Cisco UCS Manager Getting Started Guide, Release 3.2

First Published: 2017-08-18

Last Modified: 2018-03-21

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

CONTENTS

Preface

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.

Text Type	Indication
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html.

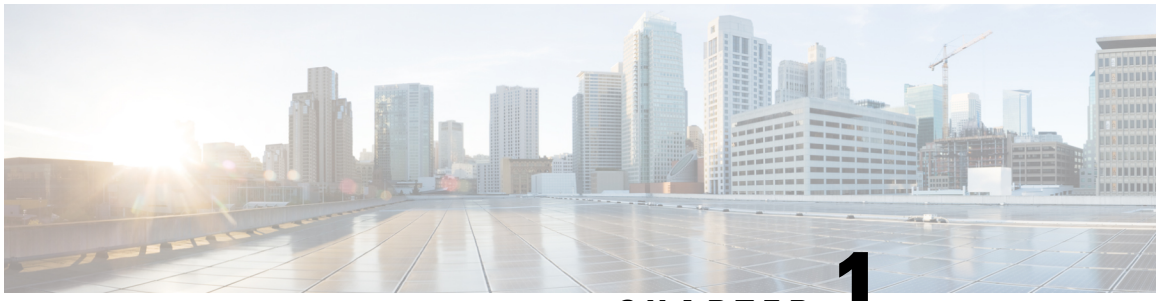
For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

Follow Cisco UCS Docs on Twitter to receive document update notifications.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@external.cisco.com. We appreciate your feedback.



CHAPTER 1

Overview

Cisco UCS Manager Getting Started Guide Overview

This guide provides an overview of Cisco Unified Computing System (Cisco UCS) essentials, procedures for performing Cisco UCS Manager initial configuration and best practices. The following table summarizes the overall organization of the guide.

Chapter	Description
Overview	Conceptual overview of Cisco UCS architecture including Cisco Fabric Interconnects, I/O Module and key server components; Introduction to Cisco UCS Central.
System Requirements	Hardware, browser, and port requirements for Cisco UCS Manager initial configuration.
Initial Configuration	Initial Configuration workflow in the following sequence: **1.** Console Setup **2.** Configure Administration Policies **3.** Configure Equipment Policies **4.** Configure Unified Ports **5.** Configure Fabric Interconnect Server Ports **6.** Configure LAN Connectivity **7.** Configure SAN Connectivity **8.** Define Workloads
Appendix	Recommendations, best practices, configuration examples, and a glossary.

Cisco UCS Manager User Documentation

Cisco UCS Manager offers you a new set of smaller, use-case based documentation described in the following table:

Guide	Description
Cisco UCS Manager Getting Started Guide	Discusses Cisco UCS architecture and Day 0 operations, including Cisco UCS Manager initial configuration and configuration best practices.
Cisco UCS Manager Administration Guide	Discusses password management, role-based access configuration, remote authentication, communication services, CIMC session management, organizations, backup and restore, scheduling options, BIOS tokens, and deferred deployments.
Cisco UCS Manager Infrastructure Management Guide	Discusses physical and virtual infrastructure components used and managed by Cisco UCS Manager.
Cisco UCS Manager Firmware Management Guide	Discusses downloading and managing firmware, upgrading through Auto Install, upgrading through service profiles, directly upgrading at endpoints using firmware auto sync, managing the capability catalog, deployment scenarios, and troubleshooting.
Cisco UCS Manager Server Management Guide	Discusses the new licenses, registering Cisco UCS domain with Cisco UCS Central, power capping, server boot, server profiles, and server-related policies.
Cisco UCS Manager Storage Management Guide	Discusses all aspects of storage management, such as SAN and VSAN in Cisco UCS Manager.
Cisco UCS Manager Network Management Guide	Discusses all aspects of network management, such as LAN and VLAN connectivity in Cisco UCS Manager.
Cisco UCS Manager System Monitoring Guide	Discusses all aspects of system and health monitoring, including system statistics in Cisco UCS Manager.
Cisco UCS S3260 Server Integration with Cisco UCS Manager	Discusses all aspects of management of UCS S-Series servers that are managed through Cisco UCS Manager.

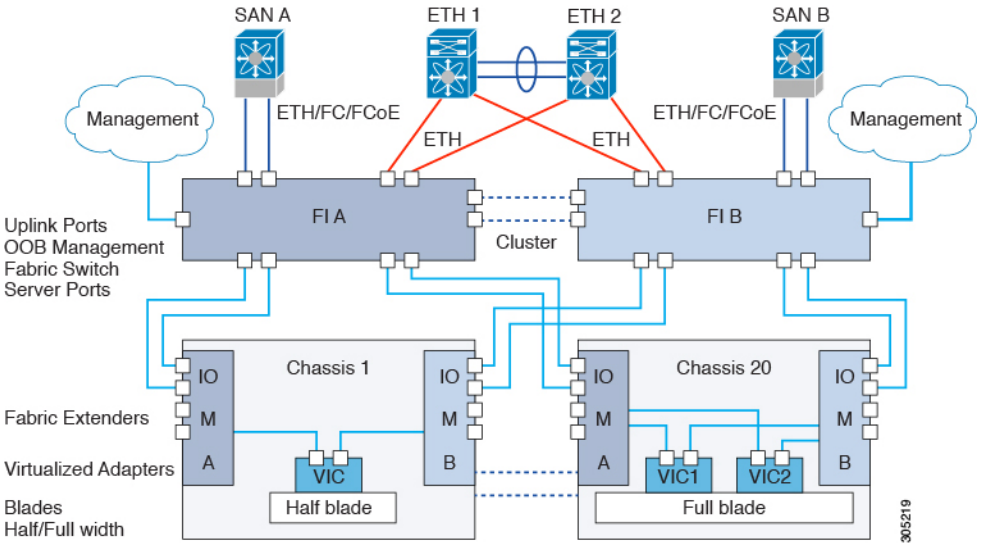
Fundamentals of Cisco Unified Computing System

Cisco Unified Computing System Overview

Cisco UCS has a unique architecture that integrates compute, data network access, and storage network access into a common set of components under a single-pane-of-glass management interface.

Cisco UCS fuses access layer networking and servers. This high-performance, next-generation server system provides a data center with a high degree of workload agility and scalability. The hardware and software components support Cisco's unified fabric, which runs multiple types of data center traffic over a single converged network adapter.

Figure 1: Cisco Unified Computing System Architecture



Architectural Simplification

The simplified architecture of Cisco UCS reduces the number of required devices and centralizes switching resources. By eliminating switching inside a chassis, network access-layer fragmentation is significantly reduced. Cisco UCS implements Cisco unified fabric within racks and groups of racks, supporting Ethernet and Fibre Channel protocols over 10 Gigabit Cisco Data Center Ethernet and Fibre Channel over Ethernet (FCoE) links. This radical simplification reduces the number of switches, cables, adapters, and management points by up to two-thirds. All devices in a Cisco UCS domain remain under a single management domain, which remains highly available through the use of redundant components.

High Availability

The management and data plane of Cisco UCS is designed for high availability and redundant access layer fabric interconnects. In addition, Cisco UCS supports existing high availability and disaster recovery solutions for the data center, such as data replication and application-level clustering technologies.

Scalability

A single Cisco UCS domain supports multiple chassis and their servers, all of which are administered through one Cisco UCS Manager. For more detailed information about the scalability, speak to your Cisco representative.

Flexibility

A Cisco UCS domain allows you to quickly align computing resources in the data center with rapidly changing business requirements. This built-in flexibility is determined by whether you choose to fully implement the stateless computing feature. Pools of servers and other system resources can be applied as necessary to respond to workload fluctuations, support new applications, scale existing software and business services, and accommodate both scheduled and unscheduled downtime. Server identity can be abstracted into a mobile service profile that can be moved from server to server with minimal downtime and no need for additional network configuration.

