Troubleshoot Secure Firewall Smart Licensing Out-of-Compliance Errors

Contents

Introduction

Background Information

Identify License Type Causing Out of Compliance Status

- Using the FMC Graphic User Interface (GUI)
- Using the Smart Account Portal
- Using the FMC Command Line Interface (CLI)

Troubleshoot

- Scenario 1 - Not Enough Licenses for a Specific Feature of FTD Physical Platforms
- Scenario 2 - Licenses Available in a Different Virtual Account
- Scenario 3 - Missing Firepower MCv Device License
- Scenario 4 - FTD is a Virtual Platform Running a pre-7.0 Version
- Scenario 5 - FTD is a Virtual Platform Running 7.0 Version or Later
- Scenario 6 - License is not in the Proper Smart Account or Virtual Account
- Scenario 7 - FMC is not in the Proper Smart Account or Virtual Account
- Scenario 8 - Removing a Product Instance from the Smart Account for On-Box Management

Introduction

This document describes the most common Cisco Smart Licensing out of compliance reasons with the Cisco FMC and FTD models.

Background Information

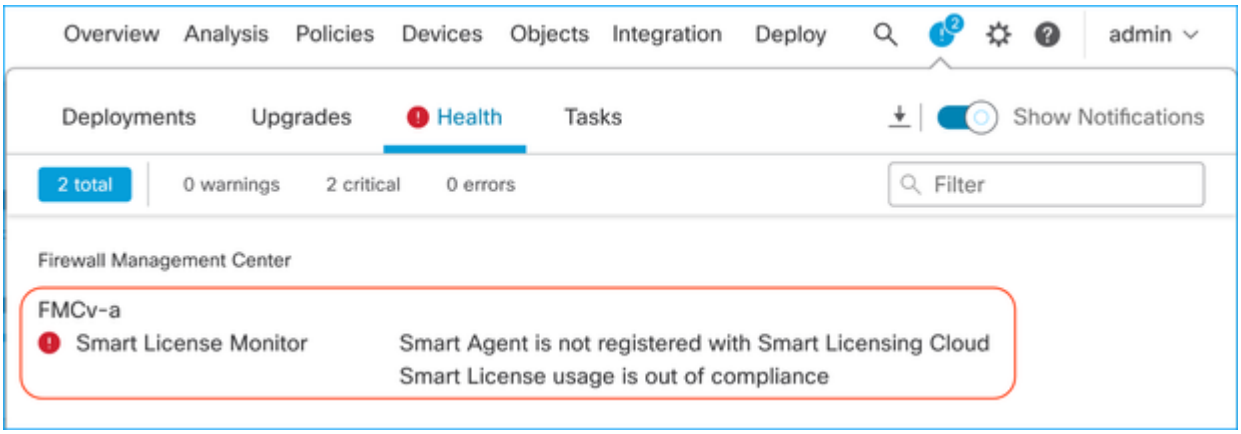
Cisco Smart Licensing offers centralized management of licenses for many products. The Cisco Secure Firewall simplifies the management of licenses across potentially large deployments of sensors, and it can be used for appliance, virtual, and public cloud models. This document provides a troubleshooting guide for Out-of-Compliance issues with Smart License for Cisco Firewall Management Center (FMC) and Cisco Firewall Threat Defense (FTD) software and appliance models.

When FMC reports that the Smart License is out of compliance, it indicates that FMC cannot find the appropriate license in the Smart Account. When that happens, a Health Alert is displayed. It could be due to several reasons outlined in this document.

Identify License Type Causing Out of Compliance Status

Using the FMC Graphic User Interface (GUI)

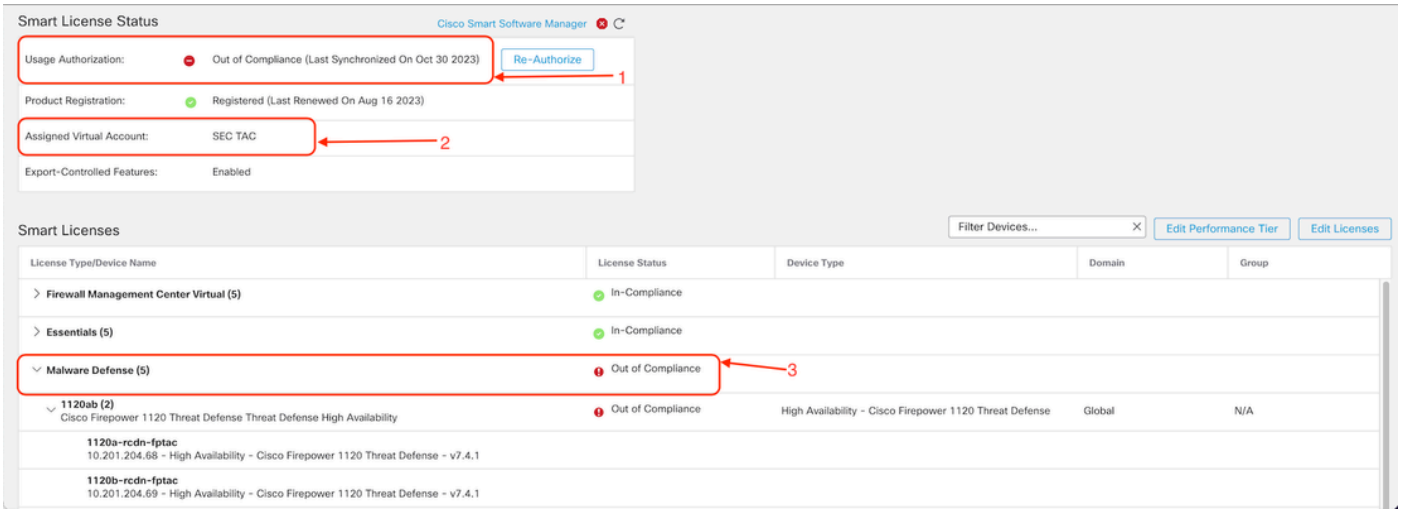
Navigate to **Health Alert** from the FMC Notification Icon and click **Health.**



Using the Smart Account Portal

Navigate to **Smart License Status** at **System > Licenses > Smart Licenses.** The Virtual Account information the FMC is registered to can be found here.

In the Smart Licenses section, the specific licenses out of compliance are indicated here. In this example, an "Out of Compliance" status is listed for a Cisco Secure Firewall 1120 feature license "Malware Defense. Note all the features/products listed as "Out of Compliance" in Red. The green "In-Compliance" checkmark indicates that the specific license type is available, and FMC is able to acquire it from the Smart Account.

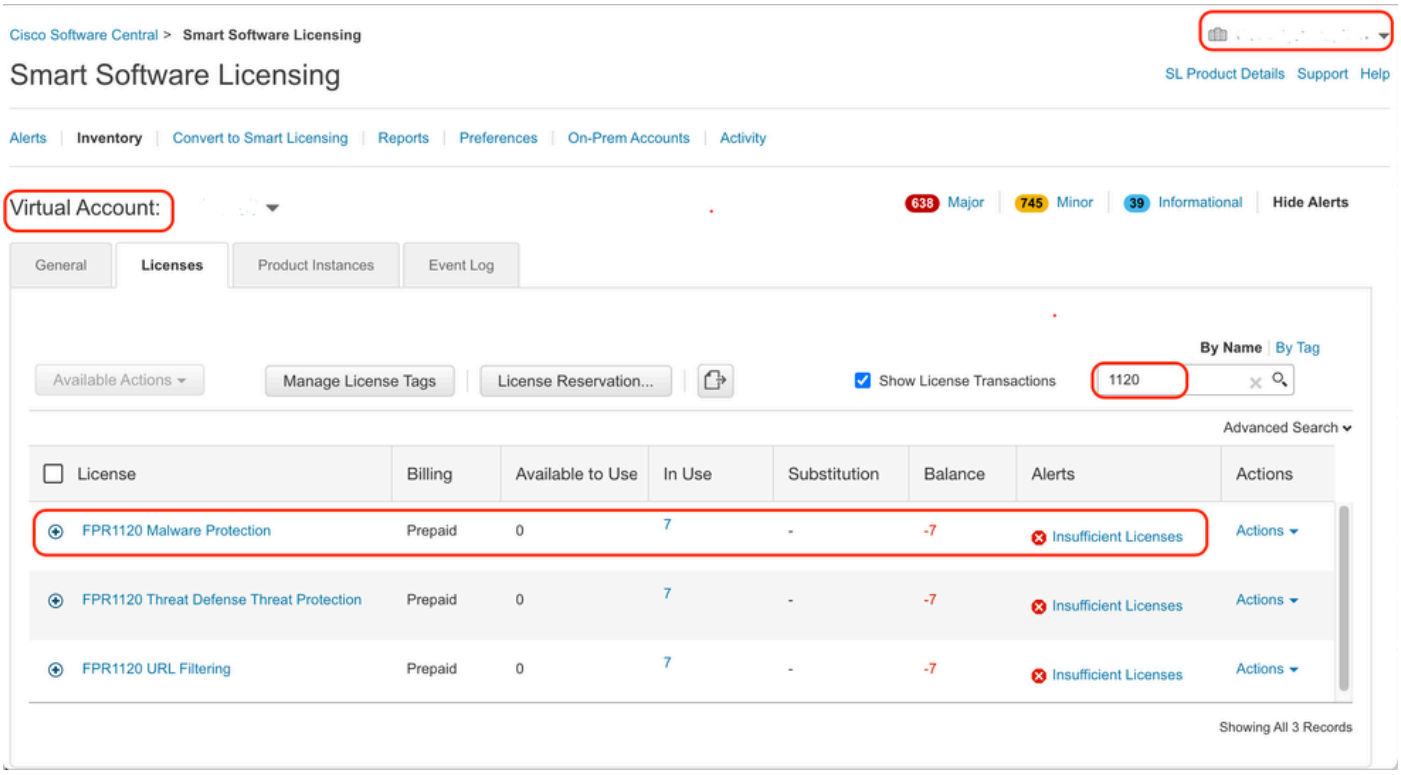


To verify these licenses' availability, you can log into the Smart Account Portal and navigate to **Smart Account > Inventory > [Virtual Account Name]**. Filter the license name if needed.

