Configure High Availability on FMC

Contents

Introduction

This document describes a configuration example of High Availability (HA) on a Firewall Management Center (FMC).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Secure FMC for VMware v7.2.5.

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

Specific requirements for this document include:

- Both FMC peers are required to be on the same software version, intrusion rule update, vulnerability database, and Lightweight Security Package
- Both FMC peers are required to have the same capacity or hardware version
- Both FMCs require a separate license

For a full set of requirements, you can visit the Administration Guide.

Warning: If there is a mismatch in the requirements listed, you cannot configure HA.

This procedure is supported on all hardware appliances.

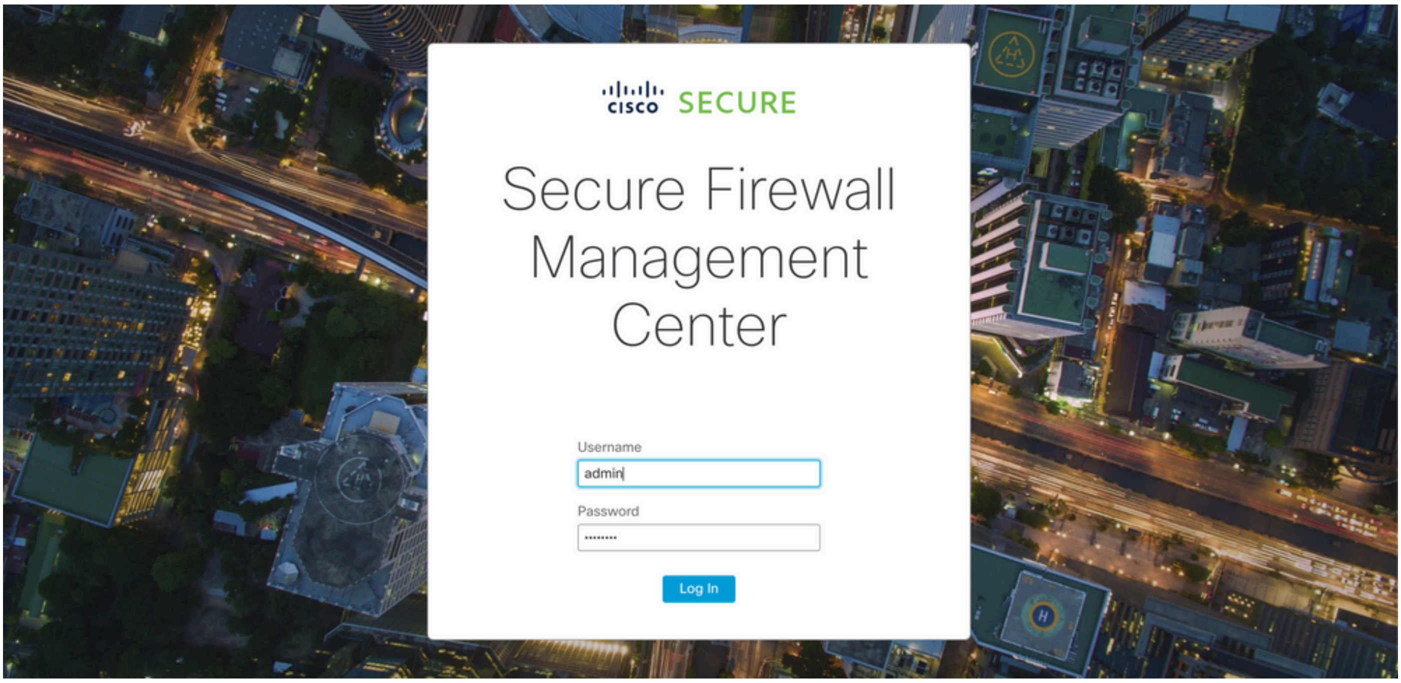
Before You Begin

- Ensure administrator access to both FMCs
- Ensure connectivity between management interfaces
- Take a moment to review software versions and ensure that all the necessary upgrades are done

