



## **Cisco MSE Virtual Appliance Installation Guide for Cisco CMX Release 10.2**

September, 2015

### **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.

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: [www.cisco.com/go/trademarks](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)

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 MSE Virtual Appliance Installation Guide for Cisco CMX Release 10.2*  
© 2015 Cisco Systems, Inc. All rights reserved.



**Preface** v

---

**CHAPTER 1**

**Installing a Cisco MSE Virtual Appliance** 1-1

- Virtualization Concepts 1-2
- Installation Overview 1-2
- Cisco MSE Virtual Appliance Deployment Checklist 1-2
- Release Upgrade Compatibility Matrix 1-3
- Cisco CMX Services Deployment Checklist 1-5
- Requirements for Installing Cisco MSE Virtual Appliance 1-5
- Hardware Guidelines 1-5
- Downloading the Cisco MSE OVA File 1-6
- Deploying the Cisco MSE OVA File Using the VMware vSphere Client 1-6
- Installing a Cisco MSE Virtual Appliance 1-8
  - Installing Cisco CMX Using Web Interface 1-15
- Upgrading Cisco CMX 10.2 to Future Releases 1-21
- Upgrading a Cisco CMX 10.1.x Deployment to 10.2 1-25
- Verifying the Cisco CMX Services 1-25

---

**CHAPTER 2**

**Virtual Machine Setup and Administration** 2-1

- Adding a Hard Disk to a Virtual Machine in the vSphere Client 2-1
- Configuring the Network 2-1





## Preface

---

This preface describes the audience for, organization of, and the conventions used in this document. It also provides information about how to obtain related documentation. It includes the following sections:

- [Audience, page v](#)
- [Document Conventions, page v](#)
- [Related Documentation, page vi](#)
- [Obtaining Documentation and Submitting a Service Request, page vi](#)

## Audience

This document is for experienced network administrators who install the Cisco Mobility Services Engine (MSE) virtual appliance, and install, configure, and maintain the Cisco Connected Mobile Experiences (CMX) services.

## Document Conventions

This document uses the following conventions:

**Table 1**      **Conventions**

<b>Convention</b>	<b>Indication</b>
<b>bold font</b>	Commands, keywords, and text entered by users appear in <b>bold font</b> .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
Option > Option	Used to describe a series of options.
[ ]	Elements in square brackets are optional.
{x   y   z}	Required alternative keywords are grouped within braces and separated by vertical bars.
[x   y   z]	Optional alternative keywords are grouped within braces and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.

**Table 1**      **Conventions (continued)**

Convention	Indication
<code>courier font</code>	Terminal sessions and information the system displays appear in <code>courier font</code> .
<code>&lt;&gt;</code>	Nonprinting characters such as passwords are in angle brackets.
<code>[ ]</code>	Default responses to system prompts are in square brackets.
<code>!, #</code>	An exclamation mark (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

**Note**

Means reader take note.

**Tip**

Means the following information will help you solve a problem.

**Caution**

Means reader be careful. In this situation, you might do something that can result in equipment damage or loss of data.

**Warning**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

## Related Documentation

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 (CMX), see:  
<http://www.cisco.com/c/en/us/solutions/enterprise-networks/connected-mobile-experiences/index.html>

For more information about Cisco CMX commands, see:  
<http://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/products-command-reference-list.html>

## Obtaining Documentation and Submitting a Service Request

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

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

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







# Installing a Cisco MSE Virtual Appliance

This chapter describes how to install and deploy a Cisco Mobility Services Engine (MSE) virtual appliance, which is distributed as an Open Virtual Appliance (OVA) file.

Cisco MSE OVA 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 OVA for the virtual appliance and as an ISO to install the software on a physical appliance.

Cisco MSE acts as a platform (physical or virtual Cisco MSE appliance) to deploy and run the Cisco Connected Mobile Experiences (CMX) services. Cisco MSE virtual appliance installation provides the choice of installing Cisco Location service or Cisco Presence Analytics service.



**Note**

Running both the Location and Presence Analytics services on the same CMX instance is not supported in Cisco CMX Release 10.2.

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

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

- PRESENCE ANALYTICS
- CONNECT & ENGAGE

This chapter contains the following sections:

- [Virtualization Concepts, page 1-2](#)
- [Installation Overview, page 1-2](#)
- [Cisco MSE Virtual Appliance Deployment Checklist, page 1-3](#)
- [Release Upgrade Compatibility Matrix, page 1-4](#)
- [Cisco CMX Services Deployment Checklist, page 1-5](#)
- [Requirements for Installing Cisco MSE Virtual Appliance, page 1-5](#)
- [Hardware Guidelines, page 1-6](#)
- [Downloading the Cisco MSE OVA File, page 1-6](#)
- [Deploying the Cisco MSE OVA File Using the VMware vSphere Client, page 1-7](#)

- [Installing a Cisco MSE Virtual Appliance](#), page 1-9
- [Upgrading Cisco CMX 10.2 to Future Releases](#), page 1-22
- [Upgrading a Cisco CMX 10.1.x Deployment to 10.2](#), page 1-26
- [Verifying the Cisco CMX Services](#), page 1-26

## Virtualization Concepts

Refer to these documents for information on virtualization:

- <http://www.vmware.com/pdf/virtualization.pdf>
- <http://pubs.vmware.com/vsphere-55/index.jsp#com.vmware.vsphere.vcenterhost.doc/GUID-ED375B12-7D08-4B7E-81EE-DCE83E51B1AF.html>
- <http://pubs.vmware.com/vsphere-55/index.jsp#com.vmware.vsphere.install.doc/GUID-41638619-B14E-4074-BB90-DACAA1440C1C.html?resultof=%2522%2545%2553%2558%2569%2522%2520%2522%2565%2573%2578%2569%2522%2520>

## Installation Overview

The following table lists the Cisco MSE virtual appliance installation process.

**Table 1-1** *Installation Overview*

Task	See...
1. Review the deployment checklist and prepare for the installation of a Cisco MSE virtual appliance.	<a href="#">“Cisco MSE Virtual Appliance Deployment Checklist”</a> section on page 1-3 and <a href="#">“Hardware Guidelines”</a> section on page 1-6
2. Download the Cisco MSE Open Virtualization Archive (OVA) file from Cisco.com.	<a href="#">“Downloading the Cisco MSE OVA File”</a> section on page 1-6
3. Deploy the Cisco MSE OVA file.	<a href="#">“Deploying the Cisco MSE OVA File Using the VMware vSphere Client”</a> section on page 1-7
4. Configure the basic configurations and install the Cisco MSE virtual appliance.	<a href="#">“Installing a Cisco MSE Virtual Appliance”</a> section on page 1-9
5. Set up the Cisco MSE virtual appliance.	<a href="#">“Installing Cisco CMX Using Web Interface”</a> section on page 1-16



**Note** If you are upgrading a 10.1 deployment to 10.2, see the [“Upgrading a Cisco CMX 10.1.x Deployment to 10.2”](#) section on page 1-26.

# Cisco MSE Virtual Appliance Deployment Checklist

Review the following checklist before attempting to deploy the Cisco MSE virtual appliance:

- Cisco Wireless LAN Controller (WLC) 7.0 or later.
- Simple Network Management Protocol (SNMP) credentials of Cisco WLC (private key for V1 and V2, or username and password for V3).
- Cisco WLC should have an IP connectivity to a Cisco CMX 10.2 instance.
- Port 16113 should be routable from Cisco WLC to the Cisco CMX 10.2 IP address.
- SNMP traffic over port 161 should be routable from Cisco WLC to the Cisco CMX 10.2 IP address.
- Cisco Prime Infrastructure 1.4 or later.
- Cisco WLC should be synchronized with Cisco Prime Infrastructure 1.4 or later.
- Map size should be less than 5 MB in Cisco Prime Infrastructure.
- There should be less than 1000 access points on a single map.
- In Cisco Prime Infrastructure, the hierarchy of maps should be campus, building, and zone, in that order.
- The following functionalities are not available in Cisco CMX 10.2:
  - Wireless intrusion prevention system (wIPS)
  - Mobile Application Server
- VMware virtualization environment ESXi 5.5 or later.
- Cisco CMX 10.2 should have been tested with the following browser:
  - Google Chrome 40 or later
- Determine the IP address, NetMask, Default Gateway, DNS IP address, and Network Time Protocol (NTP) Server IP address for the new Virtual Machine (VM).
- IP connectivity to the machine running the Cisco CMX instance.
- SSH client to log in to the root access of the VM.
- The Secure Copy (SCP) client (on MAC native or installed on PC) or a Secure File Transfer Protocol (SFTP) to move files into Cisco MSE OVA (specifically, map files and images to upgrade).
- Time displayed on the Cisco WLC is always ahead of the Cisco MSE time. Use a common NTP server to know the time.
- Cisco CMX 10.2 has a mail notification system. Use the SMTP Mail Server name and authentication mechanism.
- 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.

# Release Upgrade Compatibility Matrix

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

**Table 1-2** 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_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

The following table lists the node types supported per release.

**Table 1-3** 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

The following table lists the upgrade options by node type.

**Table 1-4 Upgrade Path by Node Type**

Upgrade Path <sup>1</sup>	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 10.2	—	—	UI upgrade script to upgrade image.	UI upgrade script to upgrade image

1. 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 1-5 Alerts on the VM**

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

## Cisco CMX Services Deployment Checklist

- During the installation of Cisco MSE virtual appliance, select the Cisco CMX services that you want to run on the Cisco MSE virtual appliance.

## Requirements for Installing Cisco MSE Virtual Appliance

- VMware ESXi host server (see [Table 4](#)).
- vSphere client.

- Cisco MSE 10.2 OVA from [www.cisco.com/go/mse](http://www.cisco.com/go/mse).
- Hostname, IP address, network mask, gateway, and DNS IP address for the new VM.
- NTP server name or IP address.
- Existing exported map file from Cisco Prime Infrastructure.
- IP address of the Cisco Wireless Controller, the Controller type, the Controller IP address, the SNMP version, and the SNMP write community string.
- Mail server settings (port number, security settings) and email address.

