いずれの ASA デバイスにも存在しないトンネルがあると、同期の問題が発生し、ASA デバイスが組織のピアとして表示されない場合があります。組織に関連付けられたトンネルを削除する前に、Umbrella のログイン情報を確認することをお勧めします。

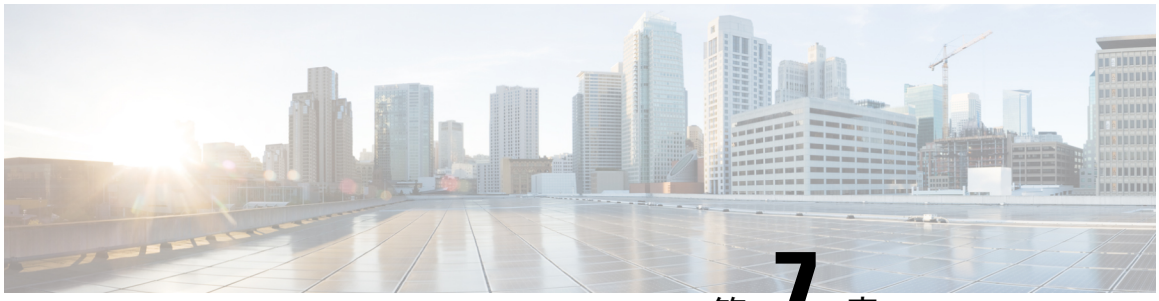
ステップ 1 CDO にログインします。

ステップ 2 [VPN] ウィンドウに移動します。[サイト間VPN] を選択します。

ステップ 3 CDO から削除するトンネルを選択します。

ステップ 4 [操作（Actions）] ウィンドウで、[削除（Delete）] をクリックします。

ステップ 5 トンネルを削除することを確認し、[OK] をクリックします。



第 7 章

CDO と SecureX を統合する

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 （559 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 （501 ページ）
- CDO の SecureX の切断 （502 ページ）
- CDO の SecureX への追加
- SecureX のトラブルシューティング （559 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 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。

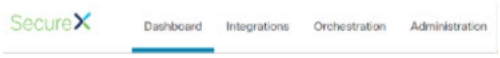
ステップ 3 ウィンドウの左側にある [全般設定（General Settings）] タブを選択します。

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。

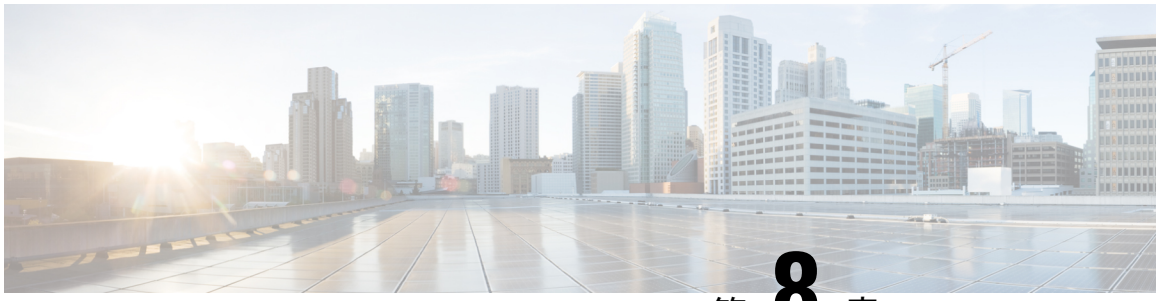
- [CDOデバイスの概要（CDO Device Summary）]：このタイルには、CDO テナントに現在導入準備されているすべてのデバイスとそのステータスの一覧が表示されます。
- [CDOオブジェクトとポリシー（CDO Objects and Policies）]：このタイルには、デバイスに現在適用されているすべてのポリシーと、それらのポリシーに関連付けられているオブジェクトの一覧が表示されます。

（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 8 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。

ASA デバイス

次の項目を使用して、ASA デバイスのトラブルシュートを行います。

- リブート後の ASA と CDO の再接続に失敗
- ASA パケットトレーサ
- ASA リアルタイムロギング
- ASA 実行設定サイズを確認する

- 大きな ASA 実行設定ファイル
- Cisco ASA Advisory cisco-sa-20180129-asa1
- 新規フィンガープリントを検出状態の解決
- 新規証明書の問題のトラブルシュート

証明書エラーのため ASA の導入準備ができない

環境：ASA はクライアント側の証明書認証で設定されています。

解決策：クライアント側の証明書認証を無効にします。

詳細：ASA はログイン情報ベースの認証とクライアント側の証明書認証をサポートします。CDO はクライアント側の証明書認証を使用する ASA に接続できません。ASA を CDO に導入準備する前に、次の手順を使用して、クライアント側の証明書認証が有効になっていないことを確認してください。

ステップ 1 ターミナルウィンドウを開き、SSH を使用して ASA に接続します。

ステップ 2 グローバル コンフィギュレーション モードを開始します。

ステップ 3 hostname (config)# プロンプトで、次のコマンドを入力します。

```
no ssl certificate-authentication interface interface-name port 443
```

インターフェイス名は、CDO が接続するインターフェイスの名前です。

リブート後の ASA と CDO の再接続に失敗

ASA のリブート後に CDO と ASA が接続しない場合、ASA が、CDO の Secure Device Connector（SDC）でサポートされていない OpenSSL 暗号スイートを再び使用するようになったことが原因である可能性があります。このトラブルシューティング トピックでは、そのようなケースをテストし、修復手順を示します。

症状

- ASA のリブート後、CDO と ASA が再接続されません。CDO に「再接続に失敗しました（Failed to reconnect）」というメッセージが表示されます。
- ASA を導入準備しようとすると、CDO に次のメッセージが表示されます。「*<ASA_IP_Address>* の証明書を取得できませんでした（*Certificate could not be retrieved for <ASA_IP_Address>*）」

ASA で使用する OpenSSL 暗号スイートの特定

この手順を使用して、ASA で使用されている OpenSSL 暗号スイートを識別します。コマンド出力で指定された暗号スイートが、CDO の Secure Device Connector でサポートされる暗号スイートにない場合、SDC はその暗号スイートをサポートしていないため、ASA の暗号スイートを更新する必要があります。

ステップ 1 SDC に到達可能なコンピュータでコンソールウィンドウを開きます。

ステップ 2 SSH を使用して SDC に接続します。CDO や SDC などの通常のユーザー、または作成した他のユーザーとしてログインできます。root としてログインする必要はありません。

ヒント　SDC IP アドレスを特定するには、次の手順を実行します。

1. CDO を開きます。
2. ユーザーメニューから、[Secure Device Connector] を選択します。
3. 表に示されている SDC をクリックします。SDC の IP アドレスが、デバイスの詳細ペインに表示されます。

ステップ 3 コマンドプロンプトで次のように入力します。 **openssl s_client -showcerts -connect** *ASA_IP_Address*:**443**

ステップ 4 コマンド出力で次の行を探します。

```
New, TLSV1/SSLv3, Cipher is DES-CB3-SHA
or
SSL-Session:
            Protocol: TLSv1.2
            Cipher: DES-CB3-SHA
```

この例では、ASA で使用されている暗号スイートは `DES-CB3-SHA` です。

CDO の Secure Device Connector でサポートされる暗号スイート

CDO の Secure Device Connector は、最新かつ最も安全な暗号のみを受け入れる node.js を使用します。したがって、CDO の SDC は次の暗号のリストのみをサポートします。

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256

- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA256

ASA で使用する暗号スイートがこのリストにない場合、SDC はその暗号スイートをサポートしていないため、ASA の暗号スイートの更新必要があります。

ASA の暗号スイートの更新

ASA で TLS 暗号スイートを更新するには、次の手順を実行します。

ステップ 1 SSH を使用して ASA に接続します。

ステップ 2 ASA に接続したら、グローバル コンフィギュレーション モードに権限を昇格させます。プロンプトは次のようになります。asaname(config)#

