

CDOでのファイアウォール移行ツールの初期化と起動

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[初期化](#)

[開始](#)

[移行例](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco Defense Orchestrator(CDO)プラットフォームでFirepower Migration Tool(FMT)を初期化、起動、および使用方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

Firepower Migration Tool(FMT)。
Cisco Defense Orchestrator(CDO)。
Firepower脅威対策(FTD)。

適応型セキュリティ アプライアンス (ASA)

使用するコンポーネント

ファイアウォール移行ツール (バージョン4.0.3) 。

Cisco Defense Orchestrator.

クラウドベースのファイアウォール管理センター。

適応型セキュリティアプライアンス。

Firepowerスレッド防御。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

CDOの移行ツールは、選択した移行元デバイスまたはアップロードした構成ファイルからデバイス構成を抽出し、CDOテナントでプロビジョニングされたクラウド配信のファイアウォール管理センターに移行します。

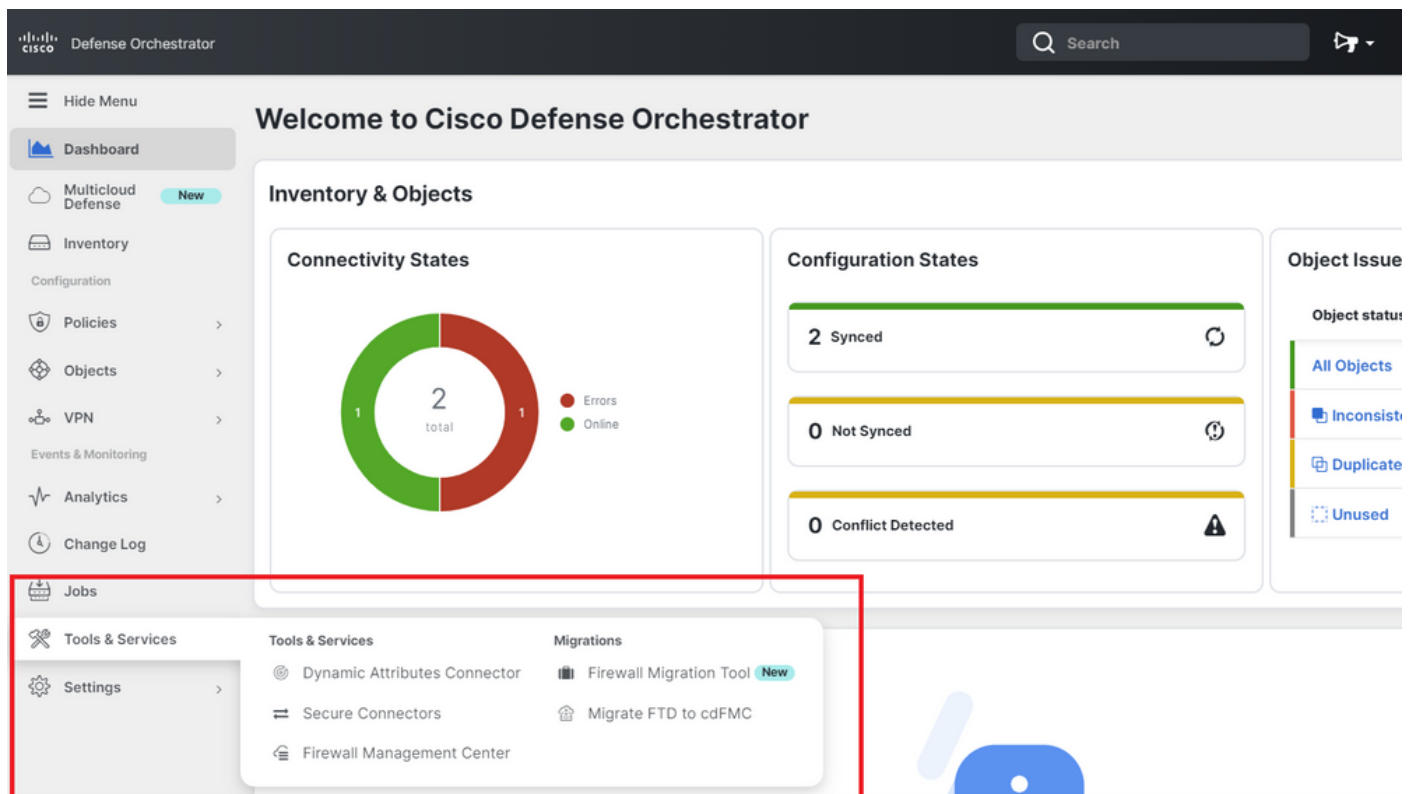
設定を検証した後、クラウド提供のファイアウォール管理センターで、サポートされていない設定を手動で設定できます。

