

Konfigurieren von FTD aus der ASA-Konfigurationsdatei mit dem FirePOWER Migration Tool

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Überprüfung](#)

[Bekannte Fehler im Zusammenhang mit dem FirePOWER Migration-Tool](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt ein Beispiel für die Migration von Adaptive Security Appliance (ASA) zu Firepower Threat Defense (FTD) auf FPR4145.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der ASA
- Kenntnisse von FirePOWER Management Center (FMC) und FTD

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ASA Version 9.12(2)
- FTD-Version 6.7.0
- FMC-Version 6.7.0
- Firepower Migration Tool Version 2.5.0

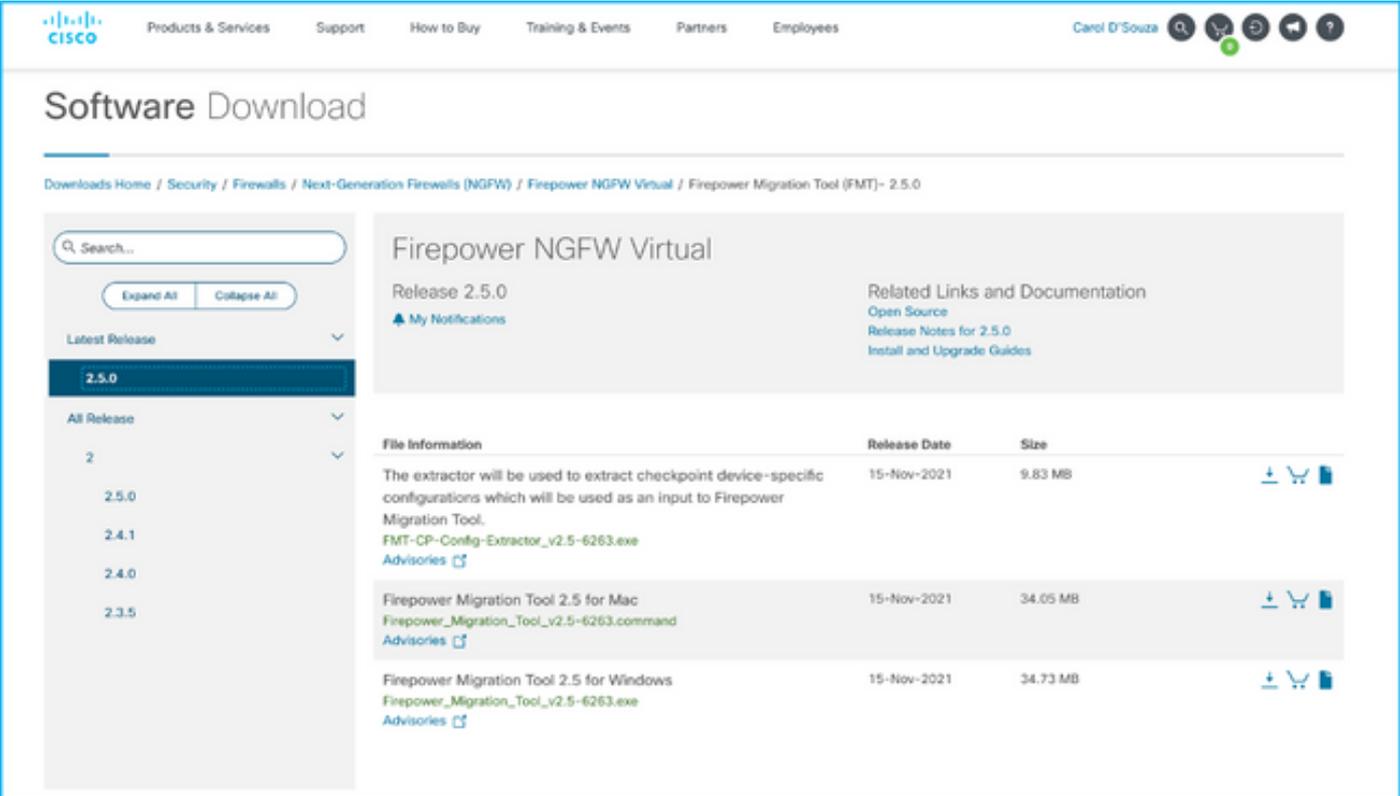
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen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

Hintergrundinformationen

Exportieren Sie die ASA-Konfigurationsdatei im Format **.cfg** oder **.txt**. FMC sollte mit FTD bereitgestellt werden, die unter diesem registriert ist.

Konfigurieren

1. Laden Sie das FirePOWER Migration Tool von software.cisco.com herunter, wie im Bild gezeigt.



The screenshot shows the Cisco Software Download page for Firepower NGFW Virtual, Release 2.5.0. The page includes a search bar, navigation tabs (Products & Services, Support, How to Buy, Training & Events, Partners, Employees), and a user profile (Carol D'Souza). The main content area displays the product name, release version, and a table of file information.

File Information	Release Date	Size	
The extractor will be used to extract checkpoint device-specific configurations which will be used as an input to Firepower Migration Tool. FMT-CP-Config-Extractor_v2.5-6263.exe Advisories 🔗	15-Nov-2021	9.83 MB	↓ 🛒 📄
Firepower Migration Tool 2.5 for Mac Firepower_Migration_Tool_v2.5-6263.command Advisories 🔗	15-Nov-2021	34.05 MB	↓ 🛒 📄
Firepower Migration Tool 2.5 for Windows Firepower_Migration_Tool_v2.5-6263.exe Advisories 🔗	15-Nov-2021	34.73 MB	↓ 🛒 📄

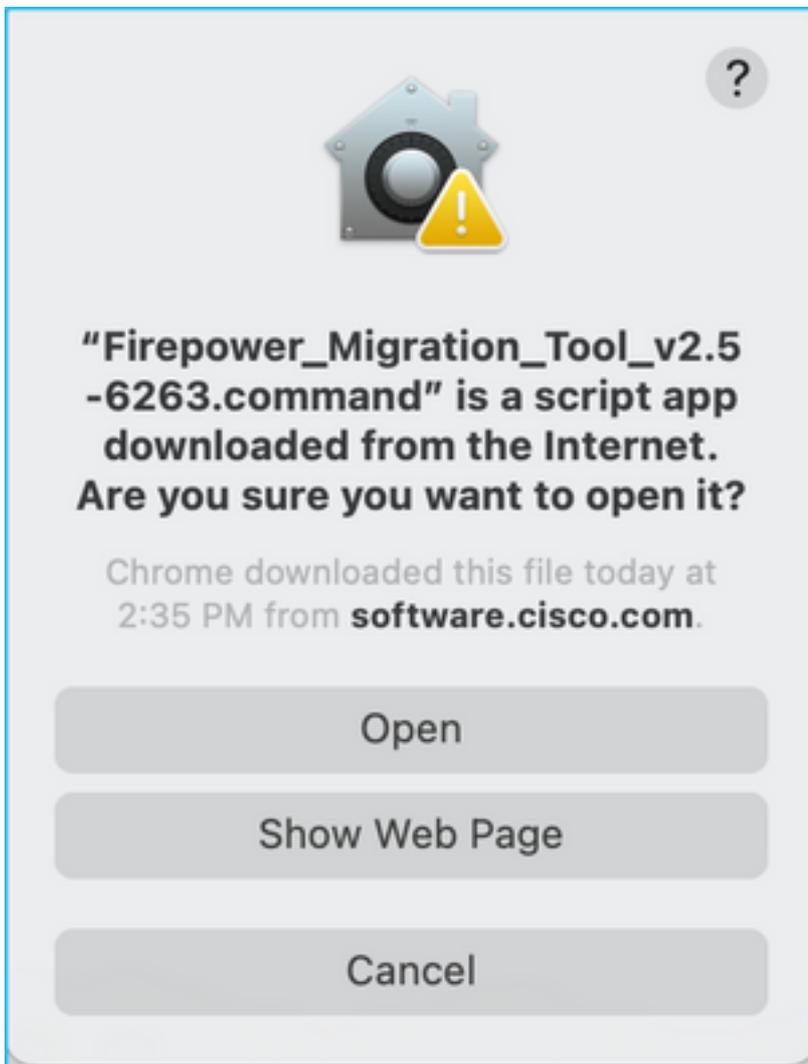
2. Überprüfen und überprüfen Sie die Anforderungen im Abschnitt [Richtlinien und Einschränkungen](#) für das Firepower Migration Tool.

