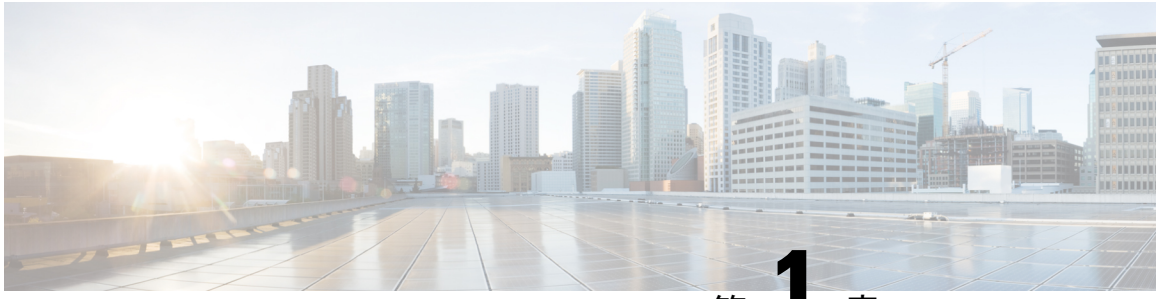
Cisco Defense Orchestrator の新機能

初版：2021 年 4 月 16 日

最終更新：2022 年 6 月 30 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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



第 1 章

2022 の新機能

この章では、2022 年に Cisco Defense Orchestrator に追加された機能の一部について説明します。

2022 年 8 月

2022 年 8 月 4 日

CDO が FDM による管理 デバイスバージョン 7.2 をサポート

CDO が FDM による管理 デバイスのバージョン 7.2 をサポートするようになりました。CDO が提供するサポートの側面は次のとおりです。

- バージョン 7.2 を実行している、サポート対象の物理または仮想 FDM による管理 デバイスの CDO への導入準備。
- バージョン 6.4 以降からバージョン 7.2 への FDM による管理デバイスのアップグレード。
- 既存の Cisco Secure Firewall Threat Defense 機能のサポート。
- バージョン 7.2 を実行している、サポート対象の物理または仮想デバイスの クラウド提供型 Firewall Management Center への導入準備。

（注） CDO は、バージョン 7.2 リリースで導入された機能をサポートしていません。

2022 年 6 月

2022 年 6 月 30 日

Cisco Secure Firewall 移行ツールが Cisco Secure Firewall Threat Defense への移行をサポート

Cisco Secure Firewall 移行ツールを使用すると、Cisco Secure Firewall ASA の設定を Cisco Secure Firewall Threat Defense に移行し、オンプレミスまたは仮想の Cisco Secure Firewall Management Center、あるいは Cisco Defense Orchestrator の新しいクラウド提供型 Firewall Management Center で管理できます。このデスクトップツールは、サードパーティベンダーの Check Point、Palo Alto Networks、および FortiNet からの移行もサポートしています。

Cisco Secure Firewall 移行ツールバージョン 3.0 は、Threat Defense ソフトウェアバージョン 7.2 を実行する Cisco Secure Firewall Threat Defense デバイスへの移行をサポートします。このバージョンの Threat Defense ソフトウェアは、CDO 上のクラウド提供型 Firewall Management Center で管理できます。移行プロセスは CDO の一部であり、CDO ライセンス以外の特定のライセンスは必要ありません。

Cisco Secure Firewall 移行ツールは、ソフトウェアのダウンロードページからダウンロードできます。

CDO には、以下に示す ASA の実行構成の要素を Threat Defense のテンプレートに移行するためのウィザードが用意されています。

- アクセス制御ルール（ACL）
- インターフェイス
- ネットワークアドレス変換（NAT）ルール
- ネットワークオブジェクトとネットワーク グループ オブジェクト
- ルート

ASA 実行構成のこれらの要素が移行されると、新しい脅威防御デバイスに構成を展開し、CDO のクラウド提供型 Firewall Management Center で管理できます。

詳細については、『Migrating ASA Firewall to Cisco Secure Firewall Threat Defense with the Cisco Secure Firewall Migration Tool』[英語] を参照してください。

2022 年 6 月 9 日

クラウド提供型 Firewall Management Center による Cisco Secure Firewall Threat Defense デバイスの管理

Cisco Defense Orchestrator（CDO）がクラウド提供型 Firewall Management Center のプラットフォームになりました。

クラウド提供型 Firewall Management Center は、Cisco Secure Firewall Threat Defense デバイスを管理する Software as a Service（SaaS）製品です。提供する機能の多くはオンプレミス型 Cisco Secure Firewall Management Center と同じです。また、外観や動作もオンプレミス型の Cisco Secure Firewall Management Center と同じであり、同じ FMC API が使用されています。

この製品は、オンプレバージョンの Cisco Secure Firewall Management Center から SaaS バージョンへの移行を希望される Cisco Secure Firewall Management Center のお客様向けに設計されました。

CDO オペレーションチームが、SaaS 製品として維持管理を担当します。新しい機能が導入されると、CDO オペレーションチームが CDO とクラウド提供型 Firewall Manager をお客様に代わって更新します。

お使いのオンプレミス型 Cisco Secure Firewall Management Center に登録されている Cisco Secure Firewall Threat Defense デバイスをクラウド提供型の Firewall Management Center に移行するための移行ウィザードが用意されています。

Cisco Secure Firewall Threat Defense デバイスの導入準備は CDO で実行します。シリアル番号によるデバイスの導入準備といった一般的なプロセスを実行するか、登録キーを含む CLI コマンドを使用します。デバイスの導入準備が完了すると、CDO とクラウド提供型 Firewall Management Center の両方に表示されますが、デバイスの設定はクラウド提供型 Firewall Management Center で行います。バージョン 7.2 以降を実行している Cisco Secure Firewall Threat Defense デバイスの導入準備が可能です。

クラウド提供型 Firewall Management Center のライセンスはデバイスごとに管理されるライセンスであるため、クラウド提供型 FMC 自体のライセンスは不要です。既存の Cisco Secure Firewall Threat Defense デバイスは既存のスマートライセンスを再利用し、新しい Cisco Secure Firewall Threat Defense デバイスは FTD に導入された各機能に対して新しいスマートライセンスをプロビジョニングします。

リモートの分散拠点が展開されている場合、脅威防御デバイスのデータインターフェイスは、デバイス上の管理インターフェイスではなく、Cisco Defense Orchestrator の管理で使用されます。ほとんどのリモート分散拠点には 1 つのインターネット接続しかないため、外部から CDO にアクセスして中央管理を行えるようにします。リモートの分散拠点が展開されている場合、CDO はデータインターフェイスを介して管理対象の脅威防御デバイスに高可用性サポートを提供します。

セキュリティ分析とロギング（SaaS）またはセキュリティ分析とロギング（オンプレミス）を使用して、導入準備した脅威防御デバイスで生成された syslog イベントを分析できます。SaaS バージョンでは、イベントがクラウドに保存され、CDO でイベントを表示します。オンプレミスバージョンでは、イベントがオンプレミスの Cisco Secure Network Analytics アプライアンスに保存され、オンプレミスの Cisco Secure Firewall Management Center で分析されます。どちらの場合も、現在のオンプレミス FMC と同様に、センサーから選択したログコレクタに直接ログを送信できます。

FTD ダッシュボードには、すべての脅威防御デバイスで収集および生成されたイベントデータを含むステータスの概要が表示されます。脅威防御デバイスはクラウド提供型の Firewall Management Center によって管理されます。このダッシュボードを使用して、環境内のデバイスの状態や全体的な正常性に関連する一連の情報を表示できます。FTD ダッシュボードが提供する情報はシステムのライセンス方法、設定方法、展開方法によって異なる点に注意してくだ

さい。FTD ダッシュボードには、CDO で管理されているすべての脅威防御デバイスに関するデータが表示されますが、デバイスベースのデータをフィルタリングすることもできます。また、時間範囲を選択して特定の時間範囲の情報を表示することもできます。

Cisco Secure Dynamic Attributes Connector を使用すると、クラウド提供型 Firewall Management Center のアクセス制御ルールで、さまざまなクラウド サービス プラットフォームのサービス タグとカテゴリを使用できます。ワークロードの動的な性質と IP アドレスの重複の必然性により、IP アドレスなどのネットワーク構造は、仮想、クラウド、およびコンテナ環境では一時的なものです。お客様は、IP アドレスや VLAN が変更されてもファイアウォールポリシーが持続するように、VM 名やセキュリティグループなどの非ネットワーク構造に基づいてポリシールールを定義する必要があります。

1 台以上の管理対象デバイスの **プロキシシーケンス**は、LDAP、Active Directory、または ISE/ISE-PIC サーバーとの通信に使用できます。Cisco Defense Orchestrator（CDO）が Active Directory か ISE/ISE-PIC サーバーと通信できない場合にのみ必要です。たとえば、CDO がパブリッククラウドにある一方、Active Directory または ISE/ISE-PIC がプライベートクラウドにあるといったケースが考えられます。

1 台の管理対象デバイスをプロキシシーケンスとして使用することはできますが、1 台の管理対象デバイスが Active Directory か ISE/ISE-PIC と通信できない場合に別の管理対象デバイスが引き継げるよう、2 台以上設定することを強くお勧めします。

すべてのお客様は、CDO を使用して、Cisco Secure Firewall ASA、Meraki、Cisco IOS デバイス、Cisco Secure Firewall Cloud Native、Umbrella、AWS 仮想プライベートクラウドなどの他のデバイスタイプを管理できます。CDO を使用して、Firepower Device Manager によるローカル管理用に構成された Cisco Secure Firewall Threat Defense デバイスを管理する場合、CDO で引き続き管理できます。CDO を初めて使用する場合は、新しいクラウド提供型の Firewall Management Center および他のすべてのデバイスタイプを使用して、Cisco Secure Firewall Threat Defense デバイスを管理できます。

クラウドで提供型の Firewall Management Center でサポートされている Firewall Management Center 機能の詳細をご覧ください。

- ヘルス モニタリング
- Cisco Secure Firewall Threat Defense デバイスのバックアップ/復元
- スケジューリング
- Import/Export
- アラート応答による外部アラート
- トランスペアレント ファイアウォール モードまたはルーテッド ファイアウォール モード
- Cisco Secure Firewall Threat Defense デバイスの高可用性
- インターフェイス
- ネットワーク アクセス コントロール（NAT）
- 静的ルートとデフォルトルート、およびその他のルーティング設定

- オブジェクト管理および証明書
- リモートアクセス VPN およびサイト間 VPN の設定
- アクセス コントロール ポリシー
- Cisco Secure 動的属性コネクタ
- 侵入検知と防御ポリシー
- ネットワークにおけるマルウェア対策およびファイルポリシー
- 暗号化トラフィックの処理
- ユーザ アイデンティティ
- FlexConfig ポリシー

SecureX を使用した オンプレミス Management Center の導入準備

SecureX アカウントに既に関連付けられているオンプレミス Management Center がある場合は、SecureX を介して Management Center を CDO に導入準備できます。SecureX を介して導入準備したデバイスには、従来の方法で導入準備した Management Center と同等の機能や機能サポートがあります。SecureX を介して Management Center を CDO に導入準備するには、「Onboard an On-Prem FMC with SecureX」[英語] を参照してください。

（注） Management Center アカウントが SecureX に関連付けられている場合でも、Management Center の導入準備を試みる前に、CDO アカウントを SecureX にマージすることを強く推奨します。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。

2022 年 5 月

2022 年 5 月 12 日

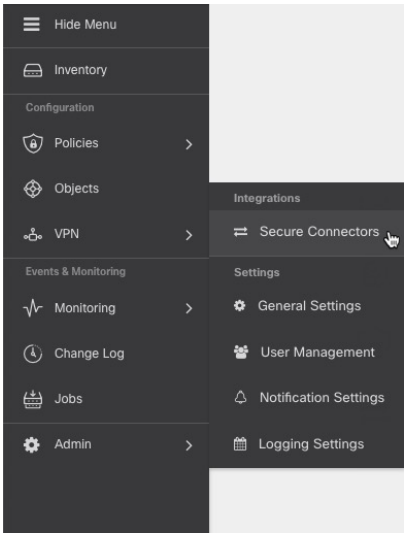
ASA ポリシーで IPv6 をサポート

ASA アクセスポリシーと NAT 設定が、IPv6 アドレスを含むネットワークオブジェクトやネットワークグループを使用したルールをサポートするようになりました。これらのルールでは、ICMP および ICMPv6 プロトコルを指定することもできます。さらに、ASA は IPv6 アドレスを含む AnyConnect 接続プロファイルをサポートするようになりました。詳細については、「ASA Network Policies」[英語] を参照してください。

[セキュアコネクタ（Secure Connectors）] ページへのアクセス

[セキュアコネクタ（Secure Connectors）] ページには、CDO メニューバーからアクセスできます。[セキュアコネクタ（Secure Connectors）] ページを表示するには、**[管理（Admin）] > [セキュアコネクタ（Secure Connectors）]** の順に選択します。

図 *1 : [セキュアコネクタ（Secure Connectors）] メニュー*



2022 年 4 月

2022 年 4 月 14 日

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

CDO が AWS Transit Gateway を使用して AWS VPC トンネルを監視できるようになりました。詳細については、「Monitor AWS VPC tunnels using AWS Transit Gateway」[英語] を参照してください。

2022 年 4 月 6 日

[グローバル検索（Global Search）]

グローバル検索機能を使用すると、CDO 内で使用可能なすべての導入準備済みデバイスと関連オブジェクトを検索できます。検索結果から対応するデバイスやオブジェクトのページに移動できます。

現在、CDO は ASA、Firepower Management Center、Secure Firewall Threat Defense、Meraki、および Cisco Secure Firewall Cloud Native デバイスのグローバル検索をサポートしています。

詳細については、次のドキュメントの「*Global Search*」を参照してください。

- Cisco Defense Orchestrator による ASA の管理
- Cisco Defense Orchestrator を使用した FMC の管理
- Cisco Defense Orchestrator を使用した FTD の管理
- Cisco Defense Orchestrator で Meraki を管理する
- Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator [英語]

Cisco Secure Firewall 3100 のサポート

Cisco Defense Orchestrator は、新しい Cisco Secure Firewall 3100 シリーズ デバイス上で動作する ASA および Secure Firewall Threat Defense デバイスの導入準備をサポートします。

Secure Firewall Threat Defense デバイスは、ロータッチプロビジョニングを使用するか、登録キーまたはシリアル番号を使用して導入準備できます。

2022 年 2 月

2022 年 2 月 3 日

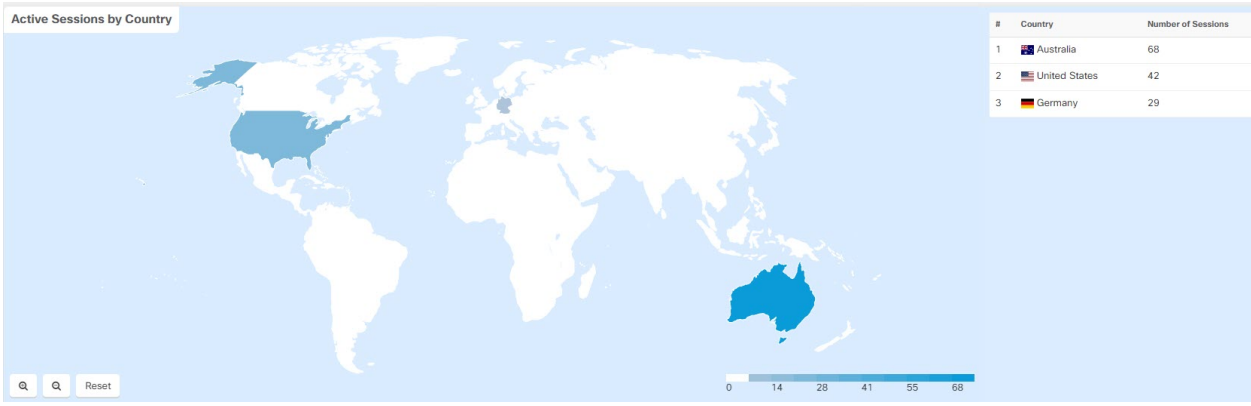
ユーザー管理の Active Directory（AD）グループ

CDO でユーザーを管理する簡単な方法として、個々のユーザーを管理する代わりに、CDO で Active Directory（AD）グループをマップできるようになりました。新しいユーザーの追加、既存のユーザーの削除、ロールの変更などのユーザーの変更は、CDO 内で何も変更せずに Active Directory で実行できるようになりました。CDO は、AD を使用してユーザーごとに複数のロールもサポートするようになりました。詳細については、デバイスの構成ガイドの「**User Management**」の章の「Active Directory Groups in User Management」セクションを参照してください。

アクティブなリモートアクセス VPN セッションのチャートビューの改善

CDO は、アクティブな RA VPN セッションの新しい改善されたチャートビューを提供するようになりました。すでにおなじみのチャートに加えて、CDO は RA VPN ヘッドエンドに接続されているユーザーの場所のヒートマップを表示するようになりました。このマップはライブビューでのみ表示されます。

新しいチャートビューを表示するには、[RA VPN監視（RA VPN Monitoring）] ページで、画面の右上隅に表示される [チャートビューを表示（Show Charts View）] アイコンをクリックします。



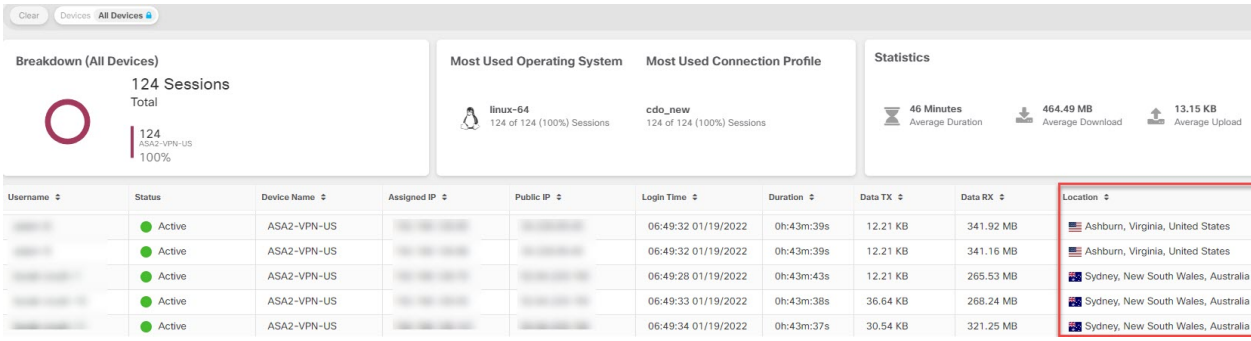
詳細については、ファイアウォールに応じて、『Managing FTD with Cisco Defense Orchestrator』、『Managing ASA with Cisco Defense Orchestrator』、または『Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator』の「Monitoring Remote Access Virtual Private Network Sessions」を参照してください。