ステップ 3 プロンプトで、次のようなコマンドを入力します。

```
ssl cipher tlsv1.2 custom "ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384 DHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256 DHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-SHA384 DHE-RSA-AES256-SHA384
ECDHE-RSA-AES256-SHA256 DHE-RSA-AES256-SHA256"
```

（注） このコマンドで ASA がサポートするように設定する暗号スイートは、引用符の間および単語 custom の後に入力されます。このコマンドの場合、指定された暗号スイートは `ECDHE-RSA-AES128-GCM-SHA256` で始まり、`DHE-RSA-AES256-SHA256` で終わります。ASA でコマンドを入力するときに、ASA がサポートしないことがわかっている暗号スイートをすべて削除します。

ステップ 4 コマンドを送信したら、プロンプトで「write memory」と入力して、ローカル設定を保存します。例：

```
asaname(config)#write memory
```

CLI コマンドを使用した ASA のトラブルシューティング

このセクションでは、ASA のトラブルシューティングと基本的な接続のテストに使用できる重要なコマンドのいくつかについて説明します。他のトラブルシューティング シナリオと CLI コマンドを確認するには、『CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide』を参照してください。「System Administration」セクションで、「Testing and Troubleshooting」の章に移動します。

各 ASA デバイスで使用可能な CDO CLI インターフェイスを使用して、これらのコマンドを実行できます。CDO での CLI インターフェイスの使用方法については、「CDO コマンド ライン インターフェイスを使用する」を参照してください。

NAT ポリシーの設定

NAT 設定を決定するための重要なコマンドの例を次に示します。

- NAT ポリシーの統計情報を確認するには、**show nat** を使用します。
- 割り当てられたアドレスとホスト、および割り当て回数を含めて、NAT プールを確認するには、**show nat pool** を使用します。

NAT に関連したその他のコマンドについては、『CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide』を参照し、「Network Address Translation (NAT)」の章に移動してください。

基本接続のテスト：アドレス向けの ping の実行

ASA CLI インターフェイスで **ping <IP address>** コマンドを使用して ASA デバイスに ping できます。次を確認するには

ルーティング テーブルの表示

show route コマンドを使用してルーティングテーブル内のエントリを表示します。

ciscoasa# show route

ASA のルーティングテーブルの出力例：

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF
Gateway of last resort is 192.168.0.254 to network 0.0.0.0
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.0.254, management
C 10.0.0.0 255.0.0.0 is directly connected, Outside
L 10.10.10.1 255.255.255.255 is directly connected, Outside
C 192.168.0.0 255.255.255.0 is directly connected, management
L 192.168.0.118 255.255.255.255 is directly connected, management
```

スイッチポートのモニタリング

- **show interface**

  インターフェイス統計情報を表示します。

- **show interface ip brief**

  インターフェイスの IP アドレスとステータスを表示します。

- **show arp**

ダイナミック、スタティック、およびプロキシARPエントリを表示します。ダイナミックARPエントリには、ARP エントリの秒単位のエージングが含まれています。

ARP エントリの出力例：

```
management 10.10.32.129 0050.568a.977b 0

management 10.10.32.136 0050.568a.5387 21

LANFAIL 20.20.21.1 0050.568a.4d70 96

outsi 10.10.16.6 0050.568a.e6d3 3881

outsi 10.10.16.1 0050.568a.977b 5551
```

ASA リモートアクセス VPN のトラブルシュート

このセクションでは、ASA デバイスでリモートアクセス VPN を設定するときに発生する可能性がある、いくつかのトラブルシューティングの問題について説明します。

RA VPN モニタリングページに情報がない

この問題は、外部インターフェイスが Webvpn に対して有効になっていない場合に発生する可能性があります。

解決策：

1. 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。
2. [デバイス] タブをクリックしてから、[ASA] タブをクリックします。
3. 問題のある RA VPN ヘッドエンド ASA デバイスを選択します。
4. 右側の [管理] ペインで、[構成] をクリックします。
5. [編集] をクリックして、「webvpn」を検索します。
6. **Enter キー**を押して、`enable` *interface_name* を追加します。ここで interface_name は、リモートアクセス VPN 接続を確立するときにユーザーが接続する外部インターフェイスの名前です。これは通常外部（インターネットに接続された）インターフェイスですが、デバイスとこの接続プロファイルがサポートしているエンドユーザー間のインターフェイスのいずれかを選択します。

   次に例を示します。

   ```
   webvpn

