Cisco IMC Supervisor Release Notes, Release 2.2

First Published: 2017-07-11

Last Modified: 2021-07-05

About Cisco IMC Supervisor

Cisco IMC Supervisor is a management system that allows you to manage rack-mount servers on a large scale. It allows you to create groups of rack-mount servers for monitoring and inventory purposes.

You can use Cisco IMC Supervisor to perform the following tasks:

- Logically grouping servers and viewing summary per group
- Collecting inventory for the managed servers
- Monitoring servers and groups
- Managing firmware including firmware download, upgrade, and activation
- Provide Northbound REST APIs to discover, monitor and manage servers and perform firmware upgrades programmatically.
- Managing standalone server actions including power control, LED control, log collection, KVM launch, and CIMC UI launch.
- Restricting access using Role Based Access Control (RBAC)
- Configuring email alerts
- Configuring server properties using policies and profiles
- Defining schedules to defer tasks such as firmware updates or server discovery
- Diagnosing server hardware issues using UCS Server Configuration Utility
- Cisco Smart Call Home provides proactive diagnostics, alerts, and remediation recommendations
- Managing Cisco UCS S3260 Dense Storage Rack Server
- Configuring the DNS server and other network settings through the Network Configuration policy
- Assigning physical drives to server through the Zoning policy
- Setting up multiple diagnostic images across different geographic locations
- Customizing email rules to include individual servers within a group

Revision History

Release	Date	Description
2.2	July 11, 2017	Created Release Notes for Cisco IMC Supervisor, Release 2.2.
2.2(0.1)	August 23, 2017	Added information for release 2.2(01).
2.2(0.2)	January 2, 2018	Added information for release 2.2(0.2)
2.2(0.3)	June 6, 2018	Added information for release 2.2(0.3). See the following sections: • Upgrading Cisco IMC Supervisor, on page 10 • New and Changed Features in Release 2.2(0.3), on page 18 • Open Bugs in Release 2.2(0.3), on page 26 • Resolved Bugs in Release 2.2(0.3), on page 30
2.2(0.3)	August 24, 2018	Added Cisco UCS VIC 1425 to the list of Supported PCiE cards.
2.2(0.4)	January 9, 2019	Added information for release 2.2(0.4). See the following sections: • New and Changed Features in Release 2.2(0.4), on page 20 • Open Bugs in Release 2.2(0.4), on page 26 • Resolved Bugs in Release 2.2(0.4), on page 30 **Important** Cisco IMC Supervisor release 2.2(0.4) is now a deferred release and is no longer available for download. You must upgrade to release 2.2(0.5). See the software deferral notice.

Release	Date	Description
2.2(0.5)	March 11, 2019	Added information for release 2.2(0.5). See the following sections: • New and Changed Features in Release 2.2(0.5), on page 21 • Upgrading Cisco IMC Supervisor, on page 10 • Open Bugs in Release 2.2(0.5), on page 27 • Resolved Bugs in Release 2.2(0.5), on page 30 **Important** Cisco IMC Supervisor release 2.2(0.5) is now a deferred release and is no longer available for download. You must upgrade to release 2.2(1.0).
2.2(0.6)	May 20, 2019	Added information for Release 2.2(0.6). See the following sections: • New and Changed Features in Release 2.2(0.6), on page 21 • Upgrading Cisco IMC Supervisor, on page 10 • Open Bugs in Release 2.2(0.6), on page 27 • Resolved Bugs in Release 2.2(0.6), on page 31 **Important** Cisco IMC Supervisor release 2.2(0.6) is now a deferred release and is no longer available for download. You must upgrade to release 2.2(1.0).

Release	Date	Description
2.2(1.0)	August 19, 2019	Added information for Release 2.2(1.0) See the following sections: • New and Changed Features in Release 2.2(1.0), on page 21 • Upgrading Cisco IMC Supervisor, on page 10 • Open Bugs in Release 2.2(1.0), on page 27 • Resolved Bugs in Release 2.2(1.0), on page 31
2.2(1.1)	October 1, 2019	Added information for Release 2.2(1.1) See the following sections: • New and Changed Features in Release 2.2(1.1), on page 21 • Upgrading Cisco IMC Supervisor, on page 10 • Open Bugs in Release 2.2(1.1), on page 28 • Resolved Bugs in Release 2.2(1.1), on page 31
2.2(1.2)	December 16, 2019	Added information for release 2.2(1.2). See the following sections: • New and Changed Features in Release 2.2(1.2), on page 23 • Upgrading Cisco IMC Supervisor, on page 10 • Open Bugs in Release 2.2(1.2), on page 28 • Resolved Bugs in Release 2.2(1.2), on page 32

Release	Date	Description
2.2(1.3)	March 18, 2020	Added information for release 2.2(1.3). See the following sections: • Upgrading Cisco IMC Supervisor, on page 10 • New and Changed Features in Release 2.2(1.3), on page 23 • Open Bugs in Release 2.2(1.3), on page 28 • Resolved Bugs in Release 2.2(1.3), on page 32
2.2(1.4)	September 30, 2020	Added information for release 2.2(1.4). See the following sections: • Upgrading Cisco IMC Supervisor, on page 10 • New and Changed Features in Release 2.2(1.4), on page 24 • Open Bugs in Release 2.2(1.4), on page 28 • Resolved Bugs in Release 2.2(1.4), on page 32

Minimum System Requirements

Supported Server Models

- UCS C-220 M3, M4 and M5
- UCS C-240 M3, M4 and M5
- UCS C-460 M4
- UCS C-480 M5
- UCS C-22 M3
- UCS C-24 M3
- UCS C-420 M3
- UCS E-160S M3

- UCS C3160
- UCS S3260 M3, M4 and M5
- UCS EN120E M2
- UCS EN120S M2
- UCS EN140N M2
- UCS E-140S M2
- UCS E-160D M2
- UCS E-180D M2
- UCS E-140S M1
- UCS E-140D M1
- UCS E-160D M1
- UCS E-140DP M1
- UCS E-160DP M1
- UCS E-1120D M3
- UCS E-180D M3
- ENCS 5406
- ENCS 5408
- ENCS 5412
- HX220C-M5S
- HX220C-M4
- HX240C-M5SX
- HX240C-M4
- HXAF240C-M5SX
- HXAF220C-M5S
- HXAF240C-M4SX

Important Cisco IMC Supervisor supports up to 1000 UCS C-Series and E-Series servers. For more information about scalability, see Cisco IMC Supervisor Deployment and Scalability, on page 8.

