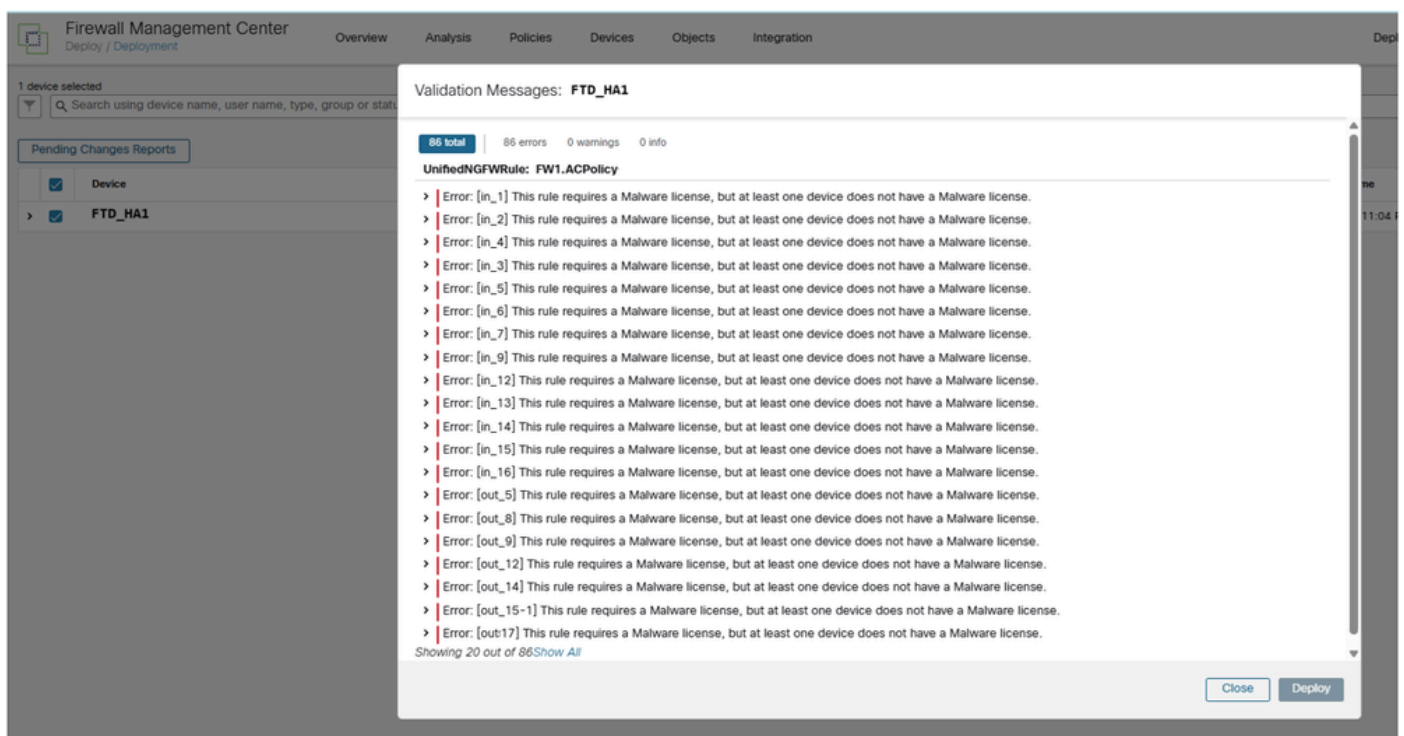


Troubleshoot Malware License Error in FTD Policy Deployment

Contents

Issue

When attempting to make policy changes in Cisco Secure Firewall Management Center (FMC), an error message appears indicating that "This rule requires a Malware license, but at least one device does not have a Malware license". This error prevents policy deployment and configuration changes from being applied to the affected firewall devices.



Environment

- FMC 7.4.2. Other software versions are also affected.
- FPR1140 running Firewall Threat Defense (FTD). Other platforms are also affected.
- FTD uses an Access Control Policy (ACP) with file policy enabled on one or more rules.

	Name	Action	Source			Destination			Applications	Users	URLs
			Zones	Networks	Ports	Zones	Networks	Ports			
1	in_1	All...	VPN	Any	Any	Any	Any	Any	Any	Any	
2	in_1.1	Tr...	VPN	Any	Any	Any	DNS_over_TCP +6 more	Any	Any	Any	
3	in_2	All...	VPN	Any	Any	Any	TCP (6):139	Any	Any	Any	
4	in_4	All...	VPN	Any	Any	any-ipv4	1433_SQL +3 more	Any	Any	Any	
5	in_3	All...	VPN	Any	Any	any-ipv4	TCP (6):524	Any	Any	Any	

Resolution

The resolution for this malware license error involves obtaining and installing the necessary Malware license on the affected device. Use these steps to resolve the issue:

Step 1. Identify the Licensing Gap

Verify that the affected firewall device has file policies configured to use Advanced Malware Protection (AMP) but lacks the corresponding Malware Defense license. This can be confirmed by checking the device configuration and comparing it against the available licenses.

In this case, only the FTD_HA2 pair has the malware license. The FTD_HA1 pair does not have it:

The screenshot shows the 'Smart License Status' section with the following details:

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

Below is the 'Smart Licenses' table:

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 firewall pair has Malware license set to No:

The screenshot shows the configuration page for 'FTD_HA1' (Cisco Firepower 1140 Threat Defense). The 'License' section is highlighted with an orange box, showing the following settings:

- Essentials: Yes
- Export-Controlled Features: Yes
- Malware Defense: No** (highlighted with an orange box)
- IPS: Yes
- Carrier: No
- URL: No
- Secure Client Premier: No
- Secure Client Advantage: No
- Secure Client VPN Only: No

The 'Security Engine' section shows 'Intrusion Prevention Engine: Snort 3.0'.

Step 2. Obtain the Required License

Work with your Cisco sales representative or authorized partner to obtain the necessary Malware license for the affected device. The license must be appropriate for your specific firewall model and deployment requirements.

Step 3. Install the Malware License

Once the license is obtained, install it on the affected device through the standard Cisco licensing process. This typically involves applying the license through the FMC or directly on the device, depending on your management configuration.

Step 4. Verify License Installation

After license installation, verify that the Malware Defense capability is now properly enabled and that the licensing error has been cleared.

Step 5. Test Policy Deployment

Attempt to deploy your policy changes again to confirm that the licensing issue has been resolved and that policy operations can proceed normally.

Cause

The error occurs due to a licensing validation mismatch where file policies are configured to use AMP functionality, but the corresponding Malware Defense license is not installed or activated on the affected firewall device. The FMC enforces license compliance and prevents policy deployment when required licenses are missing, even if the policies are technically configured.

This validation ensures that only properly licensed features are deployed to devices, maintaining compliance with Cisco's licensing requirements and preventing the use of unlicensed capabilities.

Related Content

- [Cisco Technical Support & Downloads](#)