Upgrade FTD HA Managed by FDM

Contents

Introduction

This document describes the upgrade process for a Cisco Secure Firewall Threat Defense in High Availability managed by a Firepower Device Manager.

Prerequisites

Requirements

Cisco recommends you have knowledge of these topics:

- High Availability (HA) concepts and configuration
- Cisco Secure Firepower Device Manager (FDM) configuration
- Cisco Secure Firewall Threat Defense (FTD) configuration

Components Used

The information in this document is based on Virtual Cisco FTD, version 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.

Overview

The way the FDM works is to upgrade one peer at a time. First the Standby, then the Active, doing a failover before the Active upgrade gets started.

Background Information

The upgrade package must be downloaded from **software.cisco.com** before the upgrade.

On CLI clish, run the**show high-availability config**command in the Active FTD in order to check the status of the HA.

```
> show high-availability config

Failover On

Failover unit Primary

Failover LAN Interface: failover-link GigabitEthernet0/2 (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 3 of 311 maximum

MAC Address Move Notification Interval not set

failover replication http

Version: Ours 9.18(3)53, Mate 9.18(3)53

Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C

Last Failover at: 11:57:26 UTC Oct 8 2024

        This host: Primary - Active

                Active time: 507441 (sec)

                slot 0: ASAv hw/sw rev (/9.18(3)53) status (Up Sys)

                  Interface diagnostic (0.0.0.0): Normal (Waiting)

                  Interface inside (192.168.45.1): Normal (Waiting)

                  Interface outside (192.168.1.10): Normal (Waiting)

                slot 1: snort rev (1.0)  status (up)

                slot 2: diskstatus rev (1.0)  status (up)

        Other host: Secondary - Standby Ready

                Active time: 8 (sec)

                  Interface diagnostic (0.0.0.0): Normal (Waiting)

                  Interface inside (0.0.0.0): Normal (Waiting)
```

```
  Interface outside (0.0.0.0): Normal (Waiting)

slot 1: snort rev (1.0)  status (up)

slot 2: diskstatus rev (1.0)  status (up)
```

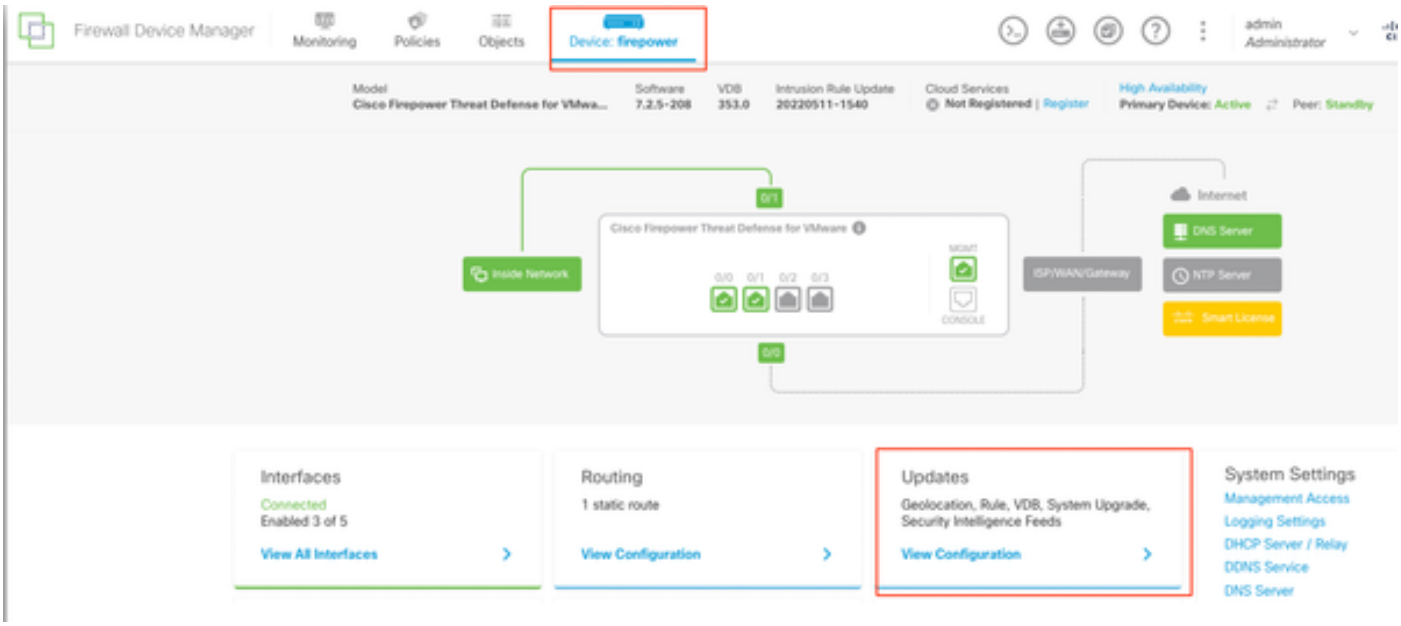
If no errors are visible, then proceed with the upgrade.

Configure

Step 1. Upload Upgrade Package

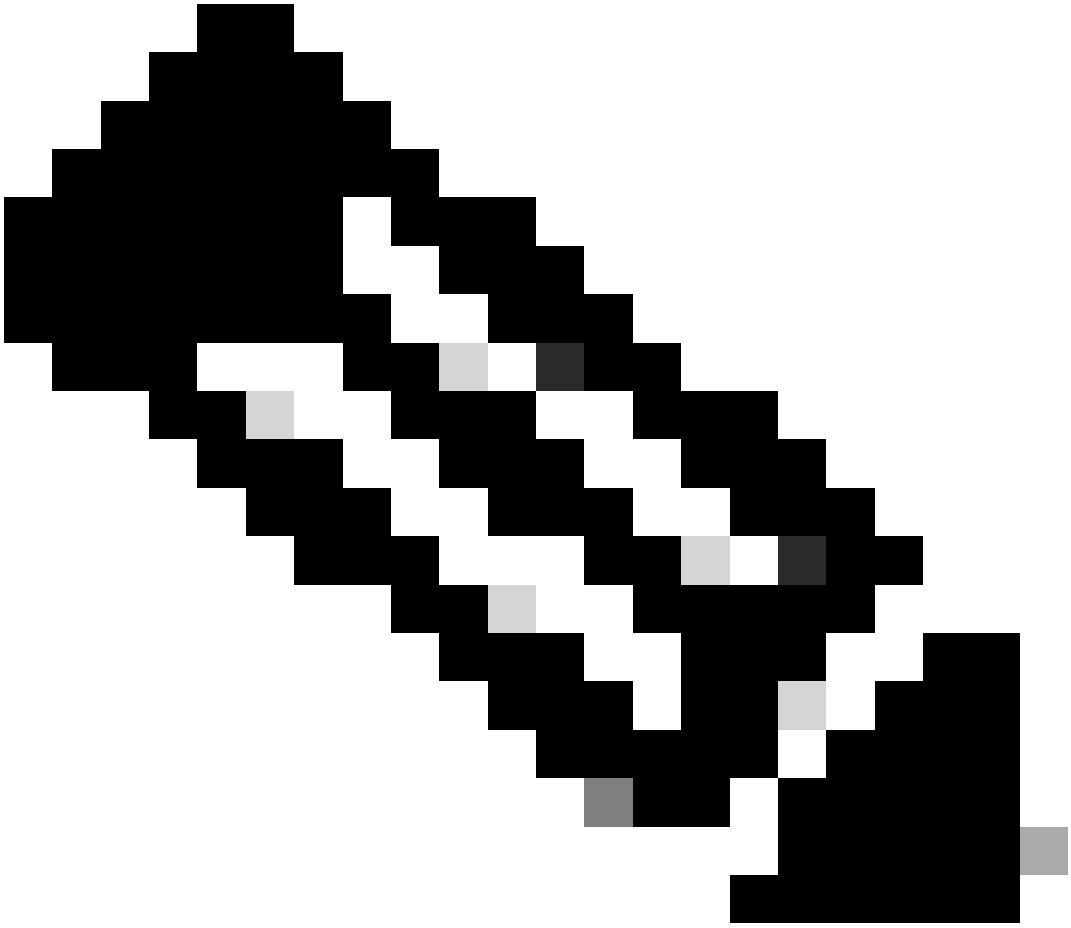
- Upload the FTD upgrade package on the FDM using the GUI.