2022 年 1 月

2022 年 1 月 20 日

リモートアクセス VPN ユーザーの位置情報

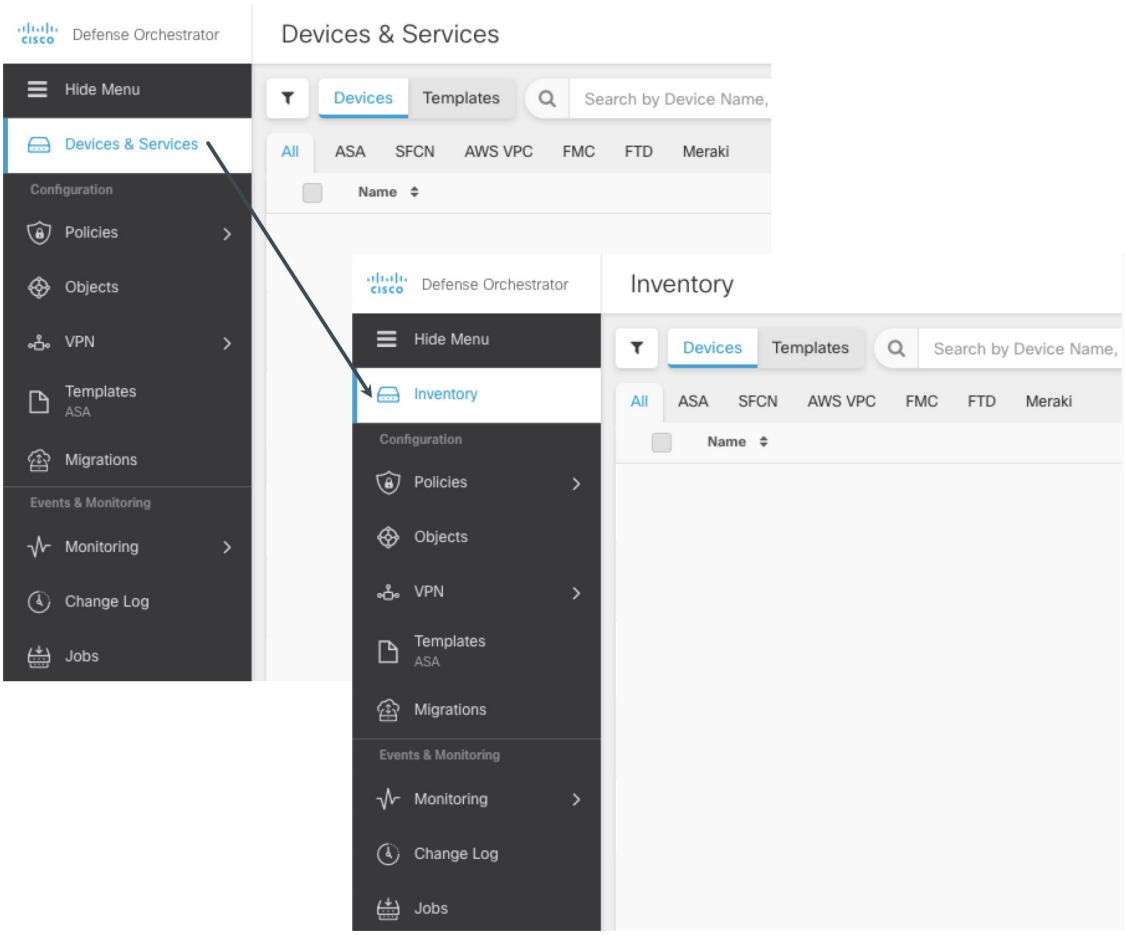
リモートアクセス VPN モニタリングページに、VPN ヘッドエンドに接続しているすべてのユーザーの場所が表示されるようになりました。CDO は、ユーザーのパブリック IP アドレスを地理的に特定することによって、この情報を取得します。この情報は、ライブビューと履歴ビューで利用できます。左ペインの [ユーザーの詳細（User Details）] エリアで場所をクリックすると、ユーザーの正確な場所が地図上に表示されます。



（注） この情報は、新しい CDO の展開後に確立されたユーザーセッションで利用でき、既存のユーザーセッションでは利用できません。

[デバイスとサービス（Devices & Services）] ページの名前を [インベントリ（Inventory）] に変更

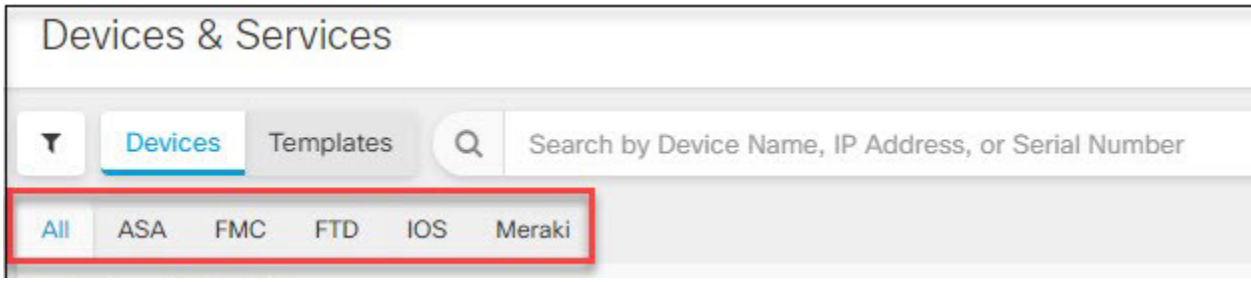
[デバイスとサービス（Devices & Services）] ページの名前が「インベントリ（Inventory）」に変更されました。Inventory テーブルには、CDO で管理するすべてのデバイスとサービスが一覧表示されます。名前の変更の結果として追加または削除された機能はありません。

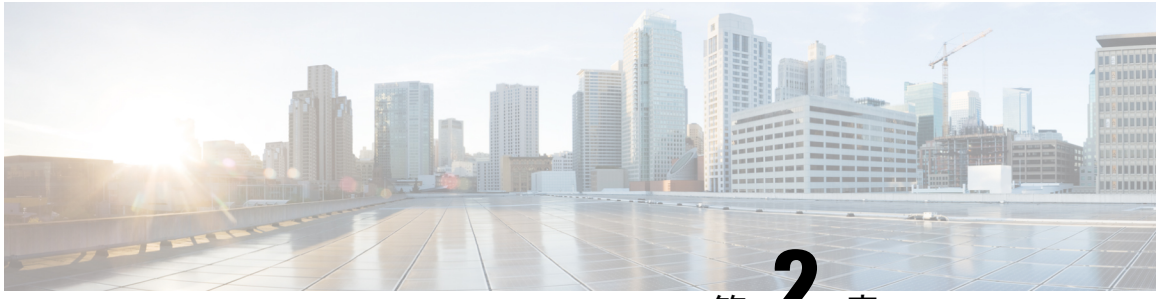


2022 年 1 月 13 日

強化された [デバイスとサービス（Devices & Services）] インターフェイス

CDO [デバイスとサービス（Devices & Services）] インターフェイスは、デバイスとテンプレートをそのタイプに基づいて分類し、各デバイスタイプ専用の対応するタブに表示するようになりました。


Devices & Services
Devices
Templates
Search by Device Name, IP Address, or Serial Number
All
ASA
FMC
FTD
IOS
Meraki



第 2 章

2021 の機能概要

この記事では、2021 年に Cisco Defense Orchestrator に追加された機能の一部について説明します。

2021 年 12 月

2021 年 12 月 9 日

Firepower Threat Defense バージョン 7.1 の CDO サポート

CDO は、Firepower Threat Defense（FTD）バージョン 7.1 デバイスをサポートするようになりました。CDO が提供するサポートの側面は次のとおりです。

- Firepower Threat Defense バージョン 7.1 を実行している、サポート対象の物理デバイスまたは仮想デバイスのオンボード。
- Firepower Threat Defense バージョン 6.4 以降からバージョン 7.1 へのアップグレード。
- 既存の Firepower Threat Defense 機能のサポート。

次の警告は、Firepower Threat Defense バージョン 7.1 のサポートに適用されます。

- CDO は現在、バージョン 7.1 を実行している Firepower Threat Defense デバイスのバックアップをサポートしていません。この機能のサポートは、Firepower Threat Defense バージョン 7.1 の最初のメンテナンスリリースで計画されています。
- CDO は、Firepower Threat Defense バージョン 7.1 リリースで導入された機能をサポートしていません。

CDO が現在サポートしている FTD 機能の詳細については、『Managing FTD with Cisco Defense Orchestrator』を参照してください。

新しい CDO ドキュメンテーション プラットフォーム

オンラインヘルプ

- すべてのデバイスを 1 か所で説明するコンテンツ。
- 状況依存。
- 検索中に見つかったコンテンツの一致。
- 目次で強調表示された検索結果は、より大きなコンテキストで情報を表示します。

Cisco.com で維持されるコンテンツ

- Cisco.com の可用性により、すべての Cisco ドキュメントが 1 つのサイトに配置されます。
- デバイス固有の構成ガイドにより、情報を簡単に見つけることができます。
- Cisco Defense Orchestrator の新機能では、CDO で利用可能な最新の機能について引き続き説明しています。

2021 年 11 月

2021 年 11 月 11 日

新しい SASE トンネル機能

CDO UI に読み込まれた、または作成された SASE トンネルを編集できるようになりました。この機能は、Umbrella 組織と、すでに CDO にオンボードされている ASA ピアデバイスとの間のトンネルのみをサポートすることに注意してください。

詳細については、『Managing an ASA with Cisco Defense Orchestrator』の「Edit a SASE Tunnel」を参照してください。

2021 年 10 月

2021 年 10 月 21 日

SecureX との統合の改善

SecureX を CDO テナントにまだリンクしていないユーザーのために、CDO は SecureX との合理化された統合を提供するようになりました。このプロセスにより、CDOテナントをSecureX組織に迅速かつ安全に接続し、CDO モジュールを 1 回のクリックで SecureX ダッシュボードに追加できます。SecureX 組織がない場合は、このプロセス中に作成できます。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Integrating CDO with SecureX」を参照してください。

CDO リポジトリから AnyConnect パッケージをアップロードする

CDO は、CDO リポジトリから ASA および FTD デバイスへの AnyConnect パッケージのアップロードをサポートするようになりました。

リモートアクセス VPN 設定ウィザードには、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、選択してデバイスにアップロードできます。

詳細については、『Managing FTD with Cisco Defense Orchestrator 』の「Upload an AnyConnect Package from CDO Repository」および『Managing ASA with Cisco Defense Orchestrator』の「Manage AnyConnect Software Packages on ASA Devices」を参照してください。

2021 年 9 月

2021 年 9 月 16 日

サービス統合による CDO 通知

CDO 通知がウェブフックと統合されるようになりました。[通知設定（Notification Settings）] ページで選択した通知は、選択したアプリケーションまたはサービス統合に送信されます。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Enable Service Integrations for CDO Notifications」を参照してください。

Cisco Security Analytics and Logging の Cisco Secure Firewall Cloud Native のサポート

Cisco Security Analytics and Logging が大幅に拡張され、Cisco Secure Firewall Cloud Native からのロギングイベントをサポートするようになりました。

Cisco Secure Firewall Cloud Native のロギング：Security Analytics and Logging（SAL SaaS）は、任意の Cisco Secure Firewall Cloud Native デバイスからのロギングをサポートするようになりました。ユーザーは、Cisco Secure Firewall Cloud Native のイベントを syslog 形式、NetFlow Security Event Logs（NSEL）形式、またはその両方で Cisco Cloud に保存することを選択し、Cisco Secure Cloud Analytics を使用してそれらを分析できます。ロギング分析を有効にしたいお客様は、NSEL ログを有効にして、上位層の SAL ライセンスに必要なテレメトリを提供する必要があります。

- トラフィック分析：Cisco Secure Firewall Cloud Native のログは、SAL のトラフィック分析を通じて実行でき、CDO から Cisco Secure Cloud Analytics を相互起動することによって、監視とアラートを確認できます。syslog イベントのみをログに記録する Cloud Native のお客様は、トラフィック分析を有効にするために NSEL ログに切り替える必要があります。
- Logging Analytics and Detection および Total Network Analytics Detection：Logging Analytics and Detection および Total Network Analytics Detection のライセンスを取得しているお客様は、分析のために Cisco Secure Cloud Analytics ポータルをプロビジョニングして使用できます。Cisco Secure Cloud Analytics の検出には、SAL ユーザーが Cisco Secure Cloud Analytics のコア機能の一部として利用できる他の検出に加えて、ファイアウォール ロギング データを使用して特に有効化された監視とアラートが含まれます。既存の Logging and Troubleshooting のライセンス所有者は、30 日間のコミットメントなしで上位ライセンスの検出機能をテストできます。
- 無料トライアル：このフォームに記入することで、すべてのライセンスに対してコミットメントのない 30 日間の SAL トライアルを開始できます。このトライアルでは、データをクラウドにエクスポートするためのオンプレミスコネクタの最小限のセットのみが必要です。SAL ライセンスの適切な 1 日あたりのボリュームを購入する前段階として、このトライアルを使用して、SAL 機能を評価し、実稼働環境をサポートするために必要なデータボリュームを見積もることができます。この目的のため、SAL トライアルでは、ほとんどのユーザーボリュームのデータを抑制しません。さらに、SAL の 1 日あたりのボリュームを見積もるために見積もりツールが役立ちます。

詳細については、『Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator』の「Cisco Security Analytics and Logging」を参照してください。

2021 年 8 月

2021 年 8 月 26 日

CDO と Umbrella 統合

CDO は、Umbrella 統合をサポートするようになりました。Umbrella 組織をオンボードし、Umbrella と ASA デバイス間に存在する SASE トンネルを表示、管理、および作成できます。ASA デバイスは、使いやすいセキュリティのための集中管理を提供する Umbrella の SIG トンネルと検査を利用します。

Umbrella 組織をオンボーディングするときは、その組織に関連付けられている ASA デバイスもオンボーディングすることをお勧めします。

Umbrella とは何か、および CDO が Umbrella と通信する方法の詳細については、『Managing ASA with Cisco Defense Orchestrator』を参照してください。

2021 年 8 月 13 日

FTD RA VPN の LDAP を使用した Duo 構成のサポート

FTD リモートアクセス VPN 接続に対して LDAP を使用して Duo 二要素認証を設定できるようになりました。

プライマリ認証ソースとしての Microsoft Active Directory（AD）または RADIUS サーバーとともに、セカンダリ認証ソースとして Duo LDAP サーバーを使用します。Duo LDAP を使用すると、セカンダリ認証により、プライマリ認証が Duo パスコード、プッシュ通知、電話コール、または SMS で検証されます。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Duo Two-Factor Authentication using LDAP」を参照してください。

2021 年 7 月

2021 年 7 月 8 日

ASA のデジタル証明書管理サポート

CDO は、ASA デバイスのデジタル証明書を管理するようになりました。ID 証明書や信頼できる CA 証明書などの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、それらを 1 つ以上の管理対象 ASA デバイスにインストールできます。インストールされている ID 証明書をエクスポートして、別の ASA のトラストポイント設定を手動で複製することもできます。

ID 証明書は、次の形式でアップロードまたは作成できます。

- パスフレーズ付きの PKCS12 ファイル
- 自己署名証明書
- 認証局によって署名された証明書署名要求（CSR）

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、ASA および AnyConnect クライア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、『Managing ASA with Cisco Defense Orchestrator』の「ASA Certificate Management」を参照してください。

RA VPN ASA および FTD の AnyConnect モジュールサポート

CDO は、ASA および FTD デバイスでの AnyConnect モジュールの管理をサポートするようになりました。

（注） 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。

RA VPN グループポリシー作成の一部として、ユーザーが Cisco AnyConnect VPN クライアントをダウンロードするときに、さまざまなオプションモジュールをダウンロードしてインストールするように設定できるようになりました。これらのモジュールは、Web セキュリティ、マルウェア保護、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できます。

各モジュールを、AnyConnect プロファイルエディタで作成され、AnyConnect ファイルオブジェクトとして CDO にアップロードされたカスタム設定を含むプロファイルに関連付けることができます。

プロファイルをアップロードしてグループポリシーに割り当てる方法の詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Upload RA VPN AnyConnect Client Profile」と「Create New FTD RA VPN Group Policies」を参照してください。

2021 年 7 月 1 日

Snort 3 のサポート

CDO は、バージョン 6.7 以降を実行している FTD デバイス用の Snort 3 処理エンジンをサポートするようになりました。Snort エンジンは、新しい snort ルールを自動的に更新して、デバイスを最新の脆弱性に準拠させます。Snort 2 から Snort 3 へのスタンドアロン アップグレードを実行するか、デバイスシステムと Snort エンジンを同時にアップグレードして、簡略化されたアップグレード エクスペリエンスを実現できます。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Upgrade to Snort 3.0」を参照してください。

カスタム侵入防御システムポリシー

CDO は、バージョン 6.7 以降を実行している FTD デバイスに対して Snort 3 およびカスタマイズされた侵入防御システム（IPS）ポリシーをサポートするようになりました。改善された Snort 3 処理エンジンにより、Cisco Talos Intelligence Group（Talos）が提供するルールを使用して IPS ポリシーを作成およびカスタマイズできます。ベストプラクティスは、提供されている Talos ポリシーテンプレートに基づいて独自のポリシーを作成し、ルールアクションを調整する必要がある場合はそれを変更することです。

（注） Snort 3 から、または Snort 3 にアップグレードする場合は、ルールの構成方法が変更される可能性があるため、相違点と制限に注意してください。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Custom Firepower Intrusion Prevention System Policy」を参照してください。

2021 年 6 月

2021 年 6 月 17 日

Firepower Threat Defense バージョン 7.0 の CDO サポート

CDO は、Firepower Threat Defense（FTD）7.0 をサポートするようになりました。FTD 7.0 を実行している FTD デバイスをオンボードするか、CDO を使用してデバイスをそのバージョンにアップグレードできます。CDO は、DNS トラフィックでの新しいレピュテーション適用機能に加えて、既存の FTD 機能を引き続きサポートします。この機能は、アクセス制御ポリシー設定です。URL フィルタリングカテゴリとレピュテーションルールを DNS ルックアップ要求に適用するには、このオプションを有効にします。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Configuring Access Policy Settings」を参照してください。

CDO では、次の機能のサポートが制限されています。

- FTDv 階層型ライセンスのサポート：バージョン 7.0 では、スループット要件と RA VPN セッションの制限に基づいて、FTDv デバイスのパフォーマンス階層型のスマートライセンスをサポートするようになりました。現時点では、CDO は階層型スマートライセンスを完全にはサポートしていません。階層型ライセンスを使用する FTDv デバイスをオンボードできますが、CDO を使用してライセンスを更新することはできません。デバイスの Firepower Device Manager を使用して、FTDv でライセンスをインストールおよび管理します。

  詳細については、『Managing FTD with Cisco Defense Orchestrator』の「FTD Licensing」を参照してください。

- スキャンインターフェイスのサポート：Firepower 4100 シリーズまたは 9300 シリーズ デバイスで、Firepower eXtensible Operating System（FXOS）Chassis Manager を使用して Firepower デバイスにインターフェイスを追加する場合は、FDM でそのインターフェイスを構成してから、CDO にデバイスへの「変更をチェック」させて構成を読み込む必要があります。

  詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Synchronizing Interfaces Added to a Firepower Device using FXOS」を参照してください

- 仮想ルータのサポート：VRF ルートは CDO に表示されません。仮想ルートをサポートするデバイスをオンボードできますが、CDO の静的ルーティングページに仮想ルートを表示することはできません。

  詳細については、『Managing FTD with Cisco Defense Orchestrator』の「About Virtual Routing and Forwarding」を参照してください

- 等コスト マルチ パス ルーティング（ECMP）：CDO は、ECMP を使用して構成を読み取るデバイスをオンボードできますが、それらを変更することはできません。FDM を使用して ECMP 構成を作成および変更し、CDO に読み込むことができます。
- ルールセット：ルールセットを FTD 7.0 デバイスに適用することはできません。

（注） CDO が現在サポートしている FTD 機能の詳細については、『Managing FTD with Cisco Defense Orchestrator』を参照してください。

2021 年 6 月 10 日

Cisco Secure Firewall Cloud Native のサポート

CDO は Cisco Secure Firewall Cloud Native をサポートするようになりました。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、スケーラビリティ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。

CDO は、このファイアウォールのオンボーディングを可能にし、完全なファイアウォール管理を提供します。

- AnyConnect RA VPN セッションからのリアルタイムおよび履歴データを表示します。
- オブジェクトを作成および管理し、ネットワークの入力トラフィックと出力トラフィックを処理するさまざまなポリシーでそれらを使用します。
- Kubernetes コマンドラインツールを使用して、CDO の外部でファイアウォールに加えられた変更を認識して調整します。

詳細については、『Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator』を参照してください。

追加情報については、『Cisco Secure Firewall Cloud Native At-a-Glance』も参照してください。

強化されたリモートアクセス VPN モニタリング

ライブ AnyConnect リモートアクセス VPN セッションの監視に加えて、CDO では、過去 3 か月間に記録された AnyConnect リモートアクセス VPN セッションからの履歴データを監視できるようになりました。

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）、Firepower Threat Defense（FTD）、および Cisco Secure Firewall Cloud Native（SFCN）VPN ヘッドエンド全体で VPN セッションを監視できます。

現在のリリースに加えられた主な機能強化の一部を次に示します。

- 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。
- 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。

[VPN] > [リモートアクセスVPNモニタリング（Remote Access VPN Monitoring）] の順にクリックして、ナビゲーションバーから [リモートアクセスVPNモニタリング（Remote Access VPN Monitoring）] 画面を開きます。

