

Initialize and Launch the Firewall Migration Tool on CDO

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Initilize](#)

[Launch](#)

[Migration example](#)

[Related Information](#)

Introduction

This document describes how to initialize, launch, and use the Firepower Migration Tool (FMT) on the Cisco Defense Orchestrator (CDO) platform.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

Firepower Migration Tool (FMT).

Cisco Defense Orchestrator (CDO).

Firepower Threat Defense (FTD).

Adaptive Security Appliance (ASA)

Components Used

Firewall Migration Tool (Version 4.0.3).

Cisco Defense Orchestrator.

cloud-delivered Firewall Management Center.

Adaptive Security Appliance.

Firepower thread Defense.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The migration tool in CDO extracts the device configurations from the source device that you select or from a configuration file that you upload and migrates them to the cloud-delivered Firewall Management Center provisioned on your CDO tenant.

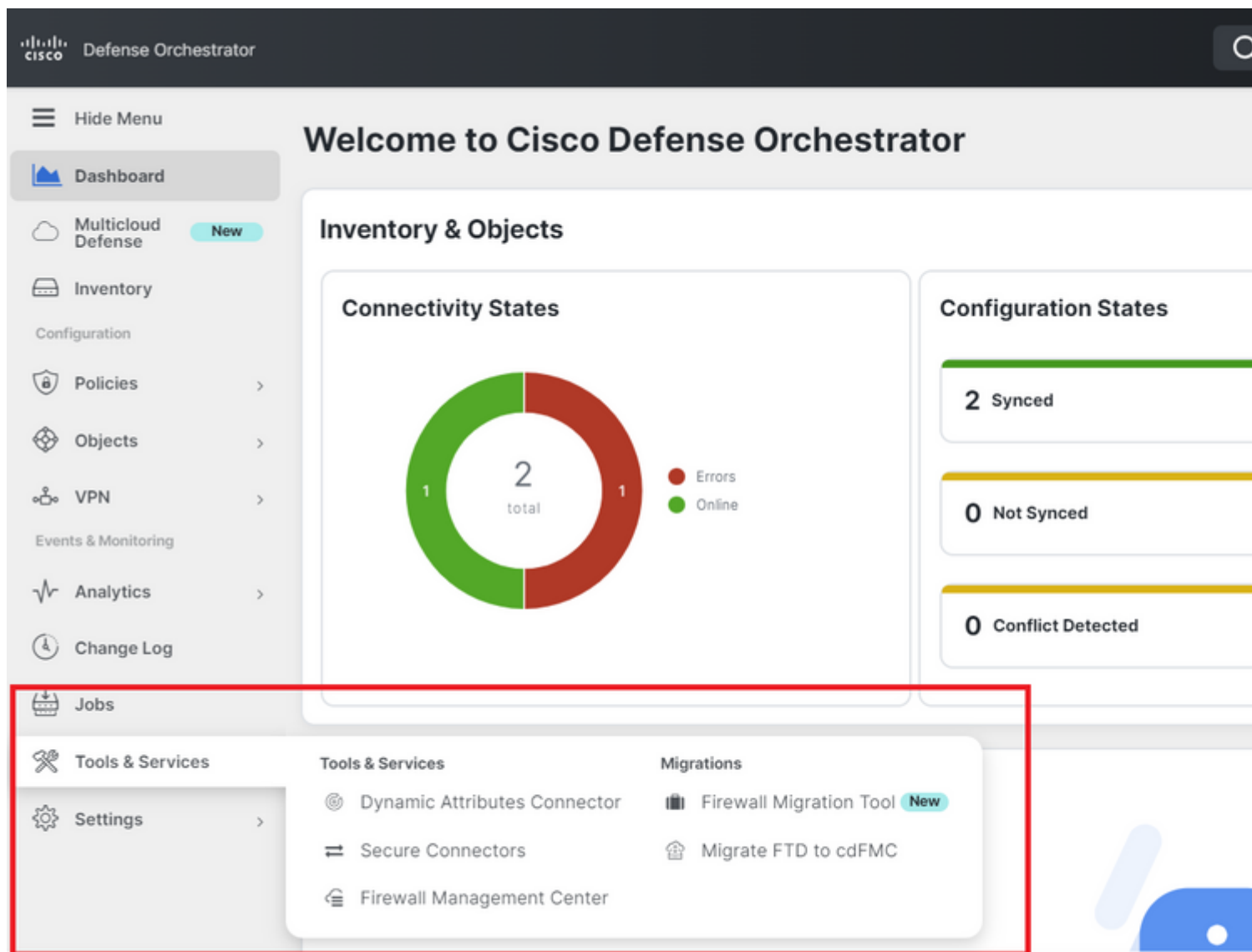
After you validate the configurations, you can configure the unsupported configuration manually on the cloud-delivered Firewall Management Center.

