2023 の機能概要

この章では、2023 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。

2023 年 12 月

2023 年 12 月 14 日

Threat Defense デバイスの追加イベントタイプの監視

CDO は、Threat Defense デバイス用の AAA 、BotNet、フェールオーバー、SSL VPN などの新しいファイアウォールイベントのタイプをサポートするようになりました。

[分析（Analytics）] > [イベントロギング（Event Logging）] に移動し、[FTDイベント（FTD Events）] で使用可能なイベントの新しいリストからフィルタ処理します。詳細については、「Event Types in CDO」[英語] を参照してください。

2023 年 12 月 7 日

CDO を使用したオンプレミス Firewall Management Center ネットワークオブジェクトの管理

CDO 管理対象オンプレミス Firewall Management Center から、他の オンプレミス Firewall Management Center や クラウド提供型 Firewall Management Center によって管理される Threat Defense デバイス、および CDO 管理対象 ASA や 脅威に対する防御 デバイスに対するのネットワークオブジェクトを管理および共有できるようになりました。その結果、CDO の管理対象プラットフォーム間でネットワークオブジェクトの定義の一貫性が促進されます。

オンプレミス Firewall Management Center をオンボーディング後、**[ツールとサービス（Tools & Services）] > [Firewall Management Center]** に移動し、デバイスを選択して [設定（Settings）] を選択し、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] トグルボタンを有効にします。

詳細については、「Discover and Manage On-Prem Firewall Management Center Network Objects」[英語] を参照してください。

2023 年 11 月

2023 年 11 月 30 日

クラウド提供型 Firewall Management Center での Cisco Secure Firewall Threat Defense デバイスバックアップのスケジュール

クラウド提供型 Firewall Management Center を使用して、管理する Cisco Secure Firewall Threat Defense デバイスのスケジュール済みバックアップを実行します。

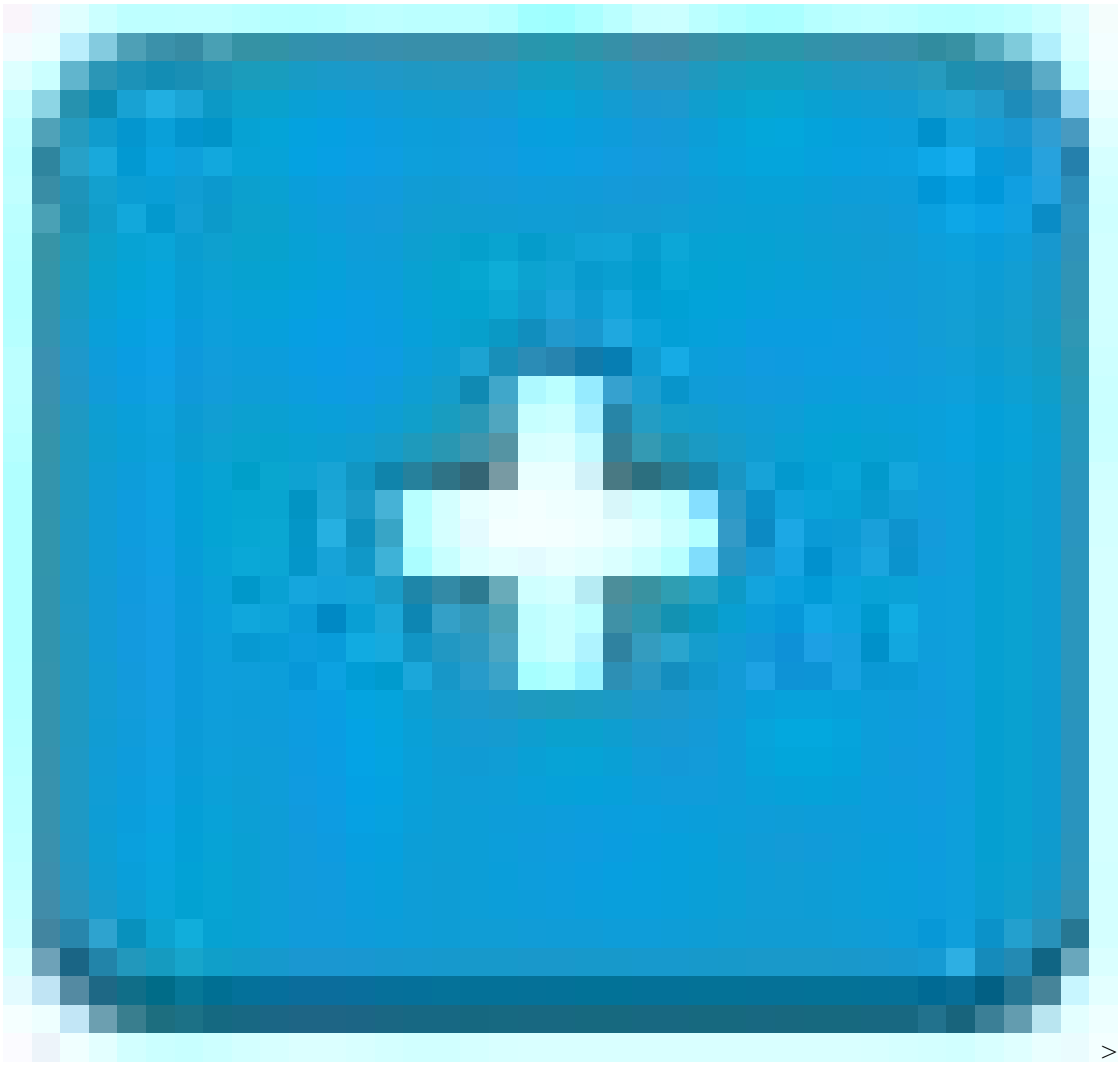
詳細については、「Schedule Remote Device Backups」[英語] を参照してください。

