Cisco HyperFlex Systems Upgrade Guide for Unsupported Cisco HX Releases

First Published: 2019-12-18

Last Modified: 2024-04-08

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2019–2024 Cisco Systems, Inc. All rights reserved.

CONTENTS

?

Communications, Services, Bias-free Language, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

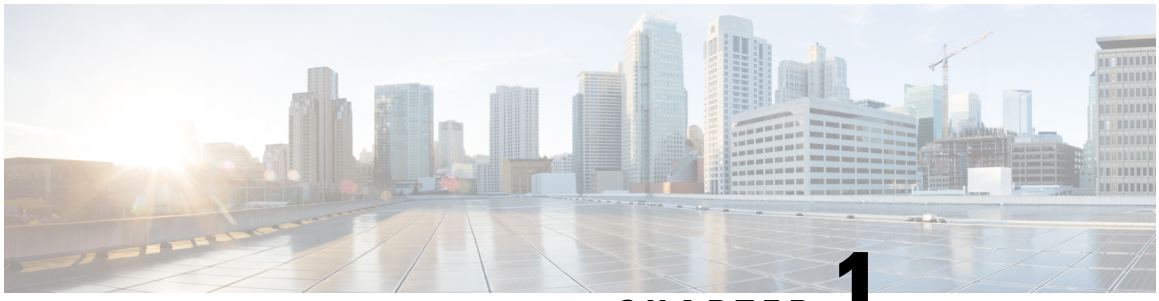
Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Bias-Free Language

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Communications, Services, Bias-free Language, and Additional Information



CHAPTER 1

Upgrading from Unsupported Cisco HyperFlex Releases

About Upgrading from Unsupported Cisco HyperFlex Releases

This document is designed to guide Cisco HyperFlex users who need to upgrade their environment from a Cisco HyperFlex HX Data Platform software release that is past the last date of support, to the latest suggested release on the Cisco Software Download site.

Important This guide covers the Cisco HyperFlex Release 1.7(x), 1.8(x), 2.0(x), 2.1(x), 2.5(x), 2.6(x), 3.0(x), 3.5(x)[1], 4.0(x), and 4.5(1x). If your release is not listed, **do not** use this document. Download the appropriate Cisco HyperFlex Upgrade Guide for your current release and environment.

This section contains the following topics:

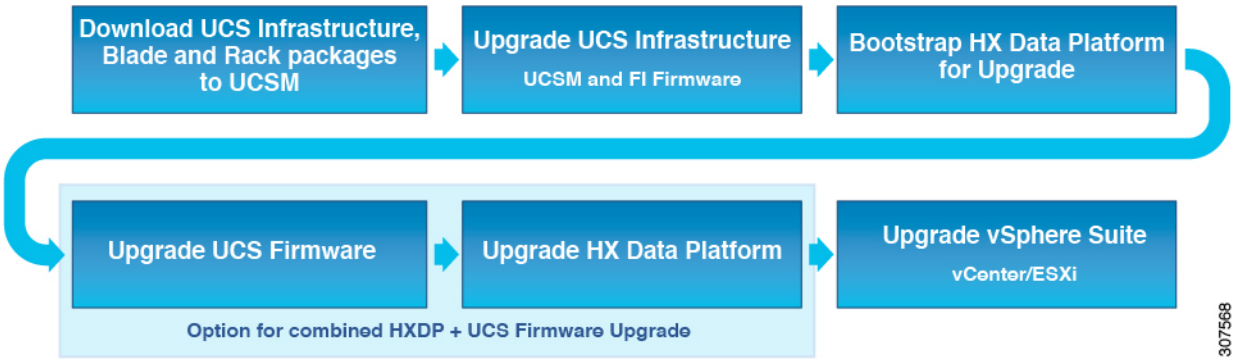
HyperFlex Upgrade Preparation

The intent of this guide is to successfully guide you through the process of upgrading an unsupported version of Cisco HyperFlex to a current feature rich supported version. Proper preparation for upgrade is as important as the actual upgrade. It is imperative that you follow the workflow and complete each task in the order presented. There are no shortcuts.

The following image describes the general upgrade workflow.

Note Users who need to upgrade to an intermediate release before their destination release will complete the upgrade workflow two times.

[1] Cisco HyperFlex Release 3.5(2i) is available for download for users who need an intermediate upgrade to get to their destination release.



The upgrade requires you to complete the following tasks in this order:

1. Complete all tasks in the Prerequisites for Upgrading Obsolete Hyperflex Releases section of this guide.
2. Run the Hypercheck Health & Pre-Upgrade tool to on your HyperFlex systems to ensure its stability and resiliency Hypercheck : Hyperflex Health & Pre-Upgrade Check Tool
3. Verify that your VMware vCenter and ESXi version is 6.0 U3 or later. For more information, see Verify the ESXi and vCenter Build Number, on page 3.
4. Select the Cisco HyperFlex Data Center release currently running in your environment and follow the upgrade workflow for your specific upgrade.
   - Upgrading Cisco HyperFlex 3.5(2x), 4.0(x), 4.5(1x) and 5.0(1x), on page 7
   - Upgrading Cisco HyperFlex 2.6(x), 3.0(x), and 3.5(1x), on page 9
   - Upgrading Cisco HyperFlex 2.1(1a), 2.1(1b), 2.1(1c) and 2.5(x), on page 17
   - Upgrading Cisco HyperFlex 1.8(1f) and 2.0(x) , on page 31
   - Upgrading Cisco HyperFlex 1.8(1a-1e), on page 47
   - Upgrading Cisco HyperFlex 1.7, on page 63
5. Post Cisco HyperFlex Upgrade: (Optional) ESXi Upgrade to 6.5 or 6.7, on page 74

What to do next:

Complete all tasks in the Prerequisites for Upgrading Obsolete Hyperflex Releases section of this guide.

Prerequisites for Upgrading Obsolete Hyperflex Releases

The following tasks should be performed prior to beginning the upgrade process:

- vCenter version check: Verify that the vCenter is version 6.0U3 or later.
- Ensure all VM network vlan vm port groups existing on all nodes in the cluster.
- Ensure that the management and storage data vlans are on the top-of-rack to ensure uninterrupted connectivity.
- If using jumbo frames in your environment, ensure jumbo frames is enabled on vmotion and data network on top of rack switch.

- Verify that the ESXi hosts are not in lockdown mode.
- Verify that **Springpath_security.properties** link exists on controller VMs (see security properties in Verifying and Recreating the Springpath User Account, on page 66).
- MTU Setting: vm-network vlans set to MTU 9000 may revert to MTU 1500 during the upgrade process. After upgrading, verify the setting and reset if to MTU 9000 if needed.
- If using ACI with LLDP this setting may revert to CDP and need to be re-enabled post-upgrade.
- If using ACI with application-centric architecture, please contact TAC before beginning your upgrade.
- Confirm pycrypto package version (if cluster was previously upgraded from 1.7.x. (see Pycrypto Minimum Version)).

What to do next:

After completing the prerequisites, continue to the Hypercheck : Hyperflex Health & Pre-Upgrade Check Tool technote (HXDP 1.8.x and above).

Hypercheck: HyperFlex and Pre-Upgrade Check Tool

The Hypercheck: HyperFlex and Pre-Upgrade Check Tool are automated health and pre-upgrade checks that are designed to ensure your clusters are healthy before you upgrade. It is imperative that this healthcheck is not just performed, but that you take corrective action on any cluster that is found to be unhealthy. Correct all issues reported by the Hypercheck health check before continuing.

Hypercheck: Hyperflex Health & Pre-Upgrade Check Tool technote (HXDP 1.8.x and above)
https://www.cisco.com/c/en/us/support/docs/hyperconverged-infrastructure/hyperflex-hx-data-platform/214101-hypercheck-hyperflex-health-pre-upgr.html

What to do next:

Once all clusters are healthy, continue to Verify the ESXi and vCenter Build Number, on page 3.

