Upgrade FMC in High Availability

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Pre-upgrade

Upgrade Procedure

- Step 1. Pause Synchronization
- Step 2. Upload the Upgrade Package
- Step 3. Readiness Check
- Step 4. Upgrade the FMC
- Step 5. Upgrade Primary (Active) Peer
- Step 6. Make the Desired FMC Active

Validation

Introduction

This document describes the steps to upgrade an environment of Secure Firewall Management Center (FMC) in High Availability (HA).

Prerequisites

Requirements

Cisco recommends you have knowledge of these topics:

- High Availability concepts
- Secure FMC configuration

Components Used

The information in this document is based on virtual Secure Firewall Management Center, version 7.4.2.

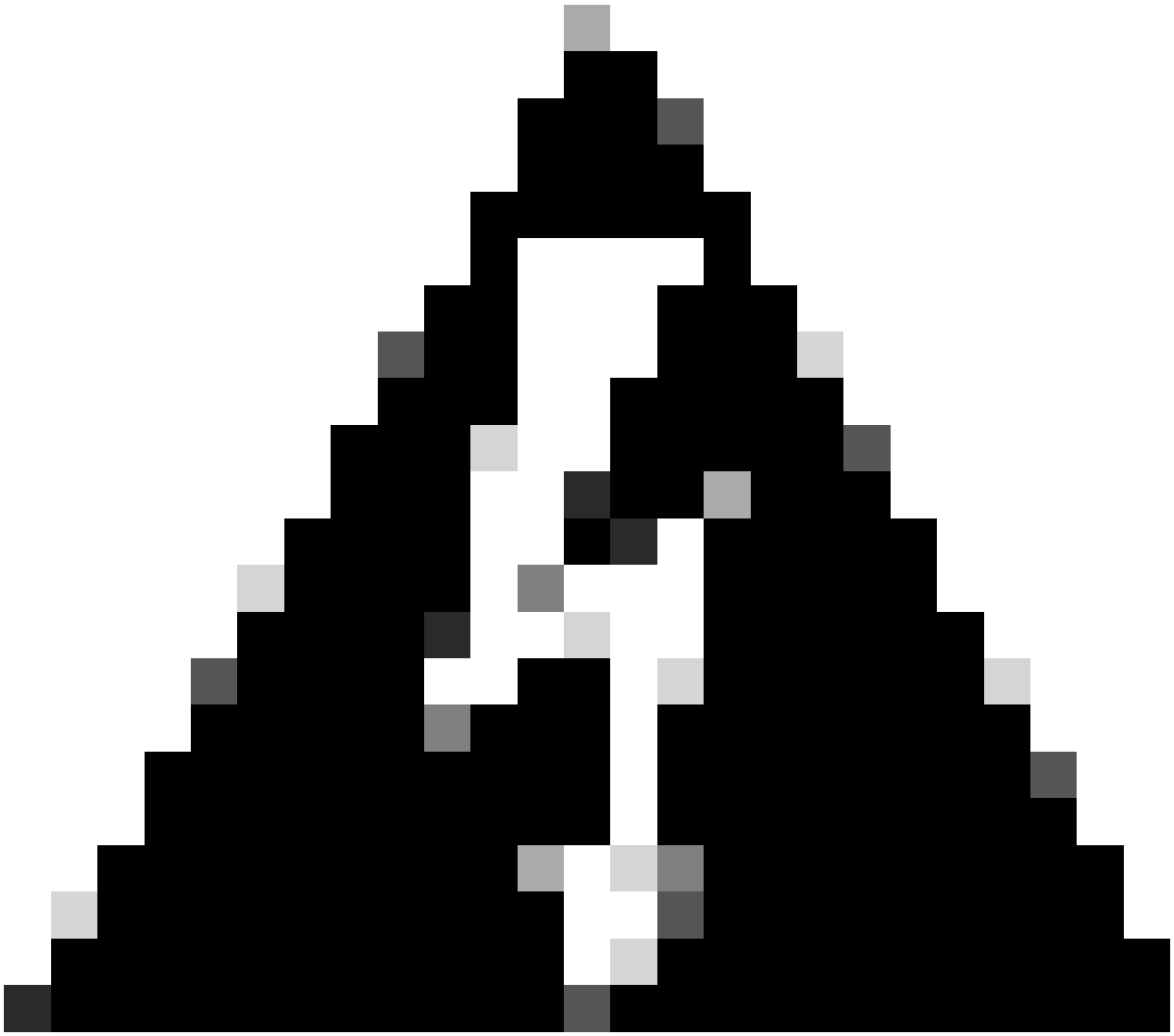
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The upgrade must be one peer at a time.

First, pause synchronization between the peers.

Then the upgrade needs to be first done in the Standby, followed by the Active FMC.



Warning: While the standby peer is working on pre-checks / installation, both peers switch to active; this is called split-brain.
It is totally expected while the upgrade. During this time, you must not make or deploy any configuration change.
If you do any configuration change, it can be lost after synchronization is restarted.

Pre-upgrade

1. Plan your upgrade path. In FMC deployments, you usually upgrade the FMC, then its managed devices. Always know which upgrade you just performed, and which is next.

2. Read all upgrade guidelines and plan configuration changes.
3. Check bandwidth. Ensure your management network has the bandwidth to perform large data transfers.

4. Schedule maintenance windows.
5. Back up the configuration before and after upgrade. **System > Tools - Back up / Restore >**

Firepower Management backup. Download the backup to your local machine.

6. Upgrade virtual hosting. This is required when you are running an older version of VMware.
7. Check configurations.
8. Check NTP synchronization.
   FMC: Choose **System > Configuration > Time**.
   Devices: Use the **show time** CLI command.

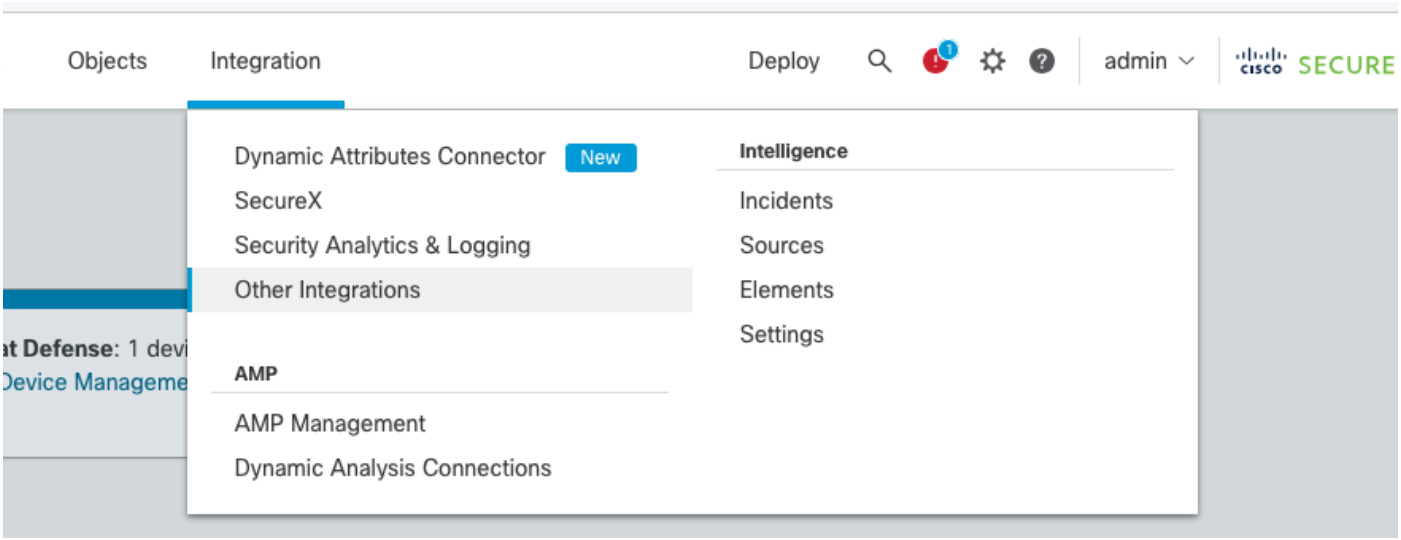
9. Check disk space.
10. Deploy configurations. In FMC high availability deployments, you only need to deploy from the active peer.
11. Check running tasks. Ensure there is no pending deployments.

Upgrade Procedure

Step 1. Pause Synchronization

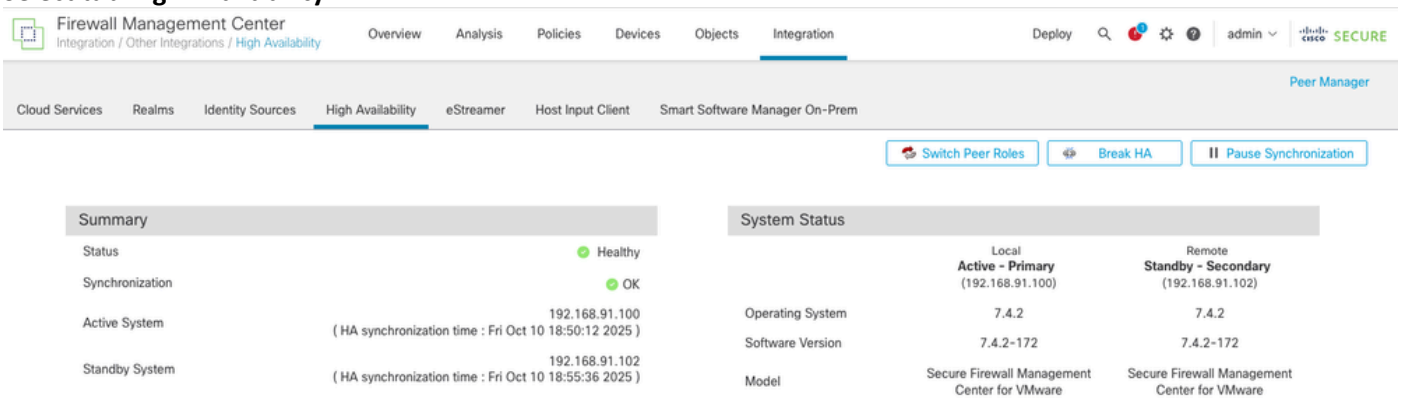
On the Primary (Active) unit, pause the **High Availability** synchronization between peers.

