对安全防火墙智能许可违规错误进行故障排除

目录

简介

背景信息

如何识别导致Out of Compliance状态的许可证类型。

- 使用FMC图形用户界面(GUI)。
- 使用智能帐户门户
- 使用FMC命令行界面(CLI)

故障排除

简介

本文档介绍最常见的思科智能许可违反思科FMC和FTD型号的合规性原因。

背景信息

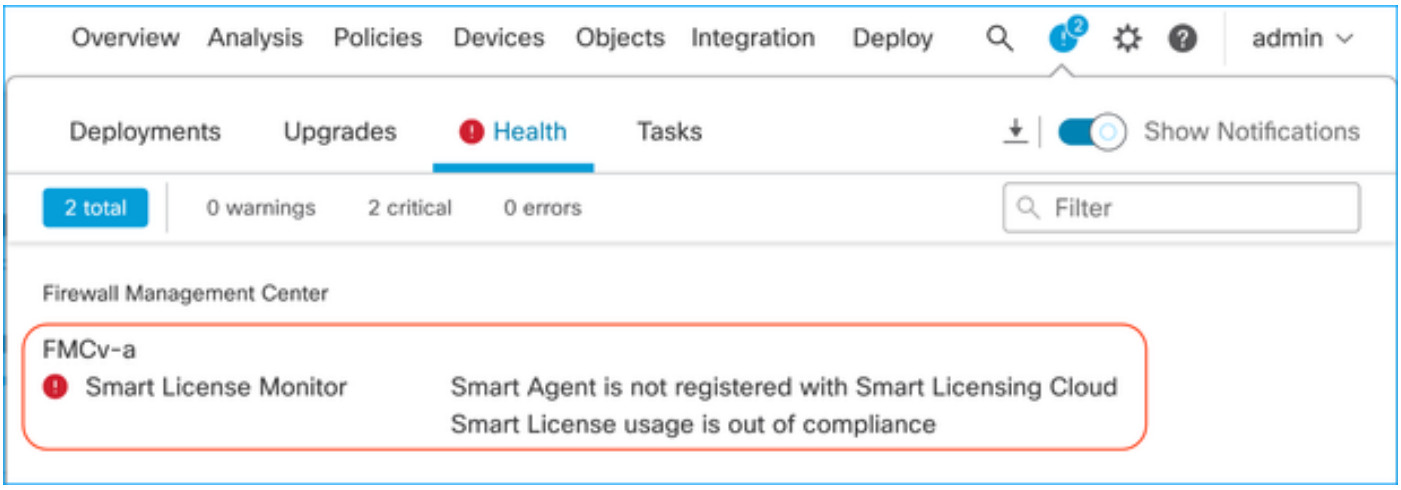
思科智能许可为许多产品提供集中式许可证管理。思科安全防火墙可简化潜在大型传感器部署中的许可证管理，并且可用于设备、虚拟和公共云模型。本文档提供针对思科防火墙管理中心(FMC)和思科防火墙威胁防御(FTD)软件和设备型号的智能许可证不合规问题的故障排除指南。

当FMC报告智能许可证不合规，表明FMC无法在智能帐户中找到适当的许可证。发生这种情况时，将显示运行状况警报。这可能是因为本文档中概述的若干原因。

如何识别导致Out of Compliance状态的许可证类型。

使用FMC图形用户界面(GUI)。

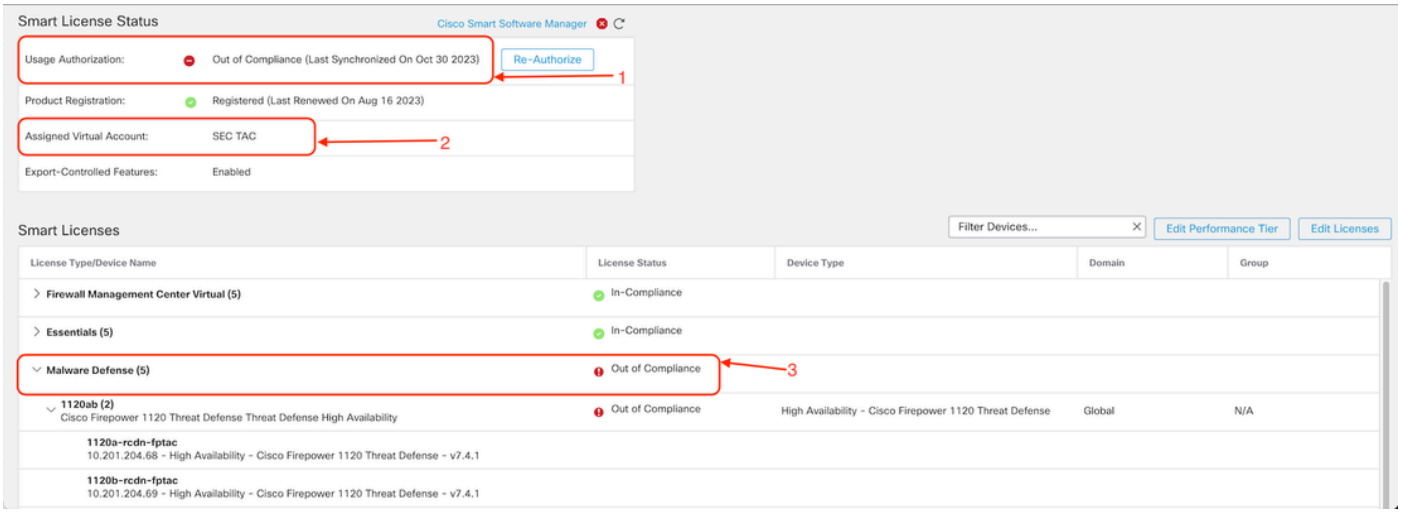
从FMC通知图标导航到运行状况警报，然后点击运行状况(Health)。



使用智能帐户门户

导航至智能许可证状态，位于系统>>许可证>>智能许可证。 在此处可以找到FMC注册的虚拟帐户信息。

在“智能许可证”(Smart Licenses)部分中，此处指出了不符合合规性的特定许可证。在本示例中，思科安全防火墙1120功能许可证“恶意软件防御”列出了“不合规”状态。注意所有列为“Out of Compliance”（不合规）的功能和产品（以红色标出）。绿色的“合规性”复选标记表示特定许可证类型可用，FMC可以从智能帐户获取该许可证。



