



Cisco Modeling Labs ISO Installation

- [Cisco UCS C-Series Server Installation, page 1](#)
- [Prepare the Cisco Integrated Management Controller \(CIMC\) Interface, page 2](#)
- [Access the CIMC Interface, page 6](#)
- [Map the Cisco Modeling Labs ISO Disk Image, page 9](#)
- [Run the VIRT Installer, page 12](#)
- [\(Optional\) Prepare for an Interface-Constrained Installation, page 27](#)
- [Reconfigure Default Console Resolution, page 29](#)
- [Launch the User Workspace Management Interface, page 30](#)
- [Determine License Key Requirements, page 41](#)

Cisco UCS C-Series Server Installation

Cisco Modeling Labs can be run natively on Cisco UCS compute platform without an underlying ESXi hypervisor. Referred to as a bare-metal deployment, the installation requires the ISO installation file downloaded and accessible to the installation workstation. Bare metal deployments are exclusively supported on Cisco UCS products. The following UCS C-Series servers are supported:

- Dual Socket servers for small to medium sized deployments:
 - Cisco UCS C220-M3
 - Cisco UCS C220-M4
 - Cisco UCS C240-M3
 - Cisco UCS C240-M4
- Quad Socket servers for larger deployments that demand higher number of CPU-cores than can be supported on the dual socket variants:
 - Cisco UCS C460-M3
 - Cisco UCS C460-M4

Cisco Modeling Labs has relatively modest storage requirements, with a 250GB capacity (or larger) Direct Attached Storage disk (DAS) recommended. RAID configurations are optional. When using a RAID configuration on the UCS C-Series server, the hardware based (MRAID module) version is the recommended method.

Storage Area Network (SAN) options are beyond the scope of this installation guide. SAN options are not supported for Cisco Modeling Labs bare metal deployments on Cisco UCS C-Series.

If the Cisco UCS C-Series server is being freshly deployed, there are some preliminary preparations that are necessary to prepare the hardware. These include configuring the server's dedicated management interface (CIMC); verifying that the necessary Virtualization Technology features are enabled in the BIOS; and preparing the storage for the installation. The following steps are associated with the Cisco UCS C220 M4S platform running Version 2.06(6d) BIOS/CICM firmware. Refer to the applicable documentation if other server types or firmware levels are to be used and adjust the process accordingly.

Prepare the Cisco Integrated Management Controller (CIMC) Interface

If not previously used, the server's Cisco Integrated Management Controller (CIMC) must be provisioned as follows:

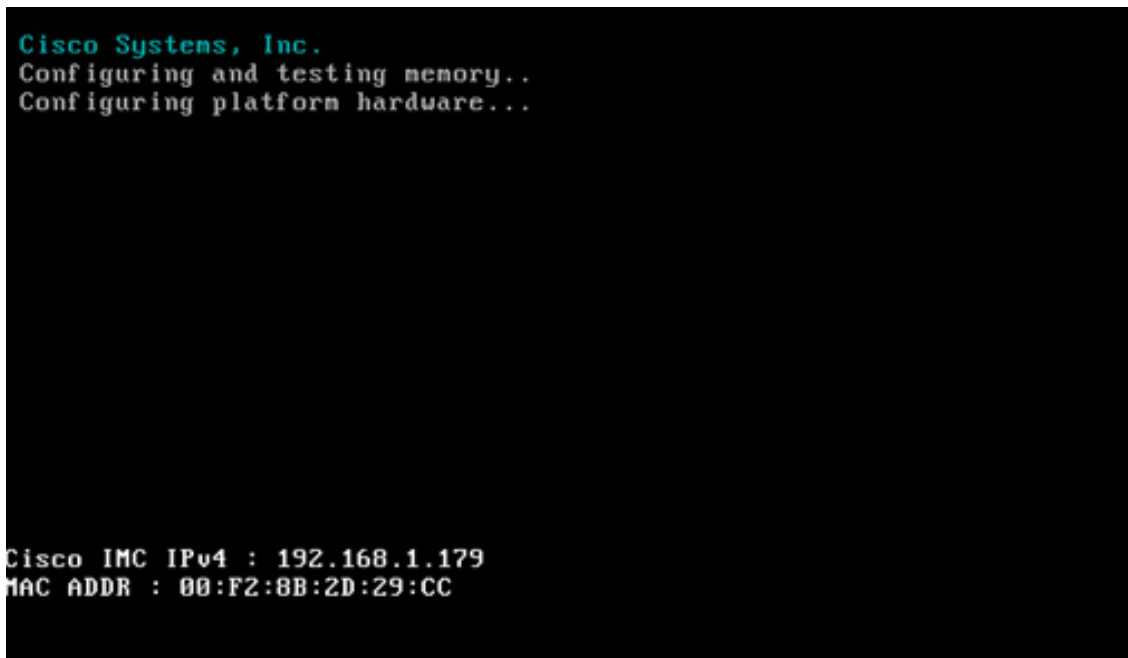
-
- Step 1** Connect a USB keyboard and VGA monitor to the server using one of the following methods:
- a) Using the corresponding connectors on the rear panel.

b) Using the optional KVM cable (Cisco PID N20-BKVM) to the connector on the front panel.

Step 2

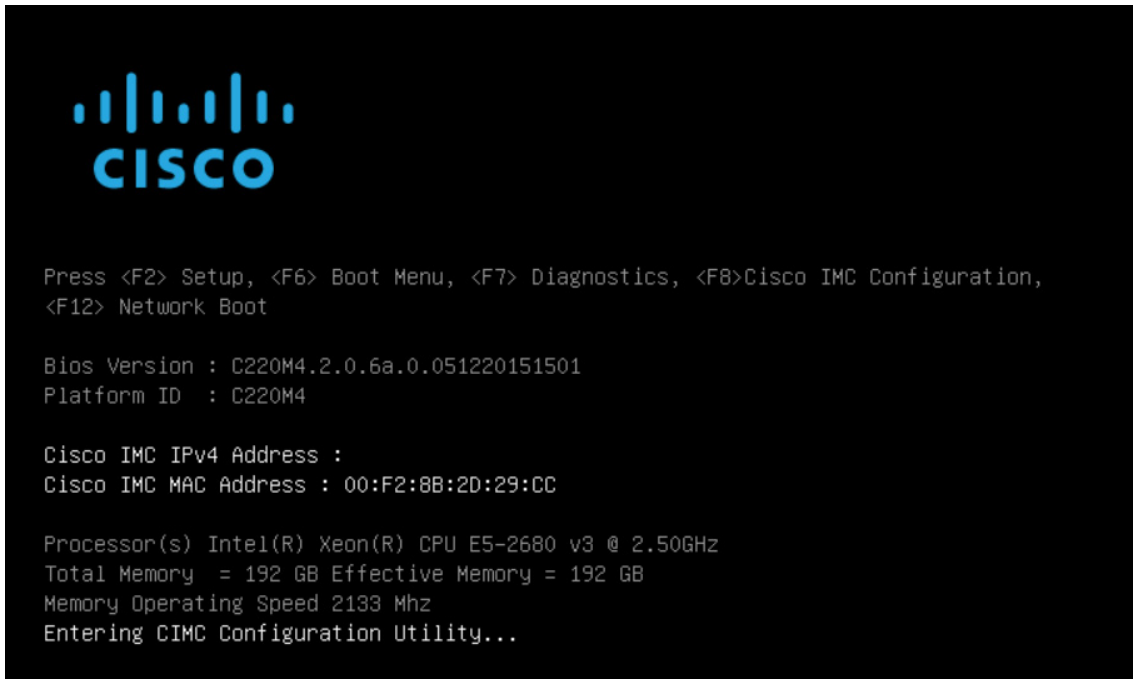
Power on the server via the front panel **Power** button. The server will undergo its Power-On Self Testing (POST) cycles and hardware initializations, as shown.

Figure 1: Power-On Self Testing Cycles and Hardware Initialization



Step 3 When the POST cycles finish, the server setup menu is presented. Press the <F8> key to enter the Cisco IMC Configuration Utility.

Figure 2: Cisco Setup Menu



- Step 4** In the Cisco IMC Configuration Utility, enter the networking details to be assigned to the server's dedicated management port. Use the <Up>/<Down> arrow keys to select parameter, and the <Space> key to toggle on/off.

Figure 3: CIMC Configuration Utility

```

Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
NIC Properties
NIC mode                               NIC redundancy
Dedicated:      [X]                    None:           [X]
Shared LDM:     [ ]                    Active-standby: [ ]
Cisco Card:    Active-active:         [ ]
  Riser1:      [ ]                    VLAN (Advanced)
  Riser2:      [ ]                    VLAN enabled:   [ ]
  MLom:        [ ]                    VLAN ID:        1
Shared LDM Ext: [ ]                    Priority:       0
IP (Basic)
IPV4:          [X]                    IPV6:          [ ]
DHCP enabled   [ ]
CIMC IP:       192.168.1.179
Prefix/Subnet: 255.255.255.0
Gateway:       192.168.1.1
Pref DNS Server: 0.0.0.0

*****
<Up/Down>Selection  <F10>Save  <Space>Enable/Disable  <F5>Refresh  <ESC>Exit
<F1>Additional settings

```

412698

Typical settings are to set **NIC mode** to **Dedicated** and to set **NIC redundancy** to **None**. Configure IP addressing and VLAN details per site requirements. Press the <F10> key to save the entries and continue the boot process.

- Step 5** If not already done, connect the server's dedicated management port to its adjacent access switch. From a Windows (or Apple) client machine, verify network connectivity to the CIMC host interface.

Access the CIMC Interface

With the CIMC interface configured, it is accessed to complete the machine preparation and to facilitate the software installation.

Step 1 Using a Windows (or Apple) workstation, initiate a browser session to the CIMC interface using the address provisioned in the previous steps.

Step 2 In the CIMC login page, enter the username and password for the CIMC interface. The default credentials are admin and password. If the password was changed during server setup, use the currently configured password.

Figure 4: CIMC Interface

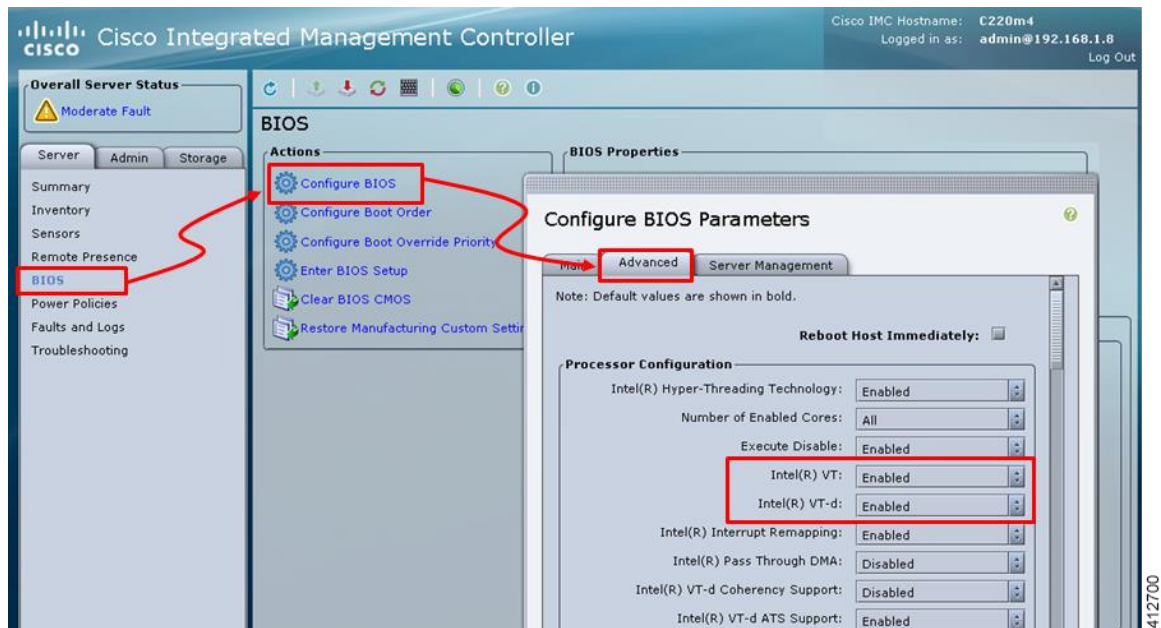


Step 3 At this point, BIOS CPU Virtualization Technology (VTx) features may be verified, as follows:

- a) Choose **Server > BIOS**.
- b) Choose **Actions > Configure BIOS**

- c) In the pop up window, select the **Advanced** tab. For Cisco UCS platforms, the VT extensions should be enabled by default, as shown.

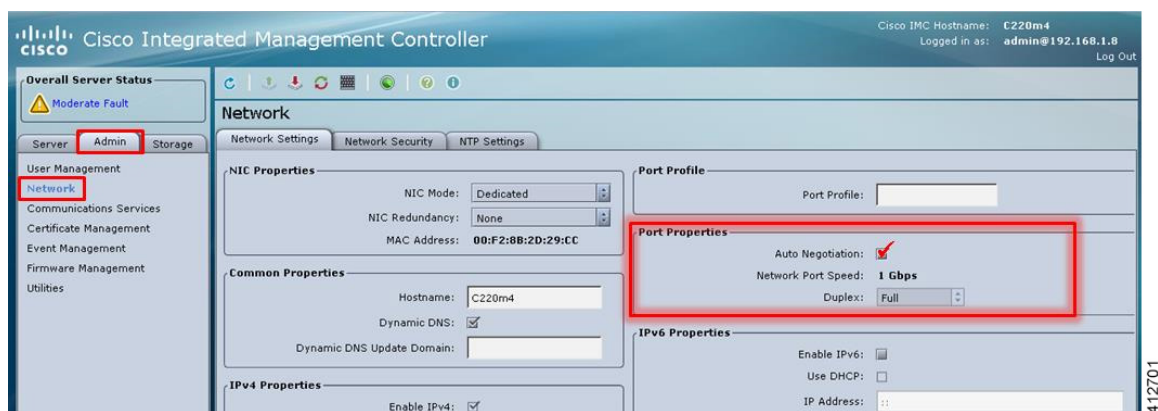
Figure 5: Verify BIOS Configuration



Step 4

Verify the CIMC network configuration is set for best performance. Select **Network** under the **Admin** tab. Enable the management port's **Auto Negotiation**. By default, the port may be set for 100mbps/Half Duplex; this will severely impair the ISO file transfer process.