   enable outside
   ```

7. [保存（Save）] をクリックします。
8. 構成をすべてのデバイスの構成変更のプレビューと展開します。

既存の RA VPN 設定に ASA を追加できない

•

始める前に

•

手順の概要

1.

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	例：	

例

次のタスク

•

ASA パケットトレーサ

パケットトレーサを使用すると、合成パケットをネットワークに送信し、既存のルーティング設定、NAT ルール、およびポリシー設定がそのパケットにどのように影響するかを評価できます。次の種類の問題をトラブルシューティングするには、このツールを使用します。

- アクセスできるはずのリソースにアクセスできないとユーザーが報告している。
- 到達できないはずのリソースに到達できるとユーザーが報告している。
- ポリシーをテストして、期待どおりに機能するかどうかを判断します。

パケットトレーサは、稼働中のオンライン ASA デバイス（物理または仮想）で使用できます。パケットトレーサはデバイス（Devices）では動作しません。パケットトレーサでは ASA に保存された設定に基づいてパケットが評価されます。CDO の段階的な変更はパケットトレーサでは評価されません。

同期状態の ASA でパケットトレーサを実行することがベストプラクティスです。デバイスが同期されていなくてもパケットトレーサは動作しますが、予期しない結果が生じる可能性があります。たとえば、CDO のステージングされた設定でルールを削除し、パケットトレース中にこの同じルールが ASA でトリガーされた場合、CDO はパケットとそのルールとの相互作用の結果を表示できません。

ASA パケットトレーサによるトラブルシューティング

パケットトレーサは、ASA のルーティング設定、NAT ルール、およびセキュリティポリシーを介してパケットを送信するため、各ステップでのパケットのステータスが表示されます。パケットがポリシーによって許可されている場合、緑色のチェックマークが表示されます。パケットが拒否されてドロップされた場合、CDO には赤い X マークが表示されます。

パケットトレーサでは、パケットトレース結果のリアルタイムログも表示されます。以下の例では、ルールによって tcp パケットが拒否された場所を確認できます。

ASA デバイスのセキュリティポリシーのトラブルシュート

ステップ 1 [デバイスとサービス] ページから ASA を選択し、[アクション] ペインで [トラブルシューティング（Troubleshoot）] Troubleshoot をクリックします。

ステップ 2 [値（Values）] ペインで、ASA を介して仮想的に送信するインターフェイスとパケットタイプを選択します。

ステップ 3 （オプション）セキュリティグループタグの値がレイヤ 2 CMD ヘッダーに埋め込まれたパケットを追跡する（Trustsec）場合は、[SGT番号（SGT number）] をオンにして、セキュリティグループタグの番号（0 ～ 65535）を入力します。

ステップ 4 送信元と接続先を指定します。Cisco TrustSec を使用する場合は、IPv4 または IPv6 アドレス、完全修飾ドメイン名（FQDN）、またはセキュリティ グループの名前あるいはタグを指定できます。送信元アドレスに対して、Domain\username 形式でユーザー名を指定することもできます。

ステップ 5 他のプロトコルの特性を指定します。

- [ICMP]：ICMP タイプ、ICMP コード（0 ～ 255）、およびオプションで ICMP 識別子を入力します。
- [TCP/UDP/SCTP]：リストから選択するか、ポートコンボボックスに値を入力して、送信元ポートと宛先ポートを入力します。
- [IP]：プロトコル番号（0 ～ 255）を入力します。

ステップ 6 [パケットトレーサを実行（Run Packet Tracer）] をクリックします。

ステップ 7 [パケットトレーサ結果の分析（Analyze Packet Tracer Results）]パケットトレーサ結果の分析 （514 ページ）に進みます。

アクセスルールのトラブルシュート

ステップ 1 **[ポリシー（Policies）]** > **[ネットワークポリシー（Network Policies）]** > **.** を選択します。

ステップ 2 ASA に関連付けられているポリシーを選択します。

ステップ 3 トラブルシューティングするネットワークポリシーのルールを選択し、詳細ペインで[トラブルシューティング（Troubleshoot）] Troubleshoot をクリックします。 トラブルシューティング ページの値パネルでは、多くのフィールドに、選択したルールの属性が事前に入力されています。

ステップ 4 残りの必要なフィールドに情報を入力します。すべての必須フィールドに入力すると、[パケットトレーサを実行（Run Packet Tracer）] ボタンが有効になります。

ステップ 5 [パケットトレーサを実行（Run Packet Tracer）] をクリックします。

ステップ 6 [パケットトレーサ結果の分析（Analyze Packet Tracer Results）]パケットトレーサ結果の分析 （514 ページ）に進みます。

NAT ルールのトラブルシュート

ステップ 1 [デバイスとサービス] ページから ASA を選択し、[アクション] ペインで [NATルールの表示（View NAT Rules）] View NAT Rules をクリックします。

ステップ 2 トラブルシュートを行うルールを NAT ルールテーブルから選択し、[詳細] ペインで [トラブルシュート（Troubleshoot）] Troubleshoot をクリックします。[トラブルシュート（Troubleshoot）] ページの値パネルでは、多くのフィールドに、選択したルールの属性が事前に入力されています。

ステップ 3 残りの必要なフィールドに情報を入力します。すべての必須フィールドに入力すると、[パケットトレーサを実行（Run Packet Tracer）] が有効になります。

ステップ 4 [パケットトレーサを実行（Run Packet Tracer）] をクリックします。

ステップ 5 [パケットトレーサ結果の分析（Analyze Packet Tracer Results）]パケットトレーサ結果の分析 （514 ページ）に進みます。

Twice NAT ルールのトラブルシュート

ステップ 1 [デバイスとサービス] ページから ASA を選択し、[アクション] ペインで [NATルールの表示（View NAT Rules）] View NAT Rules をクリックします。

ステップ 2 トラブルシュートを行うルールを NAT ルールテーブルから選択し、[詳細] ペインで [トラブルシュート（Troubleshoot）] Troubleshoot をクリックします。双方向の Twice NAT ルールの場合、これによりドロップダウンが開き、ソースパケット変換または宛先パケット変換のトラブルシューティングを選択できます。

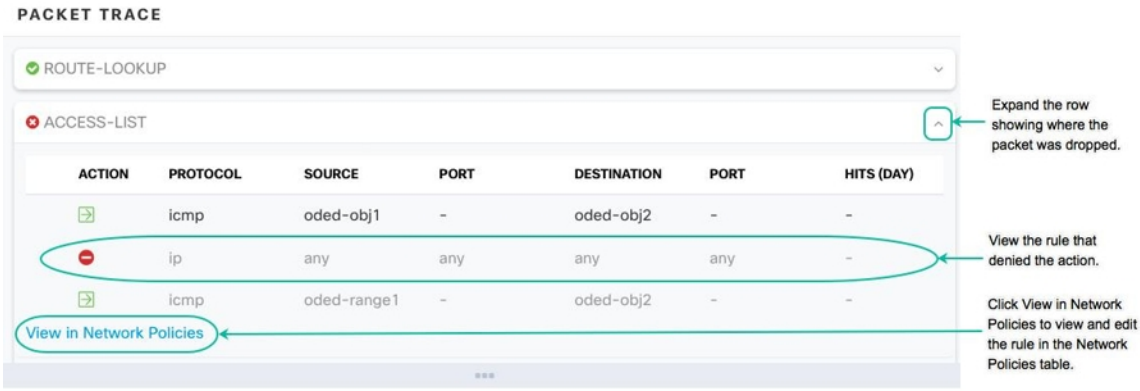
ステップ 3 残りの必要なフィールドに情報を入力します。すべての必須フィールドに入力すると、[パケットトレーサを実行（Run Packet Tracer）] が有効になります。

ステップ 4 [パケットトレーサを実行（Run Packet Tracer）] をクリックします。

パケットトレーサ結果の分析

パケットがドロップされか、許可されたかに関係なく、パケットトレーステーブルの行を展開し、そのアクションに関連するルールまたはロギング情報を読むことで理由を把握できます。以下の例では、パケットトレーサが、任意の送信元から着信して任意の接続先に向かう IP パケットを拒否するルールを含むアクセスリストポリシーを特定しています。このアクションが必要でない場合は、[ネットワークポリシーで表示]リンクをクリックして、そのルールをすぐに編集できます。ルールを編集したら、その構成変更をASAに展開してから、パケットトレーサを再実行して期待どおりのアクセス結果が得られることを確認してください。

パケットトレーサの結果とともに、CDOはASAからのASA リアルタイムロギングを表示します。

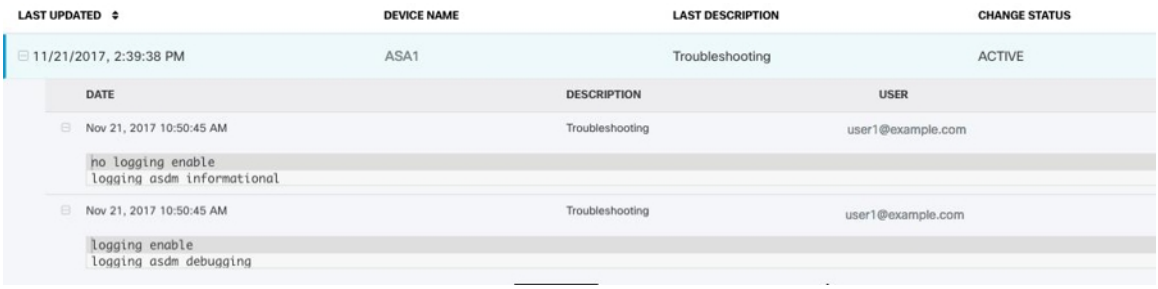


ASA リアルタイムロギング

リアルタイムロギングを使用すると、ログデータの最後の 20 秒またはログデータの最後の 10 KBのうち、先に制限に達した方が表示されます。CDOがリアルタイムデータを取得すると、ASDMの既存のロギング設定を確認し、デバッグレベルのデータを要求するように変更してから、ロギング設定を元の設定に戻します。ロギング CDO の表示には、ASDM で設定したロギングフィルタが反映されます。

変更ログを確認すると、ロギングを実行するためにCDOが送信するコマンドを確認できます。以下は、変更ログエントリの例です。最初のエントリ（下部）は、CDO が logging enable コマンドでロギングを「有効」にし、ASDM ロギングレベルをデバッグに変更したことを示しま

す。2 番目のエントリ（上部）は、ロギングの設定が以前の状態に戻ったことを示します。no logging enable コマンドでロギングが「無効」になり、ASDM ロギングレベルが情報提供に戻りました。



ASA リアルタイムログの表示

ステップ 1 [デバイスとサービス（Devices & Services）] ページで、[デバイス（Devices）] 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、リアルタイムデータを表示するデバイスを選択します。

ステップ 3 [トラブルシューティング（Troubleshoot）] Troubleshoot をクリックします。

ステップ 4 （任意）[リアルタイムログの表示（View Real-time Log）] をクリックする前に、左側のペインでフィルタを定義して、ログ検索の結果を絞り込むことができます。

ステップ 5 [リアルタイムログの表示（View Real-time Log）] をクリックします。CDO は、フィルタ条件に基づいてリアルタイムのログデータを取得して、表示します。

ステップ 6 追加の 20 秒のログデータまたは最後の 10 KB のログデータを表示するには。 [リアルタイムログの表示（View Real-Time Log）] をもう一度クリックします。

Cisco ASA Advisory cisco-sa-20180129-asa1

Cisco Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、ASA および Firepower の重大なセキュリティの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-20180129-asa1 を公開しました。影響を受ける ASA および Firepower のハードウェア、ソフトウェア、および設定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。

ASA がアドバイザリの影響を受けていると判断した場合は、CDO を使用して、パッチが適用されたバージョンに ASA をアップグレードできます。次のプロセスを使用します。

ステップ 1 影響を受ける各 ASA で ASA での DNS の設定。

ステップ 2 アドバイザリに戻って、必要なソフトウェアパッチを決定します。

ステップ 3 CDO を使用して ASA を ASA アドバイザリにリストされている修正済みリリースにアップグレードする方法が説明されているトピックについては、 単一 ASA 上の ASA と ASDM イメージのアップグレード （124

ページ）を参照してください。ASA と ASDM のアップグレードの前提条件から始めて、個々の ASA のアップグレード、アクティブ/スタンバイ設定での ASA のアップグレード、または ASA の一括アップグレードについて参照してください。

参考までに、シスコが報告したセキュリティアドバイザリの概要を以下に示します。

2018 年 2 月 5 日更新：さらなる調査の結果、シスコは、この脆弱性の影響を受ける追加の攻撃ベクトルと機能を特定しました。さらに、元の修正が不完全なことが判明したため、修正された新しいコードバージョンが利用可能になりました。詳細については、「Fixed Software」セクションを参照してください。Cisco 適応型セキュリティアプライアンス（ASA）ソフトウェアの XML パーサーの脆弱性により、認証されていないリモートの攻撃者が、影響を受けるシステムをリロードしたり、コードをリモートで実行したりする可能性があります。また、メモリ不足が原因で、ASA が着信仮想プライベートネットワーク（VPN）の認証要求の処理を停止する可能性もあります。この脆弱性は、悪意のある XML ペイロードを処理する際のメモリの割り当てと解放に関する問題に起因しています。攻撃者は、影響を受けるシステムの脆弱なインターフェイスに巧妙に細工された XML パケットを送信することにより、この脆弱性をエクスプロイトする可能性があります。エクスプロイトにより、攻撃者は任意のコードを実行してシステムの完全な制御を取得し、影響を受けるデバイスのリロードを引き起こしたり、着信 VPN 認証要求の処理を停止したりする可能性があります。脆弱であるためには、ASA は、インターフェイス上でセキュアソケットレイヤ（SSL）サービスまたは IKEv2 リモートアクセス VPN サービスを有効にする必要があります。脆弱性がエクスプロイトされるリスクは、攻撃者がインターフェースにアクセスできるかどうかによっても決まります。脆弱な ASA 機能の包括的なリストについては、「Vulnerable Products」セクションの表を参照してください。この脆弱性に対処するソフトウェア アップデートは、すでに Cisco からリリースされています。この脆弱性の影響を受けるすべての機能に対処する回避策はありません。このアドバイザリは、次のリンク先で確認できます。 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

ASA 実行設定サイズを確認する

実行構成ファイルのサイズを確認するには、次の手順を実行します。

ステップ 1 次のいずれかの方法で、ASA のコマンド ライン インターフェイスにアクセスします。

- ターミナルウィンドウを開き、SSH を使用して ASA にログインします。権限を「特権 EXEC」モードに昇格させます。これにより、表示されるプロンプトが `hostname#` になります。
- ASA の導入準備が完了している場合は、[デバイスとサービス（Devices & Service）]ページを開き、接続するデバイスを選択して、[デバイスアクション] ペインで [>_ コマンド ライン インターフェイス（>_ Command Line Interface）] ボタンをクリックします。詳細については、「単一デバイスで CLI を使用する」を参照してください。

ステップ 2 プロンプトで、`copy running-config flash` と入力します。

ステップ 3 コピー元ファイル名の入力を求められたら、何も入力せずに Enter キーを押します。

ステップ 4 コピー先ファイル名の入力を求められたら、出力ファイルの名前を入力します。指定した実行構成ファイルが ASA によってコピーされると、特権 EXEC プロンプトに戻ります。

ステップ 5 プロンプトで、`show flash` と入力します。

ステップ 6 長さ（length）の列を調べます。ファイルが 4718592 バイトを超えている場合は、4.5 MB を超えています。

コマンドと出力の例を次に示します。