Configure

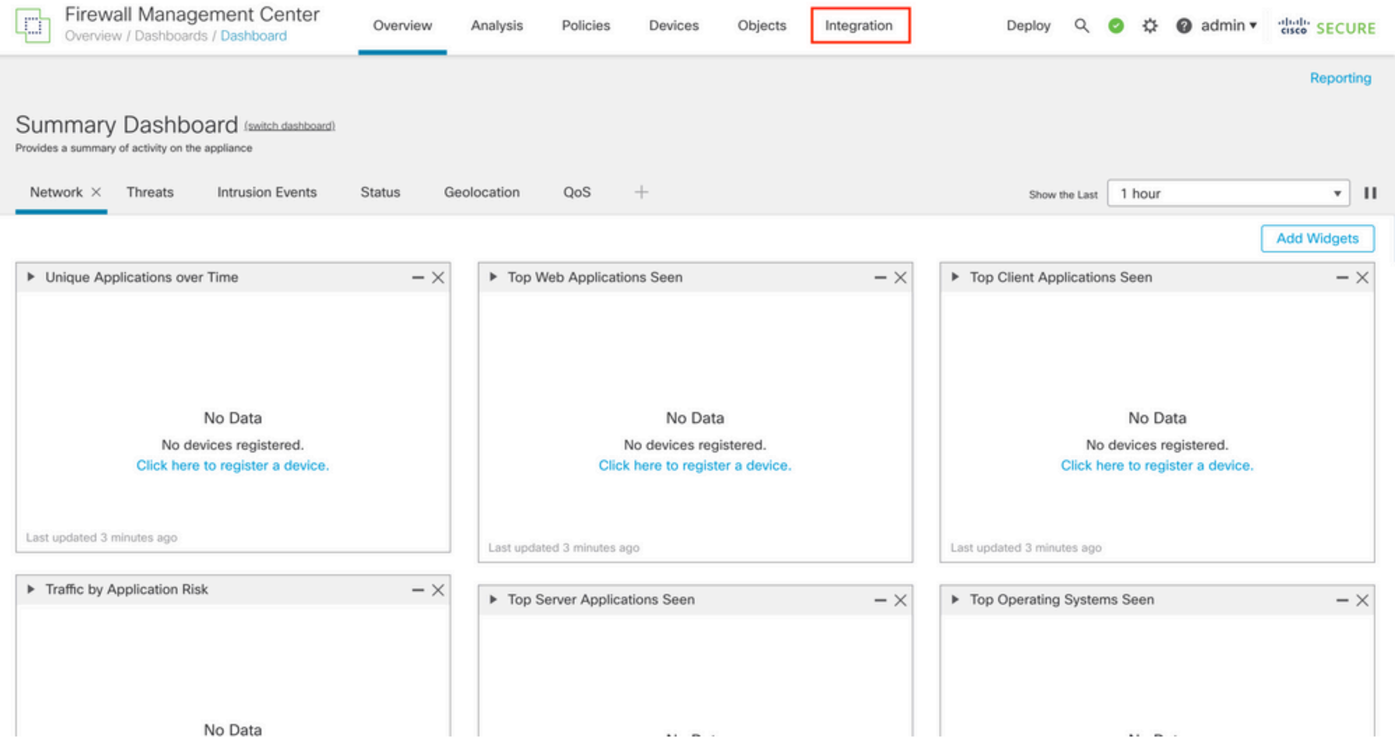
Configure Secondary FMC

Step 1. Log in to the Graphical User Interface (GUI) of the device of the FMC that is going to take the role of Secondary/Standby.



Log in to FMC

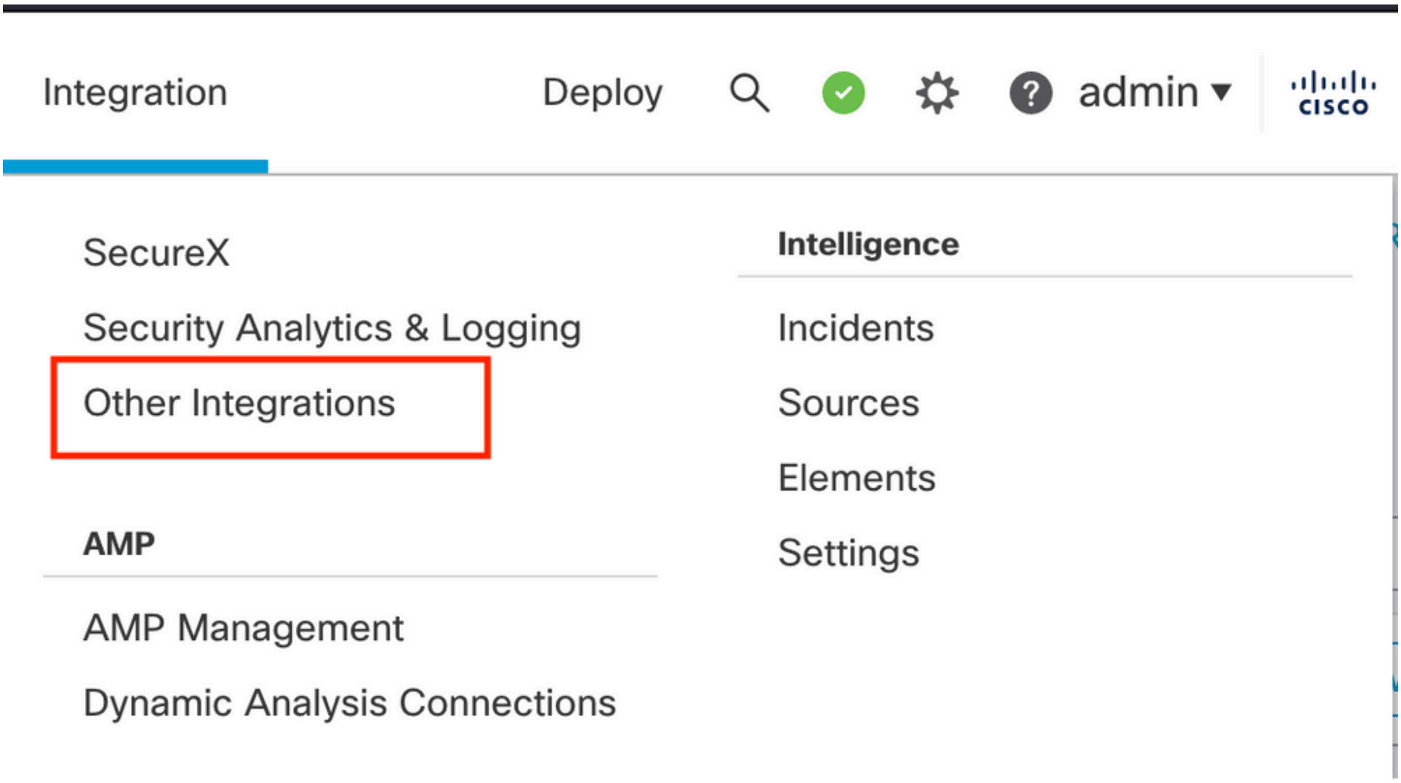
Step 2. Navigate to **Integration** tab.



Firewall Management Center
Overview / Dashboards / Dashboard
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
cisco SECURE
Reporting
Summary Dashboard (switch dashboard)
Provides a summary of activity on the appliance
Network
Threats
Intrusion Events
Status
Geolocation
QoS
Show the Last
1 hour
Add Widgets
Unique Applications over Time
Top Web Applications Seen
Top Client Applications Seen
No Data
No devices registered.
Click here to register a device.
Last updated 3 minutes ago
Traffic by Application Risk
Top Server Applications Seen
Top Operating Systems Seen

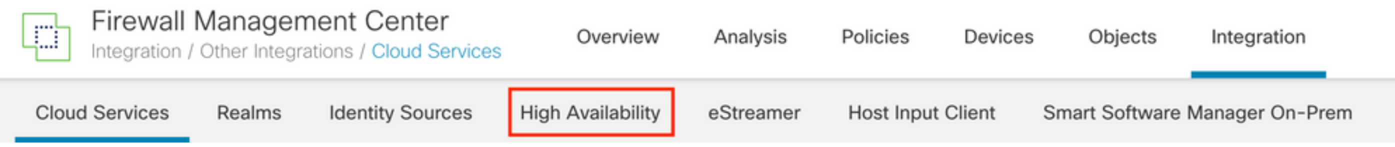
Navigate to integration

Step 3. Click **Other Integrations**.