新しいユーザ ロール

CDO は、特定のユーザーがテナントごとに VPN セッションを終了できるようにする新しいユーザーロール、VPN セッション マネージャー ユーザー ロールを提供するようになりました。VPNセッションの終了は、このロールが許可する唯一のアクションであることに注意してください。それ以外の場合、このロールで指定されたユーザーは、読み取り専用機能に制限されます。

2021 年 5 月

2021 年 5 月 27 日

CDO のデバイス通知の改善

CDO の電子メールアラートをサブスクライブし、CDO UI 内で最近の通知を表示できるようになりました。

テナントに関連付けられたデバイスでワークフローまたはイベントの変更が発生したときに、電子メールアラートを受信します。ワークフローの変更には、展開、アップグレード、または

バックアップが含まれます。イベントの変更には、オンラインまたはオフラインになるデバイス、競合検出、HA またはフェールオーバーの状態、サイト間 VPN 接続の状態が含まれます。

（注） これらのカスタマイズ可能な通知とアラートは、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、デバイス固有ではありません。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Notifcations Settings」を参照してください。

2021 年 3 月

2021 年 3 月 25 日

APJC における Cisco Security Analytics and Logging の可用性

Cisco Security Analytics and Logging は、新たに委託された東京データストアを通じてアジア（APJC）リージョンで利用できるようになりました。Security Analytics が有効なアカウントは、オーストラリアのシドニーにある Cisco Secure Cloud Analytics サービスにアクセスして、セキュリティ関連のアラートを利用できます。これにより、アジアリージョンは、南北アメリカおよび EU リージョンで利用可能な機能と同等になりました。

詳細については、『Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator』の「Cisco Security Analytics and Logging」を参照してください

2021 年 3 月 18 日

EtherChannel インターフェイスのサポート

CDO は、Firepower 1010、1120、1140、1150、2110、2120、2130、2140 など、Firepower バージョン 6.5 以降を実行しているサポート対象モデルで EtherChannel インターフェイス構成をサポートするようになりました。EtherChannel は、複数の物理イーサネットリンクのグループを作成し、スイッチ、ルータ、およびサーバー間にリンクを提供するための 1 つの論理イーサネットリンクを作成できるポート リンク アグリゲーション技術またはポートチャネル アーキテクチャです。

LAN ポートに適用した設定は、設定を適用した物理ポートだけに作用することに注意してください。

デバイスのサポートと設定の制限の詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Guidelines and Limitations for Firepower Interface Configuration」を参照してください。

2021 年 3 月 15 日

ASA リモートアクセス VPN のサポート

CDO では、適応型セキュリティアプライアンス（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）設定を作成して、リモートユーザーが ASA に接続してリモートネットワークに安全にアクセスできるようになりました。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。

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

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Configuring Remote Access VPN for an ASA」を参照してください。

ASA ファイル管理のサポート

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のファイル管理ツールを提供します。このツールを使用すると、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を使用して、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。

このツールは、新しくリリースされた AnyConnect イメージを複数の ASA デバイスに同時にアップロードするのに役立ちます。

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「ASA File Management」を参照してください。

2021 年 2 月

2021 年 2 月 11 日

複数の Secure Device Connector のサポート

テナントに複数のオンプレミスの Secure Device Connector（SDC）を展開できるようになりました。これにより、より多くのデバイスを CDO で管理し、CDO、SDC、および管理対象デバイス間の通信パフォーマンスを維持できます。

管理対象の ASA、AWS VPC、および Meraki MX デバイスを 1 つの SDC から別の SDC に移動できます。

複数の SDC を使用すると、1 つの CDO テナントを使用して、隔離されたネットワークセグメント内のデバイスを管理することもできます。これを行うには、隔離されたネットワークセグメント内のすべての管理対象デバイスを 1 つの SDC に割り当てます。

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Using Multiple SDCs on a Single CDO Tenant」を参照してください。

2021 年 1 月

2021 年 1 月 21 日

FMC オブジェクトの読み取り

FMC を CDO にオンボードすると、CDO は FMC 管理の FTD デバイスからオブジェクトをインポートするようになりました。CDO にインポートされると、オブジェクトは読み取り専用になります。FMC オブジェクトは読み取り専用ですが、CDO を使用すると、FMC によって管理されていないテナント上の他のデバイスにオブジェクトのコピーを適用できます。コピーは元のオブジェクトとの関連付けが解除されるため、FMC からインポートされたオブジェクトの値を変更せずにコピーを編集できます。FMC オブジェクトは、そのオブジェクトタイプをサポートする管理対象の任意のデバイスで使用できます。

詳細については、『Managing FMC with Cisco Defense Orchestrator』の「FMC Objects」を参照してください

2021 年 1 月 14 日

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。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Export CLI Command Results」を参照してください。

FTD デバイスのクラウドサービスの設定

Cisco Success Network への接続と、Cisco Cloud に送信されるイベントの設定は、ソフトウェアバージョン 6.6 以降を実行している FTD デバイスで設定できる機能です。

Cisco Success Network

Cisco Success Network を有効にすることで、使用情報と統計をシスコに提供して FTD を改善し、ネットワーク内のシスコ製品の価値を最大化するのに役立つ未使用または追加の機能を認識できるようにします。Cisco Success Network を有効にすると、デバイスは Cisco Cloud への安全な接続を確立し、この安全な接続を常に維持します。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Connecting to the Cisco Success Network」を参照してください。

Cisco Cloud にイベントを直接送信する

FTD から Cisco Cloud に直接送信するイベントのタイプを指定できるようになりました。Cisco Cloud に保存すると、Cisco Threat Response などのクラウドアプリケーションを使用して、イベントを分析したり、デバイスが遭遇した可能性のある脅威を評価したりできます。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Sending Events to the Cisco Cloud」を参照してください。

Web 分析

Web分析を有効にすると、ページのヒット数に基づいて匿名の製品使用情報をシスコに提供できます。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。CDO を使用して、FTD のすべてのバージョンでこの機能を設定できます。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Enabling or Disabling Web Analytics」を参照してください。

2021 年 1 月 7 日

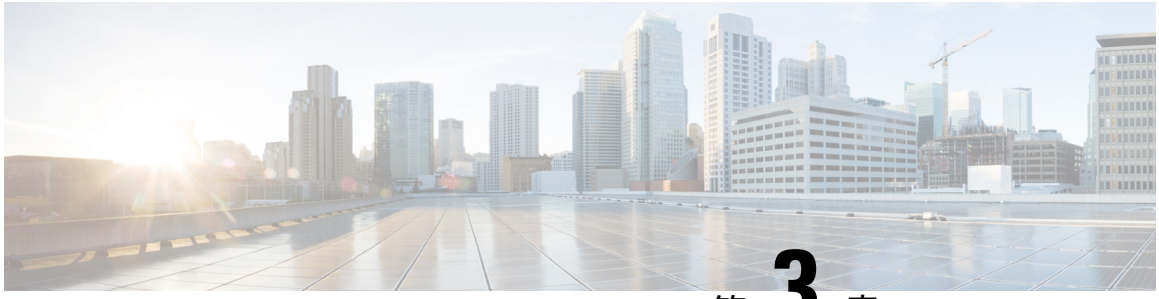
FTD HA ペアのオンボーディング

CDOは、FTDHAペアのオンボーディングのプロセスを強化しました。登録トークン方式またはログイン情報方式のいずれかを使用して HA ピアの 1 つをオンボードすると、対応するピアがまだオンボードされていないことが CDO によって自動的に検出され、アクションを実行するように求められます。この改善により、両方のデバイスのオンボードに必要な労力が最小限に抑えられ、ピアデバイスのオンボードにかかる時間が短縮され、最初のデバイスのオンボードに使用した登録キーまたはスマートライセンストークンが再利用されます。

アクティブデバイスまたはスタンバイデバイスのいずれかをオンボードでき、同期されると、CDO は常にデバイスが HA ペアの一部であることを検出します。

（注） 登録キー方式を使用して FTD デバイスをオンボードすることを強くお勧めします。

FTD HA ペアのオンボーディングの詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Onboard an FTD HA Pair with a Registration Key」または「Onboard an FTD HA Pair using Username Password and IP Address」を参照してください。



第 3 章

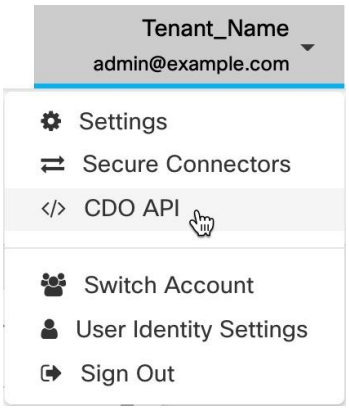
2020 の機能概要

2020 年 12 月

2020 年 12 月 17 日

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、詳細で軽く読める公式ガイド（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（docs）] タブをクリックするだけです。

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。

2020 年 12 月 10 日

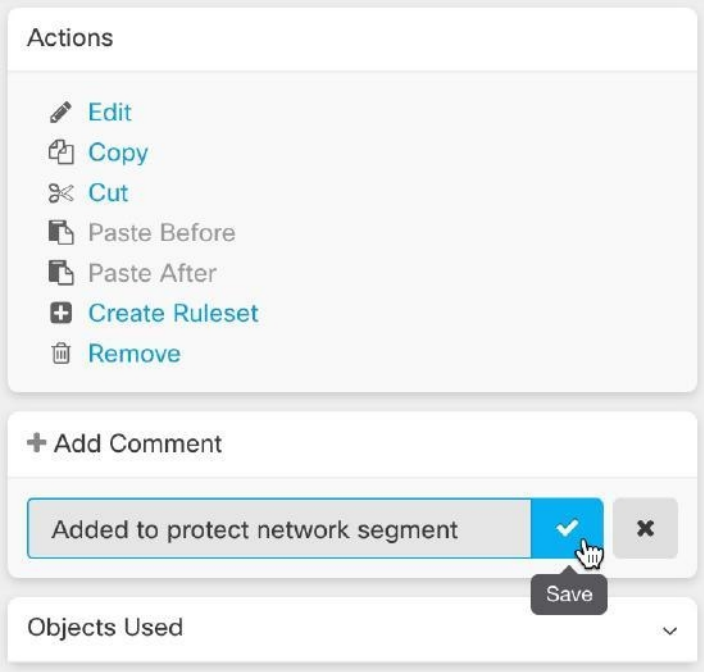
FTD 設定のエクスポート

FTDデバイスの完全な構成をCDOで読み取り可能なJSONファイルとしてエクスポートできるようになりました。このファイルは、管理する任意のCDOテナントにFTDモデル（FTDテンプレート）としてインポートできます。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Export FTD Configuration」を参照してください。

FTD ルールへのコメントの追加

FTDポリシーとルールセットのルールにコメントを追加できるようになりました。ルールコメントはCDOでのみ表示されます。FTDに書き込まれず、FDMに表示されません。



詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Adding Comments to Rules in FTD Policies and Rulesets」を参照してください。

2020 年 11 月

2020 年 11 月 13 日

ロータッチプロビジョニングとシリアル番号のオンボーディング

ロータッチプロビジョニングは、FTD ソフトウェアバージョン 6.7 以降を実行している工場出荷または再イメージ化された新しい Firepower 1000 または 2100 シリーズ デバイスで、ネットワークに接続し、CDO に自動的にオンボーディングしてから、リモートで設定することを可能にする機能です。これにより、CDO へのデバイスのオンボーディングに関連する多くの手動タスクがなくなります。ロータッチ プロビジョニング プロセスにより、物理デバイスにログインする必要性が最小限に抑えられます。これは、従業員がネットワークデバイスの操作に慣れていないリモートオフィスやその他の場所を対象としています。

工場出荷時に FTD 6.7 イメージがインストールされた Firepower 1000 および 2100 シリーズ デバイスは、2020 年の終わりまたは 2021 年の初めに、シスコから注文可能になる予定です。

また、構成済みの Firepower Threat Defense（FTD）バージョン 6.7 以降のデバイスを FTD 6.7 に、デバイスのシリアル番号を使用して CDO にオンボードすることもできます。

詳細については、次の記事を参照してください。

- Low Touch Provisioning

- Onboading a FTD 6.7 Device with its Serial Number
- Firepower Easy Deployment Guide for Cisco Firepower 1000 or 2100 Firewalls

セキュリティゾーンへの Firepower Threat Defense インターフェイスの割り当て

セキュリティゾーンに FTD インターフェイスを割り当てて、トラフィックをさらに分類および管理できるようになりました。詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Assign a Firepower Interface to a Security Zone」を参照してください。

2020 年 11 月 6 日

Firepower Threat Defense バージョン 6.6.1 および 6.7 の CDO サポート

CDO は、Firepower Threat Defense（FTD）バージョン 6.6.1 および 6.7 をサポートするようになりました。FTD 6.6.1 または 6.7 を実行している新しい FTD デバイスをオンボードするか、CDO を使用してそれらのバージョンにアップグレードできます。CDO は、既存の FTD 機能と次の新しい FTD 6.7 機能を引き続きサポートします。

- セキュリティグループタグと SGT グループ
- Active Directory レルムオブジェクト

CDO が現在サポートしている FTD 機能の詳細については、『Managing FTD with Cisco Defense Orchestrator』を参照してください。

バージョン 6.7 の CDO TLS サーバー ID ディスカバリおよび TLS 1.3

サーバー証明書からの情報を使用して、TLS 1.3 で暗号化されたトラフィックの URL フィルタリングとアプリケーション制御を実行できるようになりました。この機能が動作するためにトラフィックを復号化する必要はありません。TLS 1.3 で暗号化されたトラフィックで、アプリケーションまたは URL フィルタリングを使用するアクセスルールに対応するには、システムが TLS 1.3 証明書を復号する必要があります。暗号化された接続が適切なアクセス制御ルールに適合するように、Firepower Device Manager（FDM）または Firepower Management Center（FMC）のいずれであっても、管理 UI で [TLSサーバーアイデンティティ検出（TLS Server Identity Discovery）] を有効にすることを推奨します。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「TLS Server Identity Discovery in Firepower Threat Defense」を参照してください。

2020 年 10 月

2020 年 10 月 15 日

新しいユーザーロール

CDO は、ポリシーの編集とポリシーの展開の責任を分割する 2 つの追加のユーザーロールを提供するようになりました。新しい**編集専用**ロールでは、ユーザーはデバイスの構成を変更できますが、それらの変更を展開することはできません。新しい**展開専用**ロールでは、ユーザーは保留中の構成変更を展開できますが、構成を変更することはできません。

詳細については、『*Managing FMC with Cisco Defense Orchestrator*』の「User Roles」を参照してください。

2020 年 10 月 2 日

FTD API のサポート

CDO は、FTD デバイスで高度なアクションを実行するための Representational State Transfer（REST）アプリケーション プログラミング インターフェイス（API）要求を実行するための API ツールインターフェイスを提供するようになりました。さらに、このインターフェイスは次の機能を提供します。

- 実行済みの API コマンドの履歴を記録します。
- 再利用できるシステム定義の API マクロを提供します。
- 標準 API マクロを使用して、すでに実行したコマンドから、または別のユーザー定義マクロからユーザー定義 API マクロを作成できます。

FTD API ツールの詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Using FTD API Tool」を参照してください。

2020 年 9 月

2020 年 9 月 25 日

マルチテナントポータルのサポート

CDO は、さまざまな地域のテナントからのデバイスの統合されたビューを提供するマルチテナントポータルを導入するようになりました。このビューは、単一のウィンドウでテナントか

ら情報を収集するのに役立ちます。CDO サポートチームに、要件に基づいて 1 つ以上のポータルを作成させることができます。

- 次の情報を提供する [デバイスの詳細（Device Details）] ビューを提供します。
  - デバイスの場所、ソフトウェアバージョン、オンボーディング方法など、各デバイスの詳細を表示します。
  - デバイスを所有する CDO テナントページでデバイスを管理できます。
  - 別の地域の CDO テナントにサインインし、そのデバイスを管理するためのリンクを提供します。
- ポータルの情報をコンマ区切り値（.csv）ファイルにエクスポートして、分析するか、アクセス権のないユーザーに送信します。
- API トークンを使用して、新しいテナントをシームレスに追加できます。
- CDO からサインアウトせずにポータルを切り替えることができます。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Manage Multi-Tenant Portal」を参照してください。

クラウドベースの Secure Device Connector に対する Secure Event Connector のサポート

Cisco Security Analytics and Logging（SAL SaaS）のお客様は、Secure Device Connector が Cisco Cloud にインストールされている場合に、Secure Event Connector をインストールできるようになりました。Cisco Security Analytics and Logging を構成するために、オンプレミスの Secure Device Connector に切り替える必要がなくなりました。

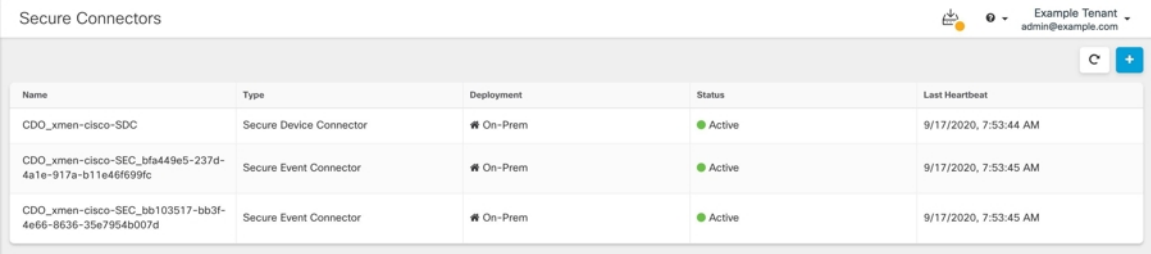
詳細については、『Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator』の次のトピックを参照してください。

- Installing Secure Event Connectors
- Installing SECs, Using CDO Images, on Tenants with Cloud SDCs
- Installing SECs, Using Your VM Image, on Tenants with Cloud SDCs

2020 年 9 月 17 日

複数のセキュアイベントコネクタのサポート

Secure Event Connector（SEC）は、ASA および FTD から Cisco Cloud にイベントを転送します。これにより、Cisco Security Analytics and Logging（SAL SaaS）ライセンスに応じて、[イベントロギング（Event Logging）] ページでイベントを表示し、Secure Cloud Analytics で調査できます。複数の SEC を使用すると、それらをさまざまな場所にインストールし、イベントを Cisco Cloud に送信する作業を分散できます。



テナントに追加の SEC をインストールする方法については、次の記事を参照してください。

- Installing Multiple SECs, Using CDO Images, on Tenants with On-Premises SDCs
- Install Multiple SECs Using Your VM Image

詳細については、『Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator』の「Cisco Security Analytics and Logging」を参照してください。

2020 年 8 月

2020 年 8 月 20 日

Firepower Management Center のサポート

CDO は、バージョン 6.4 以降を実行している Firepower Management Center（FMC）とそのすべての管理対象デバイスをオンボードできるようになりました。FMC のサポートは、FMC のオンボーディング、それが管理するデバイスの表示、および FMC UI へのクロス起動に限定されています。

CDO が FMC アプライアンスを管理する方法を確認するには、『Managing FMC with Cisco Defense Orchestrator』を参照してください。

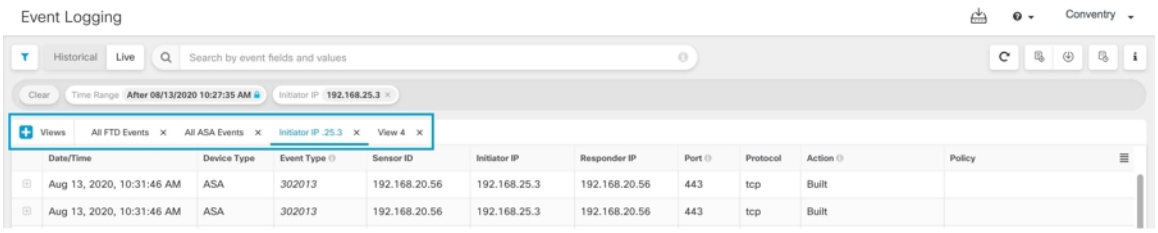
FMC のオンボーディングについては、『Managing FMC with Cisco Defense Orchestrator』の「Onboard an FMC」を参照してください。

サポート対象の FMC ハードウェアとソフトウェアのバージョンを確認するには、『Managing FMC with Cisco Defense Orchestrator』の「Software and Hardware Support by CDO」を参照してください。

