Cisco IMC Supervisor Installation Guide for VMware vSphere and Microsoft Hyper-V, Release 2.2

First Published: 2017-07-11

Last Modified: 2023-10-13

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

CONTENTS

Preface

This preface contains the following sections:

Audience

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

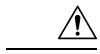
- Server administration
- Storage administration
- Network administration
- Network security
- Virtualization and virtual machines

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.

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

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



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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

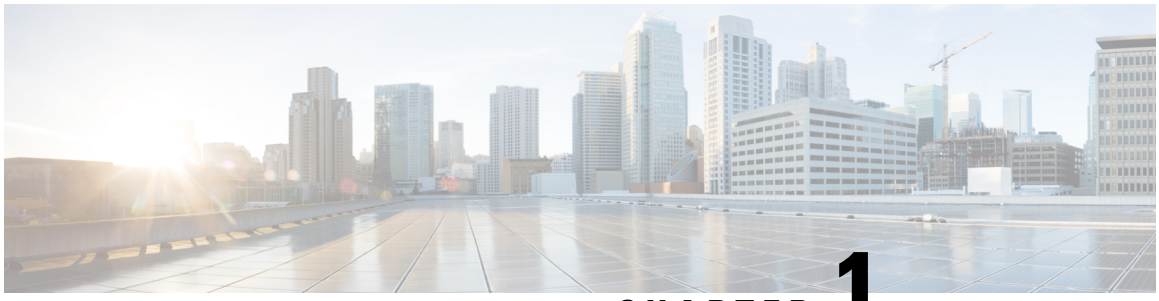
Documentation Feedback

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation.

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Overview

This chapter contains the following topics:

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

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 Deployment and Scalability.

Minimum Firmware Versions

Servers	Minimum Firmware Version
UCS C-series Servers	1.5(4)
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
- ESXi 7.0
- ESXi 7.0 U3
- 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
Minimum write speed for storage	10 MB/sec

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

Element	Small Deployment (1 - 250 rack servers)	Medium Deployment (251 - 500 rack servers)	Large Deployment (501 - 1000 rack servers)
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
Database 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 Database Buffer Pool

InnoDB buffer pool is the internal memory used by the mariadbd 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.

Supported Firewall Ports

The list of applicable services and ports are listed in the following table.

Service	Port Number
Servers	Minimum Firmware Version
SSH Port	22
HTTP (S)	80/443
DHCP	UDP 67 & 68
Active Directory	TCP / UDP 389/636 & TCP 3268/3269
DNS	TCP/UDP 53
NTP	TCP/UDP 123
Database	3306
Cisco IMC Supervisor ↔ IMC Connectivity	TCP 80/443
Sun-RPC (Remote Procedure Call) Port used for executing NTP, FTP and other remote operations.	TCP/111
Adobe flash Socket Policy Server used by Cisco IMC Supervisor.	TCP/843
Webserver (/HTTP) port to access GUI and API in non-secure mode.	TCP/8080
Webserver (/HTTPS) port to access GUI and API in secure mode.	TCP/8443
The msgsrvr port internally connected with appliance.	TCP/8787

Note If these ports and protocols are blocked by a firewall, you may experience timeouts or internal error when you are upgrading Cisco IMC Supervisor.

Starting with Cisco IMC Supervisor Release 2.2(0.3), port 3306 is no longer an open port. Use the option in the Shell Admin console (Grant/Deny client access to Database port 3306) to decide the external clients that can connect to port 3306.

About Licenses

Cisco IMC Supervisor requires you to have the following valid licenses:

- A Cisco IMC Supervisor base license.
- A Cisco IMC Supervisor bulk endpoint enablement license that you install after the Cisco IMC Supervisor base license.
- A Cisco IMC Supervisor advanced license. You can add, edit, and delete policies and profiles with the base license but you cannot apply a policy or a profile to a server without the advanced license. An error occurs if this license is unavailable when you apply a policy.
- A default embedded Cisco IMC Supervisor evaluation license. The evaluation license is generated automatically when the end user installs Cisco IMC Supervisor and all the services start for the first time. It is applicable for 50 servers.