## Hardware Guidelines

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


**Note**

The OVA will fail to boot if the hardware requirements are not met during OVA deployment. Similarly, the Cisco CMX setup will fail when the minimum requirements are not met during the installation.

**Table 1-6**      **Hardware Guidelines**

Hardware Platform	Demo Appliance	Basic Appliance	Standard Appliance	High-End Appliance
CPU	4 vCPU	8 vCPU (2.4 GHz core) \ 4 physical cores	16 vCPU (2.4 GHz core) \ 8 physical cores	20 vCPU (2.4 GHz core) \ 10 physical cores
RAM	16 GB	24 GB	48 GB	64 GB <sup>1</sup>
HDD	—	500 GB	500 GB	1 TB

1. The high-end deployment VM (20 vCPU, 64 GB RAM) reserves 64 GB RAM. However, it allows only 63.74 GB and the rest of the RAM is used by ESXi.


**Note**

- Cisco CMX 10.2 software can be installed on Cisco MSE 3365 currently running Release 8.0 using the .ISO image
- The .ISO image can either be on a DVD or mounted as a virtual drive through the use of the CIMC.
- Cisco CMX 10.2 software is deployed on a new vMSE by using the VMware vSphere client to deploy the .ova file available on CCO.

## Downloading the Cisco MSE OVA File

Cisco MSE virtual appliance is distributed as an OVA file.

To download the Cisco MSE OVA file, follow these steps:

- 
- Step 1**    Access the Cisco MSE image from:  
<https://software.cisco.com/download/navigator.html?mdfid=282152561&i=rm>
- Step 2**    Click **Mobility Services Engine Virtual Appliance**.
- Step 3**    Choose **Latest > 10.2** for download.

- Step 4** 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



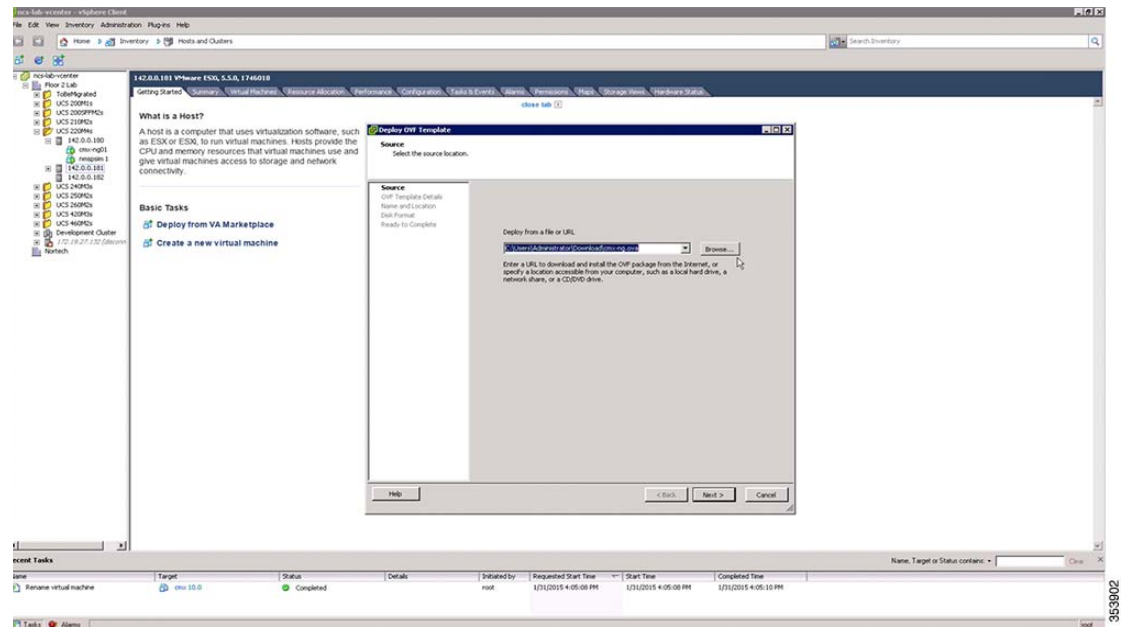
### Note

Read the “Requirements for Installing Cisco MSE Virtual Appliance” section on page 1-5 before you deploy the Cisco MSE OVA.

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

- Step 1** Download the Cisco MSE OVA file from the following location:  
<https://software.cisco.com/download/navigator.html?mdfid=282152561&i=rm>.
- Step 2** Deploy the OVA file by using the VMware vSphere Client application on your desktop.

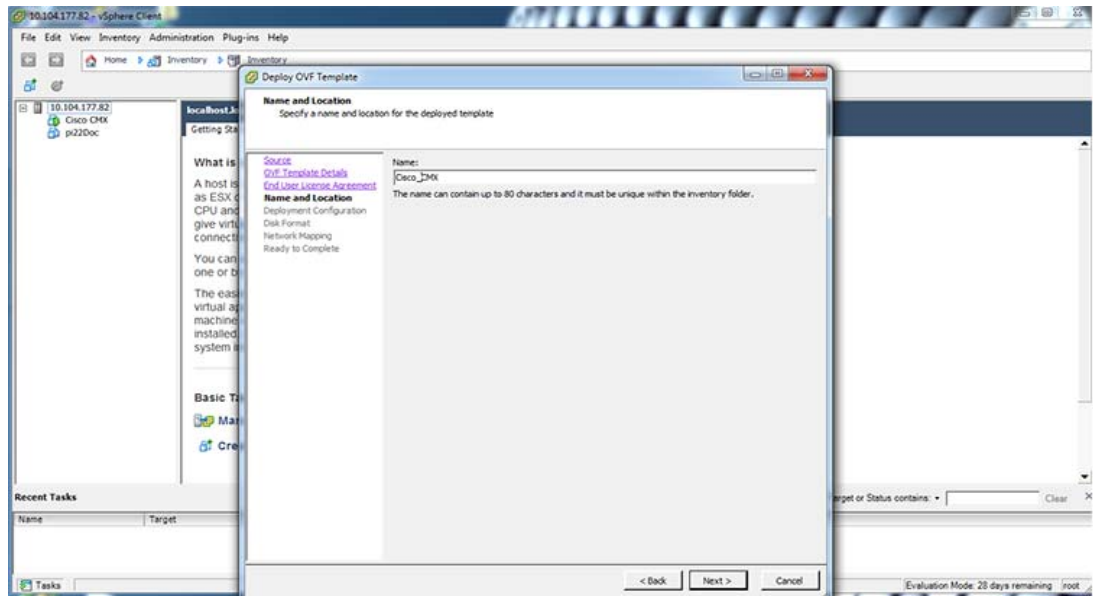
**Figure 1-1** VMware vSphere Client



After you deploy the OVA file using the vSphere client, the Deploy OVF Template window is displayed.

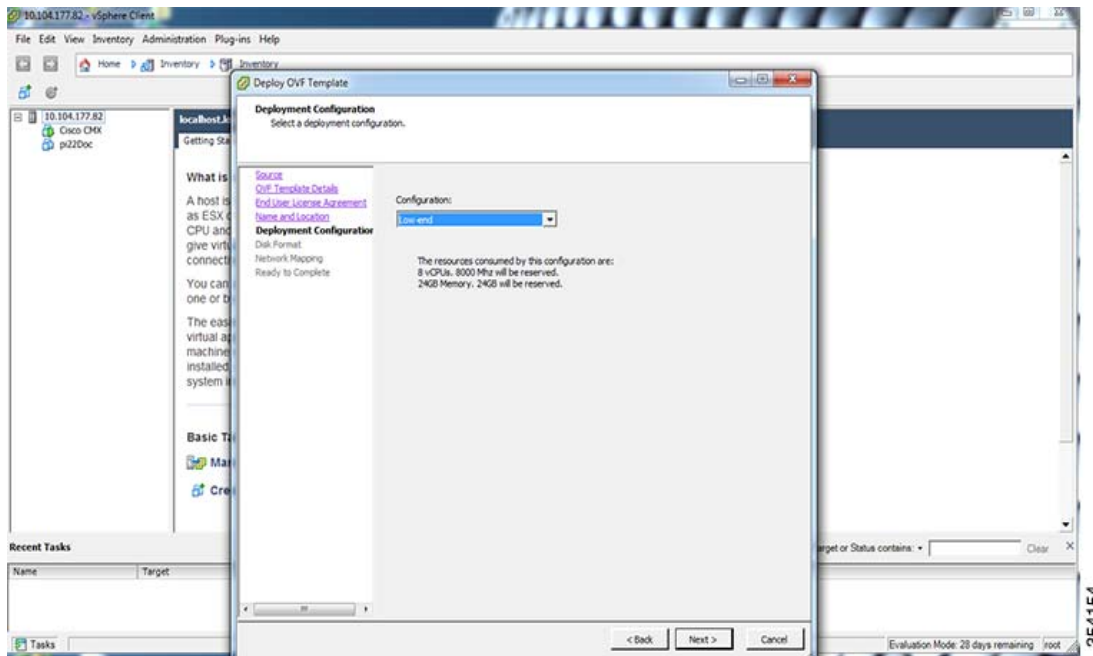
- Step 3** Enter a name for the Cisco MSE VM that is created.

