2022 の機能概要

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 12 月

2022 年 12 月 15 日

Cisco Defense Orchestrator は、クラウド提供型 Firewall Management Center の更新をリリースしました。クラウド提供型 Firewall Management Center のリリースノート [英語] を読み、更新に含まれる新機能について確認してください。

2022 年 12 月 1 日

Cisco ASA のルートベースのサイト間 VPN サポート

Cisco Defense Orchestrator を使用して、仮想トンネルインターフェイスが設定されているピア間にサイト間 VPN トンネルを作成できるようになりました。これは、各トンネルの終端に IPsec プロファイルが付加されたルートベースの VPN をサポートします。IPSec トンネルにルーティングされるトラフィックはすべて、送信元/接続先のサブネットに関係なく暗号化されます。

VTI ベースの VPN は、次の間で作成できます。

- CDO 管理対象の Cisco ASA およびルートベースの VPN 対応デバイス。
- 2 つの CDO 管理対象 ASA。

詳細については、「Site-to-Site Virtual Private Network」[英語] を参照してください。

グローバル検索

CDO でグローバル検索機能を使用すると、CDO の管理対象デバイスを検索してナビゲートできます。この機能により、クラウド提供型 Firewall Management Center で管理されているデバイスの検索機能を、CDO ユーザーインターフェイスからサポートできるようになりました。検索結果から、クラウド提供型 Firewall Management Center 内の対応するページに移動できます。

詳細については、「Global Search」[英語] を参照してください。

2022 年 10 月

2022 年 10 月 27 日

Duo Admin Panel のオンボーディングと多要素認証ロギング

CDO は Duo Admin Panel をオンボードして、ログを MFA イベントとしてダッシュボードに表形式で表示できるようになりました。また、1 つ以上のデバイスの MFA セッションをコンマ区切り値（.csv）を含むファイルにエクスポートできます。

Duo Admin Panel には、ユーザーの二要素認証の成功や失敗に関する情報を含む多要素認証（MFA）ログが記録されます。

詳細については、Cisco Defense Orchestrator ガイド [英語] の「Onboard Duo Admin Panel」および「Monitor Multi-Factor Authentication Events」を参照してください。

2022 年 10 月 12 日

Cisco ASA のポリシーベースのサイト間 VPN ウィザード

CDO で、2 つのピア間にポリシーのベースサイト間 VPN トンネルを設定できるようになりました。これは、IPSec トンネルにルーティングされるトラフィックはすべて、送信元/接続先のサブネットに関係なく暗号化されることを意味します。

ポリシーベースのサイト間 VPN を設定するには、次のいずれかの条件を満たす必要があります。

- 両方のピアが CDO 管理対象の Cisco ASA である。
- ピアの 1 つは CDO 管理対象の Cisco ASA で、もう 1 つはポリシーベースの VPN 対応デバイスである。

詳細については、「Site-to-Site Virtual Private Network」[英語] を参照してください。

2022 年 8 月

2022 年 8 月 4 日

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

CDO は、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 へのオンボード。
- 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。外観や動作もオンプレミス型の Cisco Secure Firewall Management Center と同じで、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、選択したログコレクタにセンサーから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になります。たとえば、CDO はパブリッククラウドにあり、Active Directory や ISE/ISE-PIC がプライベートクラウドにある場合があります。

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、Cisco Meraki、Cisco IOS デバイス、Cisco 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 アカウントにすで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 にオンボードできます。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 をオンボードする前に、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

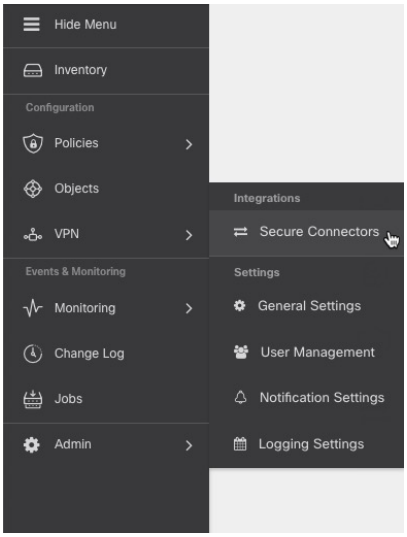
ASA ポリシーで IPv6 をサポート

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、および Cisco Meraki 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

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 デバイスのオンボードをサポートしています。

Secure Firewall Threat Defense デバイスは、ゼロ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オンボードできます。