With this level of flexibility, you can quickly and easily scale server capacity without having to change the server identity or reconfigure the server, LAN, or SAN. During a maintenance window, you can quickly do the following:

- Deploy new servers to meet unexpected workload demand and rebalance resources and traffic.
- Shut down an application, such as a database management system, on one server and then boot it up again on another server with increased I/O capacity and memory resources.

Optimized for Server Virtualization

Cisco UCS has been optimized to implement VM-FEX technology. This technology provides improved support for server virtualization, including better policy-based configuration and security, conformance with a company's operational model, and accommodation for VMware's VMotion.

Cisco UCS Building Blocks and Connectivity

Figure 2: Cisco UCS Building Blocks and Connectivity

As shown in the figure above, the primary components included within Cisco UCS are as follows:

- **Cisco UCS Manager**—Cisco UCS Manager is the centralized management interface for Cisco UCS. For more information on Cisco UCS Manager, see *Introduction to Cisco UCS manager* in *Cisco UCS Manager Getting Started Guide*
- **Cisco UCS Fabric Interconnects**—The Cisco UCS Fabric Interconnect is the core component of Cisco UCS deployments, providing both network connectivity and management capabilities for the Cisco UCS system. The Cisco UCS Fabric Interconnects run the Cisco UCS Manager control software and consist of the following components:
  - Cisco UCS 6200 series Fabric Interconnects, Cisco UCS 6332 series Fabric Interconnects, and Cisco UCS Mini
  - Transreceivers for network and storage connectivity
  - Expansion modules for the various Fabric Interconnects
  - Cisco UCS Manager software

  For more information on Cisco UCS Fabric Interconnects, see Cisco UCS Fabric Infrastructure Portfolio, on page 6.

- **Cisco UCS I/O Modules and Cisco UCS Fabric Extender**—IOM modules are also known as Cisco FEXs or simply FEX modules. These modules serve as line cards to the FIs in the same way that Nexus series switches can have remote line cards. IOM modules also provide interface connections to blade servers. They multiplex data from blade servers and provide this data to FIs and do the same in the reverse direction. In production environments, IOM modules are always used in pairs to provide redundancy and failover.

Important The 40G backplane setting is not applicable for 22xx IOMs.

- **Cisco UCS Blade Server Chassis**—The Cisco UCS 5100 Series Blade Server Chassis is a crucial building block of Cisco UCS, delivering a scalable and flexible architecture for current and future data center needs, while helping reduce total cost of ownership.
- **Cisco UCS Blade and Rack Servers**—Cisco UCS Blade servers are at the heart of the UCS solution. They come in various system resource configurations in terms of CPU, memory, and hard disk capacity. All blade servers are based on Intel Xeon processors. There is no AMD option available. The Cisco UCS rack-mount servers are standalone servers that can be installed and controlled individually. Cisco provides Fabric Extenders (FEXs) for the rack-mount servers. FEXs can be used to connect and manage rack-mount servers from FIs. Rack-mount servers can also be directly attached to the fabric interconnect.

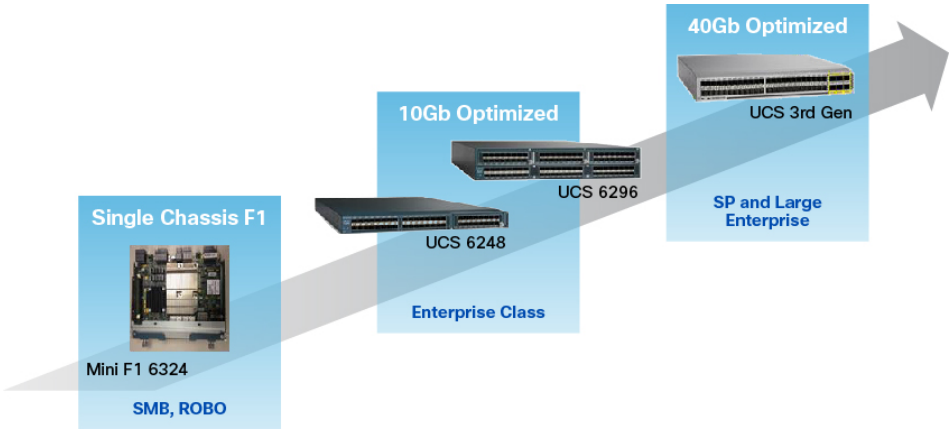
  Small and Medium Businesses (SMBs) can choose from different blade configurations as per business needs

- **Cisco UCS I/O Adapters**—Cisco UCS B-Series Blade Servers are designed to support up to two network adapters. This design can reduce the number of adapters, cables, and access-layer switches by as much as half because it eliminates the need for multiple parallel infrastructure for both LAN and SAN at the server, chassis, and rack levels.

Cisco UCS Fabric Infrastructure Portfolio

The Cisco UCS fabric interconnects are top-of-rack devices and provide unified access to the Cisco UCS domain. The following illustration shows the evolution of the Cisco UCS fabric interconnects product family. The Cisco UCS Infrastructure hardware is now in its third generation.

Note The Cisco UCS 6100 Series Fabric Interconnects and Cisco UCS 2104 I/O Modules have reached end of life.



Expansion Modules

The Cisco UCS 6200 Series supports expansion modules that can be used to increase the number of 10G, FCoE, and Fibre Channel ports.

- The Cisco UCS 6248 UP has 32 ports on the base system. It can be upgraded with one expansion module providing an additional 16 ports.
- The Cisco UCS 6296 UP has 48 ports on the base system. It can be upgraded with three expansion modules providing an additional 48 ports.

Ports on the Cisco UCS 6300 Series Fabric Interconnects

Ports on the Cisco UCS 6300 Series Fabric Interconnects can be configured to carry either Ethernet or Fibre Channel traffic. These ports are not reserved. They cannot be used by a Cisco UCS domain until you configure them.

Note When you configure a port on a fabric interconnect, the administrative state is automatically set to enabled. If the port is connected to another device, this may cause traffic disruption. You can disable the port after it has been configured.

The following table summarizes the second and third generation ports for the Cisco UCS fabric interconnects.

	Cisco UCS Mini	**Second Generation**		**Third Generation**	
Item	Cisco UCS 6324	Cisco UCS 6248 UP	Cisco UCS 6296 UP	Cisco UCS 6332	Cisco UCS 6332-16UP
Description	Fabric Interconnect with 4 unified ports and 1 scalability port	48–Port Fabric Interconnect	96–Port Fabric Interconnect	32–Port Fabric Interconnect	40–Port Fabric Interconnect
Form factor	1 RU	1 RU	2 RU	1 RU	1 RU
Number of fixed 40 GB Interfaces	—	—	—	6(Ports 17–32)	6(Ports 35–40)
Number of 1GB/10GB Interfaces (depending on the SFP module installed)	All	All	All	Ports 5–26 using breakout cable	Ports 17–34 using breakout cable
Unified Ports (8 Gb/s, FC, FCoE)	4	All	All	None	Ports 1–16
Compatibility with all IOMs	All	All	All	All	All

	Cisco UCS Mini	Second Generation		Third Generation	
Expansion Slots	None	1 (16 port)	3 (16 port)	None	None
Fan Modules	4	2	5	4	4
Power Supplies	—	2 (AC/DC available)	2 (AC/DC available)	2 (AC/DC available)	2 (AC/DC available)

Note Cisco UCS 6300 Series Fabric Interconnects support breakout capability for ports. For more information on how the 40G ports can be converted into four 10G ports, see Port Breakout Functionality on Cisco UCS 6300 Series Fabric Interconnects, on page 9.

Port Modes

The port mode determines whether a unified port on the fabric interconnect is configured to carry Ethernet or Fibre Channel traffic. You configure the port mode in Cisco UCS Manager. However, the fabric interconnect does not automatically discover the port mode.

Changing the port mode deletes the existing port configuration and replaces it with a new logical port. Any objects associated with that port configuration, such as VLANs and VSANS, are also removed. There is no restriction on the number of times you can change the port mode for a unified port.

Port Types

The port type defines the type of traffic carried over a unified port connection.

