

Deploy Cisco HyperFlex Edge systems in the cloud with Cisco Intersight



Author: Hui Chen

Last Updated: April 10, 2018

Note: This document contains material and data with multiple dependencies. The information may be updated as and when necessary and is subject to change without notice.

Contents

- Executive Summary**3
- Solution Overview**3
 - Introduction3
- Cisco HyperFlex Edge system**.....4
 - Cisco Intersight cloud-based management platform6
 - Physical topology9
 - Logical topology 10
- Installing Cisco HyperFlex Edge with the Cisco Intersight platform** 13
 - Prerequisites..... 13
 - Sample topology and pre-installation checklist..... 15
 - Cisco Integrated Management Controller configuration 16
 - Claiming devices in the Cisco Intersight platform..... 21
 - Creating and installing Cisco HyperFlex Edge clusters..... 24
 - Post-installation configuration 35
 - Cisco HyperFlex licensing 37
- Conclusion** 38
- For more information**..... 38
- Appendix**..... 39
 - Appendix A: Sample Cisco Nexus 3048TP Gigabit Ethernet switch configuration 39
 - Appendix B: Sample script for VMware ESXi post-installation configuration 42

Executive Summary

Cisco HyperFlex™ systems provide an all-purpose virtualized server platform, with hypervisor hosts, networking connectivity, and virtual server storage across a set of Cisco HyperFlex HX-Series x86 rack-mount servers. It combines the convergence of computing and networking provided by the Cisco Unified Computing System™ (Cisco UCS®) with next-generation hyperconverged storage software to uniquely provide the computing resources, network connectivity, storage, and hypervisor platform needed to run an entire virtual environment, all contained in a single uniform system.

Cisco HyperFlex systems deliver many enterprise-class features, such as:

- A fully distributed log-structured file system
- High performance and low latency from the flash-friendly architecture
- In-line data optimization with deduplication and compression
- The flexibility to scale out computing and storage resources separately
- Data-at-rest encryption using hardware-based self-encrypting disks (SEDs)
- Non-Volatile Memory Express (NVMe)-based solid-state disk (SSD) support
- Native replication of virtual machine snapshots

An important feature introduced with Cisco HyperFlex HX Data Platform Release 2.6 is support for the initial release of Cisco Intersight™ cloud-based remote monitoring and management.

Cisco HyperFlex Edge is a new version of the Cisco HyperFlex system that is optimized for remote sites, branch offices, and edge environments. A smaller form factor of the Cisco® hyperconverged solution, Cisco HyperFlex Edge offers the full power of a next-generation hyperconverged platform without the need to connect to Cisco UCS fabric interconnects. Cisco HyperFlex Edge supports a fixed configuration of three HX-Series converged nodes, but it also allows you to scale up capacity by adding capacity drives while the system is running.

The solution can be configured, deployed, managed, and monitored with existing separate tools for Cisco UCS, Cisco HyperFlex systems, and VMware solutions. You can manage a Cisco HyperFlex cluster through a VMware vSphere web client plug-in or through the HTML5-based native Cisco HyperFlex Connect management tool. But with the Cisco Intersight platform, you can deploy and manage your solution from the cloud, bringing the low cost, deployment ease, and remote-management features of Cisco HyperFlex systems to your edge environments without the need for experienced IT staff at the deployment site.

Solution Overview

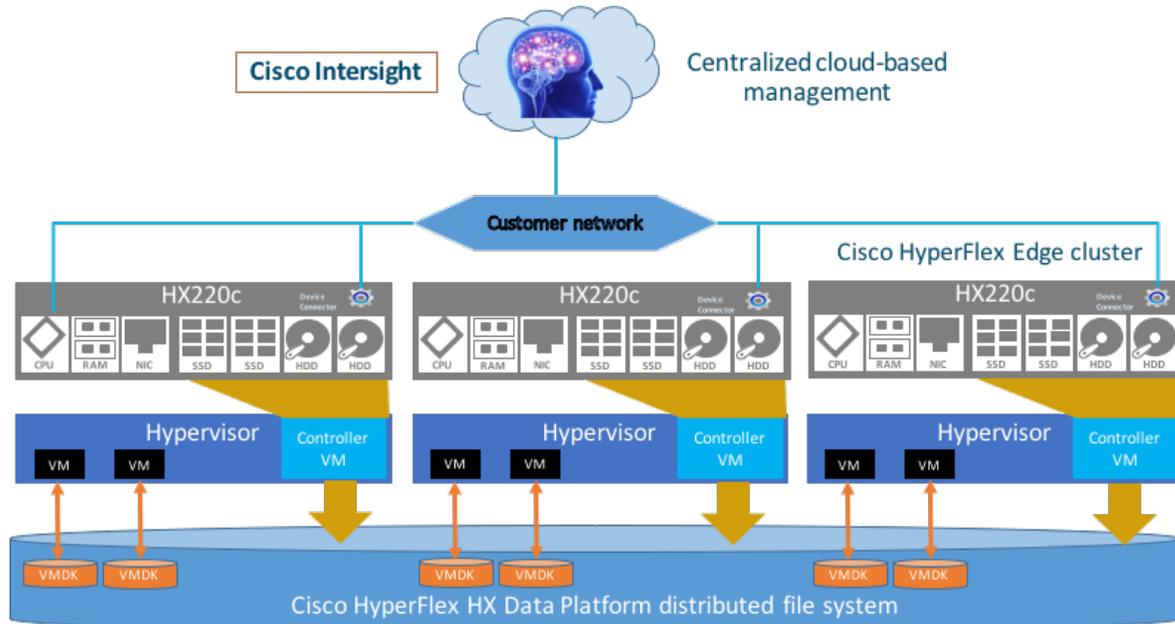
Introduction

Hyperconverged infrastructure simplifies deployment, centralizes management, and increases agility, thereby reducing the operating costs for daily IT operations. Nevertheless, with the rapidly growing quantity of data in enterprise data centers and the demanding high-availability requirements of the infrastructure, managing devices and smoothing IT operations in a large-scale environment is still complex and challenging.

Cloud-based management platforms provide unified access to applications and to infrastructure monitoring, configuration, and orchestration, therefore reducing the complexity of IT management and simplifying and unifying the deployment and management of many edge devices. The Cisco Intersight solution is Cisco's new system management platform for Cisco UCS servers and Cisco HyperFlex systems (Figure 1). It delivers intuitive computing through cloud-powered intelligence. This cloud-based platform offers centralized management that enables IT organizations to analyze, simplify, and automate their environments in ways that were not possible with traditional tools. This capability empowers organizations to achieve significant savings in total cost of ownership (TCO) and to deliver applications faster so they can support new business initiatives. To access the Cisco Intersight platform, go to <https://intersight.com/>.

At the time of this writing, cloud deployment is supported only for Cisco HyperFlex Edge. Deployment support for the entire Cisco HyperFlex product family will be provided in future Cisco Intersight releases.

Figure 1. Cisco HyperFlex Edge System and Cisco Intersight Overview



Cisco HyperFlex Edge system

A Cisco HyperFlex Edge cluster consists of three Cisco HyperFlex HX-Series converged nodes (with disk storage). Data is replicated across two nodes, and a third node is required for continuous operation in the event of a single-node failure. Each node is equipped with at least one high-performance SSD drive for data caching and rapid acknowledgment of write requests. Each node is also equipped with additional disks, up to the platform's physical limit, for long-term storage.

The following are the components of a Cisco HyperFlex Edge system:

- Cisco HyperFlex HX-Series rack-mount servers (choose three of the same model from the following list):
 - Cisco HyperFlex HX220c M5SX Node
 - Cisco HyperFlex HX220c M5SX All Flash Node
 - Cisco HyperFlex HX220c M4S Node
 - Cisco HyperFlex HX220c M4S All Flash Node
- Cisco HyperFlex HX Data Platform software
- VMware vSphere ESXi hypervisor
- VMware vCenter Server (supplied by the end user)

A Cisco HyperFlex Edge system has a fixed cluster size of three converged HX220c hybrid or all-flash nodes. Unlike with Cisco HyperFlex systems in the data center, Cisco HyperFlex Edge clusters do not support Cisco UCS computing-only nodes, and the cluster cannot be expanded with additional converged nodes. However, storage capacity can be added online at any time to open drive bays. The choice of hybrid or flash nodes is based on customer requirements for capacity, applications, performance, and budget. All-flash configurations offer repeatable and sustainable high performance, especially for scenarios with a large working set of data: that is, a large amount of data in motion. Hybrid configurations are a good option for customers who want the simplicity

of the Cisco HyperFlex solution, but who need a capacity-sensitive solution and who have smaller budgets and fewer performance-sensitive applications.

The HX220c hybrid and all-flash nodes used for building Cisco HyperFlex Edge systems are the same nodes used for building standard Cisco HyperFlex clusters. There are no separate product identifiers for Cisco HyperFlex Edge nodes. However, the choice of hardware components for the nodes, such as CPU, disks, and network adapters, differs. Customers have the flexibility to configure Cisco HyperFlex Edge nodes with a single CPU with Cisco product number HX-CPU-4114 and higher. Lower-numbered CPUs such as Cisco product number HX-CPU-3106, HX-CPU-4108, and HX-CPU-4110, are supported only in Cisco HyperFlex Edge systems configured with dual CPUs.

Table 1 summarizes the differences between Cisco HyperFlex Edge systems and standard Cisco HyperFlex all-flash and hybrid systems.

Table 1. Differences between Cisco HyperFlex systems and Cisco HyperFlex Edge systems

		Cisco HyperFlex all flash	Cisco HyperFlex hybrid	Cisco HyperFlex Edge
Converged nodes	HX220c M4S	No	Yes	Yes
	HX240c M4SX	No	Yes	No
	HX220c M4S	Yes	No	Yes
	HX240c M4SX	Yes	No	No
	HX220c M5SX	No	Yes	Yes
	HX240c M5SX	No	Yes	No
	HX220c M5SX	Yes	No	Yes
	HX240c M5SX	Yes	No	No
Computing nodes		Yes	Yes	No
Fabric interconnects		Yes	Yes	No
Server management		Cisco UCS Manager	Cisco UCS Manager	IMC
Service profile		Yes	Yes	No
Cluster size		3 to 16 converged nodes and 0 to 16 computing nodes	3 to 8 converged nodes and 0 to 8 computing nodes	3 converged nodes
Cluster expansion		Yes	Yes	No
Replication factor		2 or 3	2 or 3	2
Jumbo frame		Recommended	Recommended	Not recommended
Single CPU per node		No	No	Yes
Minimum number of capacity disks per node		6	6	3
NVMe SSD		Yes	Yes	No
Data encryption (SED)		Yes	Yes	No
Native replication		Yes	Yes	No
Cloud deployment		Future	Future	Now

Table 2 lists usable capacities for Cisco HyperFlex Edge clusters, using binary prefix values, for a variety of cluster configurations. The binary prefix values are used for all calculations in which raw or usable capacities are shown from the perspective of the Cisco HyperFlex software, file system, or operating system. These are different from the decimal prefix values used by manufacturers for raw disk capacity. This approach is used to provide a consistent set of values as seen by the end user from within the Cisco HyperFlex web plug-in for VMware vCenter and the Cisco HyperFlex Connect GUI when viewing cluster capacity, allocation, and

consumption. These are also the values seen from within most operating systems. These values are useful for determining the appropriate size of the initial Cisco HyperFlex cluster purchase and the amount of capacity that can be gained by adding capacity disks.

Table 2. Cisco HyperFlex Edge cluster usable capacity

HX-Series server model	Node quantity	Capacity disk size (each)	Capacity disk quantity (per node)	Cluster usable capacity at RF = 2
HX220c M5SX All Flash	3	3.8 TB	3	14.5 TiB
			8	38.6 TiB
		960 GB	3	3.6 TiB
			8	9.6 TiB
HX220c M4S All Flash	3	3.8 TB	3	14.5 TiB
			6	28.9 TiB
		960 GB	3	3.6 TiB
			6	7.2 TiB
HX220c M5SX	3	1.2 TB	3	4.5 TiB
			8	12.1 TiB
HX220c M4S	3	1.2 TB	3	4.5 TiB
			6	9.0 TiB

The requirements for software revisions and firmware versions for a Cisco HyperFlex Edge installation are the same as those for standard Cisco HyperFlex systems. For the minimum firmware versions for the supported components, see the [Cisco HyperFlex Installation Guide for Cisco Intersight](#).

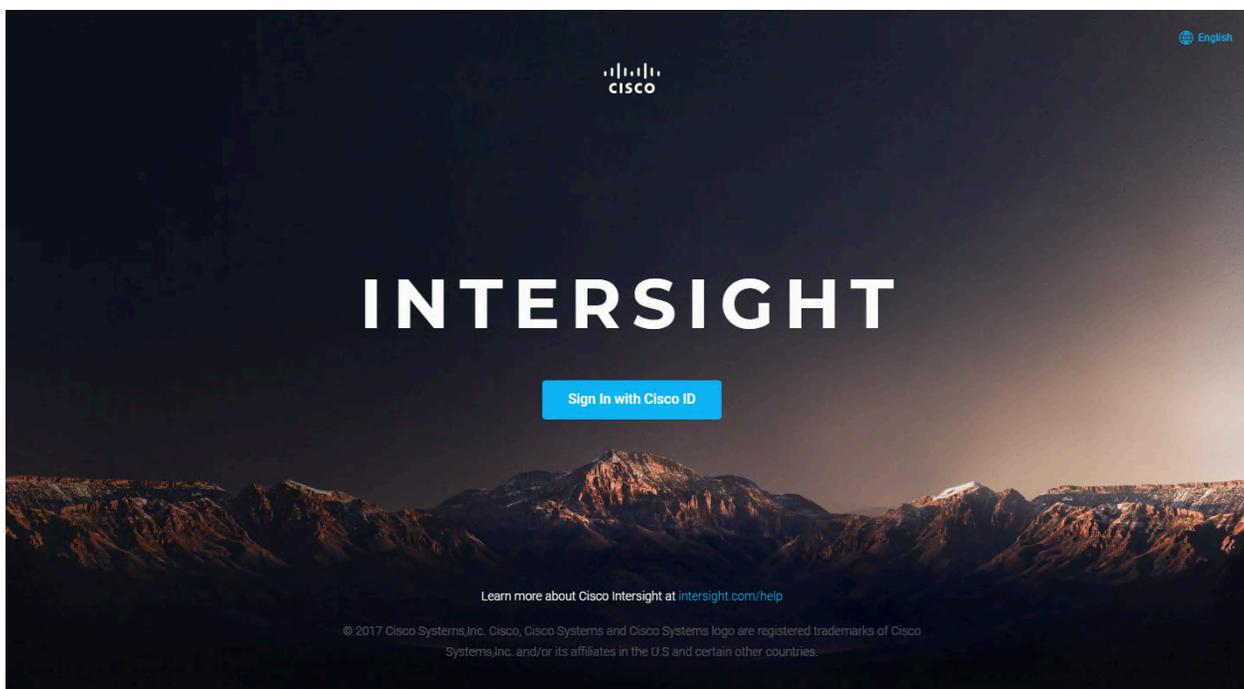
Cisco Intersight cloud-based management platform

The Cisco Intersight solution (<https://intersight.com>) is an API-driven, cloud-based system management platform (Figure 2). It is designed to help organizations implement their IT management and operations with greater automation, simplicity, and operational efficiency. It is a new-generation global management tool for Cisco UCS and Cisco HyperFlex systems and provides a holistic and unified approach to managing distributed and virtualized environments. The Cisco Intersight platform simplifies the installation, monitoring, troubleshooting, upgrading, and support processes for your infrastructure. It offers the following benefits:

- **Cloud-based management:** The capability to manage Cisco UCS and Cisco HyperFlex systems from the cloud lets you quickly and easily manage and scale your infrastructure whether it is in the data center or a remote or branch-office location.
- **Automation:** The unified API in Cisco UCS and Cisco HyperFlex systems enables policy-based configuration and management of the infrastructure. It also makes the Cisco Intersight platform and the devices connected to it fully programmable and DevOps friendly.
- **Analytics and telemetry:** The Cisco Intersight platform monitors the health and relationships of all physical and virtual infrastructure components. It also collects telemetry and configuration information to develop the intelligence of the platform in accordance with Cisco information security requirements.
- **Advanced level of support:** Solid integration with the Cisco Technical Assistance Center (TAC) enables more efficient and proactive technical support. The Cisco Intersight platform provides enhanced operations automation by expediting file transmission to accelerate troubleshooting.