Verify the ESXi and vCenter Build Number

Cisco HyperFlex Data Platform requires that your ESXi and vCenter version number be 6.0 U3 or later. To determine the data platform server build number, perform the following steps in the vSphere Web Client.

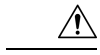
1. Log in to the vSphere Web Client.
2. Click Home.
3. Click Hosts and Clusters.
4. Expand the datacenter.
5. Expand the cluster.
6. Click the ESXi host.
7. Click the Summary tab.
8. The ESX/ESXi Version field is located under **Configuration**.

What to do next:

- If your version number is a 6.0 U3 or later, you have met the minimum version required to upgrade your HyperFlex release. Continue to the next step in HyperFlex Upgrade Preparation.
- If the VMware version number does not meet the minimum version required, upgrade the version, see Upgrading vCenter and ESXi, on page 4.

Upgrading vCenter and ESXi

ESXi Upgrade Guidelines and Limitations



Caution Using VMware Update Manager (VUM) to upgrade ESXi is discouraged.

If you are using VUM to upgrade ESXi do the following:

- Use VUM one host at a time.
- Make sure that the cluster is in healthy state before moving on to the next node.
- Do not use VUM to upgrade ESXi across a cluster, as there is no guarantee that the cluster will be healthy by the time VUM moves on to the next node.

- The ESXi hypervisor version can be upgraded without disruption to the HyperFlex cluster workload. This is achieved by performing an online, rolling upgrade of each node in the HX cluster.
- ESXi upgrade requires a manual online upgrade.
- Verify that the current ESXi version is 6.0 U3 before beginning the upgrade path. For upgrade directions see, ESXi Upgrade, on page 5.
- Use the ESXi command line interface `esxcli` for upgrading or updating ESXi.
- Replace the build numbers provided in the examples below with the latest version.

What to do next:

After reviewing the Guidelines and Limitations, download install the required software listed in Software Download: ESXI 6.0 U3 (EP 25), on page 4.

Software Download: ESXI 6.0 U3 (EP 25)

ESXI 6.0 U3 (EP 25)

Upgrade Bundle: HX-ESXi-6.0U3-15517548-Cisco-Custom-6.0.3.14-upgrade-bundle.zip

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

What to do next:

After downloading and installing the necessary software, follow the installation steps in the ESXi Upgrade, on page 5.

ESXi Upgrade

After downloading the software bundles, complete the steps to upgrade the ESXi version:

Note ESXi version 6.0 U3 is required to start the upgrade path.

1. Step 1 Download ESXi upgrade package. When upgrading ESXi from 6.0 Ux to any newer version, use the offline zip file from the Cisco Download Software site.

   Example Filename:

   ```
   HX-ESXi-6.0U3-15517548-Cisco-Custom-6.0.3.14-upgrade-bundle.zip
   ```

   Note Do not use the HX ISO file or any other VMware ISO to attempt an ESXi upgrade.

2. Select one of your hosts and put it in HX maintenance mode using the vSphere Web Client. For additional information see Entering Cisco HyperFlex Maintenance Mode.

   After the host enters maintenance mode, complete the following steps.

3. Remote secure copy the ESXi upgrade bundle to an appropriate folder with enough space.

   To copy files using SCP, start the SSH service in the destination ESXi hosts as well.

   Note
   - On HX240, you can use the local SpringpathDS datastore or a mounted HX datastore.
   - On HX220, you can use either a mounted HX datastore or create a temporary RAM disk.

   Example:

   ```
   scp local_filename user@server:/path/where/file/should/go
   ```

4. Log in to ESXi.

5. To query the list of available image profiles and for profile name verification, execute the `esxcli software sources profile list -d <location_of_the_esxi_zip_bundle_on_the_datastore>` command.

   Note The full path must be used when running the `esxcli` software command.

   Example:

   ```
   [root@localhost:~] esxcli software sources profile list -d
   /vmfs/volumes/5d3a21da-7f370812-ca58-0025
   b5a5a102/HX-ESXi-6.0U3-15517548-Cisco-Custom-6.0.3.14-upgrade-bundle.zip
   Name                                        Vendor  Acceptance Level  Creation Time
          Modification Time
   ------------------------------------------  ------  ----------------
   ------------------  -------------------
   ```

```
HX-ESXi-6.0U3-15517548-Cisco-Custom-6.0.3.14  Cisco   PartnerSupported
2019-07-02T00:14:56  2019-07-02T13:38:34
```

6. To start the upgrade, run the `esxcli software profile update -d <path_to_profile_ZIP_file> -p < profile name>`.

   Example:

   ```
   [root@localhost:~] esxcli software
   profile update -d /vmfs/volumes/5d3a21da-7f370812-ca58-0025b5a5a10
   2/HX-ESXi-6.0U3-15517548-Cisco-Custom-6.0.3.14-upgrade-bundle.zip -p
   HX-ESXi-6.0U3-15517548-Cisco-Custom-6.0.3.14
   ```

7. Once the upgrade completes, restart the ESXi host.

   Example:

   ```
   esxcli system shutdown reboot -r Update -d 10
   ```

8. After the ESXi host comes up, verify that the host has booted up with the correct version.

   Example:

   ```
   vmware -vl
   ```

9. Wait for the ESXi host to auto reconnect to vCenter.

   In some upgrade scenarios it may be necessary to force ESXi to reconnect from vCenter. Right-click on the host and select `Connection > Connect`.

10. Exit maintenance mode using the vSphere Web Client, For additional information see Entering Cisco HyperFlex Maintenance Mode

11. Ensure that the cluster becomes healthy between each ESXi upgrade.

    Example:

    ```
    stcli cluster storage-summary --detail
    ```

12. Sequentially repeat this process for all hosts in the cluster.

Note Make sure that the cluster becomes healthy between each ESXi upgrade.

What to do next:

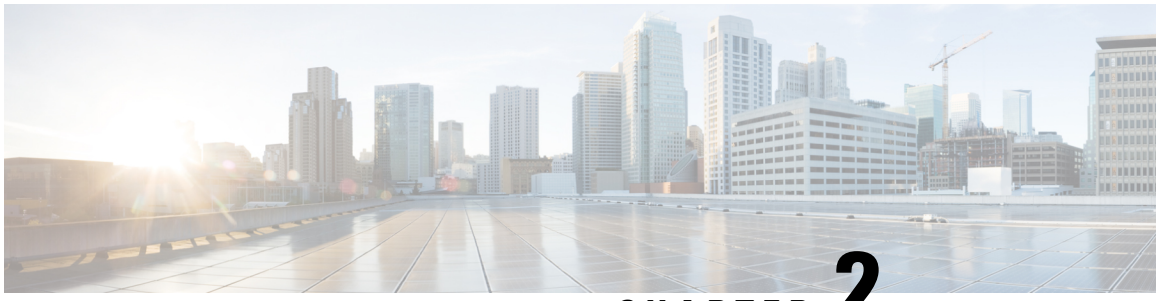
After upgrading your VMware software, continue to step 4 in HyperFlex Upgrade Preparation, on page 1.

vCenter Upgrade

For directions on upgrading vCenter, see VMware vSphere Documentation

What to do next:

Once your version number is 6.0 U3 or later, you have met the minimum version required to upgrade your Cisco HyperFlex release. Continue to the ESXi Upgrade Guidelines and Limitations, on page 4.



