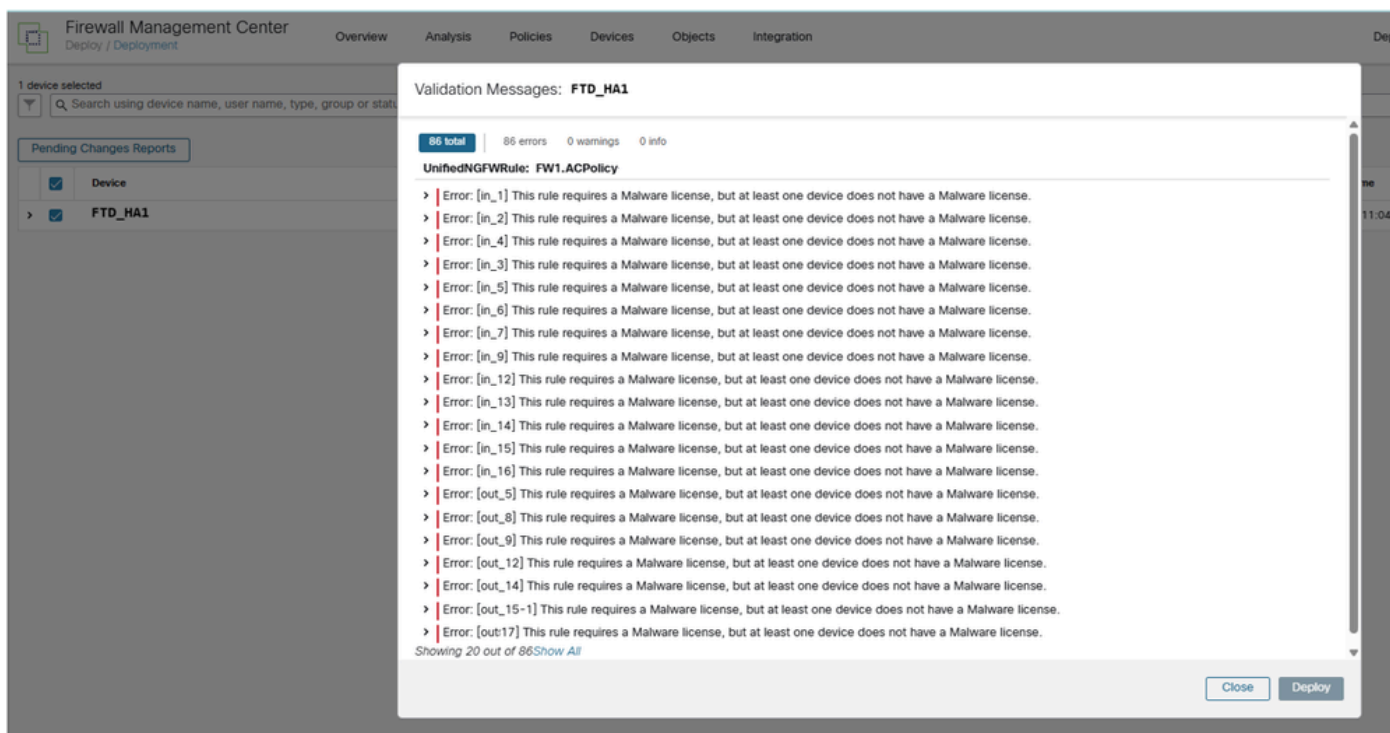


Solucionar Problemas de Erro de Licença de Malware na Implantação de Política de FTD

Contents

Problema

Ao tentar fazer alterações de política no Cisco Secure Firewall Management Center (FMC), uma mensagem de erro será exibida indicando que "Esta regra requer uma licença de malware, mas pelo menos um dispositivo não tem uma licença de malware". Esse erro impede que a implantação de política e as alterações de configuração sejam aplicadas aos dispositivos de firewall afetados.



Ambiente

- FMC 7.4.2. Outras versões de software também são afetadas.

- FPR1140 executando Firewall Threat Defense (FTD). Outras plataformas também são afetadas.
- O FTD usa uma ACP (Access Control Policy, política de controle de acesso) com a política de arquivos habilitada em uma ou mais regras.

	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	

Resolução

A resolução desse erro de licença de malware envolve a obtenção e instalação da licença de malware necessária no dispositivo afetado. Siga estas etapas para resolver o problema:

Etapa 1. Identificar a lacuna de licenciamento

Verifique se o dispositivo de firewall afetado tem políticas de arquivo configuradas para usar a Proteção avançada contra malware (AMP), mas não tem a licença correspondente da Defesa contra malware. Isso pode ser confirmado verificando a configuração do dispositivo e comparando-a com as licenças disponíveis.

Nesse caso, somente o par FTD_HA2 tem a licença de malware. O par FTD_HA1 não tem:

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... ✕ 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)				

O par de firewalls FTD_HA1 tem a licença de malware definida como Não:

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: 🟢	Malware Defense: 🚫
Primary Peer: FP1(Active)	IPS: Yes
Secondary Peer: FP2(Standby)	Carrier: No
Falover 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:

Etapa 2. Obter a Licença Necessária

Trabalhe com seu representante de vendas ou parceiro autorizado da Cisco para obter a licença de malware necessária para o dispositivo afetado. A licença deve ser apropriada para seu modelo de firewall específico e para seus requisitos de implantação.

Etapa 3. Instalar a licença de malware

Uma vez obtida a licença, instale-a no dispositivo afetado por meio do processo de licenciamento padrão da Cisco. Isso normalmente envolve a aplicação da licença através do FMC ou diretamente no dispositivo, dependendo da sua configuração de gerenciamento.

Etapa 4. Verificar a instalação da licença

Após a instalação da licença, verifique se o recurso Malware Defense está habilitado corretamente e se o erro de licenciamento foi apagado.

Etapa 5. Implantação da política de teste

Tente implantar as alterações de política novamente para confirmar se o problema de licenciamento foi resolvido e se as operações de política podem continuar normalmente.

Causa

O erro ocorre devido a uma incompatibilidade de validação de licenciamento em que as políticas de arquivo são configuradas para usar a funcionalidade AMP, mas a licença de defesa contra malware correspondente não está instalada ou ativada no dispositivo de firewall afetado. O FMC garante a conformidade com as licenças e evita a implantação de políticas quando faltam as licenças necessárias, mesmo que as políticas estejam tecnicamente configuradas.

Essa validação garante que somente os recursos devidamente licenciados sejam implantados nos dispositivos, mantendo a conformidade com os requisitos de licenciamento da Cisco e evitando o uso de recursos não licenciados.

Conteúdo relacionado

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.