3. Wenn Sie eine Migration einer großen Konfigurationsdatei planen, konfigurieren Sie die Standby-Einstellungen, damit das System während eines Migrationstempels nicht in den Ruhemodus versetzt wird.

3.1. Navigieren Sie unter Windows zu Energieoptionen in der Systemsteuerung. Klicken Sie neben Ihrem aktuellen Energiesparplan auf **Energiesparplaneinstellungen ändern**. Ändern Sie den **Energiesparmodus** auf **Nie**. Klicken Sie auf **Änderungen speichern**.

3.2. Navigieren Sie für MAC zu **System Preferences > Energy Saver (Systemvoreinstellungen > Energiesparmodus)**. Aktivieren Sie das Kontrollkästchen neben dem Eintrag, um zu verhindern, dass der Computer automatisch schließt, wenn das Display ausgeschaltet ist, und ziehen Sie den Schieberegler **Display Aus** nach dem Schieberegler Nie.

Anmerkung: Diese Warnung wird angezeigt, wenn MAC-Benutzer versuchen, die heruntergeladene Datei zu öffnen. Ignorieren Sie dies und befolgen Sie Schritt 4 A.



4. Antwort: Für MAC - Verwenden Sie das Terminal und führen Sie diese Befehle aus.

```
CAROLDSO-M-WGYT:~ caroldso$ cd Downloads/  
CAROLDSO-M-WGYT:Downloads caroldso$ chmod 750 Firepower_Migration_Tool_v2.5-6263  
.command  
CAROLDSO-M-WGYT:Downloads caroldso$ ./Firepower_Migration_Tool_v2.5-6263.command  
  
[75653] PyInstaller Bootloader 3.x  
[75653] LOADER: executable is /Users/caroldso/Downloads/Firepower_Migration_Tool  
_v2.5-6263.command  
[75653] LOADER: hompath is /Users/caroldso/Downloads  
[75653] LOADER: _MEIPASS2 is NULL  
[75653] LOADER: archivename is /Users/caroldso/Downloads/Firepower_Migration_Too  
l_v2.5-6263.command  
[75653] LOADER: Cookie found at offset 0x219AE08  
[75653] LOADER: Extracting binaries  
[75653] LOADER: Executing self as child
```

```
127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /inline.318b50c57b4eba3d437b.bundle.js HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /cui-font.880241c0aa87aa899c6a.woff2 HTTP/1.1" 200 -
2021-11-23 14:49:47,999 [INFO      | cco_login] > "EULA check for an user"
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/cisco.svg HTTP/1.1" 200 -
2021-11-23 14:49:48,013 [DEBUG     | common] > "session table records count:1"
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /api/eula_check HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/icons/login.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/1.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/2.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /favicon.ico HTTP/1.1" 200 -
```

4. B. Für Windows - doppelklicken Sie auf das Firepower Migration Tool, um es in einem Google Chrome-Browser zu starten.

5. Akzeptieren Sie die Lizenz, wie im Bild gezeigt.

← → ↻ 🏠 ⓘ localhost:8888/#/eula

 Firepower Migration Tool

END USER LICENSE AGREEMENT

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail; including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof. This agreement, any supplemental license terms and any specic product terms at www.cisco.com/go/softwareterms (collectively, the "EULA") govern Your Use of the Software.

1. **Acceptance of Terms.** By Using the Software, You agree to be bound by the terms of the EULA. If you are entering into this EULA on behalf of an entity, you represent that you have authority to bind that entity. If you do not have such authority or you do not agree to the terms of the EULA, neither you nor the entity may Use the Software and it may be returned to the Approved Source for a refund within thirty (30) days of the date you acquired the Software or Cisco product. Your right to return and refund applies only if you are the original end user licensee of the Software.

2. **License.** Subject to payment of the applicable fees and compliance with this EULA, Cisco grants You a limited, non-exclusive and non-transferable license to Use object code versions of the Software and the Documentation solely for Your internal operations and in accordance with the Entitlement and the Documentation. Cisco licenses You the right to Use only the Software You acquire from an Approved Source. Unless contrary to applicable law, You are not licensed to Use the Software on

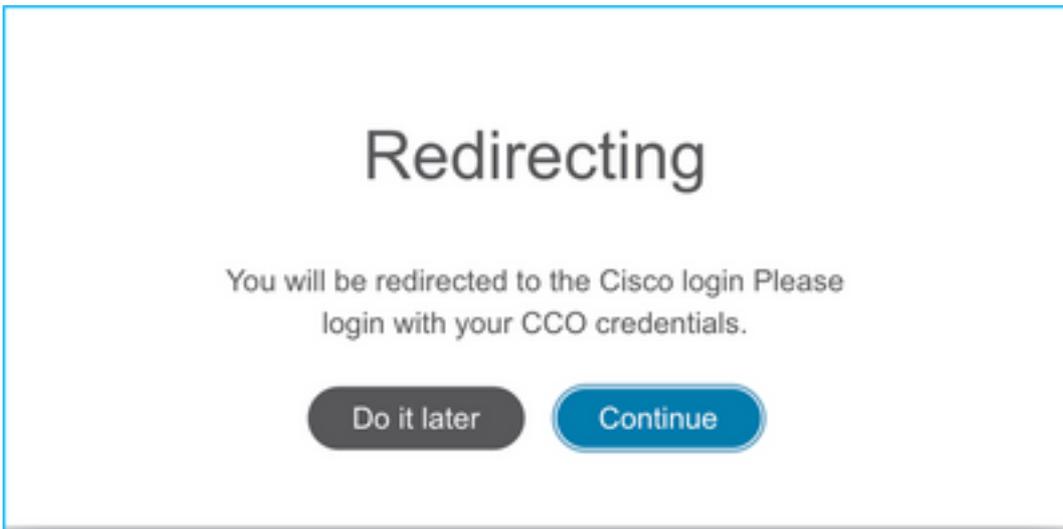
I have read the content of the EULA and SEULA and agree to terms listed.

Proceed

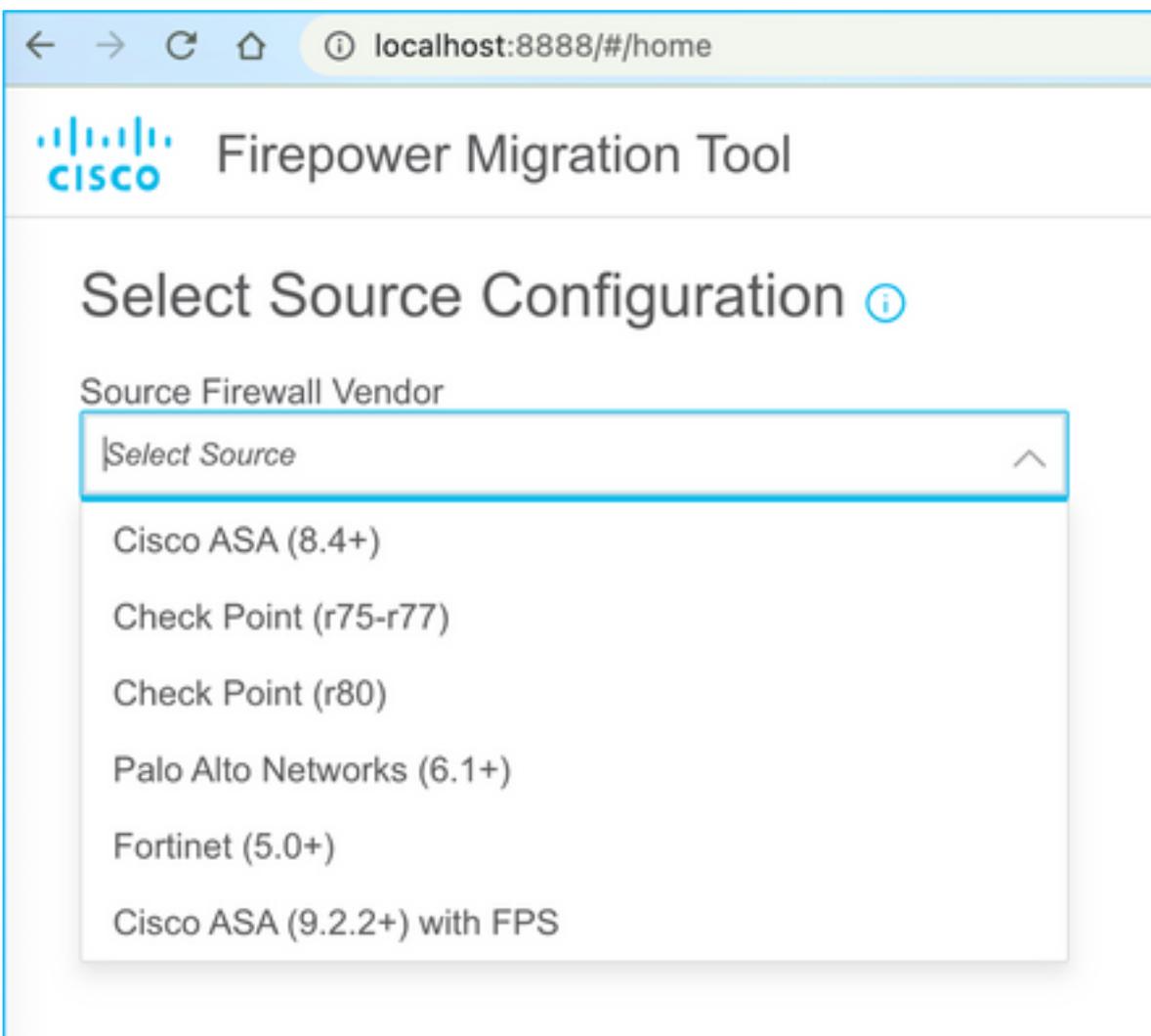
6. Klicken Sie auf der Anmeldeseite des FirePOWER Migration Tool auf den Link Anmelden mit CCO, um sich mit Ihren Anmeldeinformationen bei Ihrem Cisco.com-Konto anzumelden.