Figure 6: Verify Network Configuration



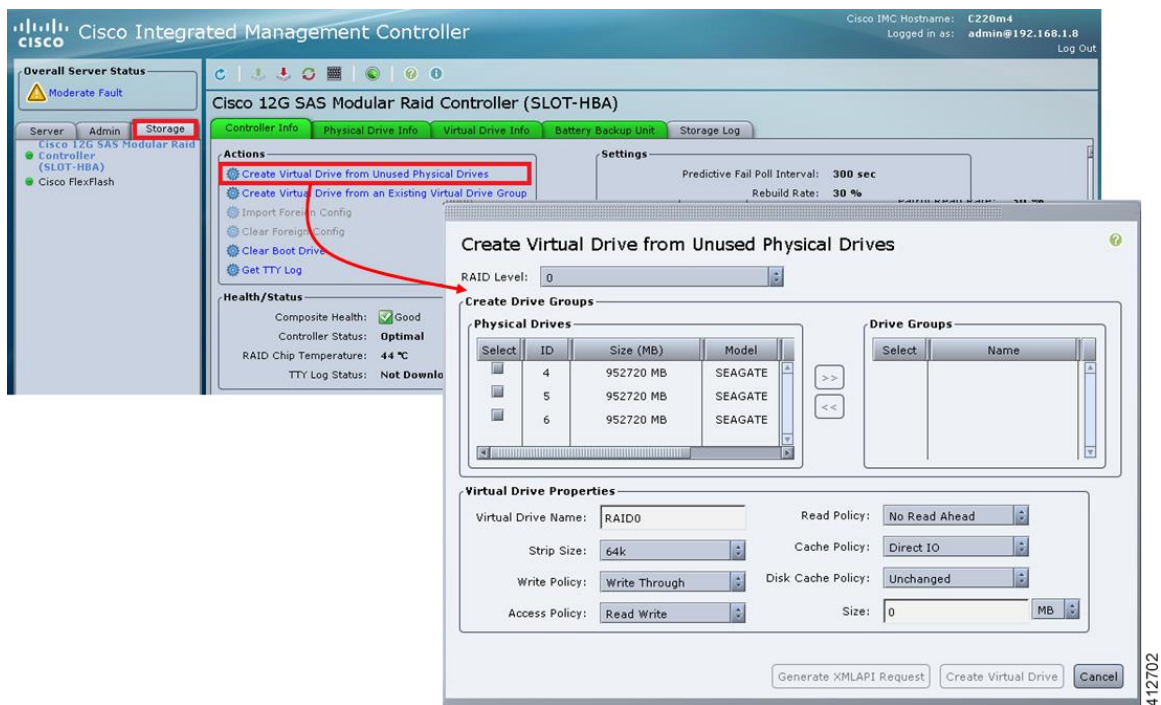
Step 5

If this is a new machine, the storage sub-system may need to be set up and initialized. As there are a wide variety of options with respect to storage, the exact deployment details will depend on the employed storage components utilized. For specific installation procedures, review product documentation and feature descriptions associated with actual storage

options. The following illustrates the most common Direct Attached Storage (DAS) using the integral MRAID module. To configure the MRAID controller:

- A pre-boot utility may be invoked by entering <Ctrl-R> during the boot-up process. This will directly access the on-board ROM-based configuration utility.
- Within the CIMC interface, select the **Storage** tab to display the Modular Raid Controller. Under the **Controller Info** tab, click the **Create Virtual Drive from Unused Physical Drives** option. In the popup window, choose the desired RAID level from the drop-down menu. In the list of **Physical Drives**, select the participating member(s) by clicking the **Select** box, as shown.

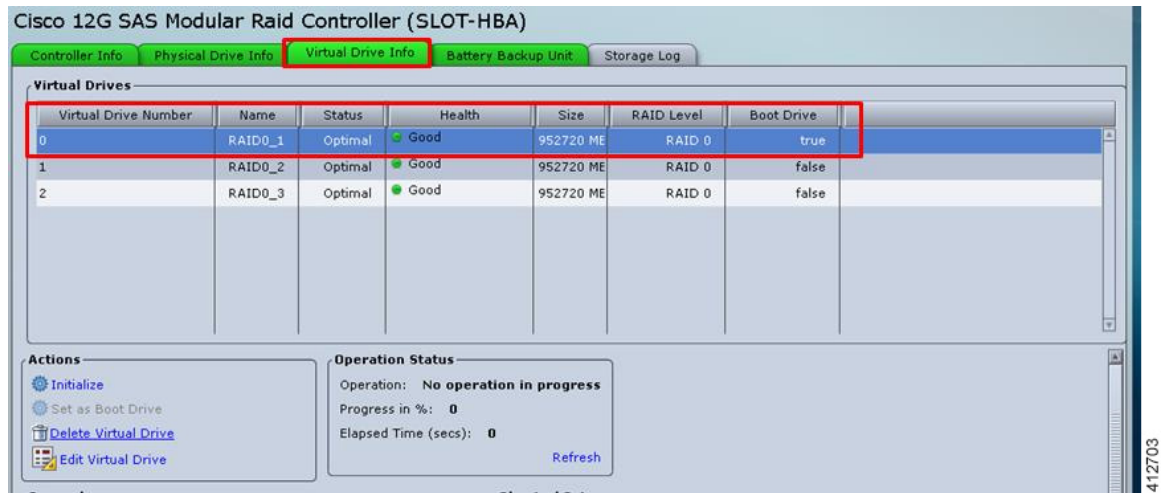
Figure 7: Configure the MRAID Controller



Depending on the selected RAID level, this can be one or more selections. When the array members have been selected, click >> to allocate them to the Drive Group. With the Drive Group membership defined, click **Create Virtual Drive**. Clicking the Virtual Drive Info tab displays a report of the Virtual Drives controlled by the MRAID module and their status.

Note In this example the Virtual Drive #0 is the selected boot drive, as shown.

Figure 8: Create a Virtual Drive



Cisco 12G SAS Modular Raid Controller (SLOT-HBA)

Controller Info Physical Drive Info **Virtual Drive Info** Battery Backup Unit Storage Log

Virtual Drives

Virtual Drive Number	Name	Status	Health	Size	RAID Level	Boot Drive
0	RAID0_1	Optimal	Good	952720 ME	RAID 0	true
1	RAID0_2	Optimal	Good	952720 ME	RAID 0	false
2	RAID0_3	Optimal	Good	952720 ME	RAID 0	false

Actions

- Initialize
- Set as Boot Drive
- Delete Virtual Drive
- Edit Virtual Drive

Operation Status

Operation: No operation in progress
 Progress in %: 0
 Elapsed Time (secs): 0
 Refresh

412703

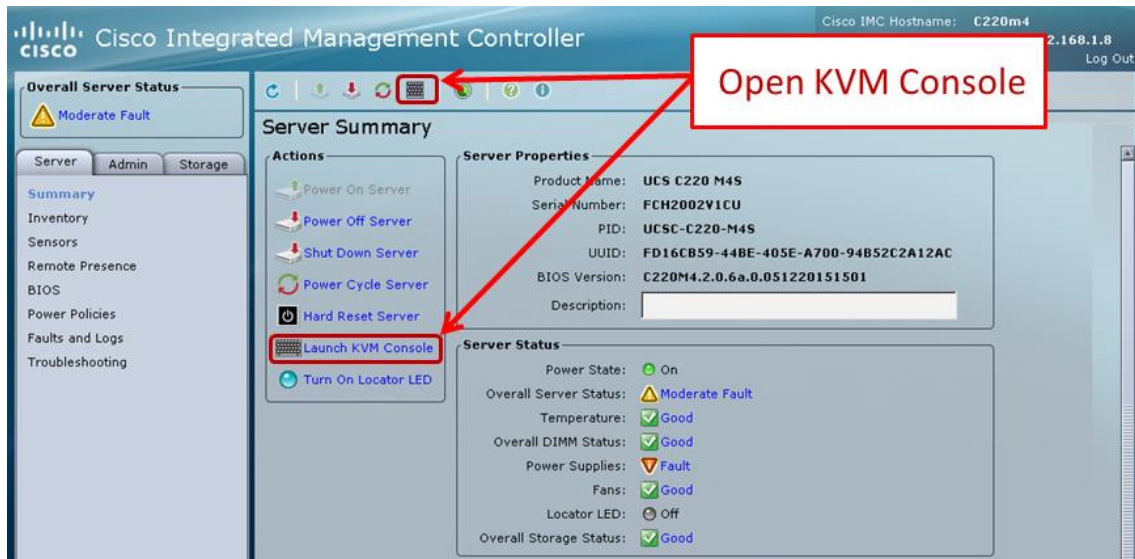
Map the Cisco Modeling Labs ISO Disk Image

To map the Cisco Modeling Labs ISO disk image, complete the following steps:

Step 1

With the Cisco UCS server properly prepared for the Cisco Modeling Labs installation, the ISO installation media must be virtually (remote) mounted to the target server. In the CIMC interface, open a KVM Console to the server by clicking the associated icon in the tool bar or the within the **Actions** pane.

Figure 9: KVM Console



Note If using a Java-enabled browser, a series of PopUp windows will appear; acknowledge each and the KVM Console window will open. If the browser is not java-enabled (e.g. Chrome), manually open the downloaded viewer.jsp file with the javaws.exe application and acknowledge the series of PopUps.

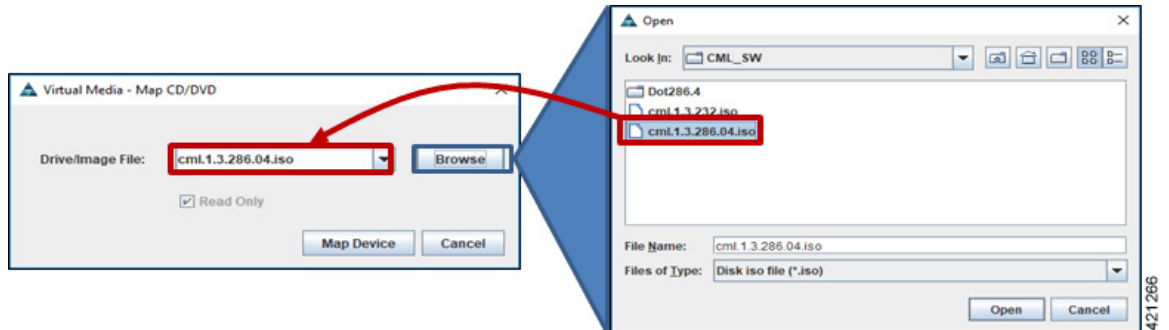
Step 2 In the KVM Console window, click **Virtual Media** from the menu bar. From the drop-down, choose the **Activate Virtual Devices**. Acknowledge the **Unencrypted Virtual Media Session** warning and click **Apply**, as shown.

Figure 10: Activate Virtual Devices



- Step 3** Click **Virtual Media** from the menu bar again. In the expanded drop-down list, choose the **Map CD/DVD...** option. In the resultant Virtual Media – Map CD/DVD dialog box, browse to and select the Cisco Modeling Labs ISO file. The ISO image file will appear in the selected Drive/Image File field; click **Map Device** to continue, as shown.

Figure 11: Map CD/DVD

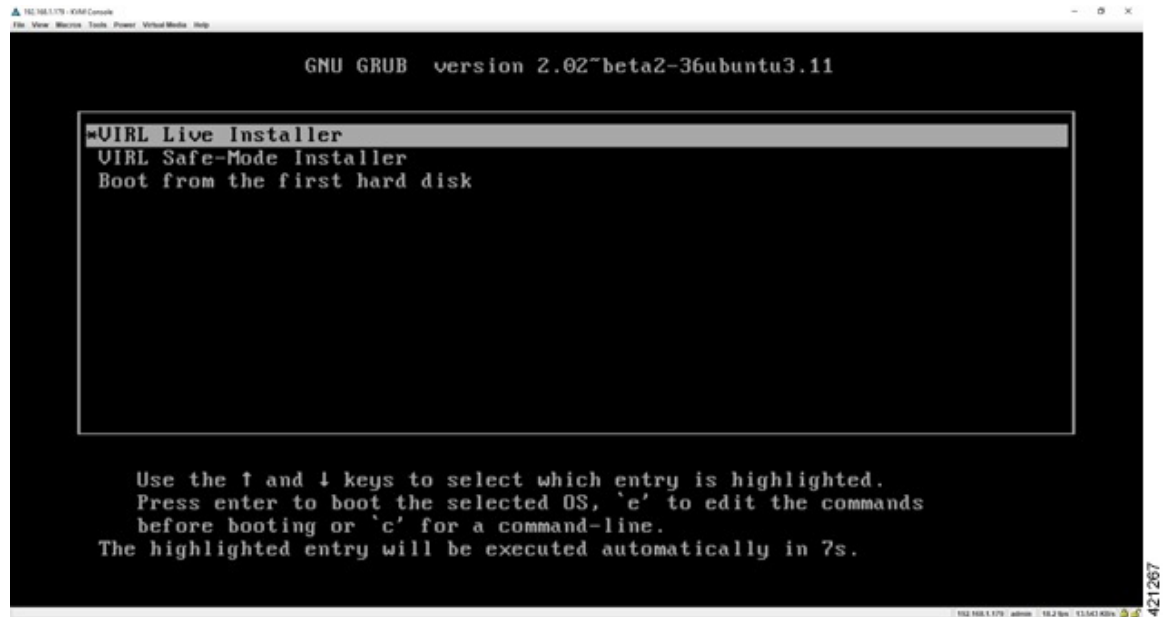


- Step 4** In the KVM Console window, click **Macros** from menu banner. In the drop-down list, choose **Static Macros > Ctrl-Alt-Del** to trigger a server reboot.
- Step 5** During the reboot cycle, when the server setup screen is displayed, press the <F6> key. Choose the **Cisco vKVM-Mapped vDVD** option for the boot device. When complete, the server will boot the ISO disk image file.

Run the VIRL Installer

The system boots from the previously mapped Virtual Media CD/DVD Device. On initial startup, the system reports the status of the eth0 interface. This can be set for the assigned static IP address later. After a small delay, the Ubuntu (GRUB) boot loader menu is displayed.