カスタマイズ可能なイベントフィルタ

Cisco Security Analytics and Logging（SAL SaaS）のお客様は、[イベントロギング（Event Logging）]ページでカスタマイズしたイベントフィルタを作成して保存し、繰り返し使用することができます。

詳細については、『Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator』の「Customizable Event Filters」を参照してください。



[イベントロギング（Event Logging）] ページの検索機能の改善

Cisco Security Analytics and Logging（SAL SaaS）のお客様は、[イベントロギング（Event Logging）] ページで改善された次の検索機能を使用できます。

- 要素の属性をクリックして、検索フィールドに追加します。
- [イベントロギング（Event Logging）] ページで列をドラッグアンドドロップして、希望する方法でイベント情報を表示します。
- [イベントロギング（Event Logging）] ページの新しい AND NOT および OR NOT 検索演算子により、より詳細なイベント検索機能が提供されます。

詳細については、『Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator』の「Searching for and Filtering Events in the Event Logging」を参照してください。

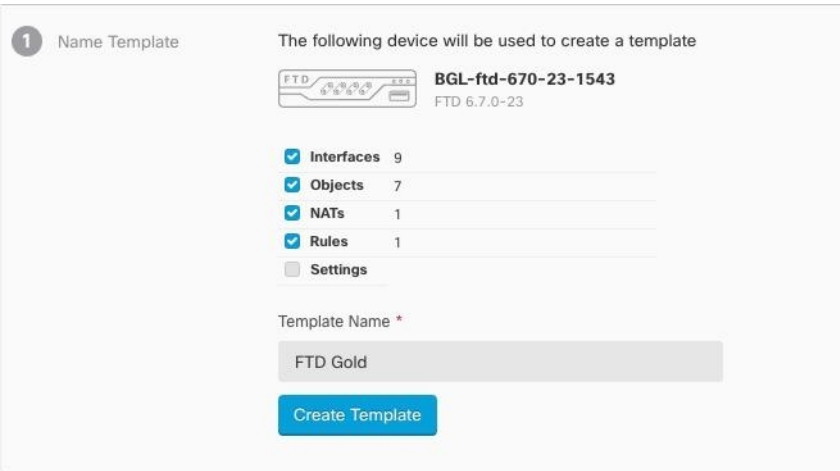
2020 年 8 月 13 日

カスタム競合検出ポーリング間隔

デバイスタイプや以前に構成されたポーリング間隔に関係なく、デバイスごとにカスタムポーリング間隔を構成できるようになりました。これには、デバイスの状態の検出や、検出されたアウトオブバンドの変更が含まれます。詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Schedule Polling for Device Changes」を参照してください。

カスタム FTD テンプレート

オンボード FTD デバイスの構成の 1 つ以上の部分（アクセスルール、NAT ルール、設定、インターフェイス、およびオブジェクト）を選択することで、カスタム FTD テンプレートを作成できるようになりました。カスタムテンプレートを他の FTD に適用すると、含まれる部分に基づいて既存の構成が保持、更新、または削除されます。ただし、CDO では引き続き、すべての部分を選択して完全なテンプレートを作成し、それを他の FTD に適用することができます。詳細については、『Managing FTD with Cisco Defense Orchestrator』の「FTD Templates」を参照してください。



2020 年 7 月

2020 年 7 月 30 日

オブジェクトのオーバーライド

CDO は、システムが指定したデバイスに使用する共有ネットワークオブジェクトの代替値を提供できる「オブジェクトのオーバーライド」を導入しています。これにより、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。オブジェクトのオーバーライドを使用すると、共有ポリシーまたはルールセットでオブジェクトを使用する一部またはすべてのデバイスでオーバーライドできるオブジェクトを作成できます。

オブジェクトをオーバーライドするには、『Managing FTD with Cisco Defense Orchestrator』の「Object Overrides」を参照してください。

ネットワーク グループ ウィザードの改善

ネットワークグループ編集ウィザードが改善され、新しいネットワークオブジェクトを即座に作成し、既存のネットワークオブジェクトを変更できるようになりました。また、共有ネット

ワークグループが定義されているデバイスにデバイス固有の追加値を追加することもできます。

ネットワーク グループ ウィザードに加えられた改善の詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Create or Edit a Firepower Network Object or Network Group」および「Create or Edit ASA Network Objects and Network Groups」を参照してください。

2020 年 7 月 9 日

RA VPN およびイベントビューのカスタマイズ

リモートアクセス仮想プライベートネットワーク（RA VPN）用に生成されたテーブル、およびライブイベントビューと履歴イベントビューの両方をカスタマイズできるようになりました。ニーズとポートフォリオにとって重要なものに最も適した方法でテーブルを整理して保存します。

カスタマイズに関連する詳細については、『Managing FTD with Cisco Defense Orchestrator』の次のセクションを参照してください。

- Customize the Remote Access VPN Monitoring View
- Viewing Historical Events in CDO

2020 年 7 月 2 日

SecureX

CDO を SecureX に組み込むことができるようになりました。これにより、デバイス、ポリシー、およびテナントごとに適用されるオブジェクトの要約が提供され、セキュリティポートフォリオ全体の可視性と自動化が強化されます。CDO と SecureX を組み込む方法の詳細については、「SecureX」を参照してください。

詳細については、『Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator』の次のトピックを参照してください。

- SecureX and CDO
- Connect SecureX in CDO

Cisco Security Analytics and Logging（SAL SaaS）のイベントのダウンロード

[イベントロギング（Event Logging）] ページで ASA および FTD イベントをフィルタリングした後、結果を圧縮された .CSV ファイルでダウンロードできるようになりました。

- ダウンロード可能な .CSV ファイルに追加するイベントは、時間範囲によって定義されます。
- 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 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 ファイルは 7 日間保存され、その後削除されます。

詳細については、『Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator』の「Downloading Events」を参照してください。

2020 年 6 月

2020 年 6 月 18 日

Firepower Threat Defense エグゼクティブサマリーのサポート

オンボードの Firepower Threat Defense（FTD）デバイスのいずれかまたはすべてについて、カスタムのエグゼクティブ サマリー レポートを生成できるようになりました。このレポートには、暗号化されたトラフィック、傍受された脅威、検出された Web カテゴリなどの運用統計のコレクションが表示されます。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の次のトピックを参照してください。

- FTD Executive Summary Report
- Managing Reports

Cisco Security Analytics and Logging の改善点

ASA Syslog および NSEL イベントのサポート

Cisco Security Analytics and Logging が大幅に拡張され、ASA からのロギングイベントをサポートするようになりました。

- **ASA ロギング**：Security Analytics and Logging（SAL SaaS）は、管理方法に関係なく、任意の Cisco ASA ファイアウォールからのロギングをサポートするようになりました。ユーザーは、syslog 形式、NetFlow Security Event Logs（NSEL）形式、またはその両方で ASA ログを送信することを選択できます。ロギング分析を有効にしたいお客様は、NSEL ログを有効にして、上位層の SAL ライセンスに必要なテレメトリを提供する必要があります。

  これにより、既存の FTD ロギングに加えて、CDO はシスコのセキュリティポートフォリオの最初の製品となり、シスコのファイアウォールフリート全体のロギングを真に集約および統合します。

  詳細については、『Managing ASA with Cisco Defense Orchestrator』の次のトピックを参照してください。

  - Cisco Security Analytics and Logging for ASA Devices
  - Implementing Cisco Security Analytics and Logging for ASA Devices

- **長期保存とダウンロード**：ユーザーは、最初に SAL を注文するときに、1 年、2 年、または 3 年間、または後でアドオンとしてログを保存することを選択できるようになりました。ファイアウォールロギングのデフォルトの保持期間は 90 日のままであることに注意してください。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Security Analytics and Logging Event Storage」を参照してください。
- **トラフィック分析**：FTD 接続レベルのログと ASA（NSEL）のログの両方を SAL のトラフィック分析で実行でき、観察とアラートは、SecureX サインオンを使用して Cisco Secure Cloud Analytics にクロス起動することで確認できます。Syslog のみをログに記録する ASA のお客様は、トラフィック分析を有効にするために NSEL ログに切り替える必要があります。Logging Analytics and Detection および Total Network Analytics and Detection ライセンスを取得したお客様は、追加料金なしで、分析用の Cisco Secure Cloud Analytics ポータルをプロビジョニングして使用できます。Cisco Secure Cloud Analytics の検出には、SAL ユーザーが Cisco Secure Cloud Analytics のコア機能の一部として利用できる他の検出に加えて、ファイアウォール ロギング データを使用して特に有効化された監視とアラートが含まれます。既存の Logging and Troubleshooting のライセンス所有者は、30 日間のコミットメントなしで上位ライセンスの検出機能をテストできます。
- **無料トライアル**：このフォームに記入することで、すべてのライセンスに対してコミットメントのない 30 日間の SAL トライアルを開始できます。このロータッチトライアルでは、データをクラウドにエクスポートするためのオンプレミスコネクタの最小限のセットのみが必要です。SAL ライセンスの適切な 1 日あたりのボリュームを購入する前段階として、このトライアルを使用して、SAL 機能を評価し、実稼働環境をサポートするために必要なデータボリュームを見積もることができます。この目的のため、SAL トライアルでは、ほとんどのユーザーボリュームのデータを抑制しません。さらに、SAL の 1 日あたりのボリュームを見積もるために見積もりツールが役立ちます。

Security Analytics and Logging のイベント監視の改善

- CDO の [イベントロギング（Event Logging）] ページで、タイプによる ASA イベントのフィルタリングが提供されるようになりました。すべての syslog イベントまたは NSEL イベントを個別に、またはまとめて表示できます。
- 多くの ASA syslog イベントが解析され、イベントに関する詳細が提供されます。その詳細を使用して、Cisco Secure Cloud Analytics でイベントを分析できます。
- 表示する情報の列のみを表示し、残りの列を非表示にすることで、[イベントロギング（Event Logging）] ページの表示をカスタマイズできます。

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Filtering Events in the Event Logging」を参照してください。

2020 年 6 月 4 日

リモートアクセス VPN セッションの監視と終了

CDO を使用して、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）および Firepower Threat Defense（FTD）VPN ヘッドエンド全体でライブ AnyConnect リモートアクセス VPN セッションを監視できるようになりました。アクティブな VPN セッションの総数、現在接続しているユーザーとセッション、送受信されたデータの量に関する情報を収集します。

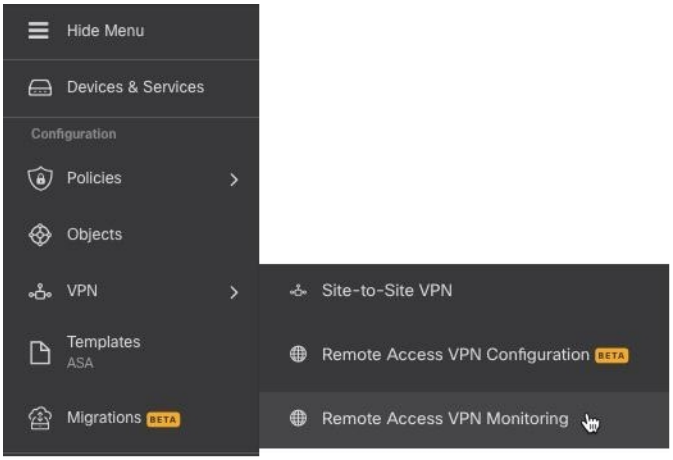
テナント内の各 RA VPN ヘッドエンドのパフォーマンスを表示し、ヘッドエンドでセッションをフィルタリングし、VPN モニタリングテーブルに表示するセッションプロパティを選択できます。また、1 つ以上のデバイスの RA VPN セッションをコンマ区切り値（.csv）ファイルにエクスポートできます。詳細については、『Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator』の「Export RA VPN Sessions to a CSV File」を参照してください。

ASA 上の 1 人のユーザーのすべてのアクティブな RA VPN セッションを終了でき、ASA 上のすべてのユーザーのすべてのアクティブな RA VPN セッションを終了できます。

詳細は、次のトピックを参照してください。

- 『Managing ASA with Cisco Defense Orchestrator』の「Disconnect Active RA VPN Sessions on ASA」
- 『Managing FTD with Cisco Defense Orchestrator』の「Disconnect Active RA VPN Sessions on FTD」

[VPN] > [リモートアクセスVPNモニタリング（Remote Access VPN Monitoring）] の順にクリックして、ナビゲーションバーから [リモートアクセスVPNモニタリング（Remote Access VPN Monitoring）] 画面を開きます。



AWS 仮想プライベートクラウド管理 - 無料トライアル

CDO から AWS VPC を 90 日間無料で管理してみてください。CDO の [デバイスとサービス（Devices & Services）] ページを開き、AWS VPC をオンボードして開始します。

詳細については、『Managing AWS with Cisco Defense Orchestrator』の「Onboard an AWS VPC」を参照してください。

新機能タイル

CDO ランディングページには、最新の機能と CDO がそれらの機能をいつ実装したかを示す新機能タイルが追加されました。興味のある機能がある場合は、その機能のタイトルをクリックして、その特定の機能に関するドキュメントをお読みください。

2020 年 5 月

2020 年 5 月 20 日

新しい API のみのユーザー

CDO では、ネットワーク管理者が、CDO REST API 呼び出しを行うときに CDO を認証するための API トークンを生成するために使用できる「API のみのユーザー」を作成できるようになりました。このユーザーアカウントと対応する API トークンは、元のネットワーク管理者が組織を離れた後も引き続き機能します。

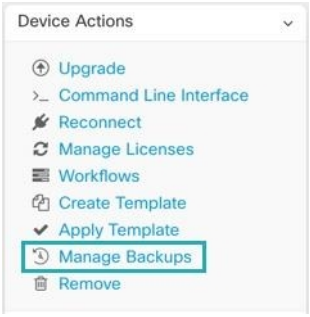
詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Create API Only Users」を参照してください。

2020 年 5 月 7 日

Firepower Threat Defense デバイスのバックアップ

CDO を使用して、Firepower Threat Defense（FTD）のシステム構成をバックアップできるようになりました。CDO を使用すると、次のことができます。

- オンデマンドでデバイスをバックアップします。
- 選択した時間に、毎日から毎月までの周期で定期的なバックアップをスケジュールします。
- バックアップをダウンロードし、Firepower Device Manager（FDM）を使用してそれらを復元します。



詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Backing Up FTDs」を参照してください。

2020 年 4 月

2020 年 4 月 16 日

Firepower Threat Defense 6.6.0 を実行しているデバイスの CDO サポート

CDO は現在、FTD 6.6.0 デバイスを管理しています。CDO が提供するサポートの新しい側面は次のとおりです。

- Firepower Threat Defense（FTD）6.6.0 を実行しているデバイスのオンボード。
- FTD 6.4.x 以上のデバイスを FTD 6.6.0 デバイスにアップグレード。デバイスは、個々の FTD または高可用性ペアで設定された FTD にすることができます。次の注意事項は、アップグレードサポートに適用されます。
  - Firepower 4100 および Firepower 9300 デバイスのアップグレードは現在サポートされていません。
  - 顧客は CDO のアップグレードページのドロップダウンを使用して、FTD 6.6.0 にアップグレードできます。
- CDO は、FTD 機能のサポートを継続的に開発し、準備ができ次第、新機能のサポートをリリースします。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Firepower Threat Defense Support Specifics」を参照してください。

2020 年 4 月 9 日

Firepower Threat Defense コマンド ライン インターフェイス

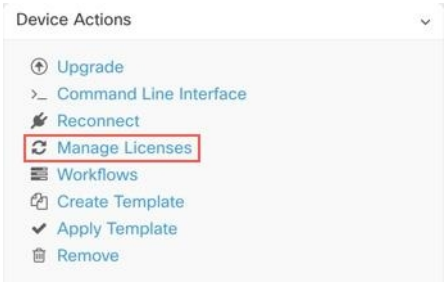
CDO から直接 FTD デバイスに CLI 要求を発行できるようになりました。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Using the CDO Command Line Interface」を参照してください。

2020 年 4 月 2 日

Firepower Threat Defense デバイスのライセンス管理の向上

FTDデバイスライセンス情報の表示、ライセンスの有効化と無効化、ライセンスの更新はすべて、[デバイスとサービス（Devices & Services）] ページの [デバイスアクション（Device Actions）] ペインの 1 つのボタンから管理されるようになりました。



2020 年 3 月

2020 年 3 月 26 日

FTD セキュリティデータベースの更新

CDO を使用すると、FTD デバイスをオンボードするときに、セキュリティデータベースをすぐに更新すると同時に、将来の更新をスケジュールすることができます。この機能は、SRU、セキュリティインテリジェンス（SI）、脆弱性（VDB）、地理位置情報データベースを更新します。オンボーディングプロセスの一部としてのみ、将来の更新をスケジュールできることに注意してください。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Update FTD Security Databases」を参照してください。

FTD サービスオブジェクトのポート範囲のサポート

CDO は、ポート番号の範囲を含むサービスオブジェクト（FTD ではポートオブジェクトとも呼ばれる）の作成をサポートするようになりました。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Create and Edit Firepower Service Objects」を参照してください。

2020 年 3 月 24 日

Cisco Secure Sign-on のドメイン移行

2020 年 3 月 24 日火曜日、太平洋夏時間の午後 5 時に、Cisco Security Single Sign-on ソリューションの公式ドメインが https://security.cisco.com から https://sign-on.security.cisco.com に移動されました。

保存されたリンクを更新し、パスワードマネージャを更新して、新しい URL を参照するようにすることをお勧めします。

この移行により、CDO へのアクセスが短期間制限されますが、ローカルデバイスマネージャまたは SSH 接続を使用して更新を実行する機能は制限されません。

問題が発生した場合は、テクニカルサポートを提供できる Cisco TAC に連絡してください。

2020 年 3 月 12 日

FTD ルールセット

CDO は、Firepower Threat Defense デバイスの**ルールセット**を導入します。ルールセットは、複数の FTD デバイスで共有できるアクセス制御ルールのコレクションです。ルールセットのルールに加えられた変更は、ルールセットを使用する他の FTD デバイスに影響します。FTD ポリシーには、デバイス固有の（ローカル）ルールと共有（ルールセット）ルールの両方を含めることができます。FTD デバイスの既存のルールからルールセットを作成することもできます。

この機能は現在、Firepower Threat Defense 6.5 以降のリリースを実行しているデバイスで使用できます。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「FTD Rulesets」を参照してください。

2020 年 3 月 5 日

FTD ポリシー内または別の FTD ポリシーへのルールのコピーまたは移動

1 つの FTD のポリシーから別の FTD のポリシーにルールをコピーまたは移動できるようになりました。また、ルールがネットワークトラフィックを評価する順序を微調整できるように、FTD ポリシー内でルールを簡単に移動できるようにしました。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Copy FTD Access Control Rules」および「Move FTD Access Control Rules」を参照してください。

AnyConnect ソフトウェアパッケージの FTD バージョン 6.5+ へのアップロード

CDO のリモートアクセス VPN ウィザードを使用して、リモートサーバーから FTD 6.5 以降を実行している Firepower Threat Defense（FTD）デバイスに AnyConnect パッケージをアップロー

ドできるようになりました。リモートサーバーが HTTP または HTTPS プロトコルをサポートしていることを確認します。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Upload AnyConnect Software Packages to an FTD Device Running FTD Version 6.5 or Later」を参照してください。

2020 年 3 月 3 日

CDO のインターフェイスでの用語の更新

デバイスを管理するために、Cisco Defense Orchestrator（CDO）は、デバイスの構成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 が構成を「読み取る」とき、デバイスに保存されている構成のコピーを作成し、CDO のデータベースに保存します。読み取りアクションを実行するときに行っていることをより適切に説明するために、いくつかのインターフェイスオプションの名前を変更しました。

以下は新しい用語です。

- **変更の確認**。デバイスの構成ステータスが [同期済み（Synced）] の場合、[変更の確認（Check for Changes）] リンクを使用できます。[変更の確認（Check for Changes）] をクリックすると、CDO は、そのデバイスの構成のコピーとデバイスの構成のデバイスのコピーを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構成のコピーをすぐに上書きします。
- **変更の破棄**。デバイスの構成が [未同期（Not Synced）] の場合、[変更の破棄（Discard Changes）] をクリックすると、CDO がデバイス構成のコピーに加えたすべての変更が削除され、デバイスで見つかった構成のコピーで上書きされます。
- **レビューなしで受け入れる。**このアクションは、デバイスの構成の CDO のコピーを、デバイスに保存されている構成のコピーで上書きします。CDO は、アクションの確認を求めません。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Reading, Discarding, Checking for, and Deploying Configuration Changes」を参照してください。

