



## 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 11](#)
- [\(Optional\) Configure Static IP, page 20](#)
- [\(Optional\) Prepare for an Interface-Constrained Installation, page 21](#)
- [Reconfigure Default Console Resolution, page 23](#)
- [Start the User Workspace Management Interface, page 24](#)
- [Determine License Key Requirements, page 33](#)

## 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 C420-M3

- Cisco UCS C420-M4
- 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

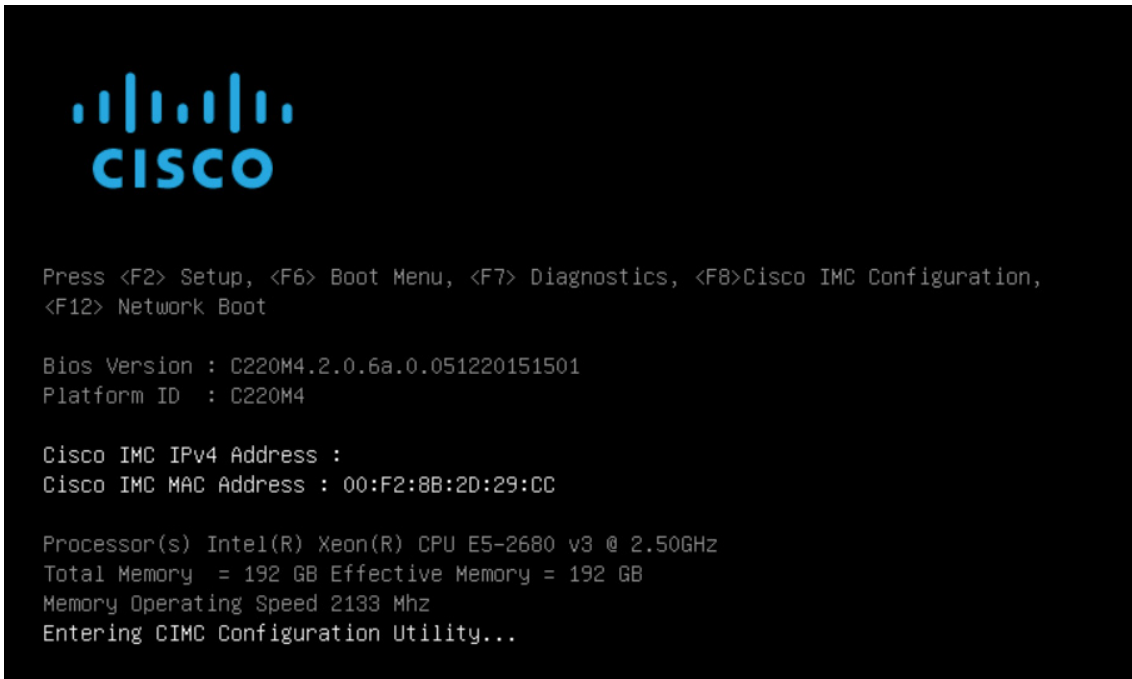
If not previously used, the server's Cisco Integrated Management Controller (CIMC) must be provisioned as follows:

- 
- 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.



**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 LOM:     [ ]                    Active-standby: [ ]
Cisco Card:
  Riser1:       [ ]                    Active-active:  [ ]
  Riser2:       [ ]                    VLAN (Advanced)
  MLOm:         [ ]                    VLAN enabled:   [ ]
  Shared LOM Ext: [ ]                    VLAN ID:        1
                                           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.

