

Initialisieren und Starten des Firewall Migration Tools auf CDO

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[Konfigurieren](#)
[Initialisieren](#)
[Starten](#)
[Migrationsbeispiel](#)
[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie das FirePOWER Migration Tool (FMT) auf der Cisco Defense Orchestrator (CDO)-Plattform initialisiert, gestartet und verwendet wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

FirePOWER Migration-Tool (FMT)
Cisco Defense Orchestrator (CDO)
FirePOWER Threat Defense (FTD)

Adaptive Security Appliance (ASA)

Verwendete Komponenten

Firewall Migration Tool (Version 4.0.3).

Cisco Defense Orchestrator

über die Cloud bereitgestelltes Firewall Management Center

Adaptive Security Appliance

FirePOWER-Thread-Schutz.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Das Migrations-Tool in CDO extrahiert die Gerätekonfigurationen aus dem ausgewählten Quellgerät oder aus einer hochgeladenen Konfigurationsdatei und migriert sie in das über die Cloud bereitgestellte Firewall Management Center, das auf Ihrem CDO-Tenant bereitgestellt wird.

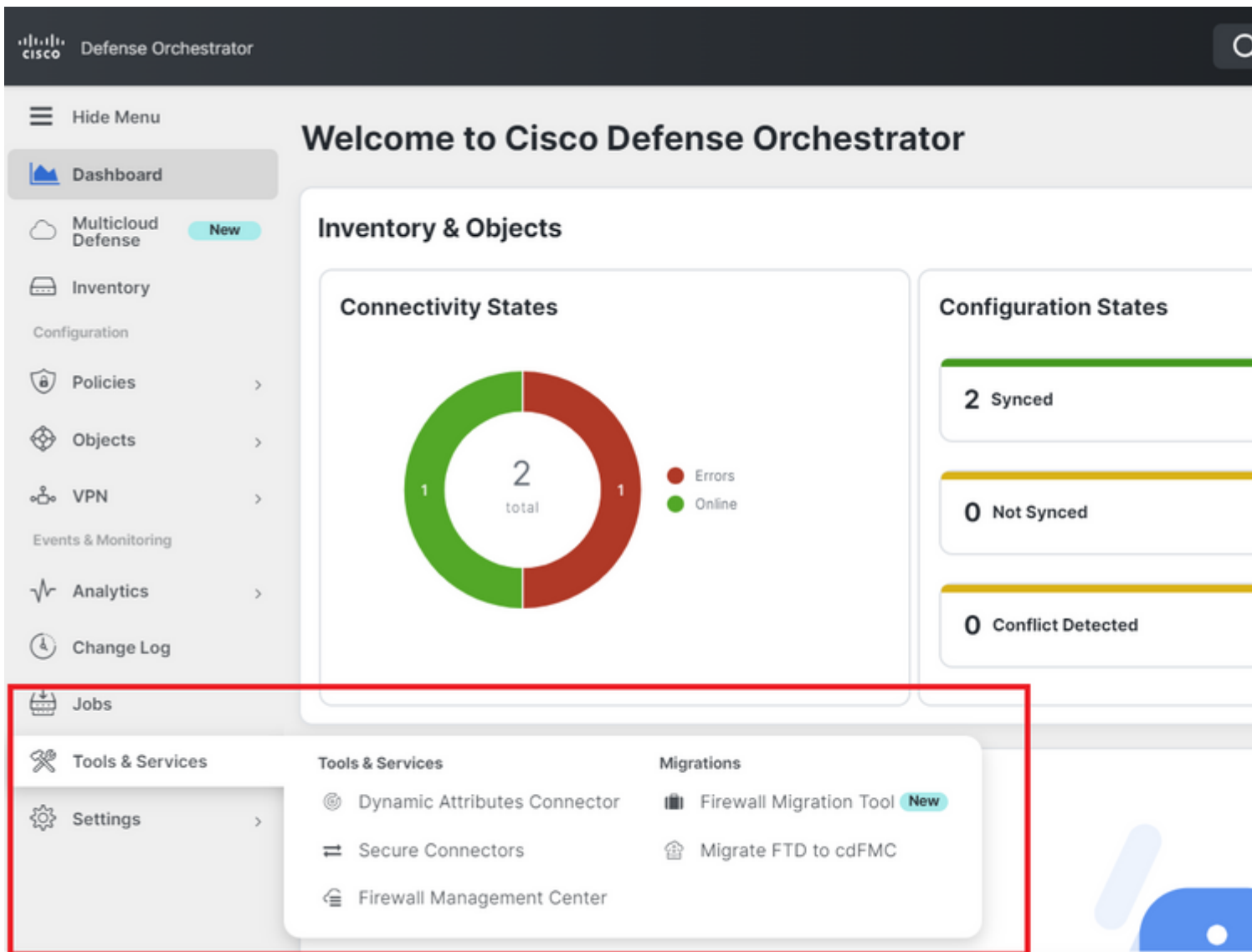
Nachdem Sie die Konfigurationen validiert haben, können Sie die nicht unterstützte Konfiguration im über die Cloud bereitgestellten Firewall Management Center manuell konfigurieren.

