

# Problemen met Malware License bij implementatie FTD-beleid oplossen

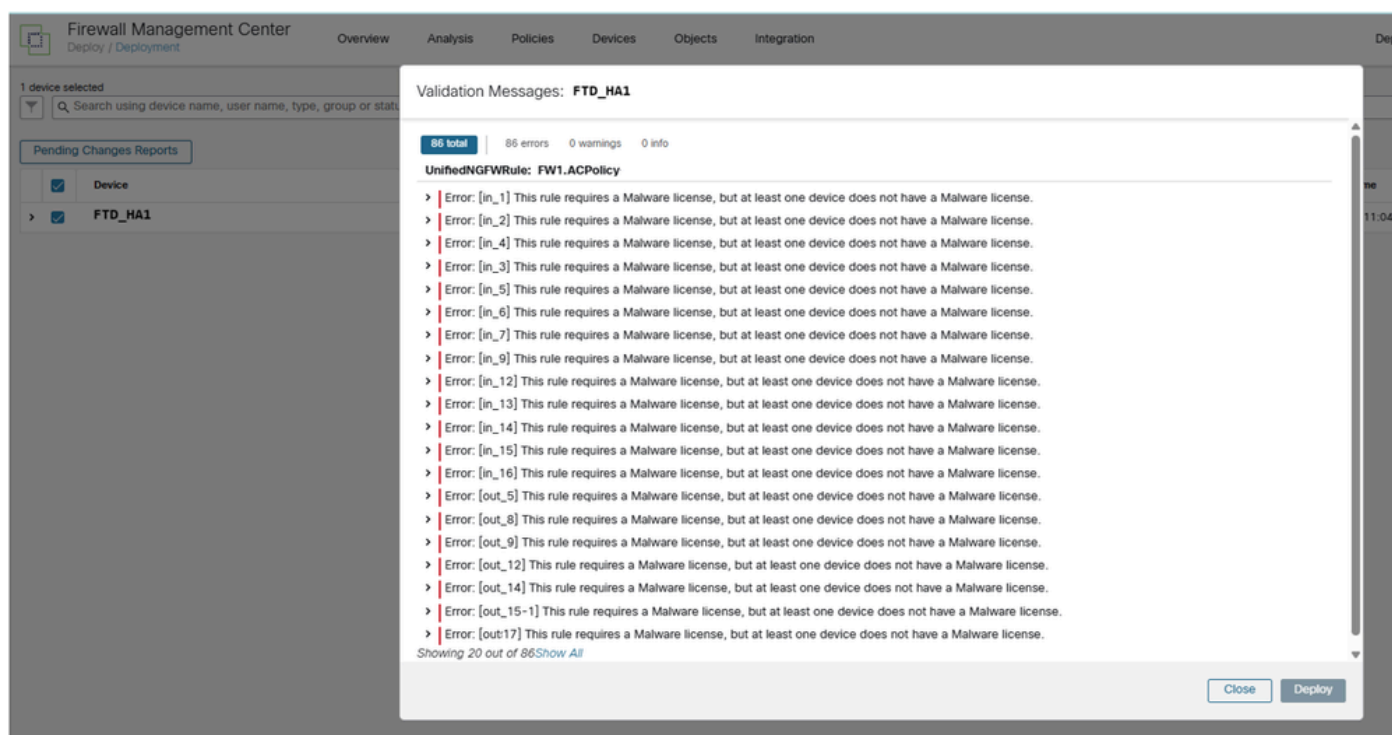
## Inhoud

---

---

## uitgeven

Wanneer u probeert beleidswijzigingen aan te brengen in het Cisco Secure Firewall Management Center (FMC), wordt een foutbericht weergegeven met de melding "Voor deze regel is een Malwarelicentie vereist, maar voor ten minste één apparaat is geen Malwarelicentie vereist". Deze fout voorkomt dat wijzigingen in de beleidsimplementatie en -configuratie worden toegepast op de getroffen firewallapparaten.



## milieu

- VCC 7.4.2. Ook andere software versies zijn hierbij betrokken.

- FPR1140 met Firewall Threat Defense (FTD). Ook andere platformen zijn getroffen.
- FTD maakt gebruik van een Access Control Policy (ACP) met bestandsbeleid ingeschakeld op een of meer regels.

