

Migratie van een VHK van het ene VCC naar een ander VCC

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u een Cisco Firepower Threat Defence (FTD) apparaat kunt migreren tussen Firepower Management Centers.

Voorwaarden

Zorg er voordat u het migratieproces start voor dat u over deze voorwaarden beschikt:

- Toegang tot de VCC's van herkomst en van bestemming.
- Administratieve referenties voor zowel het VCC als het FTD.
- Maak een back-up van de huidige VCC-configuratie.
- Zorg ervoor dat de FTD-apparaten een compatibele softwareversie uitvoeren met het FMC van de bestemming.
- Controleer of het VCC van bestemming dezelfde versie heeft als het VCC van herkomst.

Vereisten

- In beide VCC's moeten compatibele softwareversies worden uitgevoerd.
- Netwerkconnectiviteit tussen het FTD-apparaat en beide FMC's.
- Voldoende opslag en middelen op het FMC van bestemming om het FTD-apparaat te kunnen ontvangen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

Cisco Firepower Threat Defense Virtual (FTDv) versie 7.2.5

Firepower Management Center Virtual (FMCv) versie 7.2.5

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De migratie van een FTD-apparaat van het ene VCC naar het andere omvat verschillende stappen, waaronder het uitschrijven van het FMC van de bron, het voorbereiden van het FMC van bestemming en het opnieuw registreren van het apparaat. Dit proces waarborgt dat alle beleid en configuraties correct worden overgebracht en toegepast.

Configureren

Configuraties

1. Log in bij het broncontrolecentrum.



Secure Firewall Management Center

Username

Password

Log In

2. Navigeer naar Apparaten > Apparaatbeheer en selecteer het te migreren apparaat.



View By: Group

All (1) Error (0) Warning (0) Offline (0) Normal (1) Deployment Pending (0) Upgrade (0) Snort 3 (1)

[Collapse All](#)

<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	▼ Ungrouped (1)			
<input type="checkbox"/>	192.168.15.31 Snort 3 192.168.15.31 - Routed	FTDv for VMware	7.2.5	N/A

3. Navigeer in het gedeelte Apparaat naar apparaat en klik op Exporteren om uw apparaatinstellingen te exporteren.

FTD1

Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

General



Name: FTD1
Transfer Packets: Yes
Mode: Routed
Compliance Mode: None
TLS Crypto Acceleration: Disabled

Device Configuration:

Import **Export** Download

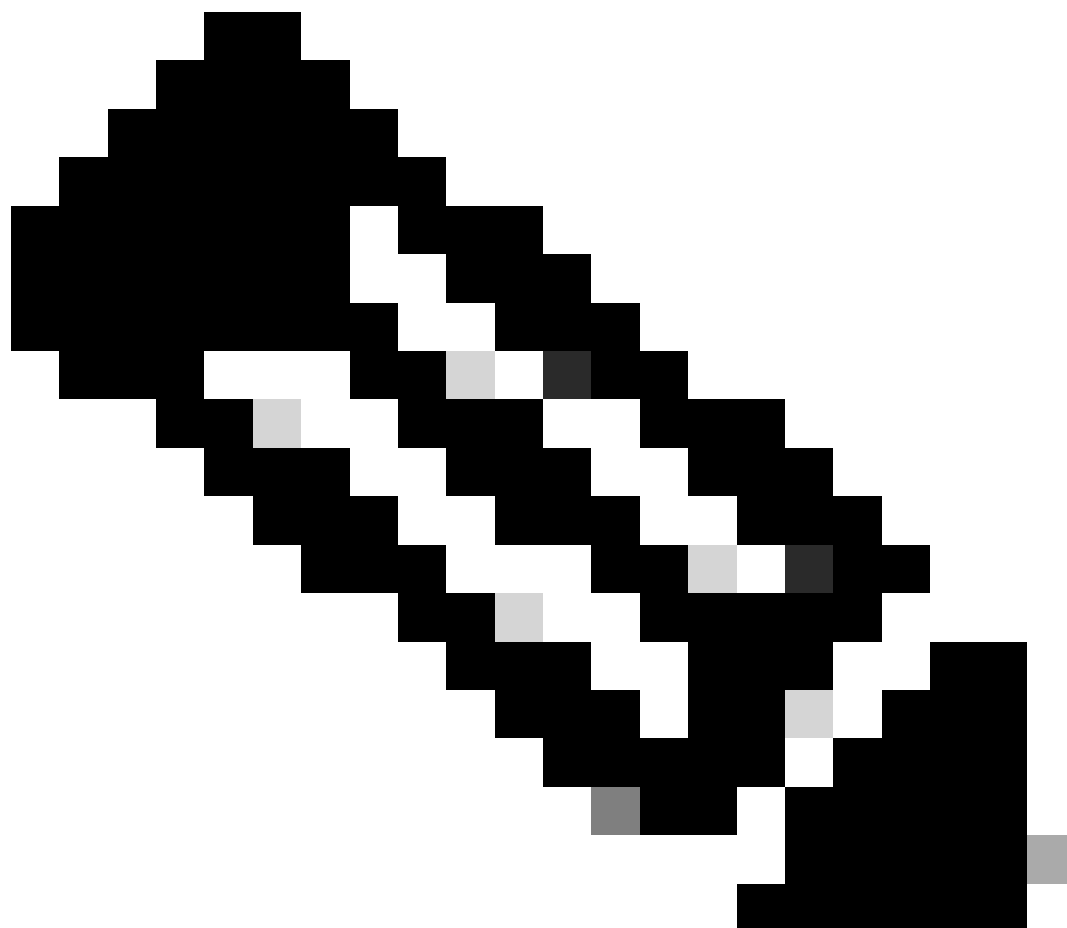
4. Zodra de configuratie is geëxporteerd, moet u deze downloaden.