要验证这些许可证的可用性，您可以登录智能帐户门户并导航到智能帐户>>资产>> [虚拟帐户名称]。根据需要过滤许可证名称。

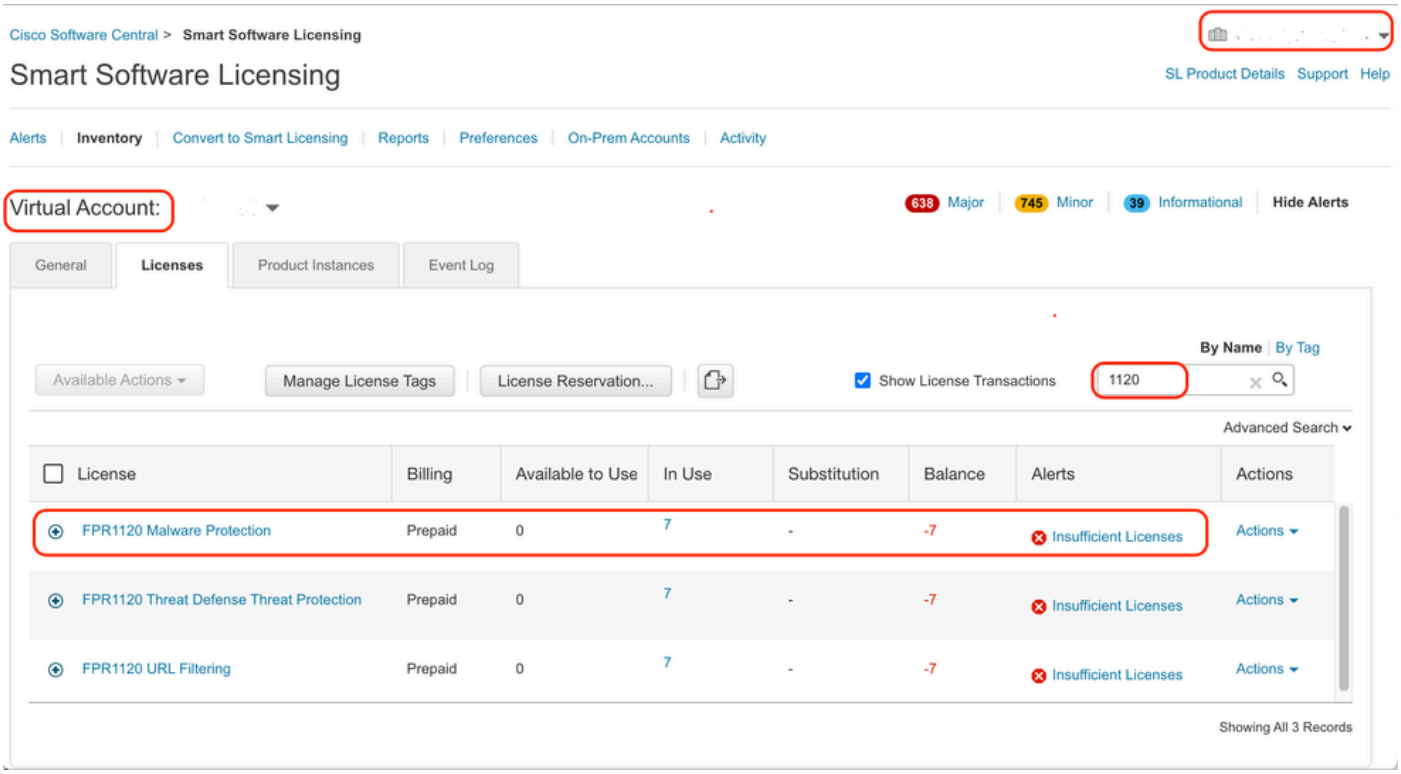
请注意以下可能状态：

可用数量=购买数量

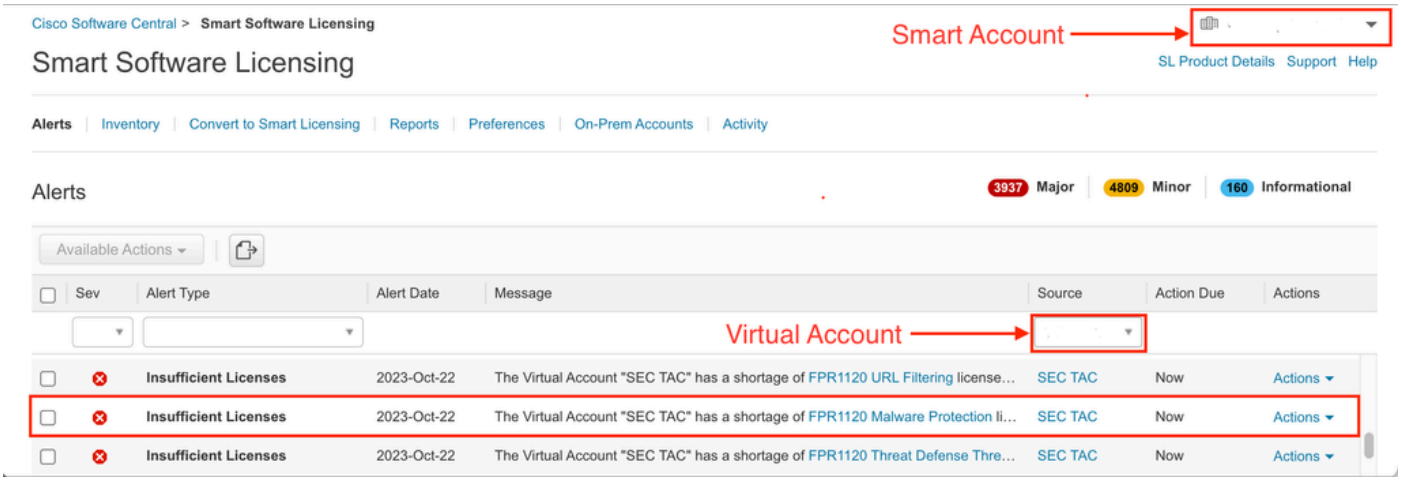
使用中=启用此功能的设备计数

余额=购买与使用之间的差额。

当余额为负时，FMC将显示该功能/产品的“不合规”状态。



此外，还可以在智能帐户>>警报中找到警报。如果需要，在“源”中过滤虚拟帐户。



使用FMC命令行界面(CLI)

步骤1:登录FMC CLI。

第二步：使用此命令访问Linux shell

```
expert
```

第三步：发出此命令。

```
less /var/log/sam.log
```

向下滚动以检查最新状态，导航至文件的最新条目。

```
Smart Licensing Tech Support info

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account:
  Virtual Account:
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Aug 16 2023 12:04:50 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Feb 12 2024 12:04:49 UTC
  Registration Expires: Aug 15 2024 11:59:51 UTC

License Authorization:
  Status: OUT OF COMPLIANCE on Sep 22 2023 15:43:12 UTC
  Last Communication Attempt: SUCCEEDED on Oct 29 2023 19:37:27 UTC
  Next Communication Attempt: Oct 30 2023 07:37:27 UTC
  Communication Deadline: Jan 27 2024 19:32:26 UTC

Export Authorization Key:
  Features Authorized:
    <none>
```

如果许可证已充分获得，则许可证将显示为AUTHORIZED。

```
License Usage
=============
Handle: 2
  License: FTDv Malware 5 Gbps
  Entitlement Tag: regid.2020-10.com.cisco.FTDv-AMP-5G,1.0_ab50f0b8-caca-45d5-bad4-41c820b0dcd5
  Description: Cisco Firepower Threat Defense Virtual Malware License, 5 Gbps
  Count: 2
  Version: 1.0
  Status: AUTHORIZED(3)
  Status time: Oct 28 2023 07:37:23 UTC
  Request Time: Oct 24 2023 19:14:13 UTC
  Export status: NOT RESTRICTED
  Soft Enforced: True
```

如果许可证不可用，则特定许可证类型显示为OUT OF COMPLIANCE。

```
Handle: 9
  License: FPR1120 Malware Protection
  Entitlement Tag: regid.2015-02.com.cisco.FPR1120TD-AMP,1.0_375e2617-5d67-4892-961b-f4aa79f31d8d
  Description: FPR1120 Malware Protection
  Count: 2
  Version: 1.0
  Status: OUT OF COMPLIANCE(4)
  Status time: Oct 02 2023 18:00:17 UTC
  Request Time: Oct 02 2023 17:59:45 UTC
  Export status: NOT RESTRICTED
  Soft Enforced: True
```

