



Installing Software for the Cisco Extended Care Application Server

The Cisco Extended Care application server installation process consists of the following tasks that are described in this chapter:

1. [Creating a Virtual Machine, page 2-1](#)
2. [Installing Cisco Extended Care on a Virtual Machine, page 2-4](#)
 - a. [Verifying the Installation, page 2-8](#)
 - b. [Changing the Password, page 2-9](#)
3. [Setting Up the Network Time Protocol \(NTP\), page 2-9](#)
4. [Synchronizing the JVM Time Zone, page 2-10](#)
5. [Generating the SSL Certificate for the Data Center Server, page 2-11](#)



Note

Refer to your server vendor's documentation for remote management configuration.

Creating a Virtual Machine

- If this is a multi-tenancy environment, create one VM for every tenant, up to a maximum of five.
- If this is a single-tenant environment, you still need to create one VM to take advantage of the high availability feature.

In both cases, after you create the VM, install the appropriate Cisco Extended Care Server software in the VM, and then set up NTP.



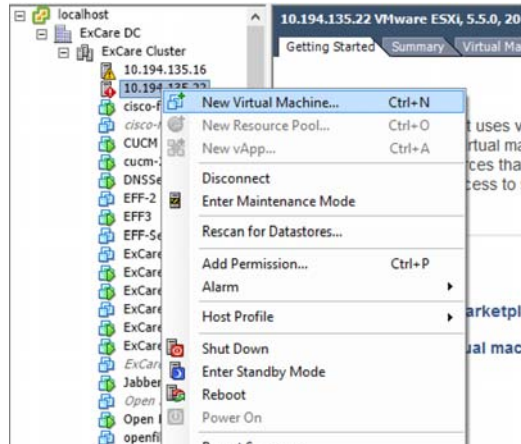
Note

- If you do not have vSphere Client installed on your system, download the vSphere Client from the EXSi server, and run the installer.
- Screen images are for reference purpose only and may change if you are using other clients like the vSphere web client.

To create a VM in a host, perform the following steps:

- Step 1** Right-click the host's IP address on the left. One of the two drop-down menus shown in [Figure 2-1](#) appears.

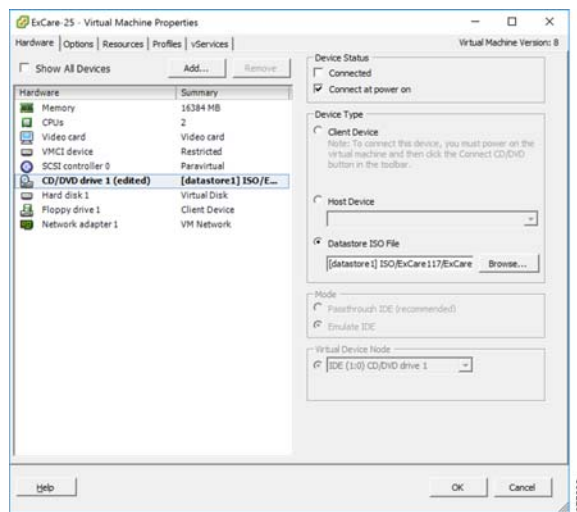
Figure 2-1 Create New Virtual Machine



- Step 2** Click **New Virtual Machine** from the drop-down menu. The **Create New Virtual Machine** window appears.
- Step 3** Select the **Custom** check box. Then, click **Next**. The **Name and Location** window appears.
- Step 4** Enter the name for the new virtual machine. Then click **Next**. The **Datastore** window appears.
- Step 5** Select the data store you want to use for this virtual machine. (For high availability, it should be the NFS server you installed.) Click **Next**. The **Virtual Machine Version** window appears.
- Step 6** Select the **Virtual Machine Version: 8** check box. Click **Next**. The **Guest Operating System** window appears.
- Step 7** Select **Linux** and choose **Red Hat Enterprise Linux 6 (64-bit)** from the drop-down menu. Click **Next**. The **CPUs** window appears.
- Step 8** Choose **2** as the number of core processors from the drop-down menu. Click **Next**. The **Memory** window appears.
- Step 9** Enter the memory size (16 GB). Click **Next**. The **Network** window appears.
- Step 10** From the following drop-down menus:
1. How many NICs do you want to connect? Choose **1**.
 2. NIC 1: Choose **VM Network**.
 3. Adapter: Choose **E1000**.
- Select the **Connect at Power On** check box. Click **Next**. The **SCSI Controller** window appears.
- Step 11** Select the **LSI Logic Parallel** check box. Click **Next**. The **Select a Disk** window appears.
- Step 12** Select the **Create a new virtual disk** check box.
- Step 13** Click **Next**. The **Create a Disk** window appears.
1. Specify the Disk Size as 100 GB. The large disk size is required to store log files. Older log files are purged, but only after a limit is reached.
 2. Select the **Allocate and commit space on demand (Thin Provisioning)** check box.
 3. Select the **Store with the virtual machine** check box.