Device Configuration Download

Backup taken on **14-Oct-2024 07:05 PM** is available.

[Click here to download the package](#)

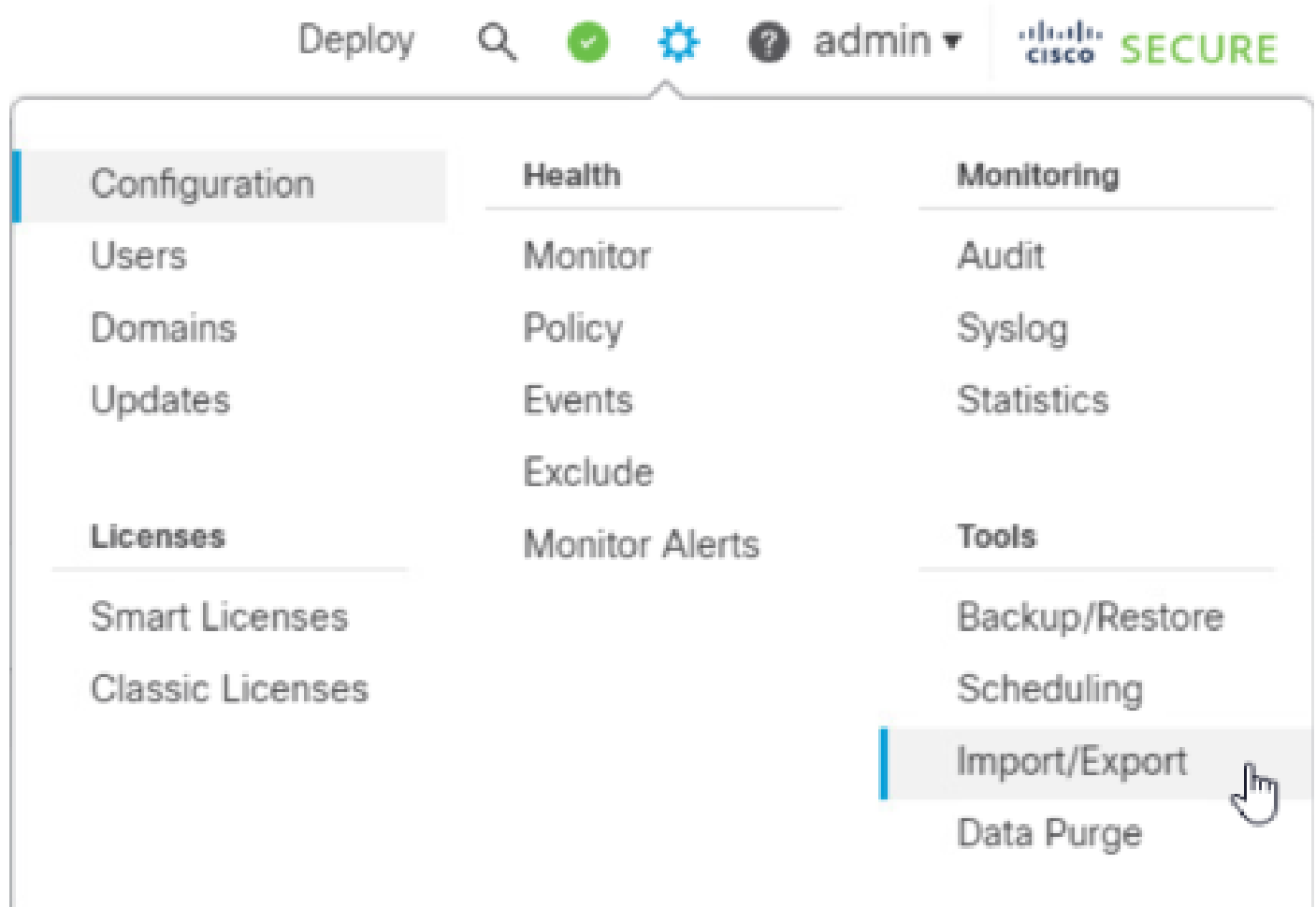
OK



Opmerking: Het gedownloade bestand moet de extensie .SFO bevatten en bevat

informatie over apparaatconfiguratie zoals IP-adressen, beveiligingszones, statische routes en andere apparaatinstellingen.