設定

初期化

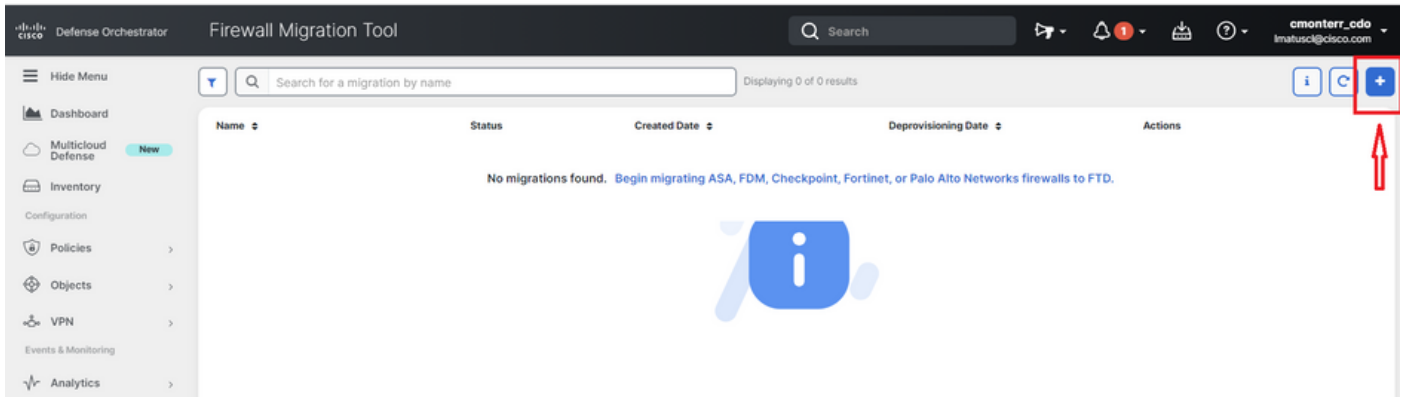
次の図は、CDOでFirepower Migration Toolを初期化する方法を示しています。

1.- Firewall Migration Toolを初期化するには、CDOテナントを開き、Tools & Services > Firewall Migration Toolの順に移動します。

