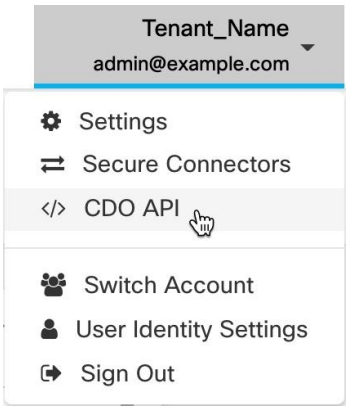
2020 の機能概要

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

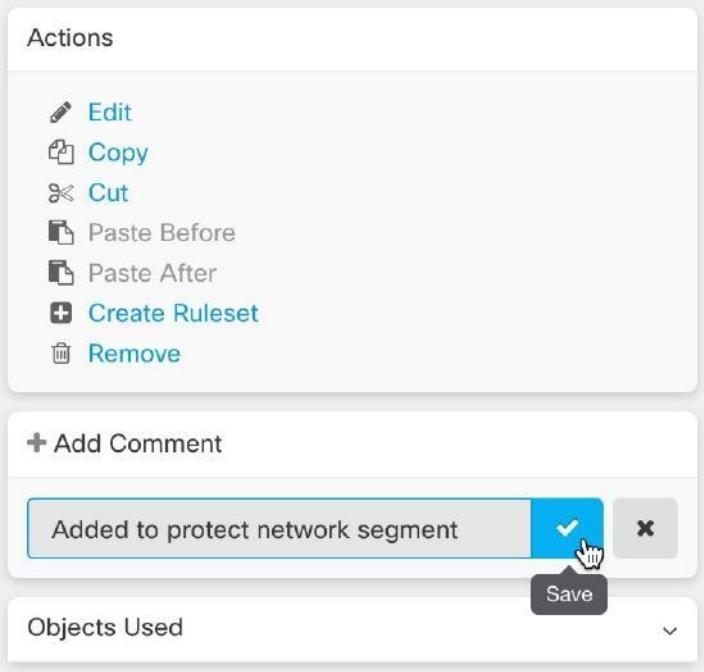
FTD 設定のエクスポート

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。

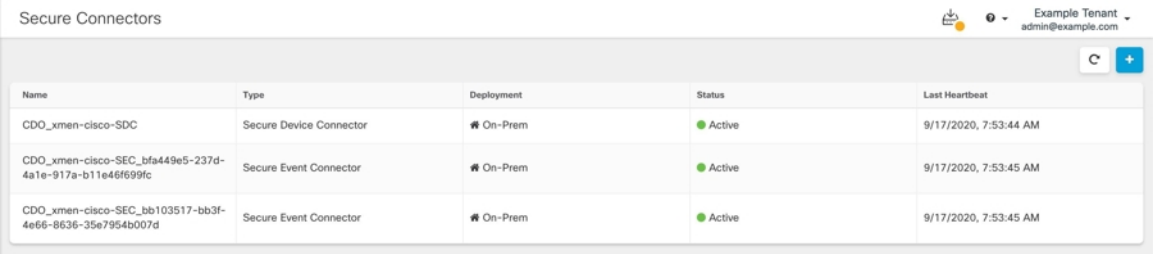
詳細については、『Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator』の次のトピックを参照してください。

- 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。

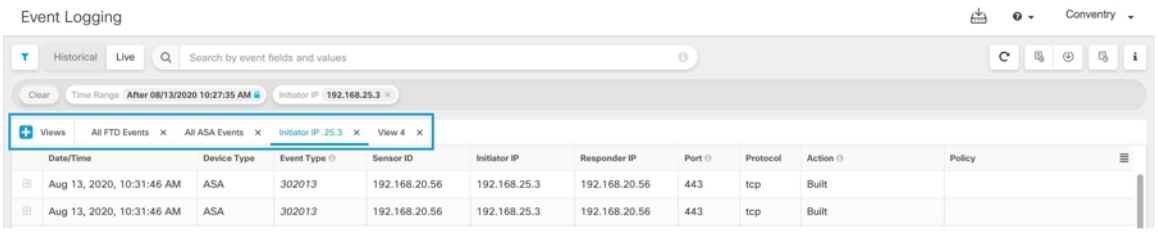
FMC のオンボーディングについては、『Managing FMC with Cisco Defense Orchestrator』の「Onboard an FMC」を参照してください。