Figure 12: VIRL Installer Window



Complete the following steps to install Cisco Modeling Labs.

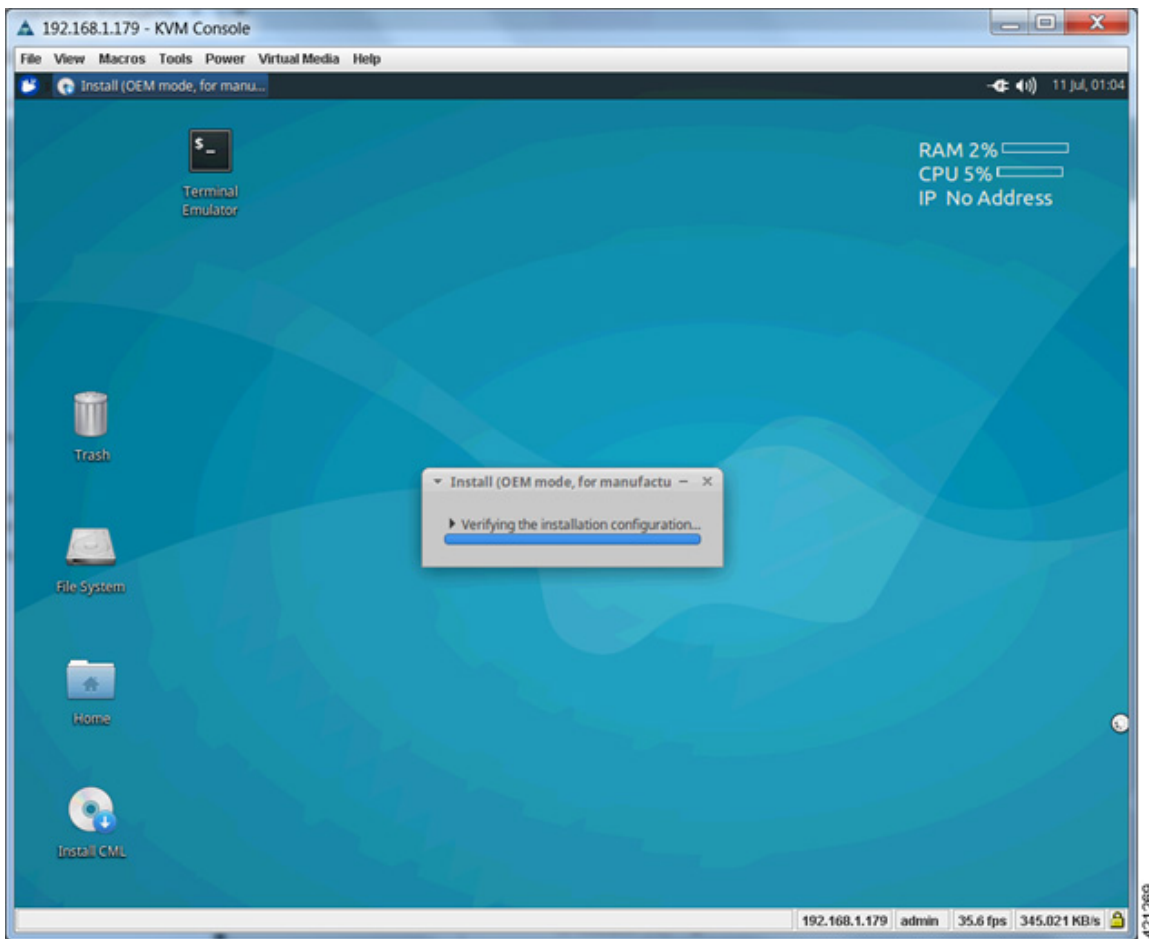
- Step 1** Select the **VIRL Live Installer** option and press **Enter** to continue booting from the mounted ISO image file. Upon completion of the startup cycle, the Ubuntu Desktop is presented.

Figure 13: Ubuntu Desktop



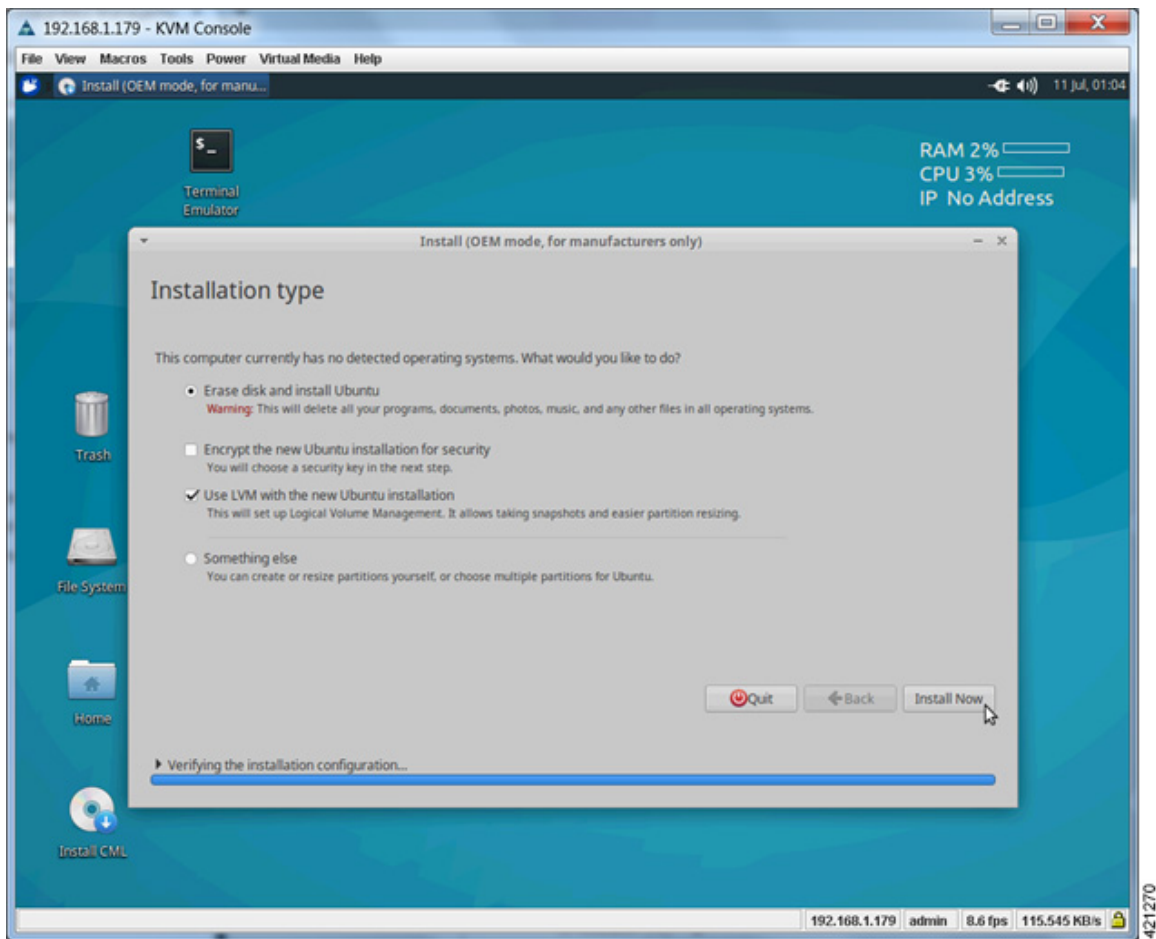
- Step 2** On the desktop, double-click **Install CML** to begin the installation.

Figure 14: Installation Started



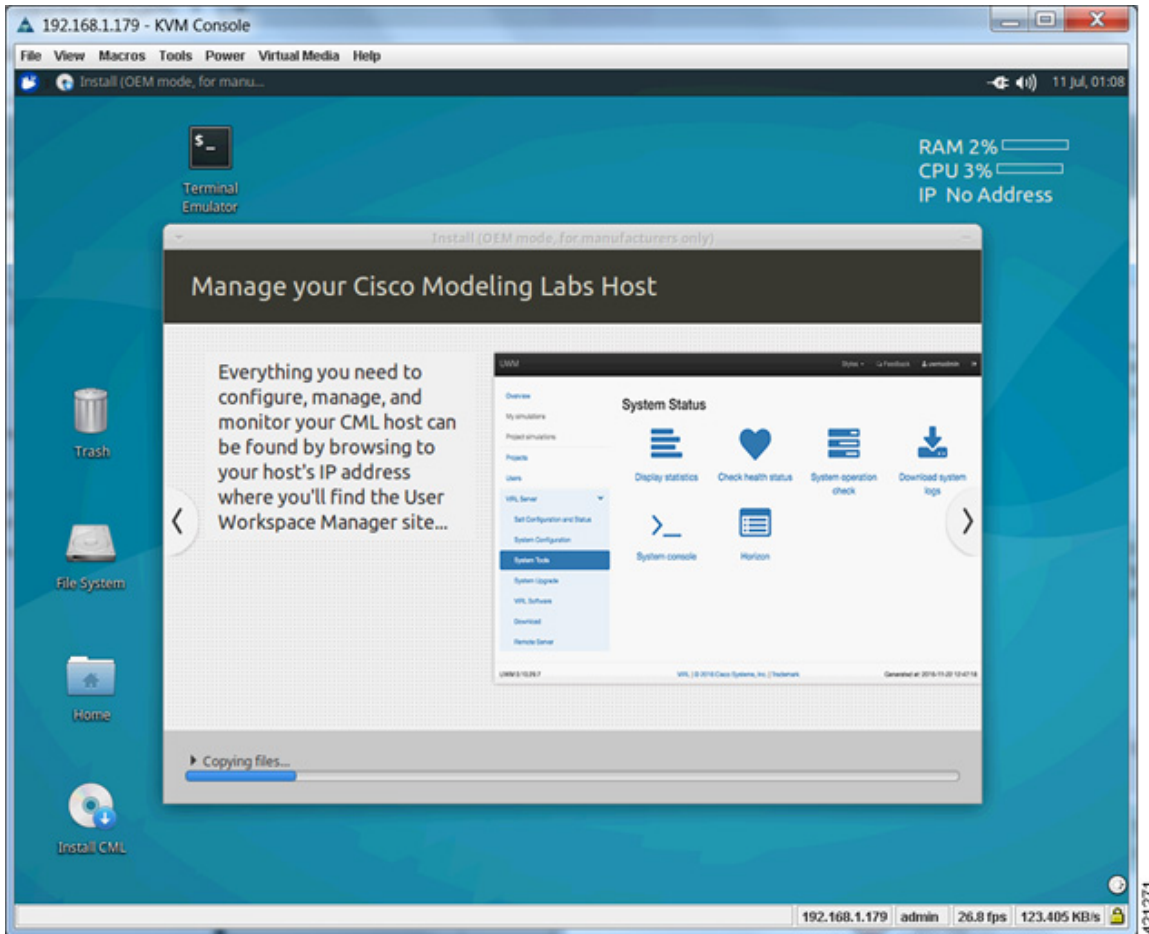
- Step 3** After verifying the installation configuration, the **Installation Type** page is presented. Set the Installation type to **Erase disk and Install Ubuntu**. We recommend that you enable the **Use LVM with the new Ubuntu installation** option, to setup Logical Volume Management. Click **Install Now**.

Figure 15: Installation Type Page



- Step 4** When the Disk formatting warning is presented, click the **Continue** button to initiate the software installation process. The bar graph indicates the software transfer process.

Figure 16: Copying Files



Step 5 When completed, you are prompted to remove the install installation medium. Using the virtual console menus, deselect the ISO mapping and returning to the console session. Press **Enter** to trigger a system reboot using the freshly installed system.

Figure 17: Newly Installed System

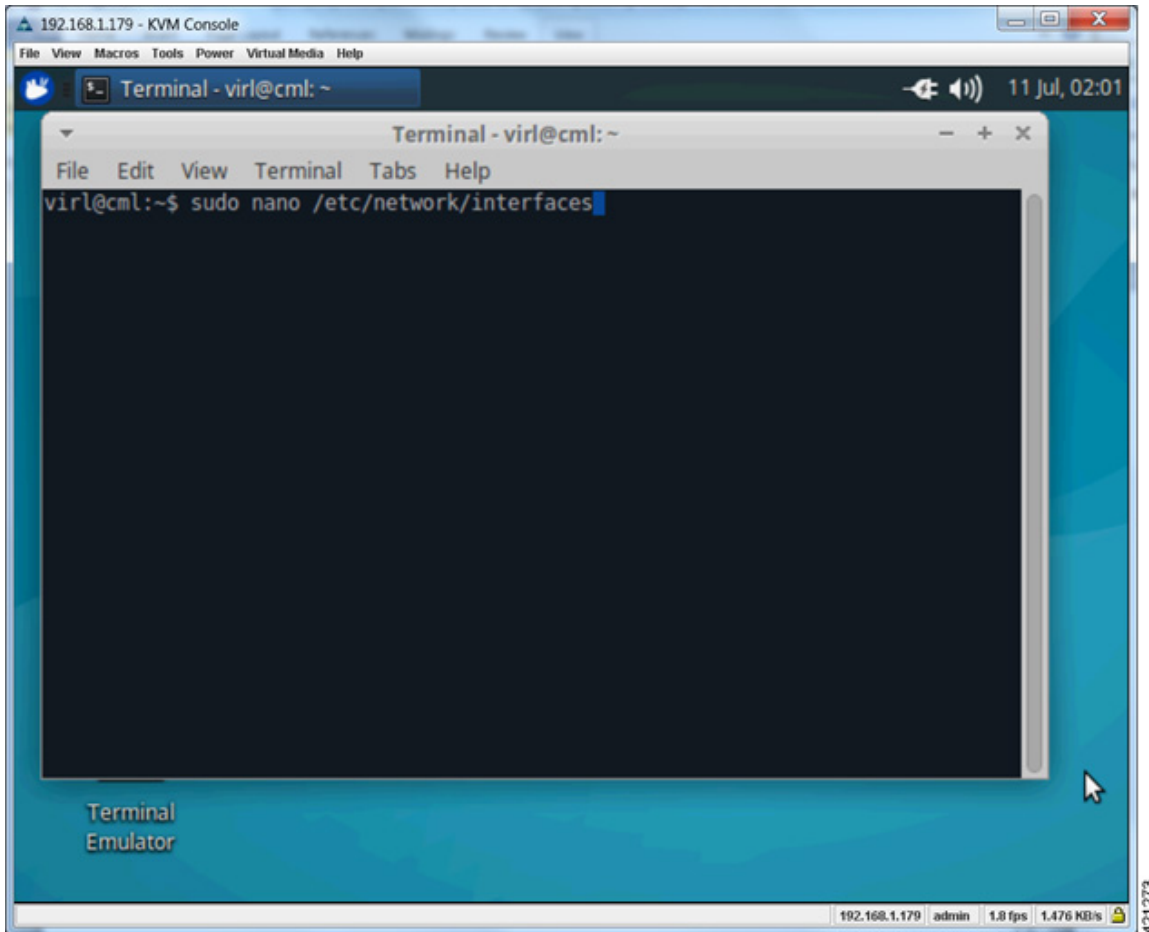


Once the system has rebooted to the local storage, return to the virtual KVM Console via the UCS CIMC interface. Logging back into the system with the virl/VIRL credentials presents the Ubuntu desktop. The upper right corner of the desktop will report the DHCP acquired IP address to the management interface. If no DHCP services are available, the report will indicate IP No Address. We recommend that the management interface be statically configured. If the system booted with an IP address, this may be changed using the **User Workspace Management** interface.