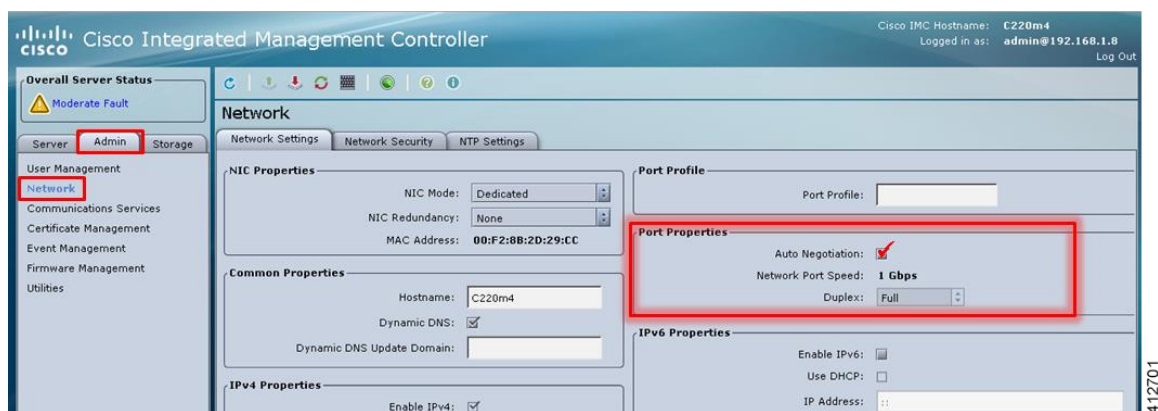
**Figure 5: Verify BIOS Configuration**



#### 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**



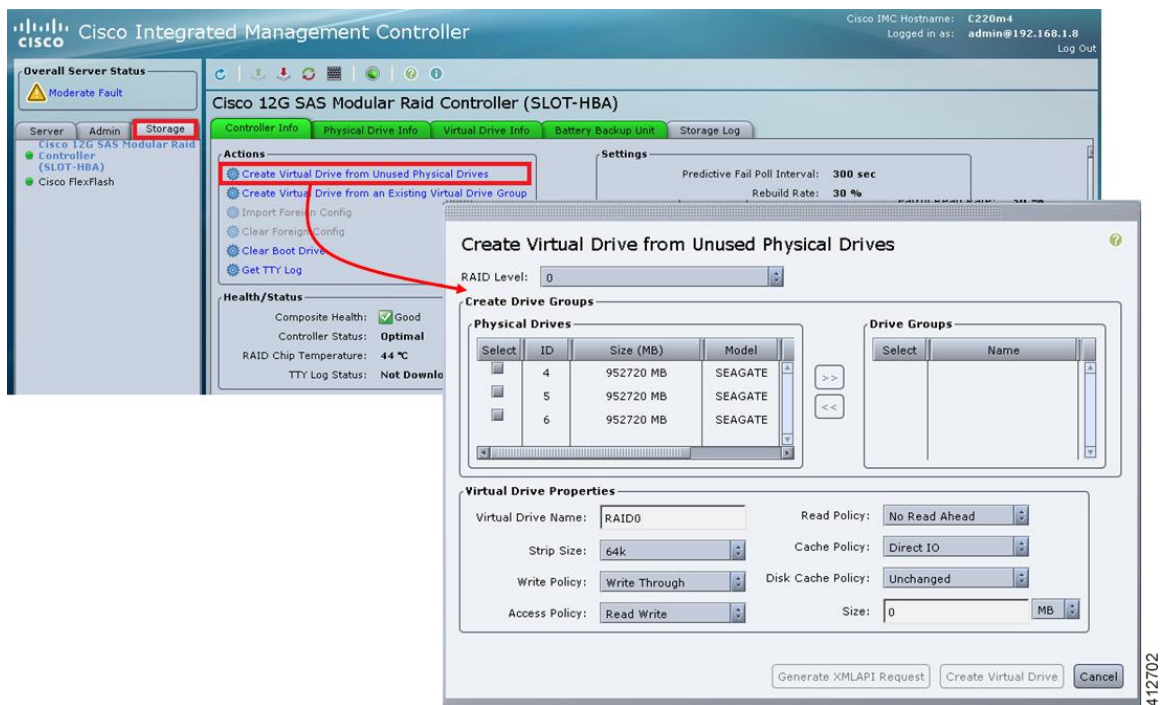
#### Step 5

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) 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.
- b) 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**