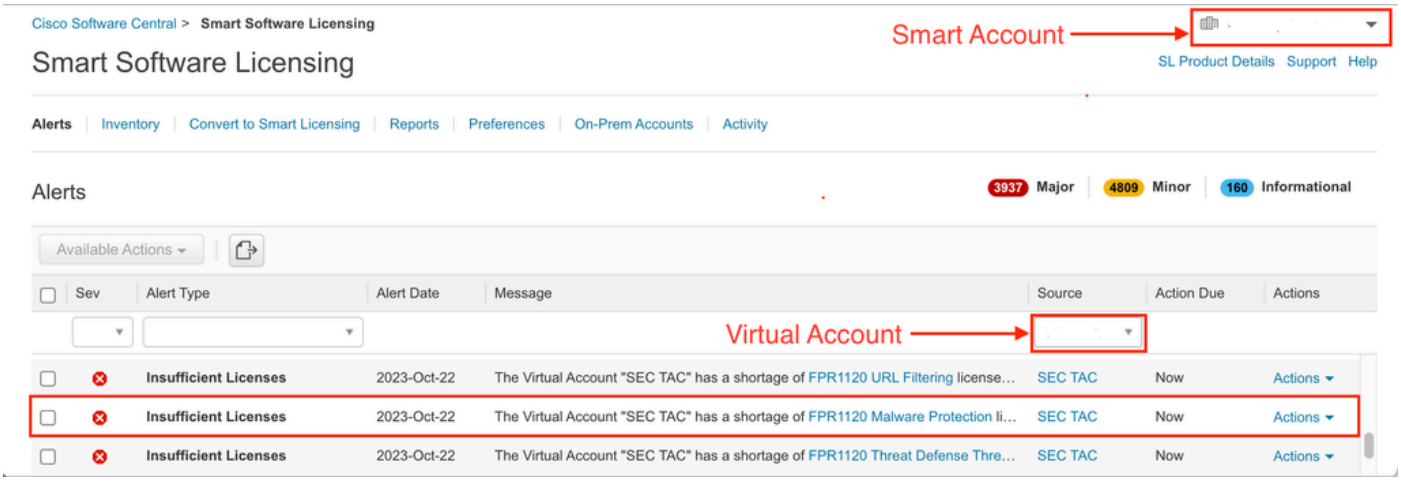
Note these possible statuses:

- Available to Use = Purchased count
- In use = Count of devices with this Feature enabled
- Balance = Offset between purchased and using.

Whenever the Balance turns negative, the FMC shows the Out of Compliance status for that feature/product.



Also, an alert can be found at **Smart Account** > **Alerts**. Filter the Virtual Account in the "Source" if needed.



Using the FMC Command Line Interface (CLI)

Step 1. Log into FMC CLI.

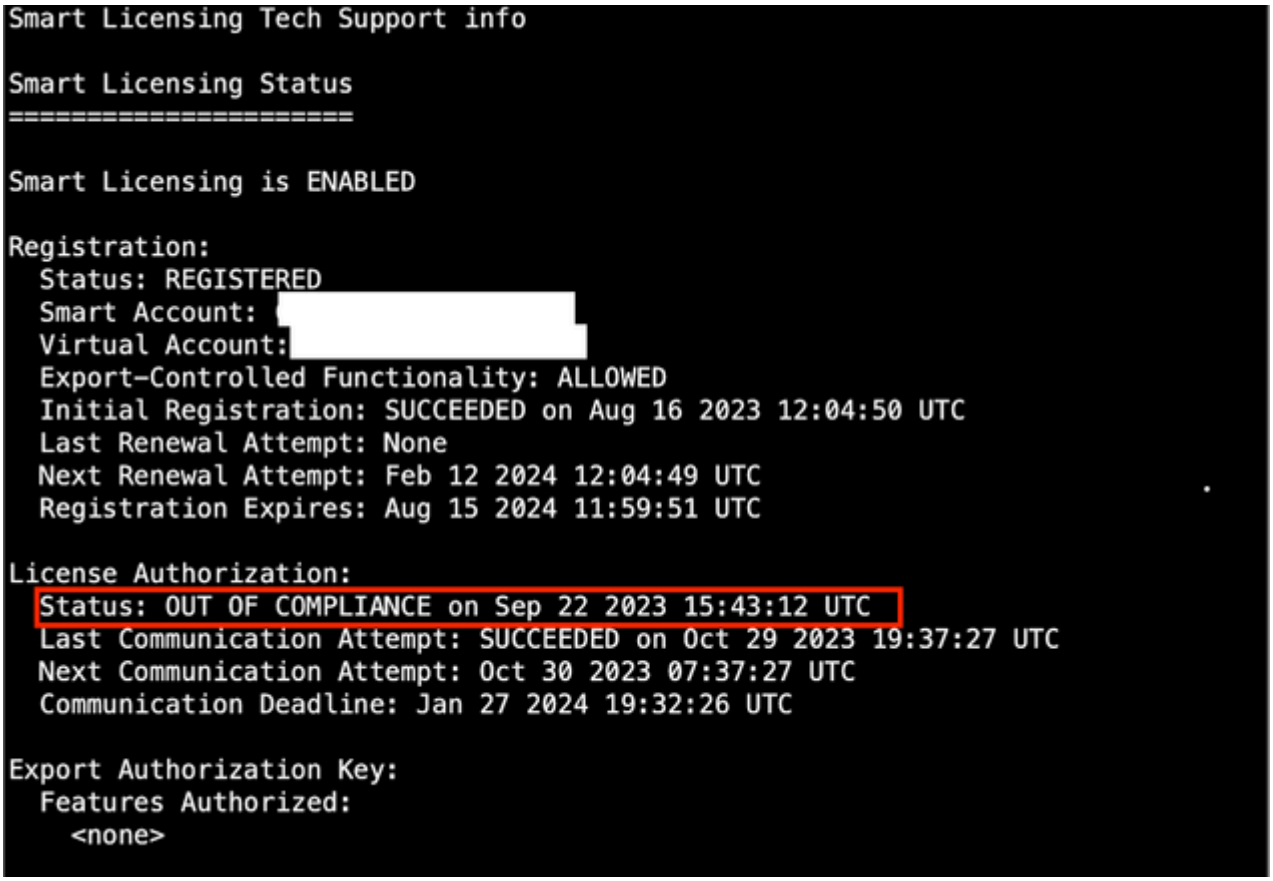
Step 2. Access the Linux shell with this command

```
expert
```

Step 3. Issue this command.

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

Navigate to the latest entry in the file by scrolling down to check the latest status.



If a License is adequately acquired, the license shows up as 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
```

If a License is unavailable, the specific license type shows as 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
```

Troubleshoot

These are some of the most common scenarios and how to troubleshoot each.

Scenario 1 - Not Enough Licenses for a Specific Feature of FTD Physical Platforms

There are different license types. These can be classified as hardware and feature-specific. The licenses can be identified based on the model displayed in the license name followed by the feature it is providing a license for.