By default, unified ports changed to Ethernet port mode are set to the Ethernet uplink port type. Unified ports changed to Fibre Channel port mode are set to the Fibre Channel uplink port type. You cannot unconfigure Fibre Channel ports.

Changing the port type does not require a reboot.

Ethernet Port Mode

When you set the port mode to Ethernet, you can configure the following port types:

- Server ports
- Ethernet uplink ports
- Ethernet port channel members
- FCoE ports
- Appliance ports
- Appliance port channel members
- SPAN destination ports
- SPAN source ports

Note For SPAN source ports, configure one of the port types and then configure the port as SPAN source.

Fibre Channel Port Mode

When you set the port mode to Fibre Channel, you can configure the following port types:

- Fibre Channel uplink ports
- Fibre Channel port channel members
- Fibre Channel storage ports
- FCoE Uplink ports
- SPAN source ports

Note For SPAN source ports, configure one of the port types and then configure the port as SPAN source.

Port Breakout Functionality on Cisco UCS 6300 Series Fabric Interconnects

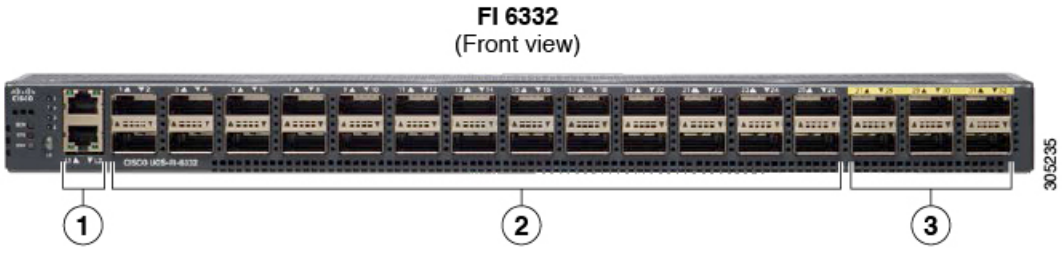
About Breakout Ports

Cisco UCS fabric interconnect 6300 series supports splitting a single QSFP port into four 10G ports using a supported breakout cable. By default, there are 32 ports in the 40G mode. These 40G ports are numbered in a 2-tuple naming convention. For example, the second 40G port is numbered as 1/2. The process of changing the configuration from 40G to 10G is called breakout and the process of changing the configuration from [4X]10G to 40G is called unconfigure.

When you break out a 40G port into 10G ports, the resulting ports are numbered using a 3-tuple naming convention. For example, the breakout ports of the second 40-Gigabit Ethernet port are numbered as 1/2/1, 1/2/2, 1/2/3, 1/2/4.

The following image shows the front view for the Cisco UCS 6332 series fabric interconnects, and includes the ports that may support breakout port functionality:

Figure 3: Cisco UCS 6332 Series Fabric Interconnects Front View

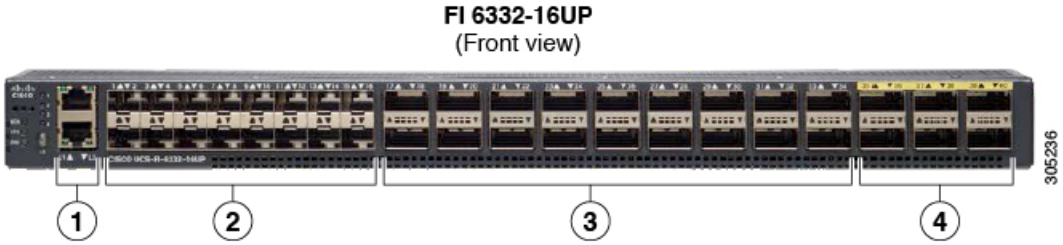


1	L1 and L2 high availability ports

2	28 X 40G QSFP ports (98 X 10G SFP ports) **Note** • QSA module is required on ports 13–14 • A QSFP to 4XSFP breakout cable is required for 10G support.
3	6 X 40G QSFP ports

The following image shows the front view for the Cisco UCS 6332-16UP series fabric interconnects, and includes the ports that may support breakout port functionality:

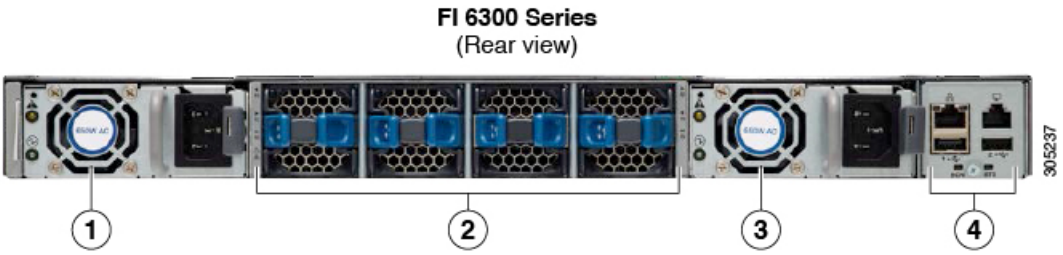
Figure 4: Cisco UCS 6332-16UP Series Fabric Interconnects Front View



1	L1 and L2 high availability ports
2	16 X 1/10G SFP (16 X 4/8/16G FC ports)
3	18 X 40G QSFP(72 X 10G SFP+) **Note** • A QSFP to 4XSFP breakout cable is required for 10G support.
4	6 X 40G QSFP ports

The following image shows the rear view of the Cisco UCS 6300 series fabric interconnects.

Figure 5: Cisco UCS 6300 Series Fabric Interconnects Rear View



1	Power supply
2	Four fans
3	Power supply
4	Serial ports

Breakout Port Constraints

The following table summarizes the constraints for breakout functionality for Cisco UCS 6300 series fabric interconnects:

Cisco UCS 6300 Series Fabric Interconnect Series	Breakout Configurable Ports	Ports without breakout functionality support
Cisco UCS 6332	1–12, 15–26	13–14, 27–32 **Note** • Auto-negotiate behavior is not supported on ports 27–32.
Cisco UCS 6332-16UP	17–34	1–16, 35–40 **Note** • Auto-negotiate behavior is not supported on ports 35–40

Important Up to four breakout ports are allowed if QoS jumbo frames are used.

For more information on how to configure breakout ports see the *Cisco UCS Manager Network Management Guide*.

Introduction to Cisco UCS Manager

Cisco UCS Manager is embedded software that resides on the fabric interconnects, providing complete configuration and management capabilities for all of the components in the Cisco UCS system. This configuration information is replicated between the two fabric interconnects, providing a highly available solution for this critical function. The most common way to access Cisco UCS Manager for simple tasks is to use a Web browser. A command-line interface (CLI) and an XML API are also included for command-line or programmatic operations.

The Cisco UCS Manager GUI provides role-based access control (RBAC) to allow multiple levels of users administrative rights to system objects. Users can be restricted to certain portions of the system based on locale, which corresponds to an optional organizational structure that can be created. Users can also be classified based on their access levels or areas of expertise, such as Storage Administrator, Server Equipment Administrator, or Read-Only.

Cisco UCS Manager provides unified, embedded management of all software and hardware components. Every instance of Cisco UCS Manager and all of the components managed by it form a domain. For organizations that deploy multiple Cisco UCS domains, Cisco UCS Central software provides a centralized user interface that allows you to manage multiple, globally distributed Cisco UCS domains with thousands of servers. Cisco UCS Central integrates with Cisco UCS Manager and utilizes it to provide global configuration capabilities for pools, policies, and firmware.