5. U moet het beleid exporteren dat aan het apparaat is gekoppeld, naar **Systeem > Gereedschappen > Importeren/Exporteren**, het beleid selecteren dat u wilt exporteren en op **Exporteren** klikken.



The screenshot displays the Cisco Secure management interface. At the top, there is a navigation bar with the following elements: 'Deploy', a search icon, a green checkmark icon, a blue gear icon, a question mark icon, the user name 'admin' with a dropdown arrow, and the Cisco Secure logo. Below the navigation bar, the main content area is divided into three columns: 'Configuration', 'Health', and 'Monitoring'. The 'Configuration' column contains 'Users', 'Domains', 'Updates', 'Licenses', 'Smart Licenses', and 'Classic Licenses'. The 'Health' column contains 'Monitor', 'Policy', 'Events', 'Exclude', and 'Monitor Alerts'. The 'Monitoring' column contains 'Audit', 'Syslog', 'Statistics', 'Tools', 'Backup/Restore', 'Scheduling', 'Import/Export', and 'Data Purge'. The 'Import/Export' option is highlighted with a blue bar and a mouse cursor icon pointing to it.

∨ Access Control Policy



test

Access Control Policy

> Contextual Cross-launch

> Custom Table View

> Custom Workflow

> Dashboard

> Health Policy

∨ NAT Threat Defense



NAT

NAT Threat Defense

∨ Platform Settings Threat Defense

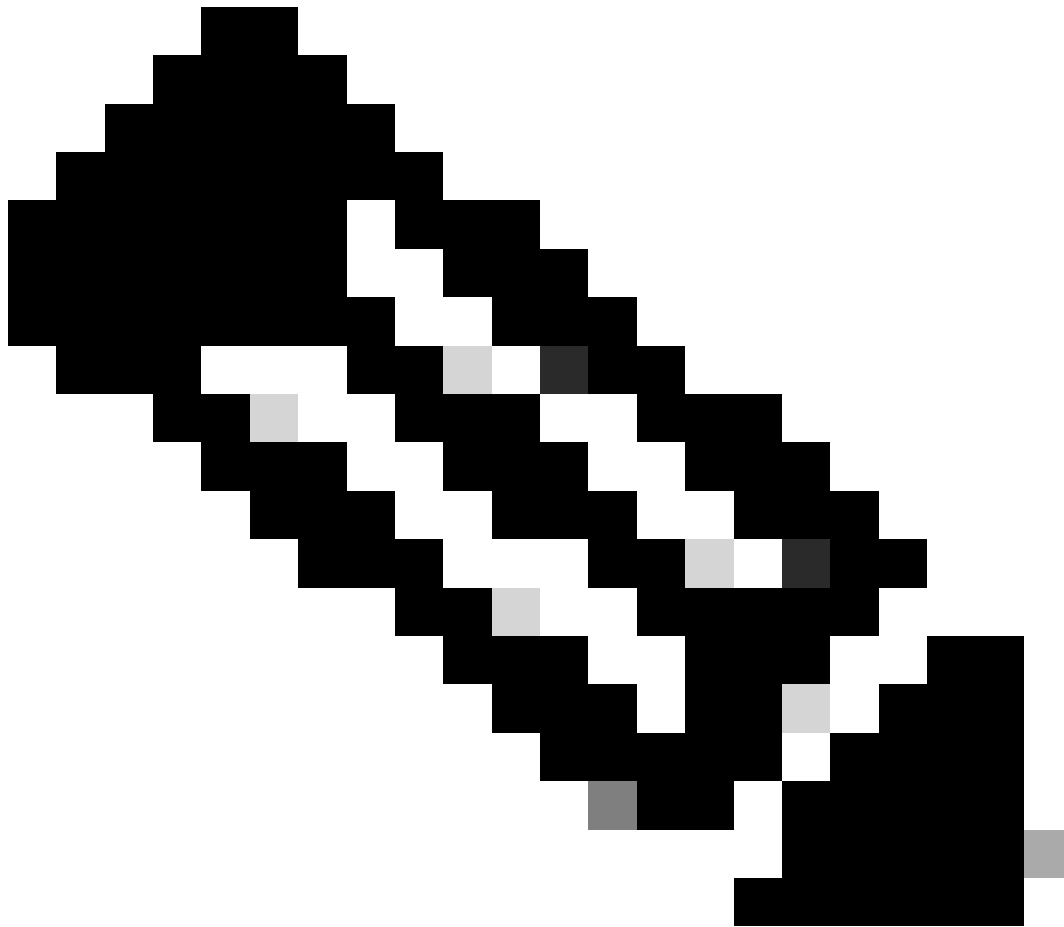


test

Platform Settings Threat Defense

> Report Template

Export