Minimum Firmware Versions

Servers	Minimum Firmware Version
UCS C-series Servers	1.5(4)

Servers	Minimum Firmware Version
UCS E-series Servers	2.3.1
UCS S3260 Servers	2.0(13e)

Supported PCiE Cards

- Cisco UCS VIC 1225
- Cisco UCS VIC 1225T
- Cisco UCS VIC 1227
- Cisco UCS VIC 1227T
- Cisco UCS VIC 1385
- Cisco UCS VIC 1387
- Cisco UCS VIC 1455
- Cisco UCS VIC 1457

Supported Hypervisor versions

- ESXi 5.1
- ESXi 5.5
- ESXi 6.0
- ESXi 6.5
- ESXi 6.7
- Windows 2008 R2 with Hyper-V Role
- Windows 2012 R2 with Hyper-V Role
- Windows 2016 with Hyper-V Role

Minimum Hardware Requirements

The Cisco IMC Supervisor environment must meet at least the minimum system requirements listed in the following table.

Element	Minimum Supported Requirement
vCPU	4
Memory	12 GB
Primary Disk (Hard Disk 1)	100 GB
Secondary Disk (Hard Disk 2)	100 GB

Element	Minimum Supported Requirement
Minimum write speed for storage	10 MB/sec

Supported Browser Versions

Cisco IMC Supervisor supports the following browser versions:

For HTML-5

- Internet Explorer 8 or higher
- Firefox 12 or higher (PC and Apple MAC)
- Safari 6 or higher
- Google Chrome 18 or higher
- Opera 12 or higher (PC and Apple MAC)

For Classic View - all browsers must have Adobe Flash Player 11 plug-in or higher

- Internet Explorer 8 or higher
- Google Chrome 4.1 or higher
- Firefox 3.5 or higher
- Safari 4.0 or higher (for Apple Mac)

Note Starting with release 2.2(0.3), Classic View is no longer available.

Cisco IMC Supervisor Deployment and Scalability

Configuring Inframgr properties

1. Modify the following properties and values from the `/opt/infra/inframgr/service.properties` file:
    - threadpool.maxthreads.inventory=50
    - cimc.inventory.max.thread.pool.size=100
2. Go to Shell Admin and restart the services by stopping and starting the Cisco IMC Supervisor services.

Deployment Recommendations

Cisco IMC Supervisor recommends the following based on the scale of rack servers you manage:

Element	Small Deployment (1 - 250 rack servers)	Medium Deployment (251 - 500 rack servers)	Large Deployment (501 - 1000 rack servers)
vCPUs	4	4	8
CPU Reservation	10000 MHz	10000 MHz	10000 MHz
Cisco IMC Supervisor VM Memory Allocation	12 GB	16 GB	20 GB
Cisco IMC Supervisor VM Memory Reservation	12 GB	16 GB	20 GB
Inframgr Memory Allocation	6 GB	8 GB	10 GB
Mysql InnoDB BufferPool Config	1GB	2 GB	3 GB
Disk write Speed (Direct IO)	10 MB/sec	10 MB/sec	15 MB/sec

Allocating Inframgr Memory

1. Go to `/opt/infra/bin/` and open the `inframgr.env` file using vi editor.
2. Edit the values MEMORY_MIN and MEMORY_MAX.

   For example, if you are managing 1000 rack servers then inframgr memory allocation must be set to 10 GB. Hence, the MEMORY_MIN and MEMORY_MAX must be set to 10240m.

Note Inframgr memory allocation must be increased only if the memory allocated to the VM is increased. If not, this process may crash due to high load. Hence, increase memory for the IMCS VM using vCenter UI, reserve the whole memory, and then change this parameter.

3. Go to Shell Admin and restart the services by stopping and starting the Cisco IMC Supervisor services.

Configuring Mysql Buffer Pool

InnoDB buffer pool is the internal memory used by the mysqld process inside the Cisco IMC Supervisor VM. You must increase the memory based on the load. To modify this pool size, perform the following procedure:

1. Go to `/etc/` and open the `my.cnf` file.
2. Navigate to the innodb_buffer_pool_size parameter.

   For example, if you are managing 1000 servers, then the value must be innodb_buffer_pool_size=3072M.
3. Go to Shell Admin and restart the services and database by stopping and starting the Cisco IMC Supervisor services and database.

Determining Direct Disk Input/Output Speed

1. After Cisco IMC Supervisor VM is deployed, go to the command prompt and enter the dd if=/dev/zero of=test.img bs=4096 count=256000 oflag=direct command. The following output for example, is displayed:

```
[root@localhost ~]# dd if=/dev/zero of=test.img bs=4096 count=256000 oflag=direct
256000+0 records in
256000+0 records out
1048576000 bytes (1.0 GB) copied, 44.0809 s, 23.8 MB/s
```

Note In the above example, 23.8 MB/s is the disk input/output speed.

Upgrading to Cisco IMC Supervisor Version 2.2

Cisco IMC Supervisor 2.2 is available as an appliance. You can upgrade from a 2.1 version to 2.2 using the **Apply Patch** option in the Shell Admin menu. For information about upgrading, see Upgrading Cisco IMC Supervisor, on page 10.

