Configure FTD High Availability on Firepower Appliances

Contents

Introduction

This document describes how to configure and verify Firepower Threat Defense (FTD) High Availability (HA) (Active/Standby failover) on Firepower devices.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- 2xCisco Firepower 9300
- 2xCisco Firepower 4100 (7.2.8)
- Firepower Management Center (FMC) (7.2.8)

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.

Note: On an FPR9300 appliance with FTD, you can configure only inter-chassis HA. The two units in a HA configuration must meet the conditions mentioned here.

Task 1. Verify Conditions

Task requirement:

Verify that both FTD appliances meet the note requirements and can be configured as HA units.

Solution:

Step 1. Connect to the FPR9300 Management IP and verify the module hardware.

Verify the FPR9300-1 hardware.

<#root>

```
KSEC-FPR9K-1-A#
```

show server inventory

```
Server Equipped PID Equipped VID Equipped Serial (SN) Slot Status      Ackd Memory (MB) Ackd Cores
------ ------------ ------------ -------------------- ---------------- ---------------- ----------
1/1    FPR9K-SM-36  V01          FLM19216KK6          Equipped                    262144         36
1/2    FPR9K-SM-36  V01          FLM19206H71          Equipped                    262144         36
1/3    FPR9K-SM-36  V01          FLM19206H7T          Equipped                    262144         36
KSEC-FPR9K-1-A#
```

Verify the FPR9300-2 hardware.

<#root>

```
KSEC-FPR9K-2-A#
```

show server inventory

```
Server  Equipped PID Equipped VID Equipped Serial (SN) Slot Status      Ackd Memory (MB) Ackd Cores
------- ------------ ------------ -------------------- ---------------- ---------------- ----------
1/1     FPR9K-SM-36  V01          FLM19206H9T          Equipped                    262144         36
1/2     FPR9K-SM-36  V01          FLM19216KAX          Equipped                    262144         36
1/3     FPR9K-SM-36  V01          FLM19267A63          Equipped                    262144         36
KSEC-FPR9K-2-A#
```

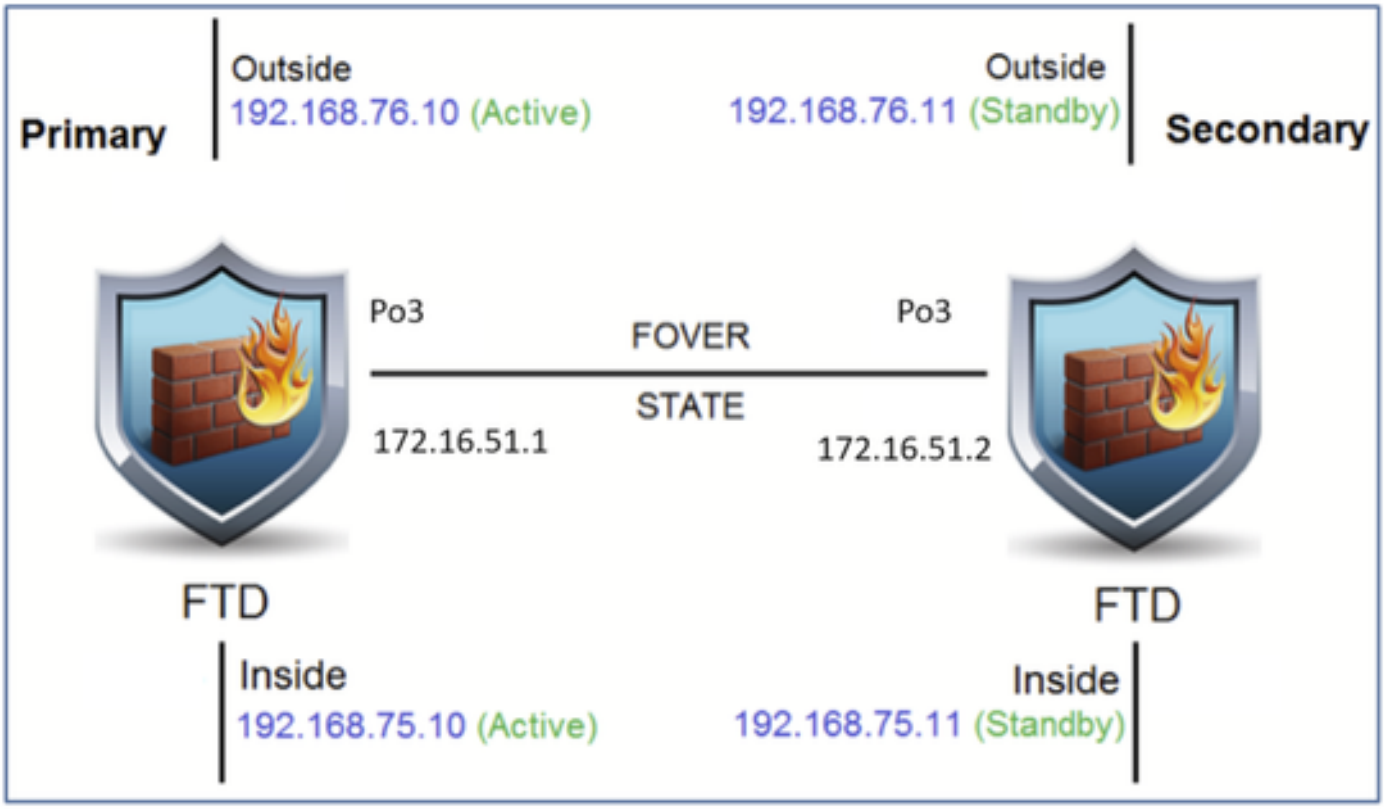
Step 2. Log into the FPR9300-1 Chassis Manager and navigate to **Logical Devices**.

Verify the software version, number, and type of interfaces.

Task 2. Configure FTD HA

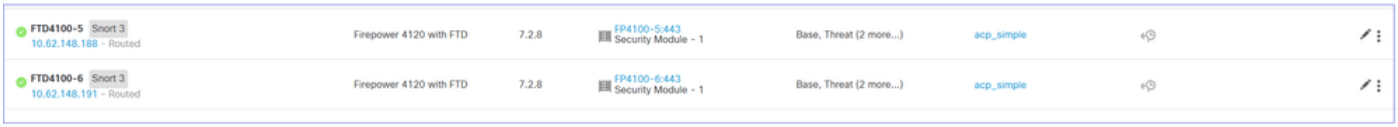
Task requirement:

Configure Active/Standby failover (HA) as per this diagram. In this case, a 41xx pair is used.