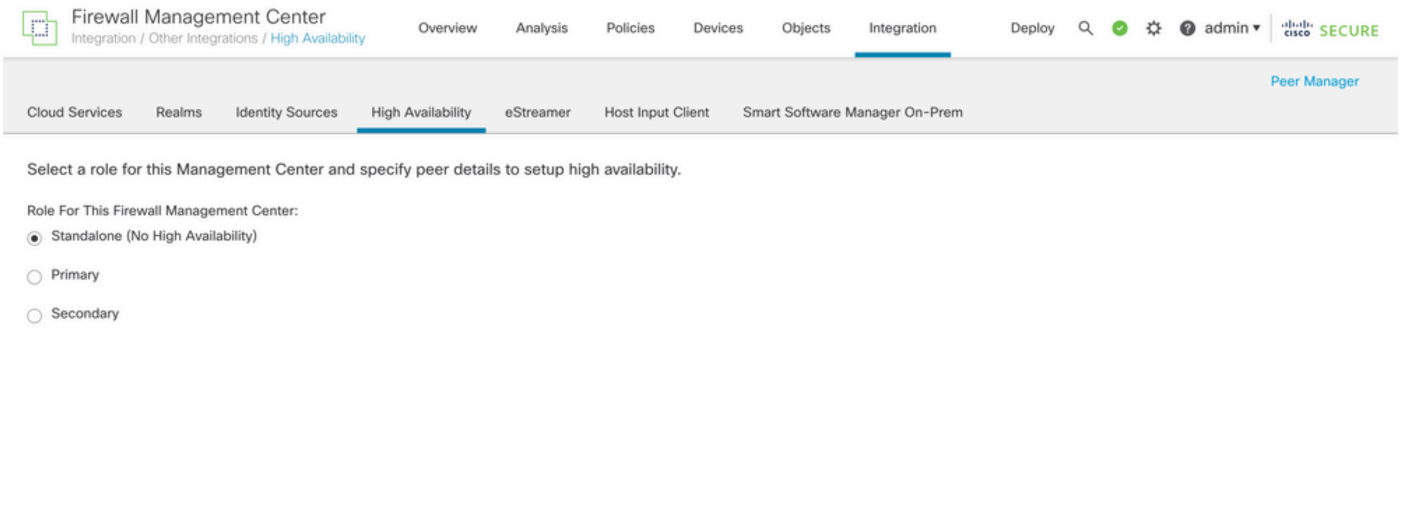
Navigate to Other Integration

Step 4. Navigate to the **High Availability** tab.



Navigate to High Availability

Step 5. Click **Secondary**.



Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

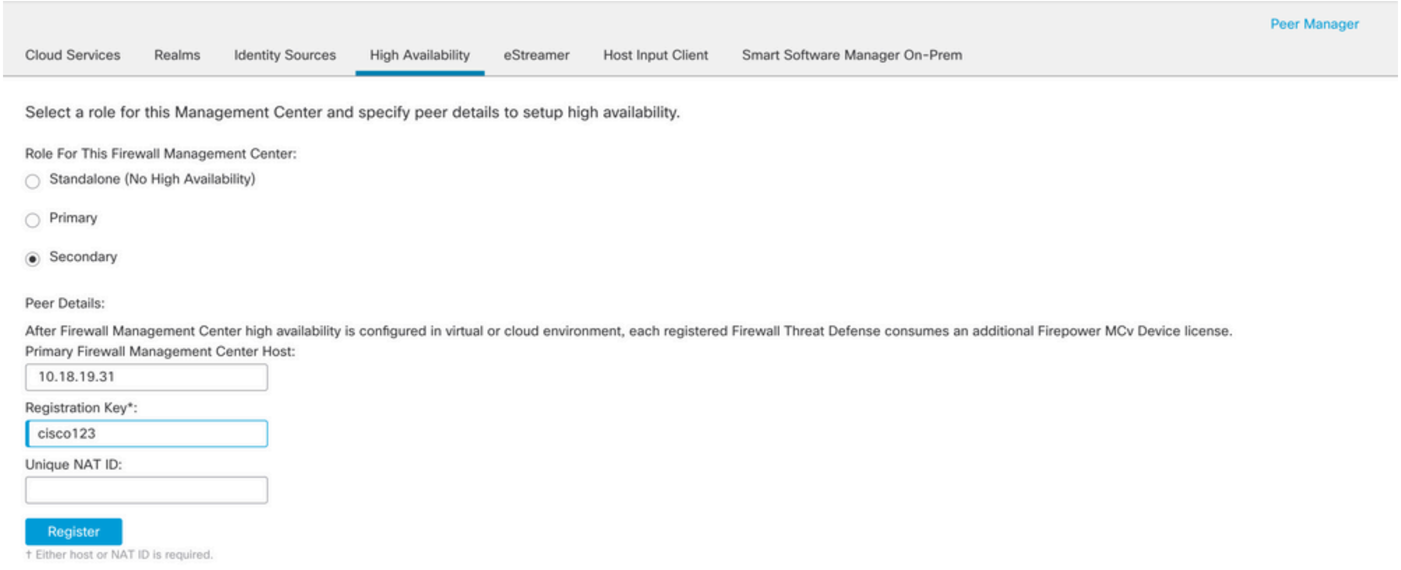
● Standalone (No High Availability)

○ Primary

○ Secondary

Input information and select desired role for current FMC

Step 6. Enter information of the Primary/Active peer and click **Register**.



Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

○ Standalone (No High Availability)

○ Primary

● Secondary

Peer Details:

After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license.