2023 年 11 月 14 日

クラウド提供型 Firewall Management Center のプロビジョニングの改善

CDO は、クラウド提供型 Firewall Management Center 用の拡張された高速なプロビジョニングプロセスを提供するようになりました。テナントでクラウド提供型 Firewall Management Center を有効にすると、CDO は自動的にプロビジョニングし、CDO 通知センター、および着信ウェブフックを設定したアプリケーションを介して通知します。有効にするには、**[ツールとサー**

ビス（**Tools & Services**）] > **[Firewall Management Center]** >



> **[FMC]** > **[クラウド提供型 FMCの有効化（Enable Cloud-Delivered FMC）]** の順に選択します。

詳細については、「Enable Cloud-delivered Firewall Management Center on Your CDO Tenant」[英語] および「Notification Settings」[英語] を参照してください。

2023 年 11 月 2 日

ゼロ タッチ プロビジョニング を使用したオンプレミス Management Center への 脅威防御 デバイスのオンボード

ゼロタッチプロビジョニング メソッドを使用して Threat Defense デバイスをオンボードするときに、管理プラットフォームとして オンプレミス Firewall Management Center を選択できるようになりました。その結果、新しいデバイス、または以前に設定または管理されていないデバイスのオンプレミス管理がサポートされます。詳細については、「Onboard a Secure Firewall Threat Defense Device With Zero-Touch Provisioning」[英語] を参照してください。

2023 年 10 月

2023 年 10 月 26 日

Firewall 移行ツールの更新

CDO は、Firewall 移行ツールの更新バージョンをホストします。CDO を使用して、Cisco Secure Firewall ASA デバイスにある複数のトランスペアレント ファイアウォール モードのコンテキストをトランスペアレントモードのインスタンスにマージして移行できます。

さらに、サイト間およびリモートアクセス VPN 設定を Fortinet および Palo Alto Networks ファイアウォールから、シスコのクラウド提供型 Firewall Management Center で管理されている Threat Defense に移行できます。詳細については、『Cisco Secure Firewall 移行ツール リリースノート』を参照してください。

2023 年 10 月 19 日

クラウド提供型 Firewall Management Center の更新

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。更新に含まれる多くの新機能については、クラウド提供型 Firewall Management Center のリリースノート [英語] を参照してください。新機能の完全なリストについては、『クラウド提供型 Firewall Management Center のリリースノート：Cisco Defense Orchestrator の機能』を参照してください。

サイト間 VPN 接続を使用したオンプレミスからクラウド提供型 Firewall Management Center への Cisco Secure Firewall Threat Defense デバイスの移行

Cisco Secure Firewall Threat Defense デバイスのサイト間 VPN 設定は、デバイスがオンプレミスの Firewall Management Center からクラウド提供型 Firewall Management Center に移行されるときに、残りの設定とともに移行されるようになりました。詳細については、「Migrate On-Prem Management Center managed Secure Firewall Threat Defense to Cloud-delivered Firewall Management Center」[英語] を参照してください。