Configure

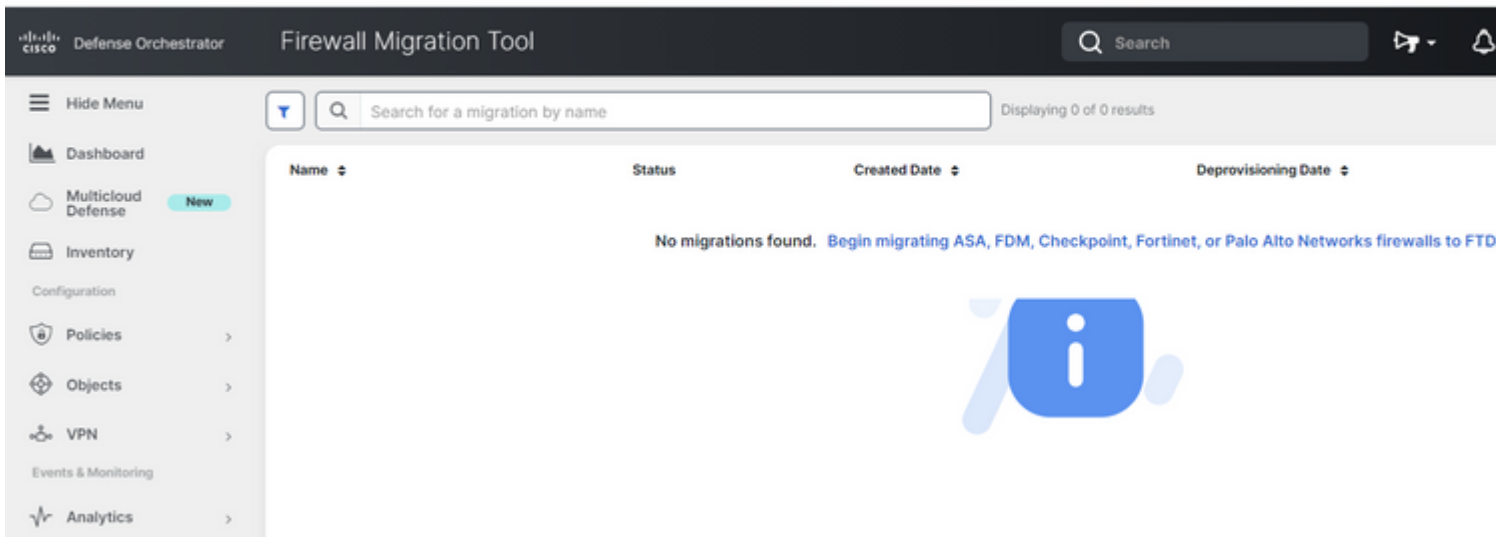
Initilize

These images describe how to Initilize the Firepower Migration Tool on CDO.