```
asa1# copy running-config flash
Source filename [running-config]?
Destination filename [running-config]? running-config-output
Cryptochecksum: 725f4c1c 4adfb8a9 8b3e7a6d 49e3420d
23648 bytes copied in 1.380 secs (23648 bytes/sec)
asa1# show flash
--#-- --length-- -----date/time------ path
 107 110325428 Feb 28 2019 15:41:42 asdm-8826067.bin
 122 5018592 Apr 30 2019 21:00:59 running-config-output
 111 102647808 Mar 12 2019 14:26:10 asa9-12-1-smp-k8.bin
```

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、修復手順が CDO 運用チームによってすでに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

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 コンテナのブレークアウト

大きな ASA 実行設定ファイル

CDO での現象

ASA が導入準備に失敗する、ASA の実行設定ファイルで定義されているすべての設定が CDO で表示されない、または CDO が変更ログへの書き込みに失敗するといった現象が見られる場合があります。

考えられる原因

ASA の実行設定ファイルが CDO に対して「大きすぎる」可能性があります。

ASA を CDO に導入準備すると、CDO は、そのデータベースに ASA の実行設定ファイルのコピーを保存します。一般に、その実行設定ファイルが大きすぎる（4.5 MB 以上）場合、含まれる行が多すぎる（約 22,000 行）場合、または単一のアクセスグループのアクセスリストエントリが多すぎる場合、CDO は、そのデバイスを予測どおりに管理できません。

実行設定ファイルのサイズを確認するには、「ASA 実行設定サイズを確認する」を参照してください。

回避策または解決策

シスコのアカウントチームに連絡して、セキュリティポリシーを中断することなく設定ファイルのサイズを安全に削減するための支援を得ます。

Secure Device Connector のトラブルシュート

オンプレミスの Secure Device Connector（SDC）のトラブルシュートを行うには、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（520 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が示されます。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。

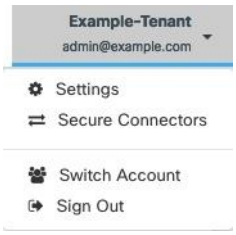
SDC の変更した IP アドレスが CDO に反映されない

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 （517 ページ）
  - カスタム SDC ホストを更新する （518 ページ）
  - バグトラッキング （518 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 コンテナのブレークアウト

Secure Event Connector のトラブルシューティング

いずれのシナリオ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。

SEC オンボーディング失敗のトラブルシューティング

以下のトラブルシューティングのトピックでは、Secure Event Connector（SEC）の導入準備の失敗に関連するさまざまな症状について説明します。

SEC の導入準備に失敗しました

症状：SEC の導入準備に失敗しました。

修復：SEC を取り外して、再度導入準備します。

このエラーが表示された場合：

1. 仮想マシンコンテナから Secure Event Connector の削除します。
2. Secure Device Connector の更新 （21 ページ）。通常、SDC は自動的に更新されるためこの手順を行う必要はありませんが、トラブルシューティングではこの手順が役立ちます。
3. SDC 仮想マシンへの Secure Event Connector のインストール （398 ページ）。

ヒント　SEC を導入準備するときは、常にコピーリンクを使用してブートストラップデータをコピーします。

（注）　この手順で問題が解決しない場合は、イベントロギングのトラブルシューティング ログ ファイルし、マネージド サービス プロバイダーまたは Cisco Technical Assistance Center に連絡してください。

SEC ブートストラップデータが指定されていません

メッセージ：ERROR cannot bootstrap Secure Event Connector, bootstrap data not provided, exiting.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector, bootstrap data not
 provided, exiting.
```

診断：プロンプトが表示されたときに、ブートストラップデータがセットアップスクリプトに入力されませんでした。

修復：導入準備時にブートストラップデータの入力を求められたら、CDO UI で生成された SEC ブートストラップデータを指定します。

ブートストラップ構成ファイルが存在しません

メッセージ：ERROR Cannot bootstrap Secure Event Connector for tenant: <tenant_name>, bootstrap config file ("/usr/local/cdo/es_bootstrapdata") does not exist, exiting.