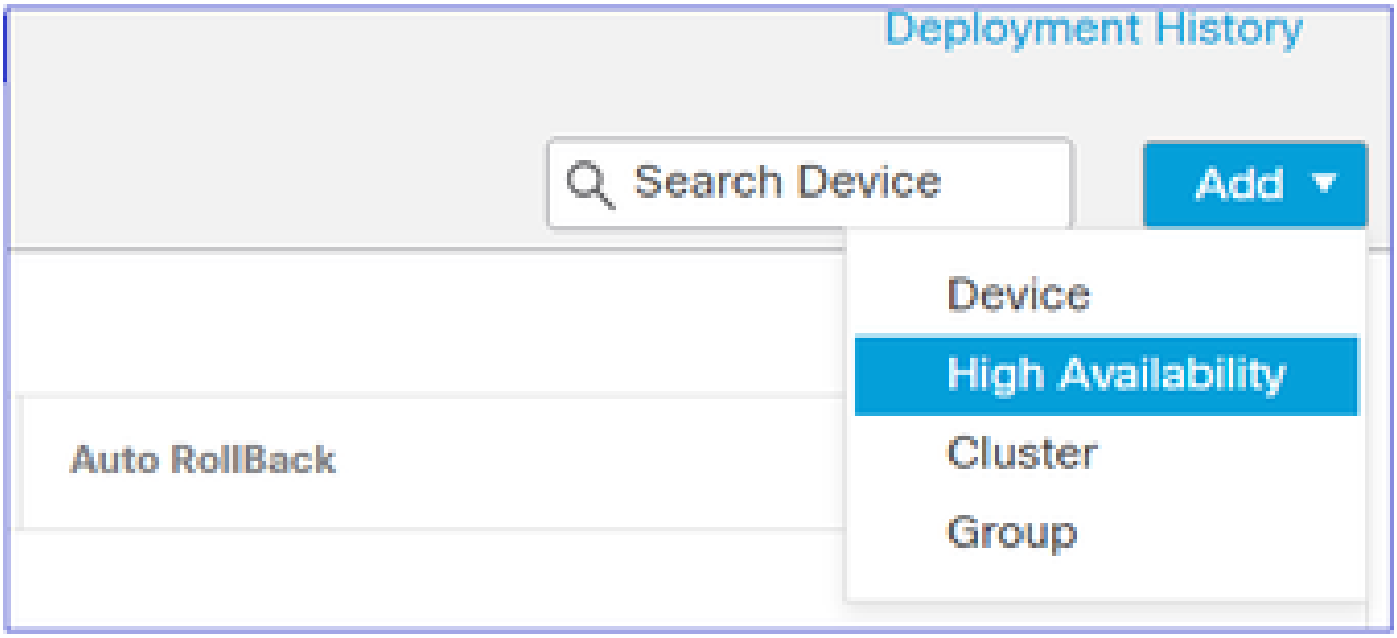


Solution

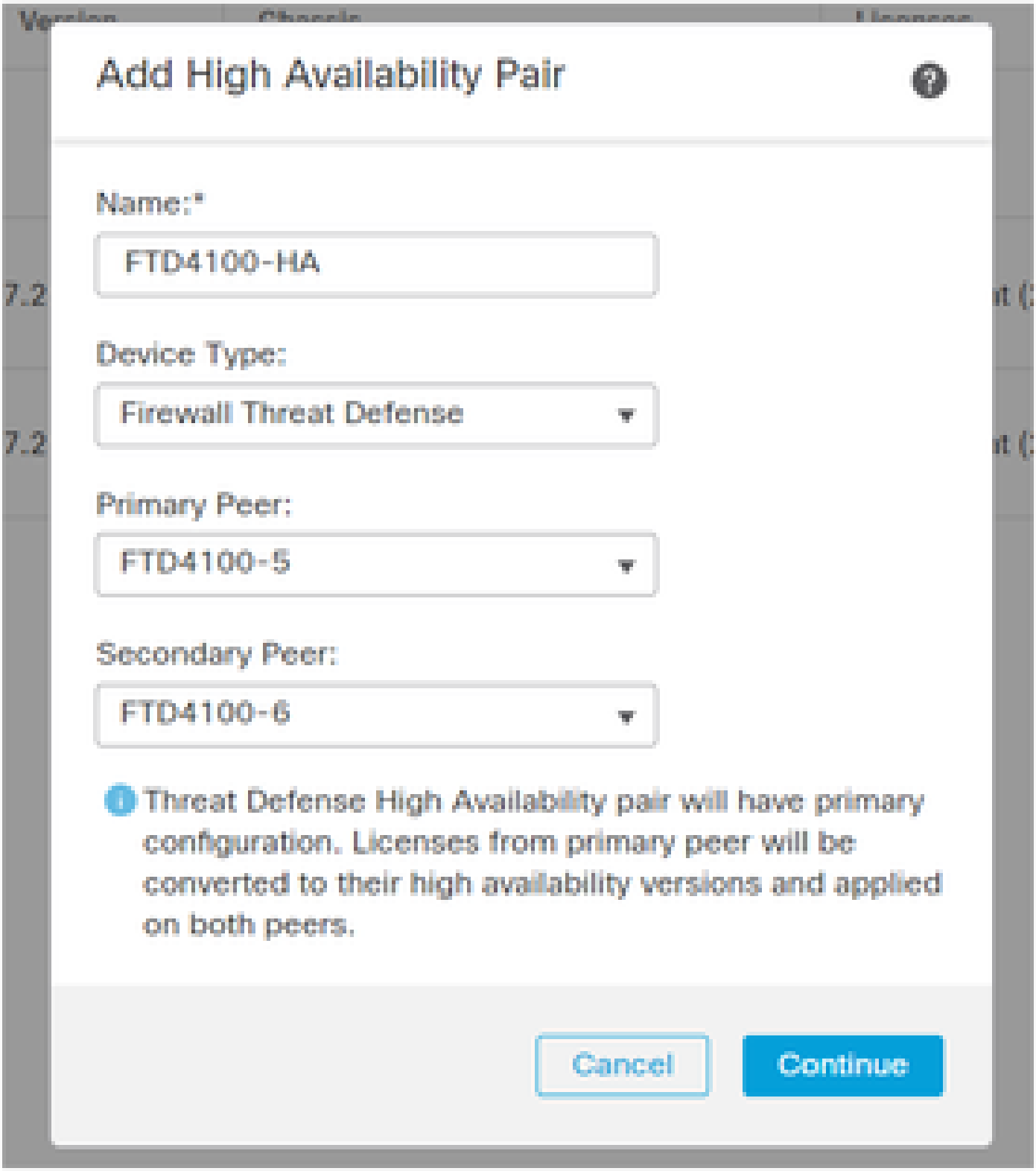
Both FTD devices are already registered on the FMC as shown in the image.



Step 1. In order to configure FTD failover, navigate to **Devices > Device Management** and choose **Add High Availability** as shown in the image.



Step 2. Enter the **Primary Peer** and the **Secondary Peer** and choose **Continue** as shown in the image.



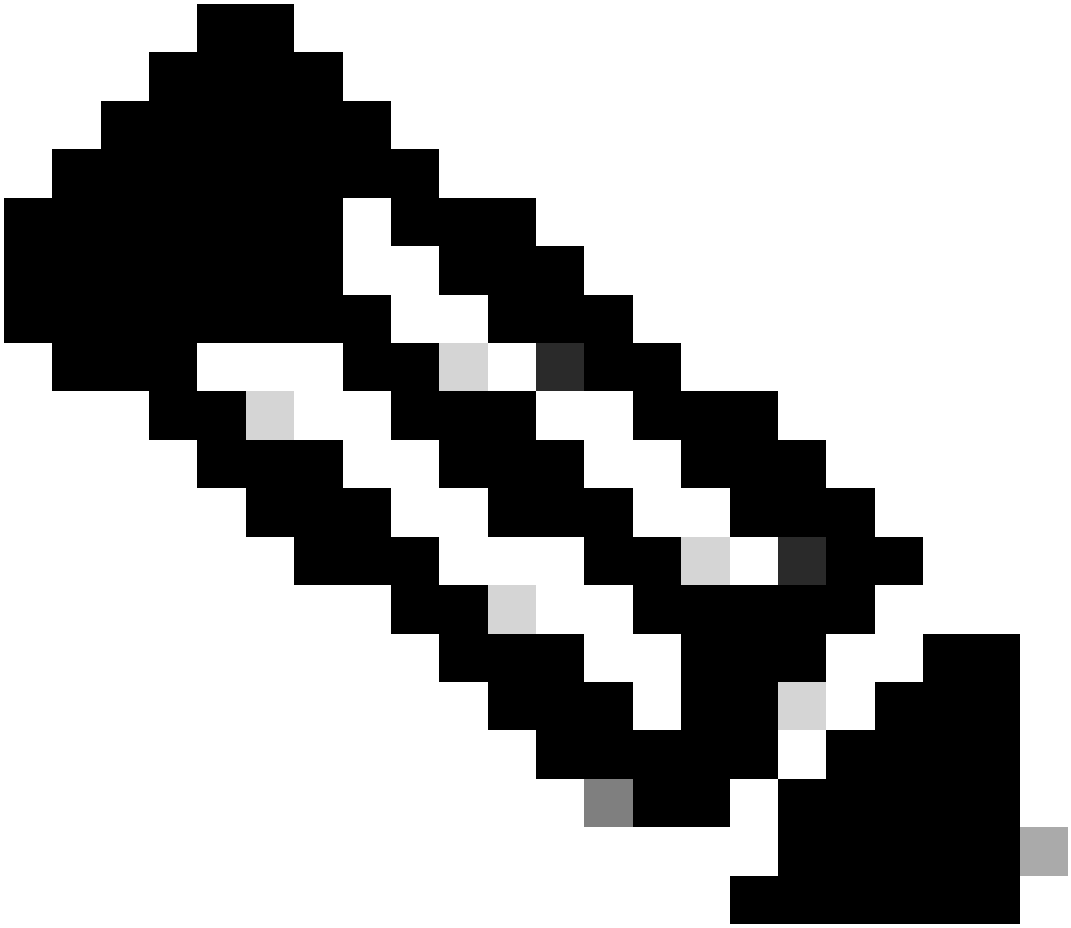
Warning: Ensure to select the correct unit as the primary unit. All configurations on the selected primary unit are replicated to the selected secondary FTD unit. As a result of replication, the current configuration on the secondary unit can be replaced.

Conditions

In order to create an HA between 2 FTD devices, these conditions must be met:

- Same model

- Same version- this applies to FXOS and to FTD - major (first number), minor (second number), and maintenance (third number) must be equal.
- Same number of interfaces
- Same type of interfaces
- Both devices as part of the same group/domain in FMC.
- Have identical Network Time Protocol (NTP) configuration.
- Be fully deployed on the FMC without uncommitted changes.
- Be in the same firewall mode: routed or transparent.



Note: This must be checked on both FTD devices and FMC GUI since there have been cases where the FTDs had the same mode, but FMC does not reflect this.

- Does not have DHCP/Point-to-Point Protocol over Ethernet (PPPoE) configured in any of the interfaces.
- Different hostname [Fully Qualified Domain Name (FQDN)] for both chassis. In order to check the chassis hostname, navigate to **FTD CLI** and run this command:

<#root>

```
firepower#
show chassis-management-url

https://
KSEC-FPR9K-1.cisco.com
:443//
```

Note: In post-6.3 FTD use the command **show chassis detail**.

```
<#root>
Firepower-module1#
show chassis detail

Chassis URL : https://FP4100-5:443//

Chassis IP : 10.62.148.187
Chassis IPv6 : ::
Chassis Serial Number : JAD19500BAB
Security Module : 1
```

If both chassis have the same name, change the name in one of them with the use of these commands:

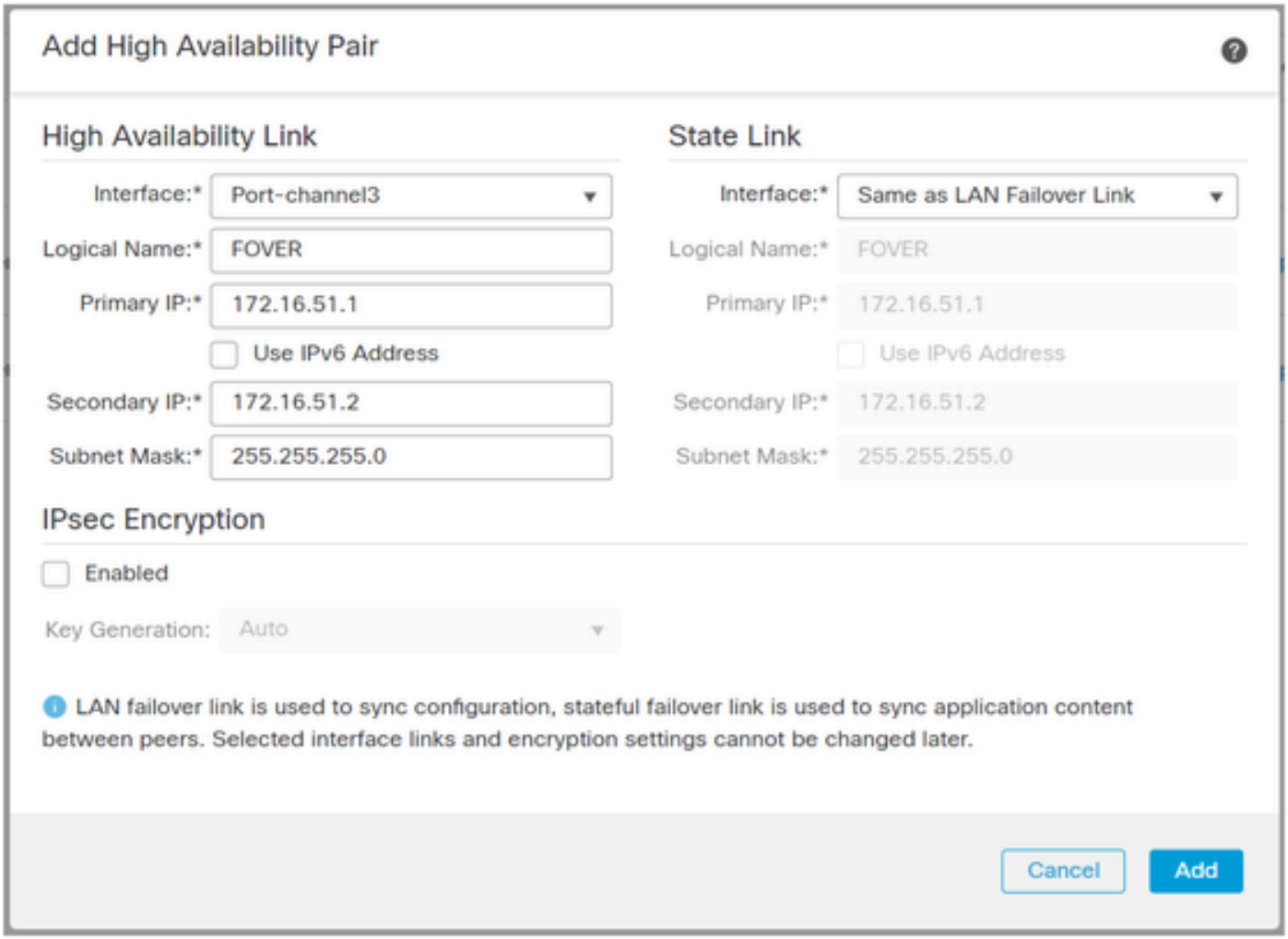
```
<#root>
KSEC-FPR9K-1-A#
scope system
KSEC-FPR9K-1-A /system #
set name FPR9K-1new
Warning: System name modification changes FC zone name and redeploys them non-disruptively
KSEC-FPR9K-1-A /system* #
commit-buffer
FPR9K-1-A /system #
exit
FPR9K-1new-A
#
```

After you change the chassis name, unregister the FTD from the FMC and register it again. Then, proceed with the HA Pair creation.

