Overview

This chapter includes the following sections:

Overview

Cisco UCS uses firmware obtained from and certified by Cisco to support the endpoints in a Cisco UCS domain. Each endpoint is a component in the Cisco UCS domain, and requires firmware to function.

This guide explains how to obtain firmware and upgrade the endpoints in a Cisco UCS domain by using Cisco UCS Manager. It also details the best practices to be followed while upgrading these endpoints.

Cisco UCS Manager Release 4.1(1) introduces the Cisco UCS 64108 Fabric Interconnect to Cisco UCS 6400 Series Fabric Interconnects. Cisco releases unified Cisco UCS Manager software and firmware upgrades for each of the following platforms with every release of Cisco UCS Manager:

- Cisco UCS 6400 Series Fabric Interconnect with Cisco UCS B-Series, and C-Series servers
- Cisco UCS 6300 Series Fabric Interconnect with Cisco UCS B-Series, and C-Series servers
- Cisco UCS 6200 Series Fabric Interconnect with Cisco UCS B-Series, and C-Series servers
- Cisco UCS 6324 Fabric Interconnect with Cisco UCS B-Series Servers and C-Series servers, which is also known as UCS Mini

Figure 1: Cisco UCS 6400 Series Fabric Interconnect with Cisco UCS B-Series and C-Series servers

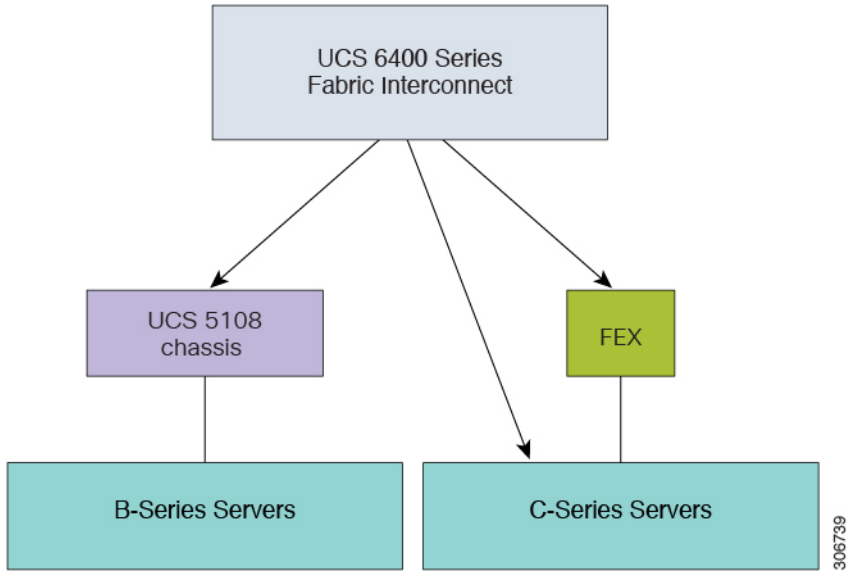


Figure 2: Cisco UCS 6300 Series Fabric Interconnect with Cisco UCS B-Series and C-Series servers

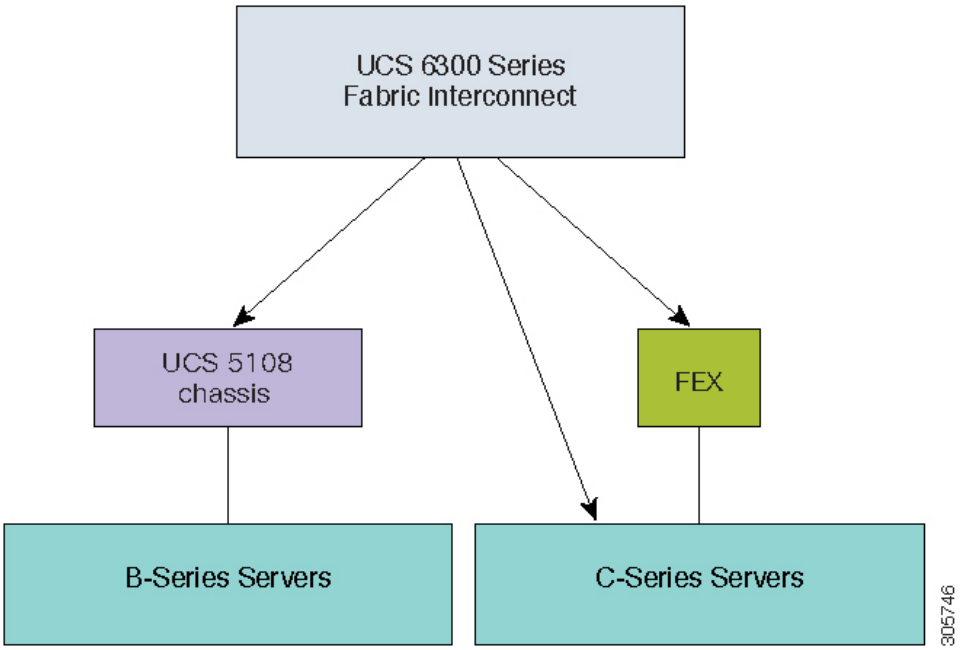


Figure 3: Cisco UCS 6200 Series Fabric Interconnect with Cisco UCS B-Series, and C-Series servers

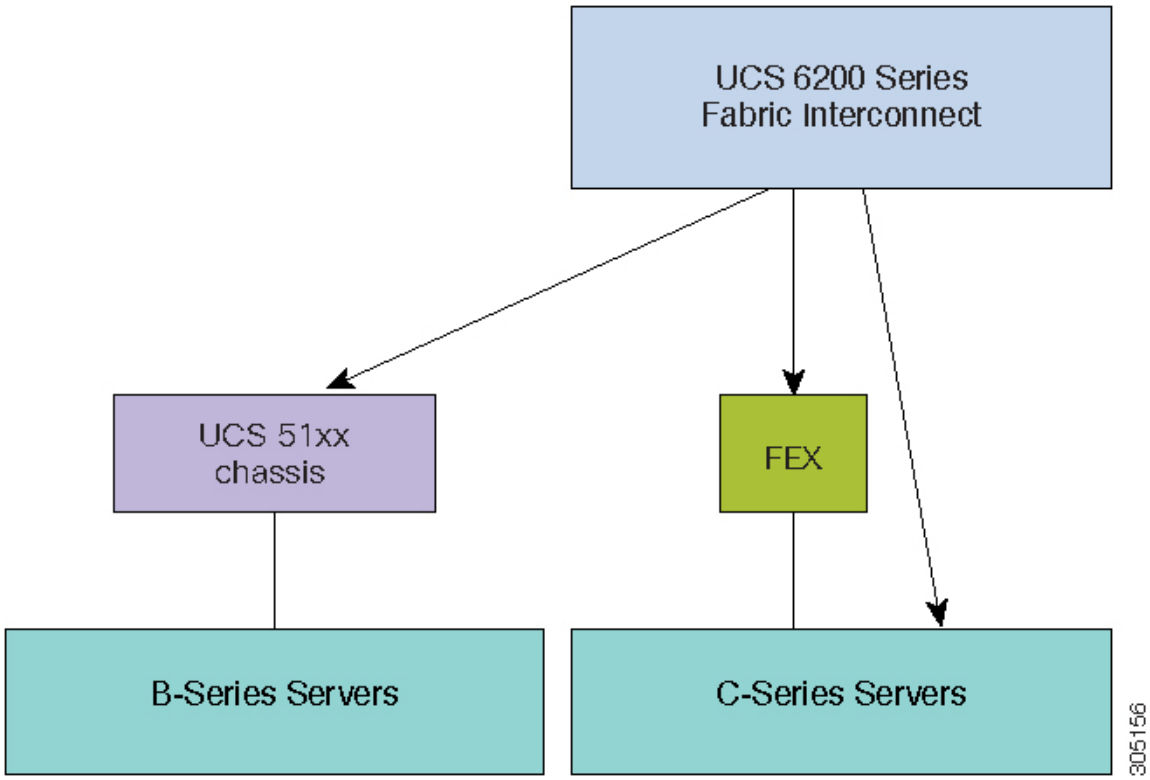
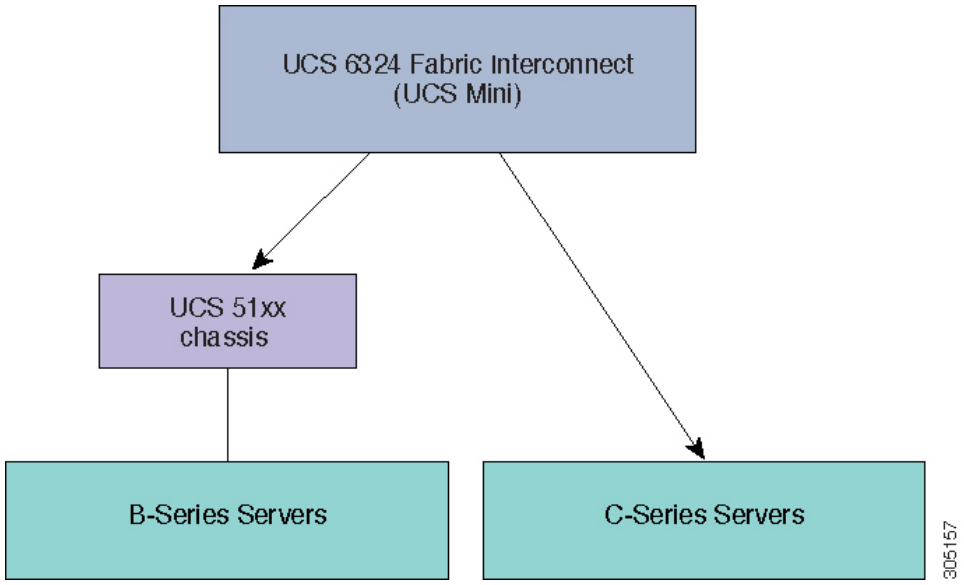