2023 年 10 月 12 日

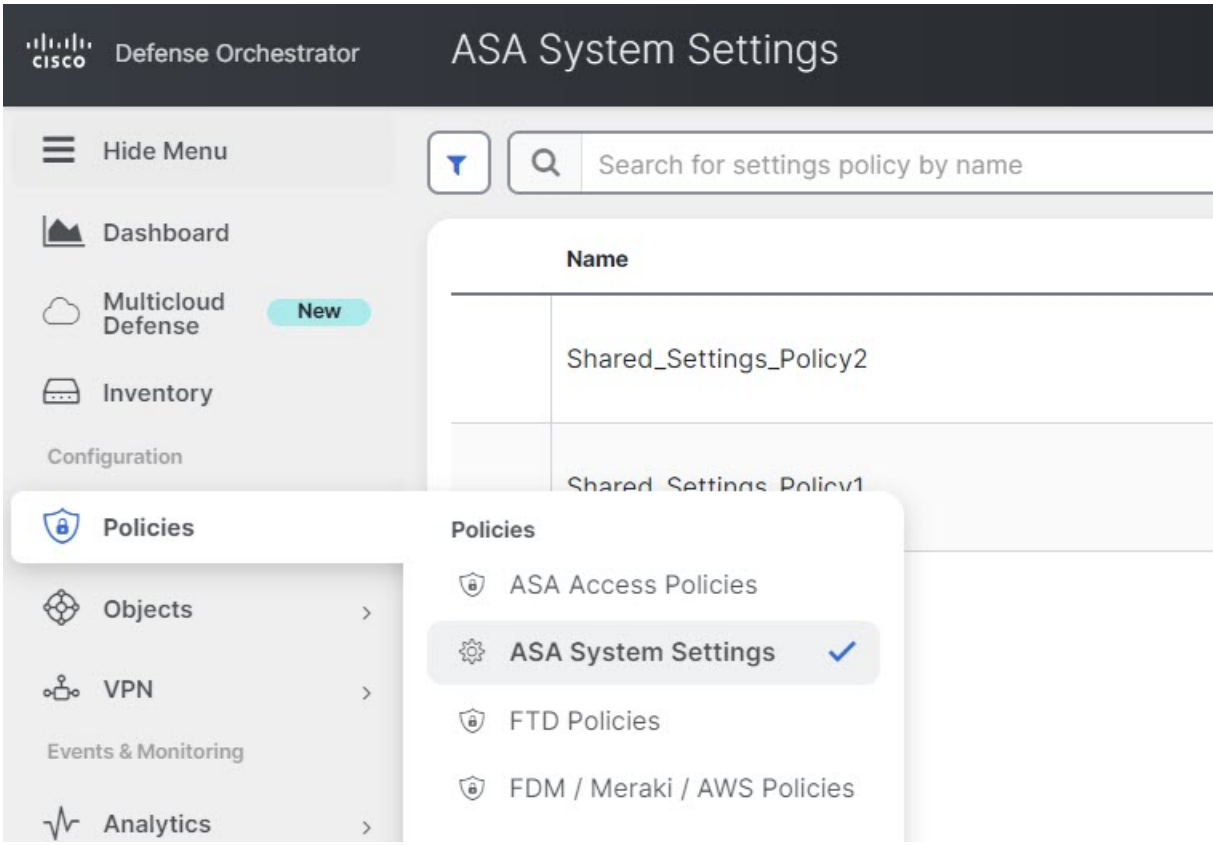
Cisco ASA システム設定ポリシー

CDO には、システム設定ポリシーを作成して、ドメインネームサービス、HTTP、セキュアコピーサーバーの有効化、メッセージロギング、アクセス制御リストをチェックしない VPN トラフィックの許可など、Cisco ASA デバイスの重要な設定を簡単に管理する機能があります。システム設定ポリシーは複数の Cisco ASA デバイスに適用でき、ポリシーに加えられた変更は、このポリシーを使用するすべてのデバイスに影響します。さらに、単一の Cisco ASA デバ