- **Recommendation engine:** Driven by analytics and machine learning, the Cisco Intersight recommendation engine provides actionable intelligence for IT operations management through a daily-increasing knowledge base and practical insights learned from the entire system.
- **Management as a service (MaaS):** The Cisco Intersight platform provides management as a service and is designed to be infinitely scalable and easy to implement. It relieves users of the burden of maintaining systems management software and hardware.

Figure 2. Cisco Intersight platform



Since the initial release of the Cisco Intersight platform, monitoring and reporting has been enabled for all Cisco HyperFlex clusters, but now cloud-based deployment is enabled for Cisco HyperFlex Edge systems using Cisco HyperFlex HX220c M5 rack servers. The Cisco Intersight website and framework can be upgraded with new and enhanced feature sets independently of the products that are managed, thus providing many new features and capabilities with no downtime or upgrades required by end users. Future releases of Cisco HyperFlex systems will enable additional functions along with upgrades to the Cisco Intersight framework. This unique combination of embedded and online technologies will provide a complete cloud-based management solution that can manage Cisco HyperFlex systems throughout the entire lifecycle: from deployment through retirement.

The minimum supported web browser versions to run the Cisco Intersight platform are:

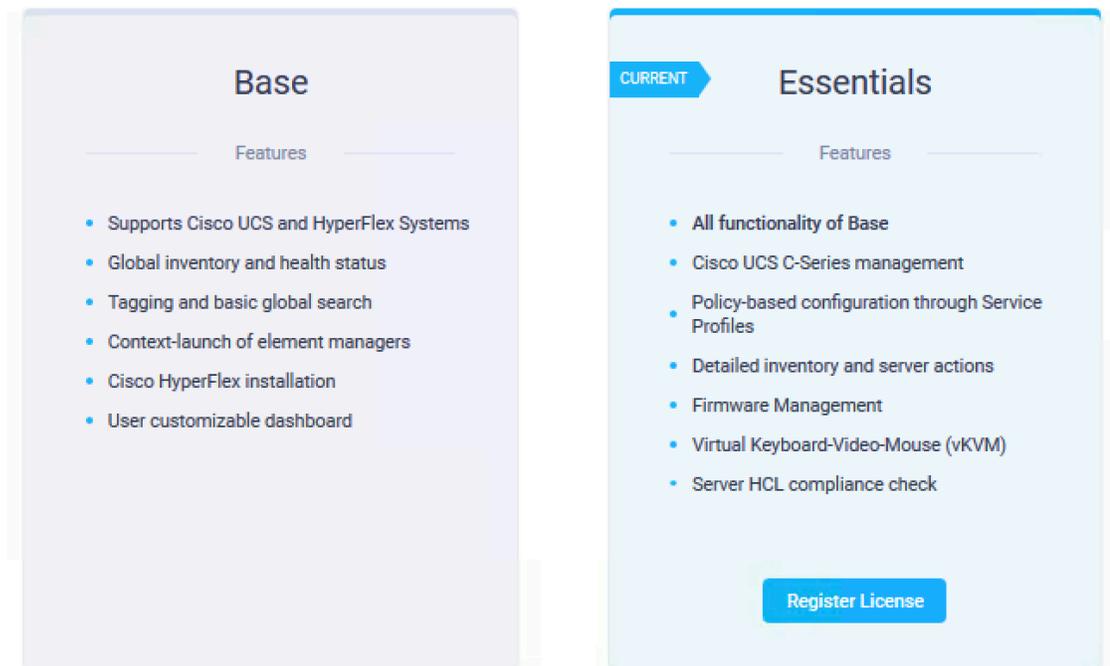
- Google Chrome: Release 62.0.3202.94
- Firefox: Release 57.0.1
- Microsoft Edge: Release 40.15063.674.0
- Safari: Release 10.1.1

The minimum supported firmware versions for Cisco HyperFlex Edge systems to be deployed by the Cisco Intersight platform are:

- Cisco IMC software: Release 3.1(2d)
- Cisco HyperFlex Data Platform: Release 2.6.1b
- Device connector: Release 1.0.4-10 or later

Two licensing editions are available for Cisco Intersight customers: Base edition and Essentials edition (Figure 3).

Figure 3. Cisco Intersight licensing options



The Base edition is available at no additional cost to customers. It is automatically included with every Cisco UCS and Cisco HyperFlex system purchase. Cisco Intersight Base edition provides access to a portal that delivers centralized monitoring and basic inventorying of managed systems, organizational capabilities including tagging and search, and the capability to launch native endpoint management interfaces including Cisco UCS Manager and Cisco HyperFlex Connect.

The Essentials edition provides additional value on top of what is provided in the Base edition. It includes features to centralize configuration management through a unified policy engine, determine compliance with the Cisco UCS Hardware Compatibility List (HCL), and initiate firmware updates. The Essentials edition provides a single interface for monitoring, management, and operations, with the capability to launch the virtual keyboard, video, and mouse (vKVM) console directly from the Cisco Intersight platform. Cisco Intersight Essentials edition can be ordered for 1-year, 3-year, and 5-year subscription periods. You can start a free 90-day evaluation trial of the Essentials edition by signing up from the licensing page in the Cisco Intersight platform.

Cisco HyperFlex cloud deployment, Cisco HyperFlex dashboards, day-2 monitoring, centralized alarms, Cisco HyperFlex cluster list view, vKVM launch (Cisco HX-Series servers only), and cross-launch to Cisco HyperFlex Connect are all included in the Base edition. The HCL feature in the Essentials edition can be purchased and used to audit compliance for hardware, OS, driver, and component firmware versions for Cisco HyperFlex systems attached through fabric interconnects. Support for HCL in Cisco HyperFlex Edge will be available in a future release. The firmware update capability using the Essentials edition is supported only for Cisco UCS C-Series Rack Servers and is not designed to work with Cisco HyperFlex Edge in the current Cisco Intersight release.

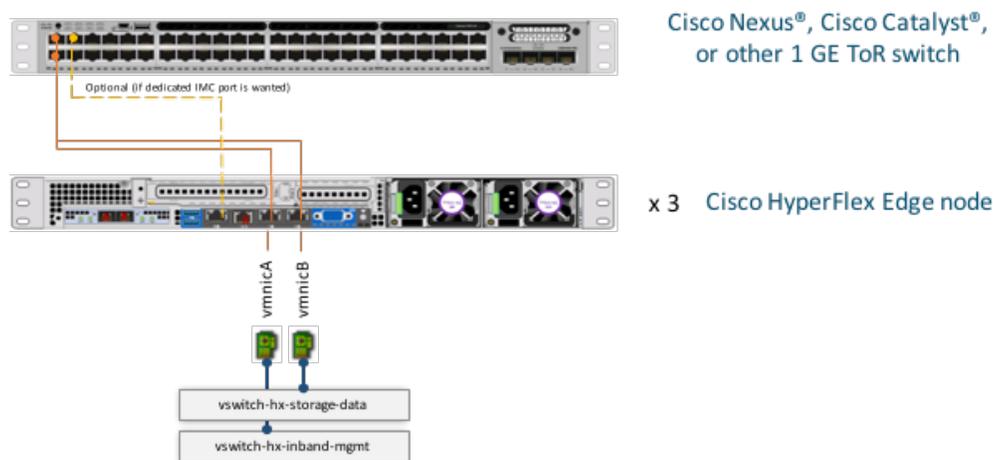
Physical topology

The topology of the Cisco HyperFlex Edge system is simple. The system is composed of three Cisco HyperFlex HX220c M4 or M5 rack-mount servers per cluster. The HX-Series converged servers are connected directly to the customer's network through onboard LAN-on-motherboard (LOM) ports or the optional Intel i350-T4 quad-port PCIe network interface card (NIC). The Cisco IMC VLAN and the Cisco HyperFlex management VLAN need outbound Internet access to reach the Cisco Intersight platform. HTTPS proxy is not currently supported for use with the Cisco HyperFlex cloud deployment feature.

Two physical topologies between the HX-Series servers and upstream network are supported: single-switch and dual-switch configurations. The choice depends on the requirements of the particular installation and the availability of hardware and networking resources.

The single-switch configuration (Figure 4) uses a simple topology that requires only a single switch and a minimum of two 1 Gigabit Ethernet ports per server. Link and switch redundancy are not provided in this basic topology. Access ports and trunk ports are the two supported network port configurations.

Figure 4. Cisco HyperFlex Edge single-switch configuration



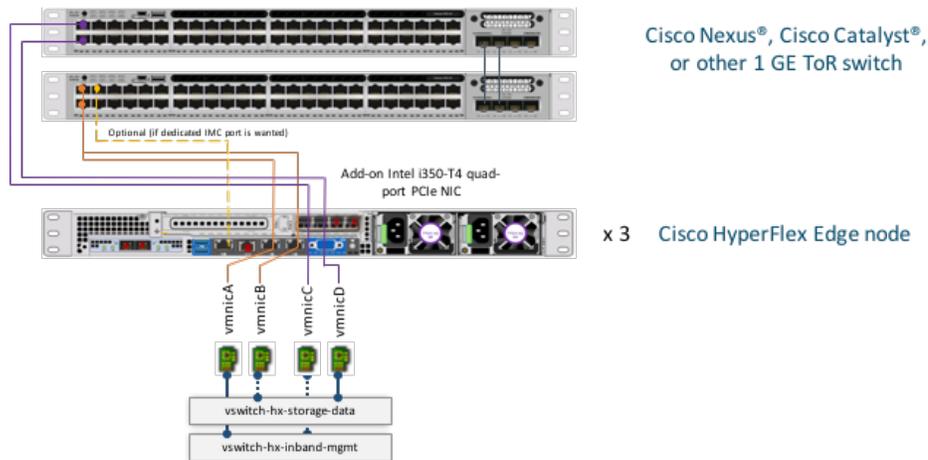
The single-switch topology requires at least two separate networks: a management network (which includes guest virtual machine network and VMware vMotion traffic) and a data network (for storage traffic). Two 1 Gigabit Ethernet ports on each server are required, with one of these two ports dedicated to Cisco HyperFlex storage traffic.

The upstream network has the following requirements:

- A managed switch with VLAN capability is required.
- A minimum of 6 physical 1 Gigabit Ethernet ports for three Cisco HyperFlex nodes is required, assuming that in-band Cisco IMC is configured on the 1 Gigabit Ethernet LOM ports in shared mode. Users can optionally configure out-of-band IMC using a dedicated port on the LOM card, which requires an additional 1 Gigabit Ethernet switch port per server.
- Jumbo frames are not required.
- PortFast or a PortFast trunk should be configured for uninterrupted IMC access.

The dual-switch configuration (Figure 5) provides a slightly more complex topology, with full redundancy that protects against switch failures, link and port failures, and LOM and PCIe NIC hardware failures. It requires two switches, which can be standalone or stacked switches, four 1 Gigabit Ethernet ports, and one additional Intel i350 PCIe NIC per server. Trunk ports are the only supported network port configuration.

Figure 5. Cisco HyperFlex Edge dual-switch configuration



The dual-switch topology also requires two separate networks: a management network (which includes the guest virtual machine network) and a data network (for storage and VMware vMotion traffic). Four 1 Gigabit Ethernet ports on each server are required: two ports from the onboard LOM card and two ports from a PCIe add-on NIC. One LOM and one PCIe port serve management and virtual machine guest traffic in a redundant configuration, and the second LOM and second PCIe port serve storage data and vMotion traffic in a redundant and load-balanced configuration.

The upstream network has the following requirements:

- Two managed switches with VLAN capability are required.
- A minimum of 12 physical 1 Gigabit Ethernet ports for three Cisco HyperFlex nodes is required, assuming that in-band Cisco IMC is configured on the 1 Gigabit Ethernet LOM ports in shared mode. Users can optionally configure out-of-band IMC using a dedicated port on the LOM card, which requires an additional 1 Gigabit Ethernet switch port per server.
- Jumbo frames are not required.
- A PortFast trunk should be configured for uninterrupted IMC access.

Note: The sample configuration presented in this document is based on the single-switch topology.

Logical topology

The Cisco HyperFlex system has communication pathways that are categorized into four zones: the management zone, data storage zone, vMotion zone, and guest virtual machine zone. This approach provides separate networks for different types of traffic with special purposes instead of multiplexing all traffic on a single network. As a result, the Cisco HyperFlex installer creates four virtual switches (vSwitches) on all HX-Series nodes, each serving a different network:

- vswitch-hx-inband-mgmt
- vswitch-hx-storage-data
- vswitch-hx-vm-network
- vmotion

For a Cisco HyperFlex Edge system, only the first two vSwitches are used: vswitch-hx-inband-mgmt and vswitch-hx-storage-data. For the single-switch configuration, one LOM port is assigned to vswitch-hx-inband-mgmt, and another LOM port is assigned to vswitch-hx-storage-data. The data storage network requires a dedicated port in this configuration. Therefore, vswitch-hx-storage-data carries the storage data traffic; and vswitch-hx-inband-mgmt carries the traffic for management, vMotion, and guest virtual machines. There is no uplink redundancy on vSwitches in this configuration.

