



Cisco Mobility Services Engine Virtual Appliance Installation Guide for Cisco CMX Release 10.4

First Published: 2017-04-02

Last Modified: 2017-06-27

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 NON-INFRINGEMENT 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Installing Cisco MSE in a VMware Virtual Machine 1

- Virtualization Concepts 2
- Installation Overview 2
- Restrictions for Installing Cisco MSE in a VMware Virtual Machine 3
- Cisco MSE Virtual Appliance Deployment Checklist 3
- Prerequisites for Installing Cisco MSE in a VMware Virtual Machine 3
- Hardware Guidelines 4
- Release Upgrade Compatibility Matrix 4
- VM Alerts 6
- Downloading the Cisco MSE OVA File 7
- Deploying the Cisco MSE OVA File Using the VMware vSphere Client 8
- Installing a Cisco MSE Virtual Appliance 19
- Creating New Virtual Machines Using Hyper-V Manager 26
- Installing Cisco CMX Using Web Interface 27
- Upgrading from Cisco CMX 10.x to 10.4 30
- Verifying Installing Cisco MSE in a VMware Virtual Machine 31

CHAPTER 2

Virtual Machine Setup and Administration 33

- Adding a Hard Disk to a Virtual Machine in the vSphere Client 33
- Configuring the Network 33
- Reconfiguring CPU and RAM for Cisco CMX installation 34

CHAPTER 3

Uploading the Cisco CMX/MSE ISO Image to the Cisco MSE 3365 35

- Uploading the Cisco CMX/MSE ISO Image to the Cisco MSE 3365 Using Newer CIMC Versions 35
- Uploading the Cisco CMX/MSE ISO Image to the Cisco MSE 3365 Using Older CIMC Versions 43



CHAPTER

1

Installing Cisco MSE in a VMware Virtual Machine

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

Cisco MSE 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 MSE 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 MSE 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, page 2](#)
- [Installation Overview, page 2](#)
- [Restrictions for Installing Cisco MSE in a VMware Virtual Machine, page 3](#)
- [Cisco MSE Virtual Appliance Deployment Checklist, page 3](#)
- [Prerequisites for Installing Cisco MSE in a VMware Virtual Machine, page 3](#)
- [Hardware Guidelines, page 4](#)
- [Release Upgrade Compatibility Matrix, page 4](#)
- [VM Alerts, page 6](#)
- [Downloading the Cisco MSE OVA File, page 7](#)

- [Deploying the Cisco MSE OVA File Using the VMware vSphere Client](#), page 8
- [Installing a Cisco MSE Virtual Appliance](#), page 19
- [Creating New Virtual Machines Using Hyper-V Manager](#), page 26
- [Installing Cisco CMX Using Web Interface](#), page 27
- [Upgrading from Cisco CMX 10.x to 10.4](#), page 30
- [Verifying Installing Cisco MSE in a VMware Virtual Machine](#), page 31

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 MSE virtual appliance installation process and contains information about the sections providing details about them:

Table 1: Installation Overview

Step	Task	See
1	Review the deployment checklist and prepare for the installation of a Cisco MSE virtual appliance.	Cisco MSE Virtual Appliance Deployment Checklist , on page 3 and Hardware Guidelines , on page 4
2	Download the Cisco MSE Open Virtualization Archive (OVA) file from Cisco.com.	Downloading the Cisco MSE OVA File , on page 7
3	Deploy the Cisco MSE OVA file.	Deploying the Cisco MSE OVA File Using the VMware vSphere Client , on page 8
4	Configure the basic configurations and install the Cisco MSE virtual appliance.	Installing a Cisco MSE Virtual Appliance , on page 19
5	Set up the Cisco MSE virtual appliance.	Installing Cisco CMX Using Web Interface , on page 27

Restrictions for Installing Cisco MSE 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 and Wireless intrusion prevention system (wIPS) are not available.
- 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.
- Cisco CMX 10.2 does not render any data on Cisco Prime Infrastructure maps. To allow client display in Cisco Prime Infrastructure 1.4 or later, a parallel Cisco MSE 8.0 is also required.

Cisco MSE 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).

Prerequisites for Installing Cisco MSE 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.
- Cisco WLC 7.6, 8.0 or later.
- IP address, type, the SNMP version, and the SNMP write community string of Cisco WLC.
- SNMP credentials of Cisco WLC (private key for V1 and V2, or username and password for V3).
- Mail server settings (port number and security settings) and email address.
- Cisco Prime Infrastructure 2.2, 3.0, or later with a hierarchy of maps in the order of campus, building, and floor.

- Existing exported map file from Cisco Prime Infrastructure.
- VMware virtualization environment ESXi 5.x, 6.0, and 6.5.

Hardware Guidelines

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



Note

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

Table 2: Hardware Guidelines

Hardware Platform	Basic Appliance	Standard Appliance	High-End Appliance
CPU	8 vCPU (2.4 GHz core)	16 vCPU (2.4 GHz core)	24 vCPU (2.4 GHz core)
RAM	24 GB	48 GB	64 GB ¹
HDD	500 GB	500 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.



Note

We recommend you to allocate the required HDD space. For more information, see step 12 in [Deploying the Cisco MSE OVA File Using the VMware vSphere Client](#) section.

Release Upgrade Compatibility Matrix

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

Table 3: Cisco CMX Releases Available on Cisco.com

Cisco CMX Release	OVA	3365 ISO	Upgrade Option Only
10.1.0	cmx-v10-1-0.ova	—	—
10.1.1	—	10.1.1	—
10.1.1-2	—	—	cisco_cmx-10.1.1-2.tar.gz (cisco_cmx-10.1.1-2-x86_64.rpm and cisco_cmx-compat1011-30-x86_64.rpm)

Cisco CMX Release	OVA	3365 ISO	Upgrade Option Only
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	—

Table 4: 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)
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
10.4B	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

Table 5: Upgrade Path by Node Type

Upgrade Path ²	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 to 10.2 and change Location and Connect to Location, Connect, and Analytics.	10.2 backend script to upgrade image to 10.2 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 to 10.2 and change Location and Connect to Location, Connect, and Analytics.	10.2 backend script to upgrade image to 10.2 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 to 10.2 and change Location and Connect to Location, Connect, and Analytics.	10.2 backend script to upgrade image to 10.2 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

² 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 6: VM Alerts

Hard Disk Status	Alert Shown
50 percent	Do Not Back Up
80 percent	System Is About To Run Out Of Space

Hard Disk Status	Alert Shown
85 percent	All The Services Are Stopped

Downloading the Cisco MSE OVA File

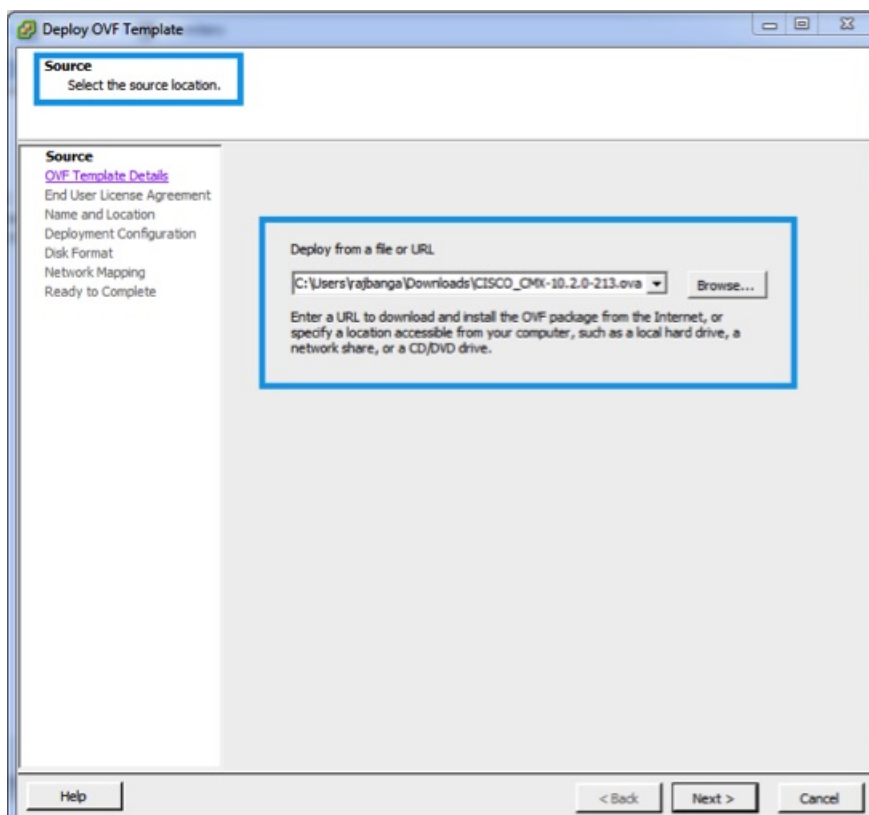
-
- Step 1** Download the Cisco MSE image from [Download Software](#) on cisco.com.
- Step 2** Save the Cisco MSE OVA installer to your computer and ensure that it is accessible.
-

Deploying the Cisco MSE OVA File Using the VMware vSphere Client

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

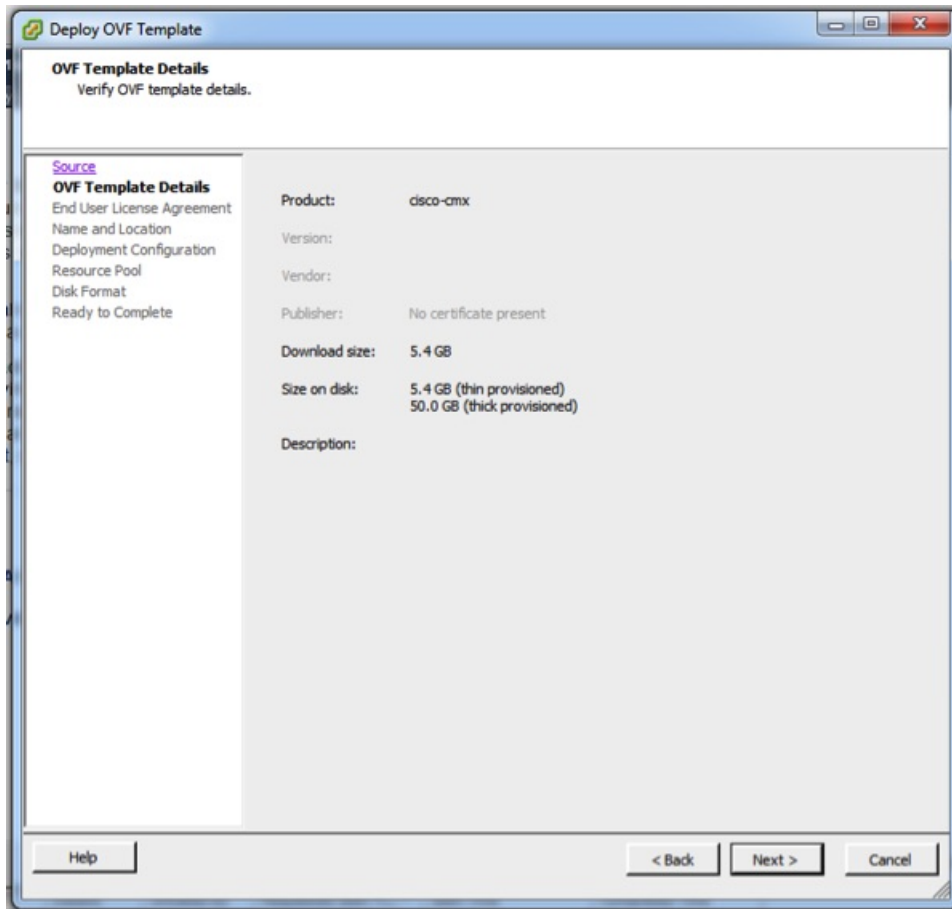
- Step 1** Launch the VMware vSphere client application on your desktop.
- Step 2** From the VMware vSphere Client application menu, choose **File > Deploy OVF Template**.
- Step 3** In the **Deploy OVF Template** window that is displayed, click **Browse** and select the Cisco MSE OVA file that is stored locally on the machine.