4. Click **Next**. The **Advanced Options** window appears.
- Step 14** Select the **SCSI (0:0)** check box. (Do not select the **Independent** check box.) Click **Next**. The summary appears.
- Step 15** Select the **Edit the virtual machine settings before completion** check box. Click **Continue**. The **Virtual Machine Properties** window appears.
- Step 16** Select the **New CD/DVD (adding)** check box to indicate that you want to boot this virtual machine from a CD.
- Step 17** Click **Datastore ISO File** and choose the ISO file.
- Step 18** Select the **Connect at power on** check box as shown in [Figure 2-2](#).

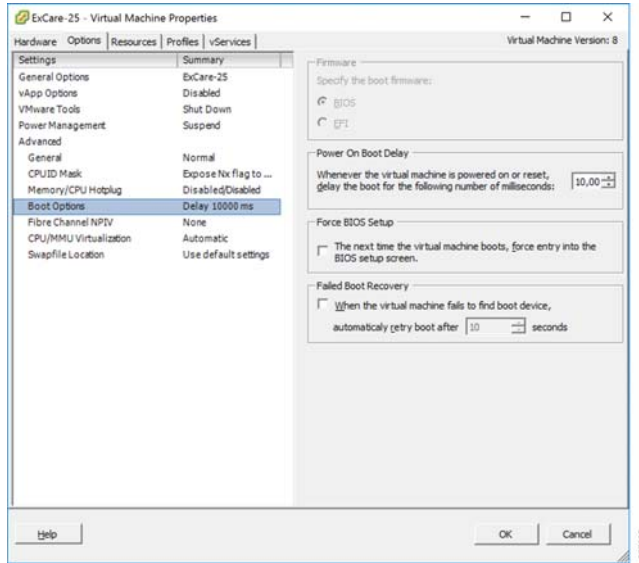
Figure 2-2 Booting from CD/DVD



Warning

If you do not select the **Connect at power on check box, the CD drive does not connect to the VM and the system fails to boot.**

- Step 19** Select **Options > Boot Options**. Increase the value in the **Power On Boot Delay** field.

Figure 2-3 Power On Boot Delay

Step 20 Click **OK**.

Step 21 To view the VM you just configured, click the VM in the left pane of the main window and click the **Summary** tab.

Installing Cisco Extended Care on a Virtual Machine

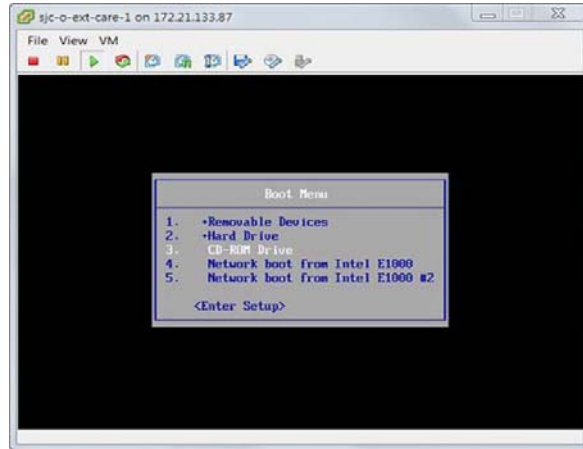
This section describes the installation process of the Cisco Extended Care application server software on a VM.

To install the application server, perform the following steps:

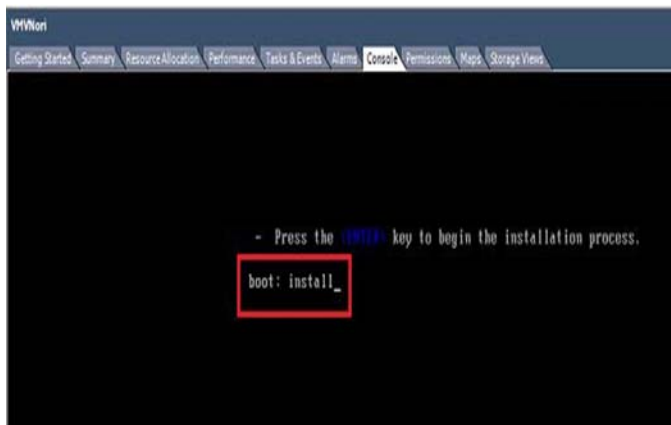
Step 1 Click the VM you configured in the left pane of the main window, and power the VM on.