Configuration Options

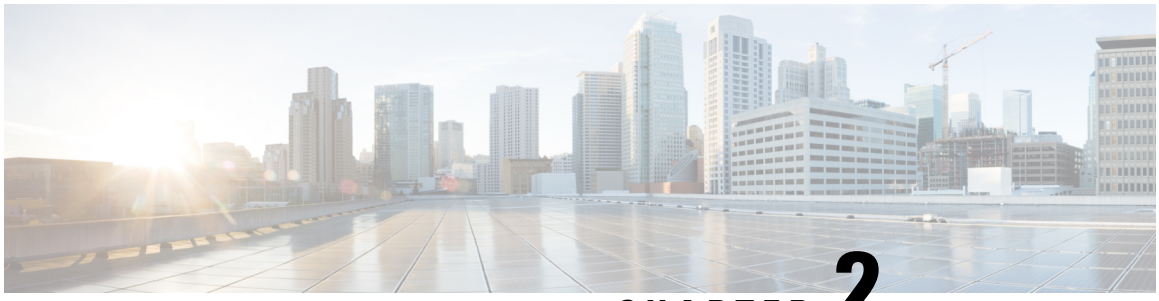
You can configure a Cisco UCS domain in the following ways:

- As a single fabric interconnect in a standalone configuration
- As a redundant pair of fabric interconnects in a cluster configuration

A cluster configuration provides high availability. If one fabric interconnect becomes unavailable, the other takes over. Only one management port (Mgmt0) connection is required to support a cluster configuration. However, both Mgmt0 ports should be connected to provide link-level redundancy. In a cluster configuration, the master and slave slots are indentified as primary and subordinate.

In addition, a cluster configuration actively enhances failover recovery time for redundant virtual interface (VIF) connections. When an adapter has an active VIF connection to one fabric interconnect and a standby VIF connection to the second, the learned MAC addresses of the active VIF are replicated but not installed on the second fabric interconnect. If the active VIF fails, the second fabric interconnect installs the replicated MAC addresses and broadcasts them to the network through gratuitous ARP messages, shortening the switchover time.

Note The cluster configuration provides redundancy only for the management plane. Data redundancy is dependent on the user configuration and might require a third-party tool to support data redundancy.



CHAPTER 2

System Requirements

System Requirements Overview

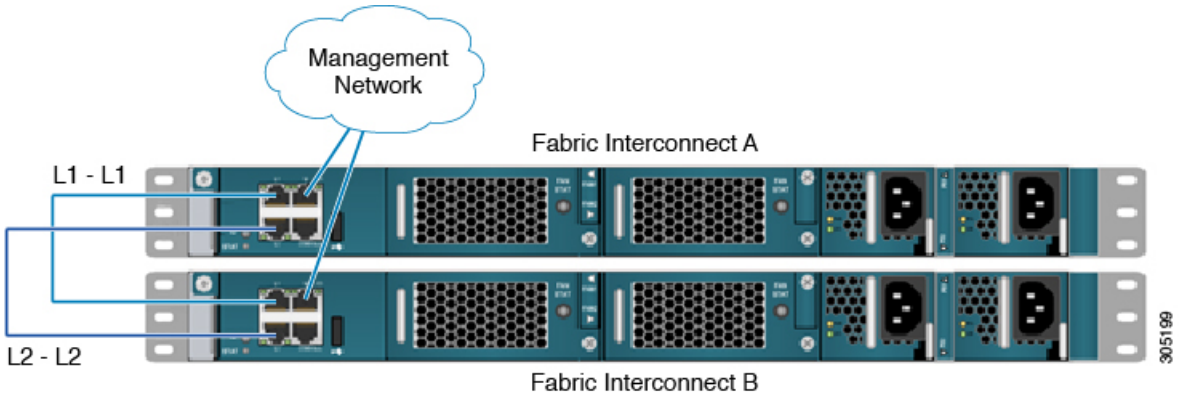
The following minimum hardware, browser, and port requirements must be met prior to Cisco UCS Manager initial configuration.

Hardware Requirements

Before you set up Cisco UCS Manager, make sure that the following physical cabling requirements are met:

Note The Cisco UCS Fabric Interconnects act as the concentration point for all cabling to and from the Blade Server Chassis. The following diagram shows the Cisco UCS Fabric Interconnects Cluster Connectivity.

Figure 6: Cisco UCS Fabric Interconnects Physical Cable Connectivity



- Connect the two fabric interconnects using the integrated ports labeled L1 and L2. These ports are used for replication of cluster information between the two fabric interconnects, not for the forwarding of data traffic.
- The management Ethernet ports of each fabric interconnect to the out-of-band Ethernet management network or Ethernet segment where they can be accessed for overall administration of the system.
- Populate each blade chassis with two fabric extenders (I/O modules) to provide connectivity back to the fabric interconnects.
- From the Blade Server Chassis, connect one I/O module to the first fabric interconnect. Connect the second I/O module to the second fabric interconnect. After you have configured the fabric interconnects, they will be designated as "A" and "B" fabric interconnects.

Note You can connect the I/O modules to the fabric interconnects by using one, two, four, or eight cables per module. For system resiliency and throughput, it is recommended that you use a minimum of two connections per I/O module

Browser Requirements

To use Cisco UCS Manager your computer must meet or exceed the following minimum browser requirements:

- Cisco UCS Manager uses web start and supports the following web browsers:
  - Microsoft Internet Explorer 11 or higher
  - Mozilla Firefox 45 or higher
  - Google Chrome 57 or higher
  - Apple Safari version 9 or higher
  - Opera version 35 or higher

Important HTML-5 UI supports one user session per browser.

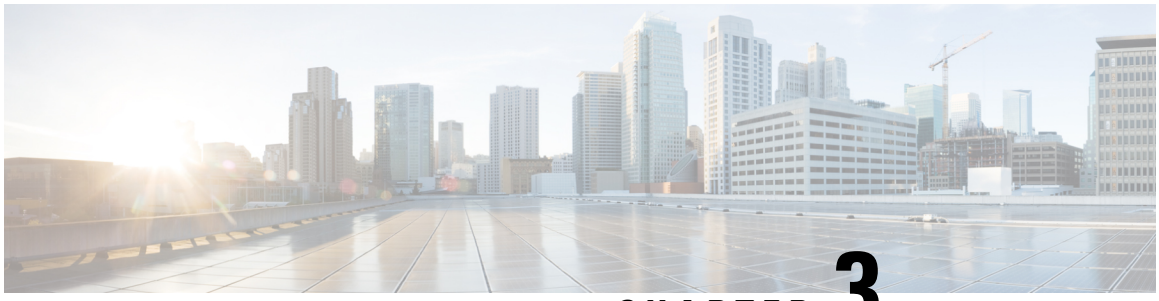
Port Requirements

Hardware and Software Requirements

Cisco UCS 6332 and Cisco UCS 6332-16UP ports are supported on the Cisco UCS 6300 Series Fabric Interconnects with Cisco UCS Manager 3.1 and later releases.

Port Channel Requirements

The ports with the same speed can be configured in a port channel. A port channel cannot have both breakout and regular ports due to the difference in the speed.



CHAPTER 3

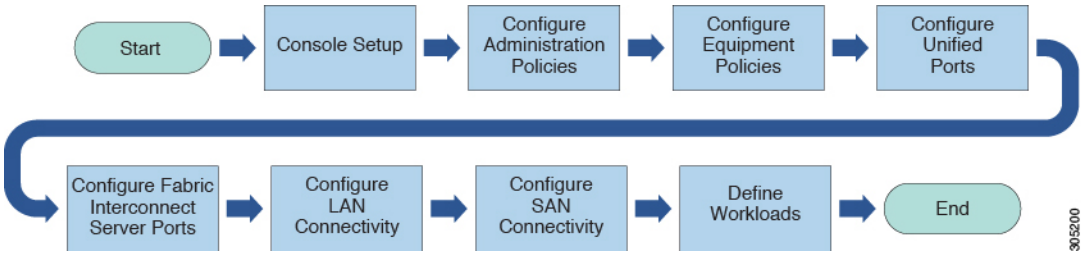
Initial Configuration

Initial Configuration Overview

Before you get started with Cisco UCS Manager initial configuration, review the *Fundamentals of Cisco Unified Computing System* and *System Requirements* sections in this guide.