Figure 4: Cisco UCS 6324 Fabric Interconnect with Cisco UCS B-Series Servers and C-Series servers



These figures illustrate the various platforms and the firmware bundles supported by Cisco UCS Manager Release 4.1.

Each release has the following firmware bundles:

- Infrastructure software bundle—This bundle is also called the A bundle. It contains the firmware images that the fabric interconnects, IO Modules, and Cisco UCS Manager require to function.

  Cisco UCS Manager 4.1 and later releases contain three separate infrastructure bundles:

  - Cisco UCS 6400 Series Fabric Interconnect—ucs-6400-k9-bundle-infra.4.x.x.xxx.A.bin
  - Cisco UCS 6300 Series Fabric Interconnect—ucs-6300-k9-bundle-infra.4.x.x.xxx.A.bin
  - Cisco UCS 6200 Series Fabric Interconnect—ucs-k9-bundle-infra.4.x.x.xxx.A.bin
  - Cisco UCS 6324 Fabric Interconnect—ucs-mini-k9-bundle-infra.4.x.x.xxx.A.bin

- B-Series server software bundle—Also called the B bundle, this bundle contains the firmware images that the B-Series blade servers require to function, such as adapter, BIOS, CIMC, and board controller firmware. *Release Bundle Contents for Cisco UCS Manager*for the appropriate 4.x release provides details about the contents of the B-Series server software bundle.

Note Starting with Cisco UCS Manager Release 3.1(2), the firmware for endpoints that are common to both the B-Series and C-Series server software bundles, such as local disk, is available in both the B-Series and C-Series server software bundles.

- C-Series server software bundle—Also called the C bundle, this bundle contains the firmware images that the C-Series rack-mount servers require to function, such as adapter, BIOS, CIMC, and board controller firmware. The C bundle also contains the firmware images for Cisco UCS S3260 storage servers. *Release Bundle Contents for Cisco UCS Manager* for the appropriate 4.1 or later release provides details about the contents of the C-Series server software bundle.

Note Starting with Cisco UCS Manager Release 3.1(2), the firmware for endpoints that are common to both the B-Series and C-Series server software bundles, such as local disk, is available in both the B-Series and C-Series server software bundles.

- Capability catalog software bundle—Also called the T bundle, this bundle specifies implementation-specific tunable parameters, hardware specifics. and feature limits.

  Cisco UCS Manager uses the capability catalog to update the display and configurability of server components such as newly qualified DIMMs and disk drives. The Cisco UCS Manager Capability Catalog is a single image, but it is also embedded in Cisco UCS Manager software. Cisco UCS Manager Release 4.1 and later releases work with any 4.1 or later catalog file, but not with 4.0 or 3.2 catalog versions. If a server component is not dependent on a specific BIOS version, using it and having it recognized by Cisco UCS Manager is primarily a function of the catalog version. In addition to the catalog being bundled with UCS infrastructure releases, it can, sometimes, also be released as a standalone image.

The upgrade order for the endpoints in a Cisco UCS domain depends upon the upgrade path.

See the required order of steps for your upgrade path to determine the appropriate order in which to upgrade the endpoints in your Cisco UCS domain.

Cisco maintains a set of best practices for managing firmware images and updates in this document and in the following technical note: Unified Computing System Firmware Management Best Practices.

This document uses the following definitions for managing firmware:

- Update—Copies the firmware image to the backup partition on an endpoint.
- Activate—Sets the firmware in the backup partition as the active firmware version on the endpoint. Activation can require or cause the reboot of an endpoint.

Note For capability catalog upgrades, update and activate occur simultaneously. You only need to update or activate those upgrades. You do not need to perform both steps.

Cisco UCS Manager User CLI Documentation

Cisco UCS Manager offers you a 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 domains 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.

Guide	Description
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.

Components That Support Firmware Upgrade

The various platforms that are supported by Cisco UCS Manager have different components that support firmware upgrade.

- Fabric Interconnects:
  - Cisco UCS 64108
  - Cisco UCS 6454
  - Cisco UCS 6332
  - Cisco UCS 6332-16 UP
  - Cisco UCS 6248 UP
  - Cisco UCS 6296 UP
  - Cisco UCS 6324
- Chassis components:
  - Blade server chassis:
    - I/O Modules

Note I/O Modules are not supported on the primary Cisco UCS Mini chassis. However, they are supported on the secondary Cisco UCS Mini chassis.

    - Power Supply Unit
  - Cisco UCS S3260 chassis:
    - Chassis Management Controller (CMC)
    - Chassis Adapter
    - SAS Expander
    - Board Controller
- Server components:
  - Blade and Rack server:

- Adapter
- Cisco Integrated Management Controller (CIMC)
- BIOS
- Storage Controller

Note Storage controller is not a supported server component in Cisco UCS Mini.

- Board Controller

- Cisco UCS S3260 storage server node:
  - Cisco Integrated Management Controller (CIMC)
  - BIOS
  - Board Controller
  - Storage Controller

Firmware Version Terminology

The firmware version terminology used depends upon the type of endpoint, as follows:

Firmware Versions in CIMC, I/O Modules, BIOS, CIMC, and Adapters

Each CIMC, I/O module, BIOS, CIMC, and Cisco adapter has two slots for firmware in flash. Each slot holds a version of firmware. One slot is active and the other is the backup slot. A component boots from whichever slot is designated as active.

The following firmware version terminology is used in Cisco UCS Manager:

Running Version

The running version is the firmware that is active and in use by the endpoint.

Startup Version

The startup version is the firmware that will be used when the endpoint next boots up. Cisco UCS Manager uses the activate operation to change the startup version.