イスのデバイス固有の設定を個別に編集し、デバイス固有の値で共有システム設定をオーバーライドできます。

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

[ポリシー（Policies）] > [Cisco ASAシステム設定（ASA System Settings）] の順に選択します。



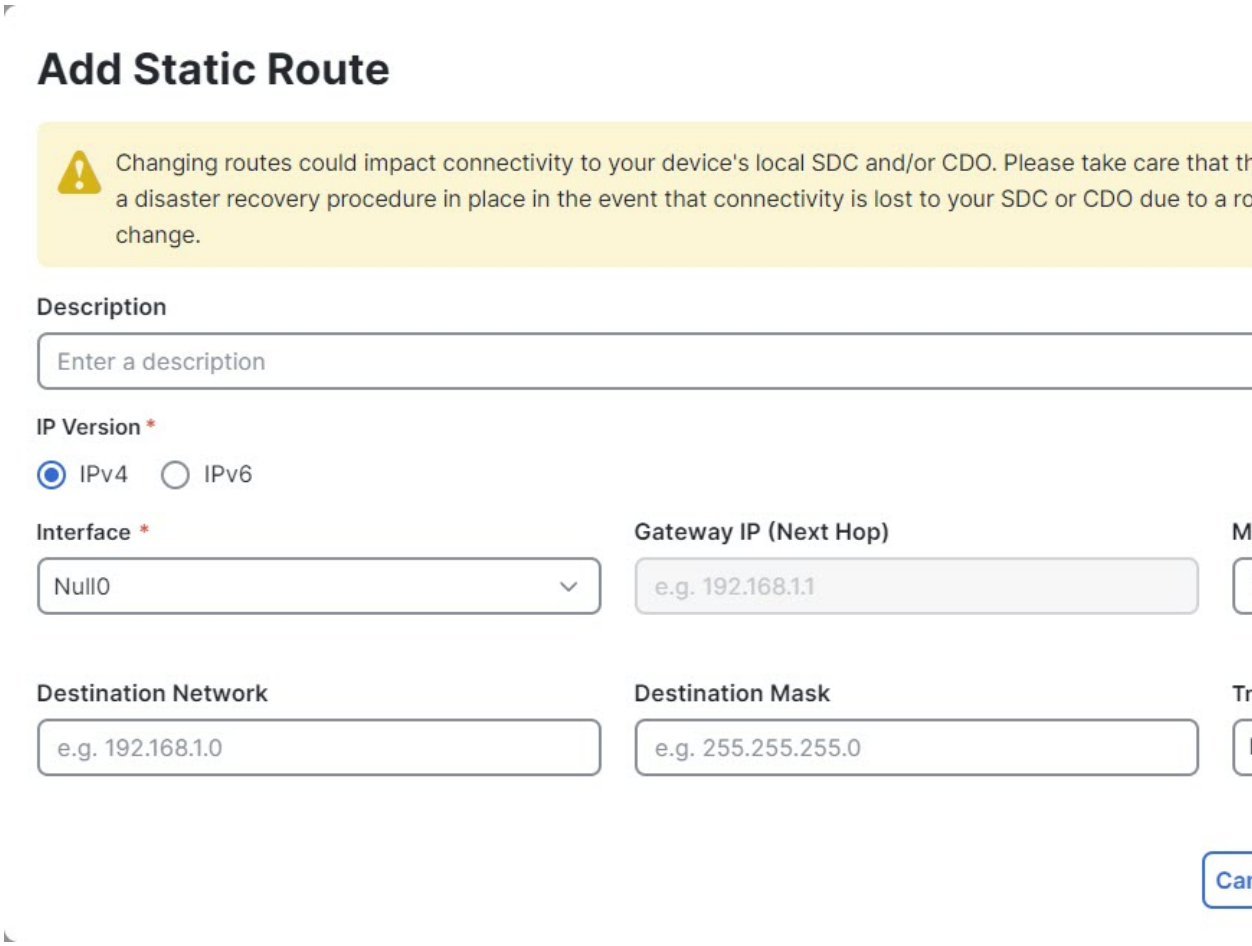
2023 年 10 月 5 日

Cisco ASA スタティックルーティングの CDO サポート

CDOユーザーインターフェイスを使用して、Cisco ASAのスタティックルートを設定できるようになりました。この機能を使用すると、CLIを使用せずに、特定のIPv4またはIPv6宛先ネットワークのトラフィックの送信先を指定できます。

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

[インベントリ（Inventory）] > [Cisco ASA（ASA）] タブ > [ルーティング（Routing）] の順に選択します。



Terraform を使用した CDO の管理

Terraform を使用し、Infrastructure as Code（IaC）の原則を使用して CDO インフラストラクチャの管理を自動化するできるようになりました。CDO は、セキュアなデバイスコネクタとセキュアなイベントコネクタを迅速に展開するための Terraform プロバイダーと Terraform モジュールを提供します。詳細については、「Terraform」[英語] を参照してください。

2023 年 9 月

2023 年 9 月 14 日

Secure Event Connector のナビゲーションの変更

右上の管理メニューを展開して [セキュアコネクタ（Secure Connectors）] ページにアクセスできなくなりました。セキュアコネクタを管理するには、**[ツールとサービス（Tools & Services）]**>