This has to be previously downloaded from the Cisco Software site based on the FTD model and desired version. Navigate to **Device > Updates > System Upgrade**.

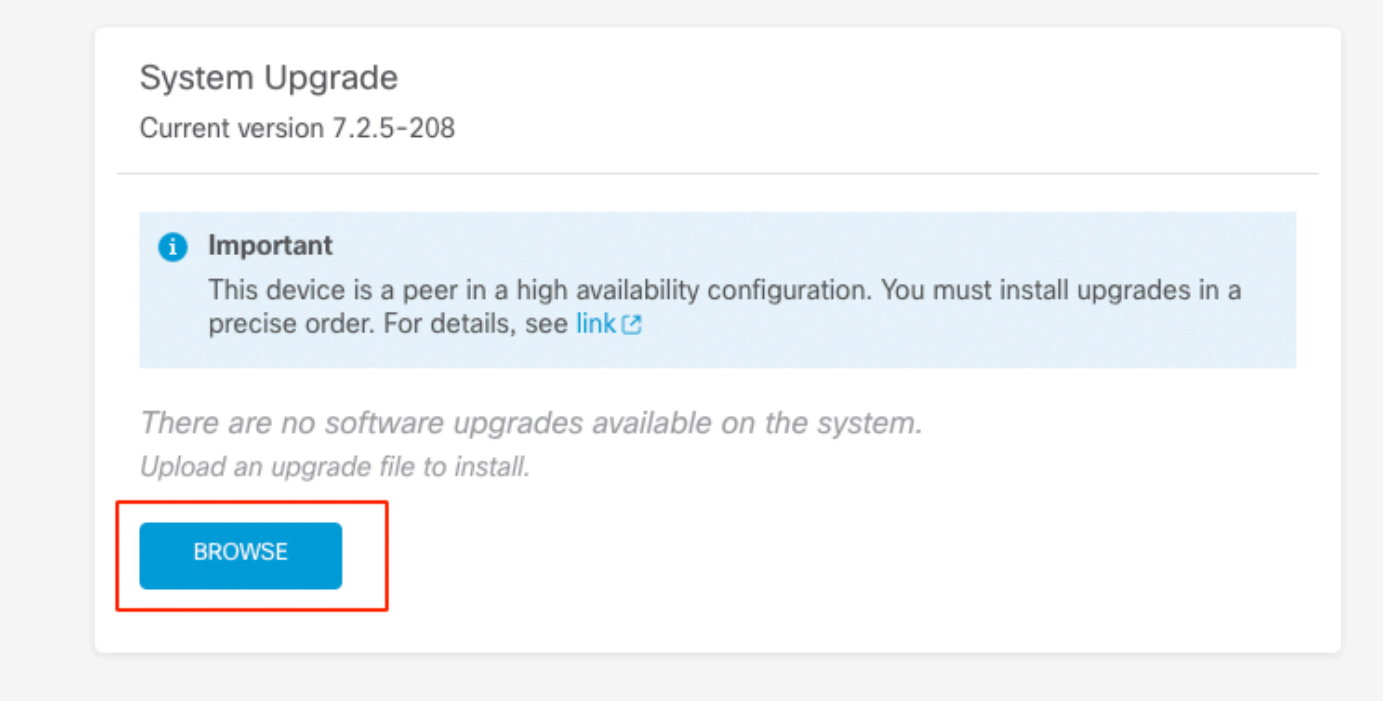


Updates

- Browse for the previously downloaded image, then choose**Upload**.



Note: Upload the image on both active and standby nodes.

