

# Initialisez et lancez l'outil de migration de pare-feu sur CDO

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Initialiser](#)

[Lancer](#)

[Exemple de migration](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit comment initialiser, lancer et utiliser l'outil de migration Firepower (FMT) sur la plate-forme Cisco Defense Orchestrator (CDO).

## Conditions préalables

### Exigences

Cisco recommande de connaître les sujets suivants :

Outil de migration Firepower (FMT).  
Cisco Defense Orchestrator (CDO).  
Défense contre les menaces Firepower (FTD).

Appareil de sécurité adaptatif (ASA)

### Composants utilisés

Outil de migration de pare-feu (version 4.0.3).

Cisco Defense Orchestrator.

Centre de gestion des pare-feu cloud.

Appareil de sécurité adaptatif.

Fil Firepower Défense.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

L'outil de migration de CDO extrait les configurations des périphériques du périphérique source que vous sélectionnez ou d'un fichier de configuration que vous téléchargez et les migre vers le Centre de gestion des pare-feu fourni dans le cloud et provisionné sur votre locataire CDO.

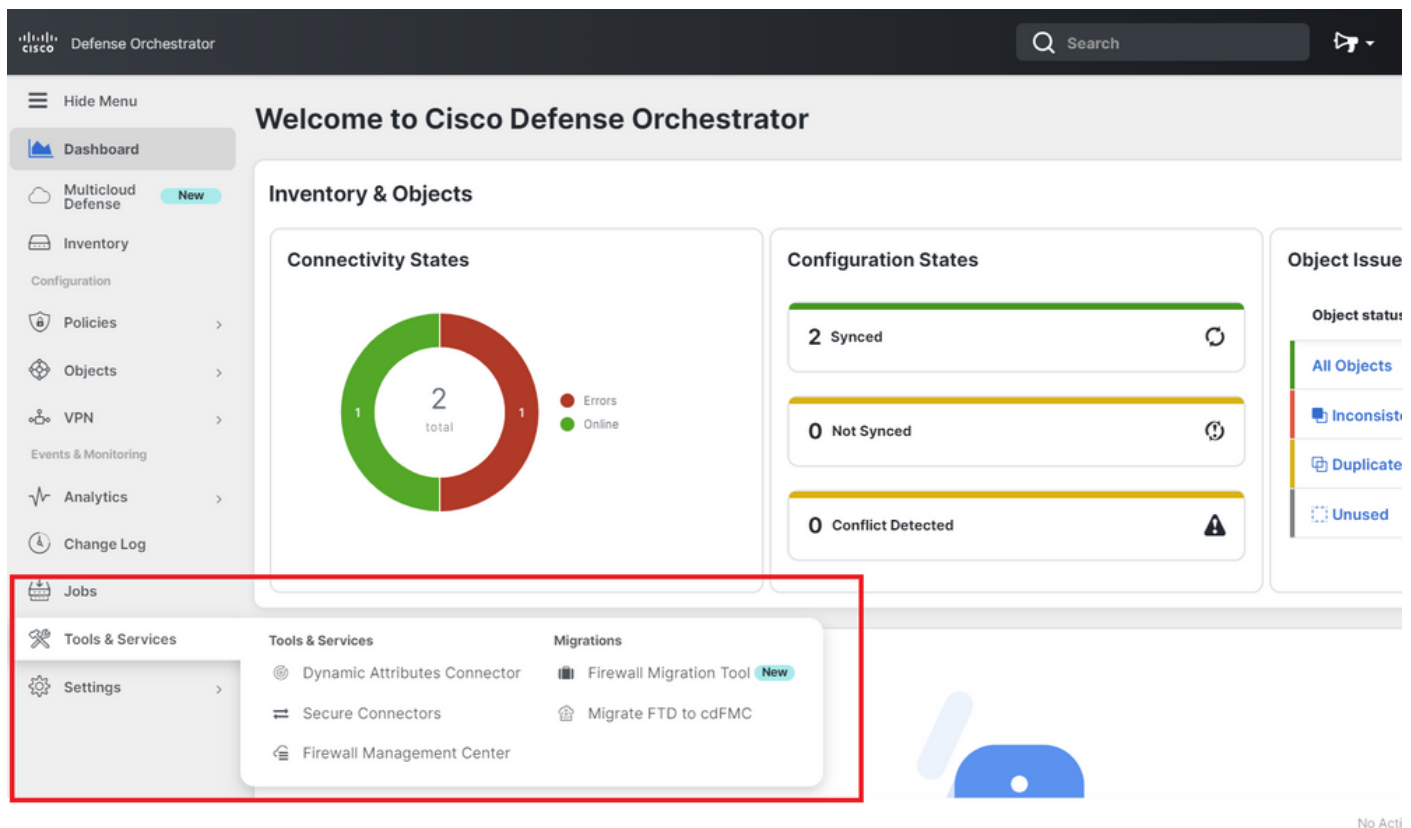
Après avoir validé les configurations, vous pouvez configurer manuellement la configuration non prise en charge sur le Centre de gestion des pare-feu fourni dans le cloud.

