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。

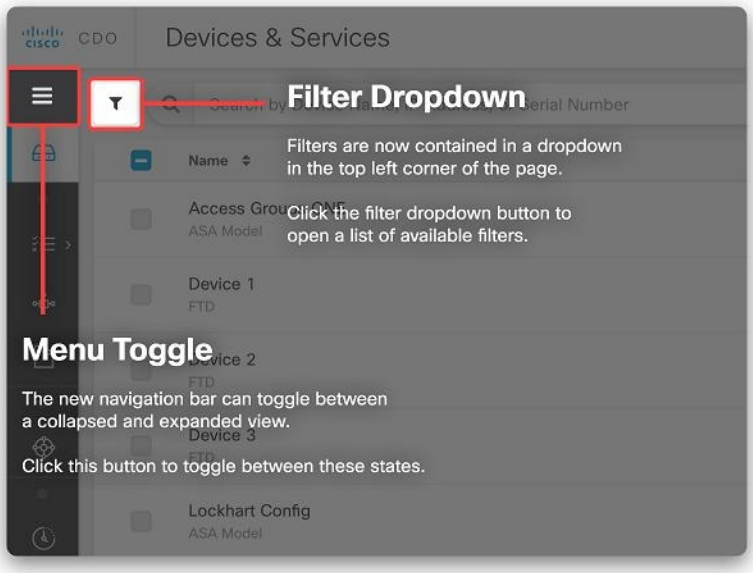
成功または失敗したコマンドを表示するには、変更が行われたデバイスの変更ログを開き、アクションのエントリを見つけて、ログエントリの最後にある [+] ボタンをクリックして展開します。