Primary Firewall Management Center Host: 10.18.19.31

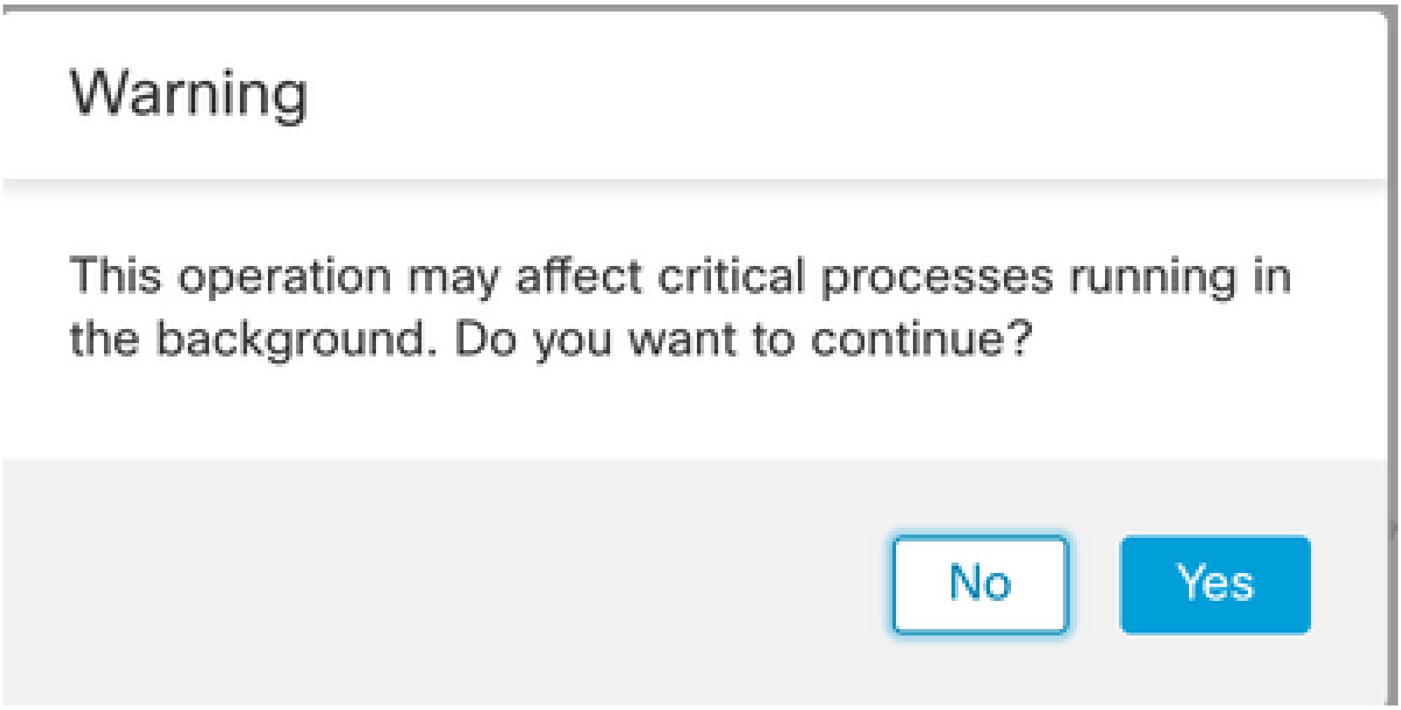
Registration Key*: cisco123

Unique NAT ID:

† Either host or NAT ID is required.

Note: Take note of the registration key, since it is going to be used on the active FMC.

Step 7. This warning asks you to confirm, click **Yes**.

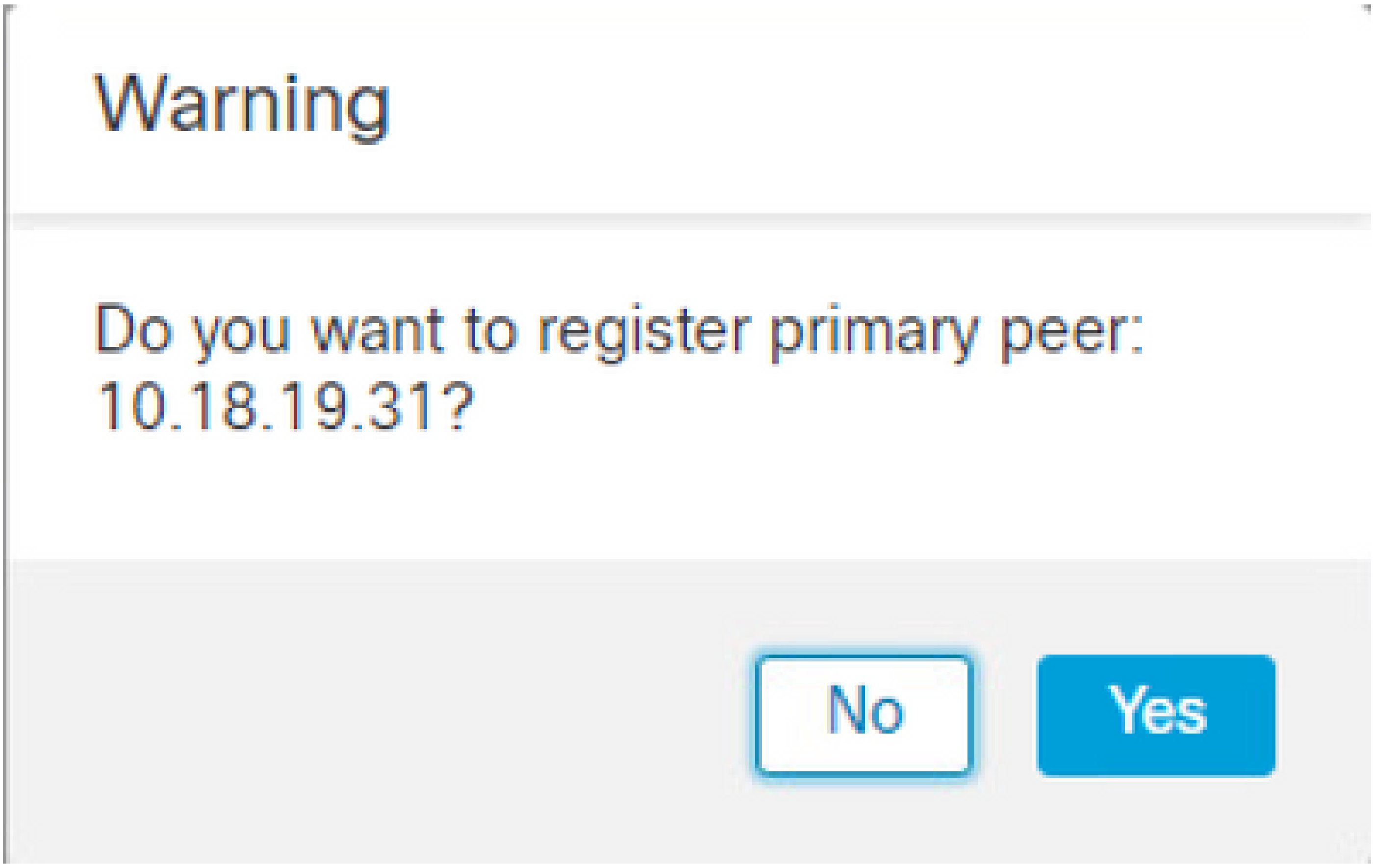


Warning

This operation may affect critical processes running in the background. Do you want to continue?