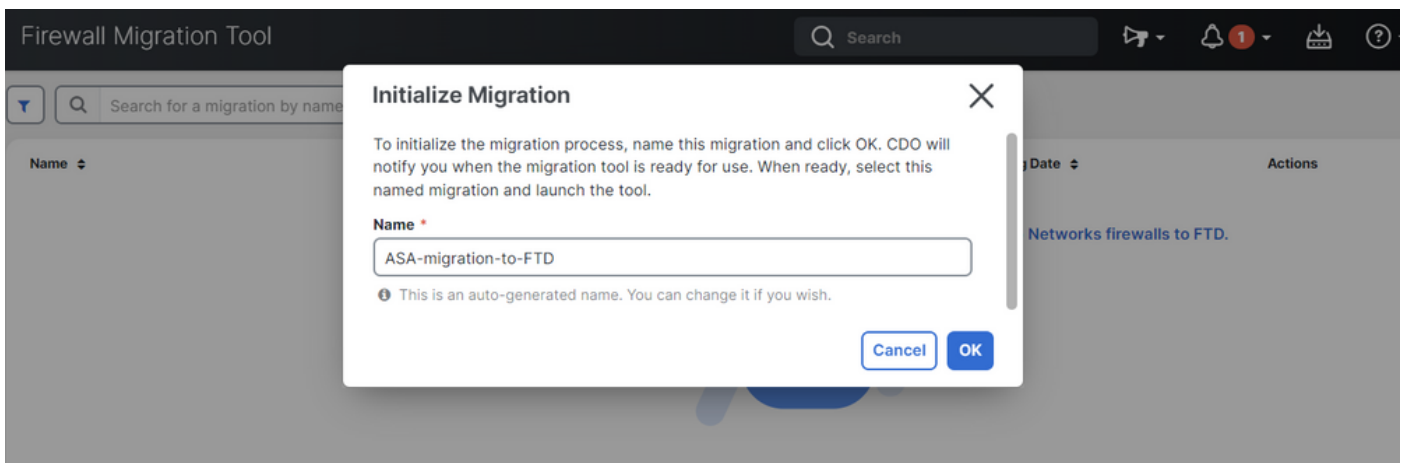


The screenshot displays the Cisco Defense Orchestrator (CDO) web interface. The main content area shows 'Inventory & Objects' with three panels: 'Connectivity States' (a donut chart showing 2 total, 1 Online, 1 Errors), 'Configuration States' (2 Synced, 0 Not Synced, 0 Conflict Detected), and 'Object Issue' (All Objects, Inconsistent, Duplicate, Unused). The left sidebar contains a navigation menu with 'Tools & Services' expanded to show 'Dynamic Attributes Connector', 'Secure Connectors', 'Firewall Management Center', 'Firewall Migration Tool' (marked as 'New'), and 'Migrate FTD to cdFMC'.

2. – 新しい移行プロセスを作成するには、青色のプラス(+)ボタンを選択します。

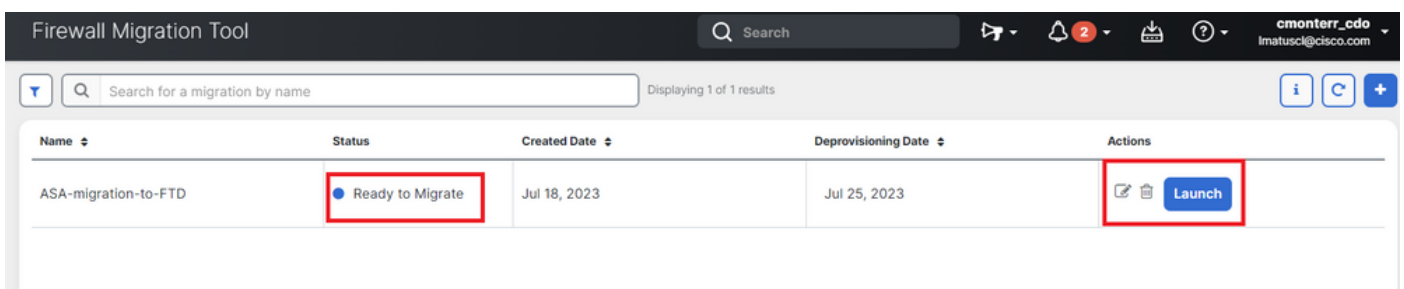


3. – 移行プロセスを初期化するために、CDOはデフォルト名を自動生成します。必要に応じて変更し、「OK」をクリックするだけです。



開始

1. – 移行プロセスが完了するのを待ちます。ステータスは「Initializing」から「Ready to Migrate」に変わる必要があります。準備ができたら、FMTを起動できます。



2. – 移行ツールのクラウドインスタンスが新しいブラウザタブで開き、ガイド付きワークフローを使用して移行タスクを実行できます。

CDOの移行ツールを使用すると、Secure Firewall移行ツールのデスクトップバージョンをダウンロードして維持する必要がなくなります。

Select Source Configuration ⓘ

Source Firewall Vendor

Cisco ASA (8.4+) ▾

Start Migration

Cisco ASA (8.4+) Pre-Migration Instructions

i This migration may take a while. Do not make any changes to the Firepower Management Center (FMC) when migration is in progress.