The Cisco UCS Manager initial configuration involves the following steps:

Figure 7: Cisco UCS Manager Initial Configuration Overview



1. **Console Setup**—This step involves launching Cisco UCS Manager using the serial console. The Fabric Interconnect runs an initial configuration wizard and assigns three IP addresses in the management and administrative subnet: one for each Fabric Interconnect and one for the virtual IP interface that defines the Cisco UCS Manager instance and enables management. For more information on this step, see Console Setup, on page 18

2. **Configure Administration Policies**—This step involves configuration of administration policies, such as DNS Server, NTP, and Time Zone, that are necessary for proper functioning of all components. For more information on this step, see Configure Administration Policies, on page 26.

3. **Configure Equipment Policies**—This step involves performing chassis discovery by setting the equipment policies in Cisco UCS Manager. The Chassis Discovery Policy specifies the minimum number of connections between the I/O modules and the Fabric Interconnects. This value must be set explicitly. For more information on this step, see Configure Equipment Policies, on page 27
4. **Configure Unified Ports**—This step involves configuring Unified Ports on the primary and subordinate Fabric Interconnects.Configure Unified Ports, on page 27
5. **Configure Fabric Interconnect Server Ports**—This step involves configuring Fabric Interconnect Server Ports. For more information on this step, see Configure Fabric Interconnect Server Ports, on page 27
6. **Configure LAN Connectivity**—This step involves establishing initial LAN connectivity from Fabric Interconnects. For more information on this step, see Configure LAN Connectivity, on page 28.
7. **Configure SAN Connectivity**—This step involves establishing initial SAN connectivity from Fabric Interconnects. For more information on this step, see Configure SAN Connectivity, on page 28
8. **Define Workloads**—After completing initial configuration, you can define your workloads. For more information on this step, see Define Workloads, on page 28.

Console Setup

Initial configuration of Cisco UCS Fabric Interconnects is performed using the console connection. It is essential to maintain symmetric Cisco UCS Manager versions between the fabric interconnects in a domain. Refer to the latest *Cisco UCS Manager Release Notes*, and *Firmware Management guide* to determine the supported firmware versions.

Before you begin

Collect the following required information for the console setup:

- System name
- Password for the admin account. Choose a strong password that meets the guidelines for Cisco UCS Manager passwords. The password field cannot be blank.
- Management port IPv4 and subnet mask, or IPv6 address and prefix.
- Default gateway IPv4 or IPv6 address.
- DNS server IPv4 or IPv6 address (optional).
- Domain name for the system (optional).

Installation method

You can set up Cisco UCS Manager via GUI or CLI.

Installation Method	See
GUI	Configure the Primary Fabric Interconnect Using GUI, on page 19
CLI	Configure the Primary Fabric Interconnect Using CLI, on page 22

Configure Fabric Interconnects

Initial configuration of fabric interconnects is performed using the console connection. It is essential to maintain symmetric Cisco UCS Manager versions between the fabric interconnects in a domain. Refer to the latest *Cisco UCS Manager Release Notes*, and *Firmware Management guide* to determine the supported firmware versions.

Configure the Primary Fabric Interconnect Using GUI

You can either follow the procedure below for configuring the primary fabric interconnect or watch Cisco UCS Manager Initial Setup part 1.

Procedure

Step 1 Power up the fabric interconnect.
You will see the power on self-test messages as the fabric interconnect boots.

Step 2 If the system obtains a lease, go to step 6, otherwise, continue to the next step.

Step 3 Connect to the console port.

Step 4 At the installation method prompt, enter **gui**.

Step 5 If the system cannot access a DHCP server, you are prompted to enter the following information:

- IPv4 or IPv6 address for the management port on the fabric interconnect.
- IPv4 subnet mask or IPv6 prefix for the management port on the fabric interconnect.
- IPv4 or IPv6 address for the default gateway assigned to the fabric interconnect.

Note In a cluster configuration, both fabric interconnects must be assigned the same management interface address type during setup.

Step 6 Copy the web link from the prompt into a web browser and go to the Cisco UCS Manager GUI launch page.

Step 7 On the Cisco UCS Manager GUI launch page, select **Express Setup**.

Step 8 On the **Express Setup** page, select **Initial Setup** and click **Submit**.

Step 9 In the **Cluster and Fabric Setup** area:

a) Click the **Enable Clustering** option.
b) For the **Fabric Setup** option, select **Fabric A**.
c) In the **Cluster IP Address** field, enter the IPv4 or IPv6 address that Cisco UCS Manager will use.

Step 10 In the **System Setup** area, complete the following fields:

Field	Description
System Name	The name assigned to the Cisco UCS domain. In a standalone configuration, the system adds "-A" to the system name. In a cluster configuration, the system adds "-A" to the fabric interconnect assigned to fabric A, and "-B" to the fabric interconnect assigned to fabric B.

Field	Description
Admin Password	The password used for the Admin account on the fabric interconnect. Choose a strong password that meets the guidelines for Cisco UCS Manager passwords. This password cannot be blank.
Confirm Admin Password	The password used for the Admin account on the fabric interconnect.
Mgmt IP Address	The static IPv4 or IPv6 address for the management port on the fabric interconnect.
Mgmt IP Netmask or **Mgmt IP Prefix**	The IPv4 subnet mask or IPv6 prefix for the management port on the fabric interconnect. **Note** The system prompts for a **Mgmt IP Netmask** or a **Mgmt IP Prefix** based on what address type you entered in the **Mgmt IP Address** .
Default Gateway	The IPv4 or IPv6 address for the default gateway assigned to the management port on the fabric interconnect. **Note** The system prompts for a **Default Gateway** address type based on what type you entered in the **Mgmt IP Address** field.
DNS Server IP	The IPv4 or IPv6 address for the DNS Server assigned to the fabric interconnect.
Domain Name	The name of the domain in which the fabric interconnect resides.

Step 11 Click **Submit**.
A page displays the results of your setup operation.

Configure the Subordinate Fabric Interconnect Using GUI

You can either follow the procedure below for configuring the subordinate fabric interconnect or watch Cisco UCS Manager Initial Setup part 2.

Note When adding a new Fabric Interconnect to an existing High Availability cluster, for example, during a new install or when replacing a Fabric Interconnect, the new device will not be able to log into the cluster as long as the authentication method is set to remote. To successfully add a new Fabric Interconnect to the cluster, the authentication method must be temporarily set to local and the local admin credentials of the primary Fabric Interconnect must be used.

Procedure

Step 1 Power up the fabric interconnect.
You will see the power-up self-test message as the fabric interconnect boots.

Step 2 It the system obtains a lease, go to step 6, otherwise, continue to the next step.

Step 3 Connect to the console port.

Step 4 At the installation method prompt, enter **`gui`**.

Step 5 If the system cannot access a DHCP server, you are prompted to enter the following information:

- IPv4 or IPv6 address for the management port on the fabric interconnect
- IPv4 subnet mask or IPv6 prefix for the management port on the fabric interconnect
- IPv4 or IPv6 address for the default gateway assigned to the fabric interconnect

Note In a cluster configuration, both fabric interconnects must be assigned the same management interface address type during setup.

Step 6 Copy the web link from the prompt into a web browser and go to the Cisco UCS Manager GUI launch page.

Step 7 On the Cisco UCS Manager GUI launch page, select **Express Setup**.

Step 8 On the **Express Setup** page, select **Initial Setup** and click **Submit**.

The fabric interconnect should detect the configuration information for the first fabric interconnect.

Step 9 In the **Cluster and Fabric Setup** Area:

a) Select the **Enable Clustering** option.
b) For the **Fabric Setup** option, make sure **Fabric B** is selected.

Step 10 In the **System Setup** Area, enter the password for the Admin account into the **Admin Password of Master** field.
The **Manager Initial Setup** Area is displayed.

Step 11 In the **Manager Initial Setup** Area, the field that is displayed depends on whether you configured the first fabric interconnect with an IPv4 or IPv6 management address. Complete the field that is appropriate for your configuration, as follows:

Field	Description
Peer FI is IPv4 Cluster enabled. Please Provide Local fabric interconnect Mgmt0 IPv4 Address	Enter an IPv4 address for the Mgmt0 interface on the local fabric interconnect.
Peer FI is IPv6 Cluster Enabled. Please Provide Local fabric interconnect Mgmt0 IPv6 Address	Enter an IPv6 for the Mgmt0 interface on the local fabric interconnect.