Step 3. Configure the HA and state the links settings.

In your case, the state link has the same settings as the High Availability Link.

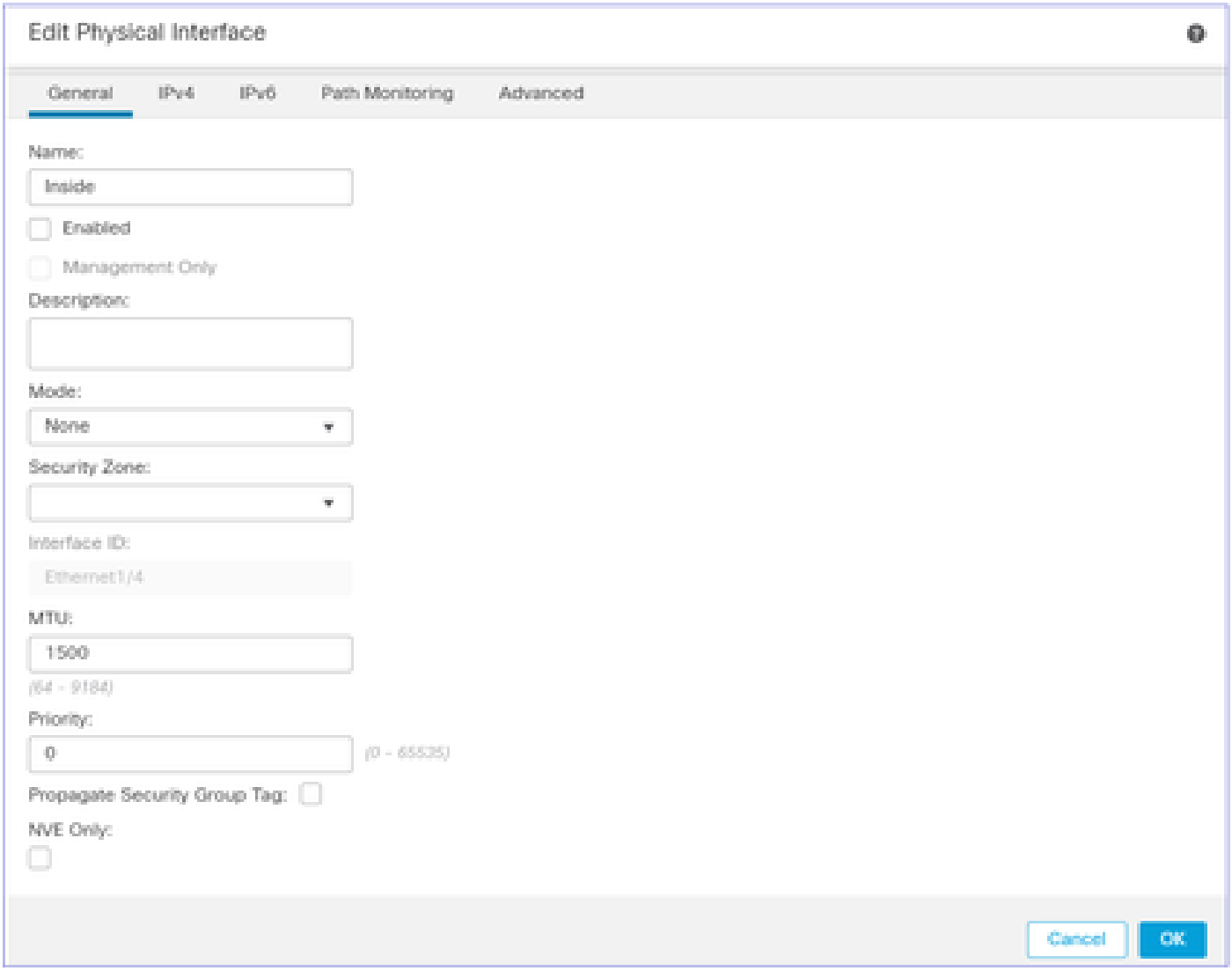
Choose **Add** and wait for a few minutes for the HA pair to be deployed as shown in the image.

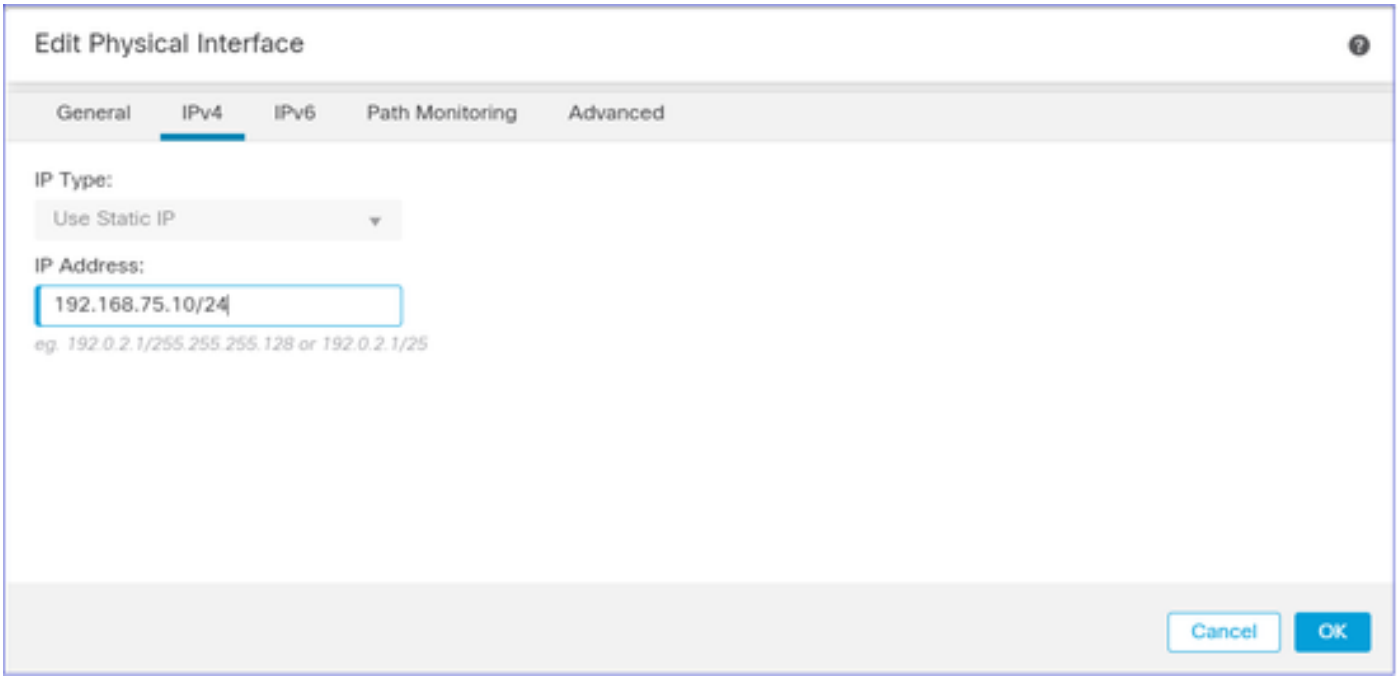


Step 4. Configure the Data interfaces (primary and standby IP addresses)

From the FMC GUI, choose the HA **Edit** as shown in the image.

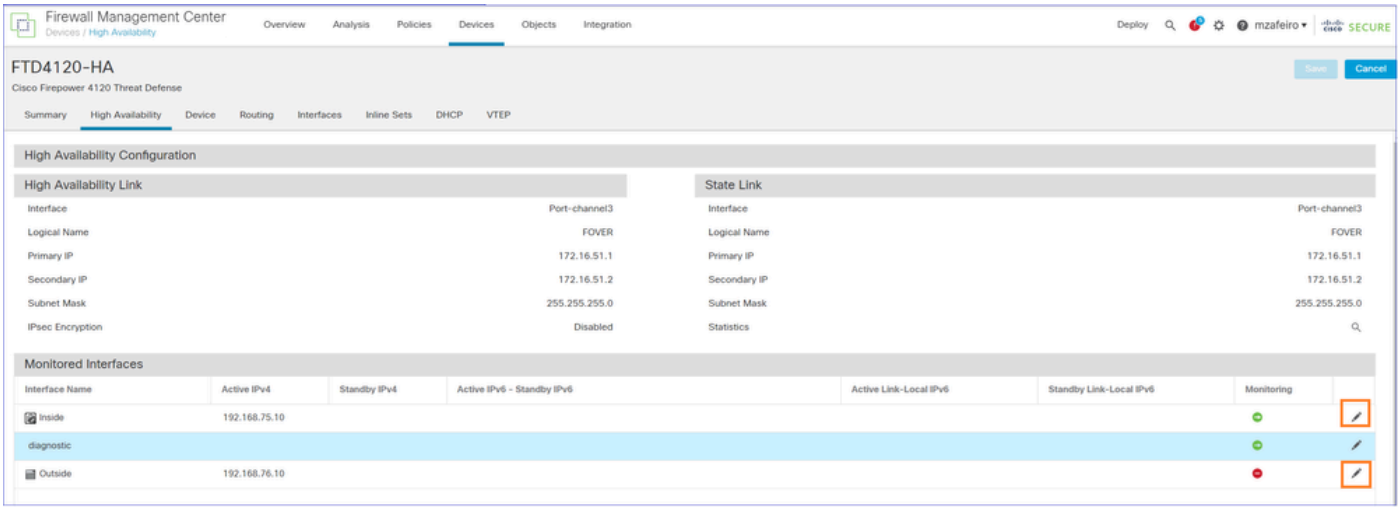
Step 5. Configure the Interface settings:



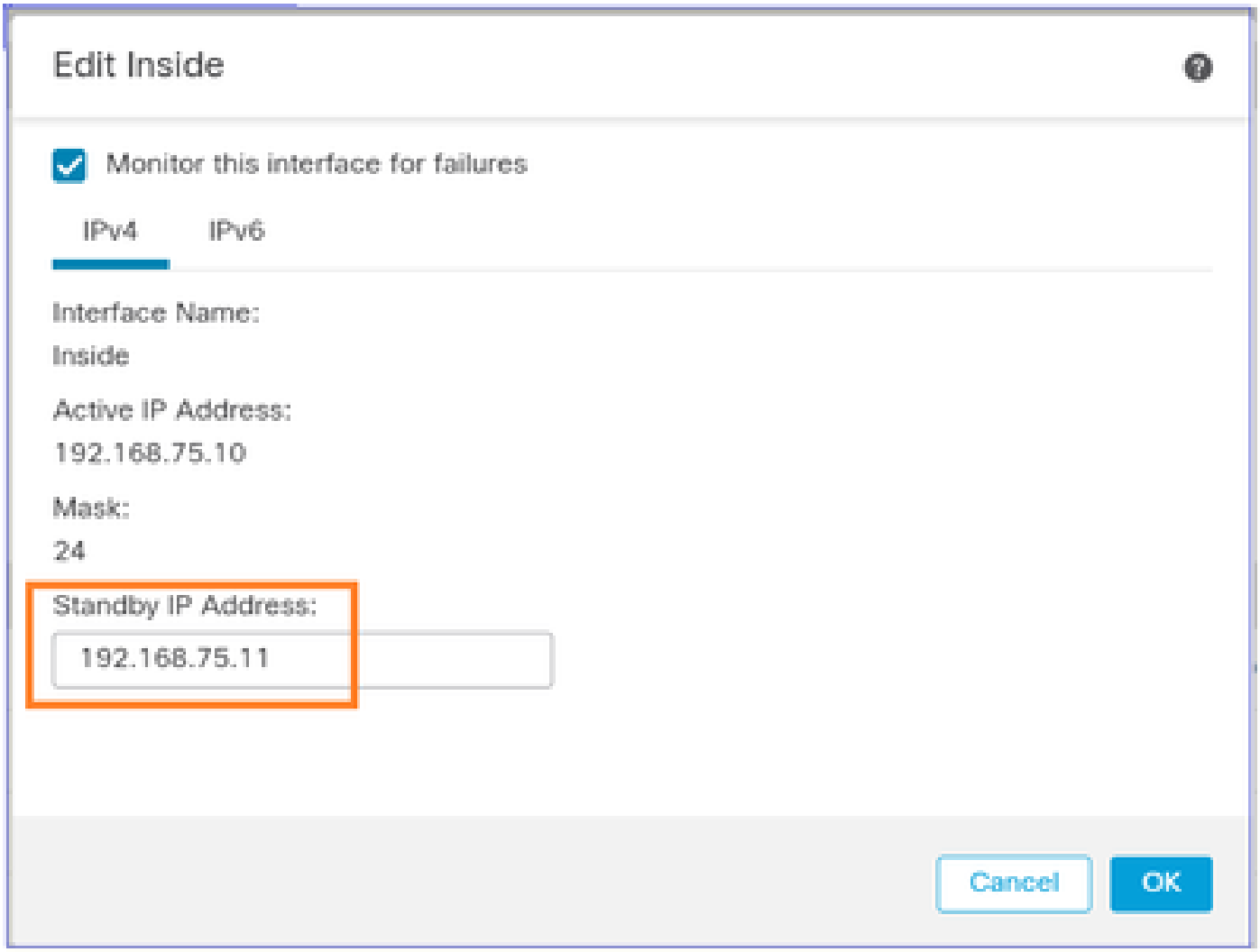


In the case of a subinterface, you need first to enable the parent interface:

Step 6. Navigate to **High Availability** and choose the Interface Name **Edit** to add the standby IP addresses as shown in the image.



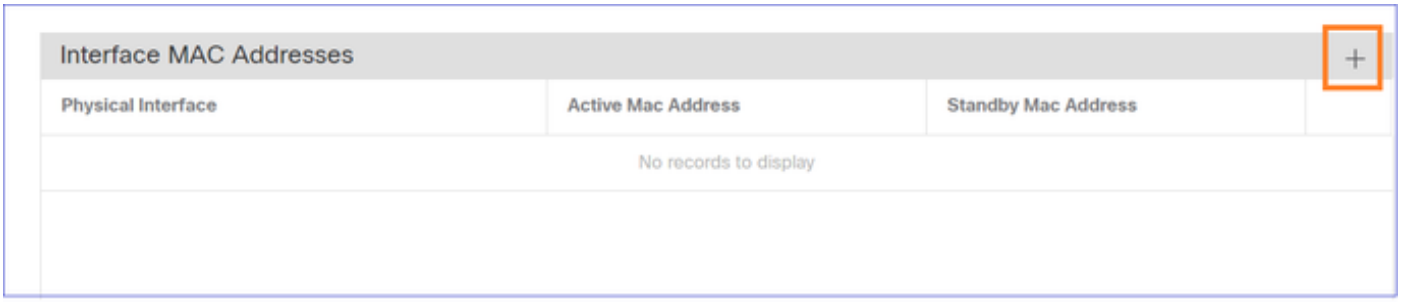
Step 7. For the Inside interface as shown in the image.



Step 8. Do the same for the Outside interface.

Step 9. Verify the result as shown in the image.

Step 10. Stay on the High Availability tab, and configure Virtual MAC addresses as shown in the image.



Step 11. For the Inside Interface is as shown in the image.

Step 12. Do the same for the Outside interface.

Step 13. Verify the result as shown in the image.

Step 14. After you configure the changes, choose **Save** and **Deploy**.

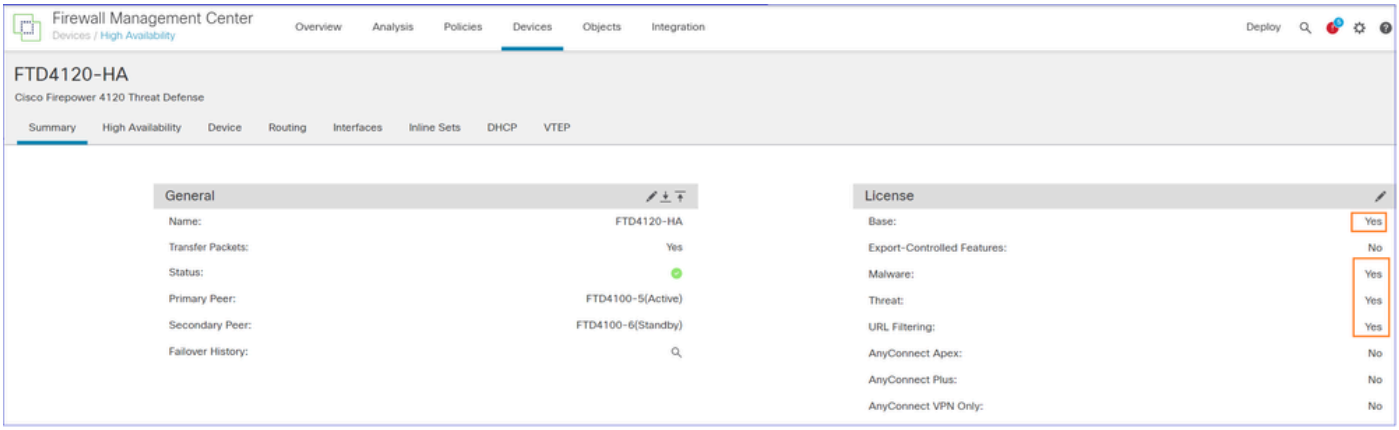
Task 3. Verify FTD HA and License

Task requirement:

Verify the FTD HA settings and enabled Licenses from the FMC GUI and from FTD CLI.

Solution:

Step 1. Navigate to **Summary** and check the HA settings and enabled Licenses as shown in the image.



Step 2. From the FTD CLISH CLI, run the '**show high-availability config**' or '**show failover**' command:

```
<#root>

>

show high-availability config


Failover On
Failover unit Primary
Failover LAN Interface: FOVER Port-channel3 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 1291 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.18(4)210, Mate 9.18(4)210
Serial Number: Ours FLM1949C5RR, Mate FLM2108V9YG
Last Failover at: 08:46:30 UTC Jul 18 2024
```

```
This host: Primary - Active

                Active time: 1999 (sec)
                slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface Inside (192.168.75.10): Link Down (Shutdown)
                  Interface Outside (192.168.76.10): Normal (Not-Monitored)
                slot 1: snort rev (1.0) status (up)
                slot 2: diskstatus rev (1.0) status (up)

Other host: Secondary - Standby Ready

                Active time: 1466 (sec)
                slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface Inside (192.168.75.11): Link Down (Shutdown)
                  Interface Outside (192.168.76.11): Normal (Not-Monitored)
                slot 1: snort rev (1.0) status (up)
                slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics
<output omitted>
```

Step 3. Do the same on the Secondary device.

Step 4. Run the **show failover state** command from the LINA CLI:

```
<#root>

firepower#

show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             18:32:56 EEST Jul 21 2016

====Configuration State===
    Sync Done
====Communication State===
    Mac set

firepower#
```

Step 5. Verify the configuration from the Primary unit (LINA CLI):

```
<#root>

>

show running-config failover
```

```
failover
failover lan unit primary
failover lan interface FOVER Port-channel3
failover replication http
failover mac address Ethernet1/4 aaaa.bbbb.1111 aaaa.bbbb.2222
failover mac address Port-channel2.202 aaaa.bbbb.3333 aaaa.bbbb.4444
failover link FOVER Port-channel3
failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2

>
```

show running-config interface

```
!
interface Port-channel2
no nameif
no security-level
no ip address
!
interface Port-channel2.202
vlan 202
nameif Outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11
!
interface Port-channel3
description LAN/STATE Failover Interface
!
interface Ethernet1/1
management-only
nameif diagnostic
security-level 0
no ip address
!
interface Ethernet1/4
shutdown
nameif Inside
security-level 0
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11
>
```

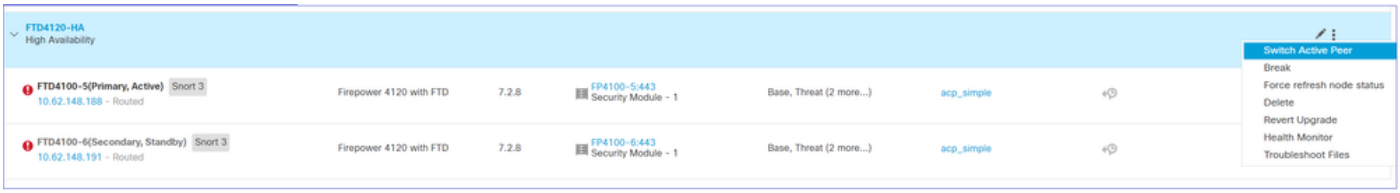
Task 4. Switch the Failover Roles

Task requirement:

From the FMC, switch the failover roles from Primary/Active, Secondary/Standby to Primary/Standby, Secondary/Active

Solution:

Step 1. Select the icon as shown in the image.