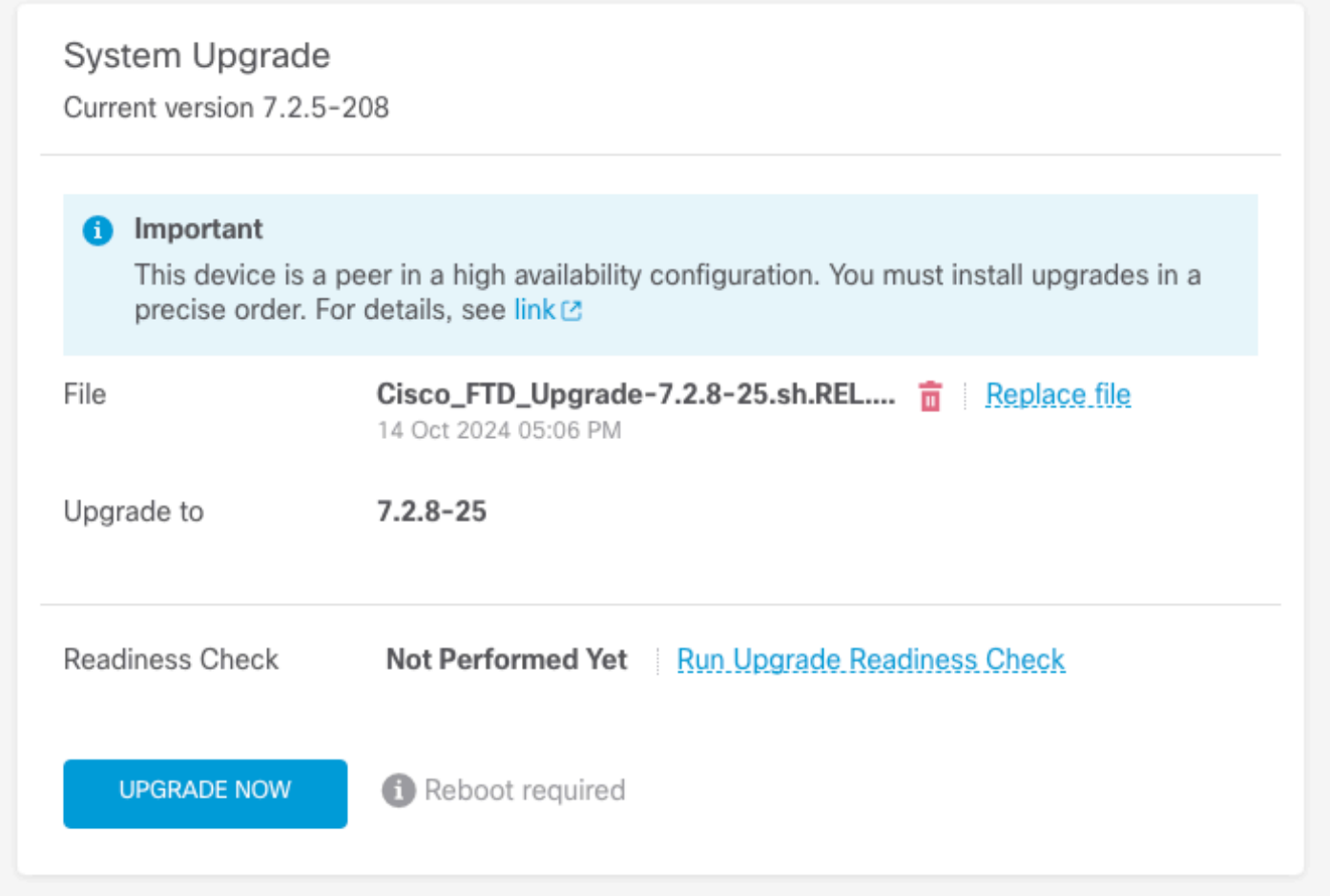


Run Readiness Check

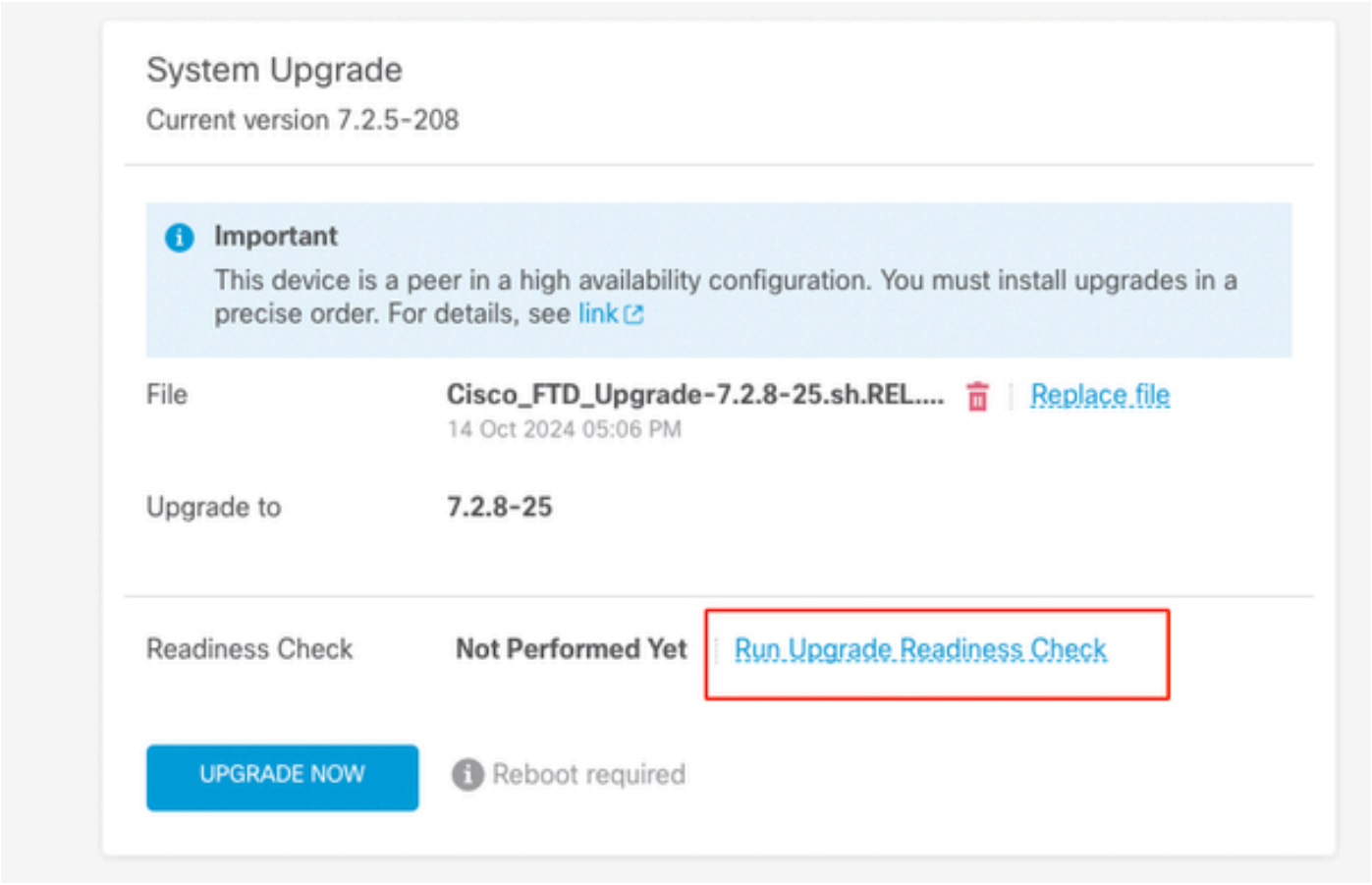
Step 2. Check Readiness

Readiness checks confirm if appliances are ready to proceed with the upgrade.

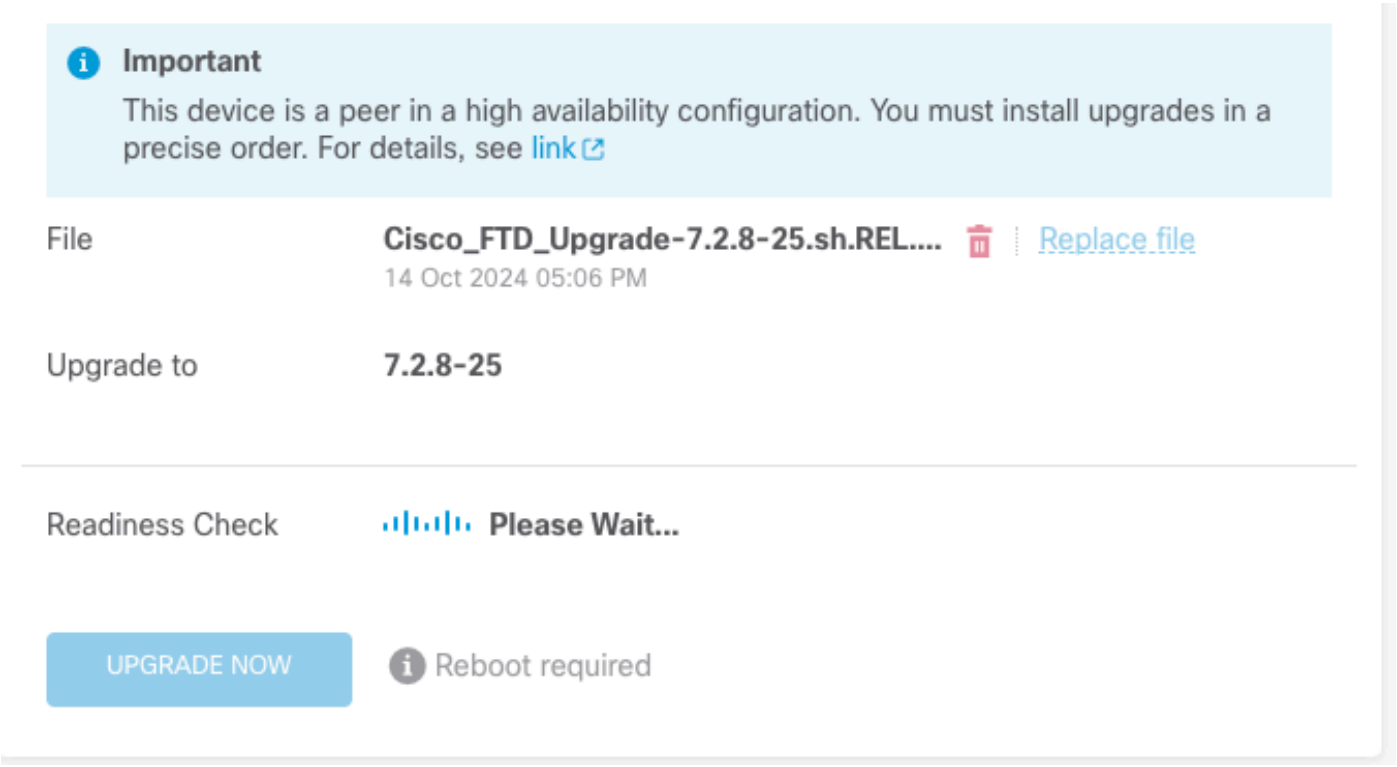
- Choose **Run Upgrade Readiness Check**.