[セキュアコネクタ（Secure Connectors）] の順に選択します。詳細については、「Secure Event Connectors」[英語] を参照してください。

2023 年 9 月 7 日

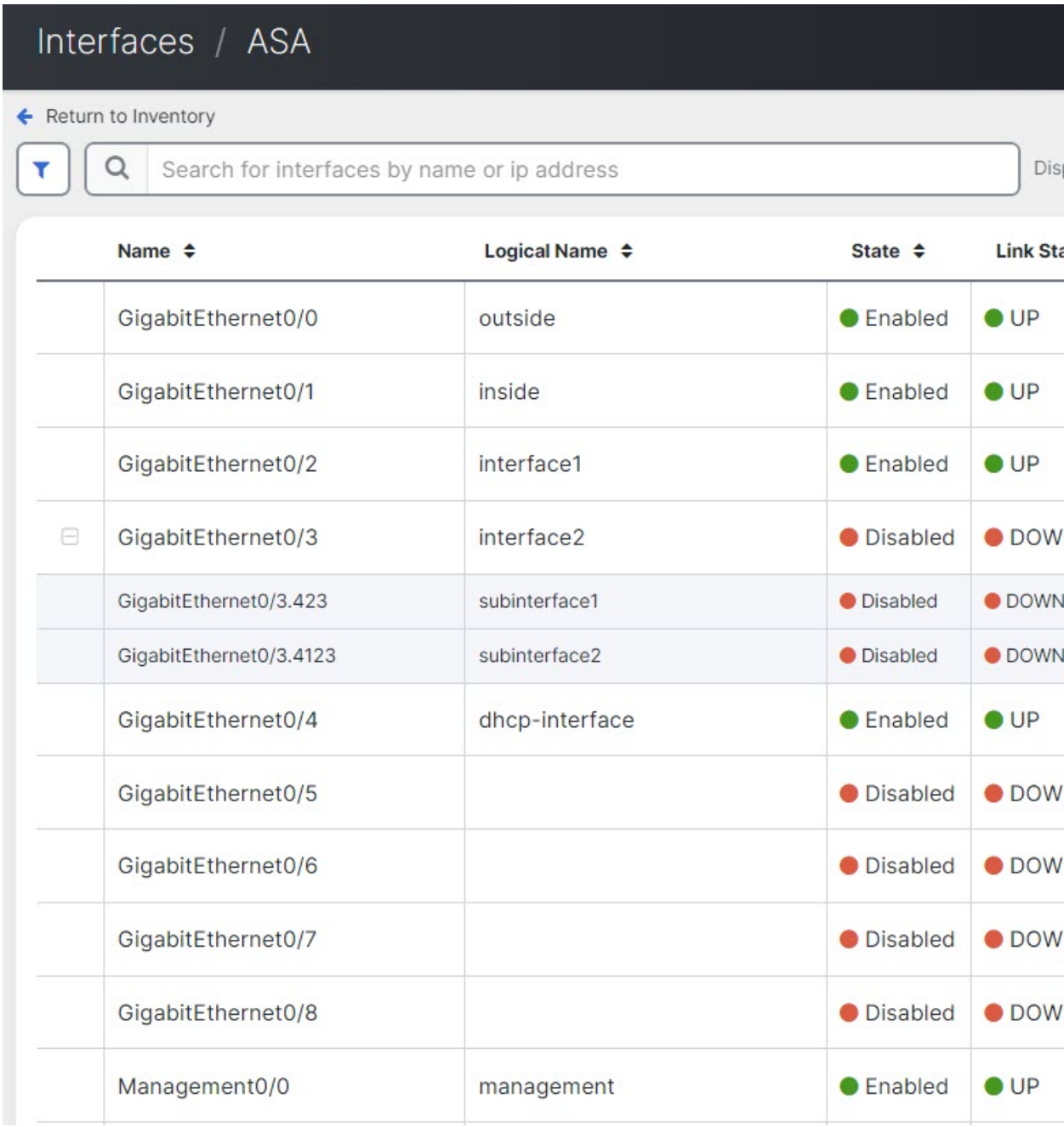
CDO ユーザーインターフェイスを使用した Cisco ASA インターフェイスの設定

CDO のグラフィカル ユーザー インターフェイスを使用して、Cisco ASA の物理ネットワークインターフェイス、論理的なサブインターフェイス、VLAN、および EtherChannel を設定できるようになりました。ルートベースのサイト間 VPN で作成された仮想トンネルインターフェイスも表示できます。