Note: Ensure there is no other task running as while HA is being created, the GUI restarts.

Step 8. Confirm that you want to register the primary peer.

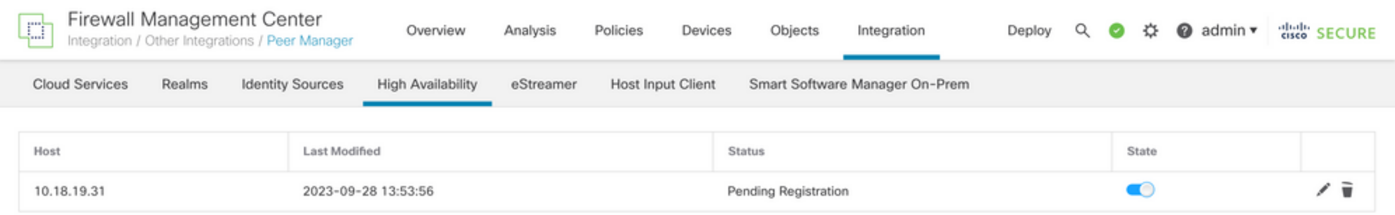


Warning

Do you want to register primary peer: 10.18.19.31?

Warning: All information on the Devices/Policy/Configuration is going to get removed from Secondary FMC once HA is created.

Step 9. Verify that the Secondary FMC status is pending.

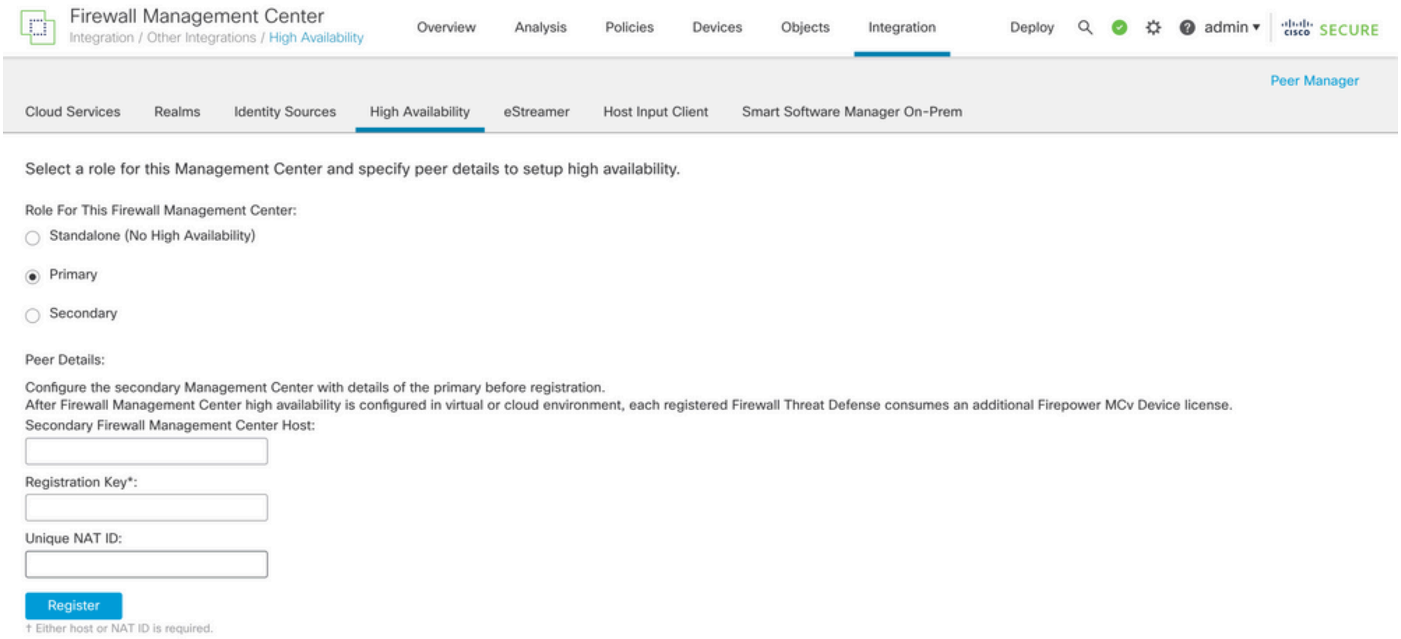


Host	Last Modified	Status	State
10.18.19.31	2023-09-28 13:53:56	Pending Registration	

Configure Primary FMC

Repeat Steps 1 - 4 on the Primary/Active FMC.

Step 5. Click **Primary**.



Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

○ Standalone (No High Availability)

● Primary

○ Secondary

Peer Details:

Configure the secondary Management Center with details of the primary before registration.
After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license.

