



## 2017 の機能概要

---

この記事では、2017 年に Cisco Defense Orchestrator に追加された機能の一部を紹介します。

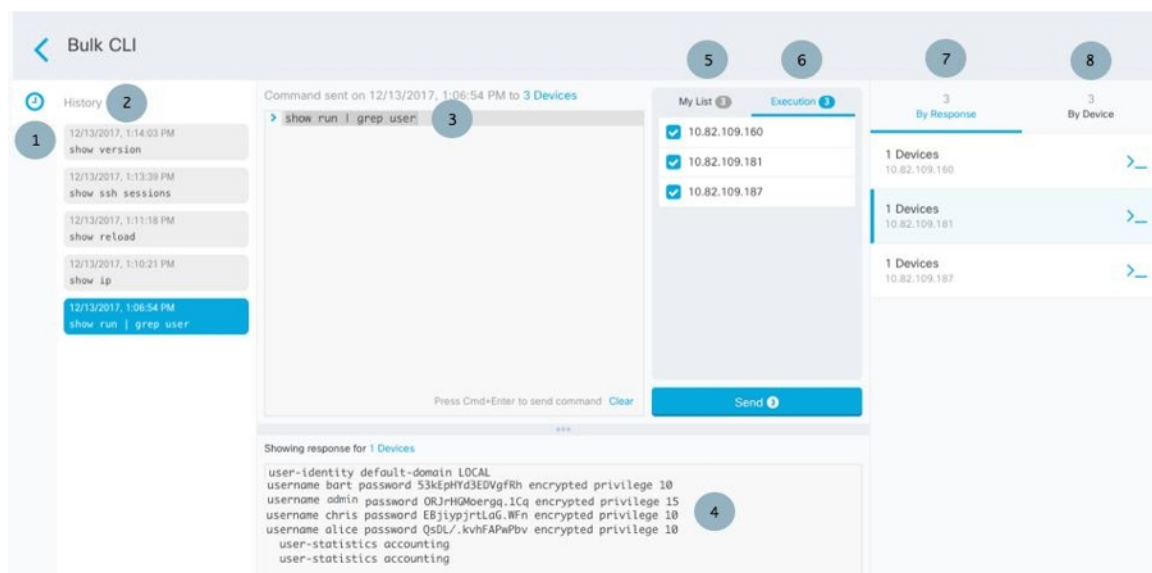
- [2017 年 12 月 \(1 ページ\)](#)
- [2017 年 11 月 \(2 ページ\)](#)
- [2017 年 10 月 \(5 ページ\)](#)
- [2017 年 9 月 \(6 ページ\)](#)
- [2017 年 8 月 \(7 ページ\)](#)
- [2017 年 6 月 \(8 ページ\)](#)
- [2017 年 5 月 \(9 ページ\)](#)
- [2017 年 4 月 \(9 ページ\)](#)
- [2017 年 2 月 \(10 ページ\)](#)
- [2017 年 1 月 \(10 ページ\)](#)

### 2017 年 12 月

#### 2017 年 12 月 14 日

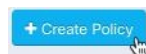
##### 一括コマンド ライン インターフェイス

Cisco Defense Orchestrator (CDO) は、管理者が 1 つのコマンドを複数のデバイスに同時に送信する機能を提供することにより、デバイス全体で一貫した構成を促進します。CDO は、一括 CLI コマンドへの応答を応答タイプおよびデバイスタイプ別にグループ化するため、特定の応答を返した ASA と特定のコマンドを送信したデバイスを識別できます。CDO は、コマンドの履歴リストを保持しているため、コマンドを再実行したり変更したりできます。詳細については、『[Managing ASA with Cisco Defense Orchestrator](#)』の「Bulk Command Line Interface」を参照してください。



### ASA ネットワークポリシーの作成

ASA のネットワークポリシーを作成できるようになりました。ポリシーにルールを追加したり、ポリシー内のルールの順序を変更したり、ポリシー内のルールをアクティブ化または非アクティブ化したり、そのポリシーを ASA から別の ASA にコピーしたりできます。開始するには、『[Managing ASA with Cisco Defense Orchestrator](#)』の「Create an ASA Network Policy」を参照してください。