Backup Version

The backup version is the firmware in the other slot and is not in use by the endpoint. This version can be firmware that you have updated to the endpoint but have not yet activated, or it can be an older firmware version that was replaced by a recently activated version. Cisco UCS Manager uses the update operation to replace the image in the backup slot.

If the endpoint cannot boot from the startup version, it boots from the backup version.

Firmware Versions in the Fabric Interconnect and Cisco UCS Manager

You can only activate the fabric interconnect firmware and Cisco UCS Manager on the fabric interconnect. The fabric interconnect and Cisco UCS Manager firmware do not have backup versions, because all the images are stored on the fabric interconnect. As a result, the number of bootable fabric interconnect images is not limited to two, like the server CIMC and adapters. Instead, the number of bootable fabric interconnect images is limited by the available space in the memory of the fabric interconnect and the number of images stored there.

The fabric interconnect and Cisco UCS Manager firmware have running and startup versions of the kernel and system firmware. The kernel and system firmware must run the same versions of firmware.

Cross-Version Firmware Support

The Cisco UCS Manager A bundle software (Cisco UCS Manager, Cisco NX-OS, IOM and FEX firmware) can be mixed with previous B or C bundle releases on the servers (host firmware [FW], BIOS, Cisco IMC, adapter FW and drivers).

The following table lists the mixed A, B, and C bundle versions that are supported on Cisco UCS 6200, 6300, and 6400 Series Fabric Interconnects:

Table 1: Mixed Cisco UCS Releases Supported on Cisco UCS 6200, 6300, 6400 Series Fabric Interconnects

	Infrastructure Versions (A Bundles)						
Host FW Versions (B or C Bundles)	2.2(8)	3.1(3)	3.2(3)	4.0(1)	4.0(2)	4.0(4)	4.1(1)
2.2(8)	6200	6200	6200	6200	6200	6200	6200
3.1(3)	—	6200,6332, 6332-16UP	6200,6332, 6332-16UP	6200,6332, 6332-16UP	6200,6332, 6332-16UP	6200,6332, 6332-16UP	6200,6332, 6332-16UP
3.2(3)	—	—	6200,6332, 6332-16UP	6200,6332, 6332-16UP	6200,6332, 6332-16UP	6200,6332, 6332-16UP	6200,6332, 6332-16UP
4.0(1)	—	—	—	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454
4.0(2)	—	—	—	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454
4.0(4)	—	—	—	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454
4.1(1)	—	—	—	—	—	—	6200,6332, 6332-16UP, 6454, 64108

The following table lists the mixed A, B, and C bundle versions that are supported on Cisco UCS Mini fabric interconnects:

Table 2: Mixed Cisco UCS Releases Supported on Cisco UCS Mini Fabric Interconnects

	Infrastructure Versions (A Bundles)					
Host FW Versions (B or C Bundles)	3.1(3)	3.2(3)	4.0(1)	4.0(2)	4.0(4)	4.1(1)
3.1(3)	6324	6324	6324	6324	6324	6324
3.2(3)	—	6324	6324	6324	6324	6324
4.0(1)	—	—	6324	6324	6324	6324
4.0(2)	—	—	6324	6324	6324	6324
4.0(4)	—	—	6324	6324	6324	6324
4.1(1)	—	—	—	—	—	6324

The following table lists the mixed B, C bundles that are supported on all platforms with the 4.1(x)A bundle:

Table 3: Mixed B, C Bundles Supported on All Platforms with the 4.1(x)A Bundle

	Infrastructure Versions (A Bundles)			
Host FW Versions (B, C Bundles)	4.1(x)			
	6200	6300	6324	6400
	ucs-k9-bundle-infra.4.1.x.xxx.A.bin	ucs-6300-k9-bundle-infra.4.1.x.xxx.A.bin	ucs-mini-k9-bundle-infra.4.1.x.xxx.A.bin	ucs-6400-k9-bundle-infra.4.1.x.xxx.A.bin
2.2(8) (B, C Bundles)	Yes	—	—	—
3.1(3) (B, C Bundles)	Yes	Yes	Yes	—
3.2(3) (B, C Bundles)	Yes	Yes	Yes	—
4.0(1), 4.0(2), 4.0(4) (B, C Bundles)	Yes	Yes	Yes	Yes
4.1(1)	Yes	Yes	Yes	Yes
4.1(2)	Yes	Yes	Yes	Yes

Important If you implement cross-version firmware, you must ensure that the configurations for the Cisco UCS domain are supported by the firmware version on the server endpoints.

Server Pack

Server Pack allows you to dynamically support new server platforms[1] on existing infrastructure without requiring a complete firmware upgrade. This support is provided by a Cisco UCS Manager catalog image. Through this model, new B-Series, or C-Series server bundles that enable the new servers are supported on the previous infrastructure A bundle.

For example, in Release 3.1(1) and later releases, B, or C server bundles will be supported with Release 3.1(1) infrastructure A bundle. However, B, or C server bundles in Release 3.1(1) and later releases are not supported with the infrastructure A bundle of any release earlier than Release 3.1(1).

The *Release Notes for Cisco UCS Manager* for a particular release provides the complete matrix of cross-version firmware support for that release. New features introduced in the B, or C server bundles may only become available after upgrading the infrastructure A bundle to the respective version.

The following servers currently support Server Pack:

- B-Series Servers—UCS B200 M4, B260 M4, B420 M4, B460 M4, B200 M5, B480 M5
- C-Series Servers—UCS C220 M4, C240 M4, C460 M4 , C220 M5, C240 M5, C480 M5

If a peripheral is not supported by the existing infrastructure bundle, it will not be supported through the Server Pack feature. You must upgrade the infrastructure bundle to support this peripheral. For example, if a server is installed with new adapters that are not supported by the existing infrastructure bundle, support for these adapters requires an upgrade to the infrastructure bundle. These adapters cannot be supported through the Server Pack feature.

Because a new catalog image can be used without disrupting any hardware or software components, Server Pack provides the additional flexibility of adding new server platforms to active UCS domains without incurring the operational overhead of upgrading firmware across the whole domain.

Light Weight Upgrades

Until Cisco UCS Manager Release 3.1(3), upgrading the firmware to a patch release involved downloading and activating the complete firmware bundle even when changes were made only to specific components. The firmware versions of all components were modified even though there were no fixes made to some components. This triggered unnecessary updates for that component firmware.

Security updates to the system were also delivered through patches and lead to rebooting of the fabric interconnect and downtime.

Cisco UCS Manager Release 3.1(3) introduces light weight upgrades, which enhances firmware upgrade in the following ways:

- The firmware version of a component will be updated only if it has been modified.

[1] This feature will apply to select server platforms.

- Security updates will be provided through service packs. In Release 3.1(3), light weight upgrade supports only security updates.
- Within a service pack, updates may only apply to certain components. These components may, at times, be upgraded without a fabric interconnect reboot.
- Infrastructure and server components updates are delivered through a common service pack bundle. For servers components, only the modified firmware images will be part of the service pack bundle. This results in smaller-sized service pack bundles, compared to the traditional B-Series and C-Series bundles.

Service Packs

Service packs are patches that you can use to apply security updates to Cisco UCS Manager infrastructure and server components. Service packs are specific to a base release. You can apply a service pack on a base release, but you cannot install the service pack independently.

A service pack is provided as a single bundle for infrastructure and server components. You can update all relevant infrastructure, chassis and server components by applying the service pack through Infrastructure, Chassis and Server Auto Install. In Cisco UCS Manager Release 3.1(3), the service pack bundle provides non-disruptive updates only for infrastructure components. Among the infrastructure components, the fabric interconnect update to a service pack may require fabric interconnect rebooting in some specific scenarios such as OpenSSL fixes. The updates for server components are disruptive and will involve application downtime.

Service packs are cumulative for a maintenance release. The latest service pack will contain all the fixes from the previous service packs released for the specific maintenance release.