（注） VLAN では 110 デバイスのみサポートされます。

詳細については、「Configure ASA Interfaces」[英語] 参照してください。

[インベントリ（Inventory）]、[Cisco ASA（ASA）]、[管理（Management）]、[インターフェイス（Interfaces）] の順に選択します。

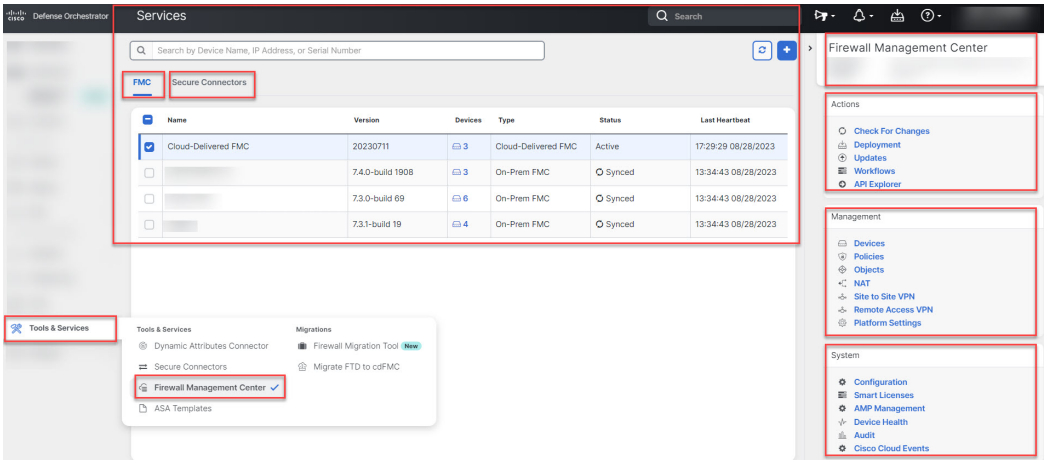

Interfaces / ASA
Return to Inventory
Search for interfaces by name or ip address
Name
Logical Name
State
Link Sta
GigabitEthernet0/0
outside
Enabled
UP
GigabitEthernet0/1
inside
Enabled
UP
GigabitEthernet0/2
interface1
Enabled
UP
GigabitEthernet0/3
interface2
Disabled
DOW
GigabitEthernet0/3.423
subinterface1
Disabled
DOWN
GigabitEthernet0/3.4123
subinterface2
Disabled
DOWN
GigabitEthernet0/4
dhcp-interface
Enabled
UP
GigabitEthernet0/5
Disabled
DOW
GigabitEthernet0/6
Disabled
DOW
GigabitEthernet0/7
Disabled
DOW
GigabitEthernet0/8
Disabled
DOW
Management0/0
management
Enabled
UP

2023 年 8 月

2023 年 8 月 31 日

[サービス（Services）] ページからのクラウド提供型 FMC、オンプレミス FMC、およびセキュアコネクタの管理

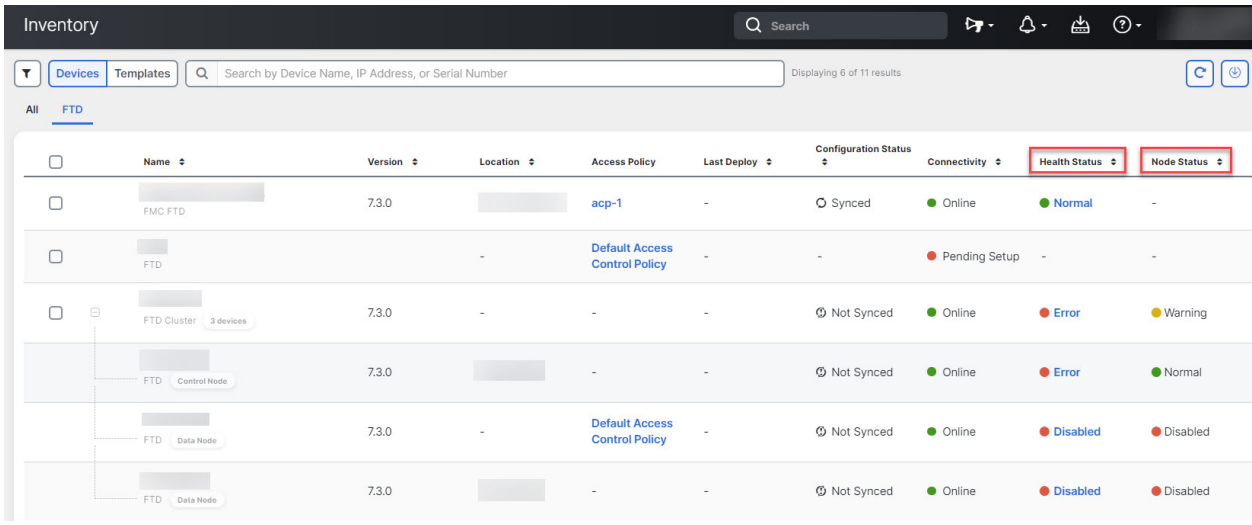
新しい [サービス（Services）] ページから、クラウド提供型 Firewall Management Center、オンプレミス Firewall Management Center、およびセキュアコネクタを管理できるようになりました。**[ツールとサービス（Tools & Services）]** > **[Firewall Management Center]** または [セキュアコネクタ（Secure Connectors）] を選択します。詳細については、「View Services Page Information」[英語] を参照してください。