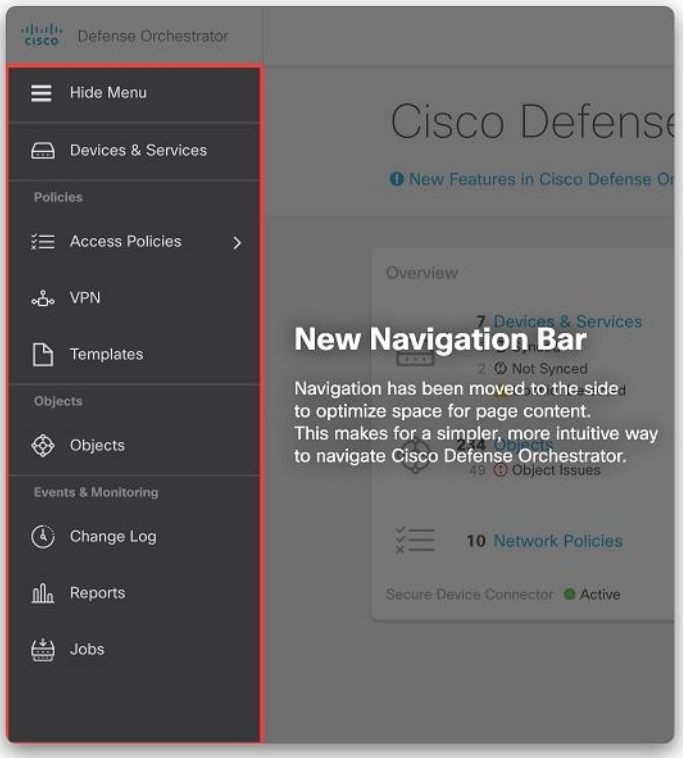
2018 年 7 月

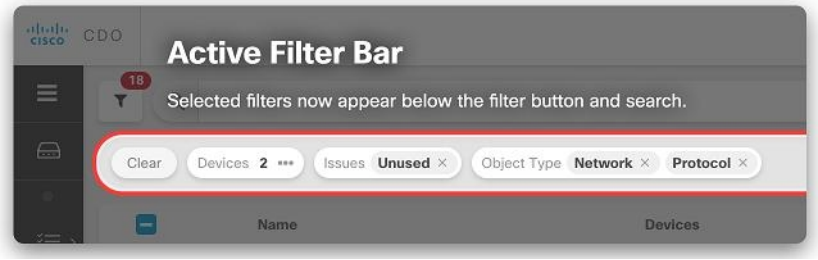
2018 年 7 月 26 日

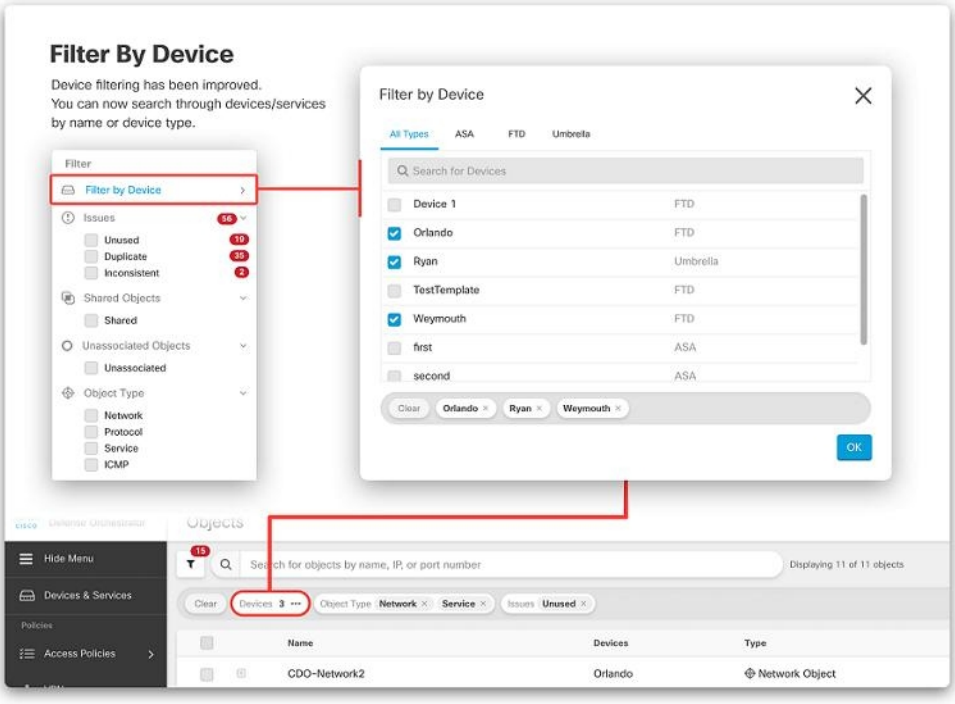
新しい CDO UI

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。



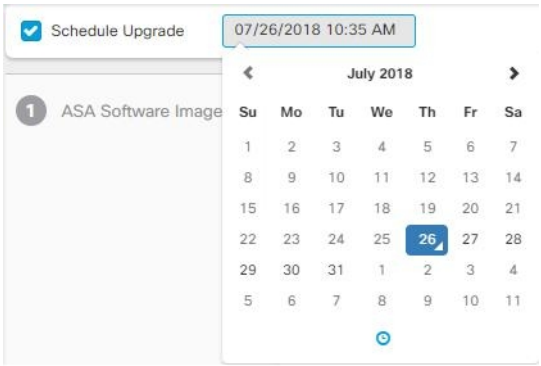

Defense Orchestrator
Hide Menu
Devices & Services
Policies
Access Policies
VPN
Templates
Objects
Objects
Events & Monitoring
Change Log
Reports
Jobs
Cisco Defense
New Features in Cisco Defense Or
Overview
7 Devices & Services
2 Not Synced
49 Object Issues
10 Network Policies
Secure Device Connector Active
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
18
Selected filters now appear below the filter button and search.
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