Anmerkung: Wenn Sie kein Cisco.com-Konto haben, erstellen Sie es auf der Anmeldeseite

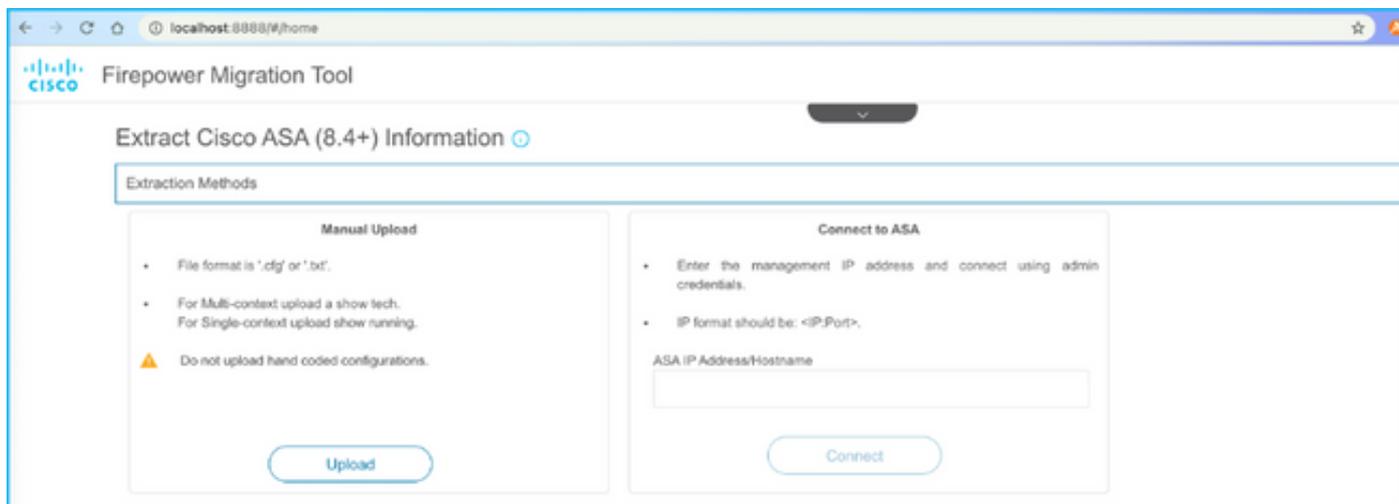
von Cisco.com. Melden Sie sich mit den folgenden Standardanmeldeinformationen an:
Benutzername - Administratorkennwort - Admin123.



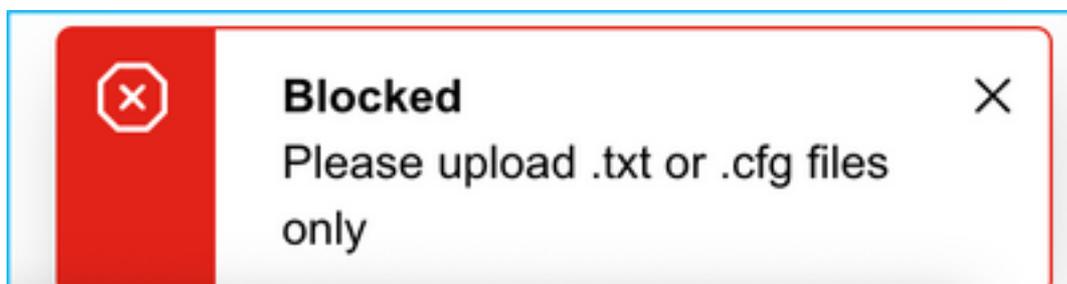
7. Wählen Sie die Quellkonfiguration aus. In diesem Szenario ist dies Cisco ASA (8.4+).



8. Wählen Sie Manual Upload (Manuelles Hochladen) aus, wenn Sie keine Verbindung zur ASA haben. Andernfalls können Sie die aktuelle Konfiguration von der ASA abrufen und die Verwaltungs-IP- und Anmeldedaten eingeben. In unserem Szenario wurde ein manueller Upload durchgeführt.



Anmerkung: Dieser Fehler wird angezeigt, wenn die Datei nicht unterstützt wird. Stellen Sie sicher, dass das Format in Nur-Text geändert wird. (Fehler wird trotz der Erweiterung .cfg angezeigt).



```
ASAConfig.cfg — Edited
asa# show running-config
: Saved
:
:
: Serial Number: FLM22160652
: Hardware: FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
:
ASA Version 9.12(2)
:
hostname asa
enable password ***** pbkdf2
:
license smart
feature tier standard
names
no mac-address auto
:
interface Ethernet1/1
no nameif
no security-level
no ip address
:
interface Ethernet1/2
nameif Inside
cts manual
security-level 0
no ip address
:
interface Ethernet1/3
nameif Outside
cts manual
security-level 0
no ip address
```

9. Nach dem Hochladen der Datei werden die Elemente analysiert, um eine Zusammenfassung bereitzustellen, wie im Bild gezeigt:

The screenshot displays the Cisco Firepower Migration Tool interface. The main heading is "Extract Cisco ASA (8.4+) Information". Below this, there are several sections: "Extraction Methods" with a dropdown menu, "Manual Upload" showing "ASAConfig.cfg.txt", "Context Selection" with a dropdown menu, and "Selected Context" set to "Single Context Mode". A "Parsed Summary" dropdown is also visible. A note states: "Collect Hitcounts: No. Hitcount information is only available when connected to a live ASA." Below this, a grid of seven cards displays the following counts: 20 Access Control List Lines, 88 Network Objects, 14 Port Objects, 8 Logical Interfaces, 9 Static Routes, 4 Network Address Translation, and 1 Site-to-Site VPN Tunnels. A footer note indicates: "Pre-migration report will be available after selecting the targets."

10. Geben Sie die FMC-IP und die Anmeldeinformationen ein, auf die die ASA-Konfiguration migriert werden soll. Stellen Sie sicher, dass der FMC IP von Ihrer Workstation aus erreichbar ist.