Step 2. Confirm the action.

You can use the **show failover history** command output:

On the new Active	**On the nev**
> **show failover history** ========== From State To State Reason ========== 09:27:11 UTC Jul 18 2024 Standby Ready Just Active Other unit wants me Active (Set by the config command) 09:27:11 UTC Jul 18 2024 Just Active Active Drain Other unit wants me Active (Set by the config command) 09:27:11 UTC Jul 18 2024 Active Drain Active Applying Config Other unit wants me Active (Set by the config command) 09:27:11 UTC Jul 18 2024 Active Applying Config Active Config Applied Other unit wants me Active (Set by the config command) 09:27:11 UTC Jul 18 2024 Active Config Applied Active Other unit wants me Active (Set by the config command)	> **show fail** ======== From State ======== 09:27:11 U Active

Step 4. After the verification, make the Primary unit Active again.

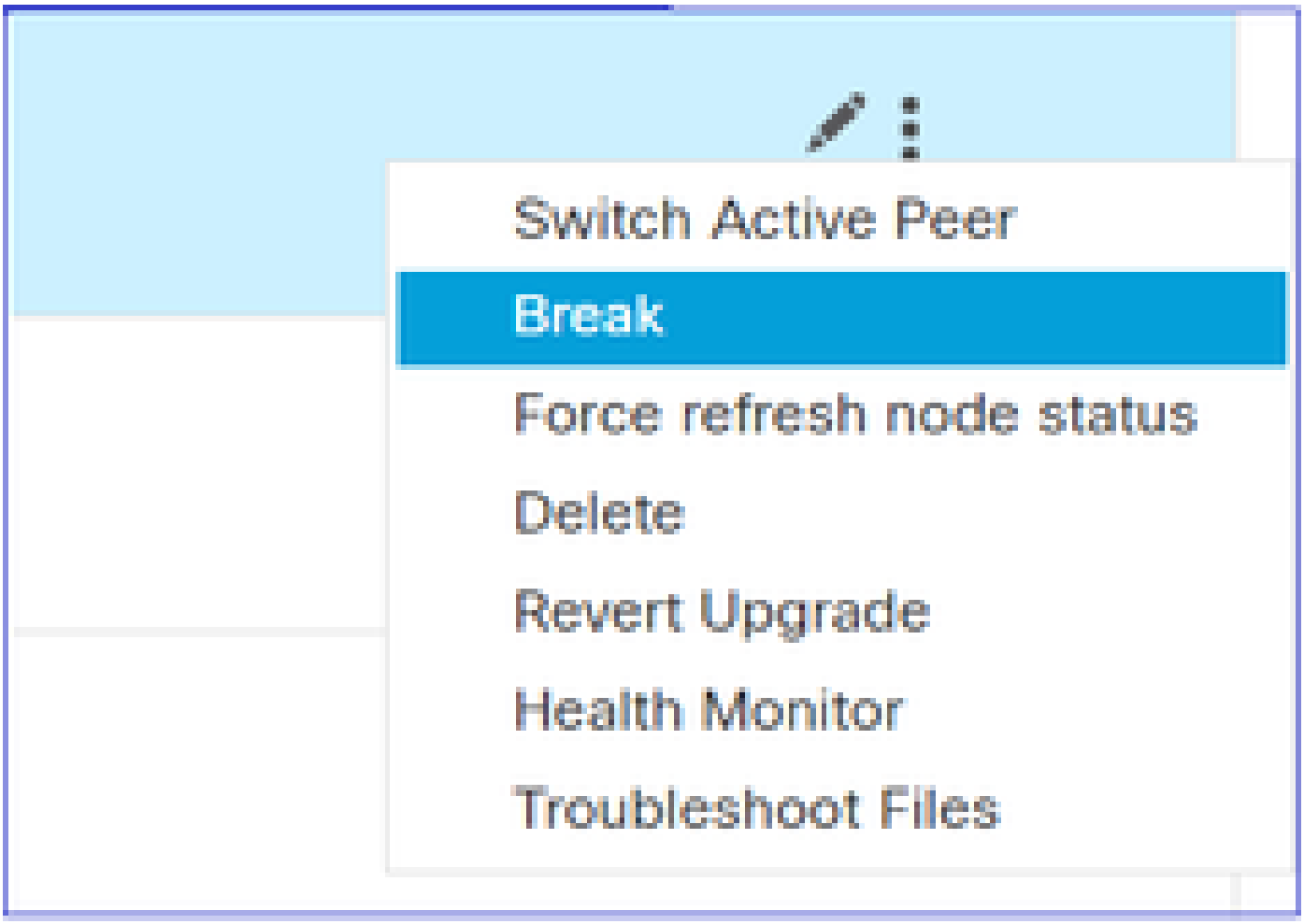
Task 5. Break the HA Pair

Task requirement:

From the FMC, break the failover pair.

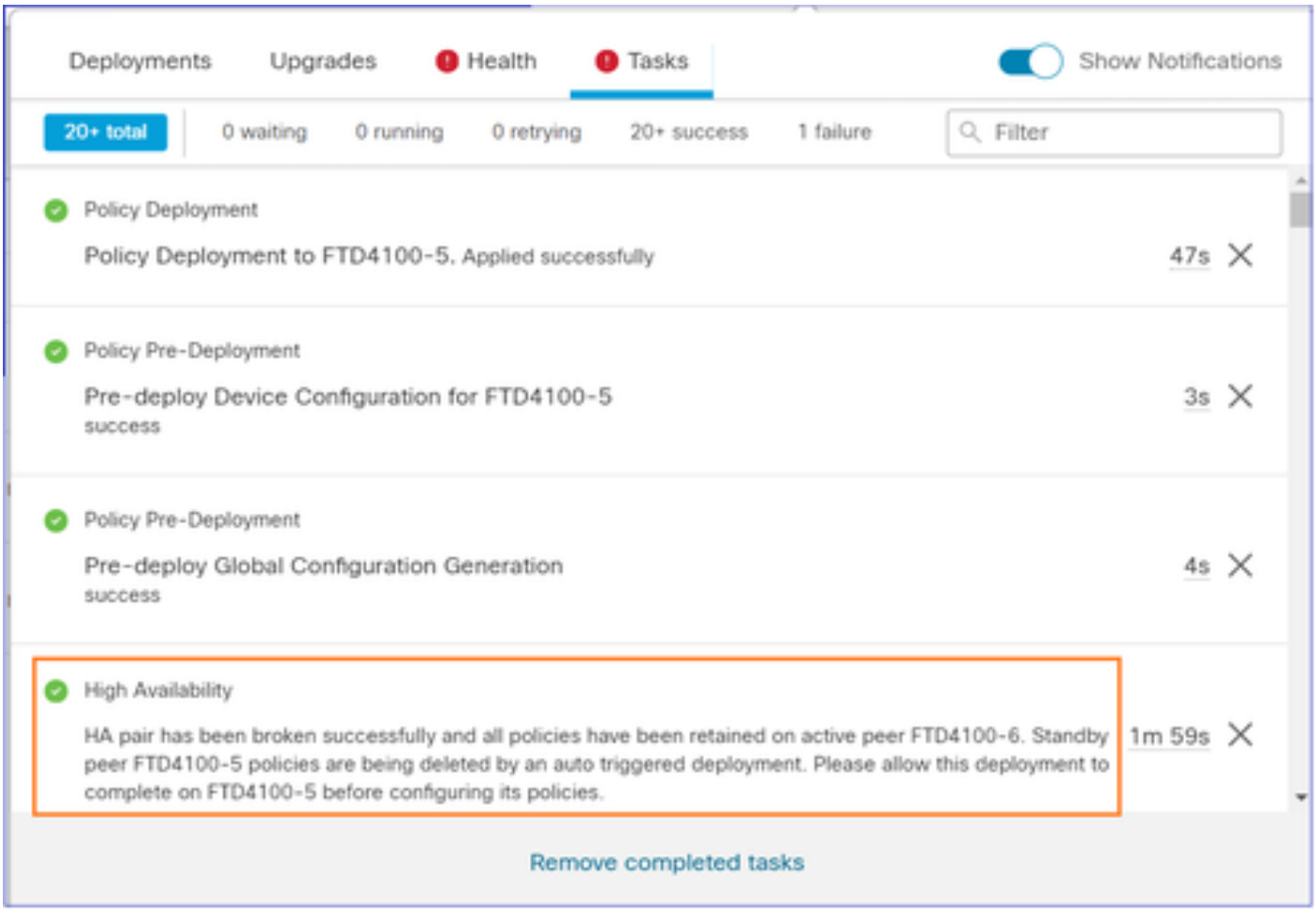
Solution:

Step 1. Select the icon as shown in the image.



Step 2. Check the notification as shown in the image.

Step 3. Note the message as shown in the image.