For the dual-switch configuration, the redundancy occurs at the vSwitch level: one LOM port and one PCIe NIC port are assigned to vswitch-hx-inband-mgmt, and the second LOM port and the second PCIe NIC port are assigned to vswitch-hx-storage-data. One difference from the single-switch configuration is the placement of the vMotion network. To make better use of port resources, the vMotion VMkernel port is on the vswitch-hx-storage-data network and uses a failover order opposite to that of the storage data network. With this approach the uplinks for storage traffic and the uplinks for vMotion traffic are set as active-standby, but each service will use the opposite active link. The vswitch-hx-inband-mgmt network is set to active-standby with the same failover order for all port groups. By default, all network services will use the active path and failover to the standby path only as needed during a failure scenario.

Because only two vSwitches are used and assigned with physical vmnics, you can manually delete vswitch-hx-vm-network and vMotion vSwitches. Alternatively, run the post_install script, and it will automatically remove vswitch-hx-vm-network and vMotion vSwitches from all clustered Cisco HyperFlex Edge nodes. The post_install script will also set the appropriate failure order automatically for the vMotion VMkernel port in the dual-switch configuration.

Without fabric interconnects in the topology, how does the Cisco Intersight platform communicate with the Cisco HyperFlex servers? It communicates with the servers through a device connector that is embedded in firmware and can be enabled from the Cisco IMC software. The IMC is a baseboard management controller that provides embedded server management for Cisco UCS C-Series Rack Servers and Cisco HyperFlex HX-Series rack servers. It gives users full control of the server, allowing complete configuration and management. It can be configured to operate in dedicated mode or shared mode. The dedicated mode uses the dedicated management port on the onboard LOM card. In shared mode, any LOM port or virtual interface card (VIC) adapter port can be used to access the IMC. The shared mode includes the shared LOM, shared LOM 10 Gigabit Ethernet, Cisco VIC, and shared LOM extended modes.

If the upstream switch or out-of-band management switch has plenty of network ports available, a dedicated IMC management port is recommended. However, this configuration consumes more switch ports and requires additional cabling, power, and configuration. Depending on the availability of the networking resources in the user environment, shared LOM or shared LOM extended mode can simplify the configuration and also reduce the number of switch ports and amount of cabling required. In shared LOM mode, all host ports must be able to pass the same management subnet by allowing the appropriate VLAN.

Depending on the logical design of the Cisco HyperFlex networking and the IMC communication required for server management, multiple VLAN configurations are recommended for the Cisco HyperFlex Edge system, as summarized in Table 3.

Table 3. VLAN configurations for Cisco HyperFlex Edge

VLAN function	VLAN ID	Purpose	Notes
Cisco IMC traffic	Customer supplied	IMC interfaces for Cisco UCS standalone servers	This VLAN must be routable and must have access to the Cisco HyperFlex Intersight platform.
VMware ESXi and Cisco HyperFlex management traffic	Customer supplied	ESXi host management interfaces Cisco HyperFlex storage controller virtual machine management interfaces Cisco HyperFlex storage cluster roaming management interface	This VLAN must be routable and must have access to the Cisco HyperFlex Intersight platform. It can be same or different from the IMC VLAN.
Cisco HyperFlex storage traffic	Customer supplied	ESXi host storage VMkernel interfaces Cisco HyperFlex storage controller storage network interfaces Cisco HyperFlex storage cluster roaming storage interface	This VLAN is used for storage traffic. Only Layer 2 connectivity is required. It cannot be combined with the management VLAN and must be dedicated to storage traffic.
VMware vMotion traffic	Customer supplied	ESXi host vMotion VMkernel interfaces	This VLAN can be the same as the management VLAN, but the recommended approach is to segregate this traffic in a unique VLAN.
Guest virtual machine traffic	Customer supplied	Networks for guest virtual machines	Multiple VLAN port groups can be created for different applications.

Figure 6 shows a logical view of the network configuration for the single-switch topology.

Figure 6. Cisco HyperFlex Edge virtual network: Single switch

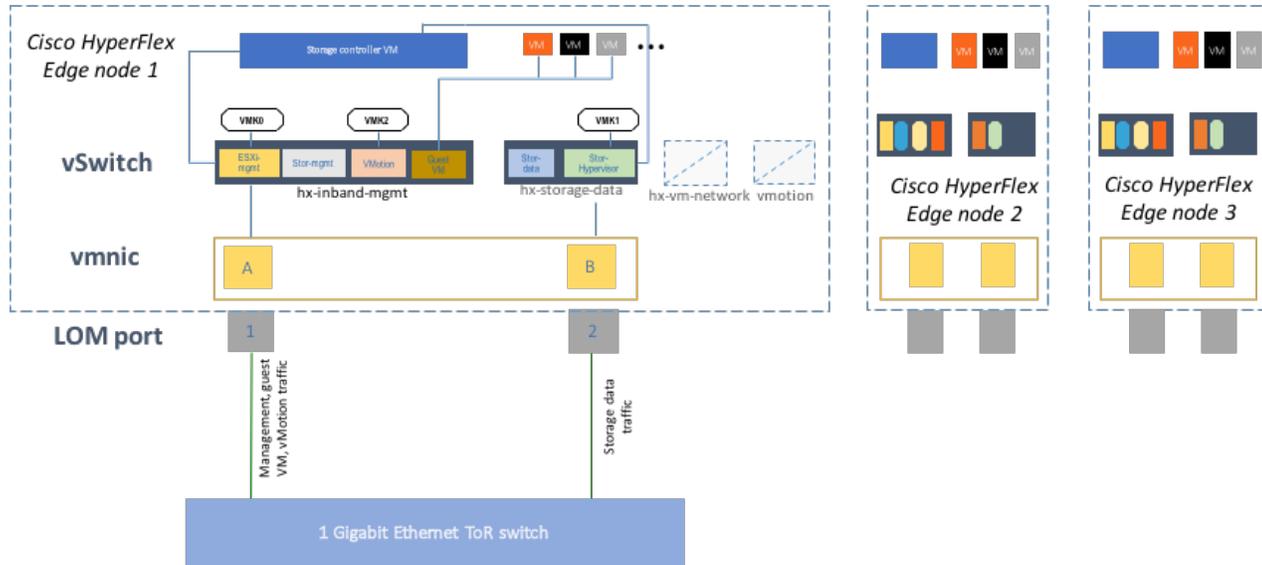
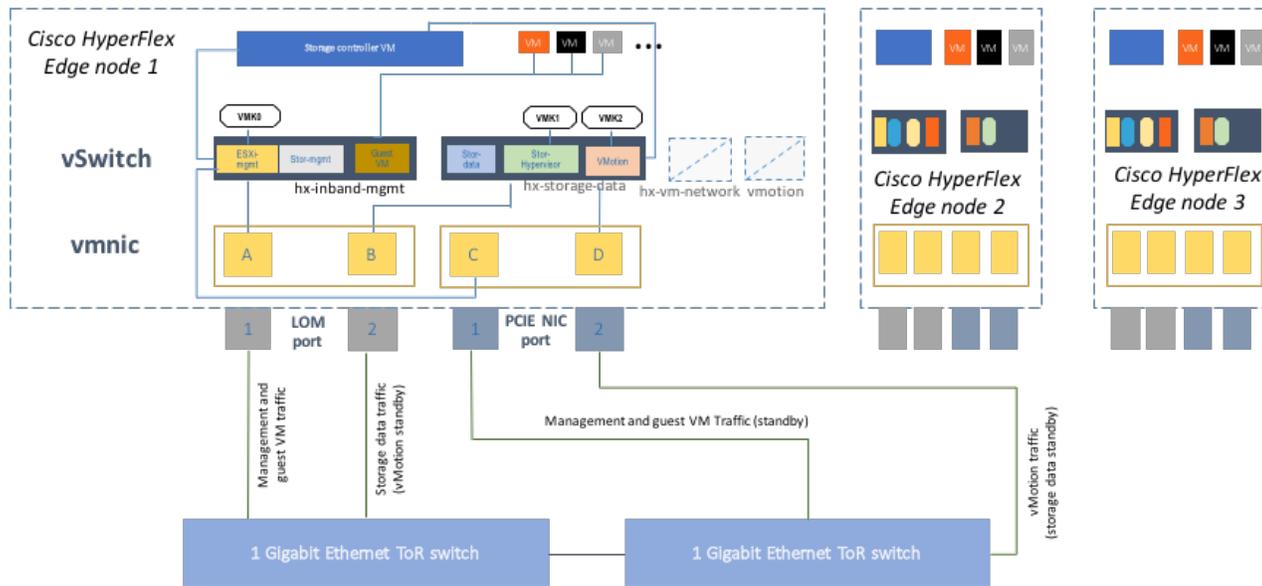


Figure 7 shows a logical view of the network configuration for the dual-switch topology.

Figure 7. Cisco HyperFlex Edge virtual network: Dual switch



Note: The sample configuration presented in this document assumes the use of in-band IMC in shared LOM mode.

Installing Cisco HyperFlex Edge with the Cisco Intersight platform

Cisco HyperFlex systems are ordered with a factory preinstalled configuration. With this factory integration, the Cisco HyperFlex servers are delivered with the proper firmware revisions preset, a copy of the VMware ESXi hypervisor software preinstalled, and some components of the Cisco HyperFlex software already prestaged. When the system arrives onsite, the customer thus needs to perform fewer final steps and the installation process is simplified as a result of the work already completed at the factory. The Cisco HyperFlex system is normally installed using a deployable Cisco HyperFlex installer virtual machine from an OVA file. Another option for installing a Cisco HyperFlex system is to use the Cisco Intersight cloud management platform. With this option, the installer function is delivered from the cloud, with no need for the user to have an installer virtual machine.

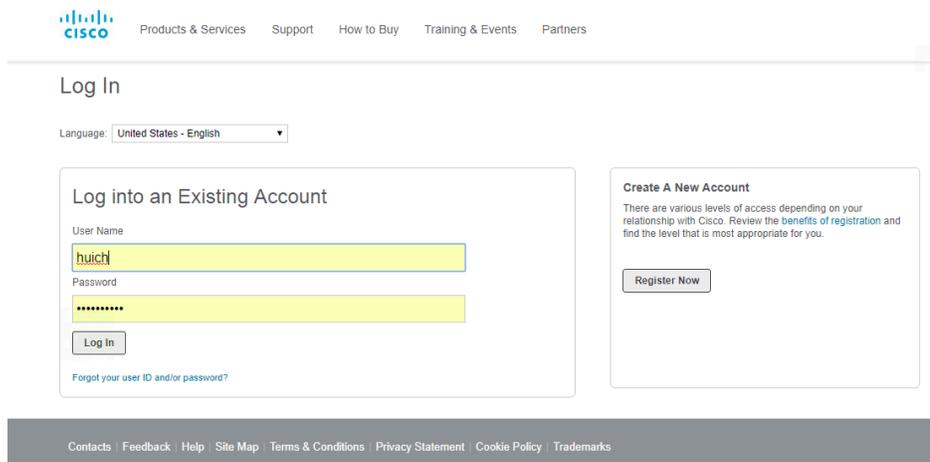
A Cisco HyperFlex Edge installation with the Cisco Intersight platform is supported only for completely new factory-shipped Cisco HyperFlex M5 rack-mount servers. Therefore, the setup process described in this document assumes that the factory preinstallation work has been completed, using the tools and processes developed by Cisco to simplify the process and dramatically reduce the deployment time. This document follows the same out-of-the-box experience that customers encounter with a new cluster purchase.

Prerequisites

Prior to beginning the installation activities, you must set up a Cisco Intersight account. You also should gather all the configuration settings contained in the preinstallation [checklist](#).

A Cisco Intersight account is required for this solution. To create your account you must first have a valid Cisco ID. If you do not yet have a Cisco ID, the account can be generated in this way:

1. Visit <https://intersight.com> from your workstation.
2. Click Sign In with Cisco ID.
3. On the Cisco Log In page, you can either choose to log into an existing account or click Register Now to create a new account.



4. Click Register Now and provide the requested information to create a Cisco.com account.
5. After a valid account has been created, use it to log in to the Cisco Intersight platform.

To install the Cisco HyperFlex HX Data Platform from Cisco Intersight platform, you need to allocate some IP addresses. The Cisco UCS IMC IP addresses and HX Data Platform management IP addresses must allow communication with the Cisco Intersight platform. Additional IP addresses for the Cisco HyperFlex Edge system need to be allocated from the appropriate subnets and VLANs to be used. IP addresses that are used by the system include addresses for Cisco UCS IMC, Cisco HyperFlex and VMware ESXi management, Cisco HyperFlex storage, and VMware vMotion. The IMC IP addresses and Cisco HyperFlex and ESXi management IP addresses can either come from the same subnet or be separate, as long as the Cisco HyperFlex management subnet permits outbound access to the Cisco Intersight platform.

By default, the Cisco HyperFlex installation will assign a static IP address to the management interface of the ESXi servers. The use of Dynamic Host Configuration Protocol (DHCP) for automatic IP address assignment is not recommended for Cisco HyperFlex and ESXi management, Cisco HyperFlex storage, or vMotion networks. For the IMC network, either DHCP or static assignment can be used to ease the configuration process.

DNS servers should be configured to query fully qualified domain names (FQDNs) in the Cisco HyperFlex and ESXi management group. DNS forward and reverse lookup records need to be created prior to beginning the installation. In addition, all device connectors on the Cisco HyperFlex nodes and all Cisco HyperFlex controller virtual machines must properly resolve public domains through DNS and permit outbound-initiated HTTPS connections on port 443 so that the latest Cisco HyperFlex software packages can be automatically downloaded and the Cisco HyperFlex Edge cluster can be fully deployed from the Cisco Intersight platform.

Consistent time clock synchronization is required across the components of the Cisco HyperFlex system, provided by reliable Network Time Protocol (NTP) servers, accessible to the IMC management network group and the Cisco HyperFlex and ESXi management group. NTP is used by the IMC, vCenter, ESXi hypervisor hosts, and Cisco HyperFlex storage platform controller virtual machines. The use of public NTP servers is highly discouraged; instead, you should use a reliable internal NTP server.

Prior to performing the installation, you need to document and create the required VLAN IDs in the upstream network as necessary. At a minimum, you need to trunk two VLANs to the upstream network: a VLAN for the Cisco HyperFlex and ESXi management group and a VLAN for the Cisco HyperFlex storage group. Following Cisco best practices, you can add two more VLANs: a VLAN for the vMotion group and at least one VLAN for the guest virtual machine traffic. The VLAN for vMotion can be the same as the management VLAN, but this setup is not recommended. During the installation process, only the VLAN ID for the management network and the VLAN ID for the storage network are required inputs.

Several user names and passwords need to be defined or known as part of the Cisco HyperFlex installation process: Cisco Intersight account, Cisco UCS IMC administrator, VMware ESXi administrator, Cisco HyperFlex administrator, and VMware vCenter administrator.