故障排除

下面是一些最常见的场景，以及如何进行故障排除。

场景1 — 没有足够的许可证用于FTD物理平台的特定功能。

有不同的许可证类型。这些可分为硬件和功能特定两类。可以根据许可证名称中显示的模型，以及许可证提供的功能，来标识许可证。

— 基础（7.x之前的版本）或基础（7.x之后的版本）

— 恶意软件防御

-IPS

-URL

— 运营商

— 安全客户端Premier

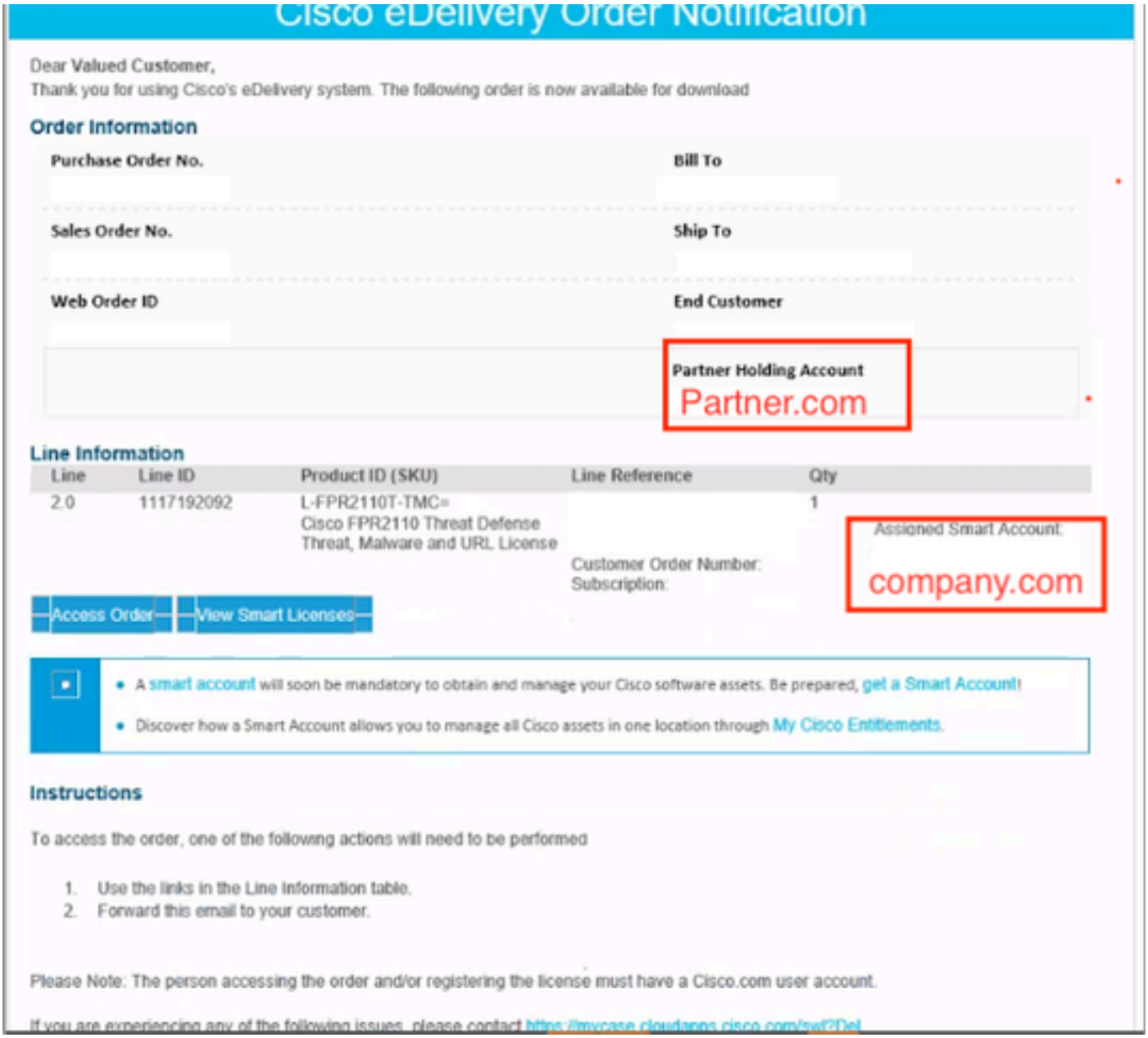
— 安全客户端优势

— 仅安全客户端VPN

如果您怀疑许可证是购买的，并且在您的智能帐户中不可用，请验证您的订单信息，并检查下单时提供的智能许可证帐户。

如果在下采购订单时提供了分配的智能帐户，则许可证将转移到“分配的智能帐户”。

如果未提供分配的智能帐户，且订单通过合作伙伴下达，则许可证将转移到合作伙伴暂持帐户。如果出现这种情况，请与您的思科合作伙伴公司联系，并提供采购订单，他们可帮助将这些许可证转移到您的智能帐户。



场景2 — 许可证在其他虚拟帐户中可用

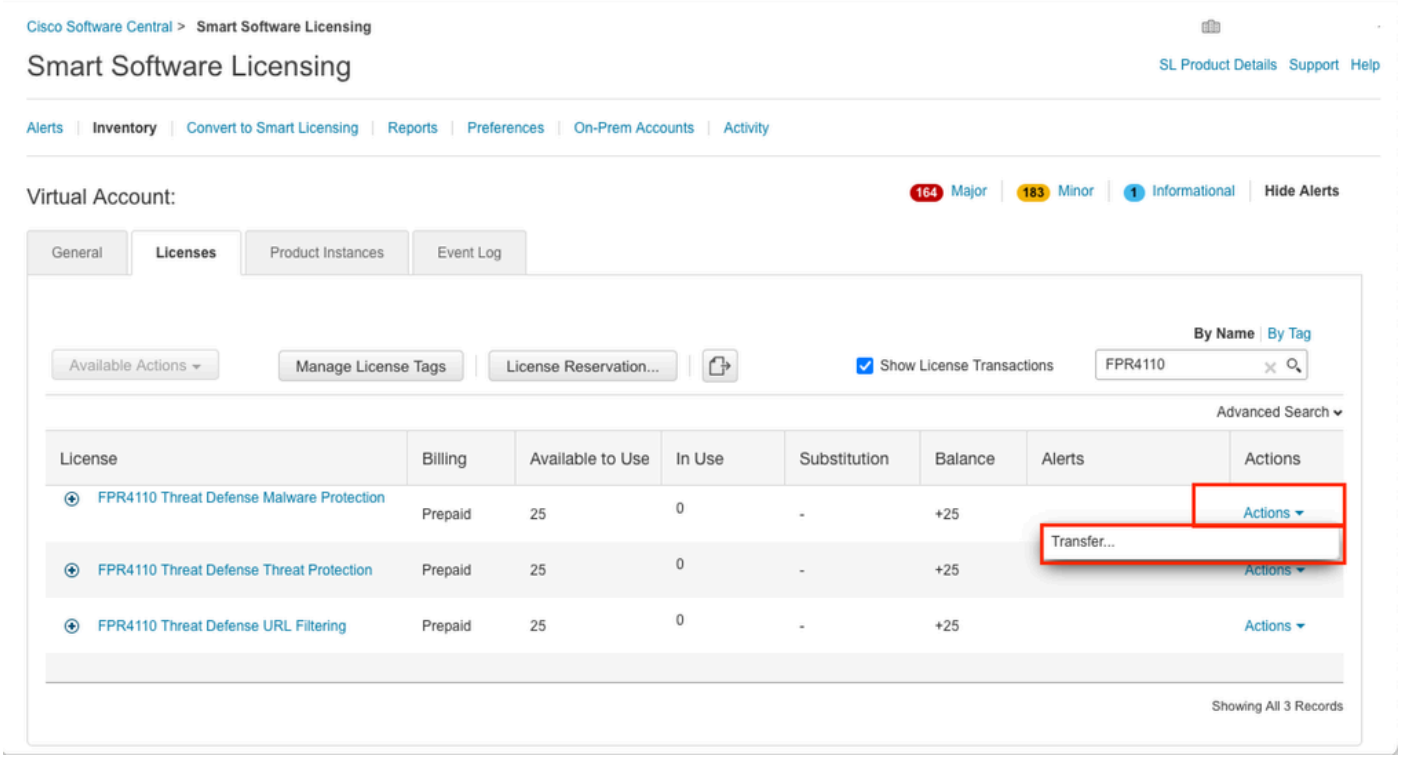
默认情况下，每个智能帐户中只有一个名为DEFAULT的虚拟帐户。智能帐户管理员可以创建多个虚拟帐户，以便于管理和其他用途。