Important

- If you are using an evaluation license for Cisco IMC Supervisor, note that when this license expires (90 days from the date the license is generated), retrieving inventory and system health information, such as faults, will not work. You will not be able to refresh system data, or even add new accounts. At that point, you must install a perpetual license to use all features of Cisco IMC Supervisor.
- If the number of servers you have added during evaluation exceeds the number of server license purchased, inventory collection will go through fine for the servers already added during evaluation, but will prevent you from adding new servers. For example, if you have added about 100 servers during evaluation and you have purchased a 25 server license, once the evaluation license expires, you will be unable to add new servers. Also, you will be unable to perform configuration related operations without an advanced license.
- While discovering and importing servers, if the number of imported servers exceed the license utilization limit, Cisco IMC Supervisor imports servers only until the limit and displays an error for additional servers.
- Licenses for Cisco IMC Supervisor is based on the number of servers. Cisco UCS S3260 chassis is a 2-server node. As a result, in Cisco IMC Supervisor, the license utilization for this chassis is considered as 2 servers.

The process for obtaining and installing the licenses is the same. For obtaining a license, perform the following procedures:

1. Before you install Cisco IMC Supervisor, generate the Cisco IMC Supervisor license key and claim a certificate (Product Access Key).
2. Register the Product Access Key (PAK) on the Cisco software license site, as described in Fulfilling the Product Access Key, on page 8.
3. After you install Cisco IMC Supervisor, update the license as described in Updating the License, on page 25.
4. After the license has been validated, you can start to use Cisco IMC Supervisor.

For various other licensing tasks you can perform, see Licensing Tasks, on page 9.

Fulfilling the Product Access Key

Perform this procedure to register the Product Access Key (PAK) on the Cisco software license site.

Before you begin

You need the PAK number.

Procedure

Step 1 Navigate to the Cisco Software License website.

Step 2 If you are directed to the Product License Registration page, you can take the training or click **Continue to Product License Registration**.

Step 3 On the Product License Registration page, click **Get New Licenses from a PAK or Token**.

Step 4 In the **Enter a Single PAK or TOKEN to Fulfill** field, enter the PAK number.

Step 5 Click **Fulfill Single PAK/TOKEN**.

Step 6 Complete the additional fields in **License Information** to register your PAK:

Field	Description
Organization Name	The organization name.
Site Contact Name	The site contact name.
Street Address	The street address of the organization.
City/Town	The city or town.
State/Province	The state or province.
Zip/Postal Code	The zip code or postal code.
Country	The country name.

Step 7 Click **Issue Key**.

The features for your license appear, and an email with the Digital License Agreement and a zipped license file is sent to the email address you provided.

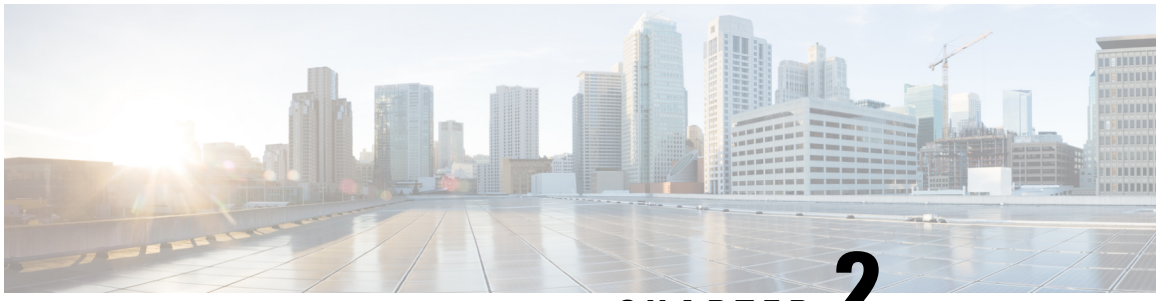
Licensing Tasks

You can use the **License** menu to view the license details and the usage of resources. The following licensing procedures are available from **Administration** > **License** menu.

