Upgrading Cisco HyperFlex 1.8(1f) and 2.0(x)

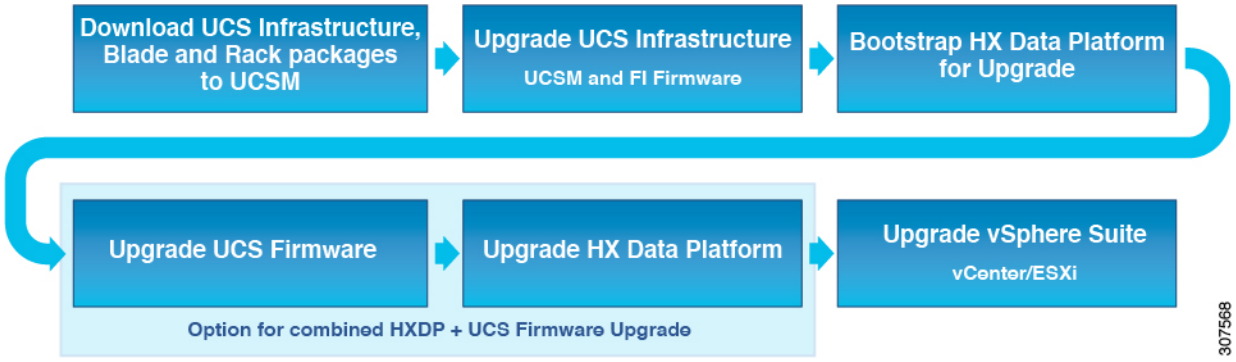
Prerequisites

Before you begin the upgrading process, you should have already completed the following tasks:

- Prerequisites for Upgrading Obsolete Hyperflex Releases
- Hypercheck: HyperFlex and Pre-Upgrade Check Tool
- Verify the ESXi and vCenter Build Number

Upgrade Path for Cisco HyperFlex Data Platform 1.8(1f) or 2.0(x)

Upgrading from Cisco HyperFlex Data Platform 1.8(1f) or 2.0(x) to the Cisco Recommended HXDP release requires that you upgrade to an intermediate release before upgrading to your destination release. You will complete the upgrade workflow twice.



The following outlines your starting release version, the intermediate release you need to upgrade to, and the destination release that completes your upgrade to a recommended Cisco HyperFlex version.

Product	Your Current Release	Upgrade to the Intermediate Release	Upgrade to the Destination Release
Hyperflex software	HXDP 1.8(1f) or 2.0(x)	3.0(1i)	The latest suggested release on theCisco Software Download site.

Product	Your Current Release	Upgrade to the Intermediate Release	Upgrade to the Destination Release
UCS firmware	HXDP 1.8(1f) or 2.0(x)	Minimum version 3.2(3h)	The recommended UCS related firmware based on the suggested HXDP release on the Cisco Software Download site.

You are now ready to begin the Cisco HyperFlex Data Center Upgrade process. Continue to complete each step in the order presented.

The upgrade process consists of the following tasks:

- Upgrading to the Intermediate Release, on page 2
- Upgrade Tasks, on page 8

Upgrading to the Intermediate Release

This upgrade requires that you upgrade to an intermediate release before upgrading to your destination release. Perform the following tasks, using the specified software releases to upgrade to your intermediate release:

- Download software bundles.
- Install software bundles.
- Upgrade UCS Firmware to a minimum version of 3.2(3h).
- Upgrade HyperFlex Data Platform Software to Version 3.0(1i).
- Perform the second upgrade process to the destination version.

Software Downloads: Upgrading to the Intermediate Release

Download the software bundles needed for your upgrade from the Cisco Software Downloads:

- Software Download: Upgrade UCS Firmware to 3.2(3h), on page 2
- Software Download: HXDP Release 3.0(1i) , on page 3

Software Download: Upgrade UCS Firmware to 3.2(3h)

UCS Firmware 3.2(3h)

Before starting the upgrade process, download and install the UCS Infra Package that matches your installation as well as the UCS Blade, and the UCS C-series Package.