Run Readiness Check

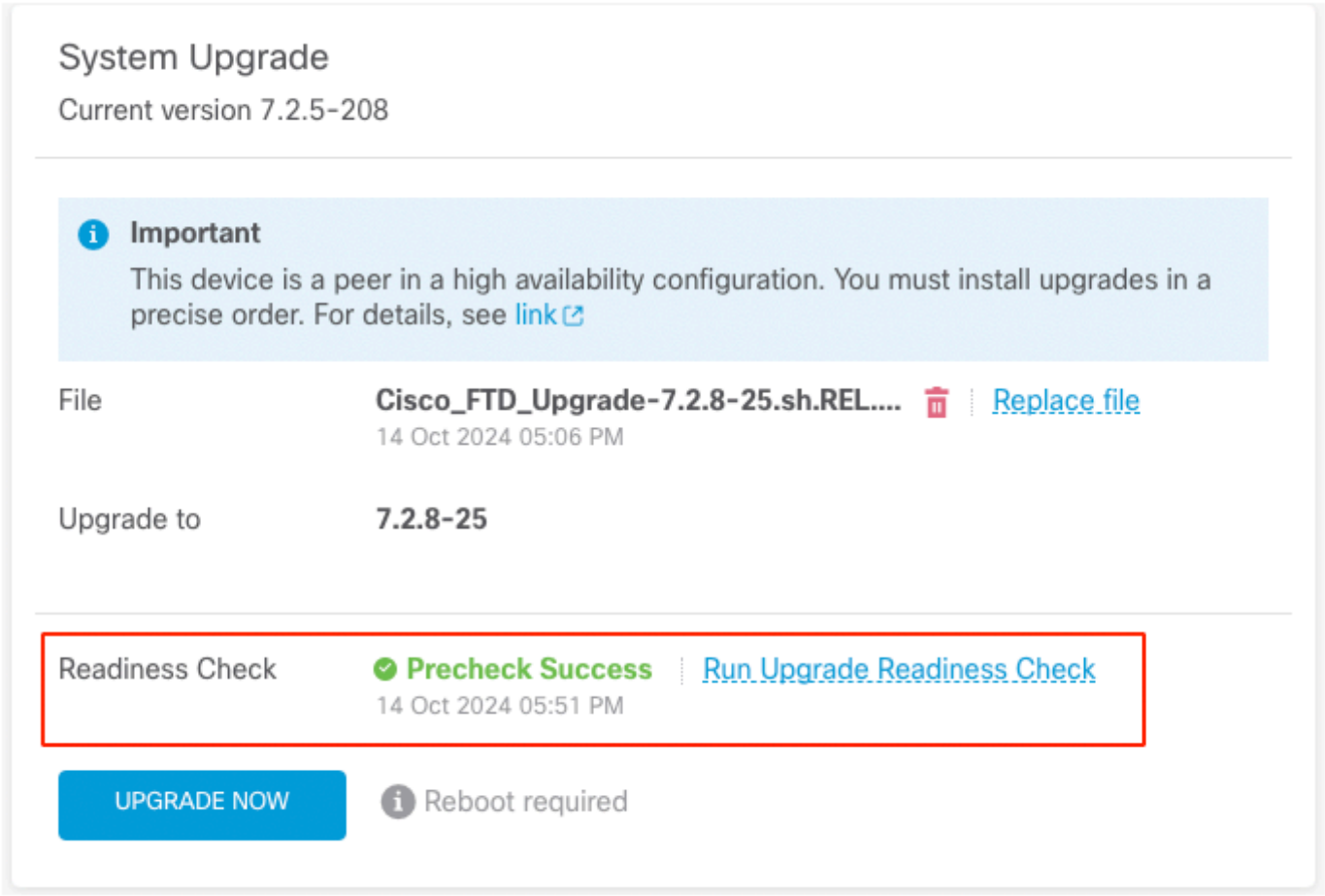


Run Readiness check



Run Readiness Check

The progress can be checked by navigating to **System > Upgrade**.

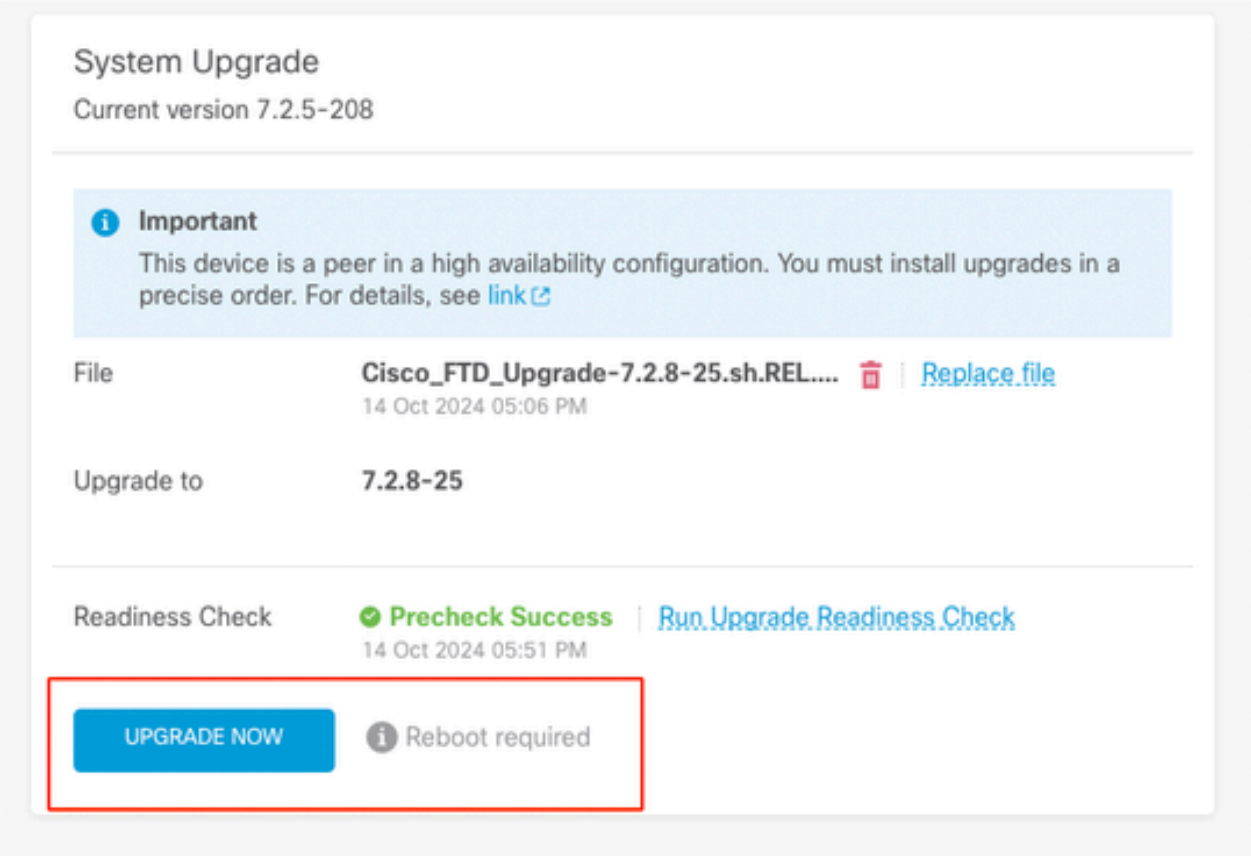


Run Readiness Check

The upgrade can be done when the readiness check is completed in both FTD and the result is Success.

Step 3. Upgrade FTD in HA

- Choose **Standby FDM** and click **Upgrade Now**.