You can remove or update a previously applied service pack through the Cisco UCS Manager GUI and the Cisco UCS Manager CLI. Consequently, the component firmware version will be from the base release bundle.

Service packs are not applicable to maintenance releases earlier than Cisco UCS Manager Release 3.1(3).

Service Pack Versions

The following guidelines apply to service pack versions:

- A service pack can be applied only on its base bundle. For example, service pack 3.1(3)SP2 can be applied only on a 3.1(3) release. It is not compatible with a 3.1(4) release, and hence, cannot be applied on it.
- Service pack version numbering in separate maintenance releases are unrelated. For example, service packs 3.1(3)SP2 and 3.1(4)SP2 are separate and unrelated.
- The same fix can be made available for separate maintenance releases through separate service packs. For example, the same fix can be made available in 3.1(3)SP2 and 3.1(4)SP3.
- Service packs are cumulative. You can use the latest service pack version with any patch version within the same maintenance release. For example, 3.1(3)SP3 will contain all the fixes that went into 3.1(3)SP2 and 3.1(3)SP1. You can apply 3.1(3)SP3 on any 3.1(3) release.
- You cannot downgrade service packs to versions below the default service pack version for a maintenance release.
- When an upgrade or downgrade of a service pack fails, the default service pack version for that maintenance release becomes the running service pack version. For example:

Base Bundle Version: 3.1(3b)

Default Service Pack Version: 3.1(3)SP2(Default)

Running Service Pack Version: 3.1(3)SP3

While upgrading from 3.1(3)SP3 to 3.1(3)SP4, if the upgrade fails, the running service pack version displayed is 3.1(3)SP2(Default).

The following table illustrates the Release Version and Running Version Displayed in the different situations that a service pack is applied.

Release Version	Running Version Displayed
3.1(3a)	Base Bundle Version: 3.1(3a) Service Pack Version: 3.1(3)SP0(Default)
3.1(3)SP1	Base Bundle Version: 3.1(3a) Service Pack Version: 3.1(3)SP1
3.1(3)SP2	Base Bundle Version: 3.1(3a) Service Pack Version: 3.1(3)SP2
3.1(3b)	Base Bundle Version: 3.1(3b) Service Pack Version: 3.1(3)SP2(Default)
3.1(3)SP3	Base Bundle Version: 3.1(3b) Service Pack Version: 3.1(3)SP3

Service Pack Rollback

You can roll back a service pack that was applied to a base release. The following sections describe the changes made to the bundle version and the service pack version during various rollback scenarios.

Remove Service Pack

Bundle Version	Service Pack Version
No change is made to the bundle version.	Service pack is the default version that comes with the bundle.

Downgrade Infrastructure Bundle to an Earlier Maintenance Release

Bundle Version	Service Pack Version
Infrastructure bundle changes to the version of the earlier maintenance release.	Service pack is removed because it is not valid for the earlier maintenance release.

Downgrade Infrastructure Bundle Within the Same Maintenance Release, But with an Earlier Service Pack Version

Bundle Version	Service Pack Version
Infrastructure bundle changes to the version of the maintenance release patch.	Service pack is removed during any infrastructure upgrade or downgrade, if a corresponding service pack version is not specified during Auto-Install.

Guidelines and Restrictions for Service Packs

- When you upgrade from one service pack that requires FI reboot to another service pack that requires FI reboot, the FI is rebooted twice - once for each service pack.
- Server Auto Sync Policy is not supported for service packs.
- Auto sync of a service pack is not supported if the subordinate FI is running on a release earlier than Release 3.1(3).

Firmware Auto Sync for FI Cluster

Addition of a secondary Fabric Interconnect to form a cluster – either as a replacement or a conversion from standby to HA – requires the infrastructure bundle firmware versions to match. Administrators today manually upgrade/downgrade the replacement FI to the correct version before they connect it to the cluster. Firmware Auto Sync allows the users to automatically upgrade/downgrade the infrastructure bundle to the same version as the survivor FI when the replacement is added as standby to HA. The software package is the UCS software/firmware that resides on the FI.

Software and Hardware Requirements

The software package on the survivor FI should be greater than or equal to Cisco UCS Release 1.4. The model numbers of the Fabric Interconnects should be same. For example, firmware Auto Sync will not trigger for a combination of 62XX and 63XX FI models that are being set up for HA.

Implementation

With the earlier implementation, the user would compulsorily configure the replacement FI as standalone mode if there was a mismatch in the version of software packages. The replacement FI is manually upgraded/downgraded to the same version of software package on survivor FI through the usual upgrade/downgrade process. Then the replacement FI is added to the cluster, since the upgrade/downgrade of the replacement FI is a manual process.

You are now given an additional option of synchronization of the software packages of the replacement FI with the survivor FI along with the current option. If the user decides to Auto Sync the firmware, the software packages of the survivor FI are copied to the replacement FI. The software packages on the replacement FI are then activated and the FI is added to the cluster. The sync-up of the Cisco UCSM database and the configuration happens via the usual mechanisms once the HA cluster is formed successfully.

Firmware Auto Sync Benefits

In a UCS cluster where one Fabric Interconnect has failed, the Auto Sync feature ensures that the software package of the replacement FI is brought up to the same revision as the survivor. The whole process requires minimal end user interaction while providing clear and concise feedback.

Options for Firmware Upgrades

You can upgrade Cisco UCS firmware through one or more of the following methods:

Note For the steps required to upgrade one or more Cisco UCS domains to a later release, see the appropriate Cisco UCS upgrade guide. If no upgrade guide is provided, contact Cisco Technical Assistance Center. A direct upgrade from that release may not be supported.

Upgrading a Cisco UCS domain through Cisco UCS Manager

If you want to upgrade a Cisco UCS domain through the Cisco UCS Manager in that domain, you can choose one of the following upgrade options:

- Upgrade infrastructure, chassis and servers with Auto Install—This option enables you to upgrade all infrastructure components in the first stage of upgrade by using Auto Install. Then you can upgrade all chassis components through chassis firmware packages and all server endpoints through host firmware packages.
- Upgrade servers through firmware packages in service profiles—This option enables you to upgrade all server endpoints in a single step, reducing the amount of disruption caused by a server reboot. You can combine this option with the deferred deployment of service profile updates to ensure that server reboots occur during scheduled maintenance windows.
- Direct upgrades of infrastructure and server endpoints—This option enables you to upgrade many infrastructure and server endpoints directly, including the fabric interconnects, I/O modules, adapters, and board controllers. However, direct upgrade is not available for all endpoints, including the storage controller, HBA firmware, HBA option ROM and local disk. You must upgrade those endpoints through the host firmware package included in the service profile associated with the server.
- Upgrade chassis through chassis firmware packages in chassis profiles—This option enables you to upgrade all S3260 Chassis endpoints in a single step.

Note Chassis profiles and chassis firmware packages are applicable only to S3260 Chassis.

Upgrading S3X60 Server Nodes in a Cisco UCS domain through Cisco UCS Manager

You can upgrade a Cisco UCS domain with a S3260 Chassis and servers through Cisco UCS Manager in the following ways:

- Upgrade infrastructure components through Auto Install—You can upgrade the infrastructure components, such as the Cisco UCS Manager software and the fabric interconnects, in a single step by using Auto Install.
- Upgrade chassis through chassis firmware packages in chassis profiles—This option enables you to upgrade all chassis endpoints in a single step.

  Cisco UCS S3260 Server Integration with Cisco UCS Manager provides detailed information about chassis profiles and chassis firmware packages.
- Upgrade servers through firmware packages in service profiles—This option enables you to upgrade all server endpoints in a single step, reducing the amount of disruption caused by a server reboot. You can combine this option with the deferred deployment of service profile updates to ensure that server reboots occur during scheduled maintenance windows.