Figure 1-2 Name for Cisco MSE VM



**Step 4** From the **Configuration** drop-down list, choose the VM configuration.

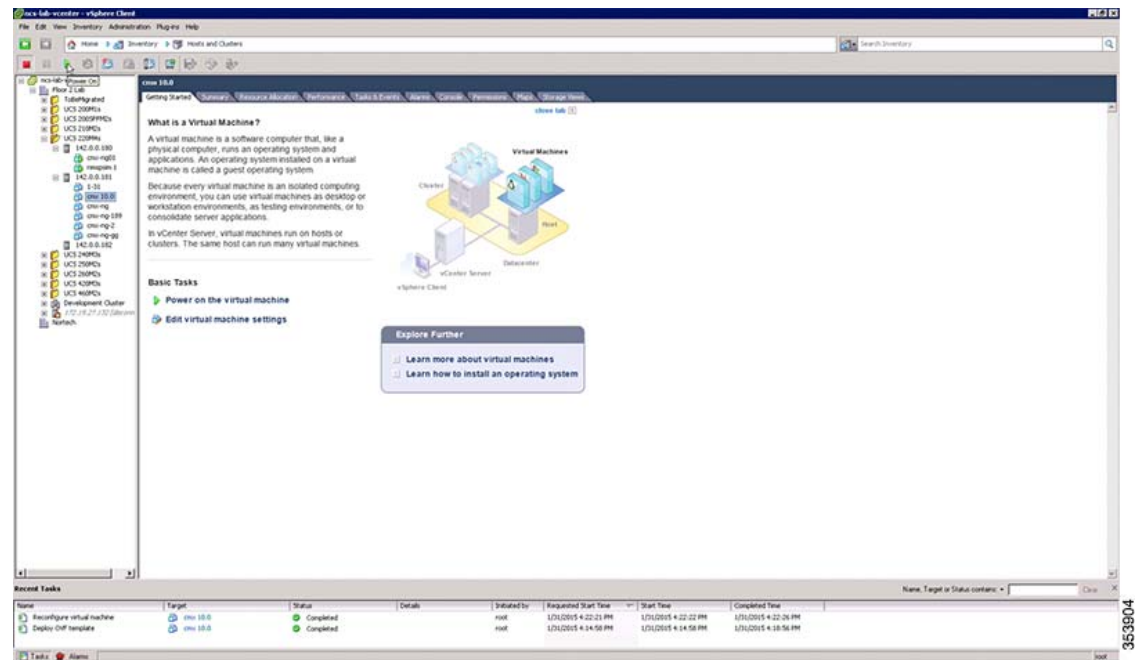
Figure 1-3 VM Configuration



**Step 5** Power on the VM by clicking **Power On the Virtual Machine**.



Figure 1-4 Powering On The Virtual Machine



## Installing a Cisco MSE Virtual Appliance

After deploying the Cisco MSE OVA file, configure the basic settings, install, and start Cisco MSE.

- There is no node install menu in Release 10.2. Instead, there is a new first boot script added to check for existence of a configuration in the box. If no valid configuration is found, the install launches into the setup routine that starts with performing network configuration tasks from the CLI and then using a browser to complete the initial setup tasks.
- New first boot script determines if the initial configuration has been completed or not– if it is not, prompts for a default login. If the initial configuration is completed, the script prompts for a normal login.
- Initial login requires password configuration for both the root and new cmxadmin users.



### Note

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

To install and configure a Cisco MSE virtual appliance, follow these steps:

**Step 1** Log in to the vSphere Client and begin the installation by providing the login credentials:

```
-----
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
```

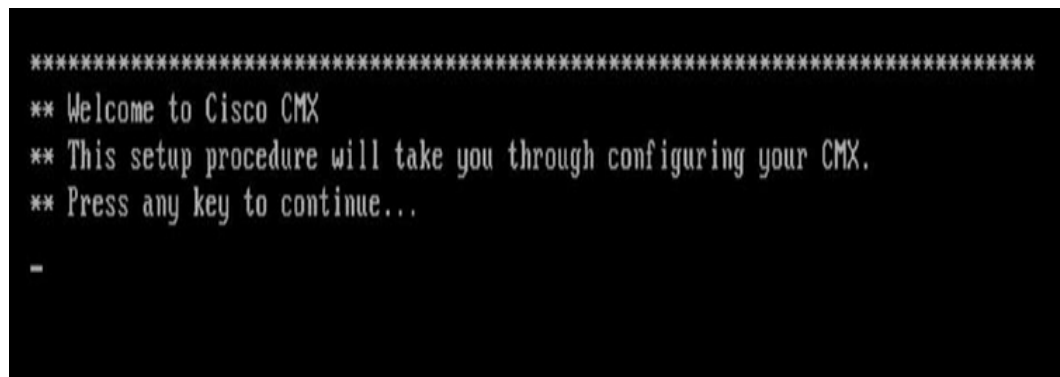
**Figure 1-5** Cisco CMX Screen



The installation is initiated.

- Step 2** Press the **Enter** key to continue.

**Figure 1-6** Cisco CMX Welcome Screen



- Step 3** Enter a new password for the root user, and reconfirm it. The password should meet the minimum requirements listed in the window. The root password is used only for root operating system configuration, and not for cmxadmin functions.

**Figure 1-7** Minimum Hardware Requirements

```

** Press any key to continue...

*****
Checking if the machine meets required specification...
*****

+-----+-----+-----+-----+
| Check | expected | actual | Result |
+-----+-----+-----+-----+
| memory | 8GB      | 18GB   | #      |
+-----+-----+-----+-----+
| cpu    | 4        | 12     | #      |
+-----+-----+-----+-----+
| disk   | 58GB     | 368GB  | #      |
+-----+-----+-----+-----+
| hostname | rfc compliant hostname | localhost.localdomain | #      |
+-----+-----+-----+-----+

```

354152

- Step 4** Enter a new password for cmxadmin and reconfirm it. The password should meet the minimum requirements listed in the screen. The cmxadmin password is used for logging into the Cisco CMX account for future network admin configurations.

**Figure 1-8** Password Change

```

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

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

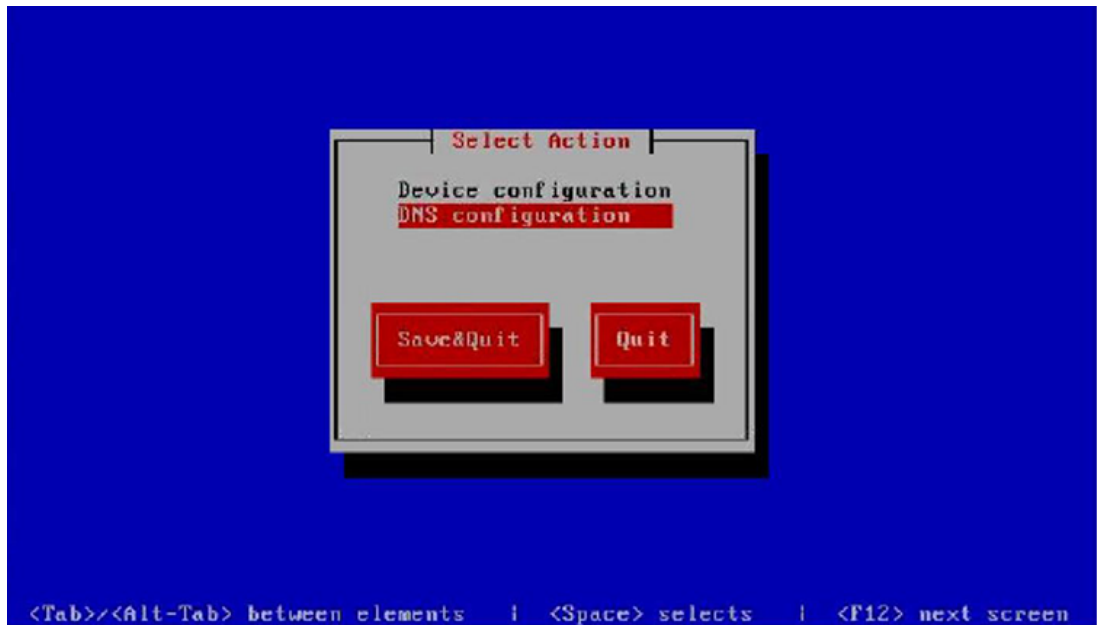
Setting new password for *cmxadmin*
Password:
Confirm: _

```

354126

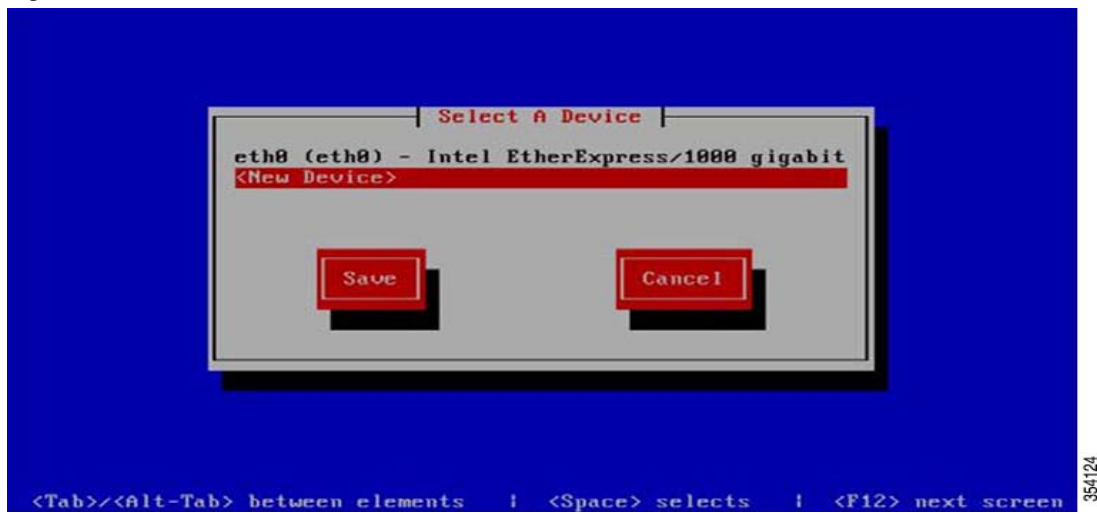
- Step 5** Click **Device Configuration**.