When no DHCP services are available, a static IP address must first be configured for the management interface.

- Step 6** From the KVM Console, double-click the **Terminal Emulator** icon. Using a text editor, open the `/etc/network/interfaces` file, as shown.

Figure 18: Edit the Interfaces File

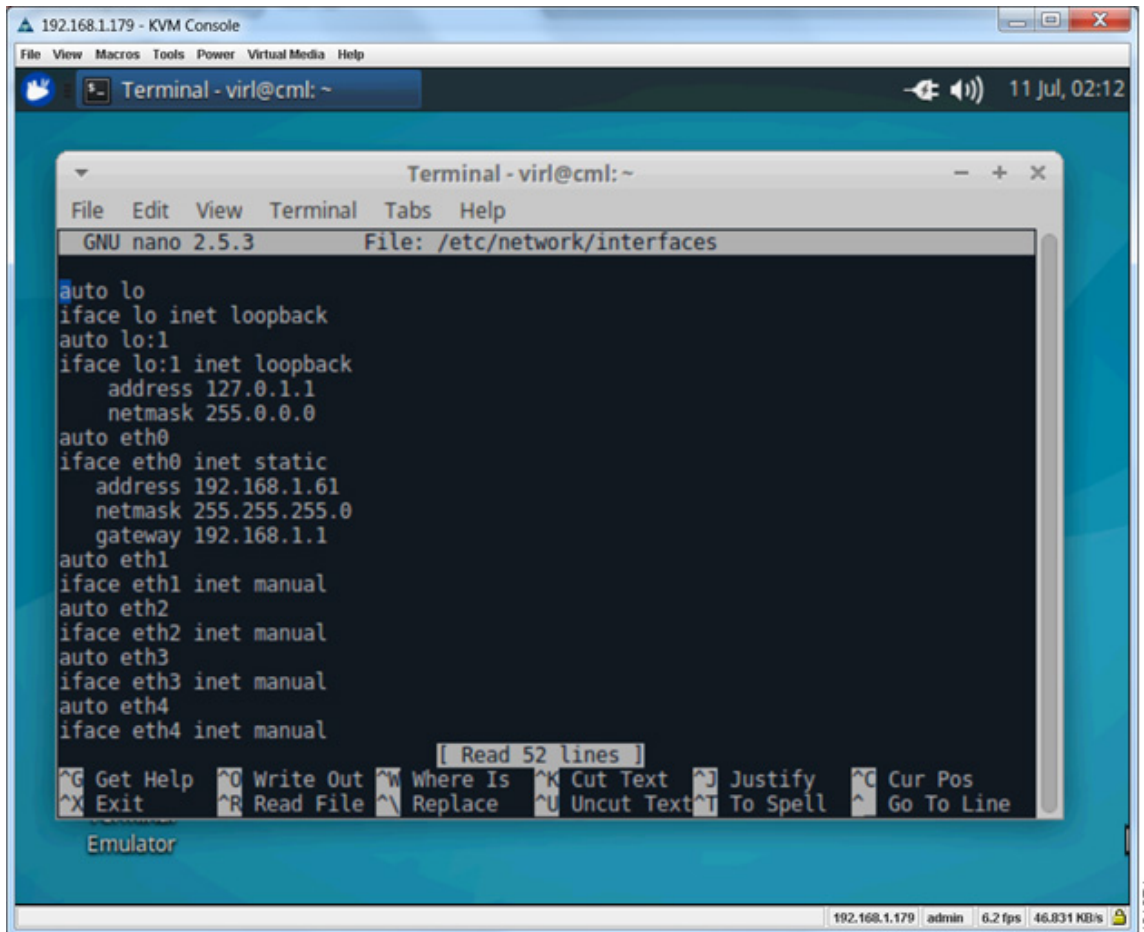


- Step 7** Scroll to the configuration associated with the `eth0` interface. Replace the **dhcp** entry with **static**. Add the following interface configuration lines to the file immediately after the **static** entry, as shown:

```
iface eth0 inet static
    address nnn.nnn.nnn.hhh
    netmask mmm.mmm.mmm.mmm
```

```
gateway nnn.nnn.nnn.ggg
```

Figure 19: Assign a Static IP Address



- Step 8** Enter **^X** to exit the file edit mode, followed by **Y** to confirm saving the changes and **Enter** to confirm overwriting the `/etc/network/interfaces` file.
- Step 9** To reboot the system, enter `sudo reboot now`.

Once the system reboot has completed, returning to the KVM virtual console shows the IP Address to the CML's management interface, as displayed in the top right-hand corner.

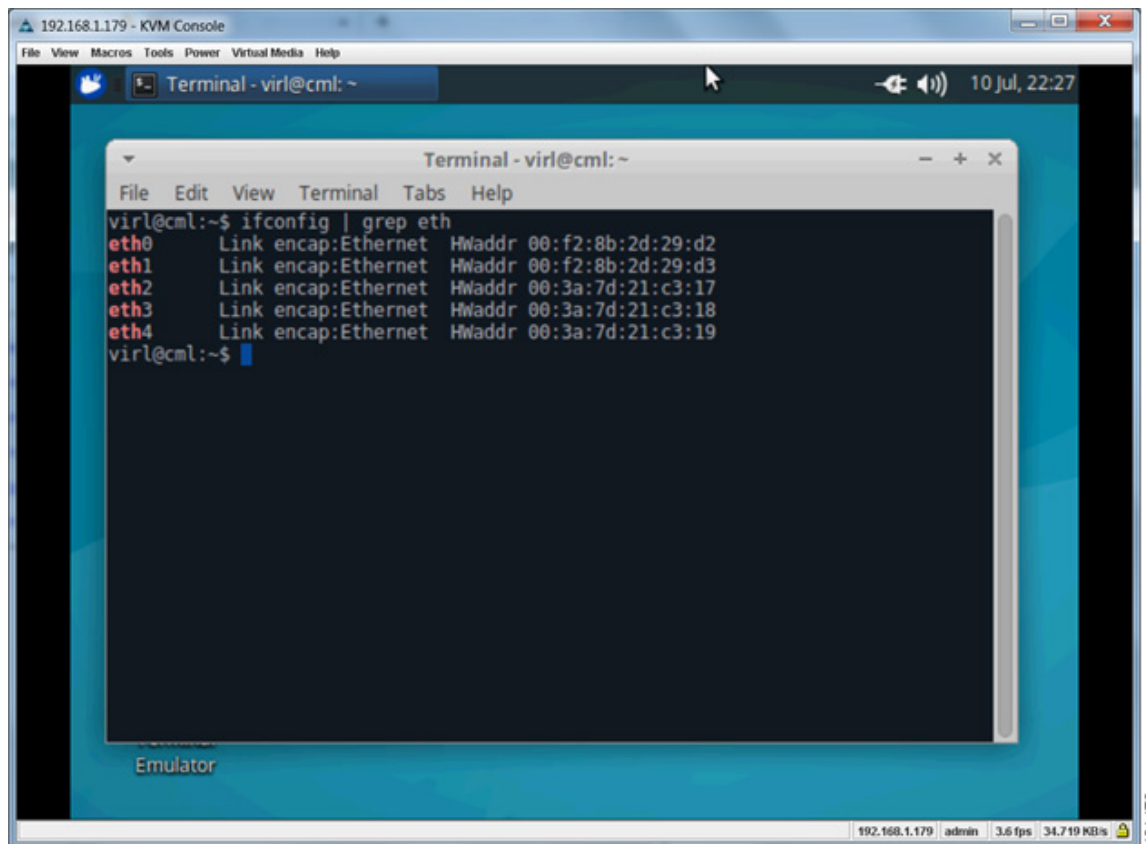
Figure 20: Static IP Address Assigned



Step 10 Cisco Modeling Labs installed directly onto hardware as a bare metal deployment requires (5) network interfaces to achieve full functionality. To verify that these required network interfaces are recognized by the system, double-click

the **Terminal Emulator** icon to open an XTerminal session on the console's desktop and enter `ifconfig | grep eth` at the command prompt, as shown.

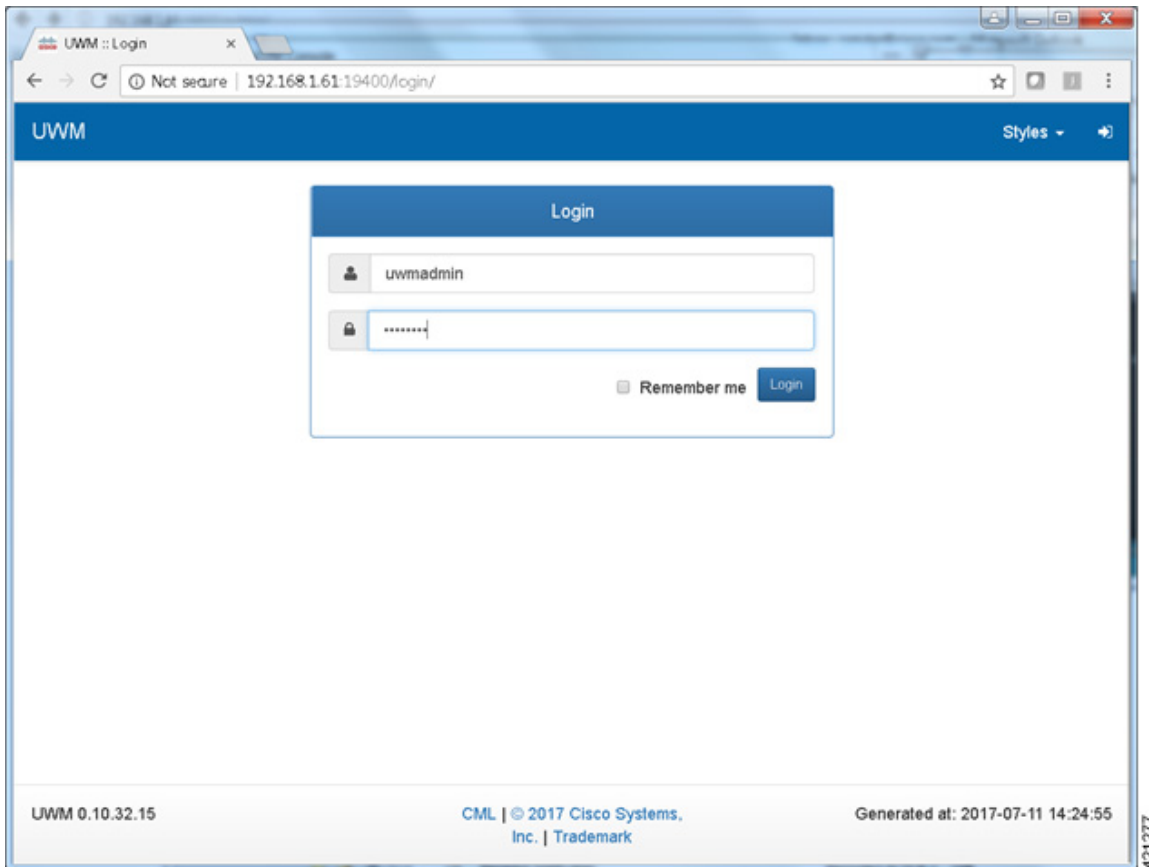
Figure 21: Verify the Required Network Interfaces



With all (5) Ethernet interfaces recognized by the system, the installation process may be completed using the **User Workplace Management** interface. If less than (5) Ethernet interfaces are reported, an interface-constrained deployment must first be prepared. This entails creating an alias for the missing OpenStack services IP address, and then creating a pseudo-interface (dummy) for each of the missing interfaces.

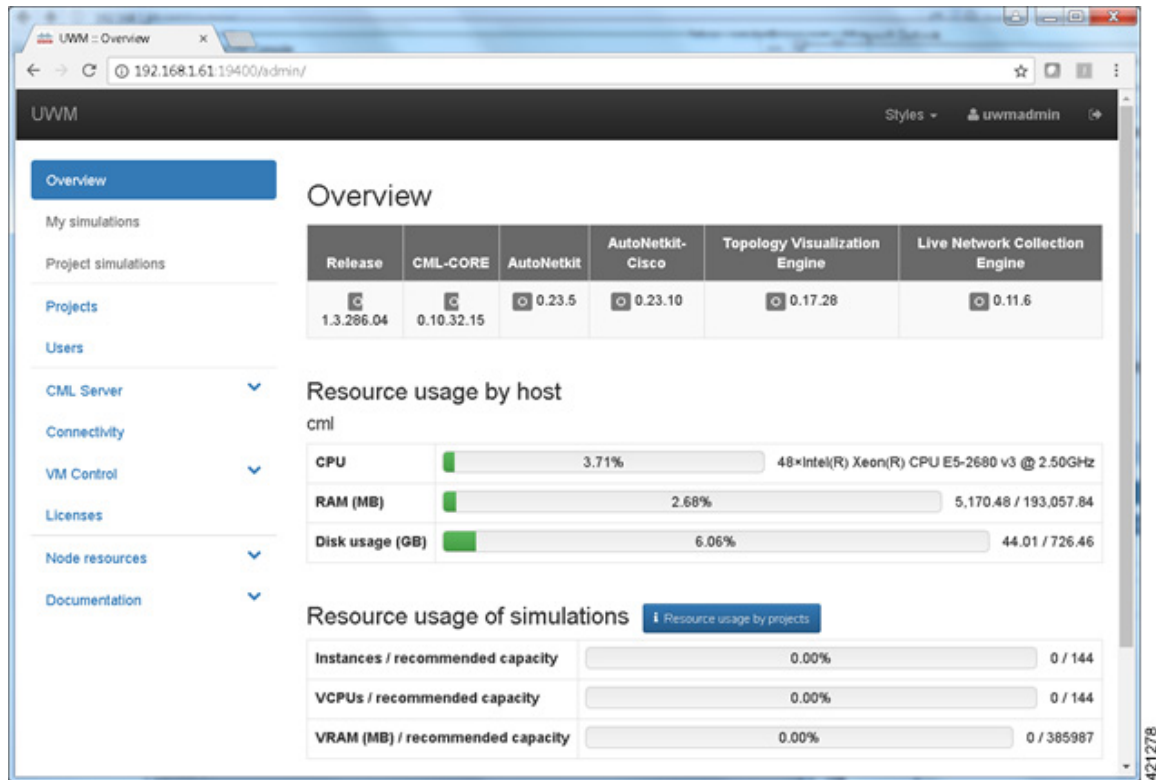
- Step 11** Using a web browser, connect to the IP address configured to the management interface and login to the administrative account using the default credentials (uwadmin/password), as shown.