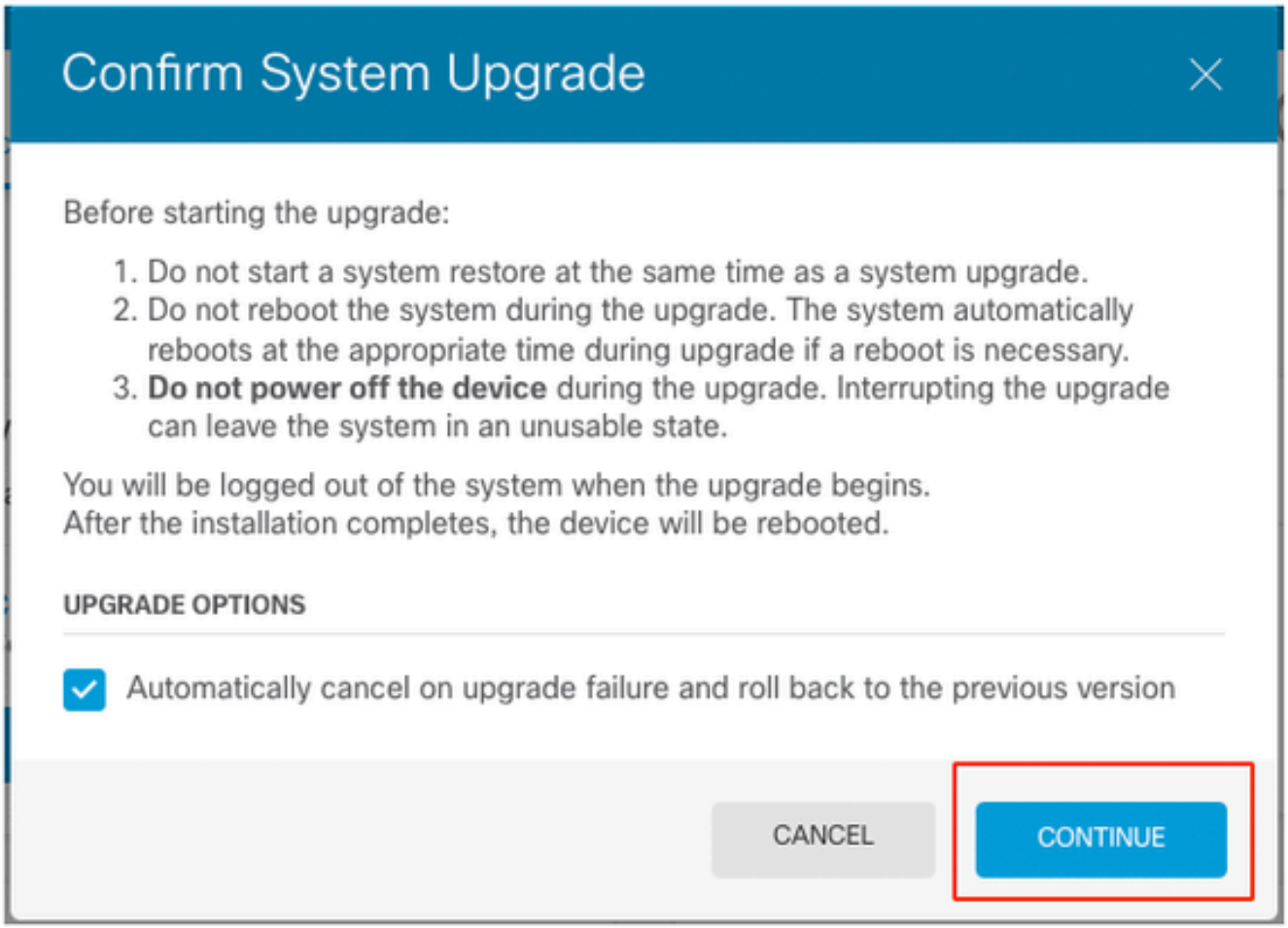


Upgrade Now

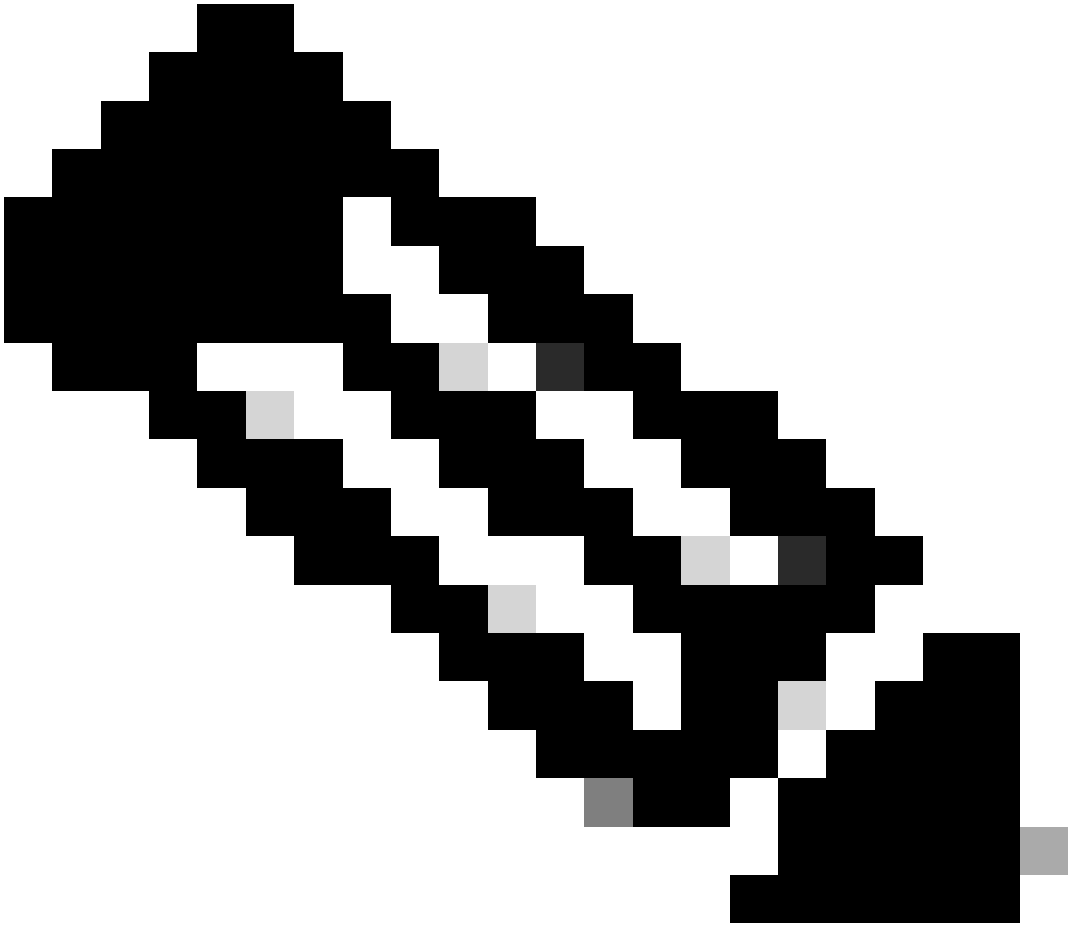
Before starting the upgrade:

1. Do not start a system restore at the same time as a system upgrade.
2. Do not reboot the system during the upgrade. The system automatically reboots at the appropriate time during the upgrade, if a reboot is necessary.
3. Do not power off the deviceduring the upgrade. Interrupting the upgrade can make the system unusable.

You are logged out of the system when the upgrade begins.
After the installation is completed, the device is rebooted.


Confirm System Upgrade
Before starting the upgrade:
1. Do not start a system restore at the same time as a system upgrade.
2. Do not reboot the system during the upgrade. The system automatically reboots at the appropriate time during upgrade if a reboot is necessary.
3. Do not power off the device during the upgrade. Interrupting the upgrade can leave the system in an unusable state.
You will be logged out of the system when the upgrade begins.
After the installation completes, the device will be rebooted.
UPGRADE OPTIONS
Automatically cancel on upgrade failure and roll back to the previous version
CANCEL
CONTINUE

Continue



Note: Upgrade takes around 20 min per FTD.

On CLI, progress can be checked in the upgrade folder /ngfw/var/log/sf; move to**expert mode**and enter**root access**.