CHAPTER 2

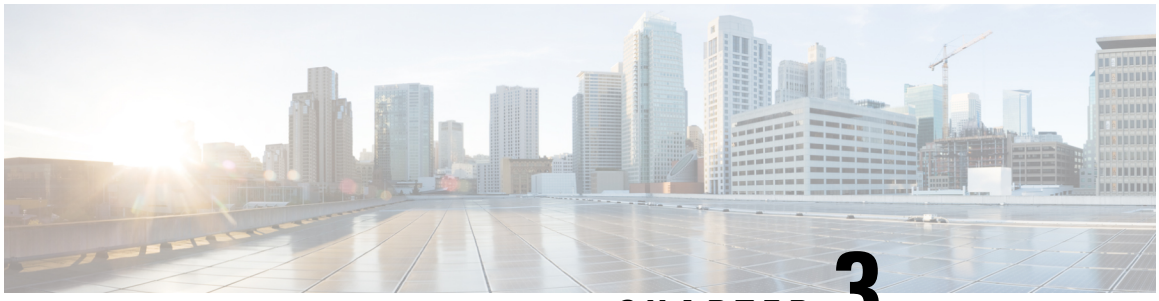
Upgrading Cisco HyperFlex 3.5(2x), 4.0(x), 4.5(1x) and 5.0(1x)

Overview: Upgrading Cisco HyperFlex 3.5(2x), 4.0(x), 4.5(1x) and 5.0(1x)

The Cisco HyperFlex Releases noted in this section have reached the end of their support. Upgrading from Cisco HyperFlex Data Platform 3.5(2x), 4.0(x)[2], 4.5(1x) and 5.0(1x) to the Cisco Recommended HXDP release is a single upgrade to your destination release is addressed in the curent upgrade guide.

To upgrade any of these releases, download and follow the Cisco HyperFlex Upgrade Guide for your current release and environment.

[2] Clusters running HXDP Release 4.0(2x) or later can upgrade directly to 5.5(1a).



CHAPTER 3

Upgrading Cisco HyperFlex 2.6(x), 3.0(x), and 3.5(1x)

Overview: Upgrading Cisco HyperFlex 2.6(x), 3.0(x), and 3.5(1x)

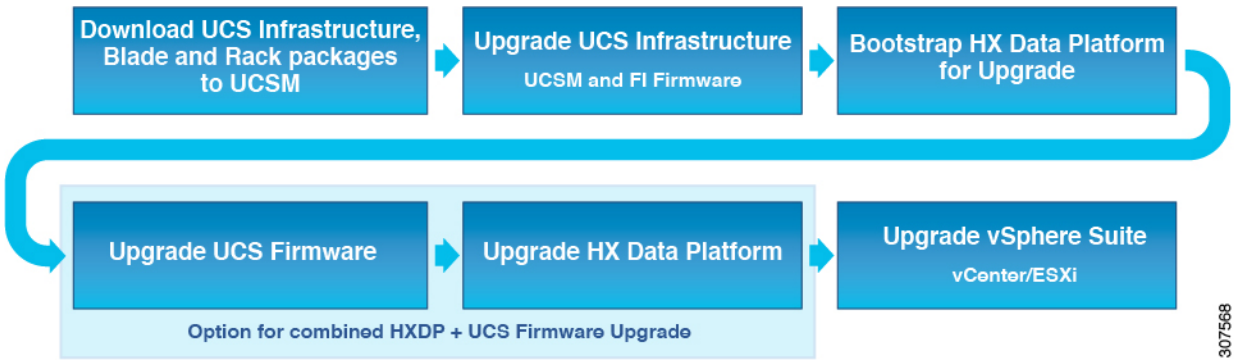
Prerequisites

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

- Prerequisites for Upgrading Obsolete Hyperflex Releases, on page 2
- Hypercheck: HyperFlex and Pre-Upgrade Check Tool, on page 3
- Verify the ESXi and vCenter Build Number, on page 3

Upgrade Path for Cisco HyperFlex Data Platform HXDP 2.6(x), 3.0(x), and 3.5(1x)

Upgrading from Cisco HyperFlex Data Platform 2.6(x), 3.0(x), and 3.5(1x) to the Cisco Recommended HXDP release is a single upgrade to your destination release. The following image describes the upgrade workflow.



The following outlines your starting release version 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 2.6(x), 3.0(x), or 3.5(1x)	4.0(2f)	The latest suggested release on the Cisco Software Download site.
UCS firmware	UCS 3.1(2g) or later.	Minimum version 4.0(4i)	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.

Note The upgrade process consists of the following tasks complete each step in the order presented.

- 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 4.0(2f) or the latest suggested release.
- (Optional) ESXi Upgrade to 6.5 or 6.7, on page 74.

Workflow 1: Upgrading to the Destination Release

Upgrading to the Destination Release

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

HXDP Software Downloads: From the Current Release to the Destination Release

To upgrade to the destination release, download the software bundles needed for your upgrade from the Cisco Software Downloads

- Software Download for the Recommended UCS Firmware, on page 10
- Software Download for HXDP Release 4.0(2f) or the latest suggested release , on page 11

Software Download

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(4k) was the compatible UCS server firmware for the suggested HXDP release of 3.5(2h) and 3.5(2i). 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 Cisco HyperFlex Recommended Software Release and Requirements Guide.

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

UCS Infra Package Download

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

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

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

UCS Blade Package:

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

UCS C-series Package:

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

Software Download for HXDP Release 4.0(2f) 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 4.0(2f) was the suggested release. For more information about how to locate the latest suggested release on the Cisco Software Download page, see Navigating the Cisco HyperFlex Data Platform Software Downloads, on page 70 and the Cisco HyperFlex Recommended Software Release and Requirements Guide.

- **Upgrade Package:** storfs-packages-4.0.2f-35930.tgz
- **Link:** https://software.cisco.com/download/home/286305544/type/286305994/release/4.0(2f)

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

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)

Note This workflow should only be used if the current HXDP version is before 3.5(1a). Beginning with HXDP Release 3.5(1a), the plugin is updated as part of the HXDP upgrade.

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-3.5.2h-32139.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

Note This workflow should only be used if the current HXDP version is before 3.5(1a).

If the current HXDP Release is 3.5(1a) or later, upgrade using HX Connect.

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. Browse and select the HXDP package `storfs-packages-<version>.tgz`.
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.

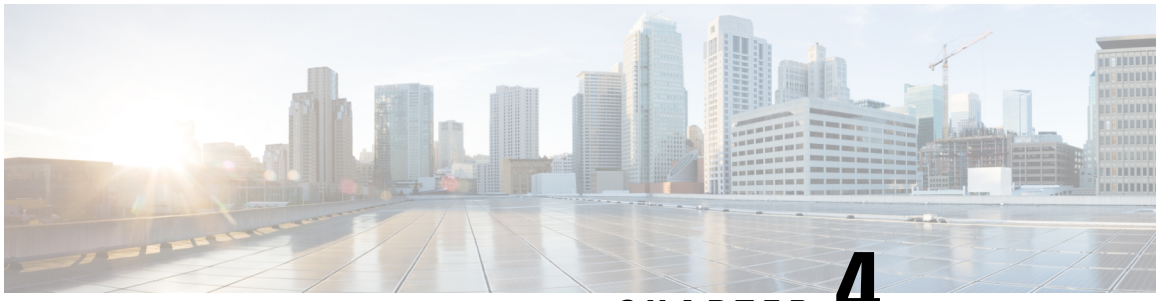
Important Type the release number exactly as shown, for example 4.0(4k). Confirm the desired version of UCS C-series and B-series firmware bundles are uploaded to the UCSM before you start the upgrade process.

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 The upgrade process performs the rolling reboot of each node in the cluster without any traffic disruptions.

If the upgrade fails, you can re-try the upgrade or contact Cisco TAC for further assistance. Running a cluster without remediation after an upgrade failure is not recommended. Care should be taken to fully complete the upgrade as soon as possible.