-Base (Pre 7.x) or Essentials (Post 7.x)

-Malware Defense

-IPS

-URL

-Carrier

-Secure Client Premier

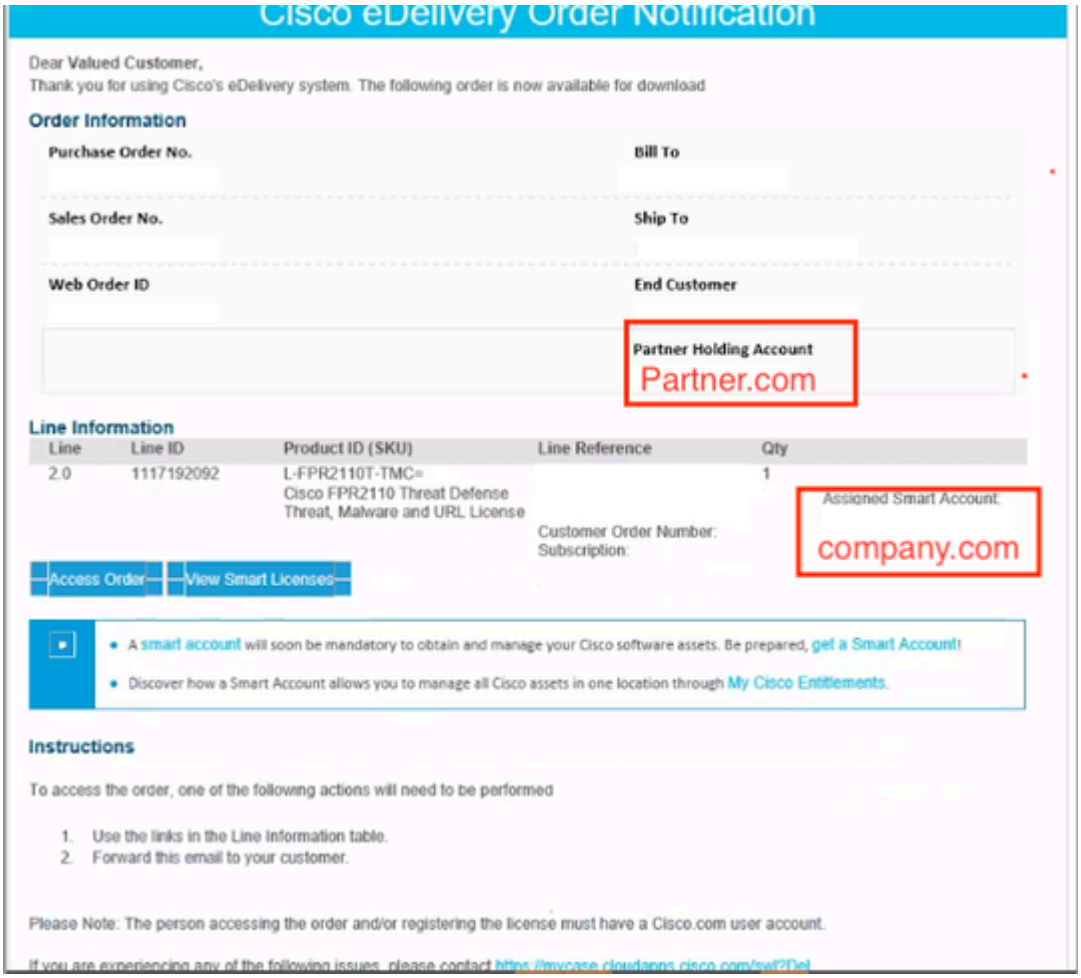
-Secure Client Advantage

-Secure Client VPN only

If you suspect that the licenses were purchased and not available in your Smart Account, verify your Order information and check the Smart License account that was provided when the order was placed.

If a Assigned Smart Account is provided when the purchase order is placed, the licenses get transferred to the "Assigned Smart Account".

If the Assigned Smart Account is not provided and the order is placed through a partner, the licenses are transferred to the Partner Holding Account. Contact your Cisco Partner company with the purchase order if this is the case and they can help in transferring these licenses to your Smart Account.



Scenario 2 - Licenses Available in a Different Virtual Account

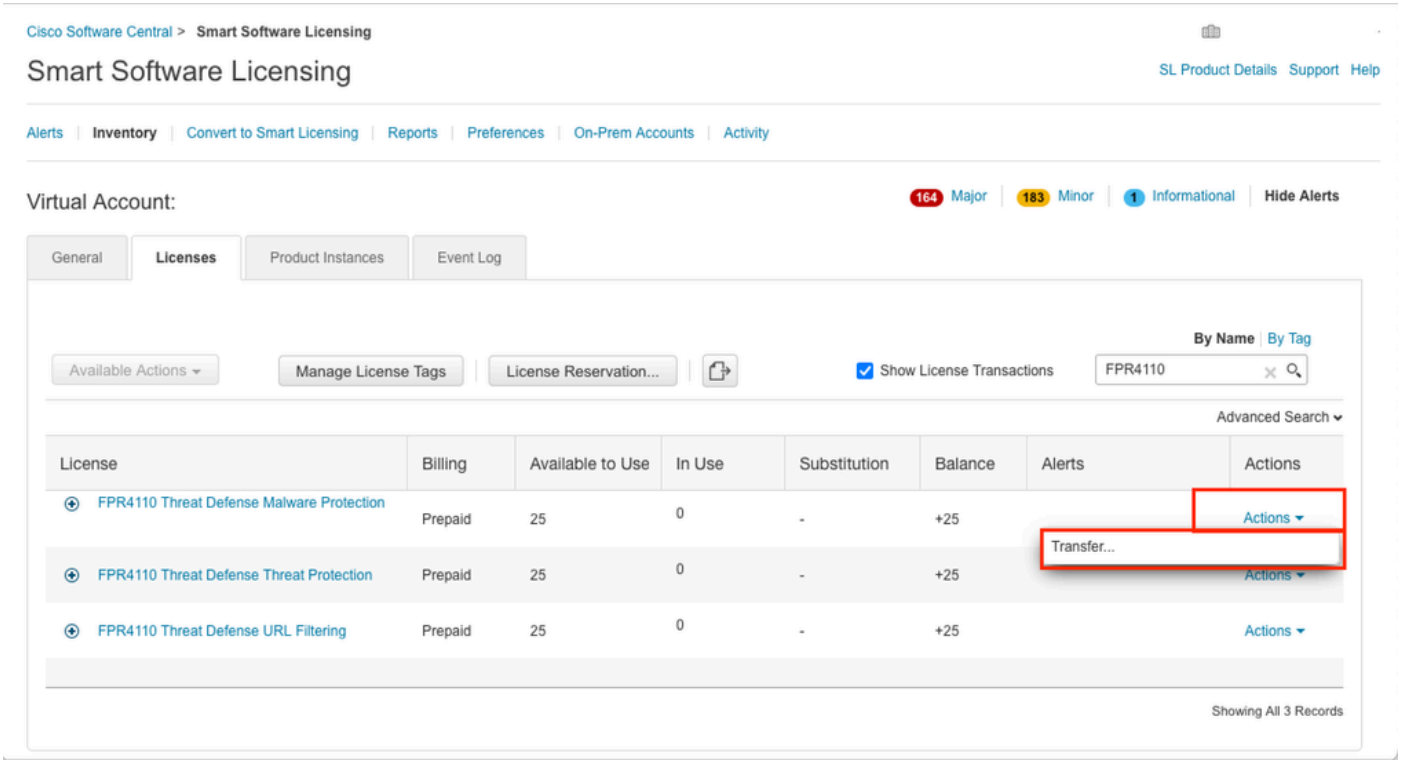
By default, there is only one virtual account named DEFAULT in every Smart Account. Smart Account Administrator can create multiple virtual accounts for administration ease and other purposes.

If the licenses needed are part of a different virtual account, those can be transferred to the proper virtual account using these steps.

Step 1. Navigate to **Smart Account > Inventory.**

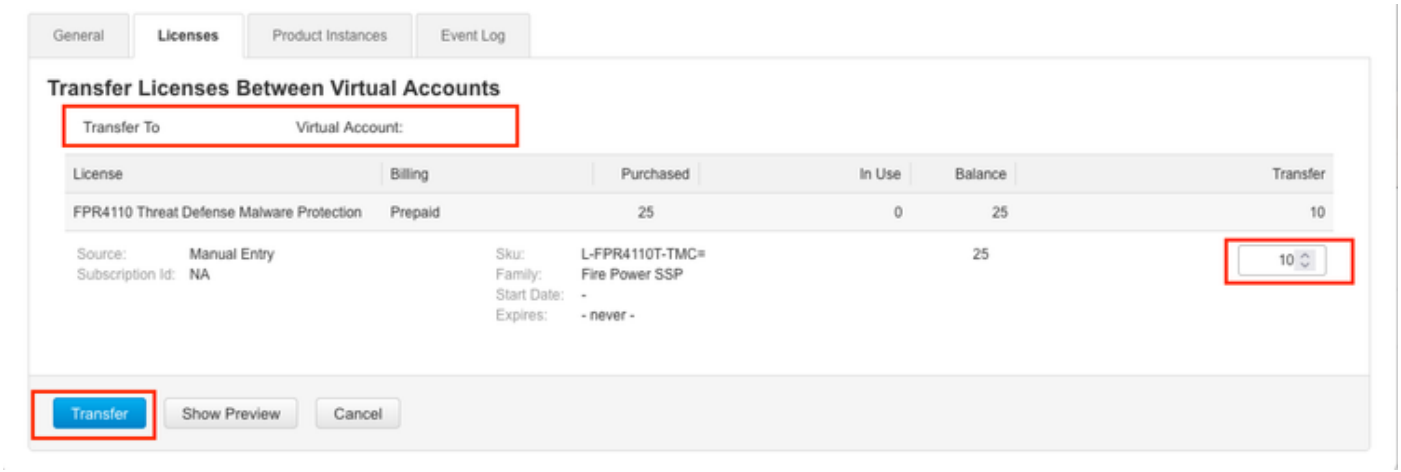
Step 2. Filter the correct Virtual Account. Filter the License if needed.