## 2017 年 11 月

### 2017 年 11 月 9 日

#### バルク操作

特定の CDO 構成タスクを複数のデバイスで同時に実行できます。それらは「一括で」行うことができます。この機能は時間を節約し、デバイス間の一貫性を向上します。これらは、一括して実行できる操作と、それらを補完するために追加されたいくつかの追加機能です。

#### ASA および ASDM の一括アップグレード

CDO のアップグレードウィザードを使用して、複数の ASA の ASA および ASDM イメージを同時にアップグレードできるようになりました。必要なすべてのアップグレード手順を舞台裏で実行することにより、プロセスを簡単にします。ウィザードは、互換性のある ASA および ASDM ソフトウェアイメージを選択し、それらをインストールし、デバイスをリブートしてアップグレードを完了するプロセスを案内します。CDO で選択したイメージが ASA にコピー

およびインストールされているものであることを検証することにより、アップグレードプロセスを保護します。詳細については、『[Managing ASA with Cisco Defense Orchestrator](#)』の「Bulk ASA and ASDM Upgrade」を参照してください。

### 一括読み取り構成

CDO の外部でデバイスの構成が変更された場合、CDO に保存されているデバイスの構成とデバイスのローカル構成は同じではなくなります。この場合、CDO は「競合が検出されました」というメッセージを表示して、管理者に警告します。管理者が「ポリシーの読み取り」アクションを実行すると、デバイスに保存されている構成で CDO の構成が上書きされます。2 つの構成は同じになり、「同期済み」になります。一括読み取り構成機能により、管理者はこのアクションを複数のデバイスで同時に実行できます。

一括読み取り構成のもう 1 つの用途は、CDO でステージングされた変更がデバイスに書き込まれないようにすることです。デバイスから CDO に構成を読み取ることにより、CDO でステージングされたすべての変更を上書きします。これは、必要に応じて、CDO でデバイスの構成に加えた変更を元に戻す良い方法でもあります。詳細については、『[Managing ASA with Cisco Defense Orchestrator](#)』の「Bulk Read Configuration」を参照してください。

### デバイスの一括再接続

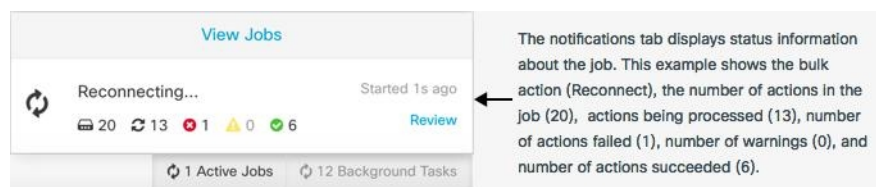
CDO を使用すると、管理者は複数の管理対象デバイスを CDO に同時に再接続を試みることができます。CDO が管理するデバイスが「到達不能」とマークされている場合、CDO は帯域外構成の変更を検出したり、デバイスを管理したりできなくなります。デバイスの再接続を試みすることは、CDO によるデバイスの管理を復元するための簡単な最初のステップです。詳細については、『[Managing ASA with Cisco Defense Orchestrator](#)』の「Bulk Reconnecting Devices」を参照してください。

### 競合検出の一括有効化と無効化

複数のデバイスの競合検出を同時に有効または無効にすることができます。競合検出を有効にすると、CDO の外部でデバイスに変更が加えられた場合に警告が表示されます。詳細については、『[Managing ASA with Cisco Defense Orchestrator](#)』の「Enabling Conflict Detection」を参照してください。

### ジョブ通知

通知タブは、CDO の右下隅にあります。ジョブで進行中のアクションのアクティブ数を表示します。



### [ジョブ (Jobs) ] ページ

[ジョブ (Jobs) ] ページには、一括操作のステータス、成功、および失敗に関する情報が表示されます。ジョブテーブルの色分けされた行は、成功または失敗した個々のアクションを示し

ます。詳細については、『[Managing ASA with Cisco Defense Orchestrator](#)』の「Jobs Page」を参照してください。

### 失敗したアクションのタスクを再開する

CDO は一括操作を記憶し、失敗した個々のアクションを識別し、失敗したアクションに対してのみタスクを再実行することで時間を節約します。[ジョブ (Jobs)] ページを確認するときに、失敗した一括操作で1つ以上のアクションが見つかった場合は、必要な修正を行った後に一括操作を再実行できます。CDO は、失敗したアクションのみでジョブを再実行します。詳細については、『[Managing ASA with Cisco Defense Orchestrator](#)』の「Reinitiating a Bulk Operation that Resulted in a Failed Action」を参照してください。