You cannot upgrade from version 2.0 Cisco IMC Supervisor to version 2.2. Any version prior to 2.1 must first be migrated to 2.1 and then upgraded to 2.2. For more information about migrating to release 2.1, see Cisco IMC Supervisor Release Notes, Release 2.1.

Important Cisco IMC Supervisor 2.2 OVF and VHD zip files are created using zip 3.x in CentOS 6.x. For Linux systems, you can extract the zip files with unzip 6.x or higher or with the latest version of the 7-Zip archiving tool. For Windows systems, you can extract the zip files with the native Extract All in Windows Explorer for Windows 10 and Windows Server 2012 R2 or with the latest versions of archiving tools such as 7-Zip or WinRAR.

Upgrading Cisco IMC Supervisor

Important Cisco IMC Supervisor Release 2.2 to Release 2.2(0.6) are no longer available for download. You must upgrade immediately to release 2.2(1.x). If you have Cisco IMC Supervisor version prior to release 2.2(0.3) installed, contact Cisco TAC to upgrade to the latest version.

Supported Upgrade Paths for Cisco IMC Supervisor Release 2.2(1.4)

- From Release 2.2(1.3) to Release 2.2(1.4)
- From Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.2(1.1) to Release 2.2(1.4)
- From Release 2.2(1.0) to Release 2.2(1.4)
- From Release 2.2(0.6) to Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.2(0.5) to Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.2(0.4) to Release 2.2(1.2) to Release 2.2(1.4)

- From Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.2(0.2) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.1.x.x to Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4)
- From Release 2.1.x.x to Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4)

Supported Upgrade Paths for Cisco IMC Supervisor Release 2.2(1.3)

- From Release 2.2(1.2) to Release 2.2(1.3)
- From Release 2.2(1.1) to Release 2.2(1.3)
- From Release 2.2(1.0) to Release 2.2(1.3)
- From Release 2.2(0.6) to Release 2.2(1.2) to Release 2.2(1.3)
- From Release 2.2(0.5) to Release 2.2(1.2) to Release 2.2(1.3)
- From Release 2.2(0.4) to Release 2.2(1.2) to Release 2.2(1.3)
- From Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3)
- From Release 2.2(0.2) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3)
- From Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3)
- From Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3)
- From Release 2.1.x.x to Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3)
- From Release 2.1.x.x to Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3)

Supported Upgrade Paths for Cisco IMC Supervisor Release 2.2(1.2)

- From Release 2.2(1.1) to Release 2.2(1.2)

  While upgrading from Release 2.2(1.1) to release 2.2(1.2), use the **Apply Signed Patch** from the Cisco IMC Supervisor Shell menu. For more information on signed patches, see Digitally Signed Images, on page 14, Requirements for Verifying Digitally Signed Images, on page 14 and Verifying a Digitally Signed Image, on page 14.

- From Release 2.2(1.0) to Release 2.2(1.2)
- From Release 2.2(0.6) to Release 2.2(1.2)
- From Release 2.2(0.5) to Release 2.2(1.2)
- From Release 2.2(0.4) to Release 2.2(1.2)
- From Release 2.2(0.3) to Release 2.2(1.2)
- From Release 2.2(0.2) to Release 2.2(0.3) to Release 2.2(1.2)
- From Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2)
- From Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2)

- From Release 2.1.x.x to Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2)
- From Release 2.1.x.x to Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2)

Supported Upgrade Paths for Cisco IMC Supervisor Release 2.2(1.1)

- From Release 2.2(1.0) to Release 2.2(1.1)
- From Release 2.2(0.6) to Release 2.2(1.1)
- From Release 2.2(0.5) to Release 2.2(1.1)
- From Release 2.2(0.4) to Release 2.2(1.1)
- From Release 2.2(0.3) to Release 2.2(1.1)
- From Release 2.2(0.2) to Release 2.2(0.3) to Release 2.2(1.1)
- From Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.1)
- From Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.1)
- From Release 2.1.x.x to Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.1)
- From Release 2.1.x.x to Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.1)

Supported Upgrade Paths for Cisco IMC Supervisor Release 2.2(1.0)

- From Release 2.2(0.6) to Release 2.2(1.0)
- From Release 2.2(0.5) to Release 2.2(1.0)
- From Release 2.2(0.4) to Release 2.2(1.0)
- From Release 2.2(0.3) to Release 2.2(1.0)
- From Release 2.2(0.2) to Release 2.2(0.3) to Release 2.2(1.0)
- From Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.0)
- From Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.0)
- From Release 2.1.x.x to Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.0)
- From Release 2.1.x.x to Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.0)

The following procedure allows you to upgrade Cisco IMC Supervisor.

Before you begin

- Download the Cisco IMC Supervisor Release <version> from http://www.cisco.com.
- Place the software in the FTP or HTTP server that you plan to use to install the upgrade.
- If NFS mount is used for application storage, disable it before you apply a patch. If you do not, the upgrade will fail.
- Obtain access to a secure shell (SSH) application.
- Ensure your system has 100GB disk space available for the upgrade.

Before you start to upgrade the version, shut down the VM, and add the secondary hard disk of 100GB size. Restart the system and wait for the user interface to be available to upgrade to release 2.2.

Note We recommend that you take a snapshot of the VM before you begin the upgrade. If you do this, you do not need to back up the existing configuration database through an FTP server.

Procedure

Step 1 Open your SSH application and enter the Cisco IMC Supervisor appliance IP address and port number.

Step 2 Log in to Cisco IMC Supervisor with your credentials.

Step 3 If you are upgrading from version 2.2(1.3) to version 2.2(1.4), from the Cisco IMC Supervisor Shell Menu, choose **Apply Signed Patch**.

Step 4 If you are upgrading from a version prior to 2.2(1.1) to version 2.2(1.4), you have to manually verify the digitally signed image. See Requirements for Verifying Digitally Signed Images, on page 14.

a) From the Cisco IMC Supervisor Shell Menu, choose **Apply Patch**.