Step 12 Click **Submit**.

A page displays the results of your setup operation.

Configure the Primary Fabric Interconnect Using CLI

Procedure

Step 1 Connect to the console port.

Step 2 Power up the Fabric Interconnect.
You will see the power-up self-test messages as the Fabric Interconnect boots.

Step 3 When the unconfigured system boots, it prompts you for the setup method to be used. Enter **console** to continue the initial setup using the console CLI.

Step 4 Enter **setup** to continue as an initial system setup.

Step 5 Enter **y** to confirm that you want to continue the initial setup.

Step 6 Enter the password for the admin account.

Step 7 To confirm, re-enter the password for the admin account.

Step 8 Enter **yes** to continue the initial setup for a cluster configuration.

Step 9 Enter the Fabric Interconnect fabric (either **A** or **B**).

Step 10 Enter the system name.

Step 11 Enter the IPv4 or IPv6 address for the management port of the Fabric Interconnect.

If you enter an IPv4 address, you will be prompted to enter an IPv4 subnet mask. If you enter an IPv6 address, you will be prompted to enter an IPv6 network prefix.

Step 12 Enter the respective IPv4 subnet mask or IPv6 network prefix, then press **Enter**.

You are prompted for an IPv4 or IPv6 address for the default gateway, depending on the address type you entered for the management port of the Fabric Interconnect.

Step 13 Enter either of the following:

- IPv4 address of the default gateway
- IPv6 address of the default gateway

Step 14 Enter **yes** if you want to specify the IP address for the DNS server, or **no** if you do not.

Step 15 (Optional) Enter the IPv4 or IPv6 address for the DNS server.

The address type must be the same as the address type of the management port of the Fabric Interconnect.

Step 16 Enter **yes** if you want to specify the default domain name, or **no** if you do not.

Step 17 (Optional) Enter the default domain name.

Step 18 Review the setup summary and enter **yes** to save and apply the settings, or enter **no** to go through the Setup wizard again to change some of the settings.

If you choose to go through the Setup wizard again, it provides the values you previously entered, and the values appear in brackets. To accept previously entered values, press **Enter**.

Example

The following example sets up the first Fabric Interconnect for a cluster configuration using the console and IPv4 management addresses:

```
Enter the installation method (console/gui)?  console
Enter the setup mode (restore from backup or initial setup) [restore/setup]? setup
You have chosen to setup a new switch.  Continue? (y/n): y
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
Do you want to create a new cluster on this switch (select 'no' for standalone setup or if
 you want this switch to be added to an existing cluster)? (yes/no) [n]: yes
Enter the switch fabric (A/B): A
Enter the system name: foo
Mgmt0 IPv4 address: 192.168.10.10
Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Virtual IPv4 address: 192.168.10.12
Configure the DNS Server IPv4 address? (yes/no) [n]: yes
  DNS IPv4 address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Join centralized management environment (UCS Central)? (yes/no) [n]: no
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Management IP Address=192.168.10.10
  Management IP Netmask=255.255.255.0
  Default Gateway=192.168.10.1
  Cluster Enabled=yes
  Virtual Ip Address=192.168.10.12
  DNS Server=20.10.20.10
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

The following example sets up the first Fabric Interconnect for a cluster configuration using the console and IPv6 management addresses:

```
Enter the installation method (console/gui)?  console
Enter the setup mode (restore from backup or initial setup) [restore/setup]? setup
You have chosen to setup a new switch.  Continue? (y/n): y
Enter the password for "admin": adminpassword%652
Confirm the password for "admin": adminpassword%652
Do you want to create a new cluster on this switch (select 'no' for standalone setup or if
 you want this switch to be added to an existing cluster)? (yes/no) [n]: yes
Enter the switch fabric (A/B): A
Enter the system name: foo
Mgmt0 address:  2001::107
Mgmt0 IPv6 prefix: 64
IPv6 address of the default gateway: 2001::1
Configure the DNS Server IPv6 address? (yes/no) [n]: yes
  DNS IP address: 2001::101
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Join centralized management environment (UCS Central)? (yes/no) [n]: no
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Enforced Strong Password=no
  Physical Switch Mgmt0 IPv6 Address=2001::107
  Physical Switch Mgmt0 IPv6 Prefix=64
```

```
  Default Gateway=2001::1
  Ipv6 value=1
  DNS Server=2001::101
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

Note Cisco UCS Fabric Interconnects contain several commands that are utilized for initial configuration of high availability and clustered configurations. The **cluster-start** command can be used during initial configuration. This command is a hidden command. However, it can be executed at anytime by an authenticated administrator such as a Cisco TAC administrator, and is not intended for configuration or maintenance use.

Configure the Subordinate Fabric Interconnect Using CLI

This procedure describes setting up the second fabric interconnect using IPv4 or IPv6 addresses for the management port.

Note When adding a new Fabric Interconnect to an existing High Availability cluster, for example, during a new install or when replacing a Fabric Interconnect, the new device will not be able to log into the cluster as long as the authentication method is set to remote. To successfully add a new Fabric Interconnect to the cluster, the authentication method must be temporarily set to local and the local admin credentials of the primary Fabric Interconnect must be used.

Procedure

Step 1 Connect to the console port.

Step 2 Power up the fabric interconnect.
You will see the power-on self-test messages as the fabric interconnect boots.

Step 3 When the unconfigured system boots, it prompts you for the setup method to be used. Enter **console** to continue the initial setup using the console CLI.

Note The fabric interconnect should detect the peer fabric interconnect in the cluster. If it does not, check the physical connections between the L1 and L2 ports, and verify that the peer fabric interconnect has been enabled for a cluster configuration.

Step 4 Enter **y** to add the subordinate fabric interconnect to the cluster.

Step 5 Enter the admin password of the peer fabric interconnect.

Step 6 Enter the IP address for the management port on the subordinate fabric interconnect.

Step 7 Review the setup summary and enter **yes** to save and apply the settings, or enter **no** to go through the Setup wizard again to change some of the settings.

If you choose to go through the Setup wizard again, it provides the values you previously entered, and the values appear in brackets. To accept previously entered values, press **Enter**.

Example

The following example sets up the second fabric interconnect for a cluster configuration using the console and the IPv4 address of the peer:

```
Enter the installation method (console/gui)? console
Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect
 will be added to the cluster. Continue (y/n) ? y
Enter the admin password of the peer Fabric Interconnect: adminpassword%958
Peer Fabric interconnect Mgmt0 IPv4 Address: 192.168.10.11
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

The following example sets up the second fabric interconnect for a cluster configuration using the console and the IPv6 address of the peer:

```
Enter the installation method (console/gui)? console
Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect
 will be added to the cluster. Continue (y/n) ? y
Enter the admin password of the peer Fabric Interconnect: adminpassword%958
Peer Fabric interconnect Mgmt0 IPv6 Address: 2001::107
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

Verify Console Setup

You can verify that both fabric interconnect configurations are complete by logging into the fabric interconnect via SSH and verifying the cluster status through CLI. For this procedure, you can watch Cisco UCS Manager Initial Setup part 3.