Figure 1-9 Device Configuration



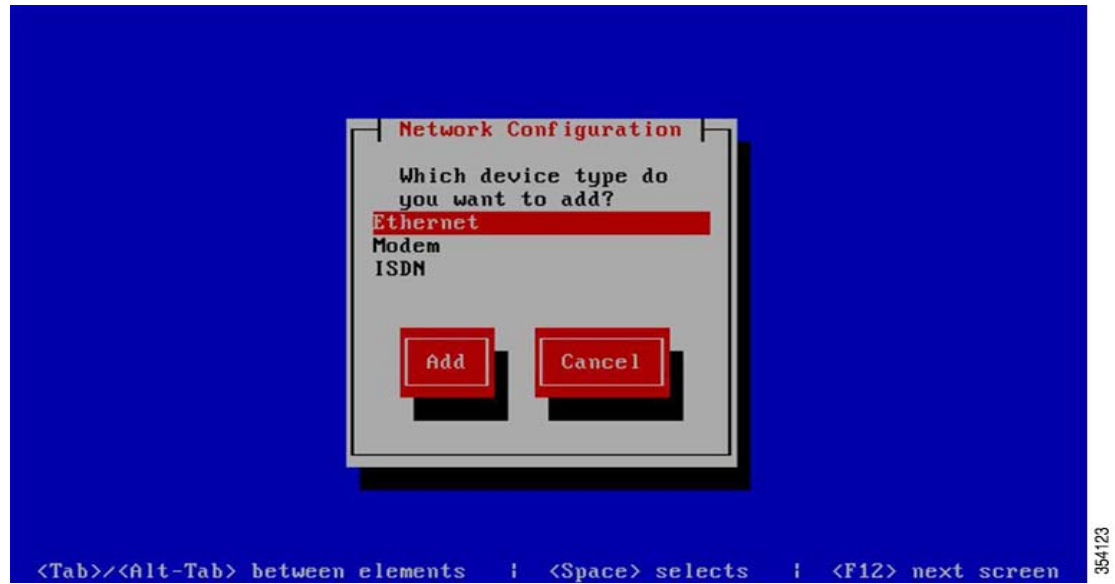
Step 6 Click <New Device>.

Figure 1-10 New Device



Step 7 Click Ethernet.

Figure 1-11 Network Configuration

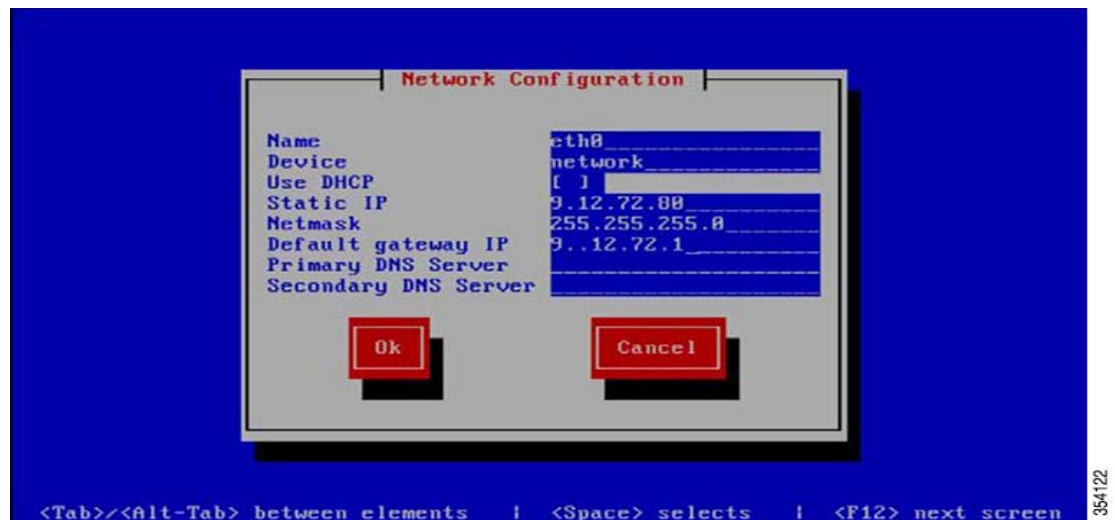


**Step 8** Enter the hostname, device name, IP address, network mask, and gateway and click **Ok**.

**Note**

- Changing the hostname through command line is not supported. You should use the **cmxos reconfigure** command to change the hostname or, IP addresses, or any of the network parameters.
- Do not enter DNS details. The DNS server information entered here is not used by the system. These details **MUST** be entered in the DNS configuration menu.
- See [Step 10](#) for DNS details.

Figure 1-12 Network Configuration Details

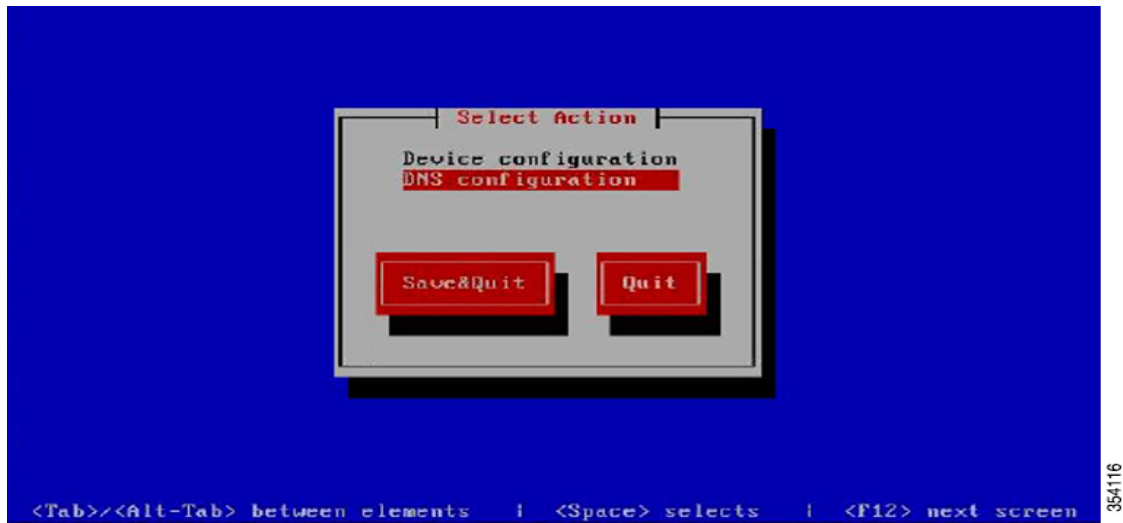


**Step 9** Click **DNS Configuration**.

**Note**

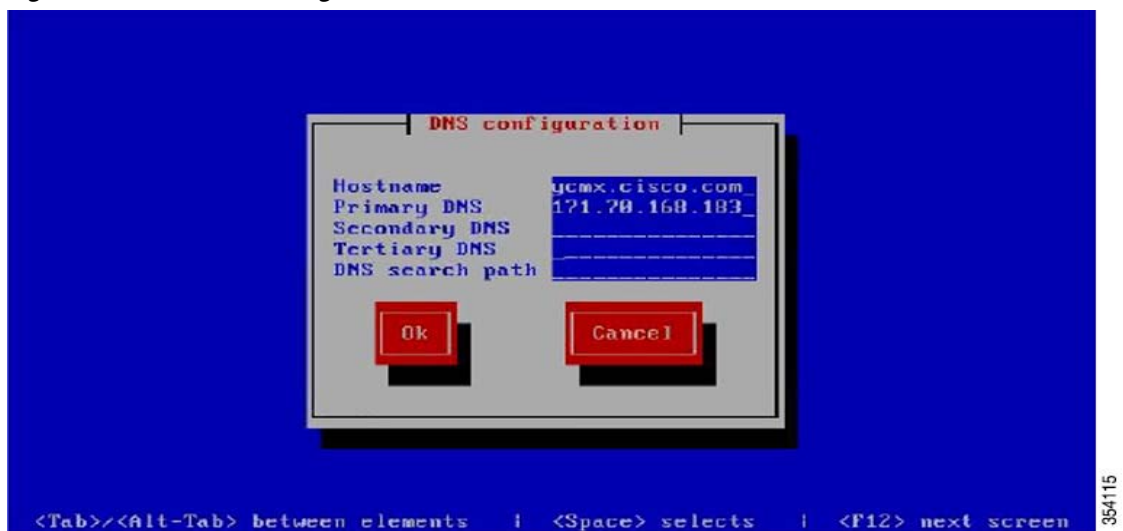
The DNS configuration is optional.

Figure 1-13 DNS Configuration



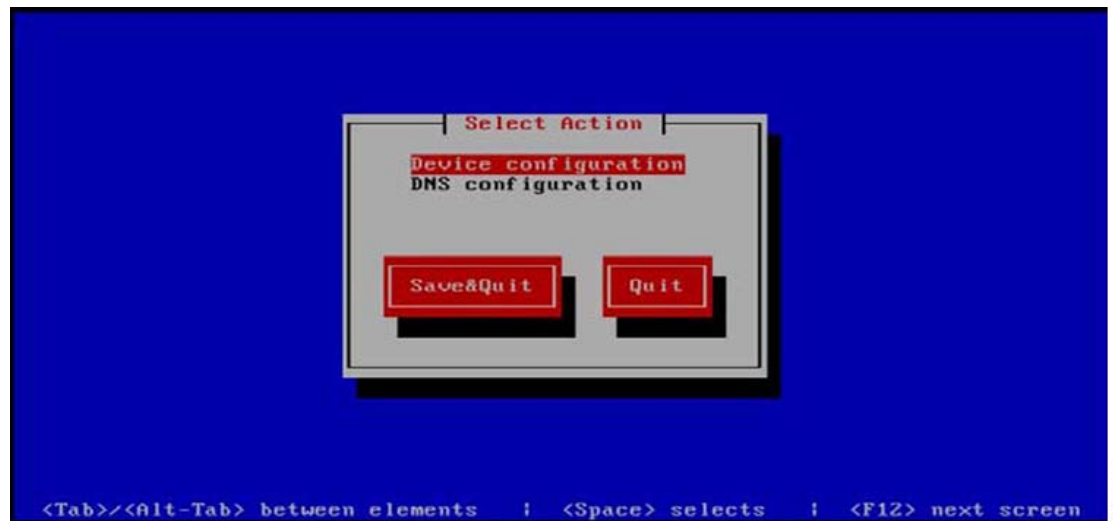
Step 10 Enter the **Hostname**, **DNS** and **DNS search path** default domain.