2020 年 2 月

2020 年 2 月 6 日

Firepower 1010 のスイッチポートモードのサポート

CDO は、Firepower 1010 デバイスのスイッチポートモード機能を完全にサポートするようになりました。

構成のガイドラインと制限事項の詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Switch Port Mode Interfaces for an FTD」および「Configure an FTD VLAN for Switch Port Mode」を参照してください。

2020 年 1 月

2020 年 1 月 22 日

サイト間接続の動的ピアサポート

ピアの VPN インターフェイスの 1 つに動的 IP アドレスがある場合、2 つのピア間にサイト間 VPN トンネルを構成できるようになりました。この動的ピアは、管理対象の FTD デバイスまたはエクストラネットデバイスにすることができます。

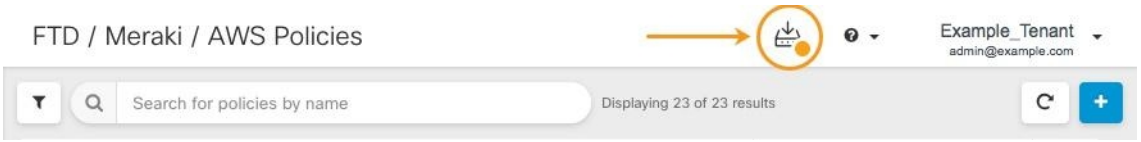
詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Configure Site-to-Site VPN Connections with Dynamically-Addressed Peers」を参照してください。

2020 年 1 月 16 日

展開エクスペリエンスの改善

CDO は、展開ワークフローを改善しました。追加の展開アイコンが CDO 全体に表示されるようになりました。構成の変更を展開するために、[デバイスとサービス（Devices & Services）] ページに戻る必要がなくなりました。

展開アイコンにオレンジ色のドットが含まれている場合、CDO で管理するデバイスの少なくとも 1 つに少なくとも 1 つの構成変更があり、展開の準備ができていることを示しています。

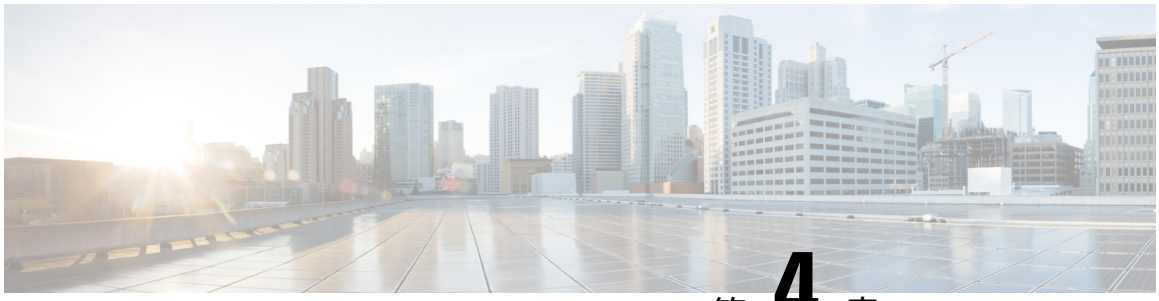


詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Preview and Deploy Configuration Changes for All Devices」を参照してください。

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。[ジョブ（Jobs）] ページに移動し、進行中の一括操作を見つけて、[キャンセル（Cancel）] をクリックしてアクションを停止できるようになりました。

2020 年 1 月 16 日



第 4 章

2019 の機能概要

2019 年 11 月

2019 年 11 月

Firepower Threat Defense 6.5.0 を実行しているデバイスの CDO サポート

CDO は現在、FTD 6.5.0 デバイスを管理しています。CDO が提供するサポートの側面は次のとおりです。

- Firepower Threat Defense（FTD）6.5.0 を実行しているデバイスのオンボード。
- Firepower 4100 や Firepower 9300 などの追加の Firepower シリーズ デバイスのサポート。
- Microsoft Azure での仮想 FTD インスタンスのサポート。サポートされているデバイスの完全なリストについては、『Managing FTD with Cisco Defense Orchestrator』の「Firepower Threat Defense Support Specifics」を参照してください。
- デバイスは、個々の FTD または高可用性ペアで設定された FTD にすることができます。詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Firepower Software Upgrade Path」を参照してください。次の注意事項は、アップグレードサポートに適用されます。

- デバイスが管理にデータインターフェイスを使用している場合、6.5.0 を実行している FTD では HA ペアのアップグレードはサポートされません。
- Firepower 4100 および Firepower 9300 デバイスのアップグレードは現在サポートされていません。
- 顧客は CDO のアップグレードページのドロップダウンを使用して、FTD 6.5.0 にアップグレードできます。6.5 イメージのダウンロードのためにデバイスに提供されるリンクは HTTP になります。これは、ダウンロードが HTTPS 経由で行われた場合よりも、イメージのダウンロード時間がわずかに長くなる可能性があることを意味する場合があります。さらに、FTD からのアウトバウンド HTTP トラフィックがブロックされている場合、イメージのダウンロードは失敗します。

- Firepower 1010 に FTD 6.5.0 がインストールされている場合、通常のファイアウォール インターフェイスとしてまたはレイヤ 2 ハードウェアスイッチポートとして実行するようにインターフェイスを設定できます。現時点では、CDO でのスイッチモードのサポートは読み取り専用です。スイッチポートモードのインターフェイスを作成または変更するには、FDM コンソールを使用します。CDO は、Firepower 1010s でのスイッチポートモードのサポートの開発を続けており、完全なサポートが利用可能になったら、新機能で発表します。
- 登録トークンを使用して FTD 6.5.0 デバイスをオンボードすると、セキュアイベントコネクタを使用せずに、接続イベント、ファイルイベントとマルウェアイベント、および侵入イベントを Cisco Cloud に直接送信できます。『Managing FTD with Cisco Defense Orchestrator』の「Implementing Cisco Security Analytics and Logging」を参照してください。
- FTD 6.4.x 機能の継続的なサポート。CDO は FTD 6.5 機能のサポートを継続的に開発しており、準備ができ次第サポートをリリースします。

CDO がサポートしている FTD 機能の詳細については、『Managing FTD with Cisco Defense Orchestrator』を参照してください。

IKEv1 によるサイト間 VPN 接続のサポート

CDO は、Internet Key Exchange バージョン 1（IKEv1）を使用したサイト間 VPN トンネルの作成をサポートするようになりました。Internet Key Exchange バージョン 2（IKEv2）をサポートしていないレガシーファイアウォールでサイト間 VPN を構成するのに役立ちます。Internet Key Exchange（IKE、インターネット キー エクスチェンジ）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA、セキュリティ アソシエーション）の自動的な確立に使用されるキー管理プロトコルです。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Site-to-Site Virtual Private Network」を参照してください。

Firepower Threat Defense のテンプレートの改善

CDO では、FTD テンプレートのいくつかの側面をパラメータ化して、テンプレートをさらにカスタマイズできるようになりました。詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Configure FTD Templates」を参照してください。

スマートライセンスの管理

CDO 内で Firepower Threat Defense デバイスのシスコ スマート ライセンスを管理できるようになりました。スマートライセンスはワークフローに組み込まれており、CDO インターフェイスから簡単にアクセスできます。CDO 内で次の Cisco Smart Licensing タスクを実行できるようになりました。

- 登録トークンを使用して FTD デバイスのオンボード中にスマートライセンスを適用する
- デバイスに適用されているライセンスを表示する
- Cisco Smart Software Manager へのライセンスを登録する
- デバイスのさまざまなライセンスタイプを有効または無効にする

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Onboard a Firepower Threat Defense Device with a Registration Token」および「Smart-licensing an Onboarded FTD」を参照してください。

2019 年 10 月

2019 年 10 月

アマゾンウェブサービスのサポート

CDO が AWS VPC を管理するようになりました。

アマゾンウェブサービス（AWS）仮想プライベートクラウド（VPC）は、AWS アカウントに関連付けられた仮想プライベートクラウドをユーザーに提供する商用クラウドコンピューティング サービスです。このネットワークは、AWS のスケーラブルなインフラストラクチャを使用する利点を備えた、独自のデータセンターで運用する従来のネットワークによく似ています。

CDO は、オブジェクトとルールの問題を特定し、それらを修正する方法を提供することにより、AWS VPC の最適化を支援します。CDO を使用して次のことを行います。

- FTD または ASA デバイスとともに AWS VPC 環境を管理します。
- AWS VPC に関連付けられたすべてのセキュリティグループルールを同時に管理します。
- FTD や ASA デバイスなど、サポートされている他のプラットフォーム間で互換性のあるオブジェクトを使用して、セキュリティグループルールを作成およびカスタマイズします。

- AWS VPC サイト間 VPN 接続を表示します。

詳細については、『Managing AWS with Cisco Defense Orchestrator』を参照してください。

CDO を使用して ASA を FTD デバイスに移行する

CDO は、適応型セキュリティアプライアンス（ASA）を Firepower Threat Defense（FTD）デバイスに移行するのに役立ちます。CDO には、ASA の実行構成の次の要素を FTD テンプレートに移行するためのウィザードが用意されています。

- インターフェイス
- ルート
- アクセス制御ルール（ACL）
- ネットワークアドレス変換（NAT）ルール
- ネットワークオブジェクトとネットワーク グループ オブジェクト
- サービスオブジェクトとサービス グループ オブジェクト

ASA 実行構成のこれらの要素を FTD テンプレートに移行したら、その FTD テンプレートを、CDO によって管理される新しい FTD デバイスに適用できます。FTD デバイスはテンプレートで定義された構成を採用するため、FTD は ASA の実行構成のいくつかの側面を使用して構成されるようになりました。

CDO を使用して ASA を FTD に移行するプロセスの詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Migrating ASA to FTD Workflow」を参照してください。

シスコが導入する Cisco Secure Sign-on と Duo Multi-Factor Authentication を使用した新しいシングル サインオン ソリューション

CDO はこの新しいソリューションを採用し、顧客のテナントを Cisco Secure Sign-on ID プロバイダー（IdP）および Duo Security 多要素オーセンティケータに変換します。

Cisco Secure Sign-On を使用すると、次のメリットが得られます。

- **強力で回復力のある ID**：AICPA SOC 2、CSA-Star、ISO 27001 などの最高の業界標準を満たすセキュリティ。また、顧客向けに分離された FedRAMP および HIPAA 環境もサポートします。
- **Duo 多要素認証（MFA）**：Cisco Secure Sign-On と統合された Duo MFA とは、適応型の階層化されたシンプルな認証を意味します。ワンプッシュ通知、ワンタップで簡単にアクセスできます。
- **シームレスなワークフローのためのシングルサインイン**：単一のユーザー名とパスワードを入力して、ワークフローを通じてコンテキストを維持しながら、場所やデバイスを問わずすべてのアプリケーションにアクセスします。
- **カスタマイズされたエクスペリエンス**：仕事用アプリを Cisco Secure Sign-On ダッシュボードに自由に配置できます。タブと検索バーで整理できます。

（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 の無料試用期間中であれば、この移行は影響します。

詳細については、『Managing AWS with Cisco Defense Orchestrator』の「Migrating to Cisco Secure Sign-On Identity Provider」を参照してください。

Secure Cloud Analytics との統合を含む Cisco Security Analytics and Logging

Cisco Security Analytics and Logging によりネットワークの可視性が向上するため、脅威をリアルタイムで迅速に検出し、インシデントを確実かつ大規模に修正できます。

Cisco Security Analytics and Logging を使用すると、すべての Firepower Threat Defense（FTD）デバイスからの接続、侵入、ファイル、マルウェア、セキュリティインテリジェンスのイベントをキャプチャし、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。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。Logging and Troubleshooting パッケージは、これらの機能を提供します。

Firewall Analytics and Monitoring パッケージを使用すると、システムは 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、動作モデリング分析を使用して 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。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Cisco Security Analytics and Logging」を参照してください。

2019 年 9 月

2019 年 9 月

登録トークンを使用した Firepower Threat Defense デバイスのオンボーディング

IP アドレス、ユーザー名、およびパスワードを使用する代わりに、登録トークンを使用して FTD デバイスをオンボードできるようになりました。これは、FTD に DHCP を使用して IP アドレスが割り当てられている場合に特に役立ちます。その IP アドレスが何らかの理由で変更されても、FTD は CDO に接続されたままになります。さらに、FTD はローカルエリアネット

ワーク上のアドレスを持つことができ、外部ネットワークにアクセスできる限り、この方法で CDO にオンボードできます。

このオンボーディング方法は、現在、FTD 6.4 リリースで、defenseorchestrator.cisco.com に接続しているお客様が利用できます。defenseorchestrator.cisco.eu に接続しているお客様はまだ利用できません。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Onboarding an FTD with a Registration Key」を参照してください。

2019 年 8 月

2019 年 8 月

Cisco Security Analytics and Logging

Cisco Security Analytics and Logging によりネットワークの可視性が向上するため、脅威をリアルタイムで迅速に検出し、インシデントを確実かつ大規模に修正できます。

Firepower Threat Defense のリモートアクセス VPN のサポート

リモートアクセス（RA）VPN を使用すると、サポートされているラップトップ、デスクトップ、およびモバイルデバイスを使用して、個人がネットワークへの安全な接続を確立できます。CDO は、オンボーディングした Firepower Threat Defense（FTD）デバイスで RA VPN をセットアップ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。

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、FTD デバイスでの RA VPN 機能の次の側面をサポートします。

- プライバシー、認証、およびデータ整合性のための Transport Layer Security（TLS）または Datagram Transport Layer Security（DTLS）
- 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 FTD デバイス間での共有 RA VPN 設定

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Remote Access Virtual Private Network」を参照してください。

Firepower Threat Defense のハイ アベイラビリティ イメージ アップグレードのサポート

CDO で FTD HA ペアをアップグレードできるようになりました。フェールオーバーペアをアップグレードすると、CDO は必要なアップグレードイメージを両方のデバイスにコピーします。CDO は、プライマリデバイスがアクティブモードになっていない場合は、それを一時的にア

クティブモードに移行してから、セカンダリデバイスをアップグレードします。セカンダリデバイスが正常にアップグレードされると、プライマリデバイスがアップグレードされます。フェールオーバーペアは、デバイスを一度に1つずつアップグレードして、ネットワークの中断を最小限に抑えます。

フェールオーバーペアをアップグレードするには、『Managing FTD with Cisco Defense Orchestrator』の「Upgrade an FTD High Availability Pair」を参照してください。

Firepower Threat Defense デバイスのサイト間 VPN

Firepower Threat Defense デバイス用のサイト間 VPN の一般提供が開始されました。

CDO を使用すると、地理的に異なる 2 つのサイト間で安全な接続を確立できます。これらのピアは、IPv4 アドレスと IPv6 アドレスの内部と外部の任意の組み合わせを持つことができます。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。CDO にオンボードされているデバイスの次のシナリオで、サイト間 IPsec 接続を作成できます。

- 2 つの管理対象デバイス間
- 管理対象デバイスとその他のシスコのピア間
- 管理対象デバイスとサードパーティのピア間

Firepower Threat Defense のハイアベイラビリティのサポート

CDO は、Firepower Threat Defense ファイアウォールのハイアベイラビリティ（HA）のサポートを一般提供します。既存の HA ペアをオンボードするか、CDO で HA ペアを作成できるようになりました。HA 構成により、アップグレード期間中や予期しないデバイス障害など、デバイスが使用できないシナリオでも安全なネットワークを維持することができます。フェールオーバーモードでは、スタンバイデバイスはすでにアクティブになるように構成されています。つまり、HA デバイスの 1 つが使用できなくなっても、もう一方のデバイスはトラフィックの処理を続行します。

スタンドアロン FTD デバイスでサポートされる機能のほとんどは、HA 用に設定されたデバイスもサポートします。詳細については、『Managing FTD with Cisco Defense Orchestrator』の「FTD High Availability」を参照してください。

近日公開... FTD HA アップグレードのサポート。現在、HA ペアをアップグレードする必要がある場合は、アクティブなデバイスの FDM コンソールからアップグレードを実行する必要があります。

2019 年 7 月

2019 年 7 月

ASA デバイスの時間範囲オブジェクト

時間範囲オブジェクトを使用して、ネットワークポリシーのルールをカスタマイズできるようになりました。これらのオブジェクトを使用すると、1 回限りのルールまたは繰り返しルールを実行し、ネットワークがトラフィックを処理する方法をカスタマイズできます。

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「ASA Time Range Objects」を参照してください。

Firepower Threat Defense のサポート

CDO は、Firepower Threat Defense ファイアウォールのサポートを一般提供します。

CDO は、Firepower Threat Defense デバイスへのシンプルな管理インターフェイスとクラウドアクセスを必要とするファイアウォール管理者向けに設計されています。Firepower Device Manager（FDM）管理者は、FDM インターフェイスと CDO インターフェイスの間に多くの類似点があることに気付くでしょう。私たちは、マネージャ間で可能な限り一貫性を保つという考えで CDO を構築しました。

CDO は、ASA 5508-x、ASA 5515-x、ASA 5516-x、ASA 5525-x、ASA 5545-x、ASA 5555-x、FTD 2100 シリーズ デバイス、FTD 1000 シリーズ デバイス、または仮想 FTD デバイスにインストールされている場合、FTD バージョン 6.4.0 以降を実行している Firepower Threat Defense（FTD）デバイスを管理できるようになりました。

CDO を使用して、物理または仮想 Firepower Threat Defense（FTD）デバイスの次の側面を管理します。

- デバイス管理
- デバイスのアップグレード
- インターフェイス管理
- ルーティング
- セキュリティ ポリシー
- ポリシーと構成の一貫性を促進する
- 変更のトラッキング
- ネットワークのモニタリング

Firepower 1000 シリーズおよび仮想 FTD を含むすべての CDO FTD PID は、CCW で注文できます。PID はプラットフォーム固有ですが、ASA と FTD に共通です。詳細については、Salesconnect の注文ガイドを参照してください。

サポートしている機能の詳細については、『Managing FTD with Cisco Defense Orchestrator』を参照してください。

Meraki MX のサポート

CDO は、Meraki MX ファイアウォールポリシーを管理するようになりました。

Meraki MX は、分散展開用に設計されたエンタープライズセキュリティおよびソフトウェア定義ワイドエリアネットワーク（SD-WAN）の次世代ファイアウォール アプライアンスです。Cisco Defense Orchestrator を使用して、Meraki MX デバイスのレイヤ 3 ネットワークルールを管理できるようになりました。

CDO は、オブジェクトとポリシーの問題を特定し、それらを修正する方法を提供することにより、Meraki 環境を最適化するのに役立ちます。これは、デバイスとテンプレートの両方に関連付けられたポリシーに適用されます。

CDO を使用して次のことを行います。

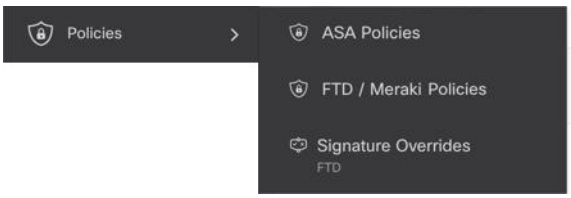
- 1 つ以上の Meraki デバイスでポリシーを同時に管理します。
- 包括的な環境で、FTD および ASA デバイスとともに Meraki ポリシーまたはテンプレートを監視および管理します。
- Meraki テンプレートを使用して複数のネットワークを管理します。
- FTD や ASA デバイスなど、サポートされている他のプラットフォーム間で互換性のあるオブジェクトを使用してアクセスルールをカスタマイズします。

詳細については、『Managing Meraki with Cisco Defense Orchestrator』を参照してください。

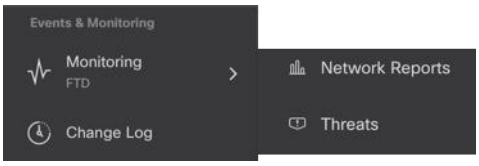
最新の GUI ナビゲーション

CDO の UI の操作がさらに簡単になりました。

ナビゲーションバーのポリシーメニューに、デバイスまたは機能別にグループ化されたポリシーが表示されるようになりました。テナントに現在存在するポリシーに到達するために必要なメニューパスのみを公開します。