Opmerking: Controleer of het SFO-bestand is gedownload. De download gebeurt automatisch nadat u op exporteren hebt geklikt. Dit bestand bevat het toegangscontrolebeleid, de platforminstellingen, het NAT-beleid en andere beleidslijnen die onmisbaar zijn voor de migratie, aangezien deze niet samen met de apparaatconfiguratie worden geëxporteerd en handmatig naar het FMC van de bestemming moeten worden geüpload.

6. Registreer het FTD-apparaat van het FMC, navigeer naar Apparaten > Apparaatbeheer, klik op de drie verticale punten aan de rechterkant en selecteer verwijderen.

Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ admin 🔒 **SECURE**

View By: Group

All (1) Error (0) Warning (0) Offline (0) Normal (1) Deployment Pending (1) Upgrade (0) Short 3 (1)

Deployment History

Search Device Add

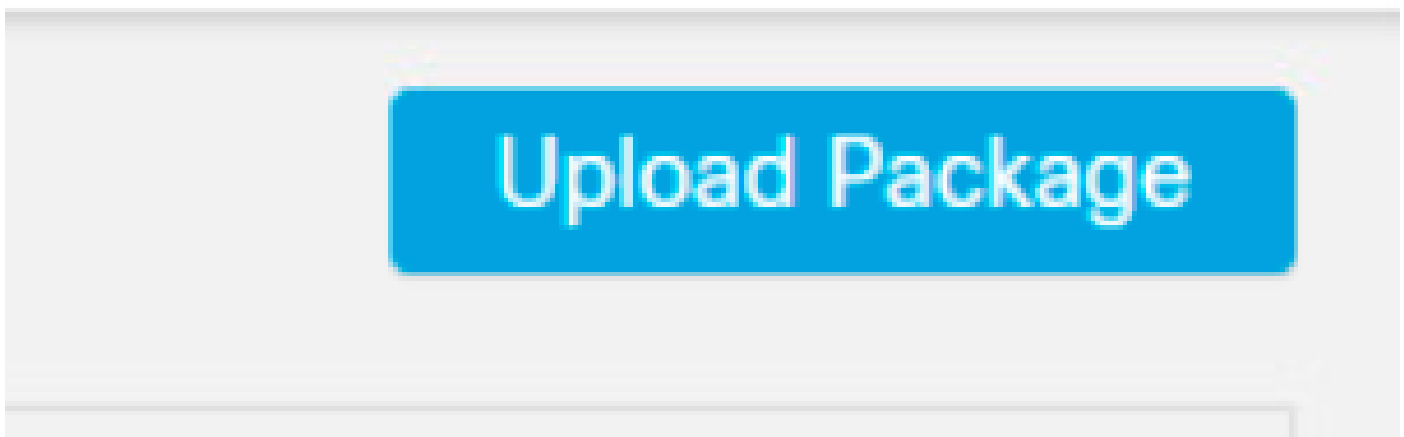
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rollback
FTD1 Short 3 192.168.15.31 - Routed	FTDv for VMware	7.2.5	N/A	Base, Threat (2 more...)	test	

Context Menu:

- Delete
- Packet Tracer
- Packet Capture
- Revert Upgrade
- Health Monitor
- Troubleshoot Files

7. Het VCC van bestemming voorbereiden:

- Log in bij het VCC van bestemming.
- Zorg ervoor dat het VCC klaar is om het nieuwe apparaat te accepteren door het FMC-bronbeleid te importeren dat u in stap 5 hebt gedownload. Navigeer naar **Systeem > Tools > Importeren/Exporteren** en klik op **Uploadpakket**. Upload het bestand dat u wilt importeren en klik op **Upload**.

