Deploy HyperFlex Fabric Interconnect Clusters

Installation Overview

The following table summarizes the installation workflow for a configuring a Fabric Interconnect-attached HyperFlex cluster:

Step	Description	Reference
1.	Complete the preinstallation checklist.	Preinstallation Checklist for Cisco HX Data platform
2.	Ensure that the network is set up.	
3.	Log in to Cisco Intersight.	Log In to Cisco Intersight
4.	Claim Targets. **Note** Skip if you have already claimed HyperFlex Nodes.	Claim Targets
5.	(Optional) Verify Cisco UCS Firmware versions.	Verify Firmware Version for Fabric Interconnect, on page 5
6.	Run the Create HyperFlex Cluster Profile Wizard.	Configure HyperFlex Fabric Interconnect Clusters, on page 5
7.	Run the post installation script through the controller VM.	Post Installation Tasks

Preinstallation Checklist for HyperFlex Fabric Interconnect-attached Clusters

Ensure that your system meets the installation and configuration requirements before you begin to install Cisco HyperFlex Fabric Interconnects-attached clusters. Refer to the Preinstallation Checklist for Cisco HX Data Platform for detailed preinstallation requirements.

Supported Models/Versions for HyperFlex with Fabric Interconnect Cluster Deployments

The following table lists the supported hardware platforms and software versions for HyperFlex with Fabric Interconnect cluster deployments. For information about the Product Identification Standards (PIDs) that are supported by Cisco Intersight, see Cisco HyperFlex HX-Series Data Sheet.

Component	Models/Versions
M6 Servers	• HXAF245C-M6SX • HX245C-M6SX • HXAF225C-M6SX • HX225C-M6SX • HX220C-M6S • HX240C-M6SX • HX240C-M6L • HXAF220C-M6S • HXAF220C-M6SN • HXAF240C-M6SX • HXAF240C-M6SN
M5 Servers	• HX220C-M5SX • HXAF220C-M5SX • HX240C-M5L • HX240C-M5SX • HXAF240C-M5SX

Component	Models/Versions
Cisco HyperFlex HX Data Platform (HXDP)	• 5.5(1a) • 5.0(2e), 5.0(2g) **Note** • HXDP versions 5.0(2a), 5.0(2b), 5.0(2c), 5.0(2d), 4.5(2a), 4.5(2b), 4.5(2c), 4.5(2d), and 4.5(2e) are still supported for cluster expansion only. • Upgrades from HXDP 4.0.2x are supported provided the ESXi version is compatible with 4.5(2x). • M6 servers require HXDP 5.0(1a) or higher.
Device Connector	Auto-upgraded by Cisco Intersight

Installation

Log In to Cisco Intersight

Log In using Cisco ID

To login to Cisco Intersight, you must have a valid **Cisco ID** to create a Cisco Intersight account. If you do not have a Cisco ID, create one here.

Important The device connector does not mandate the format of the login credentials, they are passed as is to the configured HTTP proxy server. Whether or not the username must be qualified with a domain name will depend on the configuration of the HTTP proxy server.

Log In using Single Sign-On

Single Sign-On (SSO) authentication enables you to use a single set of credentials to log in to multiple applications. With SSO authentication, you can log in to Intersight with your corporate credentials instead of your Cisco ID. Intersight supports SSO through SAML 2.0, and acts as a service provider (SP), and enables integration with Identity Providers (IdPs) for SSO authentication. You can configure your account to sign in to Intersight with your Cisco ID and SSO. Learn more about SSO with Intersight here.

Claim Fabric Interconnect Targets

Complete the following steps to claim one or more Targets to be managed by Cisco Intersight:

Before you begin

This procedure assumes that you are an existing user with a Cisco account. If not, see Log In to Cisco Intersight.

Step 1 In the Cisco Intersight, left navigation pane, select **ADMIN** > **Targets**.

Step 2 In the **Targets** details page, click **Claim a New Target**.