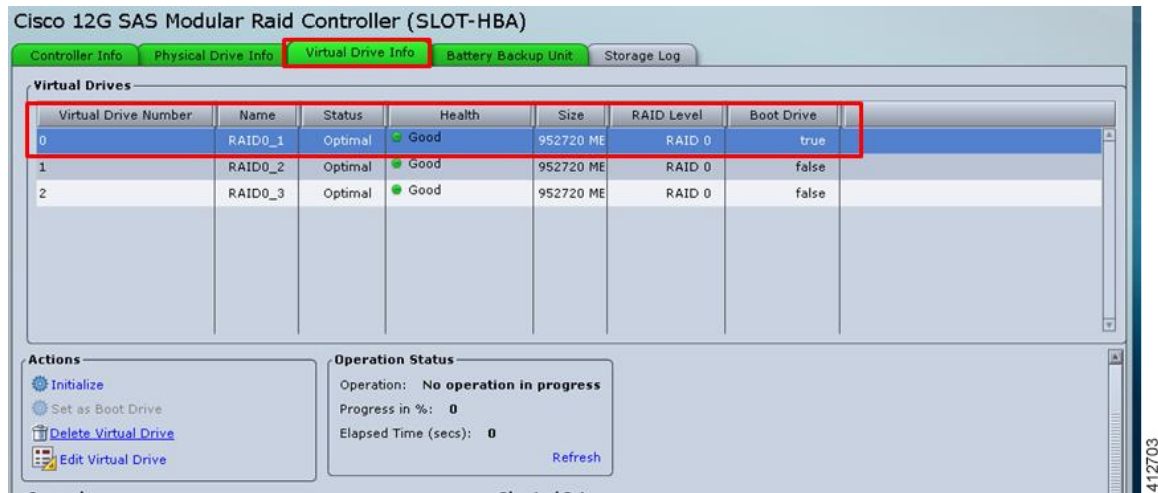


Depending on the selected RAID level, this can be one or more selections. When the array members have been selected, click >> to allocate them to the Drive Group. With the Drive Group membership defined, click **Create Virtual Drive**. Clicking the Virtual Drive Info tab displays a report of the Virtual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



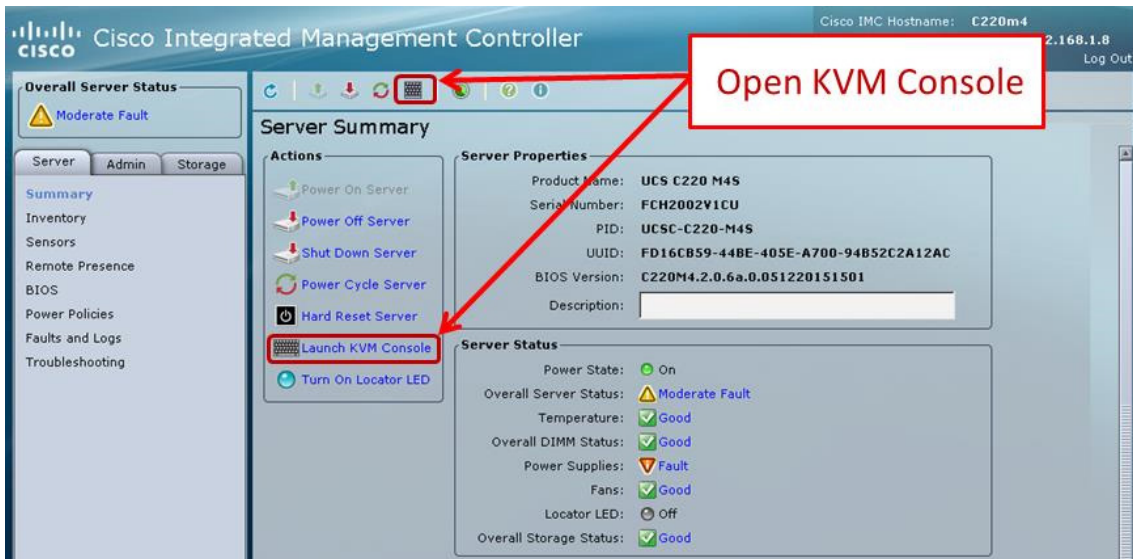
## Map the Cisco Modeling Labs ISO Disk Image

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.