Firepower Migration Tool Source: Cisco ASA (8.4+)

Select Target ⓘ

Connect to FMC ▼

FMC IP Address/Hostname
10.106.52.10

Connect

Choose FTD >

Select Features >

Rule Conversion/ Process Config >

✕

FMC LOGIN

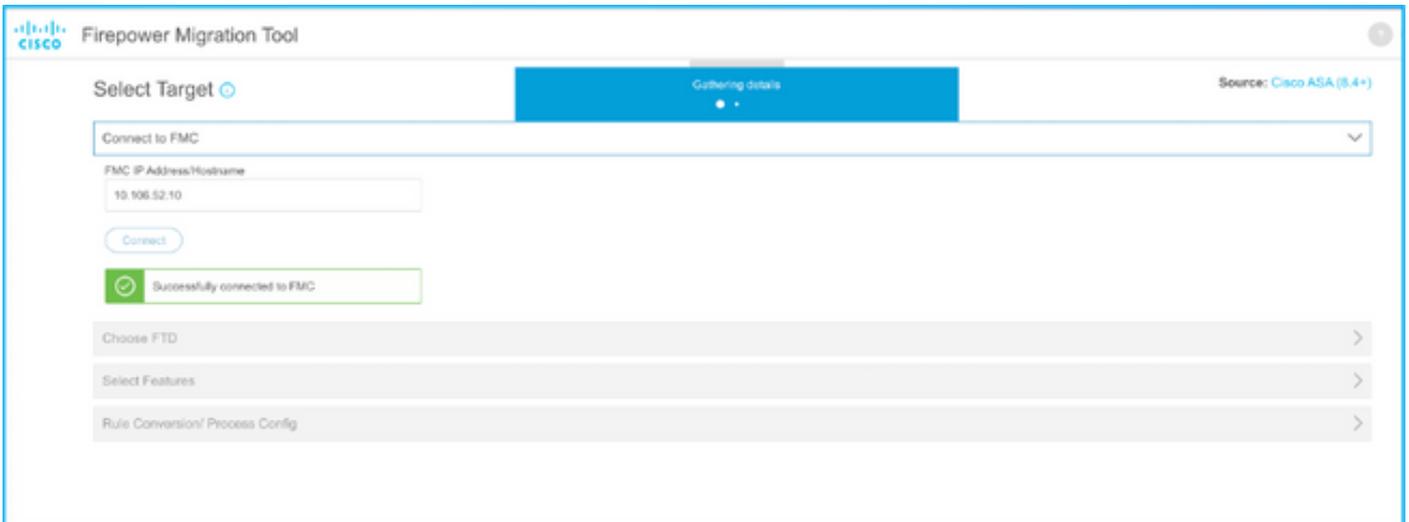
IP Address/Hostname

Username

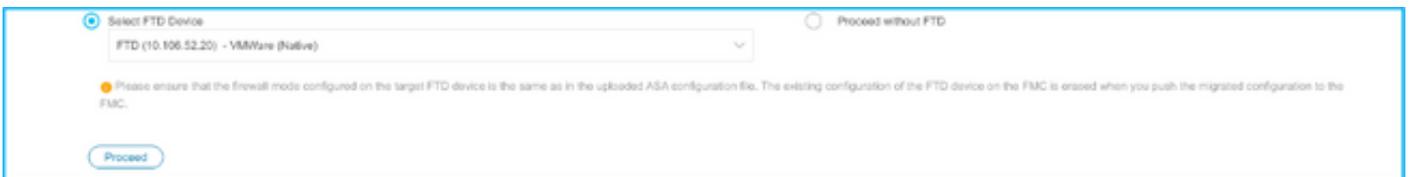
Password

Login

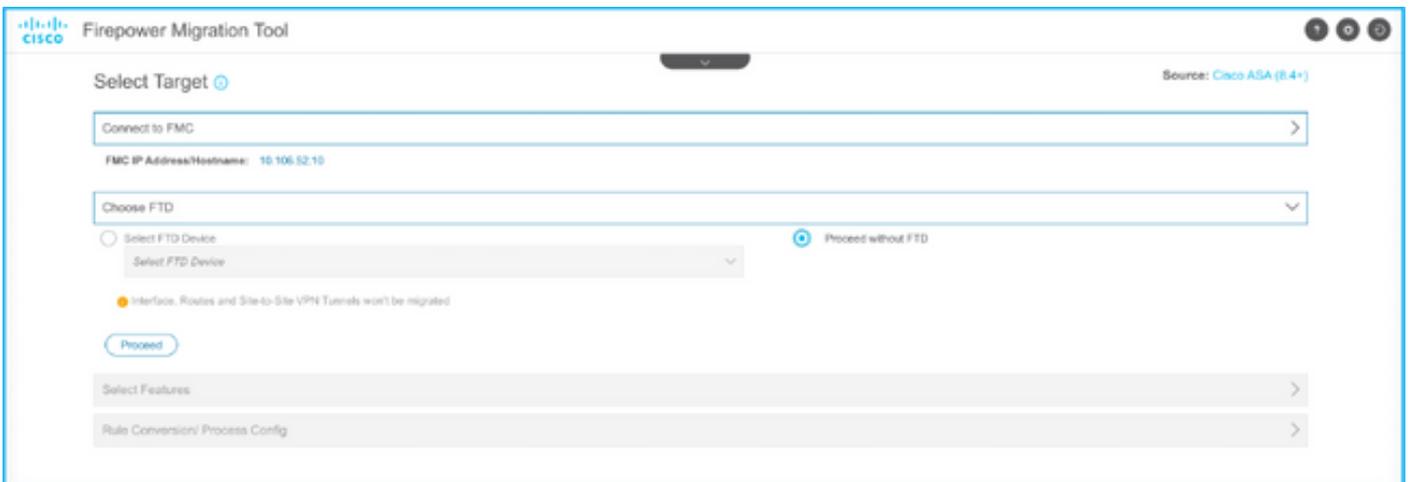
11. Sobald das FMC angeschlossen ist, werden die verwalteten FTDs darunter angezeigt.



12. Wählen Sie das FTD aus, in das Sie die Migration der ASA-Konfiguration durchführen möchten.



Anmerkung: Es wird empfohlen, das FTD-Gerät auszuwählen. Andernfalls müssen Schnittstellen, Routen und die Site-to-Site-VPN-Konfiguration manuell erfolgen.



13. Wählen Sie die zu migrierenden Funktionen aus, wie im Bild gezeigt.

Select Features

Device Configuration

- Interfaces
- Routes
- Site-to-Site VPN Tunnels
 - Policy Based (Crypto Map)
 - Route Based (VTI)

Shared Configuration

- Access Control
 - Populate destination security zones
 - Migrate tunnelled rules as PreFilter
- NAT
 - Network Objects
 - Port Objects
 - Time based Objects

Optimization

- Migrate Only Referenced Objects
- Object Group Search

Inline Grouping

- CSMASDM

[Proceed](#)

14. Wählen Sie **Konvertierung starten**, um die Vormigration einzuleiten, die die Elemente der FTD-Konfiguration ausfüllt.

Rule Conversion/ Process Config

[Start Conversion](#)

0 parsing errors found. Refer to the pre-migration report for more details.

Please download the Pre-Migration report for a detailed summary of the parsed configuration. [Download Report](#)

<p style="font-size: 24px; margin: 0;">13</p> <p style="margin: 0;">Access Control List Lines</p>	<p style="font-size: 24px; margin: 0;">98</p> <p style="margin: 0;">Network Objects</p>	<p style="font-size: 24px; margin: 0;">30</p> <p style="margin: 0;">Port Objects</p>	
<p style="font-size: 24px; margin: 0;">2</p> <p style="margin: 0;">Logical Interfaces</p>	<p style="font-size: 24px; margin: 0;">9</p> <p style="margin: 0;">Static Routes</p>	<p style="font-size: 24px; margin: 0;">4</p> <p style="margin: 0;">Network Address Translation</p>	
<p style="font-size: 24px; margin: 0;">1</p> <p style="margin: 0;">Site-to-Site VPN Tunnels</p>			

15. Klicken Sie auf **Bericht herunterladen**, um den Bericht vor der Migration anzuzeigen, wie im Bild gezeigt.

File | /Users/caroldso/Downloads/pre_migration_report_asa_2021-11-23_09-41-15.html

CISCO Pre-Migration Report

Note: Review all contents of this pre-migration report carefully. Unsupported rules will not be migrated completely, which can potentially alter your original configuration, restrict some traffic, or permit unwanted traffic. We recommend reviewing the configuration by Firepower Threat Defense after the configuration is successfully migrated.