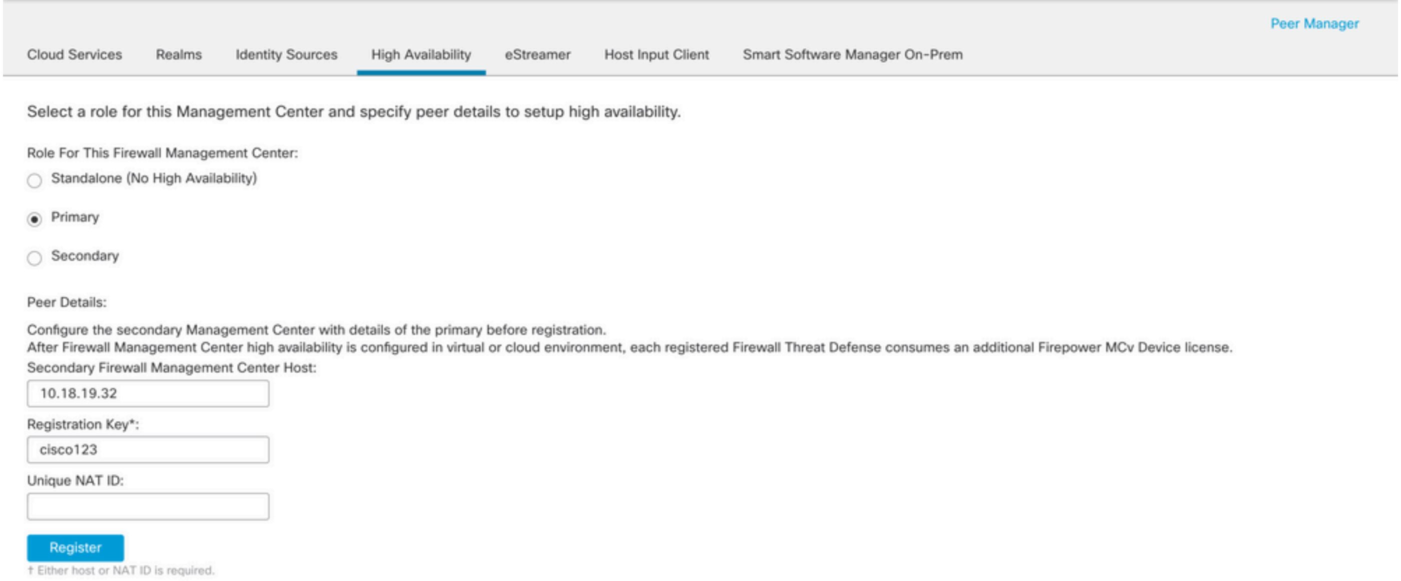
Secondary Firewall Management Center Host:

Registration Key*:

Unique NAT ID:

† Either host or NAT ID is required.

Step 6. Enter the information about Secondary FMC and click **Register**.



Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

○ Standalone (No High Availability)

● Primary

○ Secondary

Peer Details:

Configure the secondary Management Center with details of the primary before registration.
After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license.

Secondary Firewall Management Center Host: 10.18.19.32

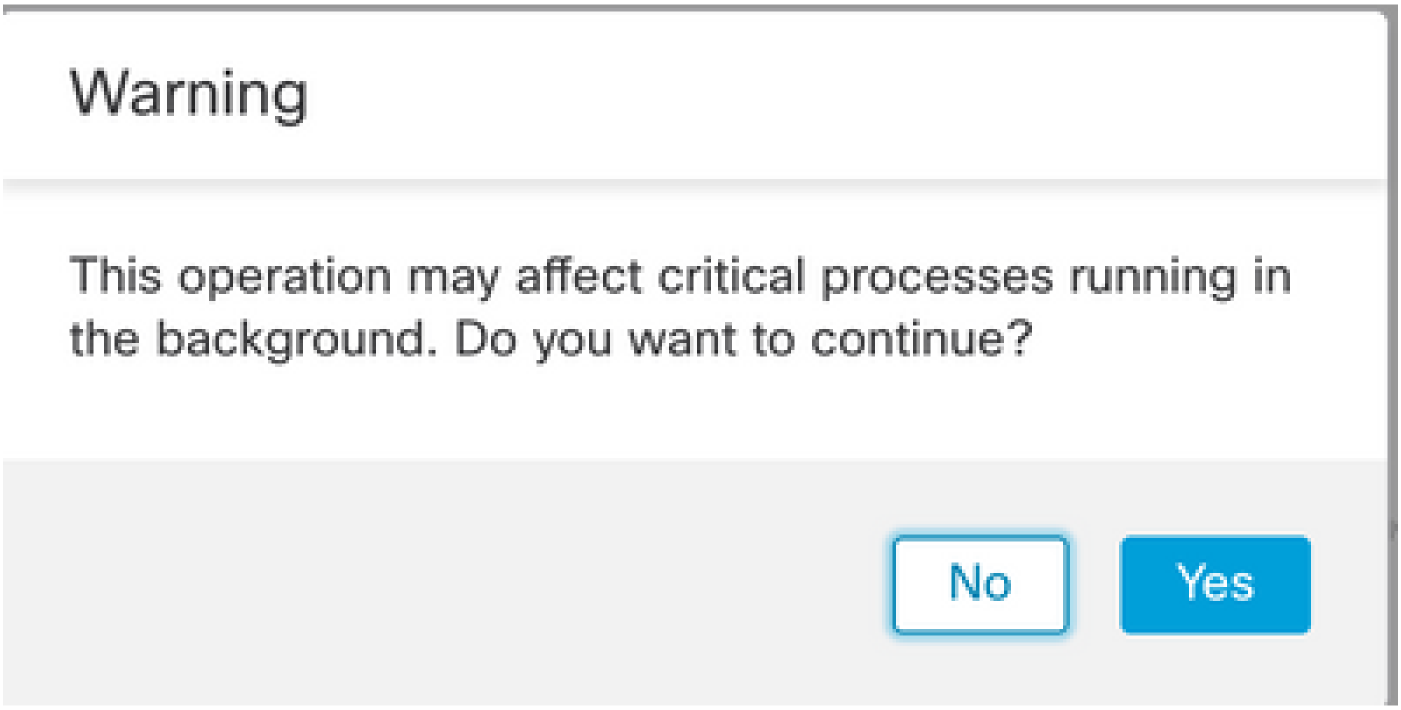
Registration Key*: cisco123

Unique NAT ID:

† Either host or NAT ID is required.

Note: Use the same Registration Key used as Secondary FMC.

Step 7. This warning asks you to confirm, click **Yes**.