For this command, use the digitally signed zip file that is included within the downloaded patch file. For example: `cimcs_patch_2_2_1_4_xxxx.zip`

Step 5 You are prompted to confirm if all the services can be stopped and if the database backup can be taken. Enter **y** to confirm both these actions.

Step 6 When prompted, for the database backup, provide the FTP server IP, login credentials and server path of the FTP server.

Step 7 When prompted, enter the location of the patch. For example, *`<transfer protocol type>: // username : password @ hostname|IP_address / software_location_and_name`*

Supported transfer protocol types are HTTP, and Local File System. You can use the following examples:

- HTTP — **http://test.cisco.com/downloads/<filename.zip>**
- Local File System — **file:////opt/infra/uploads/<filename.zip>**

Step 8 Wait for the download and installation to complete.

Note The database and the services are restarted. The upgrade process is not complete or successful until the Cisco IMC Supervisor services have started, Cisco IMC Supervisor is available, the login screen is displayed, and the admin user can log in to Cisco IMC Supervisor. All services must be started before you attempt to perform other shelladmin procedures, such as apply additional patches, take a database backup, or restore a database from a backup.

Step 9 When the upgrade is complete, choose **11) Show Version** in shelladmin to verify the current version of Cisco IMC Supervisor.

Note
- To view the status of services, choose **2) Display Services Status**.

Digitally Signed Images

Cisco IMC Supervisor release 2.2(1.2) images are delivered in digitally signed zip files. These signed zip files are wrapped in a container zip file that includes the following:

- Digitally signed zip file—Contains the Cisco IMC Supervisor installation or upgrade image
- Verification program—Verifies the certificate chain and signature. During certificate chain validation, the program verifies the authenticity of the end-entity certificate using Cisco's SubCA and root CA certificates. Then, the authenticated end-entity certificate is used to verify the signature.
- Digital signature file—Contains the signature that you can verify before installation or upgrade.
- Certificate file—Enables you to verify the digital signature. This Cisco-signed x.509 end-entity certificate contains a public key that can be used to verify the signature. This certificate is chained to the Cisco root posted on http://www.cisco.com/security/pki/certs/crcam2.cer.
- ReadMe file—Provides the information and instructions required to verify the digitally signed zip file.

Verify the image offline. Once the image is verified, you can begin the installation or upgrade of Cisco IMC Supervisor.

Requirements for Verifying Digitally Signed Images

Before you verify a Cisco IMC Supervisor digitally signed image, ensure that you have the following on your local machine:

- Connectivity to https://www.cisco.com during the verification process.
- Python 3.6.8
- OpenSSL

Verifying a Digitally Signed Image

Before you begin

Download the Cisco IMC Supervisor image from Cisco.com.

Procedure

Step 1 Unzip the file you downloaded from Cisco.com and verify that it contains the following files:

- ReadMe file
- Digitally signed zip file.
- Certificate file, for example `UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer`
- Digital signature generated for the image.
- Signature verification program, for example `cisco_x509_verify_release.py3`

Step 2 Review the instructions in the ReadMe file.

Note If there are any differences between these instructions and those in the ReadMe, follow the ones in the ReadMe.

Step 3 Run the signature verification program from the directory where you have unzipped the downloaded content.

Example: Signature Verification for Upgrade Patch

```
python3 ./cisco_x509_verify_release.py3 -e UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
-i cimcs_patch_2_3_0_0_67198.zip -s cimcs_patch_2_3_0_0_67198.zip.signature -v dgst -sha512
```

Step 4 Review the output and ensure that the verification has succeeded.

Example: Expected Output for Upgrade

```
Downloading CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully downloaded and verified crcam2.cer.
Downloading SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer
...
Successfully downloaded and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully verified the signature of cimcs_patch_2_2_1_2_67198.zip using
UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
```

New and Changed Features

This section provides an overview of the significant new and changed features in this release. This section does not provide an exhaustive list of all enhancements included in this release.

New and Changed Features in Release 2.2(0.0)

New User Interface

This release introduces a new and improved HTML-5 based administrative portal that replaces the previously available user interface. When you log in to Cisco IMC Supervisor, by default, the HTML-5 user interface is displayed. The earlier version of the interface, now referred to as the Classic View, is still available, but will be removed in a subsequent release. To enable the Classic View to be displayed when you login, choose **Edit Profile**, and check **Login with Classic View**.

The following are some of the key features of the new interface:

- Change in the navigation menu—In earlier releases, you could access pages using the main menu bar. The main menu bar is now available as a side bar. You can use your mouse or the cursor to hover over an option on the side navigation bar, and then click any of the menu options.
- Absence of user interface labels—The user interface no longer includes labels for actions such as Add, Edit, Delete, Export, Filter, and so on. These actions are represented only with icons. If you use your mouse or cursor to hover over the icon, the label displays the action you can perform using that icon.
- Context-sensitive Online Help—If you click the Help icon in the user interface, the online help system displays information on the screen that you currently are accessing.

Documented in the *Cisco IMC Supervisor Management Guide, Release 2.2*.

Support for New Servers

This release introduces support for the following servers:

- Cisco UCS C240 M5
- Cisco UCS C220 M5
- Cisco ENCS 5406
- Cisco ENCS 5408
- Cisco ENCS 5412

New Cisco UCS Hardware Compatibility Report

Cisco UCS Hardware Compatibility Report is available for Cisco C-Series/S-Series servers.

Support for Managing Controller Drive Security

Cisco IMC Supervisor provides the ability to enable, modify, and disable drive security at the physical and the virtual drive level. Also, it provides the ability to set the Security Key and Security ID for the controller with Local Key Management support. However, the Remote Key Management is not available.

Implementing a New CSV Format

The Auto Discovery Profile using a CSV file has undergone a change in the CSV format. The earlier format of providing Key-Value pairs is no longer supported. To use the new format, you must provide the parameters as comma separated values as shown in the CSV File template.