1. Overall Summary:

A summary of the supported ASA configuration elements that can be successfully migrated to Firepower Threat Defense.

Collection Method	Manual
ASA Configuration Name	ASAConfig.cfg.txt
ASA Version	9.12(2)
ASA Hostname	asa
ASA Device Model	FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
Hit Count Feature	No
IP SLA Monitor	0
Total Extended ACEs	13
ACEs Migratable	13
Site to Site VPN Tunnels	1
Logical Interfaces	2
Network Objects and Groups	98
Service Objects and Groups	30
Static Routes	9
NAT Rules	4

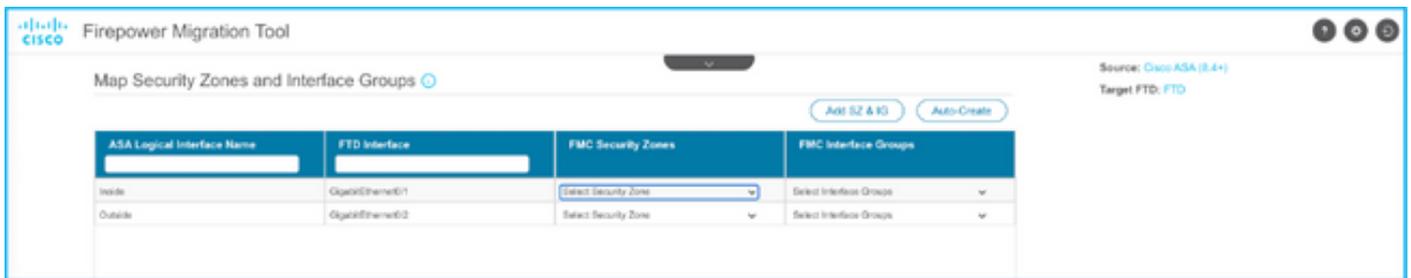
Note: ACEs that are applied outbound or not attached to interfaces using the access-group command are ignored.

16. ASA-Schnittstellen zu FTD-Schnittstellen zuordnen, wie im Bild gezeigt.

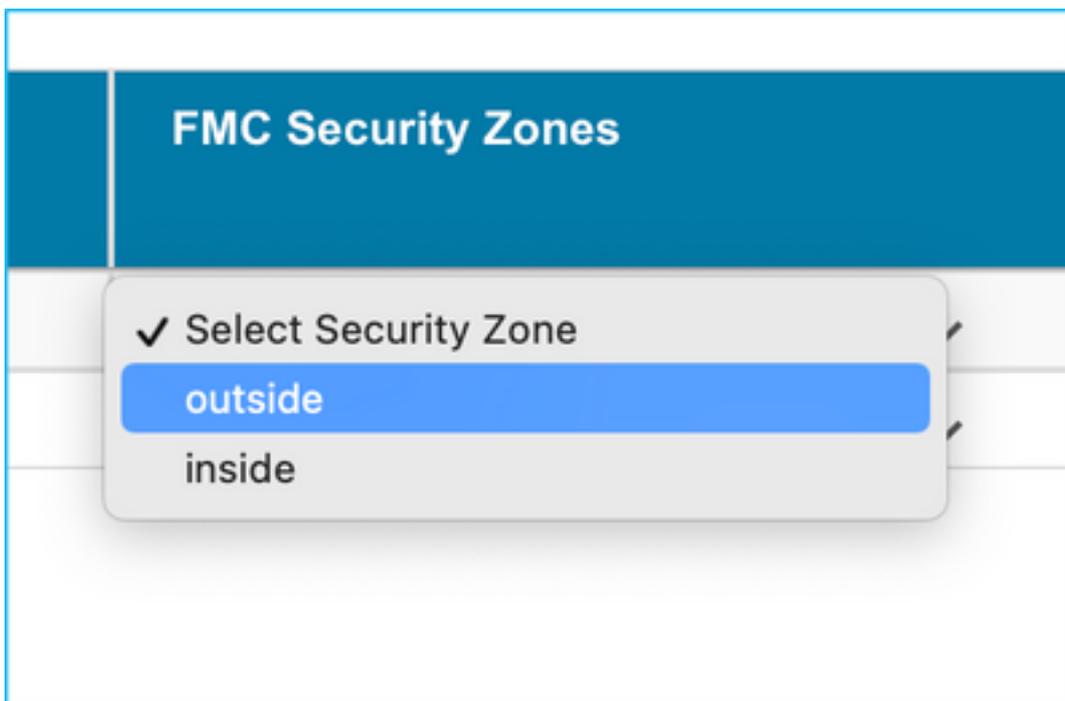
Refresh

ASA Interface Name	FTD Interface Name
Ethernet1/2	Select Interface
Ethernet1/3	GigabitEthernet0/0
	GigabitEthernet0/1
	✓ GigabitEthernet0/2

17. Weisen Sie den FTD-Schnittstellen Sicherheitszonen und Schnittstellengruppen zu.



Antwort: Wenn das FMC bereits Sicherheitszonen und Schnittstellengruppen erstellt hat, können Sie diese nach Bedarf auswählen:



B. Wenn Sicherheitszonen und eine Schnittstellengruppe erstellt werden müssen, klicken Sie auf **Add SZ & IG** wie im Bild gezeigt.

✕

Add SZ & IG

Security Zones (SZ) Interface Groups (IG)

Add

iMax 48 characters for Interface Group name. Allowed special characters are _.-+

Interface Groups	Type	Actions
<input style="width: 100%; border: 1px solid #ccc;" type="text" value="Inside"/>	ROUTED	✕ ✓

0 - 0 of 0 |< < > >|

Close

C. Andernfalls können Sie die Option **Auto-Create (Automatisch erstellen)** wählen, mit der Sicherheitszonen und Schnittstellengruppen mit dem Namen **ASA Logical Interface_sz** und **ASA Logical Interface_ig** erstellt werden.

Auto-Create

Auto-create maps ASA interfaces to existing FTD security zones and interface groups in FMC that have the same name. If no match is found, the Migration Tool creates a new FTD security zone and interface group with the same name in FMC.

Select the objects that you want to map to ASA interfaces

Security Zones Interface Groups

Cancel

Auto-Create

Firepower Migration Tool

Map Security Zones and Interface Groups

Add SZ & IG

Auto-Create

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
Inside	GigabitEthernet0/1	inside	Inside_ig (A)
Outside	GigabitEthernet0/2	outside	Outside_ig (A)

18. Überprüfen und Validieren der erstellten FTD-Elemente Warnmeldungen werden rot angezeigt, wie im Bild gezeigt.

Firepower Migration Tool

Optimize, Review and Validate Configuration

Source: Cisco ASA (8.4+)
Target FTD: FTD

Access Control | NAT | Network Objects | Port Objects | Interfaces | Routes | VPN Objects | Site-to-Site VPN Tunnels

ADP Pre-Filter

Select all 13 entries Selected 0 / 13

#	Name	SOURCE				DESTINATION				State	Action	ACE Count
		Zone	Network	Port	Zone	Network	Port					
1	Outside_access_in_01	outside	any	ANY	ANY				✓	Allow	1	
2	Outside_access_in_02	outside	any	ANY	ANY				✓	Allow	1	
3	Outside_access_in_03	outside	any	ANY	ANY				✓	Allow	2	
4	Outside_access_in_04	outside	any	ANY	ANY				✓	Allow	4	
5	Outside_access_in_05	outside	any	ANY	ANY				✓	Allow	3	
6	Outside_access_in_06	outside	any	ANY	ANY				✓	Allow	2	
7	Outside_access_in_07	outside	any	ANY	ANY				✓	Allow	3	
8	Outside_access_in_08	outside	any	ANY	ANY				✓	Allow	1	
9	Outside_access_in_09	outside	any	ANY	ANY				✓	Allow	8	
10	Outside_access_in_10	outside	any	ANY	ANY				✓	Allow	7	
11	Outside_access_in_11	outside	any	ANY	ANY				✓	Allow	2	
12	Outside_access_in_12	outside	any	ANY	ANY				✓	Allow	1	

50 perpage 1 to 13 of 13 | Page 1 of 1

Update the Pre-Shared-Key(PK) Certificate column highlighted in yellow for each VPN-tunnel rows under Site-to-Site VPN Tunnels tab to validate and proceed with migration. For additional help, click here.