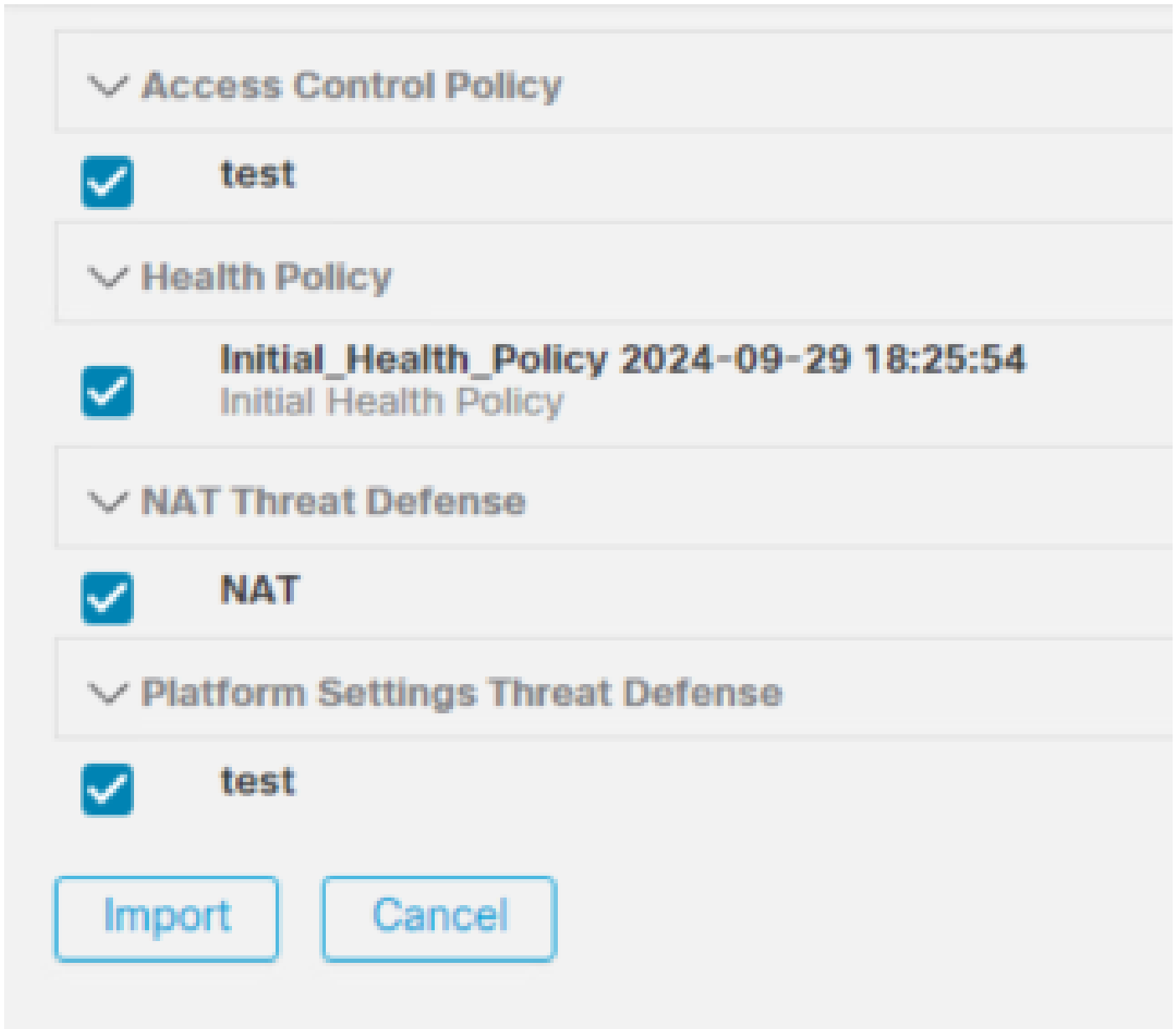


Firewall Management Center
System / Tools / Upload Package

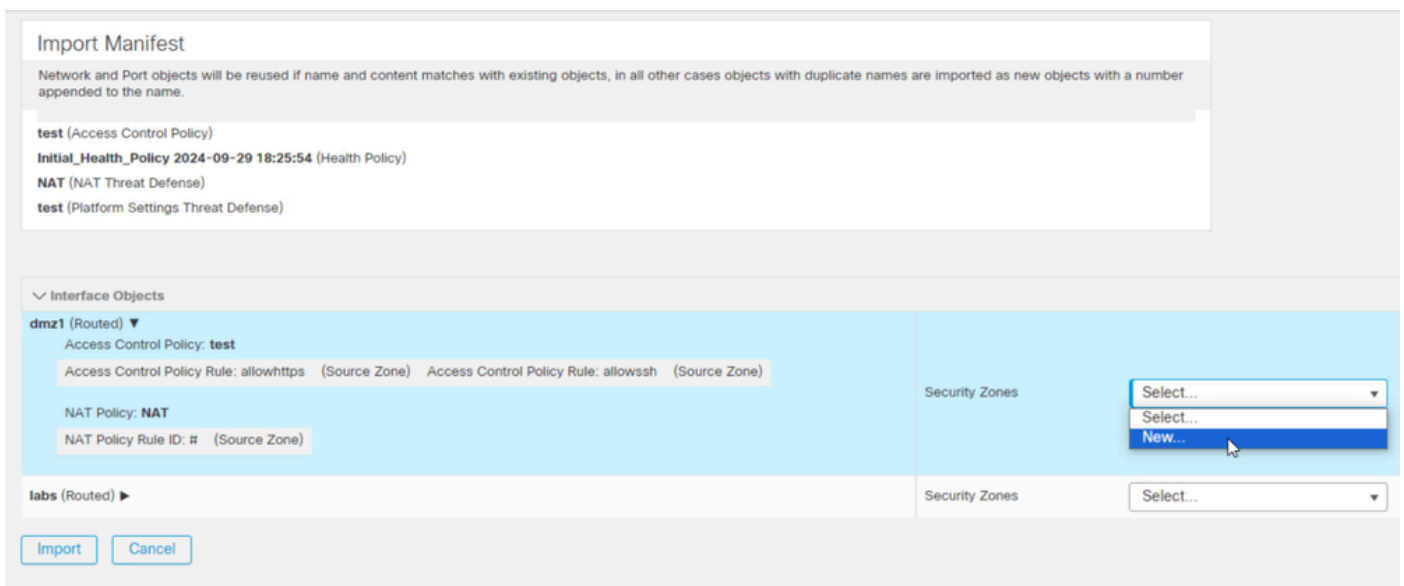
Overview Analysis Policies Devices Objects Integration