CHAPTER 4

Upgrading Cisco HyperFlex 2.1(1a), 2.1(1b), 2.1(1c) and 2.5(x)

Overview: Upgrading Cisco HyperFlex 2.1(1a), 2.1(1b), 2.1(1c) and 2.5(x)

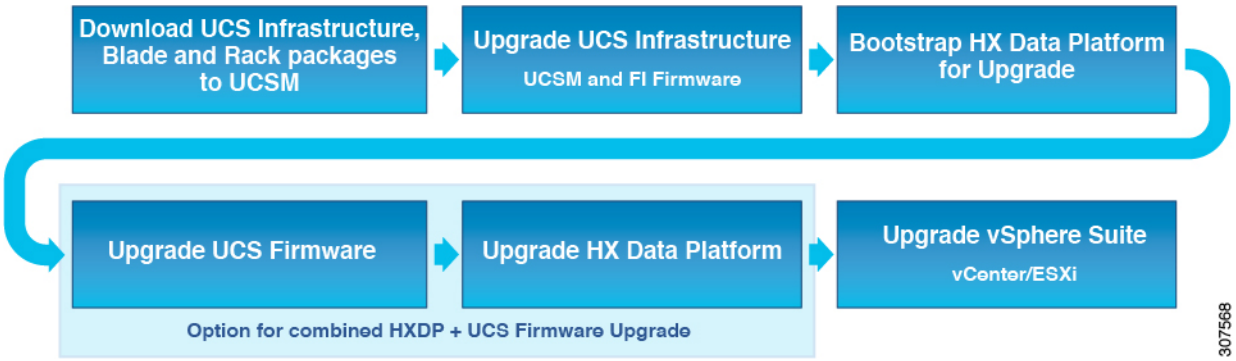
Prerequisites

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

- Prerequisites for Upgrading Obsolete Hyperflex Releases, on page 2
- Hypercheck: HyperFlex and Pre-Upgrade Check Tool, on page 3
- Verify the ESXi and vCenter Build Number, on page 3

Upgrade Path for Cisco HyperFlex Data Platform 2.1(1a), 2.1(1b), 2.1(1c) and 2.5(x)

Upgrading from Cisco HyperFlex Data Platform 2.1(1a), 2.1(1b), 2.1(1c) or 2.5(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 2.1(1a), 2.1(1b), 2.1(1c) or 2.5(x)	3.5(2i)	The latest suggested release on the Cisco Software Download site.
UCS firmware	UCS 3.1(2g) or later.	Minimum version 4.0(4e)	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.

Note The upgrade process consists of the following tasks complete each step in the order presented.

- Download software bundles.
- Install software bundles.
- Upgrade UCS Firmware to a minimum version of 4.0(4e).
- Upgrade HyperFlex Data Platform Software to Version 3.5(2i).
- Perform the second upgrade process to the destination version.

Workflow 1: Upgrading to the Intermediate Release

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:

Software Downloads: Upgrading to the Intermediate Release

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

- Software Download for UCS Firmware 4.0(4e), on page 19
- Software Download for HXDP Release 3.5(2i)

Software Downloads

Software Download for UCS Firmware 4.0(4e)

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(2f). 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, on page 70 and the Cisco HyperFlex Recommended Software Release and Requirements Guide.

Download Link: https://software.cisco.com/download/home/283612660/type/283655658/release/4.0(4e)

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(2i)

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

Note At the time this was authored, HXDP Release 3.5(2i) was the suggested HXDP release. For more information about the latest suggested release, see Navigating the Cisco HyperFlex Data Platform Software Downloads, on page 70 and the Cisco HyperFlex Recommended Software Release and Requirements Guide.

- **Upgrade Package:** storfs-packages-3.5.2i-32180.tgz
- **Link:** https://software.cisco.com/download/home/286305544/type/286305994/release/3.5(2i)

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 for Upgrading Obsolete Hyperflex Releases 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-3.0.1i-29888.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

Note This workflow should only be used if the current HXDP version is before 3.5(1a).

If the current HXDP Release is 3.5(1a) or later, upgrade using HX Connect.

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. Browse and select the HXDP package `storfs-packages-<version>.tgz`.
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(4k). Confirm the desired version of UCS C-series and B-series firmware bundles are uploaded to the UCSM before you start the upgrade process.

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 The upgrade process performs the rolling reboot of each node in the cluster without any traffic disruptions.

If the upgrade fails, you can re-try the upgrade or contact Cisco TAC for further assistance. Running a cluster without remediation after an upgrade failure is not recommended. Care should be taken to fully complete the upgrade as soon as possible.

Workflow 2: Upgrading to the Destination Release

Upgrading to the Destination Release

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

HXDP 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, on page 10

• Software Download for HXDP Release 4.0(2f) or the latest suggested release , on page 11

Software Downloads

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(4k) was the compatible UCS server firmware for the suggested HXDP release of 3.5(2h) and 3.5(2i). 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 Cisco HyperFlex Recommended Software Release and Requirements Guide.

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

UCS Infra Package Download

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

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

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

UCS Blade Package:

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

UCS C-series Package:

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

Software Download for HXDP Release 4.0(2f) 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 4.0(2f) was the suggested release. For more information about how to locate the latest suggested release on the Cisco Software Download page, see Navigating the Cisco HyperFlex Data Platform Software Downloads, on page 70 and the Cisco HyperFlex Recommended Software Release and Requirements Guide.

- **Upgrade Package:** storfs-packages-4.0.2f-35930.tgz
- **Link:** https://software.cisco.com/download/home/286305544/type/286305994/release/4.0(2f)

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

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)

Note This workflow should only be used if the current HXDP version is before 3.5(1a). Beginning with HXDP Release 3.5(1a), the plugin is updated as part of the HXDP upgrade.

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-3.5.2h-32139.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

Note This workflow should only be used if the current HXDP version is before 3.5(1a).

If the current HXDP Release is 3.5(1a) or later, upgrade using HX Connect.

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. Browse and select the HXDP package `storfs-packages-<version>.tgz`.
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.

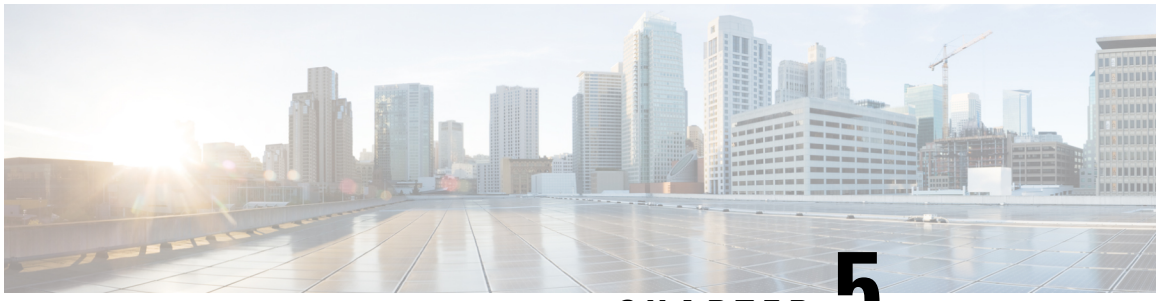
Important Type the release number exactly as shown, for example 4.0(4k). Confirm the desired version of UCS C-series and B-series firmware bundles are uploaded to the UCSM before you start the upgrade process.

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 The upgrade process performs the rolling reboot of each node in the cluster without any traffic disruptions.

If the upgrade fails, you can re-try the upgrade or contact Cisco TAC for further assistance. Running a cluster without remediation after an upgrade failure is not recommended. Care should be taken to fully complete the upgrade as soon as possible.



CHAPTER 5

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

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

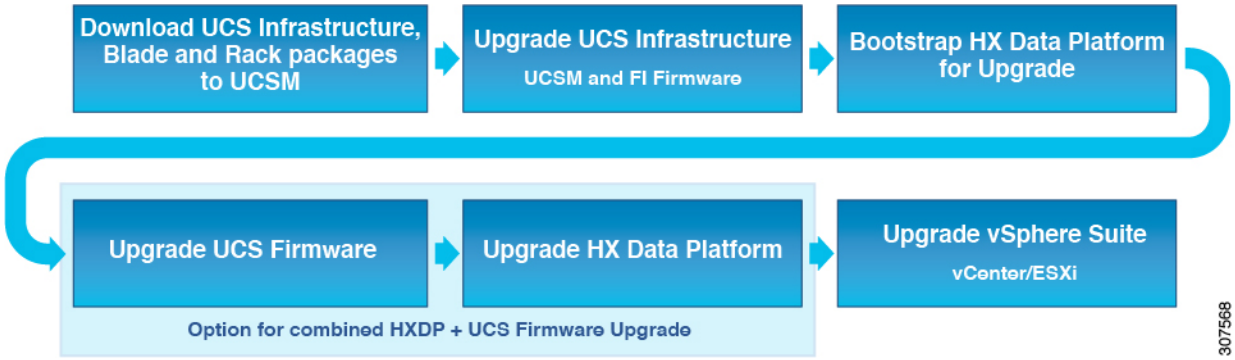
Prerequisites

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

- Prerequisites for Upgrading Obsolete Hyperflex Releases, on page 2
- Hypercheck: HyperFlex and Pre-Upgrade Check Tool, on page 3
- Verify the ESXi and vCenter Build Number, on page 3

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 Intermediate Releases		Upgrade to the Destination Release
HyperFlex software	HXDP 1.8(1f) or 2.0(x)	First: 3.0(1i)	Second: 4.0(2f)	The latest suggested release on the Cisco Software Download site.
UCS firmware	UCS 3.1(2f) or later.	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.