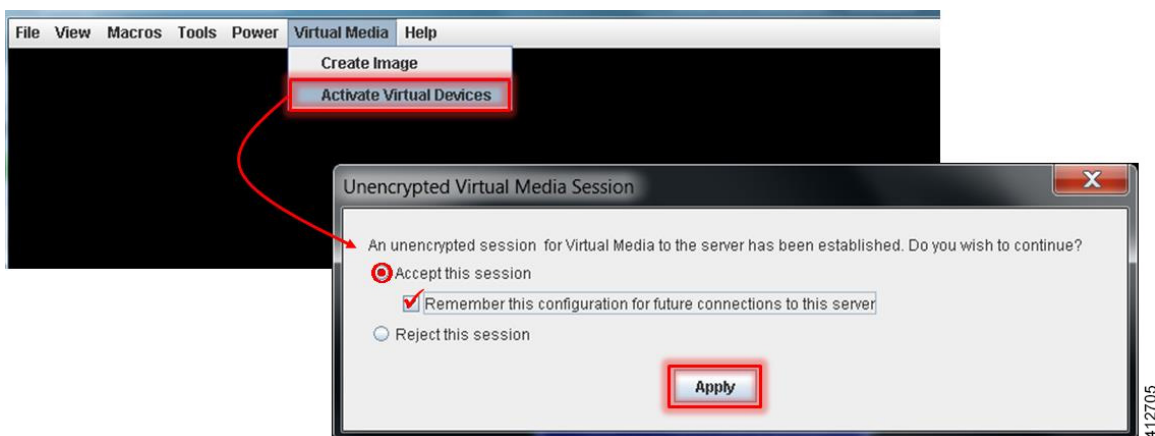
Figure 9: KVM Console



**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.

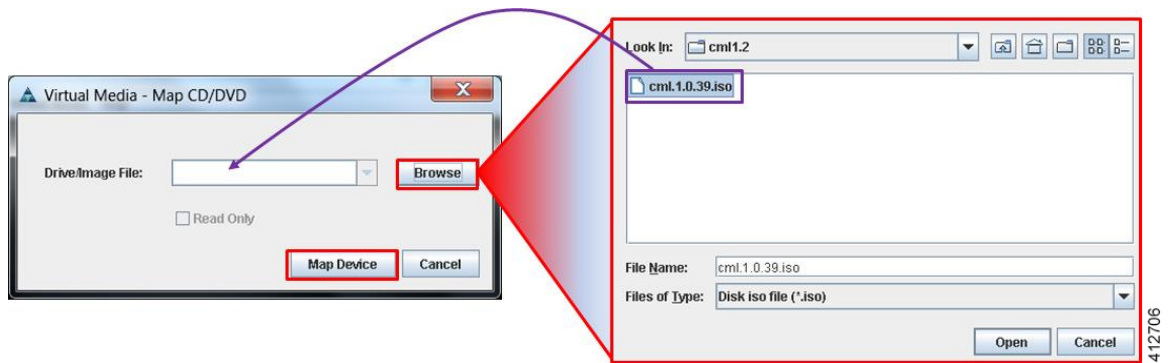
**Step 2** In the KVM Console window, click **Virtual Media** from the menu bar. From the drop-down, choose the **Activate Virtual Devices**. Acknowledge the **Unencrypted Virtual Media Session** warning and click **Apply**, as shown.

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 VIRT Installer

The VIRT Installer screen is displayed on the directly attached console. There are four options available:

- **Live**—Boots a non-persistent VIRT instance into the server. This method allows for changes to be made before the install is initiated. An **Install System to HDD** icon on the booted Ubuntu desktop initiates the software installation process.
- **Install**—Skips the initial Ubuntu load and directly initiates the system installation process.
- **Memtest**—Performs a test of the system DRAM.