The physical layout of the Cisco HyperFlex system was previously described in the “Physical Topology” section. The HX-Series rack servers need to be cabled properly to the customer’s upstream networking switches before the start of installation activities. Depending on the availability of the upstream switches or switch ports, you can choose a single-switch or dual-switch topology and with the IMC NIC policy (shared LOM or dedicated ports). After these decisions have been made, the nodes can be cabled appropriately.

The cabling for a single-switch topology is simple:

- Cable both LOM ports on each HX-Series server to the same top-of-rack (ToR) switch.
- If you choose to access the IMC through the dedicated management port, cable that management port on each server to the same switch or to an out-of-band management switch.

Cable a dual-switch topology as follows:

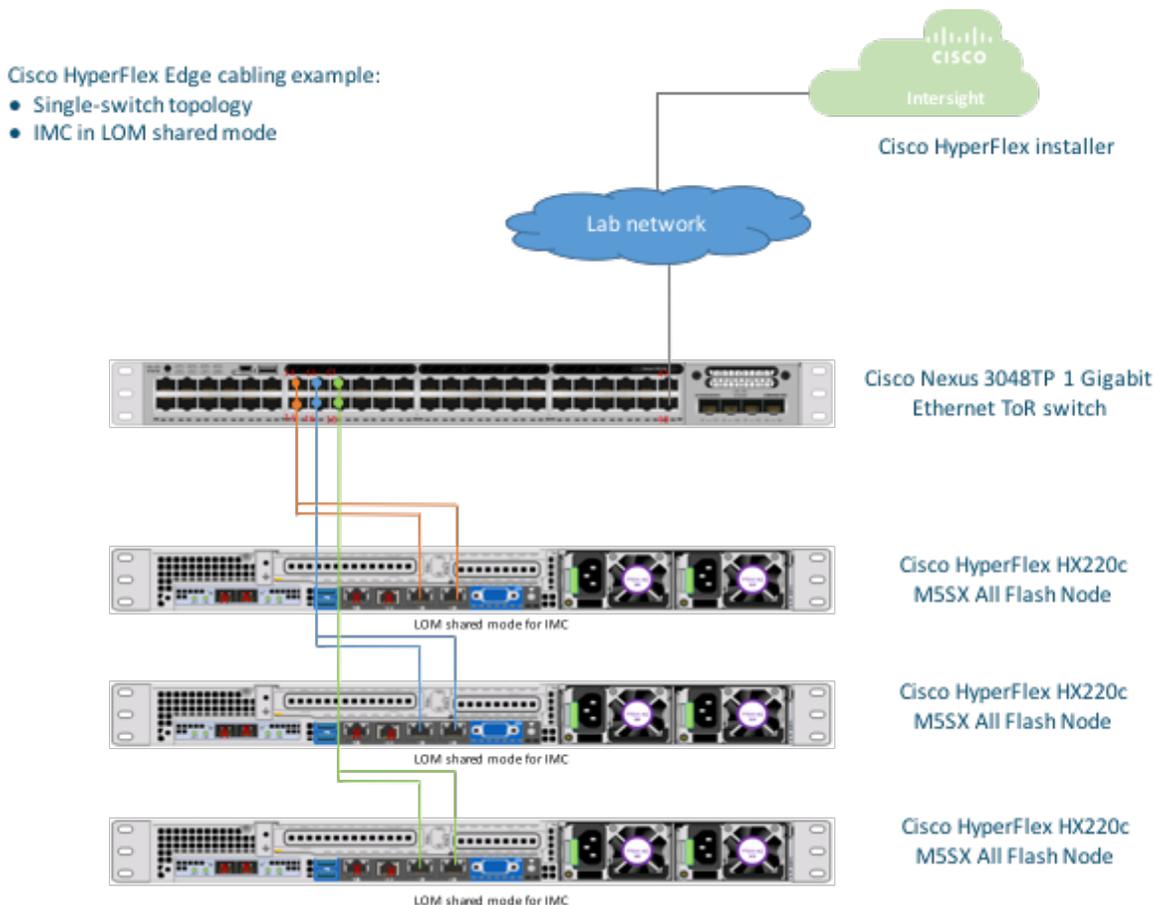
- Cable both LOM ports on each HX-Series server to the same ToR switch.
- Cable any two of the four ports on the Intel PCIe NIC on each server to the second ToR switch. Do not connect more than two PCIe NIC ports prior to the installation. After the Cisco HyperFlex cluster has been created, you can freely use the remaining ports.
- If you choose to access the IMC through the dedicated management port, cable that management port on each server to the same switch to which the LOM ports connect or to an out-of-band management switch.

Do not use the 10 Gigabit Ethernet ports on the Cisco VIC to connect to the upstream switch in either the single-switch or dual-switch topology.

Sample topology and pre-installation checklist

Figure 8 shows the sample topology validated for this document. It demonstrates the cabling of a Cisco HyperFlex Edge system in a single-switch topology.

Figure 8. Cisco HyperFlex Edge cabling example



The sample configuration for the Cisco Nexus 3048TP 1 Gigabit Ethernet ToR switch is provided in Appendix A.

Table 4 is an example of a completed pre-installation checklist for a Cisco HyperFlex Edge system.

Table 4. Pre-installation checklist

VMware vCenter	Cisco HyperFlex cluster name:	HX3Edge		Data center name:	HUIDC	
	VMware vCenter server FQDN or IP address:	hx3-vcenter.hx.lab.cisco.com		Single-sign-on server:	(Optional)	
	VMware vCenter administrator:	huich@hx	ZAQ!2wsx			
Network services	DNS server 1:	10.29.133.61		DNS server 2:	171.70.168.183	
	NTP server 1:	10.81.254.202		NTP server 2:	72.163.32.44	
	Time zone:	America/Los_Angeles PST -8				
User name and password	Cisco Intersight account	huich	xxxxxx	VMware ESXi host administrator:	root	Cisco123
	Cisco UCS IMC administrator:	admin	Cisco123	Cisco HyperFlex controller administrator:	root	Cisco12345
Address group	Cisco UCS IMC interfaces	Cisco HyperFlex and VMware ESXi management		Cisco HyperFlex storage		VMware vMotion
VLAN ID	41	41		42		43
Subnet	10.29.145.0	10.29.145.0		169.254.1.0		169.254.2.0
Subnet mask	255.255.255.0	255.255.255.0		255.255.255.0		255.255.255.0
Gateway	10.29.145.1	10.29.145.1				
Devices	Cisco UCS management addresses	VMware ESXi management interface	Storage controller management interface	VMware ESXi hypervisor storage VMkernel interface	Storage controller storage interface	VMotion VMkernel interface
Cisco HyperFlex cluster			10.29.145.162		169.254.1.20	
Cisco HyperFlex node 1	10.29.145.154	10.29.145.157	10.29.145.163	169.254.1.11	169.254.1.21	169.254.2.11
Cisco HyperFlex node 2	10.29.145.155	10.29.145.158	10.29.145.164	169.254.1.12	169.254.1.22	169.254.2.12
Cisco HyperFlex node 3	10.29.145.156	10.29.145.159	10.29.145.165	169.254.1.13	169.254.1.23	169.254.2.13

Note: Table cells shaded in yellow have auto-assigned IP addresses and don't require user configuration.

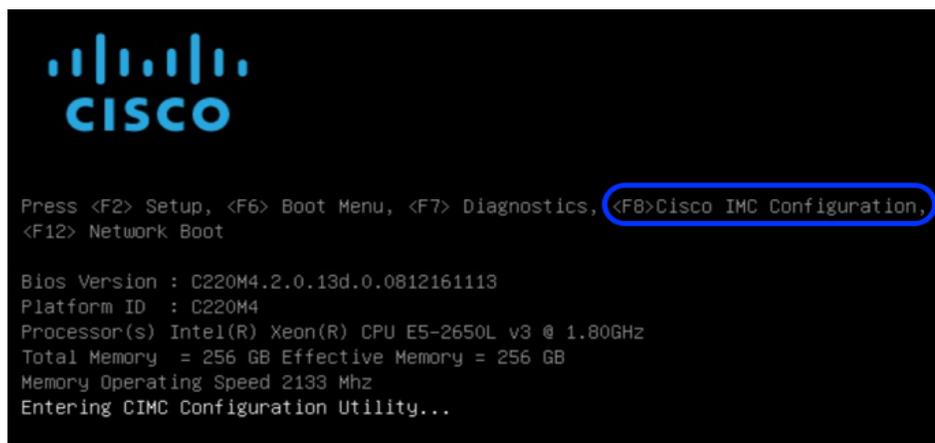
Cisco Integrated Management Controller configuration

The Cisco Intersight cloud-based management platform provides remote management of Cisco HyperFlex Edge servers through a device connector that is embedded in and can be enabled through Cisco IMC software. The Cisco UCS device connector provides access to Cisco UCS server management functions built in to the server. By pointing the device connector to the Cisco Intersight platform, Cisco UCS servers and Cisco HyperFlex clusters can be claimed as serviceable devices and easily remotely managed. The Cisco Intersight platform needs access to the IMC and to the Cisco HyperFlex management network.

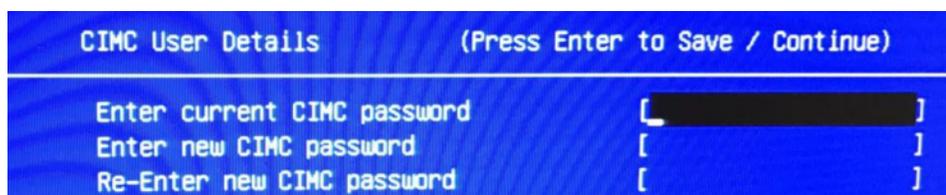
To enable the device connector on the Cisco HyperFlex nodes and the Cisco Intersight platform to communicate, the IMC interface needs to be configured on each server. Two options are available for setting the IP address for the IMC: DHCP or static configuration. If you already have a DHCP server set up in your environment, DHCP assignment will be the simplest approach. Otherwise, you can assign a static IP address to the IMC.

The following steps guide you through a static configuration:

1. Attach the VGA dongle to the new Cisco HyperFlex server and connect to a monitor and USB keyboard.
2. Power on the server.
3. Wait for some minutes until the screen with the Cisco logo is displayed.
4. When prompted for boot options, press the F8 key to enter the Cisco IMC configuration utility.



5. For a first-time configuration, you will be prompted for a new IMC password. Enter the default password **password** as the current IMC **password** and then set a new IMC password. The configuration described here uses **Cisco123** as the new password.



6. In the Cisco IMC configuration utility window, choose the desired NIC mode. Select Dedicated if you want to access the IMC through the dedicated management port. Select Shared LOM if you want to access the IMC through any LOM port. Select Shared LOM Ext mode if you want to access the IMC through any LOM or adapter port.
7. Deselect the “DHCP enabled” option and select IPV4 to set a static IP address.
8. Enter IPv4 settings for the CIMC IP, Prefix/Subnet, and Gateway options.
9. Leave NIC redundancy set to Active-active.
10. Select the “VLAN enabled” option and enter the VLAN ID for IMC management.

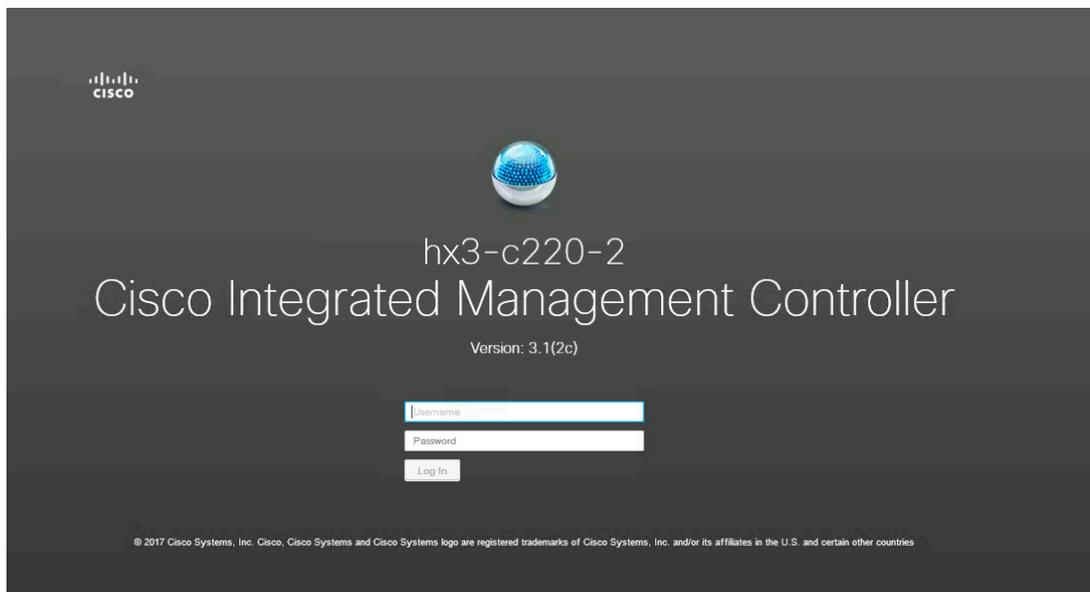
- Press F10 to save the configuration and then press Esc to exit the utility. The server will reload and may boot into the ESXi operating system preloaded at the factory. Do not worry if the server does not fully boot into an OS at this point. The installation workflow will modify the boot order automatically at the correct stage of deployment, so do not make manual configuration changes in the IMC utility outside the steps listed here.

```

Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
NIC Properties
NIC mode                               NIC redundancy
Dedicated:                             [ ]           None:                             [ ]
Shared LOM:                             [X] ①         Active-standby:                    [ ]
Cisco Card:                             [ ]           Active-active:                      [X] ④
  Riser1:                               [ ]           VLAN (Advanced)
  Riser2:                               [ ]           VLAN enabled:                       [X] ⑤
  MLom:                                 [ ]           VLAN ID:                            101
Shared LOM Ext:                         [ ]           Priority:                            0
IP (Basic) ②
IPV4:                                   [X]           IPV6:                               [ ]
DHCP enabled                            [ ]
CIMC IP:                                10.100.101.246
Prefix/Subnet:                           255.255.255.0 ③
Gateway:                                 10.100.101.1_
Pref DNS Server: 0.0.0.0

*****
<Up/Down>Selection  <F10>Save ⑥ <Space>Enable/Disable  <F5>Refresh  <ESC>Exit
<F1>Additional settings
Hit the Refresh key in 45 seconds to get the latest network settings.
    
```

- Ping the IMC IP address that was just set to validate the configuration.
- Open a web browser with `https://<CIMC-IP-Address>` to the IMC management GUI. Log in as **admin** with the configured password.