Optimize ACL (RM) [button]

19. Die Migrationsaktionen können wie im Bild gezeigt ausgewählt werden, wenn Sie eine Regel bearbeiten möchten. In diesem Schritt können FTD-Funktionen zum Hinzufügen von Dateien und IPS-Richtlinien durchgeführt werden.

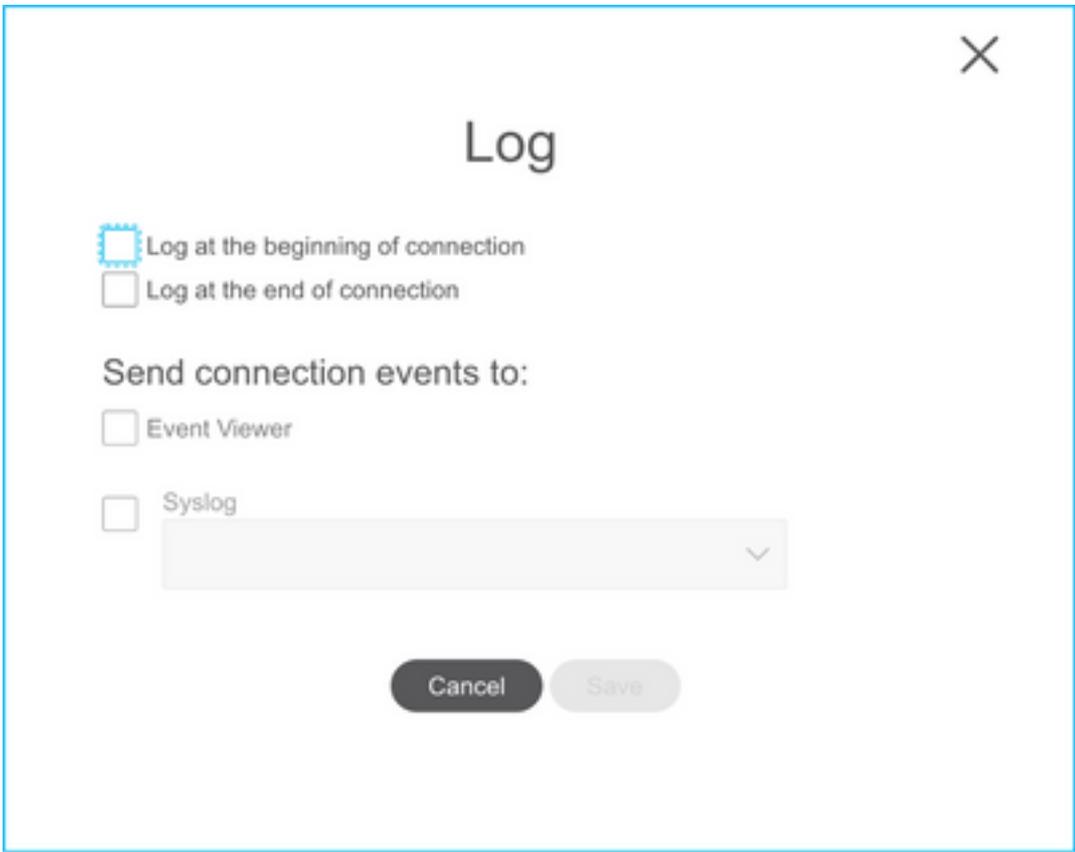
The screenshot shows a configuration interface with a table of rules. At the top, there are tabs for 'ACP' and 'Pre-filter'. Below the tabs, there is a checkbox for 'Select all 13 entries' and a status indicator 'Selected: 13 / 13'. To the right, there is an 'Actions' dropdown menu and a 'Save' button. The table has the following columns: a selection column with checkboxes, an ID column labeled '#', a Name column with a search icon, and a Source column. The 'Actions' menu is open, showing 'MIGRATION ACTIONS' (Do not migrate) and 'RULE ACTIONS' (File Policy, IPS Policy, Log, Rule Action). The table contains 6 rows of data, all with checkboxes selected.

	#	Name	SOURCE
<input checked="" type="checkbox"/>	1	Outside_access_in_#1	network
<input checked="" type="checkbox"/>	2	Outside_access_in_#2	
<input checked="" type="checkbox"/>	3	Outside_access_in_#3	
<input checked="" type="checkbox"/>	4	Outside_access_in_#4	
<input checked="" type="checkbox"/>	5	Outside_access_in_#5	
<input checked="" type="checkbox"/>	6	Outside_access_in_#6	outside any

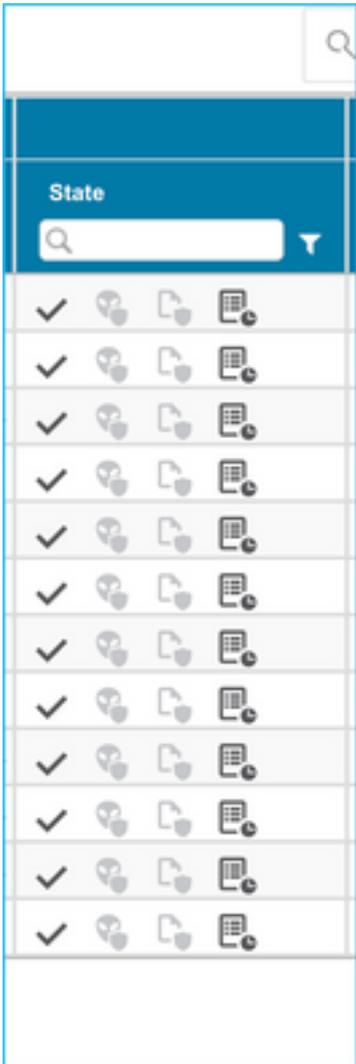
Anmerkung: Wenn File Policies (Dateirichtlinien) bereits im FMC vorhanden sind, werden sie wie im Bild gezeigt ausgefüllt. Gleiches gilt für IPS-Richtlinien zusammen mit den Standardrichtlinien.

The screenshot shows a 'File Policy' dialog box. It has a title bar with a close button (X). Below the title bar, there is a search field labeled 'Select File Policy *'. The dropdown menu is open, showing 'eicar' and 'None'. At the bottom, there are 'Cancel' and 'Select' buttons.

Die Protokollkonfiguration kann für die erforderlichen Regeln durchgeführt werden. Die auf dem FMC vorhandene Syslog-Serverkonfiguration kann zu diesem Zeitpunkt ausgewählt werden.



Die ausgewählten Regelaktionen werden für jede Regel entsprechend hervorgehoben.



20. Ebenso können NAT, Netzwerkobjekt, Port-Objekte, Schnittstellen, Routen, VPN-Objekte, Site-to-Site-VPN-Tunnel und andere Elemente entsprechend Ihrer Konfiguration Schritt für Schritt überprüft werden.

Anmerkung: Eine Warnmeldung wird wie im Bild gezeigt angezeigt, um den vorinstallierten Schlüssel zu aktualisieren, da er nicht in die ASA-Konfigurationsdatei kopiert wird. Wählen Sie **Aktionen > Vorinstallierten Schlüssel aktualisieren**, um den Wert einzugeben.