You can also directly upgrade the firmware at each infrastructure, chassis, and server endpoint. This option enables you to upgrade many infrastructure, chassis, and server endpoints directly, including the fabric interconnects, SAS expanders, CMCs, chassis adapters, storage controllers, and board controllers. However, direct upgrade is not available for all endpoints, including the storage controller, HBA firmware, HBA option ROM and local disk.

Cisco UCS S3260 Server Integration with Cisco UCS Manager provides detailed information about firmware management for S3X60 Server Nodes

Upgrading a Cisco UCS domain through Cisco UCS Central

If you have registered one or more Cisco UCS domains with Cisco UCS Central, you can manage and upgrade all firmware components in those domain through Cisco UCS Central. This option allows you to centralize the control of firmware upgrades and ensure that all Cisco UCS domains in your data center are at the required levels.

You can use Cisco UCS Central to upgrade the capability catalog, infrastructure, and host firmware in all registered Cisco UCS domains that are configured for global firmware management.

You cannot directly upgrade the firmware at each endpoint. In Cisco UCS Central, you must use host firmware policy within a global service profile to upgrade host firmware components.

Options for Service Pack Updates

You can upgrade Cisco UCS firmware to a service pack through one of the following methods:

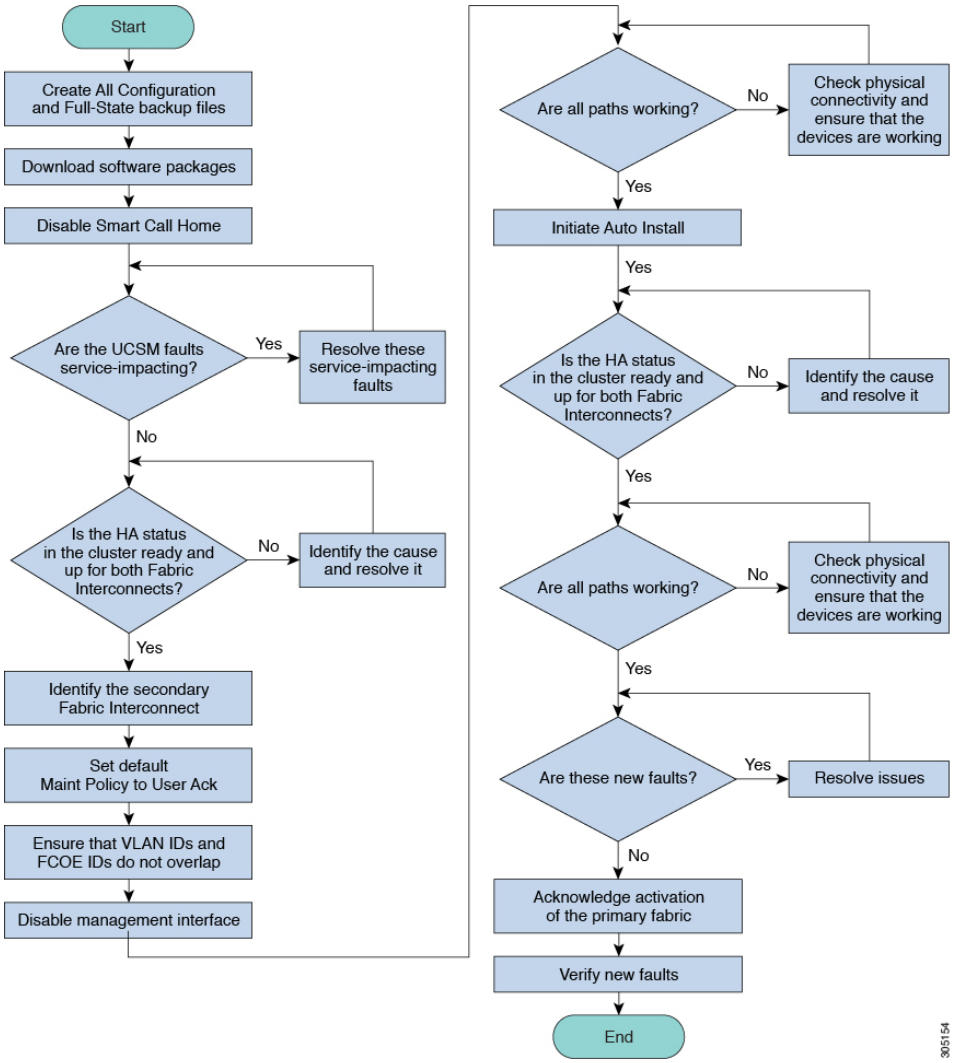
- Upgrade to a service pack through Infrastructure Auto Install
- Upgrade to a service pack through Chassis Auto Install
- Upgrade to a service pack through Server Auto Install
- Upgrade to a service pack through firmware packages in service profiles
- Upgrade to a service pack through chassis firmware packages in chassis profiles
- Directly activate a Cisco UCS Manager service pack on a base maintenance release
- Directly activate a fabric interconnect service pack on a base maintenance release

Firmware Upgrades through Auto Install

Auto Install enables you to automatically upgrade a Cisco UCS domain to the firmware versions contained in a single package, in the following stages:

- Install Infrastructure Firmware—Uses the Cisco UCS Infrastructure Software Bundle to upgrade the infrastructure components, such as the fabric interconnects, the I/O modules, and Cisco UCS Manager. Figure 5: Process Flow for Automatically Installing Infrastructure Firmware , on page 16, illustrates the recommended process flow to automatically install infrastructure firmware.

Figure 5: Process Flow for Automatically Installing Infrastructure Firmware



- Install Chassis Firmware—Uses the Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle to upgrade the chassis components.
- Install Server Firmware—As necessary, uses the Cisco UCS B-Series Blade Server Software Bundle to upgrade all blade servers in the Cisco UCS domain; the Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle to upgrade all rack servers.

These stages are independent and can be run or scheduled to run at different times.

You can use Auto Install to upgrade the infrastructure components to one version of Cisco UCS and upgrade the chassis and server components to a different version.

Cisco strongly recommends that you use Auto Install and Fabric Evacuation to upgrade a Cisco UCS domain.

Firmware Upgrades through Firmware Packages in Service Profiles

Server firmware and BIOS versions need periodic updating across multiple servers. If this is done manually, it must be done serially and involves many hours of downtime.

You can use host firmware packages by defining a host firmware policy as an attribute of a service profile template, which is an updating template. Any change made to the service profile template is automatically made to its instantiated service profiles. Subsequently, the servers associated with the service profiles are also upgraded in parallel with the firmware version.

You cannot upgrade the firmware on an I/O module, fabric interconnect, or Cisco UCS Manager through service profiles. You must upgrade the firmware on those endpoints directly.

Direct Firmware Upgrade at Endpoints

If you follow the correct procedure and apply the upgrades in the correct order, a direct firmware upgrade and the activation of the new firmware version on the endpoints is minimally disruptive to traffic in a Cisco UCS domain.