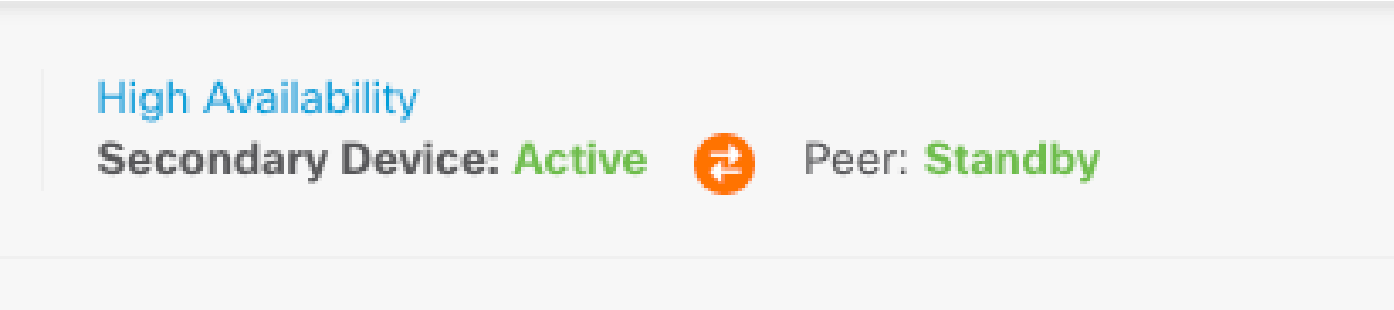
```
> expert

admin@firepower:~$ sudo su

Password:

root@firepower:/home/admin# cd /ngfw/var/log/sf



root@firepower:/ngfw/var/log/sf# ls

Cisco_FTD_Upgrade-7.2.8.
```

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# ls -lrt


root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# tail -f status.log
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/011_check_self.
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/015_verify_rpm.
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_check_dashb
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_get_snort_f
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/110_setup_upgra
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/120_generate_au
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/152_save_etc_sf


ui: Upgrade in progress: (79% done. 5 mins to reboot). Finishing the upgrade... (999_finish/999_zz_inst
ui: Upgrade in progress: (83% done. 4 mins to reboot). Finishing the upgrade... (999_finish/999_zzz_com
ui: Upgrade complete
ui: The system will now reboot.
ui: System will now reboot.


Broadcast message from root@firepower (Mon Oct 14 12:01:26 2024):
System will reboot in 5 seconds due to system upgrade.


Broadcast message from root@firepower (Mon Oct 14 12:01:31 2024):
System will reboot now due to system upgrade.


Broadcast message from root@firepower (Mon Oct 14 12:01:39 2024):
The system is going down for reboot NOW!
```

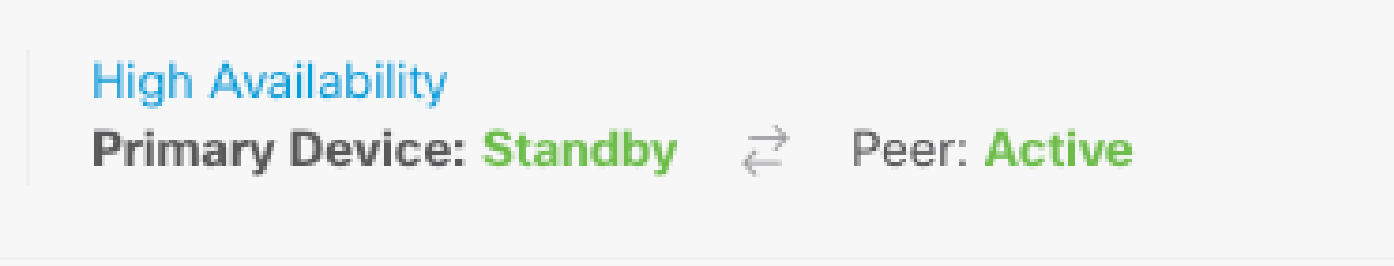
Upgrade the second unit.

Switch roles in order to make this device active: Choose **Device> High Availability**, then choose **Switch Mode** from the gear menu. Wait for the status of the unit in order to change to active and confirm that traffic is flowing normally. Then, log out.

Upgrade: Repeat the previous steps in order to log into the new standby, upload the package, upgrade the device, monitor progress, and verify success.



High Availability



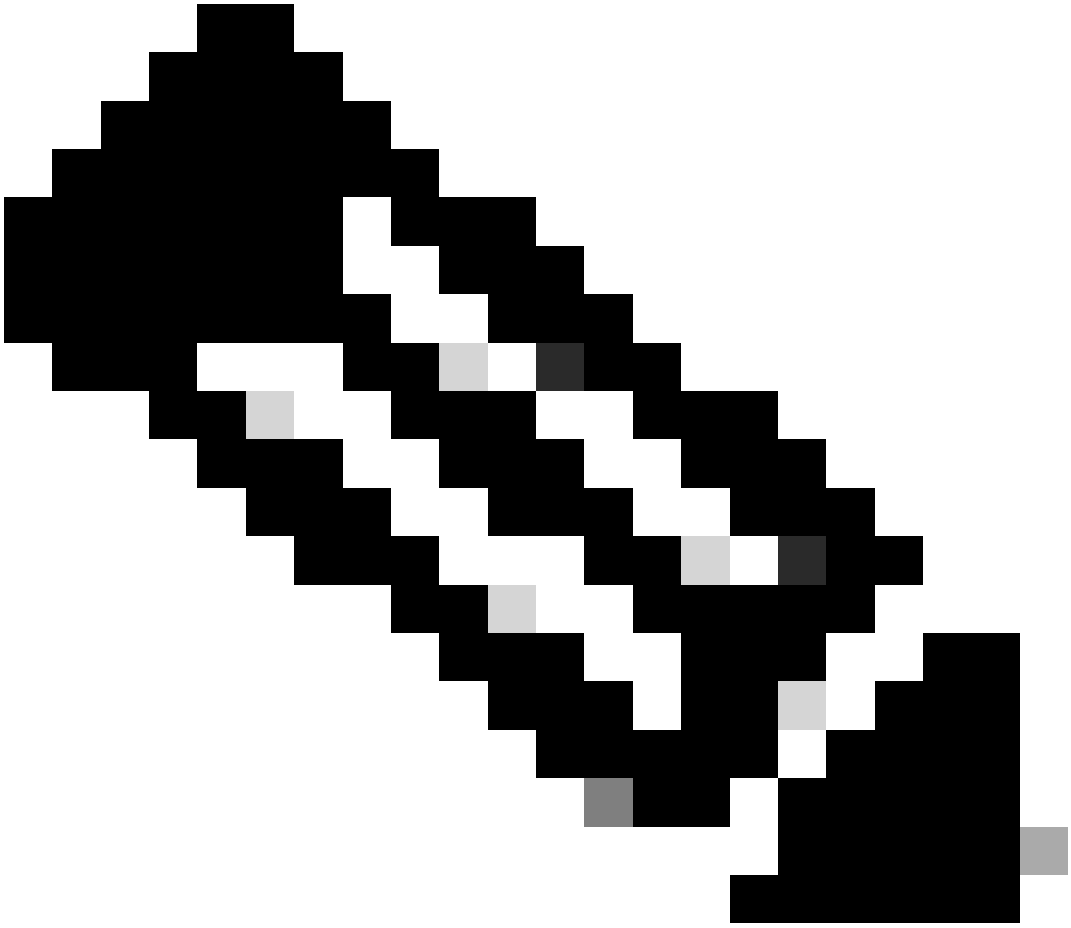
High Availability

On CLI, move to LINA (system support diagnostic-cli) and check the failover state on the Standby FTD using the command**show failover state**.

```
> system support diagnostic-cli

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.