Download Link: https://software.cisco.com/download/home/286305544/type/286305994/release/3.5(2d)

UCS Infra Package Download

6200 series UCS Infra package: ucs-k9-bundle-infra.3.2.3h.A.bin

6300 series UCS Infra package: ucs-6300-k9-bundle-infra.3.2.3h.A.bin

UCS Blade Package:

ucs-k9-bundle-b-series.3.2.3h.B.bin

UCS C-series Package:

ucs-k9-bundle-c-series.3.2.3h.C.bin

Software Download: HXDP Release 3.0(1i)

HXDP Release 3.0(1i)

Before starting the upgrade process, download and install the software bundles that match your installation.

- **Upgrade Package:** storfs-packages-3.0.1i-29888.tgz
- **Link:** https://software.cisco.com/download/home/286305544/type/286305994/release/3.0(1i)

Software Installation

To install your software bundles, follow the detailed steps located in the Cisco UCS Manager Firmware Management Guide

Upgrade the UCS Infrastructure Package

Before you begin:

- Perform all tasks in the Prerequisites section of this guide.
- Download the software bundles needed for your upgrade from the Cisco Software Downloads:

Configuring UCS Infrastructure

Perform the following steps:

1. Open the UCS Manager GUI.
2. Select `Equipment > Firmware Management > Firmware auto-install`
3. Click **Install Infrastructure Firmware**.
   a. The Install Infrastructure Firmware window appears, select **ignore all**.
4. Select the desired UCS infrastructure version. Refer the compatibility matrix to identify the version desired for your use case.
   a. Click **Next**.
5. Check the **Upgrade Now** box.
6. Click **Finish**.

Note The expected upgrade behavior is for the UCS Manager to stop and then restart with the new version. Wait until the UCS Manager is back online to log back in to UCS Manager and complete the next steps.

You may check the **Ignore All** box for warnings are not critical to user environment.

7. If the UCS blade server chassis is present, wait for IO Modules (IOM) to upgrade.
   a. Select `Equipment > Installed Firmware`. Expand each chassis and check the Update Status of the IO Module.
      - During upgrade, the IOM status is **Upgrading**.
      - When the update process completes, the IOMs state is **Pending Next Boot for Activate** status.
      - After the IOM upgrade is complete, the IOM state is **Ready**.
8. Wait for Subordinate Fabric Interconnects (FI) to be activated.
   a. Select `Equipment > Installed Firmware > Fabric Interconnects`.
   b. Check the Activate Status of the kernel and switch images.

Note During upgrade, the Activate Status is set to **Activating**.

9. During FI reboot, all HX traffic is forwarded to the primary FI (based on ESXi vSwitch failover policy).
   - This will cause a brief traffic interruption.
   - This will not cause storage IO failures.
10. Verify subordinate FI has rebooted and joined the UCS cluster.
    a. Select `Equipment > Installed Firmware > Fabric Interconnects`.
    b. After activation, the Activate Status of the FI is set to Ready.
    c. Verify that the Overall Status of the FI is operable.
    d. Verify that the kernel and switch versions of the FI match the desired and updated version.
    e. Verify that the FI has no fault.
    f. Verify that the FI cluster membership is **Subordinate**.
11. If the UCS blade server chassis is present, wait for IO Modules (IOM) to upgrade.

Note Only the IOMs connected to the subordinate FI will enter Ready state, IOMs attached to the Primary FI will remain in **Pending Next Boot Activate** Status.

    a. `Select Equipment > Blade Chassis > IO Module`.

b. Wait for the Activate Status of the IOM to change to **Ready**.

12. Wait until HX traffic is re-pinned to both FIs.

Wait for UCS Manager vNIC faults to be cleared. The fault clearing indicates ESXi has loaded the ENIC driver and the interface is up. The traffic is not re-pinned immediately when the network interface goes up because ESXi has a fail back timer. But the `Net.teampolicyupdelay` timer is very low by default (100ms).

13. Verify the HX Cluster is online, and healthy before rebooting the primary fabric interconnect.

- Access summary tab from the vSphere Web Client Navigator. Select `Home > vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Summary`.