Tab	Description
License Keys	This tab displays the details of the license used in Cisco IMC Supervisor. You can also use this tab to update, replace and migrate the license. You can update the license when a new version of Cisco IMC Supervisor is available.
License Utilization	This tab shows the licenses in use and details about each license, including license limit, available quantity, status, and remarks. License audits can also be run from this page. **Note** Licenses for Cisco IMC Supervisor is based on the number of servers. Cisco UCS S3260 chassis is a 2-server node. As a result, in Cisco IMC Supervisor, the license utilization for this chassis is considered as 2 servers.
Resource Usage Data	This tabs displays the details of the various resources used.
Deactivated Licenses	This tab displays a list of deactivated licenses.

Support for Third Party Software

Cisco IMC Supervisor has not tested or qualified any third software to be installed or used, such as security agents, etc. Such third party software installation of any kind may negatively affect the proper functioning of the product and is done at your own risk.



CHAPTER 2

Installing Cisco IMC Supervisor on VMware vSphere

Installing Cisco IMC Supervisor on VMware vSphere

Before you begin

You must have system administrator privileges for VMware vSphere or vCenter

Note If you want to use a static IP address rather than DHCP, you must know the following information:

- IP address
- Subnet mask
- Default gateway

Note VMware vSphere ESXI 6.5 , 6.7, 7.0, and 7.0 U3 are the qualified version for OVA deployment. Ensure that the IP address of the source is different from the IP address of the target system.

Procedure

Step 1 Log in to VMware vSphere Client.

Step 2 In the **Navigation** pane, click the vSphere host on which you want to deploy.

Step 3 Choose **File** > **Deploy OVF Template**.

The **Deploy OVA Template** window appears.

Step 4 On the **Source** screen pane of the**Deploy OVF Template**, do one of the following to choose your OVA source location:

- If the OVA file is stored on your local computer, browse to the location, choose the file, and click **Open**.
- If the OVA file is stored on a server on your local area network, enter the location of the file including the IP address or fully qualified domain name of the server.

Step 5 On the **OVA Template Details** screen, verify the details and click **Next**.

Step 6 On the **Name and Location** screeen, do the following:

a) In the **Name** field, enter a unique name for the VM.
b) In the **Inventory Location** area, choose the location where you want the VM to reside.
c) Click **Next**

Step 7 Select a **compute resource** by selecting the **IP address** under which the VM has to be tagged and click **Next**.

Review the template details. Details about the publisher, Download size, the size on the disk and extra configuration will be displayed.

Step 8 On the **Storage** screen, choose the storage location for the VM and click Next.

Step 9 In the **Disk Format** pane, from the drop down options available, choose one of the following and click **Next**:

- **Thin Provisioned** format—To allocate storage on demand as data is written to disk.
- **Thick Provisioned (Lazy Zeroed)** format —To allocate storage immediately in thick format.
- **Thick Provisioned (Eager Zeroed)** format —To allocate storage in thick format. It might take longer to create disks using this option.

By default 100gb of data storage will be allocated.

Step 10 In the **Network Mapping** pane, choose network for VM and click **Next**.

Step 11 In the **Properties** pane, enter the following information and click **Next**:

- Gateway IP Address
- Management IP Address
- Management IP Subnet Mask
- Root Password

  Note The root password can be configured with any value during deployment.

- Shelladmin Password

  Note Shelladmin password can be configured with any value during deployment.

Step 12 In the **Ready to Complete** pane, verify the options selected, and click **Finish**.

Make sure you have sufficient vCPU and memory to power on the VM.

Step 13 After the appliance has booted up, copy and paste the Cisco IMC Supervisor IP address that appears into a supported web browser to access the **Login** page.

Step 14 On the **Login** page, enter `admin` as the username and `admin` for the login password.