## Configurer

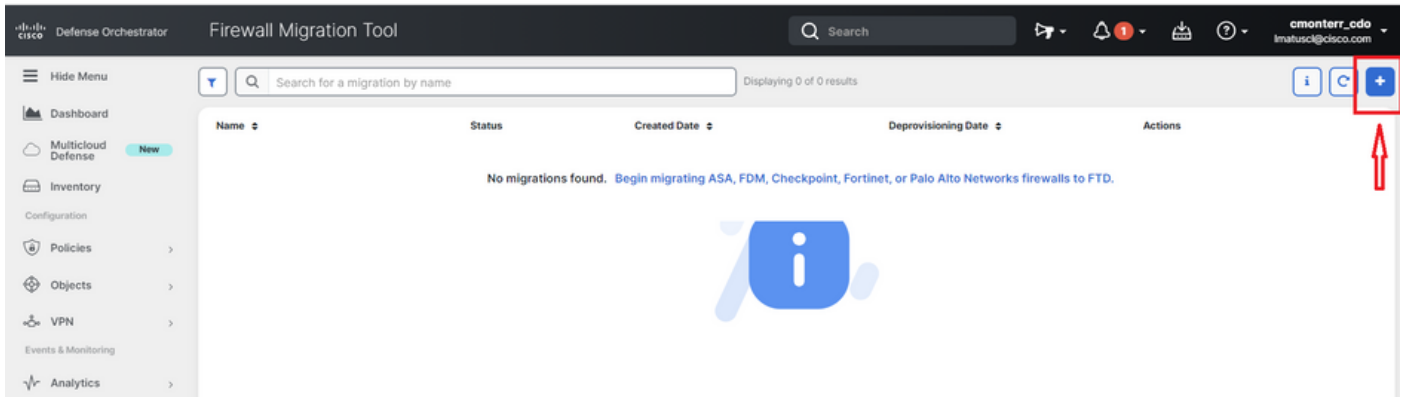
### Initialiser

Ces images décrivent comment initialiser l'outil de migration Firepower sur CDO.

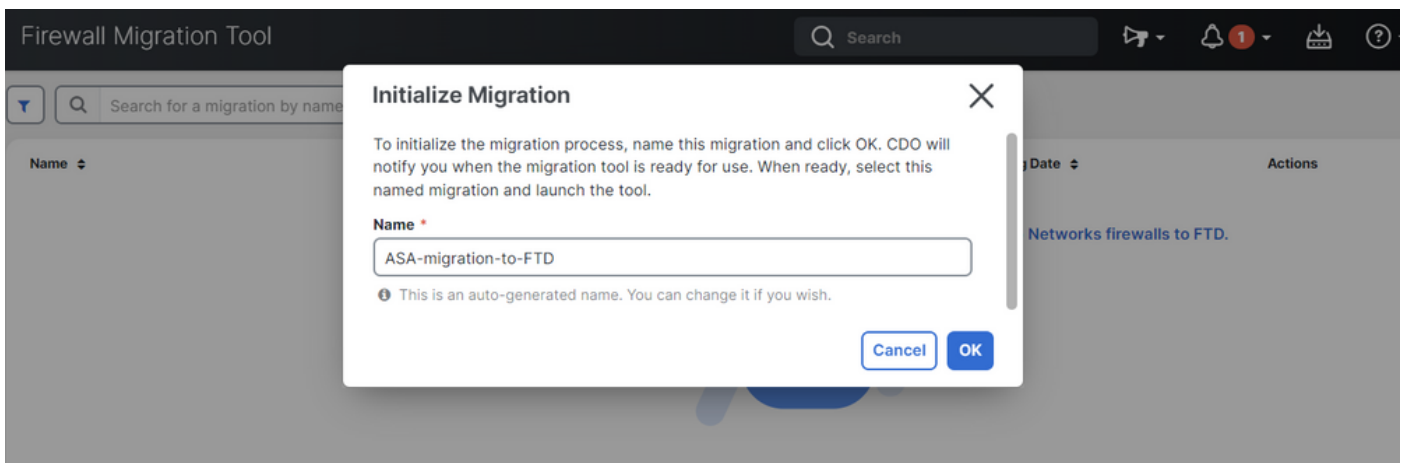
1.- Pour initialiser l'outil de migration de pare-feu, ouvrez votre client CDO et accédez à Outils et services > Outil de migration de pare-feu.



2.- Sélectionnez le bouton plus (+) bleu afin de créer un nouveau processus de migration.

