Cisco Mobility Services Engine Virtual Appliance Installation Guide for Cisco CMX Release 10.5

First Published: 2017-04-02

Last Modified: 2018-07-09

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Preface

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

- Audience, on page iii
- Conventions, on page iii
- Related Documentation, on page iv
- Communications, Services, and Additional Information, on page iv

Audience

This document is for network administrators who configure Cisco Connected Mobile Experiences (Cisco CMX) services.

Conventions

This document uses the following conventions:

Table 1: Conventions

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.

Convention	Indication
[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. Otherwise, the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
<>	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 manual.

Tip Means the following information will help you solve a problem.

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

Related Documentation

For more information on coding and specific assistance, see:

https://developer.cisco.com/site/cmx-mobility-services/

For more information about Cisco Mobility Services Engine and related products, see:

http://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/tsd-products-support-series-home.html

For more information about Cisco Connected Mobile Experiences (Cisco CMX), see:

http://www.cisco.com/c/en/us/solutions/enterprise-networks/connected-mobile-experiences/index.html

For more information about Cisco DNA Spaces, see:

https://support.dnaspaces.io/

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.

CONTENTS

PREFACE

Preface iii

Audience iii

Conventions iii

Related Documentation iv

Communications, Services, and Additional Information iv

CHAPTER 1

Installing Cisco CMX in a VMware Virtual Machine 1

Virtualization Concepts 2

Installation Overview 2

Restrictions for Installing Cisco CMX in a VMware Virtual Machine 2

Cisco CMX Virtual Appliance Deployment Checklist 3

Prerequisites for Installing Cisco CMX in a VMware Virtual Machine 3

Hardware Guidelines 4

Release Upgrade Compatibility Matrix 4

VM Alerts 7

Downloading the Cisco CMX OVA File 8

Deploying the Cisco CMX OVA File Using the VMware vSphere Web Client 8

Configuring Cisco CMX Release 10.5.x and Later 17

Installing Cisco CMX Using Web Interface 23

Verifying Installation of Cisco CMX in a VMware Virtual Machine 26

CHAPTER 2

Virtual Machine Setup and Administration 29

Adding a Hard Disk to a Virtual Machine in the vSphere Client 29

Configuring the Network 29

Reconfiguring CPU and RAM for Cisco CMX installation 29

CHAPTER 3 **Uploading the Cisco MSE/CMX ISO Image to the Cisco MSE 3365/Cisco CMX 3375** 31

Uploading Cisco CMX ISO Image to Cisco CMX 3375 Using Newer CIMC Versions 31

Uploading the Cisco CMX/MSE ISO Image to the Cisco MSE 3365 Using Newer CIMC Versions 36

Uploading the Cisco CMX/MSE ISO Image to the Cisco MSE 3365 Using Older CIMC Versions 42

CHAPTER 1

Installing Cisco CMX in a VMware Virtual Machine

This chapter describes how to install and deploy a Cisco Mobility Services Engine (MSE) virtual appliance.

Cisco CMX is a prebuilt software solution that comprises one or more virtual machines (VMs) that are packaged, maintained, updated, and managed as a single unit. Cisco CMX is distributed as an Open Virtual Appliance (OVA) for installation on a virtual appliance and as an ISO image for installation on a physical appliance.

Cisco CMX acts as a platform (physical or virtual Cisco Mobility Services Engine [MSE] appliance) to deploy and run the Cisco services.

If you choose Location during installation, you will see the following services in Cisco CMX GUI.

- DETECT & LOCATE—Active for 120 day trial period unless either a CMX base or advanced license is added.
- ANALYTICS—Active for 120 day trial period unless a CMX advanced license is added.

If you choose Presence during installation, you will see the following services in the Cisco CMX GUI.

- CONNECT—Active for 120 day trial period unless either a CMX base license is added.
- PRESENCE ANALYTICS

- Virtualization Concepts, on page 2
- Installation Overview, on page 2
- Restrictions for Installing Cisco CMX in a VMware Virtual Machine, on page 2
- Cisco CMX Virtual Appliance Deployment Checklist, on page 3
- Prerequisites for Installing Cisco CMX in a VMware Virtual Machine, on page 3
- Hardware Guidelines, on page 4
- Release Upgrade Compatibility Matrix, on page 4
- VM Alerts, on page 7
- Downloading the Cisco CMX OVA File, on page 8
- Deploying the Cisco CMX OVA File Using the VMware vSphere Web Client, on page 8
- Configuring Cisco CMX Release 10.5.x and Later, on page 17
- Installing Cisco CMX Using Web Interface, on page 23
- Verifying Installation of Cisco CMX in a VMware Virtual Machine, on page 26

Virtualization Concepts

Refer to these documents for information on virtualization:

- Virtualization Overview
- Setting Up ESXi
- Virtualization Basics

Installation Overview

The following table lists the Cisco CMX virtual appliance installation process and contains information about the sections providing details about them:

Table 2: Installation Overview

Step	Task	See
1	Review the deployment checklist and prepare for the installation of a Cisco CMX virtual appliance.	Cisco CMX Virtual Appliance Deployment Checklist, on page 3 and Hardware Guidelines, on page 4
2	Download the Cisco CMX Open Virtualization Archive (OVA) file from Cisco.com.	Downloading the Cisco CMX OVA File, on page 8
3	Deploy the Cisco CMX OVA file.	Deploying the Cisco CMX OVA File Using the VMware vSphere Web Client, on page 8
4	Configure the basic configurations and install the Cisco CMX virtual appliance.	Configuring Cisco CMX Release 10.5.x and Later, on page 17
5	Set up the Cisco CMX virtual appliance.	Installing Cisco CMX Using Web Interface, on page 23

Note Performing a Cisco CMX installation over high latency links might not work in a reliable manner. If you want to install Cisco CMX on a remote location, we recommend that you load the ISO to a remote file server that can be accessed locally by the remote server.

Restrictions for Installing Cisco CMX in a VMware Virtual Machine

- Map size must be less than 5 MB in Cisco Prime Infrastructure.

- There must be less than 1000 access points on a single map.
- The Mobile Application Server is not available.
- The Wireless Intrusion Prevention System (wIPS) is available with limited feature support. From 10.4 release onwards, Cisco CMX supports rogue access points and rogue clients.
- A common NTP server must be used to synchronize the time.
- Simple Mail Transfer Protocol (SMTP) Mail Server name and authentication mechanism must be used for the Cisco CMX mail notification system.
- VMware vSphere Storage API - Data Protection (VADP) hypervisor clone feature is not supported

Cisco CMX Virtual Appliance Deployment Checklist

- Cisco Wireless Controller has IP connectivity to a Cisco CMX instance.
- Cisco Prime Infrastructure has IP connectivity to a Cisco CMX instance.
- Port 16113 is routable from Cisco WLC to the Cisco CMX IP address.
- Port 161 (for Simple Network Management Protocol [SNMP] traffic) is routable from Cisco WLC to the Cisco CMX IP address.
- SSH client to log in with the root access to the VM is present.
- A Secure Copy (SCP) client (on MAC native or installed on PC) or a Secure File Transfer Protocol (SFTP) exists to move files into Cisco CMX OVA (specifically, map files and images to upgrade).
- Ensure that UDP port 2003 is routable from Cisco WLC to Cisco CMX IP addresss for hyperlocation .

Note If you are using Cisco 3365 CMX Appliance and need to deploy Cisco CMX 10.5, you can only restore a backup file of maximium 200GB. If your backup file size is more than 200GB, we recommend that you add external disks or perform a selective backup for restoring Cisco CMX data.

Prerequisites for Installing Cisco CMX in a VMware Virtual Machine

- VMWare vSphere client.
- Hostname IP address, netmask, default gateway, DNS IP address, and Network Time Protocol (NTP) Server IP address or name.

Hardware Guidelines

The following table lists the hardware guidelines for the Cisco CMX virtual appliance.

Note If the hardware requirements are not met, the OVA deployment fails. Similarly, the Cisco CMX setup fails during installation when the other minimum requirements listed in the table below are not met.

Table 3: Hardware Guidelines

Hardware Platform	Basic Appliance	Standard Appliance	High-End Appliance
CPU	8 vCPU (2.4 GHz core)	16 vCPU (2.4 GHz core)	20 vCPU (2.4 GHz core)
RAM	24 GB	48 GB	64 GB [1]
HDD [2]	550 GB	550 GB	1 TB

[1] The high-end deployment VM (20 vCPU, 64 GB RAM) reserves 63.74 GB for itself and the rest of the RAM is used by ESXi.

[2] For Cisco CMX OVA installation, 160 GB is the default HDD (hard disk drive) on low-end, standard and high-end virtual machines. We strongly recommend immediately after deploying the OVA file and before powering on the VM that you increase the disk space to the recommended amount as described in the above table, so that the HDD resource does not run low while using Cisco CMX. If you do not increase the disk space before powering on the VM, refer to the VMWare 6.7 guidelines on how to increase disk space: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vm_admin.doc/GUID-79116E5D-22B3-4E84-86DF-49A8D16E7AF2.html

Note We recommend you to allocate the required HDD space. For more information, see step 12 in Deploying the Cisco CMX OVA File Using the VMware vSphere Web Client, on page 8 section.

Release Upgrade Compatibility Matrix

The following table lists the Cisco CMX releases available on Cisco.com.

Table 4: Cisco CMX Releases Available on Cisco.com

Cisco CMX Release	OVA	3365 ISO	3375 ISO	Upgrade Option Only
10.1.0	cmx-v10-1-0.ova	—		—
10.1.1	—	10.1.1		—

Cisco CMX Release	OVA	3365 ISO	3375 ISO	Upgrade Option Only
10.1.1-2	—	—		cisco_cmx-10.1.1-2.tar.gz (cisco_cmx-10.1.1-2.x86_64.rpm and cisco_cmx_connect-10.1.1-30.x86_64.rpm)
10.1.2	—	—		cisco_cmx-10.1.1-2.tar.gz
10.2	10.2 OVA	10.2 ISO		10.2 backend upgrade (10.1 and 10.1.1 to 10.2) script and.CMX image file
10.3	10.3 OVA	10.3 ISO		—
10.4	10.4 OVA	10.4 ISO		—
10.5	10.5 OVA	10.5 ISO		No direct upgrade option. New OVA/ISO System
10.6	10.6 OVA	10.6 ISO	10.6 ISO	—

Table 5: Node Types Supported Per Release

Release	Location and Analytics Node	Location and Connect Node	Location, Analytics, and Connect Node (L-Node)	Connect and Presence Node (P-Node)	High Availability
10.1.0	Yes	—	—	—	—
10.1.1-2	Yes	Yes	Yes	—	—
10.1.2	Yes	Yes	Yes	—	—
10.2	Use the upgrade script to change Location and Analytics to Location, Analytics, and Connect internally.	Use the upgrade script to change Location and Connect to Location, Analytics, and Connect internally.	Yes	Yes	—
10.3	Use the upgrade script to change Location and Analytics to Location, Analytics, and Connect internally.	Use the upgrade script to change Location and Connect to Location, Analytics, and Connect internally.	Yes	Yes	Yes

Release	Location and Analytics Node	Location and Connect Node	Location, Analytics, and Connect Node (L-Node)	Connect and Presence Node (P-Node)	High Availability
10.4	Use the upgrade script to change Location and Analytics to Location, Analytics, and Connect internally.	Use the upgrade script to change Location and Connect to Location, Analytics, and Connect internally.	Use the upgrade script to change Location and Connect to Location, Analytics, and Connect internally.	Yes	Yes
10.5	No direct upgrade is available. New OVA/ISO system upgrade	No direct upgrade is available. New OVA/ISO system upgrade	Yes	Yes	Yes
10.6	Use the upgrade script to change Location and Analytics to Location, Analytics, and Connect internally.	Use the upgrade script to change Location and Connect to Location, Analytics, and Connect internally.	Yes	Yes	Yes

Table 6: Upgrade Path by Node Type

Upgrade Path 1[3]	Location and Connect Node	Location and Analytics Node	Location, Analytics, and Connect Node (L-Node)	Connect and Presence Node (P-Node)
10.1.0 OVA to 10.2	10.2 backend script to upgrade image to10.2 and change Location and Connect to Location, Connect, and Analytics.	10.2 backend script to upgrade image to10.2 and change Location and Analytics to Location, Connect, and Analytics.	10.2 backend script to upgrade image to 10.2.	—
10.1.1-2 tar.gz to 10.2	10.2 backend script to upgrade image to10.2 and change Location and Connect to Location, Connect, and Analytics.	10.2 backend script to upgrade image to10.2 and change Location and Analytics to Location, Connect, and Analytics.	10.2 backend script to upgrade image to 10.2.	—
10.1.2 tar.gz to 10.2	10.2 backend script to upgrade image to10.2 and change Location and Connect to Location, Connect, and Analytics.	10.2 backend script to upgrade image to10.2 and change Location and Analytics to Location, Connect, and Analytics.	10.2 backend script to upgrade image to 10.2.	—

10.2 OVA/ISO to 10.3	—	—	UI upgrade script to upgrade image.	UI upgrade script to upgrade image
10.3 OVA/ISO to 10.4	—	—	UI upgrade script to upgrade image.	UI upgrade script to upgrade image
10.5 OVA/ISO	—	—	UI upgrade script to upgrade image.	UI upgrade script to upgrade image
10.6 OVA/ISO	—	—	UI upgrade script to upgrade image.	Upgrade is supported from the Cisco CMX Release 10.5.x to Cisco CMX Release 10.6. **Note** Releases earlier than Cisco CMX Release 10.5 cannot be upgraded to Cisco CMX Release 10.6, for example Cisco CMX Release 10.4.1 cannot be upgraded to Cisco CMX Release 10.6.

[3] The path that is provided for upgrade is the same as that used for backup and restore.

VM Alerts

The following table displays the alerts shown on the VM for the following conditions:

Table 7: VM Alerts

Hard Disk Status	Alert Shown
50 percent	Do Not Back Up
80 percent	System Is About To Run Out Of Space
85 percent	All The Services Are Stopped

Downloading the Cisco CMX OVA File

Step 1 Download the Cisco CMX image from Download Software on cisco.com.

Step 2 Save the Cisco CMX OVA installer to your computer and ensure that it is accessible.

Deploying the Cisco CMX OVA File Using the VMware vSphere Web Client

The VMware vSphere Web Client (Flash/Flex client) is the client to manage vCenter Server 6.5 environment with all the features and plugins. From VMware vSphere release 6.5 version, the recommened option to use is vSphere Web Client.

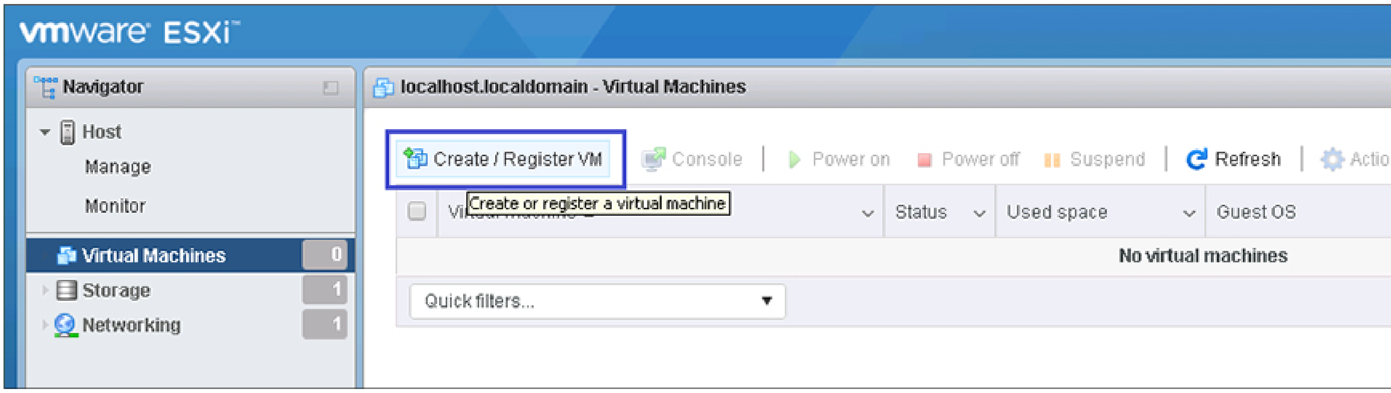
From VMware vSphere release 6.5 version, the **thick client** is no longer supported. Only the vSphere Client (HTML 5) and vSphere Web Client are supported.

To deploy the Cisco CMX OVA file using the VMware vSphere Web Client, follow these steps:

Step 1 Launch the VMware vSphere Web Client application on your desktop.

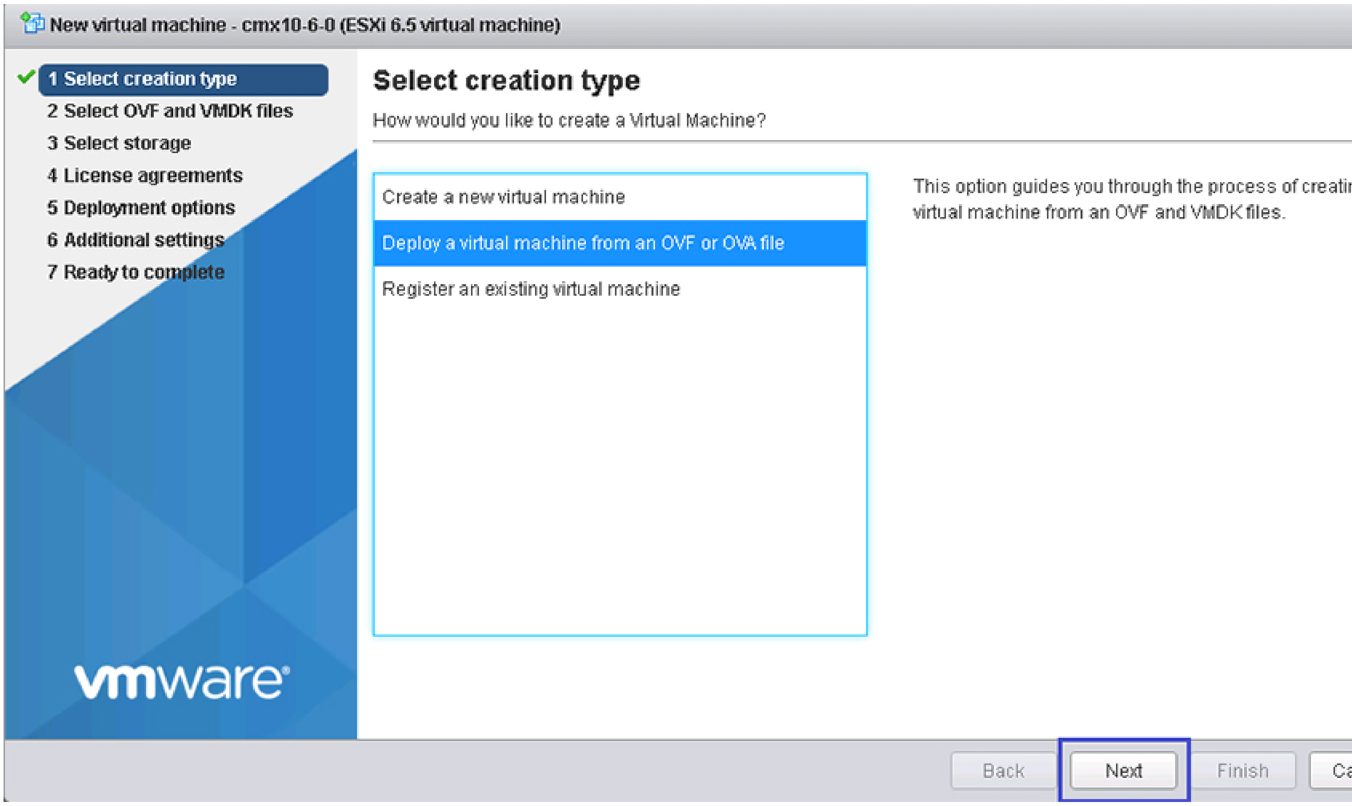
Step 2 From the **Navigator** pane, click **Create/Register VM** to create or register a virtual machine.

Figure 1: Create/Register VM



Step 3 Choose **Deploy a virtual machine from an OVF or OVA file** as a creation type and click **Next**. This option helps you to create a virtual machine from a Cisco CMX OVA file.

Figure 2: Deploy VM



New virtual machine - cmx10-6-0 (ESXi 6.5 virtual machine)

Select creation type

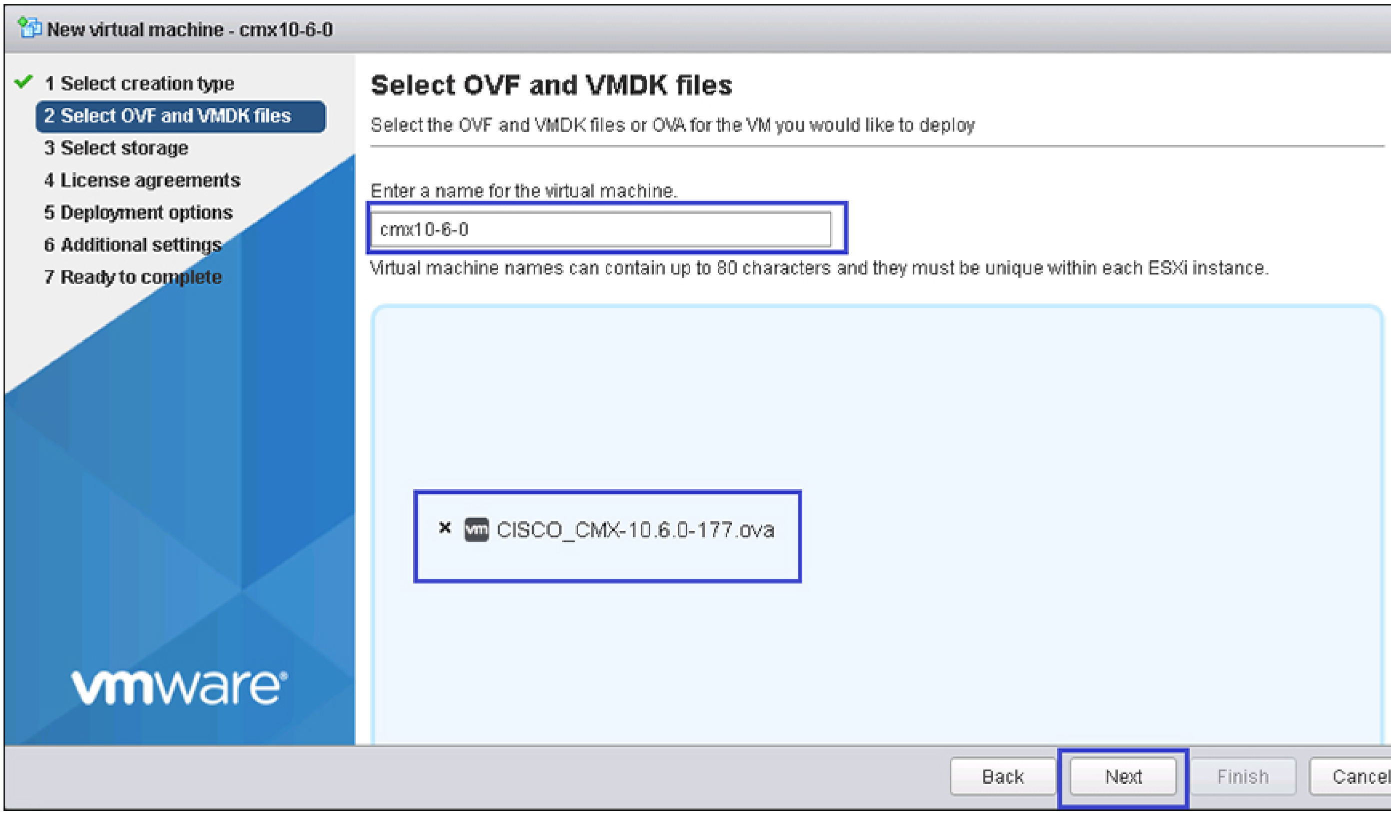
How would you like to create a Virtual Machine?

Create a new virtual machine
Deploy a virtual machine from an OVF or OVA file
Register an existing virtual machine

This option guides you through the process of creati
virtual machine from an OVF and VMDK files.

Step 4 In the **Select OVF and VMDK files** section, enter a name for the virtual machine, select the Cisco CMX OVA file that is stored locally on the machine and click **Next**.

Figure 3: Cisco CMX OVA



New virtual machine - cmx10-6-0

Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

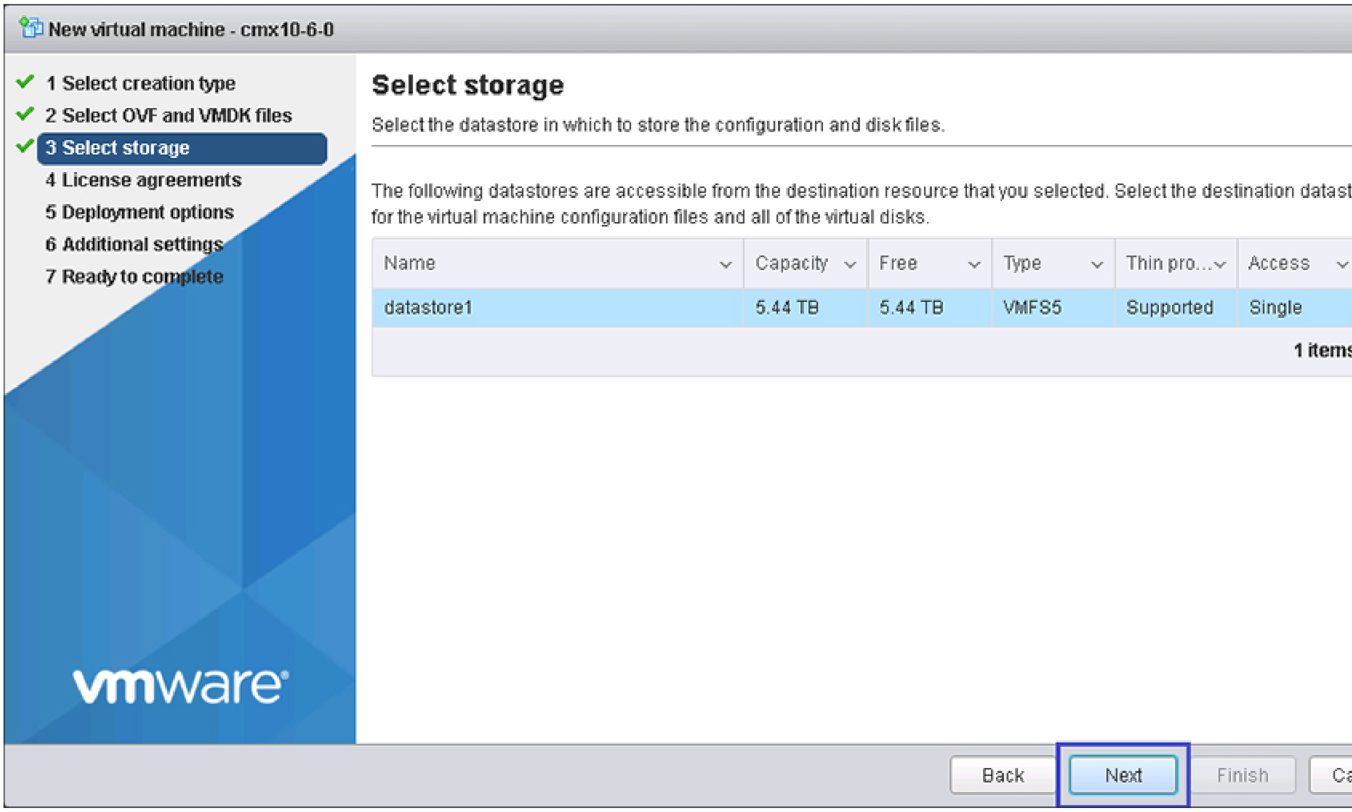
cmx10-6-0

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

CISCO_CMX-10.6.0-177.ova

Step 5 Select the destination datastore for the virtual machine configuration files and virtual disks and click **Next**.

Figure 4: Datastore



Select storage

Select the datastore in which to store the configuration and disk files.

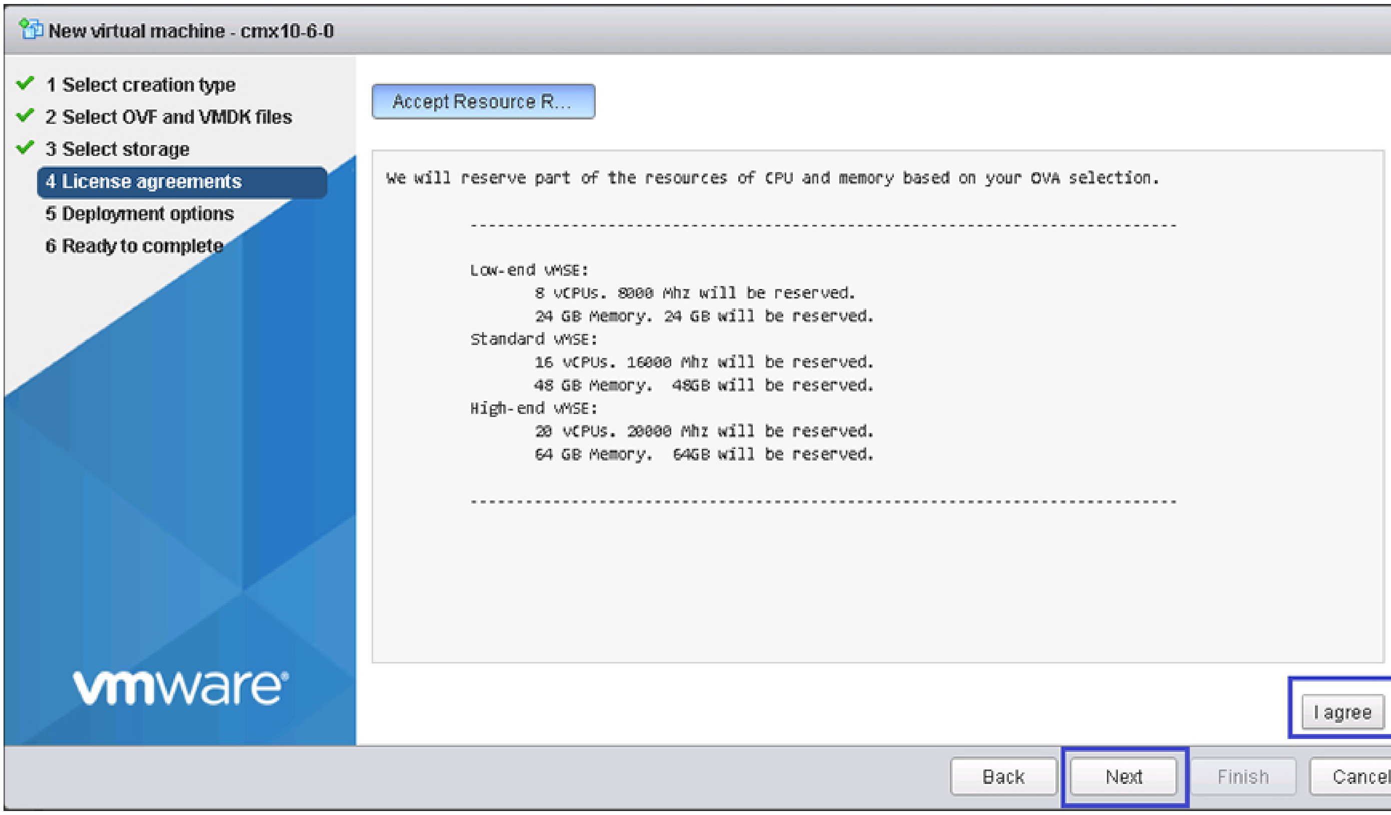
The following datastores are accessible from the destination resource that you selected. Select the destination datast
for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	5.44 TB	5.44 TB	VMFS5	Supported	Single

1 items

Step 6 Click **I Agree** to accept the End User License Agreement and then click **Next**.

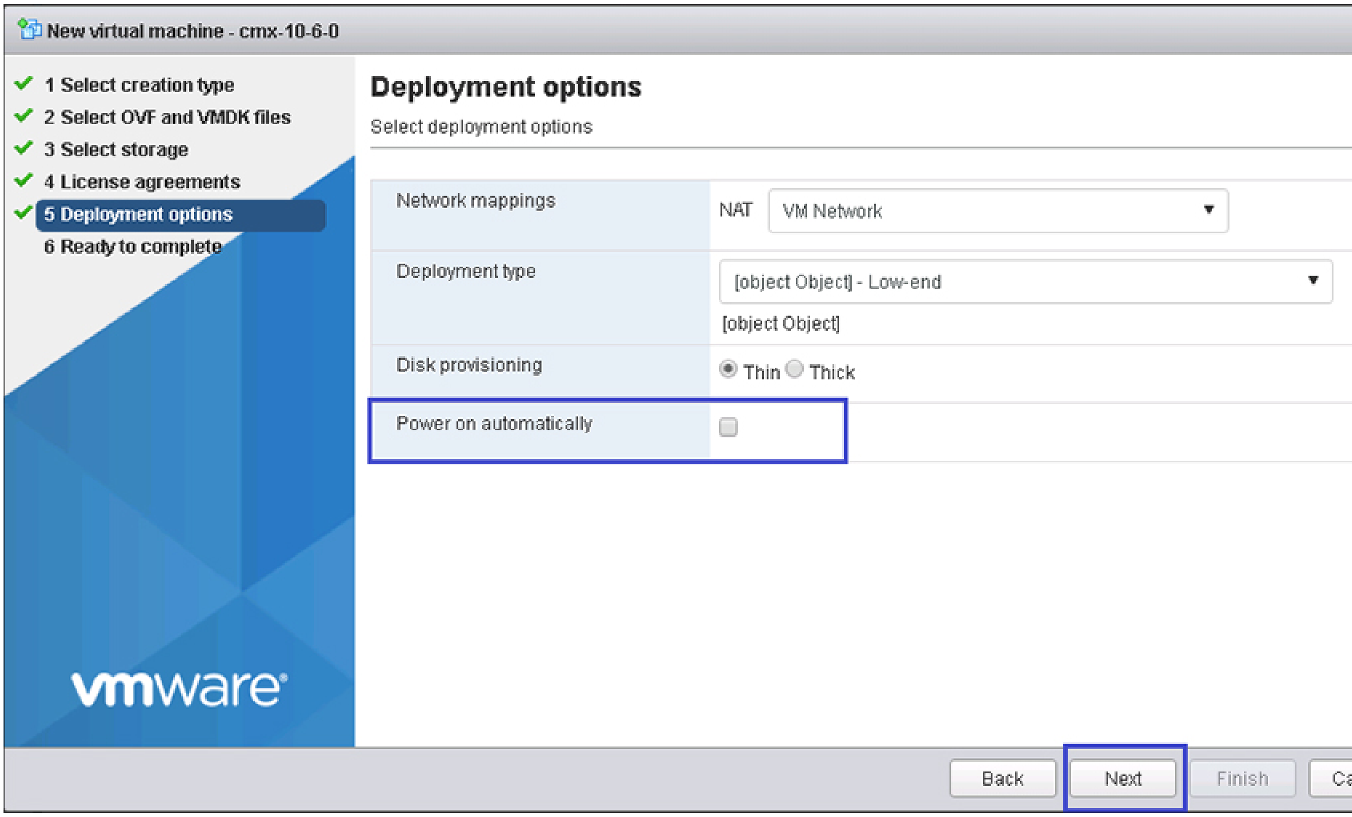
Figure 5: License Agreements



```
We will reserve part of the resources of CPU and memory based on your OVA selection.

        ---------------------------------------------------------------------------

        Low-end vMSE:
               8 vCPUs. 8000 Mhz will be reserved.
               24 GB Memory. 24 GB will be reserved.
        Standard vMSE:
               16 vCPUs. 16000 Mhz will be reserved.
               48 GB Memory.  48GB will be reserved.
        High-end vMSE:
               20 vCPUs. 20000 Mhz will be reserved.
               64 GB Memory.  64GB will be reserved.

        ---------------------------------------------------------------------------
```

Step 7 Select the deployment options. Ensure that **Power on automatically** is not checked.

Figure 6: Deployment Options



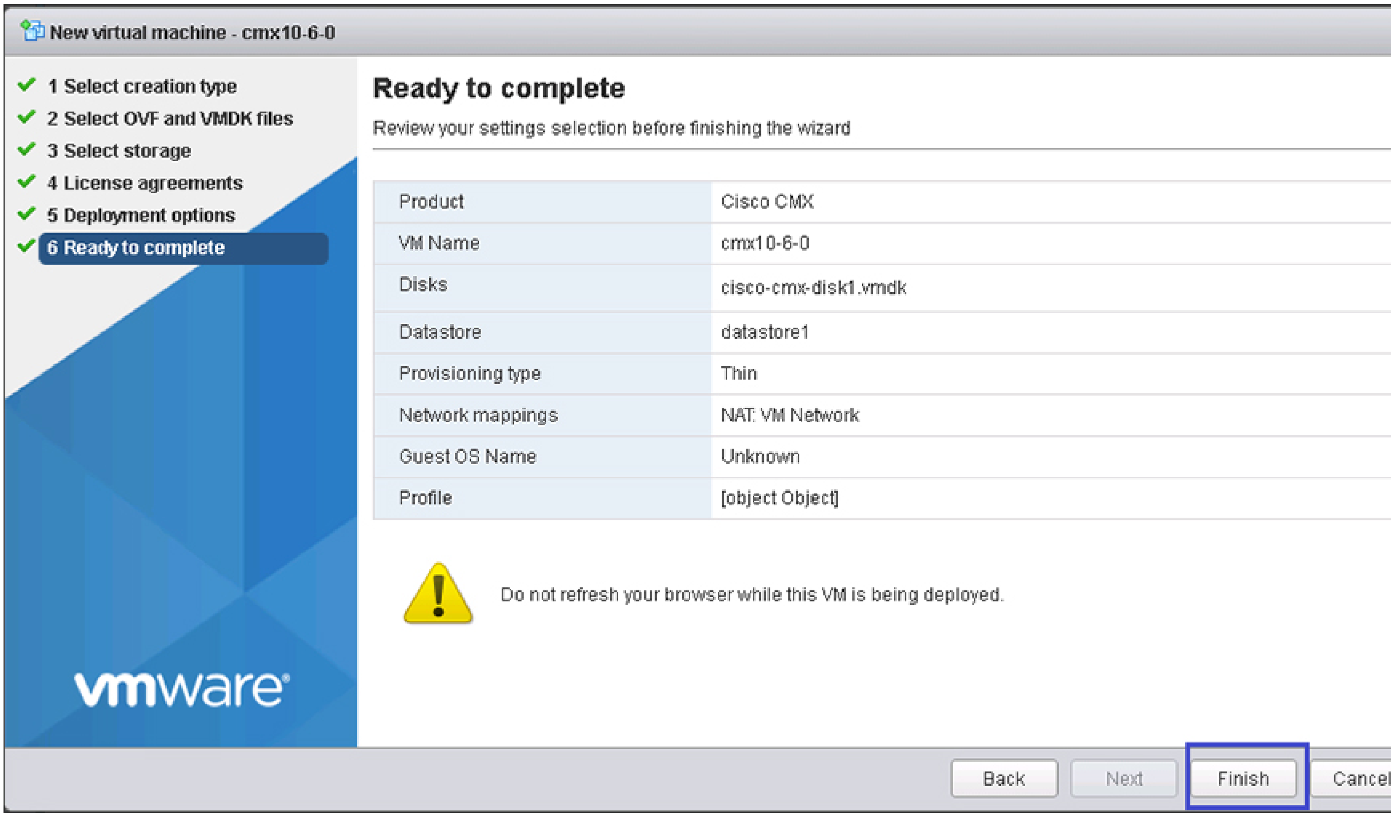
Deployment options

Select deployment options

Network mappings	NAT VM Network ▼
Deployment type	[object Object] - Low-end ▼ [object Object]
Disk provisioning	● Thin ○ Thick
Power on automatically	□

Step 8 In the Ready to complete section, review the settings and click **Finish**. Ensure that you do not refresh the browser while the VM is deployed.

Figure 7: Verify Settings



New virtual machine - cmx10-6-0

✓ 1 Select creation type
✓ 2 Select OVF and VMDK files
✓ 3 Select storage
✓ 4 License agreements
✓ 5 Deployment options
✓ 6 Ready to complete

Ready to complete

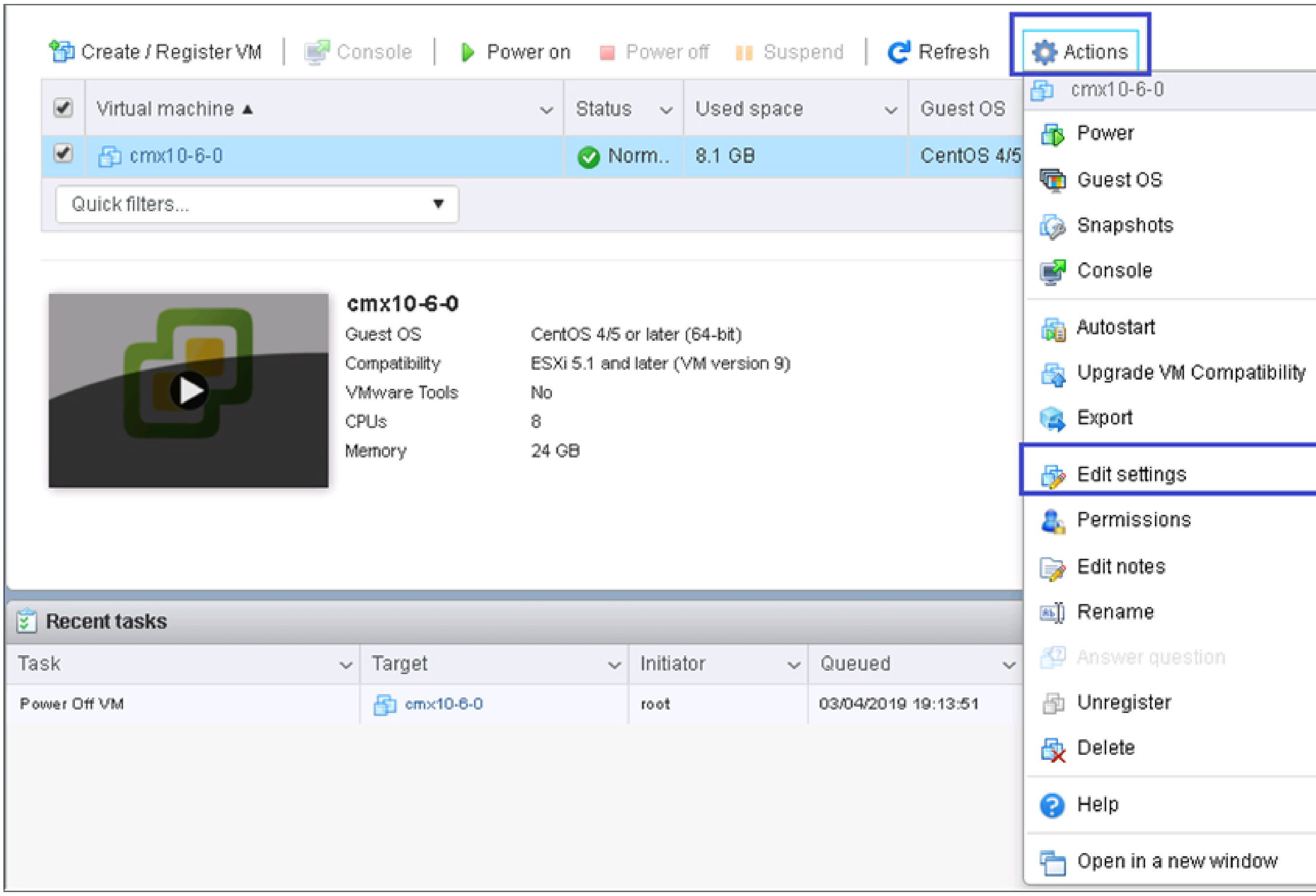
Review your settings selection before finishing the wizard

Product	Cisco CMX
VM Name	cmx10-6-0
Disks	cisco-cmx-disk1.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	NAT: VM Network
Guest OS Name	Unknown
Profile	[object Object]

Do not refresh your browser while this VM is being deployed.

Step 9 Click the deployed VM and choose **Actions** > **Edit settings**.

Figure 8: Edit Settings



☑	Virtual machine ▲	Status	Used space	Guest OS
☑	cmx10-6-0	Norm..	8.1 GB	CentOS 4/5

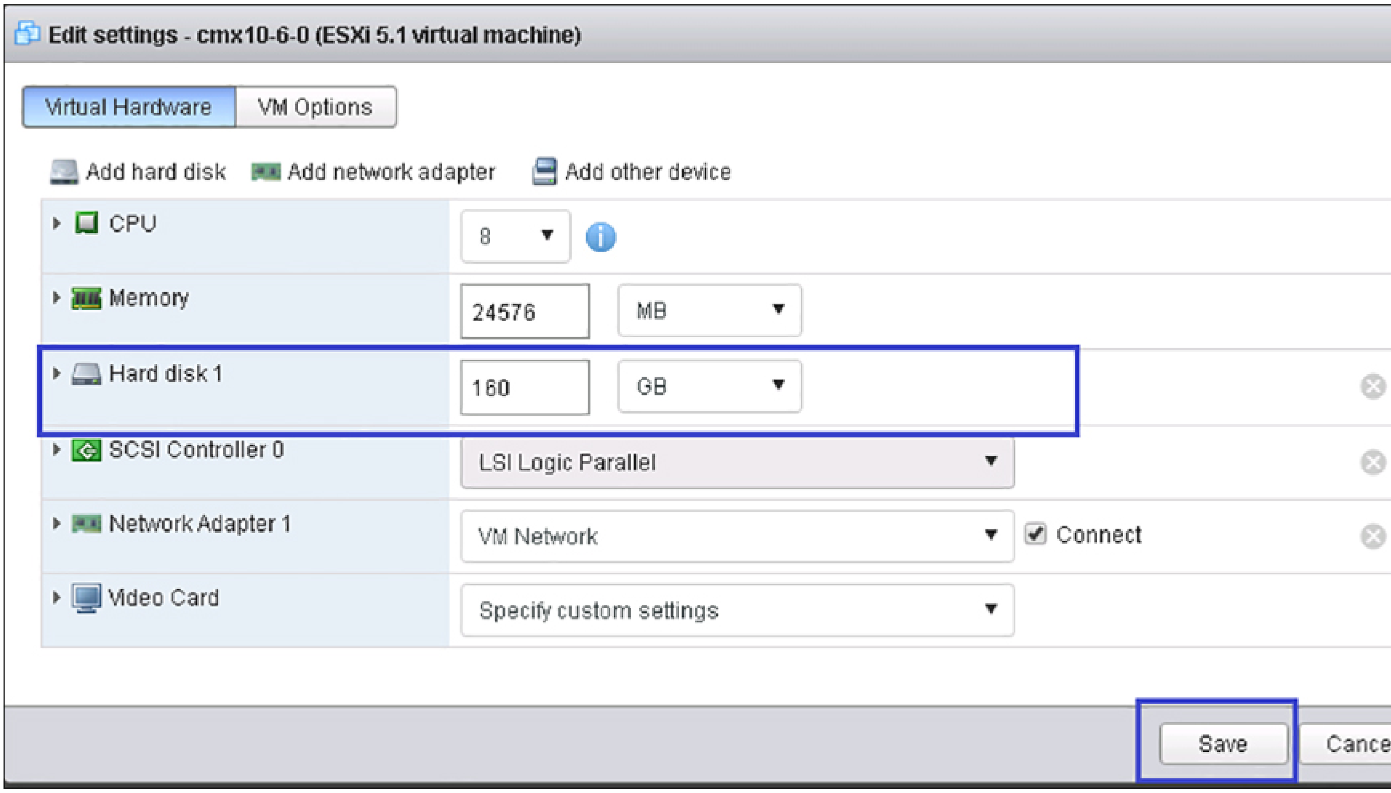
cmx10-6-0

Guest OS	CentOS 4/5 or later (64-bit)
Compatibility	ESXi 5.1 and later (VM version 9)
VMware Tools	No
CPUs	8
Memory	24 GB

Task	Target	Initiator	Queued
Power Off VM	cmx10-6-0	root	03/04/2019 19:13:51

Step 10 Click **Hard disk**, modify the provisioned size to match the instance requirement and click **Save**. The default size is 160 GB.

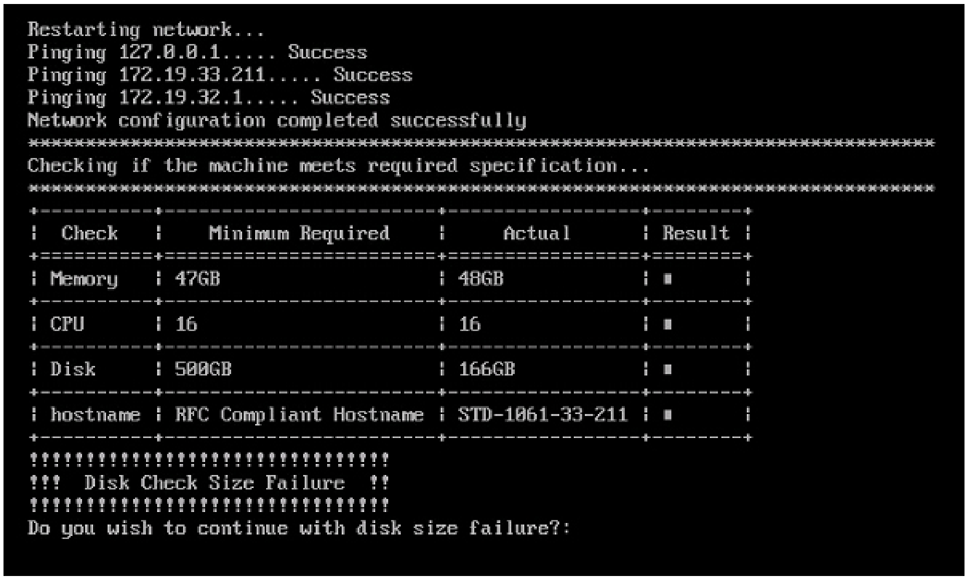
Figure 9: Hard Disk Provisioned Size



Edit settings - cmx10-6-0 (ESXi 5.1 virtual machine)

CPU: 8
Memory: 24576 MB
Hard disk 1: 160 GB
SCSI Controller 0: LSI Logic Parallel
Network Adapter 1: VM Network ☑ Connect
Video Card: Specify custom settings

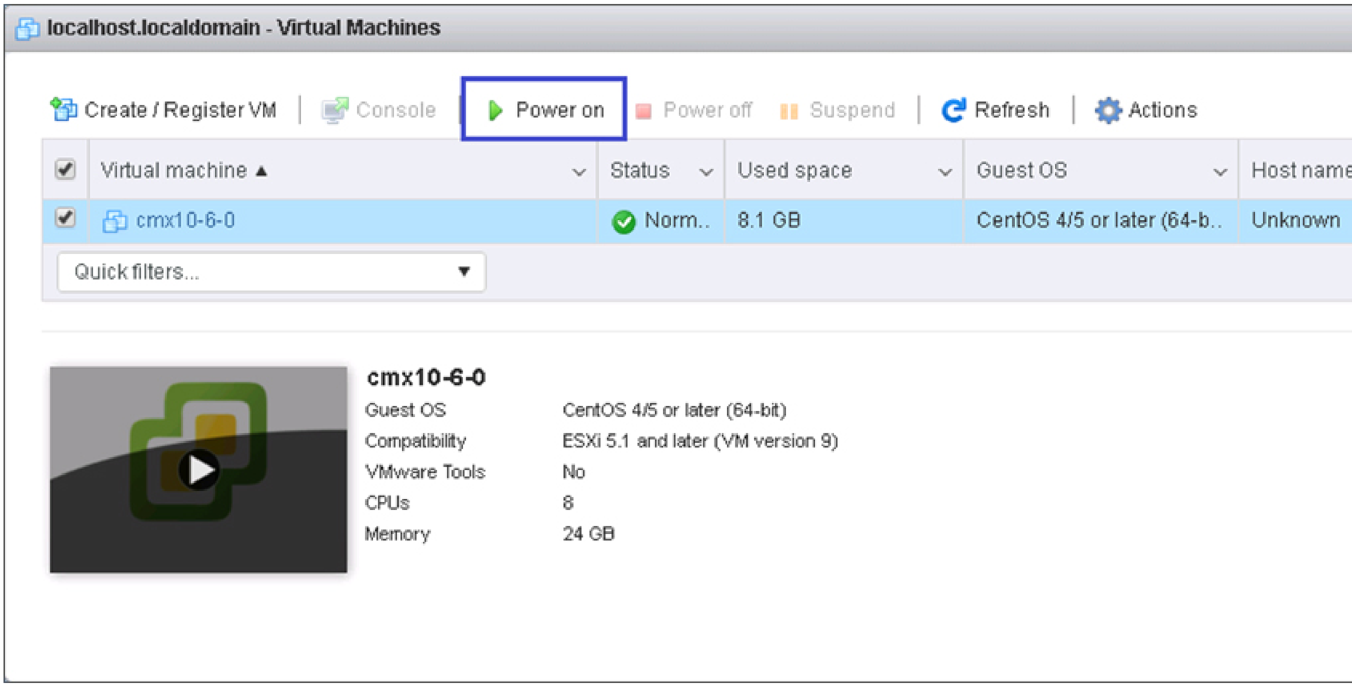
Note If the instance is powered on, it will display a warning message for the Hard Disk Size Failure (for Standard and High End instances) as shown below.



```
Restarting network...
Pinging 127.0.0.1..... Success
Pinging 172.19.33.211..... Success
Pinging 172.19.32.1..... Success
Network configuration completed successfully
********************************************************************************
Checking if the machine meets required specification...
********************************************************************************
+----------+-------------------------+-----------------+--------+
¦  Check   ¦    Minimum Required     ¦     Actual      ¦ Result ¦
+==========+=========================+=================+========+
¦ Memory   ¦ 47GB                    ¦ 48GB            ¦ ■      ¦
+----------+-------------------------+-----------------+--------+
¦ CPU      ¦ 16                      ¦ 16              ¦ ■      ¦
+----------+-------------------------+-----------------+--------+
¦ Disk     ¦ 500GB                   ¦ 166GB           ¦ ■      ¦
+----------+-------------------------+-----------------+--------+
¦ hostname ¦ RFC Compliant Hostname  ¦ STD-1061-33-211 ¦ ■      ¦
+----------+-------------------------+-----------------+--------+
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!  Disk Check Size Failure  !!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Do you wish to continue with disk size failure?:
```

Step 11 Click **Power on** to power on the VM. The first boot takes a while as the new disk has to be expanded.

Figure 10: Power On VM



☑	Virtual machine ▲	Status	Used space	Guest OS	Host name
☑	cmx10-6-0	Norm..	8.1 GB	CentOS 4/5 or later (64-b..	Unknown

cmx10-6-0

Guest OS	CentOS 4/5 or later (64-bit)
Compatibility	ESXi 5.1 and later (VM version 9)
VMware Tools	No
CPUs	8
Memory	24 GB

Configuring Cisco CMX Release 10.5.x and Later

After the Cisco CMX is deployed, you can install and configure a Cisco CMX virtual machine (VM). Note the following points:

- Cisco CMX does not have a node install menu. However, there is a first-boot script that checks if a configuration exists on the device. If the script does not find a valid configuration, it launches the setup routine and initiates network configuration tasks using the CLI, followed by the initial setup tasks on the browser.
- The new first-boot script determines if the initial configuration is completed, and then displays the normal login prompt. If the initial configuration is not completed, the default login prompt is displayed.

Note The **cmxctl node install** command is no longer valid.

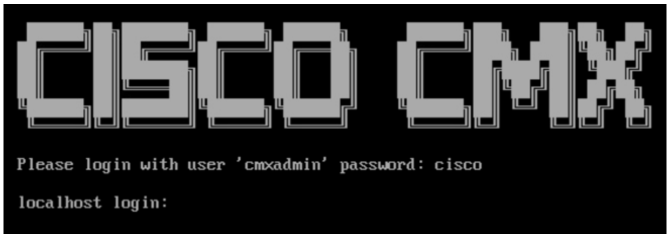
To install and configure a Cisco CMX VM, follow these steps:

Step 1 Right-click the Cisco CMX VM and click **Open Console.**

The CentOS initial boot displays 3 options, with the last option, **rescue image**, being selected by default. Retain the selection and wait for 5 seconds.

Step 2 Enter the login name cmxadmin and password cisco, as prompted.

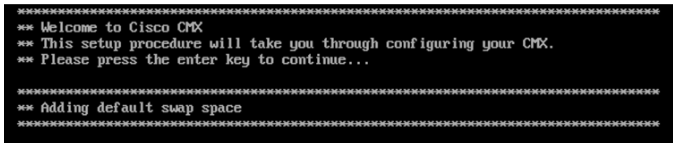
Figure 11: Console Window



```
CISCO CMX

Please login with user 'cmxadmin' password: cisco

localhost login:
```

Step 3 Press **Enter** when prompted, as shown in the figure below.

Figure 12: Press Enter



```
*****************************************************************************
** Welcome to Cisco CMX
** This setup procedure will take you through configuring your CMX.
** Please press the enter key to continue...

*****************************************************************************
** Adding default swap space
*****************************************************************************
```

Step 4 Enter a new password for the root user and reconfirm it when prompted. The password should meet the minimum requirements listed on the screen.

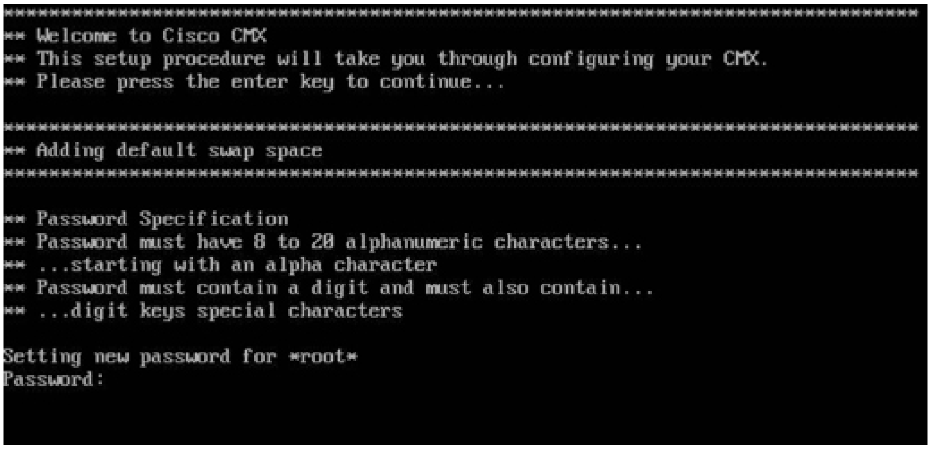
Note The root password is used only for the root operating system configuration and not for the cmxadmin user functions.

Starting Cisco CMX Release 10.6.3, you are not required to enter new password for root user.

Step 5 Enter a new password for cmxadmin user and reconfirm it. The password should meet the minimum requirements listed on the screen.

Note The cmxadmin password is used for logging in to the Cisco CMX account for future network admin configurations.

Figure 13: Set Passwords



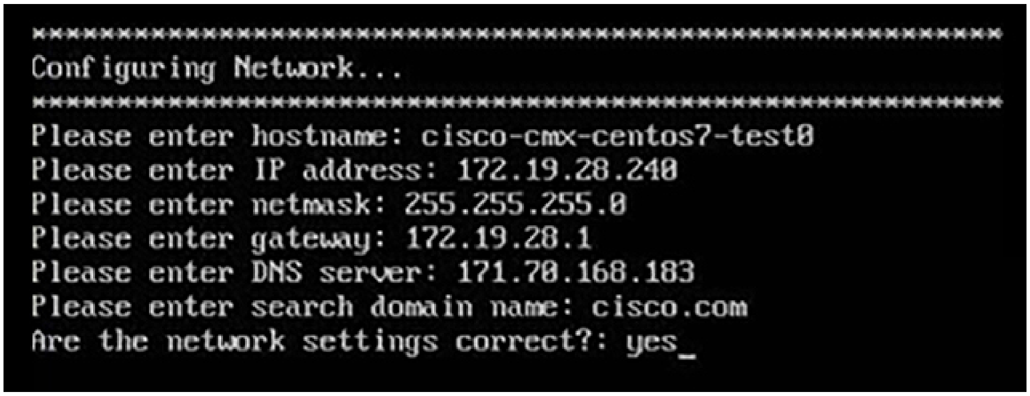
```
*****************************************************************************
** Welcome to Cisco CMX
** This setup procedure will take you through configuring your CMX.
** Please press the enter key to continue...

*****************************************************************************
** Adding default swap space
*****************************************************************************

** Password Specification
** Password must have 8 to 20 alphanumeric characters...
** ...starting with an alpha character
** Password must contain a digit and must also contain...
** ...digit keys special characters

Setting new password for *root*
Password:
```

Step 6 Enter the following network configuration parameters when prompted.

- **Hostname**

- **IP Address**
- **Netmask**
- **Gateway**
- **DNS Server**
- **Search Domain Name**

Figure 14: Network Configuration Parameters

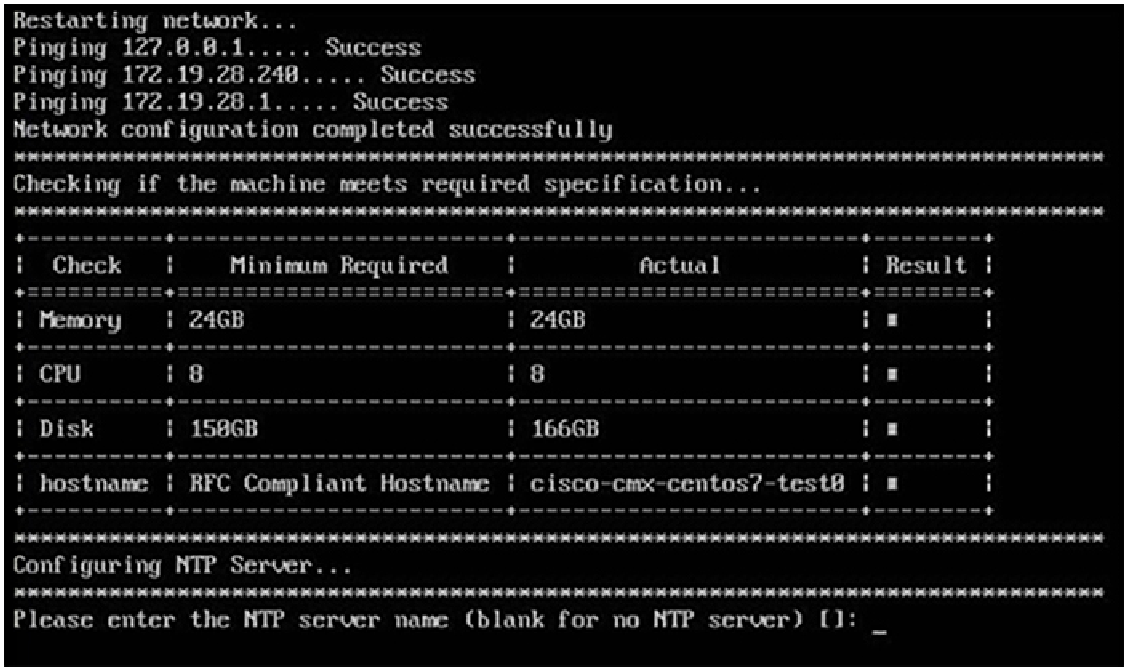


```
*******************************************************
Configuring Network...
*******************************************************
Please enter hostname: cisco-cmx-centos7-test0
Please enter IP address: 172.19.28.240
Please enter netmask: 255.255.255.0
Please enter gateway: 172.19.28.1
Please enter DNS server: 171.70.168.183
Please enter search domain name: cisco.com
Are the network settings correct?: yes_
```

Step 7 Confirm the network configurations when prompted.

Step 8 The network is restarted and a success message is displayed.

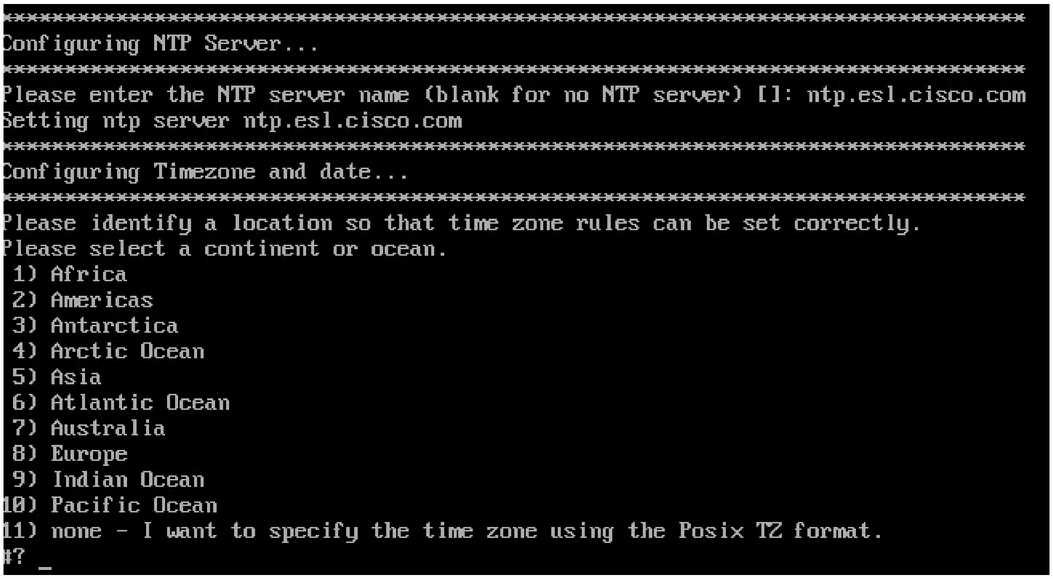
Figure 15: Network Configuration Success Message



```
Restarting network...
Pinging 127.0.0.1..... Success
Pinging 172.19.28.240..... Success
Pinging 172.19.28.1..... Success
Network configuration completed successfully
*************************************************************************
Checking if the machine meets required specification...
*************************************************************************
+----------+------------------------+-------------------------+--------+
|  Check   |    Minimum Required    |         Actual          | Result |
+==========+========================+=========================+========+
| Memory   | 24GB                   | 24GB                    | ■      |
+----------+------------------------+-------------------------+--------+
| CPU      | 8                      | 8                       | ■      |
+----------+------------------------+-------------------------+--------+
| Disk     | 150GB                  | 166GB                   | ■      |
+----------+------------------------+-------------------------+--------+
| hostname | RFC Compliant Hostname | cisco-cmx-centos7-test0 | ■      |
+----------+------------------------+-------------------------+--------+
*************************************************************************
Configuring NTP Server...
*************************************************************************
Please enter the NTP server name (blank for no NTP server) []: _
```

Step 9 (Optional) Enter the NTP server name or the IP address of the NTP server when prompted.

Figure 16: NTP Server Configuration



```
*******************************************************************************
Configuring NTP Server...
*******************************************************************************
Please enter the NTP server name (blank for no NTP server) []: ntp.esl.cisco.com
Setting ntp server ntp.esl.cisco.com
*******************************************************************************
Configuring Timezone and date...
*******************************************************************************
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#? _
```

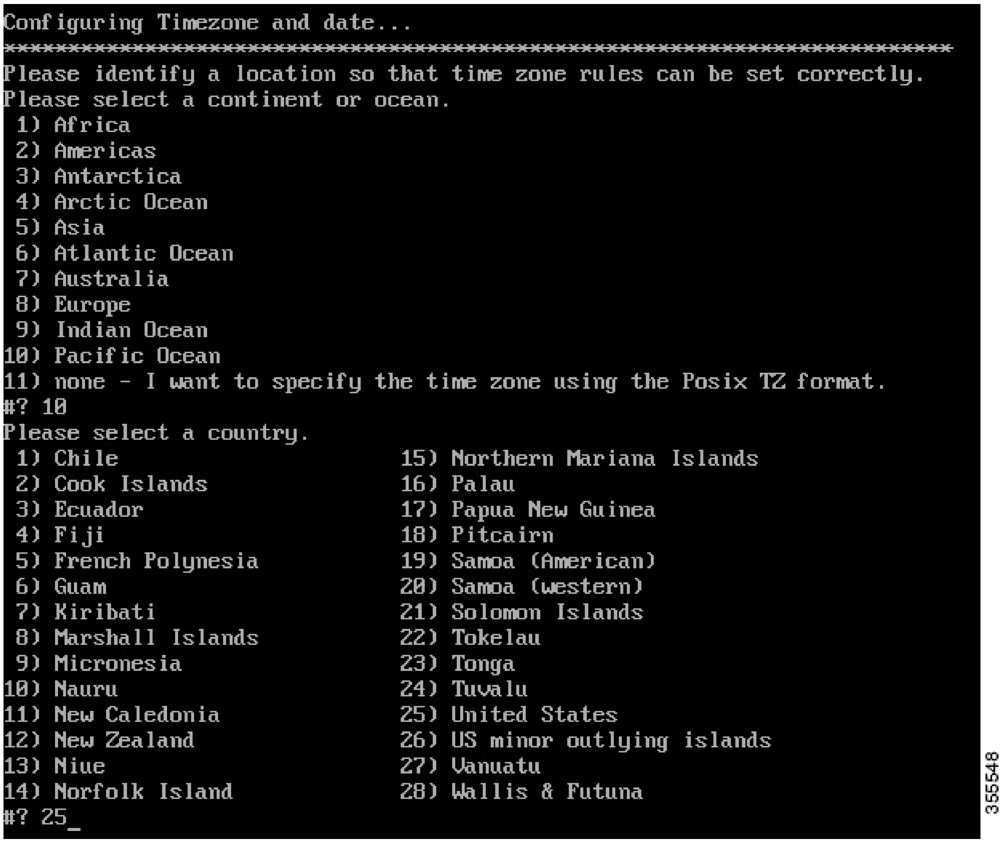
Note

- After installation, the task of changing the NTP information either through the CLI or the GUI is not supported. Use the **cmxos reconfigure** command from the CMX CLI to change the NTP information. The following example shows a workaround to change the NTP information.

```
cmxctl stop
cmxctl stop ?a
!Go to root user
su
!Run the timezone script
/opt/cmx/bin/tzselect
!Logout of the box
exit
!Log back in and check the timezone
date
!Restart the services
cmxctl start agent
cmxctl start
```

Step 10 Configure a time zone and save the changes.

Figure 17: Configuring a Time Zone



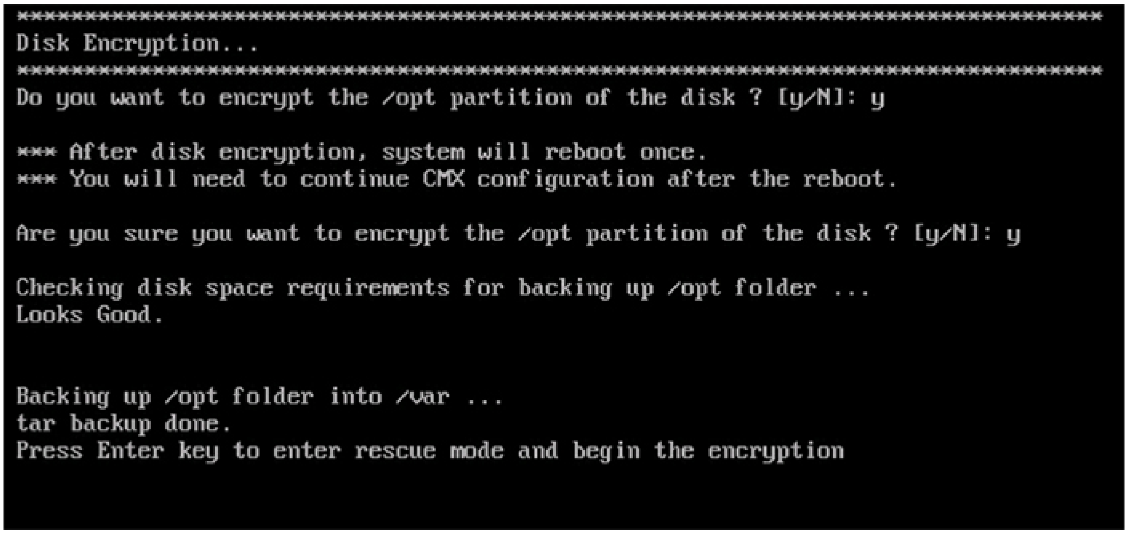
```
Configuring Timezone and date...
**************************************************************************
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#? 10
Please select a country.
 1) Chile                      15) Northern Mariana Islands
 2) Cook Islands               16) Palau
 3) Ecuador                    17) Papua New Guinea
 4) Fiji                       18) Pitcairn
 5) French Polynesia           19) Samoa (American)
 6) Guam                       20) Samoa (western)
 7) Kiribati                   21) Solomon Islands
 8) Marshall Islands           22) Tokelau
 9) Micronesia                 23) Tonga
10) Nauru                      24) Tuvalu
11) New Caledonia              25) United States
12) New Zealand                26) US minor outlying islands
13) Niue                       27) Vanuatu
14) Norfolk Island             28) Wallis & Futuna
#? 25_
```

Step 11 (Optional) Encrypt the /opt partition of the disk. You can perform disk encryption during the installation process or at a later time.

- If you do not want to perform disk encryption, enter **N** and complete the CMX operating system configuration process. However, we recommend that you perform disk encryption after the CMX operating system configuration is complete, using the **cmxos encryptdisk** command. The time taken for disk encryption is equal to the amount of data available on the /opt partition.

- If you want to perform disk encryption, enter **y**. The system performs the /opt folder backup operation and enters the rescue mode. Confirm the passphrase for encrypting the disk. A system reboot is mandatory if you perform disk encryption during the installation. After the reboot, you must complete the CMX operating system configuration from https://<*ip address or CMX DNS name*>:1984.

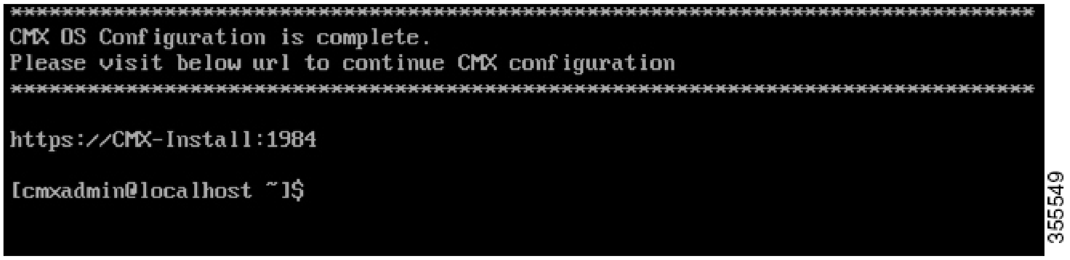
Figure 18: Disk Encryption



```
********************************************************************************
Disk Encryption...
********************************************************************************
Do you want to encrypt the /opt partition of the disk ? [y/N]: y

*** After disk encryption, system will reboot once.
*** You will need to continue CMX configuration after the reboot.

Are you sure you want to encrypt the /opt partition of the disk ? [y/N]: y

Checking disk space requirements for backing up /opt folder ...
Looks Good.


Backing up /opt folder into /var ...
tar backup done.
Press Enter key to enter rescue mode and begin the encryption
```

Step 12 Access the URL when prompted.

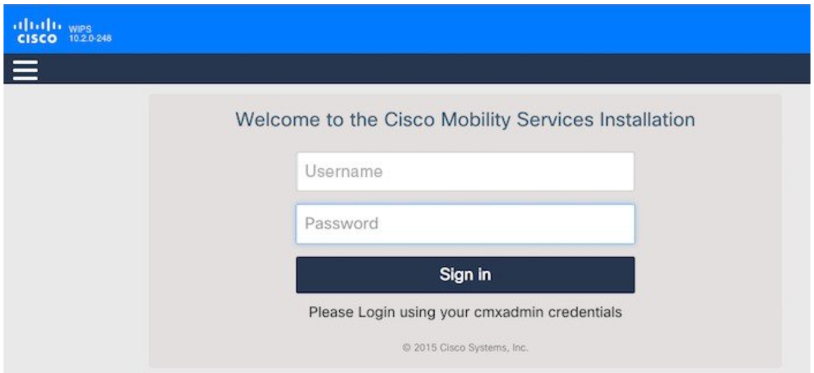
Figure 19: Access URL for CMX Configuration - No Disk Encryption



```
********************************************************************************
CMX OS Configuration is complete.
Please visit below url to continue CMX configuration
********************************************************************************

https://CMX-Install:1984

[cmxadmin@localhost ~]$
```

Step 13 Open the URL https://<*ip-address*>:1984 when prompted in the browser. The Cisco Mobility Services Installation sign-in window is displayed.

Figure 20: Sign-In Window



cisco
WIPS
10.2.0-248
Welcome to the Cisco Mobility Services Installation
Username
Password
Sign in
Please Login using your cmxadmin credentials
© 2015 Cisco Systems, Inc.

Step 14 Enter your cmxadmin credentials and proceed with the installation.

Note Use Step 13 and Step 14 while installing a new CMX VM.

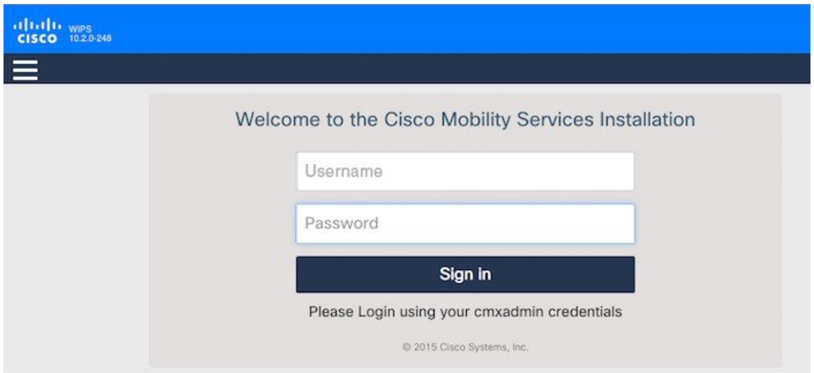
Installing Cisco CMX Using Web Interface

Launch the Cisco CMX user interface using Google Chrome 40 or later, and follow these steps:

Step 1 In the Cisco CMX web interface, enter the login credentials for a Cisco CMX administrator and click **Sign in** to continue.

The login username is **cmxadmin**. Use the password that was configured when the system was started for the first time.

Figure 21: Welcome Window



Welcome to the Cisco Mobility Services Installation

Username

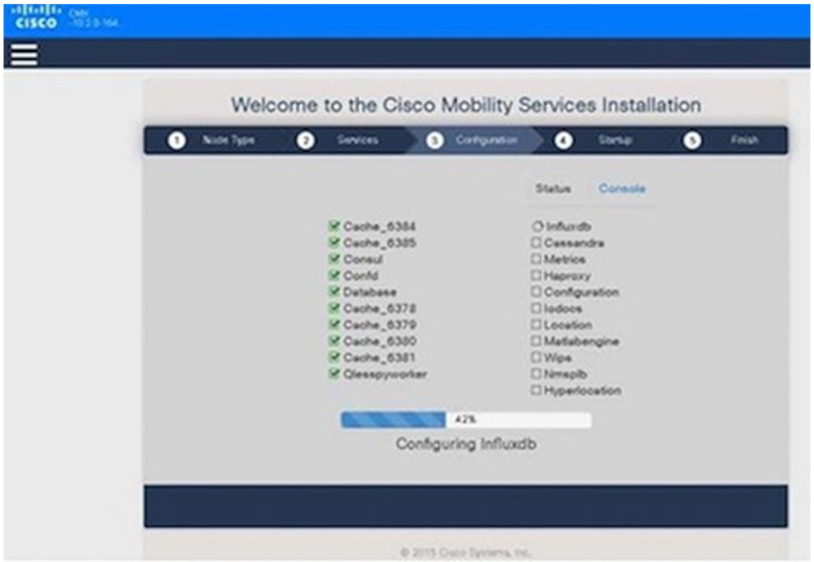
Password

Sign in

Please Login using your cmxadmin credentials

© 2015 Cisco Systems, Inc.

Step 2 Choose the Cisco CMX type as either **Location** or **Presence**.
The installation is initiated and services are started. Note that this may take a few minutes.



Welcome to the Cisco Mobility Services Installation

Status Console

☑ Cache_6384
☑ Cache_6385
☑ Consul
☑ Confd
☑ Database
☑ Cache_6378
☑ Cache_6379
☑ Cache_6380
☑ Cache_6381
☑ Qlesspyworker

○ Influxdb
□ Cassandra
□ Metrics
□ Haproxy
□ Configuration
□ Iodocs
□ Location
□ Matlabengine
□ Wips
□ Nmsplb
□ Hyperlocation

42%

Configuring Influxdb

© 2015 Cisco Systems, Inc.

The sequence of events is as follows:

a. Consul Configuration

b. DB Installation

c. Schema Migration

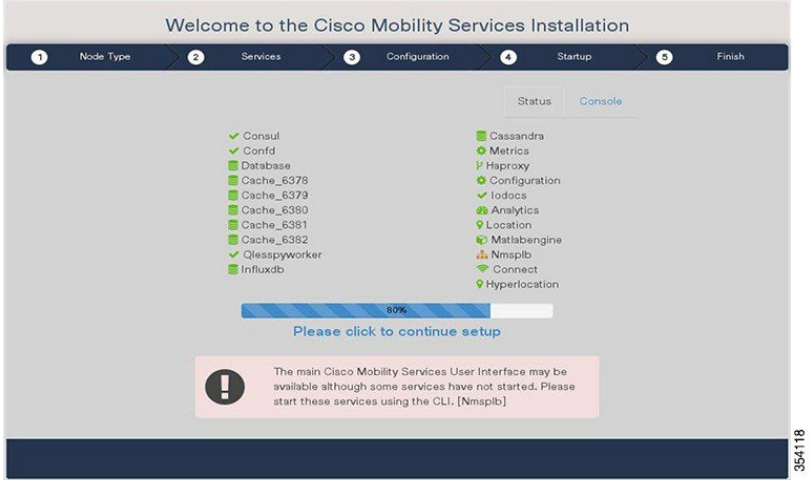
d. InfluxDB Configuration

e. Cassandra Installation

f. Node Registration

Step 3 Click **Please click to continue setup** or press **Enter** to proceed to the main portal.

Note You can monitor the progress of the installation either through the graphical status display or the console output. Note that this console is for display only.

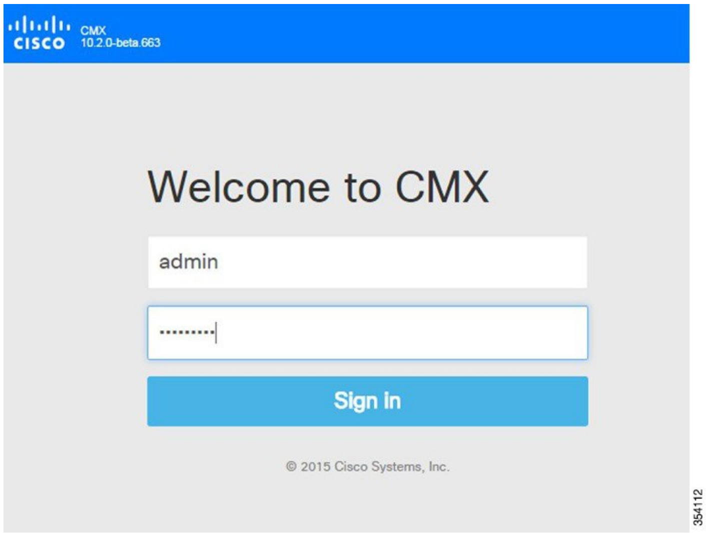

Welcome to the Cisco Mobility Services Installation

The main Cisco Mobility Services User Interface may be available although some services have not started. Please start these services using the CLI. [Nmsplb]

The installation is complete. If this is a reinstallation, the **Cisco CMX Welcome** window is displayed. If this is a fresh installation, the user is automatically authenticated and the **Cisco CMX Welcome** is skipped.

Step 4 Log in with the username **admin** and password **admin**.

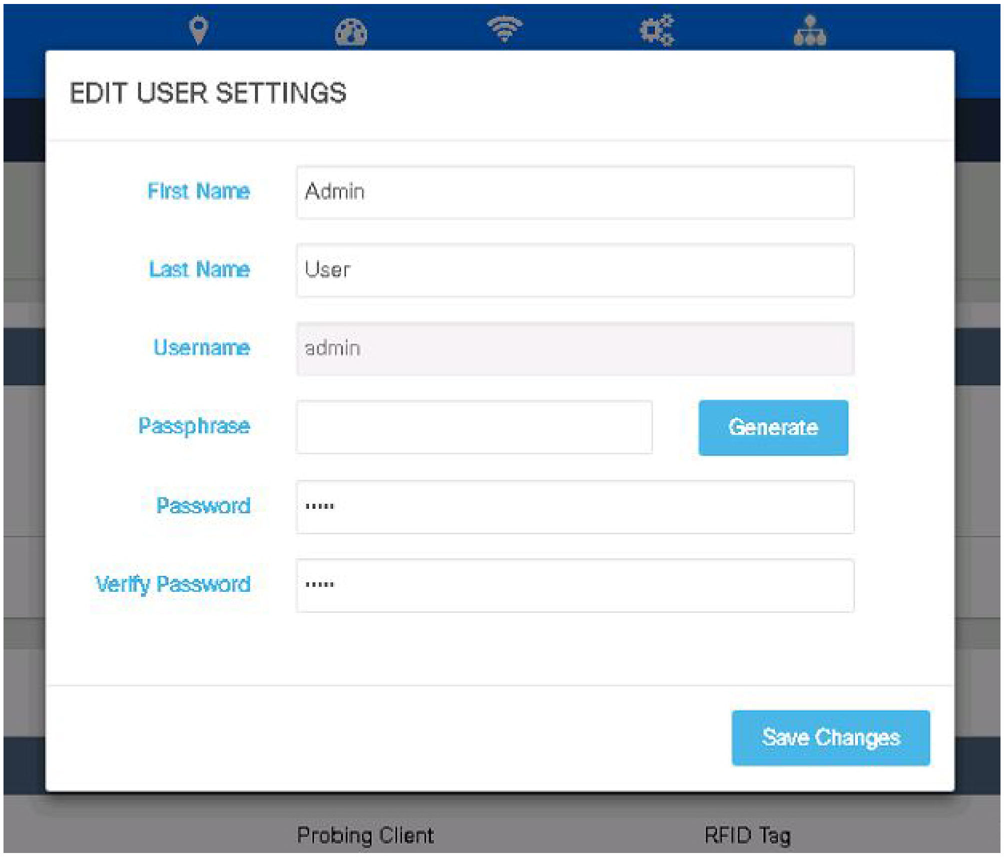
Figure 22: Welcome Screen



What to do next

A **Edit User Settings** window is displayed, from where you can complete the initial configuration. You must now set a password for the admin user using this window.

Figure 23: Edit User Settings



EDIT USER SETTINGS

First Name: Admin

Last Name: User

Username: admin

Passphrase:

Password: •••••

Verify Password: •••••

Procced to import Cisco WLC details and maps from Cisco Prime Infrastructure, and configure and test mail server settings.

Use https://<ip address> for all subsequent logins to the web user interface. Use https:// <ip-address>:1984 only for initial configuration.

Verifying Installation of Cisco CMX in a VMware Virtual Machine

You can verify the overall system health and status of the Cisco CMX services using the **System** tab in the Cisco CMX user interface. Ensure that all the services, memory, and CPU indicate a healthy status (green) for each Cisco CMX and Cisco CMX node, and that there is at least 1 active Cisco WLC.

The **System** tab contains the following subtabs:

- **Dashboard**—Provides an overall view of the system.
- **Alerts**—Enables you to view live alerts.
- **Patterns**—Enables you to detect patterns of various criteria, such as Client Count, CPU Usage, Memory Usage, and so on.

- **Metrics**—Enables you to view system metrics.

CHAPTER 2

Virtual Machine Setup and Administration

This chapter contains the following sections:

- Adding a Hard Disk to a Virtual Machine in the vSphere Client, on page 29
- Configuring the Network, on page 29
- Reconfiguring CPU and RAM for Cisco CMX installation, on page 29

Adding a Hard Disk to a Virtual Machine in the vSphere Client

When you add a hard disk to a virtual machine (VM), you can create a new virtual disk, add an existing virtual disk, or add a mapped Storage Area Network (SAN) Logical Unit Number (LUN).

In most cases, you can accept the default device node. For a hard disk, a nondefault device node is useful to control the boot order or to have different Small Computer System Interface (SCSI) controller types. For example, you might want to boot from an LSI Logic controller and use a Buslogic controller with bus sharing turned on to share a data disk with another VM.

Configuring the Network

By default, the VM uses the host network settings. Hence, no configuration is required for VM adapters on ESXi. If you have both public and private networks connected to the host and want the VM to access both the networks, you must configure the VM adapters in the vSphere client.

Reconfiguring CPU and RAM for Cisco CMX installation

Before you run any commands to reconfigure the CPU and RAM, run the **cmxctl config** command to back up the current configuration. Ensure to make the Cisco CMX device offline before the reconfiguration.

Step 1 Run the **cmxctl stop -a** command to stop all the Cisco CMX services.

Step 2 Run the **cmxos shutdown** command to shutdown the device.

Step 3 Navigate to VMWare manager.

Step 4 Change the RAM and CPU as required.

We recommend that you refer to the documentation for standard configurations. Random configurations may return unexpected results.

Step 5 Restart up the device.

Step 6 Run the **cmxctl status** command to verify if all the Cisco CMX services are running.

Step 7 (Optional) If the Cisco CMX services are not running, run the **cmxctl start** command to start the services.

Step 8 To reconfigure the RAM reserved for each service, run the **cmxctl config reload --resize=True** command.
Running this command will prompt to restart the services. Use the **cmxctl start** command to restart the services.

Step 9 To verify the configuration, run the **cmxctl config get** command and compare the current and previous configuration.

CHAPTER 3

Uploading the Cisco MSE/CMX ISO Image to the Cisco MSE 3365/Cisco CMX 3375

Note Make sure the Serial over Lan (SoL) functionality is enabled on the Cisco Unified Communication System (UCS). To enable SoL on the Cisco UCS server, use the **set enabled yes** command. For more information on enabling SoL, refer to the Cisco UCS documentation on Cisco.com.

- Uploading Cisco CMX ISO Image to Cisco CMX 3375 Using Newer CIMC Versions, on page 31
- Uploading the Cisco CMX/MSE ISO Image to the Cisco MSE 3365 Using Newer CIMC Versions, on page 36
- Uploading the Cisco CMX/MSE ISO Image to the Cisco MSE 3365 Using Older CIMC Versions, on page 42

Uploading Cisco CMX ISO Image to Cisco CMX 3375 Using Newer CIMC Versions

The Cisco CMX 3375 Appliance requires Cisco CMX Release 10.5.1 or later. Minimal configuration is done for the Cisco CMX as part of installation using the console. For hardware and software installation information, see the Cisco 3375 Appliance for Cisco Connected Mobile Experiences Installation Guide at: https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-installation-guides-list.html

Step 1 Download the Cisco CMX 10.5.1 image from Download Software on cisco.com.

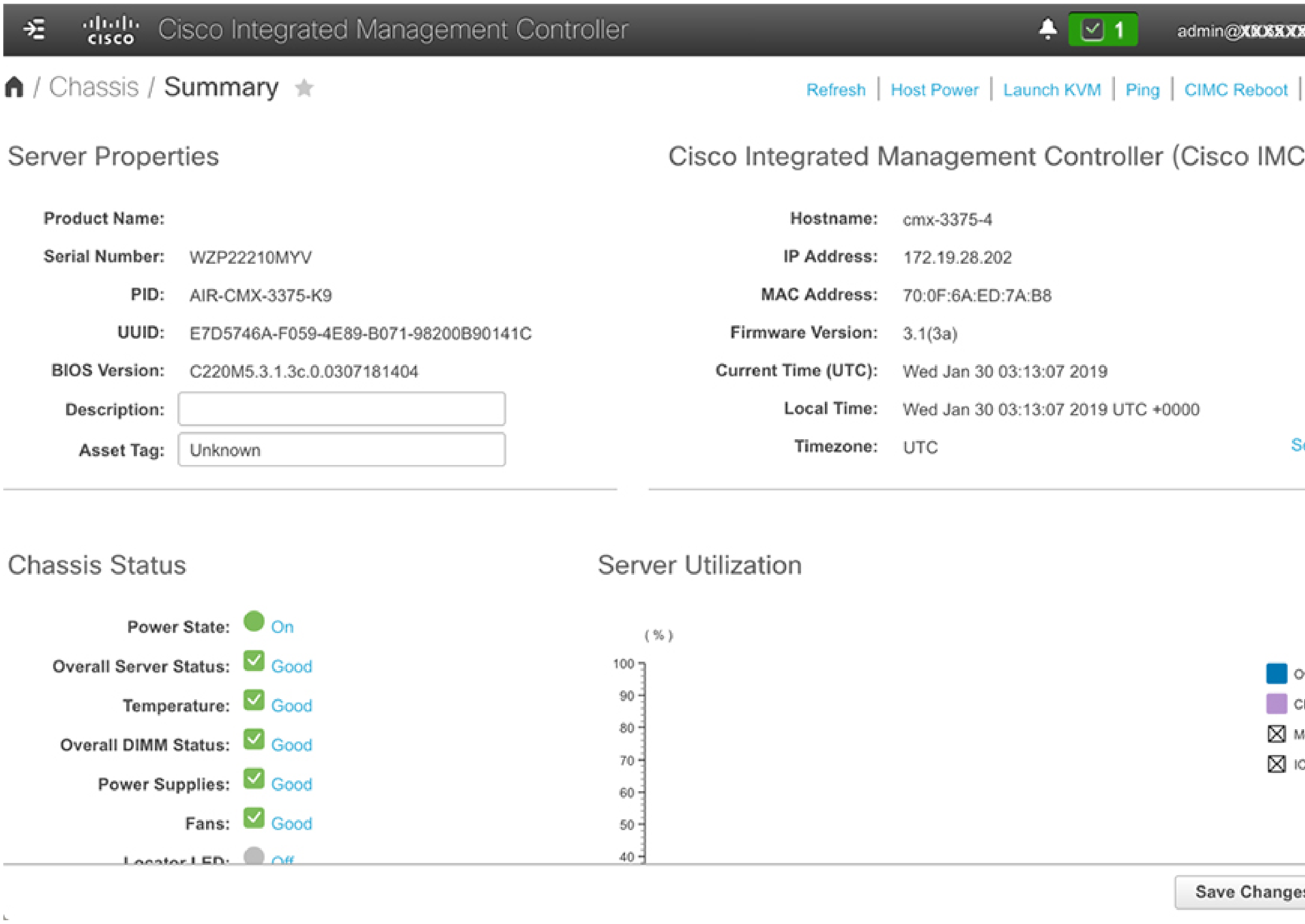
Step 2 Power up the Cisco CMX 3375 appliance and configure the CIMC IP Address and user credentials.

Step 3 Log in to CIMC IP using Internert Explorer.

Step 4 In the left pane, click **Menu** > **Compute** > **BIOS**.

Step 5 From the **Configured Boot Mode** drop-down list, choose **Legacy**.

Figure 24: BIOS Configured Boot Mode



Cisco Integrated Management Controller

admin@XXXXXX

/ Chassis / Summary

Refresh | Host Power | Launch KVM | Ping | CIMC Reboot |

Server Properties

Product Name:

Serial Number: WZP22210MYV

PID: AIR-CMX-3375-K9

UUID: E7D5746A-F059-4E89-B071-98200B90141C

BIOS Version: C220M5.3.1.3c.0.0307181404

Description:

Asset Tag: Unknown

Cisco Integrated Management Controller (Cisco IMC

Hostname: cmx-3375-4

IP Address: 172.19.28.202

MAC Address: 70:0F:6A:ED:7A:B8

Firmware Version: 3.1(3a)

Current Time (UTC): Wed Jan 30 03:13:07 2019

Local Time: Wed Jan 30 03:13:07 2019 UTC +0000

Timezone: UTC

Chassis Status

Power State: ● On

Overall Server Status: ☑ Good

Temperature: ☑ Good

Overall DIMM Status: ☑ Good

Power Supplies: ☑ Good

Fans: ☑ Good

Locator LED: ● Off

Server Utilization

Step 6 Follow the on screen instruction to reboot the system.

Step 7 Click **Configure Boot Order**.

Step 8 In the **Configure Boot Order** window, click **Advanced** tab.

Step 9 Click **Add Virtual Media**.

Step 10 Enter a name for the new virtual media.

Step 11 From the **Sub Type** drop-down list, choose **KVM MAPPED DVD**.

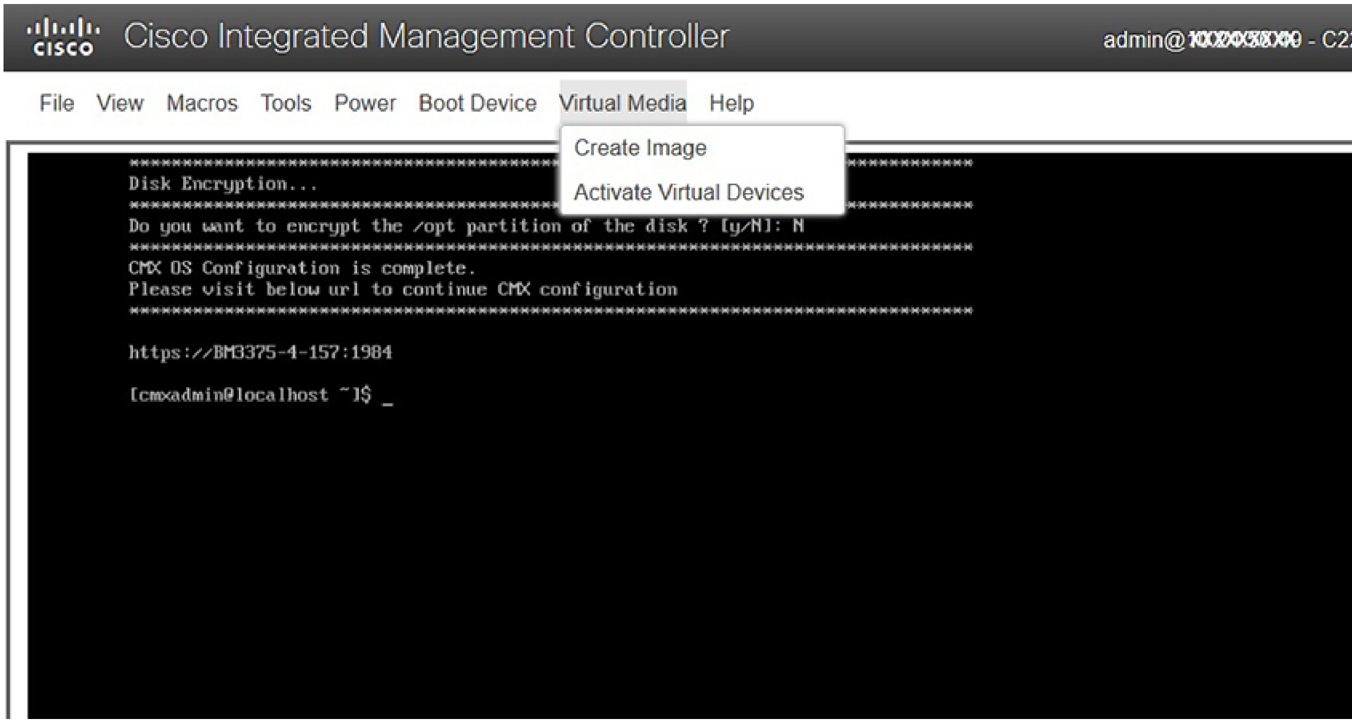
Step 12 Click **Save Changes**.

The new virtual media is created and enabled.

Step 13 Use IE and open KVM. We recommend that you use JAVA Based KVM on IE or Firefox for more consistent results.

Step 14 Click **Virtual Media** > **Activate Virtual Devices**.

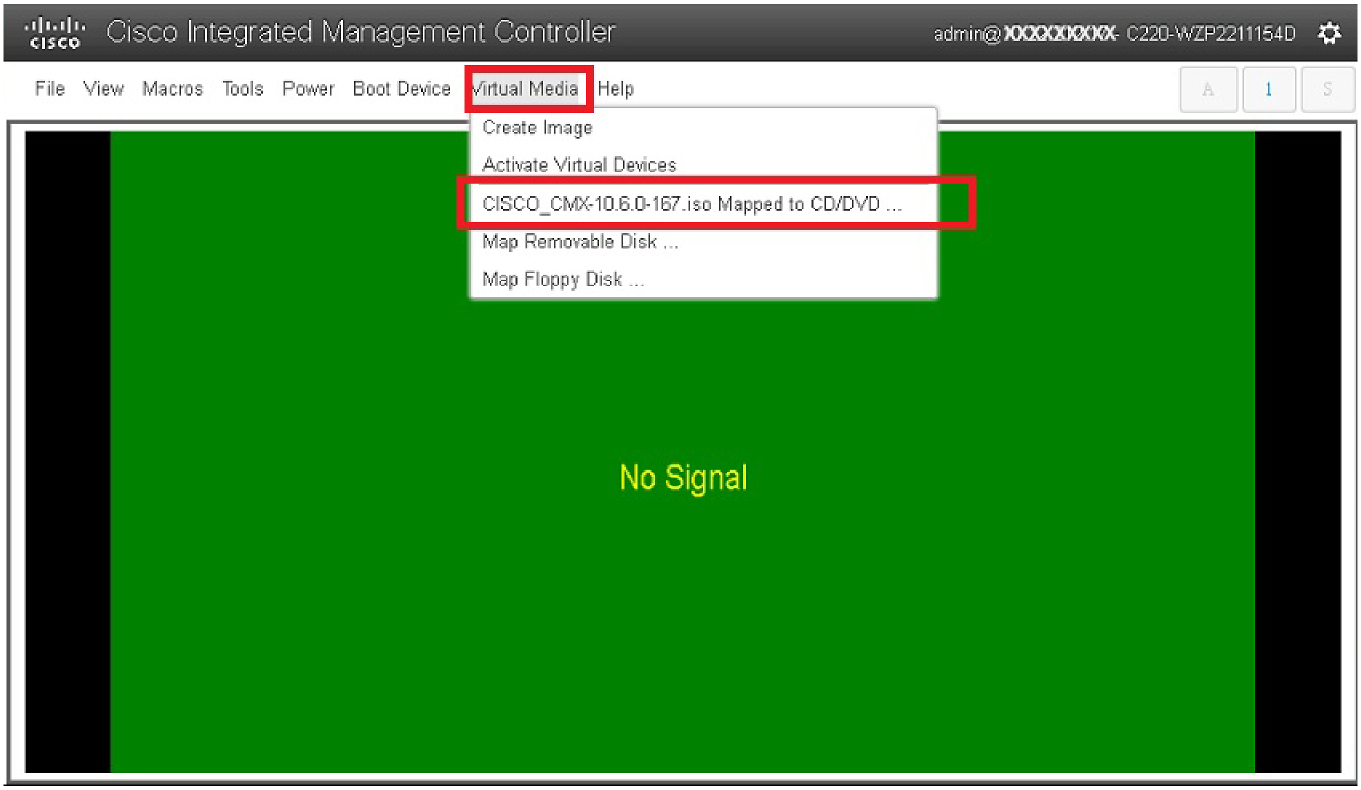
Figure 25: Activate Virtual Devices



```
********************************************************************************
Disk Encryption...
********************************************************************************
Do you want to encrypt the /opt partition of the disk ? [y/N]: N
********************************************************************************
CMX OS Configuration is complete.
Please visit below url to continue CMX configuration
********************************************************************************

https://BM3375-4-157:1984

[cmxadmin@localhost ~]$ _
```

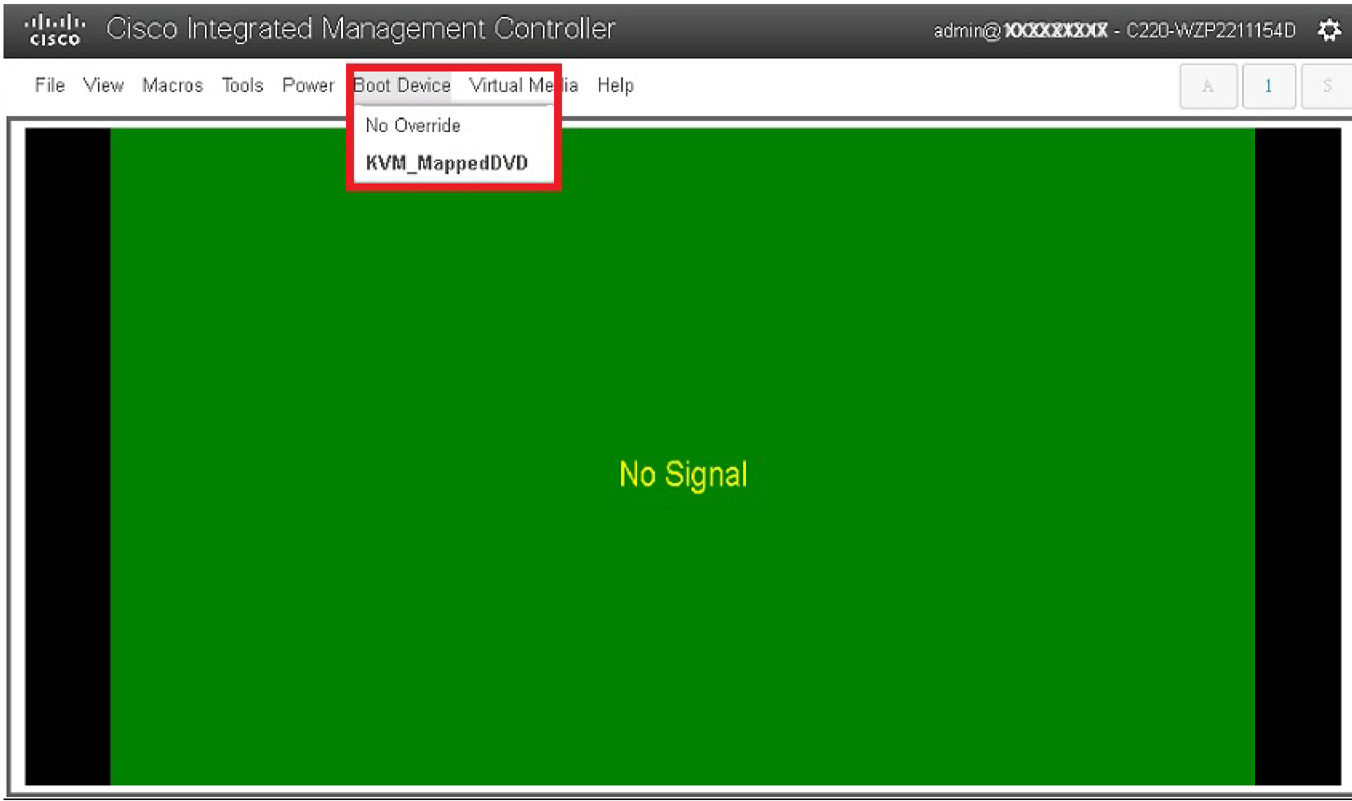
Step 15 Click Map CD/DVD and select image from your local folder.

Figure 26: Virtual Media - Cisco CMX



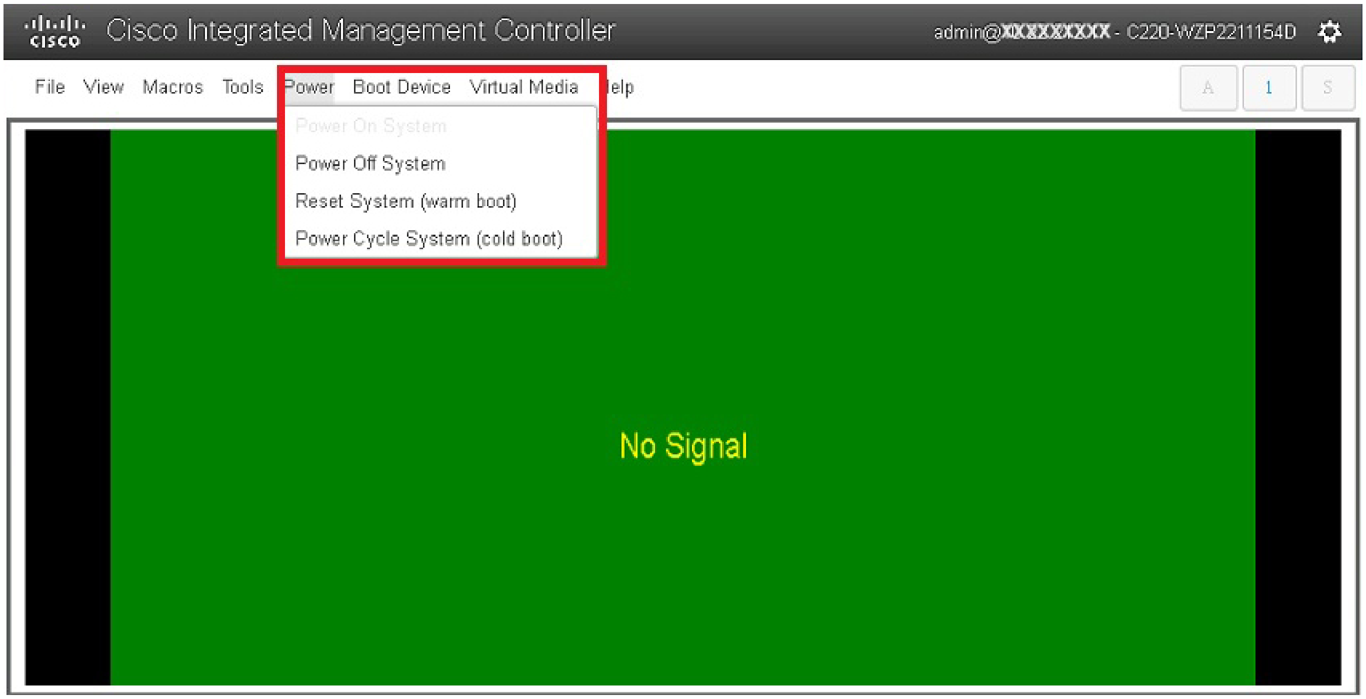
Step 16 Select the Boot Device the name given in step 10.

Figure 27: Boot Device



Step 17 In the KVM, use the **Power** option to power on the Cisco CMX 3375 Appliance.

Figure 28: Boot Device > Power On System



Step 18 After the appliance is rebooted, press **F6** to enter **Boot Menu**.

Step 19 Select **Cisco vKVM Mapped DVD**.

Step 20 Select **Install using Current Console** as the install method.

Step 21 Click **Proceed with install**. Wait for 20 to 30 minutes for copying CMX file.

The system is rebooted after the file is copied. The system is loaded with Centos 7. Cisco CMX welcome window is displayed.

What to do next

For more information about configuring Cisco CMX, see Configuring Cisco CMX Release 10.5.x and Later, on page 17.

Uploading the Cisco CMX/MSE ISO Image to the Cisco MSE 3365 Using Newer CIMC Versions

MSE 3365 Software Reset is a process used to load the MSE 3365 with a required image (MSE 8.x, or CMX 10.x). The MSE 3365 is a UCS-based device, and can be accessed through the Cisco Integrated Management Controller (CIMC) interface.

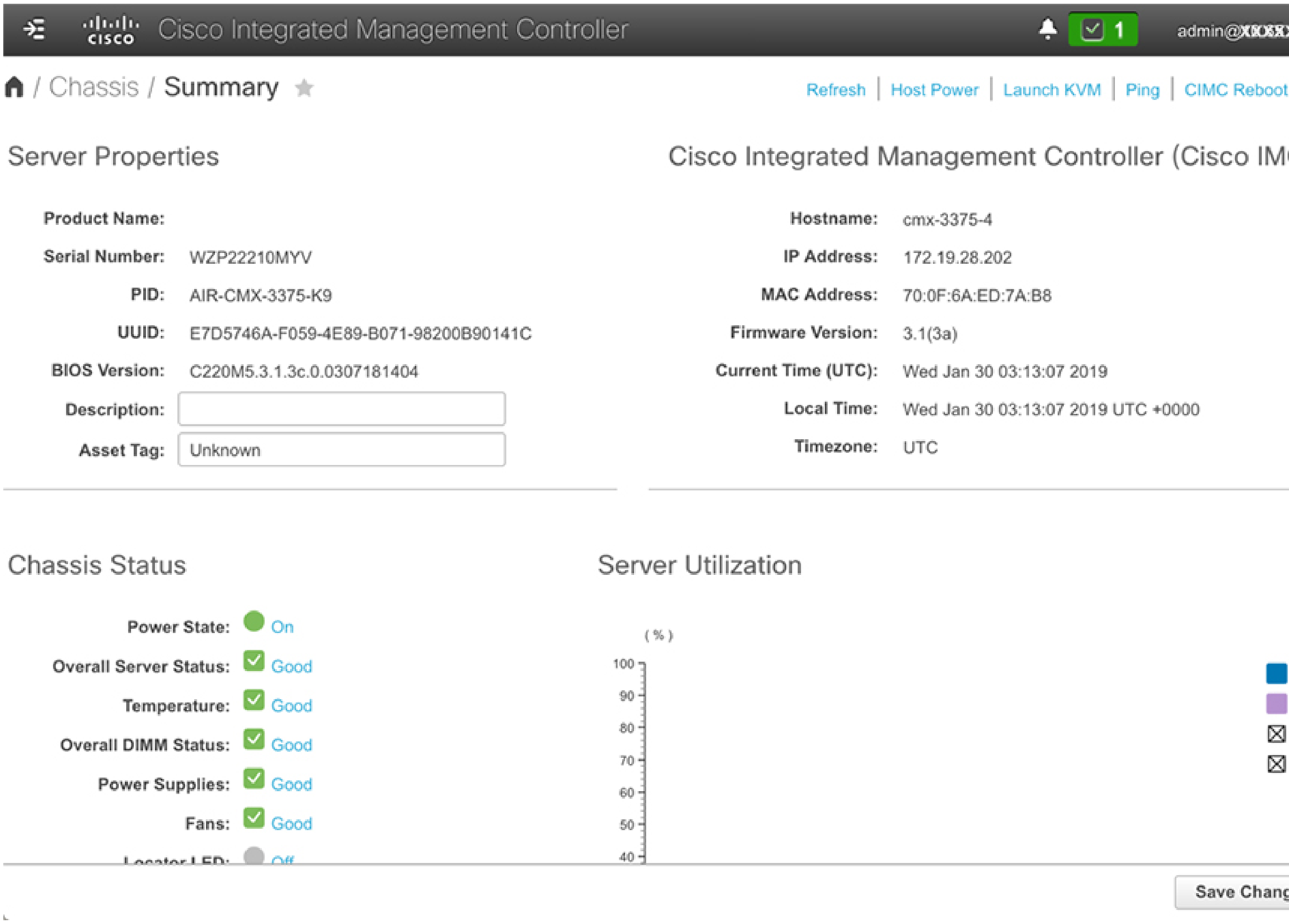
Before you begin

Java Version 1.6.0.14 must be installed on the client machine used to access your MSE 3365 device.

Step 1 Download the Cisco MSE ISO image from the Download Software page on cisco.com.

Step 2 Open a browser, and enter the IP address of your device to log in to to the Cisco Integrated Management Controller (CIMC) GUI interface (Address format is https://x.x.x.x).

Figure 29: Cisco Integrated Management Controller Interface



Cisco Integrated Management Controller
1
admin@XXXXX
Chassis / Summary
Refresh | Host Power | Launch KVM | Ping | CIMC Reboot
Save Chang
(%)
100
90
80
70
60
50
40

Server Properties

Product Name:
Serial Number: WZP22210MYV
PID: AIR-CMX-3375-K9
UUID: E7D5746A-F059-4E89-B071-98200B90141C
BIOS Version: C220M5.3.1.3c.0.0307181404
Description:
Asset Tag: Unknown

Cisco Integrated Management Controller (Cisco IM

Hostname: cmx-3375-4
IP Address: 172.19.28.202
MAC Address: 70:0F:6A:ED:7A:B8
Firmware Version: 3.1(3a)
Current Time (UTC): Wed Jan 30 03:13:07 2019
Local Time: Wed Jan 30 03:13:07 2019 UTC +0000
Timezone: UTC

Chassis Status

Power State: ● On
Overall Server Status: ☑ Good
Temperature: ☑ Good
Overall DIMM Status: ☑ Good
Power Supplies: ☑ Good
Fans: ☑ Good
Locator LED: ● Off

Server Utilization

Step 3 Click **Server** and in the **Server Summary** page, click **Launch KVM Console** and click **OK**.
A mini executable file is downloaded.

Step 4 Open the file using javaws.exe from the bin folder of your Java installation. If a security error prevents you from installing the file, add the URL of the CIMC to the list of exception sites, using the steps below.

a) Choose **Control Panel** > **Programs** > **Java**.

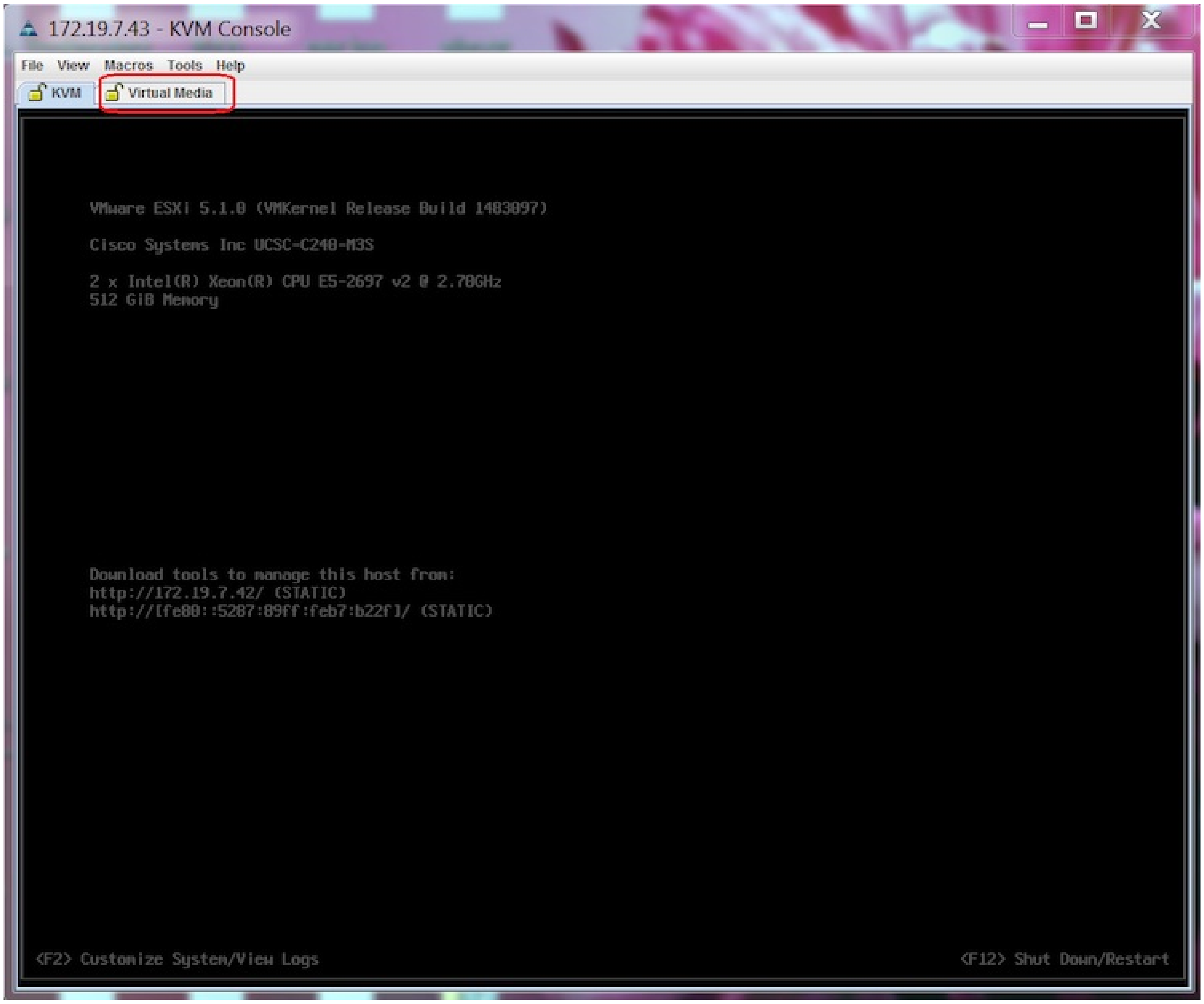
b) Choose **Security** > **Edit Site List** > **Add** and add the CIMC URL.

c) Click **OK**.

The installation is initiated.

Step 5 In the KVM Console window that is displayed after the installation, click the **Virtual Media** tab.

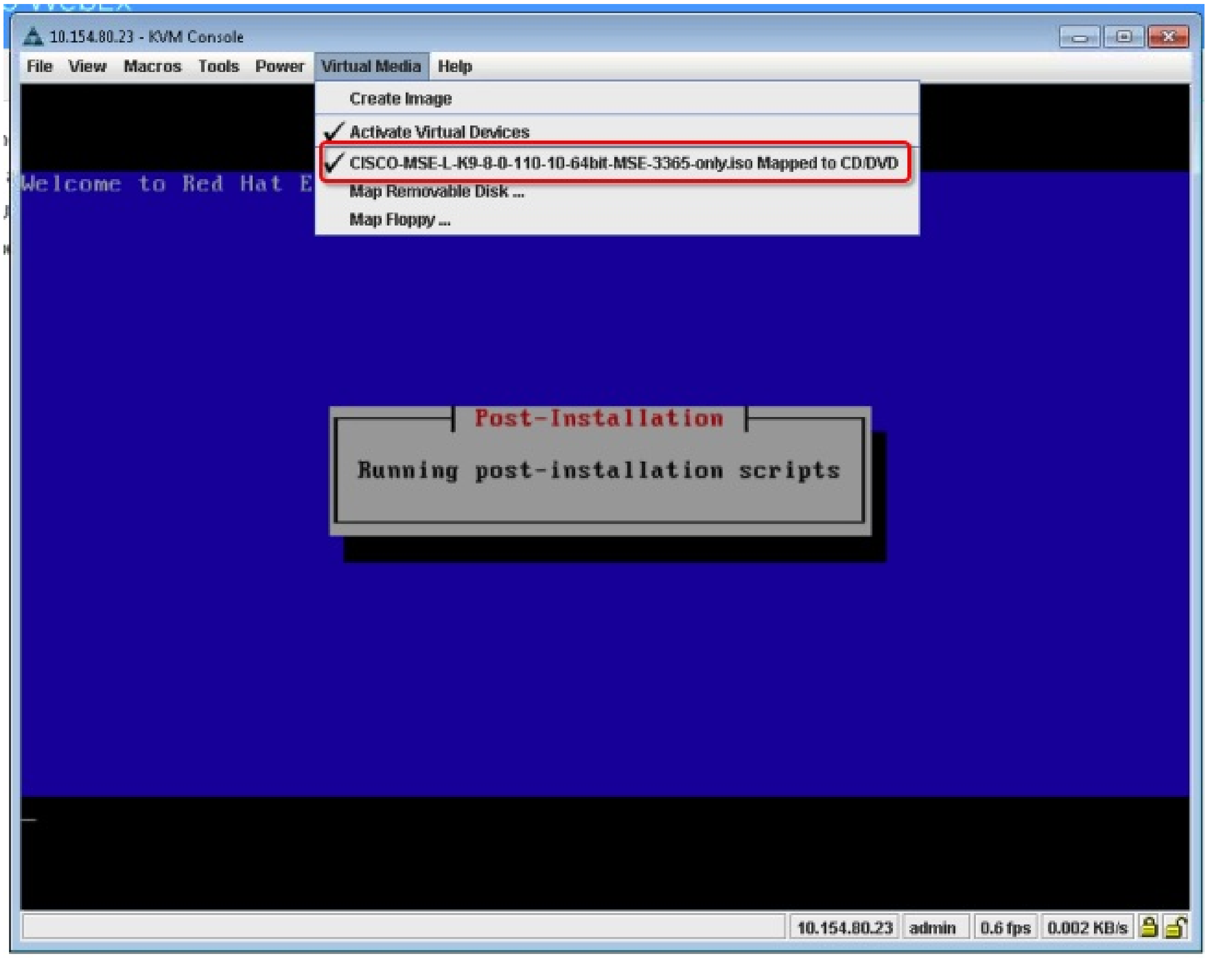
Figure 30: KVM Console



```
VMware ESXi 5.1.0 (VMKernel Release Build 1483097)

Cisco Systems Inc UCSC-C240-M3S

2 x Intel(R) Xeon(R) CPU E5-2697 v2 @ 2.70GHz
512 GiB Memory

Download tools to manage this host from:
http://172.19.7.42/ (STATIC)
http://[fe80::5287:89ff:feb7:b22f]/ (STATIC)

<F2> Customize System/View Logs                                    <F12> Shut Down/Restart
```

Step 6 In the **Virtual Media** window that is displayed, choose **Activate Virtual Devices** > **Select "Map CD/DVD**. Browse and select the downloaded MSE image.

Figure 31: ISO Image Selected


10.154.80.23 - KVM Console
File View Macros Tools Power Virtual Media Help
Create Image
✓ Activate Virtual Devices
✓ CISCO-MSE-L-K9-8-0-110-10-64bit-MSE-3365-only.iso Mapped to CD/DVD
Map Removable Disk ...
Map Floppy ...
Welcome to Red Hat E
Post-Installation
Running post-installation scripts
10.154.80.23
admin
0.6 fps
0.002 KB/s

The recovery process begins. The **Select Install Method** window is displayed.

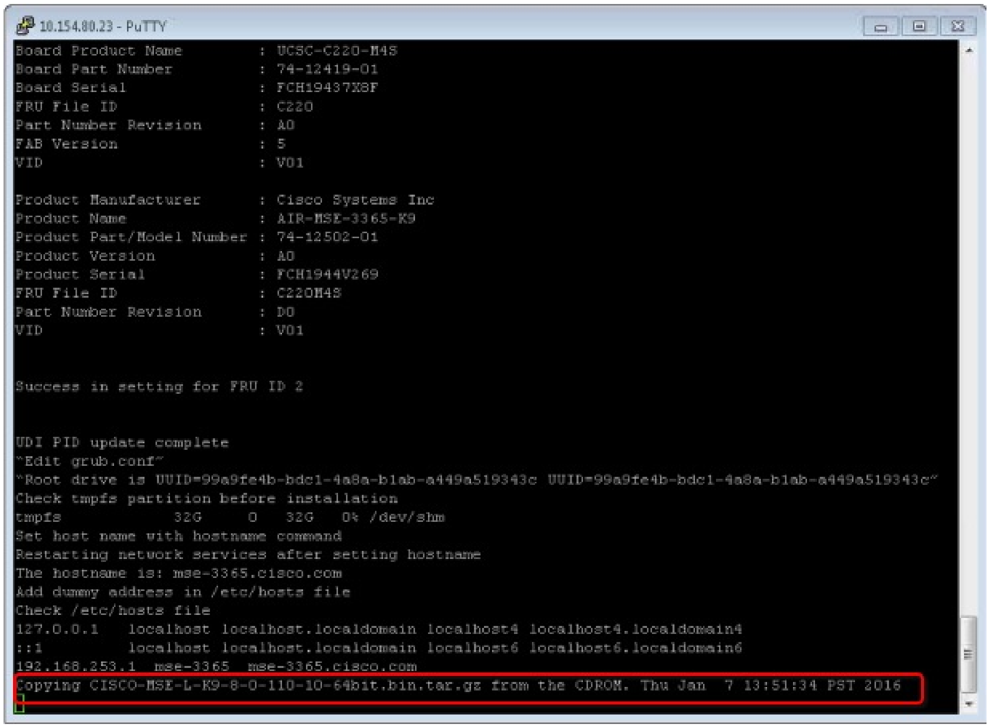
Step 7 In the **Select Install Method** window that is displayed, choose any of the following options:

- Option 1: **Install CMX using Serial**—Respond to the prompt to press ENTER by starting an SSH session to the CIMC interface, as the KVM console does not permit you to press ENTER (With CSCuw32543). Use the following commands to initiate the SSH session:

  ```
  ssh <cimc-ip-address>
  connect host
  ```

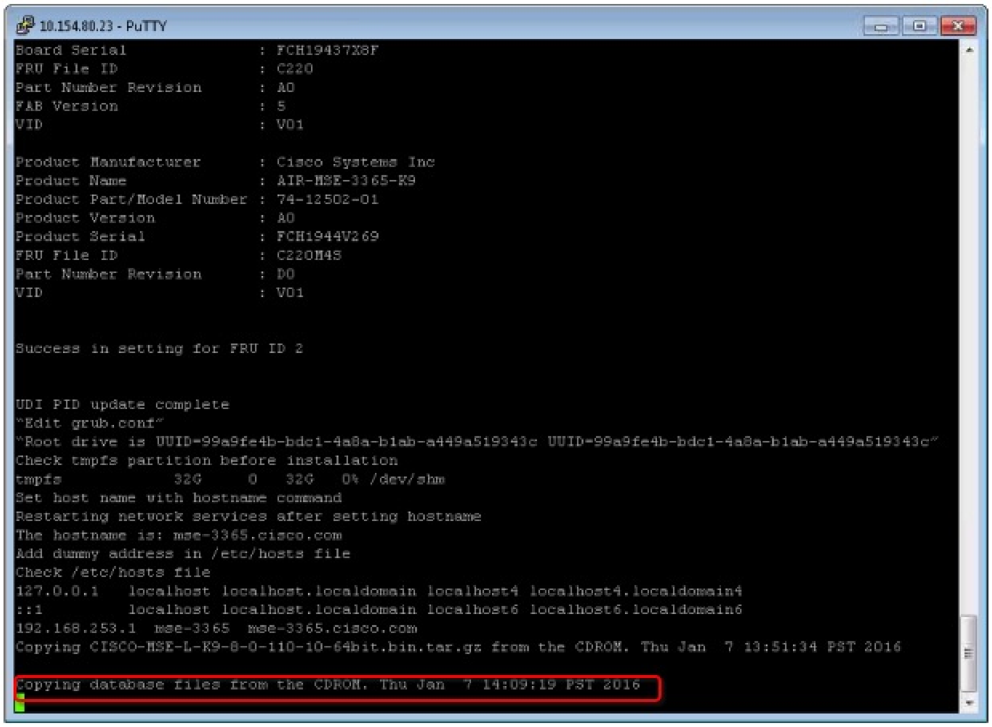
  You can see that the image is being copied from CDROM. The process can take up to forty-five minutes to copy.

Figure 32: Copying from CDROM



```
Board Product Name         : UCSC-C220-M4S
Board Part Number          : 74-12419-01
Board Serial               : FCH19437X8F
FRU File ID                : C220
Part Number Revision       : A0
FAB Version                : 5
VID                        : V01

Product Manufacturer       : Cisco Systems Inc
Product Name               : AIR-MSE-3365-K9
Product Part/Model Number  : 74-12502-01
Product Version            : A0
Product Serial             : FCH1944V269
FRU File ID                : C220M4S
Part Number Revision       : D0
VID                        : V01


Success in setting for FRU ID 2


UDI PID update complete
"Edit grub.conf"
"Root drive is UUID=99a9fe4b-bdc1-4a8a-b1ab-a449a519343c UUID=99a9fe4b-bdc1-4a8a-b1ab-a449a519343c"
Check tmpfs partition before installation
tmpfs             32G     0   32G   0% /dev/shm
Set host name with hostname command
Restarting network services after setting hostname
The hostname is: mse-3365.cisco.com
Add dummy address in /etc/hosts file
Check /etc/hosts file
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.253.1  mse-3365  mse-3365.cisco.com
Copying CISCO-MSE-L-K9-8-0-110-10-64bit.bin.tar.gz from the CDROM. Thu Jan  7 13:51:34 PST 2016
```

Figure 33: Copying Database Files from CDROM

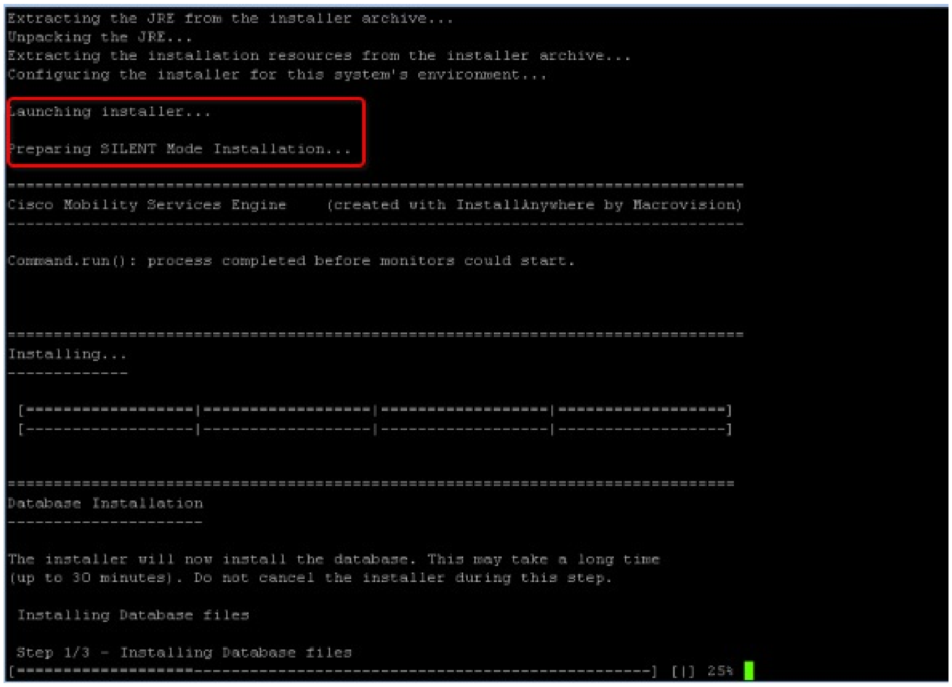


```
Board Serial               : FCH19437X8F
FRU File ID                : C220
Part Number Revision       : A0
FAB Version                : 5
VID                        : V01

Product Manufacturer       : Cisco Systems Inc
Product Name               : AIR-MSE-3365-K9
Product Part/Model Number  : 74-12502-01
Product Version            : A0
Product Serial             : FCH1944V269
FRU File ID                : C220M4S
Part Number Revision       : D0
VID                        : V01


Success in setting for FRU ID 2


UDI PID update complete
"Edit grub.conf"
"Root drive is UUID=99a9fe4b-bdc1-4a8a-b1ab-a449a519343c UUID=99a9fe4b-bdc1-4a8a-b1ab-a449a519343c"
Check tmpfs partition before installation
tmpfs             32G     0   32G   0% /dev/shm
Set host name with hostname command
Restarting network services after setting hostname
The hostname is: mse-3365.cisco.com
Add dummy address in /etc/hosts file
Check /etc/hosts file
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.253.1  mse-3365  mse-3365.cisco.com
Copying CISCO-MSE-L-K9-8-0-110-10-64bit.bin.tar.gz from the CDROM. Thu Jan  7 13:51:34 PST 2016

Copying database files from the CDROM. Thu Jan  7 14:09:19 PST 2016
```

- Option 2: **Install CMX using current console**—The recovery process is initiated using the current console.

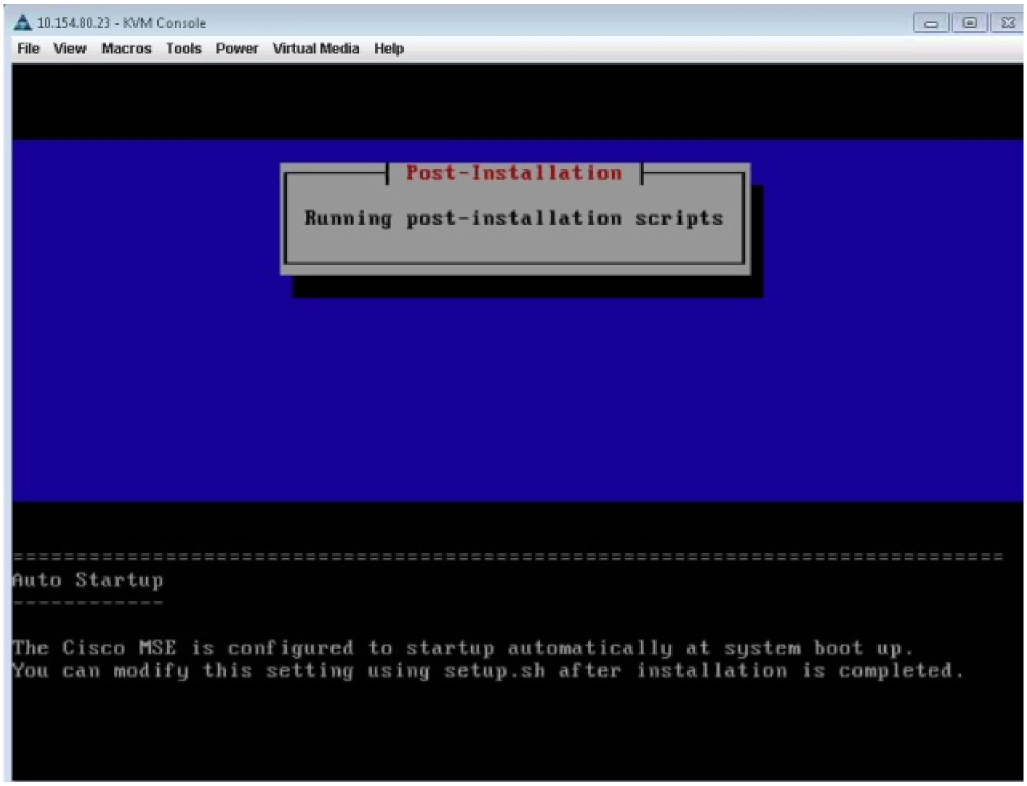
Step 8 Once the image is copied, a silent installation is initiated.

Figure 34: Preparing SILENT Mode Installation



```
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...

Preparing SILENT Mode Installation...

===============================================================================
Cisco Mobility Services Engine    (created with InstallAnywhere by Macrovision)
-------------------------------------------------------------------------------

Command.run(): process completed before monitors could start.



===============================================================================
Installing...
-------------

 [==================|==================|==================|==================]
 [------------------|------------------|------------------|------------------]


==============================================================================
Database Installation
---------------------

The installer will now install the database. This may take a long time
(up to 30 minutes). Do not cancel the installer during this step.

 Installing Database files

 Step 1/3 - Installing Database files
[===================-------------------------------------------------------] [|] 25%
```

Figure 35: Running Post-Installation Scripts

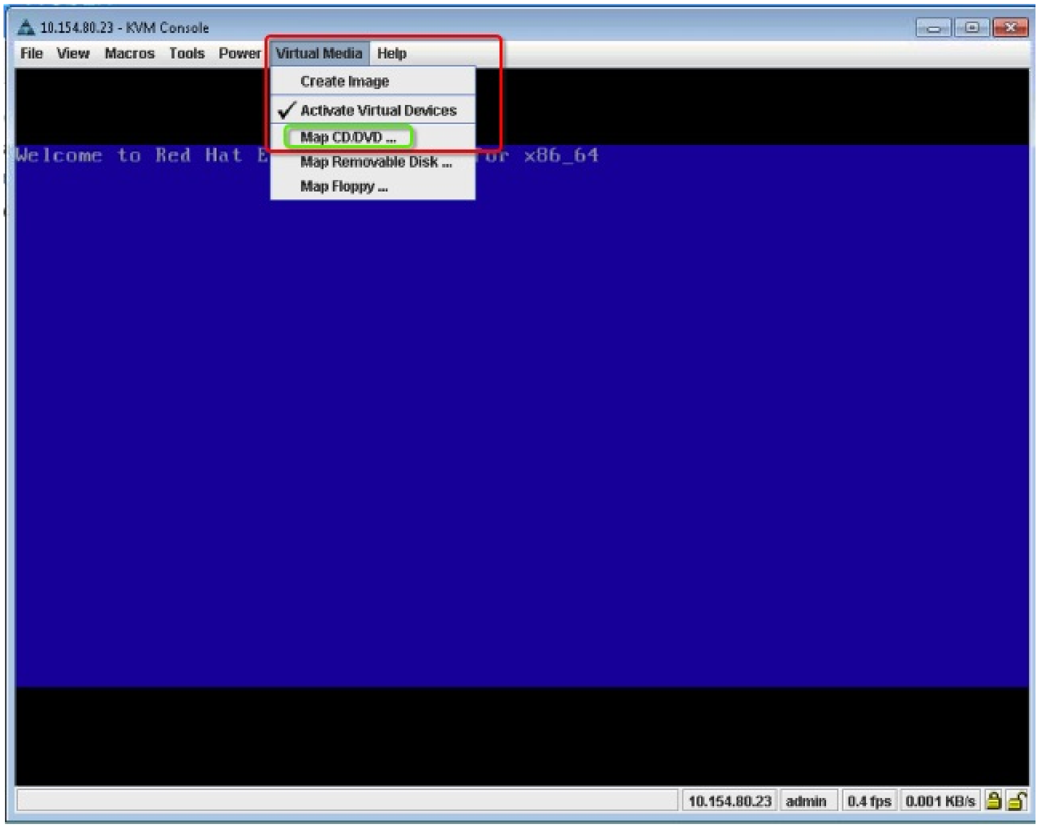


10.154.80.23 - KVM Console
File View Macros Tools Power Virtual Media Help

```
Post-Installation

Running post-installation scripts

===============================================================================
Auto Startup
------------

The Cisco MSE is configured to startup automatically at system boot up.
You can modify this setting using setup.sh after installation is completed.
```

Step 9 The device boots up with the newly loaded image. The CD/DVD mapping is automatically unchecked. In case it is checked, uncheck the **Activate Virtual Devices** option, so that the BIOS setting is checked for the image copied on the HDD every time it reboots.

Figure 36: Map CD/DVD



What to do next

For more information about configuring Cisco CMX, see Configuring Cisco CMX Release 10.5.x and Later, on page 17.

Uploading the Cisco CMX/MSE ISO Image to the Cisco MSE 3365 Using Older CIMC Versions

MSE 3365 Software Reset is a process used to load the MSE 3365 with a required image (MSE 8.x, or CMX 10.x). The MSE 3365 is a UCS-based device, and can be accessed through the Cisco Integrated Management Controller (CIMC) interface.

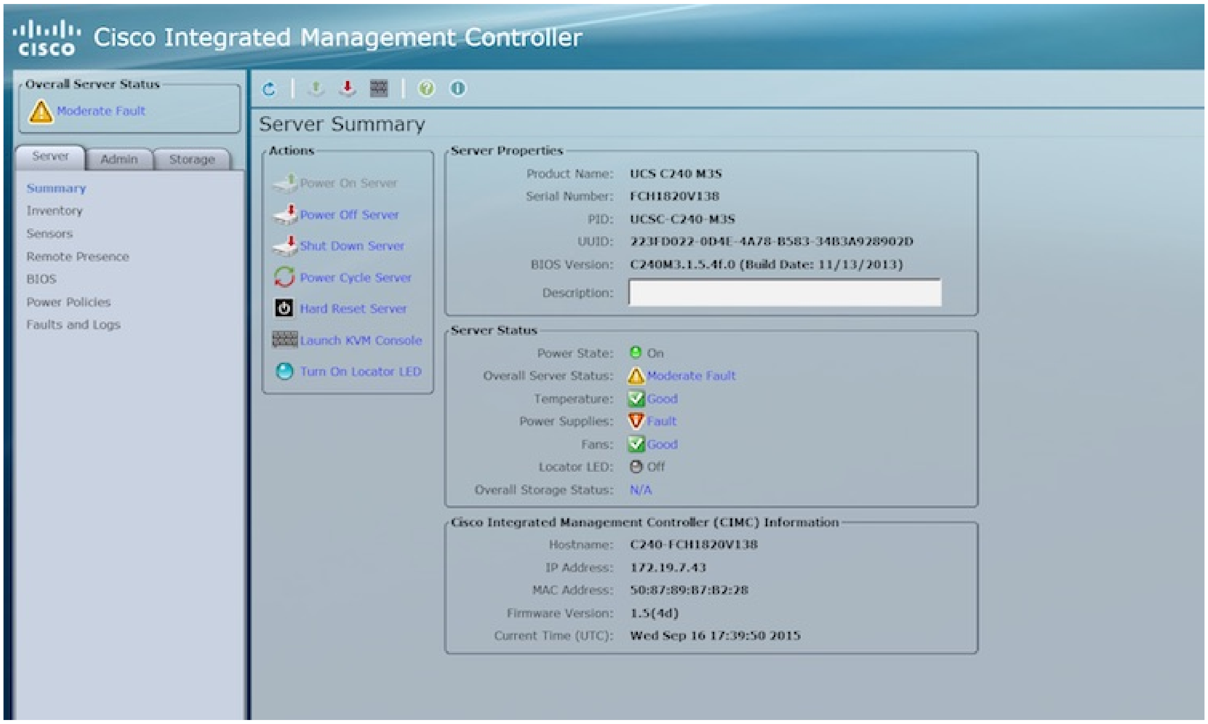
Before you begin

Java Version 1.6.0.14 must be installed on the client machine used to access your MSE 3365 device.

Step 1 Download the Cisco MSE ISO image from the Download Software page on cisco.com.

Step 2 Open a browser, and enter the IP address of your device to log in to to the Cisco Integrated Management Controller (CIMC) GUI interface (Address format is https://x.x.x.x).

Figure 37: Cisco Integrated Management Controller Interface



Server Properties

Product Name: UCS C240 M3S
Serial Number: FCH1820V138
PID: UCSC-C240-M3S
UUID: 223FD022-0D4E-4A78-B583-34B3A928902D
BIOS Version: C240M3.1.5.4f.0 (Build Date: 11/13/2013)
Description:

Server Status

Power State: On
Overall Server Status: Moderate Fault
Temperature: Good
Power Supplies: Fault
Fans: Good
Locator LED: Off
Overall Storage Status: N/A

Cisco Integrated Management Controller (CIMC) Information

Hostname: C240-FCH1820V138
IP Address: 172.19.7.43
MAC Address: 50:87:89:B7:B2:28
Firmware Version: 1.5(4d)
Current Time (UTC): Wed Sep 16 17:39:50 2015

Step 3 Click **Server** and in the **Server Summary** page, click **Launch KVM Console** and click **OK**.
A mini executable file is downloaded.

Step 4 Open the file using javaws.exe from the bin folder of your Java installation. If a security error prevents you from installing the file, add the URL of the CIMC to the list of exception sites, using the steps below.

a) Choose **Control Panel** > **Programs** > **Java**.

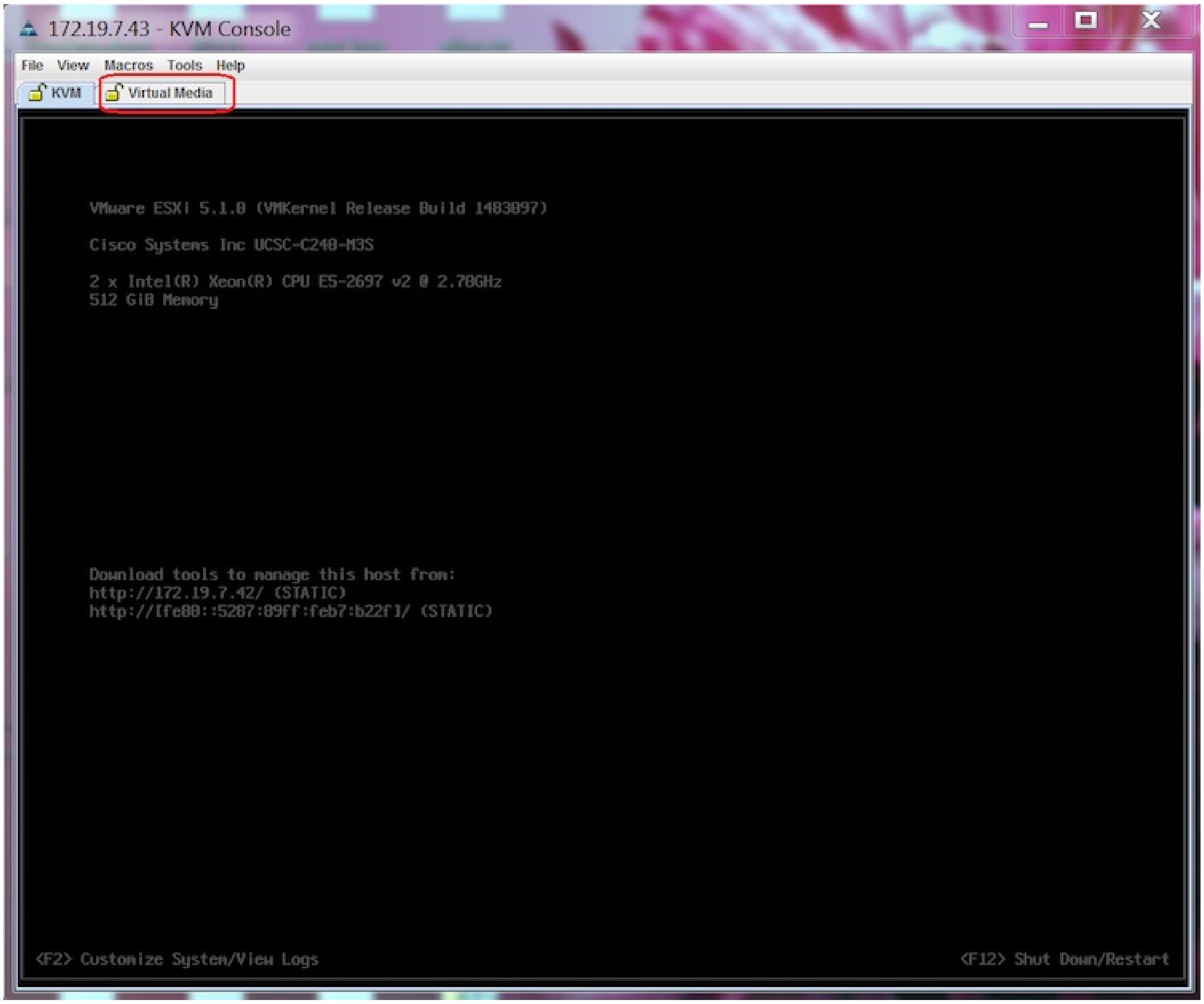
b) Choose **Security** > **Edit Site List** > **Add** and add the CIMC URL.

c) Click **OK**.

The installation is initiated.

Step 5 In the KVM Console window that is displayed after the installation, click the **Virtual Media** tab.

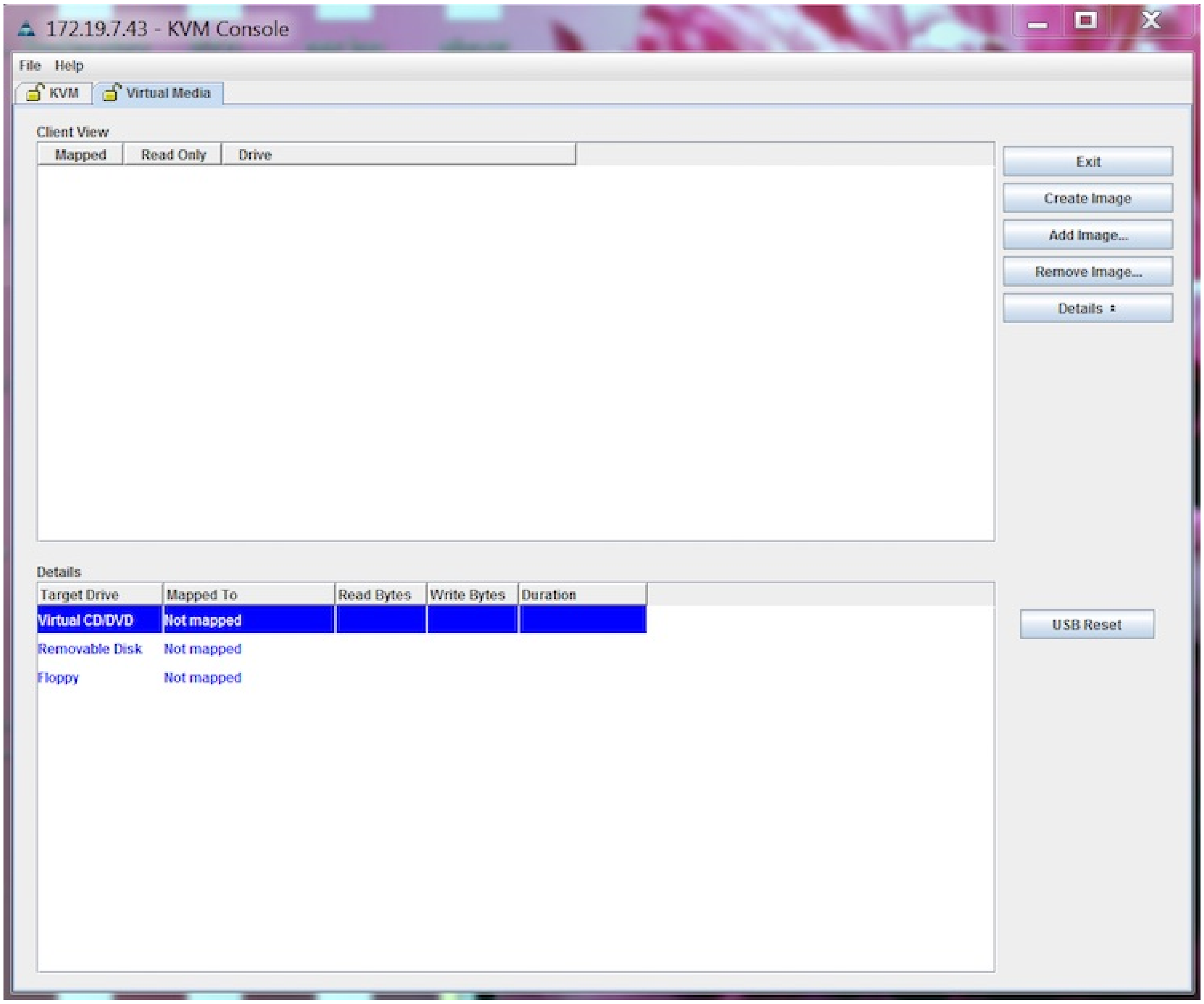
Figure 38: KVM Console



```
VMware ESXi 5.1.0 (VMKernel Release Build 1483097)

Cisco Systems Inc UCSC-C240-M3S

2 x Intel(R) Xeon(R) CPU E5-2697 v2 @ 2.70GHz
512 GiB Memory




Download tools to manage this host from:
http://172.19.7.42/ (STATIC)
http://[fe80::5287:89ff:feb7:b22f]/ (STATIC)




<F2> Customize System/View Logs                                   <F12> Shut Down/Restart
```

Step 6 In the **Virtual Media** window that is displayed, click **Add Image**.

Figure 39: Virutal Media



Client View

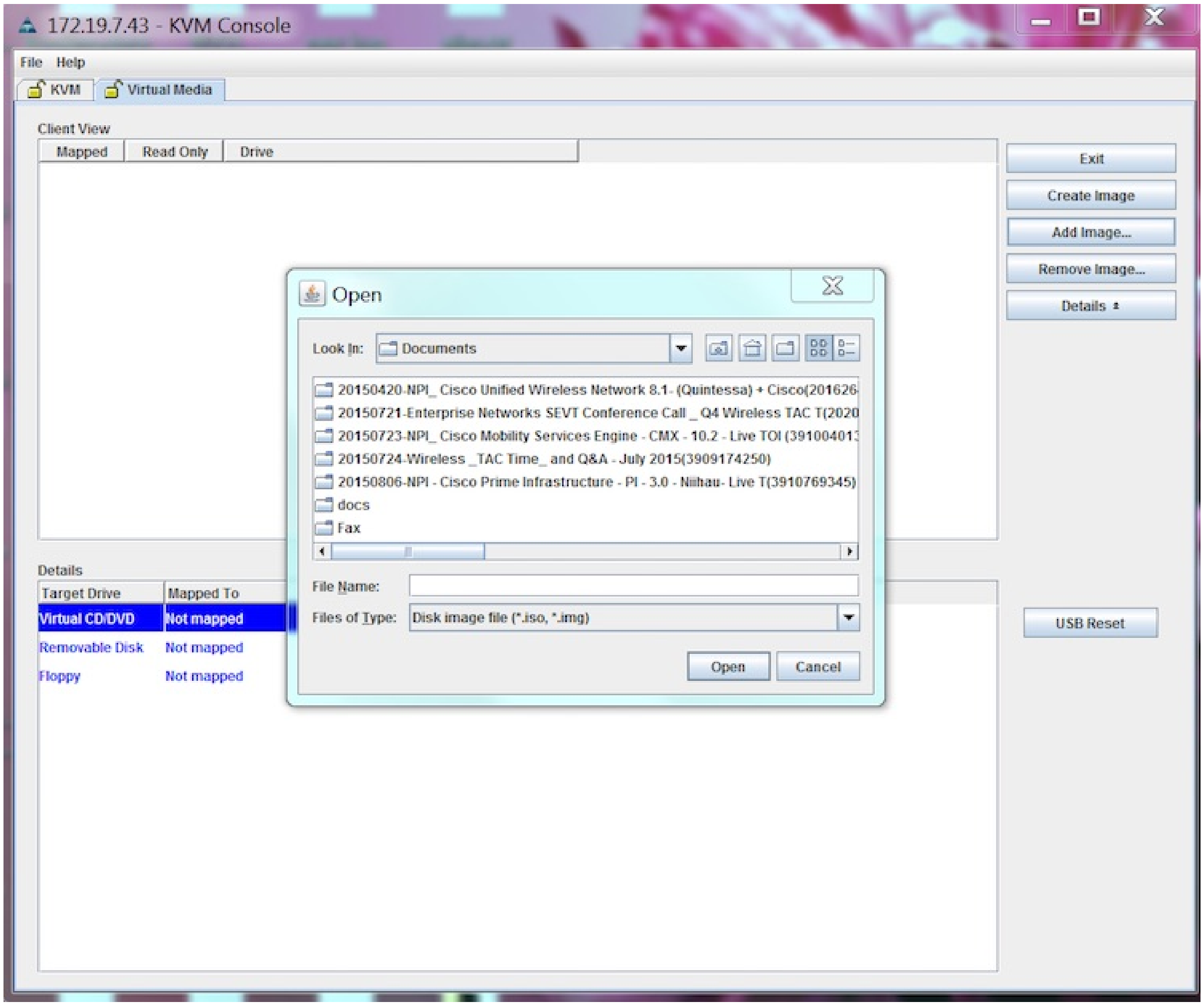
Mapped	Read Only	Drive

Details

Target Drive	Mapped To	Read Bytes	Write Bytes	Duration
Virtual CD/DVD	Not mapped			
Removable Disk	Not mapped			
Floppy	Not mapped			

Step 7 Browse and select the downloaded MSE image and click **Open**.

Figure 40: Select Downloaded Cisco MSE ISO Image



Look In: Documents

- 20150420-NPI_ Cisco Unified Wireless Network 8.1- (Quintessa) + Cisco(201626
- 20150721-Enterprise Networks SEVT Conference Call _ Q4 Wireless TAC T(2020
- 20150723-NPI_ Cisco Mobility Services Engine - CMX - 10.2 - Live TOI (39100401
- 20150724-Wireless _TAC Time_ and Q&A - July 2015(3909174250)
- 20150806-NPI - Cisco Prime Infrastructure - PI - 3.0 - Niihau- Live T(3910769345)
- docs
- Fax

File Name:

Files of Type: Disk image file (*.iso, *.img)

Details

Target Drive	Mapped To
Virtual CD/DVD	Not mapped
Removable Disk	Not mapped
Floppy	Not mapped

The recovery process begins.

Step 8 During the recovery process, respond to the prompt to press ENTER by starting an SSH session to the CIMC interface, as the KVM console does not permit you to press ENTER (With CSCuw32543). Use the following commands to initiate the SSH session:

```
ssh <cimc-ip-address>
connect host
```

The device boots up with the newly loaded image.

What to do next

For more information about configuring Cisco CMX, see Configuring Cisco CMX Release 10.5.x and Later, on page 17.