Step 3 In the **Claim a New Target** wizard, select **Hyperconverged** > **Cisco HyperFlex Cluster** and complete the following fields:

Note You can locate the **Device ID** and the **Claim Code** information in:

a. Cisco UCS Manager and Cisco IMC by navigating to **Admin** > **Device Connector**.

b. Cisco HyperFlex by navigating to **HyperFlex Connect UI** > **Settings** > **Device Connector**.

c. Cisco UCS Director by navigating to **Administration** > **Device Connector**.

UI Element	Essential Information
Device ID	Enter the applicable Device ID. • For a UCS Domain, use the serial number of the primary and subordinate FIs, in this format: (Serial number of FI-A & Serial number of FI-B). Example: [SAL1924GKV6&SAL1913CJ7V] • For a standalone server, use serial number. Example: NGTR12345 • For HyperFlex, use Cluster UUID. Example: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx. • For Cisco UCS Director, use Device ID. Example Example: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx.
Claim Code	Enter device claim code. You can find this code in the Device Connector for the target type. **Note** Before you gather the Claim Code, ensure that the Device Connector has outbound network access to Cisco Intersight, and is in the "Not Claimed" state.

Step 4 Click **Claim**.

Note Refresh the Targets page to view the newly claimed target.

Verify Firmware Version for Fabric Interconnect

In Cisco UCS Manager, from **Equipment** > **Firmware Management** > **Installed Firmware** tab, verify for the correct firmware version.

For a complete list of hardware and software inter-dependencies, refer to respective UCSM release version using the UCS Hardware and Software Compatibility tool.

Configure HyperFlex Fabric Interconnect Clusters

To configure a HyperFlex Fabric Interconnect Cluster in Intersight, do the following:

Step 1 Log in to Intersight with HyperFlex Cluster administrator or Account Administrator privileges.

Step 2 Navigate to **CONFIGURE** > **Profiles**.

Step 3 In the **Profiles** page, make sure that the **HyperFlex Cluster Profiles** tab is selected, and click **Create HyperFlex Cluster Profile** to launch the Create HyperFlex Cluster Profile installation wizard.

Step 4 Select **Standard** as the deployment type. Click **Start**.

Step 5 In the **General** page, complete the following fields:

Field	Description
Organization drop-down list	You can make the HyperFlex Cluster Profile belong to the default organization or a specific organization. Choose: • default—To make the Cluster Profile belong to the default organization. All the policies that belong the default organization will be listed on the Create HyperFlex Cluster Profile wizard. • *Specific*Organization—To make the HyperFlex Cluster Profile belong to the specified organization only. Only the policies that belong to the selected organization will be listed on the Create HyperFlex Cluster Profile wizard. For example, if HyperFlex nodes are shared across two organizations and are associated to a Cluster Profile in one organization, you cannot associate the same node to a Cluster Profile in another organization. The Cluster Profile will be available only to users who belong the specified Organization.
Name field	Enter a name for the HyperFlex cluster. The cluster name will be used as the vCenter cluster name, HyperFlex storage controller name, and HyperFlex storage cluster name.

Field	Description
HyperFlex Data Platform Version drop-down list	Select the version of the Cisco HyperFlex Data Platform to be installed. This can be one of the following: • 5.5(1a) • 5.0(2e), 5.0(2g) **Note** The version that you select impacts the types of HyperFlex policies that you can choose later in the configuration wizard.
Server Firmware Version drop-down list	Manually enter the server firmware bundle version used for server components such as CIMC, adapters, BIOS, etc. Refer to the Release Notes for Cisco HX Data Platform for the recommended firmware for each HX Data Platform release.
(Optional) **Description** field	Add a description for the HyperFlex cluster profile.
(Optional) **Set Tags** field	A tag key.

Click **Next**.

Step 6 In the **Nodes Assignment** page, you can assign nodes now or optionally, you can choose to assign the nodes later. To Assign nodes, click the **Assign nodes** check box and select the node you want to assign. You can view the node role based on Server Personality.

You can view the node role based on Server Personality in the **Node Type** column. If you choose a node that has a *HyperFlex Compute Server* or no personality, you must ensure that the required hardware is available in the server for succesful cluster deployment. For information about the Product Identification Standards (PIDs) that are supported by Cisco Intersight, see Cisco HyperFlex HX-Series Data Sheet

Important Cisco HyperFlex Fabric Interconnect cluster allows a minimum of 3 to a maximum of 32 nodes. All selected nodes should belong to the same UCS domain.