Integration > Other Integrations:



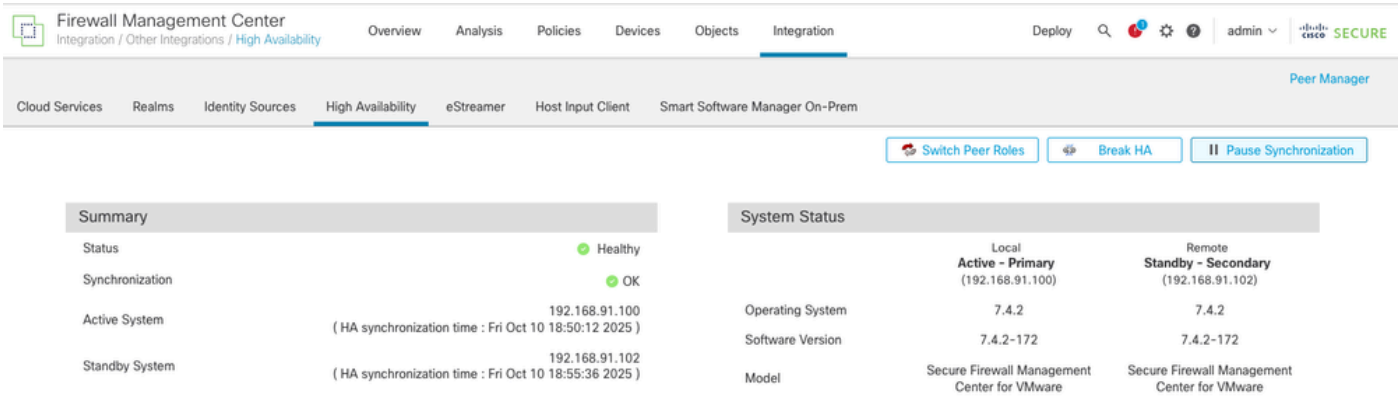
Pause Synchronization. Select Integration, Other Integration, High Availability

Select tab **High Availability**:



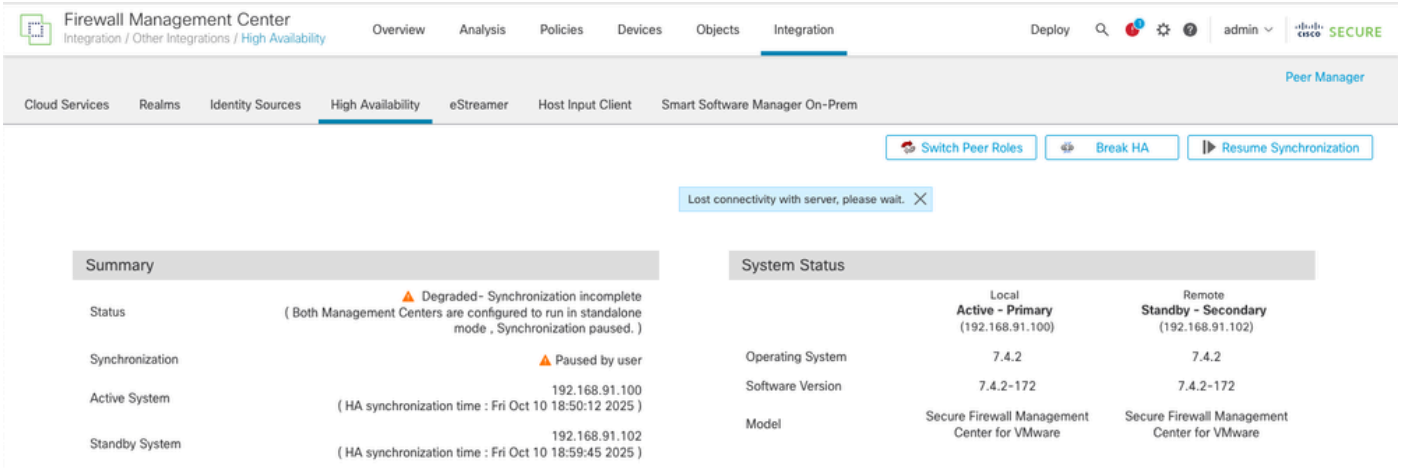
FMC High Availability section

Select **Pause Synchronization**:



Select Pause Synchronization

Wait for the synchronization to be paused. Status must be paused by user when complete.

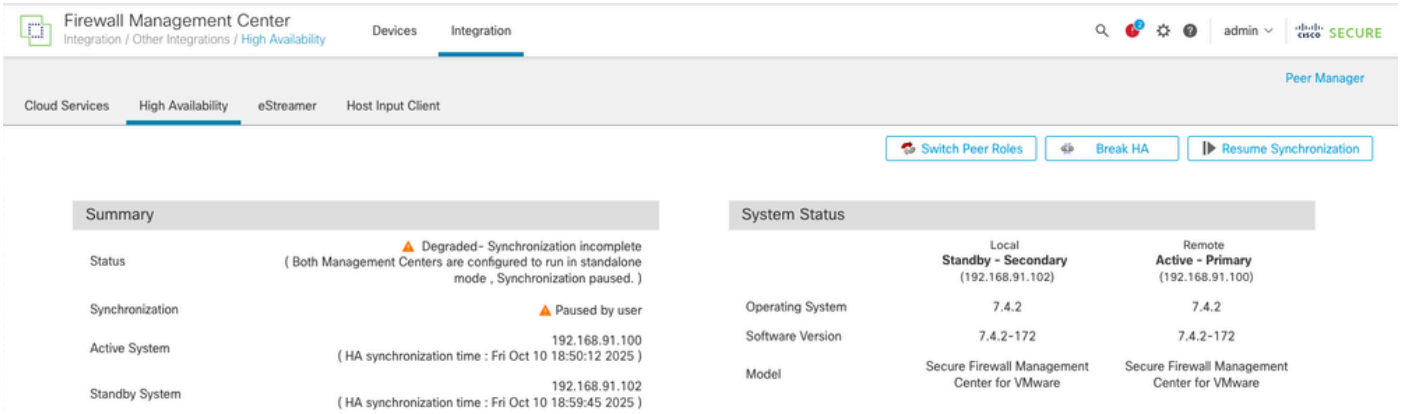


Alert on Degraded Synchronization. Paused by user

Step 2. Upload the Upgrade Package

Log in to the Secondary (Standby) unit, confirm the synchronization is paused.

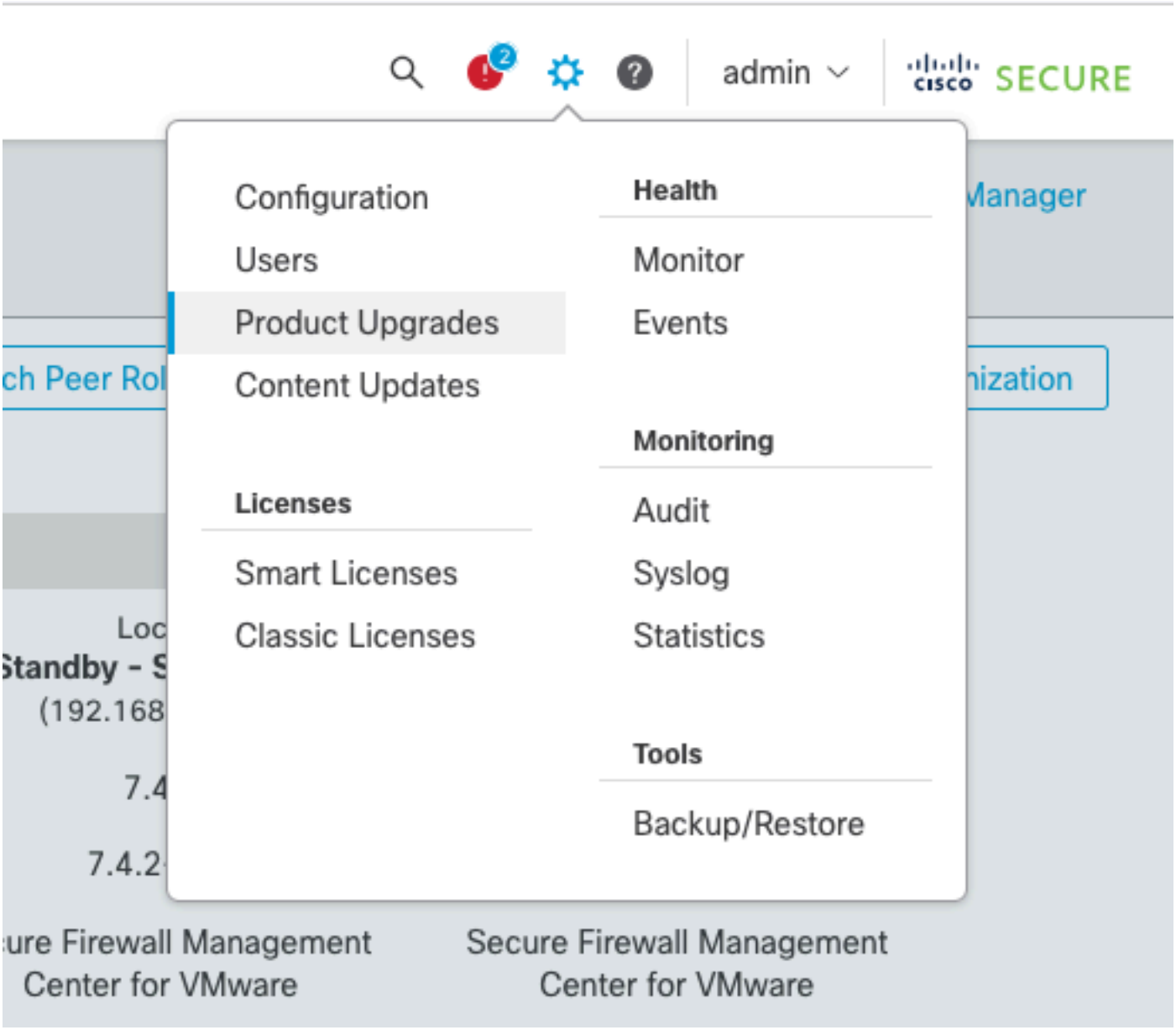
Integration > Other Integrations > High Availability:



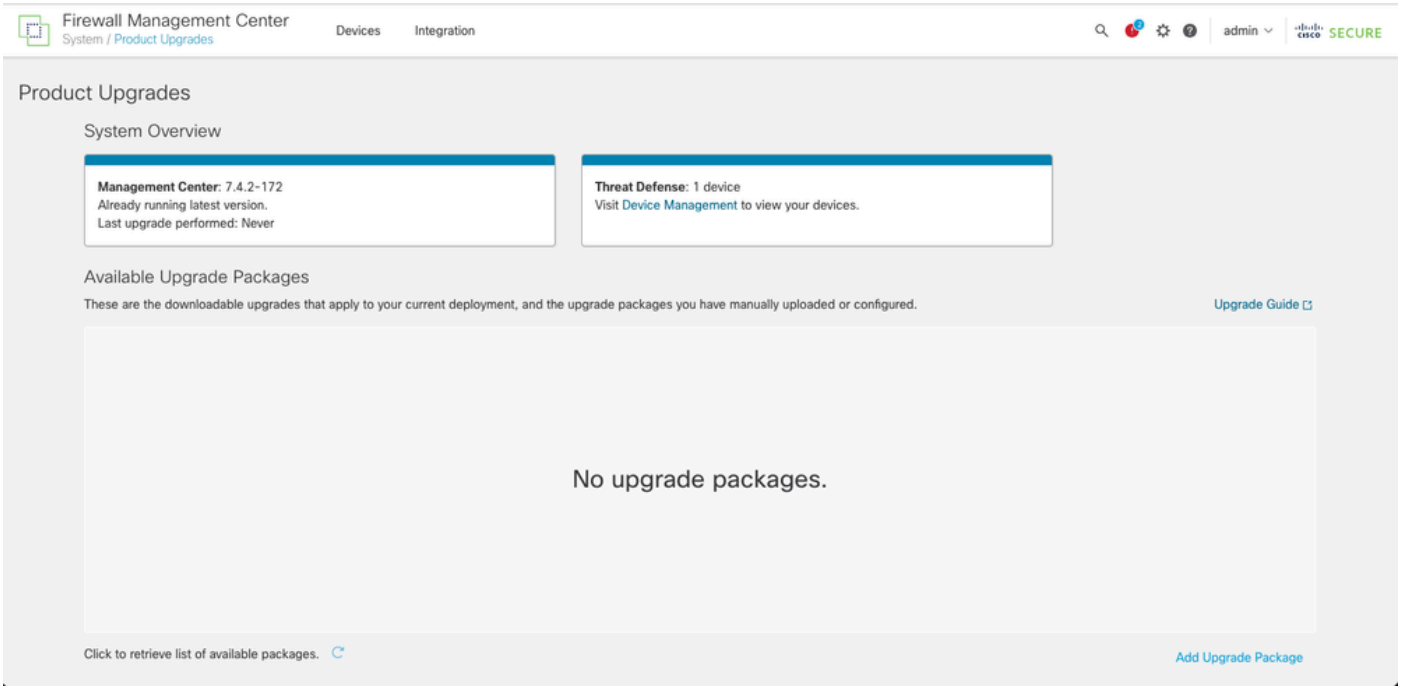
On Standby Unit. Synchronization Paused by User

Once confirmed, continue to upload the upgrade package.