Figure 1-14 DNS Configuration Details



Step 11 Click **Save&Quit**.

Figure 1-15 Select Action



- Step 12** Enter the NTP server name or IP address. The setup validates whether sufficient compute resources are available and prompts for either an NTP server or system-time configuration, besides asking for NTP details. Even if you skip NTP configuration, we strongly recommend that you use the NTP server.

**Note**

If the NTP server is unreachable, use 127.0.0.1 as the server address during installation.

Figure 1-16 NTP Server Details

```

Pinging 172.19.34.1.... Success
Network configuration completed successfully
-----
Configuring NTP Server...
Please enter the NTP server name (blank for no NTP server) []: ntp.esl.cisco.com
Pinging ntp.esl.cisco.com.... Success
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.

**Note**

After time zone information is verified the operating system configuration is completed, but not the Cisco CMX services installation.

Figure 1-17 Time Zone

```

Enter nameserver: 171.78.168.183
*****
Configuring ntp...
*****
Checking for ntp:
The ntp server is not configured
please enter the ntp server name:: 172.19.28.258
updating ntpd config ...
*****
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** Finally, the setup will ask you to go to the admin URL (For example, [https://CMX10.2\\_IP:1984](https://CMX10.2_IP:1984). For further setup. See the “[Installing Cisco CMX Using Web Interface](#)” section on page 1-16 for details.

## Installing Cisco CMX Using Web Interface

To install Cisco CMX using web interface, follow these steps:

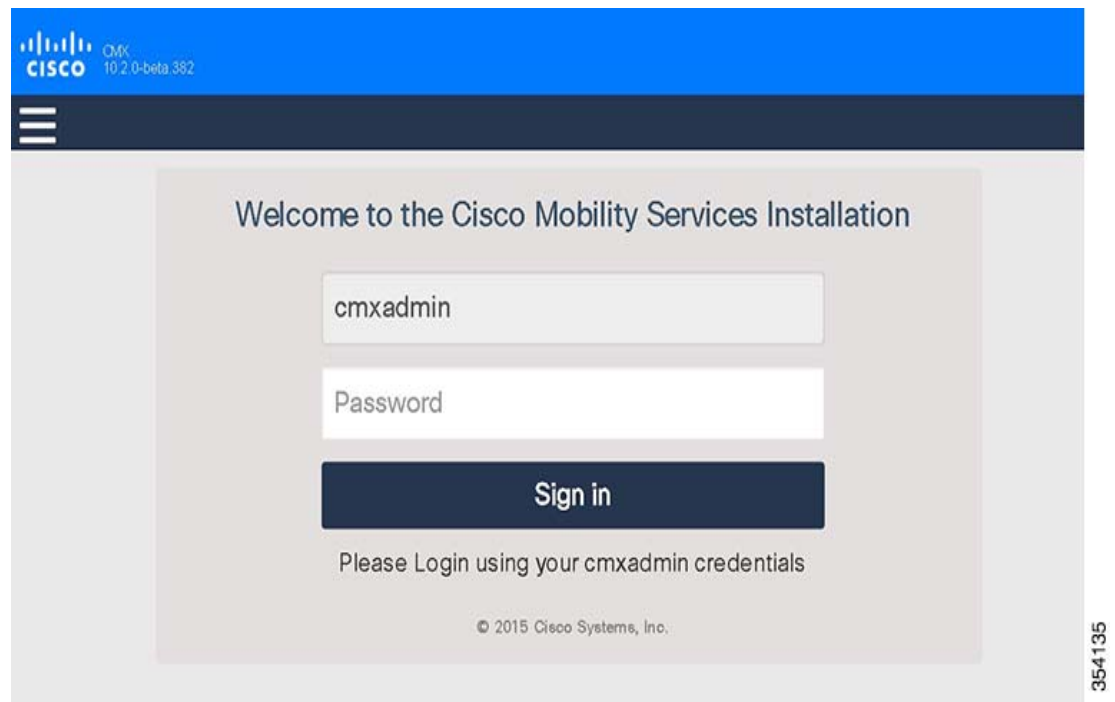
- Step 1** In the Cisco CMX web interface, enter the login credentials (Cisco CMX admin credentials) and press **Sign In** to continue.



**Note** The only available login is `cmxadmin`, with the password you configured during the initial power on of the system. Contact the Cisco MSE installation admin for the VM IP details to access the Cisco CMX web interface for the first time.



**Figure 1-18** Cisco CMX Web Interface



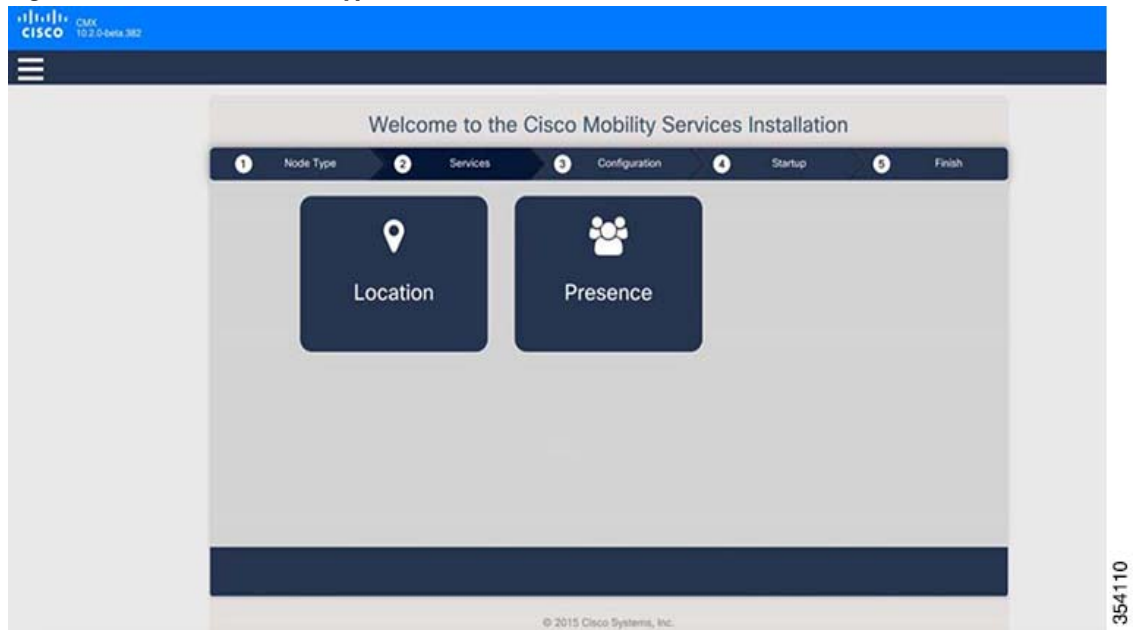
**Step 2** Choose the Cisco CMX type as either **Location** or **Presence**.

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

- DETECT & LOCATE
- ANALYTICS
- CONNECT & ENGAGE
- MANAGE
- SYSTEM

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

- PRESENCE ANALYTICS
- CONNECT & ENGAGE
- MANAGE
- SYSTEM

**Figure 1-19** Cisco CMX Type Selection

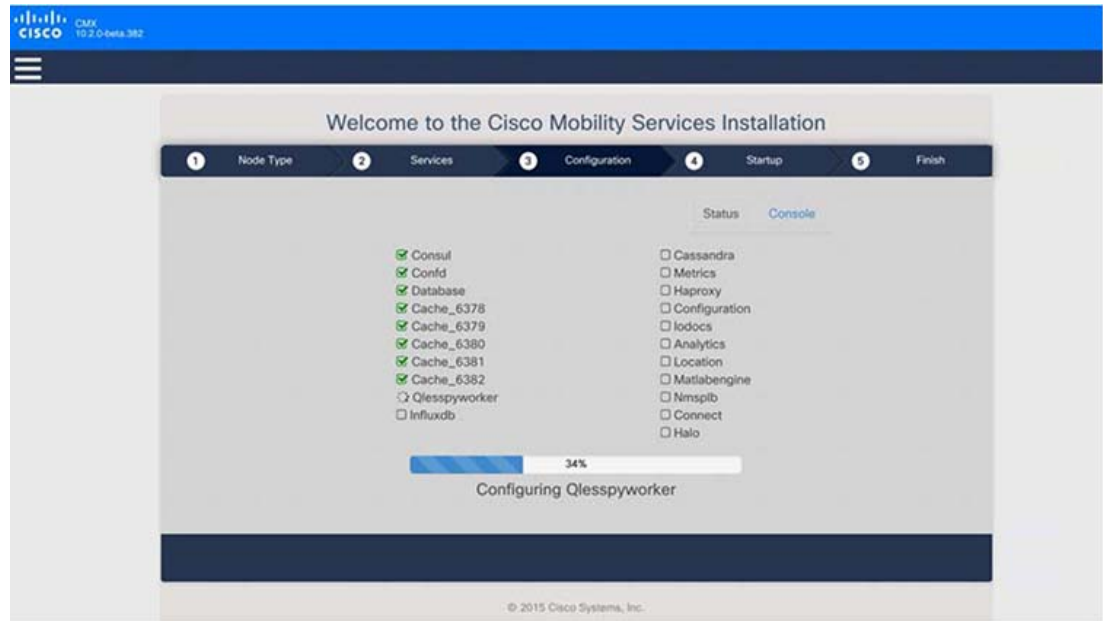
**Note** If Cisco CMX services are already installed, the login process takes you to the Cisco CMX services upgrade options.