2023 年 8 月 17 日

Threat Defense デバイスの正常性ステータスの把握

CDO の [インベントリ（Inventory）] ページに、Threat Defense デバイスの正常性とノードステータスが表示されるようになりました。デバイスの正常性の詳細については、デバイスの正常性ステータスをクリックし、クラウド提供型 Firewall Management Center またはオンプレミス Firewall Management Center のユーザーインターフェイスのデバイスの [正常性モニタリング（Health Monitoring）] ページに移動して、確認できます。ノードステータスは、クラウド提供型 Firewall Management Center によって管理される Threat Defense デバイスに対してのみ表示されることに注意してください。



詳細については、「Cisco Defense Orchestrator を使用したオンプレミス FMC の管理」および「Managing Cisco Secure Firewall Threat Defense Devices with Cloud-delivered Firewall Management Center」[英語] を参照してください。

2023 年 8 月 3 日

Firewall 移行ツールの更新

CDO は、Firewall 移行ツールの更新バージョンをホストするようになりました。Cisco Secure Firewall ASA デバイスの複数のコンテキストをルーテッドモードインスタンスにマージし、クラウド提供型 Firewall Management Center によって管理される Threat Defense デバイスに移行できるようになりました。さらに、移行ツールは、Virtual Routing and Forwarding（VRF）機能を活用して、マルチコンテキストの Cisco ASA 環境で観察される分離されたトラフィックフローを複製できるようになりました。複製されたフローは新たにマージされた設定の一部になります。

詳細については、Cisco Defense Orchestrator の Firewall 移行ツールを使用したファイアウォールの移行ガイド [英語] の「Migrating Secure Firewall ASA Managed by CDO」を参照してください。

2023 年 7 月

2023 年 7 月 20 日

GCP によって管理される仮想 脅威防御 デバイスの EasyDeploy

仮想 脅威に対する防御 デバイスを作成し、Google Cloud Platform（GCP）プロジェクトに同時に展開できるようになりました。EasyDeploy メソッドでは、新しい仮想デバイスを作成し、デ

バイスをクラウド環境に関連付けるために必要な手順を組み合わせることで、手順が合理化され、セットアップに必要な時間が最小限に抑えられます。

オンボーディングフローでは、クラウド提供型 Firewall Management Center を有効にする**必要があります**。詳細については、「Deploy a Threat Defense Device to Google Cloud Platform」[英語] を参照してください。

2023 年 7 月 13 日

異なるブラウザタブで CDO と クラウド提供型 Firewall Management Center ポータルを開く

CDO と クラウド提供型 Firewall Management Center ポータルページを異なるブラウザタブで開き、CDO と クラウド提供型 Firewall Management Centerの両方で同時に作業できるようになりました。

詳細については、「Support to Open CDO and Cloud-delivered Firewall Management Center Applications on Different Tabs」[英語] を参照してください。

2023 年 6 月

2023 年 6 月 29 日

イベントビューアでのバックグラウンド検索のスケジュール設定

定期的なスケジュールでイベントビューアを使用してバックグラウンド検索を実行できるようになりました。スケジュールは、絶対時間（例：5 月 1 日から 5 月 5 日）またはスライディングウィンドウ（例：「最終日」）に対応しています。

詳細については、「Schedule a Background Search in the Event Viewer」[英語] を参照してください。

新しいイベント属性のサポート

現在、セキュリティグループ、暗号化された可視性プロセスの確実性スコア、暗号化された可視性脅威の信頼性、暗号化された可視性脅威の確実性スコア、暗号化された可視性フィンガープリントは、CDO のイベントビューアでサポートされている syslog イベント属性です。イベントロギングビューをカスタマイズすると、新たにサポートされた属性の列を作成できます。