Session Telemetry:

Cisco collects the firewall telemetry set forth below in connection with this migration. By completing the migration, you consent to Cisco's collection and use of this telemetry data for purposes of tracking and following up on firewall device migrations and performing related migration analytics.

Acronyms used:

FMT: Firewall Migration Tool

FMC: Firepower Management Center

FTD: Firepower Threat Defense

Before you begin your Adaptive Security Appliance (ASA) to Firepower Threat Defense migration, you must have the following items:

- **Stable IP Connection:**

移行例

次の図は、FMTプロセスの簡単な例を示しています。この例では、ASA設定ファイルを、CDOでホストされるクラウド配信のファイアウォール管理センター(FMC)に移行します。

1.- ASA設定をエクスポートし、「Manual Configuration Upload」オプションにアップロードします。すでにASAがCDOにオンボーディングされている場合は、「ASAに接続」オプションを使用できます。

Extract Cisco ASA (8.4+) Information ⓘ

Source: Cisco ASA (8.4+)

Extraction Methods ▾

Manual Configuration Upload

- File format is '.cfg' or '.txt'.
- For Multi-context upload a show tech.
For Single-context upload show running.

⚠ Do not upload hand coded configurations.

Upload

Connect to ASA

- Select any ASA device onboarded on CDO from the below dropdown.
- Only devices with online connectivity and synced status will be displayed in the dropdown.

Connect

Context Selection >

Parsed Summary >

2. – この例では、FMTは「コンテキスト選択」を自動的にシングルコンテキストモードに設定します。ただし、ASA設定がマルチモードで実行されている場合は、移行するコンテキストを選択できます。

Extract Cisco ASA (8.4+) Information ⓘ

Source: Cisco ASA (8.4+)

Extraction Methods >

Manual Upload: [shitech_asav-a.txt](#)

Context Selection ▼

Selected Context: Single Context Mode

Parsed Summary ▼

Collect Hitcounts: No. Hitcount information is only available when connected to a live ASA.

2 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	0 Network Objects	0 Port Objects	0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
--------------------------------	--	----------------------	-------------------	--

Back Next

3.- FMTがASA設定を解析し、設定のサマリーを表示します。検証し、「次へ」を押して次の手順に進みます。

Parsed Summary ▼

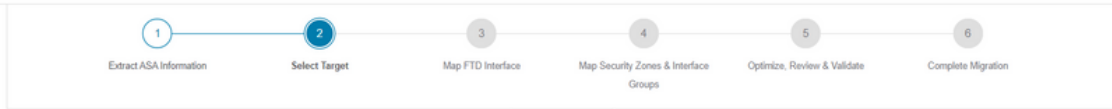
Collect Hitcounts: No. Hitcount information is only available when connected to a live ASA.

2 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	0 Network Objects	0 Port Objects	0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
0 Network Address Translation	4 Logical Interfaces	3 Routes (Static Routes, Policy Based Routing, ECMP)	0 Site-to-Site VPN Tunnels	0 Remote Access VPN (Connection Profiles)

● Pre-migration report will be available after selecting the targets.

Back Next

3. – デスクトップバージョンツールと同じ通常のFMT手順を続行します。この例では、実用的な目的で選択されたターゲットデバイスがないことに注意してください。



Select Target ⓘ

Source: Cisco ASA (8.4+)

Firewall Management - Cloud-delivered FMC >

Choose FTD >

Select FTD Device
Select FTD Device v

Proceed without FTD

● Interface, Routes and Site-to-Site VPN Tunnels won't be migrated

Proceed Change Device Status

Select Features >

Rule Conversion/ Process Config >

4. – すべてのFMT検証が完了すると、クラウド提供のFirepower Management Centerに設定がプッシュされます。



Complete Migration ⓘ

Migration Status

✔ Migration is complete, policy is pushed to FMC.
Next Step - Login to FMC to deploy the policy to FTD.

Manual Upload: shtech_asav-a.txt

Selected Context: Single Context Mode

Migration Summary (Post Push)

関連情報

- [Secure Firewall Migration Toolのトラブルシューティング](#)
- [Cisco Defense Orchestratorのファイアウォール移行ツールについて](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。