**Step 3** The installation is initiated and starts all the services, which takes a few minutes to complete.

The following is the sequence of events:

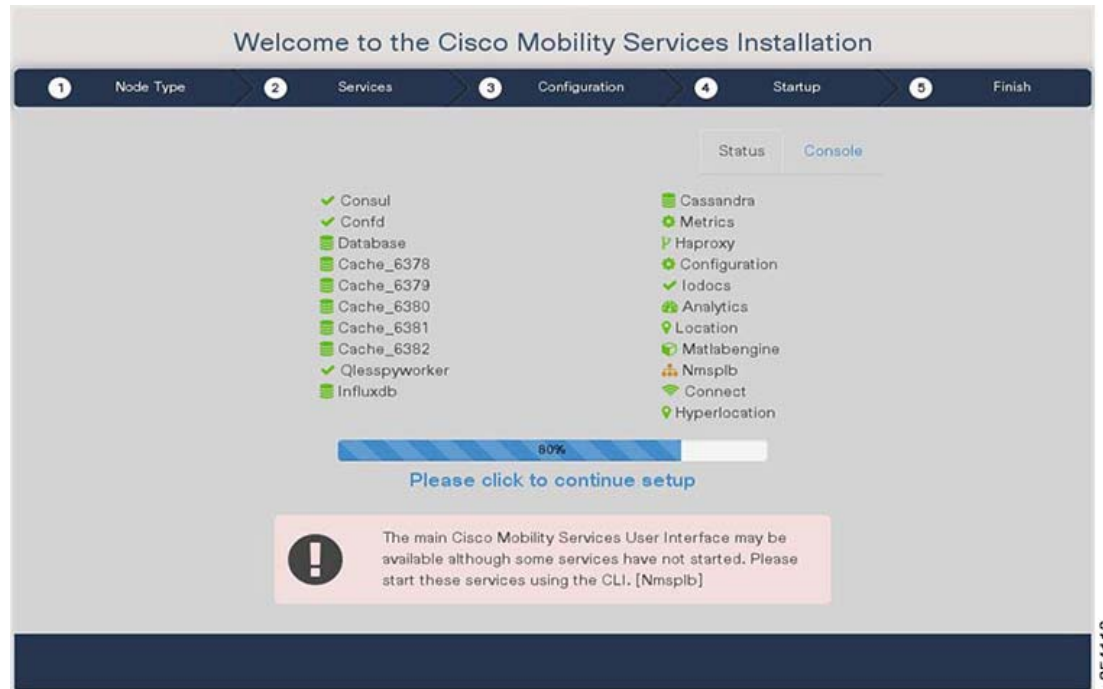
1. Consul Configuration
2. DB Installation
3. Schema Migration
4. InfluxDB Configuration
5. Cassandra Installation
6. Node Registration

**Figure 1-20 Services Installation Progress**



**Step 4** After the services are started, continue to the main portal by clicking the blue text (Please click to continue setup) or by pressing **Enter**.

**Figure 1-21 Installation Completion**

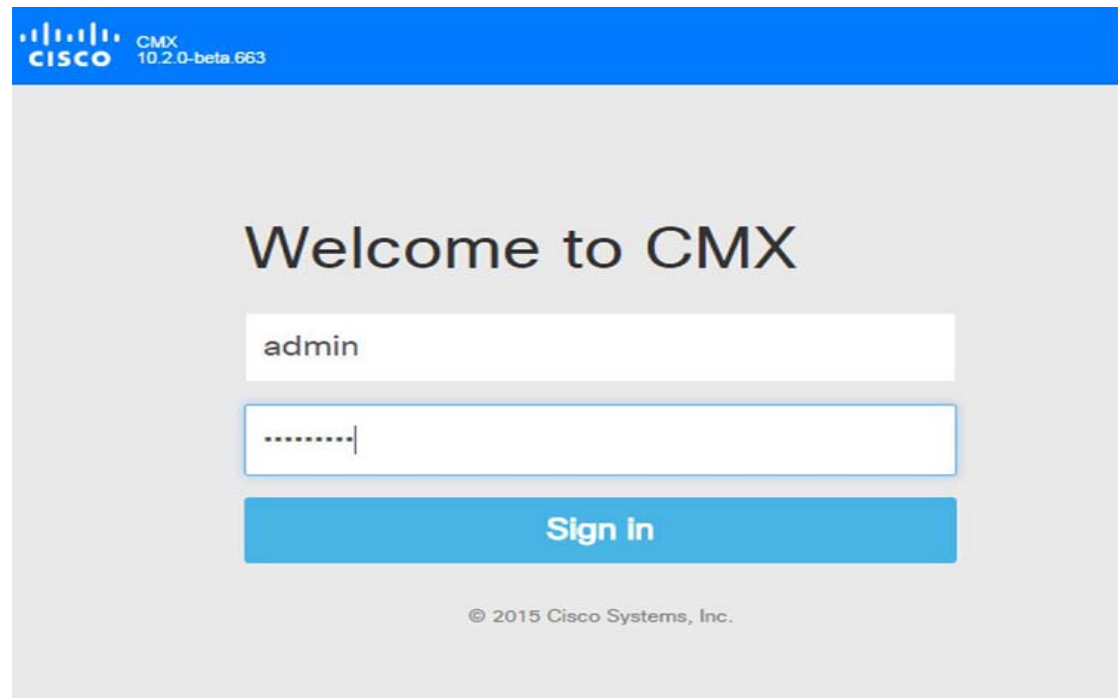


**Note** You can monitor the progress of the installation through either the graphical status display or the console (display only) output.

The installation is completed and the Cisco CMX Welcome window is displayed. The Welcome window is displayed only for a reinstall and not for fresh install. After the fresh install, the user is directly logged in to Cisco CMX, without having to enter user credentials.

**Step 5** Login with the username and password (admin and admin).

**Figure 1-22** Cisco CMX Welcome Page



**Step 6** After the installation, the Setup Assistant displays the GUI configuration window, which you can use to configure Maps, Controllers, and Mail Server. For more information, see, [Configuring the GUI](#) section.

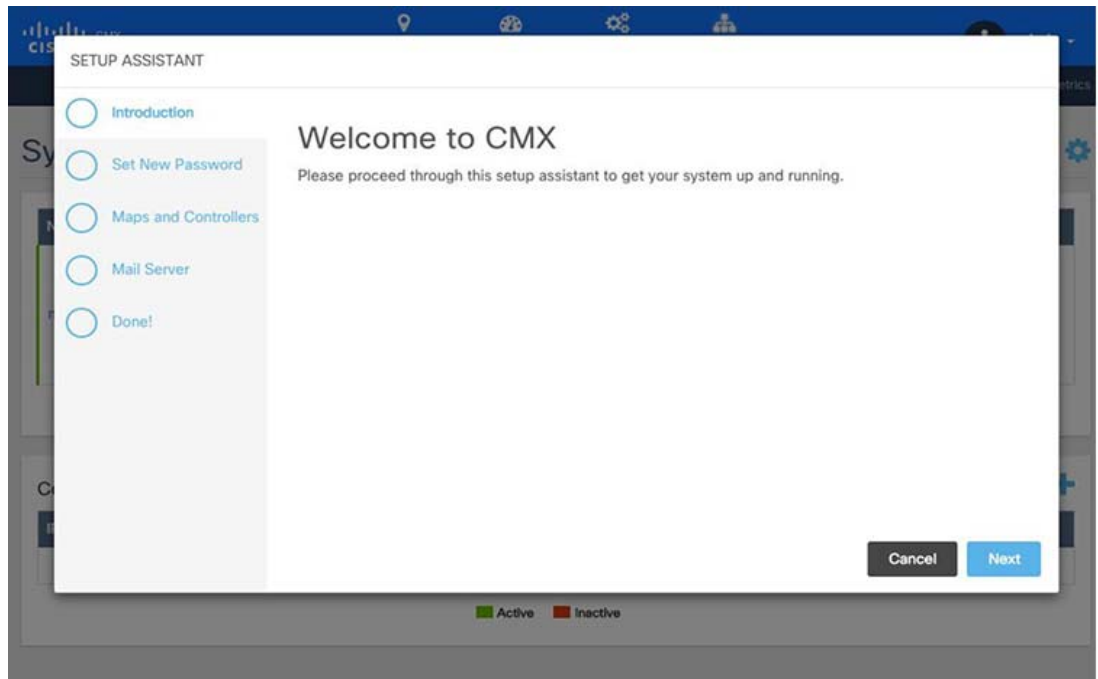


**Note** In Cisco CMX 10.2, the Cisco CMX initial configuration is now completed via a web user interface rather than the CLI. The Setup Assistant is used to perform the initial configuration, which requires you to set a password for the admin user, import controllers and maps from Cisco Prime Infrastructure, and configure and test mail server settings.



**Note** Use `https://<ip address>` for subsequent logins to the web user interface because `https://<ip-address>:1984` is used only for initial configuration.

Figure 1-23 Setup Assistant



# Upgrading Cisco CMX 10.2 to Future Releases

You can upgrade Cisco CMX 10.2 to future releases using the Cisco CMX web interface.



**Note**

The web interface upgrade is applicable only for upgrades from 10.2 to future releases of Cisco CMX, for example, to upgrade from 10.2.0 to 10.2.1 or 10.3. The web interface cannot be used for upgrades from 10.1.x to 10.2.0.