Step 4. Verify the result from the FMC GUI or from the CLI

show running-config on the Primary unit before and after the HA break:

Primary/Standby unit before the HA Break	**Primary unit after the HA Break**
> show running-config : Saved : : Serial Number: FLM1949C5RR : Hardware: FPR4K-SM-24, 73850 MB RAM, CPU Xeon E5 series 2200 MHz, 2 CPUs (48 cores) : NGFW Version 7.2.8 ! hostname firepower enable password ***** encrypted strong-encryption-disable service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 names no mac-address auto !	> INFO: This unit is currently in standby state. By disabling failover, this unit will remain in standby state. > **show running-config** : Saved : : Serial Number: FLM1949C5RR : Hardware: FPR4K-SM-24, 73850 MB RAM, CPU Xeon E5 series 2200 MHz, 2 CPUs (48 cores) : NGFW Version 7.2.8 ! hostname firepower enable password ***** encrypted strong-encryption-disable service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6

interface Port-channel2
no nameif
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
no security-level
no ip address
!
interface Port-channel2.202
vlan 202
nameif Outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11
!
interface Port-channel3
description LAN/STATE Failover Interface
!
interface Ethernet1/1
management-only
nameif diagnostic
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
no ip address
!
interface Ethernet1/4
nameif Inside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11
!
ftp mode passive
ngips conn-match vlan-id
object-group-search access-control
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any

names
no mac-address auto

!
interface Port-channel2
shutdown
no nameif
no security-level
no ip address
!
interface Port-channel3
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet1/1
management-only
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet1/4
shutdown
no nameif
no security-level
no ip address
!
ftp mode passive
ngips conn-match vlan-id
object-group-search access-control
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 268439552: ACCESS POLICY: acp_simple - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268439552: L7 RULE: rule1
access-list CSM_FW_ACL_ advanced permit ip any

range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 268434433: ACCESS POLICY: acp_simple - Default
access-list CSM_FW_ACL_ remark rule-id 268434433: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434433
!
tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow
tcp-options range 9 18 allow
tcp-options range 20 255 allow
urgent-flag allow
!
no pager
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
mtu Outside 1500
mtu diagnostic 1500
mtu Inside 1500
failover
failover lan unit primary
failover lan interface FOVER Port-channel3
failover replication http
failover mac address Ethernet1/4 aaaa.bbbb.1111 aaaa.bbbb.2222
failover mac address Port-channel2.202 aaaa.bbbb.3333 aaaa.bbbb.4444
failover link FOVER Port-channel3
failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2

<output omitted>

any rule-id 268439552
!
tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow
tcp-options range 9 18 allow
tcp-options range 20 255 allow
urgent-flag allow
!
no pager
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
no failover
<output omitted>

Secondary/Active unit before the HA Break	**Secondary unit after the HA Break**

> **show running-config**
: Saved

:
: Serial Number: FLM2108V9YG
: Hardware: FPR4K-SM-24, 73850 MB RAM, CPU Xeon E5 series 2200 MHz, 2 CPUs (48 cores)
:
NGFW Version 7.2.8
!
hostname firepower
enable password ***** encrypted
strong-encryption-disable
service-module 0 keepalive-timeout 4
service-module 0 keepalive-counter 6
names
no mac-address auto

!
interface Port-channel2
no nameif
no security-level
no ip address
!
interface Port-channel2.202
vlan 202
nameif Outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11
!
interface Port-channel3
description LAN/STATE Failover Interface
!
interface Ethernet1/1
management-only
nameif diagnostic
security-level 0
no ip address
!
interface Ethernet1/4
nameif Inside
security-level 0
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11
!
ftp mode passive
ngips conn-match vlan-id
object-group-search access-control
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id 9998:

> **show running-config**
: Saved

:
: Serial Number: FLM2108V9YG
: Hardware: FPR4K-SM-24, 73850 MB RAM, CPU Xeon E5 series 2200 MHz, 2 CPUs (48 cores)
:
NGFW Version 7.2.8
!
hostname firepower
enable password ***** encrypted
strong-encryption-disable
service-module 0 keepalive-timeout 4
service-module 0 keepalive-counter 6
names
no mac-address auto

!
interface Port-channel2
no nameif
no security-level
no ip address
!
interface Port-channel2.202
vlan 202
nameif Outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11
!
interface Port-channel3
no nameif
no security-level
no ip address
!
interface Ethernet1/1
management-only
nameif diagnostic
security-level 0
no ip address
!
interface Ethernet1/4
nameif Inside
security-level 0
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11
!
ftp mode passive
ngips conn-match vlan-id

PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 268439552: ACCESS POLICY: acp_simple - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268439552: L7 RULE: rule1
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268439552
!
tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow
tcp-options range 9 18 allow
tcp-options range 20 255 allow
urgent-flag allow
!
no pager
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
mtu Outside 1500
mtu diagnostic 1500
mtu Inside 1500
failover
failover lan unit secondary
failover lan interface FOVER Port-channel3
failover replication http
failover link FOVER Port-channel3
failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2

object-group-search access-control
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 268439552: ACCESS POLICY: acp_simple - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268439552: L7 RULE: rule1
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268439552
!
tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow
tcp-options range 9 18 allow
tcp-options range 20 255 allow
urgent-flag allow
!
no pager
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
mtu Outside 1500
mtu diagnostic 1500
mtu Inside 1500
no failover
no monitor-interface Outside
no monitor-interface service-module

<output omitted>

<output omitted>	

Main points to note for the HA break:

Primary/Standby Unit	Secondary/Active Unit
• All failover configuration is removed • All IP configuration is removed	• All failover configuration is removed • Standby IPs remain, but is removed in the next deployment

Step 5. After you finish this task, recreate the HA pair.

Task 6. Delete an HA pair

This task is based on an HA setup on 41xx using 7.2.8 software. In this case, initially the devices were in these states:

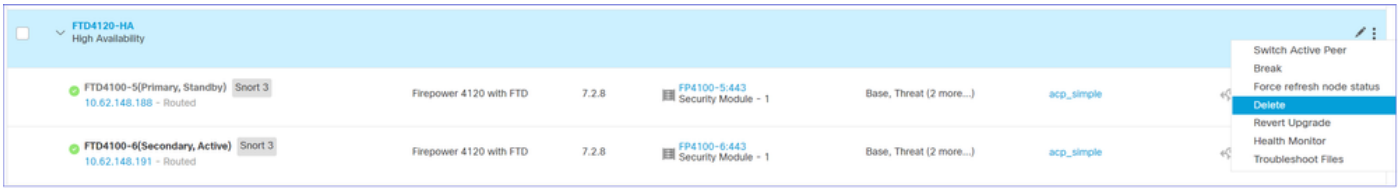
- Primary/Stadnby
- Secondary/Active

Task requirement:

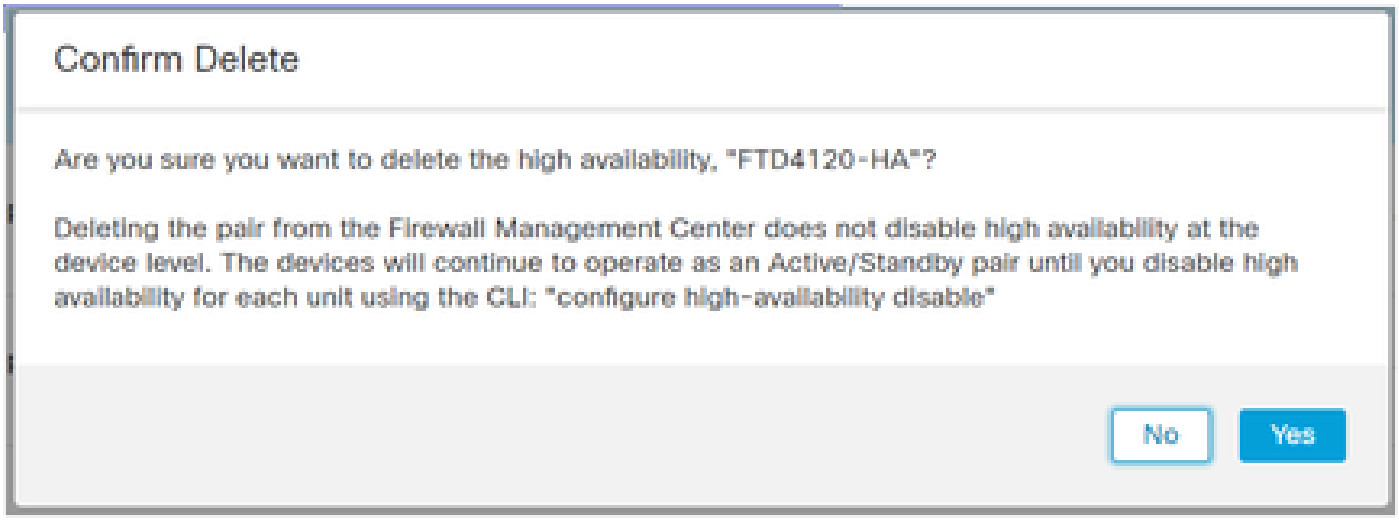
From the FMC, delete the failover pair.

Solution:

Step 1. Choose the icon as shown in the image:



Step 2. Check the notification and confirm as shown in the image:



Step 3. After you delete the HA, both devices are unregistered (removed) from the FMC.

show running-config result from the LINA CLI is as shown in the table here:

Primary Unit (Standby)	**Secondary Unit (Active)**
> **show running-config** : Saved : : Serial Number: FLM1949C5RR : Hardware: FPR4K-SM-24, 73853 MB RAM, CPU Xeon E5 series 2200 MHz, 2 CPUs (48 cores) : NGFW Version 7.2.8 ! hostname Firepower-module1 enable password ***** encrypted strong-encryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 names no mac-address auto ! interface Port-channel2 no nameif no security-level no ip address ! interface Port-channel2.202 vlan 202 nameif NET202 cts manual propagate sgt preserve-untag policy static sgt disabled trusted	> **show running-config** : Saved : : Serial Number: FLM2108V9YG : Hardware: FPR4K-SM-24, 73853 MB RAM, CPU Xeon E5 series 2200 MHz, 2 CPUs (48 cores) : NGFW Version 7.2.8 ! hostname Firepower-module1 enable password ***** encrypted strong-encryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 names no mac-address auto ! interface Port-channel2 no nameif no security-level no ip address ! interface Port-channel2.202 vlan 202 nameif NET202 cts manual propagate sgt preserve-untag policy static sgt disabled trusted

security-level 0 **ip address 172.16.202.1 255.255.255.0 standby 172.16.202.2** ! interface Port-channel2.203 vlan 203 nameif NET203 cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 **ip address 172.16.203.1 255.255.255.0 standby 172.16.203.2** ! interface Port-channel3 description LAN/STATE Failover Interface ! interface Ethernet1/1 management-only nameif diagnostic cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 no ip address ! interface Ethernet1/4 nameif NET204 cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 **ip address 172.16.204.1 255.255.255.0 standby 172.16.204.2** ! ftp mode passive ngips conn-match vlan-id no object-group-search access-control access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL_ advanced permit gre	security-level 0 **ip address 172.16.202.1 255.255.255.0 standby 172.16.202.2** ! interface Port-channel2.203 vlan 203 nameif NET203 cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 **ip address 172.16.203.1 255.255.255.0 standby 172.16.203.2** ! interface Port-channel3 description LAN/STATE Failover Interface ! interface Ethernet1/1 management-only nameif diagnostic cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 no ip address ! interface Ethernet1/4 nameif NET204 cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 **ip address 172.16.204.1 255.255.255.0 standby 172.16.204.2** ! ftp mode passive ngips conn-match vlan-id no object-group-search access-control access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL_ advanced permit gre

any any rule-id 9998 access-list CSM_FW_ACL_ remark rule-id 268434433: ACCESS POLICY: acp_simple - Default access-list CSM_FW_ACL_ remark rule-id 268434433: L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434433 ! tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 18 allow tcp-options range 20 255 allow tcp-options md5 clear urgent-flag allow ! no pager no logging message 106015 no logging message 313001 no logging message 313008 no logging message 106023 no logging message 710003 no logging message 106100 no logging message 302015 no logging message 302014 no logging message 302013 no logging message 302018 no logging message 302017 no logging message 302016 no logging message 302021 no logging message 302020 mtu NET202 1500 mtu NET203 1500 mtu diagnostic 1500 mtu NET204 1500 **failover** **failover lan unit primary** **failover lan interface FOVER Port-channel3** **failover replication http** **failover link FOVER Port-channel3** **failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2** monitor-interface NET202 monitor-interface NET203 icmp unreachable rate-limit 1 burst-size 1 <output omitted>	any any rule-id 9998 access-list CSM_FW_ACL_ remark rule-id 268434433: ACCESS POLICY: acp_simple - Default access-list CSM_FW_ACL_ remark rule-id 268434433: L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434433 ! tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 18 allow tcp-options range 20 255 allow tcp-options md5 clear urgent-flag allow ! no pager no logging message 106015 no logging message 313001 no logging message 313008 no logging message 106023 no logging message 710003 no logging message 106100 no logging message 302015 no logging message 302014 no logging message 302013 no logging message 302018 no logging message 302017 no logging message 302016 no logging message 302021 no logging message 302020 mtu NET202 1500 mtu NET203 1500 mtu diagnostic 1500 mtu NET204 1500 **failover** **failover lan unit secondary** **failover lan interface FOVER Port-channel3** **failover replication http** **failover link FOVER Port-channel3** **failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2** monitor-interface NET202 monitor-interface NET203 icmp unreachable rate-limit 1 burst-size 1 <output omitted>
> **show ip** System IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG	> **show ip** System IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG

Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG
Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset
Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG
Current IP Addresses:
Interface Name IP address Subnet mask Method
Port-channel2.202 NET202 172.16.202.2 255.255.255.0 CONFIG
Port-channel2.203 NET203 172.16.203.2 255.255.255.0 CONFIG
Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset
Ethernet1/4 NET204 172.16.204.2 255.255.255.0 CONFIG

> **show failover**
Failover On
Failover unit Primary
Failover LAN Interface: FOVER Port-channel3 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 1291 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.18(4)210, Mate 9.18(4)210
Serial Number: Ours FLM1949C5RR, Mate FLM2108V9YG
Last Failover at: 13:56:37 UTC Jul 16 2024
This host: Primary - Standby Ready
Active time: 0 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys)
Interface NET202 (172.16.202.2): Normal (Monitored)
Interface NET203 (172.16.203.2): Normal (Monitored)
Interface diagnostic (0.0.0.0): Normal (Waiting)
Interface NET204 (172.16.204.2): Normal (Monitored)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)
Other host: Secondary - Active
Active time: 70293 (sec)
Interface NET202 (172.16.202.1): Normal (Monitored)
Interface NET203 (172.16.203.1): Normal (Monitored)
Interface diagnostic (0.0.0.0): Normal (Waiting)
Interface NET204 (172.16.204.1): Normal

Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG
Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset
Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG
Current IP Addresses:
Interface Name IP address Subnet mask Method
Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG
Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG
Port-channel3 FOVER 172.16.51.2 255.255.255.0 unset
Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG

> **show failover**
Failover On
Failover unit Secondary
Failover LAN Interface: FOVER Port-channel3 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 1291 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.18(4)210, Mate 9.18(4)210
Serial Number: Ours FLM2108V9YG, Mate FLM1949C5RR
Last Failover at: 13:42:35 UTC Jul 16 2024
This host: Secondary - Active
Active time: 70312 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys)
Interface NET202 (172.16.202.1): Normal (Monitored)
Interface NET203 (172.16.203.1): Normal (Monitored)
Interface diagnostic (0.0.0.0): Normal (Waiting)
Interface NET204 (172.16.204.1): Normal (Monitored)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)
Other host: Primary - Standby Ready
Active time: 0 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys)
Interface NET202 (172.16.202.2): Normal (Monitored)
Interface NET203 (172.16.203.2): Normal (Monitored)

(Monitored) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0) status (up) <output omitted>	Interface diagnostic (0.0.0.0): Normal (Waiting) Interface NET204 (172.16.204.2): Normal (Monitored) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0) status (up) <output omitted>

Step 4. Both FTD devices were unregistered from the FMC:

<#root>

```
> show managers

No managers configured.
```

Main points to note for the Disable HA option in FMC:

Primary Unit	**Secondary Unit**
The device is removed from the FMC. No configuration is removed from the FTD device.	The device is removed from the FMC. No configuration is removed from the FTD device.

Scenario 1

Run the '**configure high-availability disable**' command to remove the failover configuration from the Active FTD device:

<#root>

```
>

configure high-availability disable

 ?
Optional parameter to clear interfaces (clear-interfaces) optional parameter to clear interfaces (clear
<cr>
```

<#root>

```
>

configure high-availability disable

High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':

yes

Successfully disabled high-availability.
```

The result:

Primary Unit (ex-Standby)	**Secondary Unit (ex-Active)**
> INFO: This unit is currently in standby state. By disabling failover, this unit will remain in standby state. > **show failover** **Failover Off (pseudo-Standby)** Failover unit Primary Failover LAN Interface: FOVER Port-channel3 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 0 of 1291 maximum MAC Address Move Notification Interval not set failover replication http > **show ip** System IP Addresses: Interface Name IP address Subnet mask Method Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Current IP Addresses: Interface Name IP address Subnet mask Method Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset	> **show failover** Failover Off Failover unit Secondary Failover LAN Interface: not Configured Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 4 of 1291 maximum MAC Address Move Notification Interval not set > **show ip** System IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG Current IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG
Primary (ex-Standby)	**Secondary (ex-Active)**
> **show running-config** : Saved : : Serial Number: FLM1949C5RR : Hardware: FPR4K-SM-24, 73853 MB RAM, CPU	> **show running-config** : Saved : : Serial Number: FLM2108V9YG : Hardware: FPR4K-SM-24, 73853 MB RAM, CPU

Xeon E5 series 2200 MHz, 2 CPUs (48 cores) : NGFW Version 7.2.8 ! hostname Firepower-module1 enable password ***** encrypted strong-encryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 names no mac-address auto ! interface Port-channel2 shutdown no nameif no security-level no ip address <- **IPs are removed** ! interface Port-channel3 description LAN/STATE Failover Interface ! interface Ethernet1/1 management-only shutdown no nameif no security-level no ip address ! interface Ethernet1/4 shutdown no nameif no security-level no ip address ! ftp mode passive ngips conn-match vlan-id no object-group-search access-control access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL_ advanced permit gre	Xeon E5 series 2200 MHz, 2 CPUs (48 cores) : NGFW Version 7.2.8 ! hostname Firepower-module1 enable password ***** encrypted strong-encryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 names no mac-address auto ! interface Port-channel2 no nameif no security-level no ip address ! interface Port-channel2.202 vlan 202 nameif NET202 cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 **ip address 172.16.202.1 255.255.255.0 standby 172.16.202.2** ! interface Port-channel2.203 vlan 203 nameif NET203 cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 **ip address 172.16.203.1 255.255.255.0 standby 172.16.203.2** ! interface Port-channel3 no nameif no security-level no ip address ! interface Ethernet1/1 management-only nameif diagnostic cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 no ip address ! interface Ethernet1/4

```
any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id
268434433: ACCESS POLICY: acp_simple -
Default
access-list CSM_FW_ACL_ remark rule-id
268434433: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip any
any rule-id 268434433
!
tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow
tcp-options range 9 18 allow
tcp-options range 20 255 allow
tcp-options md5 clear
urgent-flag allow
!
no pager
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
no failover
failover lan unit primary
failover lan interface FOVER Port-channel3
failover replication http
failover link FOVER Port-channel3
failover interface ip FOVER 172.16.51.1
255.255.255.0 standby 172.16.51.2
no monitor-interface service-module

<output omitted>
```

```
nameif NET204
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 172.16.204.1 255.255.255.0 standby
172.16.204.2
!
ftp mode passive
ngips conn-match vlan-id
no object-group-search access-control
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id 9998:
PREFILTER POLICY: Default Tunnel and Priority
Policy
access-list CSM_FW_ACL_ remark rule-id 9998:
RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit ipinip
any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp
any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp
any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any
any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre
any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id
268434433: ACCESS POLICY: acp_simple -
Default
access-list CSM_FW_ACL_ remark rule-id
268434433: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip any
any rule-id 268434433
!
tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow
tcp-options range 9 18 allow
tcp-options range 20 255 allow
tcp-options md5 clear
urgent-flag allow
!
no pager
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
```

	no logging message 302017 no logging message 302016 no logging message 302021 no logging message 302020 mtu NET202 1500 mtu NET203 1500 mtu diagnostic 1500 mtu NET204 1500 **no failover** monitor-interface NET202 monitor-interface NET203 no monitor-interface service-module

Main points to note for the Disable HA from Active FTD CLI:

Active Unit	**Standby Unit**
• Failover configuration is removed • Standby IPs are not removed	• Interface configurations are removed. • Failover configuration is not removed, but failover is disabled (pseudo-Standby)

At this point you can disable the HA also on the ex-Standby unit.

Scenario 2 (**Not recommended**)

Warning: This scenario leads to Active/Active situation, thus it is not recommended. It is shown only for awareness.