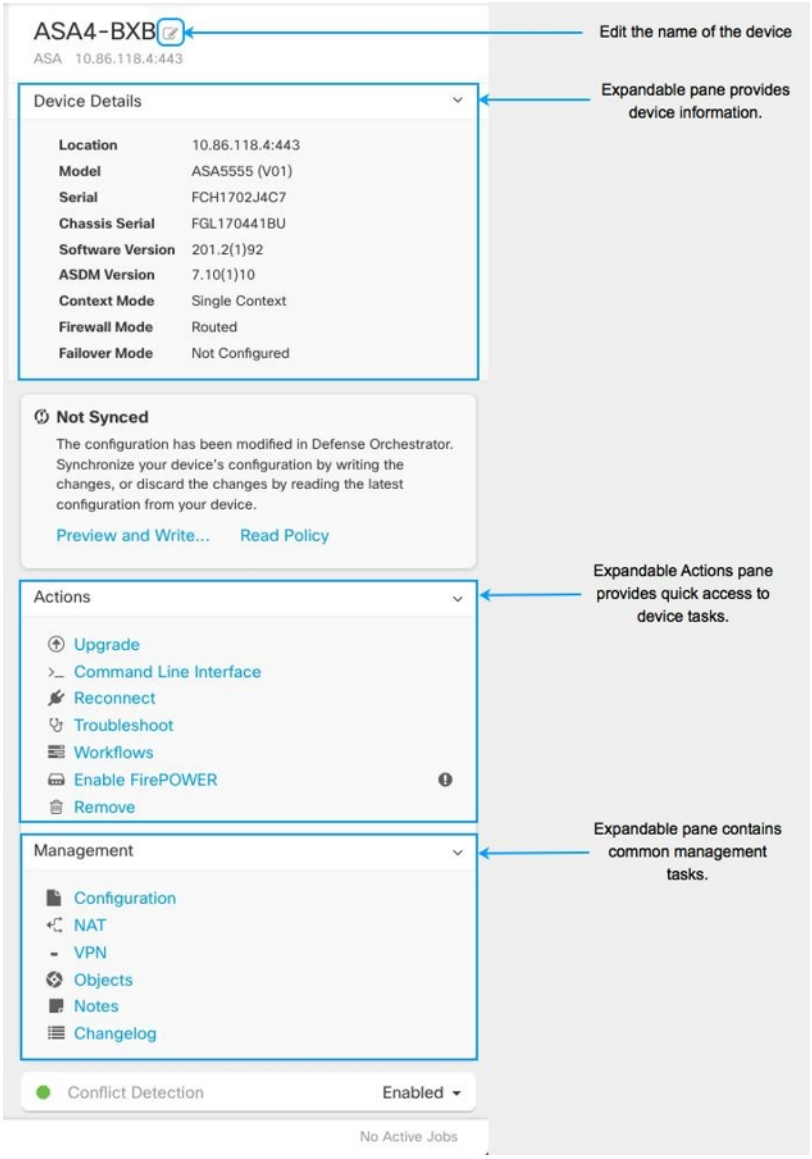
時間ベースの ASA ネットワークポリシーのサポート

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

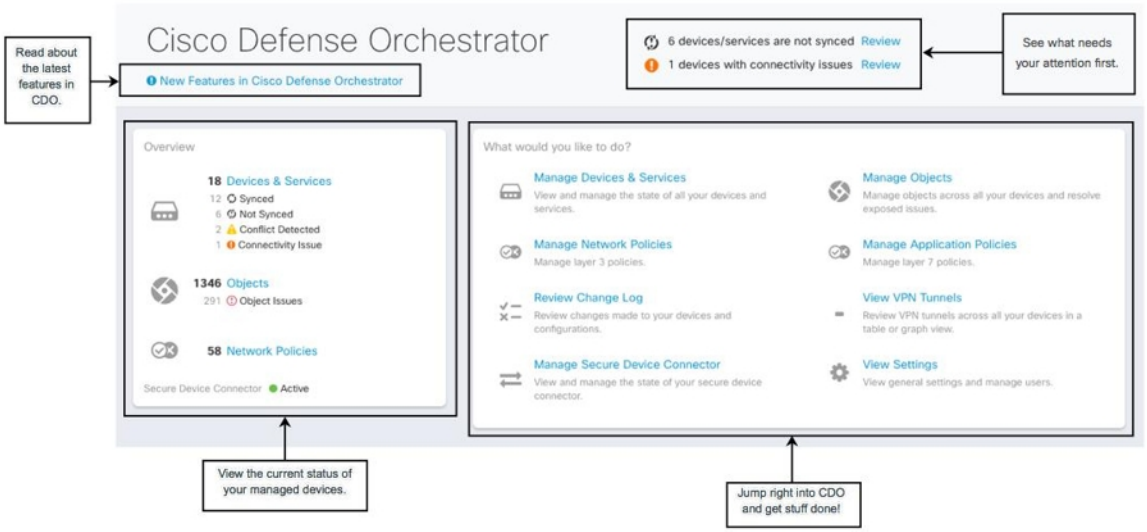
独自のイメージリポジトリに保持している ASA ソフトウェアと ASDM イメージを使用して、ASA デバイスをアップグレードできるようになりました。ASA にインターネットへのアウトバウンドアクセスがない場合、または CDO のイメージリポジトリにまだないイメージが必要な場合は、これが ASA をアップグレードする最良の方法です。FTP、TFTP、HTTP、HTTPS、SCP、および SMB のいずれかのプロトコルを使用して、リポジトリからイメージを取得できます。