Figure 1: Select CMX Image



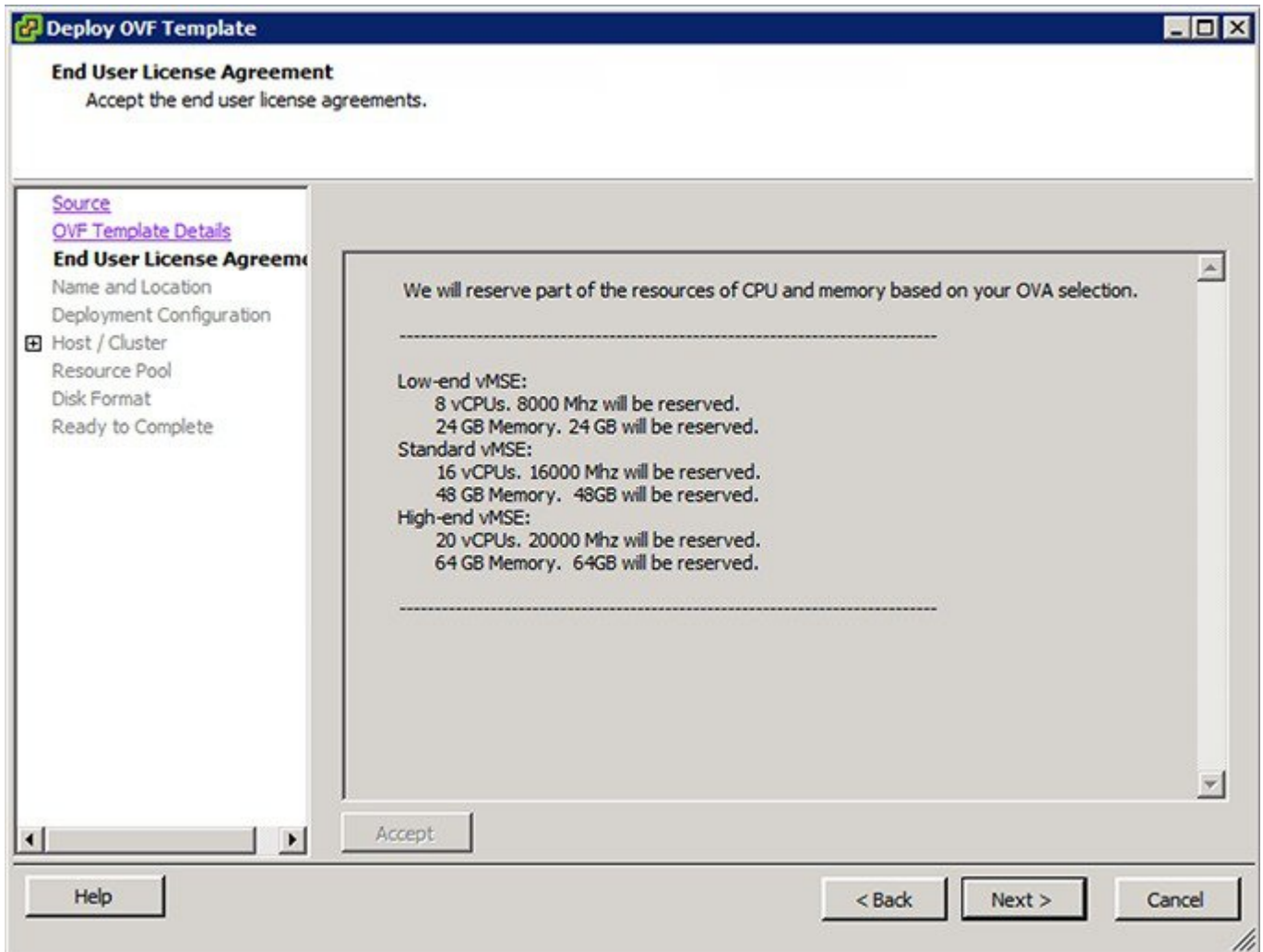
Step 4 Verify the **OVF Template Details** details, and click **Next**.

Figure 2: OVF Template Details



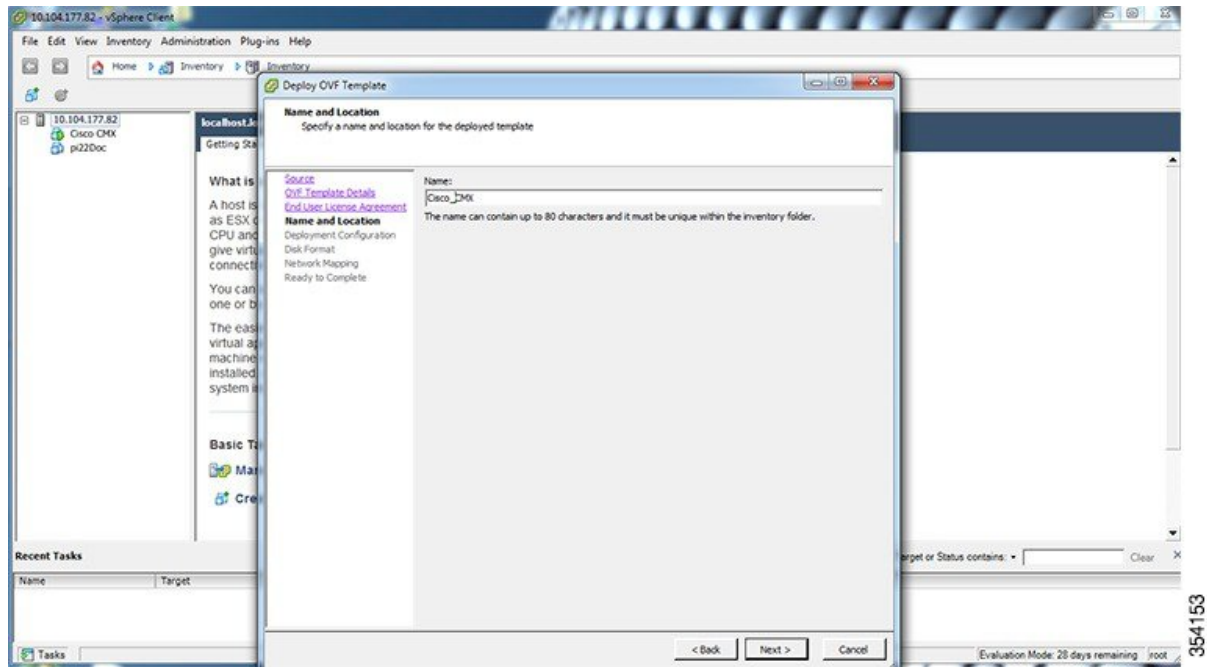
Step 5 Click **Accept** to accept the End User License Agreement and then click **Next**.

Figure 3: End User License Agreement



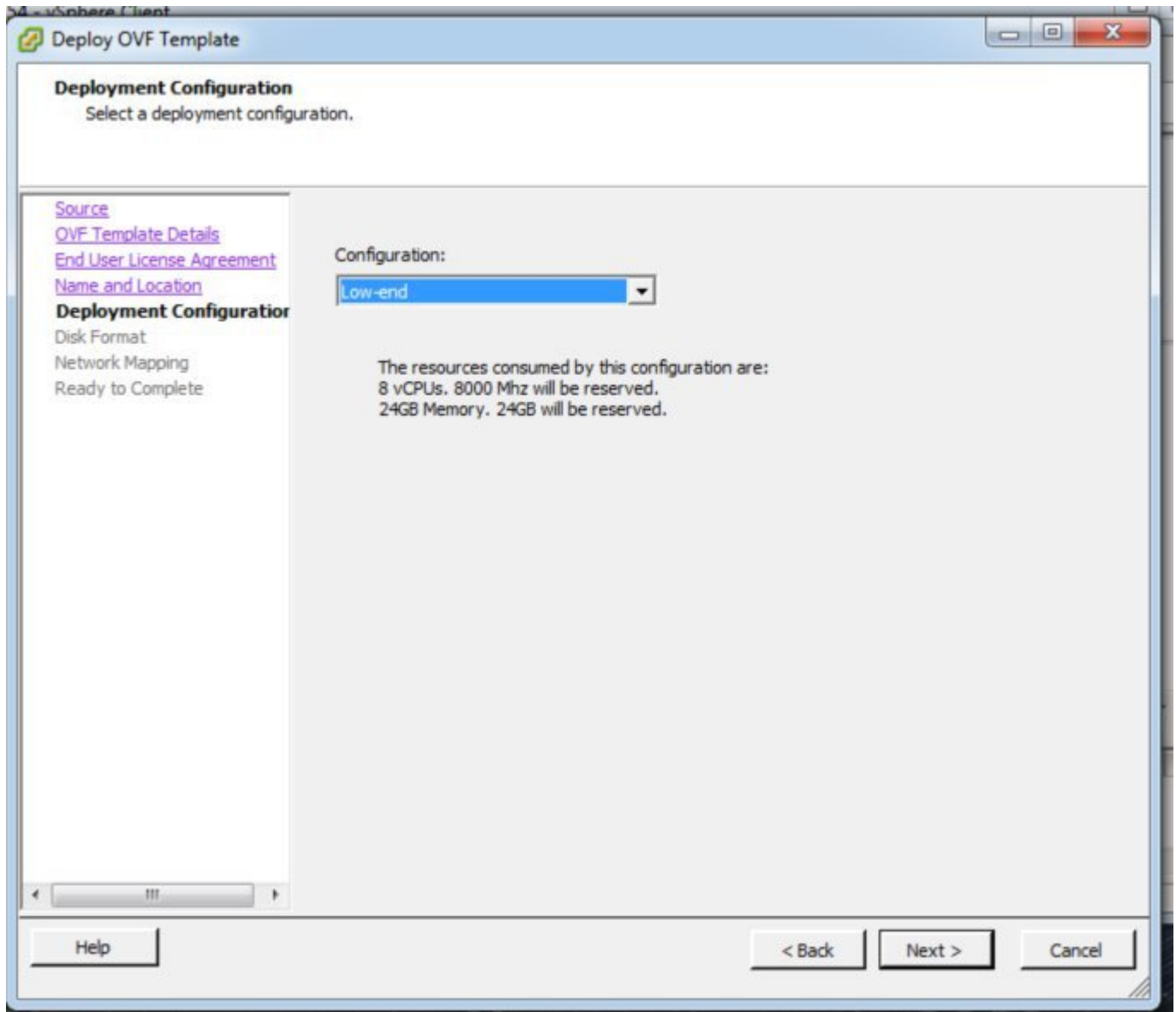
Step 6 Enter a name for the Cisco MSE VM and click **Next**.

Figure 4: Name and Location



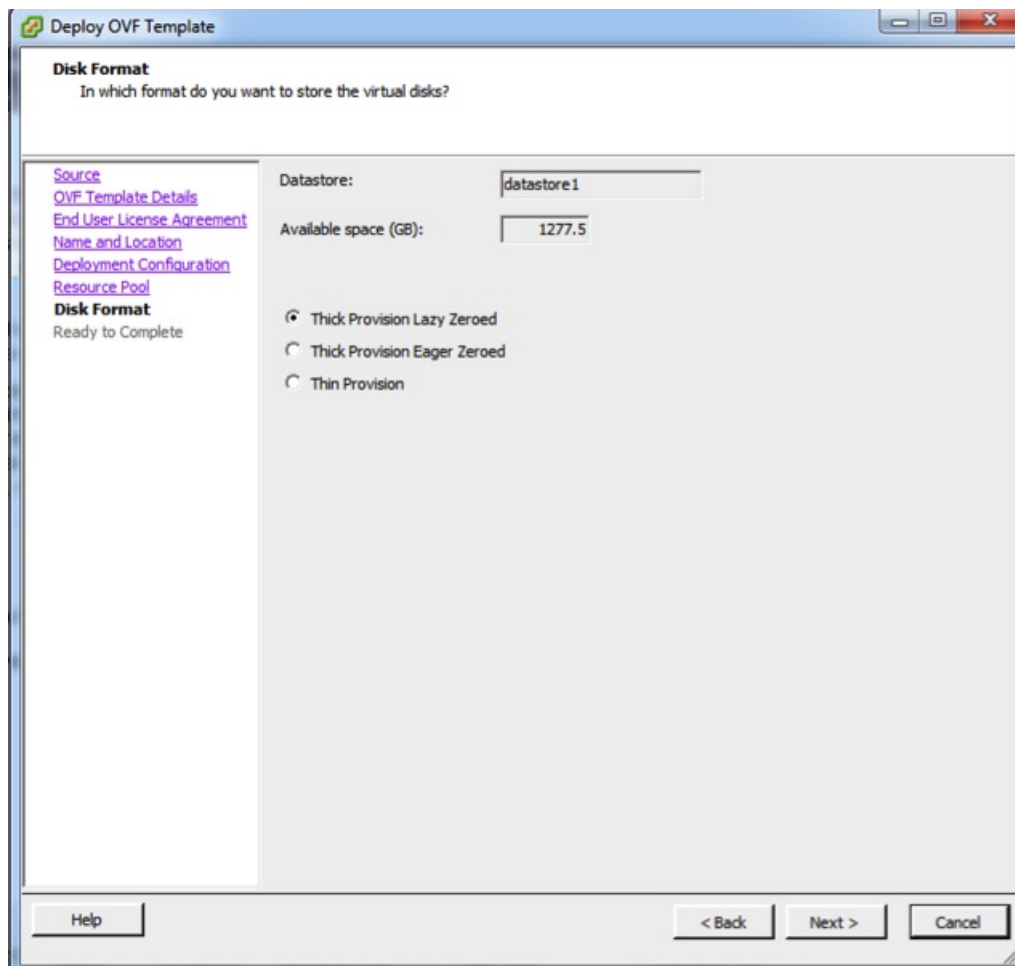
Step 7 From the **Configuration** drop-down list, choose the VM configuration of your choice. The available options are **Low-end**, **Standard**, **High-end**.

Figure 5: Deployment Configuration



Step 8 Check the format in which you want to store the virtual disk.

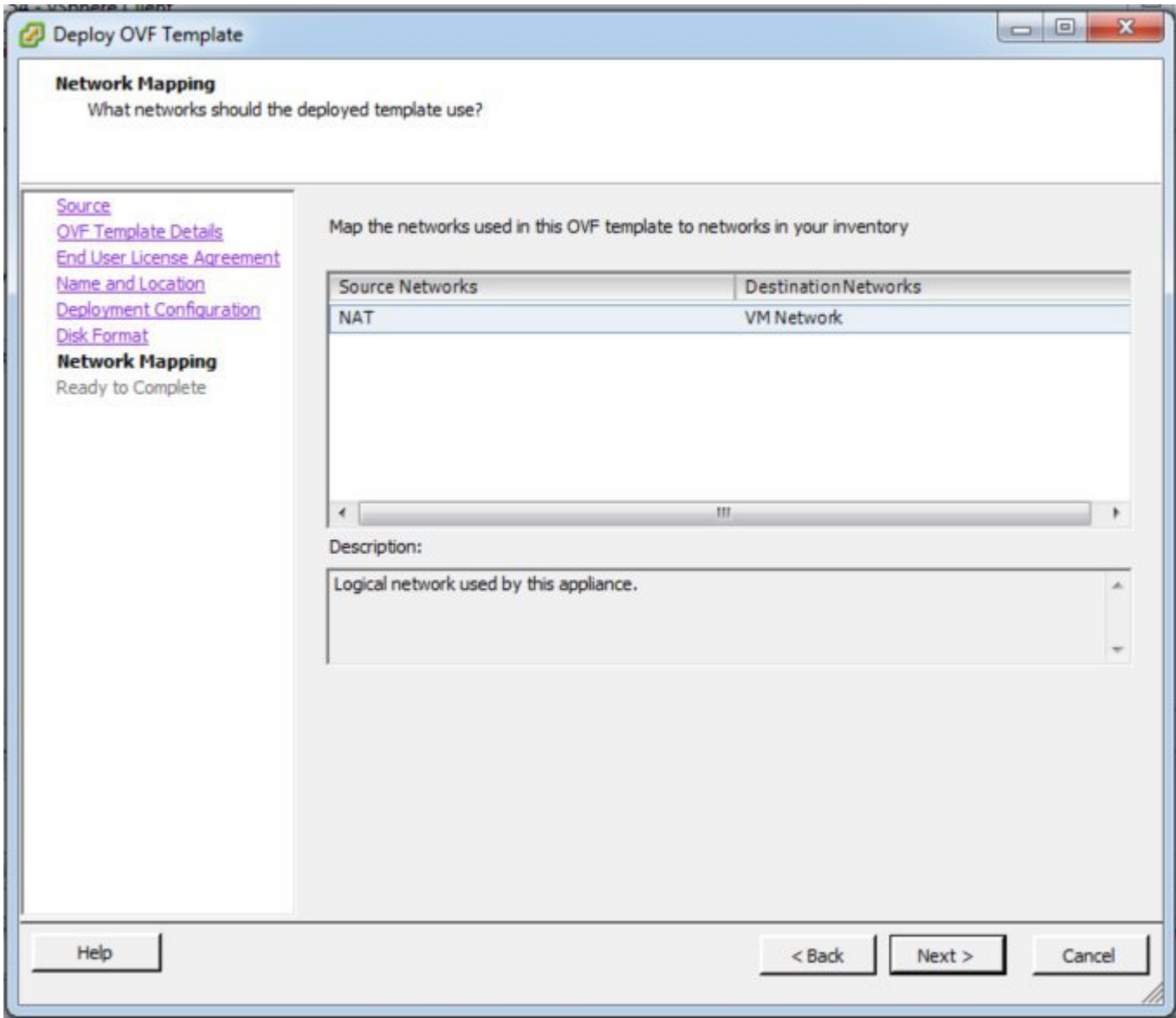
Figure 6: Format



Step 9 Map the networks used in the OVF template to the networks in your directory.

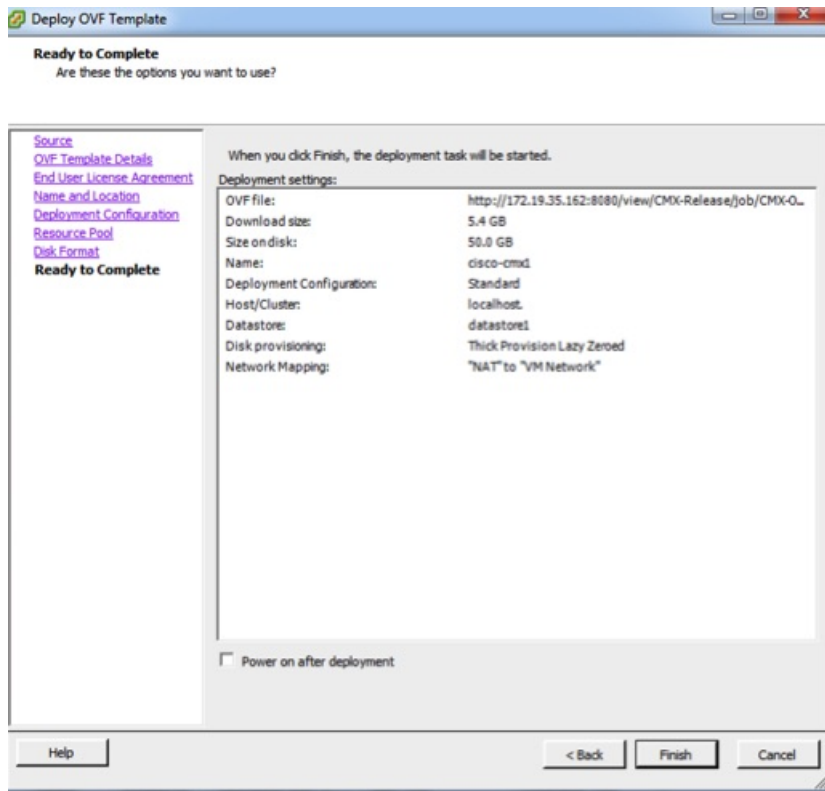
Note With CSCve21967, you cannot deploy the Cisco MSE OVA file with standard and high end VM types with the VMWare ESXi 6.x web client. The web client interface does not show the inventory items drop-down options (low end, standard, and so on) and the option to select VM type is not enabled on the Deployment Options window. However, you can use the VMWare vSphere desktop client from ESXi 5.x to successfully deploy standard and high end VM types to an ESXi 6.x. For more information, see https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2121185.

Figure 7: Network Mapping



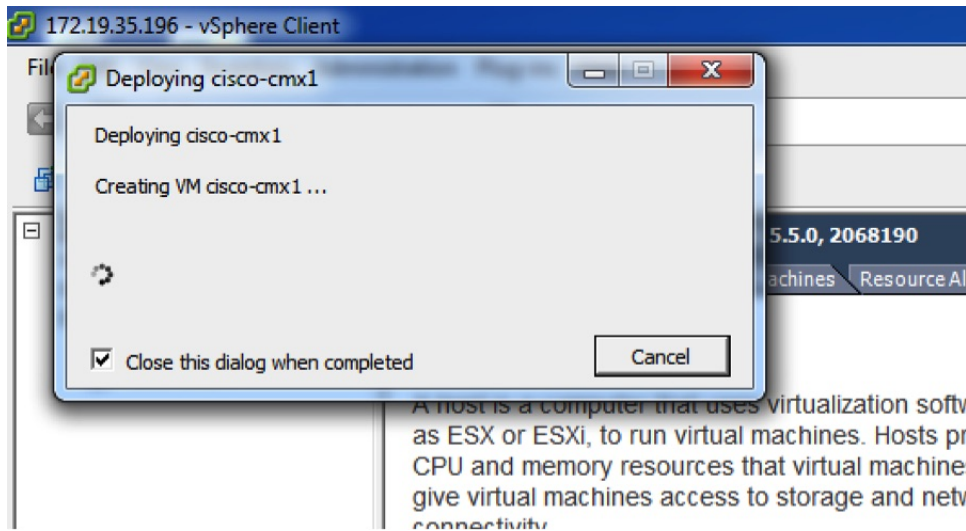
Step 10 Click **Finish**. Ensure that **Power On the Virtual Machine** is not checked.

Figure 8: Complete the Deployment



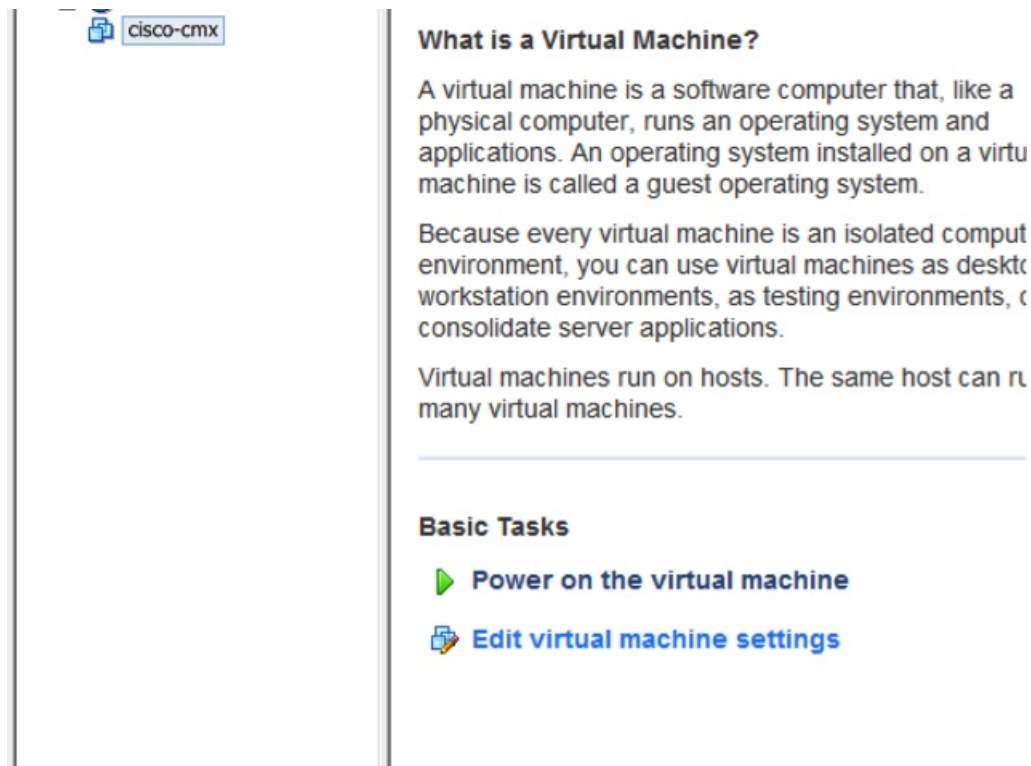
Wait for the deployment to complete. This will take a few minutes.

Figure 9: Deploying the OVA



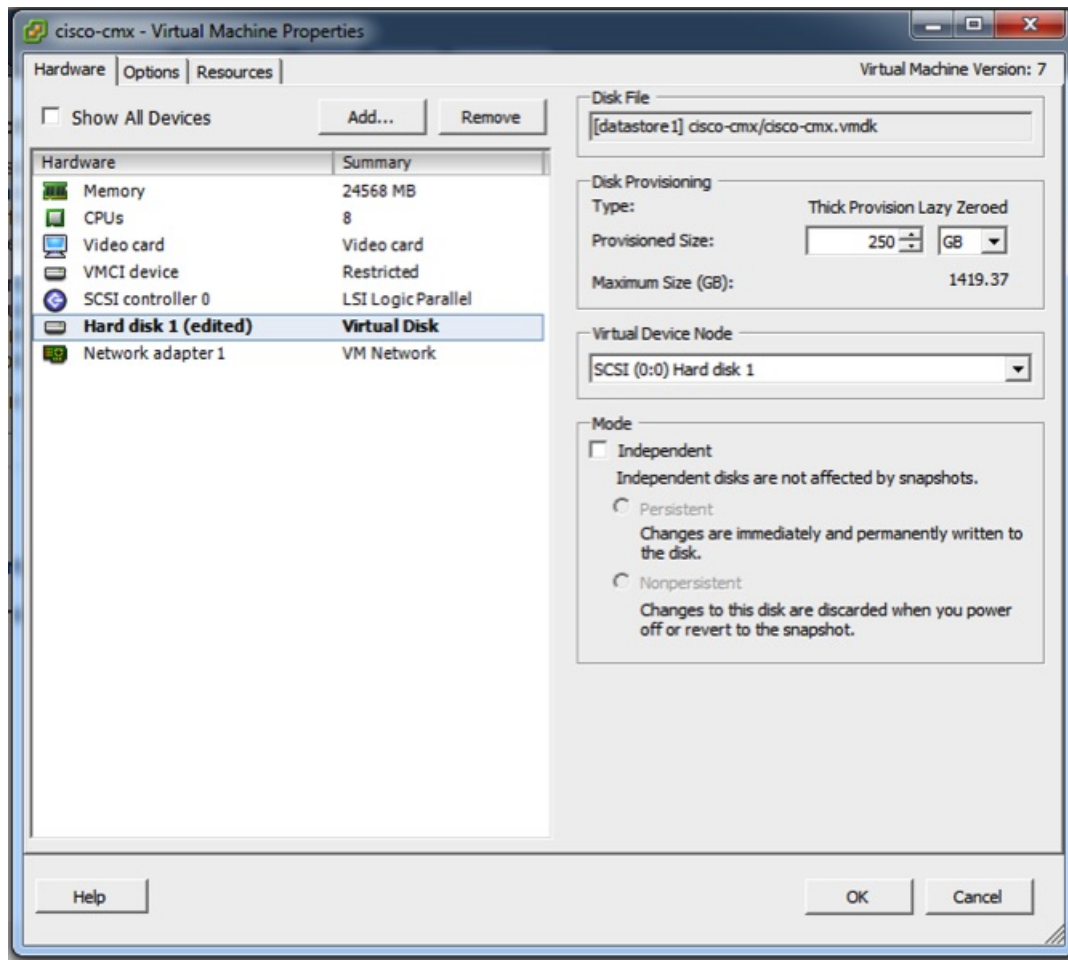
Step 11 Click the deployed VM and choose **Edit Virtual Machine**.

Figure 10: Edit Virtual Machine



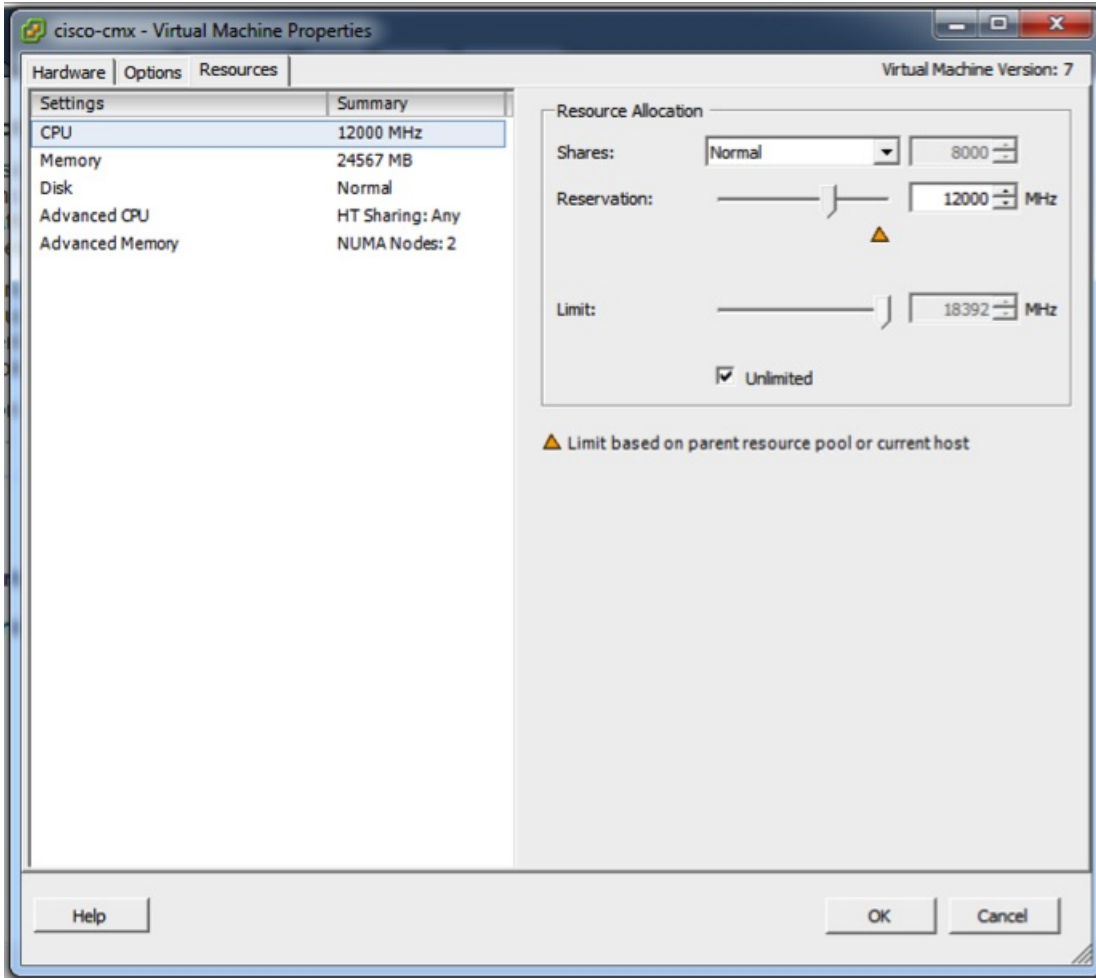
Step 12 (Optional) Click **Hard disk** and modify the **Provisioned Size** as per your requirement and capacity.

Figure 11: Edit Provisioned Size



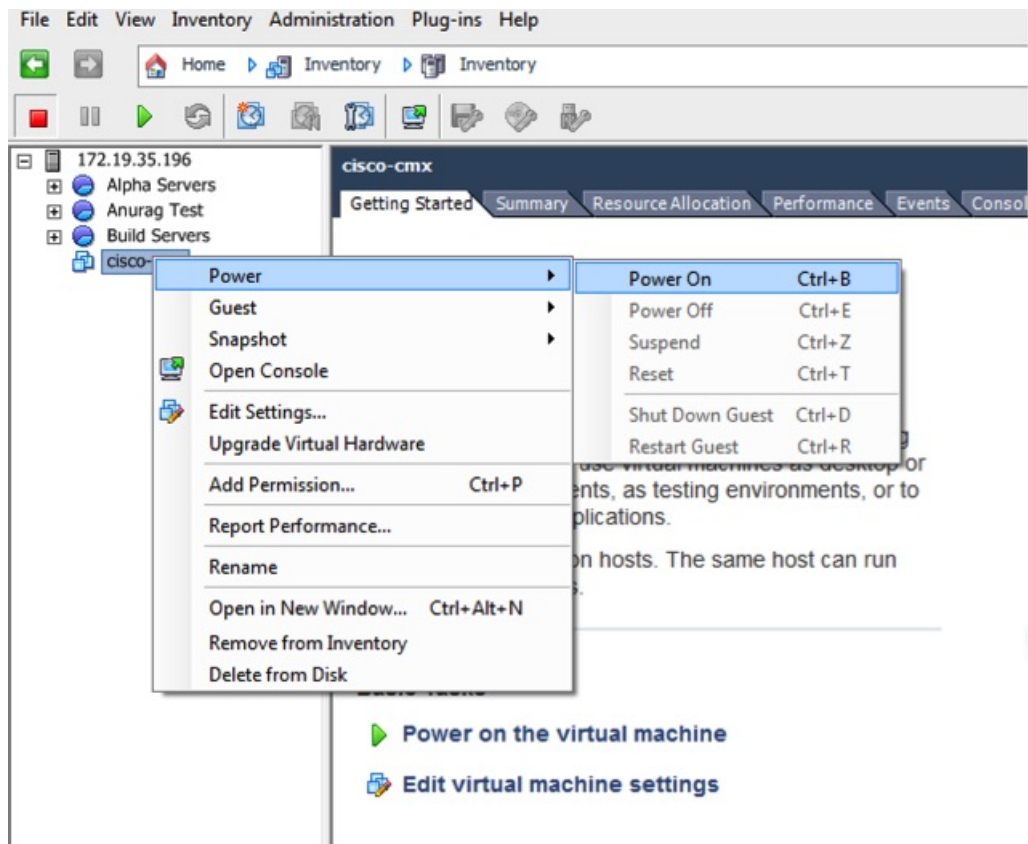
Step 13 (Optional) Click **Resources>CPU** and modify the reservations if your OVA fails to start because of insufficient resources.

Figure 12: Modify CPU Reservations



Step 14 Power ON the VM. The first boot takes a while as the new disk has to be expanded.

Figure 13: Power ON VM



Installing a Cisco MSE Virtual Appliance

After the Cisco MSE is deployed, you can install and configure a Cisco MSE virtual appliance. Note the following points:

- Cisco MSE 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 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 MSE virtual appliance, follow these steps:

Step 1 Right-click the Cisco MSE VM and click **Open Console**.
The console window is displayed with the following information:

```
CentOS release 6.6 (Final)
Kernal 2.6.32-504.el6.x86_64 on an x86_64

localhost login: cmxadmin
password: cisco
Last login: Sun May 15 19:31:03 from 10.0.2.2
```

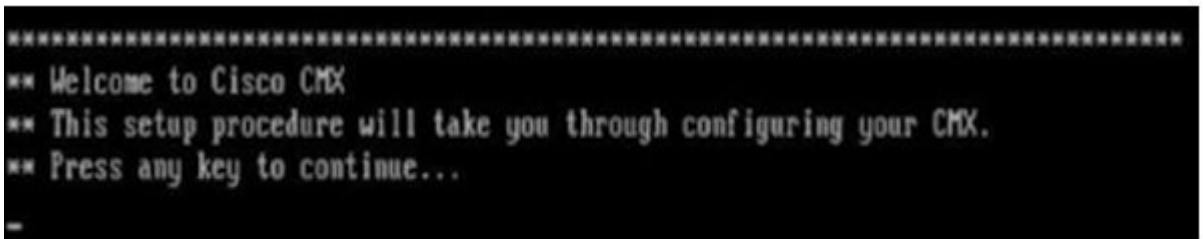
Step 2 Enter the login name and password as prompted.

Figure 14: Console Window



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

Figure 15: Press Enter



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

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

Step 5

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

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

Figure 16: Set Passwords

```
Setting new password for *root*
Password:
Confirm:
Password changed successfully for root

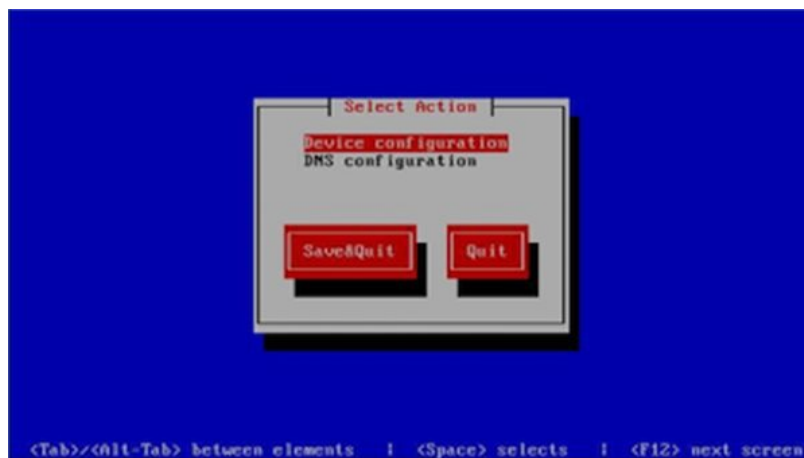
** Password Specification
** Password must have 8 to 28 alphanumeric characters starting with an alpha character
** Password must contain a digit and may also contain digit keys special characters

Setting new password for *cmxadmin*
Password:
Confirm: _
```

Step 6

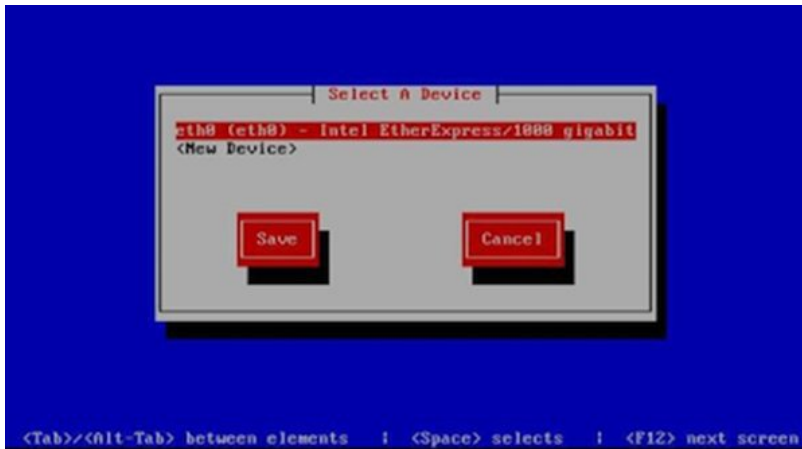
In the Select Action window, click **Device configuration**.

Figure 17: Device Configuration



Step 7 In the **Select A Device** window, click the **eth0** interface.

Figure 18: Select A Device



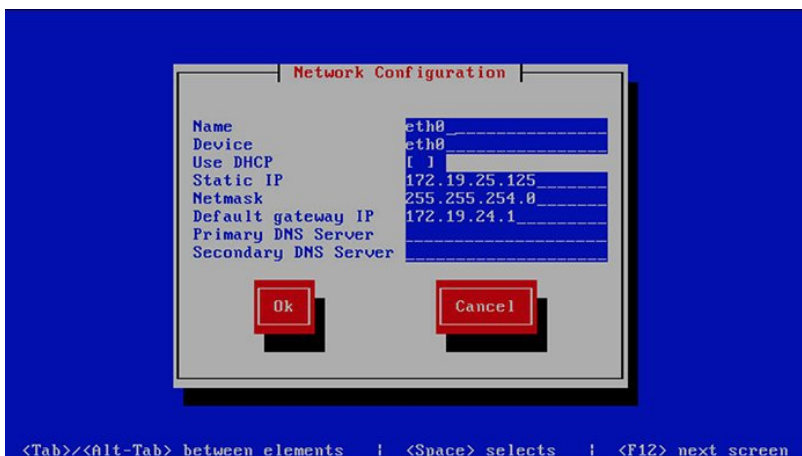
Note With CSCux07068, CMX 10.2 and 10.2.1 installation fails when **New Device** option is selected under device configuration. We recommend that you do not select **New Device** option.

Step 8 In the **Network Configuration** window, toggle the **Use DHCP** field and then enter the Static IP address, Netmask, and Default gateway IP, and click **Ok**.

Note

- To set the hostname, see the **Hostname** field in Step 10. Changing the hostname through the CLI is not supported. After the initial setup, to change the hostname, use the **cmxos reconfigure** command to display the **Network Configuration** and **DNS Configuration** windows again.
- Do not change the **Device** field as this is automatically detected.
- Do not enter DNS details because the information entered here is not used by the system. These details can be entered in the DNS configuration step (Step 10) that follows.

Figure 19: Network Configuration



Note Do not change the name of the interface. The default interface **Name** is `eth0` and it should not be changed.

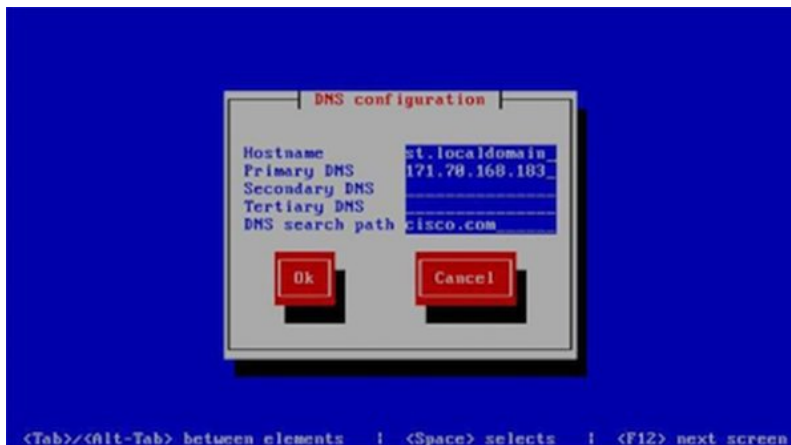
Step 9 In the **Select Action** window, click **DNS Configuration**.

Figure 20: Select DNS Configuration



Step 10 In the **DNS configuration** window, enter the **Hostname**, **DNS**, and **DNS search path** default domain.

Figure 21: DNS Configuration



Step 11 In the **Select Action** window, click **Save&Quit**.

Figure 22: Select Action



Step 12 (Recommended) Enter the NTP server name or the IP address of the NTP server when prompted.

Note

- After installation, changing the NTP information through the CLI or GUI is not supported. To change the NTP information, use the **cmxos reconfigure** command from the CMX CLI to change the NTP information. Given below is a workaround.

```
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
```

Figure 23: Configuring NTP

```

*****
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.
#? _

```

Step 13 Configure the time zone and save the changes.

Figure 24: Configuring Time Zone

```

*****
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.
#? _

```

Step 14 Access the URL when prompted.

Figure 25: Access URL

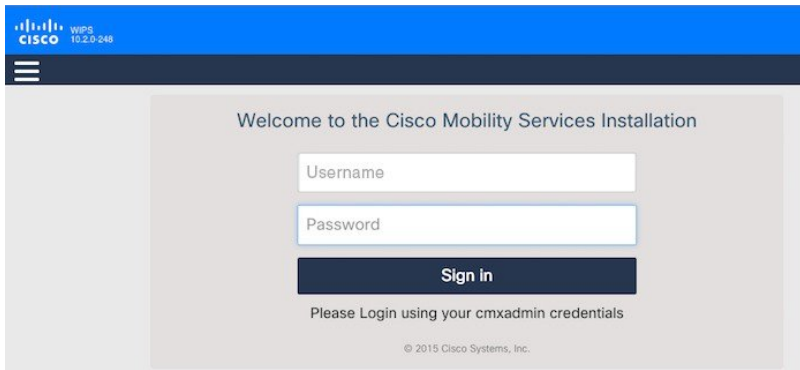
```

*****
CMX OS Configuration is complete.
Please visit below url to continue CMX configuration
*****
https://localhost.localdomain:1984
[cmxadmin@localhost ~]$ _

```

- Step 15** Open the URL `http://<ip-address>:1984` when prompted in the browser. The Cisco Mobility Services Installation sign in page is displayed.

Figure 26: Welcome Menu



- Step 16** In the Cisco Mobility Services Installation sign in page, enter your cmxadmin credentials and proceed with the installation.
- Note** Use steps 15-16 while installing a new MSE virtual appliance.

Creating New Virtual Machines Using Hyper-V Manager

You can now run Cisco CMX on Microsoft Hyper-V virtualization hosts. This enables you to use Cisco CMX on virtual machines using any Hyper-V capable host running Windows Server 2008 R2 or later.

You can create a new virtual machine using Hyper-V Manager application. Ensure to specify 24 GB of memory or higher when creating the virtual machine in Hyper-V manager, and to subsequently increase the processor count for the virtual machine to 8 vCPU or higher before starting the new virtual machine.

If you are running Windows Server 2012 or later, we recommend you to convert the Cisco CMX .vhd disk image to .vhdx format before adding it to the new virtual machine.

To create a new virtual machine:

- Step 1** Download the CMX .vhd file to the location on the drive where it will reside.
- Step 2** (Optional) Convert the .vhd file to .vhdx format.
- Step 3** Open the Hyper-V Manager application and verify the Hyper-V virtual network switch configuration.
- Note** To configure a Hyper-V virtual network switch, click **Virtual Switch Manager** at the right side of the Hyper-V Manager window.

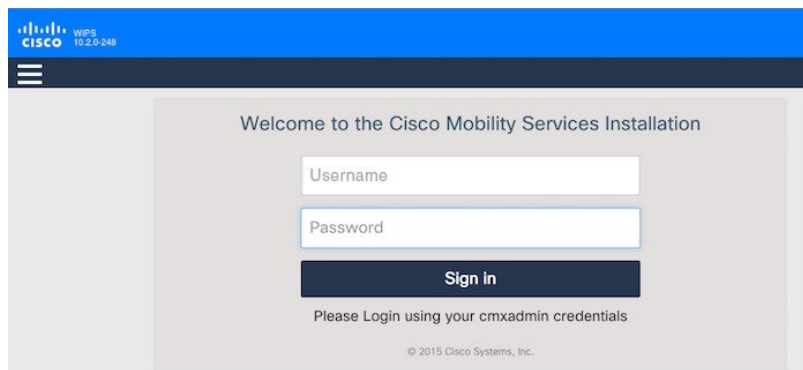
- Step 4** To create a new VM, choose **Action > New > Virtual Machine**.
- Step 5** Enter a name for the new virtual machine.
- Step 6** Select to store the virtual machine in a different location, browse to the folder containing the .vhd or converted .vhdx file, and then click **Next**.
- Step 7** Choose **Generation 1** as the machine type, and then click **Next**.
Note Only certain Windows guests support Generation 2.
- Step 8** Specify 8192 or greater for the VM memory, and then click **Next**.
Note Do not enable Dynamic Memory.
- Step 9** Under **Connections**, choose the appropriate virtual network switch to connect the VM, and then click **Next**.
- Step 10** Select **Use an existing hard disk**, and then navigate to the .vhd or .vhdx file on your hard disk.
- Step 11** In the **Summary** window, click **Finish**.
- Step 12** Edit the new VM settings and change the processor count to a minimum of 4.
-

Installing Cisco CMX Using Web Interface

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

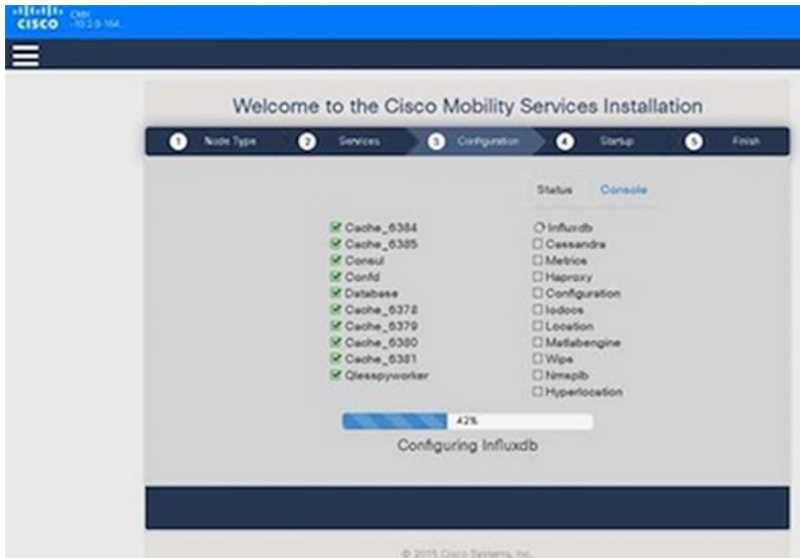
- Step 1** In the Cisco CMX web interface, enter the login credentials for a Cisco CMX administrator and click **Sign in** to continue. The login username is **cmxadmin**. Use the password that was configured when the system was started for the first time.

Figure 27: Welcome Window



- 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.



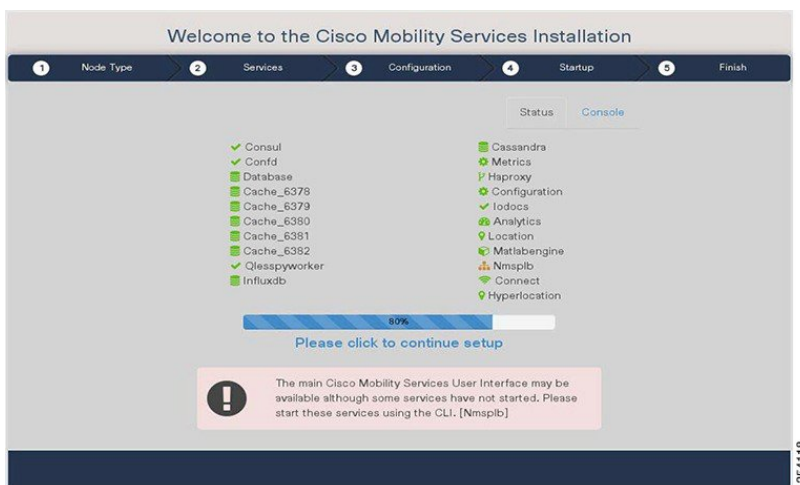
The sequence of events is as follows:

- 1 Consul Configuration
- 2 DB Installation
- 3 Schema Migration
- 4 InfluxDB Configuration
- 5 Cassandra Installation
- 6 Node Registration

Step 3

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

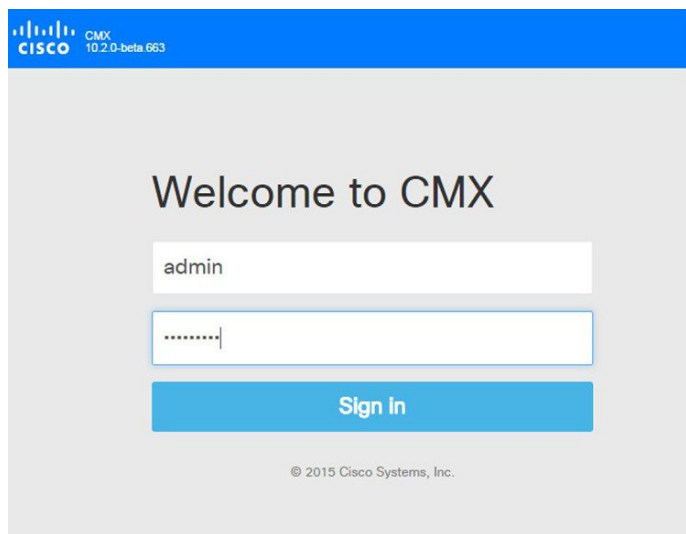
Note You can monitor the progress of the installation either through the graphical status display or the console output. Note that this console is for display only.



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 28: Welcome Screen

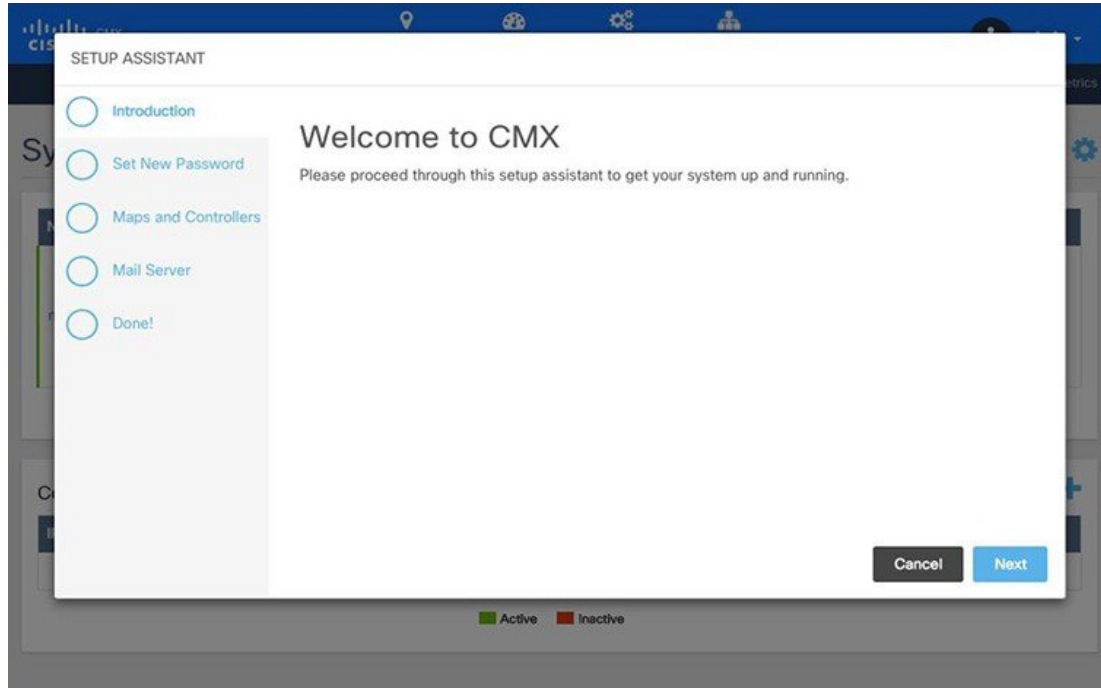


What to Do Next

A **Setup Assistant** window is displayed, from where you can complete the initial configuration. You must now set a password for the admin user, 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.

Figure 29: Setup Assistant



Upgrading from Cisco CMX 10.x to 10.4

There are three options to upgrade from Cisco CMX 10.x to Cisco CMX 10.4:

- Option 1—Copy the Cisco CMX image into the Cisco CMX node, and then use the **cmxos upgrade** `<cmx-file>` command from the command line to perform the upgrade.
- Option 2—Use the web installer on port 1984, and choose **Remote File** to download the Cisco CMX image from a hosted site, for example, the Cisco CMX image may be available in an internal web server for download.
- Option 3—Use the web installer on port 1984, and choose **Local File** to upload the Cisco CMX image from your local machine through the web browser.



Note

We recommend either option 1 or 2.

Upload of the Cisco CMX image might fail if you use option 3. This is due to a memory leak with a third-party library used in the installer. However, this library will be fixed in subsequent versions of the installer. If you chose option 3 and the upload fails, restart the installer program by using the **cmxos adminui stop** command and then the **cmxos adminui start** command. Option 3 might succeed after several tries.

Verifying Installing Cisco MSE in a VMware Virtual Machine

You can verify the overall system health and status of the Cisco MSE services using the **System** tab in the Cisco MSE user interface. Ensure that all the services, memory, and CPU indicate a healthy status (green) for each Cisco MSE and Cisco CMX node, and that there is at least one 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 detect patterns of various criteria, such as Client Count, CPU Usage, Memory Usage, and so on..
- **Metrics**—Enables you to view system metrics.



Virtual Machine Setup and Administration

This chapter contains the following sections:

- [Adding a Hard Disk to a Virtual Machine in the vSphere Client, page 33](#)
- [Configuring the Network, page 33](#)
- [Reconfiguring CPU and RAM for Cisco CMX installation, page 34](#)

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 **shutdown -h now** 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.
-



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



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 the Cisco CMX/MSE ISO Image to the Cisco MSE 3365 Using Newer CIMC Versions, page 35](#)
- [Uploading the Cisco CMX/MSE ISO Image to the Cisco MSE 3365 Using Older CIMC Versions, page 43](#)

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.

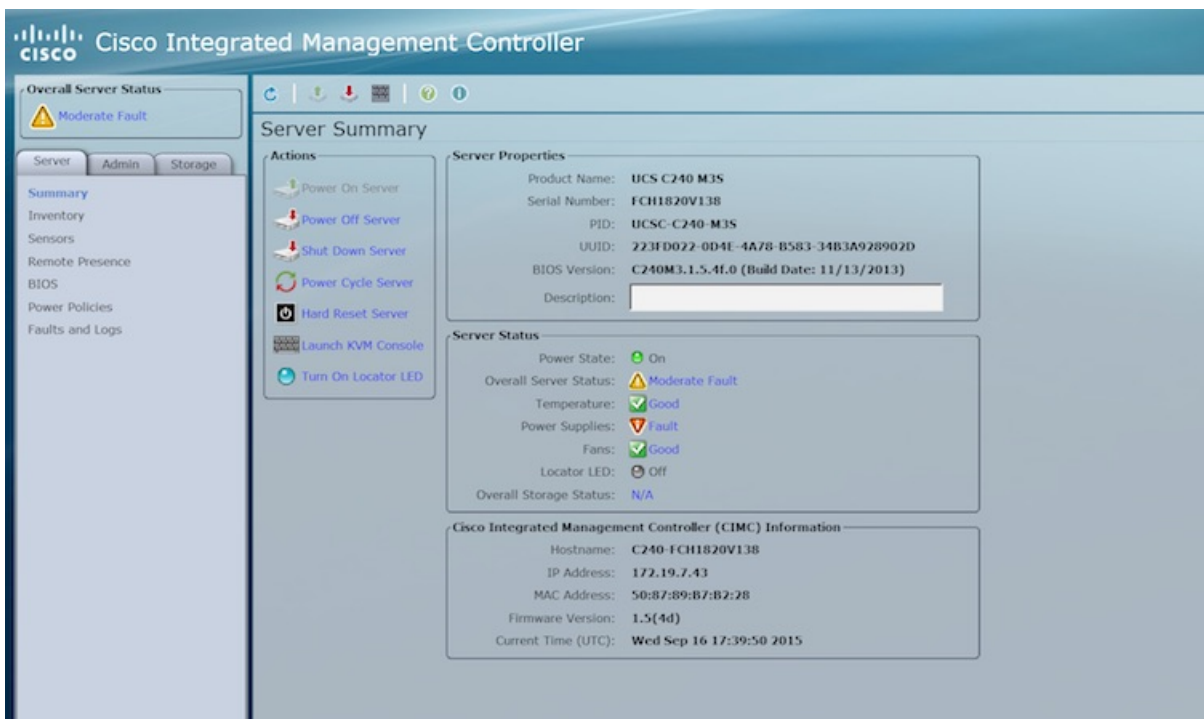
Before You Begin

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 the Cisco Integrated Management Controller (CIMC) GUI interface (Address format is https://x.x.x.x).

Figure 30: Cisco Integrated Management Controller Interface



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

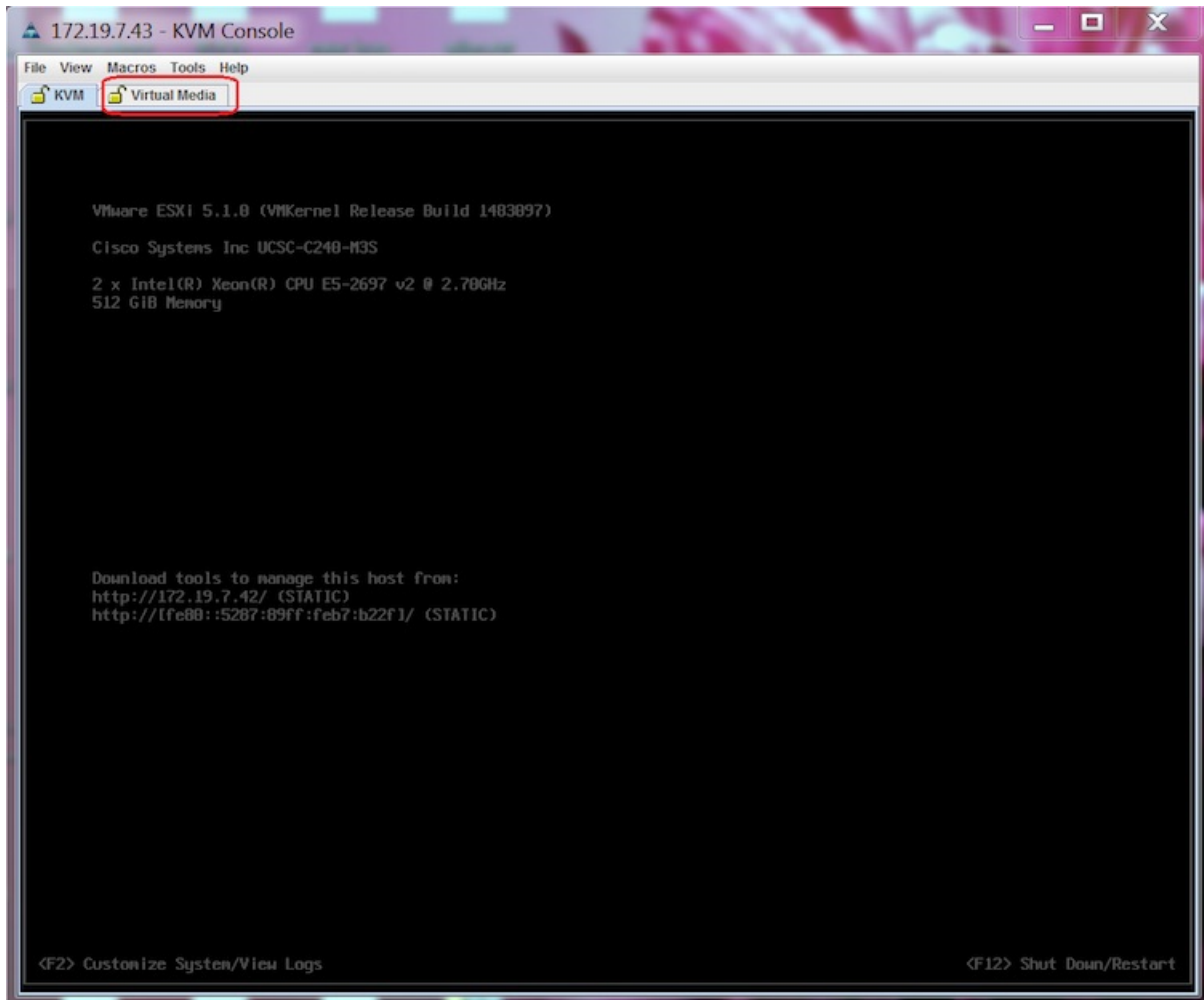
Step 4 Open the file using javaws.exe from the bin folder of your Java installation. If a security error prevents you from installing the file, add the URL of the CIMC to the list of exception sites, using the steps below.

- 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.

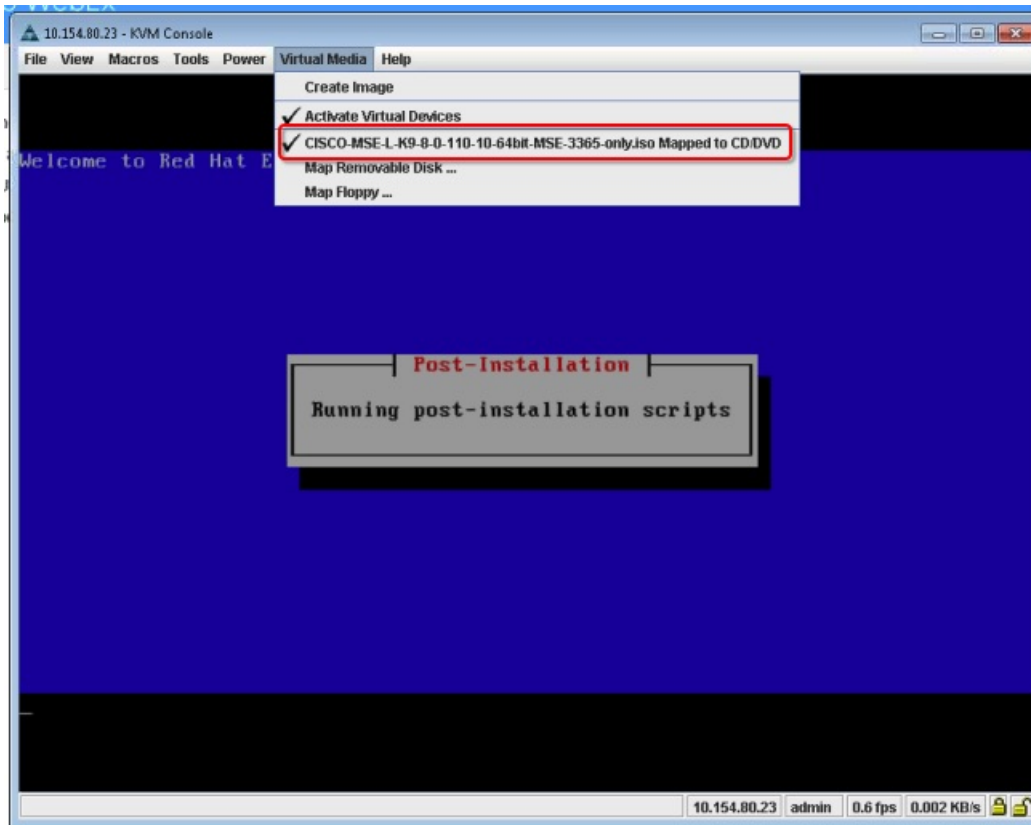
Step 5 In the KVM Console window that is displayed after the installation, click the **Virtual Media** tab.

Figure 31: KVM Console



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 32: ISO Image Selected



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 33: Copying from CDROM

```

10.154.80.23 - PuTTY
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 34: Copying Database Files from CDROM

```

10.154.80.23 - PuTTY
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-R9
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 35: 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...
-----

[-----]-----]-----]-----]-----]
[-----]-----]-----]-----]

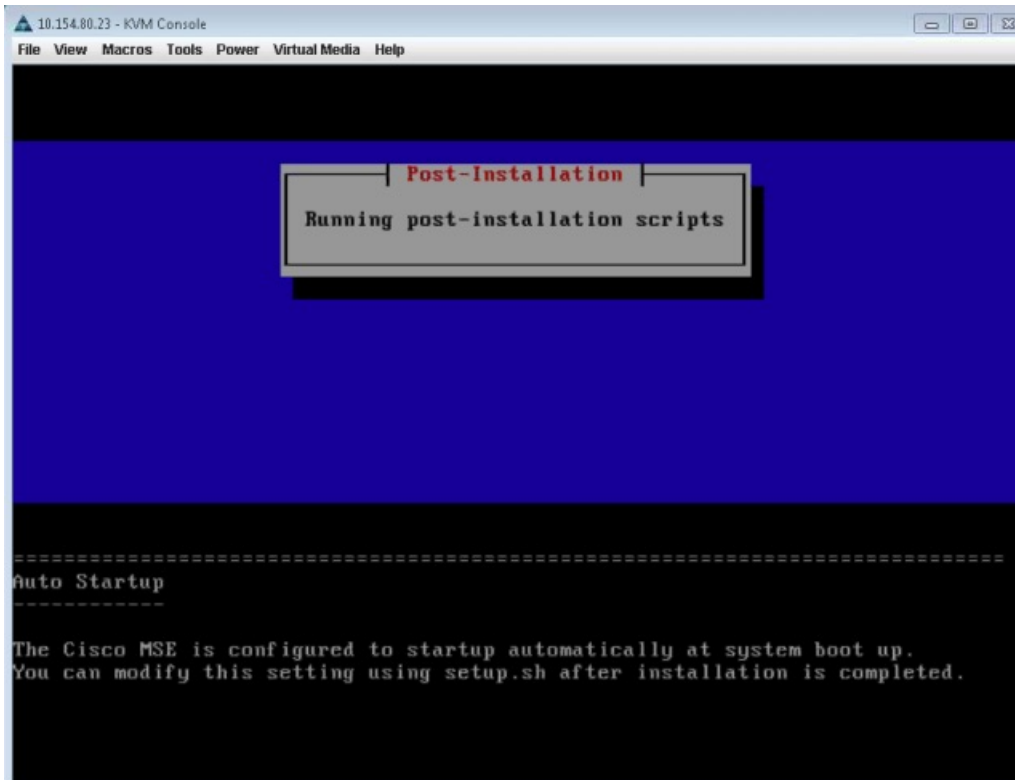
=====
Database Installation
-----

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

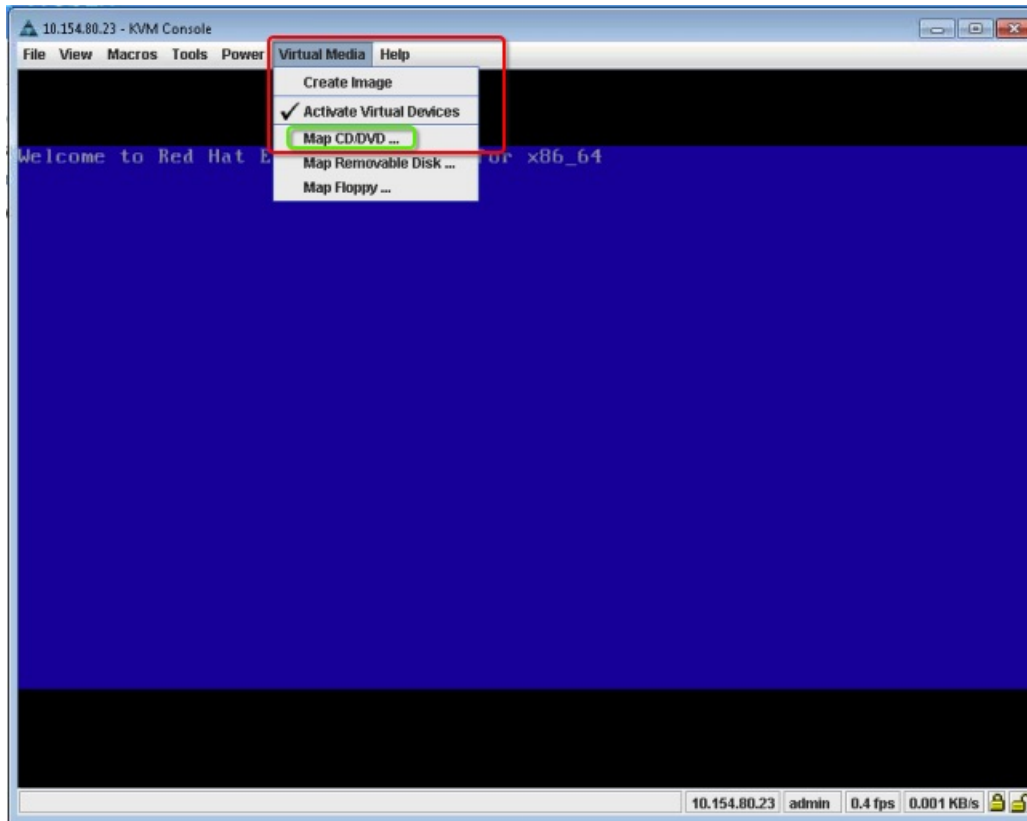
Step 1/3 - Installing Database files
[-----] [ ] 25% █
    
```

Figure 36: Running Post-Installation Scripts



- 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 37: Map CD/DVD



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.

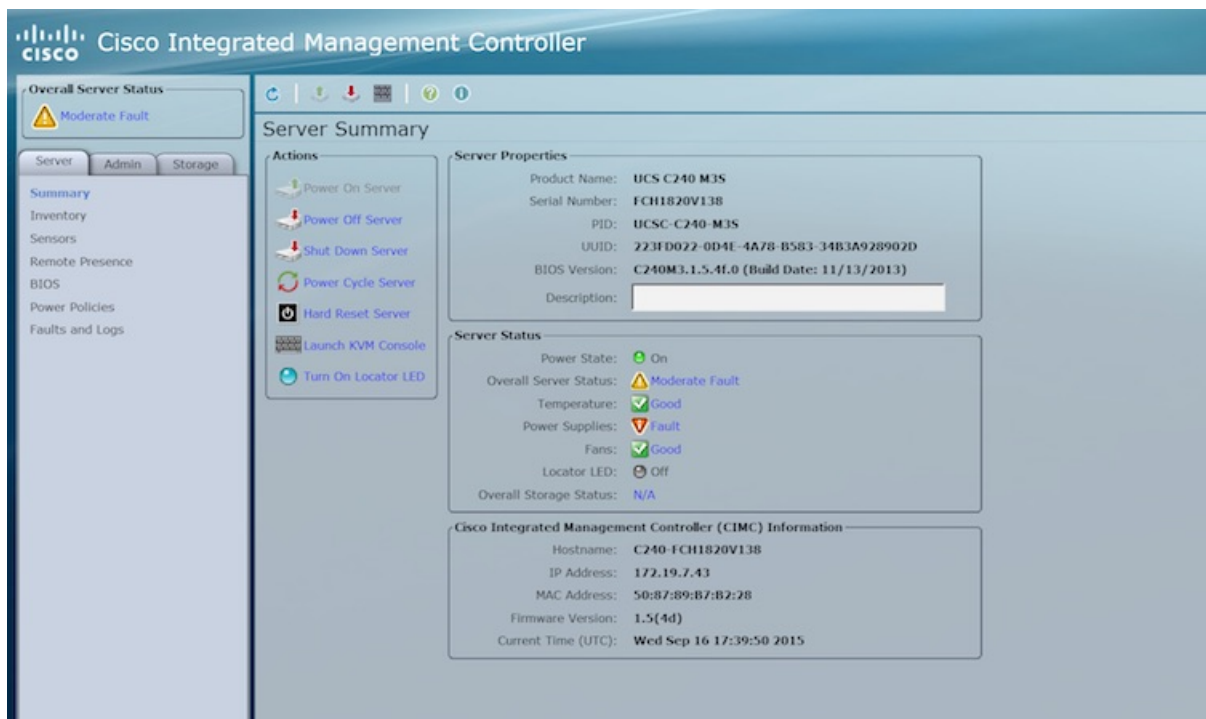
Before You Begin

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 the Cisco Integrated Management Controller (CIMC) GUI interface (Address format is https://x.x.x.x).

Figure 38: Cisco Integrated Management Controller Interface



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

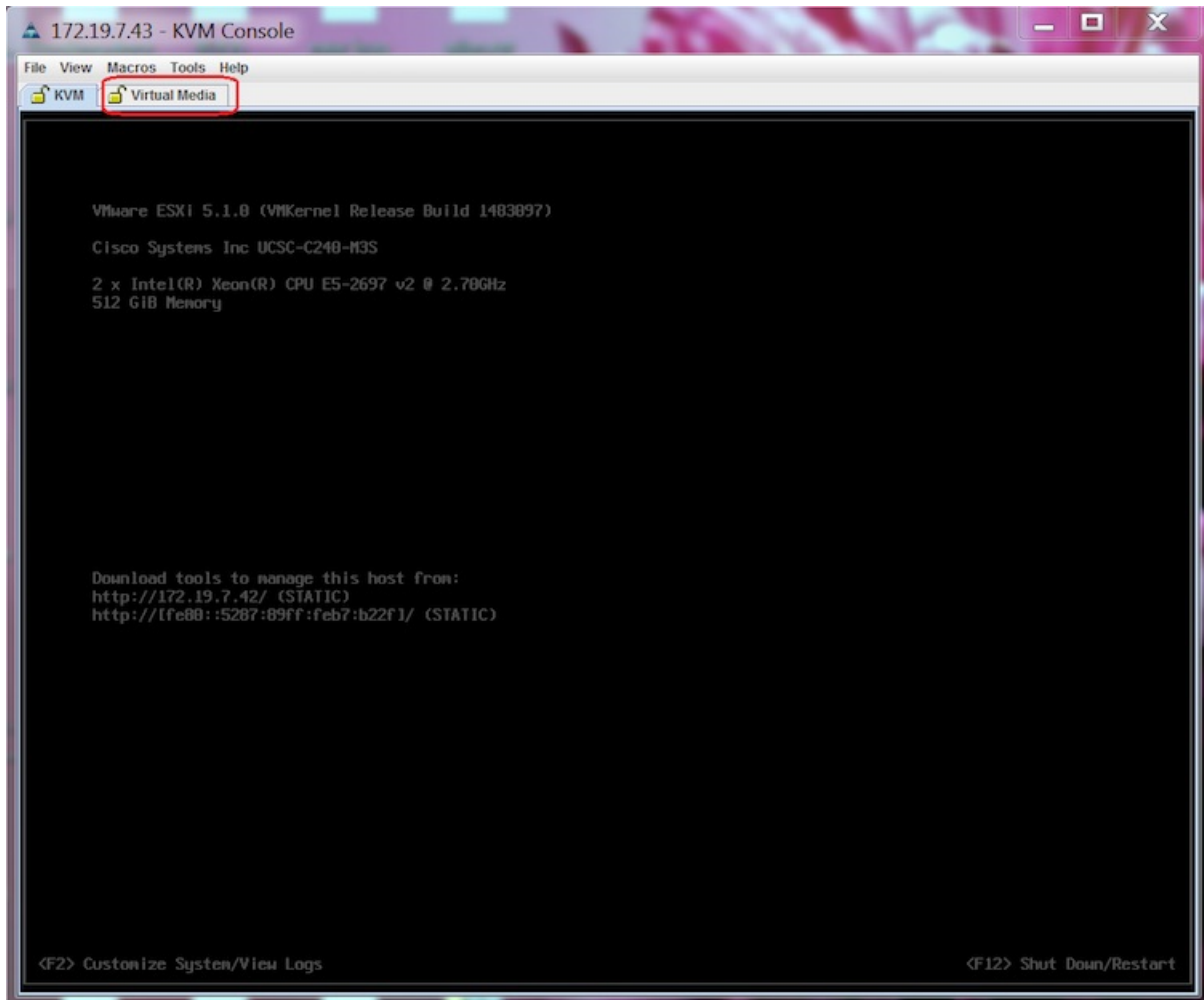
Step 4 Open the file using javaws.exe from the bin folder of your Java installation. If a security error prevents you from installing the file, add the URL of the CIMC to the list of exception sites, using the steps below.

- 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.

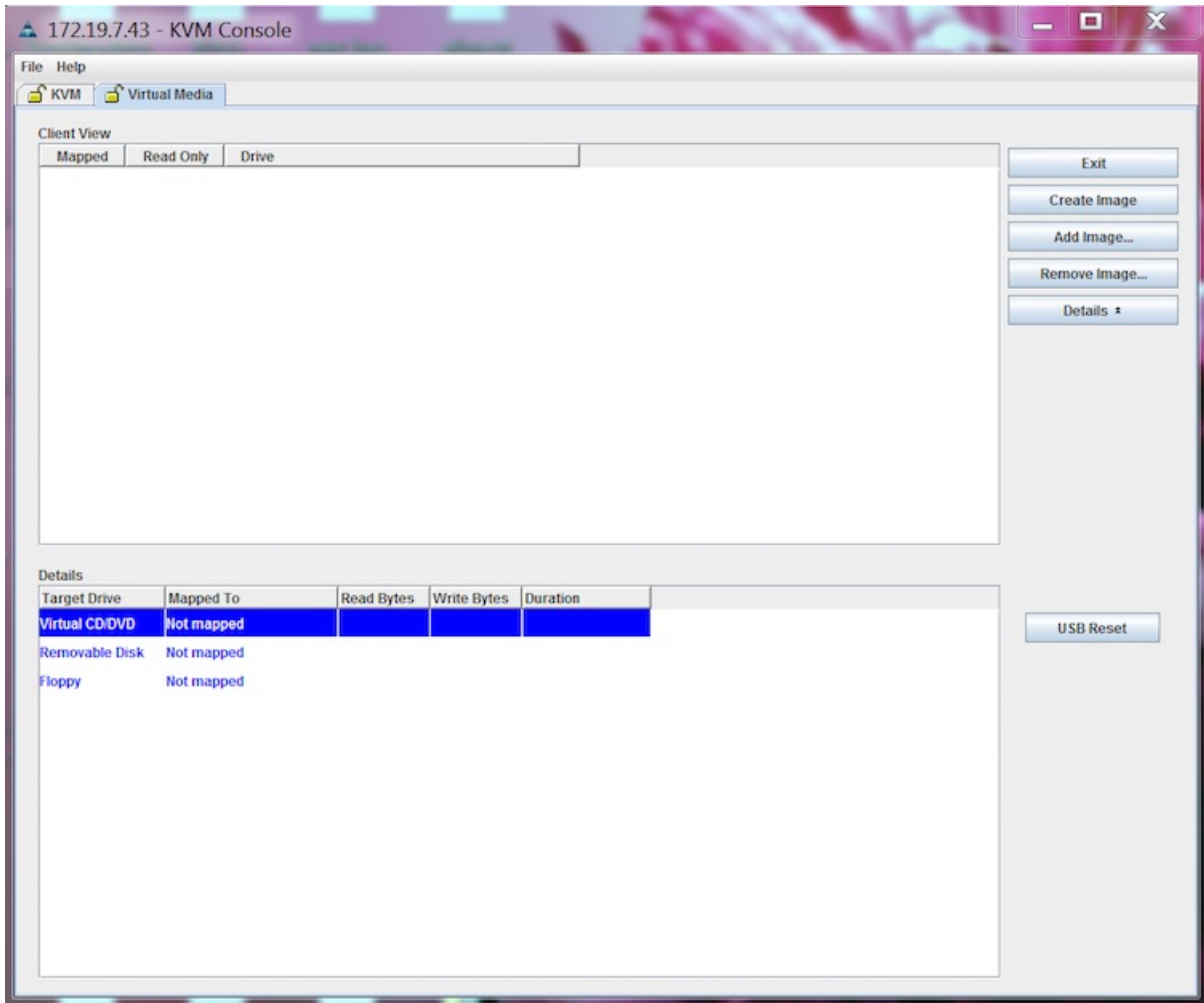
Step 5 In the KVM Console window that is displayed after the installation, click the **Virtual Media** tab.

Figure 39: KVM Console



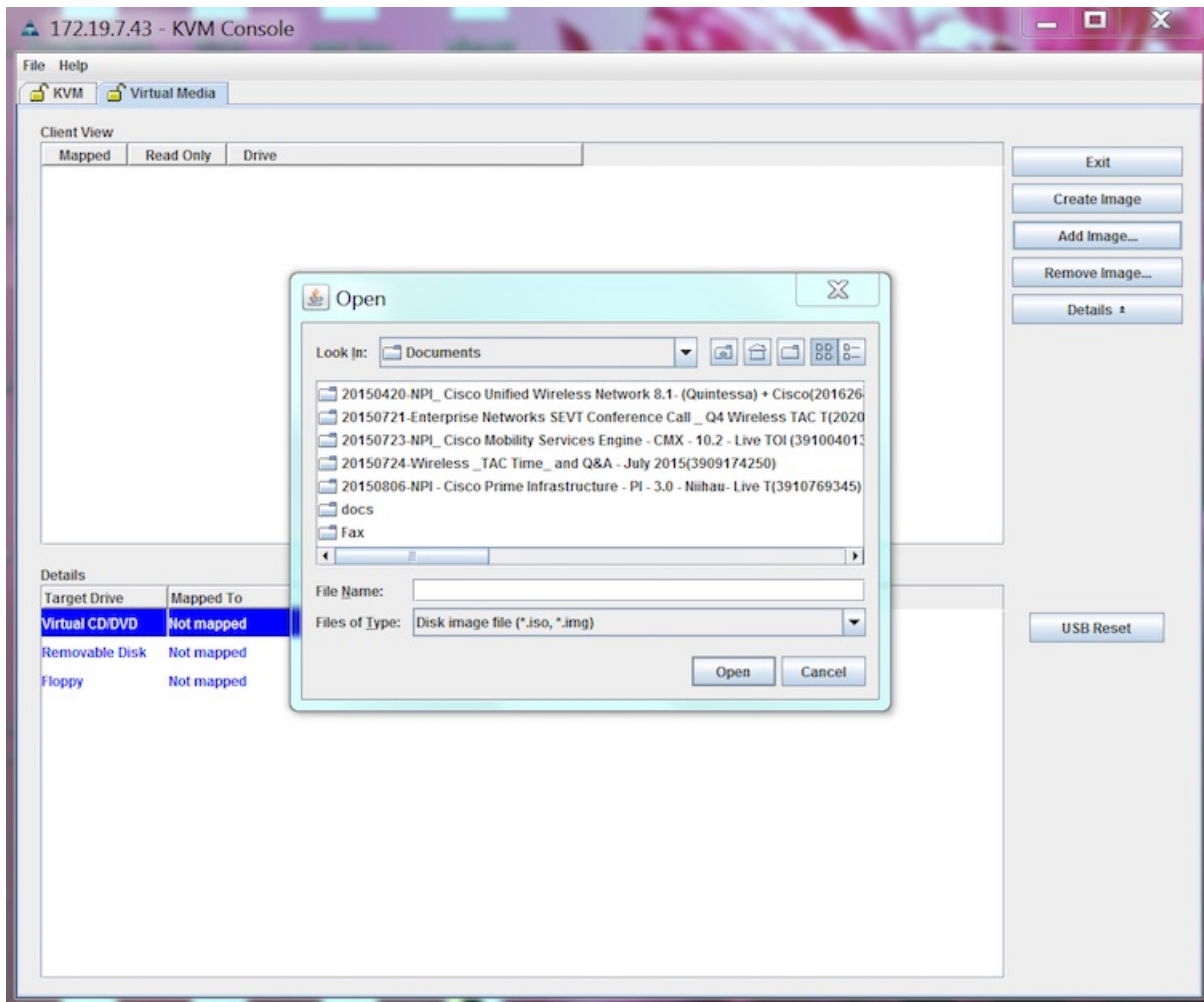
Step 6 In the **Virtual Media** window that is displayed, click **Add Image**.

Figure 40: Virtual Media



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

Figure 41: Select Downloaded Cisco MSE ISO Image



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.