Note The upgrade process consists of the following tasks complete each step in the order presented.

- 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.

Workflow 1: Upgrading to the Intermediate Release

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:

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 33
- Software Download: HXDP Release 3.0(1i) , on page 33

Software Downloads

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/283612660/type/283655658/release/3.2(3h)

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 for Upgrading Obsolete Hyperflex Releases 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-3.0.1i-29888.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. Browse and select the HX Data Platform upgrade package `storfs-packages-3.0.1i-29888.tgz`.
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). Confirm the desired version of UCS C-series and B-series firmware bundles are uploaded to the UCSM before you start the upgrade process.

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 The upgrade process performs the rolling reboot of each node in the cluster without any traffic disruptions.

If the upgrade fails, you can re-try the upgrade or contact Cisco TAC for further assistance. Running a cluster without remediation after an upgrade failure is not recommended. Care should be taken to fully complete the upgrade as soon as possible.

Workflow 2: Upgrading to the Destination Release

Upgrading to the Destination Release

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

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, on page 10
- Software Download for HXDP Release 4.0(2f) or the latest suggested release , on page 11

Software Downloads

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(4k) was the compatible UCS server firmware for the suggested HXDP release of 3.5(2h) and 3.5(2i). 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 Cisco HyperFlex Recommended Software Release and Requirements Guide.

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

UCS Infra Package Download

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

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

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

UCS Blade Package:

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

UCS C-series Package:

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

Software Download for HXDP Release 4.0(2f) 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 4.0(2f) was the suggested release. For more information about how to locate the latest suggested release on the Cisco Software Download page, see Navigating the Cisco HyperFlex Data Platform Software Downloads, on page 70 and the Cisco HyperFlex Recommended Software Release and Requirements Guide.

- **Upgrade Package:** storfs-packages-4.0.2f-35930.tgz
- **Link:** https://software.cisco.com/download/home/286305544/type/286305994/release/4.0(2f)

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 for Upgrading Obsolete Hyperflex Releases 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-3.5.2h-32139.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 HX Data Platform and UCS Firmware

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-3.5.2h-32139.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.

UI Element	Essential Information
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(4h)

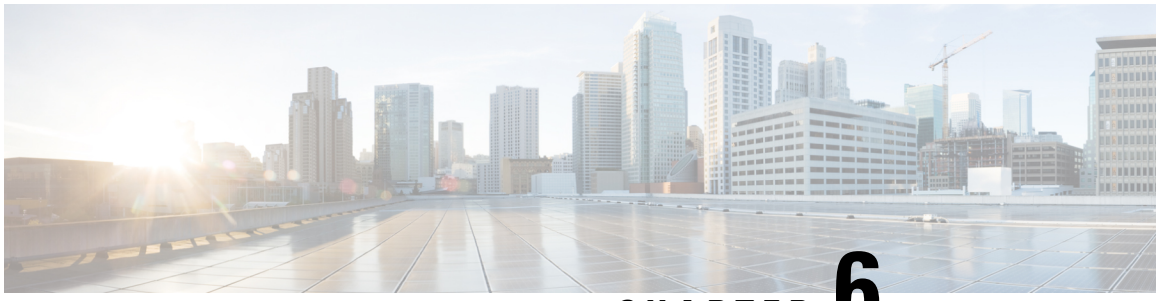
Note If you don't see the desired UCS firmware version in the drop-down, verify that the B-series and C-series firmware bundles are uploaded to UCSM and retry your action.

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.

The upgrade process performs the rolling reboot of each node in the cluster without any traffic disruptions.

If the upgrade fails, you can re-try the upgrade or contact Cisco TAC for further assistance. Running a cluster without remediation after an upgrade failure is not recommended. Care should be taken to fully complete the upgrade as soon as possible.



CHAPTER 6

Upgrading Cisco HyperFlex 1.8(1a-1e)

Overview: Upgrading Cisco HyperFlex 1.8(1a-1e)

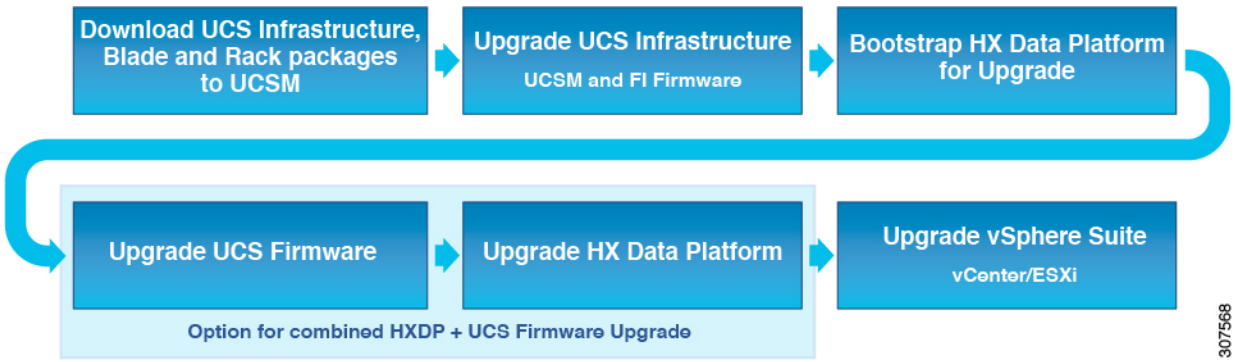
Prerequisites

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

- Prerequisites for Upgrading Obsolete Hyperflex Releases, on page 2
- Hypercheck: HyperFlex and Pre-Upgrade Check Tool, on page 3
- Verify the ESXi and vCenter Build Number, on page 3

Upgrade Path for Cisco HyperFlex Data Platform 1.8(1a-1e)

Upgrading from Cisco HyperFlex Data Platform 1.8(1a-1e) 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 upgrade to a recommended Cisco HyperFlex version.

Product	Your Current Release	Upgrade to Intermediate Releases		Upgrade to the Destination Release
HyperFlex software	HXDP 1.8(1a-1e)	First: 2.6(1e)	Second: 4.0(2f)	The latest suggested release on the Cisco Software Download site.
UCS firmware	UCS 3.1(2b) or later.	Minimum version 3.2(3d)		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.

Note The upgrade process consists of the following tasks complete each step in the order presented.

- Download software bundles.
- Install software bundles.
- Upgrade UCS Firmware to a minimum version of 3.2(3d).
- Upgrade HyperFlex Data Platform Software to Version 2.6(1e).
- Perform the second upgrade process to the destination version.

Workflow 1: Upgrading to the Intermediate Release

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:

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(3d), on page 49
- Software Download: HXDP Release 2.6(1e), on page 49

Software Downloads

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

UCS Firmware 3.2(3d)

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/283612660/type/283655658/release/3.2(3d)

UCS Infra Package Download

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

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

UCS Blade Package:

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

UCS C-series Package:

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

Software Download: HXDP Release 2.6(1e)

HXDP Release 2.6(1e)

- **Upgrade Package:** storfs-packages-2.6.1e-26812.tgz
- **Link:** https://software.cisco.com/download/home/286305544/type/286305994/release/2.6(1e)

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 for Upgrading Obsolete Hyperflex Releases 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-2.6.1e-26812.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

Note This workflow should only be used if the current HXDP version is before 3.5(1a).