Figure 22: Log in to the User Workspace Management Interface



The UWM Overview page is displayed.

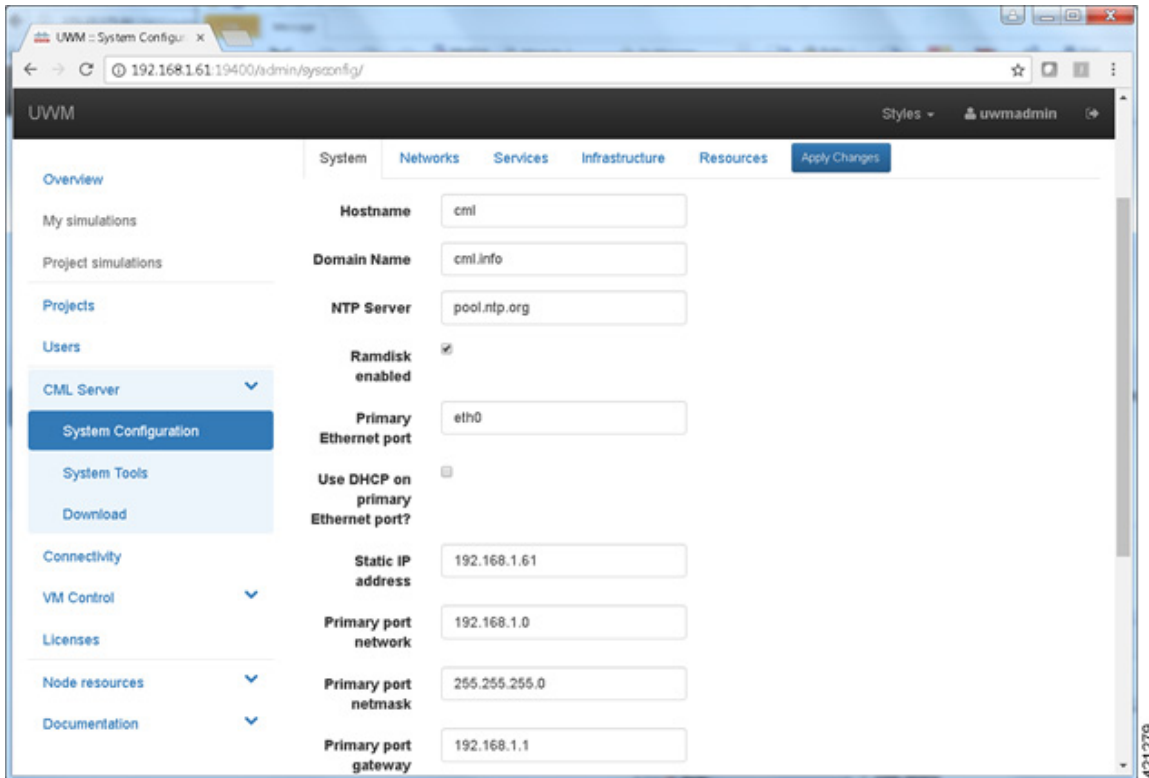
Figure 23: Overview Page



Step 12 Access the **CML Server > System Configuration** page to set the server's attributes. Under the **System** tab, update the details for the primary (eth0) Ethernet port. To reconfigure the management interface, uncheck the **Use DHCP on**

primary Ethernet port toggle to disable the DHCP assignment motif and enter the desired static assignments for the primary Ethernet port in their respective fields.

Figure 24: System Configuration Page



If the external communication interfaces must be adapted to integrate to local requirements, select the **Networks** tab, and edit the entries associated with the Flat, Flat1, and SNAT interfaces.

When the adjustments have been completed, click **Apply Changes**. A summary list of changes is presented. You must **Enable Maintenance Mode** to effect the changes. A message may be sent to any current users notifying them of the system reconfiguration event. When all simulations are shut down, the system will commence its reconfiguration. For most scenarios, this process may range from 20 minutes up to about an hour to complete. When finished, the system will prompt for a reboot, after which **Maintenance Mode may be disabled**.

Important See the section [Launch the User Workspace Management Interface](#), on page 30 for detailed instructions on how to **Enable Maintenance Mode** (Steps 13 to 19).

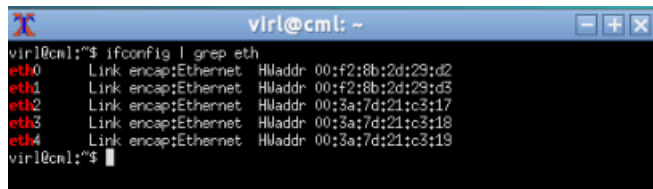
Verify that Required Interfaces are Present

The Cisco Modeling Labs bare-metal install requires 5 network interfaces, named eth0, eth1, eth2, eth3, and eth4. The presence of these interfaces should be verified at this point. Following install options 1 (live) or 2

(install), the Cisco Modeling Labs server is re-booted from the local disk. On completion of the reboot, log back into the console and open an xterm session.

From a console xterm session, running the command `ifconfig | grep eth` should return a list of 5 interfaces named eth0 through eth4.

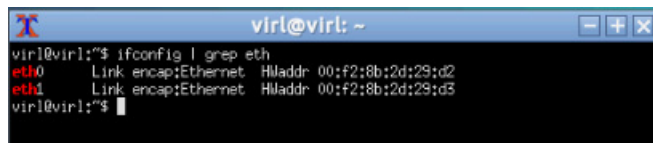
Figure 25: List of Five Interfaces



```
vir1@cml: ~  
vir1@cml:~$ ifconfig | grep eth  
eth0    Link encap:Ethernet  HWaddr 00:f2:8b:2d:29:d2  
eth1    Link encap:Ethernet  HWaddr 00:f2:8b:2d:29:d3  
eth2    Link encap:Ethernet  HWaddr 00:3a:7d:21:c3:17  
eth3    Link encap:Ethernet  HWaddr 00:3a:7d:21:c3:18  
eth4    Link encap:Ethernet  HWaddr 00:3a:7d:21:c3:19  
vir1@cml:~$
```

If a PCI or LOM-based Ethernet controller is confirmed as installed, but the `ifconfig` command returns a listing of only 2 interfaces, it is possible that the server detected the interfaces using a different name (e.g. em2, em3, and so on).

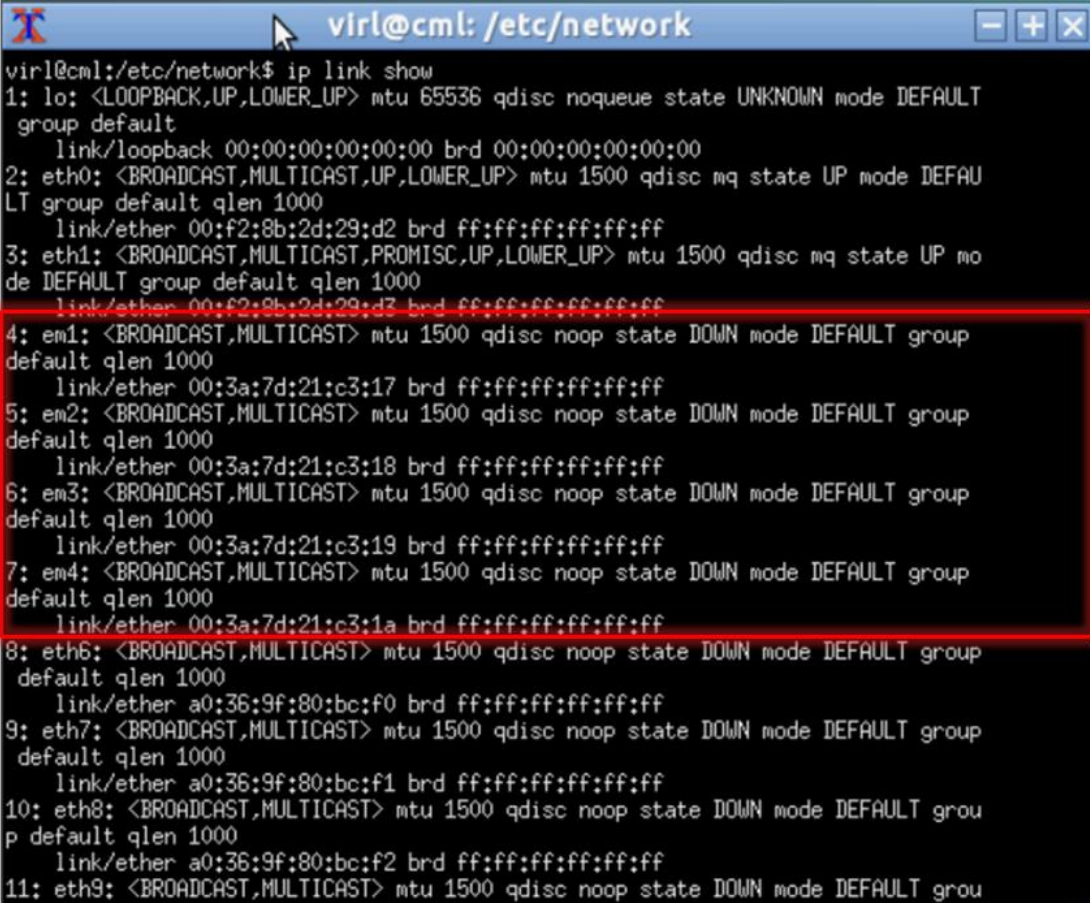
Figure 26: List of Two Interfaces Only



```
vir1@vir1: ~  
vir1@vir1:~$ ifconfig | grep eth  
eth0    Link encap:Ethernet  HWaddr 00:f2:8b:2d:29:d2  
eth1    Link encap:Ethernet  HWaddr 00:f2:8b:2d:29:d3  
vir1@vir1:~$
```

This naming discrepancy can be verified using the `ip link show` command. In this example, the PCIe-based interfaces are recognized as `em1 – em4` as highlighted.

Figure 27: Use the `ip link show` Command



```

virl@cml:/etc/network
virl@cml:/etc/network$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
   group default
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAU
   LT group default qlen 1000
   link/ether 00:f2:8b:2d:29:d2 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc mq state UP mo
   de DEFAULT group default qlen 1000
   link/ether 00:f2:8b:2d:29:d3 brd ff:ff:ff:ff:ff:ff
4: em1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT group
   default qlen 1000
   link/ether 00:3a:7d:21:c3:17 brd ff:ff:ff:ff:ff:ff
5: em2: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT group
   default qlen 1000
   link/ether 00:3a:7d:21:c3:18 brd ff:ff:ff:ff:ff:ff
6: em3: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT group
   default qlen 1000
   link/ether 00:3a:7d:21:c3:19 brd ff:ff:ff:ff:ff:ff
7: em4: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT group
   default qlen 1000
   link/ether 00:3a:7d:21:c3:1a brd ff:ff:ff:ff:ff:ff
8: eth6: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT group
   default qlen 1000
   link/ether a0:36:9f:80:bc:f0 brd ff:ff:ff:ff:ff:ff
9: eth7: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT group
   default qlen 1000
   link/ether a0:36:9f:80:bc:f1 brd ff:ff:ff:ff:ff:ff
10: eth8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT grou
   p default qlen 1000
   link/ether a0:36:9f:80:bc:f2 brd ff:ff:ff:ff:ff:ff
11: eth9: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT grou

```

To reset the interface names to the format expected by the Cisco Modeling Labs installer, complete the following steps:

- 1 Edit the `/etc/default/grub` file: `sudo nano /etc/default/grub`
- 2 Search for the follow two lines:

```

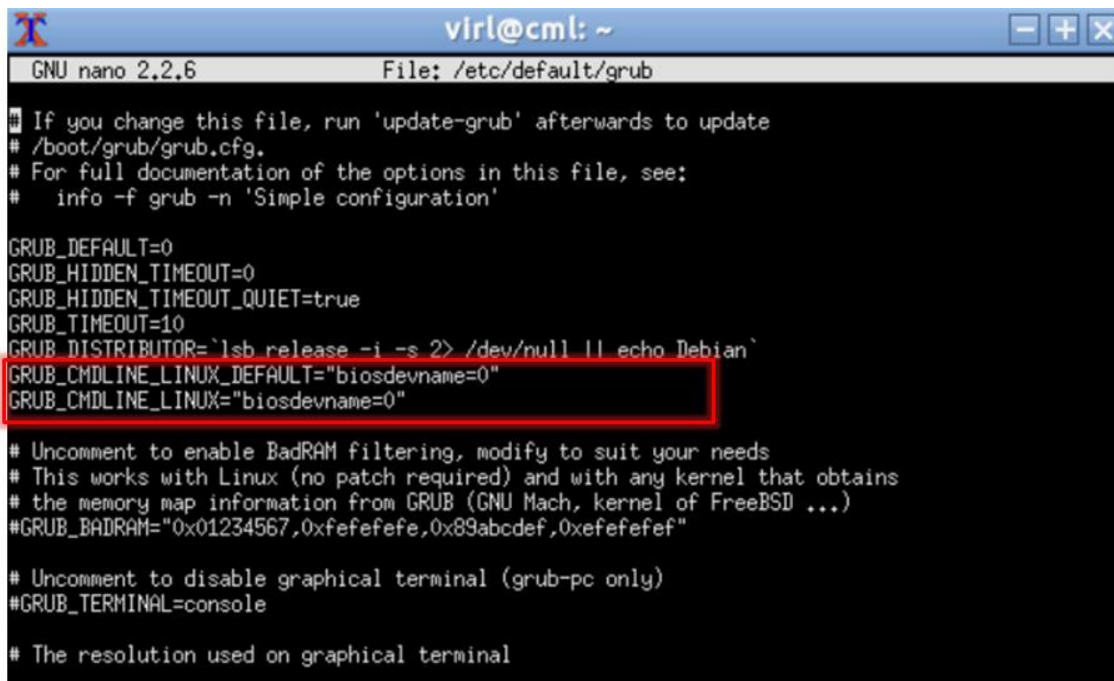
GRUB_CMDLINE_LINUX_DEFAULT=""
GRUB_CMDLINE_LINUX=""