Figure 2-4 Power On the VM

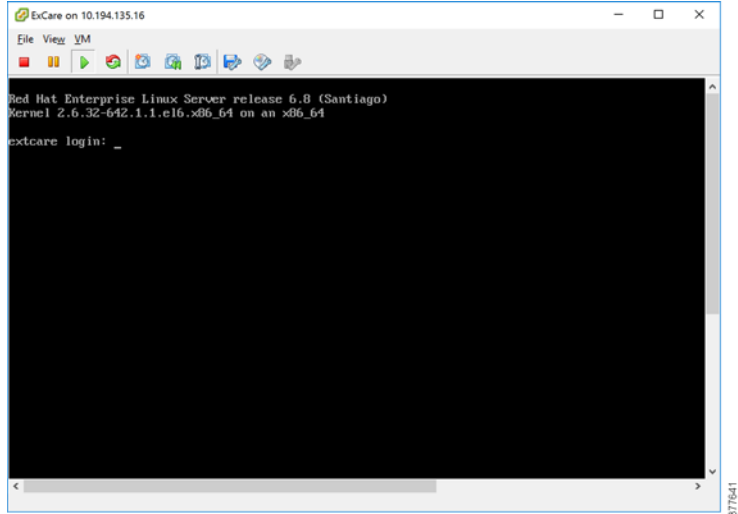
Step 2 Click the **Console** tab, then click into the window, and press the **Esc** key to bring up the boot menu.

Figure 2-5 Boot Menu

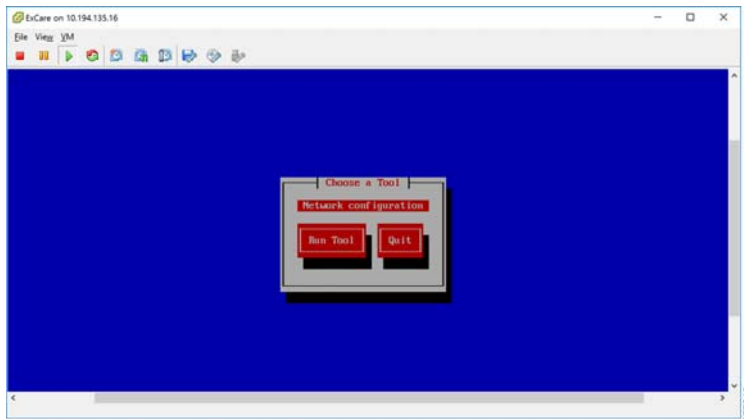
- Step 3** Use the up and down arrow keys to navigate to the CD-ROM Drive option, and then press **Enter**.
- Step 4** Enter the following command: **#install**.

Figure 2-6 Initiate Install Process

- Step 5** Press **Enter**. The installation process starts and takes several minutes to complete.
- Step 6** After the installation process is completed, log in to the server with the following credentials:
- Login: root
 - Password: changeit

Figure 2-7 Log in to the VM

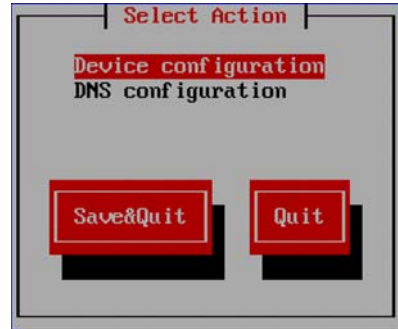
Step 7 After you are logged in, enter the following command: **setup** to set up the network configuration. Then, press **Enter**. The **Choose a Tool** window appears.

Figure 2-8 Setup Network Configuration

Note Use the arrow keys, tab key, and the enter key on your keyboard to navigate through the subsequent pages.

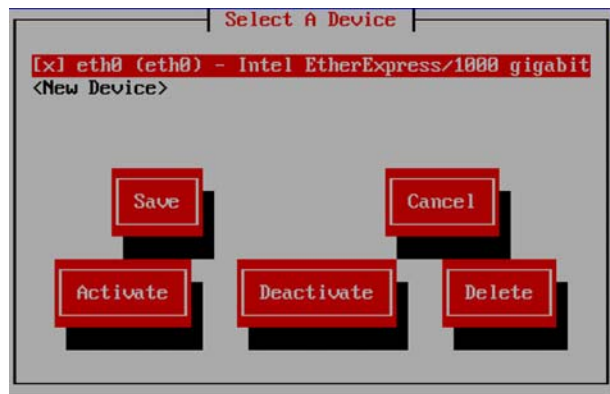
Step 8 Use the tab key to select **Run Tool**, and press **Enter**. The **Select Action** window appears.