Use the following commands to verify the cluster state:

Command	Purpose	Sample Output

show cluster state	Displays the operational state and leadership role for both fabric interconnects in a high availability cluster.	The following example displays that both fabric interconnects are in the Up state, HA is in the Ready state, fabric interconnect A has the primary role, and fabric interconnect B has the subordinate role:
		`UCS-A# show cluster state`
		`Cluster Id:`
		`0x4432f72a371511de-0xb97c000de1b1ada4`
		
		`A: UP, PRIMARY`
		`B: UP,`
		`SUBORDINATE HA READY`

Command	Purpose	Sample Output

show cluster extended-state	Displays extended details about the cluster state and typically used when troubleshooting issues.	The following example shows how to view the extended state of a cluster:
		`UCSC# show cluster extended-state 0x2e95deadbd0f11e2-0x8ff35147e84f3de2Start time: Thu May 16 06:54:22 2013Last election time: Thu May 16 16:29:28 2015System Management Viewing the Cluster State A: UP, PRIMARY B: UP, SUBORDINATE`
		
		`A: memb state UP, lead state PRIMARY, mgmt services state: UP B: memb state UP, lead state SUBORDINATE, mgmt services state: UP heartbeat state PRIMARY_OK HA READY Detailed state of the device selected for HA quorum data: Device 1007, serial: a66b4c20-8692-11df-bd63-1b72ef3ac801, state: active Device 1010, serial: 00e3e6d0-8693-11df-9e10-0f4428357744, state: active Device 1012, serial: 1d8922c8-8693-11df-9133-89fa154e3fa1, state: active`

Configure Administration Policies

After completing initial configuration, configure global system administration settings such as faults, events, users, external directory services, communication services, and licensing.

Use the following table for specific guidance on how to configure various administration policies.

Task	See
Add DNS Servers	*Cisco UCS Manager Infrastructure Management Guide*
Time Zone Management	*Cisco UCS Manager Administration Management Guide*
Register with Cisco UCS Central	*Cisco UCS Manager Infrastructure Management Guide*
User Management	*Cisco UCS Manager Infrastructure Management Guide*

Task	See
Communications Management	*Cisco UCS Manager Administration Management Guide*
(Optional) Key Management	*Cisco UCS Manager Administration Management Guide*
License Management	*Cisco UCS Manager Administration Management Guide*

Configure Equipment Policies

After configuring administration policies, set equipment policies such as Chassis/FEX Discovery policy, Power Policy, MAC Address changing policy and SEL Policy.

Use the following table for specific guidance on how to configure various equipment policies.

Task	See
Configure global policies including Chassis/FEX Discovery Policy, Power Policy and Information Policy	*Cisco UCS Manager Infrastructure Management Guide*
Configure SEL Policy	*Cisco UCS Manager Administration Management Guide*

Configure Unified Ports

After configuring equipment policies, enable Unified Ports. It is recommended that you first configure Unified Ports on the Primary Fabric Interconnect, then on the Subordinate Fabric Interconnect.

Use the following table for specific guidance on how to configure Unified ports.

Task	See
Configure Unified Ports	*Cisco UCS Network Management Guide*

Configure Fabric Interconnect Server Ports

After configuring Unified Ports, enable Fabric Interconnect Server Ports.

Use the following table for specific guidance on how to configure fabric interconnect server ports.

Task	See
Configure Fabric Interconnect Server Ports **Note** Starting with Cisco UCS Manager release 3.1(3), you can automatically configure the fabric interconnect server ports.	*Cisco UCS Manager Network Management Guide*

Configure LAN Connectivity

After configuring Fabric Interconnect Server Ports, complete initial LAN connectivity by enabling Fabric Interconnect Ethernet Ports.

Use the following table for specific guidance on how to configure LAN connectivity.

Task	See
Configure Fabric Interconnect Ethernet Ports	*Cisco UCS Manager Network Management Guide*

Configure SAN Connectivity

After configuring LAN connectivity, complete initial SAN connectivity by enabling Fabric Interconnect FC Ports.

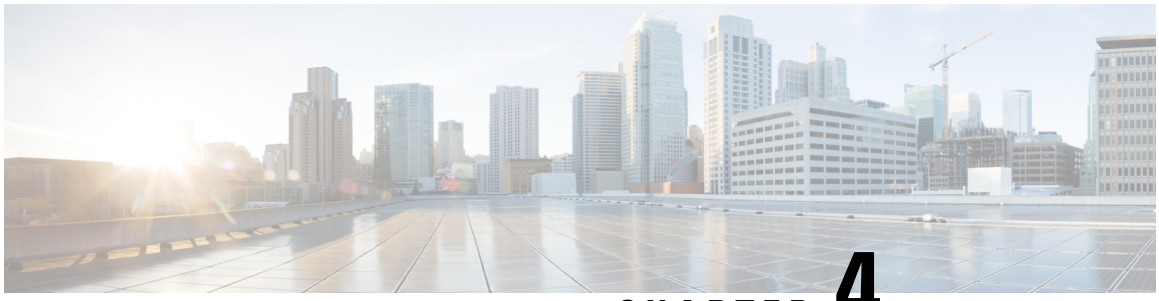
Use the following table for specific guidance on how to configure SAN connectivity.

Task	See
Configure Fabric Interconnect FC Ports	*Cisco UCS Manager Storage Management Guide*

Define Workloads

After completing Cisco UCS Manager initial configuration, use the following steps in the recommended order to define your workload:

Step	Description	See
Define organizational hierarchy	Cisco UCS organizational structure facilitates hierarchical configuration of Cisco UCS resources. An Organization can be created for policies, pools, and service profiles. The default Organization for any resource category is Root. Based on requirements, multiple sub-organizations can be created under the Root organization. You can create nested sub-organization under a sub-organization.	*Cisco UCS Manager Administration Management Guide*
Define Pools	Pools in Cisco UCS Manager are used for abstracting unique identities and resources for devices such as vNICs, vHBAs and server pools can assign servers in groups based on similar server characteristics.	*Cisco UCS Manager Network Management Guide*
Configure Adapters	Cisco UCS contains predefined adapter policies for most operating systems, including hypervisors. The settings in these predefined policies are for optimal adapter performance.	*Cisco UCS Manager Network Management Guide*
Configure Server Policies	Configuring Server Policies in Cisco UCS Manager includes Server-Related Policies such as BIOS Policy, Local Disk Configuration Policy, IPMI Access Profiles, and Server Autoconfiguration.	*Cisco UCS Manager Server Management Guide*
Configure Service Profile Templates	Cisco UCS Service Profile Templates are used to create multiple services profiles with similar characteristics.	*Cisco UCS Manager Server Management Guide*



CHAPTER 4

Appendix

Recommendations and Best Practices

Pools

Pools are the base building blocks for uniquely identifying hardware resources. As the basis for the UCS management model, they allow Service Profiles to be associated with any blade, while still providing the exact same ID and presentation to the upstream LAN or SAN. There are three sets of pools used as part of best practices:

- WWNN and WWPN pools: Provide unique IDs for Fibre Channel resources on a server (Fibre Channel nodes and ports).
- MAC address pools: Provide unique IDs for network interface ports.
- UUID pools: Provide IDs similar to a serial number or service tag.

In the Cisco UCS Manager GUI, these pools are all functionally organized, with UUID pools maintained from the Server tab, WWNN and WWPN pools maintained from the SAN tab, and MAC address pools maintained from the LAN tab.

Define and use Pools as a standard practice. Ensure the following:

- UUID pools are referenced when you create Service Profiles.
- MAC address pools are referenced when you create vNICs.
- WWNN pools are referenced when you create Service Profiles.
- WWPN pools are referenced when you create vHBAs.

Similarly, Pools should also be referenced when you create any corresponding template objects (vNICs, vHBAs, and Service Profiles). Trade-offs exist when considering pool management. There are two simple ways to manage pools: populate and use the default pools, or create domain-wide pools. This approach reduces the number of objects that need to be configured and managed. Alternatively, operators are free to configure

different pools on a per-tenant or per-application basis. This approach can provide more specific identity management and more granular traffic monitoring of tenants, applications.

Policies

Policies are a primary mechanism for enforcing rules, which helps ensure consistency and repeatability. Defining and using a comprehensive set of policies enables greater consistency, control, predictability and automation. The following sections contain various policy-related best practices.

Boot Policies

Boot Policy determines how a server boots, specifying the boot devices, the method, and the boot order.

The traditional use of SAN boot requires manual configuration for each server performing SAN boot. Typically, having 100 servers SAN-boot would require configuring 100 servers manually and individually. Cisco UCS inverts this unwieldy model, and instead requires configuring only in proportion to the number of storage arrays serving SAN-boot images, regardless of the number of servers doing SAN-boot. A single boot policy, with the WWPNs of a single storage array can be referenced and reused by any number of servers, without additional manual configuration.