- On the Summary page, check the running versions of the BIOS and IMC firmware to verify that these versions meet the requirements for Cisco HyperFlex and Cisco Intersight deployment. The factory-shipped systems should already have the recommended firmware preloaded. If an IMC upgrade is needed, go to the Cisco website to download the latest [Host Upgrade Utility \(HUU\)](#) and use that utility to upgrade the firmware to a compatible version.

- If desired, click Select Timezone to set the correct time zone for the server.
- From the navigation pane, choose Compute and then click the Power Policies tab. Change the Power Restore Policy from the default Power Off to the desired action.

17. From the navigation pane, expand Admin. Then click Networking, under the Network tab, review the IMC IP settings, add an alternative DNS server here if desired. You can change the host name here as well.

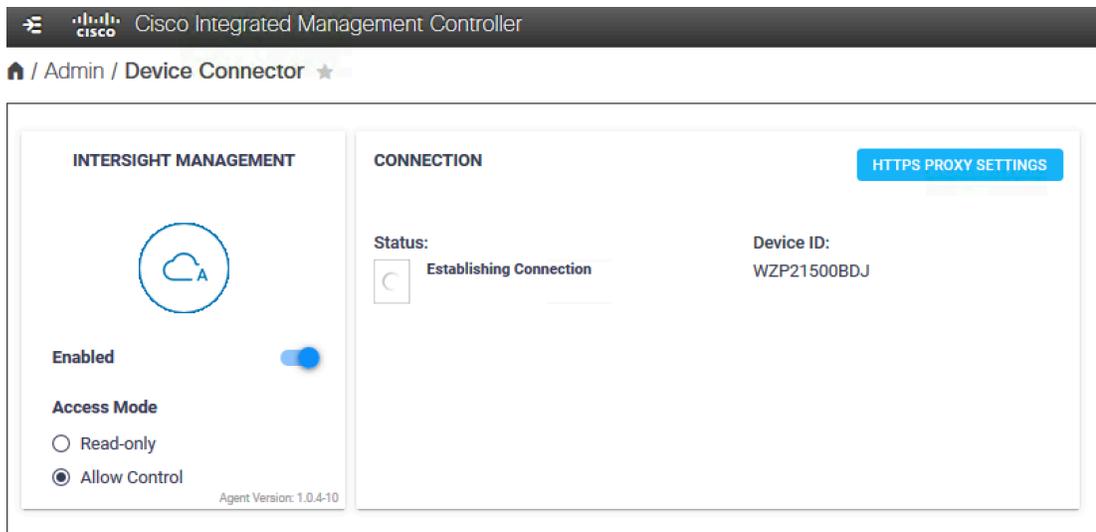
18. Click the NTP Setting tab. Then add your NTP server information.

19. After making the changes you want, click Save Changes to save and apply the changed values. A host-name change will create a new certificate for the web browser and require you to log in again to the web GUI. The system may take several minutes to commit the changes.
20. Repeat the preceding steps for all three Cisco HyperFlex Edge servers.

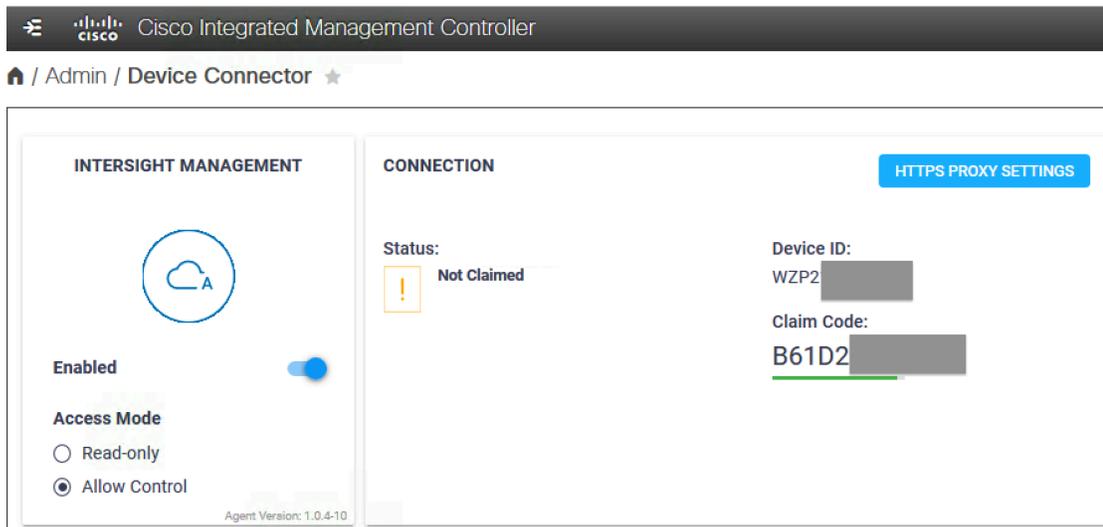
Claiming devices in the Cisco Intersight platform

Now you can enable the device connector on the Cisco HyperFlex servers and let the Cisco Intersight platform claim them for cloud management:

1. Log in to the IMC web management GUI with `https://<CIMC-IP-Address>`.
2. From the navigation pane, expand Admin. Then click Device Connector and enable Cisco Intersight management on the device connector using Allow Control as the access mode (this option may already be set). This configuration enables the IMC to establish a connection to the Cisco Intersight platform.



3. Wait until the connection succeeds and a claim code has been generated for this device. Note that the device is not claimed yet. Write down the device ID (server system number) and claim code as they will be needed in a subsequent step.



- Repeat steps 1 through 3 for all three Cisco HyperFlex Edge servers to gather all device IDs and claim codes. Note that each claim code has an expiration time as indicated by the colored bar under the claim code. Be sure to claim the servers before the codes expire.
- Go to Cisco Intersight Cloud Management platform: <https://intersight.com/>.
- Log in with your Cisco ID and password. If this is your first time using the Cisco Intersight platform, you should take a site tour to learn about some of the platform's main features.

WELCOME TO CISCO INTERSIGHT



Take a Site Tour



Learn How to Claim a New Device

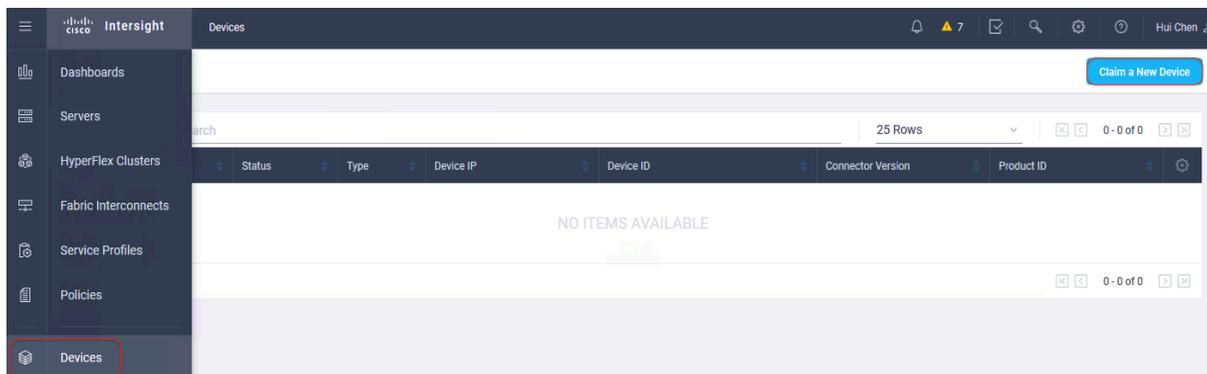


Learn How to Add a New User

Remind Me Later

Start Tour

- To claim a new device, in the Navigation pane at the left, click Devices. Then, at the top right corner of the Devices window, click Claim a New Device.



- Enter the device ID and claim code obtained from the IMC management GUI. Use copy and paste for accuracy. Click Claim.

CLAIM A NEW DEVICE

To claim your device, you must have the Device ID and Claim Code.

Device ID *

Claim Code *

Cancel Claim

- Wait until the device has been claimed successfully.
- Go to the server's IMC page to verify the claim. The Device Connector page should now show that this device has been claimed.

Cisco Integrated Management Controller

Admin / Device Connector

INTERSIGHT MANAGEMENT

Enabled

Access Mode

Read-only

Allow Control

Agent Version: 1.0.4-10

CONNECTION HTTPS PROXY SETTINGS

Status: ✔ Claimed
by huichon Tue Feb 13 18:51:35 2018

Device ID: WZP21500BJ0

- Repeat steps 7 through 10 to claim all three Cisco HyperFlex servers on the Cisco Intersight platform.
- Review the Device window again. The three Cisco HyperFlex nodes should now be listed as connected devices.

Name	Status	Type	Device IP	Device ID	Connector Version	Product ID
HX4Edge	Connected	HyperFlex C...	10.29.145.208	e4ee51fa-f2f9-432b-a5a5-ebbac832d81e	1.0.5-1001	HXAF220C-M4S
HX3-D25-FI	Connected	UCS Domain	10.29.145.134	SSI191109SX & SSI1911099Y	1.0.5-2000	UCS-FI-6248UP
hx3-c220-1	Connected	Standalone ...	10.29.145.154	WZP21500BJ0	1.0.4-10	HXAF220C-M5SX
hx3-c220-3	Connected	Standalone ...	10.29.145.156	WZP21500BDJ	1.0.4-10	HXAF220C-M5SX
hx3-c220-2	Connected	Standalone ...	10.29.145.155	WZP21500BGU	1.0.4-10	HXAF220C-M5SX
HuiEdge	Not Connected	HyperFlex C...	10.29.145.162	f2bc8798-984d-4341-989b-1e3c2aefe095	1.0.3-827	HXAF220C-M5SX
HX3Edge	Connected	HyperFlex C...	10.29.145.162	0c38d590-c1b1-460e-acfb-0fc33d9cd6ab	1.0.3-827	HXAF220C-M5SX

13. You now have the option to launch the IMC management GUI directly from the Cisco Intersight platform. If you want to do so, click Launch IMC.

Name	Status	Type	Device IP	Device ID	Connector Version	Product ID
HX4Edge	Connected	HyperFlex C...	10.29.145.208	e4ee51fa-f2f9-432b-a5a5-ebbac832d81e	1.0.5-1001	HX220C-M4S
HX3-025-FI	Connected	UCS Domain	10.29.145.134	SSI191109SX & SSI1911099Y	1.0.5-2000	UCS-FI-6248UP
hx3-c220-1	Connected	Standalone ...	10.29.145.154	WZP21500BJ0	1.0.4-10	HXAF220C-MSSX
hx3-c220-3	Connected	Standalone ...	10.29.145.156	WZP21500BDJ	1.0.4-10	HXAF220C-MSSX
hx3-c220-2	Connected	Standalone ...	10.29.145.155	WZP21500BGU	1.0.4-10	HXAF220C-MSSX
HuiEdge	Not Connected	HyperFlex C...	10.29.145.162	f2bc8798-984d-4341-989b-1e3c2aefe095	1.0.3-827	HXAF220C-MSSX
HX3Edge	Connected	HyperFlex C...	10.29.145.162	0c38d590-c1b1-460e-acfb-0fc33d9cd6ab	1.0.3-827	HXAF220C-MSSX

14. To unclaim (remove) a device from the Cisco Intersight platform, select the device and click the trash icon. On the pop-up confirmation page, click Remove to confirm the removal.

Name	Status	Type	Device IP	Device ID	Connector Version	Product ID
HX4Edge	Connected	HyperFlex C...	10.29.145.208	e4ee51fa-f2f9-432b-a5a5-ebbac832d81e	1.0.5-1001	HX220C-M4S
HX3-025-FI	Connected	UCS Domain	10.29.145.134	SSI191109SX & SSI1911099Y	1.0.5-2000	UCS-FI-6248UP
hx3-c220-1	Connected	Standalone ...	10.29.145.154	WZP21500BJ0	1.0.4-10	HXAF220C-MSSX
hx3-c220-3	Connected	Standalone ...	10.29.145.156	WZP21500BDJ	1.0.4-10	HXAF220C-MSSX
hx3-c220-2	Connected	Standalone ...	10.29.145.155	WZP21500BGU	1.0.4-10	HXAF220C-MSSX
HuiEdge	Not Connected	HyperFlex C...	10.29.145.162	f2bc8798-984d-4341-989b-1e3c2aefe095	1.0.3-827	HXAF220C-MSSX
HX3Edge	Connected	HyperFlex C...	10.29.145.162	0c38d590-c1b1-460e-acfb-0fc33d9cd6ab	1.0.3-827	HXAF220C-MSSX

Creating and installing Cisco HyperFlex Edge clusters

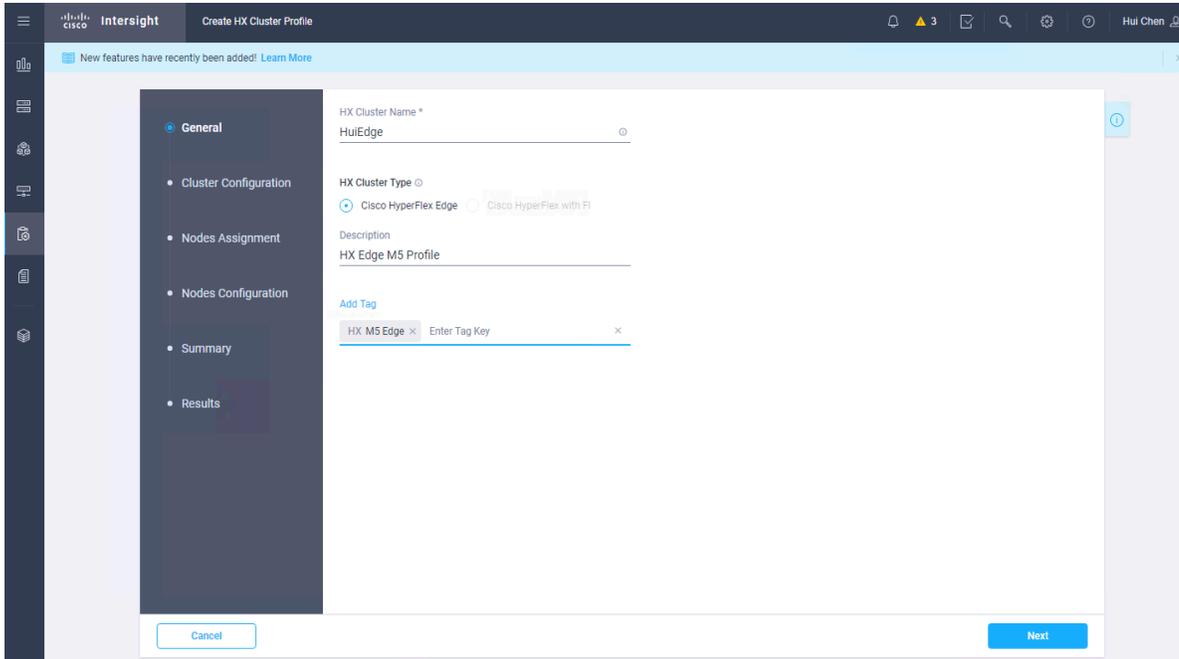
The Cisco Intersight platform provides an installation wizard to install, configure, and deploy Cisco HyperFlex Edge clusters. The wizard constructs a preconfiguration definition of an Edge cluster called a Cisco HyperFlex cluster profile. The cluster profile is policy-based, with administrator-defined sets of rules and operating characteristics such as the node identity, interfaces, and vCenter connectivity. Every active node in the Edge cluster must be associated with a Cisco HyperFlex cluster profile. After the user enters all the configuration settings, the installation wizard will validate and deploy the cluster profile on the Cisco HyperFlex Edge nodes. You can clone a successfully deployed Cisco HyperFlex cluster profile and then use that copy as a template to easily create many more new clusters.