Click **Next**.

Step 7 In the **Cluster Configuration** page, complete the following fields:

Note For the various cluster configuration tasks, you can enter the configuration details or import the required configuration data from policies. To use pre-configured policies, click **Select Policy**, next to the configuration task and choose the appropriate policy from the list.

Field	Description
Security	
Hypervisor Admin field	Hypervisor administrator username must contain only alphanumeric characters. **Note** Use root account for ESXi deployments.

Field	Description
Hypervisor Password field	Enter the Hypervisor password, this can be one of the following: **Remember** The default ESXi password of Cisco123 must be changed as part of installation. For fresh ESXi installation, ensure the checkbox for **The Hypervisor on this node uses the factory default password is checked**. Provide a new ESXi root password that will be set on all nodes during installation. If the ESXi installation has a non-default root password, ensure the checkbox The **Hypervisor on this node uses the factory default password** is unchecked. Provide the ESXi root password that you configured. This password will not be changed during installation.
Hypervisor Password Confirmation field	Retype the Hypervisor password.
Controller VM Admin Password field	Enter a user-supplied HyperFlex storage controller VM password. The password must contain a minimum of 10 characters, with at least 1 lowercase, 1 uppercase, 1 numeric, and 1 of these -_@#$%^&*! special characters. **Note** Make a note of this password as it will be used for the administrator account.
Controller VM Admin Password Confirmation field	Retype the Controller VM administrator password.
DNS, NTP, and Timezone	
Timezone field	Select the local timezone.
DNS Servers field	Enter one or more DNS servers. A DNS server that can resolve public domains is required for Intersight.
NTP Servers field	Enter one or more NTP servers (IP address or FQDN). A local NTP server is highly recommended.
(Optional) **DNS Suffix** field	Enter the DNS search suffix. This field is applicable only for Cisco HX Data Platform release 3.0 and later.
vCenter (Optional Policy)	
vCenter Server FQDN or IP field	Enter the vCenter server FQDN or IP address.
vCenter Username field	Enter the vCenter username. For example, *administrator@vsphere.local*

Field	Description
vCenter Password field	Enter the vCenter password.
vCenter Datacenter Name field	Enter the vCenter datacenter name.
Storage Configuration (Optional Policy)	
VDI Optimization check box	Check this check box to enable VDI optimization (hybrid HyperFlex systems only).
Logical Availability Zones check box	Logical Availability Zones configuration is recommended. This option is available for HyperFlex cluster sizes with 8 or more nodes and clusters deployed on Cisco HX Data Platform, Release 3.0 or higher. **Note** Logical Availability Zones configuration is recommended for HyperFlex Clusters with 8 or more nodes connected to Fabric Interconnect.
Auto Support (Optional Policy)	
Auto Support check box	Check this check box to enable Auto Support.
Send Service Ticket Notifications To field	Enter the email address recipient for support tickets.
Node IP Ranges	
Note This section configures the management IP pool. You must complete the management network fields to define a range of IP addresses for deployment. On the node configuration screen, these IP addresses will be automatically assigned to the selected nodes. If you wish to assign a secondary range of IP addresses for the controller VM Management network, you may optionally fill out the additional fields below. Both IP ranges must be part of the same subnet.	
Management Network Starting IP field	Enter the starting IP address for the management IP pool.
Management Network Ending IP field	Enter the ending IP address for the management IP pool.
Management Network Subnet Mask field	Enter the subnet mask for the management VLAN.
Management Network Gateway field	Enter the default gateway for the management VLAN.
Controller VM Management Network Starting IP (Optional)	Enter the starting IP address for the controller VM management network.
Controller VM Management Network Ending IP (Optional)	Enter the ending IP address for the controller VM management network.
Controller VM Management Network Subnet Mask (Optional)	Enter the subnet mask for the controller VM management network.
Controller VM Management Network Gateway (Optional)	Enter the default gateway for the controller VM management network.