Depending on the target chassis that you use, you can directly upgrade the firmware on various components:

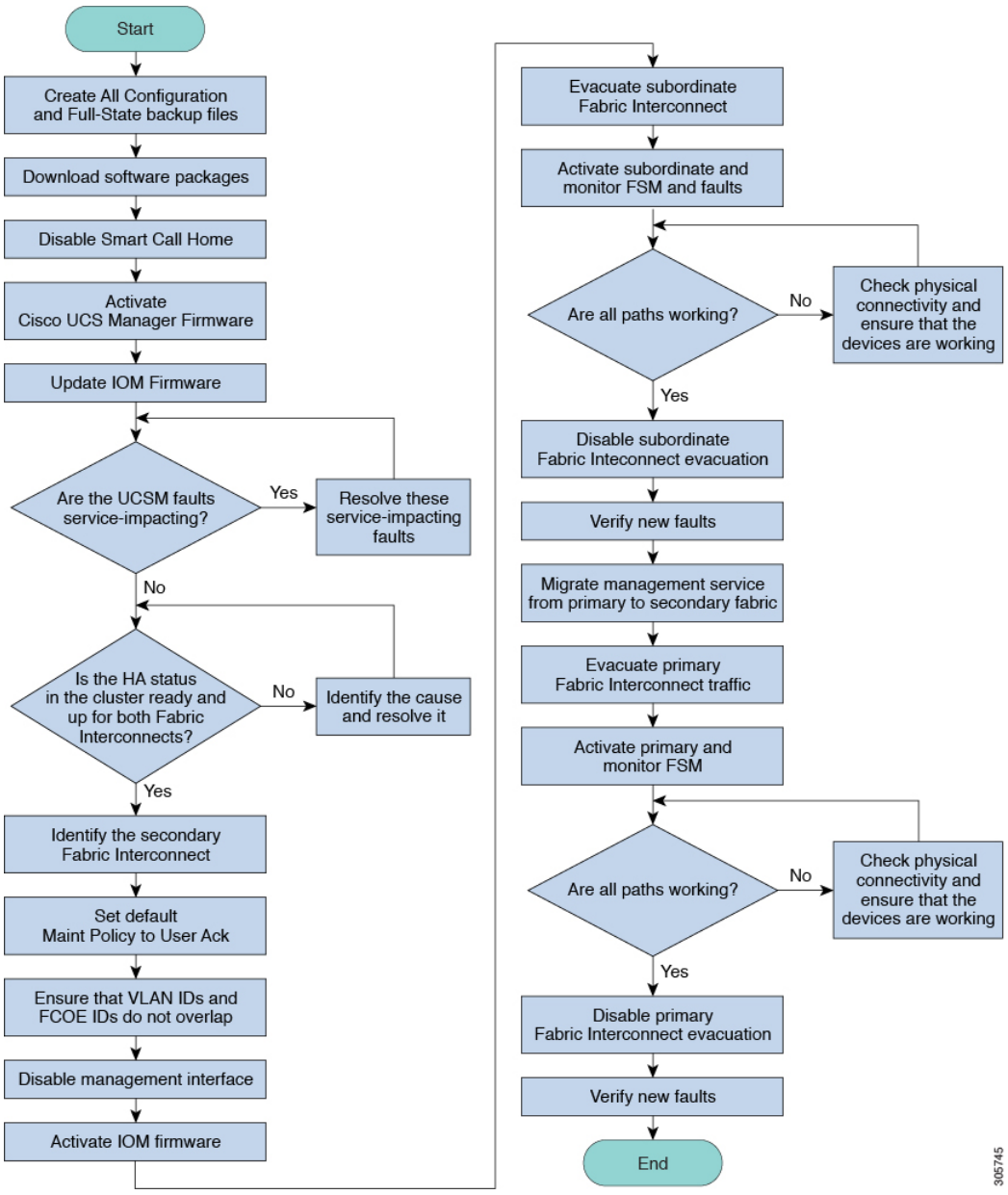
Infrastructure	UCS 5108 Chassis	UCS Rack Server	Cisco UCS S3260 Chassis

• Cisco UCS Manager
• Fabric interconnects
 	
Ensure that you upgrade Cisco UCS Manager first and then the fabric interconnects.
	• I/O modules
	• Power supply unit
	• Server:
	  • Adapter
	  • CIMC
	  • BIOS
	  • Storage controller
	  • Board controller
		• Adapter
		• CIMC
		• BIOS
		• Storage controller
		• Board controller
			• CMC
			• Chassis adapter
			• SAS expander
			• Chassis board controller
			• Server:
			  • CIMC
			  • BIOS
			  • Board controller
			  • Storage controller

Note Directly upgrading firmware on server endpoints is possible only on discovered, unassociated servers and Cisco adapters.

Figure 6: Process Flow for Manually Installing Infrastructure Firmware, on page 18, illustrates the recommended process flow.

Figure 6: Process Flow for Manually Installing Infrastructure Firmware



The adapter and board controller firmware can also be upgraded through the host firmware package in the service profile. If you use a host firmware package to upgrade this firmware, you can reduce the number of times a server needs to be rebooted during the firmware upgrade process.

Note Upgrades of an adapter through a firmware package in the service profile associated with the server take precedence over direct firmware upgrades. You cannot directly upgrade an endpoint if the service profile associated with the server includes a firmware package. To perform a direct upgrade, you must remove the firmware package from the service profile.

Firmware Upgrade While Migrating from Cisco UCS 6200 Series Fabric Interconnects to Cisco UCS 6400 Series Fabric Interconnects

These upgrade guidelines must be followed while migrating:

- The Cisco UCS 6200 Series fabric interconnect should be upgraded to Cisco UCS Manager Release 4.1(1) or later releases.
- The Cisco UCS 6400 Series Fabric Interconnect must be loaded with the same build version that is on the Cisco UCS 6200 Series Fabric Interconnect that it will replace.
- You can migrate from Cisco UCS 6200 Series Fabric Interconnects to Cisco UCS 6400 Series Fabric Interconnects, but not from Cisco UCS 6400 Series Fabric Interconnects to Cisco UCS 6200 Series Fabric Interconnects. You cannot migrate between the following:
  - Cisco UCS 6332 and Cisco UCS 6332 16UP Fabric Interconnects
  - Cisco UCS 6332 and Cisco UCS 6454 Fabric Interconnects
  - Cisco UCS 6332 and Cisco UCS 64108 Fabric Interconnects
  - Cisco UCS 6332 16UP and Cisco UCS 6454 Fabric Interconnects
  - Cisco UCS 6332 16UP and Cisco UCS 64108 Fabric Interconnects
- All fabric interconnects should have the same versions of kickstart, system, and UCSM images.

Note UCS 6400 Series Fabric Interconnects have a unified image - kickstart and system images are no longer separate.

- Upgrading the fabric interconnect should be done before upgrading to a new FEX or virtual interface card.
- For a cluster configuration, both fabric interconnects must have symmetrical connection topologies between the fabric interconnects and FEXes.
- Standalone installations should expect down time. Upgrading a fabric interconnect is inherently traffic disruptive.
- A best practice would be to perform a full configuration and software backup before performing this hardware upgrade.

Software Feature Configuration on Cisco UCS 6400 Series Fabric Interconnects

Cisco UCS Manager Release 4.0(1) and 4.0(2) introduced support for various software features on Cisco UCS 6454 Fabric Interconnects. Cisco UCS Manager Release 4.1 extends support for these features on Cisco UCS 64108 Fabric Interconnects. These software features are:

- Switching Modes—Support for Ethernet and FC switching modes on Cisco UCS 6400 Series Fabric Interconnects .
- MAC Security—Support for MAC security on Cisco UCS 6400 Series Fabric Interconnects.
- Breakout Uplink Ports—Support for splitting a single 40/100G QSFP port into four 10/25G ports using a supported breakout cable. These ports can be used only as Ethernet uplink or FCoE uplink ports connecting to a 10/25G switch. They cannot be configured as server ports, FCoE storage ports, appliance ports or monitoring ports.
- MTU Configuration—Cisco UCS 64108 Fabric Interconnects support MTU configuration for QOS drop class policy.

Cisco UCS 6400 Series Fabric Interconnects do not support the following software features:

- Chassis Discovery Policy in Non-Port Channel Mode—Cisco UCS 6400 Series Fabric Interconnects support only Port Channel mode.
- Chassis Connectivity Policy in Non-Port Channel Mode—Cisco UCS 6400 Series Fabric Interconnects support only Port Channel mode.
- Multicast Hardware Hash—Cisco UCS 6400 Series Fabric Interconnects do not support multicast hardware hash.
- Service Profiles with Dynamic vNICS—Cisco UCS 6400 Series Fabric Interconnects do not support Dynamic vNIC Connection Policies.
- Multicast Optimize—Cisco UCS 6400 Series Fabric Interconnects do not support Multicast Optimize for QoS.
- NetFlow—Cisco UCS 6400 Series Fabric Interconnects do not support NetFlow related configuration.
- Port profiles and DVS Related Configurations—Cisco UCS 6400 Series Fabric Interconnects do not support configurations related to port profiles and distributed virtual switches (DVS).