2023 年 6 月 15 日

CDO の Firewall 移行ツールを使用したファイアウォールの移行

Cisco Defense Orchestrator の Firewall 移行ツールを使用して、Secure Firewall ASA デバイス、FDM による管理 Threat Defense デバイス、および Check Point、Palo Alto Networks、Fortinet ファ

イアウォールなどのサードパーティ製ファイアウォールからクラウド提供型Firewall Management Center に設定を移行できるようになりました。詳細については、Cisco Defense Orchestrator の Firewall 移行ツールを使用したファイアウォールの移行ガイド [英語] を参照してください。https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide-firewall-migration-tool-on-cdo/migrating-firewalls-with-the-firewall-migration-tool-in-cisco-defense-orchestrator.html

2023 年 6 月 8 日

AWS および Azure によって管理される仮想 脅威防御 デバイスの EasyDeploy

仮想 脅威に対する防御 デバイスを作成し、Amazon Web Services（AWS）または Azure 環境に同時に展開できるようになりました。EasyDeploy メソッドでは、新しい仮想デバイスを作成し、デバイスをクラウド環境に関連付けるために必要な手順を組み合わせることで、手順が合理化され、セットアップに必要な時間が最小限に抑えられます。

オンボーディングフローでは、クラウド提供型Firewall Management Centerを有効にする**必要があります**。詳細については、「Deploy a Threat Defense Device with AWS」[英語] および「Deploy a Threat Defense Device with an Azure VNet」[英語] をそれぞれ参照してください。

2023 年 6 月 5 日

CDO に導入された Multicloud Defense ソリューション

Multicloud Defense ソリューション は、クラウド ネットワーク トラフィック、およびクラウド アプリケーションとワークロードのセキュリティ ポリシー オーケストレーションと保護に特化したソリューションです。複数のクラウドタイプに対して統合されたセキュリティポリシーと Web 保護を提供し、クラウド資産に対するネットワークの可視性を提供し、脅威インテリジェンスや外部ロギングなどのサービスを統合します。クラウドアカウントとの間の入出力トラフィックと、クラウドアカウントの「East-West」ネットワークトラフィックを適用します。

Multicloud Defense ソリューション は現在、AWS、Azure、Google Cloud Platform（GCP）、および Oracle OCI クラウドアカウントをサポートしています。

詳細 については、「About Multicloud Defense」[英語] を参照してください。Multicloud Defense ソリューションを試す場合は、「Multicloud Defense 90 日間無料トライアル」を参照してください。

2023 年 6 月 1 日

SecureX の統合によるオンプレミスの Cisco Secure Firewall Management Center の自動検出

CDO は、CDO アカウントにリンクされている SecureX テナントに関連付けられているすべての オンプレミス Management Center をオンボードできるようになりました。また、それらの オンプレミス Management Center にリンクされている Cisco Secure Firewall Threat Defense のデバ

イスがオンボードされます。詳細については、「Auto Onboard an On-Prem Firewall Management Center with SecureX」[英語] を参照してください。

2023 年 4 月

2023 年 4 月 27 日

イベントフィルタリングの改善

相対時間範囲を使用して、イベントをさらにフィルタ処理できるようになりました。絶対時間範囲は、明示的に指定された時間フレームです。相対時間範囲の例は、過去 3 日間または 過去 3 時間です。相対時間範囲は、絶対時間範囲に必ずしも含まれていない可能性があるトラフィックとイベントをターゲットにするのに役立ちます。詳細については、「Search for Events in the Events Logging Page」[英語] を参照してください。

2023 年 3 月

2023 年 3 月 23 日

イベントロギングのバックグラウンド検索

CDO では、検索条件を定義し、定義された検索条件に基づいてイベントログ内のイベントを検索できます。バックグラウンド検索機能を使用すると、バックグラウンドでイベントログの検索を実行して、バックグラウンド検索が完了した後に検索結果を表示できます。

設定したサブスクリプションアラートとサービス統合に基づいて、バックグラウンド検索が完了すると通知されます。「Learn more about background searches used with event logging」[英語] を参照してください。

2023 年 1 月

2023 年 1 月 18 日

FTD のリモートアクセス VPN セッションの監視

CDO は、CDO の クラウド提供型 Firewall Management Center を使用して管理される FTD のリモートアクセス VPN セッションを監視できるようになりました。

[RA VPNモニタリング（RA VPN Monitoring）] ページには次の情報が表示されます。

- アクティブなセッションと履歴セッションのリスト。
- 各セッションに関連付けられているデバイスとユーザーの詳細。

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。