To install and configure a Cisco HyperFlex Edge cluster with the Cisco Intersight platform, complete the following steps:

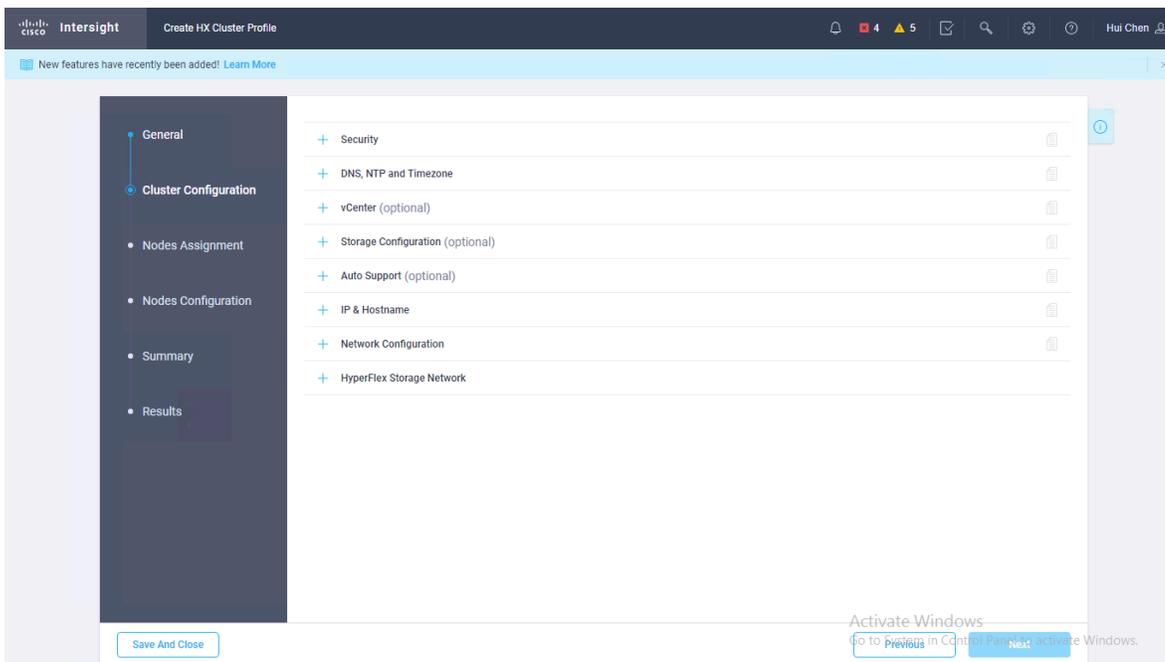
1. Log in to the Cisco Intersight cloud management platform at <https://intersight.com/> with your Cisco ID and password.
2. In the navigation pane at the left, choose Service Profiles. On the Service Profiles page, click the HX Cluster Profile tab and click Create HX Cluster Profile.

Name	Description	Status	Last Update
HuiEdge	HX Edge M5 Profile	Not Assigned	a few seconds ago

- The HX Cluster Profile installation wizard is displayed. Proceed through the installation steps. First, on the General page, enter a cluster name under HX Cluster Name. This cluster name must be unique and will be used as the HX Data Platform cluster name, vCenter cluster name, and Cisco Intersight cluster name. Under HX Cluster Type, select Cisco HyperFlex Edge. Add the necessary description and tags for this cluster for reference.



- Click Next to move to the Cluster Configuration page.



- Click the + sign to expand the Security configuration. Enter **root** as the hypervisor administration user name and enter **Cisco123** as the default hypervisor password in Cisco HyperFlex 2.6. Enter a user-supplied password for the Cisco HyperFlex controller virtual machine and then confirm that password in the second text field.

- When you close the Security configuration page, the settings are automatically saved to a policy named <HX-Cluster-Name>-local-credential-policy. This policy is reusable and can be selected when you create your next Cisco HyperFlex cluster profile.
- (Optional) To choose an existing policy for your cluster profile, at the policy line click the Select Policy button. Choose the desired policy from the available policy list and click Select.

- Click the + sign to expand the DNS, NTP and Timezone configuration page. Choose a time zone from the drop-down list and enter DNS server and NTP server information. Click the + sign to enter secondary DNS and NTP servers.

- After you close the DNS, NTP and Timezone configuration page, the settings are automatically saved to a reusable policy named <HX-Cluster-Name>-sys-config-policy.

- Click the + sign to expand the vCenter configuration page. Enter the vCenter Server FQDN or IP address, administration user name, and password. Enter the data center name for the vCenter hosting the Cisco HyperFlex Edge cluster. Leave the vCenter Single Sign-On Server field blank unless instructed otherwise by the Cisco Technical Assistance Center (TAC). If you are deploying your system in a nested vCenter configuration, you can leave the vCenter fields blank and register the cluster to vCenter after it has been deployed on the cluster. For help, see the guide [How to Deploy vCenter on the HX Data Platform](#).

— vCenter (optional)
huiedge-vcenter-config-policy

vCenter Server FQDN or IP *	vCenter Username *	vCenter Password *
<input type="text" value="10.29.133.79"/>	<input type="text" value="huich@hx"/>	<input type="password" value="*****"/>
vCenter Datacenter Name *	vCenter Single-Sign-On Server	
<input type="text" value="HUIDC"/>	<input type="text"/>	

- After you close the vCenter configuration, the settings are automatically saved to a reusable policy named <HX-Cluster-Name>-vcenter-config-policy.
- Click the + sign to expand the Storage configuration page. Select Clean Up Disk Partitions if you are performing a reinstallation on top of an existing deployment. If you are deploying a virtual desktop infrastructure (VDI) environment on a hybrid Cisco HyperFlex cluster, select the box to enable file system optimization.

— Storage Configuration (optional)

Clean up Disk Partitions

Vdi Optimization

- After you close the Storage configuration, the settings are automatically saved to a reusable policy named <HX-Cluster-Name>-cluster-storage-policy.
- Click the + sign to expand the Auto Support configuration page. Select the box to enable Auto-Support. Enter your email address for service ticket notification.

— Auto Support (optional)
Select Policy

Auto-Support

Send Service Ticket Notification to

- After you close the Auto Support configuration, the settings are automatically saved to a reusable policy named <HX-Cluster-Name>-auto-support-policy.

16. Click the + sign to expand the IP & Hostname configuration page. Enter a host-name prefix. In a later step, host names will be sequentially assigned to hosts using this prefix. Enter the starting IP address, ending IP address, netmask, and gateway for the management IP address pool. IP addresses from this range will automatically be assigned to hosts in the node configuration step. If you enter only the management network IP addresses, the same range will be used for both ESXi management and Cisco HyperFlex controller virtual machine management IP addresses. If you want to use a second, noncontiguous range of IP addresses for the Cisco HyperFlex controller virtual machines, you may optionally enter the starting IP address, ending IP address, netmask, and gateway for the controller virtual machine management IP address pool. Note that these two IP ranges must fall within the same IP subnet and VLAN.

— IP & Hostname ✔
huiedge-node-config-policy 📄

Hostname Prefix *

hx3edge ⊙

Management Network Starting IP * 10.29.145.157 ⊙	Management Network Ending IP * 10.29.145.159 ⊙
Management Network Subnet Mask * 255.255.255.0 ⊙	Management Network Gateway * 10.29.145.1 ⊙
Controller VM Management Network Starting IP 10.29.145.163 ⊙	Controller VM Management Network Ending IP 10.29.145.165 ⊙
Controller VM Management Network Subnet Mask 255.255.255.0 ⊙	Controller VM Management Network Gateway 10.29.145.1 ⊙

17. After you close the IP & Hostname configuration, the settings are automatically saved to a reusable named <HX-Cluster-Name>-node-config-policy.
18. Click the + sign to expand the Network configuration page. Enter the VLAN ID for the management network. Leave the Jumbo Frames checkbox unselected for Cisco HyperFlex Edge deployments.

— Network Configuration ✔
huiedge-cluster-network-policy 📄

Management Network VLAN ID *

41 ⊙

Jumbo Frames ⊙

19. After you close the Network configuration, the settings are automatically saved to a reusable policy named <HX-Cluster-Name>-cluster-network-policy.
20. Click the + sign to expand the HyperFlex Storage Network configuration page. Enter the VLAN ID for the data storage network. As a best practice, use a unique storage VLAN for each cluster if you are deploying multiple clusters in the same network.

— HyperFlex Storage Network ✔

Storage Network VLAN ID

42 ⊙

21. Click Next to move to the Nodes Assignment page. Select three available Cisco HyperFlex Edge nodes. You also have the option to assign nodes later, saving the Cisco HyperFlex cluster profile now and returning when the hardware is available to assign after it has been claimed in the Cisco Intersight platform.

Name	Assign Status	Model	Serial
hx3-c220-1	Not Assigned	HXAF220C-M5SX	WZP21500BJ0
hx3-c220-3	Not Assigned	HXAF220C-M5SX	WZP21500BDJ
hx3-c220-2	Not Assigned	HXAF220C-M5SX	WZP21500BGU

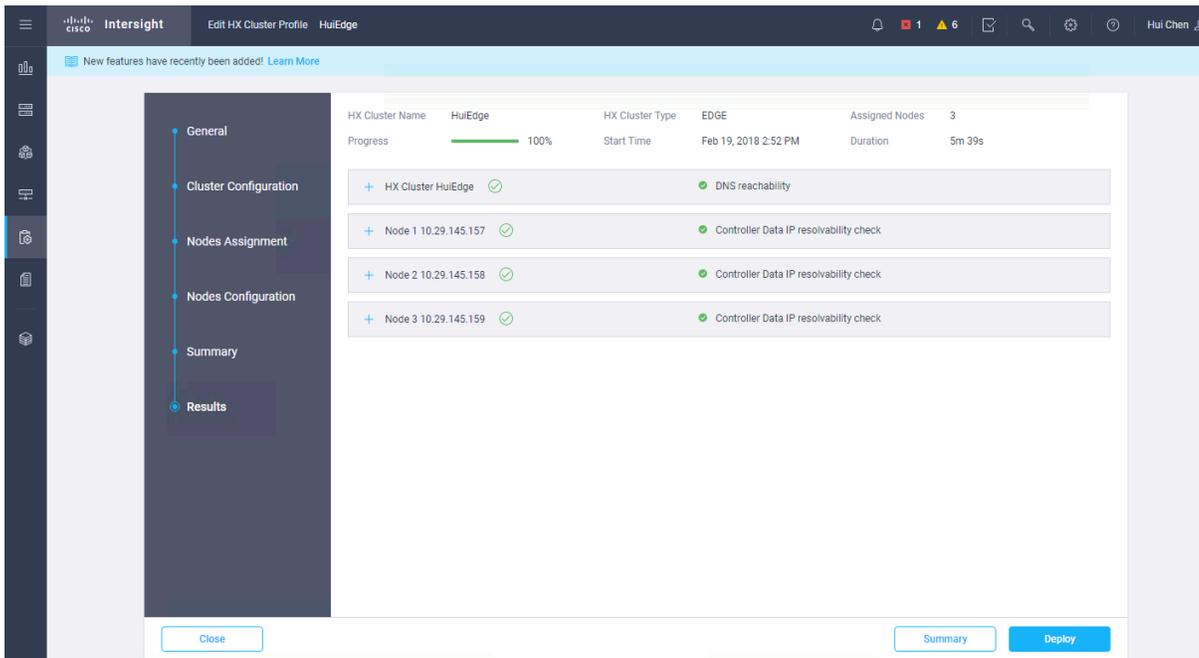
22. Click Next to navigate to the Nodes Configuration page. Review the node configuration for all three Cisco HyperFlex Edge nodes. You can freely modify the host name defined by automatic IP address assignment if desired. Enter the cluster management IP address within the same IP management subnet.

23. Click Next to move to the Summary page. Review the Cluster Configuration and Nodes Configuration pages. Check for errors.

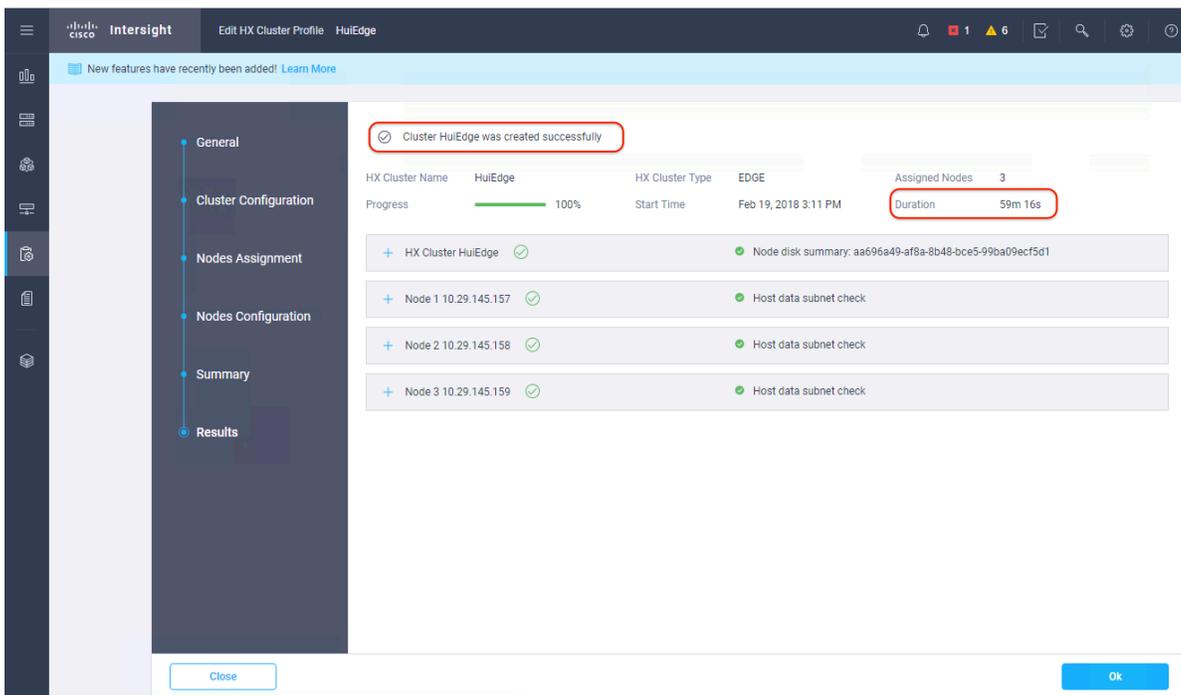
24. Click Validate to validate the Cisco HyperFlex Edge cluster configuration, without starting deployment. This selection will start a series of hardware, software, and environmental checks that will take a few minutes to complete. Alternatively, click Validate & Deploy to complete validation and deployment together. This document performs an explicit validation first, followed by the start of the actual deployment.