如果所需的许可证属于不同的虚拟帐户，可以使用以下步骤将这些许可证转移到正确的虚拟帐户。

步骤1:导航到智能帐户>>资产。

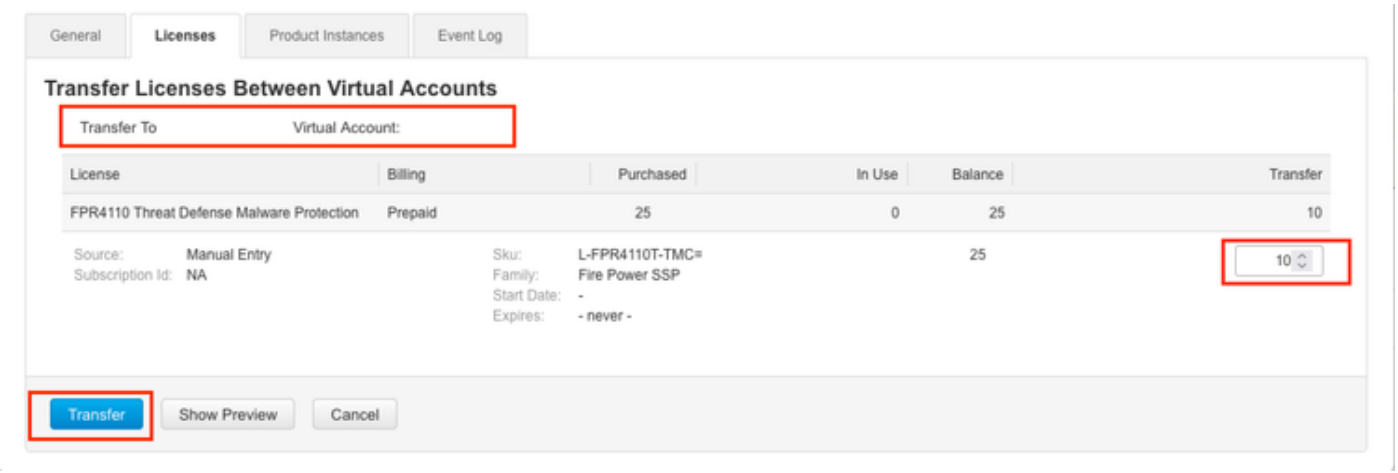
第二步：过滤正确的虚拟帐户。 根据需要过滤许可证。

第三步： 确定正确的许可证后，单击Actions下拉列表，然后选择Transfer。



第四步：选择需要许可证的目标虚拟帐户，并提供大量要传输的许可证。

第五步：单击Show Preview进行验证，然后单击Transfer。



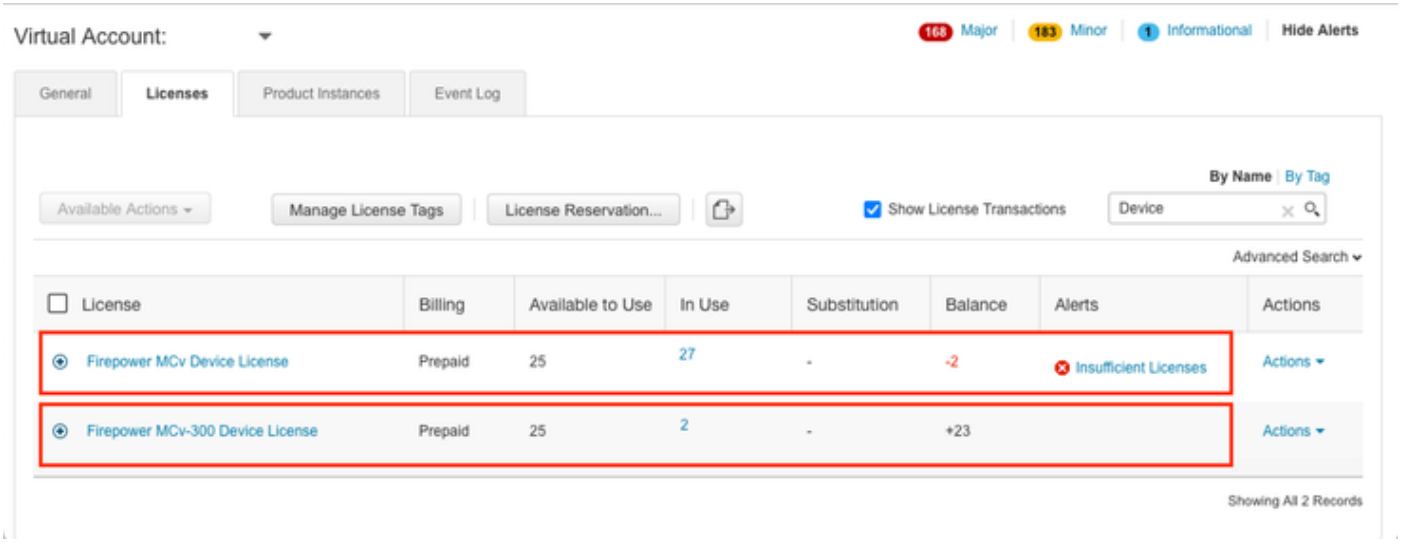
在FMC注册到的虚拟帐户中提供所有许可证后，点击FMC上的Re-Authorize按钮以清除“不合规”状态。

场景3 — 缺少Firepower MCv设备许可证

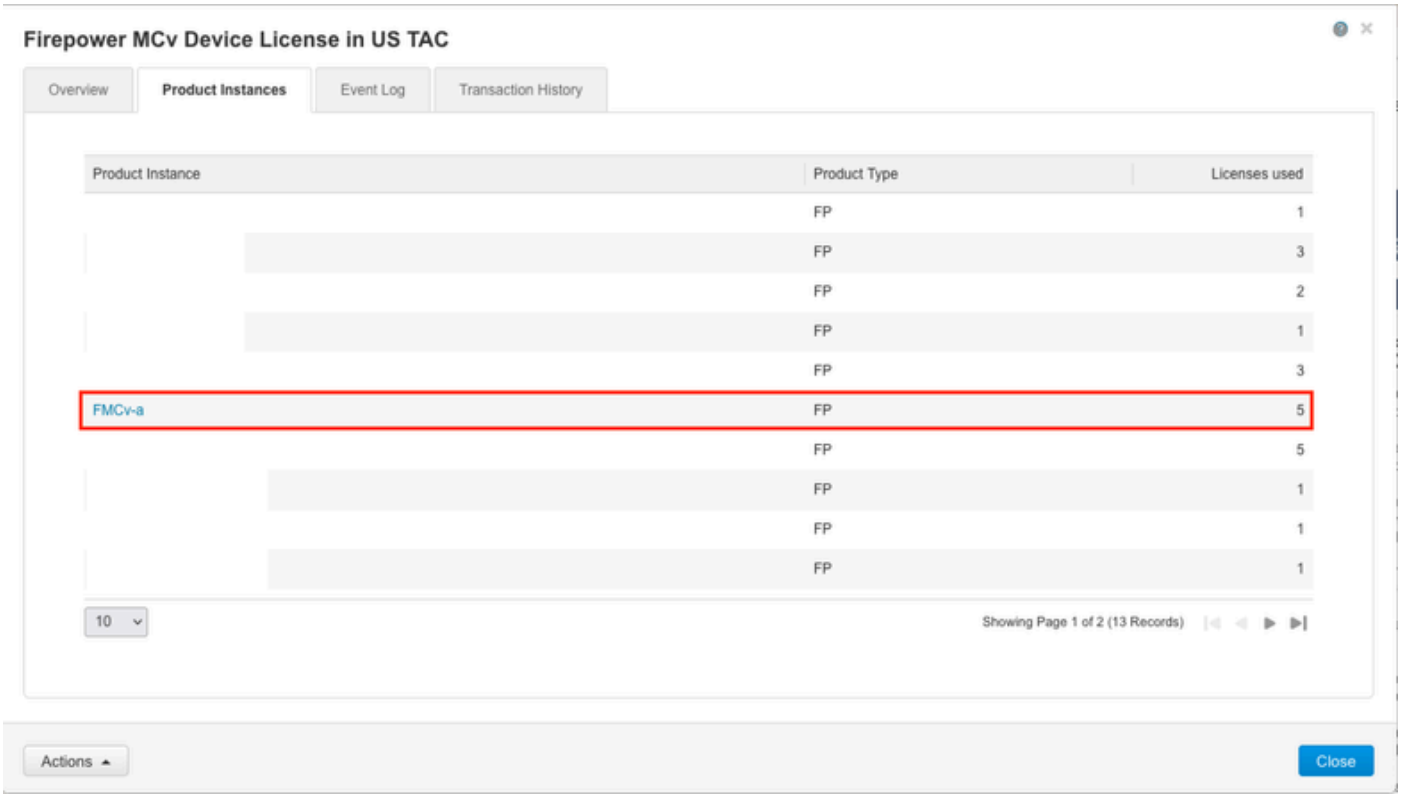
对于虚拟管理模型，通常混用两个不同的平台。

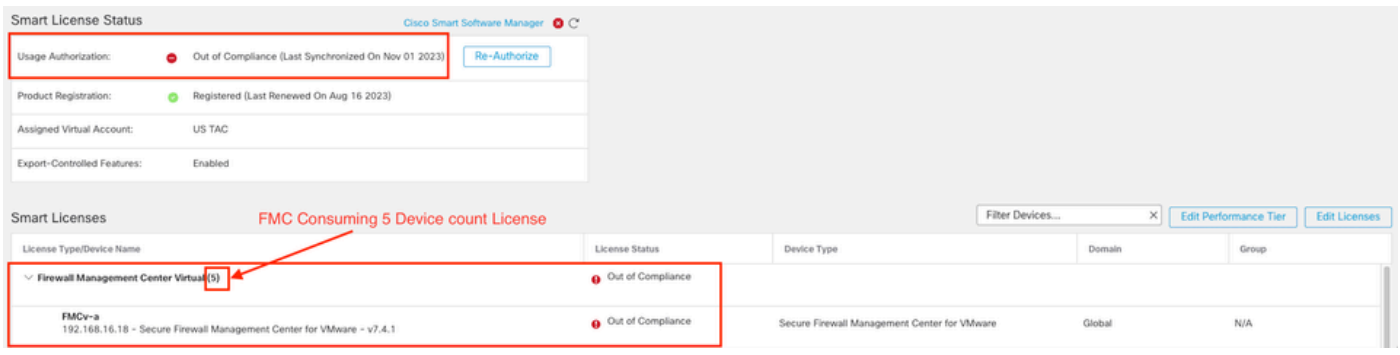
FMCv设备许可证显示为Firepower MCv设备许可证，而FMCv300设备许可证显示为Firepower MCv300设备许可证。

要管理防火墙，FMC还需要设备许可证。



点击License type（许可证类型）有助于确定哪些正在使用这些许可证的FMC。在本示例中，FMCv-a占用五个许可证，这些许可证与FMC智能许可证页面匹配。





场景4 - FTD是运行7.0之前版本的虚拟平台

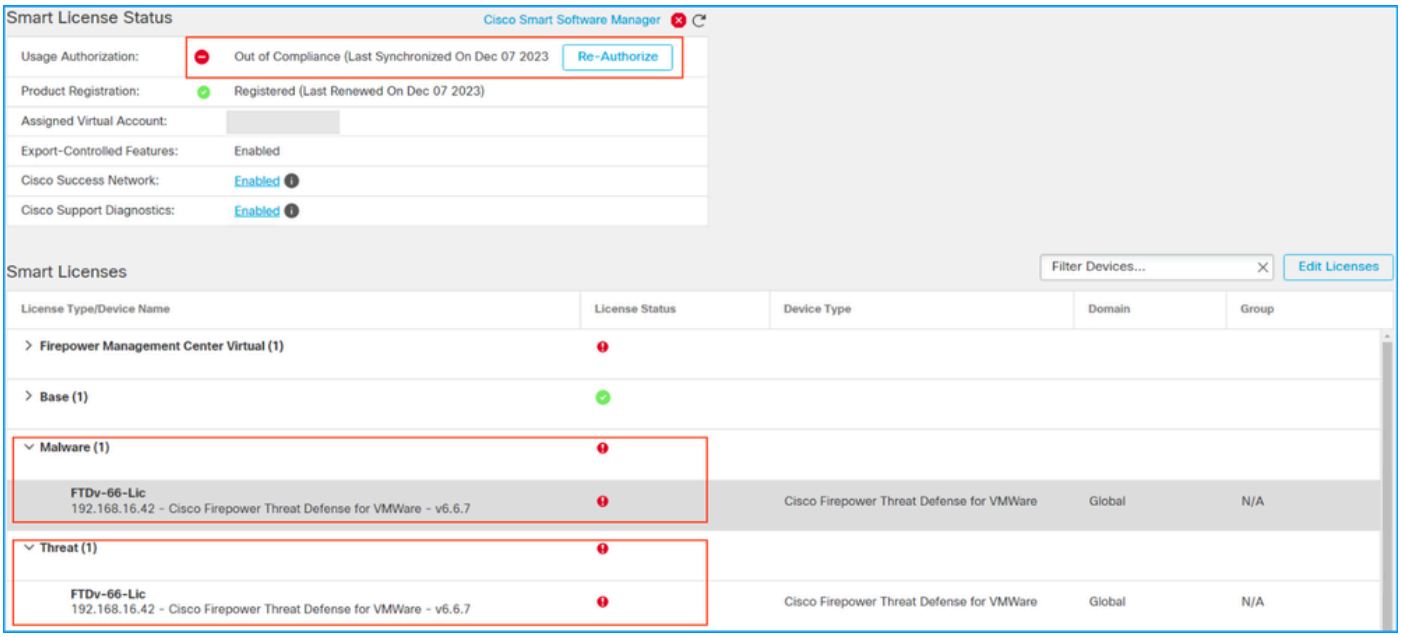
基本许可证将自动请求且不分层。有关7.x以前的FTDv库存单位(SKU)，请参阅思科网络安全订购指南中的表60和表61。