Konfigurieren

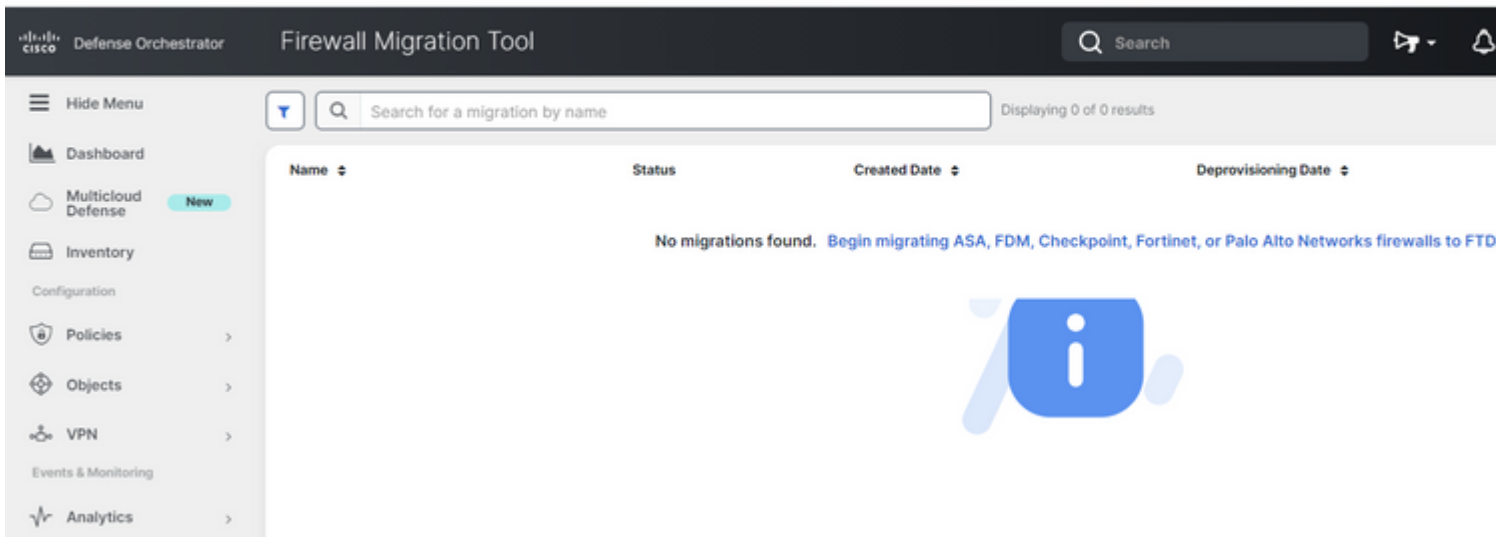
Initialisieren

Diese Bilder beschreiben, wie das FirePOWER Migration Tool auf CDO initialisiert werden kann.

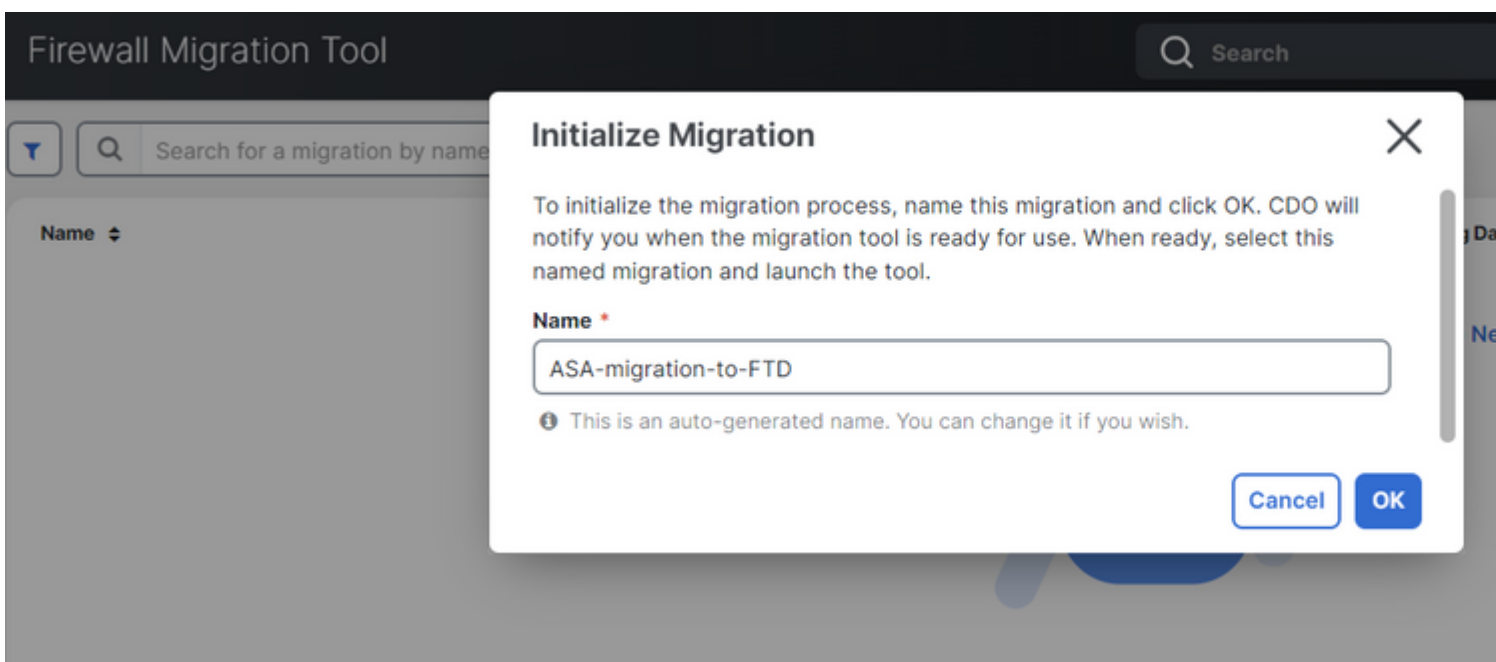
1.- Um das Firewall Migration Tool zu initialisieren, öffnen Sie Ihren CDO-Tenant, und navigieren Sie zu **Tools & Services > Firewall Migration Tool**.