Figure 2-9 Select Action Window



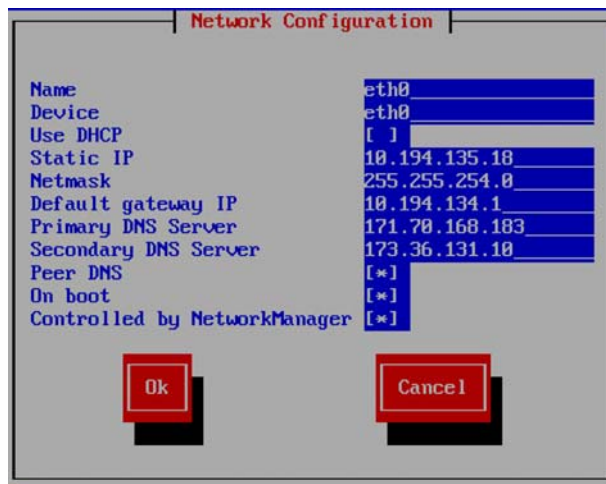
Step 9 Use the tab key to select **Device Configuration**, and press **Enter**. The **Select a Device** window appears.

Figure 2-10 Select a Device Window



Step 10 The default device is already selected. Press **Enter**. The **Network Configuration** window appears.

Figure 2-11 Network Configuration Window

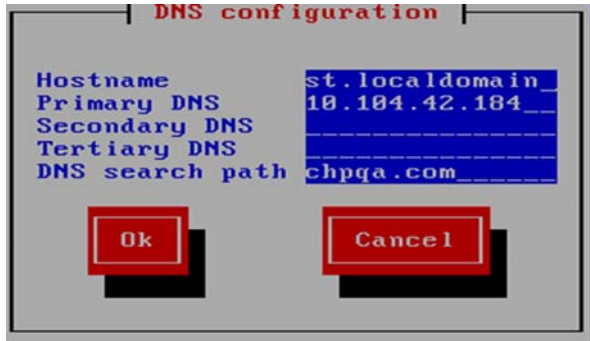


Step 11 Enter the appropriate network configuration details. Use the tab key to select **OK**, and then press **Enter**. The **Select a Device** window appears.

Step 12 Use the tab key to select **Save**, and then press **Enter**. The device configuration details are saved. The **Select Action** window appears.

- Step 13** Use the tab key to select **DNS Configuration**, and then press **Enter**. The **DNS configuration** window appears.

Figure 2-12 DNS Configuration Window



- Step 14** Enter the appropriate DNS configuration details. Use the tab key to select **OK**, and then press **Enter**. The DNS configuration details are saved. The **Select Action** window appears.
- Step 15** Use the tab key to select **Save&Quit**, and then press **Enter**. The Choose a Tool window appears.
- Step 16** Use the tab key to choose **Quit**, and then press **Enter**.
- Step 17** Reboot the server/VM by entering the following command: **#reboot**.

Upgrading the Extended Care Server

The following steps are used to upgrade extended care server:

- Step 1** Download the upgrade files from cisco.com and copy it to the */opt* folder on the Extended Care server.
- Step 2** Extract the zip file.
- Step 3** Add execute permissions to *upgrade-extcare-XXX.sh* - `chmod 777 upgrade-extcare-XXX.sh`.
- Step 4** Run the upgrade script - `./upgrade-extcare-XXX.sh`.
- Step 5** Check the *upgrade-extcare.log* for any errors.
- Step 6** Log in to the **Admin** page and then check the **About** page.
- Step 7** Verify the new version in the Web UI.

Verifying the Installation

To verify the server installation, perform the following steps:

- Step 1** After the server boots up, verify that you can log into the server as a root user via ssh.
- Step 2** Verify that the services are running using the following command: **# service cec status**.

The command output for the Cisco Extended Care application server should be:


```

Apache is running.
Tomcat is running.
MySQL is running.

```

Changing the Password

To change the password, perform the following steps:

-
- Step 1** After the server boots up, verify that you can log into the server as a root user via SSH.
 - Step 2** Enter the following command: # **passwd**.
 - Step 3** Enter the new password in the **New Password** field, and then press **Enter**.
 - Step 4** Re-enter the new password in the **Retype New Password** field, and then press **Enter**. The password is updated.
-

Setting Up the Network Time Protocol (NTP)



Note

All UC-related servers and the EC application server must be NTP synchronized. For example, if you are using VCS and MCU with the EC application server, they both should be NTP synchronized. The reset session timer will execute at the proper time only when the server time is in sync with the NTP timing.

