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 ニ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。

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。