FTD のすべての監視機能は、ナビゲーションバーの [イベントと監視（Events & Monitoring）] エリアにグループ化されています。[監視（Monitoring）] メニューには、[ネットワーク レポート（Network Reports）] と [脅威（Threats）] が表示されます。



2019 年 5 月

2019 年 5 月

デバイス接続のトラブルシューティング

このツールを使用すると、セキュアデバイスコネクタ（SDC）と任意のデバイス間の接続の問題をテストまたはトラブルシューティングできます。デバイスがオンボーディングに失敗した場合、またはオンボーディングの前に 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。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Troubleshoot a Secure Device Connector with the SDC」を参照してください。

2019 年 4 月

2019 年 4 月

CDO ユーザーエクスペリエンスの向上にご協力ください

CDO のユーザーエクスペリエンスについてお聞かせいただきたく、簡単にできる方法をご用意しました。CDO ポータルを離れることなくフィードバックを送信できるように、[ヘルプ（Help）] メニューに [フィードバックの提供（Provide Feedback）] ボタンを追加しました。気に入った点と改善点を教えてください。

フィードバックを送信する際は、会社でのあなたの役割を教えてください。あなたは、ネットワーク オペレーション センター、セキュリティ オペレーション センターにいますか。それとも IT 関連全般を扱うセンターにいますか。完了しようとしているタスクを教えてください。セキュリティポリシーを編集しようとしていますか、または変更ログで何かを見つけようとしていますか。

フィードバックを残す方法は次のとおりです。

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、[フィードバックの提供（Provide Feedback）] を選択します。

ステップ 3 フィードバックを入力して [電子メールの送信（Send Email）] をクリックします。これにより、ローカルメールサーバーに電子メールが生成されます。 これは手動で送信する必要があります。

サポートスタッフができるだけ早く対応します。

2019 年 2 月

2019 年 2 月

セキュアデバイスコネクタに影響を与えるコンテナ権限昇格の脆弱性への解決策：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。

CDO 標準の SDC ホストとカスタム SDC ホストを更新する方法の手順については、「Container Privilege Escalation Vulnerability Affecting Secure Device Connector」（cisco-sa-20190215-runc）を参照してください。

ASA デバイスの一括オンボーディング時にラベルを追加する

ASA デバイスを一括でオンボーディングするときに、カスタムデバイスラベルを指定できるようになりました。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Onboard ASAs in Bulk」を参照してください。

Cisco IOS デバイスのサポート

Cisco Defense Orchestrator（CDO）を使用すると、Cisco IOS デバイスを管理できます。これらのデバイスでサポートされている機能は次のとおりです。

- Cisco IOS デバイスのオンボーディング
- デバイス構成の表示
- デバイスからのポリシーと構成の変更の終了

- アウトオブバンド変更の検出
- コマンド ライン インターフェイスのサポート
- 個々の CLI コマンドおよびコマンドのグループを、編集および再利用可能なマクロに変換可能
- SSH フィンガープリントの変更の検出と管理
- 変更ログに IOS デバイスへの変更を表示

自動展開のスケジュール

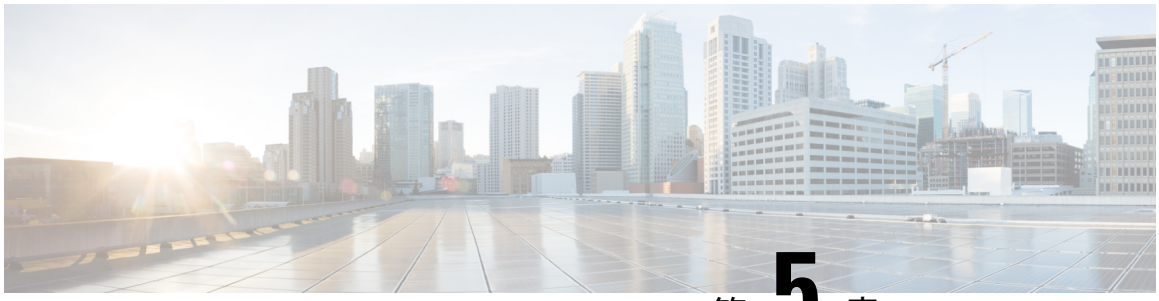
CDO を使用して 1 つ以上のデバイスの構成変更を行った後、都合のよい日時にそれらのデバイスへの変更の展開をスケジュールできるようになりました。たとえば、メンテナンスの時間帯やネットワークトラフィックが少ない時間帯に展開を実行するようにスケジュールできます。

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Enable the Option to Schedule Automatic Deployments」および「Schedule Automatic Deployments」を参照してください。

用語の変更：CDO が管理するデバイスへの変更を「展開」する

デバイスの構成の CDO のローカルコピーに加えた変更をデバイス自体に転送することを説明するために使用する用語を更新しました。以前はその転送を説明するために「書き込み」という言葉を使用していましたが、現在はその転送を説明するために「展開」という言葉を使用しています。

CDO を使用してデバイスの構成を管理および変更すると、CDO は構成ファイルの独自のコピーに加えた変更を保存します。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構成変更は、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。



第 5 章

2018 の機能概要

2018 年 11 月

2018 年 11 月 22 日

帯域外の変更を自動的に受け入れる

管理対象デバイスで構成を直接変更し、Defense Orchestrator が検出時に自動的に受け入れるように設定できるようになりました。Defense Orchestrator を監視して、帯域外の変更を手動で受け入れる必要はありません。

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Automatically Accept Out-of-Band Changes from your Device」を参照してください。

2018 年 11 月 8 日

システム オブジェクト フィルタ

システム オブジェクト フィルタを使用すると、オブジェクトテーブル内の最も重要なオブジェクトを表示できます。

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

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

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Object Filters」を参照してください。

2018 年 9 月

2018 年 9 月 20 日

ポリシーのエクスポートの改善

指定された時間範囲で ASA ポリシーをエクスポートすると、時間範囲のオブジェクト名が .CSV ファイルに含まれるようになりました。これにより、ポリシーのルールがいつアクティブになるかをよりよく理解できます。

CLI 処理の改善

Defense Orchestrator は、実行する ASA CLI コマンドの末尾のスペースをトリミングしなくなりました。

マニュアルの更新

ASA 変更ログと「差分」ドキュメントが追加され、変更ログのエントリと「差分」ページの内容を明確に理解できるようになりました。構成変更の前後を並べて比較します。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Change Log」を参照してください。

2018 年 9 月 13 日

関心のある変更ログエントリのみをエクスポートする

以前は、Defense Orchestrator の変更ログ全体しかエクスポートできませんでした。変更ログにフィルターと検索条件を適用し、関心のあるエントリのみをエクスポートできるようになりました。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Exporting the Change Log to a CSV file」を参照してください。

2018 年 9 月 6 日

新しいネットワーク管理者ロールは新しいユーザーレコードの作成とユーザーロールの変更が可能

Defense Orchestrator に、ネットワーク管理者ロールのサポートが追加されました。この新しいロールには、管理者ロールのすべての権限があり、ユーザーレコードを管理できる追加の権限があります。Defense Orchestrator サポートチームは、既存の管理者アカウントをネットワーク管理者にアップグレードできます。ネットワーク管理者ロールを持つユーザーがいると、サポートチケットを開かなくても、追加のユーザーレコードを作成および管理できます。

会社が SAML ID プロバイダー（IdP）を Defense Orchestrator と統合している場合、Defense Orchestrator アカウントへのユーザーアクセスを完全に管理できるようになりました。

複数の Defense Orchestrator アカウントを持つマネージドサービスプロバイダーの場合、Defense Orchestrator でサポートチケットを開くことなく、既存のユーザーのアカウントアクセスを許可および取り消すことができるようになりました。

会社が Defense Orchestrator のデフォルト ID プロバイダー（OneLogin）を使用している場合は、引き続きサポートチケットを開いて新しいユーザーアカウントを作成する必要がありますが、サポートチケットを開かなくても、Defense Orchestrator アカウントへのアクセスを取り消すことができます。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「User Management」を参照してください。

2018 年 8 月 16 日

変更ログの改善

CDO を介して ASA に変更を加え、構成の変更が成功すると、変更ログに、変更に使用された CLI コマンドが表示されるようになりました。

CDO を介して ASA に変更を加え、設定の変更が失敗した場合、変更ログには失敗した CLI コマンドが表示され、それらを簡単に見つけることができるようにアスタリスクで囲まれます。

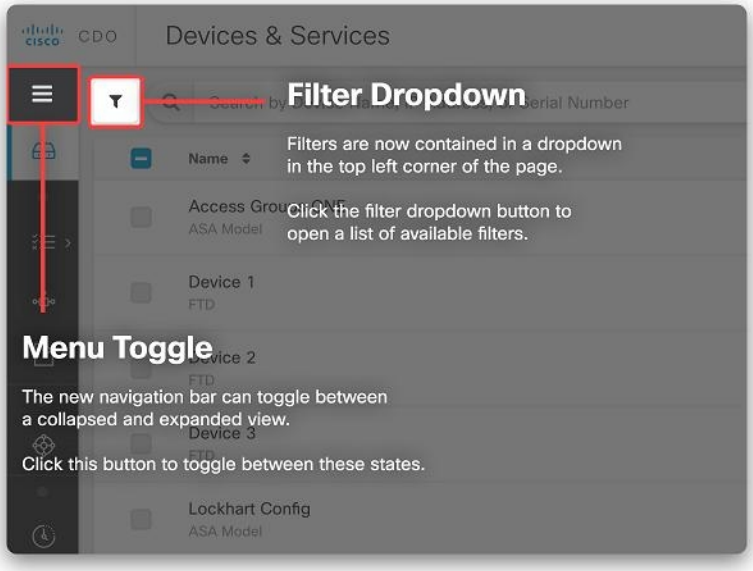
成功または失敗したコマンドを表示するには、変更が行われたデバイスの変更ログを開き、アクションのエントリを見つけて、ログエントリの最後にある [+] ボタンをクリックして展開します。

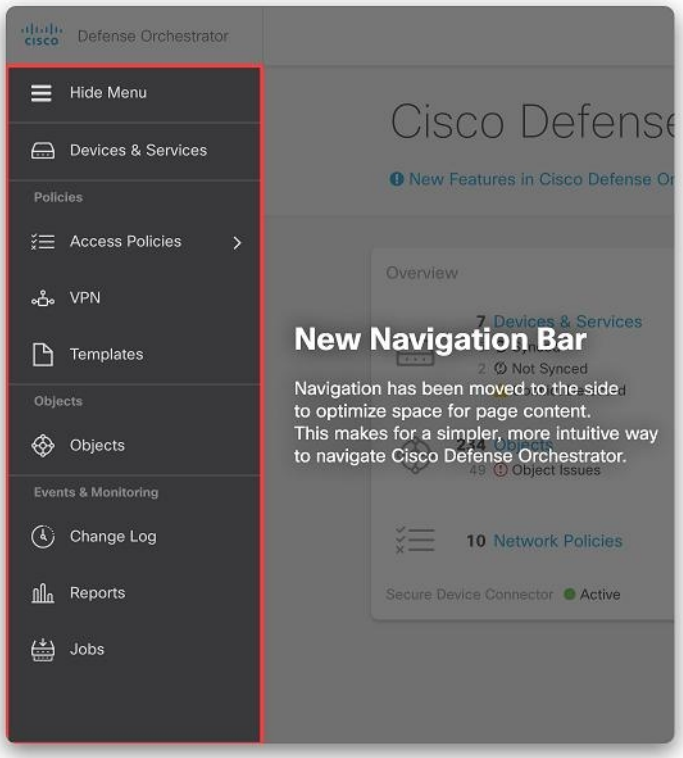
2018 年 7 月

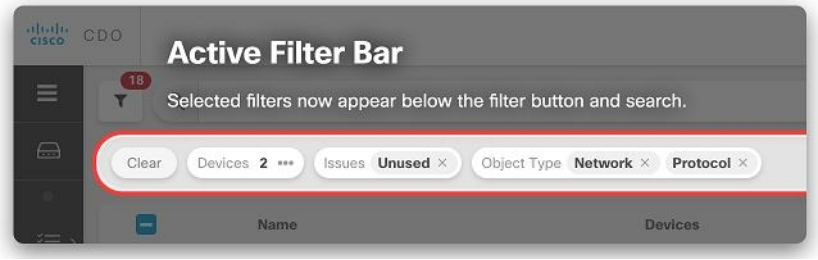
2018 年 7 月 26 日

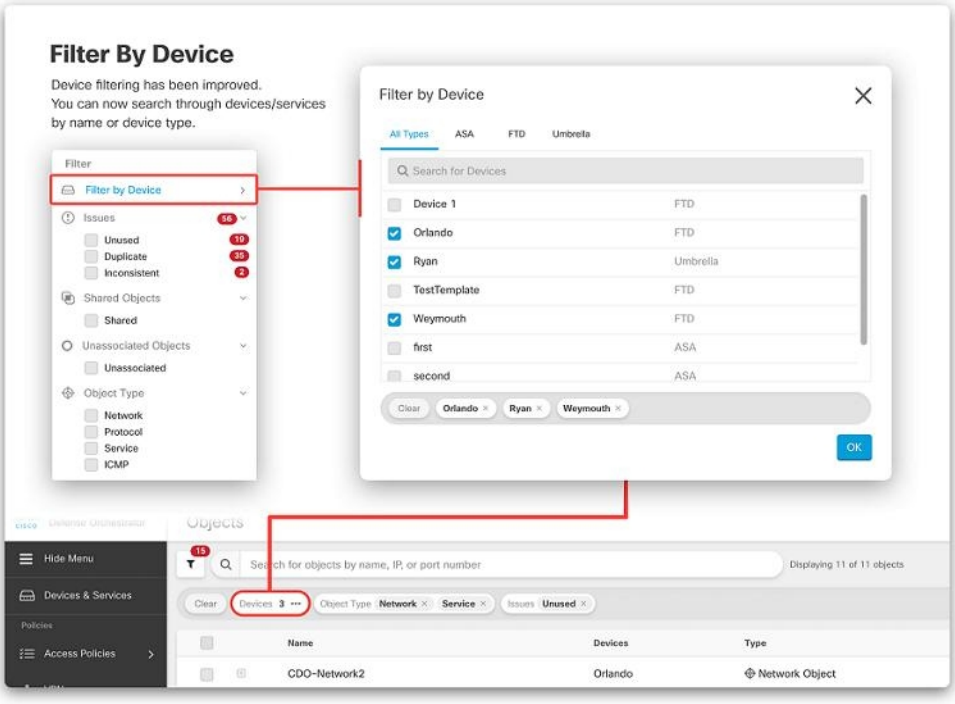
新しい CDO UI

ナビゲーションとフィルタリングが再設計され、より直感的になり、環境をより効率的に管理できるようになりました。



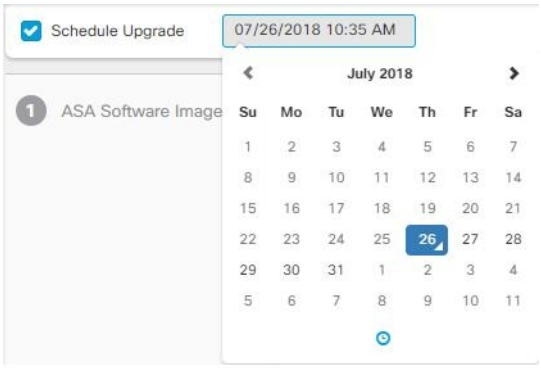

Defense Orchestrator
Hide Menu
Devices & Services
Policies
Access Policies
VPN
Templates
Objects
Objects
Events & Monitoring
Change Log
Reports
Jobs
Cisco Defense
New Features in Cisco Defense Or
Overview
7 Devices & Services
2 Not Synced
49 Object Issues
10 Network Policies
Secure Device Connector Active
New Navigation Bar
Navigation has been moved to the side to optimize space for page content.
This makes for a simpler, more intuitive way to navigate Cisco Defense Orchestrator.


CDO
Active Filter Bar
Selected filters now appear below the filter button and search.
18
Clear
Devices 2
Issues Unused
Object Type Network
Protocol
Name
Devices



デバイスアップグレードのスケジュール設定

デバイスへのソフトウェアアップグレードをスケジュールできるようになりました。[デバイスのアップグレード（Device Upgrade）] ページで、[アップグレードのスケジュール（Schedule Upgrade）] チェックボックスをオンにして、後の日時を設定します。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Upgrade Devices and Services」を参照してください。



ログイン情報の一括更新

CDO が複数の ASA デバイスの ASA に接続するために使用するログイン情報を一度に更新できるようになりました。[デバイスとサービス（Devices & Services）] ページで、複数の ASA デバイスを選択し、[ログイン情報の更新（Update Credentials）] をクリックします。詳細につ

いては、『Managing ASA with Cisco Defense Orchestrator』の「Update ASA Connection Credentials」を参照してください。

デバイスの場所の更新

IP アドレスの横にある編集ボタンをクリックして、オンボードされた ASA のデバイスの場所を更新できるようになりました。

2018 年 7 月 20 日

資格情報の更新

CDO が ASA への接続に使用するログイン情報を更新できるようになりました。ASA のオンボーディングプロセスで、CDO が ASA 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。以前は、これらのログイン情報を変更するか、パスワードを変更する場合は、ASA を CDO から削除し、新しいログイン情報で再度オンボードする必要がありました。ASA を再オンボードせずにログイン情報を変更できるようになりました。

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Updating ASA Connection Credentials」を参照してください。

2018 年 7 月 12 日

新しい ASA デフォルトルールの動作

新しいルールが ASA ネットワークポリシーに追加されると、デフォルトで「許可」アクションが割り当てられます。

エクスポートされたデバイスリストにテナント名が含まれる

特定のテナントのデバイスリストをエクスポートすると、テナントの名前がエクスポートされたファイル名に組み込まれるようになりました。

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Export List of Devices and Services」を参照してください

ネットワークグループの一括入力

ASA ネットワーク オブジェクト グループを作成または編集するときに、IP アドレスを一度に 1 つずつではなく、まとめて追加できるようになりました。

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Create or Edit ASA Network Objects and Network Groups」を参照してください。

2018 年 5 月

2018 年 5 月 24 日

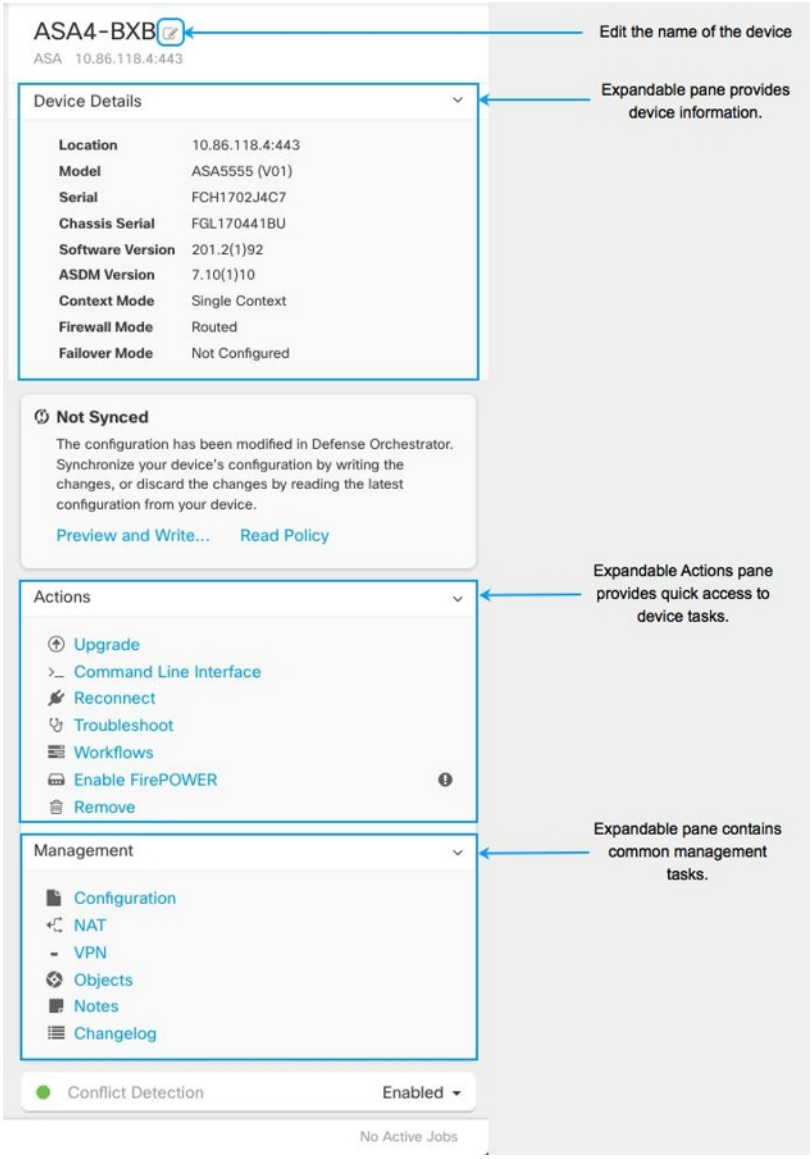
時間ベースの ASA ネットワークポリシーのサポート

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。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Define a Time Range for a Policy」を参照してください。