The CSV format available in prior releases will no longer work with Release 2.2.

Support for Cisco IMC Release 3.0(x)

This release of Cisco IMC Supervisor includes support for the following new features of Cisco IMC release 3.0(x):

- Enhancement to Network Security Policy

  You can specify IP filtering properties along with IP blocking properties.

- Enhancement to BIOS Policy

  An administrator password must be set in the BIOS policy which will be used as the Power On password.

- Enhancement to Precision Boot Order Policy

  You can set the parameters for a One Time Boot device.

- Setting asset tag for a property

  You can set the asset tag property for all supported servers.

- Support for Password Expiration Policy

  You can create a password expiration policy and associate with a User policy.

- Support for Smart Information for Solid State Drive

Support for smart information for a Solid State Drive (SSD) has been introduced in the Storage Controller screens.

Support for Cisco HyperFlex Edge

This release of Cisco IMC Supervisor supports Cisco HyperFlex Edge, a HyperFlex Systems solution for remote and branch office (ROBO) and edge environments. For more information, see the Cisco HyperFlex Edge Deployment Guide.

Following are the servers supported:

- HX220C-M4
- HX240C-M4
- HXAF240C-M4SX

Rebranding for Cisco UCS C3260 Dense Storage Rack Server

The Cisco UCS C3260 Dense Storage Rack Server is now changed to Cisco UCS S3260 Storage Servers.

Changes in the UI to accept Cisco.com Credentials

Firmware Policy and Updating Cisco IMC Supervisor automatically accept Cisco.com credentials. You can configure these credentials centrally by choosing **Administration** > **System** > **Cisco.com**. All features that require Cisco.com credentials will use the details specified on this screen.

Enhancement to FlexFlash Policy

FlexFlash policy includes options to enable and erase the virtual drives for the Mirror and Util firmware modes.

Support for Host Image Mapping

Host Image Mapping is a commonly used feature for E-Series servers, using which you can apply a profile and trigger an upgrade action to upgrade the Cisco IMC. In addition, you can map, unmap and delete the added image.

Changes to Proxy Server Configuration

Folowing are the changes made to the proxy server configuration:

- Proxy server configuration is now available from **Administration** > **System** menu.
- This release includes proxy server configuration with authentication.

Important Cisco IMC Supervisor, Release 2.2 is no longer available for download. It is recommended that you must upgrade immediately to release 2.2(1.0).

Updated Support in Cisco IMC Supervisor Patch Release 2.2(0.2)

Cisco IMC Supervisor patch release 2.2(0.2) introduces support for the following servers:

- UCS E-1120D M3
- UCS E-180D M3
- HX220C-M5S
- HXAF220C-M5S
- HX240C-M5SX
- HXAF240C-M5SX

Important Cisco IMC Supervisor, Release 2.2(0.2) is no longer available for download. It is recommended that you must upgrade immediately to release 2.2(1.0).

New and Changed Features in Release 2.2(0.3)

Enhancements to Host Image Mapping on E-series Servers

Host Image Mapping allows you to download a firmware file to Cisco IMC, and upgrade the firmware on E-series servers. Using Cisco IMC Supervisor, you can create a host image mapping profile to download and upgrade either one of the following:

- ISO firmware image
- CIMC image or
- BIOS image

Using Cisco IMC Supervisor, you can download the firmware image on Cisco IMC in one of the following methods:

- Provide a location on the network (an FTP, FTPS, HTTP or HTTPS server) where the firmware file is currently available.
- Choose the firmware file from a location on your system.
- Download the firmware image from www.cisco.com.

Important To perform these tasks, Cisco IMC version 3.2.4 must be installed on the E-series servers. This feature does not work with prior versions of Cisco IMC.

In prior versions of Cisco IMC Supervisor, you accessed the host image functionality from **Policies** > **Manage Policies** > **Host Image Mapping and Profiles**. From release 2.2(0.3) onwards, you must click **Systems** > **Firmware Management** > **Host Image Mapping**.

Important Host image mapping profiles created in prior versions of Cisco IMC Supervisor will no longer work after you upgrade to release 2.2(0.3). You must delete these profiles and create it again after upgrading to release 2.2(0.3).

Documented in the *Cisco IMC Supervisor Rack-Mount Servers Management Guide, Release 2.2(0.3)*.

Introduction of Power Restore Policy for E-series Servers

This release introduces a Power Restore policy that allows you to change the value set for the power restore policy on an E-series server without logging into the Cisco IMC of that server.

Documented in the *Cisco IMC Supervisor Rack-Mount Servers Management Guide, Release 2.2(0.3)*.

Cisco IMC Log and System Event log are disabled on E-series Servers

In Cisco IMC Supervisor versions prior to 2.2(0.2), the HTTP/HTTPS API allows you to query for logs and events with a plain text password. Cisco IMC Supervisor version 2.2(0.2) onwards, an encrypted password is required to query for logs and events on servers. However, support for this encrypted password is not yet available on E-series Cisco IMC. As a result, Active Directory accounts for E-series servers get locked as the encrypted passwords were read as invalid by the E-Series servers. To prevent this issue, starting with version 2.2(0.3), Cisco IMC Log and System Event log are disabled for E-series servers.

Support for Configuring Graceful Timeout on UCS C-series Servers

This release introduces support for configuring a timeout for host systems to shut down before a firmware upgrade process is initiated.

While uploading a firmware image from a local server, or while uploading a firmware image from a network server, you can now specify a timeout period, in minutes, within which the host system must gracefully shut down. You can also enable the host system to forcibly shutdown before the firmware upgrade process is initiated.

Note You can configure graceful timeout for systems running Cisco IMC version 3.1(3a) or higher.

Documented in the *Cisco IMC Supervisor Rack-Mount Servers Management Guide, Release 2.2(0.3)*.