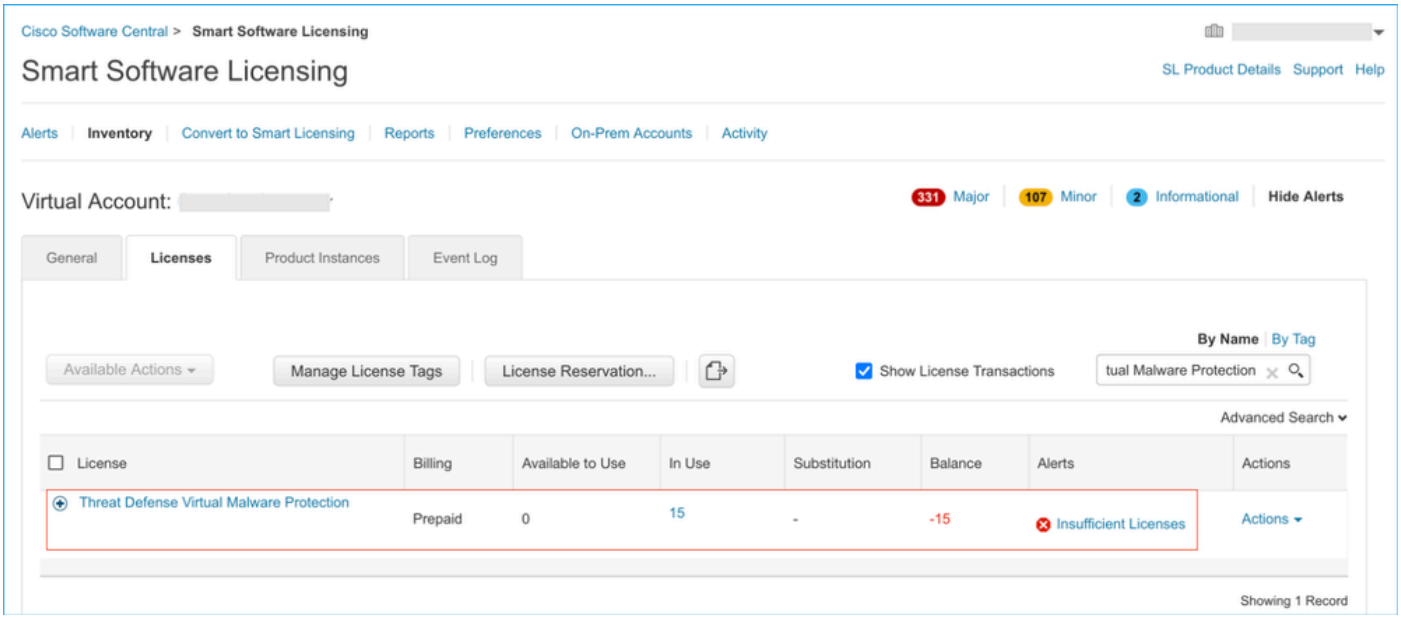
这些是智能帐户中的7.x之前FTDv许可证名称。

威胁防御虚拟恶意软件防护
威胁防御虚拟URL过滤
Firepower MCv设备许可证
Firepower威胁防御基础功能
威胁防御虚拟威胁防护
Cisco AnyConnect Plus许可证
Cisco AnyConnect Apex许可证
仅Cisco AnyConnect VPN许可证