診断：SEC ブートストラップ データ ファイル（"/usr/local/cdo/es_bootstrapdata"）が存在しません。

修復：CDO UI で生成された SEC ブートストラップデータをファイル **/usr/local/cdo/es_bootstrapdata** に配置し、導入準備を再試行します。

1. 導入準備手順を繰り返します。
2. ブートストラップデータをコピーします。
3. 「sdc」ユーザーとして SEC VM にログインします。
4. CDO UI で生成された SEC ブートストラップデータをファイル **/usr/local/cdo/es_bootstrapdata** に配置し、導入準備を再試行します。

ブートストラップデータのデコードに失敗しました

メッセージ：ERROR cannot bootstrap Secure Event Connector for tenant: <tenant_name>, faile to decode SEC boostrap data, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
base64: invalid input
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
 failed to decode SEC bootstrap data, exiting.
```

診断：ブートストラップデータのデコードに失敗しました

修復：SEC ブートストラップデータを再生成し、導入準備を再試行します。

ブートストラップデータに SEC を導入準備するために必要な情報がありません

メッセージ：

- ERROR cannot bootstrap Secure Event Connector container for tenant: <tenant_name>, SSE_FQDN not set, exiting.
- ERROR cannot bootstrap Secure Event Connector container for tenant: <tenant_name>, SSE_OTP not set, exiting.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
 SSE_FQDN not set, exiting.
```

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
 SSE_FQDN not set, exiting.
```

診断：ブートストラップデータに SEC を導入準備するために必要な情報がありません。

修復：ブートストラップデータを再生成し、導入準備を再試行します。

ツールキット cron が現在実行中

メッセージ：ERROR SEC toolkit already running, exiting.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
 [2020-06-10 04:37:26] ERROR SEC toolkit already running.
```

診断：ツールキット cron が現在実行中です。

修復：導入準備コマンドを再試行します。

十分な CPU とメモリがない

メッセージ：ERROR unable to setup Secure Event Connector, minimum 4 cpus and 8 GB ram required, exiting.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, minimum 4 cpus and
8 GB ram required, exiting.
```

診断：十分な CPU とメモリがありません。

修復：VM の SEC 専用に最低 4 つの CPU と 8 GB の RAM がプロビジョニングされていることを確認し、導入準備を再試行します。

SEC がすでに実行中

メッセージ：ERROR Secure Event Connector already running, execute 'cleanup' before onboarding a new Secure Event Connector, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR Secure Event Connector already running, execute 'cleanup'
before onboarding a new Secure Event Connector, exiting.
```

診断：SEC がすでに実行中です。

修復：新しい SEC を導入準備する前に、SEC クリーンアップコマンドを実行します。

SEC ドメインに到達不能

メッセージ：

- Failed connect to api-sse.cisco.com:443; Connection refused
- ERROR unable to setup Secure Event Connector, domain api-sse.cisco.com unreachable, exiting.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
curl: (7) Failed connect to api-sse.cisco.com:443; Connection refused
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, domain
api-sse.cisco.com unreachable, exiting.
```

診断：SEC ドメインに到達できません。

修復：オンプレミス SDC にインターネット接続があることを確認し、導入準備を再試行します。

導入準備 SEC コマンドはエラーなしで成功しましたが、SEC Docker コンテナが起動していません

症状：導入準備 SEC コマンドはエラーなしで成功しましたが、SEC Docker コンテナが起動していません

診断：導入準備 SEC コマンドはエラーなしで成功しましたが、SEC docker コンテナが起動していません

修復：

1. 「sdc」ユーザーとして SEC にログインします。
2. SEC Docker コンテナの起動ログ（/usr/local/cdo/data/<tenantDir>/event_streamer/logs/startup.log）でエラーがないか確認してください。
3. エラーがある場合は、SEC クリーンアップコマンドを実行して、導入準備を再試行してください。

CDO サポートに連絡する

いずれのシナリオ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。

Secure Event Connector の登録失敗のトラブルシューティング

症状：クラウドイベントサービスへの Cisco Secure Event Connector の登録が失敗します。

診断：SEC がイベントクラウドサービスに登録できない最も一般的な理由は、次のとおりです。

- **SEC が SEC からイベントクラウドサービスに到達できない**

  修復：インターネットがポート 443 でアクセス可能であり、DNS が正しく設定されていることを確認します。

- **SEC ブートストラップデータの無効または期限切れのワンタイムパスワードによる登録の失敗**

  修復：

ステップ 1 「sdc」ユーザーとして SDC にログオンします。

ステップ 2 コネクタログ（/usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log）を表示して、登録状態を確認します。

無効なトークンが原因で登録に失敗した場合は、ログファイルに次のようなエラーメッセージが表示されます。

context:(*contextImpl).handleFailed] registration - CE2001: Registration failed - Failed to register the device because of invalid token. Retry with a new valid token. - Failed"

ステップ 3 SDC VM で SEC クリーンアップコマンド手順を実行して、[セキュアコネクタ（Secure Connectors）] ページから SEC を削除します。

ステップ 4 新しい SEC ブートストラップデータを生成し、SEC 導入準備手順を再試行します。

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ト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。

NSEL データフローのトラブルシューティング

CDO マクロを使用して ASA デバイスの NSEL を設定するしたら、次の手順を使用して、NSEL イベントが ASA から Cisco Cloud に送信されていること、および Cisco Cloud がそれらのイベントを受信していることを確認します。

NSEL イベントを Secure Event Connector（SEC）に送信してから Cisco Cloud に送信するように ASA を設定すると、データはすぐには流れないことに注意してください。ASA で NSEL 関連

のトラフィックが生成されていると仮定すると、最初のNSELパケットが到着するまでに数分かかることがあります。

（注） このワークフローは、「flow-export counters」コマンドと「capture」コマンドを単純に使用してNSELデータフローをトラブルシューティングする方法を示しています。これらのコマンドの使用法の詳細については、CLI ブック 1：Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）[英語] および Cisco ASA NetFlow 実装ガイド [英語] の「Monitoring NSEL」を参照してください。

次のタスクを実行します。

- NetFlow パケットが SEC に送信されていることを確認する
- NetFlow パケットが Cisco Cloud 受信されていることを確認する

イベントロギングのトラブルシューティング ログ ファイル

Secure Event Connector（SEC）の troubleshoot.sh は、すべてのイベントストリーマログを収集して、単一の .tar.gz ファイルに圧縮します。

次の手順を使用して、comparessed.tar.gz ファイルを作成し、ファイルを解凍します。

1. トラブルシューティング スクリプトの実行 （529 ページ）。
2. sec_troubleshoot.tar.gz ファイルの圧縮解除 （530 ページ）。

トラブルシューティング スクリプトの実行

Secure Event Connector（SEC）の troubleshoot.sh は、すべてのイベントストリーマログを収集して、単一の .tar.gz ファイルに圧縮します。次の手順に従って、troubleshoot.sh スクリプトを実行します。

ステップ 1 VM ハイパーバイザを開き、Secure Device Connector（SDC）のコンソールセッションを開始します。

ステップ 2 ログインしてから、[ルート（root）] ユーザーに切り替えます。

```
[cdo@localhost ~]$sudo su root
```

（注） SDCユーザーに切り替える一方でrootとして操作することもできます。その場合、IPテーブルの情報も受信することになります。IPテーブルの情報には、デバイス上でファイアウォールが実行中であることと、すべてのファイアウォールルートが表示されます。ファイアウォールが Secure Event Connector TCP ポートまたはUDPポートをブロックしている場合、[イベントロギング]テーブルにイベントが表示されません。IP テーブルは、そのような状況が発生しているかどうかを判断する際に役立ちます。

ステップ 3 プロンプトで、トラブルシューティング スクリプトを実行し、テナント名を指定します。コマンド構文は次のとおりです。

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_[tenant_name]
```