Step 3. Once the right license is identified, click the **Actions** dropdown and select **Transfer**.



Step 4. Select the destination Virtual Account that needs the licenses and provide a number of licenses to transfer.

Step 5. Click **Show Preview** to validate, then click **Transfer.**



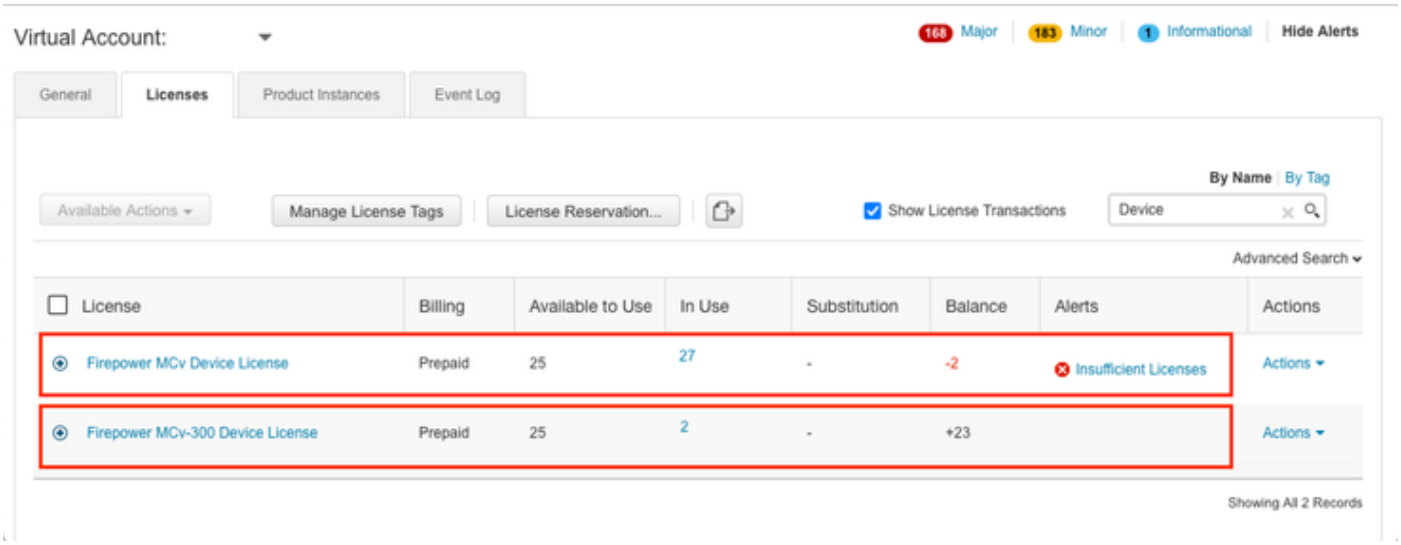
Once all the licenses are available in the virtual account the FMC Is registered to, click the **Re-Authorize** button on the FMC to clear the Out of Compliance status.

Scenario 3 - Missing Firepower MCv Device License

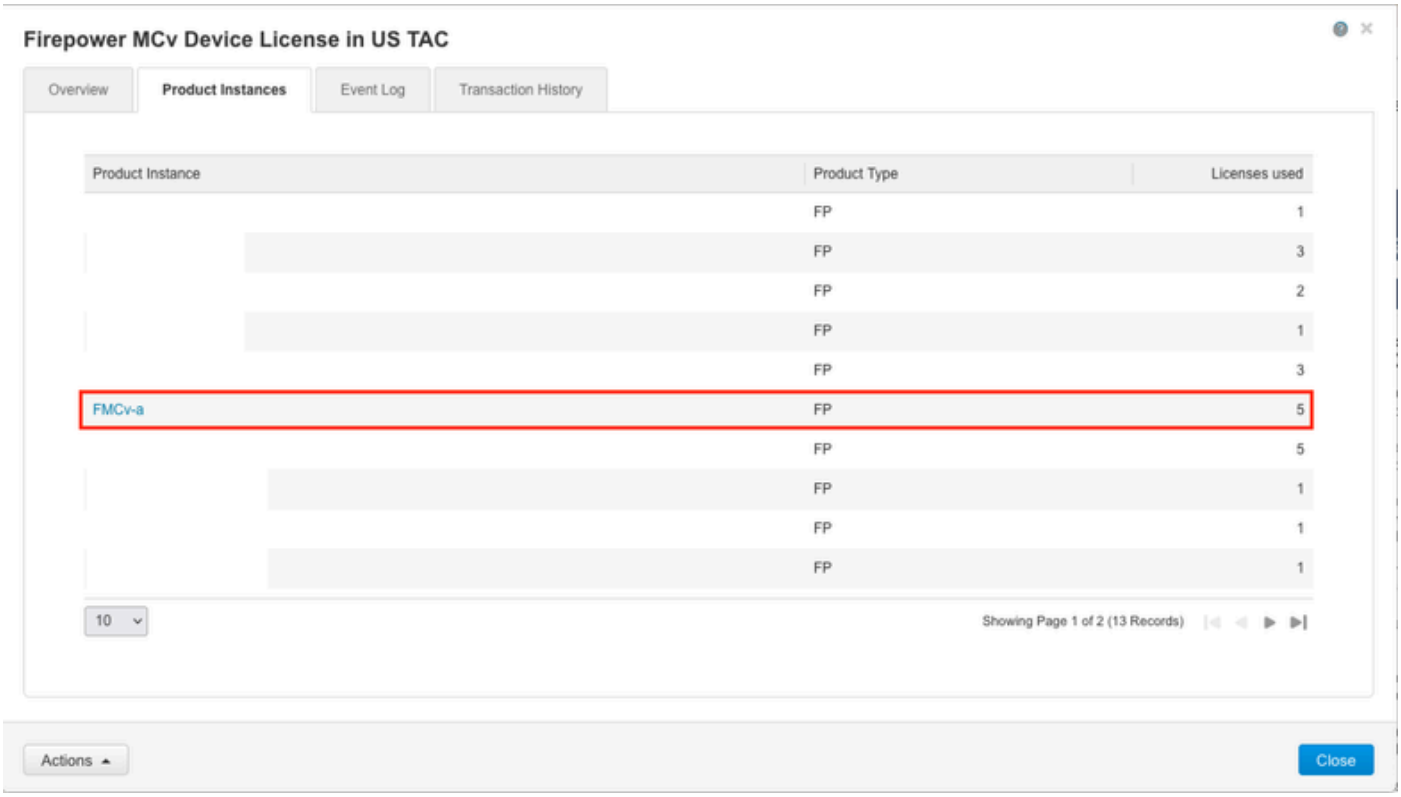
For virtual management models, two different platforms are commonly mixed up.

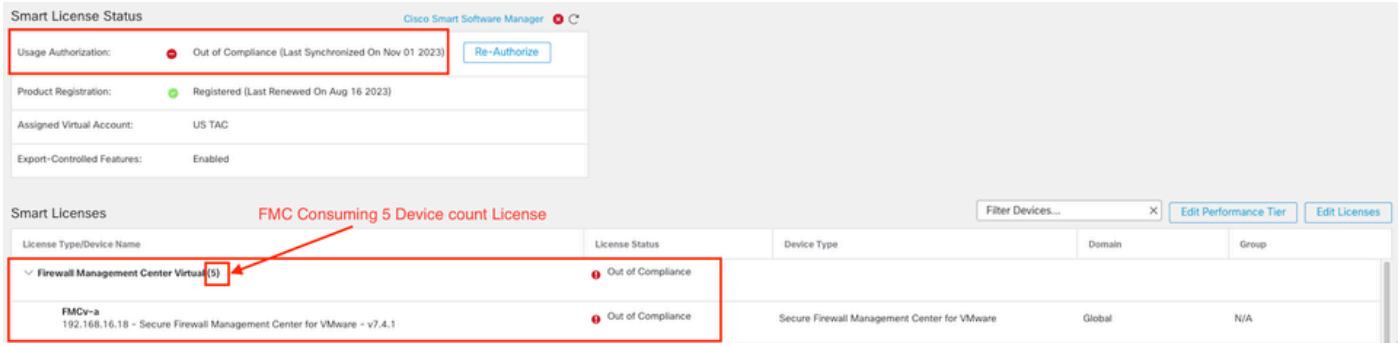
The FMCv Device license shows up as the **Firepower MCv Device License** and the FMCv300 Device license is the **Firepower MCv300 Device License**.

To Manage Firewalls, FMC needs a Device license as well.