Configuration of the following software features has changed for Cisco UCS 6400 Series Fabric Interconnects:

- Unified Ports—Cisco UCS 6400 Series Fabric Interconnects support up to 16 unified ports, which can be configured as FC. These ports appear at the beginning of the module.
- VLAN Optimization—On Cisco UCS 6400 Series Fabric Interconnects, you can configure VLAN port count optimization through port VLAN (VP) grouping when the PV count exceeds 16000. The following table illustrates the PV Count with VLAN port count optimization enabled and disabled on Cisco UCS 6400 Series Fabric Interconnect, Cisco UCS 6300 Series Fabric Interconnects, and Cisco UCS 6200 Series Fabric Interconnects.

	6200 Series FI	6300 Series FI	6400 Series FI
PV Count with VLAN Port Count Optimization Disabled	32000	16000	16000

	6200 Series FI	6300 Series FI	6400 Series FI
PV Count with VLAN Port Count Optimization Enabled	64000	64000	64000

When a Cisco UCS 6400 Series Fabric Interconnect is in Ethernet switching mode:

- The Fabric Interconnect does not support **VLAN Port Count Optimization Enabled**
- The Fabric Interconnect supports 16000 PVs, similar to EHM mode, when set to **VLAN Port Count Optimization Disabled**

- Limited Restriction on VLAN—Cisco UCS 6400 Series Fabric Interconnects reserve 128 additional VLANs for system purposes.

Firmware Upgrade to Cisco UCS Manager Release 4.1

Scenarios for Firmware Upgrade to Cisco UCS Manager Release 4.1

Upgrading the Infrastructure software bundle (A bundle) directly to Cisco UCS Manager Release 4.1(x) is supported from Release 3.1(3), and 3.2(3) and later releases.

For Cisco UCS Mini, upgrading the Infrastructure software bundle (A bundle) directly to Cisco UCS Manager Release 4.1(x) is supported from Release 3.1(3), and 3.2(3) and later releases.

Starting with Release 4.1(3a), the FPGA upgrade is supported in Cisco UCS 6454 Fabric Interconnect and Cisco UCS 64108 Fabric Interconnect:

- On upgrading Infrastructure to Cisco UCS Manager release 4.1(3a) or later releases, the version of IOFPGA gets upgraded to v22 on Cisco UCS 6454 Fabric Interconnect.
- Starting with Cisco UCS Managerrelease 4.1(3a), the secure FPGA upgrade feature is enabled for Cisco UCS 64108 Fabric Interconnect, by default. The FPGA will get upgraded when Infrastructure is upgraded from 4.1(3) to later releases.

Post the IOFPGA version upgrade, upgrade golden regions of FPGA on Fabric Interconnect to address Secure Boot vulnerability. To upgrade golden regions of FPGA, install secure FPGA in fabric interconnect. For more information on secure FPGA installation procedure, see Cisco UCS Manager Network Management Guide and Cisco UCS Manager Network Management Guide using the CLI.

The following table lists the upgrade paths for various Cisco UCS Manager releases.

Note Before initiating the release upgrade, refer the Firmware Management guides of respective version to understand the limitations and the correct path to do the upgrade.

Table 4: Upgrade Paths to Release 4.1

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
2.1(x)	4.1(x)	Upgrading directly to Release 4.1(x) is not supported from this release. To upgrade to Release 4.1(x), do the following in order: **1.** Upgrade the Infrastructure A bundle to Release 3.1(3) or 3.2(3). **2.** Upgrade the B and C bundles for all servers to Release 3.1(3) or 3.2(3). **3.** Upgrade the Infrastructure A bundle to Release 4.1(x).
2.2(1), 2.2(2), 2.2(3), 2.2(4), 2.2(5), 2.2(6), 2.2(7)	4.1(x)	Upgrading directly to Release 4.1(x) is not supported from this release. To upgrade to Release 4.1(x), do the following in order: **1.** Upgrade the Infrastructure A bundle to Release 3.1(3) or 3.2(3). **2.** Upgrade the B and C bundles for all servers to Release 3.1(3) or 3.2(3). **3.** Upgrade the Infrastructure A bundle to Release 4.1(x).
2.2(8)	4.1(x)	Upgrading directly to Release 4.1(x) is not supported from this release. To upgrade to Release 4.1(x), do the following in order: **1.** Upgrade the Infrastructure A bundle to Release 3.1(3) or 3.2(3). **2.** Upgrade the B and C bundles for all servers to Release 3.1(3) or 3.2(3). **3.** Upgrade the Infrastructure A bundle to Release 4.1(x).
3.0(x)	4.1(x)	Upgrading directly to Release 4.1(x) is not supported from this release. To upgrade to Release 4.1(x), do the following in order: **1.** Upgrade the Infrastructure A bundle to Release 3.1(3) or 3.2(3). **2.** Upgrade the B and C bundles for all servers to Release 3.1(3) or 3.2(3). **3.** Upgrade the Infrastructure A bundle to Release 4.1(x).

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
3.1(1), 3.1(2)	4.1(x)	Upgrading directly to Release 4.1(x) is not supported from this release. To upgrade to Release 4.1(x), do the following in order: **1.** Upgrade the Infrastructure A bundle to Release 3.1(3) or 3.2(3). **2.** Upgrade the B and C bundles for all servers to Release 3.1(3) or 3.2(3). **3.** Upgrade the Infrastructure A bundle to Release 4.1(x).
3.1(3)	4.1(x)	Upgrade directly to Release 4.1(x).
3.2(1), 3.2(2)	4.1(x)	Upgrading directly to Release 4.1(x) is not supported from this release. To upgrade to Release 4.1(x), do the following in order: **1.** Upgrade the Infrastructure A bundle to Release 3.2(3) or 4.0(x). **2.** Upgrade the B and C bundles for all servers to Release 3.2(3) or 4.0(x). **3.** Upgrade the Infrastructure A bundle to Release 4.1(x).
3.2(3)	4.1(x)	Upgrade directly to Release 4.1(x).
4.0(x)	4.1(x)	Upgrade directly to Release 4.1(x).

Important You can replace an FI in a cluster with an FI that runs on Cisco UCS Manager Release 2.1(2) or later releases and upgrade this FI directly to a 3.2(x) release by using the Auto Sync feature.

Prerequisites for Upgrade to Cisco UCS Manager Release 4.1

- Before upgrading to Cisco UCS Manager Release 4.1, ensure that the existing infrastructure and server bundles are on one of the following Cisco UCS Manager releases:
  - Cisco UCS Manager Release 3.1(3)
  - Cisco UCS Manager Release 3.2(3) or later releases

  For Cisco UCS Mini, you can upgrade to Cisco UCS Manager Release 4.1 from any Release 3.1(3), 3.2(3), or 4.0(x) release.
- Before upgrading to Cisco UCS Manager Release 4.1, ensure that the key ring in use has a modulus size of 2048 bits or more by doing the following:

  1. Verify the modulus size of the key ring in use by using the following commands:

```
UCS-A# scope security
UCS-A /security # scope keyring keyring-name
UCS-A /security/keyring # show detail
```

2. If the default key ring is in use, and has a modulus size less than 2048 bits, reconfigure the modulus size to 2048 bit or more, and regenerate the certificate by using the following commands:

```
UCS-A# scope security
UCS-A /security # scope keyring default
UCS-A /security/keyring # set modulus mod2048
UCS-A /security/keyring # set regenerate yes
UCS-A /security/keyring # commit-buffer
UCS-A /security/keyring # show detail
```

3. If the key ring in use is not the default key ring, and has a modulus size less than 2048 bits, delete the existing key ring and create a new one with a modulus value equal to or more than 2048 bits.