在本示例中，由于虚拟帐户没有足够的许可证，恶意软件和威胁许可证不符合要求。

要获得许可证合规性，用户必须确保智能许可虚拟帐户具有足够的可用许可证。有关7.x之前的FTDv SKU，请参阅思科网络安全订购指南。

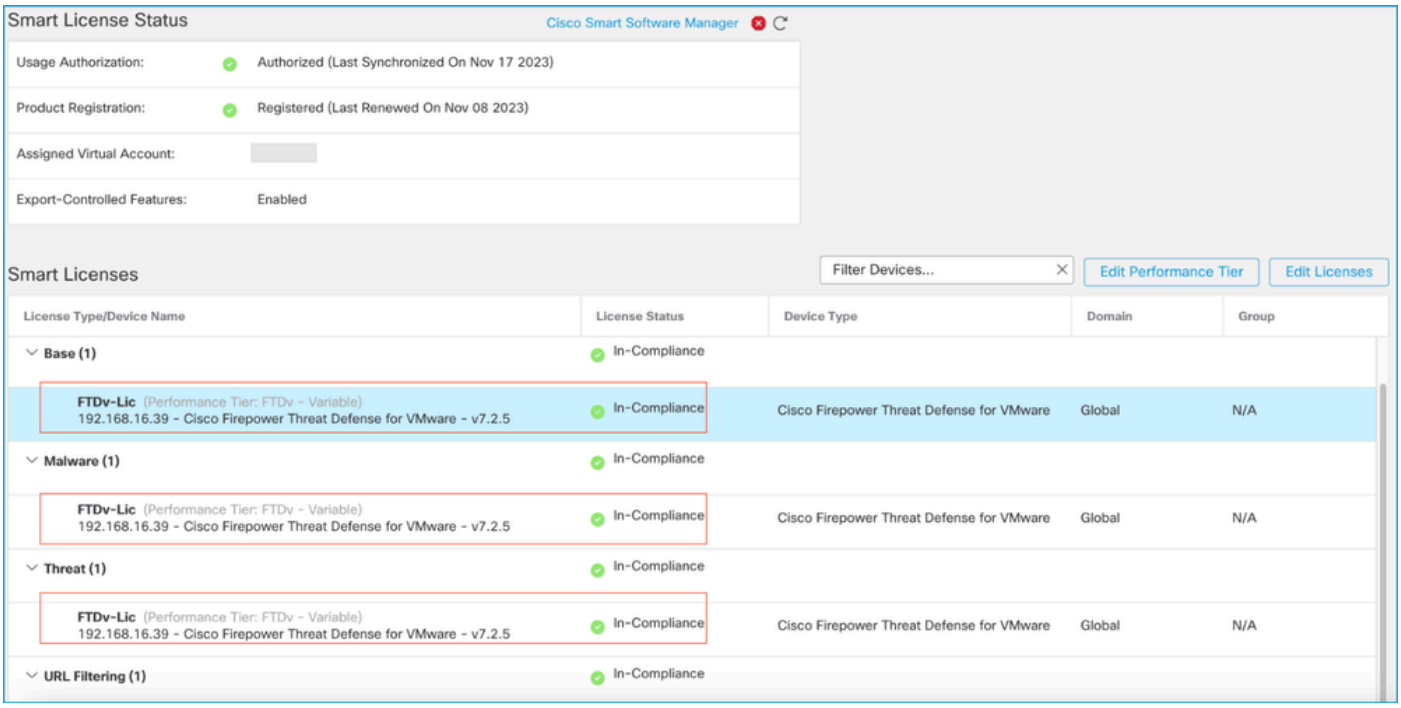




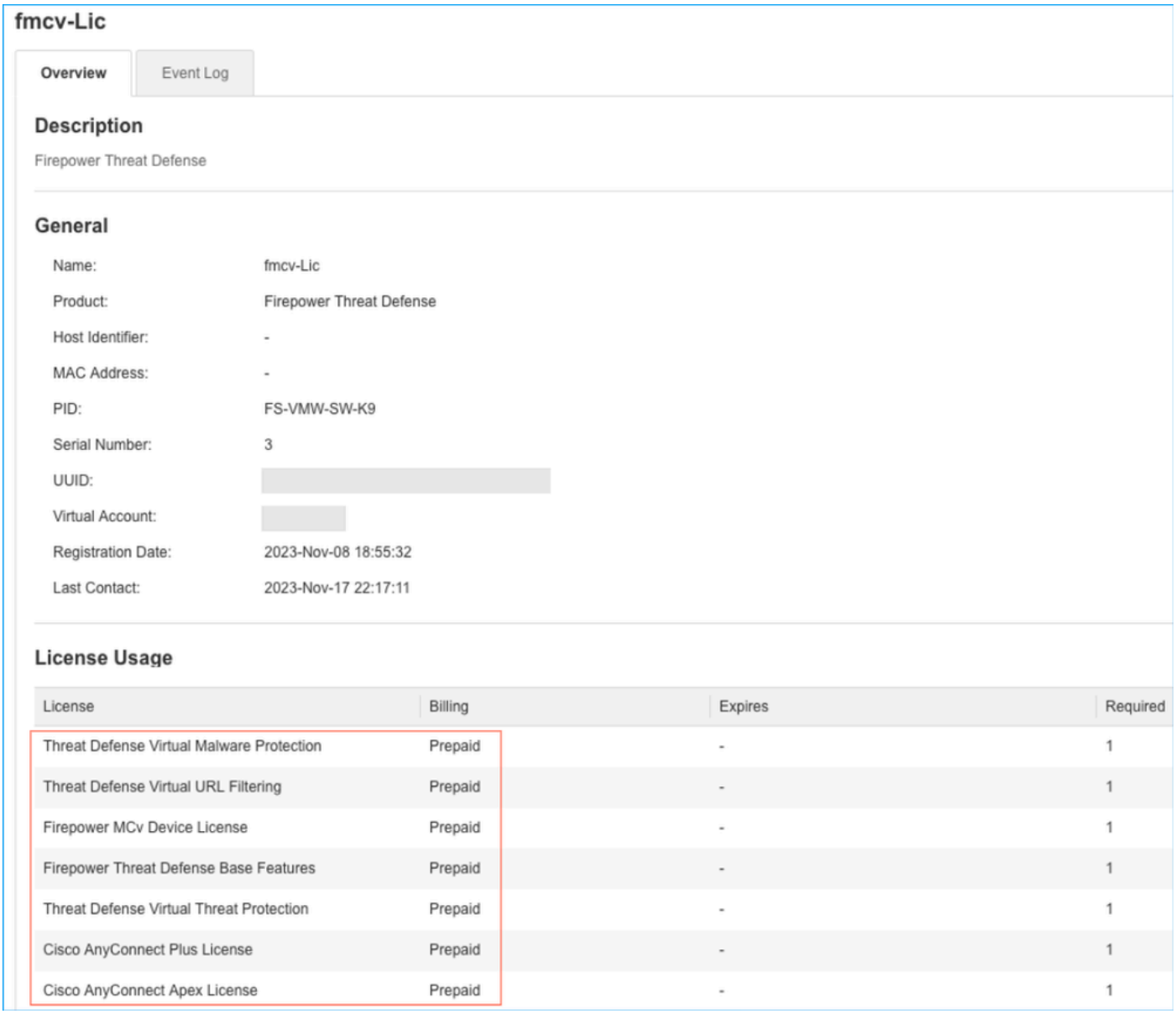
场景5 - FTD是运行7.0版或更高版本的虚拟平台

基本许可证基于订用，并映射到层。虚拟帐户必须具有FTDvs和威胁、恶意软件和URL过滤的基本许可证授权。

当FTDv升级到版本7.0或更高版本时，设备会自动移动到FTDv — 变量层，并使用非分层授权。在本例中，FTD从6.6.7升级到7.2.5，智能许可证状态显示已授权和不合规。