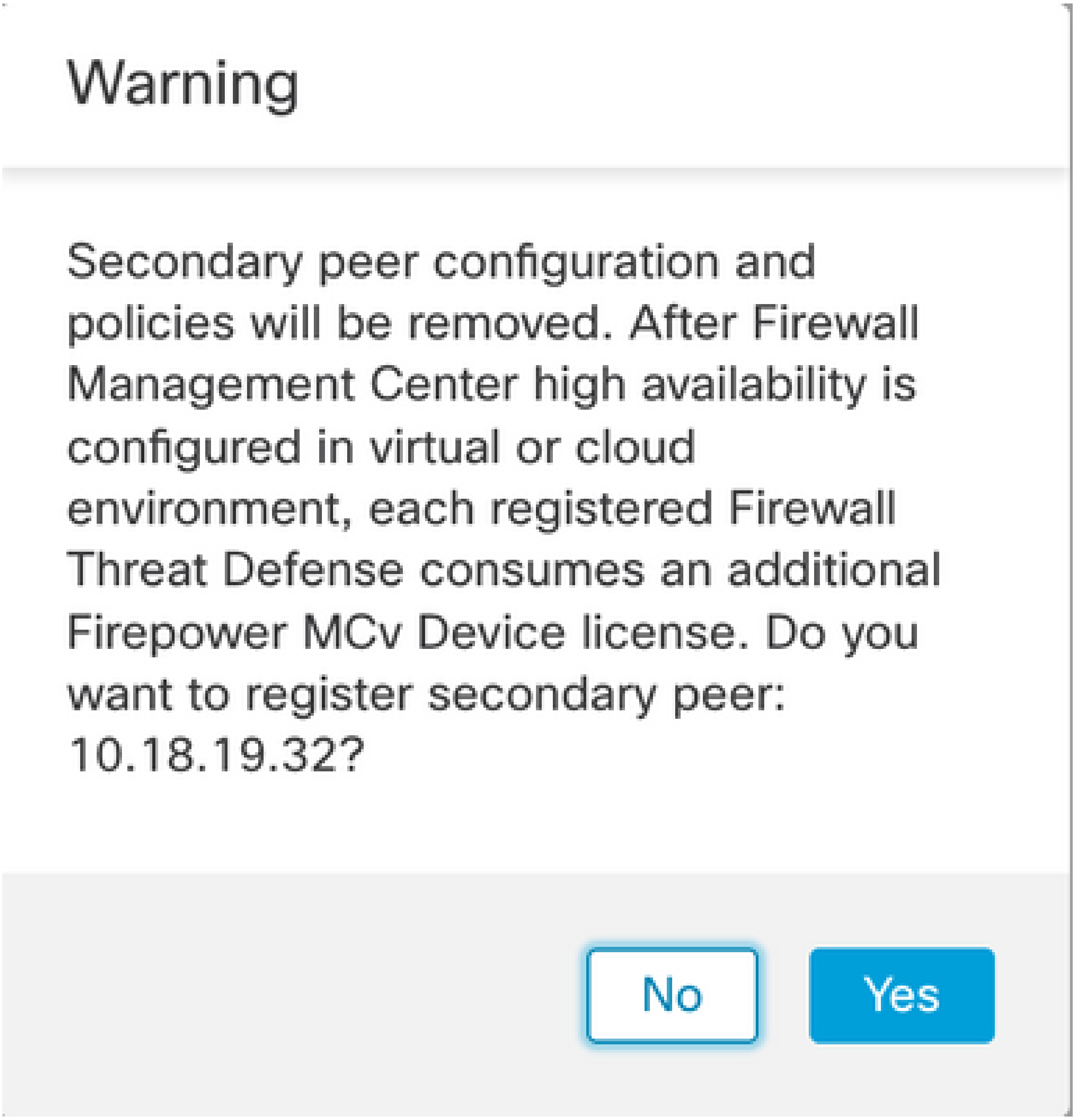


Warning

This operation may affect critical processes running in the background. Do you want to continue?

Note: Ensure there is no other task running.

Step 8. Confirm that you want to register for Secondary FMC.

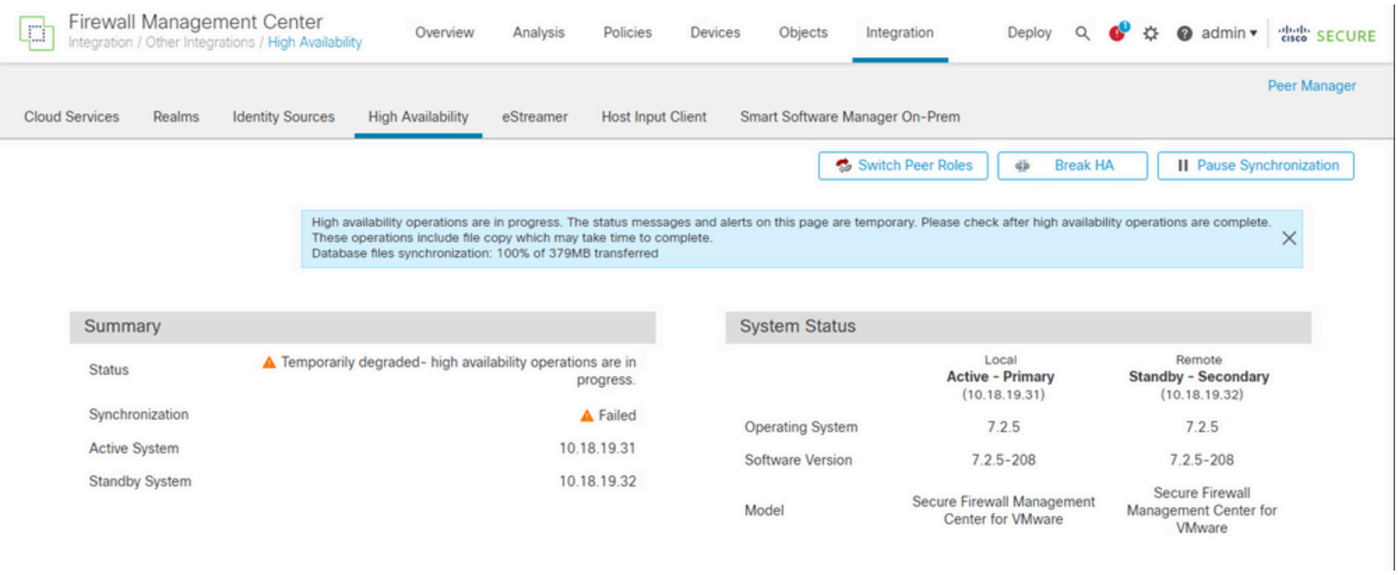


Warning

Secondary peer configuration and policies will be removed. After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license. Do you want to register secondary peer: 10.18.19.32?