次に例を示します。

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_example_tenant
```

コマンド出力で、sec_troubleshoot ファイルが SDC の **/tmp/troubleshoot** ディレクトリに保存されていることがわかります。ファイル名は、**sec_troubleshoot-*timestamp*.tar.gz** の表記法に従います。

ステップ 4 ファイルを取得するには、CDO ユーザーとしてログインし、SCP または SFTP を使用してダウンロードします。

次に例を示します。

```
[root@localhost troubleshoot]# scp sec_troubleshoot-timestamp.tar.gz
root@server-ip:/scp/sec_troubleshoot-timestamp.tar.gz
```

次のタスク

sec_troubleshoot.tar.gz ファイルの圧縮解除 （530 ページ） に進みます。

sec_troubleshoot.tar.gz ファイルの圧縮解除

Secure Event Connector（SEC）の トラブルシューティング スクリプトの実行 は、すべてのイベントストリーマログを収集して、単一の sec_troubleshoot.tar.gz ファイルに圧縮します。sec_troubleshoot.tar.gz ファイルの圧縮を解除するには、次の手順を実行します。

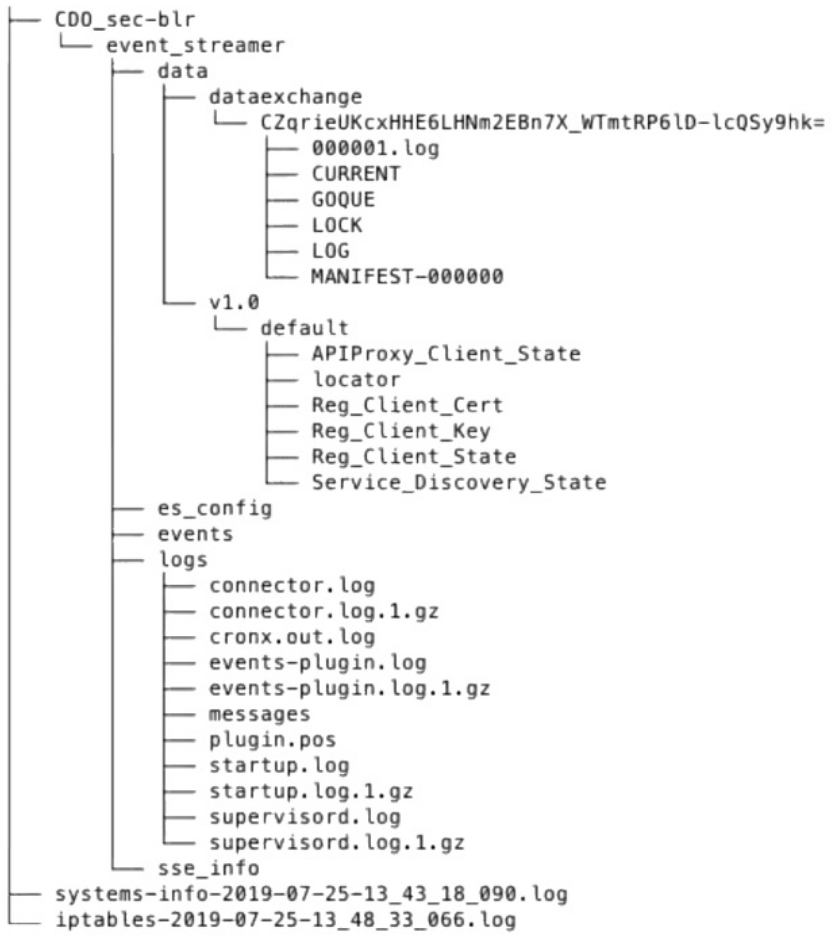
1. VM ハイパーバイザを開き、Secure Device Connector（SDC）のコンソールセッションを開始します。
2. ログインしてから、[ルート（root）] ユーザーに切り替えます。

   ```
   [cdo@localhost ~]$sudo su root
   ```

   （注） **sdc** ユーザーに切り替える一方で root として操作することもできます。その場合、IP テーブルの情報も受信することになります。IP テーブルの情報には、デバイス上でファイアウォールが実行中であることと、すべてのファイアウォールルートが表示されます。ファイアウォールが Secure Event Connector TCP ポートまたは UDP ポートをブロックしている場合、[イベントロギング] テーブルにイベントが表示されません。IP テーブルは、そのような状況が発生しているかどうかを判断する際に役立ちます。
3. プロンプトで、次のコマンドを入力します。

   ```
   [root@localhost ~]$ tar xvf sec_troubleshoot-timestamp.tar.gz
   ```

ログファイルは、テナントにちなんで名付けられたディレクトリに保存されます。これらのタイプのログは、sec_troubelshoot-timestamp.tar.gz ファイルに保存されます。root ユーザーとしてすべてのログファイルを収集した場合は、iptables ファイルが含まれています。



SEC ブートストラップデータの生成に失敗しました。

症状：CDO で SEC ブートストラップデータを生成しているときに、「ブートストラップの生成」ステップでエラーが発生し、次のメッセージが表示されます。「ブートストラップデータの取得中にエラーが発生しました。再試行してください」。

修復：ブートストラップデータの生成を再試行します。それでも失敗する場合は、TAC でサポートチケットを開く。

導入準備後、[CDOセキュアコネクタ（CDO Secure Connectors）]ページで SEC ステータスが [非アクティブ（Inactive）] になる

症状：次のいずれかの理由により、[CDOセキュアコネクタ（CDO Secure Connectors）] ページで Secure Event Connector のステータスが [非アクティブ（Inactive）] と表示されます。

- ハートビートに失敗した
- コネクタの登録に失敗した

修復：

- **ハートビートに失敗した**：SEC ハートビートを要求し、[セキュアコネクタ（Secure Connector）] ページを更新して、ステータスが [アクティブ（Active）] に変わるか確認します。変わらない場合は、Secure Device Connector の登録が失敗していないか確認します。
- **コネクタの登録に失敗した**：「Secure Event Connector の登録失敗のトラブルシューティング」を参照してください。

SEC は「オンライン」ですが、CDO イベントログページにはイベントがありません

症状：Secure Event Connector の CDO セキュアコネクタページには「アクティブ」と表示されているのに、CDO イベントビューアにイベントが表示されません。

解決策または回避策：

ステップ 1 オンプレミス SDC の VM に「sdc」ユーザーとしてログインします。プロンプトで、**sudo su - sdc** と入力します。

ステップ 2 次のチェックを実行します。

- SEC コネクタのログ（/usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log）を確認し、SEC 登録が成功していることを確認します。成功していない場合は、「Secure Event Connector の登録失敗のトラブルシューティング」を参照してください。
- SEC イベントのログ（/usr/local/cdo/data/<tenantDir> /event_streamer/logs/events-plugin.log）を確認し、イベントが処理されていることを確認します。処理されていない場合は、TAC でサポートチケットを開くください。
- SEC Docker コンテナにログインし、コマンド「supervisorctl -c /opt/cssp/data/conf/supervisord.conf」を実行します。出力が以下のようになり、すべてのプロセスが RUNNING 状態であることを確認します。そうでない場合は、TAC でサポートチケットを開くください。

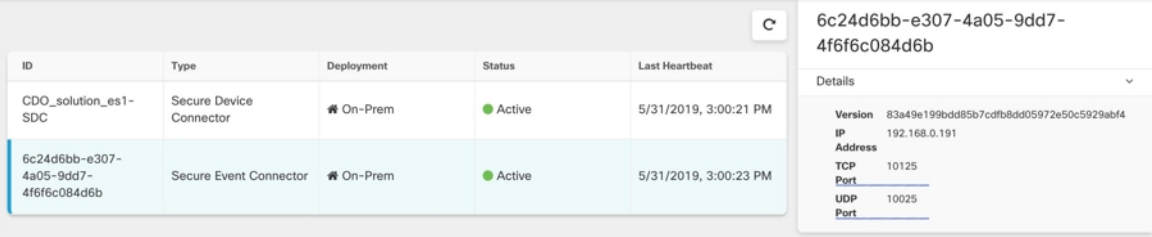
estreamer-connector RUNNING pid 36, uptime 5:25:17

estreamer-cron RUNNING pid 39, uptime 5:25:17

estreamer-plugin RUNNING pid 37, uptime 5:25:17

estreamer-rsyslog RUNNING pid 38, uptime 5:25:17

- オンプレミス SDC のファイアウォール ルールが、[セキュアコネクタ（Secure Connectors）] ページの SEC に表示される UDP および TCP ポートをブロックしていないことを確認します。どのポートを開くかを判断するには、「Secure Logging Analytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。



- 独自の CentOS 7 VM を使用して SDC を手動でセットアップし、ファイアウォールが着信要求をブロックするように設定している場合は、次のコマンドを実行して UDP および TCP ポートのブロックを解除できます。

firewall-cmd --zone=public --add-port=<udp_port>/udp --permanent

firewall-cmd --zone=public --add-port=<tcp_port>/tcp --permanent

firewall-cmd --reload

- 選択した Linux ネットワークツールを使用して、これらのポートでパケットが受信されているかどうかを確認します。受信していない場合は、FTD ロギング設定を再確認してください。

上記のいずれの修復も機能しない場合は、TAC でサポートチケットを開くします。 .

SEC クリーンアップコマンド

Secure Event Connector（SEC）クリーンアップコマンドは、SEC コンテナとその関連ファイルを Secure Device Connector（SDC）VM から削除します。このコマンドは、Secure Event Connector の登録失敗のトラブルシューティング（527 ページ）または導入準備が失敗した場合に実行できます。

このコマンドを実行するには、次の手順を実行します。

始める前に

このタスクを実行するには、自分のテナントの名前を知っている必要があります。テナント名を見つけるには、CDO でユーザーメニューを開き、[設定] をクリックします。ページを下にスクロールして、[テナント名（Tenant Name）] を見つけます。

ステップ 1 「sdc」ユーザーとして SDC にログインします。プロンプトで、`sudo su - sdc` と入力します。

ステップ 2 `/usr/local/cdo/toolkit` ディレクトリに接続します。

ステップ 3 `sec.sh remove`*`tenant_name`* を実行し、SEC を削除することを確認します。

例：