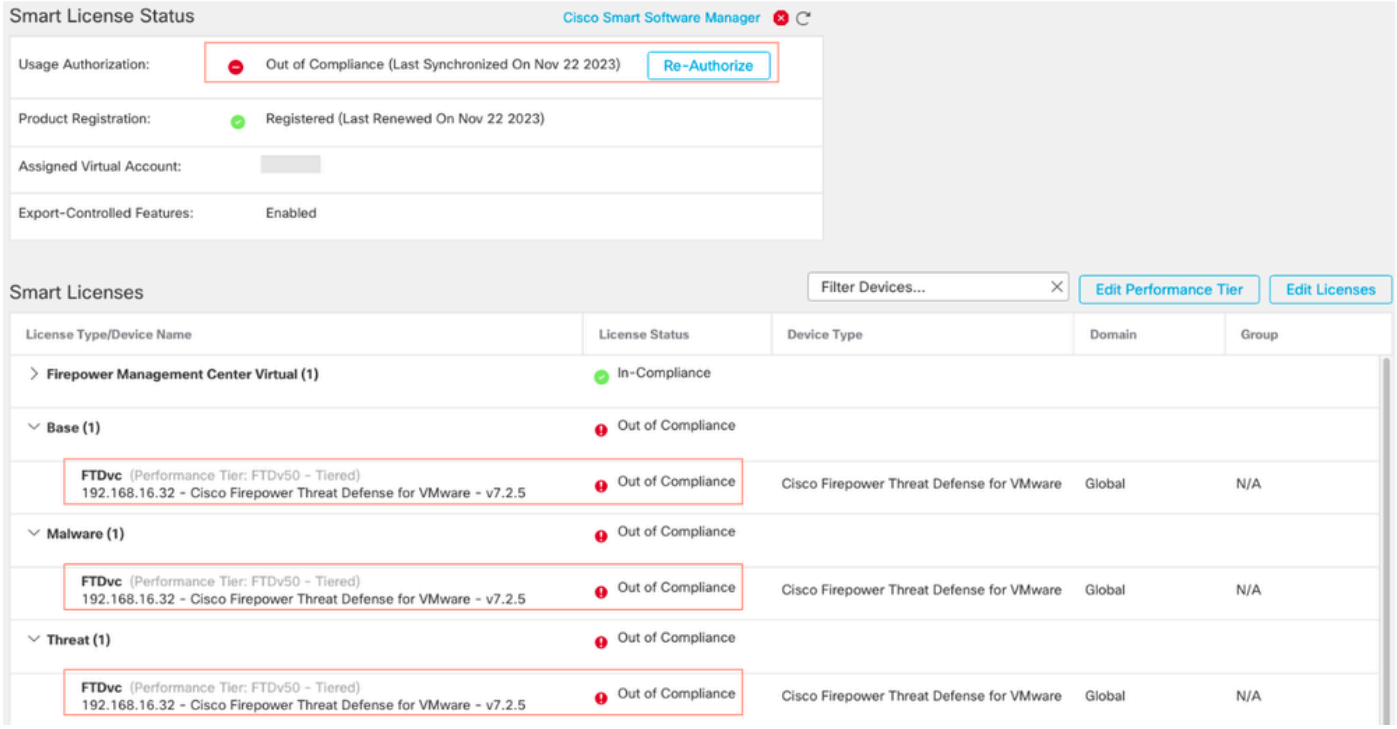


它继续使用非分层授权。

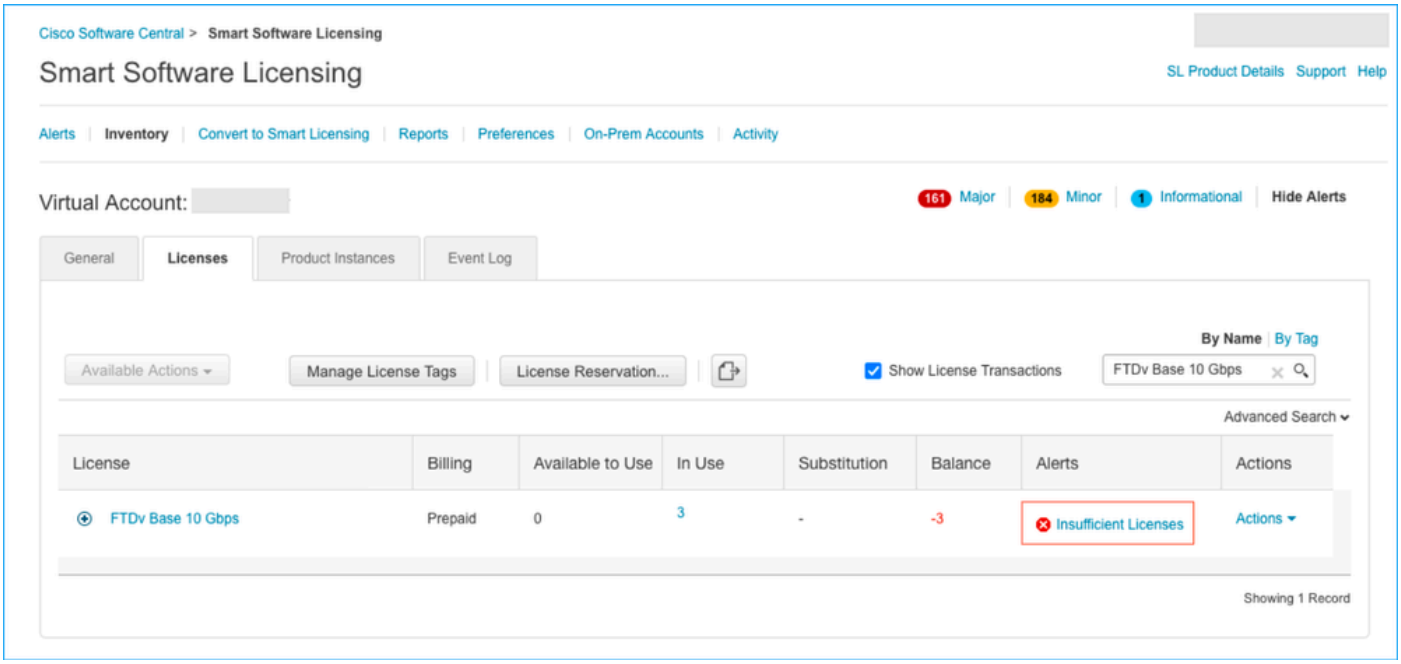


如果用户选择（或默认为自动分配的）没有授权的Performance Tier，则会显示Out of Compliance状态。

在本示例中，用户选择性能层FTDv50，注册虚拟帐户中没有基本恶意软件和威胁许可证。



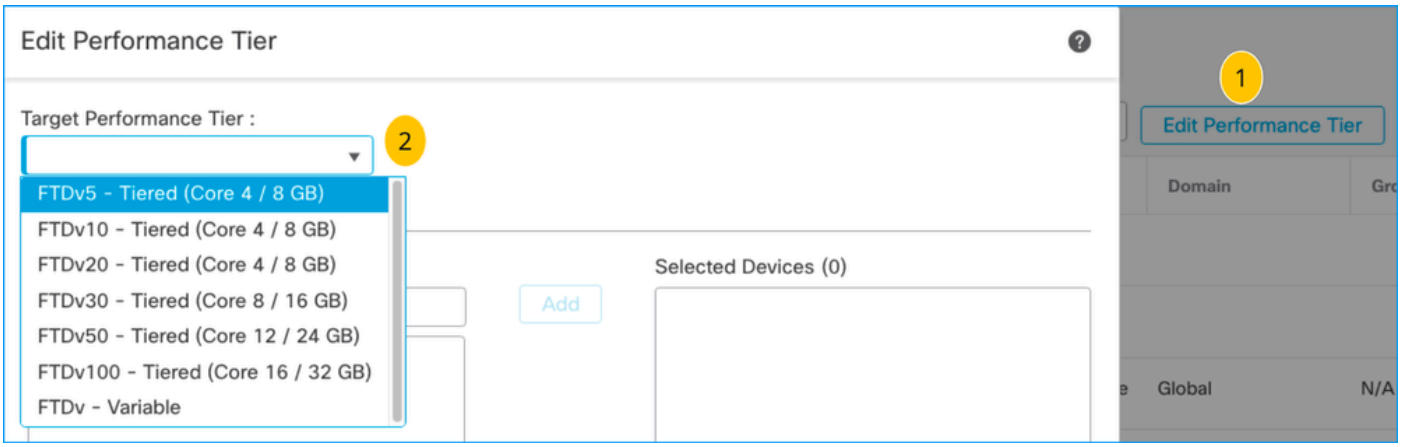
虚拟帐户必须为请求的性能层显示更多许可证/授权。



为符合要求，用户必须在其虚拟智能许可帐户中选择性能层授权。如果选择了错误的性能层，用户可转到FMC或FDM上的页面，并将性能层调整为其虚拟帐户中的内容。

如果虚拟智能许可帐户没有为性能层选择请求的许可证/授权，请参考场景1作为下一步。

要编辑性能层，请导航到FMC Gear Icon > Smart Licenses > Edit Performance Tier，然后选择正确的性能层。



此表用于快速参考性能层及其相关规格、许可证和限制。

表-1

性能层	设备规格（核心/RAM）	丢包率限制	RA VPN会话限制	许可证名称	许可证PID	RA VPN许可证和PID
FTDv5,100Mbps	4核/8 GB	100Mbps	50	FTDv Base 100 Mbps	FTD-V-5S-BSE-K9	Cisco AnyConnect Apex许可证 Cisco AnyConnect Plus许可证 仅Cisco AnyConnect VPN许可证 有关RA VPN许可证PID，请参阅Cisco安全客户端订购指南。
				FTDv恶意软件100 Mbps	FTD-V-5S-TMC	
				FTDv URL过滤100 Mbps		
				FTDv威胁防护100 Mbps		
				Firepower FTDv运营商许可证	FTDV-CAR	
FTDv10,1Gbps	4核/8 GB	1Gbps	250	FTDv Base 1 Gbps	FTD-V-10S-BSE-K9	
				FTDv恶意软件1	FTD-V-	

				Gbps	10S-TMC	
				FTDv URL过滤1 Gbps		
				FTDv威胁防护1 Gbps		
				Firepower FTDv运营商许可证	FTDV-CAR	
FTDv20,3Gbps	4核/8 GB	3Gbps	250	FTDv Base 3 Gbps	FTD-V-20S-BSE-K9	
				FTDv恶意软件3 Gbps	FTD-V-20S-TMC	
				FTDv URL过滤3 Gbps		
				FTDv威胁防护3 Gbps		
				Firepower FTDv运营商许可证	FTDV-CAR	
FTDv30,5Gbps	8核/16 GB	5Gbps	250	FTDv Base 5 Gbps	FTD-V-30S-BSE-K9	
				FTDv恶意软件5 Gbps	FTD-V-30S-TMC	
				FTDv URL过滤5 Gbps		

				FTDv威胁防护5 Gbps		
				Firepower FTDv运营商许可证	FTDV-CAR	
FTDv50,10Gbps	12核/24 GB	10Gbps	750	FTDv Base 10 Gbps	FTD-V-50S-BSE-K9	
				FTDv恶意软件10 Gbps	FTD-V-50S-TMC	
				FTDv URL过滤10 Gbps		
				FTDv威胁防护10 Gbps		
				Firepower FTDv运营商许可证		
FTDv100,16Gbps	16核/32 GB	16Gbps	10,000	FTDv Base 16 Gbps	FTD-V-100S-BSE-K9	
				FTDv恶意软件16 Gbps	FTD-V-100S-TMC	
				FTDv URL过滤16 Gbps		
				FTDv威胁防护16 Gbps		
				Firepower FTDv运营商许可	FTDV-CAR	

				证		
FTDv变量		基于设备功能	基于设备功能	Firepower威胁防御基础功能		
				威胁防御虚拟恶意软件防护		
				威胁防御虚拟URL过滤		
				威胁防御虚拟威胁防护		
				Firepower FTDv运营商许可证	FTDV-CAR	