System > Product Upgrade:

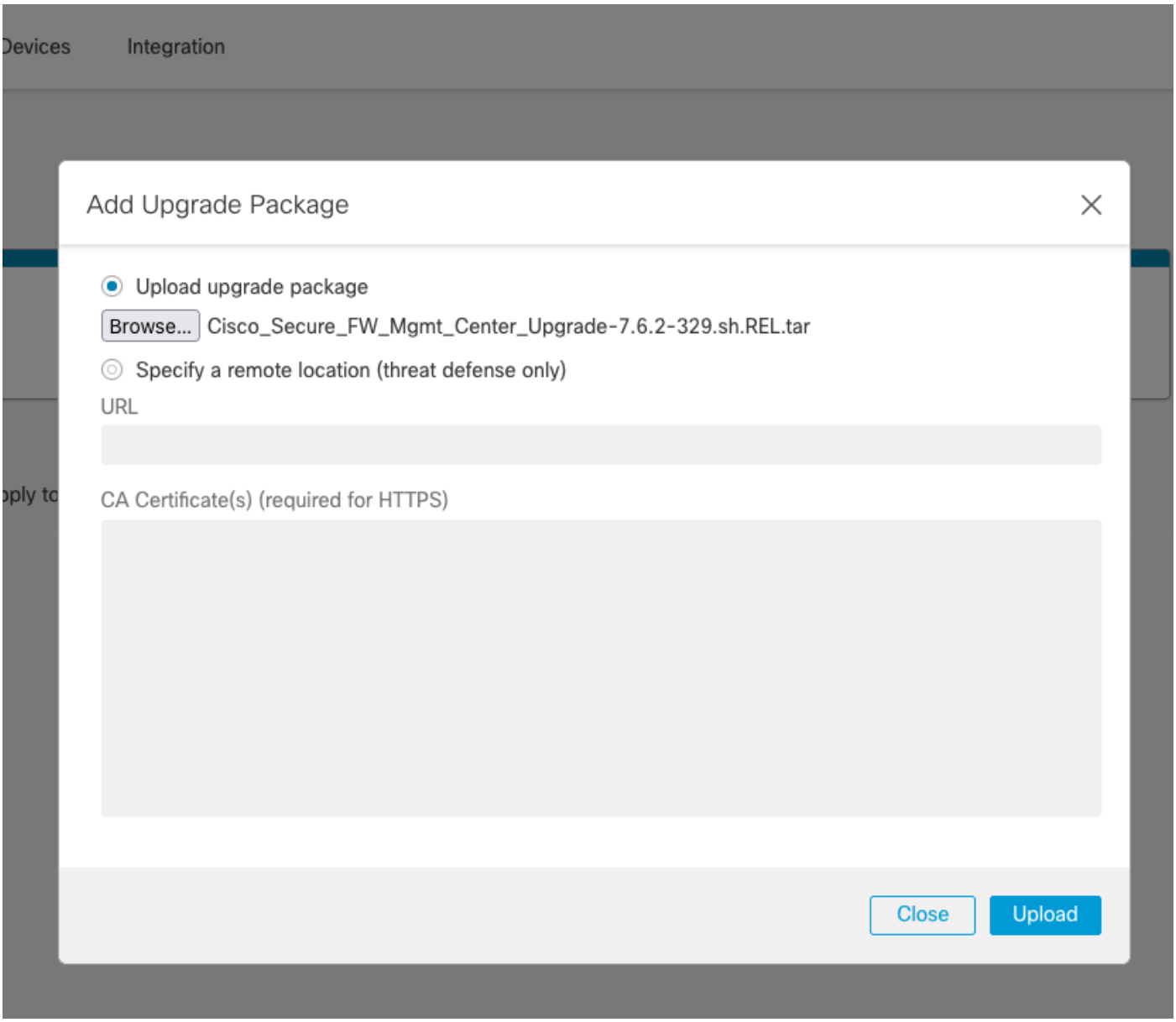


System, Product Upgrades



Select Upgrade Package

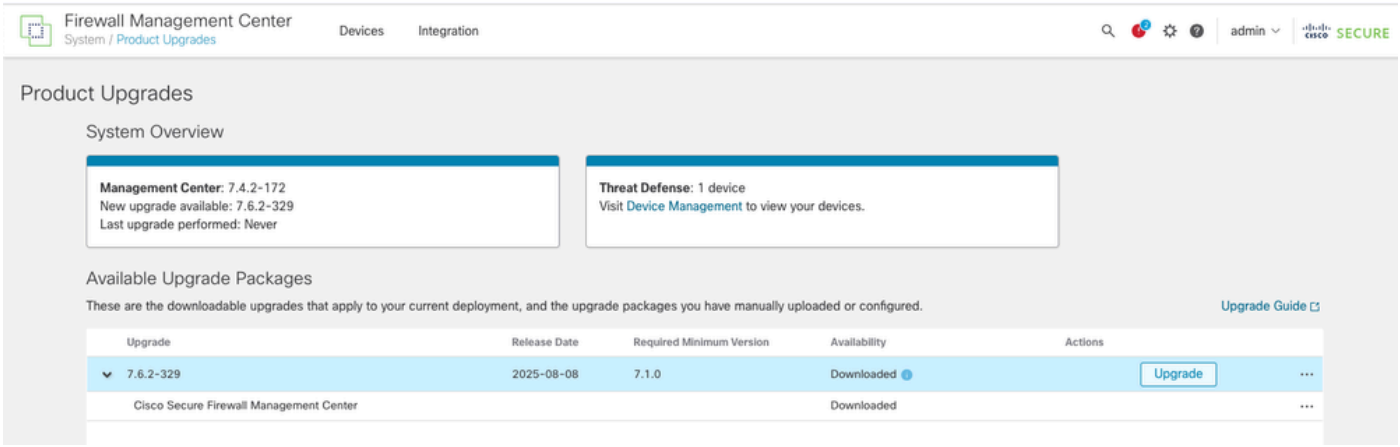
Browse the previously downloaded package of the version to be upgraded.



Browse Upgrade Package, select Upload

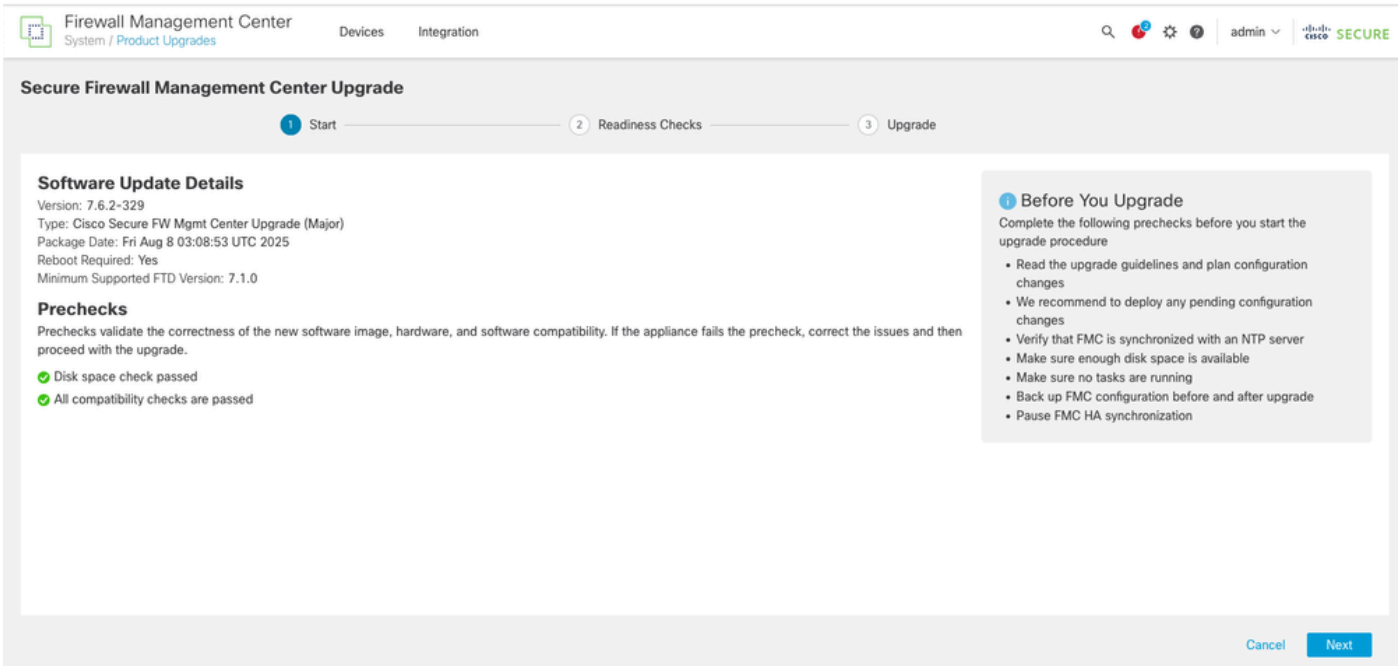
Step 3. Readiness Check

On the Available Upgrade Packages list, select the desire version. Proceed with **Upgrade** option:



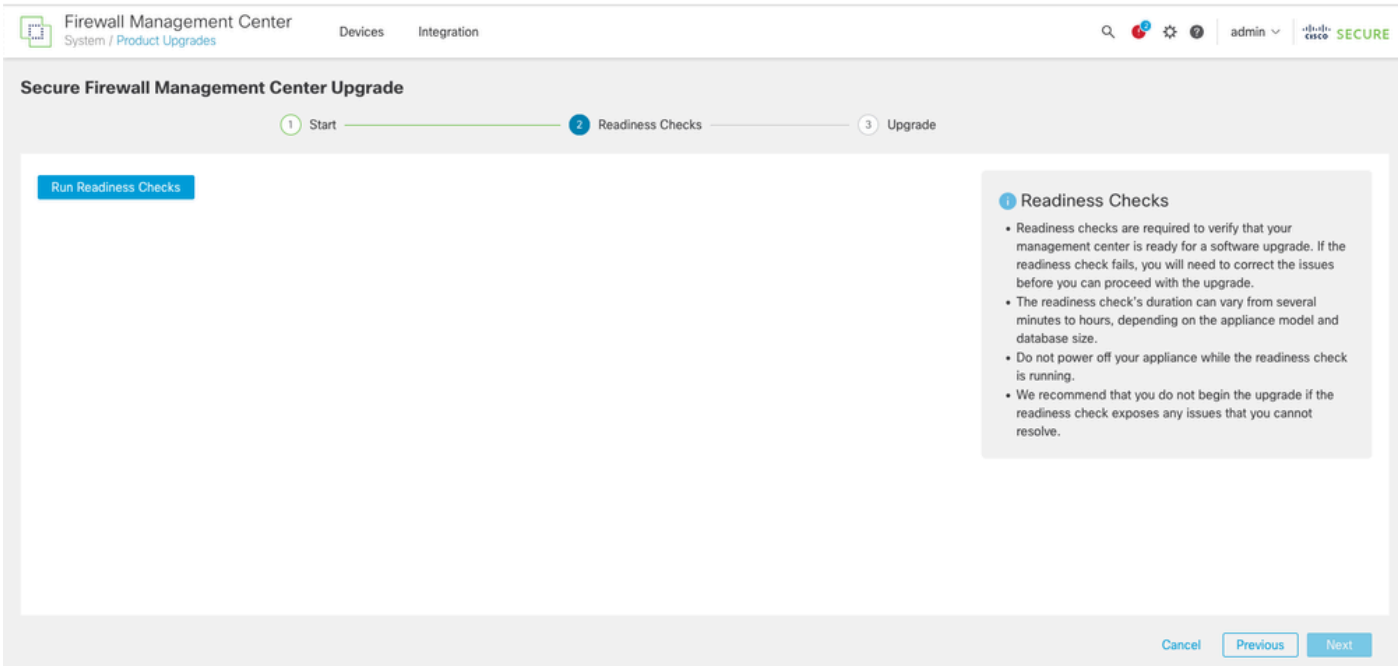
Available Upgrade Packages. Proceed with Upgrade