14. In the UCS manager GUI toolbar, click **Pending Activities**.

15. Click on **Fabric Interconnects** tab that display the tasks requiring user acknowledgment before they can complete.

a. Click **Reboot Now** for each pending activity that you want to deploy immediately.

b. Click **OK**. Cisco UCS Manager immediately reboots the primary FI and makes the subordinate FI the primary FI (FI failover).

During FI reboot, all HyperFlex traffic is forwarded to the new primary FI. This will cause a brief traffic interruption, but it will not cause storage IO failures.

16. Wait for UCS Manager to disconnect, then reconnected the UCS Manager to the other FI. This step is necessary because a UCS fail over occurs during the primary FI reboot (step 15).

17. Verify the FI settings:

- Verify that the subordinate FI is primary.
- Verify that the FI cluster membership is Primary.

18. Once the FI is activated, `Select Equipment > Installed Firmware > Fabric Interconnects`.

19. Wait for the Activate Status of the FI to be **Ready** and verify the following:

- Check the Overall Status of FI is operable.
- Check the FI has no fault.
- Verify FI has rebooted and joined the UCS cluster as subordinate.
- Check that the FI cluster membership is Subordinate.

20. Wait for IOM activation to complete, then select `Equipment > Blade Chassis > IO Module`.

21. Wait for the Activate Status of the IP module to be **Ready**.

- You can monitor the status on the FSM tab.

Note You will lose connectivity to UCS Manager throughout the entire upgrade. This is normal behavior

22. Wait for the HX traffic to re-pin to both FIs.
23. In the UCS manager GUI, wait for all server vNIC faults to clear.
24. In the vSphere Web Client Navigator. Select `Home > vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Summary`. Verify the HX Cluster is online and healthy after rebooting the FI.

Combined HXDP and UCS Firmware Upgrade

Upgrade the Plugin User Interface (UI)

1. From the vSphere Web Client Navigator, select `vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster`.
2. Navigate to `Actions > Summary` and note the Cluster Management IP address.
3. SSH to the cluster management IP address with root privileges.
4. Transfer the latest HX Data Platform upgrade bundle to the controller VM's `/tmp` directory. Depending on your operating system, use you can either use SCP directly or download third-party tools, such as WinSCP or MobaXterm.
5. From the controller VM shell, change to the `/tmp` directory.

Warning Do not use any folder other than `/tmp` and do not create any subfolders.

6. Uncompress and extract all files to the root using tar `-zxvf <storfs package name>.tgz`.

   Example:

   ```
   storfs-packages-3.5.2f-31787.tgz
   ```

7. To invoke the cluster-bootstrap.sh script to bootstrap packages for upgrade, execute the command `~# ./cluster-bootstrap.sh`
   a. Enter the vCenter FQDN or IP address and administrator level username and password.
   b. Wait for the system management service to restart and the bootstrap process to complete. Verify if the HX Data Platform Plug-in is now updated.
8. Log out from the cluster management IP controller VM.
9. Log out of vSphere Web Client.

Note Do not merely close the browser.

10. Log in to vSphere Web Client again to refresh the HX Data Platform Plug-in.
11. Verify the plugin version in vCenter by navigating to `Administration > Client Plug-Ins > Springpath` Plugin in the vSphere Web Client. Confirm the current version matches the new version you are upgrading to.

Upgrade the HXDP/UCS Firmware from the Plugin UI

1. From the vSphere Web Client Navigator, select `vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > HX-Cluster > Summary`.
2. Select **Upgrade Cluster**.
3. Select both, **HX Data Platform** and **UCS Firmware**.
4. Click **Next**.
5. Navigate to the `.tgz` package file on your local PC. Upload the Cisco HX Data Platform upgrade bundle. This is the same `.tgz` package file that was used to upgrade the HX Data Platform Plug-in.
6. To verify the integrity of the uploaded upgrade package bundle, enter administrator level vCenter credentials.
   a. Under Advanced Options, enter the MD5 Checksum # information. The file checksum can be found on the Cisco.com download page by clicking on the download title to reveal the md5 checksum.
7. Enter administrator level UCS Manager credentials.
8. To view the current firmware package version, click **Discover**.
9. Type the latest version of Cisco UCS firmware in the **Target** version field.

Important Type the release number exactly as shown, for example 4.0(4e)

10. Click **Upgrade**.

    The Cisco UCS servers are now upgraded with the desired firmware packages. The pending activities are automatically acknowledged in a rolling fashion.

Note You can monitor the progress in the Cisco UCS Manager GUI, under the FSM tab for the service profile. The Validation screen shows the progress of checks performed. Fix validation errors, if any.

The upgrade process proceeds as follows:

- HyperFlex cluster readiness for upgrade is checked.
- One by one, the HX nodes enter maintenance mode.

- HyperFlex vSphere Installation Bundles (VIBs) on Hypervisor are upgraded.
- Cisco HX Data Platform is upgraded followed by a reboot of the host server.
- The HX Data Platform requests Cisco UCS Manager to begin firmware upgrade. This process can take up to 1 hour.
- HX node exits maintenance mode.
- Cluster will begin to rebuild back to full health.
- Once the cluster is healthy, upgrade moves on to the next node in the HyperFlex cluster.
- Confirm Upgrade is completed

Upgrade Tasks

Perform the following tasks, using the specified software releases to upgrade to your destination release:

- Download and Install Software Bundles.
- Upgrade UCS firmware to the latest suggested version for your HyperFlex Data Platform Software.
- Upgrade HyperFlex Data Platform Software to Version 3.5(2g) or the latest suggested release.
- (Optional) ESXi Upgrade to 6.5 or 6.7.

Software Downloads: From the Intermediate Release to the Destination Release

The second upgrade you need to complete is to upgrade from the intermediate release to the destination release. Download the software bundles needed for your upgrade from the Cisco Software Downloads.

- Software Download for the Recommended UCS Firmware
- Software Download for HXDP Release 3.5(2g) or the latest suggested release , on page 9

Software Download for the Recommended UCS Firmware

Before starting the upgrade process, download and install the UCS Infra Package that matches your installation as well as the UCS Blade, and the UCS C-series Package.

Note At the time of authoring 4.0(4e) was the compatible UCS server firmware for the suggested HXDP release of 3.5(2g). Before selecting a UCS server firmware to use, start with the current suggested HX release, and choose the corresponding UCS server firmware. For more information about the latest suggested release, see Navigating the Cisco HyperFlex Data Platform Software Downloads.

Download Link: https://software.cisco.com/download/home/286305544/type/286305994/release/3.5(2g)

UCS Infra Package Download

UCS 6200 Fabric Interconnects: ucs-k9-bundle-infra.4.0.4e.A.bin

6300 series UCS Infra package: ucs-6300-k9-bundle-infra.4.0.4e.A.bin

6400 series UCS Infra package: ucs-6400-k9-bundle-infra.4.0.4e.A.bin

UCS Blade Package:

ucs-k9-bundle-b-series.4.0.4e.B.bin

UCS C-series Package:

ucs-k9-bundle-c-series.4.0.4e.C.bin

Software Download for HXDP Release 3.5(2g) or the latest suggested release

Before starting the upgrade process, download and install all software bundles needed to complete this upgrade.

Note At the time this document was authored HDPX Release 3.5(2g) was the suggested release. For more information about the latest suggested release, see Navigating the Cisco HyperFlex Data Platform Software Downloads.

- **Upgrade Package:** storfs-packages-3.5.2g-32110.tgz
- **Link:** https://software.cisco.com/download/home/286305544/type/286305994/release/3.5(2g)

Software Installation

To install your software bundles, follow the detailed steps located in the Cisco UCS Manager Firmware Management Guide

Upgrade the UCS Infrastructure Package

Before you begin:

- Perform all tasks in the Prerequisites section of this guide.
- Download the software bundles needed for your upgrade from the Cisco Software Downloads:

Configuring UCS Infrastructure

Perform the following steps:

1. Open the UCS Manager GUI.
2. Select `Equipment > Firmware Management > Firmware auto-install`
3. Click **Install Infrastructure Firmware**.
   a. The Install Infrastructure Firmware window appears, select **ignore all**.
4. Select the desired UCS infrastructure version. Refer the compatibility matrix to identify the version desired for your use case.
   a. Click **Next**.

5. Check the **Upgrade Now** box.
6. Click **Finish**.

Note The expected upgrade behavior is for the UCS Manager to stop and then restart with the new version. Wait until the UCS Manager is back online to log back in to UCS Manager and complete the next steps.

You may check the **Ignore All** box for warnings are not critical to user environment.

7. If the UCS blade server chassis is present, wait for IO Modules (IOM) to upgrade.
   a. Select `Equipment > Installed Firmware`. Expand each chassis and check the Update Status of the IO Module.
      - During upgrade, the IOM status is **Upgrading**.
      - When the update process completes, the IOMs state is **Pending Next Boot for Activate** status.
      - After the IOM upgrade is complete, the IOM state is **Ready**.
8. Wait for Subordinate Fabric Interconnects (FI) to be activated.
   a. Select `Equipment > Installed Firmware > Fabric Interconnects`.
   b. Check the Activate Status of the kernel and switch images.

Note During upgrade, the Activate Status is set to **Activating**.

9. During FI reboot, all HX traffic is forwarded to the primary FI (based on ESXi vSwitch failover policy).
   - This will cause a brief traffic interruption.
   - This will not cause storage IO failures.
10. Verify subordinate FI has rebooted and joined the UCS cluster.
    a. Select `Equipment > Installed Firmware > Fabric Interconnects`.
    b. After activation, the Activate Status of the FI is set to Ready.
    c. Verify that the Overall Status of the FI is operable.
    d. Verify that the kernel and switch versions of the FI match the desired and updated version.
    e. Verify that the FI has no fault.
    f. Verify that the FI cluster membership is **Subordinate**.
11. If the UCS blade server chassis is present, wait for IO Modules (IOM) to upgrade.

Note Only the IOMs connected to the subordinate FI will enter Ready state, IOMs attached to the Primary FI will remain in **Pending Next Boot Activate** Status.

   a. `Select Equipment > Blade Chassis > IO Module`.

   b. Wait for the Activate Status of the IOM to change to **Ready**.

12. Wait until HX traffic is re-pinned to both FIs.

    Wait for UCS Manager vNIC faults to be cleared. The fault clearing indicates ESXi has loaded the ENIC driver and the interface is up. The traffic is not re-pinned immediately when the network interface goes up because ESXi has a fail back timer. But the `Net.teampolicyupdelay` timer is very low by default (100ms).

13. Verify the HX Cluster is online, and healthy before rebooting the primary fabric interconnect.

    - Access summary tab from the vSphere Web Client Navigator. Select `Home > vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Summary`.

14. In the UCS manager GUI toolbar, click **Pending Activities**.

15. Click on **Fabric Interconnects** tab that display the tasks requiring user acknowledgment before they can complete.

    a. Click **Reboot Now** for each pending activity that you want to deploy immediately.

    b. Click **OK**. Cisco UCS Manager immediately reboots the primary FI and makes the subordinate FI the primary FI (FI failover).

    During FI reboot, all HyperFlex traffic is forwarded to the new primary FI. This will cause a brief traffic interruption, but it will not cause storage IO failures.

16. Wait for UCS Manager to disconnect, then reconnected the UCS Manager to the other FI. This step is necessary because a UCS fail over occurs during the primary FI reboot (step 15).

17. Verify the FI settings:

    - Verify that the subordinate FI is primary.
    - Verify that the FI cluster membership is Primary.

18. Once the FI is activated, `Select Equipment > Installed Firmware > Fabric Interconnects`.

19. Wait for the Activate Status of the FI to be **Ready** and verify the following:

    - Check the Overall Status of FI is operable.
    - Check the FI has no fault.
    - Verify FI has rebooted and joined the UCS cluster as subordinate.
    - Check that the FI cluster membership is Subordinate.

20. Wait for IOM activation to complete, then select `Equipment > Blade Chassis > IO Module`.
21. Wait for the Activate Status of the IP module to be **Ready**.
    - You can monitor the status on the FSM tab.

Note You will lose connectivity to UCS Manager throughout the entire upgrade. This is normal behavior

22. Wait for the HX traffic to re-pin to both FIs.
23. In the UCS manager GUI, wait for all server vNIC faults to clear.
24. In the vSphere Web Client Navigator. Select `Home > vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Summary`. Verify the HX Cluster is online and healthy after rebooting the FI.