Much of the Cisco UCS core value around availability is predicated on SAN boot. Therefore, the use of SAN boot within a Boot policy is a most highly recommended best practice to improve service availability.

Refer to the following best practices for boot policies:

- Have a CD-ROM as the first in the boot order, for emergencies and for booting in recovery mode.
- For SAN boot, define separate boot policies for each storage array that would be serving boot LUNs.
- For network boot, define the vNIC device as last in the boot order, following either SAN or local boot. This allows you to perform a network boot and installation, only if the OS was not previously been installed.

Host Firmware Policies

Use Host Firmware Policy to associate qualified or well-known versions of the BIOS, adapter ROM, or local disk controller with logical Service Profiles, as described earlier. A best practice is to create one policy, based on the latest packages that correspond with the Cisco UCS Manager infrastructure and server software release, and to reference that Host Firmware Package for all Service Profiles and templates created. This best practice will help ensure version consistency of a server's lowest-level firmware, regardless of physical server failures that may cause re-association of Service Profiles on other blades.

Maintenance Policies

Use the Maintenance Policy to specify how Cisco UCS Manager should proceed for configuration changes that will have a service impact or require a server reboot. Values for the Maintenance Policy can be "immediate," "userack," or "timer automatic". The best practice is to not use the "default" policy, and instead to create and use Maintenance Policies for either "user-ack" or "timer automatic", and to always have these as elements of the Service Profile or Service Profile Template definition.

Local Disk Policies

Local disk policy specifies how to configure any local disks on the blade. A best practice is to specify no local storage for SAN boot environments, thereby precluding any problems at Service Profile association time,

when local disks may present themselves to the host OS during installation. You can also remove or unseat local disks from blades completely, especially blades used for OS installation.

Scrub Policies

Scrub policy determines what happens to local disks and BIOS upon Service Profile disassociation. The default policy is no scrubbing. A best practice is to set the policy to scrub the local disk, especially for service providers, multi-tenant customers, and environments in which network installation to a local disk is used.

BIOS Policies

BIOS policy enables very specific control of CPU settings that are normally accessible only through the console during startup. For VMware and virtual environments that depend on CPU support for Intel Virtualization Technology, a corresponding policy can be created, removing any requirement for manual intervention during server provisioning. Similarly, applications that are sensitive to Intel Turbo Boost or Hyper-Threading can have dedicated BIOS policies referenced. Also, setting "Quiet Boot" to "disabled" allows diagnostic message visibility, which may be helpful in troubleshooting situations.

Templates

Refer to the following best practices for templates:

- In the Cisco UCS Manager GUI, use expert mode when creating Service Profile templates to achieve the optimal level of control and definition.
- When creating templates, reference the subordinate Pools and Policies that have been previously defined.

vNIC and vHBA Templates

Create reusable vNIC and vHBA templates in which termination is either reflected in the name (e.g., "fc0-A") or through well-accepted conventions (e.g., an even interface to A side, and an odd interface to B side). vNIC templates should be thought of as application-specific network profiles that include important security definitions, such as VLAN mappings.

Service Profile Templates

Use a Service Profile template as a definition for a class or type or version of an application, service, or operating system.

Monitoring

Cisco UCS provides the standard set of health and monitoring methods, such as syslog and Simple Network Management Protocol (SNMP) with its associated MIBs8 (get and fault traps only; no set). The best practice for Cisco UCS monitoring is to use existing methods and frameworks that are already familiar and well understood, such as SCOM, OpenView, or BPPM.

Network Availability

For network availability, either use hardware failover or use NIC teaming (or bonding), but do not use both concurrently. After a vNIC and vHBA template is defined, it can be referenced through expert-mode service-profile creation by selecting Use LAN (or SAN) Connectivity Template.

Best Practices for Installing ESXi 5.5 U2 Custom ISO to FlexFlash

Before installing the ESXi 5.5 U2 custom ISO to FlexFLash, scrub the FlexFlash drives to avoid any ISO installation issues.

Configuration Backup

The Cisco UCS configuration can be backed up easily and should be backed up regularly through the GUI or automated scripts. There are four types of backups:

Type	Description
Full State	Used for full system restore as part of disaster recovery.
System Configuration	Roles, Call Home, communication services and distributed virtual switch.
Logical Configuration	Service profiles, VLANs, VSANs, pools, policies and templates
All Configurations	Both Logical and System configurations

For the Logical Configuration and All Configurations backups, select the Cisco UCS Manager Preserve Identities feature to preserve the actual MAC address, WWN, and UUID values; otherwise, the backup references only the logical pool names, but not the actual identities. The following are configuration backup related best practices:

- Use the Preserve Identities feature when backing up individual domains for prescribed restoration (same site or domain or exact recovery site or domain).
- Do not use Preserve Identities when creating "gold UCSM domain configuration" templates.

Configuration Examples

Refer to Configuration Examples and TechNotes for Cisco UCS Manager configuration examples.

Glossary

AD

Active Directory. A distributed directory service.

adapter port channel

A channel that groups all the physical links from a Cisco UCS Virtual Interface Card (VIC) to an IOM into one logical link.

BIOS

Basic Input Output System. In a computer system, it performs the power up self-test procedure, searches, and loads to the Master Boot Record in the system booting process.

DNS

Domain Name System. An application layer protocol used throughout the Internet for translating hostnames into their associated IP addresses.

Dyname FCoE

The ability to overlay FCoE traffic across Spine-Leaf data center switching architecture. In its first instantiation, Dynamic FCoE allows running FCoE on top of Cisco FabricPath network in a converged fashion.

Ethernet Port

A generic term for the opening on the side of any Ethernet node, typically in an Ethernet NIC or LAN switch, into which an Ethernet cable can be connected.

Fabric port channel

Fibre Channel uplinks defined in a Cisco UCS Fabric Interconnect, bundled together and configured as a port channel, allowing increased bandwidth and redundancy.

FCoE

Fibre Channel over Ethernet. A computer network technology that encapsulates Fibre Channel frames over Ethernet networks. This allows Fibre Channel to use 10 Gigabit Ethernet networks (or higher speeds) while preserving the Fibre Channel protocol characteristics. The specification is part of the International Committee for Information Technology Standards T11 FC-BB-5 standard published in 2009. FCoE maps Fibre Channel directly over Ethernet while being independent of the Ethernet forwarding scheme.

Hypervisor

A software allowing multiple operating systems, known as guest operating systems, to share a single physical server. Guest operating systems run inside virtual machines and have fair scheduled access to underlying server physical resources.

IP address (IP version 4)

IP version 4 (IPv4), a 32-bit address assigned to hosts using TCP/IP. Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork.

IP address (IP version 6)

In IP version 6 (IPv6), a 128-bit address assigned to hosts using TCP/IP. Addresses use different formats, commonly using a routing prefix, subnet, and interface ID, corresponding to the IPv4 network, subnet, and host parts of an address.

KVM

Keyboard, video, and mouse

LAN

Logical Area Network. A computer network that interconnects computers within a limited area, such as a home, school, computer laboratory, or office building, using network media. The defining characteristics

of LANs, in contrast to Wide-Area Networks (WANs), include their smaller geographic area and non-inclusion of leased telecommunication lines.

Logical unit number

Logical unit number. In computer storage, a number used to identify a logical unit, which is a device addressed by the SCSI protocol or protocols that encapsulate SCSI, such as Fibre Channel or iSCSI. A LUN may be used with any device that supports read/write operations, such as a tape drive, but is most often used to refer to a logical disk as created on a SAN.

MAC address

A standardized data link layer address that is required for every device that connects to a LAN. Ethernet MAC addresses are 6 bytes long and are controlled by the IEEE.

out-of-band

A storage virtualization method that provides separate paths for data and control, presenting an image of virtual storage to the host by one link and allowing the host to directly retrieve data blocks from physical storage on another.