Select **Next** when Pre-checks validation is complete:



Precheck Validation

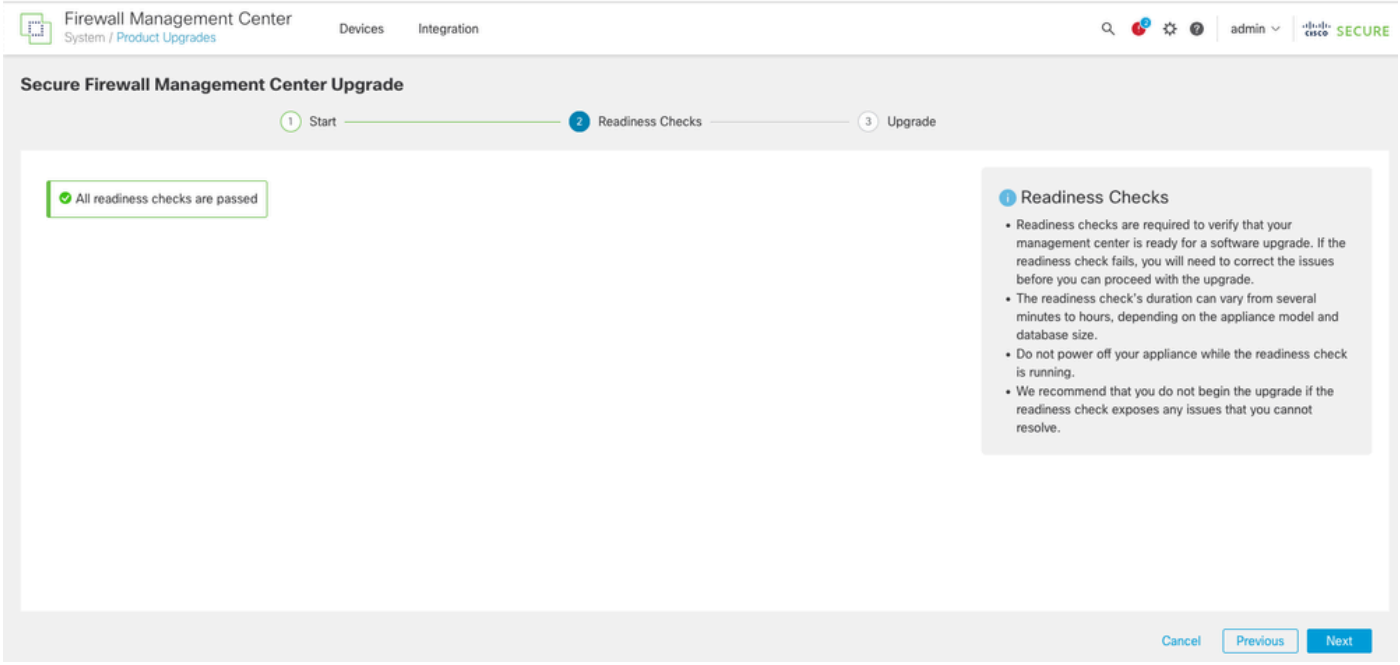
Click **Run Readiness Check**, the process must start on the appliance to be upgraded:



Run Readiness Checks

Once completed, you can see the status in the Readiness Check Results.

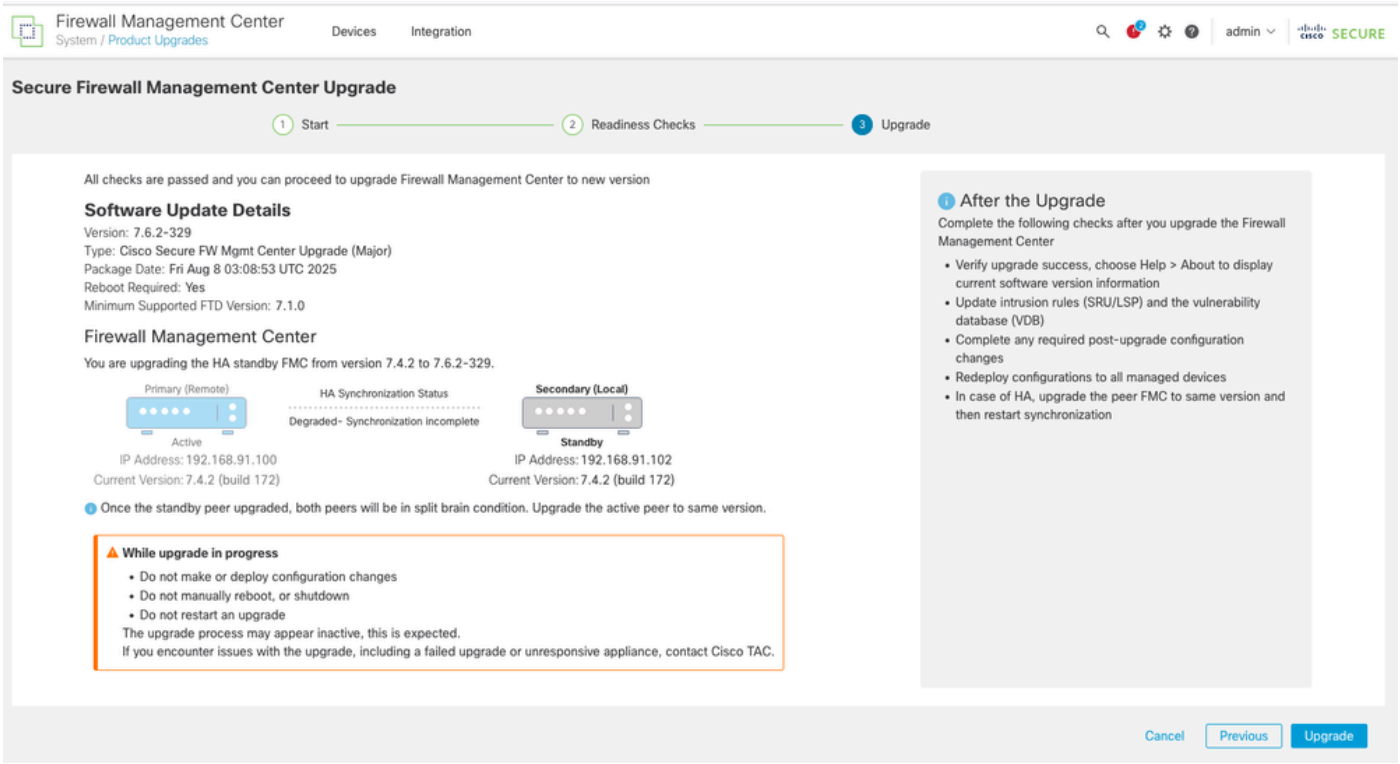
If successful, then you can select **Next**:



Readiness check passed, Select Next

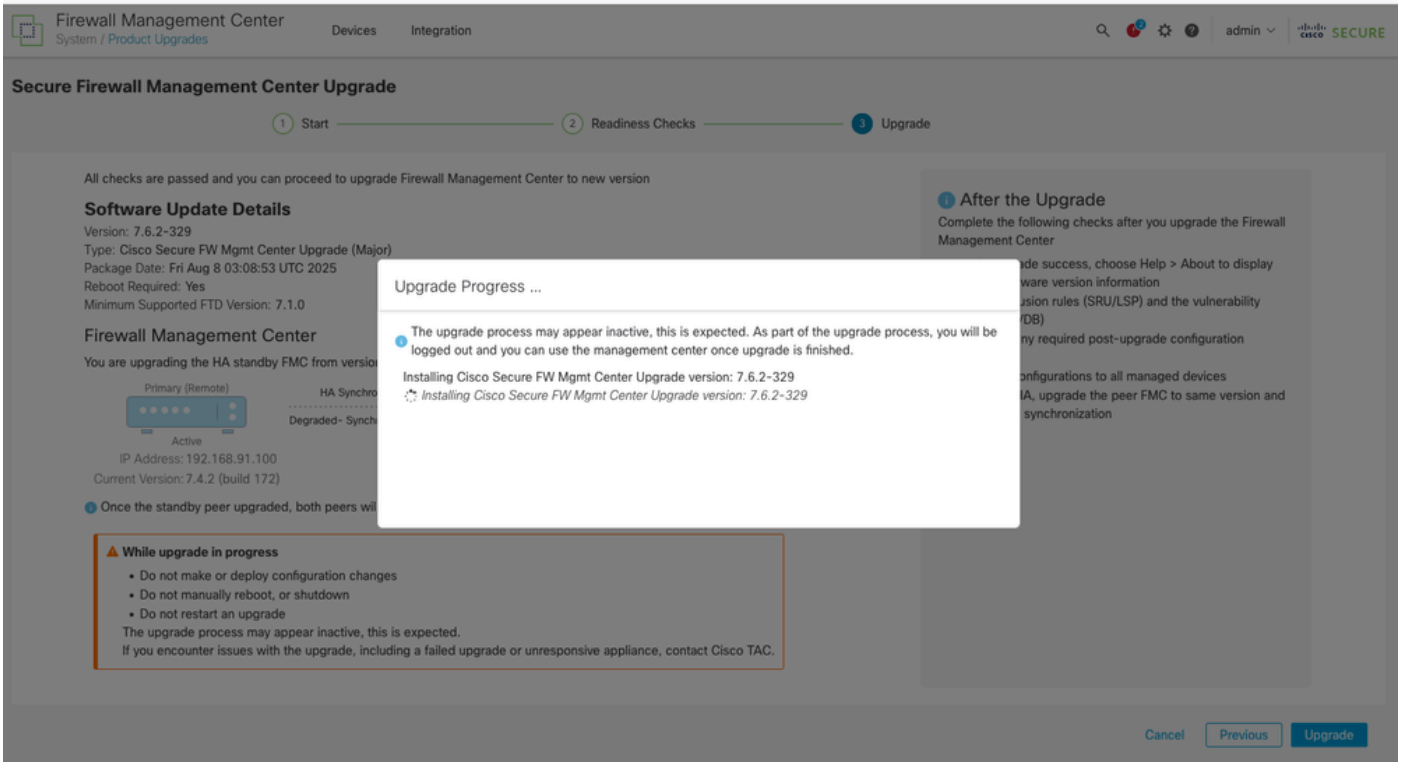
Step 4. Upgrade the FMC

Select **Upgrade** to start with upgrade process:



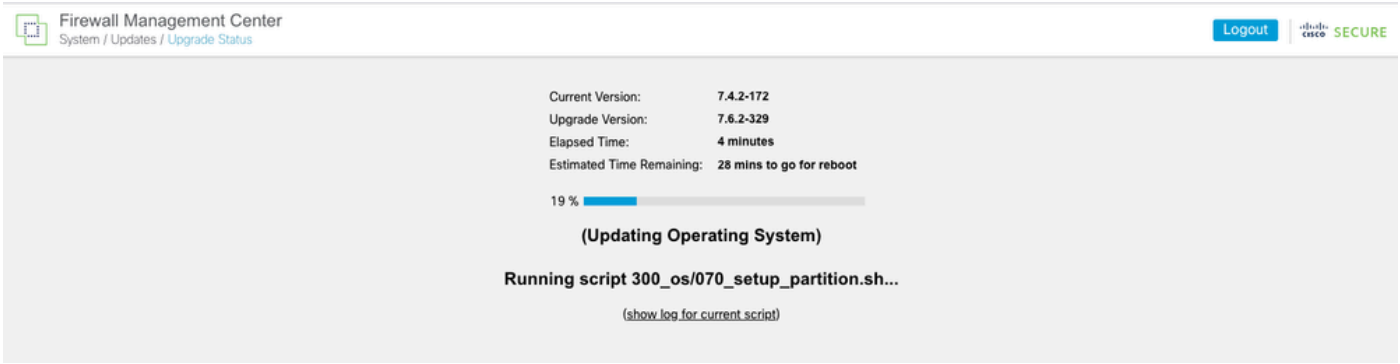
Start Upgrade

Upgrade progress can be seen on the FMC site:

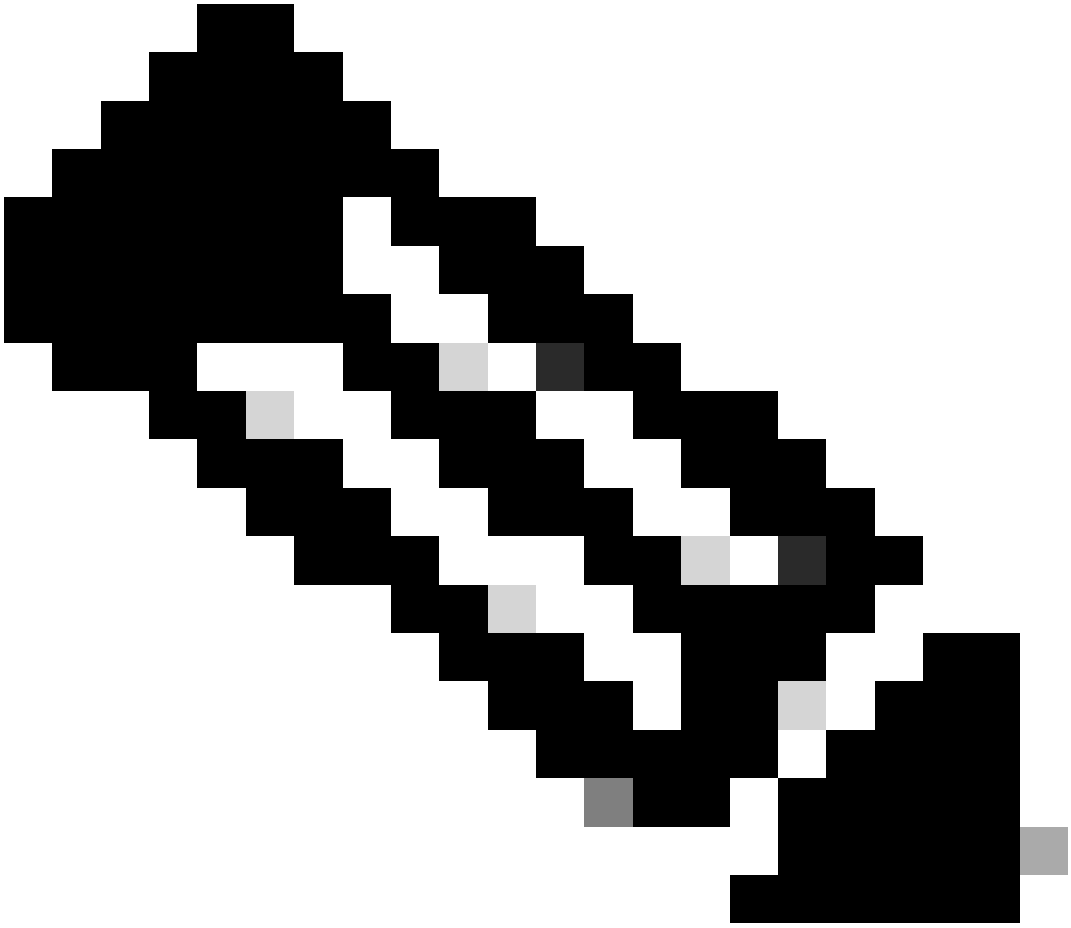


Upgrade Progress

The GUI can be logged out, log in again and the progress of the upgrade is displayed:



Upgrade progress in GUI



Note: Installation takes around 30 minutes to complete.

If you have CLI Access, progress can be checked in upgrade folder /var/log/sf; move to **expert mode** and enter **root access**.

```
> expert
admin@firepower:~$ sudo su
Password:
root@firepower:/Volume/home/admin# cd /var/log/sf/

root@firepower:/var/log/sf# ls
Cisco_Secure_FW_Mgmt_Center_Upgrade-7.6.2

root@firepower:/var/log/sf/Cisco_Secure_FW_Mgmt_Center_Upgrade-7.6.2# ls
000_start  AQ_UUID  DBCheck.log  exception.log  flags.conf  main_upgrade_script.log  status.log  status

root@firepower:/var/log/sf/Cisco_Secure_FW_Mgmt_Center_Upgrade-7.6.2# tail -f status.log
```

When the upgrade completes, the FMC reboots.

```
ui:[100%] [1 mins to go for reboot]Running script 999_finish/999_zzz_complete_upgrade_message.sh...
ui:[100%] [1 mins to go for reboot] Upgrade complete
ui:[100%] [1 mins to go for reboot] The system will now reboot.
ui:System will now reboot.

Broadcast message from root@firepower (Fri Oct 10 20:23:08 2025):

System will reboot in 5 seconds due to system upgrade.

Broadcast message from root@firepower (Fri Oct 10 20:23:13 2025):

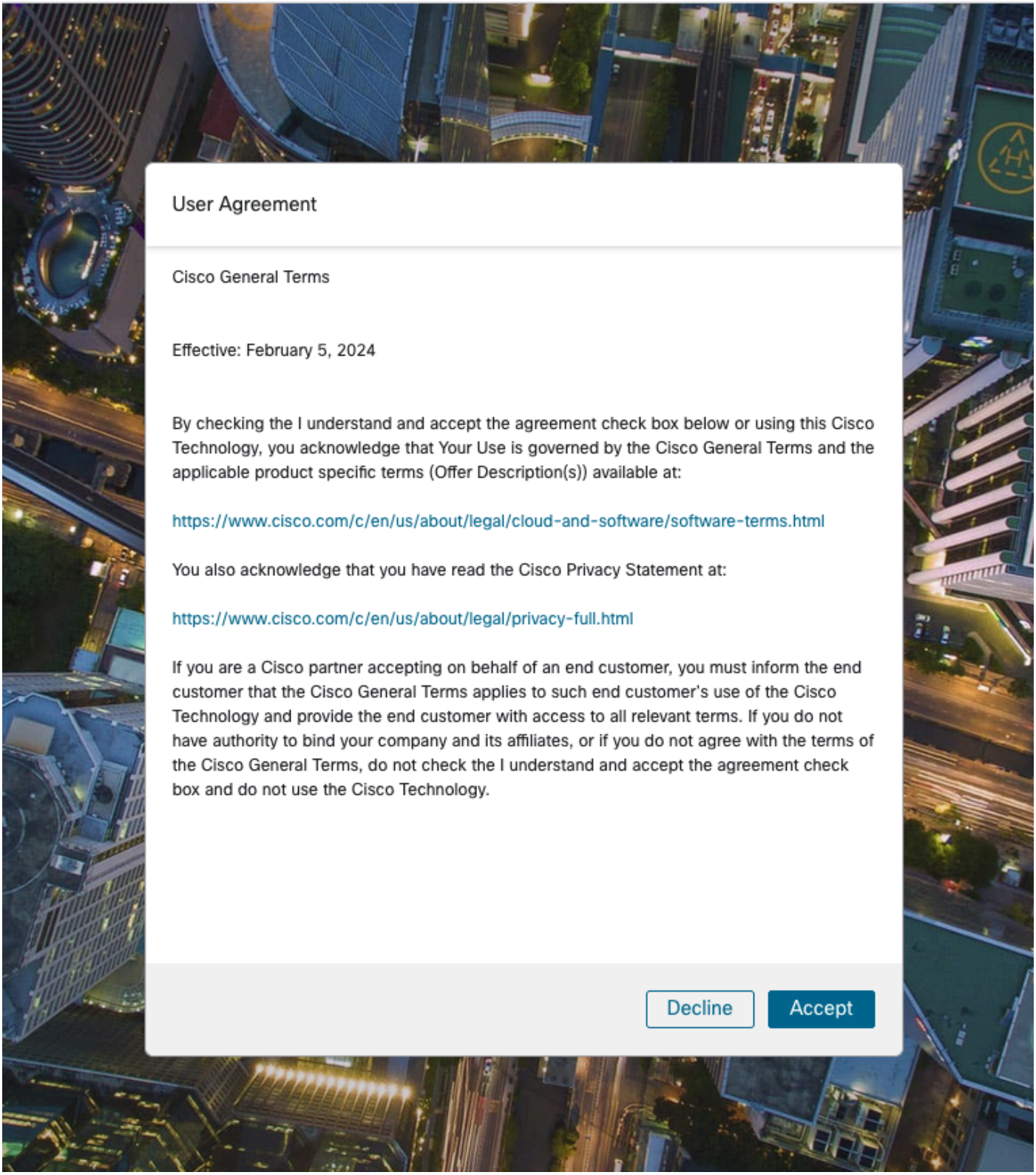
System will reboot now due to system upgrade.

ui:[100%] [1 mins to go for reboot] Installation completed successfully.
ui:Upgrade has completed.
state:finished

Broadcast message from root@firepower (Fri Oct 10 20:23:25 2025):

The system is going down for reboot NOW!
```