Type help or '?' for a list of available commands.



primary_ha> enable

Password:

primary_ha# show failover state



               State          Last Failure Reason      Date/Time

This host  -   Primary

               Standby Ready  None

Other host -   Secondary
```

```
                Active          None


====Configuration State===

        Sync Skipped - STANDBY

====Communication State===

        Mac set


primary_ha#
```

Step 4. Switch Active Peer (Optional)

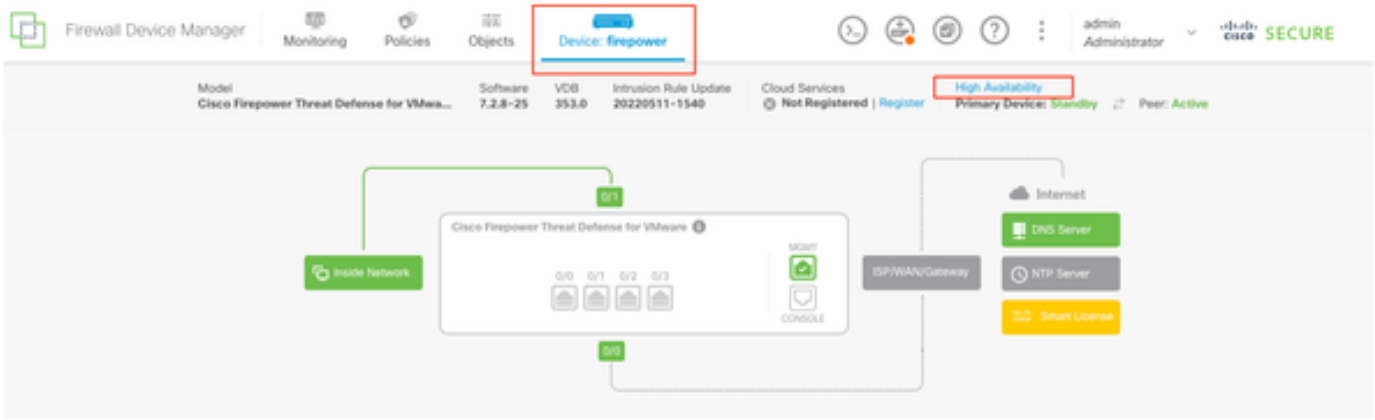


Note: If the Secondary device is Active, it does not have any operational impact.

Having the Primary device as Active and Secondary as Standby is a best practice that helps track any failover that can occur.

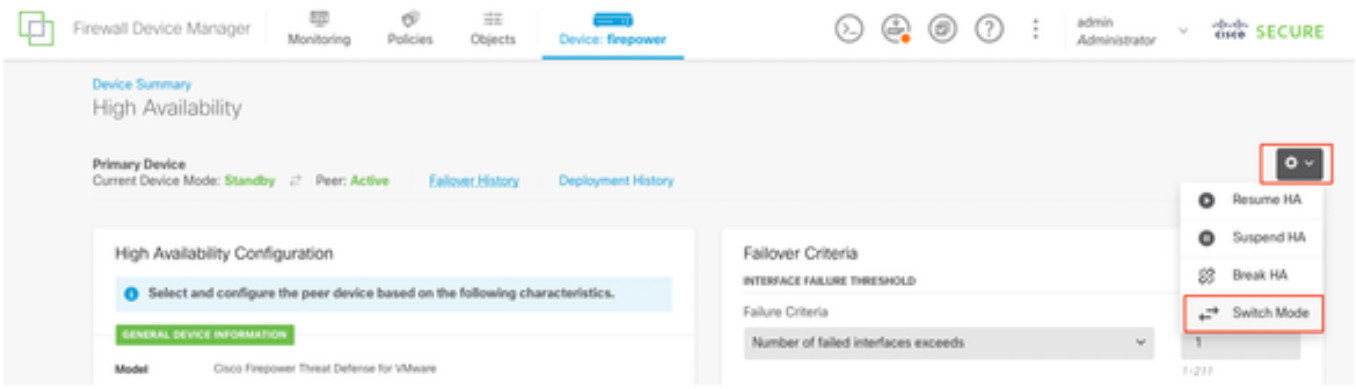
In this case, the FTD Active is now Standby, a manual failover can be used to set it back to Active.

- Navigate to **Devices > High Availability**.



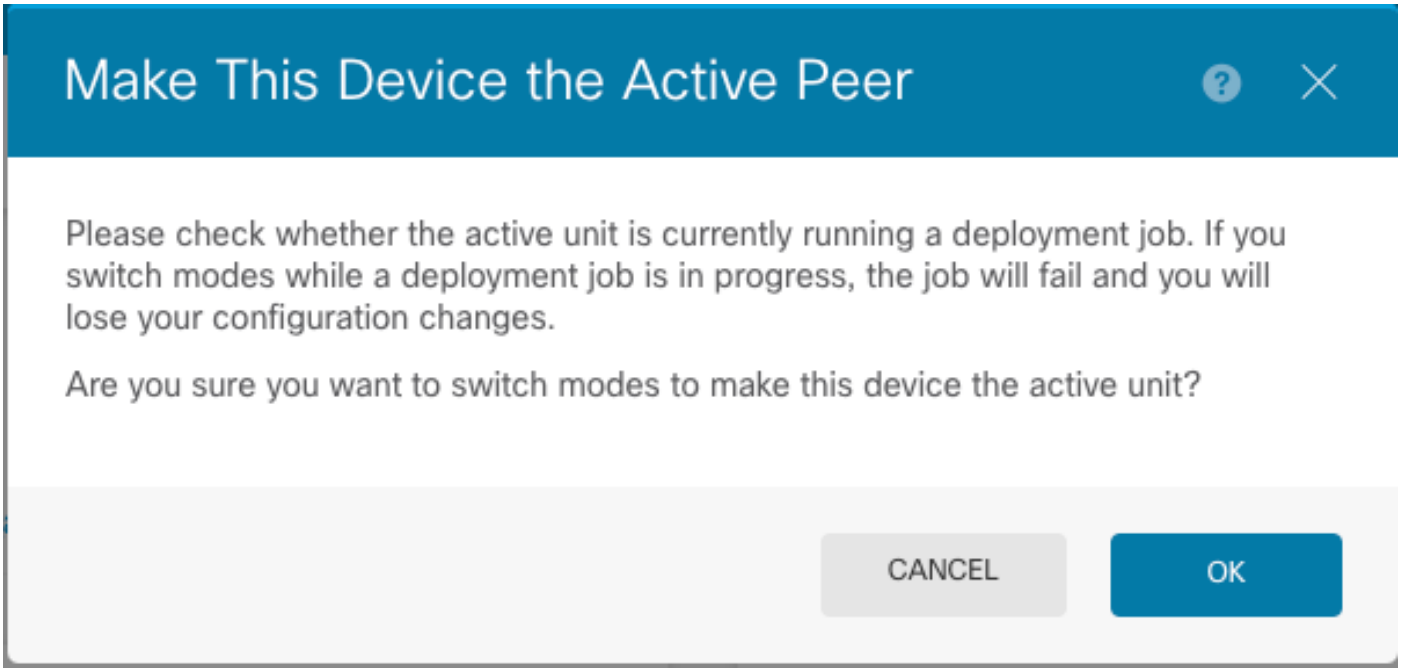
High Availability

- Choose**Switch Mode**.



Switch Mode

- Choose **OK** in order to confirm the failover.



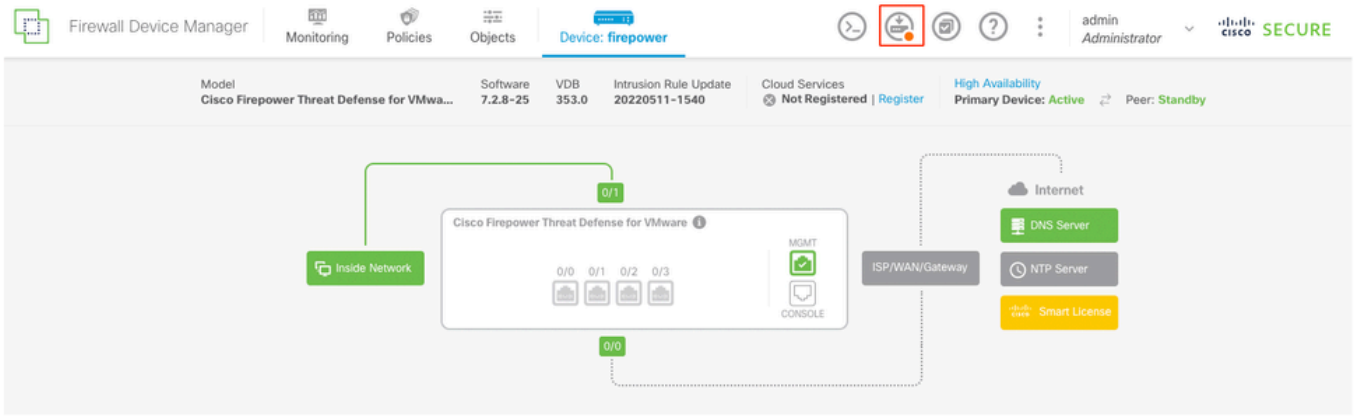
Active Peer

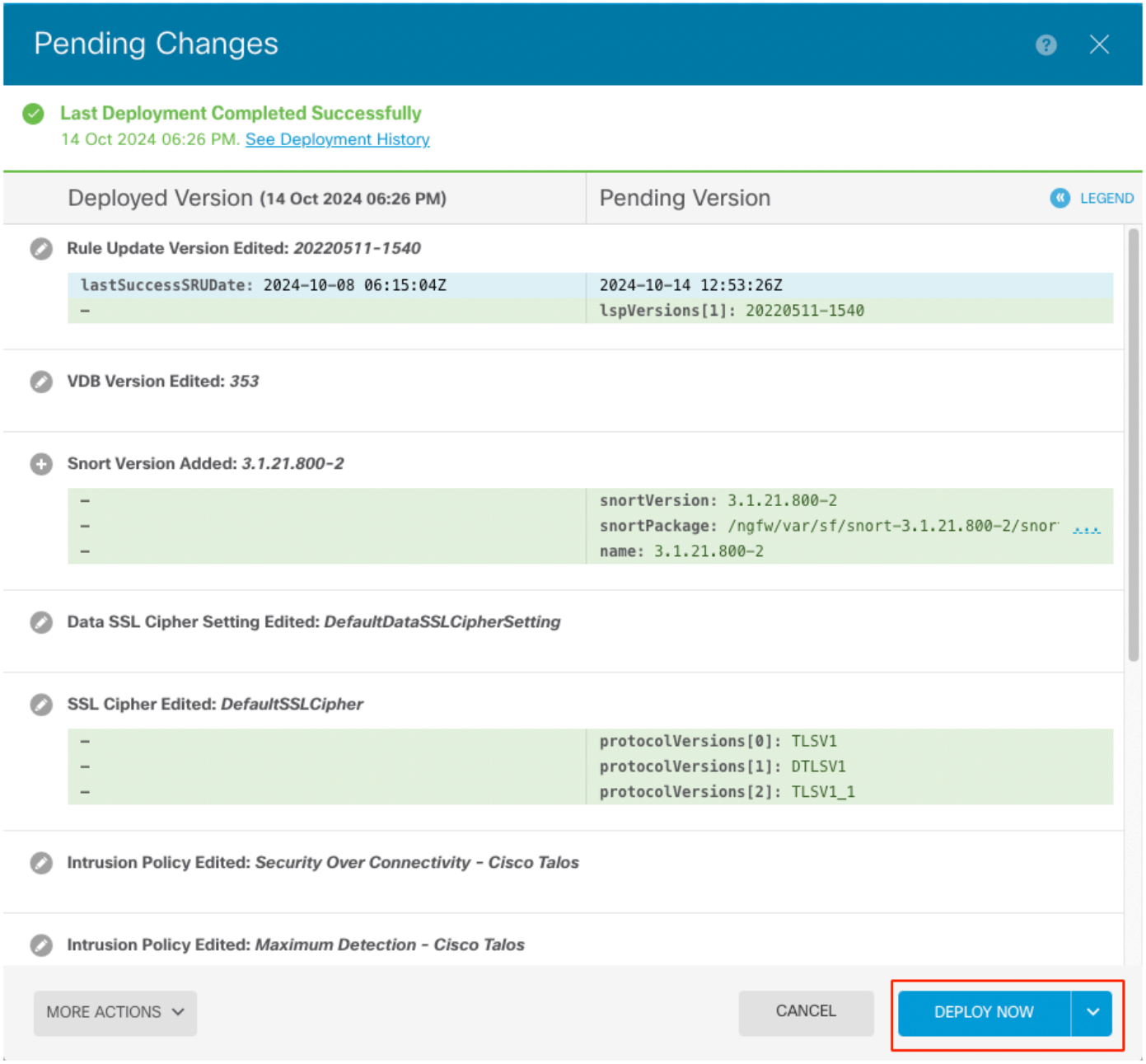
Validation of HA status at the end of the upgrade and failover done.

Devices

Step 5. Final Deploy

- Deploy the policy to devices by clicking **DEPLOY NOW** under the Deployment tab.





Policy Deployment

Validate

In order to validate that HA status and upgrade are complete, you must confirm the status:
Primary: Active
Secondary: Standby Ready

Both are under the version that is the recently changed one (7.2.8 in this example).

Failover

- Over CLI clish, check the failover state using the commands**show failover state**and**show failover**for more detailed information.

Cisco Firepower Extensible Operating System (FX-OS) v2.12.1 (build 73)
Cisco Firepower Threat Defense for VMware v7.2.8 (build 25)