```
 [sdc@localhost~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ
Are you sure you want to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y
```

次のタスク

このコマンドでSECの削除に失敗した場合は、SECクリーンアップコマンドの失敗（534ページ）に進みます。

SEC クリーンアップコマンドの失敗

SEC クリーンアップコマンド（533 ページ） が失敗した場合は、この手順を使用します。

メッセージ：SEC が見つかりません。終了します。

症状：Cleanup SEC コマンドが既存の SEC のクリーンアップに失敗します。

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ Are you sure you want
 to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y [2020-06-10 04:50:42]
 SEC not found, exiting.
```

修復：クリーンアップコマンドが失敗した場合、Secure Event Connector を手動でクリーンアップします。

すでに実行中の SEC docker コンテナを削除します。

ステップ 1 「sdc」ユーザーとして SDC にログインします。プロンプトで、`sudo su - sdc` と入力します。

ステップ 2 **docker ps** コマンドを実行して、SEC コンテナの名前を探します。SEC 名は、"es_*name*" の形式になります。

ステップ 3 **docker stop** コマンドを実行して、SEC コンテナを停止します。

ステップ 4 **rm** コマンドを実行して、SEC コンテナを削除します。

例：

```
$ docker stop <SEC_docker_container_name>
$ docker rm <SEC_docker_container_name>
```

Secure Event Connector の状態を把握するためのヘルスチェックの使用

Secure Event Connector（SEC）のヘルスチェックスクリプトは、SEC の状態に関する情報を提供します。

ヘルスチェックを実行するには、次の手順に従います。

ステップ 1 VM ハイパーバイザを開き、Secure Device Connector（SDC）のコンソールセッションを開始します。

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ます。

```
[cdo@tenant]$sudo su sdc
```

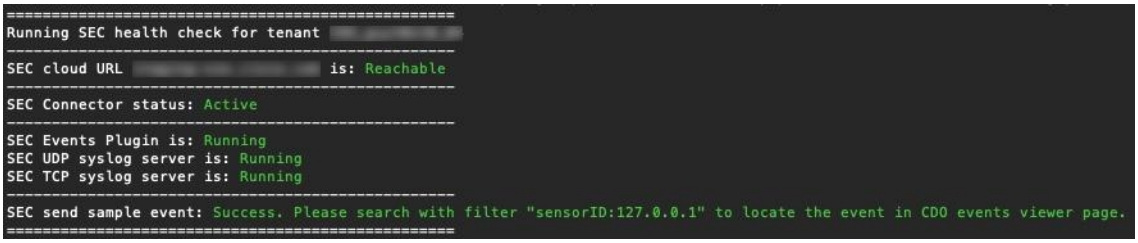
ステップ 4 プロンプトで healthcheck.sh スクリプトを実行し、テナント名を指定します。

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_[tenant_name]
```

次に例を示します。

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_example_tenant
```

スクリプトの出力には、次のような情報が表示されます。



ヘルスチェック出力の値：

- [SECクラウドURL（SEC Cloud URL）]：CDO クラウド URL と、SEC が CDO に到達できるかどうかを表示します。
- [SECコネクタ（SEC Connector）]：SEC コネクタが正しく導入準備され、開始されている場合は、「実行中（Running）」と表示されます。
- [SEC UDP syslogサーバー（SEC UDP syslog server）]：UDP syslog サーバーが UDP イベントを送信する準備ができている場合は、「実行中（Running）」と表示されます。
- [SEC TCP syslogサーバー（SEC TCP syslog server）]：TCP syslog サーバーが TCP イベントを送信する準備ができている場合は、「実行中（Running）」と表示されます。
- [SECコネクタのステータス（SEC Connector status）]：SEC が実行中で、CDO への導入準備が完了している場合は、[アクティブ（Active）] と表示されます。
- [SEC送信サンプルイベント（SEC Send sample event）]：ヘルスチェックの終了時点ですべてのステータスチェックが「緑色」になっている場合、ツールはサンプルイベントを送信します。（いずれかのプロセスが[停止中（Down）]になっている場合、ツールはテストイベントの送信をスキップします）。このサンプルイベントは、「sec-health-check」という名前のポリシーとしてイベントログに表示されます。

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 （63 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

CDO でのユーザーアクセスのトラブルシューティング

ユーザーがアクセスする必要があるリソースへのアクセスを拒否された場合を考えてみましょう。問題を診断して修復するために実行できるアプローチを次に示します。

ステップ 1 ユーザーは、リソースへのアクセスがブロックされていることをセキュリティチームに通知します。そのリソースの通常のアクセス方法を確認します。IP アドレスは何か。特定のポートに到達するか。リソースに情報を送信するために使用されるプロトコルは何か。

ステップ 2 [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。

ステップ 3 [FTD] タブをクリックして ASA を選択し、パケットトレーサを実行します。詳細については、「ASA パケットトレーサ」を参照してください。

ステップ 4 リソースへのアクセスを拒否した可能性のあるルールについて、パケットトレーステーブルを調べます。

ステップ 5 アクセスを拒否しているルールを特定したら、CDO で変更リクエストラベルを作成して有効にします。「変更リクエスト管理 （331 ページ）」を参照してください。これは、リソースへのアクセスを許可するために行った変更ログポリシーの変更を特定するのに役立ちます。