If the current HXDP Release is 3.5(1a) or later, upgrade using HX Connect.

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. Browse and select the HXDP package `storfs-packages-<version>.tgz`.
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(4k). Confirm the desired version of UCS C-series and B-series firmware bundles are uploaded to the UCSM before you start the upgrade process.

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 The upgrade process performs the rolling reboot of each node in the cluster without any traffic disruptions.

If the upgrade fails, you can re-try the upgrade or contact Cisco TAC for further assistance. Running a cluster without remediation after an upgrade failure is not recommended. Care should be taken to fully complete the upgrade as soon as possible.

Workflow 2: Upgrading to the Destination Release

Upgrading to the Destination Release

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

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, on page 10
- Software Download for HXDP Release 4.0(2f) or the latest suggested release , on page 11

Software Download

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(4k) was the compatible UCS server firmware for the suggested HXDP release of 3.5(2h) and 3.5(2i). 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 Cisco HyperFlex Recommended Software Release and Requirements Guide.

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

UCS Infra Package Download

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

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

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

UCS Blade Package:

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

UCS C-series Package:

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

Software Download for HXDP Release 4.0(2f) 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 4.0(2f) was the suggested release. For more information about how to locate the latest suggested release on the Cisco Software Download page, see Navigating the Cisco HyperFlex Data Platform Software Downloads, on page 70 and the Cisco HyperFlex Recommended Software Release and Requirements Guide.

- **Upgrade Package:** storfs-packages-4.0.2f-35930.tgz
- **Link:** https://software.cisco.com/download/home/286305544/type/286305994/release/4.0(2f)

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 for Upgrading Obsolete Hyperflex Releases 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-3.5.2h-32139.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 HX Data Platform and UCS Firmware

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 5: 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-3.5.2h-32139.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 6: vCenter Credentials

UI Element	Essential Information
User Name field	Enter the vCenter <admin> username.

UI Element	Essential Information
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 7: 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 8: 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(4h)

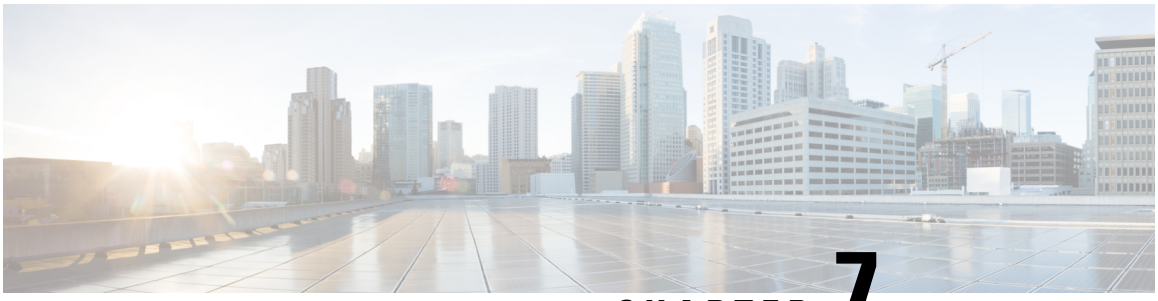
Note If you don't see the desired UCS firmware version in the drop-down, verify that the B-series and C-series firmware bundles are uploaded to UCSM and retry your action.

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.

The upgrade process performs the rolling reboot of each node in the cluster without any traffic disruptions.

If the upgrade fails, you can re-try the upgrade or contact Cisco TAC for further assistance. Running a cluster without remediation after an upgrade failure is not recommended. Care should be taken to fully complete the upgrade as soon as possible.

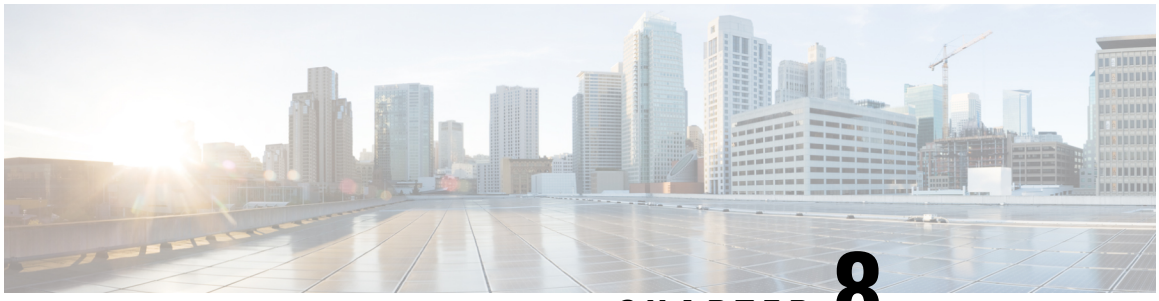


CHAPTER 7

Upgrading Cisco HyperFlex 1.7

Upgrading Cisco HyperFlex 1.7 Upgrade

If you are currently running Cisco HyperFlex 1.7(x) in your environment, please contact Cisco TAC for assistance with upgrading. Do not attempt to upgrade on your own.



CHAPTER 8

Troubleshooting

Verifying and Recreating the HX User Account

Important This troubleshooting task requires root access provided by TAC via a challenge response.

Step 1 Check for missing hxuser account:

a) Secure Shell (SSH) to all esxi hosts.

b) Type **`esxcli system account list`**.

c) Verify that the hxuser account is present on all esxi hosts. If the hxuser account is missing, proceed to step 2.

Step 2 Secure Shell (SSH) to any controller:

a) Type **`cd /opt/springpath/storfs-mgmt/hxtoolbox-1.0/bin`**.

b) Type **`./hxtoolbox -u`**.

Note If you see an error, open a TAC case.

c) Verify that the huxser is created on the esxi hosts (Repeat step 1).

Step 3 Rerun the upgrade.

Verifying and Recreating the Springpath User Account

Step 1 Check for missing Springpath user account:

a) Secure Shell (SSH) to all esxi hosts.

b) Type **esxcli system account list**.

c) Verify that the Springpath user account is present on all esxi hosts. If the Springpath user account is missing, proceed to step 2.

Step 2 On the ESXi hosts where springpath user is missing:

a) Type **esxcli system account add -i springpath -p spr!n9p@th -c spr!n9p@th**.

b) Type **esxcli system permission set -i springpath -r Admin**.

c) Verify that the Springpath User is present on missing nodes (Repeat step 1).

Step 3 Rerun the upgrade.

After Upgrade Cluster Shows Offline from CLI/nodes Show Offline in vCenter HXDP Plugin Summary

Step 1 Recreate Springpath_security.properties link:

a) Secure Shell (SSH) to all controller VMs.

b) Type **ls /usr/share/springpath/storfs-misc/** and confirm the **springpath_security.properties** link exists on all controllers.

c) Type **ls /etc/springpath/secure** to confirm that the **springpath_security.properties** file exists on all nodes.

Step 2 If the file is missing, copy the file from another node to the missing node:

Example (from controller with the file):

```
scp /etc/springapth/secure/springapth_security.properties root@10.10.10.5:
/etc/springpath/secure/springpath_security.properties
```

Step 3 If the alias link is missing, you must recreate the link on the missing node:

Example:

```
/etc/springpath/secure/springpath_security.properties
```

a) Type **ln -s /usr/share/springpath/storfs-misc/springpath_security.properties /etc/springpath/secure/springpath_security.properties**.

b) Type **restart stMgr**.

Step 4 Verify the fix:

a) Type **stcli cluster info** and confirm that the vCluster state is online.

b) In the HXDP vCenter plugin, confirm that the nodes all show as online in the summary section.