```

- 3 Edit the lines as follows:

```
GRUB_CMDLINE_LINUX_DEFAULT="biosdevname=0"
GRUB_CMDLINE_LINUX="biosdevname=0"
```

Figure 28: Updated File



```
virl@cml: ~
GNU nano 2.2.6 File: /etc/default/grub
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
# info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
GRUB_HIDDEN_TIMEOUT=0
GRUB_HIDDEN_TIMEOUT_QUIET=true
GRUB_TIMEOUT=10
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="biosdevname=0"
GRUB_CMDLINE_LINUX="biosdevname=0"

# Uncomment to enable BadRAM filtering, modify to suit your needs
# This works with Linux (no patch required) and with any kernel that obtains
# the memory map information from GRUB (GNU Mach, kernel of FreeBSD ...)
#GRUB_BADRAM="0x01234567,0xfefefefe,0x89abcdef,0xefefefef"

# Uncomment to disable graphical terminal (grub-pc only)
#GRUB_TERMINAL=console

# The resolution used on graphical terminal
```

- 4 Save the /etc/default/grub file and exit using [Ctrl-X; Yes; Enter]
- 5 Complete the update using the command: `sudo update-grub`
- 6 Reboot the server to effect the changes: `sudo reboot now`
- 7 On completion of the system restart, verify that the required number of Ethernet interfaces conforming to the ethN naming format are now available on the operating system. If not, this must be diagnosed and resolved before proceeding, or the interface-constrained installation steps performed.

(Optional) Prepare for an Interface-Constrained Installation

In a bare metal deployment, if the Cisco Modeling Labs server does not have the required 5 network interfaces, the missing interfaces require pseudo-interface (dummy) references. This is done by creating an alias for the missing OpenStack services IP address, and then creating a pseudo-interface for each of the missing interfaces.

The steps described here are for a server fitted with only two network interfaces (eth0 and eth1). Three pseudo-interfaces (dummy1, dummy2, and dummy3) must be configured to compensate for the missing

interfaces. Adapt the number of pseudo-interfaces in accordance with the number required for your specific deployment. This section can be skipped if the server has the requisite five network interfaces.

-
- Step 1** From a console xterm session, edit the network configuration file: `sudo nano /etc/network/interfaces`
- Step 2** Add a new line in the eth0 section and enter `up ip addr add 172.16.10.250/24 dev eth0` to create a new alias for the missing OpenStack services address.
For example:
- ```
iface eth0 inet dhcp
 dns-nameservers 8.8.8.8 8.8.4.4
 up ip addr add 172.16.10.250/24 dev eth0
```
- Note** When configuring a server for interface-constrained deployment, this is a good time to also set the application's management interface for static address assignment and to enter its primary interface details. This will save time associated with machine reset cycles.  
For example:
- ```
iface eth0 inet static
    address nnn.nnn.nnn.hhh
    netmask nnn.nnn.nnn.0
    gateway nnn.nnn.nnn.g
    dns-nameservers 8.8.8.8 8.8.4.4
    up ip addr add 172.16.10.250/24 dev eth0
```
- Note** When setting the eth0 static IP assignment, the dns-nameservers should be set to a local DNS reference, or pointed to a loopback reference (127.0.0.1) if there is no Internet access. Otherwise, issues can arise during the rehost process as a result of timeouts from failed DNS queries.
- Step 3** Open the configuration file for editing: `sudo nano /etc/virl.ini`
- Step 4** Change the hostname to **ubuntu**. This can be modified later during customization if desired.
- Step 5** Enter Ctrl-W and search for 'l2_port':
- Note** If the host has only one network interface, 'l2_port' would need to be set to a dummy interface, starting with dummy1 and incrementing sequentially for additional interfaces. In this case, it is left as eth1.
- Step 6** Enter Ctrl-W and search for 'l2_port2:'. In this example, since interface eth2 is missing, l2_port2: must be mapped to interface dummy1. Replace eth2 with dummy1.
- Step 7** Enter Ctrl-W and search for 'l3_port:'. In this example, since interface eth3 is missing, l3_port: must be mapped to interface dummy2. Replace eth3 with dummy2.
- Step 8** Enter Ctrl-W and search for 'internalnet_port:'. In this example, since interface eth4 is missing, internalnet_port: must be mapped to interface dummy3. Replace eth4 with dummy3.
- Step 9** Enter Ctrl-W and search for 'dummy_int'. Since dummy interfaces are required dummy_int must be set to True.
- Step 10** Enter Ctrl-X to exit nano.
- Step 11** Enter Y and Enter to confirm saving the configuration file and exit.
- Step 12** Enter `sudo reboot now` to reboot the virtual machine.
- Step 13** Once rebooted, log in again using username virl and password VIRL.
- Step 14** Click the **xterm** icon to open a terminal window.
- Step 15** Confirm that the OpenStack services IP address is reachable: `ping -c 4 172.16.10.250`
- Note** If no replies are received, check that the interfaces were updated correctly.
- Step 16** Enter `nova service-list` to display the status of the Nova services.
Verify that the status for each Nova service is enabled and that the state for each is up.

Note If the Nova services are not enabled and up, verify the changes to the network configuration file, reboot, and try again.

Step 17 Enter `neutron agent-list` to display the status of the OpenStack Neutron agents. Verify that the status for the Metadata, DHCP, and L3 agents is :-).

Note If the Metadata, DHCP, or L3 agents are not alive, verify the changes to the network configuration file, reboot, and try again.

Important Check that the following requirements are in place before proceeding to the next step in the installation process.

- Confirm that the OpenStack services IP address is reachable.
- Verify that the status for each Nova service is enabled and that the state for each is up.
- Verify that the status for the Metadata, DHCP, and L3 agents is :-).

Reconfigure Default Console Resolution

Once the software has been installed on the server, changing the default video resolution will enable the Cisco Modeling Labs Desktop Manager GUI (Ubuntu Light Display Manager) to be accessible via the CIMC's virtual KVM. This requires applying a shell script changing the default resolution to the lightdm configuration file.



Note Changing the video resolution via the Desktop Manager's GUI menu (Preferences > Monitor Settings) is ineffective, as it does not apply to the Login page, thus preventing remote logins.

To manually set the video to a resolution supported by the CIMC's virtual KVM, complete the following steps:

Step 1 In the KVM Console window, click **Macros** on the menu bar.

Step 2 From the drop-down menu, choose the **Macros > Static Macros > Ctrl-Alt-F > Ctrl-Alt-F2**, followed by **<Enter>** to switch the vConsole to a command line interface (CLI). If necessary, login with `vir1/VIRL`.

Step 3 Edit the `lightdm.conf` file: `sudo nano /etc/lightdm/lightdm.conf`

Step 4 Add the following line to the file: `display-setup-script=/etc/lightdm/lightdm_cml.sh`

Step 5 Save the file, and exit the editor: `Ctrl-x; Yes; Enter`

Step 6 Create a `lightdm_cml.sh` file: `sudo nano /etc/lightdm/lightdm_cml.sh`

Step 7 Add the following lines:

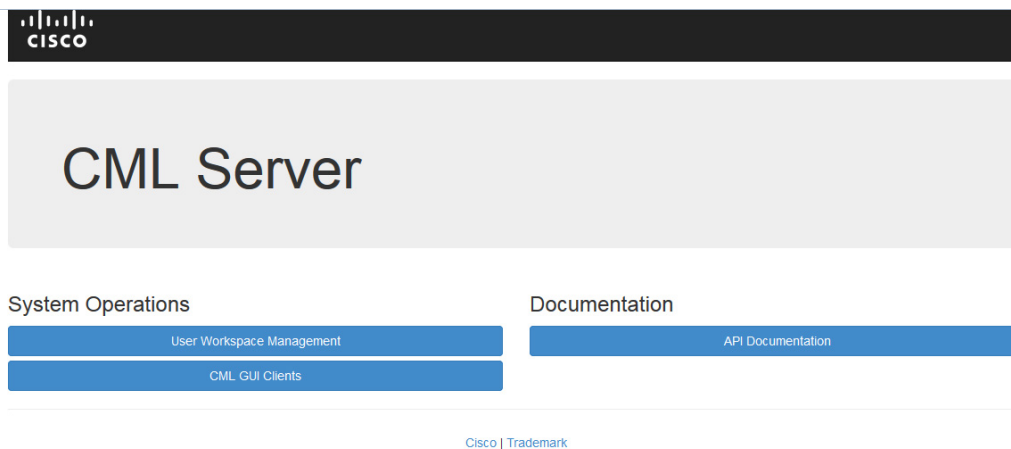
```
#!/bin/sh
xrandr --output default --mode 1024x768
```

- Step 8** Save the file, and exit the editor: `Ctrl-x; Yes; Enter`
- Step 9** Set the shell-script as executable by entering: `sudo chmod +x /etc/lightdm/lightdm_cml.sh`
- Step 10** Reboot the machine using the command: `sudo reboot now`
-

Launch the User Workspace Management Interface

- Step 1** Once the virtual machine completes the reboot cycle, establish a browser session to the Cisco Modeling Labs server's management interface (either the DHCP acquired address noted earlier, or the static address added to the `/etc/network/interfaces` file.)

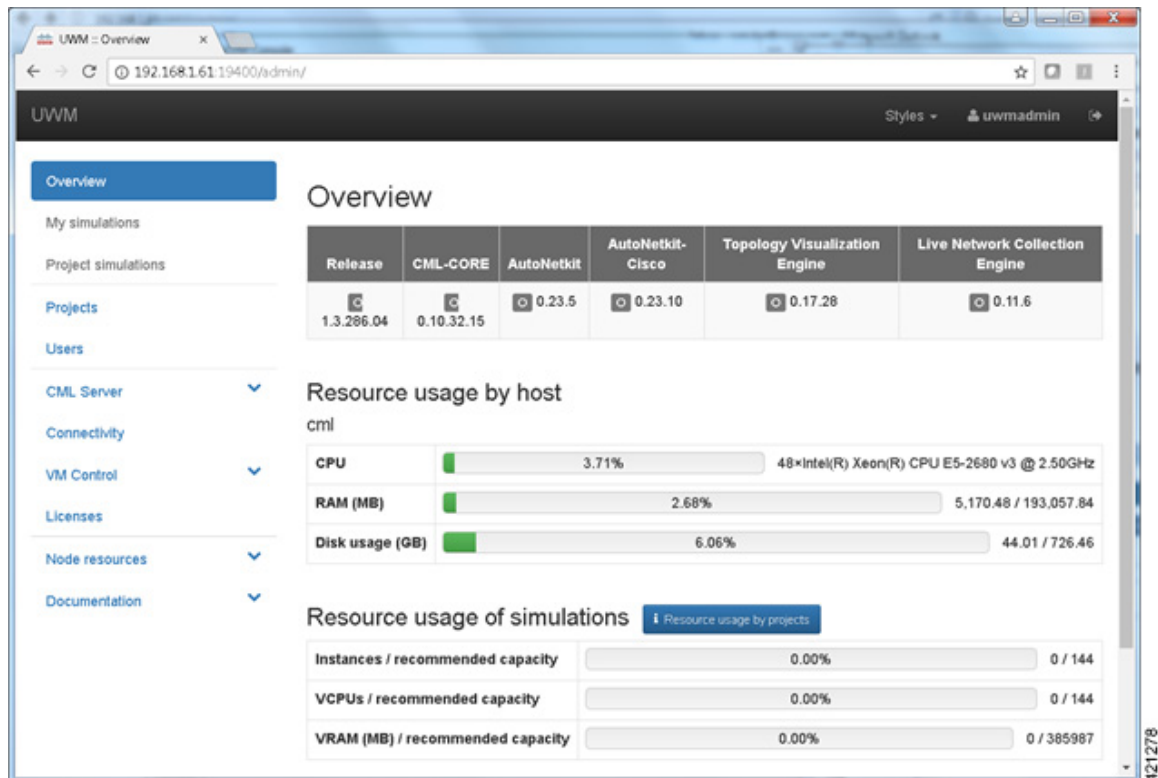
Figure 29: CML Server Main Menu



417982

Step 2 Click the **User Workspace Management** interface link. Login with the default credentials (username= uwmadmin, password=password). The **User Workspace Management** Overview page is displayed.

Figure 30: User Workspace Management Overview



Step 3 From the options on the left, expand the **CML Server** option and select **System Configuration**. Click **System** to set the system management details.