### NAT ドキュメント

次のユースケースの手順が文書化されています。

- 内部ネットワーク上のサーバーがパブリック IP アドレスを使用してインターネットに到達できるようにする
- パブリック IP アドレスの特定のポートでユーザーが内部ネットワーク上のサーバーを使用できるようにする
- プライベート IP アドレスの範囲をパブリック IP アドレスの範囲に変換する

### CLI ロギング

CDO を使用して ASA で CLI コマンドを実行するたびに、コマンドとコマンドの結果がデバイスの変更ログに記録されるようになりました。次の例では、CLI 実行 (CLI Execution) 行のエントリに送信されたコマンドが示され、変更された ASA 構成 (Changed ASA Config) 行に、コマンドの結果として構成ファイルで変更された内容が示されています。

DATE	DESCRIPTION
Nov 8, 2017 11:00:38 AM	Changed ASA Config
<pre> @@ -5,1 +5,1 @@ -: Written by admin at 07:45:21.397 UTC Wed Nov 8 2017 +: Written by admin at 08:51:15.997 UTC Wed Nov 8 2017 @@ -87,0 +87,2 @@ +object network spd2-test-obj +host 209.165.1.10 @@ -226,1 +228,1 @@ -Cryptochecksum:a6 f8 +Cryptochecksum:a4 5e </pre>	
Nov 8, 2017 11:00:35 AM	CLI Execution
<pre> object network spd2-test-obj host 209.165.1.10 tunnel-group DefaultGroup2 ipsec-attributes ikev1 pre-shared-key ***** </pre>	

## 2017 年 10 月

### 2017 年 10 月 19 日

#### ASA の一括オンボーディング

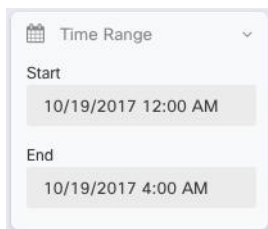
1 回のバッチで複数の ASA を CDO にオンボードできるようになりました。詳細については、『[Managing ASA with Cisco Defense Orchestrator](#)』の「Onboard ASAs in Bulk」を参照してください。

#### 共有ネットワークポリシー

Cisco Defense Orchestrator (CDO) は、複数の ASA によって使用される同一のネットワークポリシーを見つけ、ネットワークポリシーページでそれらを識別します。共有ネットワークポリシーがある場合は、一度変更して、ポリシーを共有する他のデバイスに変更を配布できます。これにより、デバイス間でネットワークポリシーの一貫性が保たれます。詳細については、『[Managing ASA with Cisco Defense Orchestrator](#)』の「Shared Network Policies」を参照してください。

#### 変更ログを日時にフィルタリングする

変更ログのイベントを日時にフィルタリングできるようになりました。[監視 (Monitoring)] > [変更ログ (Change Log)] の順に移動し、フィルターバーでこの日時のカレンダーを見つけます。



Field	Value
Time Range	▼
Start	10/19/2017 12:00 AM
End	10/19/2017 4:00 AM

### 2017 年 10 月 12 日

#### パケットトレーサ

パケットトレーサは、アクセスとポリシーの問題のトラブルシューティングに役立ちます。パケットトレーサは、合成パケットをネットワークに送信し、保存されたルーティング構成、NAT ルール、およびポリシー構成がそのパケットとどのように相互作用するかを評価します。たとえば、ルールがパケットをドロップしている場合、パケットトレーサはそのルールを識別し、そのルールへのリンクを提供するため、ルールを評価して編集することができます。パケットトレーサは、ライブ、オンライン、物理、または仮想の適応型セキュリティアプライア

ンス (ASA) で使用できます。詳細については、『[Managing ASA with Cisco Defense Orchestrator](#)』の「ASA Packet Tracer」を参照してください。



## 2017 年 10 月 5 日

### 新しいスクリーンキャスト



CDOを使用して、アクティブ/スタンバイ フェールオーバーペアとして設定された単一の ASA または 2 つの ASA をアップグレードする方法を示す新しい[スクリーンキャスト](#)です。