Clicking the License type helps to identify what FMCs are consuming those licenses. In this example, FMCv-a is consuming five licenses, which matches the FMC Smart License page.





Scenario 4 - FTD is a Virtual Platform Running a pre-7.0 Version

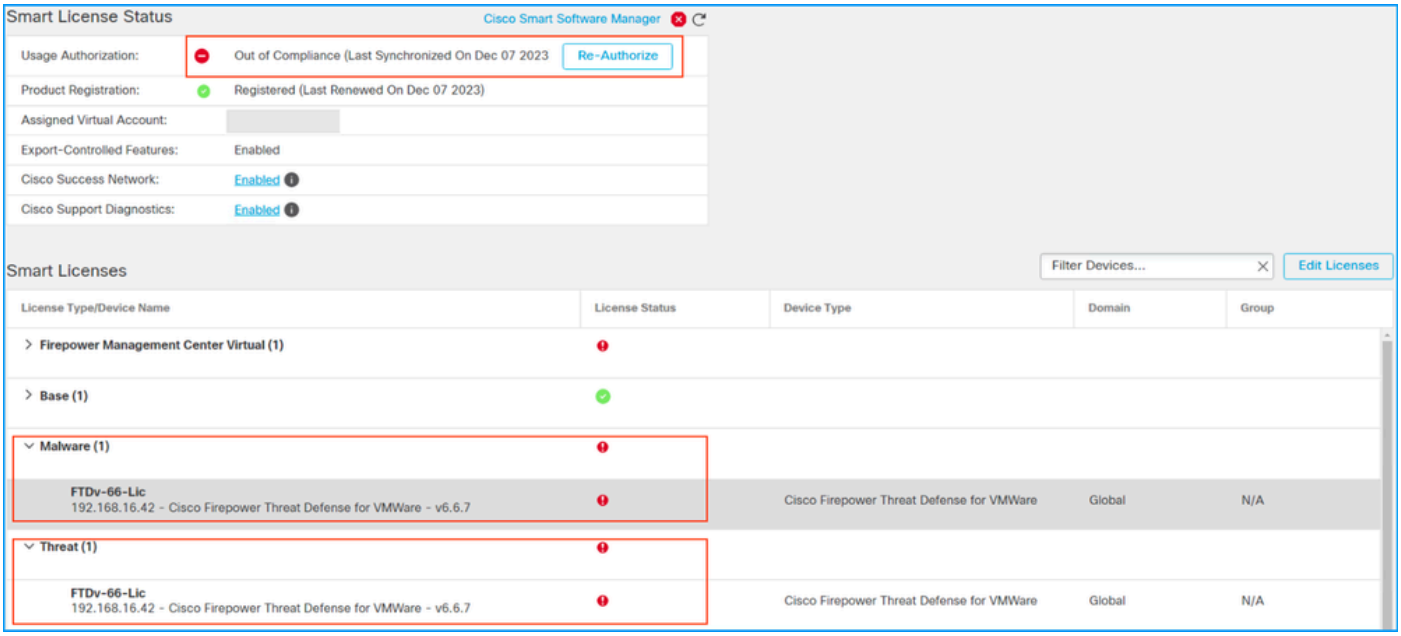
Base licenses are automatically requested and are not tiered. Refer to Tables 60 and 61 in the Cisco Network Security Ordering Guide for pre 7.x FTDv Stock Keeping Units (SKUs).

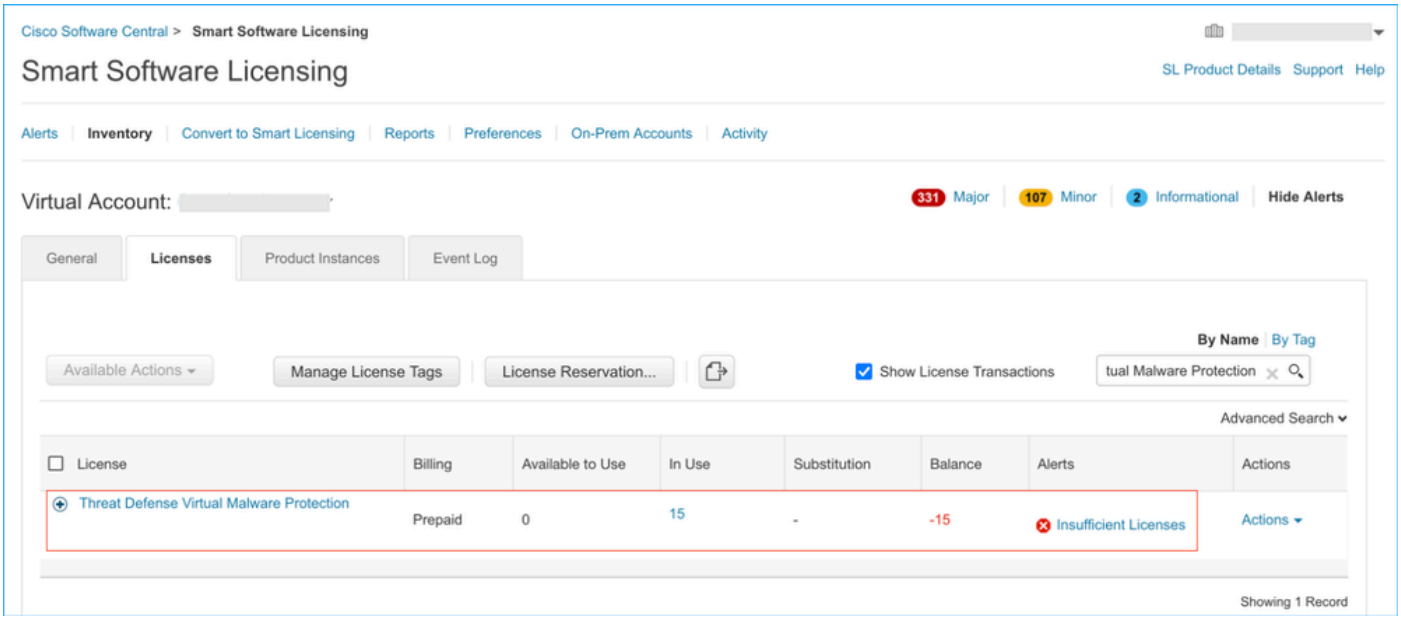
These are the Pre 7.x FTDv License Names in the Smart Account.

Threat Defense Virtual Malware Protection
Threat Defense Virtual URL Filtering
Firepower MCv Device License
Firepower Threat Defense Base Features
Threat Defense Virtual Threat Protection
Cisco AnyConnect Plus License
Cisco AnyConnect Apex License
Cisco AnyConnect VPN Only License

In this example, the Malware and Threat Licenses are out of compliance due to the Virtual Account not having sufficient licenses.

To get the license compliant, the user must ensure the Smart Licensing virtual account has enough licenses available. Refer to the Cisco Network Security Ordering Guide for pre-7.x FTDv SKUs.