Combined HXDP and UCS Firmware Upgrade

Upgrade the Plugin User Interface (UI)

1. From the vSphere Web Client Navigator, select `vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster`.
2. Navigate to `Actions > Summary` and note the Cluster Management IP address.
3. SSH to the cluster management IP address with root privileges.
4. Transfer the latest HX Data Platform upgrade bundle to the controller VM's `/tmp` directory. Depending on your operating system, use you can either use SCP directly or download third-party tools, such as WinSCP or MobaXterm.
5. From the controller VM shell, change to the `/tmp` directory.

Warning Do not use any folder other than `/tmp` and do not create any subfolders.

6. Uncompress and extract all files to the root using tar `-zxvf <storfs package name>.tgz`.

   Example:

   ```
   storfs-packages-3.5.2d-31738.tgz
   ```

7. To invoke the cluster-bootstrap.sh script to bootstrap packages for upgrade, execute the command `~# ./cluster-bootstrap.sh`
   a. Enter the vCenter FQDN or IP address and administrator level username and password.
   b. Wait for the system management service to restart and the bootstrap process to complete. Verify if the HX Data Platform Plug-in is now updated.
8. Log out from the cluster management IP controller VM.

9. Log out of vSphere Web Client.

Note Do not merely close the browser.

10. Log in to vSphere Web Client again to refresh the HX Data Platform Plug-in.
11. Verify the plugin version in vCenter by navigating to `Administration > Client Plug-Ins > Springpath` Plugin in the vSphere Web Client. Confirm the current version matches the new version you are upgrading to.

Upgrade UCS Firmware from HX Connect UI

1. Log in to HX Connect.
   a. Enter the HX Storage Cluster management IP address in a browser.
   b. Navigate to `https://<storage-cluster-management-ip>`.
   c. Enter the administrative username and password.
   d. Click **Login**.
2. Select Upgrade types:
   - HX Data Platform
   - UCS Manager firmware
3. Click **Continue**.
4. Complete the following fields on the Enter Credentials page.

Table 1: Upgrade HX Data Platform and UCS Manager Firmware

UI Element	Essential Information
Drag the HX file here or click to browse	Upload the latest Cisco HyperFlex Data Platform Upgrade Bundle for upgrading existing clusters with previous release.tgz package file from Software Download - Hyperflex HX Data Platform **Example:** `storfs-packages-3.5.2d-31738.tgz`
Current version	Displays the current HyperFlex Data Platform version
Current cluster details	Lists the HyperFlex cluster details like the Hypervisor version and Cluster upgrade state.
Bundle version	Displays the HyperFlex Data Platform version of the uploaded bundle.

Table 2: vCenter Credentials

UI Element	Essential Information
User Name field	Enter the vCenter <admin> username.
Admin Password field	Enter the vCenter <root> password.
(Optional) Checksum field	The MD5 checksum can be obtained from the Cisco.com download page by hovering your mouse over the download package. This is an optional step that helps you verify the integrity of the uploaded upgrade package bundle.

Table 3: UCS Manager Credentials

UI Element	Essential Information
UCS Manager Host Name field	Enter the Cisco UCS Manager host name.
User Name field	Enter the Cisco UCS Manager <admin> username.
Admin Password field	Enter the Cisco UCS Manager root password.

Table 4: Discover Current Version

UI Element	Essential Information
Discover button	Click Discover to view the current UCS firmware package version, in the Current Version field.
Current Version field	Displays the current Cisco UCS firmware version.
Target Version drop-down list	To upgrade to a higher Cisco UCS firmware version, choose the version of Cisco UCS firmware **Example:** 4.0(2d)

5. Click **Upgrade**.
6. The Validation Screen on the Upgrade Progress page displays the progress of the checks performed. Fix validation errors, if any. Confirm that the upgrade is complete.

Note When the upgrade is in progress, you may see the error message, 'Websocket connection failed. Automatic refresh disabled'. To clear the error message, you can either refresh the page, or log out and log back in. You can safely ignore this error message.