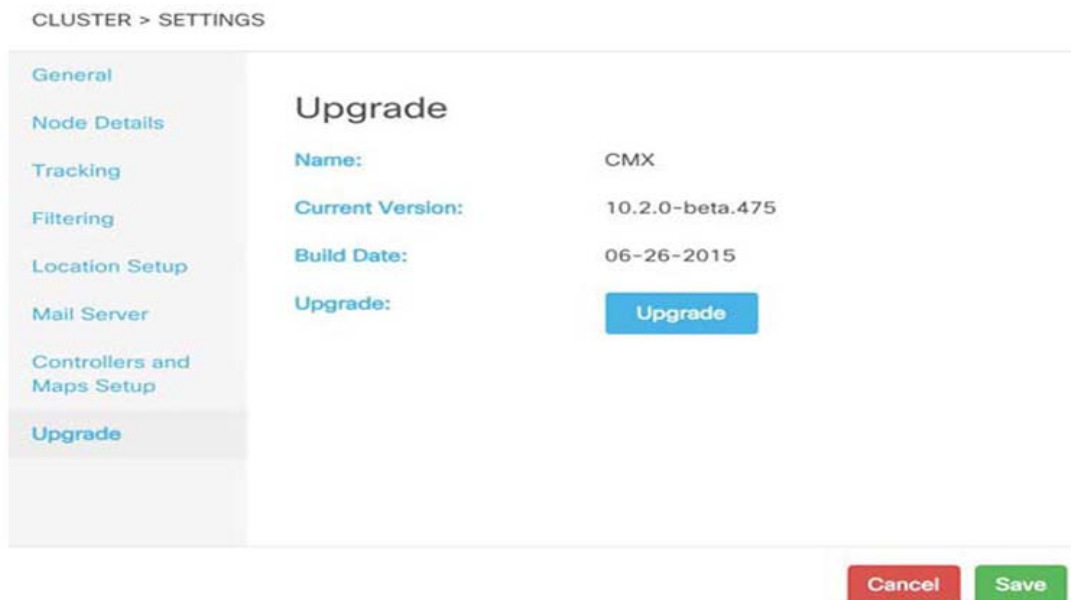
**Note**

After upgrading from Cisco CMX 10.1 to 10.2, or from 10.2 to a future release, clear the cache of your browser before launching the Cisco CMX Connect UI. Failure to do so will result in the portal not being upgraded and the Cisco CMX Connect features not working properly.

To upgrade Cisco CMX using web interface, follow these steps:

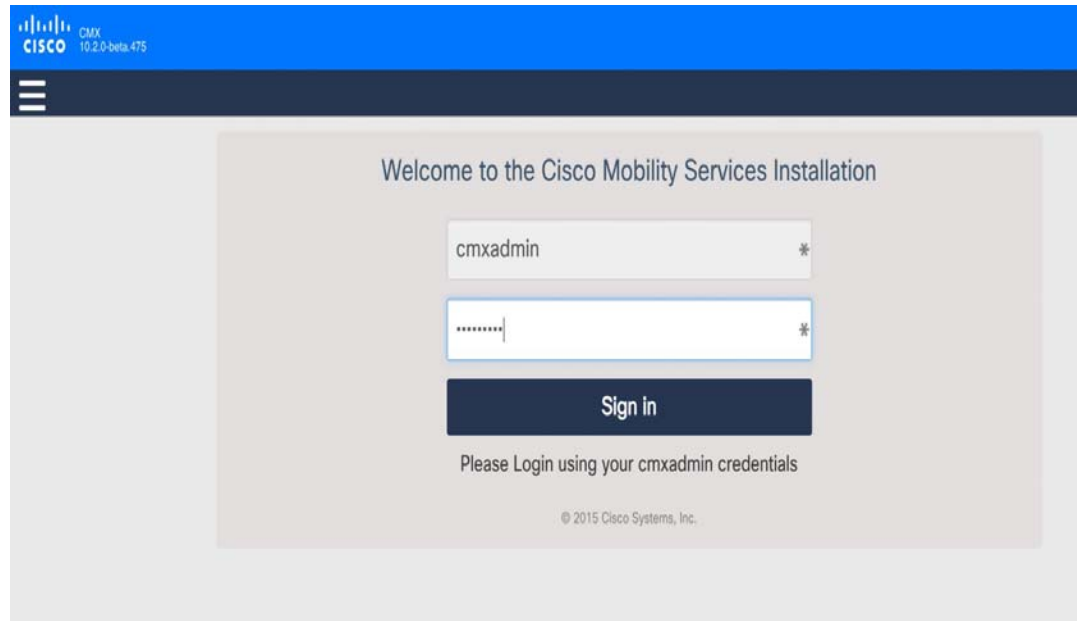
- Step 1** Log in to the Cisco CMX web interface.
- Step 2** Choose **SYSTEM > Dashboard**.  
The **System at a Glance** window is displayed.
- Step 3** Click the **Gear** icon at the top right corner of the **System at a Glance** window.  
The **SETTINGS** window is displayed.
- Step 4** In the left pane of the **SETTINGS** window, click **Upgrade**.

**Figure 1-24** Cisco CMX Upgrade

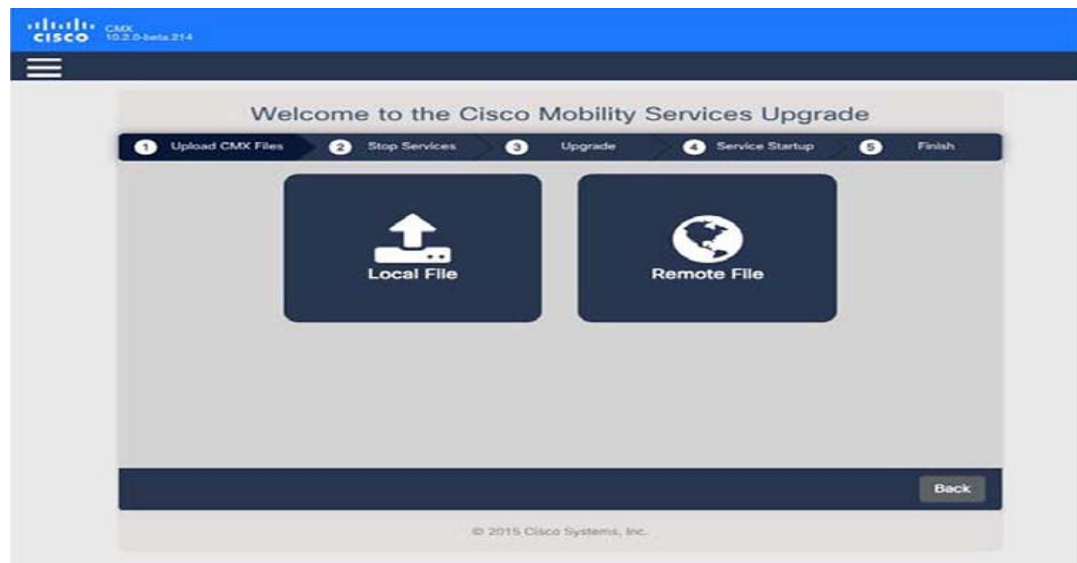


354133

- Step 5** Enter the Cisco CMX admin password and click **Sign In**.

**Figure 1-25 Login Credentials**

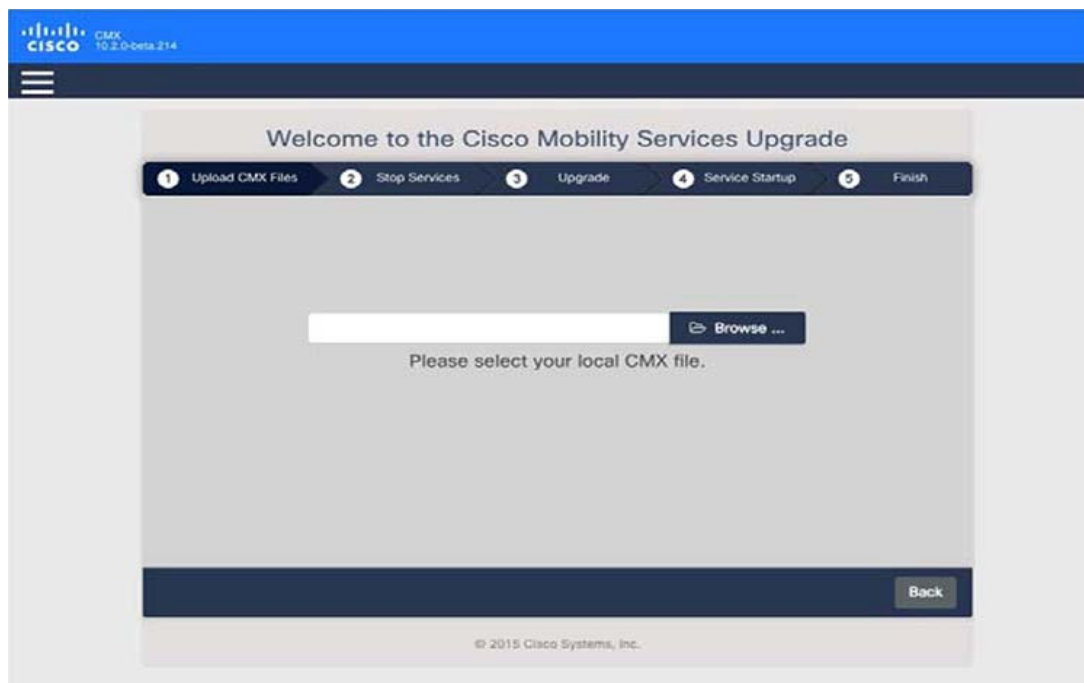
**Step 6** Click either **Local File** or **Remote File**.