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

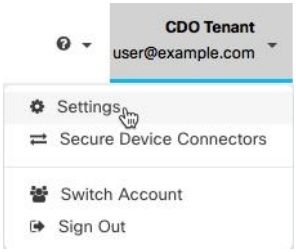
テナントに関連付けられているすべてのユーザーを [ユーザー管理（User Management）] 画面に表示できるようになります。これには、サポートチケットを解決するために一時的にアカウントに関連付けられたシスコサポートエンジニアが含まれます。

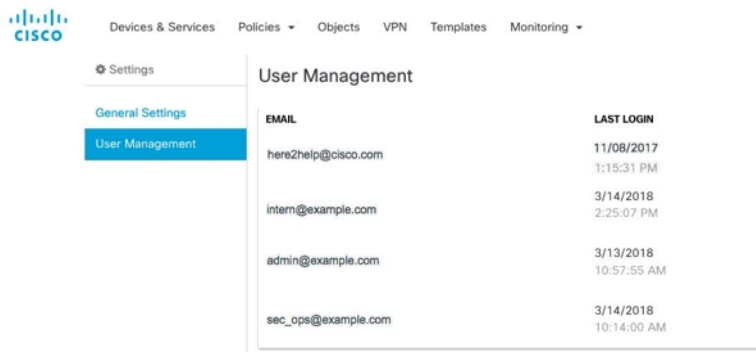
テナントに関連付けられているユーザーを表示するには、次の手順を実行します。

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

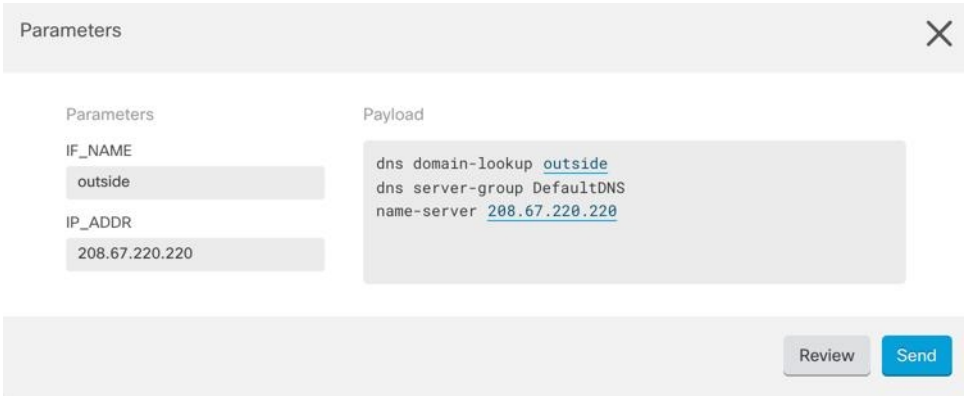
CDO は、カスタマイズして ASA で実行できる完全な CLI ベースのコマンドとコマンドテンプレートのリストを提供します。これらの CLI マクロは、単一の ASA または複数の ASA で一括して実行できます。定期的に監視または保守作業を行っていますか。独自の CLI ベースのコマンドを作成して CDO に保存し、必要なときに再利用できます。

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。

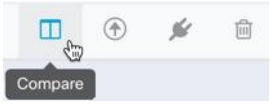


ステップ 4 それをすべての ASA に送信します。

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。

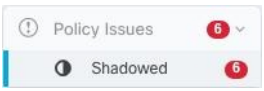
エラー：CDO は、600 文字を超える長さのこのコマンドの一部を実行しようとしました。コマンドのリストを分割して間に追加の空行を挿入することにより、適切なコマンド分離ポイントがどこにあるかを CDO に示すことができます。

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。

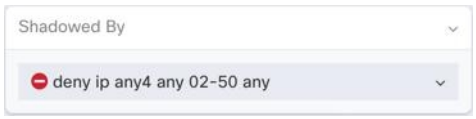
2018 年 1 月 18 日

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。



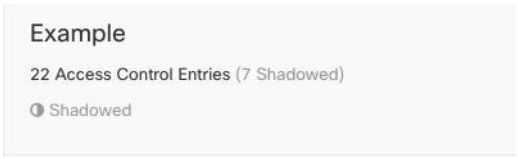
- ASA ネットワークポリシー内のルールの横にある新しいバッジ⚠は、ポリシー内の別のルールをシャドウイングしていることを示しています。
- シャドウルールの場合、ネットワークポリシーの詳細ペインは、ポリシー内のどのルールがそれをシャドウイングしているかを識別します。



- 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 ▶

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。