Node	IP Address	Status	Check Name
Node 1	10.29.145.157	✓	Controller Data IP resolvability check
Node 2	10.29.145.158	✓	Controller Data IP resolvability check
Node 3	10.29.145.159	✓	Controller Data IP resolvability check

25. Wait until validation succeeds. Fix any errors found and note any warnings before continuing.

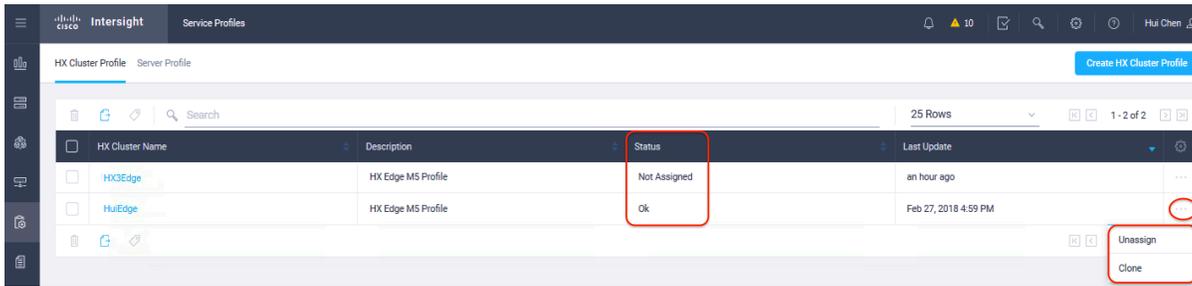


26. On the Results page for the validation process, click Deploy to install the Cisco HyperFlex Edge cluster. Optionally, you can click Save and Close to complete deployment later. Installation time will vary based on network bandwidth, but typically takes about one hour. You can remain on the Results page to watch the cluster deployment progress in real time. Alternatively, you can click Close to send the task to the background and navigate elsewhere within the Cisco Intersight platform. To return to the results view, navigate back to the Service Profiles > HX Cluster Profile list view and select the cluster name.



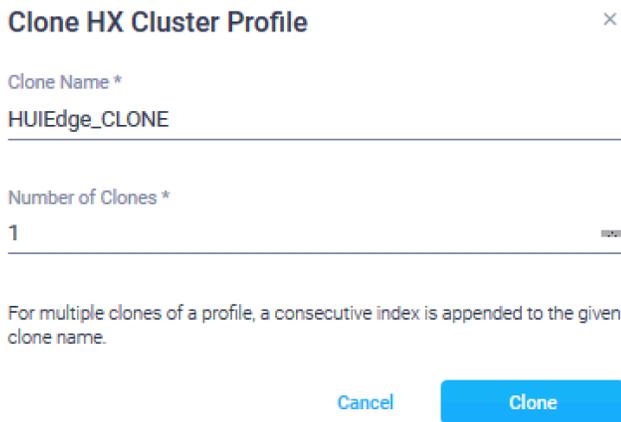
27. After the deployment has completed successfully, click OK.

28. When you are back on the Service Profiles > HX Cluster Profile page, find the newly deployed Cisco HyperFlex cluster profile with a status of OK.



29. You can clone and modify the cluster profile to quickly create many new cluster profiles. To clone a cluster profile, select the profile that you want to clone, in the Settings column click ..., and then click Clone.

30. In the pop-up Clone window, enter the name for the cloned cluster and choose the number of clones. Click Clone.

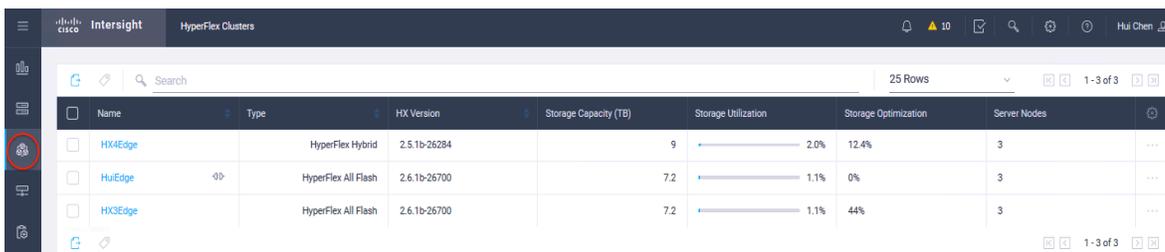


31. Before deploying the new copy of the cloned cluster profile, review the configuration and make any necessary changes to the policies.

32. To unassign the servers from the selected cluster profile, in the Settings column click ... and then click Unassign and Unassign again.

Note: Unassigning will remove all assigned servers from the cluster profile. This action is specific to the Cisco Intersight platform and will not result in a factory reset or affect the operation of the running cluster. To completely clean up this cluster from the Cisco Intersight platform, unclaim the cluster and associated servers. Contact the TAC for return materials authorization (RMA) support or cluster reinstallation procedures.

33. Verify the Cisco HyperFlex Edge cluster information on the Cisco Intersight platform. In the navigation pane, go to the HyperFlex Clusters page and click the hyperlinked cluster name.



34. On the HyperFlex Clusters page, on the General tab, review summary information about the new cluster: health state, storage capacity, node count, etc. Check for any critical alarms requiring your attention.

The screenshot shows the 'General' tab for a HyperFlex Cluster named 'HX3Edge'. The 'Health' status is 'Healthy'. Key metrics include: Hypervisor Version (VMware ESXi 6.0.0 build-5572656), HX Version (2.6.1b-26700), Storage Optimization (44%), Storage Utilization (1.1%), Storage Capacity (TB) (7.2), and Uptime (9 days 16 hours 19 minutes 19 seconds). A 'Server Nodes 3' button is visible. Below, 'Converged Node Count' is 3 and 'Compute Node Count' is 0. A table lists three nodes (hx3-c220-1, hx3-c220-3, hx3-c220-2) all with a 'Warning' health status and 'Converged' type. The 'Alarms' section shows three warnings for HX-370, stating 'Node is unable to reach callhome endpoint'.

35. On the same page, click the Profile tab, which allows you to review the newly created HX Cluster Profile information. Under Cluster Configuration, you can review the details of the policies you just configured.

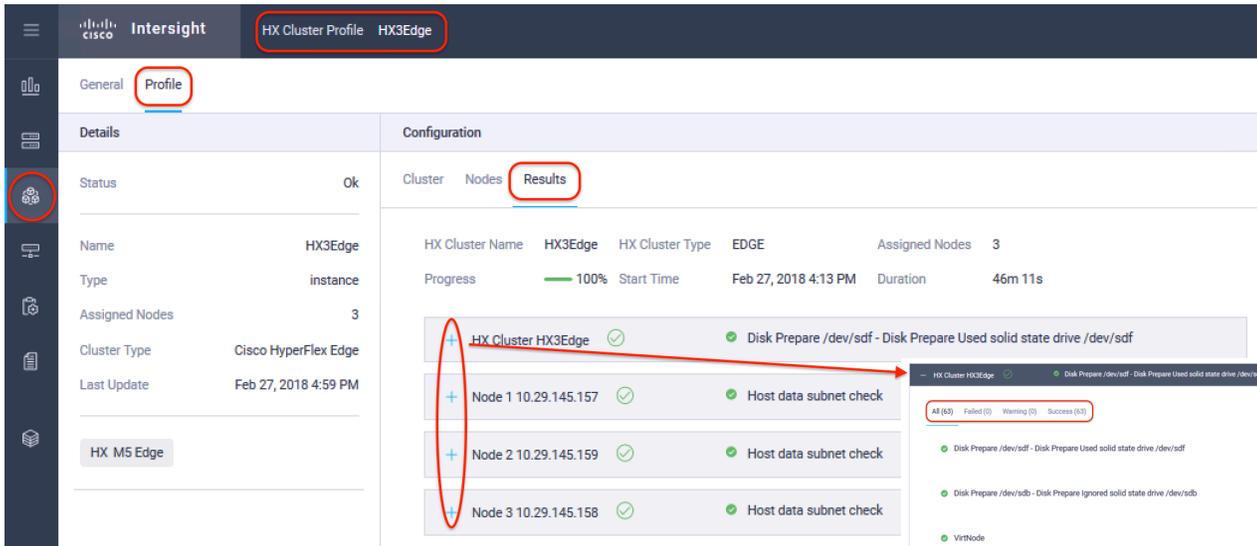
The screenshot shows the 'Profile' tab for the 'HX Cluster Profile HX3Edge'. The 'Status' is 'Ok'. The 'Configuration' section lists several policies: vCenter (huedge-vcenter-config-policy), Auto Support (huedge-auto-support-policy), Security (huedge-local-credential-policy), Network Configuration (huedge-cluster-network-policy), IP & Hostname (huedge-node-config-policy), DNS, NTP and Timezone (huedge-sys-config-policy), and Storage Configuration (huedge-cluster-storage-policy). A detailed view of the 'huedge-local-credential-policy' is shown on the right, with 'Name' as 'huedge-local-credential-policy', 'Usage' as 2, and 'Main' user as 'Hypervisor Admin' with 'root' privileges.

36. Review the Nodes configuration.

The screenshot shows the 'Nodes' configuration tab. A table lists the nodes and their IP addresses:

Name	Hypervisor IP	Storage Controller IP
hx3edge-1	10.29.145.157	10.29.145.163
hx3edge-2	10.29.145.158	10.29.145.164
hx3edge-3	10.29.145.159	10.29.145.165

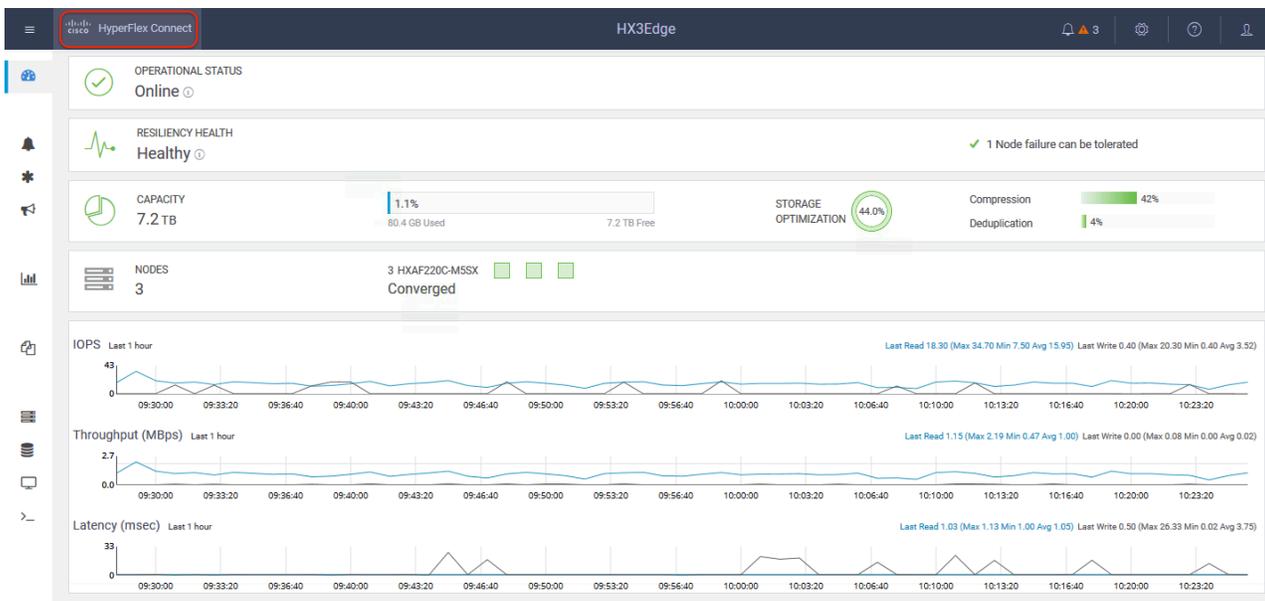
37. Review the details of the installation process under Results. Click the + sign at the top of each panel to expand the detailed information.



38. You can review more detailed status information for the new Cisco HyperFlex Edge cluster in the Cisco HyperFlex Connect management GUI. Cisco HyperFlex Connect can be directly launched from the Cisco Intersight platform. To find the cross-launch feature, first navigate back to the cluster list view by selecting HyperFlex Clusters in the navigation pane at the left.

39. Find the desired cluster in the list, in the Settings column click ..., and then click Launch HyperFlex Connect. The native Cisco HyperFlex Connect user interface will launch in a new browser tab. You can easily manage large-scale Cisco HyperFlex deployments directly from the Cisco Intersight platform.

All Cisco HyperFlex functions are available through cross-launch except cluster upgrade, support bundle download, and HX Data Platform device connector settings. These operations must be performed by directly launching Cisco HyperFlex Connect over the local network.



Post-installation configuration

Prior to putting your Cisco HyperFlex Edge cluster into production, you should complete a few post-installation tasks. To automate the post-installation procedures and verify the Cisco HyperFlex cluster configuration, a script is provided on the Cisco HyperFlex controller virtual machines. These steps can also be performed manually or with a Power CLI script in vCenter if preferred (a sample script is shown in Appendix B).