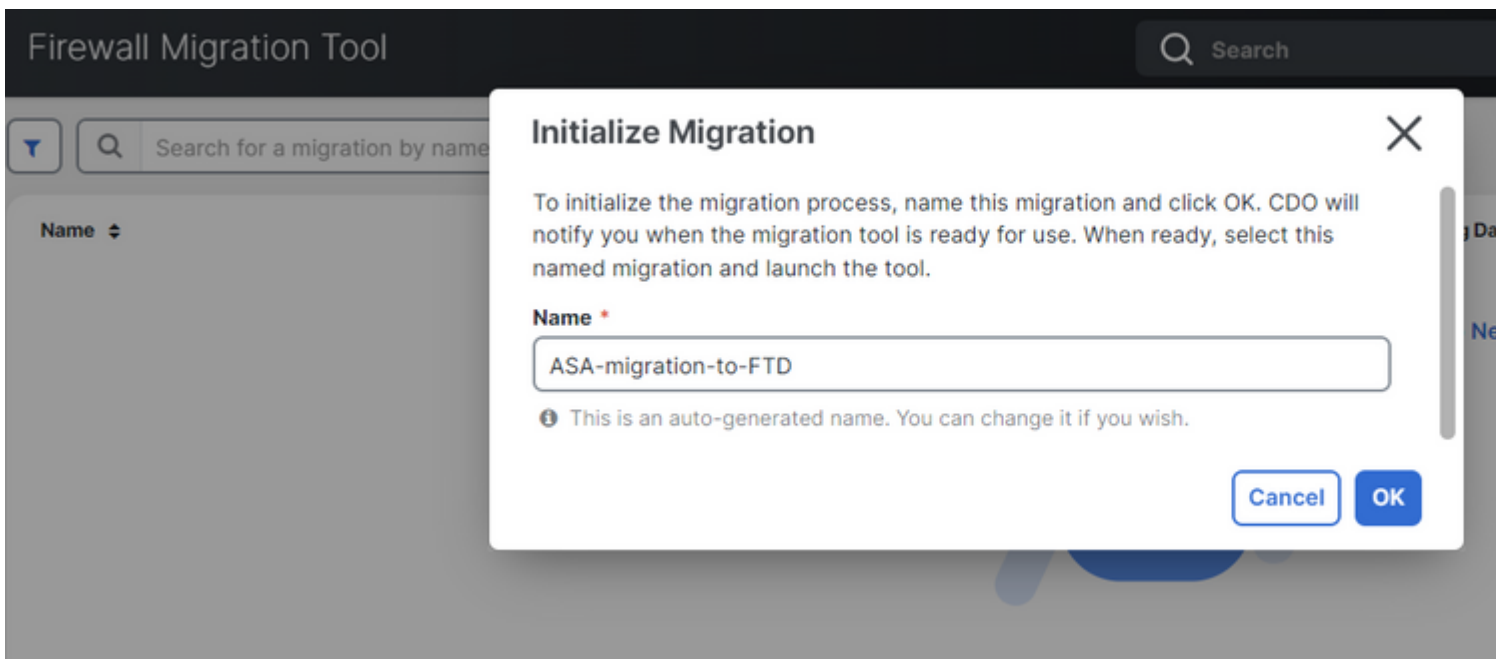
1.- In order to initialize the Firewall Migration Tool, open your CDO tenant and navigate to **Tools & Services > Firewall Migration Tool**.



2.- Select the blue plus (+) button in order to create a new migration process.



3.- In order to initialize the migration process, the CDO auto-generates a default name, you can change it if you wish and just click "OK".



Launch

1.- Wait for the Migration process to be completed; the status must change from "Initializing" to "Ready to Migrate". Once this is ready you can Launch the FMT.

Name	Status	Created Date	Deprovisioning Date
ASA-migration-to-FTD	Ready to Migrate	Jul 18, 2023	Jul 25, 2023

2.- A cloud instance of the migration tool opens in a new browser tab and enables you to perform your migration tasks using a guided workflow.

The migration tool in CDO eliminates the need for you to download and maintain the desktop version of the Secure Firewall migration tool.

Firewall Migration Tool (Version 4.0.3)

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 M progress.

Session Telemetry:

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

Acronyms used:

FMT: Firewall Migration Tool FMC: Firepower Management
 FTD: Firepower Threat Defense

Before you begin your Adaptive Security Appliance (ASA) to Firepower Threat Defense

Stable IP Connection:

Migration example

These images show a quick example of the FMT process. This example migrates an ASA configuration file to the cloud-delivered Firewall Management Center hosted on CDO.

1.- Export the ASA configuration and upload it to the **"Manual Configuration Upload"** option. If you have an ASA already onboarded to your CDO, you can use the **"Connect to ASA"** option.

Extract Cisco ASA (8.4+) Information ⓘ

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.- In this example, the FMT sets the "context selection" to single context mode automatically. However, you can select the desired context to be migrated if your ASA config is running on multiple mode.

Extract Cisco ASA (8.4+) Information ⓘ

Extraction Methods

Manual Upload: [shotech_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

3.- The FMT parses the ASA configuration and displays a summary of your config. Validate and hit "next" to continue with the next steps.

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 Network Address Translation	4 Logical Interfaces	3 Routes (Static Routes, Policy Based Routing, ECMP)	0 Site-to-Site VPN Tunnels

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

3.- Continue with the normal FMT steps same as in the desktop version tool. Notice in this example there is no target device selected for practical purposes.

Firewall Migration Tool (Version 4.0.3)



Select Target ?

Firewall Management - Cloud-delivered FMC

Choose FTD

Select FTD Device Proceed without FTD

Select FTD Device ▼

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

[Proceed](#)

[Change Device Status](#)

Select Features

Rule Conversion/ Process Config

4.- Once all FMT validations are completed, the configuration is pushed to the cloud-delivered Firepower Management Center.



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)

Related Information

- [Troubleshooting for the Secure Firewall Migration Tool.](#)
- [Getting Started with the Firewall Migration Tool in Cisco Defense Orchestrator.](#)