Field	Description
Cluster Network	
VM Migration VLAN Name field	Enter the VLAN name for the VM Migration. The name can be from 1 to 32 characters long and can contain a combination of alphanumeric characters, underscores, and hyphens.
VM Migration VLAN ID field	Enter the VLAN ID for the VM Migration. An ID of 0 means the traffic is untagged. The ID can be any number between 0 and 4095, inclusive.
VM Network VLAN Name field	Enter the VLAN name for the VM Network. The name can be from 1 to 32 characters long and can contain a combination of alphanumeric characters, underscores, and hyphens. You can add additional VM Network VLAN Names if necessary.
VM Network VLAN ID field	Enter the VLAN ID for the VM Network. The ID can be any number between 0 and 4095, inclusive.
KVM Starting IP field	Enter the Start IP address for out-of-band KVM access. One IP address per node is required. The range must fall in the same address range as UCS Manager management interfaces.
KVM Ending IP field	Enter the End IP address for out-of-band KVM access.
KVM Subnet Mask field	Enter the Subnet mask for the KVM.
KVM Gateway field	Enter the Gateway for the KVM.
Management Network VLAN Name field	Enter the VLAN name for the management network. The name can be from 1 to 32 characters long and can contain a combination of alphanumeric characters, underscores, and hyphens.
Management Network VLAN ID field	Enter the VLAN ID for the management network. VLAN must have access to Intersight. The name can be from 1 to 32 characters long and can contain a combination of alphanumeric characters, underscores, and hyphens.
Jumbo Frames check box	For best performance, enable Jumbo Frames.
External FC Storage (Optional Policy) If you want to add external storage, configure **FC Storage** by completing the following fields:	
Enable FC Storage check box	Check this check box to enable FC Storage.

Field	Description
VSAN A Name field	The name of the VSAN for the primary Fabric Interconnect (FI-A). Enter the name of the first Virtual Storage Area Network. The name can be from 1 to 32 characters long and can contain a combination of alphanumeric characters, underscores, and hyphens.
VSAN A ID field	The unique identifier assigned to the network for the primary Fabric Interconnect (FI-A). **Attention** Do not enter VSAN IDs that are currently used on the UCS or HyperFlex system. If you enter an existing VSAN ID in the installer which utilizes UCS zoning, zoning will be disabled in your existing environment for that VSAN ID. Enter the ID of the first Virtual Storage Area Network. The ID can be any number between 1 and 4093, inclusive.
VSAN B Name field	The unique identifier assigned to the network for the subordinate Fabric Interconnect (FI-B). **Note** Do not enter VSAN IDs that are currently used on the UCS or HyperFlex system. If you enter an existing VSAN ID in the installer which utilizes UCS zoning, zoning will be disabled in your existing environment for that VSAN ID. Enter the name of the second Virtual Storage Area Network. The name can be from 1 to 32 characters long and can contain a combination of alphanumeric characters, underscores, and hyphens.
VSAN B ID field	Enter the ID of the second Virtual Storage Area Network. The ID can be any number between 1 and 4093, inclusive.
WWxN Range Starting Address field	Enter the start address of the WWxN range in the form of 20:00:00:25:B5:XX.
WWxN Range Ending Address field	Enter the end address of the WWxN range in the form of 20:00:00:25:B5:XX.
External iSCSI Storage (Optional Policy) If you want to add external storage, configure **iSCSI Storage** by completing the following fields:	
Enable iSCSI Storage check box	Check this check box to enable iSCSI Storage.