Classic View No Longer Available

From this release onwards, the Classic View of the user interface is no longer available. In release 2.2, administrators could set the system to launch the Classic View user interface for subsequent login sessions. Also, administrators could specify this setting for login sessions of other users as well. These options have now been removed.

Support for Enabling and Disabling HTTP

This release introduces support for enabling and disabling HTTP in Cisco IMC Supervisor.

Starting with Cisco IMC Supervisor version 2.2(0.3), to perform firmware upgrade through Images – Local or through uploading images from a local file system on Cisco IMC versions prior to 3.0(3e), you must enable HTTP using the Shell menu.

Documented in the *Cisco IMC Supervisor Rack-Mount Servers Management Guide, Release 2.2(0.3)* and *Cisco IMC Supervisor Shell Guide, Release 2.2*.

Enhanced Scheduling Capabilities for System Tasks

This release introduces an option to schedule a system task with a **Fixed Delay** option. This option enables a fixed time delay between consecutive executions of a system task. This release also introduces the capability to configure a customized frequency for the system tasks.

Documented in the *Cisco IMC Supervisor Rack-Mount Servers Management Guide, Release 2.2(0.3)*.

Important Cisco IMC Supervisor, Release 2.2(0.3) is no longer available for download. It is recommended that you must upgrade immediately to release 2.2(1.0).

New and Changed Features in Release 2.2(0.4)

Support for Upgrading Firmware from MicroSD cards or FlexFlash cards on Rack Mount Servers

Starting with this release, you can upgrade firmware on rack servers using ISO images from MicroSD cards (for M5 servers) or FlexFlash cards (for M4 servers).

This feature is only supported on Cisco UCS M5 or higher servers running Cisco IMC version 3.1(3a) or higher and on Cisco UCS M4 servers running Cisco IMC version 4.0(2) or higher.

Documented in the *Cisco IMC Supervisor Management Guide, Release 2.2(0.4)*.

Support for Scheduling Upgrades Using Host Image Mapping Profiles on Rack Mount Servers

Starting with this release, new scheduling options have been introduced in the **Run Upgrade** and **Apply Profile** screens for host image profile procedures. Using these options, you can schedule these processes to run at a later point in time.

Documented in the *Cisco IMC Supervisor Management Guide, Release 2.2(0.4)*.

Introduction of Power Restore Policy for Cisco UCS C-series Servers

Starting with this release, you can configure a power restore policy for Cisco UCS C-series servers. You cannot create this policy on ENCS servers.

Documented in the *Cisco IMC Supervisor Management Guide, Release 2.2(0.4)*.

Enhancements to Email Alerts on Faults

Starting with this release, you can configure the system to send email alerts for all open faults, based on the configured email alert rule, irrespective of whether you have been notified previously for a fault or not. A new option **Send alert for all faults every 24 hours** has been introduced in the **Add Email Alert Rule** screen. If you select this option, the system will send email alerts every 24 hours for all open faults that match the specified alert rule.

Documented in the *Cisco IMC Supervisor Management Guide, Release 2.2(0.4)*.

Important Cisco IMC Supervisor, Release 2.2(0.4) is no longer available for download. It is recommended that you must upgrade immediately to release 2.2(1.0).

New and Changed Features in Release 2.2(0.5)

Defect Fixes

This release of Cisco IMC Supervisor includes only defect fixes and no new features.

Important Cisco IMC Supervisor, Release 2.2(0.5) is no longer available for download. It is recommended that you must upgrade immediately to release 2.2(1.0).

New and Changed Features in Release 2.2(0.6)

Defect Fixes

This release of Cisco IMC Supervisor includes only defect fixes and no new features.

Important Cisco IMC Supervisor, Release 2.2(0.6) is no longer available for download. It is recommended that you must upgrade immediately to release 2.2(1.0).

New and Changed Features in Release 2.2(1.0)

Enhancements to BIOS Policy

Starting with this release, support included for new BIOS tokens that were introduced by the IMC firmware release 4.0.(4b).

New and Changed Features in Release 2.2(1.1)

Enhancements to Zoning Policy

Starting with this release of Cisco IMC Supervisor, you can use the zoning policy to assign physical drives to a specific controller slot on servers that support dual controllers such as Cisco UCS S3260 Dual Raid Controller (UCS-S3260-DRAID). However, choosing a specific controller slot is not mandatory. If you do not choose a specific controller slot, then the ownership of the physical drives is assigned to the first controller slot that is available on the server that you selected.

Documented in the *Cisco IMC Supervisor Rack-Mount Servers Management Guide, Release 2.2(1.1)*.

Enhancements to RAID Policy

Following are the enhancements introduced in this release of Cisco IMC Supervisor to confguring a RAID policy:

- **Deriving the Policy**
    - **Drive Security**

Drive security for the RAID policy is retrieved only if the security properties, such as the security Key ID, are common for all controller slots associated with the server. If the security Key ID is not common across all controller slots in the server, deriving the policy will fail.

- **Virtual Drive Configuration**
    - While creating a RAID policy based on an existing server configuration, virtual drives from all controller slots in the server are retrieved and listed in the **Virtual Drives Configuration** screen of the RAID policy. In addition, all related disk group policies are also created.

- **Applying the policy**

  While applying the policy, the Drive Security configuration is applied commonly to all controllers that are associated with the server.

  Applying the policy to virtual drives is determined by the disk group policy associated with the virtual drives. If a disk group includes slots from multiple controllers in the server, then the **Apply Policy** action fails. But a single RAID policy can include virtual drives with disk groups that belong to different controllers.

  The **Enable JBOD/UnConfigured Good** configuration is applied to unused disks that belong to all the controllers associated with the server.

Introduction of New Option in the Shell Admin Console

This release of Cisco IMC Supervisor introduces a new option, **Apply Signed Patch**, in the Shell Admin console. You can use this option to upgrade your system from release 2.2(1.1) to a subsequent release.