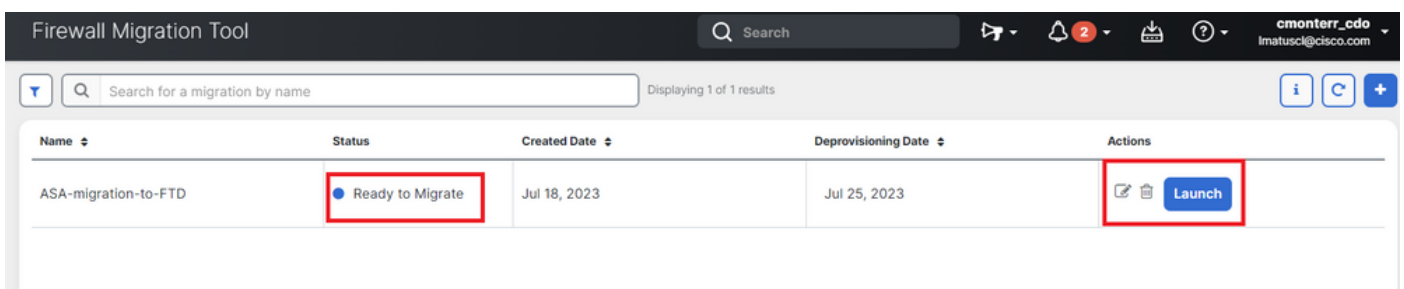


3.- Afin d'initialiser le processus de migration, le CDO génère automatiquement un nom par défaut, vous pouvez le changer si vous le souhaitez et cliquez simplement sur "OK".



## Lancer

1.- Attendez que le processus de migration soit terminé ; l'état doit passer de "Initializing" à "Ready to Migrate". Une fois que c'est prêt, vous pouvez lancer le FMT.



2.- Une instance cloud de l'outil de migration s'ouvre dans un nouvel onglet de navigateur et vous permet d'effectuer vos tâches de migration à l'aide d'un workflow guidé.

L'outil de migration de CDO vous évite d'avoir à télécharger et à gérer la version de bureau de l'outil de migration Secure Firewall.

This screenshot shows the 'Select Source Configuration' step in the Firewall Migration Tool. The 'Source Firewall Vendor' dropdown menu is set to 'Cisco ASA (8.4+)'. A blue 'Start Migration' button is located below the dropdown. To the right, the 'Cisco ASA (8.4+) Pre-Migration Instructions' section is visible, containing a warning message and details about session telemetry and acronyms used.

**Select Source Configuration**

Source Firewall Vendor  
Cisco ASA (8.4+)

Start Migration

**Cisco ASA (8.4+) Pre-Migration Instructions**

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:

## Exemple de migration

Ces images montrent un exemple rapide du processus FMT. Cet exemple migre un fichier de configuration ASA vers le Centre de gestion des pare-feu hébergé sur CDO et fourni dans le cloud.

1.- Exportez la configuration ASA et téléchargez-la vers l'option "Manual Configuration Upload". Si un ASA est déjà intégré à votre CDO, vous pouvez utiliser l'option « Se connecter à ASA ».

This screenshot displays the 'Extract Cisco ASA (8.4+) Information' screen. The 'Extraction Methods' dropdown menu is set to 'Manual Configuration Upload'. Below this, there are two main panels: 'Manual Configuration Upload' and 'Connect to ASA'. The 'Manual Configuration Upload' panel includes instructions on file formats and upload modes, with a warning icon and an 'Upload' button. The 'Connect to ASA' panel provides instructions on selecting devices and includes a 'Connect' button. At the bottom, there are sections for 'Context Selection' and 'Parsed Summary'.

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 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.- Dans cet exemple, le FMT définit automatiquement la "sélection de contexte" en mode de contexte unique. Cependant, vous pouvez sélectionner le contexte souhaité à migrer si votre configuration ASA est exécutée sur plusieurs modes.

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.- Le FMT analyse la configuration ASA et affiche un résumé de votre configuration. Validez et cliquez sur « Suivant » pour passer aux étapes suivantes.

Parsed Summary

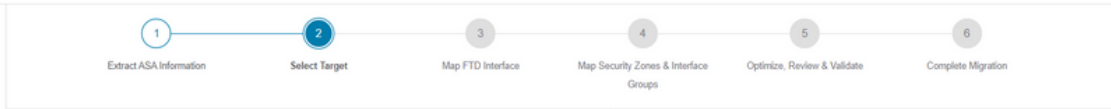
Collect Hitcounts: No. Hitcount information is only available when connected to a live ASA.

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.- Continuez avec les étapes FMT normales comme dans l'outil de version de bureau. Notez que dans cet exemple, aucun équipement cible n'est sélectionné à des fins pratiques.



Select Target ⓘ

Source: Cisco ASA (8.4+)

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

Select Features

Rule Conversion/ Process Config

4.- Une fois toutes les validations FMT terminées, la configuration est transmise au centre de gestion Firepower fourni dans le cloud.

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)

## Informations connexes

- [Dépannage de l'outil de migration Secure Firewall.](#)
- [Mise en route de l'outil de migration de pare-feu dans Cisco Defense Orchestrator.](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.