2018年5月17日

新しいデバイス詳細パネルのレイアウト

デバイス情報と一般的に使用されるコマンドボタンを見つけやすくするために、デバイスの詳細パネルを再編成しました。



ASA グローバルアクセスポリシーのサポート

CDO を使用して ASA のグローバルアクセスポリシーを作成できるようになりました。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。これは、インバウンド ネットワーク トラフィックに適用されます。CDO を使用すると、グローバルアクセスポリシーを 1 つの ASA から別の ASA にコピーして、デバイス間の一貫性を維持することもできます。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Configure an ASA Global Access Policy」を参照してください。

ASA デバイスのネットワークアドレス変換ルールウィザード

次の使用例の ASA デバイスで NAT ルールを作成するのに役立つ新しいネットワークアドレス変換（NAT）ルールウィザードがあります。

- 内部ユーザーのインターネットアクセスを有効にする
- 内部サーバーをインターネットに公開する

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Network Address Translation Rule Wizard」を参照してください。

2018 年 4 月

2018年4月26日

新しいトラブルシューティング ドキュメント

ASA のリブート後に Cisco Defense Orchestrator（CDO）と ASA が接続しない場合、ASA が、CDO の Secure Device Connector 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。「ASA がリブート後に CDO に再接続できない」のトラブルシューティング トピックでは、サポートされている暗号スイートと修復手順のリストが提供されています。

2018 年 4 月 5 日

アクセス コントロール エントリ（ACE）制限の計算

CDO は、個々のルール、ネットワークポリシー、および ASA で実行されている総数のアクセス コントロール エントリ（ACE）の数を表示します。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、アクセス コントロール エントリの数が多すぎると、ASA のパフォーマンスが低下します。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Access Control Entries (ACEs)」を参照してください。

2018 年 3 月

2018年3月22日

サポートされていないデバイス

現時点では、CDO は **ASA サービスモジュール**（ASASM）をサポートしています。

2018 年 3 月 15 日

読み取り専用ユーザー

読み取り専用のユーザーロールを作成しました。読み取り専用ユーザーは CDO ですべてを表示できますが、ページで何かを作成、更新、構成、または削除することはできません。また、デバイスをオンボードすることもできません。

読み取り専用ユーザーには、「読み取り専用ユーザー。設定ページは作成できません。」という青いバナーが各ページに表示されます。

また、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、『Managing ASA with Cisco Defense Orchestrator』の「User Roles」を参照してください。

接続ログイン情報の更新

デバイスをオンボードするときは、そのデバイスのユーザー名とパスワードを指定します。Cisco Defense Orchestrator は、これらのログイン情報を使用してデバイスに接続し、デバイスにコマンドを送信するときにそのユーザーとして機能します。デバイスでユーザーまたはパスワードが変更された場合は、デバイスのログイン情報を更新して、それらの変更を反映できます。

詳細は、次のトピックを参照してください。

- 「Updating ASA Connection Credentials」—『Managing ASA with Cisco Defense Orchestrator』
- 「Updating AWS Connection Credentials」—『Managing AWS with Cisco Defense Orchestrator』
- 「Updating Meraki MX Connection Credentials」—『Managing Meraki with Cisco Defense Orchestrator』

ネットワーク ポリシー フィルタリングの改善

ポリシーが実行されている ASA を最初に知らなくても、ヒットカウントでネットワークポリシーをフィルタリングできるようになりました。これにより、展開内のどこでもヒットカウントがゼロのネットワークポリシーを見つけることができます。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Filtering Use Cases」を参照してください。

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。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Export Network Policy Rules」を参照してください。

2018 年 3 月 7 日

新しい CDO ポータル

ポータルを再設計して、知っておくべきこと、する必要があること、それを行う場所をすばやく伝えることができます。

カスタム URL のアップグレード

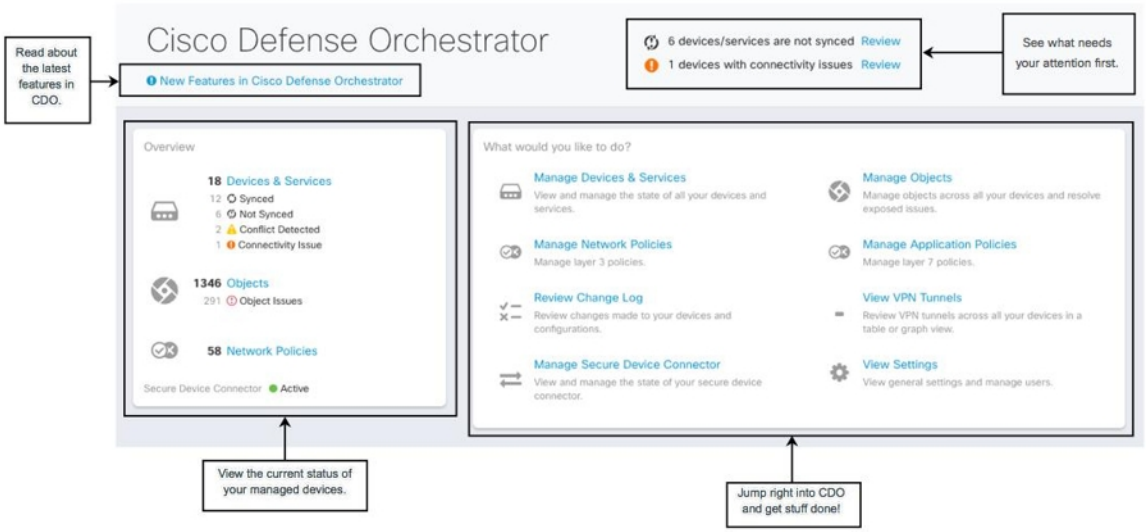
独自のイメージリポジトリに保持している ASA ソフトウェアと ASDM イメージを使用して、ASA デバイスをアップグレードできるようになりました。ASA にインターネットへのアウトバウンドアクセスがない場合、または CDO のイメージリポジトリにまだないイメージが必要な場合は、これが ASA をアップグレードする最良の方法です。FTP、TFTP、HTTP、HTTPS、SCP、および SMB のいずれかのプロトコルを使用して、リポジトリからイメージを取得できます。

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Custom URL Upgrade」を参照してください。

デバイスノート

CDO を離れることなく、特定の ASA に関するメモを単一のプレーンテキストファイルに保存できるようになりました。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Device Notes」を参照してください。

2018 年 2 月



2018 年 2 月 29 日

テナントに関連付けられているすべてのアカウントを表示する

テナントに関連付けられているすべてのユーザーを [ユーザー管理（User Management）] 画面に表示できるようになります。これには、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が含まれます。

テナントに関連付けられているユーザーを表示するには、次の手順を実行します。

1. ユーザーメニューから、[設定（Settings）] を選択します。
2. [ユーザー管理（User Management）] をクリックします。

テナントへのシスコアクセスの管理

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、シスコサポートがアカウントにアクセスしないようにすることができます。詳細については、『Managing FTD with Cisco Defense Orchestrator』の「General Settings」を参照してください。

テナントに関連付けられているすべてのアカウントを表示する

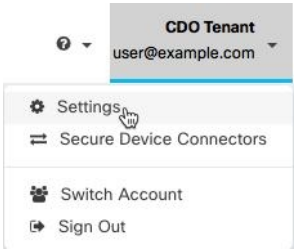
テナントに関連付けられているすべてのユーザーを [ユーザー管理（User Management）] 画面に表示できるようになります。これには、サポートチケットを解決するために一時的にアカウントに関連付けられたシスコサポートエンジニアが含まれます。

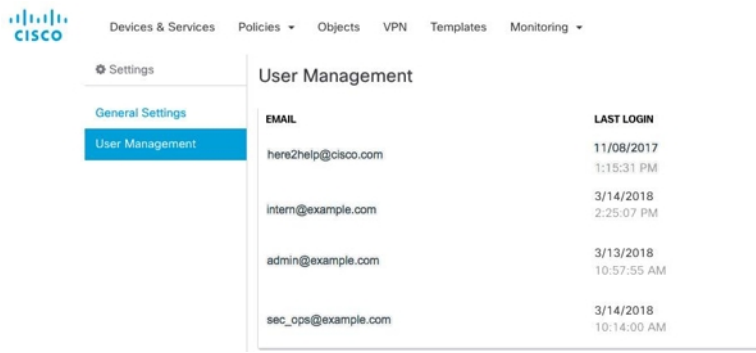
テナントに関連付けられているユーザーを表示するには、次の手順を実行します。

手順の概要

1. ユーザーメニューから、[設定（Settings）] を選択します
2. [ユーザー管理（User Management）] をクリックします

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	ユーザーメニューから、[設定（Settings）] を選択します	

	コマンドまたはアクション	目的
ステップ 2	[ユーザー管理（User Management）] をクリックします	

テナントへのシスコアクセスの管理

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、シスコサポートがアカウントにアクセスしないようにすることができます。参照先 を参照してください。

2018 年 2 月 15 日

CLI マクロを使用した ASA の管理

CDO は、カスタマイズして ASA で実行できる完全な CLI ベースのコマンドとコマンドテンプレートのリストを提供します。これらの CLI マクロは、単一の ASA または複数の ASA で一括して実行できます。定期的に監視または保守作業を行っていますか。独自の CLI ベースのコマンドを作成して CDO に保存し、必要なときに再利用できます。

CLI マクロを使用した ASA の管理

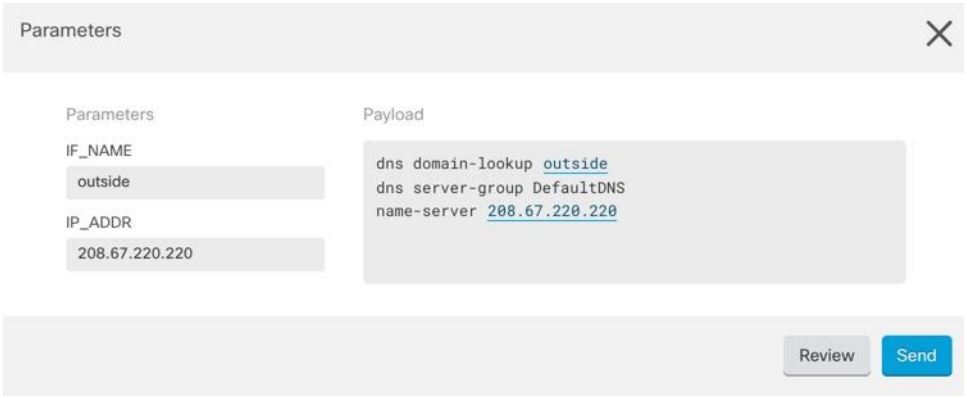
CDO は、カスタマイズして ASA で実行できる完全な CLI ベースのコマンドとコマンドテンプレートのリストを提供します。これらの CLI マクロは、単一の ASA または複数の ASA で一括して実行できます。定期的に監視または保守作業を行っていますか。独自の CLI ベースのコマンドを作成して CDO に保存し、必要なときに再利用できます。

CLI マクロを使用して ASA で DNS サーバーを設定する例を次に示します。

ステップ 1 構成する必要があるデバイスを選択します。

ステップ 2 DNS マクロの構成を選択します。

ステップ 3 パラメータフィールドに情報を入力します。

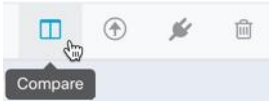


ステップ 4 それをすべての ASA に送信します。

2018 年 2 月 11 日

ASA 構成の比較

2 つの ASA 構成を簡単に比較できるようになりました。[デバイスとサービス（Devices & Services）] ページで 2 つの ASA を選択し、[比較（compare）] ボタンをクリックします。CDO は、デバイスの構成を並べて比較します。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Compare ASA Configurations」を参照してください。



2018 年 1 月

2018年1月31日

CDO を使用して最近の Cisco ASA セキュリティアドバイザリのリスクを軽減する

2018 年 1 月 29 日、シスコの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（PSIRT）は、ASA および Firepower の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。「CDO を使用して Cisco ASA アドバイザリ cisco-sa-20180129-asa1 に応答する」記事を読んで、アドバイザリの影響を受ける企業内の ASA を見つけて、パッチを適用したバージョンの ASA にアップグレードする方法を学習してください。

CDO により長い CLI シーケンスが可能

CLI のコマンドボックスにコマンドの長いリストを入力すると、CDO はコマンドを複数のコマンドに分割して、ASA API に対して一度に実行できるようにします。CDO がコマンドで適切な区切りを判断できない場合、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。

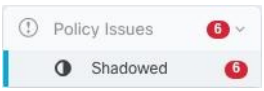
エラー：CDO は、600 文字を超える長さのこのコマンドの一部を実行しようとしました。コマンドのリストを分割して間に追加の空行を挿入することにより、適切なコマンド分離ポイントがどこにあるかを CDO に示すことができます。

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「ASA Command Line Interface」を参照してください。

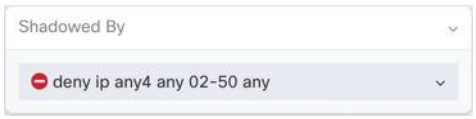
2018 年 1 月 18 日

シャドウルールの問題を管理するための機能強化

- ASA ネットワークポリシーの問題フィルタは、ポリシーにシャドウルールがあるかどうかを示します。



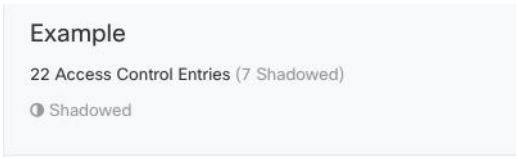
- ASA ネットワークポリシー内のルールの横にある新しいバッジ⚠は、ポリシー内の別のルールをシャドウイングしていることを示しています。
- シャドウルールの場合、ネットワークポリシーの詳細ペインは、ポリシー内のどのルールがそれをシャドウイングしているかを識別します。



- シャドウルールの問題の解決に関する新しいドキュメント。

CDO は ASA ネットワークポリシーのアクセス コントロール エントリを計算します

Cisco Defense Orchestrator（CDO）は、ASA ネットワークポリシーのすべてのルールから派生したアクセスコントロールエントリ（ACE）の数を計算し、その合計をネットワークポリシーの詳細ペインの上部に表示します。ネットワークポリシーのルールのいずれか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。

ASA には、デバイスで作成される ACE の数に推奨される制限があります。これらの推奨事項に従うことで、ASA はネットワークトラフィックを最適な速度で処理できます。未使用のルールまたはシャドウルールを削除すると、ACE の数を抑えることができます。

ネットワークポリシーの番号付き行

CDO は、ネットワークポリシーのルールを読みやすいように番号付けします。ポリシーでルールを追加および削除したり、ルールを並べ替えたりすると、行の番号が付け直されます。

2018 年 1 月 4 日

強化された ASA ネットワークポリシー管理

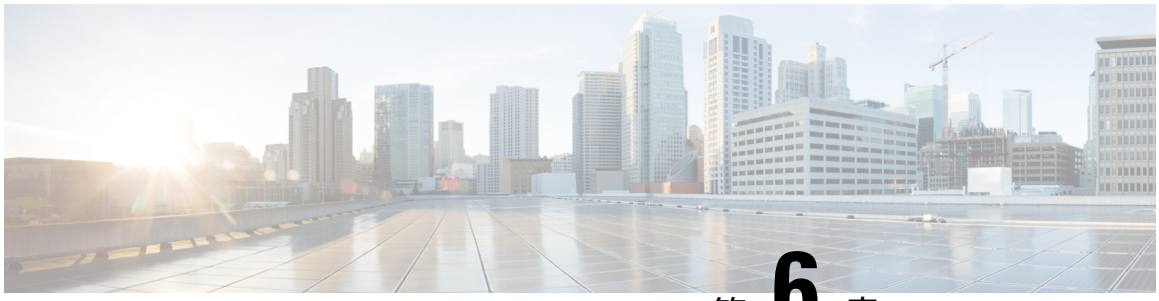
これらのタスクを ASA ネットワークポリシーで実行できるようになりました。

- **ASA デバイス間でポリシーをコピーアンドペーストします**。ポリシーを 1 つの ASA から別の ASA にコピーし、特定のインターフェイスに割り当てます。
- **ポリシー内でルールをカットアンドペーストします**。ポリシー内のルールをルールテーブルにカットアンドペーストして、ルールの優先順位を変更します。
- **ポリシー間でルールをコピーアンドペーストします**。あるポリシーから別のポリシーにルールをコピーすることにより、ポリシーの一貫性を向上します。これらのポリシーは、同じデバイスまたは異なるデバイスに置くことができます。

これらの拡張機能は、ASA ネットワークポリシーの作成、ポリシー内のルールのアクティブ化または非アクティブ化、ポリシー内のルールによって生成されたアクティビティのログ記録などの既存の機能を補完します。

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Create or Edit ASA Network Objects and Network Groups」および「ASA Network Policies」を参照し、ページの下部にあるトピックの矢印を使用して ASA ネットワークポリシーのドキュメントを移動します。

◀ ASA Network Policies | Edit an ASA Network Policy ▶



第 6 章

2017 の機能概要

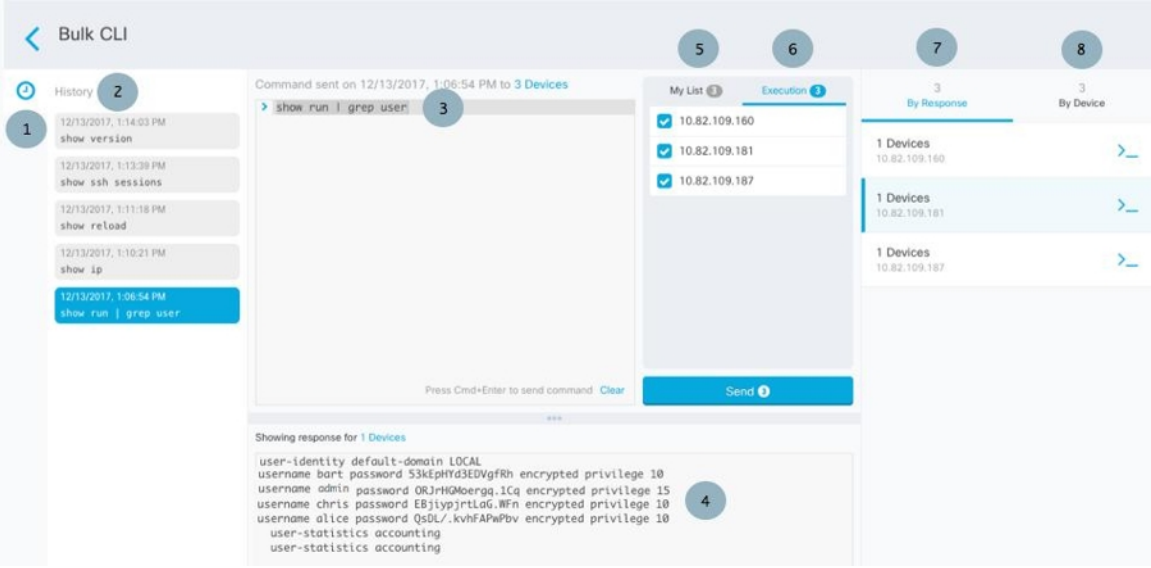
この記事では、2017 年に Cisco Defense Orchestrator に追加された機能の一部を紹介します。