Run the **'configure high-availability disable'** command to remove the failover configuration from the Standby FTD device:

```
<#root>

>

configure high-availability disable


High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':

YES


Successfully disabled high-availability.
```

The result:

Primary (ex-Standby)	Secondary (Active)
> **show failover** Failover Off Failover unit Secondary Failover LAN Interface: not Configured Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 4 of 1291 maximum MAC Address Move Notification Interval not set > **show ip** System IP Addresses: Interface Name IP address Subnet mask Method **Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manual <- The device uses the same IPs as the ex-Active!** Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manual Ethernet1/4 NET204 172.16.204.1 255.255.255.0 manual Current IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manual Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manual Ethernet1/4 NET204 172.16.204.1 255.255.255.0 manual	> **show failover** **Failover On <- Failover is not disabled** Failover unit Secondary Failover LAN Interface: FOVER Port-channel3 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 4 of 1291 maximum MAC Address Move Notification Interval not set failover replication http Version: Ours 9.18(4)210, Mate 9.18(4)210 Serial Number: Ours FLM2108V9YG, Mate FLM1949C5RR Last Failover at: 12:44:06 UTC Jul 17 2024 This host: Secondary - Active Active time: 632 (sec) slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys) Interface diagnostic (0.0.0.0): Normal (Waiting) Interface NET204 (172.16.204.1): Normal (Monitored) Interface NET203 (172.16.203.1): Normal (Monitored) Interface NET202 (172.16.202.1): Normal (Monitored) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0) status (up) Other host: Primary - Disabled Active time: 932 (sec) slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys) Interface diagnostic (0.0.0.0): Unknown (Waiting) Interface NET204 (172.16.204.2): Unknown (Monitored) Interface NET203 (172.16.203.2): Unknown (Monitored) Interface NET202 (172.16.202.2): Unknown (Monitored) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0) status (up) > **show ip** System IP Addresses: Interface Name IP address Subnet mask Method **Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manual <- The device uses the same IPs as the ex-Standby!** Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manual

	Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Ethernet1/4 NET204 172.16.204.1 255.255.255.0 manual Current IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manual Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manual Port-channel3 FOVER 172.16.51.2 255.255.255.0 unset Ethernet1/4 NET204 172.16.204.1 255.255.255.0 manual

Main points to note for the Disable HA from Active FTD CLI:

Active Unit	**Standby Unit**
• Failover configuration is not removed and remains enabled • The device uses the same IPs as the ex-Standby unit	• Failover configuration is removed • The device uses the same IPs as the Active unit

Scenario 3

Run the **'configure high-availability disable clear-interfaces'** command to remove the failover configuration from the Active FTD device:

```
<#root>

>

configure high-availability disable clear-interfaces


High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':

yes


Successfully disabled high-availability.

>
```

The result:

Primary (ex-Standby)	**Secondary (ex-Active)**

> **show failover** **Failover Off (pseudo-Standby)** Failover unit Primary Failover LAN Interface: FOVER Port-channel3 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 0 of 1291 maximum MAC Address Move Notification Interval not set failover replication http > **show ip** System IP Addresses: Interface Name IP address Subnet mask Method Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Current IP Addresses: Interface Name IP address Subnet mask Method Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset >	> **show failover** Failover Off Failover unit Secondary Failover LAN Interface: not Configured Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 0 of 1291 maximum MAC Address Move Notification Interval not set > **show ip** System IP Addresses: Interface Name IP address Subnet mask Method Current IP Addresses: Interface Name IP address Subnet mask Method >

Main points to note for the Disable HA along with '**clear-interfaces**' from Active FTD CLI:

Active Unit	**Standby Unit**
• Failover configuration is removed • The IPs are removed	• Failover configuration is not removed, but failover is disabled (pseudo-Standby) • The IPs are removed

Scenario 4

Run the '**configure high-availability disable clear-interfaces**' command to remove the failover configuration from the Standby FTD device:

```
<#root>

>

configure high-availability disable clear-interfaces


High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':

YES


Successfully disabled high-availability.
```

>

The result:

Primary (ex-Standby)	**Secondary (Active)**
> **show failover** **Failover Off** Failover unit Secondary Failover LAN Interface: not Configured Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 0 of 1291 maximum MAC Address Move Notification Interval not set > **show ip** System IP Addresses: Interface Name IP address Subnet mask Method Current IP Addresses: Interface Name IP address Subnet mask Method >	> **show failover** **Failover On** Failover unit Secondary Failover LAN Interface: FOVER Port-channel3 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 4 of 1291 maximum MAC Address Move Notification Interval not set failover replication http Version: Ours 9.18(4)210, Mate 9.18(4)210 Serial Number: Ours FLM2108V9YG, Mate FLM1949C5RR Last Failover at: 07:06:56 UTC Jul 18 2024 This host: Secondary - Active Active time: 1194 (sec) slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys) Interface diagnostic (0.0.0.0): Normal (Waiting) Interface NET204 (172.16.204.1): Normal (Monitored) Interface NET202 (172.16.202.1): Normal (Monitored) Interface NET203 (172.16.203.1): Normal (Monitored) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0) status (up) Other host: Primary - Disabled Active time: 846 (sec) slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys) Interface diagnostic (0.0.0.0): Unknown (Waiting) Interface NET204 (172.16.204.2): Unknown (Monitored) Interface NET202 (172.16.202.2): Unknown (Monitored) Interface NET203 (172.16.203.2): Unknown (Monitored) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0) status (up) > **show ip**

	System IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manual Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manual Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Ethernet1/4 NET204 172.16.204.1 255.255.255.0 manual Current IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manual Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manual Port-channel3 FOVER 172.16.51.2 255.255.255.0 unset Ethernet1/4 NET204 172.16.204.1 255.255.255.0 manual

Main points to note for the Disable HA along with '**clear-interfaces**' from Active FTD CLI:

Active Unit	**Standby Unit**
• Failover configuration is not removed • The IPs are not removed	• Failover configuration is removed • The IPs are removed

Step 6. After you finish the task, register the devices to the FMC and enable HA pair.

Task 7. Suspend HA

Task requirement:

Suspend the HA from the FTD CLISH CLI

Solution:

Step 1. On the Primary FTD, run the command and confirm (type **YES**).

<#root>

```
> configure high-availability suspend

Please ensure that no deployment operation is in progress before suspending high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to

YES

Successfully suspended high-availability.
```

Step 2. Verify the changes on Primary unit:

<#root>

>

show high-availability config

Failover Off

```
Failover unit Primary
Failover LAN Interface: fover_link Ethernet1/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

Step 3. The result on Secondary unit:

<#root>

>

show high-availability config
Failover Off (pseudo-Standby)

```
Failover unit Secondary
Failover LAN Interface: fover_link Ethernet1/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

Step 4. Resume HA on Primary unit:

<#root>

>

configure high-availability resume

```
Successfully resumed high-availablity.
```

```
> .

    No Active mate detected
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate
```

```
>
```

```
<#root>
```

```
>
```

show high-availability config

Failover On

```
Failover unit Primary
Failover LAN Interface: fover_link Ethernet1/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

Step 5. The result on the Secondary unit after you resume HA:

```
<#root>
```

```
> ..
```

Detected an Active mate

```
Beginning configuration replication from mate.


WARNING: Failover is enabled but standby IP address is not configured for this interface.
WARNING: Failover is enabled but standby IP address is not configured for this interface.
End configuration replication from mate.
```

```
>
```

```
<#root>
```

```
>
```

show high-availability config

Failover On

```
Failover unit Secondary
Failover LAN Interface: fover_link Ethernet1/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

>

Frequently Asked Questions (FAQ)

When the configuration is replicated, is it saved immediately (line-by-line) or at the end of the replication?
At the end of the replication. The evidence is at the end of the **debug fover sync** command output which shows the config/command replication:

<#root>

```
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1506 remark rule-id 268442578: L7 RUL
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1507 advanced permit tcp object-group
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1508 remark rule-id 268442078: ACCESS
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1509 remark rule-id 268442078: L4 RUL
...
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: ACC
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: L7
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: ACC
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: L4
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268442078
cli_xml_server: frep_write_cmd: Cmd: crypto isakmp nat-traversal
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_311
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_433
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_6
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_2
cli_xml_server: frep_write_cmd: Cmd:

write memory        <--
```

What happens if a unit is in a pseudo-Standby state (failover disabled) and then you reload it while the other unit has failover enabled and is Active?
You end up in an Active/Active scenario (although technically it is an Active/Failover-off). Specifically, once the unit comes UP the failover is disabled, but the unit uses the same IPs as the Active unit. So effectively, you have:

- Unit-1: Active
- Unit-2: failover is off. The unit uses the same data IPs as Unit-1, but different MAC addresses.

What happens to the failover configuration if you manually disable the failover (configure high-availability suspend), and then you reload the device?
When you disable the failover, it is not a permanent change (not saved in the startup-config unless you decide to do this explicitly). You can reboot/reload the unit in 2 different ways and with the second way you must be careful:

Case 1. Reboot from CLISH

Reboot from CLISH does not ask for confirmation. Thus, the configuration change is not saved into startup-config:

```
<#root>

>

configure high-availability suspend

Please ensure that no deployment operation is in progress before suspending high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to

YES

Successfully suspended high-availability.
```

The running-config has the failover disabled. In this case, the unit was Standby and got into the pseudo-Standby state as expected in order to avoid an Active/Active scenario:

```
<#root>

firepower#

show failover | include Failover

Failover Off (

pseudo-Standby

)
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

The startup-config has the failover still enabled:

```
<#root>

firepower#

show startup | include failover

failover

failover lan unit secondary
failover lan interface FOVER Ethernet1/1
failover replication http
failover link FOVER Ethernet1/1
failover interface ip FOVER 192.0.2.1 255.255.255.0 standby 192.0.2.2
failover ipsec pre-shared-key *****
```

Reboot the device from CLISH (**reboot** command):

```
<#root>
```

```
>
```

reboot

```
This command will reboot the system.  Continue?
Please enter 'YES' or 'NO':
```

YES

```
Broadcast message from root@
Threat Defense System: CMD=-stop, CSP-ID=cisco-ftd.6.2.2.81__ftd_001_JMX2119L05CYRIBVX1, FLAG=''
Cisco FTD stopping ...
```

Once the unit is UP, since the failover is enabled, the device enters the failover Negotiation phase and tries to detect the remote peer:

<#root>

```
User enable_1 logged in to firepower
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower> .
```

Detected an Active mate

Case 2. Reboot from LINA CLI
Reboot from LINA (**reload** command) asks for confirmation. Thus, in case you select **Y** (Yes) the configuration change is saved into startup-config:

<#root>

```
firepower#
```

reload

```
System config has been modified. Save? [Y]es/[N]o:
```

Y <-- Be careful. This disables the failover in the startup-config

```
Cryptochecksum: 31857237 8658f618 3234be7c 854d583a

8781 bytes copied in 0.940 secs
Proceed with reload? [confirm]
firepower#
```

show startup | include failover

no failover

```
failover lan unit secondary
failover lan interface FOVER Ethernet1/1
failover replication http
failover link FOVER Ethernet1/1
```

```
failover interface ip FOVER 192.0.2.1 255.255.255.0 standby 192.0.2.2
failover ipsec pre-shared-key *****
```

Once the unit is UP the failover is disabled:

<#root>

```
firepower#
```

show failover | include Fail

Failover Off

```
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

Note: To avoid this scenario, ensure that when you are prompted, you do not save the changes to the startup-config.

Related Information

- All versions of the Cisco Firepower Management Center configuration guide can be found here

Navigating the Cisco Secure Firewall Threat Defense Documentation

- All versions of the FXOS Chassis Manager and CLI configuration guides can be found here

Navigating the Cisco Firepower 4100/9300 FXOS Documentation

- Cisco Global Technical Assistance Center (TAC) strongly recommends this visual guide for in-depth practical knowledge on Cisco Firepower Next-Generation Security Technologies:

Cisco Firepower Threat Defense (FTD): Configuration and Troubleshooting Best Practices for the Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Advanced Malware Protection (AMP)

- For all Configuration and Troubleshoot TechNotes that pertain to the Firepower technologies

Cisco Secure Firewall Management Center

- Technical Support & Documentation - Cisco Systems