**Figure 1-26 Upgrade Options**

**Step 7** Depending on your selection, one of the following windows will be displayed:

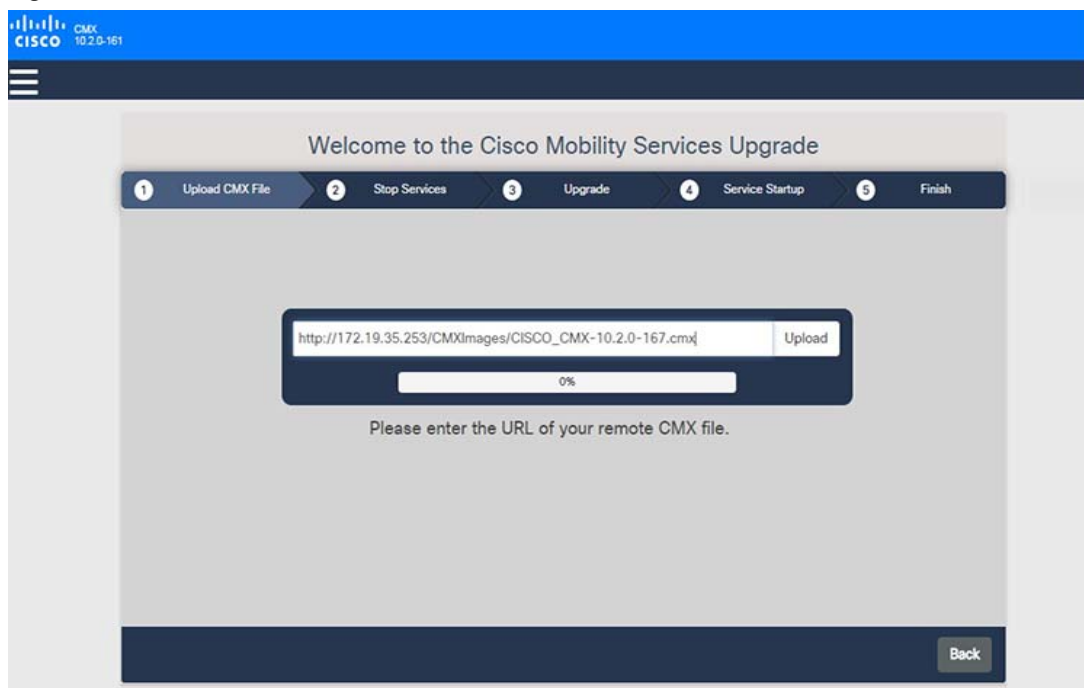
- a. For the **Local File** option, click **Browse** to select the local Cisco CMX file. In order to be able to do this, ensure that the .cmx file is available on the machine from which you are accessing the web user interface.

**Figure 1-27 Local Cisco CMX File Selection**



b. For the **Remote File** option, enter the URL of the installation file.

**Figure 1-28 Remote Cisco CMX File Selection**

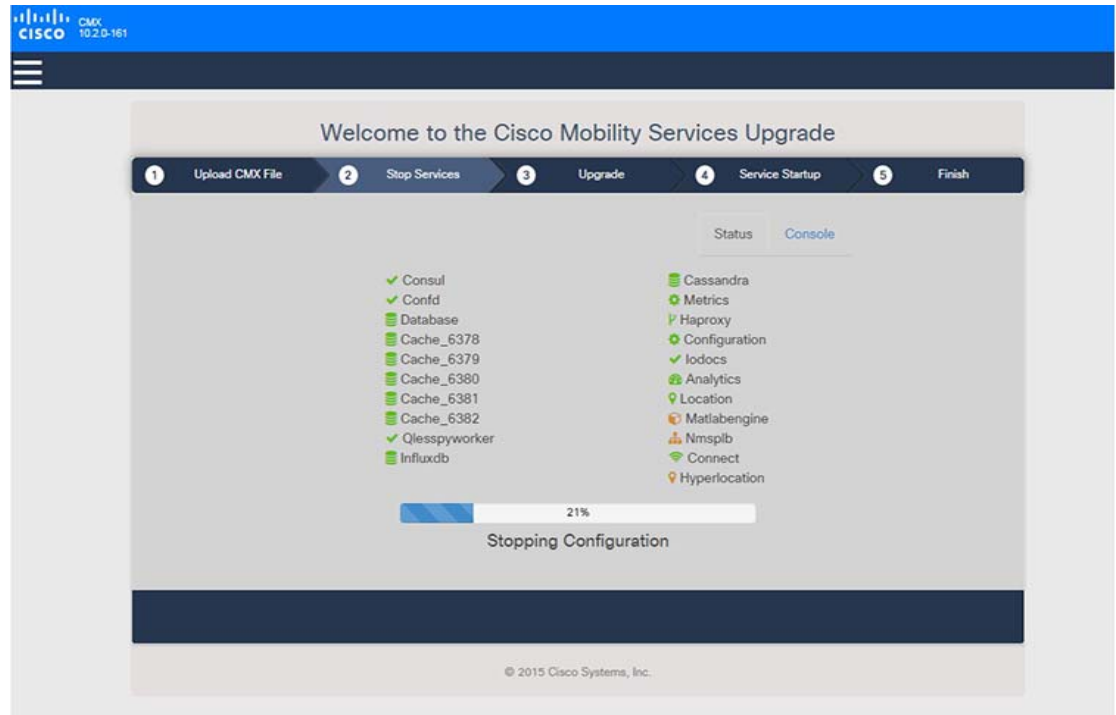


**Step 8** Click **Upload**.

**Step 9** After the file is uploaded completely, the upgrade process is initiated.

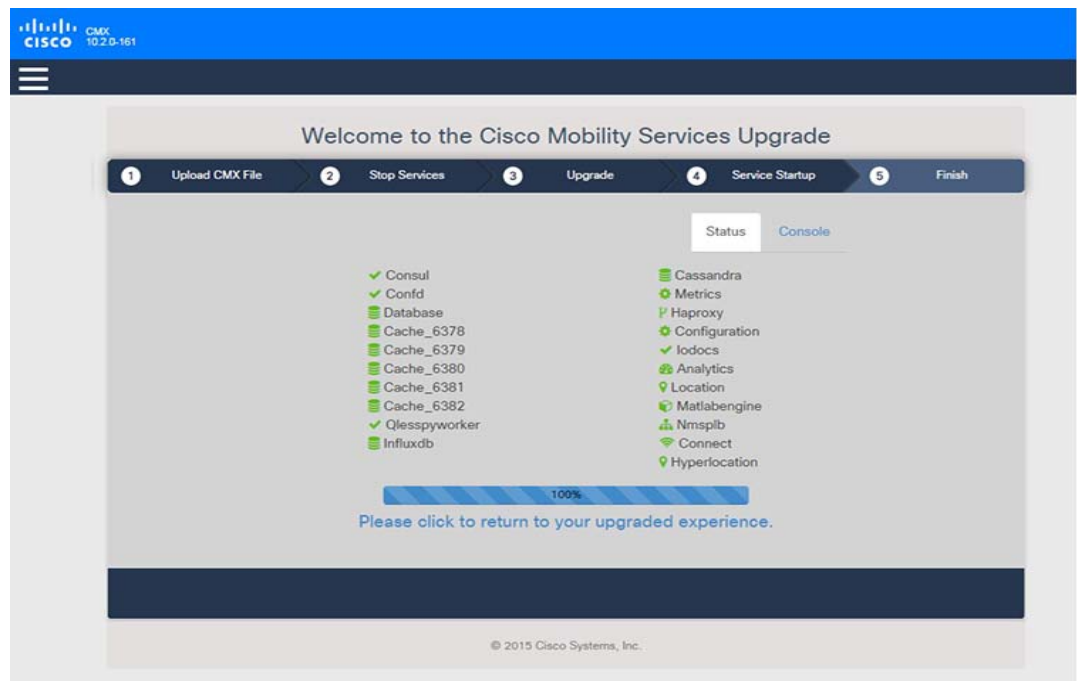


**Figure 1-29 Cisco CMX Upgrade**



**Step 10** After the upgrade is complete, the following window is displayed. Click the blue text (Please click to return to your upgraded experience) to go to the Cisco CMX Welcome page, and login using the username and password (admin and admin).

**Figure 1-30 Upgrade Completion Window**



## Upgrading a Cisco CMX 10.1.x Deployment to 10.2

The upgrade from Cisco CMX 10.1 to Cisco CMX 10.2 is accomplished through the use of a helper script and a .cmx file

To perform the upgrade, perform the following steps:

- 
- Step 1** Download the .cmx file and the helper script as a .zip file from CCO.
- Step 2** Unzip the downloaded file.
- Step 3** Connect to the Cisco CMX CLI via SSH or CIMC KVM.
- Step 4** Move to the root directory: `cd /`
- Step 5** Create a folder to hold the script and .cmx file.  
**mkdir upgrade**
- Step 6** Move to the newly created upgrade directory  
**cd /upgrade**
- Step 7** Use the Secure Copy Protocol to transfer both the cmx\_upgrade.sh script and its associated .cmx file to the upgrade folder on the existing 10.1 installation:  
**scp username@hostname\_or\_IP:/Users/username/Downloads/<CISCO\_CMX\$\$\$>.cmx> .**




---

**Note** Ensure that you enter the space and the period at the end of the command.

---

- Step 8** Ensure that both the script and the .cmx file can be executed by the root user:  
**chmod +x cmx\_upgrade.sh**  
**chmod +x <CISCO\_CMX\$\$\$>.cmx>**
- Step 9** Run the upgrade script by entering the following at the CLI prompt:  
**./cmx\_upgrade.sh <CISCO\_CMX\$\$\$>.cmx>**
- 

## Verifying the Cisco CMX Services

Use the System tab of the Cisco CMX 10.2 user interface to verify the overall system health, including the status of the Cisco CMX services.

The **System** tab contains four 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.

In the **System** tab Dashboard, make sure that all the services, memory, and CPU have a healthy status (green) for each Cisco MSE and Cisco CMX node, and that there is at least one active Cisco WLC.





## Virtual Machine Setup and Administration

---

This chapter contains the following sections:

- [Adding a Hard Disk to a Virtual Machine in the vSphere Client, page 2-1](#)
- [Configuring the Network, page 2-1](#)

### 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.

For more information, see: [Add a Hard Disk to a Virtual Machine in the vSphere Client](#).

### 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.

For more information, see: [Configuring Networking for Host Machines in the vSphere Web Client](#).