The following procedure uses the `post_install` script. To run this script, complete the following steps:

1. Use SSH to go to the cluster management IP address and log in using the `<root>` user name and the controller virtual machine password provided during installation. Verify that the cluster is online and healthy by using the `stcli cluster info` or `stcli cluster storage-summary` command.
2. Type the following command in the shell and press Enter to update to the latest post-installation script. Look for the message "Scripts successfully updated."

```
curl -L http://cs.co/hxupdate | sh
```

```
root@ip-10-29-145-164:~# curl -L http://cs.co/hxupdate | sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left     Speed
100   25    0   25    0    0    137    0  --:--:--  --:--:--  --:--:--   137
0     0    0    0    0    0     0     0  --:--:--  --:--:--  --:--:--    0
100    3  100    3    0    0     2     0  0:00:01  0:00:01  --:--:--    2
100  458  100  458    0    0    328    0  0:00:01  0:00:01  --:--:--  2008
Scripts succesfully updated
```

3. Type the following command in the shell and press Enter:


```
/usr/share/springpath/storfs-misc/hx-scripts/post_install.py
```
4. Enter the Cisco HyperFlex storage controller virtual machine root password for the Cisco HyperFlex cluster (use the password entered during the Cisco HyperFlex cluster installation). Also enter the vCenter user name and password. You must license the vSphere hosts through the script or complete this task in vCenter before continuing. Failure to apply a license will result in an error when you attempt to enable VMware High Availability (HA) or Distributed Resource Scheduler (DRS) in subsequent steps.

```
root@ip-10-29-145-164:~# /usr/share/springpath/storfs-misc/hx-scripts/post_install.py
Logging in to controller localhost
HX CVM root password:
Getting ESX hosts from HX cluster...
vCenter URL: 10.29.133.79
Enter vCenter username (user@domain): huich@hx
vCenter Password:
Found datacenter HUIDC
Found cluster HX3Edge
HX Edge configuration detected

Enter vSphere license key? (y/n) n
```

5. Enter `y` to enable HA/DRS.

```
Enable HA/DRS on cluster? (y/n) y
```

6. Enter `y` to disable the ESXi hosts' SSH warning. SSH running in ESXi is required in HX Data Platform 2.6.

```
Disable SSH warning? (y/n) y
```

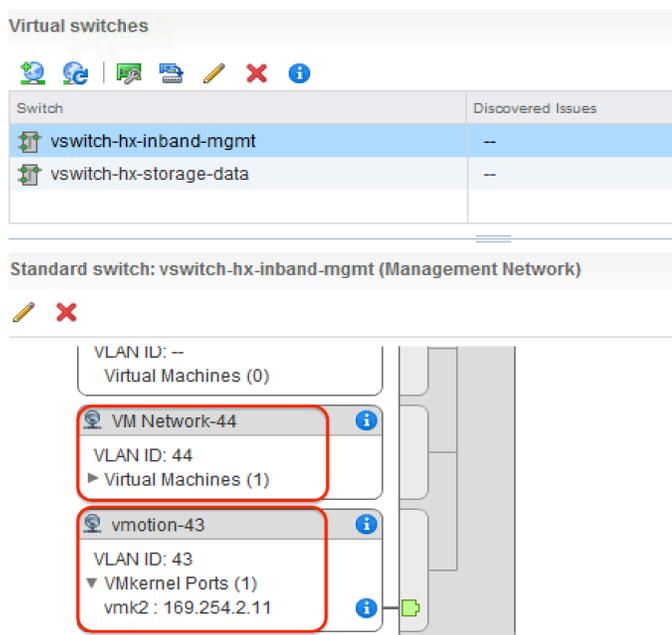
7. Add the vMotion VMkernel interfaces to each node by entering y. Enter the netmask, the vMotion VLAN ID, and the vMotion IP addresses for each of the hosts as prompted. vMotion will be configured using best practices according to the choice of a single- or dual-switch configuration. In the case of single-switch configuration, a traffic shaper will automatically be applied to the VMkernel port to help ensure that vMotion does not consume all the bandwidth available on the shared uplink port.

```
Add vmotion interfaces? (y/n) y
Netmask for vMotion: 255.255.255.0
VLAN ID: (0-4096) 43
vMotion IP for hx3edge-1.hx.lab.cisco.com: 169.254.2.11
Adding vmotion-43 to hx3edge-1.hx.lab.cisco.com
Adding vmkernel to hx3edge-1.hx.lab.cisco.com
Updating portgroup vmotion-43 on hx3edge-1.hx.lab.cisco.com
vMotion IP for hx3edge-2.hx.lab.cisco.com: 169.254.2.12
Adding vmotion-43 to hx3edge-2.hx.lab.cisco.com
Adding vmkernel to hx3edge-2.hx.lab.cisco.com
Updating portgroup vmotion-43 on hx3edge-2.hx.lab.cisco.com
vMotion IP for hx3edge-3.hx.lab.cisco.com: 169.254.2.13
Adding vmotion-43 to hx3edge-3.hx.lab.cisco.com
Adding vmkernel to hx3edge-3.hx.lab.cisco.com
Updating portgroup vmotion-43 on hx3edge-3.hx.lab.cisco.com
```

8. You can add virtual machine network port groups for guest virtual machine traffic. Enter n to skip this step and create the port groups manually in vCenter. Alternatively, you can create virtual machine network port groups and add them to the virtual machine vSwitch. This step will add the same network configuration to all nodes in the cluster.

```
Add VM network VLANs? (y/n) y
Port Group Name to add (VLAN ID will be appended to the name): VM Network
VLAN ID: (0-4096) 44
Adding VM Network-44 to hx3edge-1.hx.lab.cisco.com
Adding VM Network-44 to hx3edge-2.hx.lab.cisco.com
Adding VM Network-44 to hx3edge-3.hx.lab.cisco.com
Add additional VM network VLANs? (y/n) n
```

After the post-installation script is complete, a vMotion VMkernel port and virtual machine network port groups are visible for each host in vCenter:



Virtual switches

Switch	Discovered Issues
vswitch-hx-inband-mgmt	--
vswitch-hx-storage-data	--

Standard switch: vswitch-hx-inband-mgmt (Management Network)

- VLAN ID: --
Virtual Machines (0)
- VM Network-44** (VLAN ID: 44)
Virtual Machines (1)
- vmotion-43** (VLAN ID: 43)
VMkernel Ports (1)
vmk2: 169.254.2.11

9. Enter n to skip the testing of the autosupport email function.
 10. A summary of the cluster will be displayed upon completion of the script. Verify that the cluster is healthy.
- You should enable a syslog destination for permanent storage of the ESXi host logs. The configuration can be performed manually in vCenter or through a Power CLI script.

Cisco HyperFlex licensing

Cisco HyperFlex 2.5 and later uses Cisco Smart Licensing, which communicates with a Cisco Smart Account to validate and check out Cisco HyperFlex licenses to the nodes from the pool of available licenses in the account. At the beginning, Smart Licensing is enabled, but the Cisco HyperFlex storage cluster is unregistered and in a 90-day evaluation period, or Eval Mode. For the Cisco HyperFlex storage cluster to start reporting license consumption, it must be registered with the Cisco Smart Software Manager (SSM) through a valid Cisco Smart Account. Before beginning, verify that you have a Cisco Smart Account and that valid Cisco HyperFlex licenses are available to be checked out by your Cisco HyperFlex cluster.

To create a Smart Account, see Cisco Software Central > Request a Smart Account at <https://webapps.cisco.com/software/company/smartaccounts/home?route=module/accountcreation>.

To activate and configure Smart Licensing, complete the following steps:

1. Log in to a controller virtual machine. Confirm that your Cisco HyperFlex storage cluster is in Smart Licensing mode.

```
# stcli license show status
```

```
Smart Licensing is ENABLED
```

Registration:

```
Status: UNREGISTERED
Export-Controlled Functionality: Not Allowed
```

License Authorization:

```
Status: EVAL MODE
Evaluation Period Remaining: 79 days, 8 hr, 52 min, 57 sec
Last Communication Attempt: NONE
```

Feedback will show that Smart Licensing is Enabled, with Status: Unregistered, and the amount of time left during the 90-day evaluation period (in days, hours, minutes, and seconds).

2. Navigate to Cisco Software Central (<https://software.cisco.com/>) and log in to your Smart Account.
3. From Cisco Smart Software Manager, generate a registration token.
4. In the License pane, click Smart Software Licensing to open Cisco Smart Software Manager.
5. Click Inventory.
6. From the virtual account in which you want to register your Cisco HyperFlex storage cluster, click General; then click New Token.

7. In the Create Registration Token dialog box, add a short description for the token, enter the number of days that you want the token to be active and available for use on other products, and allow export-controlled functions on the products registered with this token.
8. Click Create Token.
9. From the New ID Token row, click the Actions drop-down list and click Copy.
10. Log into a controller virtual machine.
11. Register your Cisco HyperFlex storage cluster, where **idtoken-string** is the new ID token from Cisco Smart Software Manager.

```
# stcli license register --idtoken idtoken-string
```

12. Confirm that your Cisco HyperFlex storage cluster is registered.

```
# stcli license show summary
```

The cluster is now ready. You can now run any other preproduction tests that you want to run.

Conclusion

Cisco HyperFlex Edge is optimized for remote-office and branch-office (ROBO) and edge environments. The Cisco Intersight cloud management platform is designed to deploy, monitor, manage, and provide additional value-added services with strengthened security to Cisco UCS and Cisco HyperFlex products. All of these functions can be performed remotely without requiring IT staff to be physically present near the hardware.

As described in this document, Cisco HyperFlex Edge systems also can be remotely deployed from the cloud with the Cisco Intersight platform. This is a big step forward in Cisco's strategy to build cloud-managed, on-premises, intelligent infrastructure. In the future, Cisco Intersight capabilities will continue to improve, with the end goal of providing customers with the industry's lowest operating costs, greatest scale, and fastest time to value. The Cisco Intersight platform combined with Cisco HyperFlex systems will completely transform the way that IT infrastructure is managed in the future.

For more information

- Cisco HyperFlex Installation Guide for Cisco Intersight:
https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/HyperFlex_Installation_Guide_for_Intersight/b_HyperFlex_Installation_Guide_for_Intersight.pdf
- Cisco HyperFlex 2.6 for Virtual Server Infrastructure Deployment Guide:
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/hyperflex_26_vsi.html

Appendix

Appendix A: Sample Cisco Nexus 3048TP Gigabit Ethernet switch configuration

```
!Time: Tue Mar 6 22:00:50 2018

version 5.0(3)U2(2b)
feature telnet
feature lldp

username admin password 5 $1$NnbI43MT$w.3G7okndrYkU4jtNARUL. role network-admin
no password strength-check
ip domain-lookup
switchname HX4N3K
... ..

snmp-server user admin network-admin auth md5 0x9bb06bfe292d2c5b0da33e0581b5a74d priv
0x9bb06bfe292d2c5b0da33e0581b5a74d localizedkey
ntp server 10.81.254.202 use-vrf management

vrf context management
    ip route 0.0.0.0/0 10.29.145.1
vlan 1
vlan 41
    name hx-mgmt
vlan 42
    name hx-data
vlan 43
    name hx-vmotion
vlan 44
    name hx-vmnet

interface Ethernet1/1
    negotiate auto

interface Ethernet1/2
    negotiate auto

... ..
```

```
interface Ethernet1/13
  switchport mode trunk
  switchport trunk allowed vlan 41,43-44
  spanning-tree port type edge trunk
  speed 1000
  negotiate auto
```

```
interface Ethernet1/14
  switchport mode trunk
  switchport trunk allowed vlan 41-42
  spanning-tree port type edge trunk
  speed 1000
  negotiate auto
```

```
interface Ethernet1/15
  switchport mode trunk
  switchport trunk allowed vlan 41,43-44
  spanning-tree port type edge trunk
  speed 1000
  negotiate auto
```

```
interface Ethernet1/16
  switchport mode trunk
  switchport trunk allowed vlan 41-42
  spanning-tree port type edge trunk
  speed 1000
  negotiate auto
```

```
interface Ethernet1/17
  switchport mode trunk
  switchport trunk allowed vlan 41,43-44
  spanning-tree port type edge trunk
  speed 1000
  negotiate auto
```

```
interface Ethernet1/18
  switchport mode trunk
  switchport trunk allowed vlan 41-42
  spanning-tree port type edge trunk
  speed 1000
  negotiate auto
```

```
interface Ethernet1/19
  negotiate auto
```

```
interface Ethernet1/20
  negotiate auto
```

```
... ..
```

```
interface Ethernet1/47
  negotiate auto
```

```
interface Ethernet1/48
  switchport access vlan 41
  spanning-tree port type network
  speed 1000
  negotiate auto
```

```
interface Ethernet1/49
```

```
interface Ethernet1/50
```

```
interface Ethernet1/51
```

```
interface Ethernet1/52
```

```
interface mgmt0
  ip address 10.29.145.141/24
  line console
  line vty
```

```
boot kickstart bootflash:/n3000-uk9-kickstart.5.0.3.U2.2b.bin
```

```
boot system bootflash:/n3000-uk9.5.0.3.U2.2b.bin
```

Appendix B: Sample script for VMware ESXi post-installation configuration

```
# Configure_ESX_post_install.ps1
# Description: Configures ESXi options and settings after HyperFlex installation.
# Usage: Modify the variables to specify the ESXi root password, the servers to be
# configured, the guest VLAN ID, and the IP addresses used for the vMotion vmkernel
# interfaces.
#
Set-PowerCLIConfiguration -InvalidCertificateAction Ignore -Confirm:$false | Out-Null

$domainname ="hx.lab.cisco.com"

$array="hx3edge-1.hx.lab.cisco.com", "hx3edge-2.hx.lab.cisco.com", "hx3edge-3.hx.lab.cisco.com"

$ip=11

Foreach ($i in $array)
{

Connect-VIServer -server $i -user root -password Cisco123
$vh=Get-VMHost -Name $i

#disable shell warning
$vh | Set-VMHostAdvancedConfiguration UserVars.SuppressShellWarning 1

#Configuring default DNS suffix
#Write-Host "Configuring DNS and Domain Name on $vmhost" -ForegroundColor Green
#Get-VMHostNetwork -VMHost $vmhost | Set-VMHostNetwork -DomainName $domainname -hostName $myarray2
-DNSAddress $dnsip -Confirm:$false
Get-VMHostNetwork -VMHost $vh | Set-VMHostNetwork -SearchDomain $domainname -Confirm:$false

#configure syslog traffic to send to vCenter or syslog server
Set-VMHostSysLogServer -SysLogServer '10.29.133.63:514' -VMHost $vh

#add port groups to VM-Network
```

```
$vsw0 = Get-VirtualSwitch -VMHost $vh -Name "vswitch-hx-inband-mgmt"
write-host $vsw0

$vpgrp = Get-VirtualPortGroup -VirtualSwitch $vsw0 -Name "VM Network"
Set-VirtualPortGroup -VirtualPortGroup $vpgrp -VLanID 44

$vmip="169.254.2."+$ip

New-VirtualPortGroup -VirtualSwitch $vsw0 -Name "VMotion" -VLanID 43
New-VMHostNetworkAdapter -VMHost $vh -VirtualSwitch $vsw0 -PortGroup "VMotion" -VMotionEnabled
$true -IP $vmip -SubnetMask 255.255.255.0 -Confirm:$false

$ip=$ip+1

Disconnect-VIServer -server $server -Confirm:$False
}
```

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

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: 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)