Enabling Faster Download of Firmware Images

Starting with this release of Cisco IMC Supervisor, you can enable faster download of firmware images if you configure a proxy server in Cisco IMC Supervisor. To configure a proxy server, choose **Administration** > **System** > **Proxy Configuration**.

Important Support for downloading firmware images and receiving automated updates of Cisco IMC Supervisor on versions prior to 2.2(1.1) is deprecated. You are required to upgrade to Cisco IMC Supervisor 2.2(1.1) or later to continue using these features.

Changes to Managing E-series Servers

The following actions have been disabled for E-series servers:

- Downloading local firmware images
- Enabling a Cisco.com profile for Host Image Mapping

New and Changed Features in Release 2.2(1.2)

Removed Proxy Configuration Prerequisite for Faster Download of Firmware Images

Cisco IMC Supervisor version 2.2(1.1) supports faster download of firmware images only when a proxy server is configured. Starting with release, the requirement of a proxy server configuration to download firmware images faster has been removed.

Important Support for downloading firmware images and automated updates of Cisco IMC Supervisor on versions prior to 2.2(1.1) is deprecated. You are required to upgrade to Cisco IMC Supervisor 2.2(1.1) or later to continue using these features.

Enhancements to VIC Adapter Policy

Starting with this release, for a VIC adapter policy, Cisco IMC Supervisor allows you to enable or disable port channel configuration. This port channel configuration is applicable only for Cisco UCS VIC 1455 and 1457 adapters.

Note

- By default, port channel configuration is enabled on Cisco UCS VIC 1455 and 1457 adapters.
- When you change the port channel configuration, all previously created vNICs and vHBAs are deleted and the configuration is restored to factory defaults.
- VNTAG mode is supported only in the port-channel mode.

Documented in the *Cisco IMC Supervisor Management Guide, Release 2.2(1.2)*.

New and Changed Features in Release 2.2(1.3)

Enhancements to VIC Adapter Policy

Starting with this release, for a VIC adapter policy, Cisco IMC Supervisor allows you to configure the Admin Forward Error Correction (FEC) mode for the following adapters:

- Cisco VIC 1455
- Cisco VIC 1457
- Cisco VIC 1495
- Cisco VIC 1497

By default, four ports are configured for these adapters and you cannot delete them. However, the number of ports configured with the Admin FEC mode varies depending on the adapter you have selected. For example, in a Cisco VIC 1497 adapter, there are only two ports. Hence, the Admin FEC mode is configured only on the first two ports (port 0 and port1), ignoring the remaining ports (port 2 and port 3). For the existing policies, this field is set to **Auto**. But you can change this value to **cl91**, **cl74**, and **Off**.

Note **cl74** option is not supported for Cisco VIC 1495 and Cisco VIC 1497 adapters.

In addition to the default vNICs and vHBAs configured on these adapters, you can create additional vNICs and vHBAs based on the selected port channel state.

Note When you modify the port channel configuration for an adapter, all previously configured vNICs and vHBAs are deleted and the configuration is restored to the factory default settings.

New and Changed Features in Release 2.2(1.4)

Introduction of SFTP User Configuration

Starting with this release, you will need to configure a password for an SFTP user in Cisco IMC Supervisor. This user configuration is used in server diagnostics and tech support processes to transfer files to Cisco IMC Supervisor using SFTP. This SFTP user configuration replaces the previously available SCP user configuration functionality. After installing or upgrading to this release, you must configure the password for the SFTP user. To do so, choose **Administration** > **Users and Groups** > **SFTP User Configuration** and enter a password.

Documented in the Cisco IMC Supervisor Rack-Mount Servers Management Guide, Release 2.2(1.4).

Support for New Versions of Cisco IMC

This release introduces support for Cisco IMC version 4.1 and 4.1.2a. In addition to new features, these software versions include support for new BIOS tokens. All the newly introduced BIOS tokens are now displayed in the Cisco IMC Supervisor user interface while creating a BIOS policy. For information on the BIOS tokens introduced in the Cisco IMC releases, see the CLI and GUI confguration guides available at:

https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-integrated-management-controller/products-installation-and-configuration-guides-list.html

REST API Changes

Following are the APIs introduced in this release:

- **AssociatedHardwareProfilesbyServer**—Displays the list of policies associated with a specific rack server account.
- **AssociatedServersByPolicyName**—Displays the list of rack servers that are associated with a specific hardware profile.

Documented in the Cisco IMC Supervisor REST API Cookbook, Release 2.2.

Support for Downloading Images and Receiving Automated Updates

Automated Software Distribution (ASD) apis to enable support for downloading firmware images and updates has been updated to a newer version 4.0. The earlier version 3 of ASD API will be sunset end of Q2FY22 (February, 2022). In order to be able to continue supporting the feature, you have to upgrade to Cisco IMC Supervisor 2.2(1.4) or later.

Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Open Bugs

All open bugs for this release are available in the Cisco Bug Search Tool through the following searches.

The results of that search include workarounds for the open bugs, if any.

Open Bugs in Release 2.2

You can find detailed information about all open bugs in Release 2.2 through the open bug search for Release 2.2. This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter `Cisco IMC Supervisor 2.x`.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter `2.2`.
Filter	Choose **Open** from the **Status** drop-down list.

Open Bugs in Release 2.2(0.1)

You can find detailed information about all open bugs in Release 2.2 through the open bug search for Release 2.2(0.1). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(0.1).
Filter	Choose **Open** from the Status drop-down list.

Open Bugs in Release 2.2(0.2)

You can find detailed information about all open bugs in Release 2.2(0.2) through the open bug search for Release 2.2(0.2). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(0.2).
Filter	Choose **Open** from the Status drop-down list.