- **Hd**—Aborts the installation and restarts the system with the first hard disk.

**Figure 12: VIRL Installer Window**



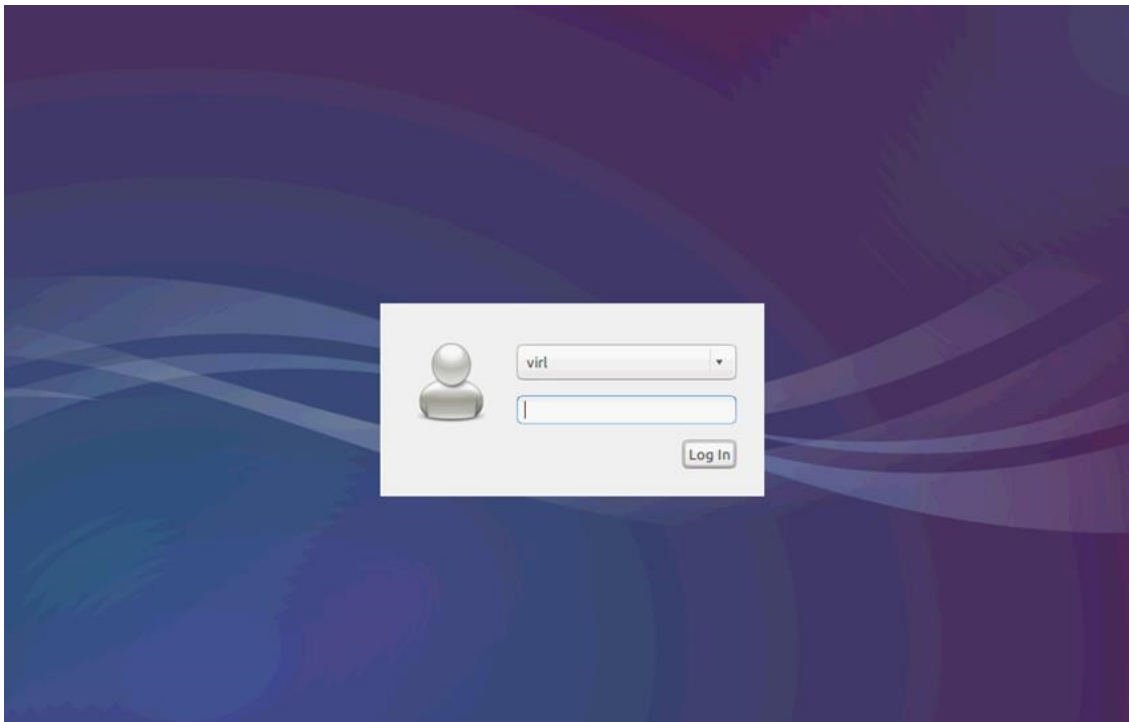
**Note**

From this point onwards, installation actions should be performed using the directly attached console. Attempting to perform the installation process using the CIMC's virtual KVM console may trigger a virtual screen resolution fault.