To set up NTP, perform the following steps:

-
- Step 1** Open the file `/etc/ntp.conf` for editing.
 - Step 2** Add the following line to the top of the `ntp.conf` file: **tinker panic 0**
 - Step 3** Locate the following lines in the file:


```

server 0.rhel.pool.ntp.org iburst
server 1.rhel.pool.ntp.org iburst
server 2.rhel.pool.ntp.org iburst

```

These represent the Red Hat NTP servers. Ideally, you should use NTP servers within close proximity to your data center. While these work, they are not the best choice.
 - Step 4** Add the # character at the beginning of each of these the lines to make them comments. They should now appear as follows:


```

# server 0.rhel.pool.ntp.org iburst
# server 1.rhel.pool.ntp.org iburst
# server 2.rhel.pool.ntp.org iburst

```
 - Step 5** Add an entry for the NTP server with which this server will sync time. (These should be listed in the NIP.) The entry should look similar to these:


```

server [ip_addr_ntp_server1]

```

```
server [ip_addr_ntp_server2]
server [ip_addr_ntp_server3]
```

Step 6 Save and exit editor.

Step 7 Open the following file for editing: */etc/ntp/step-tickers*

Step 8 Add a server entry for each of the NTP servers with which this server will sync time, as listed in the NIP. The entries should be similar to the following:

```
[ip_addr_ntp_server1]
[ip_addr_ntp_server2]
[ip_addr_ntp_server3]
```

Step 9 Click **Save** and then close the file.

Step 10 Run the following command to sync the server time with one of the NTP servers.

```
# ntpdate -u <one of the NTP servers>
```

For example, to sync time with a server, you would enter: **# ntpdate -u 1.ntp.companyx.com**

appears:

```
29 Apr 16:42:29 ntpdate[5748]: adjust time server 171.68.10.80 offset 0.000016 sec
```

Step 11 Repeat Step 10 until the offset value is less than 1 second.

Step 12 Run the following command to start NTP after a server reboot: **# chkconfig ntpd on**

Step 13 Run the following command to start the NTP service: **# service ntpd start**

The command output should be: Starting ntpd: [OK]

Step 14 After about 15-20 minutes, verify that NTP is syncing time with the other NTP servers using the following command: **# ntpq -np**

The output will be similar to the following (there will be one line printed for every server):

```
remote          refid          st t when poll reach delay  offset  jitter
*17.151.16.20   17.107.131.11  2  u 227m 1024 0    6.578  6.692  0.001
```

At least one server should have a '*' character in front of its name. The delay, offset and jitter values should be non-zero.

Synchronizing the JVM Time Zone

In the ISO build, the JVM time zone should be in sync with the VM time zone.

Whenever the user changes the VM time zone, the user has to manually run the following script to keep JVM time zone in sync with the updated VM/OS time zone.

```
vi /etc/sysconfig/clock
```

Update the following settings:

```
ZONE="{server timezone}"
UTC=false
ARC=false
Write and Exit (:wq)
```

```
service cec restart
```

To synchronize time, use the following command:

```
hwclock --systohc --localtime
```

Use the "hwclock" command to check status of hardware clock:

Generating the SSL Certificate for the Data Center Server

This section describes how to generate the Secure Socket Layer (SSL) certificates for the Data Center servers.

**Note**

Before performing this procedure, determine if your installation uses the Domain Name Server (DNS) or IP addresses at the endpoints to identify the Data Center servers.

To install OpenSSL signed certificate, perform the following steps:

Step 1 SSH/console into the server and run the following commands, with the desired server address:

```
export SERVER_IP=<Server Address>
sudo openssl genrsa -out /etc/pki/tls/private/localhost.key 4096
```

**Note**

For netcaler use encryption key - 2048 instead of 4096.

```
sudo openssl req -new -key /etc/pki/tls/private/localhost.key -subj "/CN=${SERVER_IP}" -out
/etc/pki/tls/certs/localhost.csr
```

Step 2 Submit the contents of `/etc/pki/tls/certs/localhost.csr` to the certificate signer.

**Note**

Request the certificate in BASE64 fFormat.

Step 3 After you receive the signed certificate from the certificate signer, place it in `/etc/pki/tls/certs/localhost.crt`.

Step 4 Restart Apache HTTPD via `sudo service httpd restart`.