Open Bugs in Release 2.2(0.3)

You can find detailed information about all open bugs in Release 2.2(0.3) through the open bug search for Release 2.2(0.3). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(0.3).
Filter	Choose **Open** from the Status drop-down list.

Open Bugs in Release 2.2(0.4)

You can find detailed information about all open bugs in Release 2.2(0.4) through the open bug search for Release 2.2(0.4). This search uses the following parameters:

Important Cisco IMC Supervisor Release 2.2(0.4) is now a deferred release. It is no longer available for download.

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(0.4).
Filter	Choose **Open** from the Status drop-down list.

Open Bugs in Release 2.2(0.5)

You can find detailed information about all open bugs in Release 2.2(0.5) through the open bug search for Release 2.2(0.5). This search uses the following parameters:

Important Cisco IMC Supervisor Release 2.2(0.5) is now a deferred release. It is no longer available for download.

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(0.5).
Filter	Choose **Open** from the Status drop-down list.

Open Bugs in Release 2.2(0.6)

You can find detailed information about all open bugs in Release 2.2(0.6) through the open bug search for Release 2.2(0.6). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(0.6).
Filter	Choose **Open** from the Status drop-down list.

Open Bugs in Release 2.2(1.0)

You can find detailed information about all open bugs in Release 2.2(1.0) through the open bug search for Release 2.2(1.0). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(1.0).
Filter	Choose **Open** from the Status drop-down list.

Open Bugs in Release 2.2(1.1)

You can find detailed information about all open bugs in Release 2.2(1.1) through the open bug search for Release 2.2(1.1). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(1.1).
Filter	Choose **Open** from the Status drop-down list.

Open Bugs in Release 2.2(1.2)

You can find detailed information about all open bugs in release 2.2(1.2) through the open bug search for Release 2.2(1.2). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(1.2).
Filter	Choose **Open** from the Status drop-down list.

Open Bugs in Release 2.2(1.3)

You can find detailed information about all open bugs in release 2.2(1.3) through the open bug search for Release 2.2(1.3). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(1.3).
Filter	Choose **Open** from the Status drop-down list.

Open Bugs in Release 2.2(1.4)

You can find detailed information about all open bugs in release 2.2(1.4) through the open bug search for Release 2.2(1.4). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(1.4).
Filter	Choose **Open** from the Status drop-down list.

Resolved Bugs

All resolved bugs for this release are available in the Cisco Bug Search Tool through the following searches.

Resolved Bugs in Release 2.2

You can find detailed information about all fixed bugs in Release 2.2 through the fixed bug search for Release 2.2. This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter `Cisco IMC Supervisor 2.x`.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter `2.2`.
Filter	Choose **Fixed** from the **Status** drop-down list.

Resolved Bugs in Release 2.2(0.1)

You can find detailed information about all fixed bugs in Release 2.2(0.1) through the fixed bug search for release 2.2(0.1). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(0.1).
Filter	Choose **Fixed** from the Status drop-down list.

Resolved Bugs in Release 2.2(0.2)

You can find detailed information about all fixed bugs in Release 2.2(0.2) through the fixed bug search for release 2.2(0.2). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(0.2).
Filter	Choose **Fixed** from the Status drop-down list.

Resolved Bugs in Release 2.2(0.3)

You can find detailed information about all resolved bugs in Release 2.2(0.3) through the fixed bug search for Release 2.2(0.3). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(0.3).
Filter	Choose **Fixed** from the Status drop-down list.

Resolved Bugs in Release 2.2(0.4)

You can find detailed information about all resolved bugs in Release 2.2(0.4) through the resolved bug search for Release 2.2(0.4). This search uses the following parameters:

Important Cisco IMC Supervisor Release 2.2(0.4) is now a deferred release. It is no longer available for download.

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(0.4).
Filter	Choose **Fixed** from the Status drop-down list.

Resolved Bugs in Release 2.2(0.5)

You can find detailed information about all resolved bugs in Release 2.2(0.5) through the resolved bug search for Release 2.2(0.5). This search uses the following parameters:

Important Cisco IMC Supervisor Release 2.2(0.5) is now a deferred release. It is no longer available for download.

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(0.5).
Filter	Choose **Fixed** from the Status drop-down list.

Resolved Bugs in Release 2.2(0.6)

You can find detailed information about all resolved bugs in Release 2.2(0.6) through the resolved bug search for Release 2.2(0.6). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(0.6).
Filter	Choose **Fixed** from the Status drop-down list.

Resolved Bugs in Release 2.2(1.0)

You can find detailed information about all resolved bugs in Release 2.2(1.0) through the resolved bug search for Release 2.2(1.0). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(1.0).
Filter	Choose **Fixed** from the Status drop-down list.

Resolved Bugs in Release 2.2(1.1)

You can find detailed information about all resolved bugs in Release 2.2(1.1) through the resolved bug search for Release 2.2(1.1). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(1.1).
Filter	Choose **Fixed** from the Status drop-down list.

Resolved Bugs in Release 2.2(1.2)

You can find detailed information about all resolved bugs in Release 2.2(1.2) through the resolved bug search for Release 2.2(1.2). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(1.2).
Filter	Choose **Fixed** from the Status drop-down list.

Resolved Bugs in Release 2.2(1.3)

You can find detailed information about all resolved bugs in Release 2.2(1.3) through the resolved bug search for Release 2.2(1.3). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(1.3).
Filter	Choose **Fixed** from the Status drop-down list.

Resolved Bugs in Release 2.2(1.4)

You can find detailed information about all resolved bugs in Release 2.2(1.4) through the resolved bug search for Release 2.2(1.4). This search uses the following parameters:

Field	Parameter
Product drop-down list	Choose **Series/Model** and enter Cisco IMC Supervisor 2.x.
Releases drop-down list	Choose **Affecting or Fixed in these Releases** and enter 2.2(1.4).

Field	Parameter
Filter	Choose **Fixed** from the Status drop-down list.

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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