Field	Description
VLAN A Name field	Name of the VLAN associated with the iSCSI vNIC, on the primary Fabric Interconnect (FI-A). Enter the name of the first Virtual Local Area Network. The name can be from 1 to 32 characters long and can contain a combination of alphanumeric characters, underscores, and hyphens.
VLAN A ID field	ID of the VLAN associated with the iSCSI vNIC, on the primary Fabric Interconnect (FI-A). Enter the ID of the first Virtual Local Area Network. The ID can be any number between 0 and 4095, inclusive.
VLAN B Name field	Name of the VLAN associated with the iSCSI vNIC, on the subordinate Fabric Interconnect (FI-B). Enter the name of the second Virtual Local Area Network. The name can be from 1 to 32 characters long and can contain a combination of alphanumeric characters, underscores, and hyphens.
VLAN B ID field	ID of the VLAN associated with the iSCSI vNIC, on the subordinate Fabric Interconnect (FI-A). Enter the ID of the second Virtual Local Area Network. The ID can be any number between 0 and 4095, inclusive.
Proxy Setting (Optional Policy)	
Hostname field	Enter the HTTP proxy server FQDN or IP address.
Port field	Enter the proxy port number.
Username field	Enter the HTTP Proxy username.
Password field	Enter the HTTP Proxy password.
HyperFlex Storage Network	
Storage Network VLAN Name field	Enter the VLAN name for the storage network. The name can be from 1 to 32 characters long and can contain a combination of alphanumeric characters, underscores, and hyphens.

Field	Description
Storage Network VLAN ID field	Enter the VLAN ID for the storage VLAN traffic. The VLAN must be unique per HyperFlex cluster. The ID can be any number between 0 and 4095, inclusive. **Note** The storage VLAN must be unique per HyperFlex cluster. This VLAN does not need to be routable and can remain layer 2 only. IP addresses from the link local range *169.254.x.x/24* are automatically assigned to storage interfaces.

Click **Next**.

Step 8 In the **Nodes Configuration** page, you can view the IP and Hostname settings that were automatically assigned. Intersight will make an attempt to auto-allocate IP addresses. Complete the following fields:

Field	Description
Cluster Management IP Address field	The cluster management IP should belong to the same subnet as the Management IPs.
MAC Prefix Address field	The MAC Prefix Address is auto-allocated. You can overwrite the MAC Prefix address, using a MAC Prefix address from the range 00:25:B5:00 to 00:25:B5:EF. **Attention** Ensure that the MAC prefix is unique across all clusters for successful HyperFlex cluster deployment. Intersight does a validation for duplicate MAC prefix and shows appropriate warning if any duplicate MAC prefix is found.
Replication Factor radio button	The number of copies of each data block written. The options are 2 or 3 redundant replicas of your data across the storage cluster. Replication factor 3 is the recommended option.
Hostname Prefix field	The specified Hostname Prefix will be applied to all nodes.

Step 9 In the **Summary** page, you can view the cluster configuration and node configuration details. Review and confirm that all information entered is correct. Ensure that there are no errors triggered under the **Errors/Warnings** tab.

Step 10 Click **Validate and Deploy** to begin the deployment. Optionally, click **Validate**, and then click **Save & Close** to complete deployment later. The **Results** page displays the progress of the various configuration tasks.

What to do next

Monitoring cluster deployment

Check your cluster deployment progress in the following ways:

- You can remain on the **Results** page to watch the cluster deployment progress in real time.
- You can also close the current view and allow the installation to continue in the background. To return to the results screen, navigate to **CONFIGURE** > **Profiles** > **HyperFlex Cluster Profiles**, and click on the name of your cluster.
- You can see the current state of your deployment in the status column in the HyperFlex Cluster Profile Table view.
- You can also view the progress of the HyperFlex Cluster Profile deployment from the **Requests** page.

Post Installation

Post Installation Tasks

Step 1 Confirm that the HyperFlex Cluster is claimed in Intersight.

Step 2 Confirm that the cluster is registered to vCenter.

Step 3 Navigate to **HyperFlex Clusters**, select your cluster and click **...** to launch HyperFlex Connect.

Step 4 SSH to the cluster management IP address and login using **admin** username and the controller VM password provided during installation. Verify the cluster is online and healthy.

Step 5 Paste the following command in the Shell, and hit enter:

```
hx_post_install
```

Step 6 Follow the on-screen prompts to complete the installation. The **post_install** script completes the following:

- License the vCenter host.
- Enable HA/DRS on the cluster per best practices.
- Suppress SSH/Shell warnings in vCenter.
- Configure vMotion per best practices.
- Add additional guest VLANs/portgroups.
- Perform HyperFlex configuration check.