Update Net.Team Policy

Perform the following steps on ALL ESXi Hosts:

Step 1 Confirm current value is set to 100.

```
[root@JR-NODE-1:~] esxcli system settings advanced list -o /Net/TeamPolicyUpDelay
```

Step 2 Change **/Net/TeamPolicyUpDelay --int-value** from 100 (Default value) to 30000.

```
[root@JR-NODE-1:~] esxcli system settings advanced set -o /Net/TeamPolicyUpDelay --int-value 30000
```

Step 3 Confirm the new value of **/Net/TeamPolicyUpDelay --int-value** is 30000.

```
[root@JR-NODE-1:~] esxcli system settings advanced list -o /Net/TeamPolicyUpDelay
 Path: /Net/TeamPolicyUpDelay
 Type: integer
 Int Value: 30000 <— Value set in Step-1 above from 100(Default value) to 30000
 Default Int Value: 100
 Min Value: 0
 Max Value: 600000 String Value:
 Default String Value:
 Valid Characters:
 Description: Delay (ms) before considering an 'uplink up' event relevant
```

Precheck Validation Failure Due to an Algorithm Change in 6.0 U3

While upgrading HX, with version 6.0 U3 and later, we see following error: **Failed upgrade validations : Checking vCenter configuration. Reason: Upgrade validations failed. Failed to query ESX version on host X.X.X.X**

```
root@SpringpathControllerXXXX:~# stcli cluster upgrade --components hxdp --location
/tmp/storfs-packages-3.5.2d-31738.tgz --vcenter-user administrator@XXX.com
…Waiting for upgrade validations to finish... ['Checking vCenter configuration']
Failed upgrade validations : Checking vCenter configuration. Reason: Upgrade validations
 failed. Failed to query ESX version on host: X.X.X.X

From ESXi  /var/run/log/auth.log

2019-07-03T19:56:18Z sshd[757807]: Connection from X.X.X.Xport 42416
2019-07-03T19:56:18Z sshd[757807]: Unable to negotiate with X.X.X.Xport 42416:
no matching key exchange method found. Their offer: diffie-hellman-group1-sha1,
diffie-hellman-group-exchange-sha1 [preauth]
```

Step 1 **Workaround:** On each ESXI host in the cluster, edit the **/etc/ssh/sshd_config** file. Add `KexAlgorithms diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1` to the end of the file.

Step 2 Rerun the upgrade command or resume from UI.

Pycrypto Minimum Version

Verify the minimum package version is 2.6.

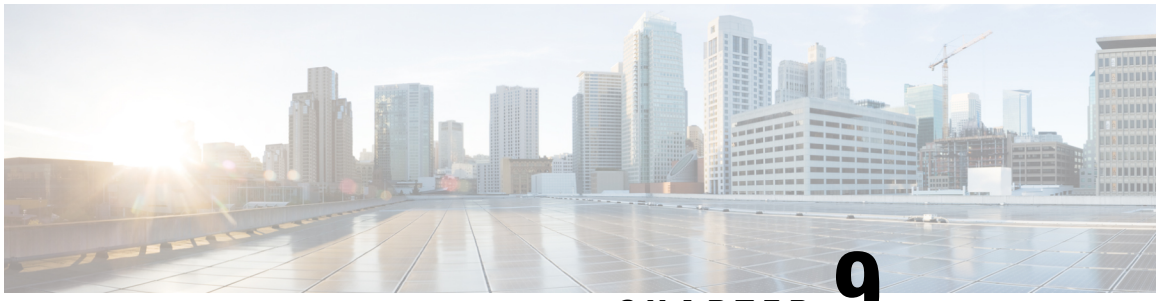
```
EXAMPLE:
 $ pip show pycrypto
---
Name: Jinja2
Version: 2.6.1
```

Extra or Duplicate stNode is Present in stcli after Upgrade

Contact TAC.

Duplicate pnode is Present in stcli cluster info after Upgrade

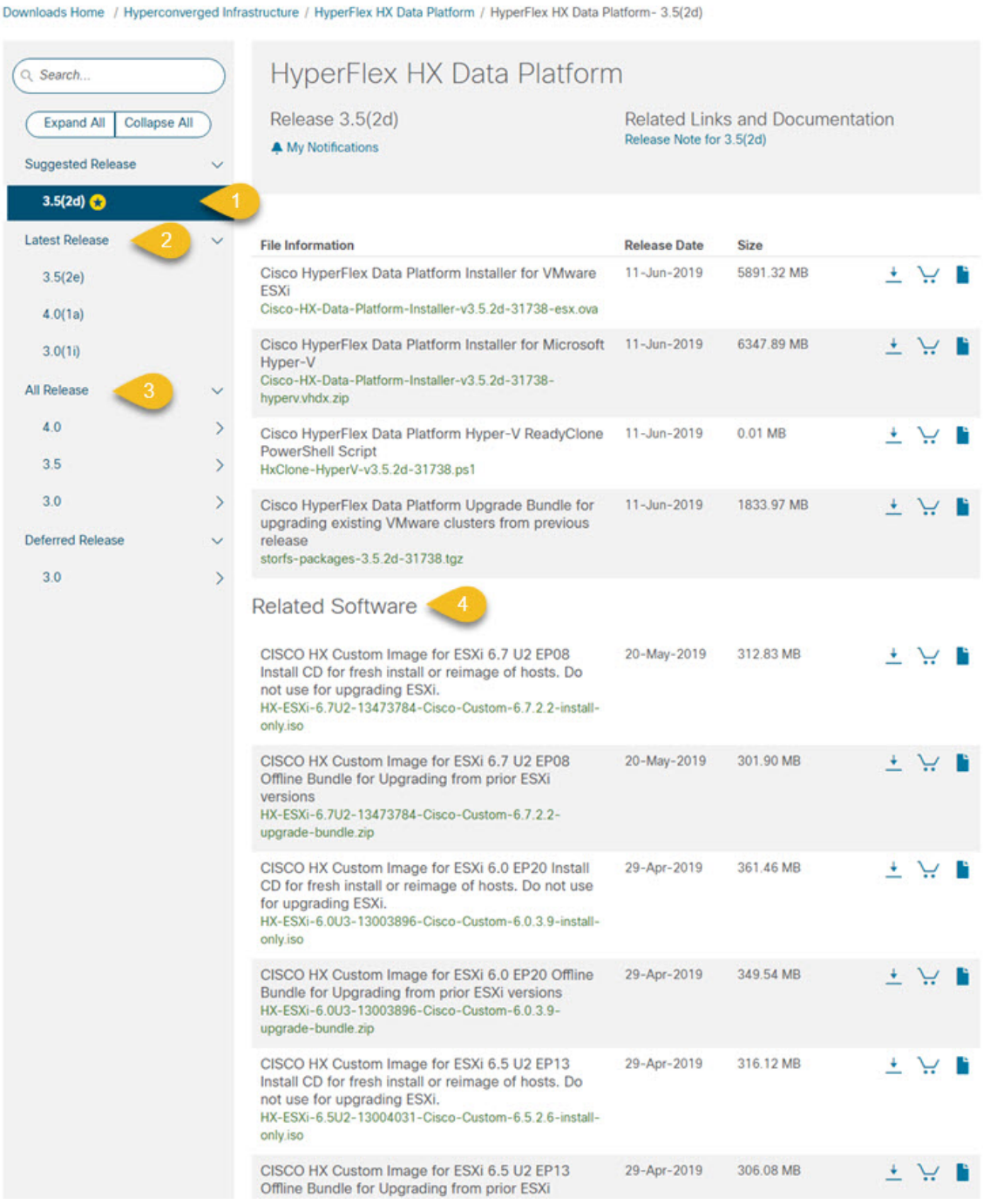
Contact TAC.



CHAPTER 9

Appendix

Navigating the Cisco HyperFlex Data Platform Software Downloads



https://software.cisco.com/download/home/286305544/type/286305994/

Locating your release

The left navigation pane allows you to search, scroll, and click to your desired Cisco HyperFlex Data Center release. Click on a release number to display all the available software bundles in the right panel with the available software.