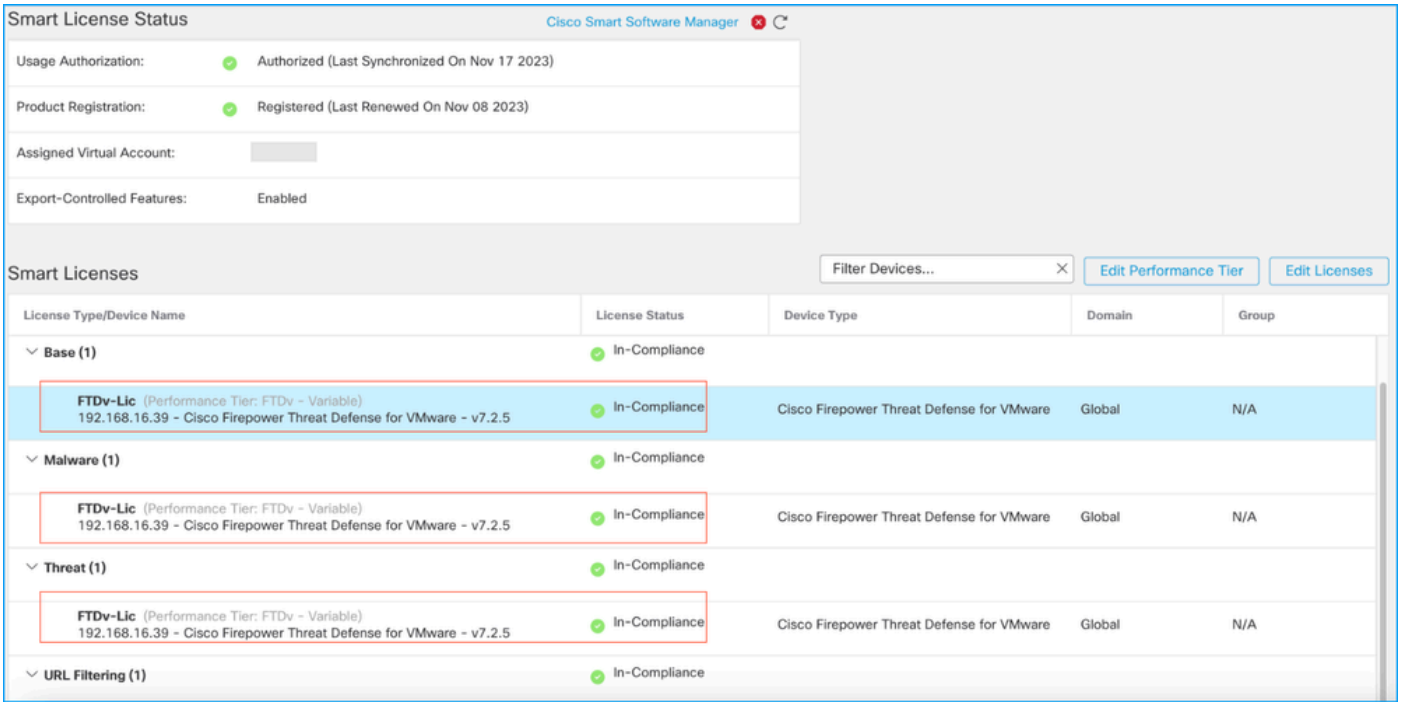


Scenario 5 - FTD is a Virtual Platform Running 7.0 Version or Later

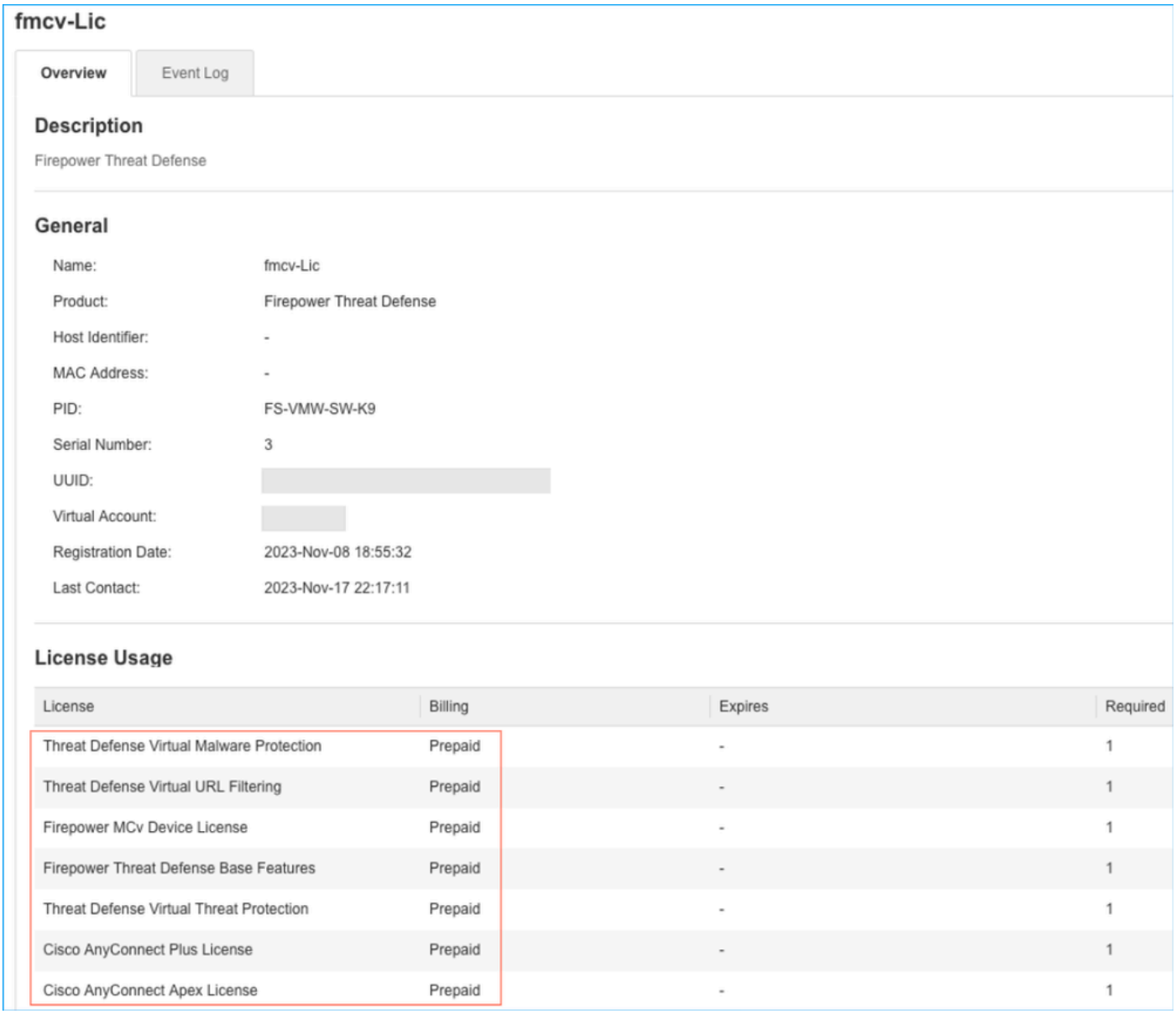
Base licenses are subscription-based and mapped to tiers. Virtual accounts must have Base license entitlements for FTDvs and Threat, Malware, and URL Filtering.

When an FTDv is upgraded to Version 7.0 or later, the device is automatically moved to an **FTDv - Variable** tier and consumes non-tiered entitlements. In this example, an FTD is upgraded from 6.6.7 to

7.2.5, and the Smart License status shows Authorized and In-Compliance.

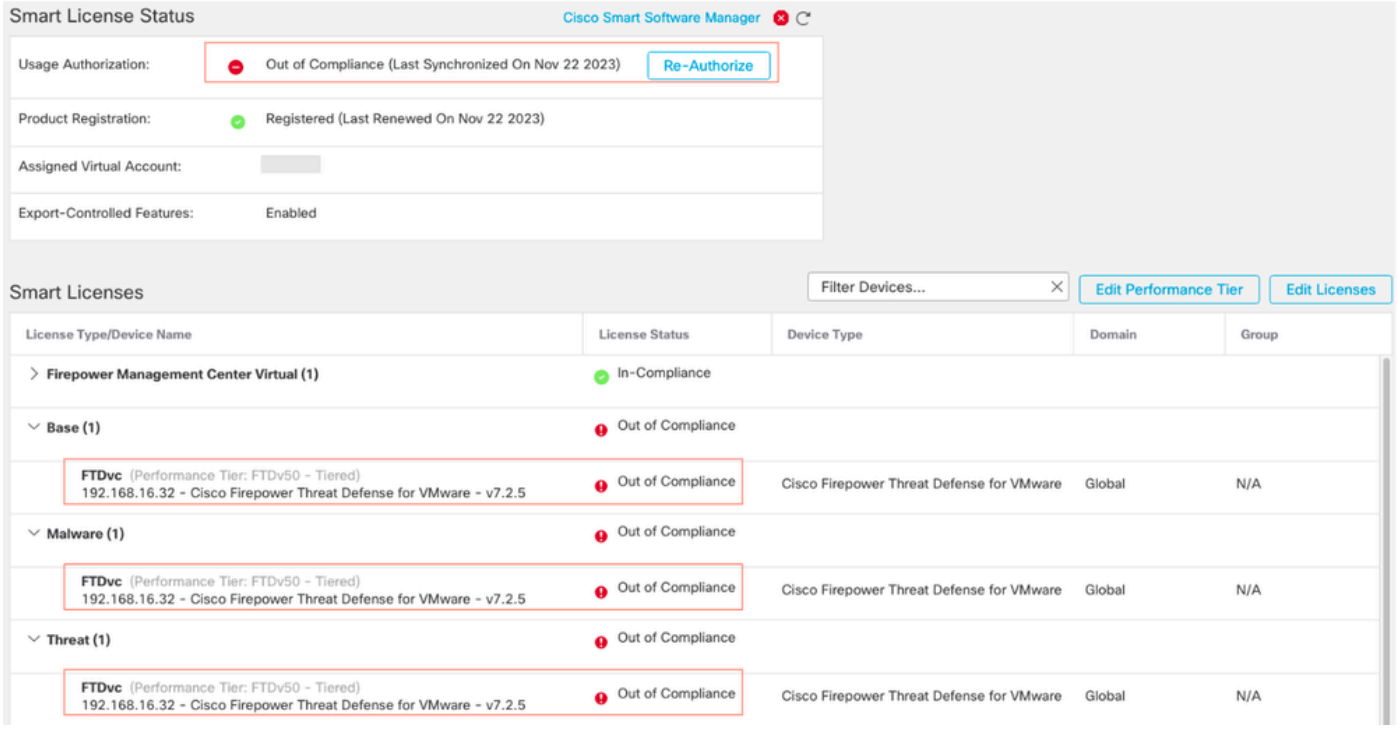


It continues to consume non-tiered entitlements.

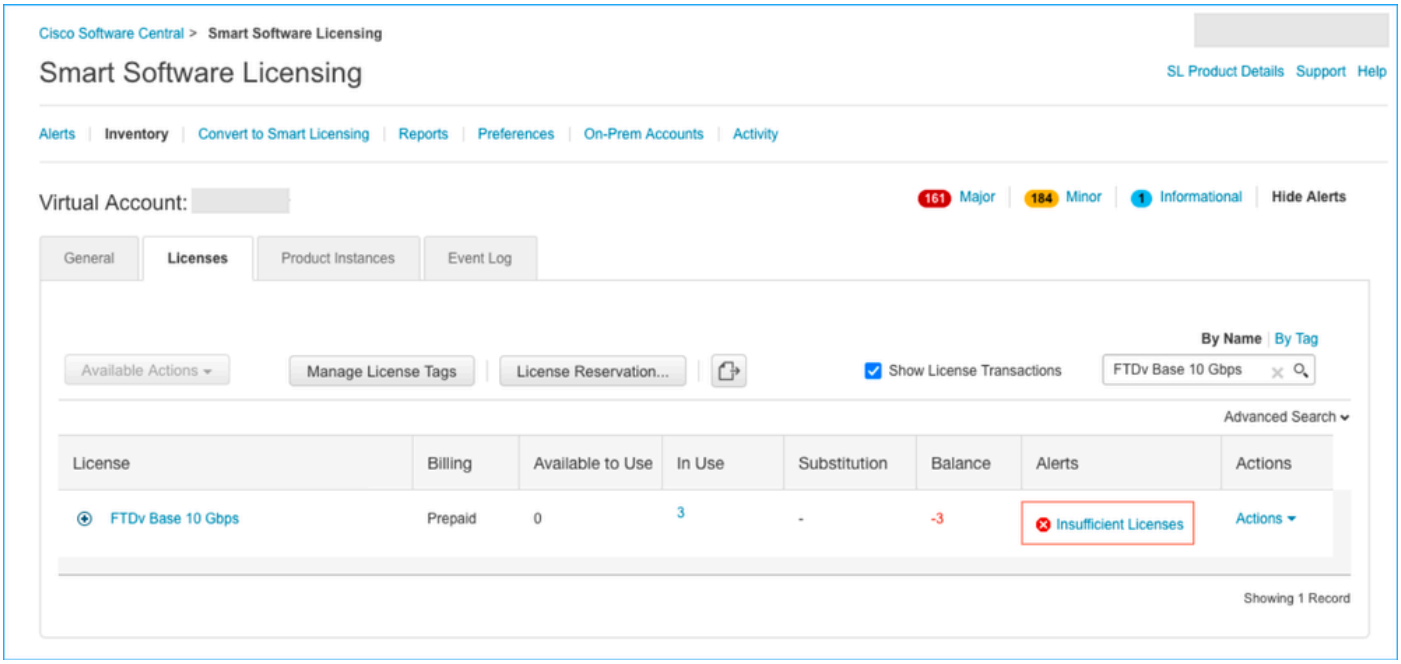


If a user selects a (or defaults to an auto-assigned) Performance Tier for which they do not have entitlements, the status **Out of Compliance** is displayed.

In this example, the user selects Performance Tier FTDv50 with no Base Malware and Threat licenses in the registered Virtual account.



The Virtual Account must display more Licenses/entitlements for the requested Performance Tier.

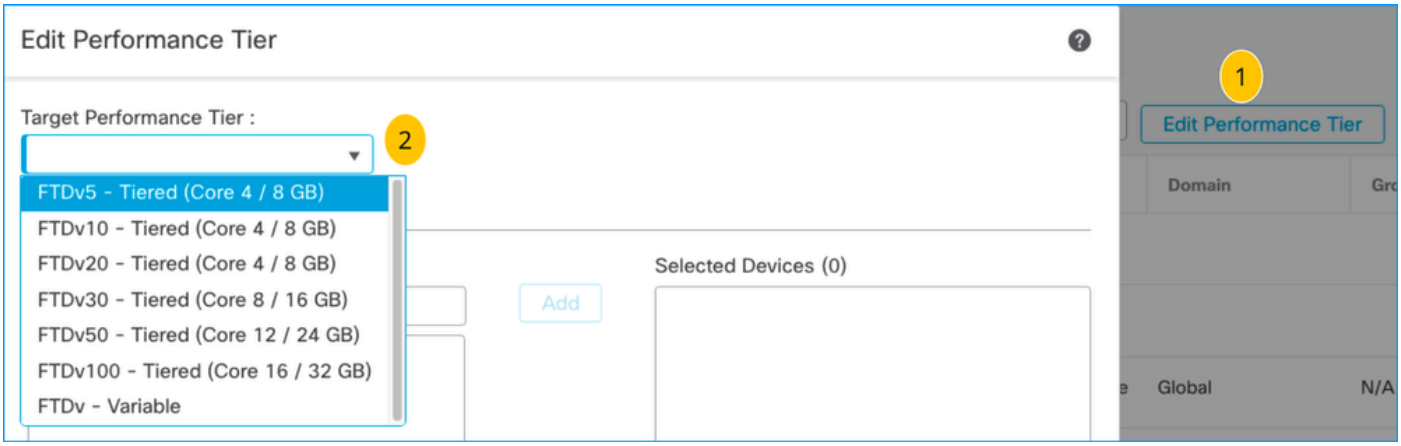


To comply, the user must select the Performance Tier entitlements in their Virtual Smart Licensing account. If a wrong performance Tier is chosen, the user can go to the page on FMC or FDM and adjust the Performance Tier to what they have in their Virtual Account.

If the Virtual Smart Licensing account does not have the requested Licenses/entitlements for the Performance Tier picked, refer to Scenario 1 as the next step.

To edit the performance Tier, navigate to the **FMC Gear Icon > Smart Licenses > Edit Perforamance**

Tier and choose the correct Perforamance Tier.



This table is for quick reference of Performance Tier and their associated specifications, licenses, and limits.

Table-1

Performance Tier	**Device Specifications (Core/RAM)**	**Rate Limit**	**RA VPN Session Limit**	**License Names**	**License PIDs**	**RA VPN License and PIDs**
FTDv5, 100Mbps	4 core/8 GB	100Mbps	50	FTDv Base 100 Mbps	FTD-V-5S-BSE-K9	Cisco AnyConnect Apex License Cisco AnyConnect Plus License Cisco AnyConnect VPN Only License For RA VPN License PID please —See the Cisco Secure Client Ordering Guide.
				FTDv Malware 100 Mbps	FTD-V-5S-TMC	
				FTDv URL Filtering 100 Mbps		
				FTDv Threat Protection 100 Mbps		
				Firepower FTDv Carrier License	FTDV-CAR	
FTDv10, 1Gbps	4 core/8 GB	1Gbps	250	FTDv Base 1 Gbps	FTD-V-10S-BSE-K9	

				FTDv Malware 1 Gbps	FTD-V-10S-TMC	
				FTDv URL Filtering 1 Gbps		
				FTDv Threat Protection 1 Gbps		
				Firepower FTDv Carrier License	FTDV-CAR	
FTDv20, 3Gbps	4 core/8 GB	3Gbps	250	FTDv Base 3 Gbps	FTD-V-20S-BSE-K9	
				FTDv Malware 3 Gbps	FTD-V-20S-TMC	
				FTDv URL Filtering 3 Gbps		
				FTDv Threat Protection 3 Gbps		
				Firepower FTDv Carrier License	FTDV-CAR	
FTDv30, 5Gbps	8 core/16 GB	5Gbps	250	FTDv Base 5 Gbps	FTD-V-30S-BSE-K9	
				FTDv Malware 5 Gbps	FTD-V-30S-TMC	
				FTDv URL Filtering 5 Gbps		
				FTDv Threat Protection 5 Gbps		

				Firepower FTDv Carrier License	FTDV-CAR	
FTDv50, 10Gbps	12 core/24 GB	10Gbps	750	FTDv Base 10 Gbps	FTD-V-50S-BSE-K9	
				FTDv Malware 10 Gbps	FTD-V-50S-TMC	
				FTDv URL Filtering 10 Gbps		
				FTDv Threat Protection 10 Gbps		
				Firepower FTDv Carrier License		
FTDv100, 16Gbps	16 core/32 GB	16Gbps	10,000	FTDv Base 16 Gbps	FTD-V-100S-BSE-K9	
				FTDv Malware 16 Gbps	FTD-V-100S-TMC	
				FTDv URL Filtering 16 Gbps		
				FTDv Threat Protection 16 Gbps		
				Firepower FTDv Carrier License	FTDV-CAR	
FTDv Variable		Based on device	Based on device	Firepower Threat Defense		

		capabilities	capabilities	Base Features		
				Threat Defense Virtual Malware Protection		
				Threat Defense Virtual URL Filtering		
				Threat Defense Virtual Threat Protection		
				Firepower FTDv Carrier License	FTDV-CAR	