2022 年 2 月

2022 年 2 月 3 日

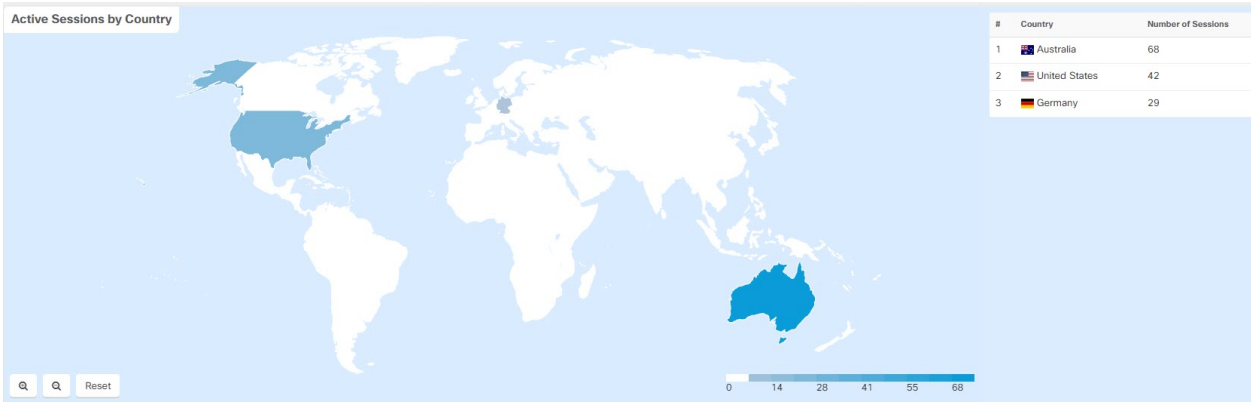
ユーザー管理の Active Directory（AD）グループ

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。



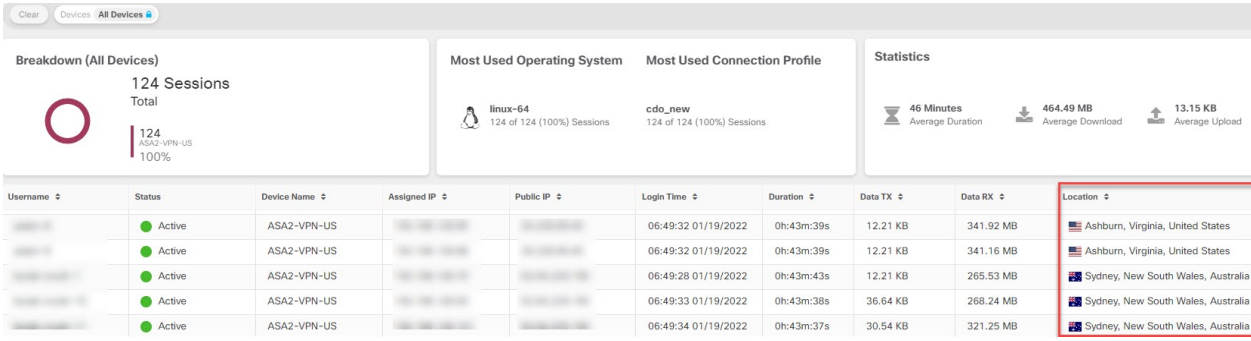
詳細については、使用しているファイアウォールに応じて、『Cisco Defense Orchestrator での FTD の管理』、『Cisco Defense Orchestrator による ASA の管理』の「Monitoring Remote Access Virtual Private Network Sessions」を参照してください。