```
> show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  None

====Configuration State===
        Sync Skipped
====Communication State===
        Mac set

> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover-link GigabitEthernet0/2 (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 3 of 311 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 9A1QUNFWPK1, Mate 9A45VNEHB5C
Last Failover at: 14:13:56 UTC Oct 15 2024
        This host: Primary - Active
                Active time: 580 (sec)
                slot 0: ASAv hw/sw rev (/9.18(4)210) status (Up Sys)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface inside (192.168.45.1): Normal (Waiting)
                  Interface outside (192.168.1.10): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - Standby Ready
                Active time: 91512 (sec)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface inside (0.0.0.0): Normal (Waiting)
                  Interface outside (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)


Stateful Failover Logical Update Statistics
        Link : failover-link GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         11797      0          76877      0
        sys cmd         11574      0          11484      0
```

up time	0	0	0	0
RPC services	0	0	0	0
TCP conn	0	0	0	0
UDP conn	176	0	60506	0
ARP tbl	45	0	4561	0
Xlate_Timeout	0	0	0	0
IPv6 ND tbl	0	0	0	0
VPN IKEv1 SA	0	0	0	0
VPN IKEv1 P2	0	0	0	0
VPN IKEv2 SA	0	0	0	0
VPN IKEv2 P2	0	0	0	0
VPN CTCP upd	0	0	0	0
VPN SDI upd	0	0	0	0
VPN DHCP upd	0	0	0	0
SIP Session	0	0	0	0
SIP Tx	0	0	0	0
SIP Pinhole	0	0	0	0
Route Session	1	0	0	0
Router ID	0	0	0	0
User-Identity	0	0	30	0
CTS SGTNAME	0	0	0	0
CTS PAC	0	0	0	0
TrustSec-SXP	0	0	0	0
IPv6 Route	0	0	0	0
STS Table	0	0	0	0
Umbrella Device-ID	0	0	0	0
Rule DB B-Sync	0	0	30	0
Rule DB P-Sync	1	0	266	0
Rule DB Delete	0	0	0	0

```
Logical Update Queue Information
                Cur     Max     Total
Recv Q:         0       31      123591
Xmit Q:         0       1       12100
```

If both FTDs are on the same version, and the HA status is healthy, the upgrade is complete.