## 2017 年 9 月

### 2017年9月28日

#### 更新されたドキュメント

- 構成の競合を解決する：デバイスが「未同期」の場合、または「競合が検出されました」と報告された場合の対処方法を説明する[トラブルシューティング トピック](#)です。
- アクティブ-アクティブ フェールオーバー モードの ASA に加えられた設定変更：フェールオーバーモードでアクティブ-アクティブのペアとして設定された ASA の設定変更に関する重要な情報を提供します。
- 証明書の問題の解決：CDO が証明書を拒否する理由と、その対処方法について説明する[トラブルシューティング トピック](#)です。
- よくある質問ページの更新です。

## 2017 年 9 月 14 日

### CDO サービスステータスページ

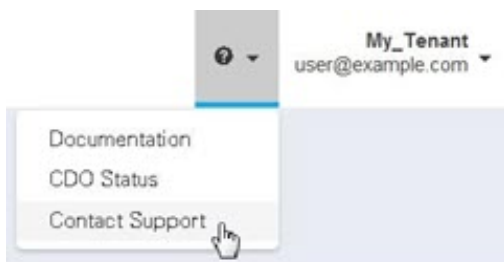
CDO は、顧客向けのサービスステータスページを <https://status.defenseorchestrator.com/> で維持しています。このページには、CDO サービスが稼働しているかどうかと、サービスの中断があったかどうかが表示されます。稼働時間情報を日次、週次、または月次のグラフで表示できます。

ステータスページで、[更新をサブスクライブ (Subscribe to Updates)] をクリックして、CDO サービスがダウンした場合に通知を受け取ることができます。

## CDO サポートページ

お客様は、CDO インターフェイスを介してサポートを受けることができます。

- 有料のお客様は、新しい[サポートに問い合わせる (Contact Support)] ページの[サポート ケースマネージャ (Support Case Manager)] をクリックして、シスコのテクニカル アシスタンス センター (TAC) で直接サポートケースを開く必要があります。
- デモ、社内、およびトライアルのすべてのお客様は、[サポートに問い合わせる (Contact Support)] ページの詳細リクエストフォームに質問を入力して、[cdo.support@cisco.com](mailto:cdo.support@cisco.com) に電子メールを送信できます。サポートスタッフができるだけ早く対応します。



## 2017年9月7日

### デバイスの外部リンク

外部リソースへのハイパーリンクを作成し、CDO で管理するデバイスに関連付けることができるようになりました。この機能を使用して、検索エンジン、ドキュメントリソース、企業 wiki、または選択したその他の URL への便利なリンクを作成できます。必要な数の外部リンクをデバイスに関連付けることができます。同じリンクを同時に複数のデバイスに関連付けることもできます。

## 2017 年 8 月

### 2017 年 8 月 17 日

### 新しいオブジェクト関数

- **重複、不整合、および未使用のオブジェクトの解決**：オブジェクトの問題を解決すると、ネットワークおよびサービスオブジェクトの可視性が向上します。グループ内のすべてのオブジェクトの統合ビューが表示されるため、オブジェクト間の比較が容易になります。オブジェクトの問題をマージ、名前変更、または無視して解決するコマンドボタンもあります。
- **新しいオブジェクトフィルタリング**：探しているオブジェクトを見つけるためのより正確な検索機能です。

## 2017 年 8 月 10 日

### アクティブ/スタンバイ フェールオーバー ペアとして設定された ASA へのアップグレード

CDO のアップグレードウィザードの機能が拡張され、アクティブ/スタンバイ フェールオーバー ペアとして設定された ASA のアップグレードが含まれました。個々の ASA のアップグレードと同じウィザード機能を使用しますが、アクティブ/スタンバイ フェールオーバー ペアをアップグレードできるようになりました。この機能の詳細については、『[Managing ASA with Cisco Defense Orchestrator](#)』の「Upgrading ASA and ASDM Images in an Active-Standby Pair」を参照してください。

## 2017 年 8 月 3 日

### シングルコンテキストまたはマルチコンテキストモードでの個々の ASA へのアップグレード

CDO は、シングルコンテキストまたはマルチコンテキストモードで個々の ASA にインストールされている ASA および ASDM イメージをアップグレードできるウィザードを提供するようになりました。必要なすべてのアップグレード手順を舞台裏で実行することにより、プロセスを簡単にします。ウィザードは、互換性のある ASA ソフトウェアおよび ASDM イメージを選択し、それらをインストールし、デバイスをリブートしてアップグレードを完了するプロセスを案内します。CDO で選択したイメージが ASA にコピーおよびインストールされているものであることを検証することにより、アップグレードプロセスを保護します。