ステップ 6 CDO のルールを編集して、動作を修正します。ASA は CDO と同期していません。

ステップ 7 [デバイスとサービス] ページから ASA に変更を展開します。CDO は、CDO でステージングされた設定ではなく、ASA に保存された設定を通じてパケットをトレースします。CDO でステージングされた他の設定変更も ASA に展開することに注意してください。

ステップ 8 パケットトレーサを再実行して、ポリシーの変更によって望ましい結果が得られるかどうかを判断します。ユーザーがリソースにアクセスできることを確認します。

ステップ 9 ユーザーがアクセスできるようになったと見なして、CDO の変更リクエストラベルをクリアすると、無関係なアクティビティがこの修正に関連付けられないようになります。

（注） 行った変更で問題が解決しないか、新たな問題が発生し、以前の設定に戻したい場合は、ASA の設定を復元できます。「ASA 設定の復元」を参照してください。

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 （322 ページ）

SecurityandAnalyticsLogging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ト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 または認証局ピニング）

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）ピニング」と呼ばれる手法が使用されます。SSL ピニング手法では、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 ピニ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 ピニ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 ピニ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 SSL ALERT メッセージを送信します。アラートは、通常、SSL ピニングを示す「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 （63 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

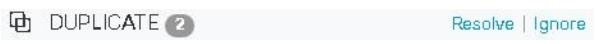
重複オブジェクトの問題の解決

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、オブジェクトをオブジェクトフィルタして、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。



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、変更に問題がなければ[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 （79 ページ）
- CDO へのデバイス一括再接続 （83 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、オブジェクトをオブジェクトフィルタして、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 （308 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、オブジェクトをオブジェクトフィルタして、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 2 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、オブジェクトをオブジェクトフィルタして、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

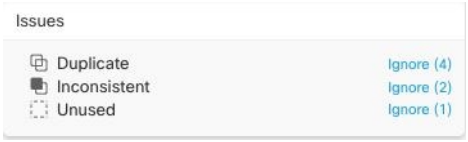
未使用オブジェクトの問題の解決、重複オブジェクトの問題の解決、不整合オブジェクトの問題を解決する （542 ページ）の問題のあるオブジェクトを解決する方法の 1 つは、それらを無視することです。オブジェクトに複数の問題がある場合でも、複数のオブジェクトを選択して無視できます。たとえば、オブジェクトに一貫性がなく、さらに未使用の場合、一度に無視できる問題タイプは 1 つだけです。

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、実行した無視アクションは、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無視し、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無視しても、不整合のオブジェクトとして無視されるわけではありません。

問題を一括で無視するには、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オブジェクトフィルタできます。

ステップ 2 オブジェクトテーブルで、無視す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。



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

ステップ 4 [OK] をクリックして、それらのオブジェクトを無視す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。	ライセンス不足のトラブルシュート （546 ページ）
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。	無効なログイン情報のトラブルシュート （547 ページ）
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。	新規証明書の問題のトラブルシュート （547 ページ）
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。	オンボーディングエラーのトラブルシュート （557ページ）

ライセンス不足のトラブルシュート

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ト

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（322 ページ）

新規証明書の問題のトラブルシュート

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...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/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...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/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-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....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ッ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...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/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...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/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-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+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...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/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なものになります。

```
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 （320 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と、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 privile）」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。

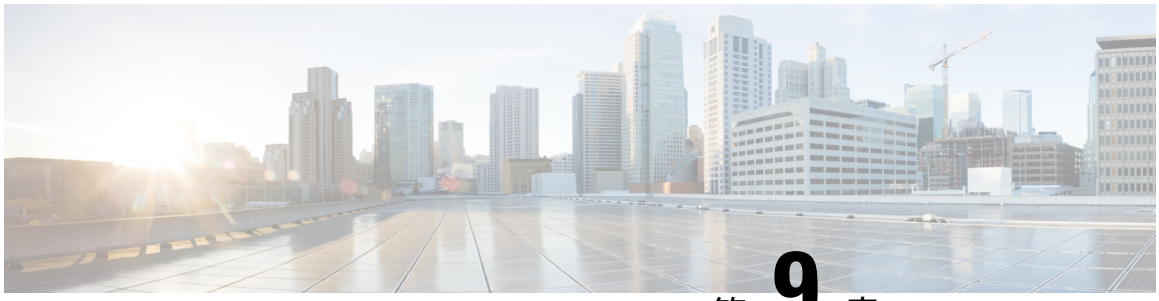
間違ったアカウントでリボンにログインしている

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 9 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

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 （308 ページ）
- CDO から ASA に設定変更を展開します。

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

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

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

CDO が私の証明書を拒否するのはなぜですか？

「新規証明書の問題のトラブルシュート」を参照してください。

ロータッチプロビジョニングで使用される用語と定義

- **要求（Claimed）**：CDO でシリアル番号の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ー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ー問題を特定できます。詳細については、「ASA レガシー ネットワーク ポリシー」を参照してください。

（注） CDO は、完全にシャドー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 deamon>#service docker stop
Change IP address
Start Docker deamon >#service docker start
Restart container on the SDC virtual appliance >bash-4.2$ ./cdo/toolkit/toolkit.sh
restartSDC <tenant-name>
```

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

デバイスの IP アドレスが何らかの理由で変更された場合、それが静的 IP アドレスの変更であるか、DHCP による IP アドレスの変更であるかにかかわらず、CDO がデバイスへの接続に使用する IP アドレスを変更して（CDO のデバイスの IP アドレスを変更する （77 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 （83 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。

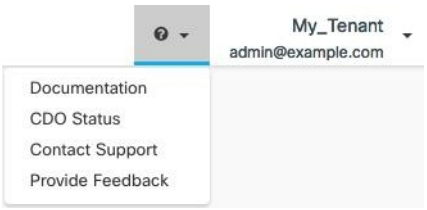
ステップ 5 ページ右上のイベントテーブルの上にある [エクスポート（Export）] ボタンをクリックします。ファイルは、**.json** ファイルとしてローカルに自動的に保存されます。このファイルを、TAC で開いた電子メールまたはチケットに添付します。

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。

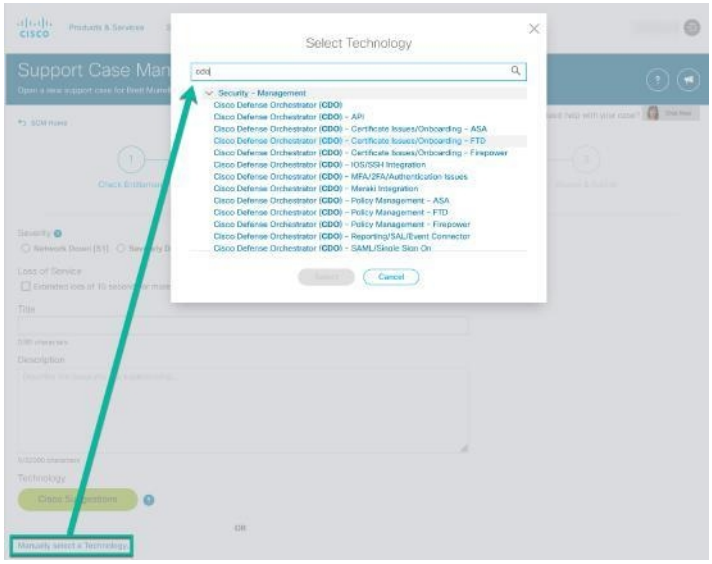
- [製品名（PID）（Product Name (PID)）]：この番号がわからない場合は、『Cisco Defense Orchestrator データシート』を参照してください。
- [製品の説明（Product Description）]：PID の説明です。
- [サイト名（Site Name）]：サイト名を入力します。シスコパートナーがお客様に代わってケースを開いている場合は、お客様の名前を入力します。
- [サービス契約（Service Contract）]：サービス契約番号を入力します。
  - **重要**：ケースを Cisco.com アカウントに関連付けるには、契約番号を 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。