Figure 31: System Configuration Controls

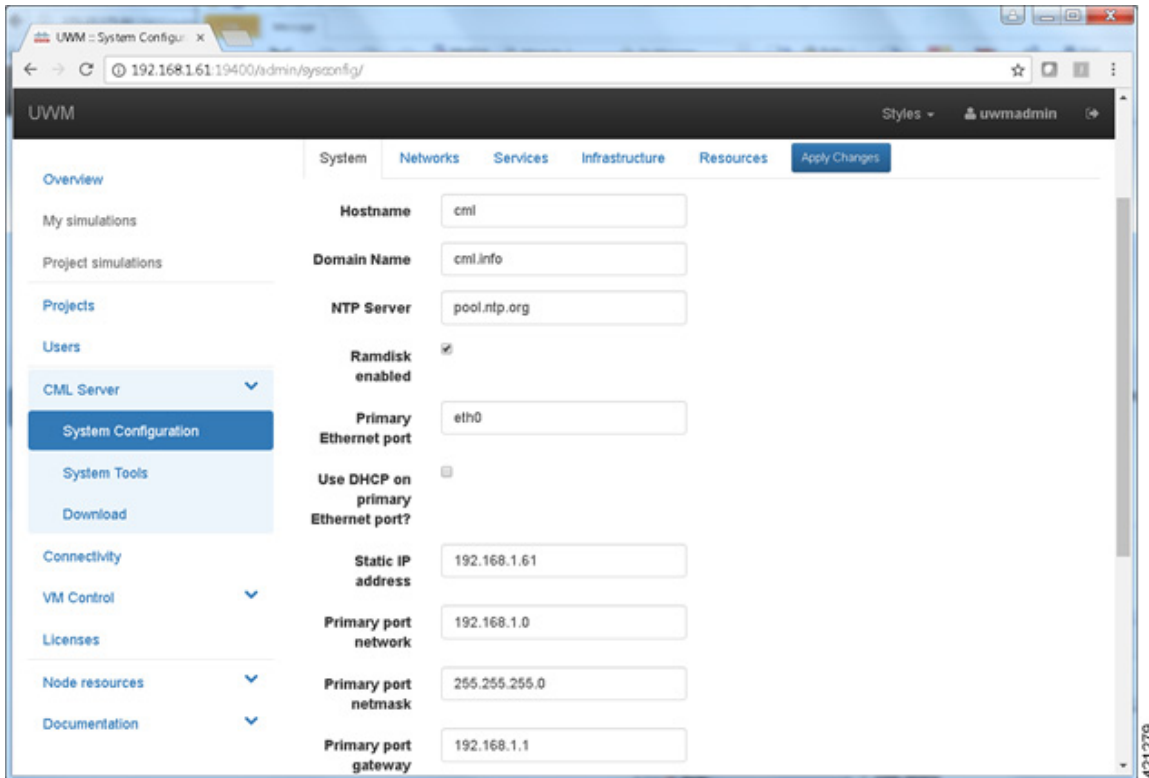


Table 1: System Configuration Parameters

Parameter	Default	Description
Hostname	cml	Changing this parameter is not supported.
Domain Name	cml.info	
NTP Server	pool.ntp.org	An NTP resource is required. If behind a firewall/proxy, this parameter should point to an NTP server reachable by this device.
Ramdisk enabled	unchecked	This option must be enabled to speed up I/O operations.
VNC enabled	unchecked	Use this option to start the VNC server on the host. It operates on TCP port 5901.
VNC Password	letmein	Enter the password for the VNC server.
Primary Ethernet Port	eth0	Enter the primary ethernet port.

Parameter	Default	Description
Use DHCP on Primary Ethernet port?	checked	When enabled, permits DHCP to configure the management interface (Ethernet0.) A static IP configuration is recommended. This parameter should be unchecked and the primary port configuration options set manually.
Static IP address	127.0.0.1	Set as the desired IP address. Entries are not allowed when DHCP is enabled.
Primary port network	127.16.16.0	Set as the IP network. Entries are not allowed when DHCP is enabled.
Primary port netmask	255.255.255.0	Set network mask information. Entries are not allowed when DHCP is enabled.
Primary port gateway	127.16.16.1	Set network gateway IP address. Entries are not allowed when DHCP is enabled.
Primary DNS server IP address	8.8.8.8	Enter the primary DNS server IP address.
Secondary DNS server IP address	8.8.4.4	Enter the secondary DNS server IP address. Ensure you do not set the same address as you set for the primary DNS server IP address.
Is your system behind a proxy?	unchecked	Use this option if your system is behind a proxy.
HTTP/HTTPS Proxy	http://mke.com:80	Replace with the URL of the Internet Access Proxy, in the format "http://<proxy IP or name>:<port number>/".

Step 4 Click **Networks** to configure the other interfaces for external communications.

Table 2: Networks Configuration Parameters

Parameter	Default	Description
Flat Network Port	Eth1	Enter the Flat network port.
Flat Network Address	172.16.1.254/24	Enter the Flat network address.
Flat Network Address/Mask	172.16.1.0/24	Enter the Flat network address/mask.
Flat Network Netmask	255.255.255.0	Enter the Flat network netmask.

Parameter	Default	Description
Flat Network Gateway IP Address	172.16.1.1	Enter the Flat network gateway IP address.
Flat Address Pool Start Address	172.16.1.50	Enter the Flat address pool start address.
Flat Address Pool End Address	172.16.1.253	Enter the Flat address pool end address.
Flat Primary DNS server IP address	8.8.8.8	Enter the Flat primary DNS server IP address.
Flat Secondary DNS server IP address	8.8.4.4	Enter the Flat secondary DNS server IP address. Ensure you do not set the same address as you set for the primary DNS server IP address.
2nd Flat Network Enabled	Unchecked	Use this option if a second Flat network, Flat1, is to be enabled.
2nd Flat Network Port	Eth2	Enter the name of the host's physical port used for the L2 Flat network, Flat1.
2nd Flat Network Address	172.16.2.254/24	Enter the IP address for the second Flat network, Flat1.
2nd Flat Network Address/Mask	172.16.2.0/24	Enter the Flat network address/mask for Flat1.
2nd Flat Network Netmask	255.255.255.0	Enter the Flat network netmask for Flat1.
2nd Flat Network Gateway IP Address	172.16.2.1	Enter the Flat network gateway IP address for Flat1.
2nd Flat Address Pool Start Address	172.16.2.50	Enter the Flat address pool start address for Flat1.
2nd Flat Address Pool End Address	172.16.2.253	Enter the Flat address pool end address for Flat1.
2nd Flat Primary DNS server IP address	8.8.8.8	Enter the Flat primary DNS server IP address for Flat1.
2nd Flat Secondary DNS server IP address	8.8.4.4	Enter the Flat secondary DNS server IP address for Flat1. Ensure you do not set the same address as you set for the primary DNS server IP address.

Parameter	Default	Description
Snat Network Port	Eth3	Enter the name of the host's physical port used for L3 Snat network, ext-net.
Snat Network Address	172.16.3.254/24	Enter the IP address for the CML host in the L3 Snat network.
Snat Network Address/Mask	172.16.3.0/24	Enter the Snat network address/mask.
Snat Network Netmask	255.255.255.0	Enter the Snat network netmask.
Snat Network Gateway IP Address	72.16.3.1	Enter the Snat network gateway IP address.
Snat Address Pool Start Address	172.16.3.50	Enter the Snat address pool start address.
Snat Address Pool End Address	172.16.3.253	Enter the Snat address pool end address.
Snat Primary DNS server IP address	8.8.8.8	Enter the Snat primary DNS server IP address.
Snat Secondary DNS server IP address	8.8.4.4	Enter the Snat secondary DNS server IP address. Ensure you do not set the same address as you set for the primary DNS server IP address.

Step 5 Click **Services** to configure the port numbers for services.

Table 3: Services Configuration Parameters

Parameter	Default	Description
Apache Server Port	80	Enter the number of the VIRT Apache server port.
Start Host-granted TCP Port	10000	Host grants TCP ports to the simulations starting from this value.
End Host-granted TCP Port	17000	Host grants TCP ports to the simulations starting ending with this value.
First VM Serial Console TCP Port	17000	Simulated VMs with serial consoles use TCP ports starting from this value.
Last VM Serial Console TCP Port	18000	Simulated VMs with serial consoles use TCP ports ending with this value.

Parameter	Default	Description
VIRL Web Services Port	19399	Enter the TCP port number for the simulation engine services.
UWM Port	19400	Enter the TCP port number for the User Workspace Management interface.
AutoNetkit Webserver Port	19401	Enter the TCP port number for the configuration engine preview interface.
Live Visualization Webserver Port	19402	Enter the TCP port number for the Live Visualization interface.
UWM Web-SSH Port	19403	Enter the TCP port number for the User Workspace Management SSH web interface.
Nova Websocket Serial Port	19406	Enter the TCP port number for the websocket-based serial console connections.
Disable Serial Timeout	Unchecked	Disable timeout of serial consoles after 15 minutes of inactivity.
Nova Websocket VNC Port	19407	Enter the TCP port number for the websocket-based VNC console connections.
Docker Registry Port	19397	Enter the port number for the docker registry.

Step 6 Click **Infrastructure** to configure the other interfaces for external communications.

Table 4: Infrastructure Configuration Parameters

Parameter	Default	Description
OpenStack Password	password	Enter the password for administrator access to OpenStack operations.
MySQL Password	password	Enter the password for OpenStack database access.
Guest Account Present?	checked	Use this option to create a default guest account.

Step 7 Click **Resources** to configure the other interfaces for external communications to meet integration requirements.

Table 5: Resources Configuration Parameters

Parameter	Default	Description
Download Proxy		Enter the proxy server for downloading files, such as images and external git repositories, from outside the local network. Leave blank if the use of a proxy is not required.
Download Proxy Authentication		Enter download proxy credentials in the format "<username>:<password>".
Download Proxy Exceptions		Provide a list all host names and/or IP addresses for image and git repository sources where the download proxy shall not be used, such as servers, on the local network.

Step 8 With all configuration options set, click **Apply Changes**. At this point, the system will ask you to please enable maintenance mode first as shown.

Figure 32: Enable Maintenance Mode

System Configuration

CONFIG
SET MAINTENANCE MODE
APPLY
REBOOT
DISABLE MAINTENANCE MODE
COMPLETE

Changes:

Field	Current value	New value
Primary port gateway	N/A	172.16.150.154
Primary port netmask	N/A	255.255.255.0
Primary port network	N/A	172.16.150.0
Static IP address	N/A	172.16.150.156
Use DHCP on primary Ethernet port?	True	False

Changes impact:

```
state -s <v> -i <v> -i <v> -i <v>
state -s <v> -i <v> -i <v> -i <v>
state -s <v> -i <v> -i <v> -i <v>
```

NOTE: You will need to reboot the CML Server after the changes.

Please enable maintenance mode first.

417984

Click **Enable Maintenance Mode** as requested.

A Maintenance Mode dialog box is displayed.

Figure 33: Maintenance Mode Dialog Box

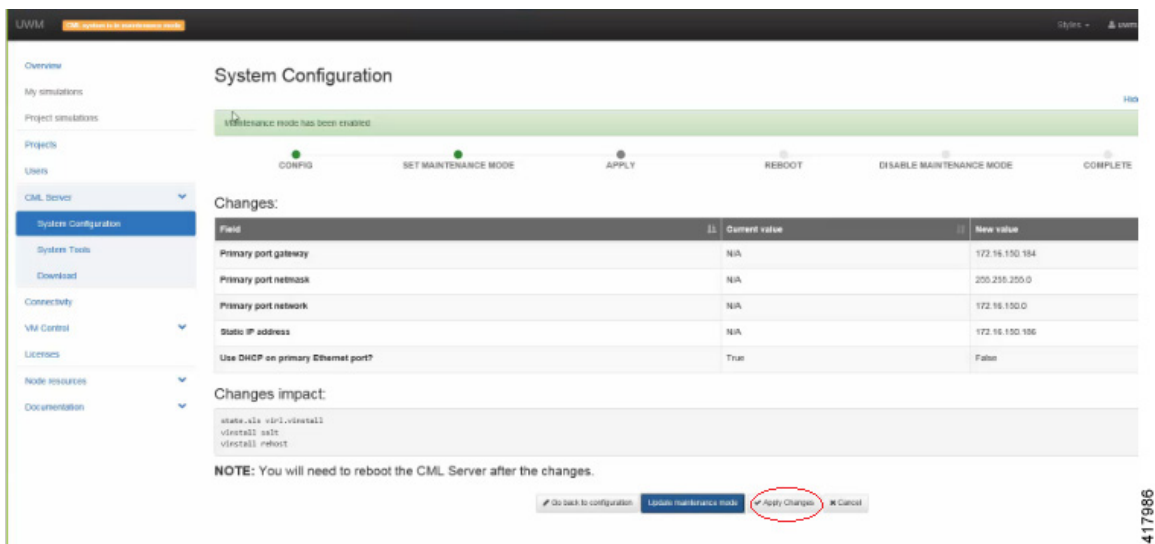


Click **Enable**. The system is now in maintenance mode.

Step 9

Click **Apply Changes** as shown.

Figure 34: Apply Changes Made



Note You must click **Apply Changes** at this point in order for your configuration updates to take effect.

Under the **Jobs in Progress** panel, you can see the progress of the rehost operations as the page refreshes periodically, as shown.

Figure 35: Jobs in Progress

System Configuration

CONFIG SET MAINTENANCE MODE APPLY REBOOT DISABLE MAINTENANCE MODE COMPLETE

Jobs in progress

Job	Status	Last update	Runtime	Success	Options
state.sls.virt.vinstall	finished	2017-02-01 15:48:13	6s	✓ (1 out of 1)	
vinstall.salt	⌚ scheduled	2017-02-01 15:48:01	—	⚠ N/A	Cancel
vinstall.rehost	⌚ scheduled	2017-02-01 15:48:01	—	⚠ N/A	Cancel

NOTE: You will have to reboot the CML Server after these jobs finish.

Refresh

Please wait... You will be able to get back to system configuration once the above jobs finish and get confirmed.

417987

- Step 10** When completed, click **Reboot** to reboot the system.
The Reboot System dialog box is displayed.

Figure 36: Reboot System Dialog Box

CML system needs to reboot

System Configuration

CONFIG SET MAINTENANCE MODE APPLY REBOOT DISABLE MAINTENANCE MODE COMPLETE

Jobs in progress

Job	Status	Last update
state.sls.virt.vinstall	finished	2017-02-01 15:48:13
vinstall.salt	finished	2017-02-01 15:48:37
vinstall.rehost	finished	2017-02-01 16:09:07

Reboot system

The system must now reboot to complete the upgrade.
Once completed, return the system to operation by disabling *maintenance mode*.
Press **reboot** to proceed with the reboot.