Package Name

8. Selecteer het beleid dat in het VCC van bestemming moet worden ingevoerd.

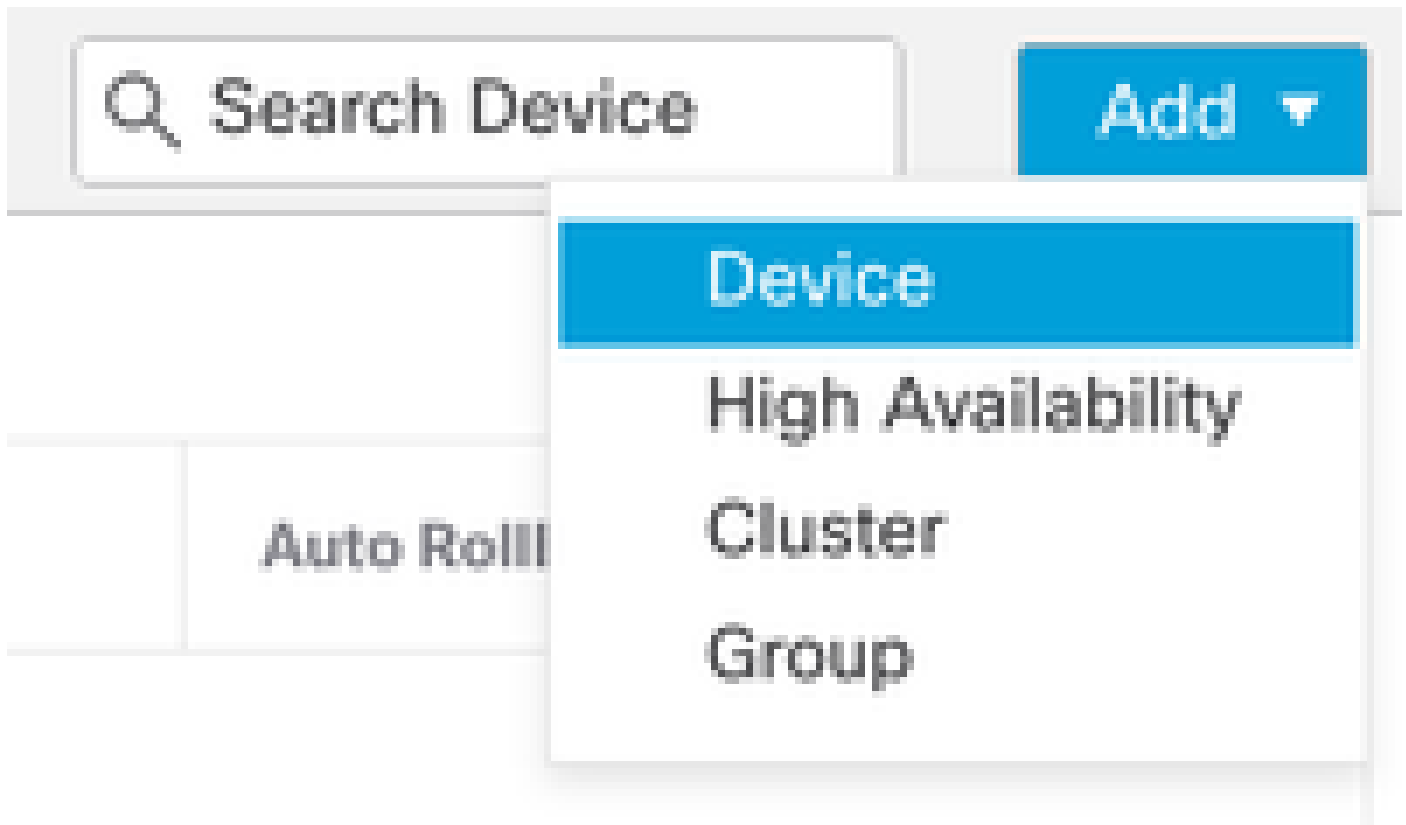


9. Selecteer in het importmanifest een beveiligingszone of maak een nieuwe die u aan het interfaceobject wilt toewijzen en klik op Importeren.



10. Registreer het FTD bij het VCC van bestemming:

- Navigeer in het FMC van de bestemming naar het tabblad Apparaat > Beheer en selecteer Toevoegen > Apparaat.
- Voltooi het registratieproces door op de aanwijzingen te reageren.



Add Device



CDO Managed Device

Host:†

Display Name:

Registration Key:*

Group:

Access Control Policy:*

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click [here](#) for information about the Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

- Malware
- Threat
- URL Filtering

Advanced

Unique NAT ID:†

Transfer Packets

† Either host or NAT ID is required.

Cancel

Register




Raadpleeg de configuratiehandleiding van Firepower Management Center, [voeg apparaten toe aan het Firepower Management Center voor meer informatie](#)

11. Navigeer naar apparaat > Apparaatbeheer > selecteer het FTD > Apparaat en klik op Importeren. Een waarschuwing toont het vragen om uw bevestiging om de apparatenconfiguratie te vervangen, ja klikt.

FTD1

Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

General		  
Name:		FTD1
Transfer Packets:		Yes
Mode:		Routed
Compliance Mode:		None
TLS Crypto Acceleration:		Disabled
Device Configuration:	<input type="button" value="Import"/>	<input type="button" value="Export"/> <input type="button" value="Download"/>