Note: Ensure there is no critical information on the Secondary FMC, as accepting this prompt removes all the configurations from the FMC.

Synchronization between Primary and Secondary starts; the duration depends on configuration and devices. This process can be monitored from both units.



High availability operations are in progress. The status messages and alerts on this page are temporary. Please check after high availability operations are complete.
These operations include file copy which may take time to complete.
Database files synchronization: 100% of 379MB transferred

Summary

Status	⚠ Temporarily degraded- high availability operations are in progress.
Synchronization	⚠ Failed
Active System	10.18.19.31
Standby System	10.18.19.32

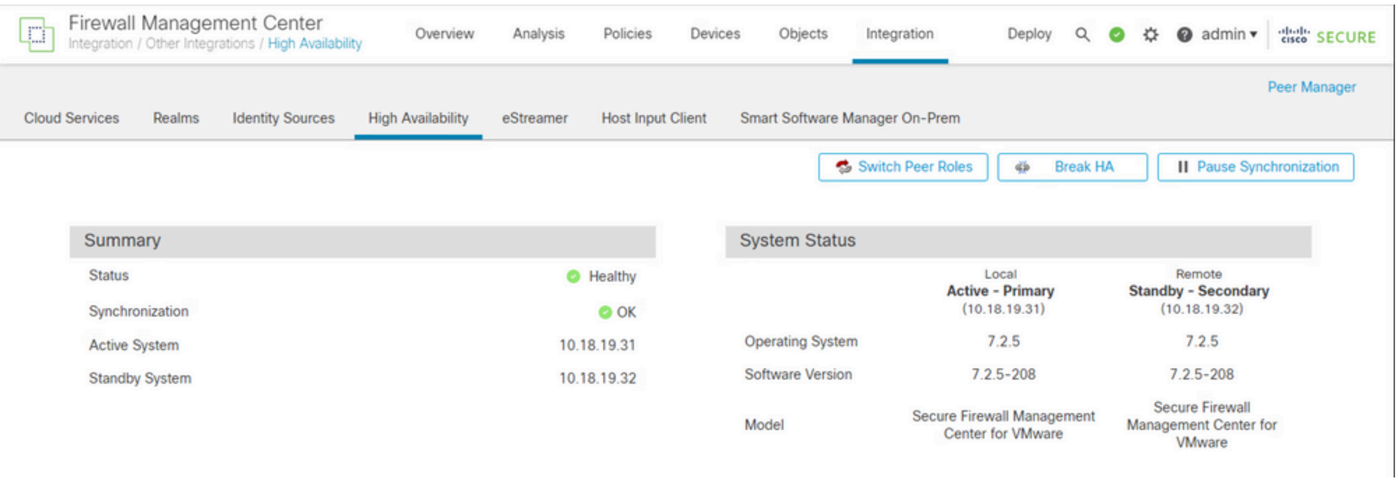
System Status

	Local **Active - Primary** (10.18.19.31)	Remote **Standby - Secondary** (10.18.19.32)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

Note: While synchronization is taking place, expect to see the status as **Failed** and **Temporary degraded**. This status shows until the process is completed.

Verification

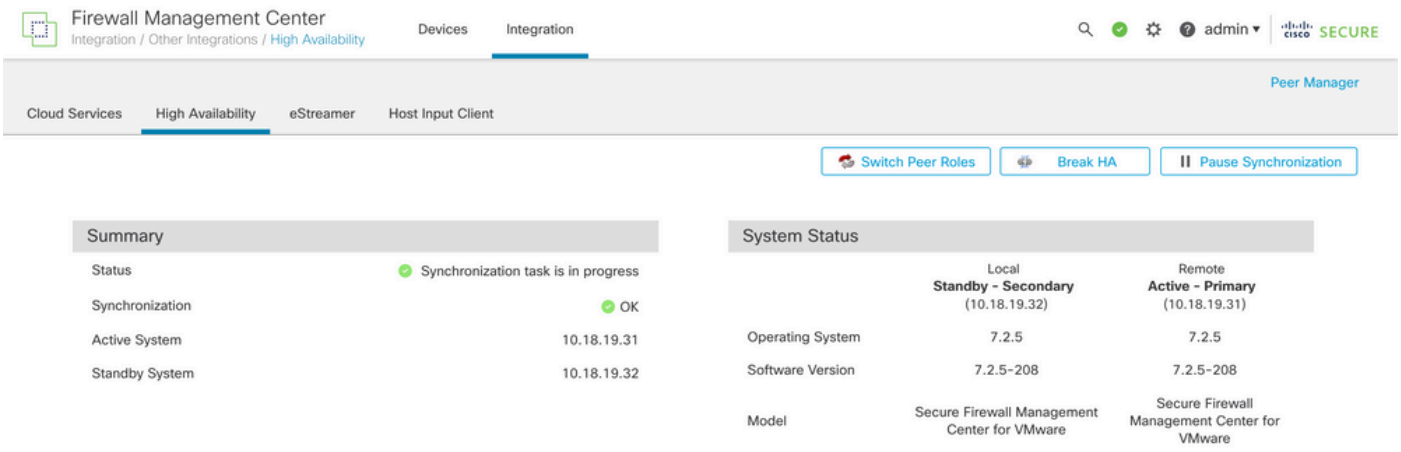
Once the synchronization is completed, the expected output is Status **Healthy** and Synchronization **OK**.



Summary	
Status	● Healthy
Synchronization	● OK
Active System	10.18.19.31
Standby System	10.18.19.32

System Status	Local **Active - Primary** (10.18.19.31)	Remote **Standby - Secondary** (10.18.19.32)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

The Primary and Secondary keep synchronizing; this is normal.



Summary	
Status	● Synchronization task is in progress
Synchronization	● OK
Active System	10.18.19.31
Standby System	10.18.19.32

System Status	Local **Standby - Secondary** (10.18.19.32)	Remote **Active - Primary** (10.18.19.31)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

Take a moment to review that your devices are showing correctly on both Primary and Secondary.