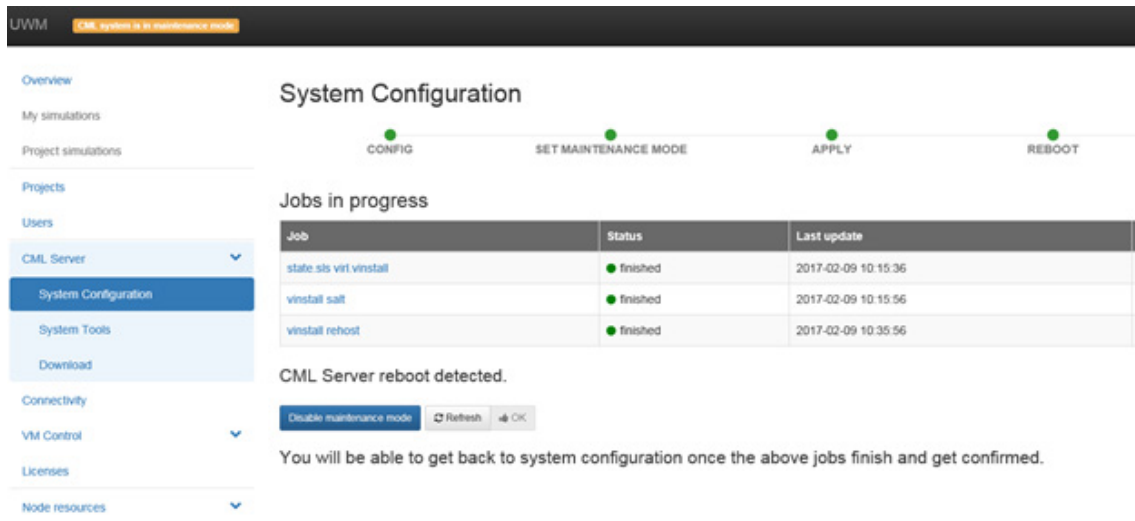
Reboot Close

417988

- Step 11** Click **Reboot** to reboot the system.

The System Configuration page is displayed.

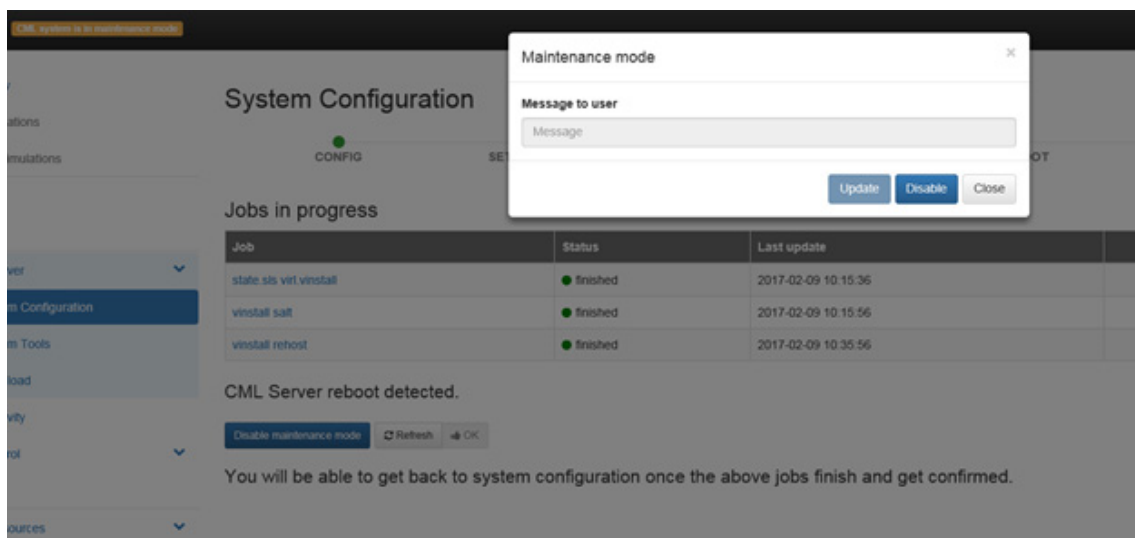
Figure 37: System Configuration Page



417989

- Step 12** Click **Disable Maintenance Mode**.
A Maintenance Mode dialog box is displayed.

Figure 38: Maintenance Mode Dialog Box

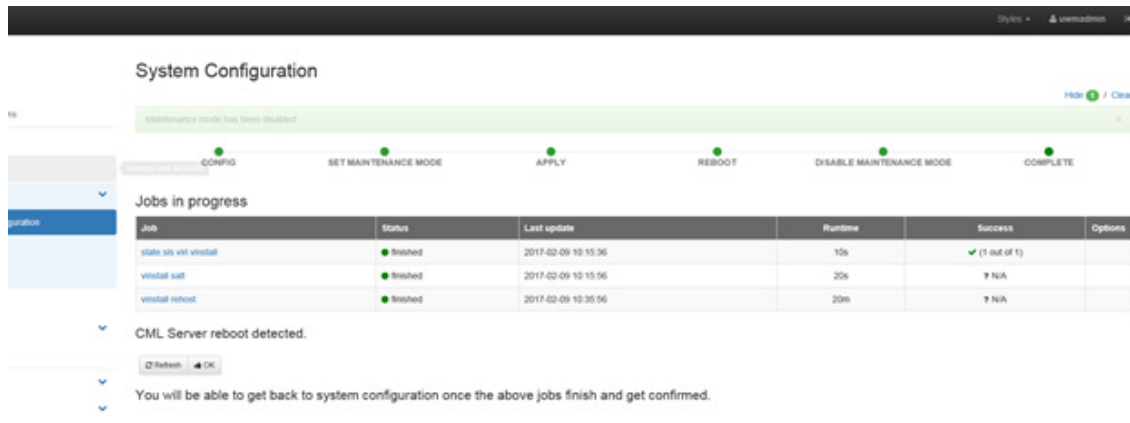


417990

- Step 13** Click **Disable**. The system is no longer in maintenance mode.

Your configuration is complete.

Figure 39: System Configuration Completed



The screenshot shows the 'System Configuration' page with a progress bar at the top indicating 'Maintenance mode has been disabled'. The progress bar has six steps: CONFIG, SET MAINTENANCE MODE, APPLY, REBOOT, DISABLE MAINTENANCE MODE, and COMPLETE. Below the progress bar, there is a 'Jobs in progress' table:

Job	Status	Last update	Runtime	Success	Options
state sta vst vinstat	finished	2017-02-09 10:15:36	10s	✓ (1 out of 1)	
vinstat salt	finished	2017-02-09 10:15:56	20s	⚠ N/A	
vinstat reboot	finished	2017-02-09 10:30:56	20m	⚠ N/A	

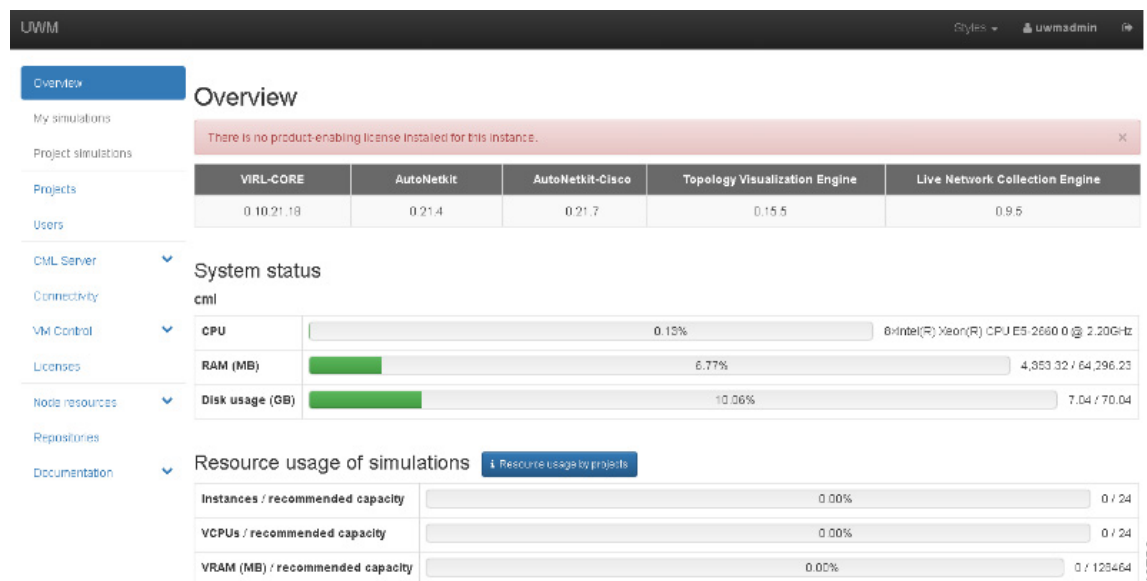
Below the table, there is a message: 'CML Server reboot detected.' and an 'OK' button. At the bottom, there is a message: 'You will be able to get back to system configuration once the above jobs finish and get confirmed.'

417991

Step 14 Click **OK** on the **System Configuration** page to return to the **System Configuration Controls** page.

Determine License Key Requirements

Returning to the User Workplace Management interface shows the server's current licensing status; the red banner indicates that there is no product licensing in place.



The screenshot shows the 'UWM' interface with the 'Overview' page selected. A red banner at the top indicates: 'There is no product-enabling license installed for this instance.' Below the banner, there is a table showing the status of various components:

	VIRL-CORE	AutoNetkit	AutoNetkit-Cisco	Topology Visualization Engine	Live Network Collection Engine
Projects	0.10.21.18	0.21.4	0.21.7	0.15.5	0.9.5

Below the table, there is a 'System status' section for the 'cml' instance:

Resource	Usage	Capacity
CPU	0.13%	8x Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz
RAM (MB)	6.77%	4,953.32 / 64,296.23
Disk usage (GB)	10.06%	7.04 / 70.04

Below the system status, there is a 'Resource usage of simulations' section:

Resource	Usage	Capacity
Instances / recommended capacity	0.00%	0 / 24
VCPUs / recommended capacity	0.00%	0 / 24
VRAM (MB) / recommended capacity	0.00%	0 / 125464

412758

To license the Cisco Modeling Labs server, complete the following steps:

Step 1 In the left pane, click **Licenses**.

The **Licenses** page is displayed.

Figure 40: Licenses Page

Licenses

[Register licenses](#)

License ID	Feature name	Node count	Expiry date	Remove license
You have no licenses registered.				
Active node capacity (will drop on)		0	-	

License verification results:

Product licensing status is
unlicensed.

Product license expires
expired.

Licensed Cisco VM capacity is
not available.

Failed to validate license status

Failed to fetch license data: The desired vendor daemon is down.

In case of unexpected license verification results, please consult the latest entries in the verification log below.

[Reload](#) [Hide log](#)

412764

Step 2 In the **Licenses** page, click **Register Licenses**.

Step 3 Record the **Host Name** and **Mac Address** for license key registration.

Figure 41: Information for License Key Registration

Register licenses

Licenses / Register

Licenses are required for enabling functionality on the Cisco Modeling Labs server.

The license is bound to this server instance, therefore you will need to provide the Host Name and MAC Address information when obtaining a license.

Host Name
cml

Mac Address
000c29f0642c

Paste the license key text into the area below and press register.

Licenses

Licenses

Register Cancel

412765

Use this information when completing the **Register Claim Certificates** instructions in the eDelivery Order Notification email to request your license key for use with the Cisco Modeling Labs server.

Two types of licenses are available, as shown in the following table.

Table 6: License Types

License Type	Description
Base Subscription	15-node capacity for initial deployment.
Capacity Subscription	10-node, 50-node, and 100-node bundles available. Note You can have any number or type of licenses. Licenses are determined by the node capacity you want to deploy.

You will receive your license key as an attachment via an email.

- Step 4** Open the attachment in a text editor and copy all of the contents.
- Step 5** Return to the **Register Licenses** page and paste the details into the **Licenses** text area.

Figure 42: License Key Details

Licenses are required for enabling functionality on the Cisco Modeling Labs server.

The license is bound to this server instance, therefore you will need to provide the Host Name and MAC Address information when obtaining a license.

Host Name
cml

Mac Address
000c29f0642c

Paste the license key text into the area below and press register.

Licenses

```
SERVER cml 000c29f0642c
USE_SERVER
VENDOR cisco
INCREMENT CML_CORPORATE cisco 1.0 20-jul-2016 1 HOSTID=HOSTNAME=cml \
NOTICE="<LicFileID>20160421204341718</LicFileID><LicLineID>1</LicLineID> \
<PAK></PAK>" SIGN="1391 1E7E BBFC DC3D 83F0 C35E 152F 4ED0 \
AB96 BFCA 3ABF 5111 6986 3A27 068D 15F3 AB58 5B4A F946 FE36 \
976E 9C50 80E4 FC94 4B9B 0F77 F07B 05B9 A6F6 5E88"
INCREMENT CML_CISCO_VM_CAPACITY cisco 1.0 20-jul-2016 15 \
HOSTID=HOSTNAME=cml \
NOTICE="<LicFileID>20160421204341718</LicFileID><LicLineID>2</LicLineID> \
<PAK></PAK>" SIGN="0BB0 F56A F6B6 44FD BB95 ECCF 4053 DCF7 \
683F 69BF 92B2 E70C CB43 FCA3 7F3E 153D 099A 97BD B631 E27F \
5BE2 A26C 4AE8 CC2D DF58 27CC 7269 CC36 4D21 04FA"
```

412766

- Step 6** Click **Register** to register the license key.
- Note** We recommend that you add the Base Subscription license first.

Under **Licenses**, you will see the license that is added, the number of nodes permissible, and an expiry date for the license.

Figure 43: Licenses Applied

Licenses

Licenses successfully registered. ✕

Register licenses

License ID	Feature name	Node count	Expiry date	Remove license
20160421204341718	CML_CORPORATE	-	20-Jul-2016	Remove
	CML_CISCO_VM_CAPACITY	15	20-Jul-2016	
Active node capacity (will drop on)		15	20-Jul-2016	

License verification results:

Product licensing status is
licensed as CML_CORPORATE.
Product license expires
in **89** days.
Licensed Cisco VM capacity is
15 nodes.

412767

Step 7 Repeat Steps 4 – 6 for each license file received from the registration process. Verify that the **Licenses** page correctly reports the applied node count and expiration dates.

Step 8 Click **Log Out** to exit the **User Workspace Management** interface.