有关FTDv性能层许可证SKU的详细信息，请参阅表59。思科安全防火墙威胁防御虚拟性能分层基本订用和威胁、恶意软件和URL过滤订用SKU

场景6 — 许可证不在正确的智能帐户或虚拟帐户中

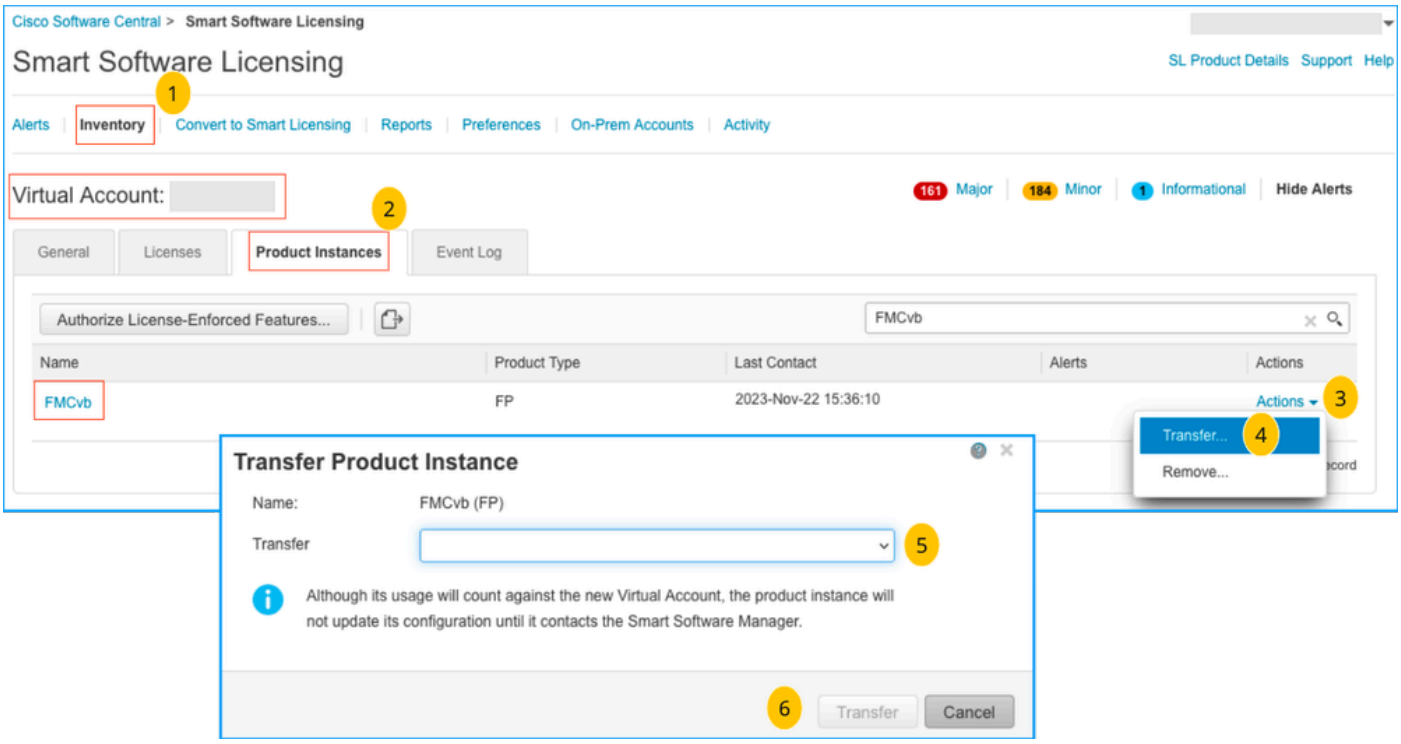
产品实例可以转移到正确的虚拟帐户。

步骤1:使用您的浏览器访问software.cisco.com

第二步：导航到管理许可证

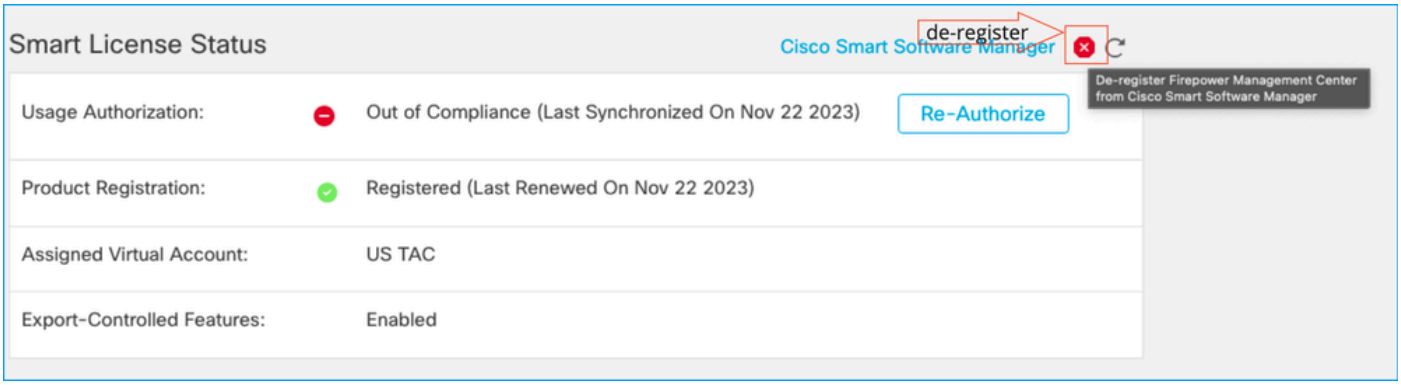
第三步：在右上角下拉列表中选择正确的智能帐户，然后导航到Inventory > [Virtual Account Name] > Product Instances > Actions，然后点击Transfer > Transfer product Instance。

第四步：对话框打开后，选择正确的虚拟帐户以移动FMC或FTD产品实例。



场景7 - FMC不在正确的智能帐户或虚拟帐户中

如果FMC或FTD未使用正确的智能帐户进行注册，请通过点击FMC智能许可页面中的注销图标，从智能软件管理器中注销FMC。



接下来，从正确的智能帐户和虚拟帐户生成令牌，并向智能软件管理器注册FMC。

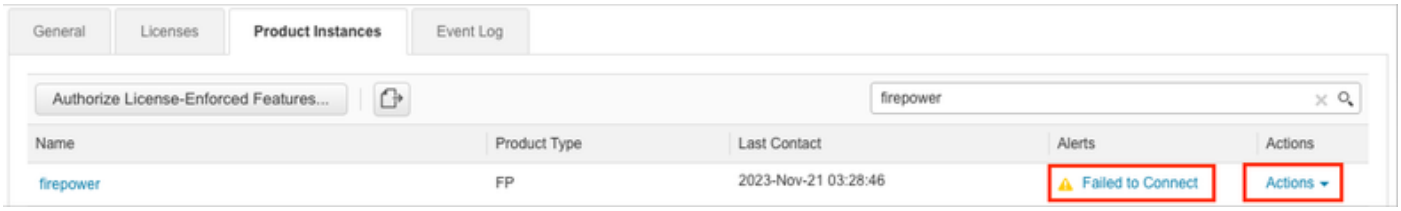
场景8 — 从智能帐户中删除产品实例以进行机上管理

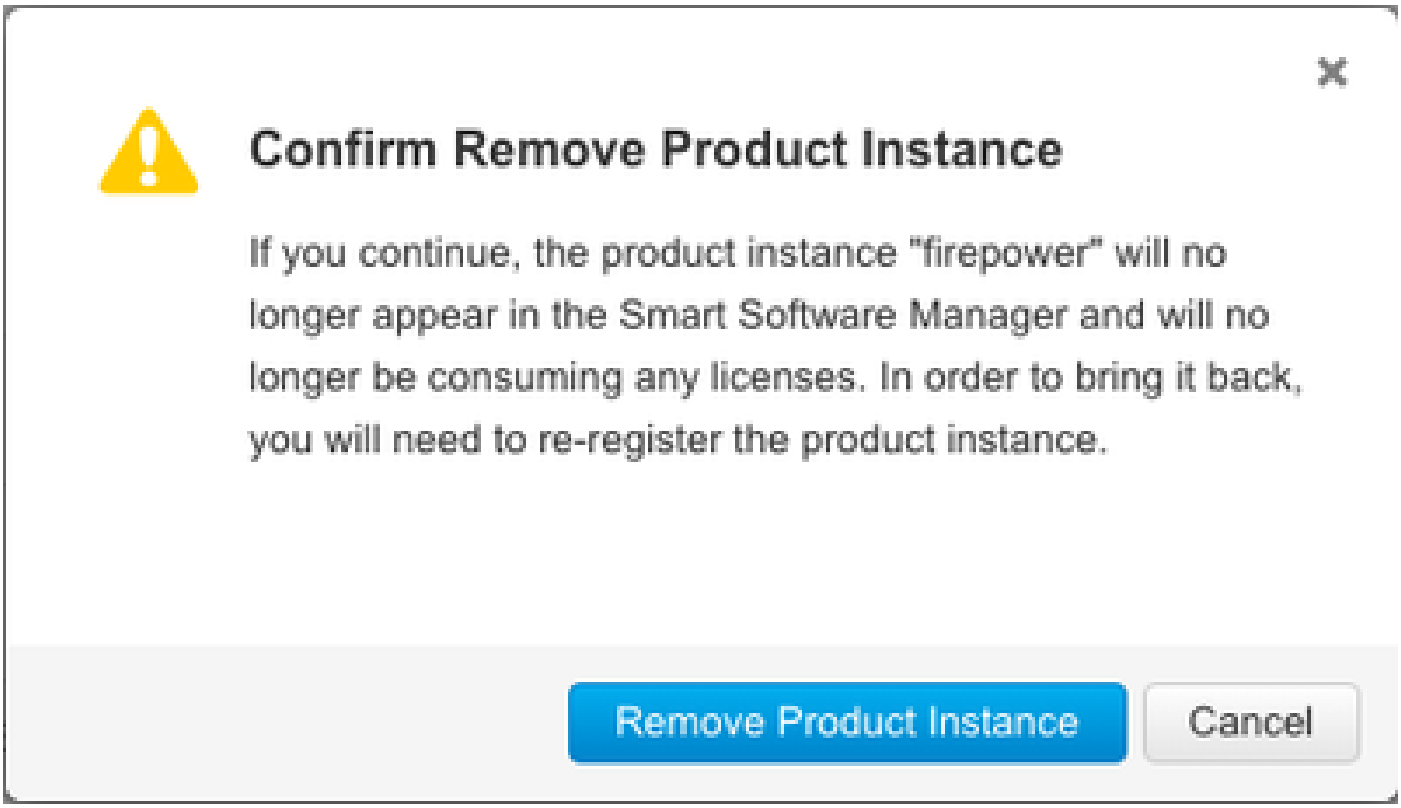
这不适用于FMC管理的设备，因为FMC只获取其管理的设备的许可证。

如果设备重新映像时未从智能帐户中注销许可证，则可能会出现许可证过度使用的情况。

步骤1:导航到智能帐户产品实例，以使用主机名标识实例

第二步：单击操作>>删除。





第三步：单击“删除产品实例”按钮。

如果列出的方案均无帮助，您可以联系Cisco技术支持中心。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。