2.- Klicken Sie auf das blaue Pluszeichen (+), um einen neuen Migrationsprozess zu erstellen.



3.- Um den Migrationsprozess zu initialisieren, generiert das CDO automatisch einen Standardnamen, den Sie bei Bedarf ändern können und klicken Sie einfach auf "OK".



Starten

1.- Warten Sie, bis der Migrationsprozess abgeschlossen ist. Der Status muss von "**Initialisierung**" zu "**Bereit zur Migration**" wechseln. Sobald dies bereit ist, können Sie die FMT starten.

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

2.- Eine Cloud-Instanz des Migrations-Tools wird in einer neuen Browser-Registerkarte geöffnet und ermöglicht Ihnen, Ihre Migrationsaufgaben mithilfe eines geführten Workflows auszuführen.

Das Migrations-Tool von CDO macht das Herunterladen und Verwalten der Desktop-Version des Migrationstools für sichere Firewalls überflüssig.

Cisco 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:

Migrationsbeispiel

Diese Bilder zeigen ein kurzes Beispiel für den FMT-Prozess. In diesem Beispiel wird eine ASA-Konfigurationsdatei zu dem über die Cloud bereitgestellten Firewall Management Center migriert, das auf CDO gehostet wird.

1.- Exportieren Sie die ASA-Konfiguration, und laden Sie sie in die Option "**Manuelles Hochladen der Konfiguration**" hoch. Wenn Sie eine ASA bereits an Ihr CDO angeschlossen haben, können Sie die Option "Mit ASA verbinden" verwenden.

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 diesem Beispiel setzt das FMT die "Kontextauswahl" automatisch auf den Einzel-Kontextmodus. Sie können jedoch den gewünschten zu migrierenden Kontext auswählen, wenn Ihre ASA-Konfiguration im Mehrfachmodus ausgeführt wird.

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/RAVPNEIGRP)

0

Network Objects

0

Port Objects

3.- Das FMT analysiert die ASA-Konfiguration und zeigt eine Zusammenfassung Ihrer Konfiguration an. Validieren Sie, und klicken Sie auf "Weiter", um mit den nächsten Schritten fortzufahren.

Parsed Summary

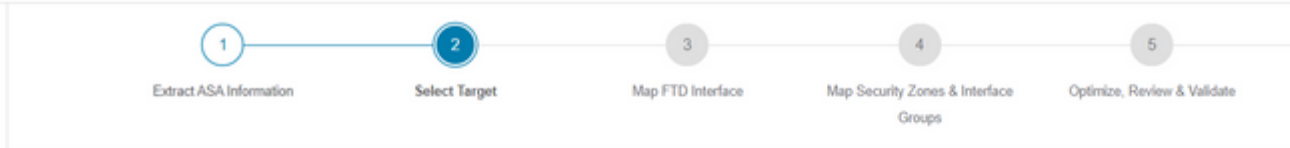
Collect Hitcounts: No. Hitcount information is only available when connected to a live ASA.

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.- Fahren Sie mit den normalen FMT-Schritten wie im Desktop-Versionswerkzeug fort. Beachten Sie, dass in diesem Beispiel kein Zielgerät für praktische Zwecke ausgewählt wurde.

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.- Nach Abschluss aller FMT-Validierungen wird die Konfiguration an das Cloud-basierte FirePOWER Management Center weitergeleitet.



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)

Zugehörige Informationen

- [Fehlerbehebung für das Secure Firewall Migration-Tool.](#)
- [Erste Schritte mit dem Firewall Migration Tool in Cisco Defense Orchestrator.](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.