	Name	Action	Source			Destination			Applications	Users	URLs
			Zones	Networks	Ports	Zones	Networks	Ports			
Mandatory 158 rules (1 - 158)											
<input type="checkbox"/>	1 in_1	All...	VPN	Any	Any	Any	Any	Any	Any	Any	
<input type="checkbox"/>	2 in_1.1	Tr...	VPN	Any	Any	Any	DNS_over_TCP +6 more	Any	Any	Any	
<input type="checkbox"/>	3 in_2	All...	VPN	Any	Any	Any	TCP (6):139	Any	Any	Any	
<input type="checkbox"/>	4 in_4	All...	VPN	Any	Any	any-ipv4	1433_SQL +3 more	Any	Any	Any	
<input type="checkbox"/>	5 in_3	All...	VPN	Any	Any	any-ipv4	TCP (6):524	Any	Any	Any	

## resolutie

De oplossing voor deze malwarelicentiefout omvat het verkrijgen en installeren van de benodigde malwarelicentie op het getroffen apparaat. Gebruik deze stappen om het probleem op te lossen:

### Stap 1. Identificeer de licentiekloof

Controleer of op het betreffende firewallapparaat bestandsbeleid is geconfigureerd voor het gebruik van AMP (Advanced Malware Protection), maar de bijbehorende Malware Defense-licentie ontbreekt. Dit kan worden bevestigd door de apparaatconfiguratie te controleren en deze te vergelijken met de beschikbare licenties.

In dit geval heeft alleen het FTD\_HA2-paar de malwarelicentie. Het FTD\_HA1-paar heeft het niet:

Firewall Management Center  
System / Licenses / Smart Licenses

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

### Smart License Status

Cisco Smart Software Manager 🔄

Usage Authorization:	🟢 Authorized (Last Synchronized On Mar 16 2026)
Product Registration:	🟢 Registered (Last Renewed On Oct 01 2025)
Assigned Virtual Account:	██████████
Export-Controlled Features:	Enabled

### Smart Licenses

Filter Devices... [X] Edit Performance Tier Edit Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
> Essentials (4)	🟢 In-Compliance			
▼ Malware Defense (2)	🟢 In-Compliance			
> FTD_HA2 (2) Cisco Firepower 1150 Threat Defense Threat Defense High Availability	🟢 In-Compliance	High Availability - Cisco Firepower 1150 Threat Defens	Global	N/A
> IPS (4)	🟢 In-Compliance			
> URL (2)	🟢 In-Compliance			
Carrier (0)				
> Secure Client Premier (2)	🟢 In-Compliance			
Secure Client Advantage (0)				

FTD\_HA1-firewallpaar heeft Malwarelicentie ingesteld op Nee:

Firewall Management Center  
Devices / High Availability

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

### FTD\_HA1

Cisco Firepower 1140 Threat Defense

Summary High Availability Device Interfaces Inline Sets Routing DHCP VTEP SNMP

General	License
Name: FTD_HA1	Essentials: Yes
Transfer Packets: Yes	Export-Controlled Features: Yes
Status: 🟢	<b>Malware Defense: No</b>
Primary Peer: FP1(Active)	IPS: Yes
Secondary Peer: FP2(Standby)	Carrier: No
Fallover History: 🔍	URL: No
Troubleshoot: 📄 🗑️	Secure Client Premier: No
Onboarding Method: Registration Key	Secure Client Advantage: No
	Secure Client VPN Only: No
Security Engine	Applied Policies
Intrusion Prevention Engine: Snort 3.0	Access Control Policy: ACPolicy
Revert to Snort 2	Prefilter Policy: Default Prefilter Policy
	SSL Policy:
	DNS Policy:
	Identity Policy:

## Stap 2. Verkrijgen van de vereiste licentie

Werk samen met uw Cisco-vertegenwoordiger of geautoriseerde partner om de benodigde Malware-licentie voor het betreffende apparaat te verkrijgen. De licentie moet geschikt zijn voor uw specifieke firewallmodel en implementatievereisten.

### Stap 3. De Malware-licentie installeren

Zodra de licentie is verkregen, installeert u deze op het betreffende apparaat via het standaard Cisco-licentieproces. Dit omvat meestal het toepassen van de licentie via de FMC of rechtstreeks op het apparaat, afhankelijk van uw beheerconfiguratie.

### Stap 4. Licentie-installatie controleren

Controleer na de installatie van de licentie of de Malware Defence-functie nu correct is ingeschakeld en of de licentiefout is gewist.

### Stap 5. Implementatie van testbeleid

Probeer uw beleidswijzigingen opnieuw te implementeren om te bevestigen dat het licentieprobleem is opgelost en dat beleidsbewerkingen normaal kunnen worden uitgevoerd.

## Oorzaak

De fout treedt op als gevolg van een fout in de licentievalidatie waarbij het bestandsbeleid is geconfigureerd om AMP-functionaliteit te gebruiken, maar de bijbehorende Malware Defense-licentie niet is geïnstalleerd of geactiveerd op het betreffende firewallapparaat. De FMC zorgt ervoor dat de licenties worden nageleefd en voorkomt beleidsimplementatie wanneer de vereiste licenties ontbreken, zelfs als het beleid technisch is geconfigureerd.

Deze validatie zorgt ervoor dat alleen de juiste gelicentieerde functies worden geïmplementeerd op apparaten, waarbij de naleving van de licentievereisten van Cisco wordt gehandhaafd en het gebruik van niet-gelicentieerde mogelijkheden wordt voorkomen.

## Verwante inhoud

- [Cisco Technical Support en downloads](#)

## 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.