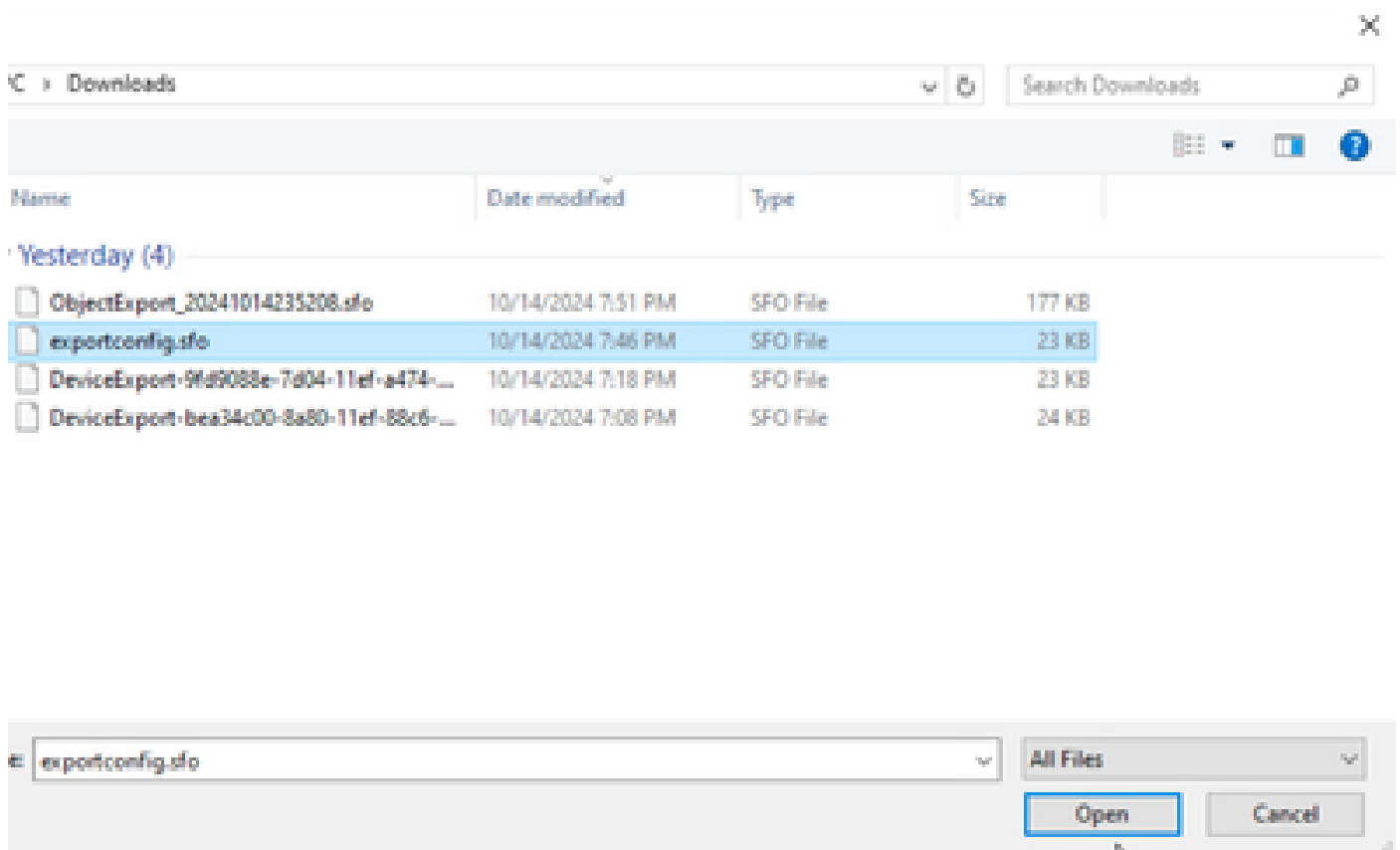
Device Configuration Import

This will replace current device configuration with new configuration from imported file. Do you want to continue?

No

Yes

12. Selecteer het invoerconfiguratiebestand dat de extensie .SFO moet hebben, klik op Upload, en u ziet dat er een bericht verschijnt dat aangeeft dat het importeren is gestart.



File Explorer window showing the Downloads folder. The file list is as follows:

Name	Date modified	Type	Size
Yesterday (4)			
ObjectExport_20241014235208.sfo	10/14/2024 7:51 PM	SFO File	177 KB
exportconfig.sfo	10/14/2024 7:46 PM	SFO File	23 KB
DeviceExport-9fd9088e-7d04-11ef-a474-...	10/14/2024 7:18 PM	SFO File	23 KB
DeviceExport-bea34c00-8a80-11ef-88c6-...	10/14/2024 7:08 PM	SFO File	24 KB

File selection dialog showing the file 'exportconfig.sfo' selected. The file type is set to 'All Files'. The 'Open' button is highlighted.

Device Configuration Import

Device configuration import task initiated. View the progress of task from Tasks view.

OK

Only:

13. Ten slotte wordt er een waarschuwing weergegeven en wordt er automatisch een rapport gegenereerd wanneer de import is voltooid, zodat u de geïmporteerde objecten en beleidsregels kunt bekijken.

The screenshot displays the Cisco Secure interface. At the top, there is a navigation bar with 'Deploy', a search icon, a notification bell with '2', a settings gear, a help icon, and the user 'admin'. The 'Cisco SECURE' logo is on the right. Below the navigation bar, there are tabs for 'Deployments', 'Upgrades', 'Health', and 'Tasks'. The 'Tasks' tab is selected and highlighted. To the right of the tabs is a 'Show Notifications' toggle switch, which is currently turned on. Below the tabs, there is a summary bar showing '20+ total' (highlighted