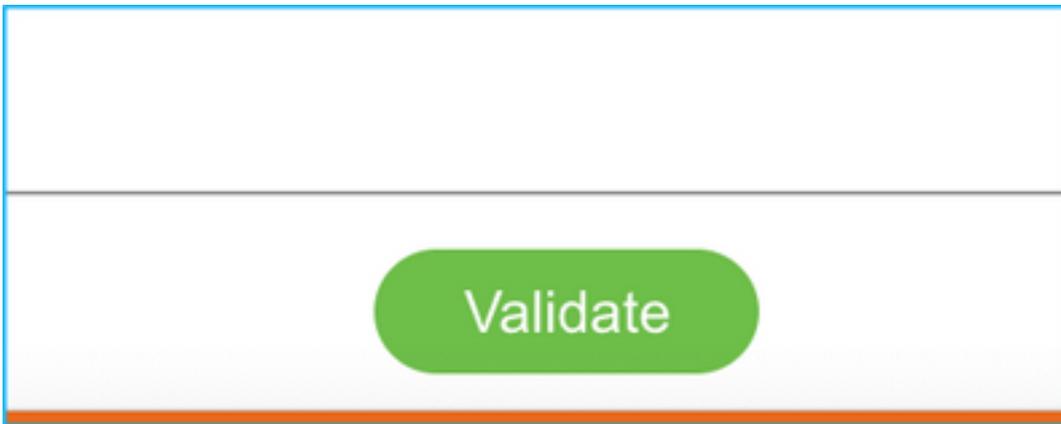
#	Source Interface N...	MIGRATION ACTIONS	Peer IP	IKE	IKEv1 IKEv2 P...	IKEv1 IKEv2 PSEC P...	Auth-entication Type	Protected Networks
1	Outside	Update Pre-shared Key	dynamic	Ikev2	asa_ikev2_psk_key_1	AES256AES128AES3DES...	Preshare...	Source Net... Remote Net...

Update Pre-Shared Key

Pre-Shared Key IKEv2

Cancel Save

21. Klicken Sie schließlich auf das Symbol **Validieren** unten rechts im Bildschirm, wie im Bild gezeigt.



22. Wenn die Validierung erfolgreich war, klicken Sie auf **Konfiguration übertragen** wie im Bild gezeigt.

A dialog box titled "Validation Status" with a close button (X) in the top right corner. It shows a green checkmark icon and the text "Successfully Validated". Below this is a "Validation Summary (Pre-push)" section with seven cards displaying counts for different configuration elements: Access Control List Lines (13), Network Objects (37), Port Objects (14), Logical Interfaces (2), Static Routes (9), Network Address Translation (4), and Site-to-Site VPN Tunnels (1). A yellow note at the bottom states: "Note: The configuration on the target FTD device FTD (10.106.52.20) will be overwritten as part of this migration." A green "Push Configuration" button is located at the bottom center.

Validation Status

✓ Successfully Validated

Validation Summary (Pre-push)

13 Access Control List Lines	37 Network Objects	14 Port Objects	
2 Logical Interfaces	9 Static Routes	4 Network Address Translation	1 Site-to-Site VPN Tunnels

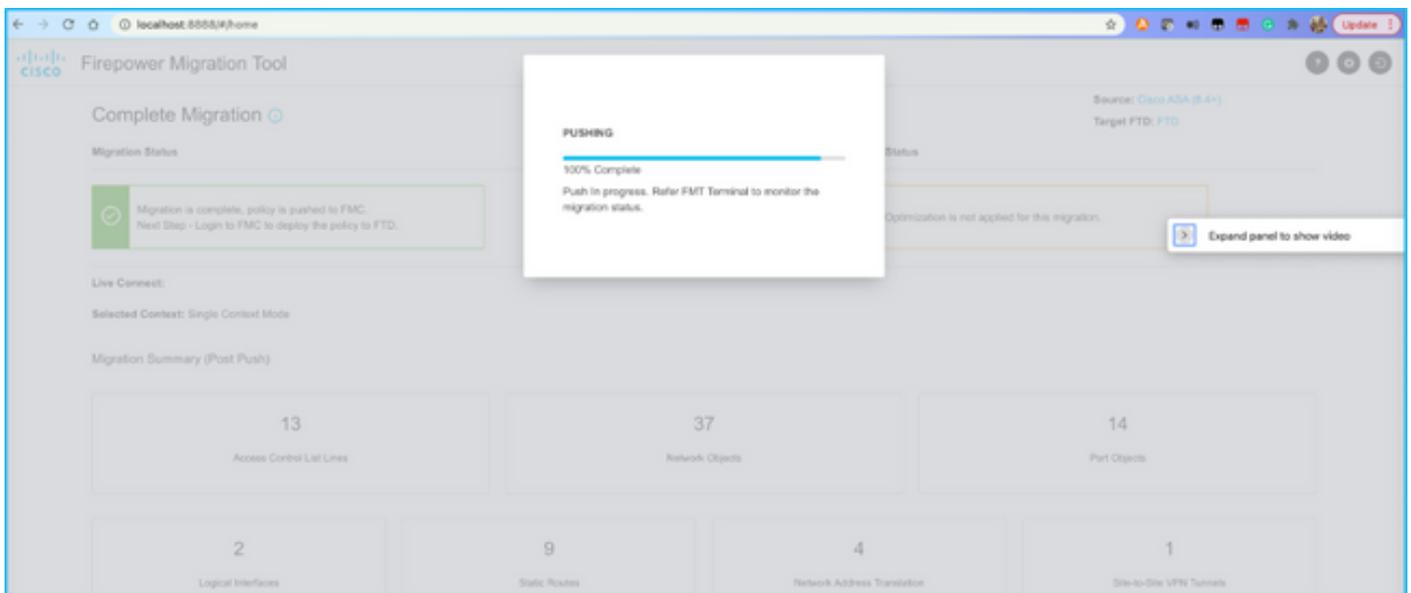
Note: The configuration on the target FTD device FTD (10.106.52.20) will be overwritten as part of this migration.