1. **Suggested Release** The star next to 3.5(2d) identifies this as the current recommended long-lived release for HyperFlex. Long-lived release is a stable roll-up of features from previous short-lived feature releases with additional hardening and bug fixes. This release does not introduce any new major features and will require fewer upgrades to remain current. Customers who need a release that is supported for a longer period of time are encouraged to use the Suggested Release. All upgrades in this guide should use a suggested release.
2. **Latest Release** This grouping presents the releases in the order they are released. The newest being listed first and includes long-lived and short-lived feature release. Use the arrow on the right to collapse and expand the list. Click on a release number to view all software bundles that are associated with that specific release.
3. **All Release** This grouping orders the releases based on their feature number (the first two digits of a release. such as 4.0) and includes long-lived and short-lived feature release. Use the arrow on the right to collapse and expand the list.
4. **Related Software** Download your related software from the HyperFlex Data Platform release page. The related software listed with each HXDP release is the compatible UCSM, UCS Server Firmware, and ESXi versions for use with the selected HX version.

For information on the supported HX upgrade paths, see the HX Upgrade Guide.

Known Issues

The following caveats are known. To review the details in the Cisco Bug Search Tool, click on the caveat number or enter search parameters in the Bug Search Tool to find matching results.

Caveat Number	Title	Workaround
CSCvq81434	HXDP upgrade from 2.1.1c to 3.5.2g failing.	Fixed in 3.5(2g) and 4.0(2a).

Caveat Number	Title	Workaround
CSCvk02032	Unable to log into HX Connect or installation failed due to Lib mount issue.	If you are unable to log into HX Connect after rebooting of the controller VM perform the following steps: SSH to each controller one at a time: 1. Verify files are populated in `/var/lib/tomcat7/webapps/` 2. Run `echo manual > /etc/init/ureadahead.override` 3. Run `echo manual > /etc/init/ureadahead-other.override` 4. Run `mount | grep lib` If only `/var/old-lib` is mounted, run steps 5 through 7 5. Run `python /usr/share/springpath/storfs-misc/relinquish_node.py` 6. Run `reboot` 7. Wait for cluster to become healthy. 8. Run steps 1 through 7 on the next controller.
CSCvn09831	Upgrade fails for HX cluster that were originally installed for HX 1.7 release only due to missing pycrypto package.	Manually install pycrypto version only for clusters that started with HX 1.7. (see Troubleshooting, on page 65).
CSCvk09073	During upgrade from 2.x to 3.x, if the upgrade encounters a failure, the Cluster Management IP may no longer be reachable (not present on any of the controller VMs).	CLI upgrade required-Contact TAC
CSCvp79604	The same stNodes are present before and after the upgrade.	Manually remove stNode. Contact Cisco TAC.
CSCvp79629	After upgrade, an extra pnode is present in stcli.	Manually remove pnode. Contact Cisco TAC.

Caveat Number	Title	Workaround
CSCvo16282	Cluster may lose access to storage during UCSM Infrastructure upgrade of the Fabric interconnects. Pre-upgrade check to change setting of `Net.TeamPolicyUpDelay` for each ESXi host.	Pre-upgrade check to change setting of `Net.TeamPolicyUpDelay` to 30 seconds for each ESXi host (see Troubleshooting, on page 65).
CSCvp42925	Any modification from HX installer is causing LLDP to be disabled on all HX vNICs.	Re-enable LLDP post-upgrade.
CSCvn73127	Kernel Migration failed on Searching For Local Datastore on ESXi Host.	Disconnect external storage and retry kernel upgrade.
CSCvm97558	`storfs` restarted due to Out of Memory - 3.01c.	Fixed in 3.0(1i).
CSCvh04307	Installing Software Packages on Storage Controller VM failed .	Manually unlock the drives. Fixed in UCS firmware version 4.0(1b). Contact Cisco TAC.
CSCvk62990	HX Deployments on M5 servers with ESXi version 6.0 may experience a PSOD during install or upgrade workflows.	Upgrade ESXi using HX ESXi offline bundle to 6.5 or 6.0 Cisco custom build 9919195 or later. Fixed in Cisco custom image ESXi 6.0 EP 19/6.0 U3 EP 18 Offline bundle. Related Software Advisory .
CSCvk39622	With ESXi hosts in Normal lock-down mode, HX Connects upgrade tab shows, "server call failed" error.	If vCenter is unavailable, perform the follow the steps below in VMware Host Client to add an exception user. 1. Click Manage in VMware Host Client inventory and click Security & Users. 2. Click Lockdown mode 3. Click Add user exception, enter the name of the user("hxuser"), and click Add exception. **Note** These alarms are manually reset to green.
CSCvm90352	HX Zookeeper fails due to high `/var/zookeeper` utilization.	Fixed in 3.0(1e). Contact Cisco TAC.

Caveat Number	Title	Workaround
CSCvm46965	Cluster rebalance/upgrade hang. If the cluster becomes unhealthy due node or disk removal/crash, it will not become healthy.	Fixed in 3.0(1i)/3.5(2a). When observed, stop the write intensive workload, or upgrade to 3.0(1i)/3.5(2a). If rebalance doesn't progress after 30 minutes, contact TAC.
CSCvo91624	HXDP 3.5.1a - HX Connect - UCS firmware upgrade server auto acknowledge failed after HFP	Fixed on 4.0(2a). Manually acknowledge pending reboots one at a time.
CSCvm77294	[VMware issue] Upgrade validations failed. DRS Fault: Insufficient resources to satisfy configured failover.	Disable admissions control. Detailed workaround steps are located in CSCvm77294.

(Optional) ESXi Upgrade to 6.5 or 6.7

Upgrading to VMware 6.5 or 6.7 is and optional post Cisco HyperFlex upgrade. Once you have successfully upgraded to the latest suggested release on the Cisco Software Download site, you may upgrade the vSphere and ESXi versions.

To get started, download the software bundles as described below:

Note Example upgrade bundles are listed. be sure that you download the latest 6.5 or 6.7 upgrade ZIP bundle that is listed as related software for your HXDP version.

Note Do not use the HX ISO to upgrade ESXi. You must use the offline ZIP bundle to perform ESXi upgrades.

Software Download: ESXI 6.5

Example Upgrade Bundle: CISCO HX Custom Image for ESXi 6.5 U2 EP09
HX-ESXi-6.5U2-10175896-Cisco-Custom-6.5.2.3-upgrade-bundle.zip

Download Link: https://software.cisco.com/download/home/286305544/type/286305994/

Software Download: ESXi 6.7

Example Upgrade Bundle: CISCO HX Custom Image for ESXi 6.7 U2 EP08
HX-ESXi-6.7U2-13473784-Cisco-Custom-6.7.2.2-upgrade-bundle.zip

Download Link: https://software.cisco.com/download/home/286305544/type/286305994/

Upgrading vSphere and ESXi to 6.5 or 6.7

1. Log in to HX Connect.
   a. Enter the HX Storage Cluster management IP address in a browser. Navigate to `https://<storage-cluster-management-ip>`.
   b. Enter the administrative username and password.
   c. Click Login.
2. In the Navigation pane, select **Upgrade**.
3. On the Select Upgrade Type page, select ESXi and complete the following fields:

UI Element	Essential Information
Drag the ESXi file here or click to browse field	Upload the latest Cisco HyperFlex Custom Image Offline Bundle for upgrading existing ESXi hosts from Download Software - HyperFlex HX Data Platform. **Example:** `HX-ESXi-6.5U2-13004031-Cisco-Custom-6.5.2.6-upgrade-bundle.zip`
Current version field	Displays the current ESXi version.
Current hypervisor details field	Lists the HyperFlex cluster details like the Hypervisor version and Cluster upgrade state.
Bundle details field	Displays the ESXi version of the uploaded bundle.

Additional References

The following sections provide references related upgrading Cisco HyperFlex Data Center

Table 9: Related Documents

Related Topic	Document Title / Link
Recommended Cisco HyperFlex HX Data Platform Software Releases - for Cisco HyperFlex HX-Series Systems	https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/release-guidelines-and-support-timeline/b-recommended-hx-data-platform-sw-releases.html
Cisco HyperFlex Software Release Model and Release Support Timeline	https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/release-guidelines-and-support-timeline/b-release-bulletin-hyperflex.html

Technical Assistance

	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport