Cisco Mobility Services Engine Virtual Appliance Installation Guide for Cisco CMX Release 11.0.0

First Published: 2017-04-02

Last Modified: 2023-05-19

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.

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 standards documentation, or language that is used by a referenced third-party product.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.

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 standards 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.

Cisco CMX is the on-premise location service that is provided as part of the Cisco Spaces overall location as a platform service.

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.

Convention	Indication
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string. 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 Spaces, see Cisco Spaces support page.

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 DevNet.
- 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 gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

CONTENTS

PREFACE

Preface iii

Audience iii

Conventions iii

Related Documentation iv

Communications, Services, and Additional Information iv

Cisco Bug Search Tool v

Documentation Feedback v

CHAPTER 1

Installing Cisco CMX 1

Installing Cisco CMX in a VMware Virtual Machine 1

Virtualization Concepts 1

Installation Overview 1

Restrictions for Installing Cisco CMX in a VMware Virtual Machine 2

Cisco CMX Virtual Appliance Deployment Checklist 2

Prerequisites for Installing Cisco CMX in a VMware Virtual Machine 3

Hardware Guidelines 3

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 11.0.0 17

Verifying Installation of Cisco CMX in a VMware Virtual Machine 22

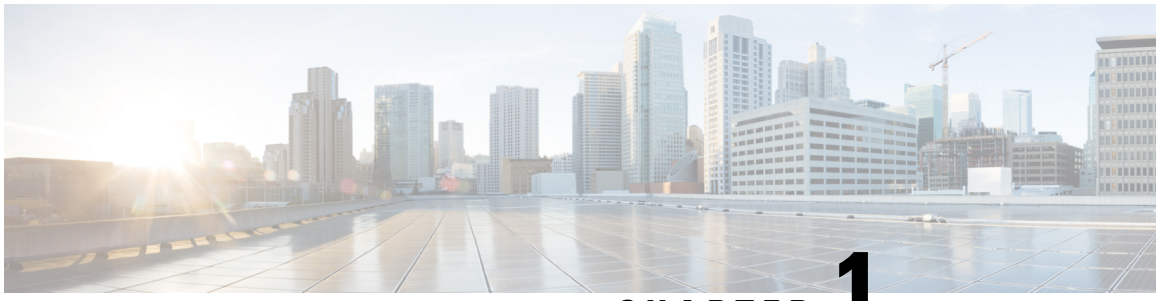
CHAPTER 2

Virtual Machine Setup and Administration 23

Adding a Hard Disk to a Virtual Machine in the vSphere Client 23

Configuring the Network 23

Reconfiguring CPU and RAM for Cisco CMX installation 23



CHAPTER 1

Installing Cisco CMX

- Installing Cisco CMX in a VMware Virtual Machine, on page 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.

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 2 and Hardware Guidelines, on page 3
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 11.0.0, on page 17

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.
- Cisco 11.0.0 OVA, which can be downloaded from Download Software page on cisco.com.
- 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, 250 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 Deploying the Cisco CMX OVA File Using the VMware vSphere Web Client, on page 8.

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		—
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	—	—

Release	Location and Analytics Node	Location and Connect Node	Location, Analytics, and Connect Node (L-Node)	Connect and Presence Node (P-Node)	High Availability
10.2	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
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 the Download Software page 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) manages the vCenter Server 6.5 environment with all the features and plugins. From VMware vSphere Release 6.5, we recommend that you use vSphere Web Client.

From VMware vSphere Release 6.5, 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.

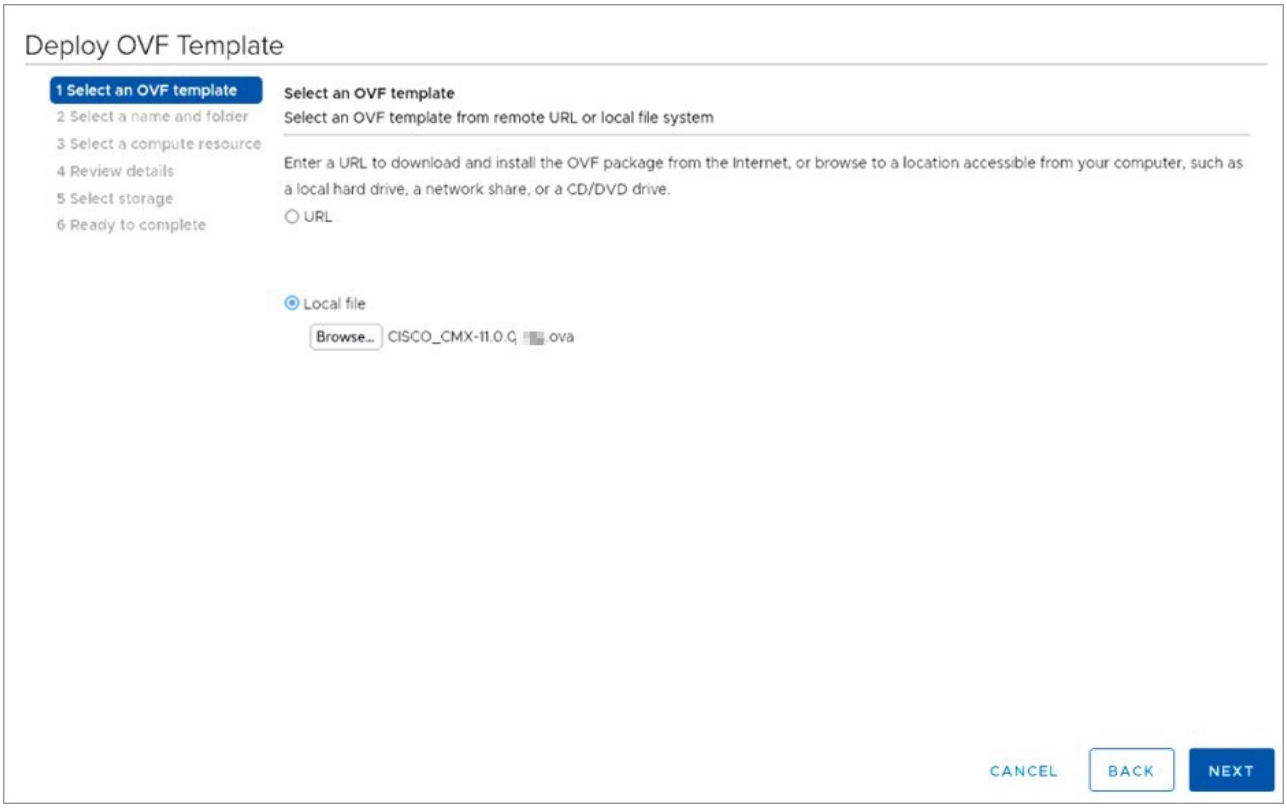
Step 2 From the **Navigator** pane, click **Create/Register VM** to create or register a virtual machine (VM).

The **Deploy OVF Template** window is displayed.

Step 3 In the **Select an OVF Template** section, click the **Local file** radio button to browse to a local directory, select the Cisco CMX OVA file that is stored locally, and click **Next**.

This helps you create a VM from a Cisco CMX OVA file.

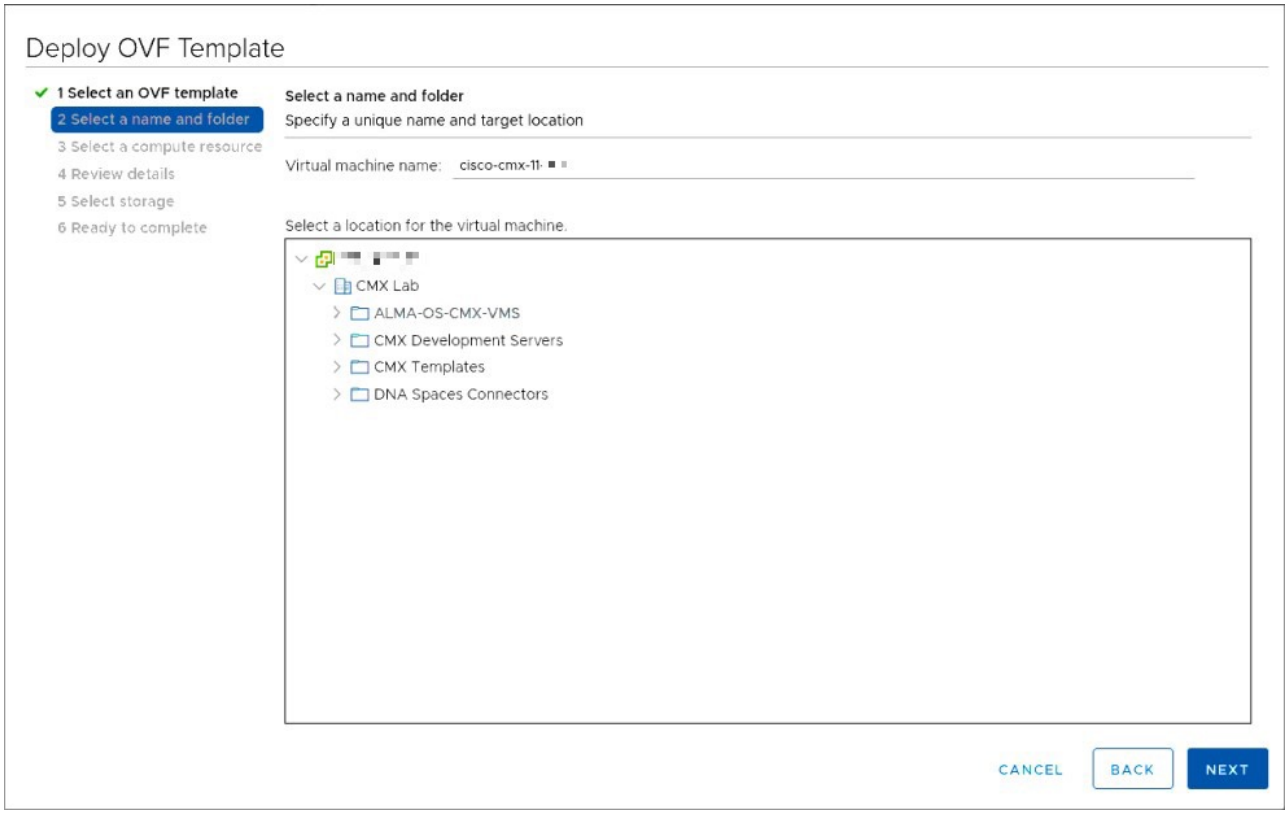
Figure 1: Select an OVF Template



Step 4 In the **Select a name and folder** section, enter the following information and click **Next**.

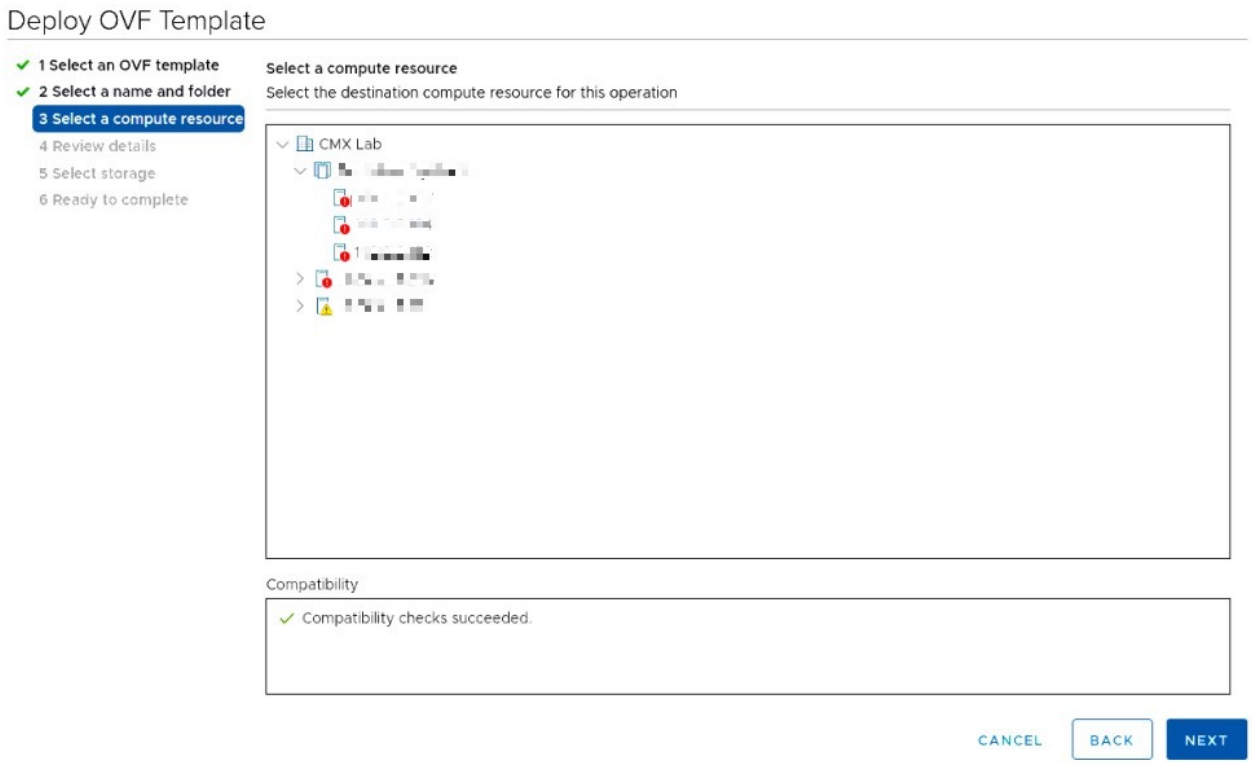
- **Virtual machine name**: Enter a name for the VM.
- **Select a location for the virtual machine**: Select a location for VM.

Figure 2: Select a Name and Folder



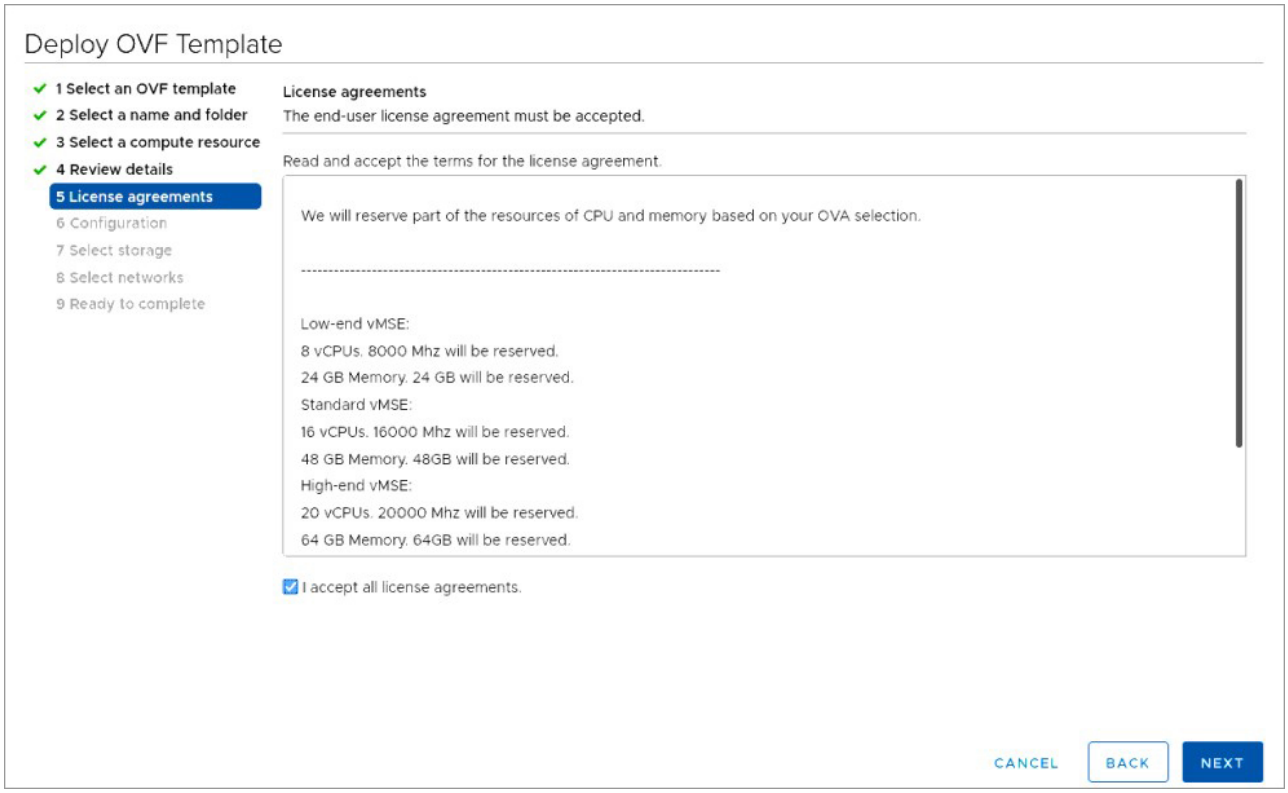
Step 5 In the **Select a compute resource** section, select the destination data store for the VM configuration files and virtual disks and click **Next**.

Figure 3: Select a Compute Resource



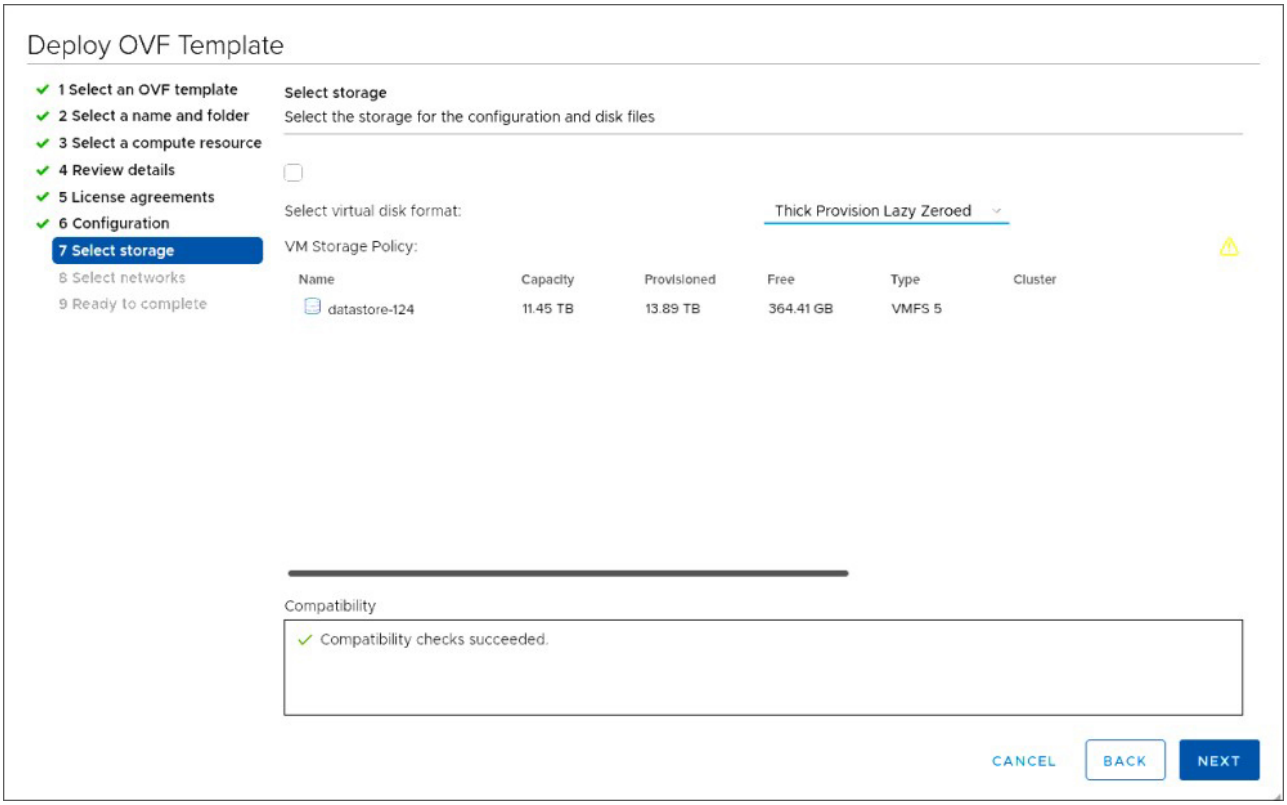
Step 6 In the **License agreements** section, click the **I accept all license agreements** check box to accept the End User License Agreement and click **Next**.

Figure 4: License Agreements



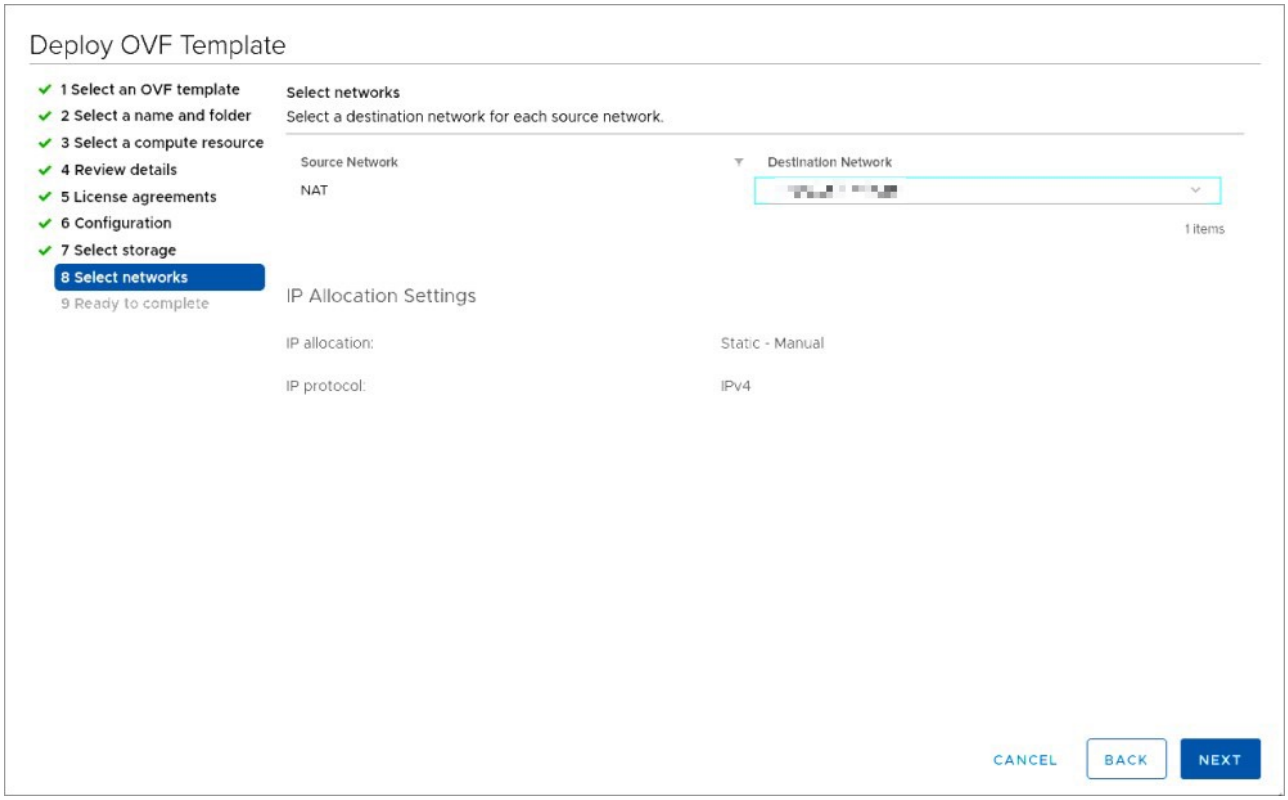
Step 7 In the **Select storage** section, select the storage for the configuration and disk files and click **Next**.

Figure 5: Select Storage



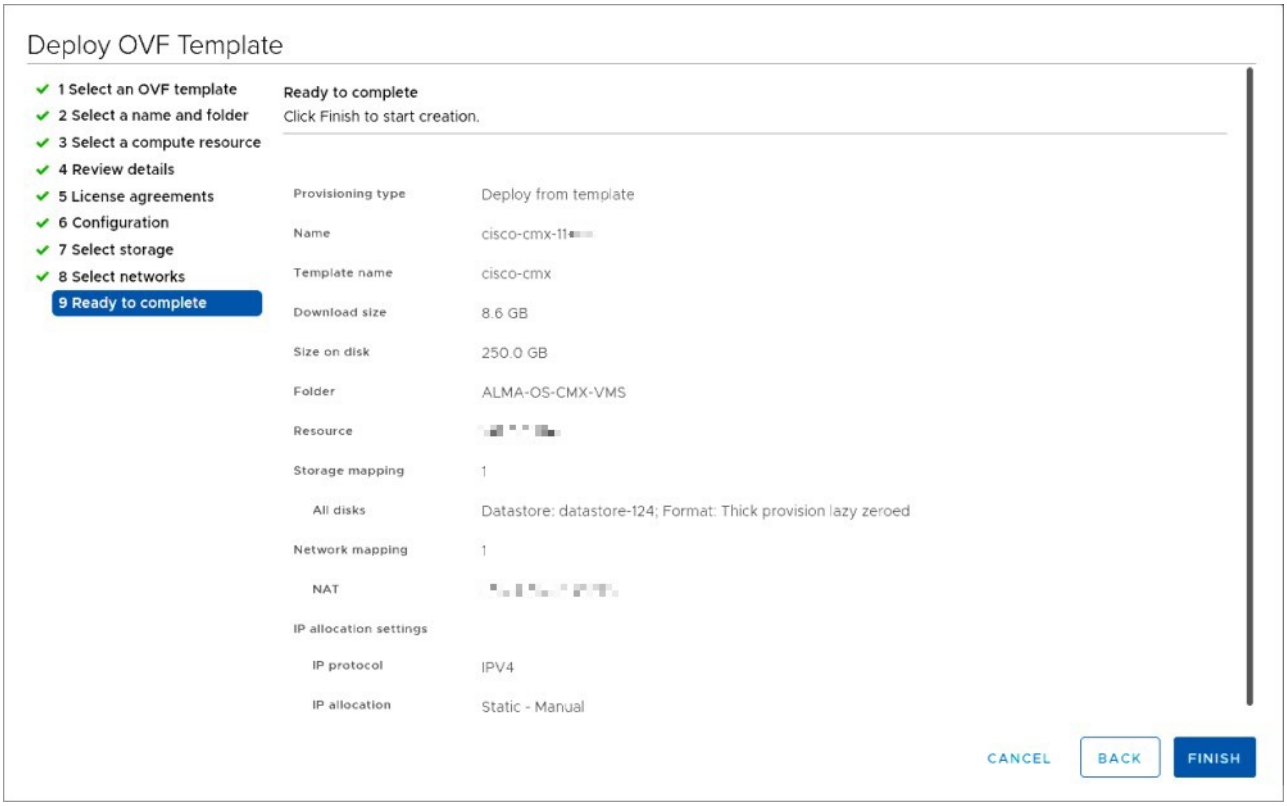
Step 8 In the **Select Networks** section, from the **Destination Network** drop-down list, choose a destination network for each source network and click **Next**.

Figure 6: Select Networks



Step 9 In the **Ready to complete** section, review the settings and click **Finish**. Do not refresh the browser when the VM is deployed.

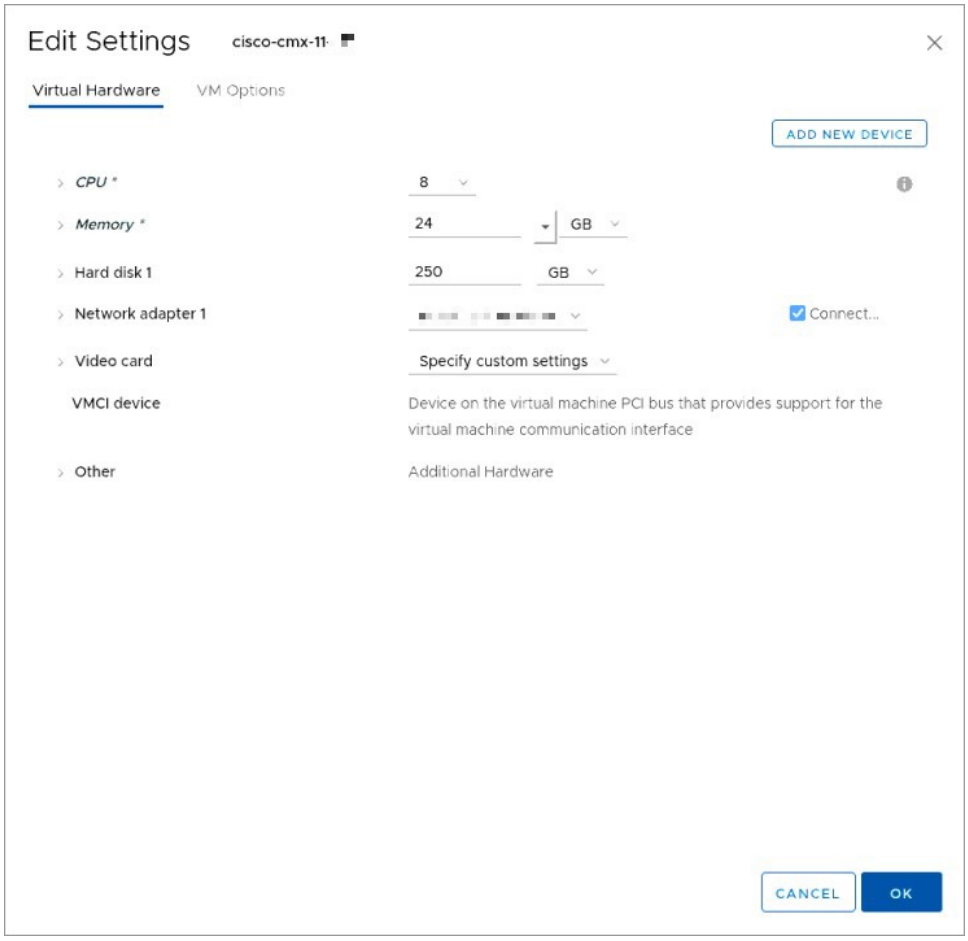
Figure 7: Ready to Complete



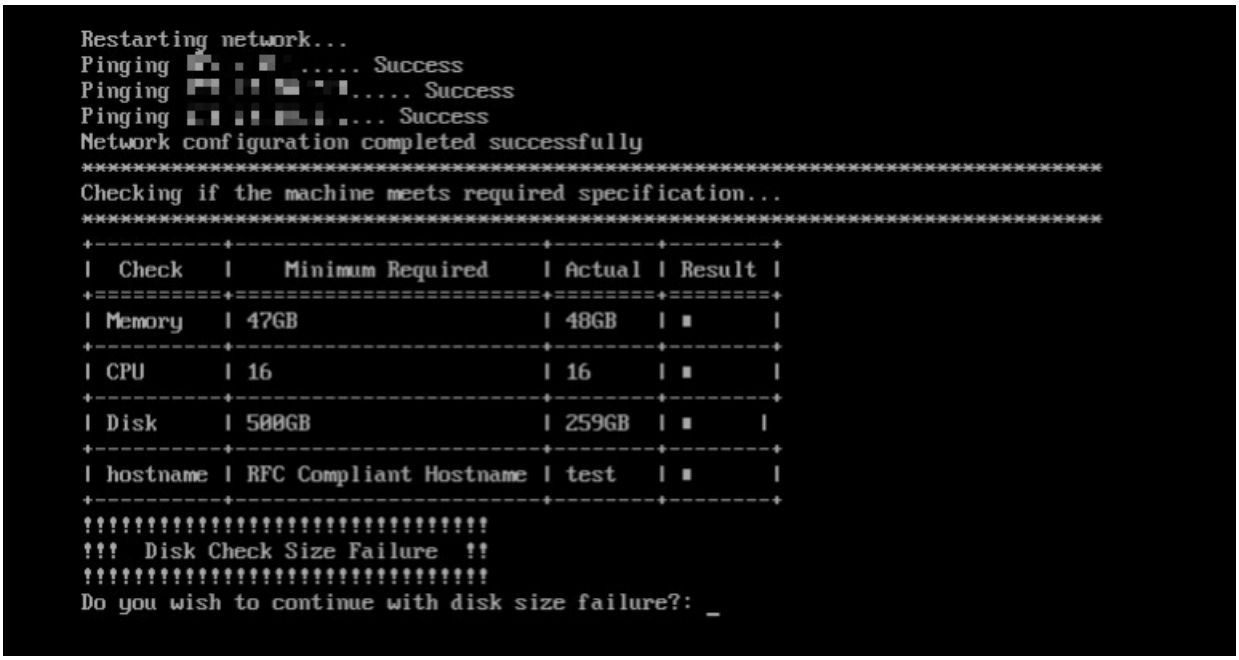
Step 10 Click the deployed VM and choose **Actions > Edit Settings**.

Step 11 In the **Virtual Hardware** tab, in the **Hard disk 1** field, modify the provisioned size to match the instance requirement and click **OK**. The default size is 250 GB.

Figure 8: Hard Disk Provisioned Size



Note If the instance is powered on, it will display a warning message—`Hard Disk Size Failure`—for Standard and High End instances.



Step 12 Click **Power on** to power on the VM. The first boot takes a while because the new disk has to be expanded.

Figure 9: Power On VM

Configuring Cisco CMX Release 11.0.0

After the Cisco CMX is deployed, you can install and configure a Cisco CMX 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 and completes the installation. You should not use the Web install.
- 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.**

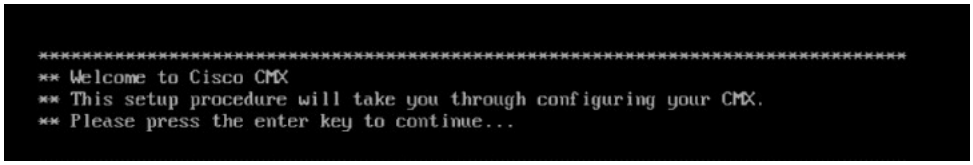
The initial boot displays two options, with the first option being selected by default. Retain the selection and wait for five seconds.

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

Figure 10: Console

Step 3 Press **Enter** when prompted.

Figure 11: 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 on the screen.

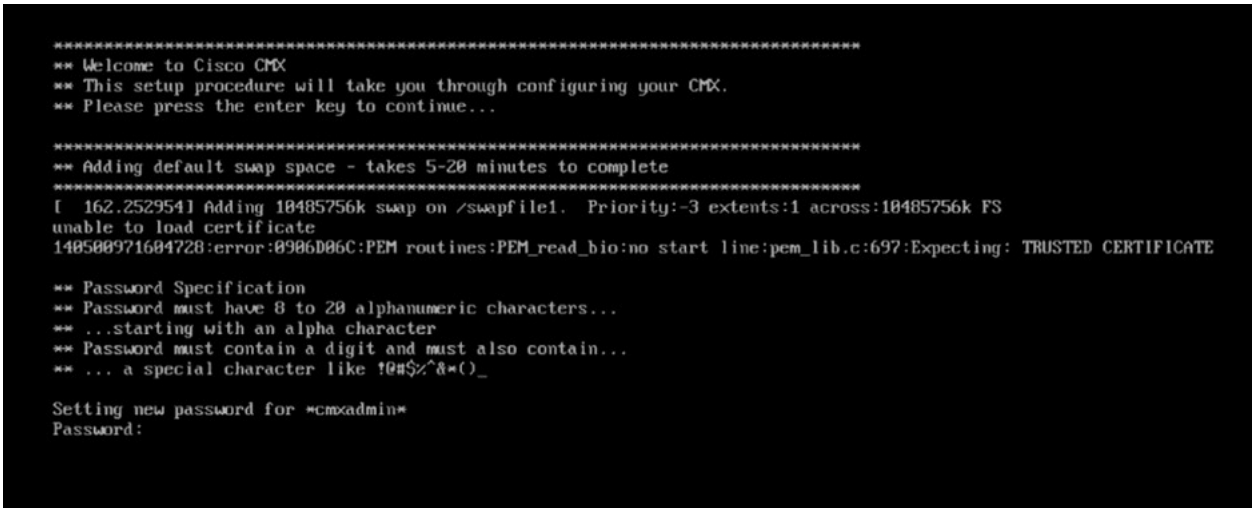
Note The root password is used only for the root operating system configuration and not for the cmxadmin user functions.

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

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

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

Figure 12: Set Passwords



Step 6 Enter the following network configuration parameters when prompted.

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

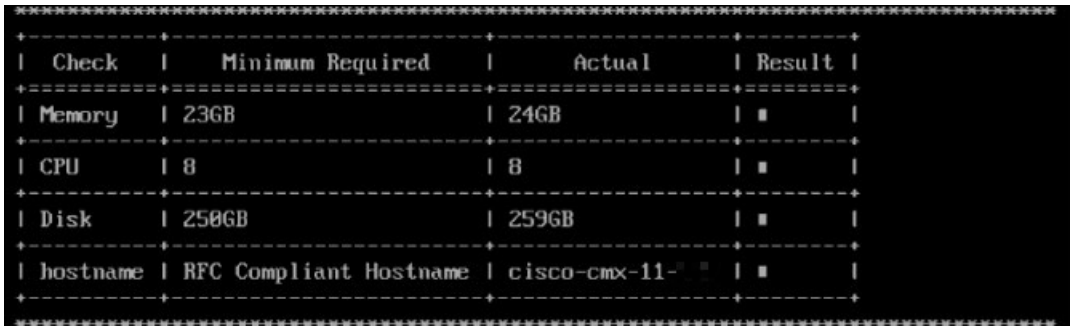
Figure 13: Network Configuration Parameters

Note For a successful validation, hostname:

- can include a hyphen, however never end or start the hostname with a hyphen
- can include alphanumeric data
- cannot not start with a digit
- cannot not have special characters (for example, .,?,*,_)

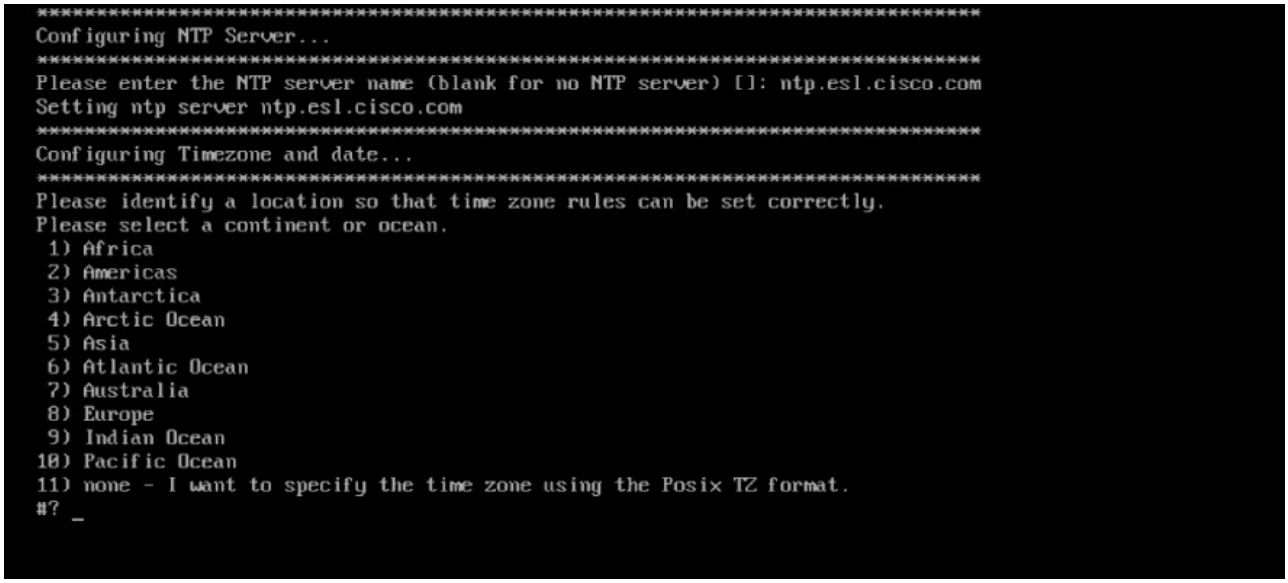
Step 7 Confirm the network configurations when prompted.

Figure 14: Network Configuration



Step 8 (Optional) Enter the NTP server name or the IP address of the NTP server when prompted.

Figure 15: NTP Server Configuration

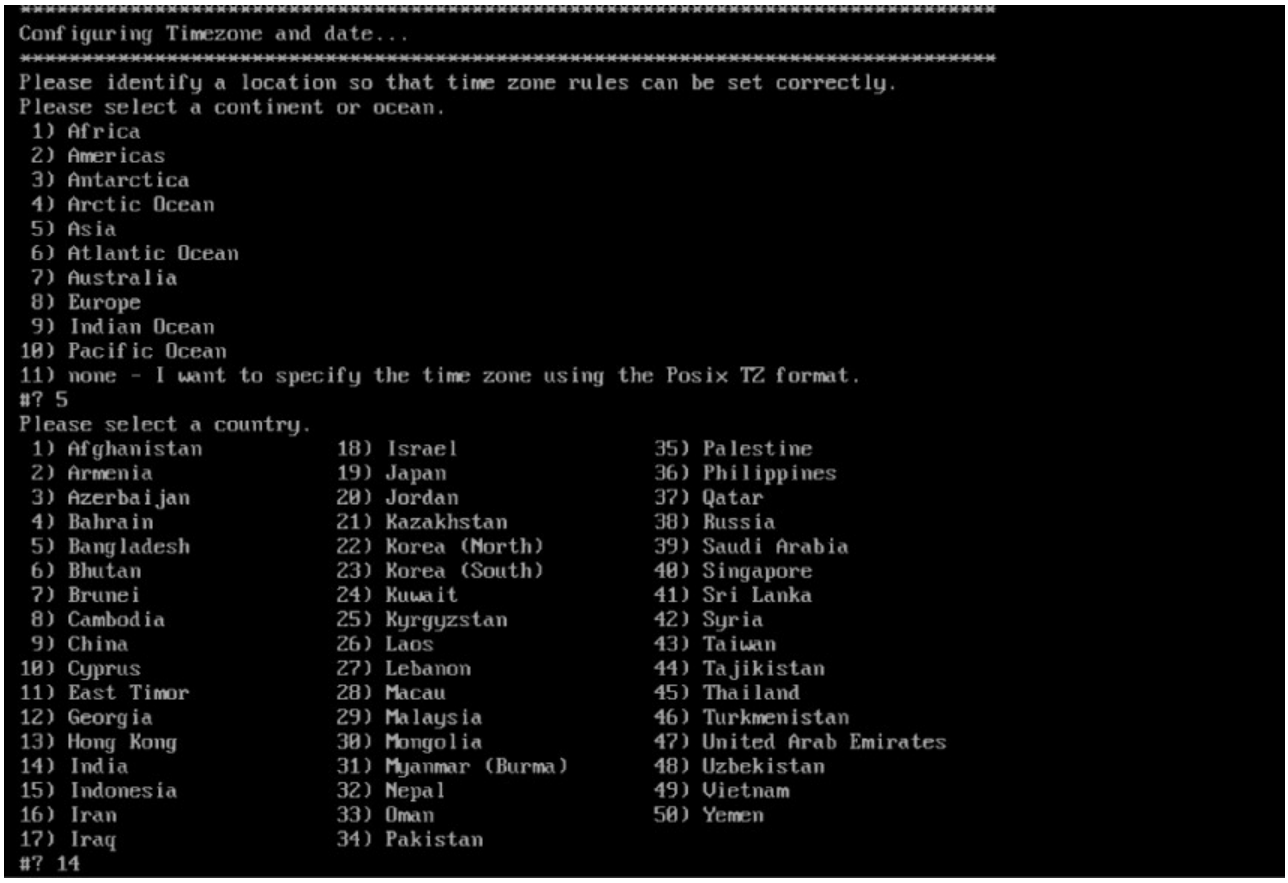


Note After installation, the task of changing the NTP information either through the CLI or the GUI is not supported. Use the **cmxos reconfigure** command from the CMX CLI to change the NTP information. The following example shows a workaround to change the NTP information:

```
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 9 Configure a time zone and save the changes.

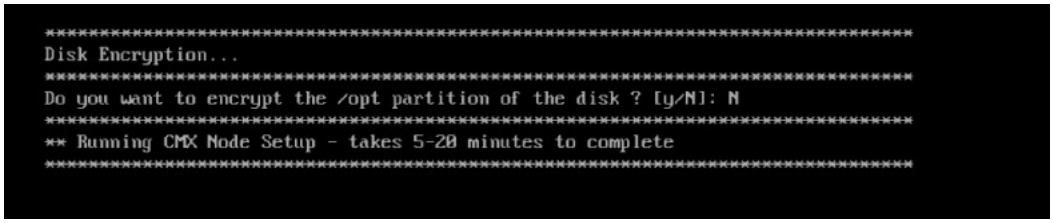
Figure 16: Configuring a Time Zone



Step 10 Encrypt the /opt partition of the disk. For Cisco CMX Release 11.0.0, select **N**.

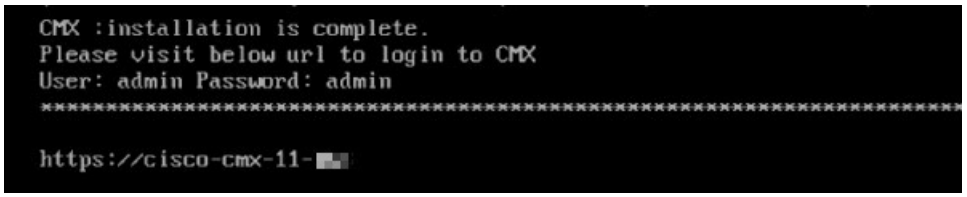
Note Disk encryption is not supported in Cisco CMX Release 11.0.0. If you perform disk encryption, Cisco CMX Release 11.0.0 installation fails.

Figure 17: Disk Encryption



Step 11 After the Cisco CMX installation is complete, the following success message is displayed.

Figure 18: Success Message



Step 12 To stop all the Cisco CMX services, run the **cmxctl stop -a** command.

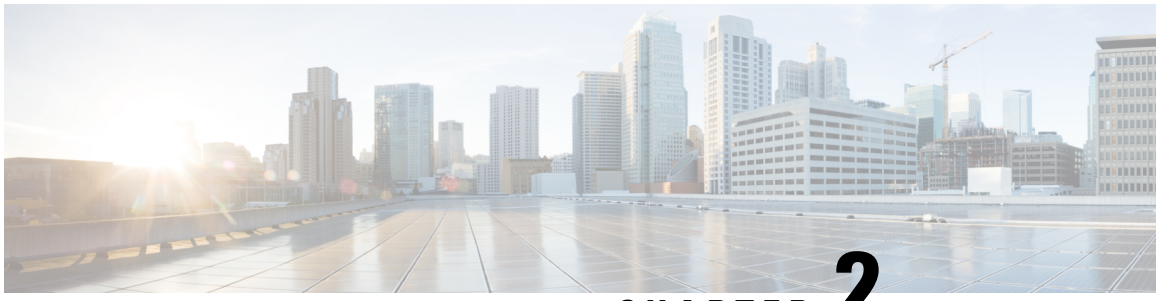
Step 13 To restart the Cisco CMX services, run the **cmxctl start -a** command.

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 GUI. 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 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 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 23
- Configuring the Network, on page 23
- Reconfiguring CPU and RAM for Cisco CMX installation, on page 23

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.