Note A key ring in use cannot be deleted. To delete a key ring that is in use, first configure HTTPS to use another key ring.

Cisco UCS Manager Release 3.1 and later releases do not support key rings that have modulus size less than 2048 bits.

Conditions Under Which Upgrade to Cisco UCS Manager Release 4.1 Fails

Upgrading to Cisco UCS Manager Release 4.1 from an earlier release will fail in the following scenarios, and Cisco UCS Manager will roll back to the earlier release:

- Upgrade with insufficient free space in fabric interconnect partitions:
  - Less than 20 percent free space in `/var/sysmgr`
  - Less than 30 percent free space in `/mnt/pss`
  - Less than 20 percent free space in `/bootflash`
- Cisco UCS Manager validation failures because of misconfiguration.

SNMP is Automatically Disabled During Upgrade

When upgrading from an earlier release to Cisco UCS Manager Release 4.1, SNMP, if previously enabled, is automatically disabled. The SNMP state will be restored after the upgrade of both fabric interconnects is complete. During upgrade, when SNMP is automatically disabled, all SNMP operations will be suspended. Cisco recommends that you restart SNMP operations only after the upgrade of both fabric interconnects is complete.

Important Although the SNMP state is restored after Cisco UCS Manager is upgraded, you can run SNMP operations only after both the fabric interconnects are upgraded.

Firmware Upgrade to a Minor or a Patch Release

The release number of Cisco UCS Manager software consists of a major release identifier, minor release identifier, and patch release identifier. The minor release identifier and patch release identifier are listed together in parentheses. For example, if the software version number is **4.1(2a)**:

- **4.1** is the major release identifier
- **2** is the minor release identifier
- **a** is the patch release identifier

Read together, it indicates the **a** patch of the **first** minor release of the **4.1** release train.

Firmware upgrade to maintenance releases and patches within a major release are done in exactly the same way as for the major release.

For more information about what is in each maintenance release and patch, see the latest version of the Release Notes.

Firmware Downgrades

You downgrade firmware in a Cisco UCS domain in the same way that you upgrade firmware. The package or version that you select when you update the firmware determines whether you are performing an upgrade or a downgrade.

Note The Cisco UCS Manager CLI does not allow you to downgrade hardware that is not supported in the release to which you are downgrading, Cisco UCS Manager CLI displays an error message if you attempt to downgrade hardware to an unsupported release.

Downgrade From Cisco UCS Manager Release 4.1

In a system with Cisco UCS 64108 Fabric Interconnects, you cannot downgrade from Cisco UCS Manager Release 4.1.

MD5 SNMPv3 User Authentication

When downgrading to a release earlier than Cisco UCS Manager Release 3.2(3), SNMPv3 users with MD5 authentication will not be deployed. To deploy such a user, do one of the following:

- Modify the **Auth Type** field to **SHA**.
- Delete the user and recreate it.

AES Privacy Protocol for SNMPv3 Users

Cisco UCS Manager Release 3.2(3) and later releases do not support SNMPv3 users without AES encryption. Hence, when downgrading to a release earlier than Cisco UCS Manager Release 3.2(3), SNMPv3 users without AES encryption will not be deployed. To deploy such a user, do one of the following:

- Enable **AES-128** encryption.
- Delete the user and recreate it.

Cisco UCS Domain with UCS M5 Servers

In a Cisco UCS domain with UCS M5 servers, when you downgrade from Cisco UCS Manager Release 3.2(1) to earlier releases, ensure that you decommission the UCS M5 servers. This is because UCS M5 servers are supported only by Cisco UCS Manager Release 3.2(1) and later releases.

If you downgrade from Cisco UCS Manager Release 3.2(1) to earlier releases without decommissioning UCS M5 servers, upgrade validation will fail and Cisco UCS Manager will prompt you to decommission the servers before continuing with the downgrade operation.

Board Controller Firmware for Blade Servers

Important

- You never need to downgrade the board controller firmware.

  The board controller firmware in Cisco UCS B-Series blade servers is not designed to be downgraded. When you are performing a full system firmware downgrade operation, if the system displays this error message “Error: Update failed: Server does not support board controller downgrade”, it is safe to ignore the error message and continue with downgrading system firmware. Cisco UCS Manager will automatically skip over the board controller firmware and continue with the downgrade of the other firmware components.

- The board controller firmware version of the blade server should be the same as or later than the installed software bundle version. Leaving the board controller firmware at a later version than the version that is currently running in your existing Cisco UCS environment does not violate the software matrix or TAC supportability.

Unsupported Features Must Be Unconfigured Before Downgrade

If you plan to downgrade a Cisco UCS domain to an earlier release, you must first unconfigure all features from the current release that are not supported in the earlier release and correct all failed configurations. If you downgrade B, or C server bundles without unconfiguring unsupported features, the feature may not work in the downgraded release. For example, the On Next Reboot maintenance policy is supported by the 3.1 B, and C bundles. If you downgrade any server bundle, this maintenance policy option will not work for the corresponding server.

If you attempt to downgrade the infrastructure bundle without unconfiguring all features that are not supported in the earlier release, the downgrade may fail.

SNMP Must be Disabled Before Downgrade

You must disable SNMP before downgrading from Cisco UCS Manager Release 3.2 to an earlier release. The downgrade process does not begin until SNMP is disabled.

Recommended Order of Steps for Firmware Downgrades

If you need to downgrade the firmware to an earlier release, we recommend that you do it in the following order:

1. Retrieve the configuration backup from the release to which you want to downgrade. This is the backup you created when you upgraded to the current release.
2. Unconfigure the features that are not supported in the release to which you want to downgrade.
3. Create Full State and All Configuration backup files.
4. Downgrade Cisco UCS Manager.
5. Perform an erase-config.
6. Import the configuration backup from the release to which you downgraded.

Note Steps 5 and 6 are optional. Perform these steps only if the existing configuration becomes unusable. In this case, import the configuration backup either from Step 1 or Step 3.

Firmware Management in Cisco UCS Central

Cisco UCS Central enables you to manage all firmware components for all registered Cisco UCS domains.

Note To manage Cisco UCS domains firmware from Cisco UCS Central, you must enable the global firmware management option in Cisco UCS Manager. You can enable the global firmware management option when you register Cisco UCS Manager with Cisco UCS Central. You can also turn the global management option on or off, based on your management requirements.

Important Do not unregister a Cisco UCS domain from Cisco UCS Central.

The Cisco UCS domains are categorized into domain groups in Cisco UCS Central for management purposes. You can manage firmware for each domain group separately at the domain group level or for all domain groups from the domain group root. Cisco UCS Central provides you the option to manage the following Cisco UCS domain firmware packages:

- **Capability Catalog**— One capability catalog per domain group. All Cisco UCS domains registered to a particular domain group will use the capability catalog defined in the domain group.
- **Infrastructure Firmware**— One infrastructure firmware policy per domain group . All Cisco UCS domains registered to a particular domain group will use the same Infrastructure firmware version defined in the domain group.
- **Host Firmware**— You can have more than one host firmware policy for the different host firmware components in a domain group. The Cisco UCS domains registered in the domain group will be able to choose any defined host firmware policy in the group. Cisco UCS Central provides you the option to upgrade the host firmware globally to all Cisco UCS domains in a domain group at the same time.

Note For more information on managing firmware in Cisco UCS Central, see the Firmware Management chapters in the *Cisco UCS Central Administration Guide* and *Cisco UCS Central CLI Reference Manual*.