Push Configuration

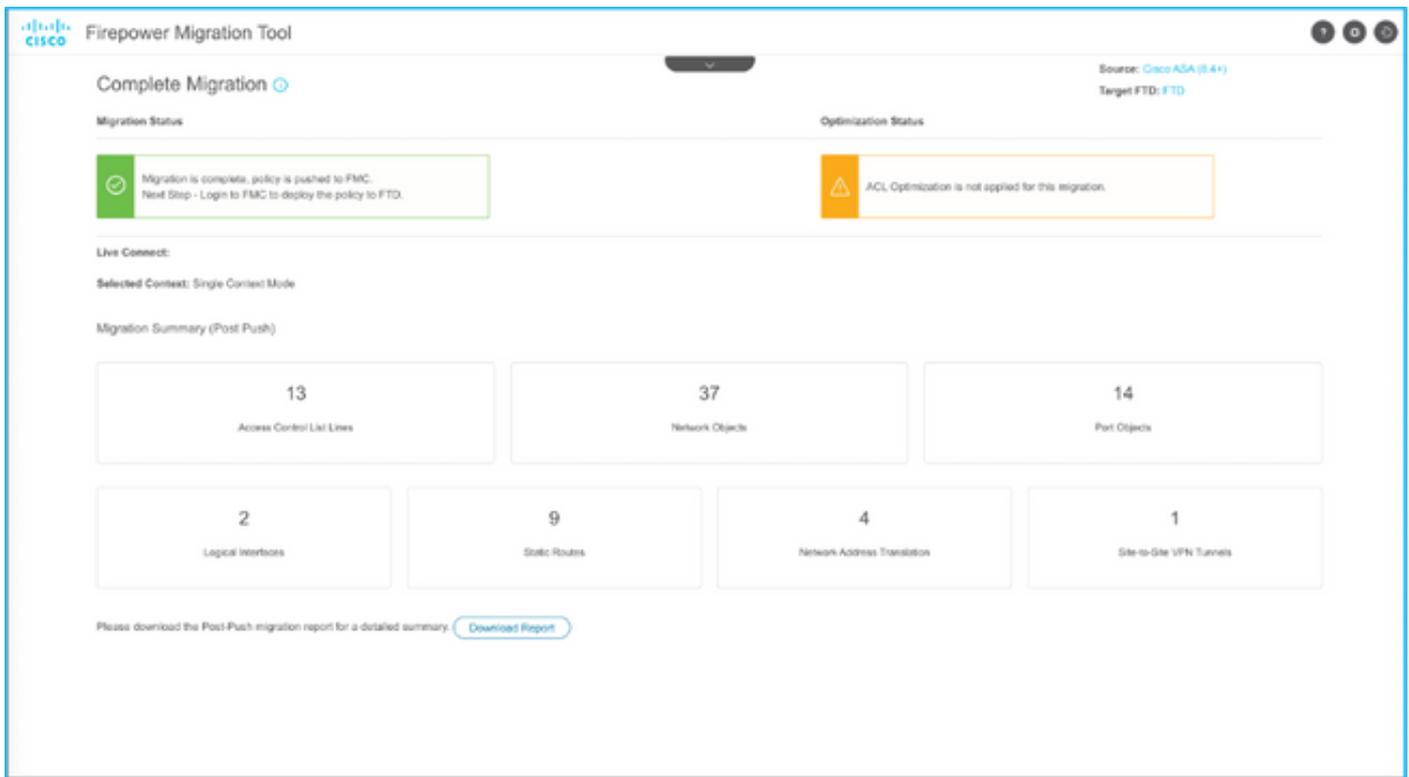
PUSHING

0% Complete

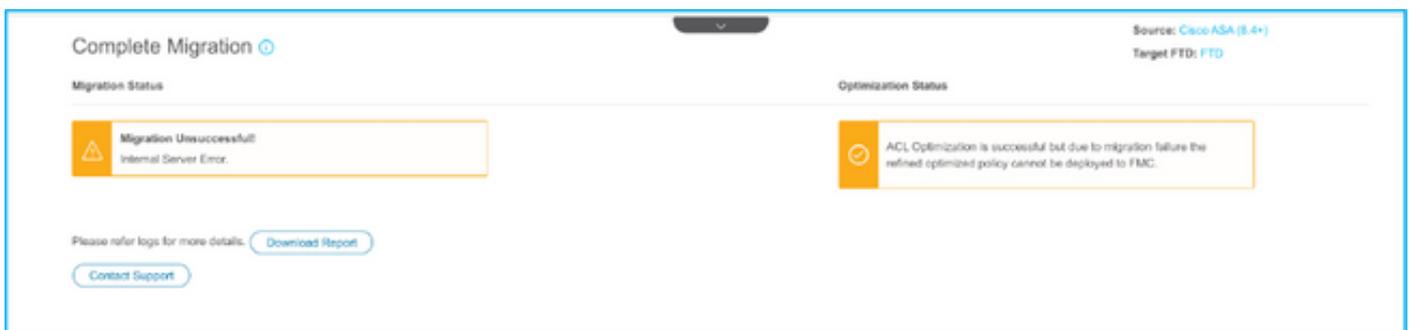
Push In progress. Refer FMT Terminal to monitor the migration status.



23. Nach erfolgreicher Migration wird die Meldung im Bild angezeigt.



Anmerkung: Wenn die Migration nicht erfolgreich war, klicken Sie auf **Bericht herunterladen**, um den Bericht nach der Migration anzuzeigen.

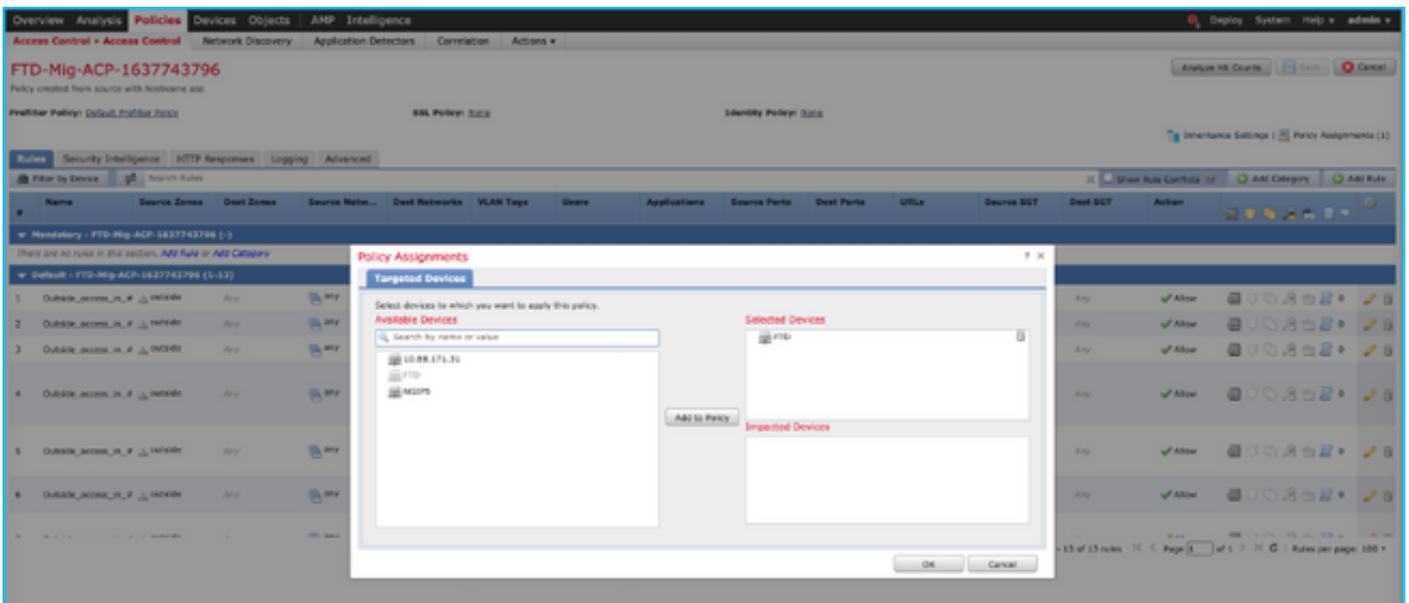


Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

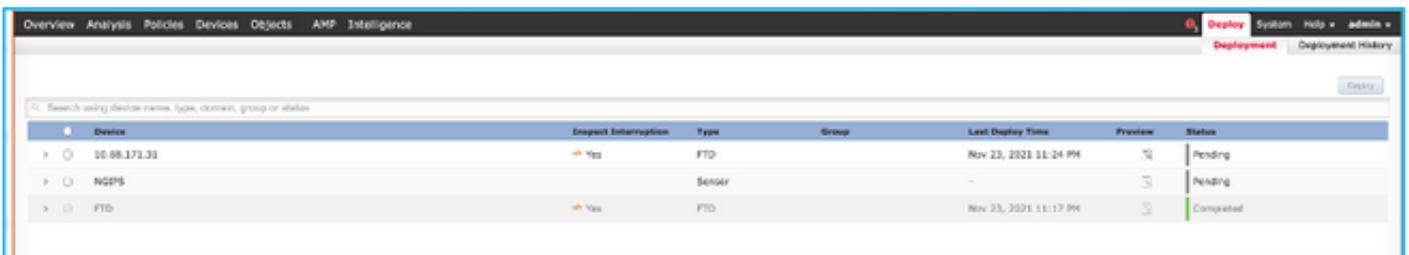
Validierung auf dem FMC.

1. Navigieren Sie zu **Richtlinien > Zugriffskontrolle > Zugriffskontrollrichtlinie > Richtlinienzuweisung**, um zu bestätigen, dass die ausgewählte FTD eingetragen ist.



Anmerkung: Die Richtlinie für die Migrationszugriffskontrolle hätte einen Namen mit dem Präfix **FTD-Mig-ACP**. Wenn in Schritt 2.8 kein FTD ausgewählt wurde, muss das FTD im FMC ausgewählt werden.

2. Schicken Sie die Richtlinie an die FTD. Navigieren Sie zu **Deploy > Deployment > FTD Name > Deploy (Bereitstellung > Bereitstellung > FTD-Name > Bereitstellen)**, wie im Bild gezeigt.



Bekannte Fehler im Zusammenhang mit dem FirePOWER Migration-Tool

- Cisco Bug ID [CSCwa56374](#) - Das FMT-Tool stürzt auf der Seite für die Zonenzuordnung ab und weist bei hoher Speichernutzung einen Fehler auf.
- Cisco Bug ID [CSCvz88730](#) - Interface Push Failure für den Schnittstellentyp FTD Port-Channel Management
- Cisco Bug ID [CSCvx21986](#) - Port-Channel-Migration zur Zielplattform - Virtuelles FTD wird nicht unterstützt
- Cisco Bug ID [CSCvy63003](#) - Das Migrations-Tool sollte die Schnittstellenfunktion deaktivieren, wenn FTD bereits Teil des Clusters ist.
- Cisco Bug ID [CSCvx08199](#) - Die ACL muss geteilt werden, wenn die Anwendungsreferenz mehr als 50 beträgt.

Zugehörige Informationen

- [Migration der ASA Firewall zum Schutz vor Bedrohungen mit dem Firewall Migration-Tool](#)

- [Technischer Support und Dokumentation für Cisco Systeme](#)