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

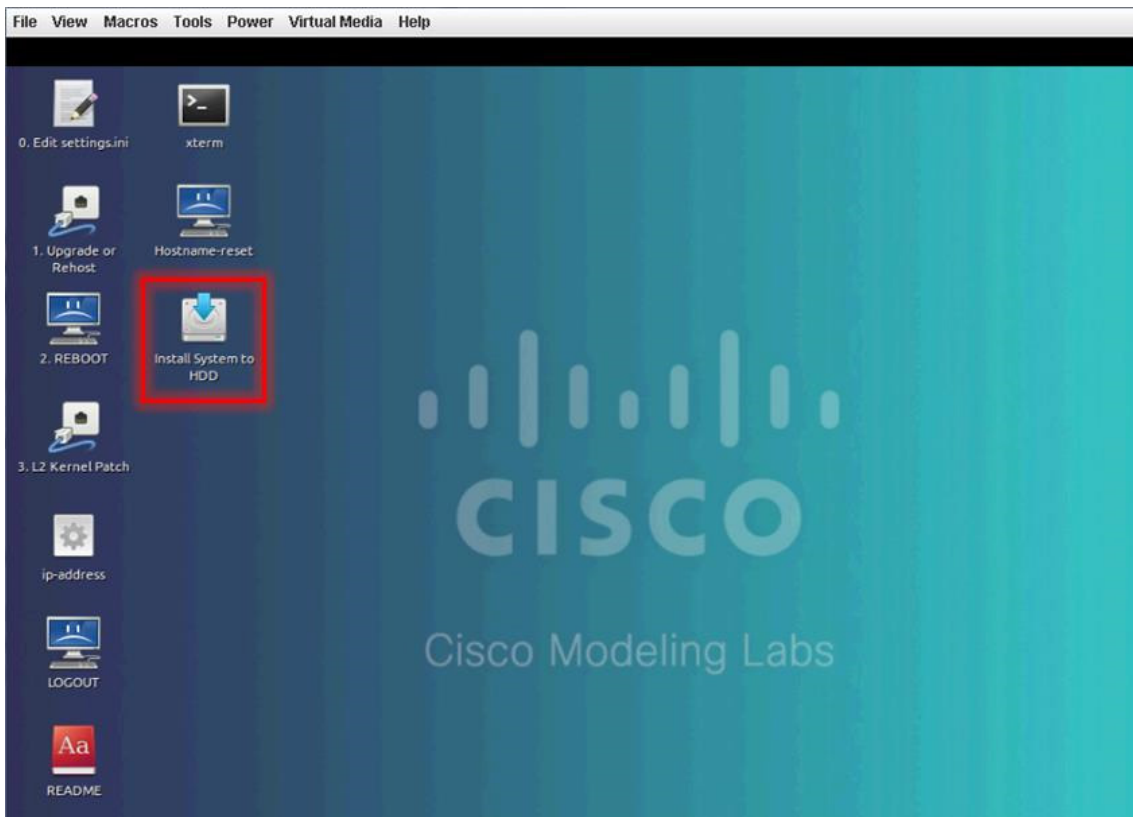
- Step 1** Choose **Install Option 1: live - boot VIRL for changes before install**. When the log in screen is displayed, log into the virtual machine using username virl and password VIRL.