What to do next

Update your license.

Configuring the Network Interface using Shelladmin

This procedure is optional.

Procedure

Step 1 Log in to the Cisco IMC Supervisor VM console using the Shell admin credentials configured during deployment.

Step 2 Choose `Configure Network Interface`.

Step 3 At the `Do you want to Configure DHCP/STATIC IP [D/S]` prompt, enter one of the following choices:

- If DHCP is enabled, enter **D** (IP addresses are assigned automatically)
- To configure static IP, enter **S**, and then choose the interface you want to configure at the next prompt followed by the option to select IPv4 or IPv6. This is followed by the confirmation of the interface selected and the version of IP for which you select **Y** to continue. Then enter the following details:
  - IP address
  - Netmask
  - Gateway
  - (Optional) DNS Server 1
  - (Optional) DNS Server 2

Step 4 Confirm when prompted.

Reserving System Resources

For optimal performance, we recommend reserving extra system resources for Cisco IMC Supervisor beyond the minimum system requirements.

Note For more information about how to reserve system resources, see the VMWare documentation.

Procedure

Step 1 Log into VMware vCenter.

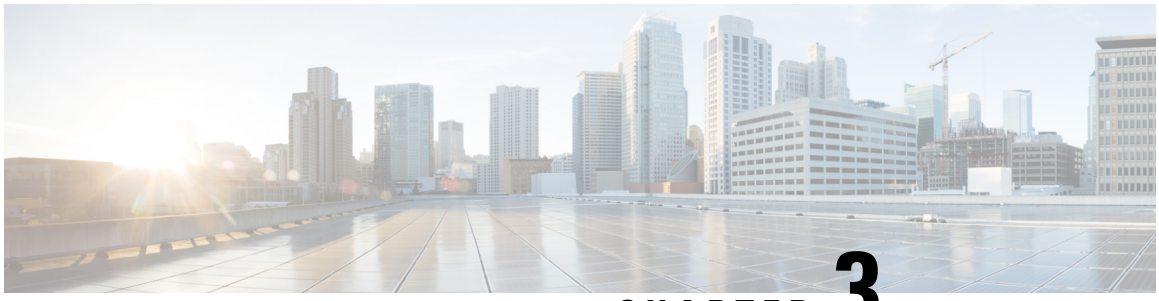
Step 2 Choose the VM for Cisco IMC Supervisor.

Step 3 Shut down the VM.

Step 4 In VMware vCenter, click the **Resource Allocation** tab to view the current resource allocations, and click **Edit.**

Step 5 In the **Virtual Machine Properties** pane, edit resource allocations by choosing a resource and entering the new values.

Step 6 Verify that the new resource allocations have been made.



CHAPTER 3

Installing Cisco IMC Supervisor on Microsoft Hyper-V

About Cisco IMC Supervisor for Hyper-V

Deploying Cisco IMC Supervisor in a Hyper-V environment is supported.

Note We recommend deploying Cisco IMC Supervisor on the Hyper-V Manager host, rather than the SCVMM console.

Prerequisites

- Installation of Hyper-V Manager
- Configured system administrator privileges
- Cisco IMC Supervisor installed on Hyper-V host

Installing Cisco IMC Supervisor on Microsoft Hyper-V 2008 R2

Before you begin

System administrator privileges for Hyper-V are required.

Note If you do not want to use DHCP, you need the following information: IP address, subnet mask, and default gateway.

Note Ensure that the IP address of the source is different from the IP address of the target system.

Procedure

Step 1 Log into the Hyper-V host.

Step 2 Choose **Start** > **Administrative Tools** to open **Hyper-V Manager.**

Step 3 In the **Hyper-V Manager** dialog box, choose **New** > **Virtual Machine**.

Step 4 In the **Before You Begin** pane, choose the custom configuration option and click **Next**.

Step 5 In the **Specify Name and Location** pane, in the **Name** field, edit the VM name and click **Next**.