in blue), '0 waiting', '0 running', '0 retrying', '20+ success', and '1 failure'. A search box labeled 'Filter' is also present. The main content area shows a notification for 'Device Configuration Import' with a green checkmark icon. The message reads 'Device configurations imported successfully' and includes a link to 'View Import Report'. The notification has a '6s' timer and a close 'X' button.

Configuration Import Summary

Initiated by:
Initiated at: Tue Oct 15 00:40:18 2024

Policies

Policies imported: 3

Type	Name
PG.PLATFORM.AutomaticApplicationBypassPage	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.AutomaticApplicationBypassPage
PG.PLATFORM.PixInterface	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.PixInterface
PG.PLATFORM.NgfwinlineSetPage	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.NgfwinlineSetPage

Verifiëren

Controleer na de migratie of het FTD-apparaat correct is geregistreerd en functioneert met het FMC van bestemming:

- Controleer de status van het apparaat op het FMC van bestemming.
- Zorg ervoor dat alle beleid en configuraties correct worden toegepast.
- Voer een test uit om te bevestigen dat de voorziening gebruiksklaar is.

Problemen oplossen

Als u tijdens het migratieproces problemen ondervindt, kunt u deze stappen voor probleemoplossing overwegen:

- Controleer de netwerkverbinding tussen het FTD-apparaat en beide FMC's.
- Controleer of de softwareversie op beide VCC's gelijk is.
- Controleer de waarschuwingen op beide VCC's op foutmeldingen of waarschuwingen.

Gerelateerde informatie

- [Beheerdershandleiding voor Cisco Secure Firewall Management Center](#)
- [Firepower Device Registration configureren, controleren en problemen oplossen](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.