For more details on FTDv Performance Tier license SKUs, refer to Table 59. Cisco Secure Firewall Threat Defense Virtual Performance tiered Base Subscription and Threat, Malware and URL Filtering Subscription SKUs

Scenario 6 - License is not in the Proper Smart Account or Virtual Account

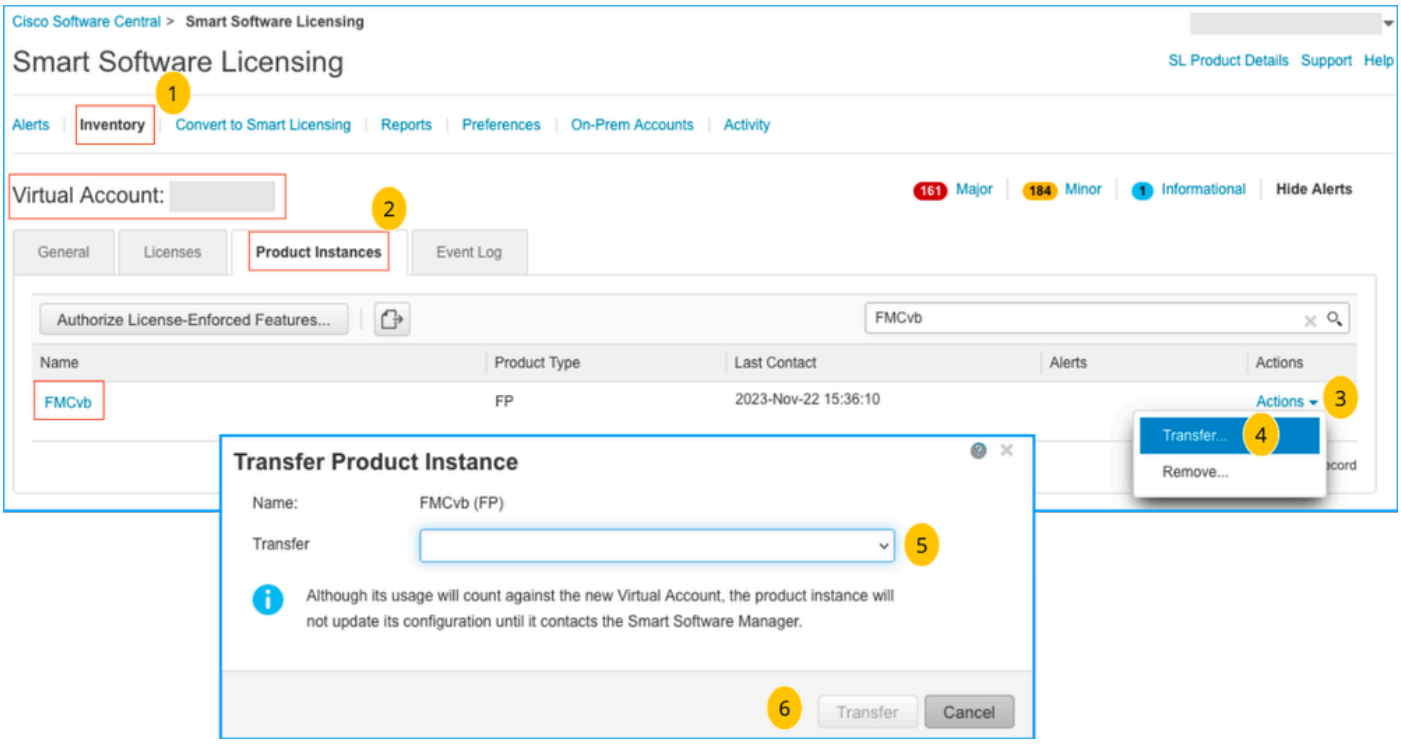
The product instance can be transferred to the correct virtual account.

Step 1. Go to **software.cisco.com** using your browser

Step 2. Navigate to **Manage Licenses**

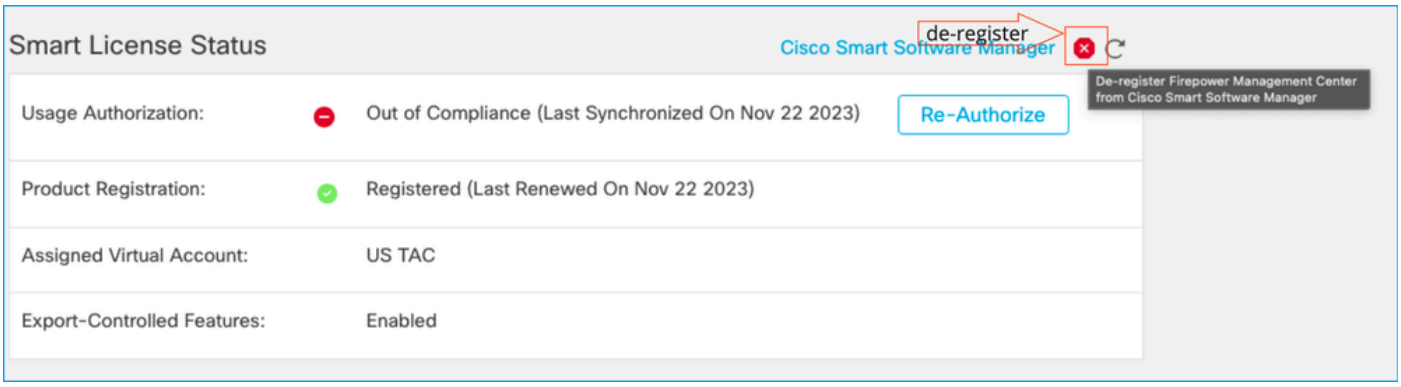
Step 3. Select the proper Smart Account on the top right dropdown and navigate to **Inventory > [Virtual Account Name] > Product Instances > Actions** and click **Transfer > Transfer product Instance.**

Step 4. Once the dialog box opens, choose the correct virtual account to move the FMC or FTD product instance.



Scenario 7 - FMC is not in the Proper Smart Account or Virtual Account

If the FMC or FTD is not registered with the correct Smart Account, deregister the FMC from Cisco License Central by clicking the **De-register** icon from the FMC Smart Licensing page.



Next, generate the token from the right Smart Account and Virtual account and register the FMC with Cisco License Central.

Scenario 8 - Removing a Product Instance from the Smart Account for On-Box Management

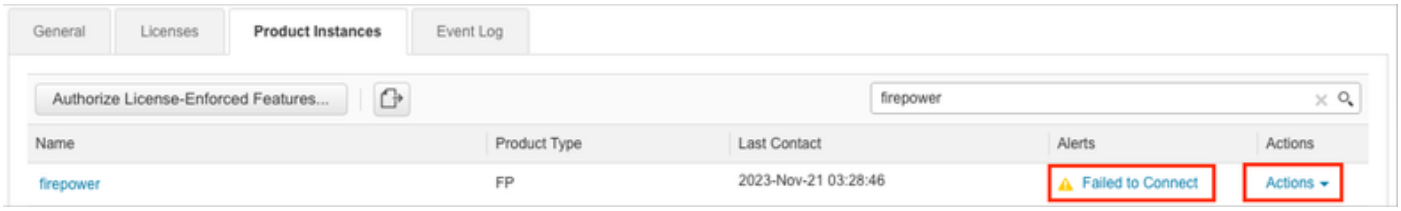
This does not apply to devices being managed by FMC, as the FMC only acquires the licenses for the devices it manages.

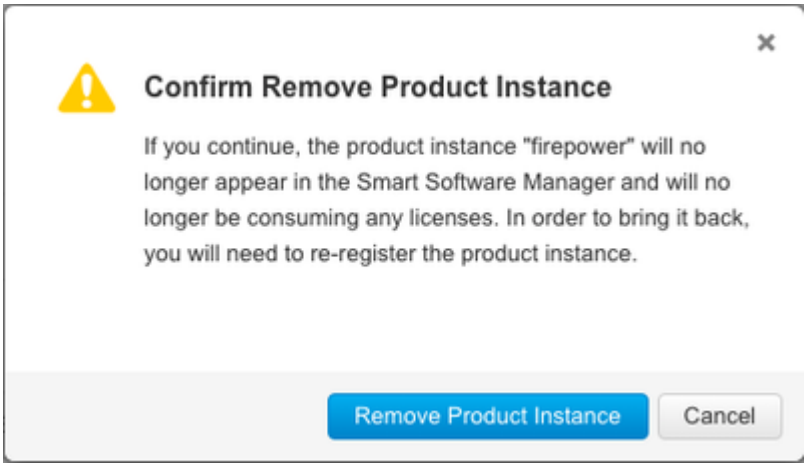
There could be scenarios where the licenses are being over-consumed when a device is re-imaged without

de-registering the license from the Smart account.

Step 1. Navigate to the Smart account Product Instances to Identify the instance using the hostname

Step 2. Click **Actions > Remove**.





Step 3. Click the **Remove Product Instanc**e button.

If none of the listed scenarios help, you can contact the Cisco Technical Support Center.