Step 6 In the **Specify Name and Location** pane, check the **Store the virtual machine in a different location** checkbox and specify the alternate location or the virtual machine is stored in the default folder.

Step 7 Click **Next**.

Step 8 In the **Assign Memory** pane, enter the amount of memory to allocate to this VM (recommended12 GB) and click **Next**.

Step 9 In the **Configure Networking** pane, do not make any changes to the settings specified for the **Connection** field and click **Next**.

Step 10 In the **Connect Virtual Hard Disk** pane, select use an existing virtual hard disk or attach a virtual hard disk later and click **Next**.

Step 11 Click **Next**.

Step 12 In the **Completing the New Virtual Machine Wizard** pane, verify the settings and click **Finish**.

Step 13 In the **Hyper-V Manager** pane, right-click the new VM and choose **Settings**.

Step 14 In the **Navigation** pane, choose **IDE Controller 0**.

Step 15 In the **IDE Controller** pane, choose **Hard Drive** and click **Add.**

Note You need to add two hard drives as there are two separate VHD files - one for the OS and application, and the other for the database.

Step 16 In the **Hard Drive** pane, click **Browse**, choose the downloaded Cisco IMC Supervisor .vhd file and click **Open.**

Step 17 Click **Apply**.

Step 18 Review the virtual hard drive properties.

Step 19 In the **Navigation** pane, choose **Memory.**

Step 20 In the **Memory** pane, enter the recommended value (minimum 12 GB) and drag the **Memory weight** to **High**.

Step 21 In the **Navigation** pane, choose **Processor**.

Step 22 In the **Processor** pane, choose the recommended value (4 vCPU) and in the **Resource Control** pane, enter 100 in the **Virtual machine reserve (percentage)** field.

Step 23 In the **Navigation** pane, choose **Network Adapter**.

Step 24 Click **Remove** to remove the network adapter that was created when you created the new VM.

Step 25 In the **Navigation** pane, choose **Add Hardware**.

Step 26 In the **Add Hardware** pane, choose **Legacy Network Adapter** and click **Add**.

Step 27 In the **Legacy Network Adapter** pane, in the **Network** field, choose **Local Area Connection - Virtual Network** and click **Apply**.

Step 28 Verify that you have sufficient vCPU and Memory resources allocated.

For the minimum system requirements, see Minimum System Requirements.

Step 29 Click **OK**.

Step 30 Power on the VM.

Step 31 Optionally, you can configure network properties from the shelladmin. For more information about configuring network properties, see Configuring the Network Interface using Shelladmin, on page 13.

Step 32 After the appliance restarts, copy and paste the Cisco IMC Supervisor IP address that is displayed into a supported web browser to access the **Login** page.

Step 33 At the login prompt, enter `admin` for username and `admin` for the password to log into Cisco IMC Supervisor.

Note Change your administrator password after this initial login.

What to do next

Update your license.

Installing Cisco IMC Supervisor on Microsoft Hyper-V for Windows 2012 R2

Before you begin

- System administrator privileges for Hyper-V are required.
- Windows 2012 R2 with Hyper-V Manager version 6.3.9

Note

- You will be creating a standard VM with the wizard. Accept the defaults and at the end you will be editing the VM.
- By default, this version of Microsoft Hyper-V uses DHCP. If you want to use a static IP address instead of DHCP, you can change this configuration through the shelladmin.

Procedure

Step 1 Log into the Hyper-V host.

Step 2 Choose **Start** > **Administrative Tools** to open **Hyper-V Manager.**

Step 3 In the **Hyper-V Manager** dialog box, choose **New** > **Virtual Machine**.

Step 4 In the **Before You Begin** pane, click **Next**.

Step 5 In the **Name and Location** pane, in the **Name** field, edit the VM name and click **Next**.

Step 6 In the **Specify Name and Location** pane, check the **Store the virtual machine in a different location** checkbox and specify the alternate location or the virtual machine is stored in the default folder.

Step 7 Choose **Generation 1** for this virtual machine.

Step 8 Click **Next**.

Step 9 In the **Assign Memory** pane, enter the amount of memory to allocate to this VM (recommended12 GB) and click **Next**.

Step 10 In the **Configure Networking** pane, do not make any changes to the settings specified for the **Connection** field and click **Next**.

Step 11 In the **Connect Virtual Hard Disk** pane, select use an existing virtual hard disk or attach a virtual hard disk later and click **Next**.

Step 12 In the **Completing the New Virtual Machine Wizard** pane, verify the settings and click **Finish**.

Step 13 In the **Navigation** pane, right-click the new VM and choose **Settings**.

Step 14 In the **Navigation** pane, choose **IDE Controller 0**.

Step 15 In the **IDE Controller** pane, choose **Hard Drive** and click **Add.**

Note You need to add two hard drives as there are two separate VHD files - one for the OS and application, and the other for the database.

Step 16 In the **Hard Drive** pane, choose the downloaded Cisco IMC Supervisor .vhd file and click **OK.**

Step 17 Review the virtual hard drive properties.

Step 18 In the **Navigation** pane, choose **Memory.**

Step 19 In the **Memory** pane, enter the recommended value (minimum 12 GB).

Step 20 In the **Navigation** pane, choose **Processor**.

Step 21 In the **Processor** pane, enter the recommended value (4 vCPU).

Step 22 Remove the network adapter that was created when you created the new VM.

Step 23 In the **Navigation** pane, choose **Add Hardware**.

Step 24 In the **Add Hardware** pane, choose **Legacy Network Adapter** or **Network Adapter** and click **Add**.

Step 25 In the **Navigation** pane, choose the legacy network adapter.

Step 26 In the **Legacy Network Adapter** pane, in the **Network** field, choose **Local Area Connection - Virtual Network** and click **Apply**.

Step 27 Verify that you have sufficient vCPU and Memory resources allocated.

For the minimum system requirements, see Minimum System Requirements.

Step 28 Power on the VM.

Step 29 Optionally, you can configure network properties from the shelladmin. For more information about configuring network properties, see Configuring the Network Interface using Shelladmin, on page 13.

Step 30 After the appliance restarts, copy and paste the Cisco IMC Supervisor IP address that is displayed into a supported web browser to access the **Login** page.

Step 31 At the login prompt, enter `admin` for username and `admin` for the password to log into Cisco IMC Supervisor.

Note Change your administrator password after this initial login.

What to do next

Update your license.

Configuring the Network Interface using Shelladmin

This procedure is optional.

Procedure

Step 1 Log in to the Cisco IMC Supervisor VM console with the following credentials:

- User—shelladmin
- Password—changeme

If you have already logged into the shelladmin and changed the default password, use your new password instead.

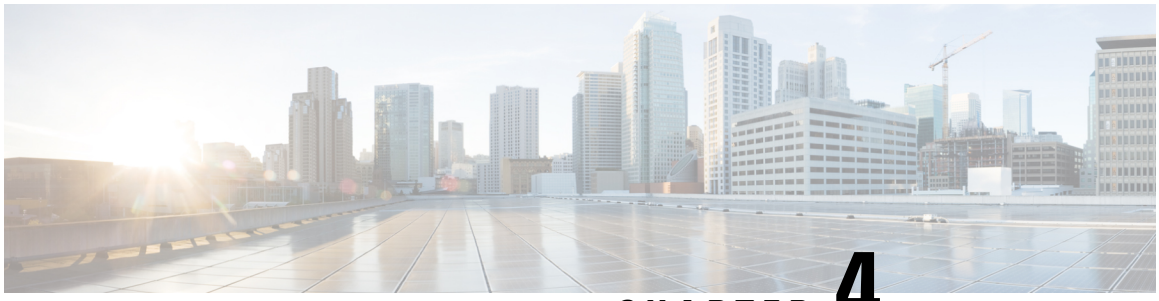
After you have logged in, you can choose `Change shelladmin password` to change the default password.

Step 2 Choose `Configure Network Interface`.

Step 3 At the `Do you want to Configure DHCP/STATIC IP [D/S]` prompt, enter one of the following choices:

- If DHCP is enabled, enter **D** (IP addresses are assigned automatically)
- To configure static IP, enter **S**, and then choose the interface you want to configure at the next prompt followed by the option to select IPv4 or IPv6. This is followed by the confirmation of the interface selected and the version of IP for which you select **Y** to continue. Then enter the following details:
  - IP address
  - Netmask
  - Gateway
  - (Optional) DNS Server 1
  - (Optional) DNS Server 2

Step 4 Confirm when prompted.



CHAPTER 4

Upgrading Cisco IMC Supervisor From Older Versions

This chapter contains the following topics:

Upgrading to Cisco IMC Supervisor Version 2.2

To upgrade to Cisco IMC Supervisor 2.2, deploy either through VMware vSphere or Micrsoft Hyper -V and follow the upgrade path below to migrate data from the old system to the new system.

- 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)

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.

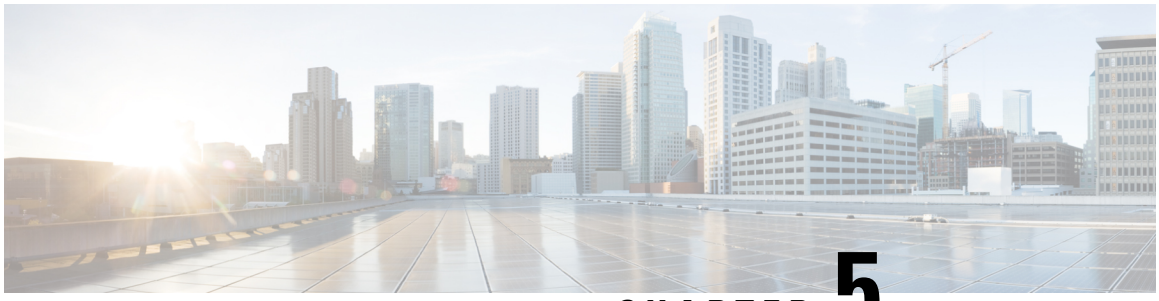
Example: Signature Verification for Upgrade Patch

```
python3 ./cisco_x509_verify_release.py3 -e UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
-i cimcs_patch_2_3_2_0_67198.zip -s cimcs_patch_2_3_2_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_3_2_0_67198.zip using
UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
```



CHAPTER 5

Post-Installation Tasks

Changing the Default Password

Procedure

Step 1 From the menu choose **Administration** > **Users**.

Step 2 Click the **Login Users** tab.

Step 3 Choose **admin** from the list of Login Users.

Step 4 Click **Change Password**.

Step 5 In the **Change Password** dialog box, enter the new password and confirm it.

Step 6 Click **Save**.

Updating the License

You must perform the following procedure to update the license before you start using Cisco IMC Supervisor. For the list of valid licenses, see About Licenses, on page 7. You must generate a license key, claim and register the Product Access Key. After installing Cisco IMC Supervisor, the license is validated and you can start using Cisco IMC Supervisor.

Before you begin

If you received a zipped license file by email, extract and save the **.lic** file to your local machine.

Procedure

Step 1 Choose **Administration** > **License**.

Step 2 On the **License** page, choose **License Keys**.

Step 3 On the **License Keys** page, click **Update License**.

Step 4 On the **Update License** screen, do one of the following:

- To upload a **.lic** file, click **Browse**, navigate to and select the **.lic** file, then click **Upload**.
- For a license key, check the **Enter License Text** check box then copy and paste the license key only into the **License Text** field. The license key is typically at the top of the file, after Key ->.

  You can also copy and paste the full text of a license file into the **License Text** field.

Step 5 Click **Submit**.
The license file is processed, and a message appears confirming the successful update.