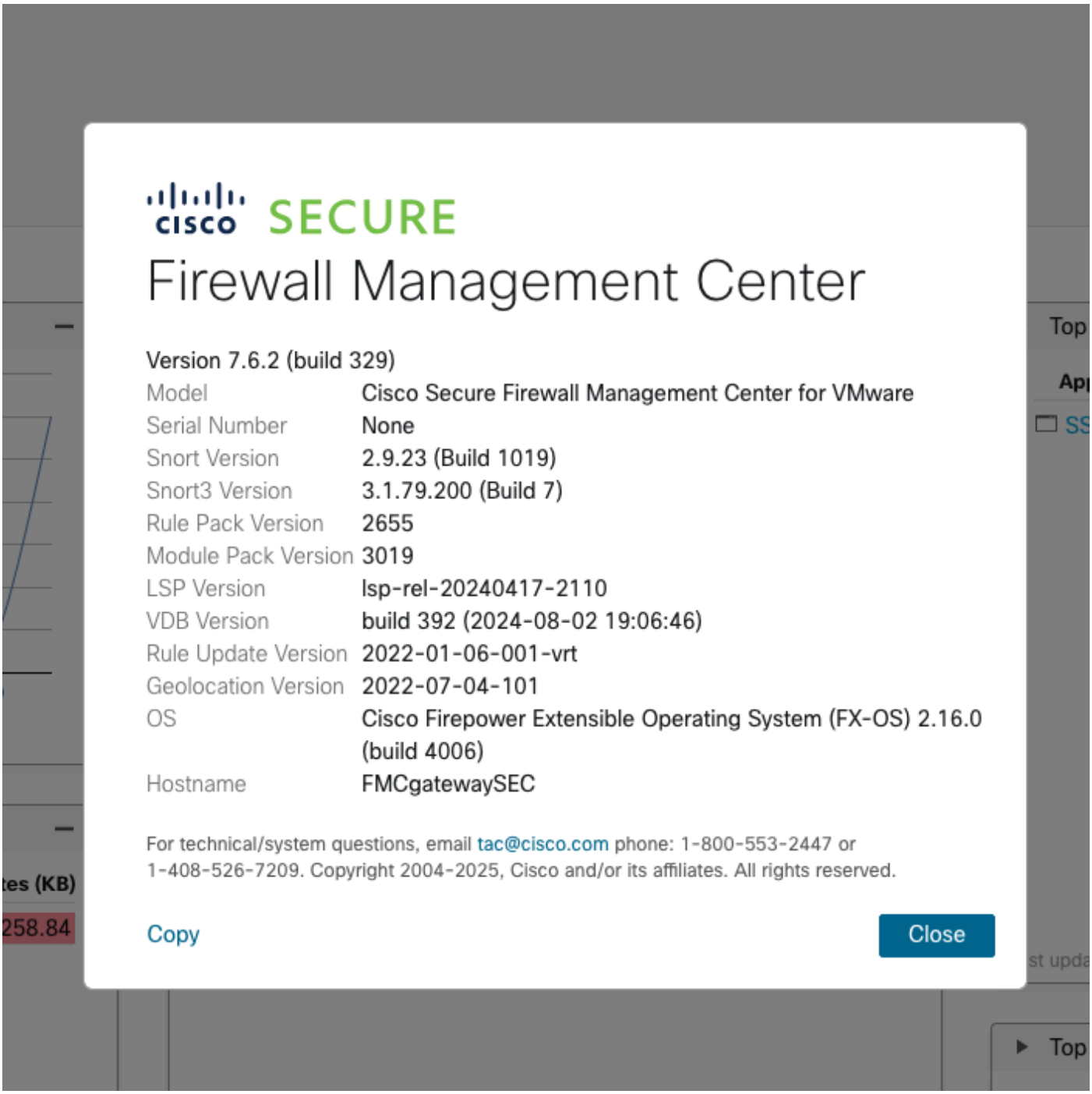
After reboot, log back in to the FMC GUI, Accept the User Agreement:



Accept the User Agreement

The new version can be confirmed on FMC.

Help > About:



New version confirmation

In the CLI, the version can be checked after accepting the User Agreement.

```
Copyright 2004-2025, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

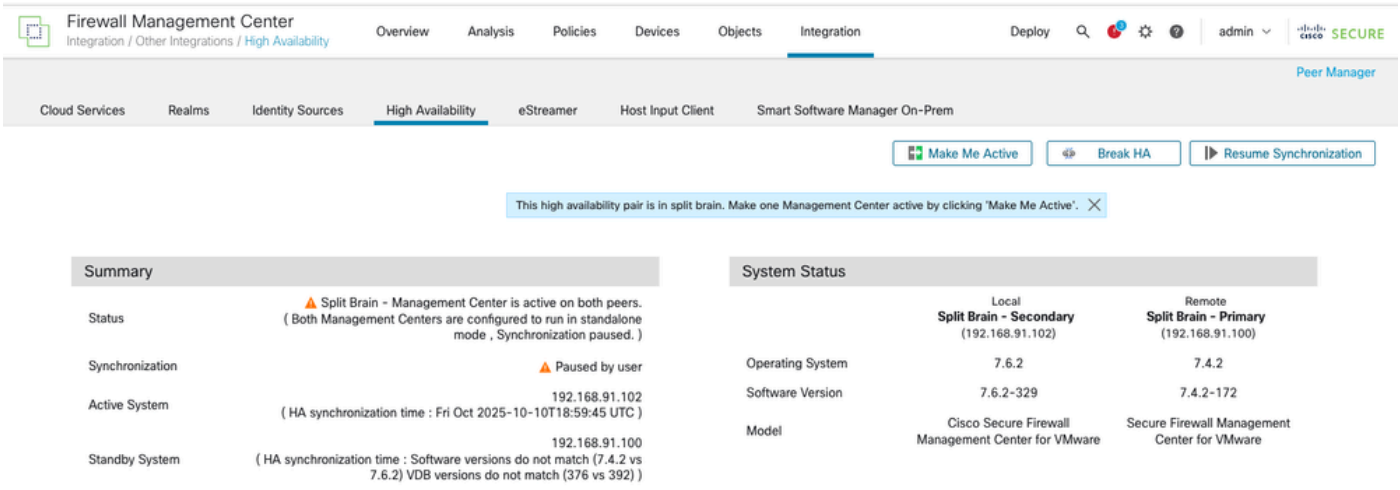
Cisco Firepower Extensible Operating System (FX-OS) v2.16.0 (build 4006)
Cisco Secure Firewall Management Center for VMware v7.6.2 (build 329)

>
> show version
-------------------[ firepower ]--------------------
Model                     : Secure Firewall Management Center for VMware (66) Version 7.6.2 (build 329)
```

```
UUID                        : 1c71ae24-1e60-11ed-8459-9758e19f1a24
Rules update version        : 2022-01-06-001-vrt
LSP version                 : lsp-rel-20240417-2110
VDB version                 : 392
----------------------------------------------------
```

FMC High Availability after the upgrade goes to Split Brain, Local peer (Secondary) is now a completed upgrade.

Integration > Other Integration > High Availability:

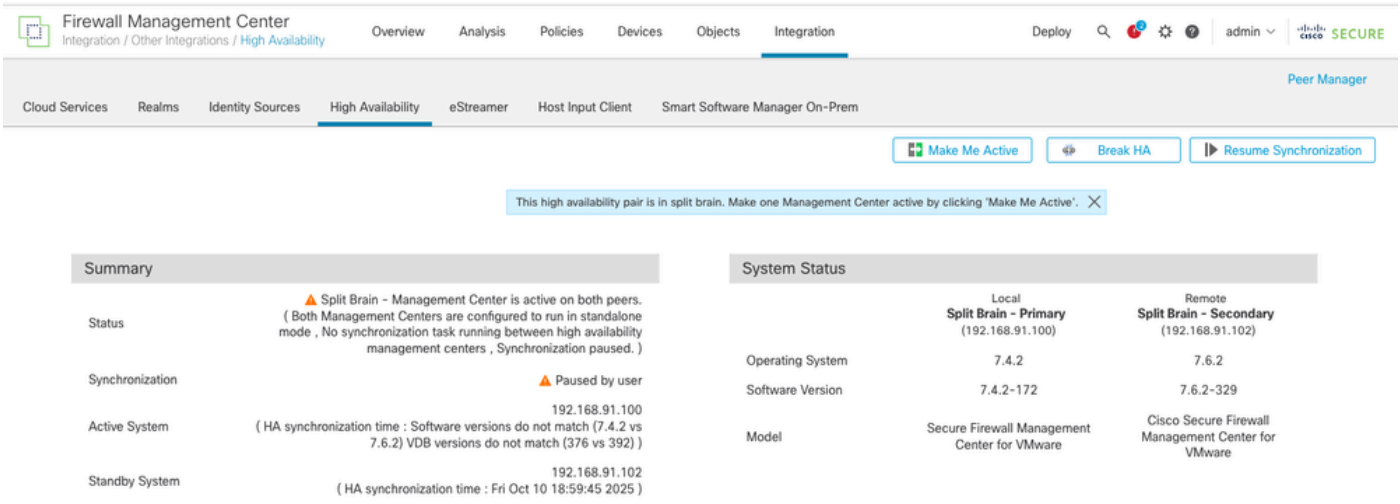


Split Brain in High Availability

Step 5. Upgrade Primary (Active) Peer

Sign in to the Primary Unit, confirm that the Local peer is the one with the oldest version.

Integration > Other Integration > High Availability:



Confirm Local Peer Version

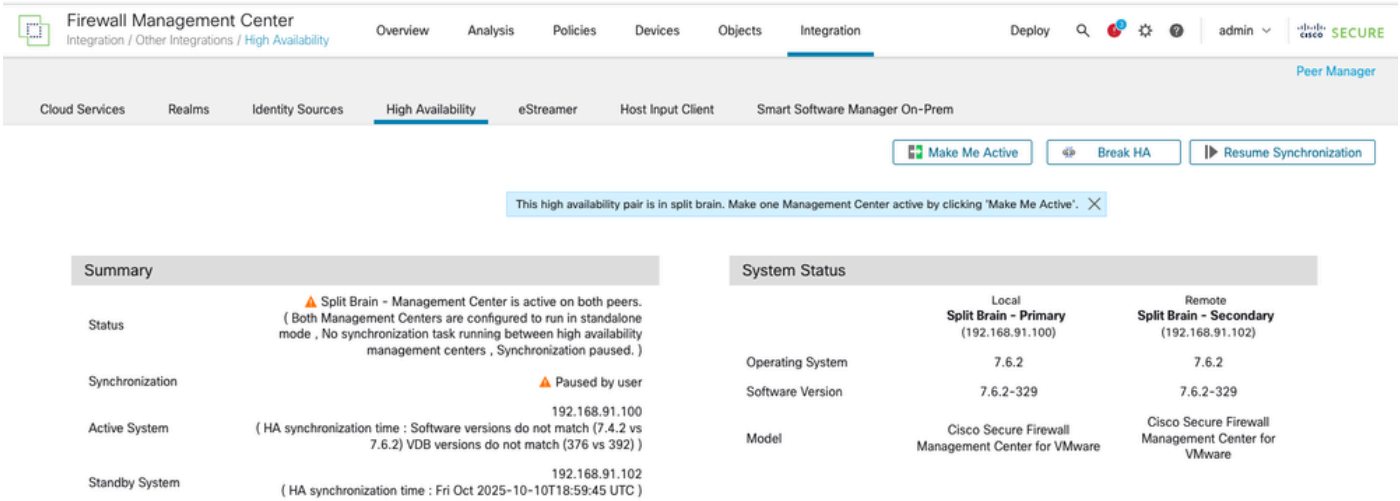
Repeat Steps two to four in this peer:

1. Upload the Upgrade Package.
2. Readiness Check.
3. Upgrade device.

Step 6. Make the Desired FMC Active

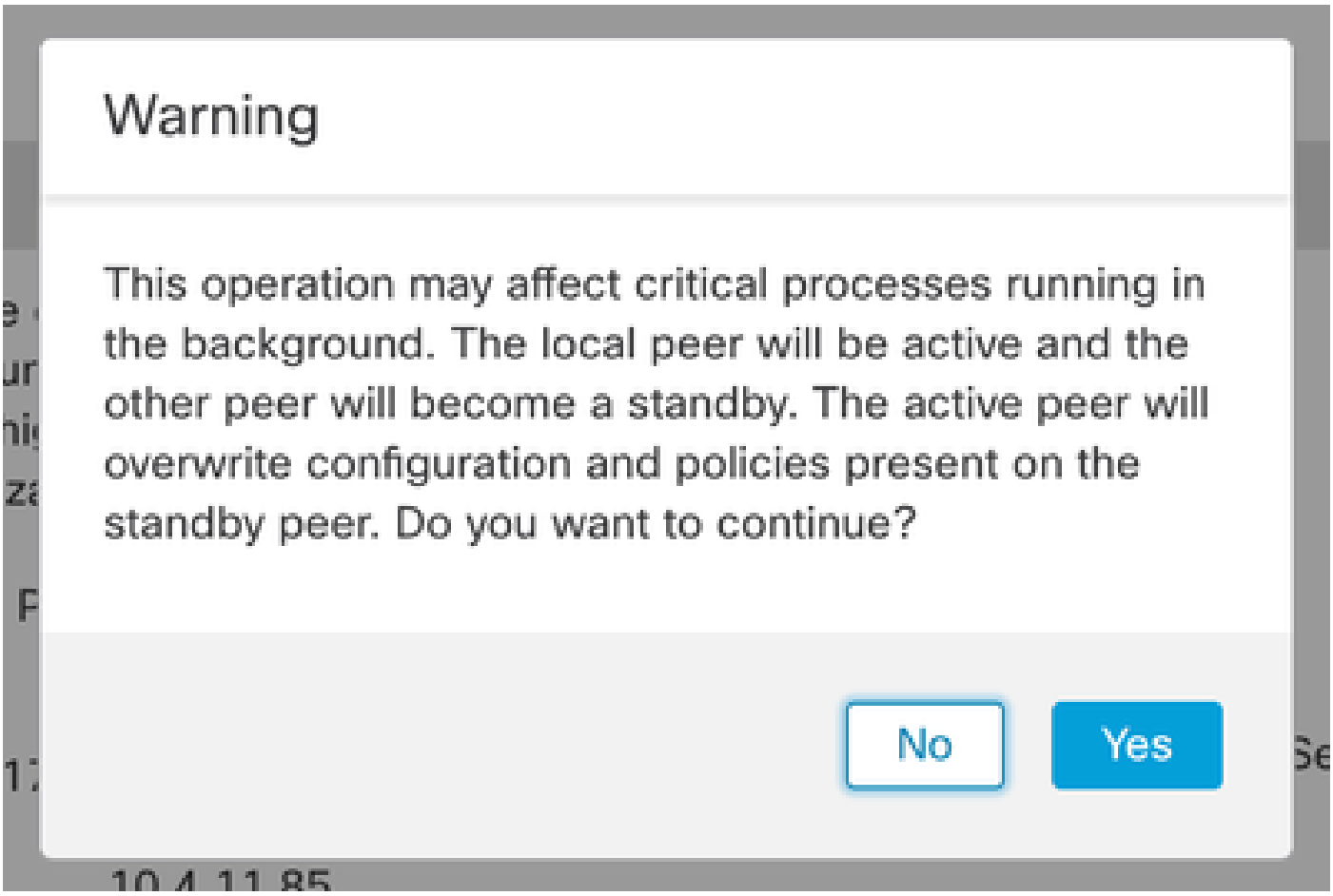
After the upgrade has been completed on both FMC, log in to the FMC that you want to make the Active unit and select the option **Make Me Active**.

Integration > High Availability > Make Me Active:

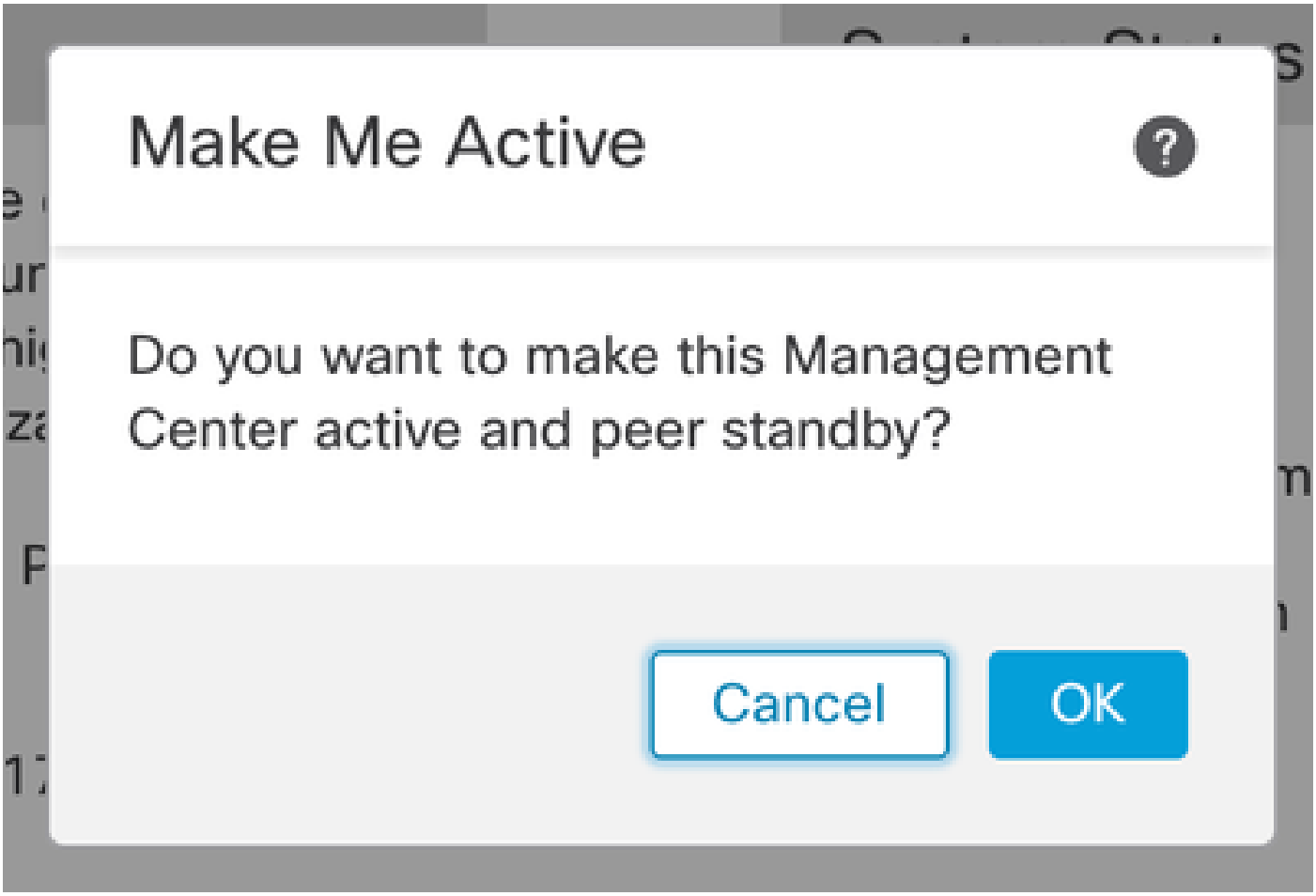


Select the desire unit to be Active

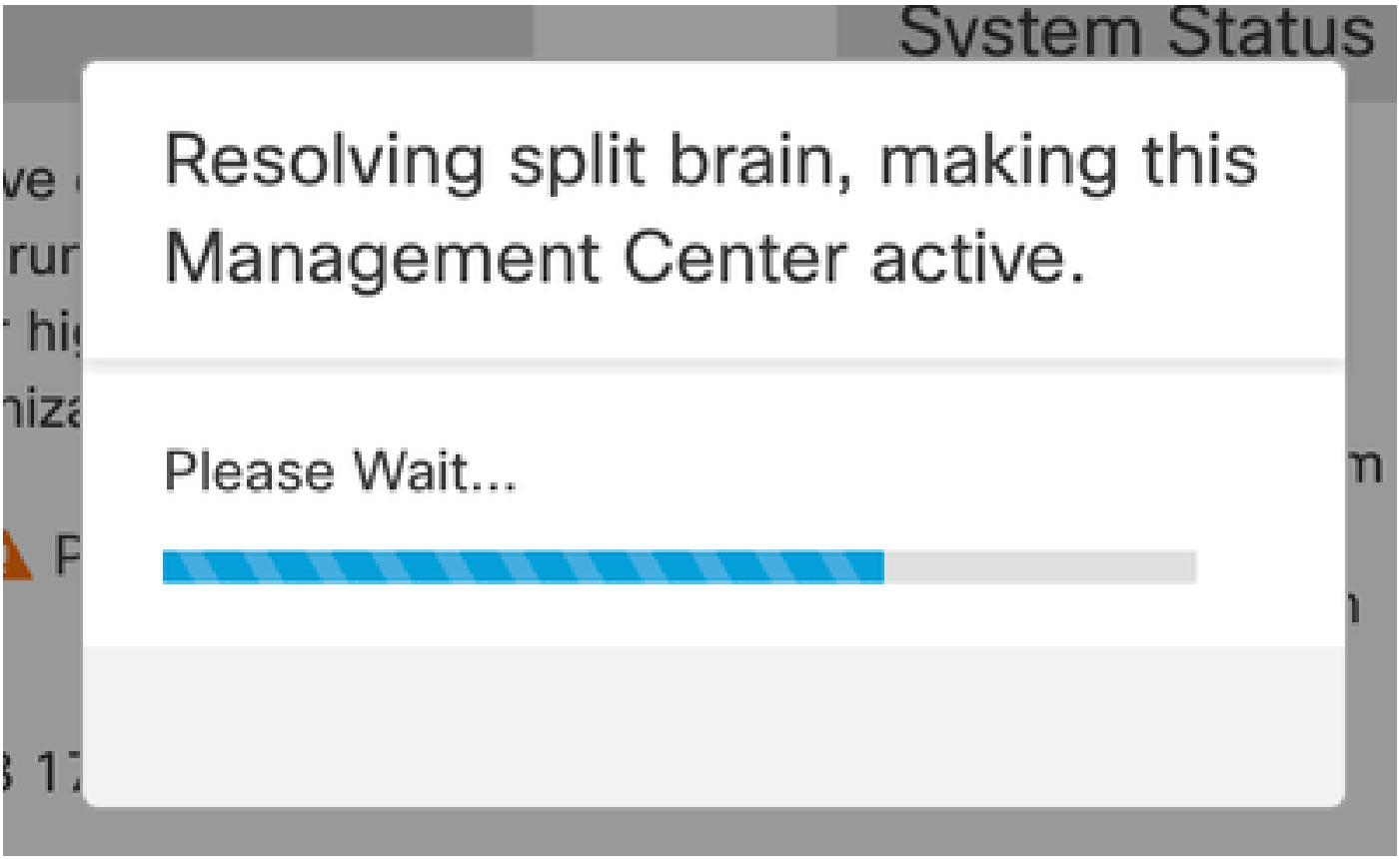
Warnings about processes and overwrite any configuration done in the standby peer, select **YES** to continue.



