

# Dépannage des erreurs de licence de programme malveillant dans le déploiement de la stratégie FTD

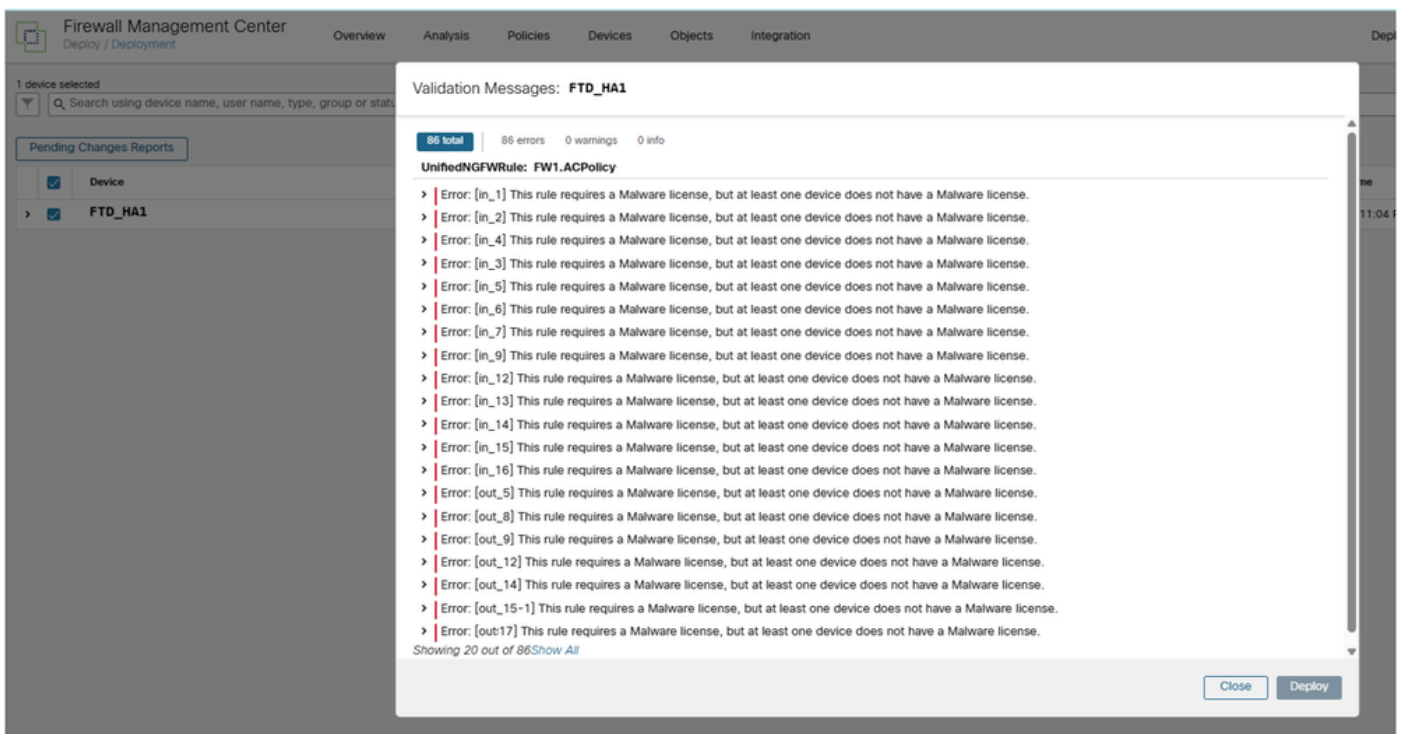
## Table des matières

---

---

## Problème

Lorsque vous tentez d'apporter des modifications à la stratégie dans Cisco Secure Firewall Management Center (FMC), un message d'erreur apparaît indiquant que « Cette règle nécessite une licence de programme malveillant, mais qu'au moins un périphérique ne dispose pas d'une licence de programme malveillant ». Cette erreur empêche le déploiement des stratégies et les modifications de configuration d'être appliqués aux périphériques pare-feu affectés.



## Environnement

- FMC 7.4.2. D'autres versions logicielles sont également affectées.
- FPR1140 exécutant Firewall Threat Defense (FTD). D'autres plates-formes sont également concernées.
- FTD utilise une politique de contrôle d'accès (ACP) avec une politique de fichiers activée sur une ou plusieurs règles.

	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	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	

## Résolution

La résolution de cette erreur de licence de programme malveillant implique l'obtention et l'installation de la licence de programme malveillant nécessaire sur le périphérique affecté. Suivez ces étapes pour résoudre le problème :

### Étape 1 : identification des lacunes en matière de licences

Vérifiez que le périphérique pare-feu affecté dispose de stratégies de fichiers configurées pour utiliser Advanced Malware Protection (AMP), mais qu'il ne dispose pas de la licence Malware Defense correspondante. Vous pouvez le confirmer en vérifiant la configuration du périphérique et en la comparant aux licences disponibles.

Dans ce cas, seule la paire FTD\_HA2 possède la licence du programme malveillant. La paire FTD\_HA1 ne l'a pas :

Firewall Management Center  
System / Licenses / Smart Licenses

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin 🔒 cisco 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... | 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)				

La licence de programme malveillant de la paire de pare-feu FTD\_HA1 est définie sur Non :

Firewall Management Center  
Devices / High Availability

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ 👤 admin 🔒 cisco 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
<a href="#">Revert to Snort 2</a>	Prefilter Policy: Default Prefilter Policy
	SSL Policy:
	DNS Policy:
	Identity Policy:

## Étape 2. Obtention de la licence requise

Contactez votre représentant commercial Cisco ou votre partenaire agréé pour obtenir la licence Malware nécessaire pour le périphérique concerné. La licence doit être adaptée à votre modèle de pare-feu et à vos exigences de déploiement.

## Étape 3. Installation de la licence de programme malveillant

Une fois la licence obtenue, installez-la sur le périphérique concerné via le processus de licence Cisco standard. Cela implique généralement l'application de la licence via le FMC ou directement sur le périphérique, en fonction de votre configuration de gestion.

## Étape 4 : vérification de l'installation de la licence

Après l'installation de la licence, vérifiez que la fonction Malware Defense est maintenant correctement activée et que l'erreur de licence a été effacée.

## Étape 5. Test du déploiement des stratégies

Essayez à nouveau de déployer vos modifications de stratégie pour confirmer que le problème de licence a été résolu et que les opérations de stratégie peuvent se poursuivre normalement.

## Motif

L'erreur se produit en raison d'une non-correspondance de validation de licence où les stratégies de fichiers sont configurées pour utiliser la fonctionnalité AMP, mais la licence Malware Defense correspondante n'est pas installée ou activée sur le périphérique pare-feu affecté. Le FMC applique la conformité des licences et empêche le déploiement des stratégies lorsque les licences requises sont manquantes, même si les stratégies sont configurées techniquement.

Cette validation garantit que seules les fonctionnalités correctement concédées sous licence sont déployées sur les périphériques, ce qui garantit la conformité aux exigences de licence de Cisco et empêche l'utilisation de fonctionnalités non concédées sous licence.

## Autres informations utiles

- [Assistance technique de Cisco et téléchargements](#)

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.