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

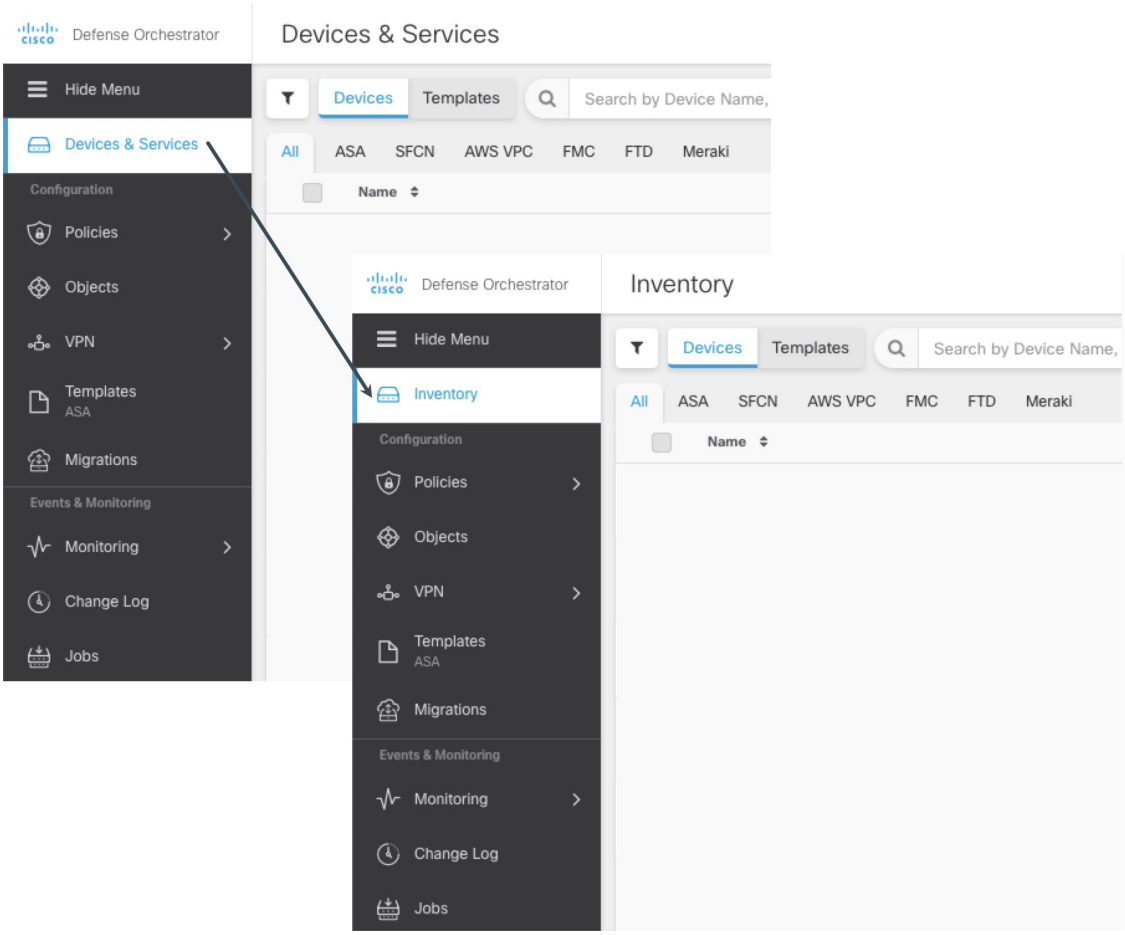
リモートアクセス VPN モニタリングページに、VPN ヘッドエンドに接続しているすべてのユーザーの場所が表示されるようになりました。CDO は、ユーザーのパブリック IP アドレスを地理的に特定することによって、この情報を取得します。この情報は、ライブビューと履歴ビューで利用できます。左ペインの [ユーザーの詳細（User Details）] エリアで場所をクリックすると、ユーザーの正確な場所が地図上に表示されます。



（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

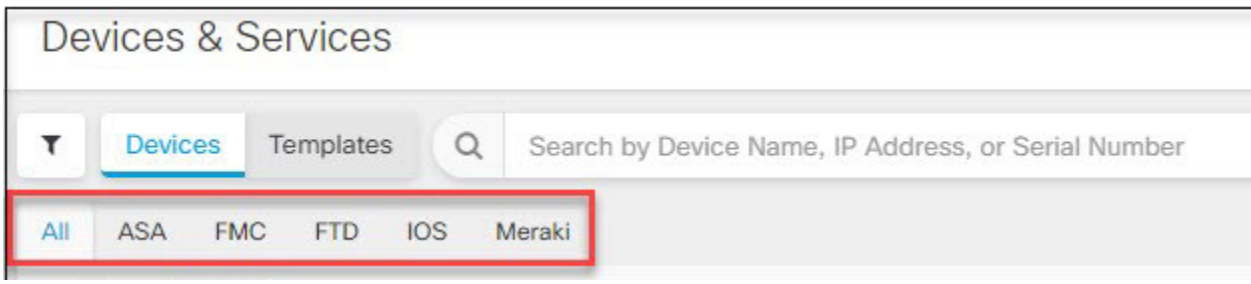
[デバイスとサービス（Devices & Services）] ページの名前が「インベントリ（Inventory）」に変更されました。Inventory テーブルには、CDO で管理するすべてのデバイスとサービスが一覧表示されます。名前の変更の結果として追加または削除された機能はありません。



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

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。