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。

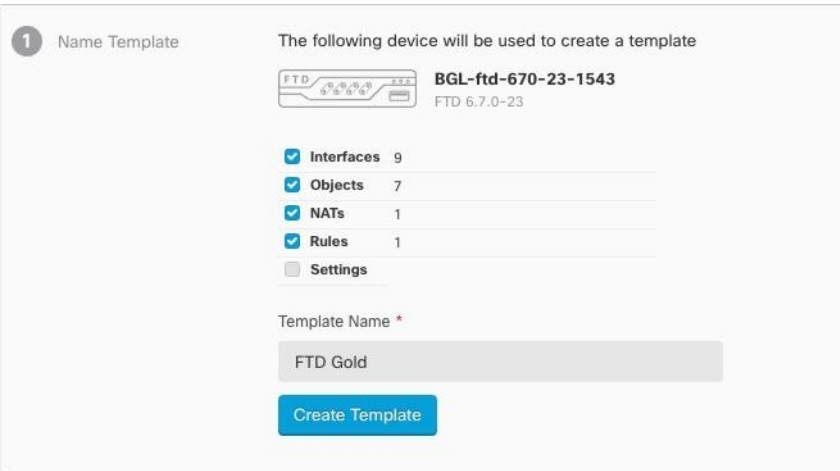
2020 年 8 月 13 日

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。

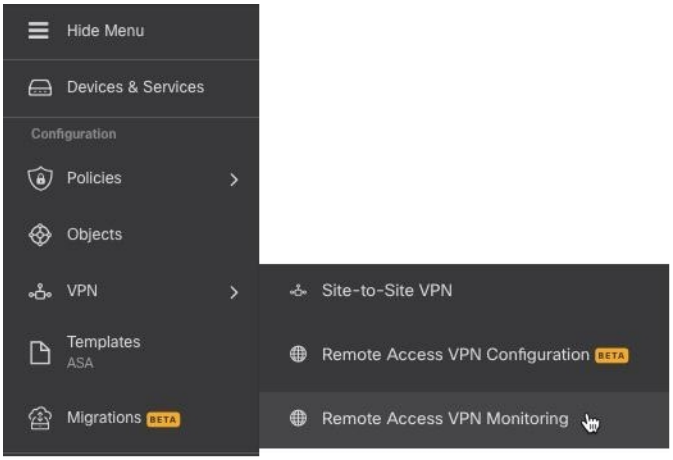
テナント内の各 RA VPN ヘッドエンドのパフォーマンスを表示し、ヘッドエンドでセッションをフィルタリングし、VPN モニタリングテーブルに表示するセッションプロパティを選択できます。また、1 つ以上のデバイスの RA VPN セッションをコンマ区切り値（.csv）ファイルにエクスポートできます。詳細については、『Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator』の「Export RA VPN Sessions to a CSV File」を参照してください。

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。

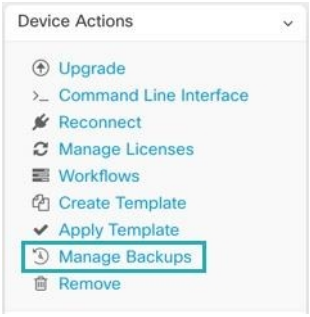
詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Create API Only Users」を参照してください。

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

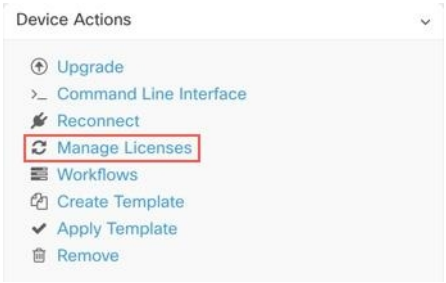
CDO から直接 FTD デバイスに CLI 要求を発行できるようになりました。

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。

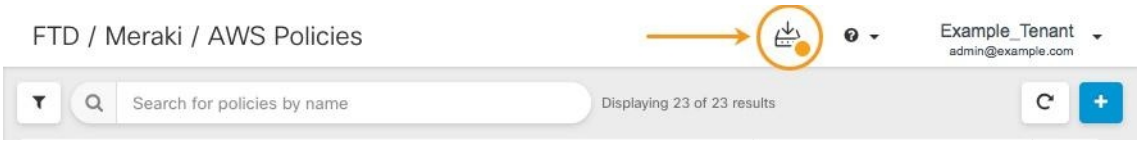
詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Configure Site-to-Site VPN Connections with Dynamically-Addressed Peers」を参照してください。

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

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。