Warning About Active Overwriting Configuration on Standby Peer

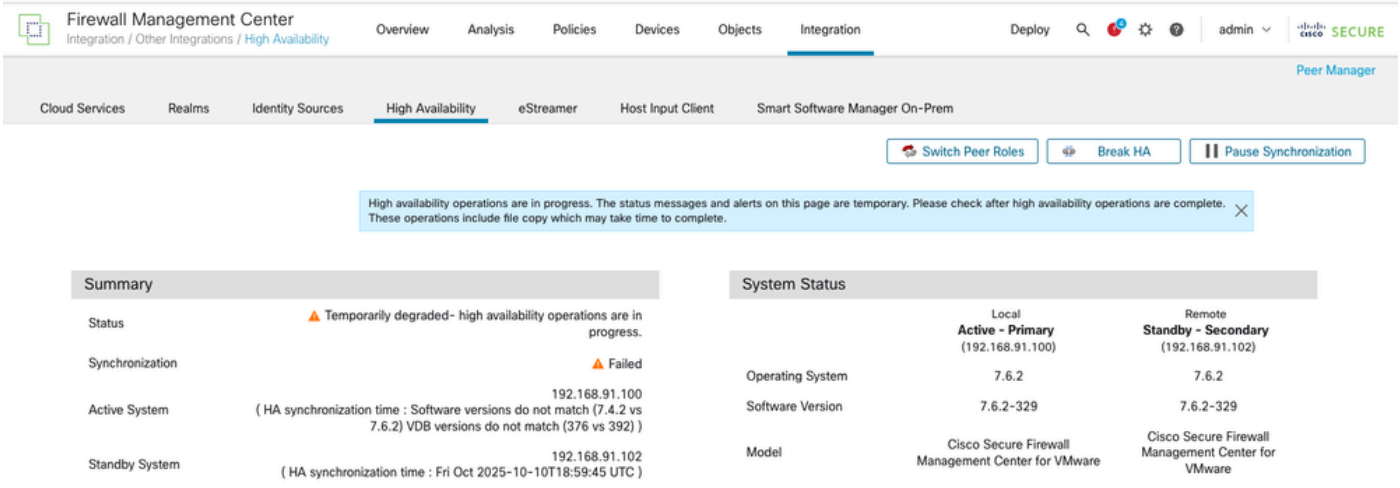


Select OK

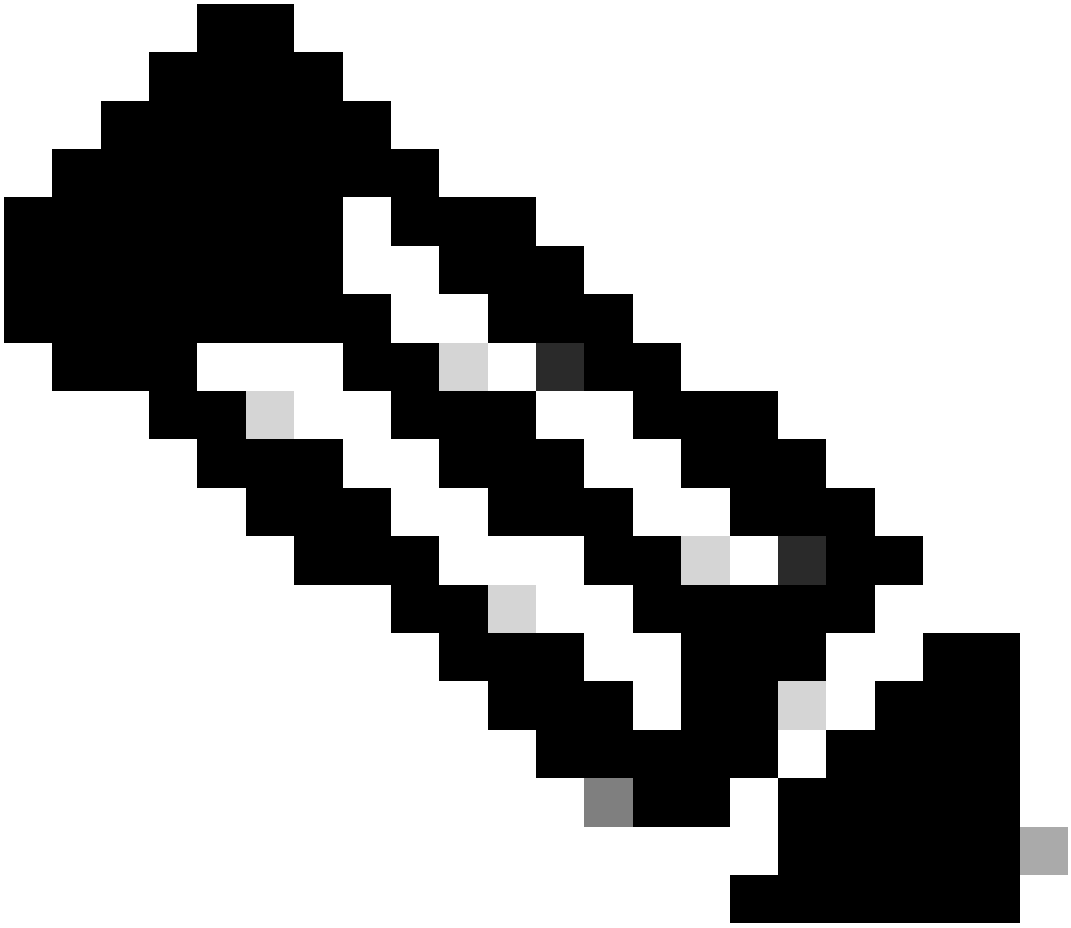


Resolving Split Brain

Wait until synchronization is complete. Remote peer must appear as Standby.



High Availability Temporarily Degraded



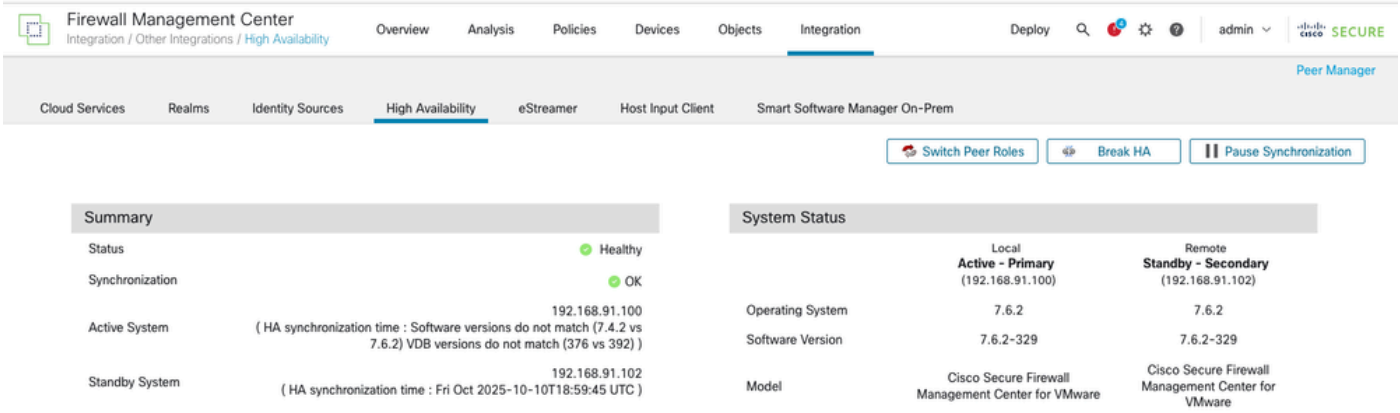
Note: Synchronization can take up to 20 minutes to complete.

Deploy pending changes on the FMC Active unit to complete upgrade process.

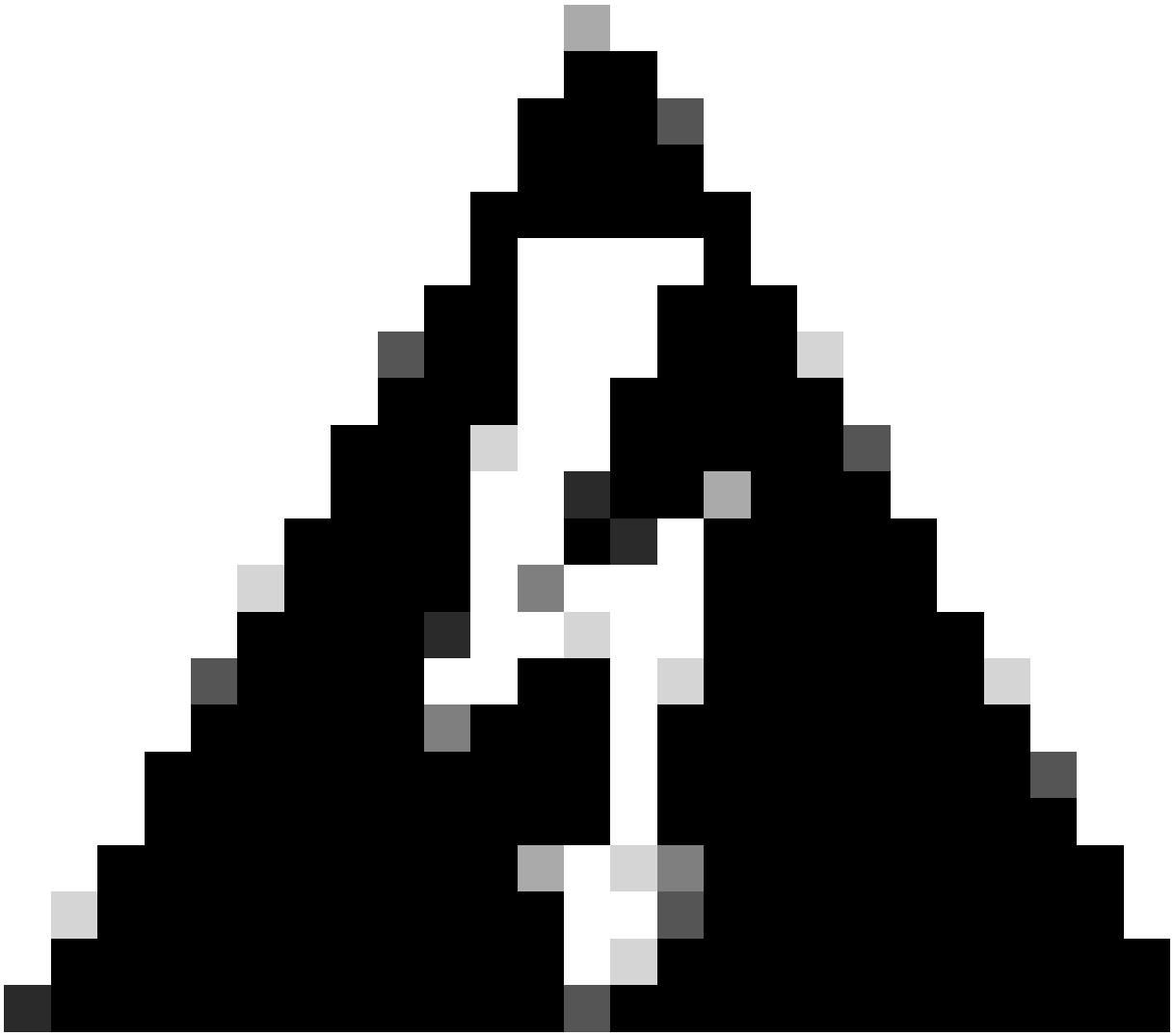
Validation

After both FMC are in the same version and synchronization has completed, HA Summary tab must look like this.

Integration > Other Integration > High Availability:



Synchronization complete



Warning: If the final synchronization status shows degraded or other result than OK, please contact TAC.