2017 年 12 月

2017 年 12 月 14 日

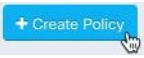
一括コマンド ライン インターフェイス

Cisco Defense Orchestrator（CDO）は、管理者が 1 つのコマンドを複数のデバイスに同時に送信する機能を提供することにより、デバイス全体で一貫した構成を促進します。CDO は、一括 CLI コマンドへの応答を応答タイプおよびデバイスタイプ別にグループ化するため、特定の応答を返した ASA と特定のコマンドを送信したデバイスを識別できます。CDO は、コマンドの履歴リストを保持しているため、コマンドを再実行したり変更したりできます。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Bulk Command Line Interface」を参照してください。



ASA ネットワークポリシーの作成

ASA のネットワークポリシーを作成できるようになりました。ポリシーにルールを追加したり、ポリシー内のルールの順序を変更したり、ポリシー内のルールをアクティブ化または非アクティブ化したり、そのポリシーを ASA から別の ASA にコピーしたりできます。開始するには、『Managing ASA with Cisco Defense Orchestrator』の「Create an ASA Network Policy」を参照してください。



2017 年 11 月

2017 年 11 月 9 日

バルク操作

特定の CDO 構成タスクを複数のデバイスで同時に実行できます。それらは「一括で」行うことができます。この機能は時間を節約し、デバイス間の一貫性を向上します。これらは、一括して実行できる操作と、それらを補完するために追加されたいくつかの追加機能です。

ASA および ASDM の一括アップグレード

CDO のアップグレードウィザードを使用して、複数の ASA の ASA および ASDM イメージを同時にアップグレードできるようになりました。必要なすべてのアップグレード手順を舞台裏で実行することにより、プロセスを簡単にします。ウィザードは、互換性のある ASA および ASDM ソフトウェアイメージを選択し、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案内します。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。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Bulk ASA and ASDM Upgrade」を参照してください。

一括読み取り構成

CDO の外部でデバイスの構成が変更された場合、CDO に保存されているデバイスの構成とデバイスのローカル構成は同じではなくなります。この場合、CDOは「競合が検出されました」というメッセージを表示して、管理者に警告します。管理者が「ポリシーの読み取り」アクションを実行すると、デバイスに保存されている構成で CDO の構成が上書きされます。2 つの構成は同じになり、「同期済み」になります。一括読み取り構成機能により、管理者はこのアクションを複数のデバイスで同時に実行できます。

一括読み取り構成のもう 1 つの用途は、CDO でステージングされた変更がデバイスに書き込まれないようにすることです。デバイスから CDO に構成を読み取ることにより、CDO でステージングされたすべての変更を上書きします。これは、必要に応じて、CDO でデバイスの構成に加えた変更を元に戻す良い方法でもあります。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Bulk Read Configuration」を参照してください。

デバイスの一括再接続

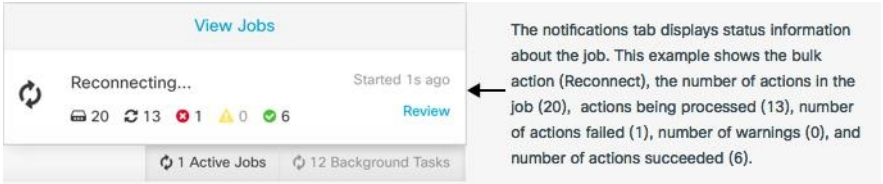
CDO を使用すると、管理者は複数の管理対象デバイスを CDO に同時に再接続を試みることができます。CDO が管理するデバイスが「到達不能」とマークされている場合、CDO は帯域外構成の変更を検出したり、デバイスを管理したりできなくなります。デバイスの再接続を試みることは、CDO によるデバイスの管理を復元するための簡単な最初のステップです。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Bulk Reconnecting Devices」を参照してください。

競合検出の一括有効化と無効化

複数のデバイスの競合検出を同時に有効または無効にすることができます。競合検出を有効にすると、CDO 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。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Enabling Conflict Detection」を参照してください。

ジョブ通知

通知タブは、CDO の右下隅にあります。ジョブで進行中のアクションのアクティブ数を表示します。



[ジョブ（Jobs）] ページ

[ジョブ（Jobs）] ページには、一括操作のステータス、成功、および失敗に関する情報が表示されます。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。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Jobs Page」を参照してください。

失敗したアクションのタスクを再開する

CDO は一括操作を記憶し、失敗した個々のアクションを識別し、失敗したアクションに対してのみタスクを再実行することで時間を節約します。[ジョブ（Jobs）] ページを確認するときに、失敗した一括操作で 1 つ以上のアクションが見つかった場合は、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。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Reinitiating a Bulk Operation that Resulted in a Failed Action」を参照してください。

NAT ドキュメント

次のユースケースの手順が文書化されています。

- 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
- パブリック IP アドレスの特定のポートでユーザーが内部ネットワーク上のサーバーを使用できるようにする
- プライベート IP アドレスの範囲をパブリック IP アドレスの範囲に変換する

CLI ロギング

CDO を使用して ASA で CLI コマンドを実行するたびに、コマンドとコマンドの結果がデバイスの変更ログに記録されるようになりました。次の例では、CLI 実行（CLI Execution）行のエントリに送信されたコマンドが示され、変更された ASA 構成（Changed ASA Config）行に、コマンドの結果として構成ファイルで変更された内容が示されています。

2017 年 10 月

2017 年 10 月 19 日

ASA の一括オンボーディング

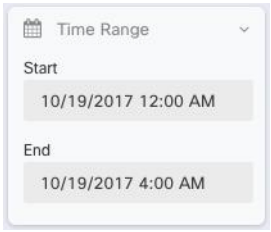
1 回のバッチで複数の ASA を CDO にオンボードできるようになりました。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Onboard ASAs in Bulk」を参照してください。

共有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。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Shared Network Policies」を参照してください。

変更ログを日時でフィルタリングする

変更ログのイベントを日時でフィルタリングできるようになりました。[監視（Monitoring）]> [変更ログ（Change Log）] の順に移動し、フィルターバーでこの日時のカレンダーを見つけます。



2017 年 10 月 12 日

パケットトレーサ

パケットトレーサは、アクセスとポリシーの問題のトラブルシューティングに役立ちます。パケットトレーサは、合成パケットをネットワークに送信し、保存されたルーティング構成、NAT ルール、およびポリシー構成がそのパケットとどのように相互作用するかを評価します。たとえば、ルールがパケットをドロップしている場合、パケットトレーサはそのルールを識別し、そのルールへのリンクを提供するため、ルールを評価して編集することができます。パケットトレーサは、ライブ、オンライン、物理、または仮想の適応型セキュリティアプライア

ンス（ASA）で使用できます。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「ASA Packet Tracer」を参照してください。

2017 年 10 月 5 日

新しいスクリーンキャスト

CDO を使用して、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単一の ASA または 2 つの ASA をアップグレードする方法を示す新しいスクリーンキャストです。

2017 年 9 月

2017年9月28日

更新されたドキュメント

- 構成の競合を解決する：デバイスが「未同期」の場合、または「競合が検出されました」と報告された場合の対処方法を説明するトラブルシューティング トピックです。
- 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：フェールオーバーモードでアクティブ-アクティブのペアとして設定された ASA の設定変更に関する重要な情報を提供します。
- 証明書の問題の解決：CDO が証明書を拒否する理由と、その対処方法について説明するトラブルシューティング トピックです。
- よくある質問ページの更新です。

2017 年 9 月 14 日

CDO サービスステータスページ

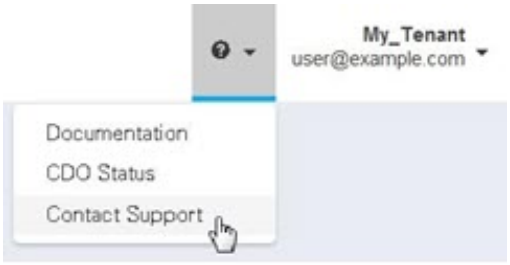
CDO は、顧客向けのサービスステータスページを https://status.defenseorchestrator.com/ で維持しています。このページには、CDO サービスが稼働しているかどうかと、サービスの中断があったかどうかが表示されます。稼働時間情報を日次、週次、または月次のグラフで表示できます。

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。

CDO サポートページ

お客様は、CDO インターフェイスを介してサポートを受けることができます。

- 有料のお客様は、新しい [サポートに問い合わせる（Contact Support）] ページの [サポートケースマネージャ（Support Case Manager）] をクリックして、シスコのテクニカル アシスタンス センター（TAC）で直接サポートケースを開く必要があります。
- デモ、社内、およびトライアルのすべてのお客様は、[サポートに問い合わせる（Contact Support）] ページの詳細リクエストフォームに質問を入力して、cdo.support@cisco.com に電子メールを送信できます。サポートスタッフができるだけ早く対応します。



2017年9月7日

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るようになりました。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 への便利な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。

2017 年 8 月

2017 年 8 月 17 日

新しいオブジェクト関数

- **重複、不整合、および未使用のオブジェクトの解決**：オブジェクトの問題を解決すると、ネットワークおよびサービスオブジェクトの可視性が向上します。グループ内のすべてのオブジェクトの統合ビューが表示されるため、オブジェクト間の比較が容易になります。オブジェクトの問題をマージ、名前変更、または無視して解決するコマンドボタンもあります。
- **新しいオブジェクトフィルタリング**：探しているオブジェクトを見つけるためのより正確な検索機能です。

2017 年 8 月 10 日

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 へのアップグレード

CDO のアップグレードウィザードの機能が拡張され、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 のアップグレードが含まれました。個々の ASA のアップグレードと同じウィザード機能を使用しますが、アクティブ/スタンバイ フェールオーバー ペアをアップグレードできるようになりました。この機能の詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Upgrading ASA and ASDM Images in an Active-Standby Pair」を参照してください。

2017 年 8 月 3 日

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の個々の ASA へのアップグレード

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 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するようになりました。必要なすべてのアップグレード手順を舞台裏で実行することにより、プロセスを簡単にします。ウィザードは、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、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案内します。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。

[デバイスとサービス（Devices & Services）] ページの詳細ペインをクリックして、アップグレードを開始します。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Upgrading ASA and ASDM Images」を参照してください。

2017 年 6 月

2017 年 6 月 20 日

デバイスとサービスのリストをエクスポートする

[インベントリ（Inventory）] ページの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できるようになりました。そこから、Microsoft Excel などのスプレッドシートアプリケーションでファイルを開いて、リスト内のアイテムを並べ替えたり、フィルター処理したりできます。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Exporting the Change Log to a CSV File」を参照してください。

2017 年 6 月 13 日

ASA 構成の復元

ASA を以前に保存した設定の 1 つに戻すことができるようになりました。これは、予期しない、または望ましくない結果をもたらした構成変更を削除する便利な方法です。復元する ASA 設定を選択すると、CDO はその設定とメモリに最後に保存された設定の比較を表示します。目的の設定を復元することに問題がなければ、復元できます。

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Restoring ASA Configurations」を参照してください。

2017 年 5 月

2017 年 5 月 3 日

変更要求管理

別のチケットシステムで開かれた変更要求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るようになりました。変更要求管理を使用すると、CDO で変更要求を作成し、一意の名前で識別し、変更の説明を入力して、変更要求を変更ログイベントに関連付けることができます。後で変更ログで変更要求名を検索できます。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Change Request Management」を参照してください。

2017 年 4 月

検索の改善：[インベントリ（Inventory）] ページの検索バーで部分一致がサポートされるようになり、必要なデバイスまたはサービスを簡単に見つけられるようになりました。

VPN：さまざまな使いやすさが改善されました。

2017 年 2 月

Cisco Defense Orchestrator の新しい EMEA サイト

Application Visibility Control（AVC）ID プロファイルのサポート

2017 年 1 月

読み取り専用 IPSec VPN トンネル管理

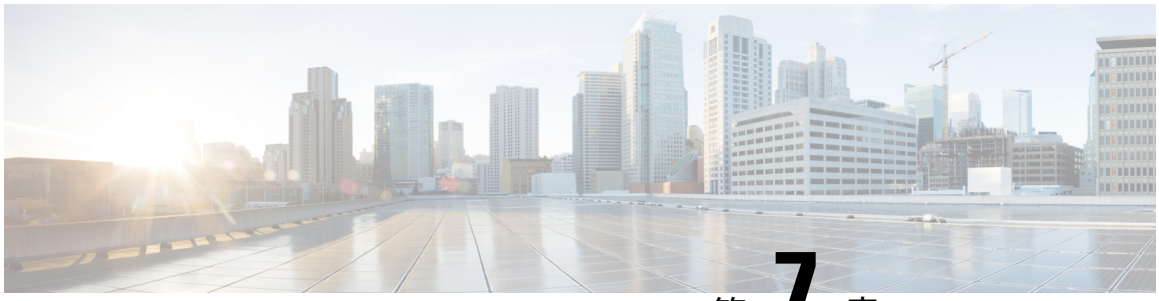
Cisco Defense Orchestrator は、IPsec サイト間 VPN ASA デバイス構成の解析と処理をサポートするようになりました。ネットワークベースの VPN トンネルダイアグラムが利用可能であり、単一のピアに接続されているすべてのトンネルの完全なビュー、アクセスポリシー、キー交換暗号化、およびその接続ステータスを含むトンネルの詳細を提供します。CDO は、組織のオンボード ASA デバイスの構成で使用可能なすべてのトンネルの完全なビューも提供します。CDO の新しい VPN 管理機能により、組織およびネットワーク運用エンジニアは次のことができます。

- デバイスごととすべてのデバイスの両方で、VPN トンネル全体を視覚化します
- トンネルの接続状態を使用し、アクセスポリシーとクリプトマップ暗号化を一目で確認できるため、トンネルの設定ミスを簡単に特定できます

VPN は安全ですが、安定した安全な通信を確保するために適切に構成する必要があります。CDO は、ユーザーが VPN 構成を組織的に表示できるようにして、肥大化した古いポリシーの削減を促進します。

ネットワークおよびサービス シングル オブジェクトのサポート

現在利用可能なオブジェクトグループのサポートに加えて、Cisco Defense Orchestrator では、アクセスルールの変更時に、または[オブジェクト（Objects）]ページから直接、ネットワークタイプとサービスタイプの両方の単一オブジェクトを作成できるようになりました。



第 7 章

2016 の機能概要

この記事では、2016 年に Cisco Defense Orchestrator に追加された機能の一部について説明します

2016 年 12 月

2016年12月22日

NAT ポリシー管理

Cisco Defense Orchestrator は、使いやすいナビゲーションウィザードと高度なインターフェイスベースのダイアグラムを介してNATポリシーの読み取り、編集、検索、および作成をサポートし、ASA デバイスで定義された NAT ポリシーの完全なリスト（およびその順序）を表示するようになりました。

2016 年 12 月 15 日

廃止された名前（オブジェクト）の変換

お使いのデバイスの設定には、レガシーの（廃止された）名前が含まれていますか。Cisco Defense Orchestrator では、オブジェクトの問題の解決中に、オブジェクト、オブジェクトグループ、名前全体を調査して、ポリシーで使用されるすべてのオブジェクトに一貫性を持たせ、名前からオブジェクトへの変換を支援できるようになりました。

2016 年 11 月

2016 年 11 月 18 日

完全にシャドウされたルールのサポート

すべてのトラフィックはルールセットの順序でルールによって処理されるため、意図したトラフィックを処理しない余分なネットワークポリシーをフィルタリングして特定できるようになりました。ネットワークポリシーに変更を加えると、編集または追加されたルールが別のルールによってシャドウされている場合、CDO はアラートを出します。

2016 年 11 月 8 日

オンプレミスの Secure Device Connector

Cisco Defense Orchestrator は、CDO とサポートされているデバイスおよびサービスとの間の直接通信を可能にします。この通信は、リモートロケーションと CDO クラウドサービス間のプロキシとして機能する CDO Secure Device Connector（SDC）によって可能になります。このサービスは、次の 2 つの展開モデルで利用できるようになりました。

オンプレミス セキュア デバイス コネクタ – オンプレミス セキュア デバイス コネクタは、要求されたアカウント専用の事前構成された仮想アプライアンスです。

クラウド セキュア デバイス コネクタ – すべてのクラウド セキュア デバイス コネクタは自動的にプロビジョニングされ、Cisco Defense Orchestrator チームによって管理されます。

2016 年 9 月

2016 年 9 月 29 日

ログの変更

Cisco Defense Orchestrator を介して実行されたアプリケーション（レイヤ 7）とネットワーク（レイヤ 3）の両方のポリシー変更を、オンボードのデバイスとサービス全体で 1 つのビューで継続的にキャプチャします。新しい変更ログには、最新の変更がひと目でわかるビューが一覧表示されます。さらに、デバイス、変更ステータス、ユーザーなどでリビジョンを並べ替えたり、フィルタリングしたりできます。新しい変更ログ機能により、組織は次のことができます。

- ネットワークおよびアプリケーションポリシーの変更（新規、編集、および削除されたルール、オンボードまたは削除されたデバイスおよびサービスなど）の前後のインライン増分表示（差分）

- ポリシー変更の競合の検出（Cisco Defense Orchestrator の外部で発生）およびデバイスまたはサービスとの間の上書き
- インシデントの調査またはトラブルシューティング中に、誰が、何を、いつ、に回答可能
- 一般的な形式またはサードパーティの監視システムにエクスポート

（注） Cisco Defense Orchestrator によって現在管理されているデバイスとサービスは、最初の展開または読み取りの後にのみ、変更ログイベントの収集を開始します。詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Secure Logging Analytics for FTD Devices」を参照してください。

ヒット率。Cisco Defense Orchestrator により、ネットワーク運用ユーザーは、安全でスケーラブルなポリシーの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、根本原因への迅速な実用的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できます。新しいヒット率機能により、組織は次のことができます。

- 古くて一致したことのないポリシールールを排除し、セキュリティ体制を強化
- 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（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）
- 設定されたデータ保持（1 年間）のデバイスまたはポリシールールがリセットされても、ヒット率の履歴情報を維持
- 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。それらの更新または削除についての疑問を解消
- 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

2016 年 9 月 23 日

ユーザーインターフェイスの再設計：ライトテーマへの変更

Cisco Defense Orchestrator のユーザーエクスペリエンスを、軽量でまったく新しいユーザー エクスペリエンス テーマで再設計し、より直感的で自明の Cisco スタイルに合わせます。お試しください。

複数のオブジェクトのサポート

Cisco Defense Orchestrator オブジェクト管理により、オブジェクトおよびオブジェクトグループ値のインライン編集が可能になり、単一のアクセスリストパラメータで複数のオブジェクト

を参照できるようになりました。ユーザー定義のオブジェクトグループに自動的に割り当てます（dm_inline_* オブジェクトを作成する必要はありません）。

アウトオブバンドポリシーの変更を承認または拒否する

実行されたリモート変更または変更内容（デバイスまたはサービス上）を特定するだけでなく、特定されたアウトオブバンド変更をリアルタイムで承認または拒否する機能により、ポリシー オーケストレーションの実施が強化されました。

2016 年 8 月

2016 年 8 月 18 日

委任管理サポート

委任管理のサポート。Cisco Defense Orchestrator を使用すると、アカウントのセキュリティを維持し、アカウント（テナント）間の完全なデータ分離を維持しながら、ユーザーごとに複数のアカウント（テナント）を管理して、割り当てられたアカウント間のピボットをより簡単かつ迅速に行うことができます。

事前定義されたテンプレートのインポートとエクスポート

事前定義テンプレートのインポートを有効にします。組織内またはサードパーティから入手可能な事前定義されたデバイス構成テンプレートを活用して、組織内のすべてのデバイスとサービスをオンボーディングするスケーラブルなオーケストレーションを可能にします。

デバイスとサービスの接続ステータス管理

デバイス接続ステータスの評価。新しい [再接続（Reconnect）] ボタンが追加され、デバイスとサービスの可用性の状態を継続的に監視できるようになり、変更またはアクションを自動的にまたはオンデマンドで実行する必要がある場合にアラートが表示されます（デバイスログイン情報の更新、デバイス証明書の更新など）。

2016 年 8 月 11 日

テンプレート管理の強化

テンプレート管理の機能強化。新規のデバイステンプレート構成ファイルを作成するとき、または既存のデバイステンプレート構成ファイルを更新するとき、Cisco Defense Orchestrator ユーザーは、デバイス構成ファイル全体を簡単に検索し、アカウントのデバイス間で使用するために、新規または既存のパラメータに複数の値を割り当てることができるようになりました。

.テンプレートの作成と管理の詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Templates」を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。