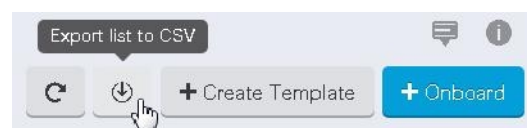
[デバイスとサービス (Devices & Services)] ページの詳細ペインをクリックして、アップグレードを開始します。詳細については、『[Managing ASA with Cisco Defense Orchestrator](#)』の「Upgrading ASA and ASDM Images」を参照してください。

## 2017 年 6 月

## 2017 年 6 月 20 日

### デバイスとサービスのリストをエクスポートする

[インベントリ (Inventory)] ページのデバイスとサービスのリストをコンマ区切り値 (.csv) ファイルにエクスポートできるようになりました。そこから、Microsoft Excel などのスプレッドシートアプリケーションでファイルを開いて、リスト内のアイテムを並べ替えたり、フィルター処理したりできます。





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。

## 2017 年 6 月 13 日

### ASA 構成の復元

ASA を以前に保存した設定の 1 つに戻すことができるようになりました。これは、予期しない、または望ましくない結果をもたらした構成変更を削除する便利な方法です。復元する ASA 設定を選択すると、CDO はその設定とメモリに最後に保存された設定の比較を表示します。目的の設定を復元することに問題がなければ、復元できます。



詳細については、『[Managing ASA with Cisco Defense Orchestrator](#)』の「Restoring ASA Configurations」を参照してください。

## 2017 年 5 月

### 2017 年 5 月 3 日

#### 変更要求管理

別のチケットシステムで開かれた変更要求とそのビジネス上の正当性を、変更ログのイベントに関連付けることができるようになりました。変更要求管理を使用すると、CDO で変更要求を作成し、一意の名前で識別し、変更の説明を入力して、変更要求を変更ログイベントに関連付けることができます。後で変更ログで変更要求名を検索できます。

詳細については、『[Managing FTD with Cisco Defense Orchestrator](#)』の「Change Request Management」を参照してください。

## 2017 年 4 月

**検索の改善**：[インベントリ (Inventory)] ページの検索バーで部分一致がサポートされるようになり、必要なデバイスまたはサービスを簡単に見つけられるようになりました。

**VPN**：さまざまな使いやすさが改善されました。

## 2017 年 2 月

**Cisco Defense Orchestrator の新しい EMEA サイト**

**Application Visibility Control (AVC) ID プロファイルのサポート**

## 2017 年 1 月

**読み取り専用 IPSec VPN トンネル管理**

Cisco Defense Orchestrator は、IPsec サイト間 VPN ASA デバイス構成の解析と処理をサポートするようになりました。ネットワークベースの VPN トンネルダイアグラムが利用可能であり、単一のピアに接続されているすべてのトンネルの完全なビュー、アクセスポリシー、キー交換暗号化、およびその接続ステータスを含むトンネルの詳細を提供します。CDO は、組織のオンボード ASA デバイスの構成で使用可能なすべてのトンネルの完全なビューも提供します。CDO の新しい VPN 管理機能により、組織およびネットワーク運用エンジニアは次のことができます。

- デバイスごととすべてのデバイスの両方で、VPN トンネル全体を視覚化します
- トンネルの接続状態を使用し、アクセスポリシーとクリプトマップ暗号化を一目で確認できるため、トンネルの設定ミスを簡単に特定できます

VPN は安全ですが、安定した安全な通信を確保するために適切に構成する必要があります。CDO は、ユーザーが VPN 構成を組織的に表示できるようにして、肥大化した古いポリシーの削減を促進します。

**ネットワークおよびサービス シングル オブジェクトのサポート**

現在利用可能なオブジェクトグループのサポートに加えて、Cisco Defense Orchestrator では、アクセスルールの変更時に、または[オブジェクト (Objects)] ページから直接、ネットワークタイプとサービスタイプの両方の単一オブジェクトを作成できるようになりました。

## 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。