*Figure 13: Log In Window*



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

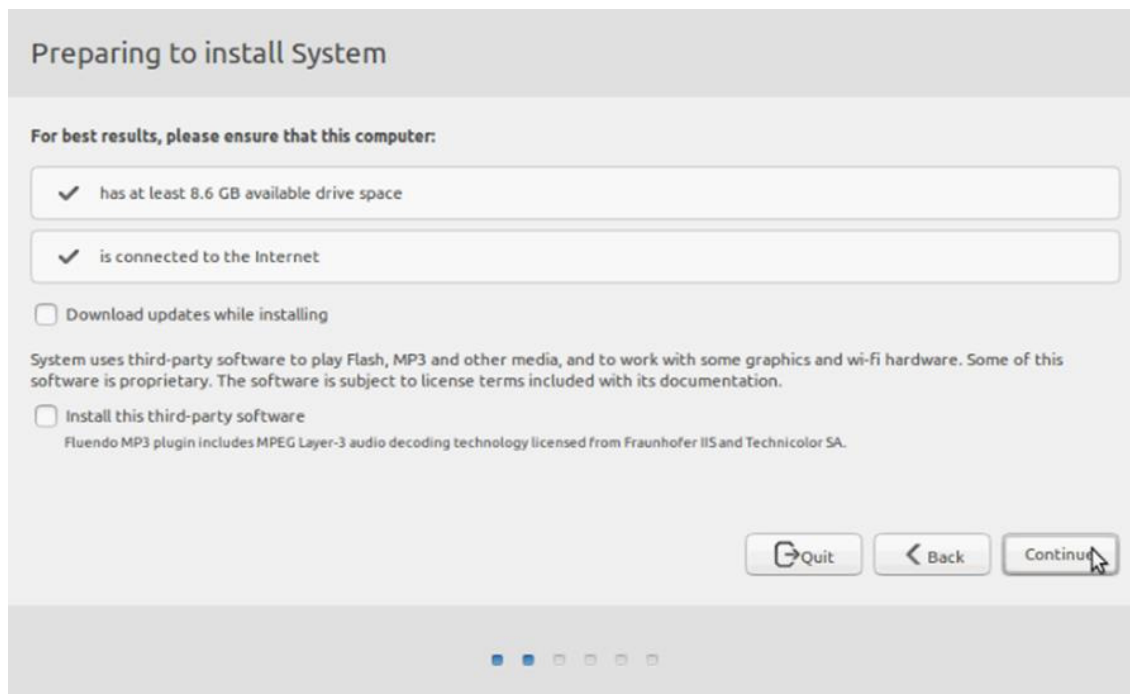
Figure 14: Desktop Main Menu



**Step 3** In the **Welcome** window, choose the applicable language from the list and click **Continue**.

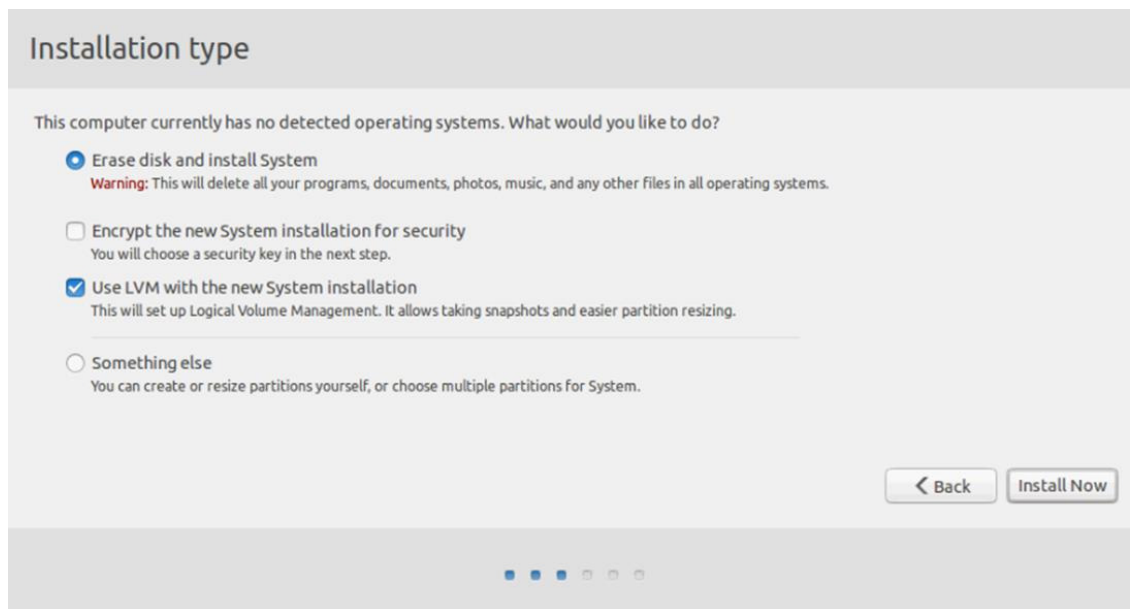
**Step 4** The **Preparing to install System** window will request affirmation that minimum requirements have been met. The recommended storage for Cisco Modeling Labs is 250G or larger. Do not enable download updates or third-party software while installing. Click **Continue**.

Figure 15: Preparing to Install System Window

**Step 5**

In the **Installation Type** window, the Installation type should be set to **Erase disk and Install System**. We recommend that you enable the **Use LVM with the new System installation** option, to setup Logical Volume Management. Click **Install Now**.

Figure 16: Installation Type Window



**Step 6** Confirm the disk partitioning information displayed and click **Continue**.

**Figure 17: Write the Changes to Disks? Window**

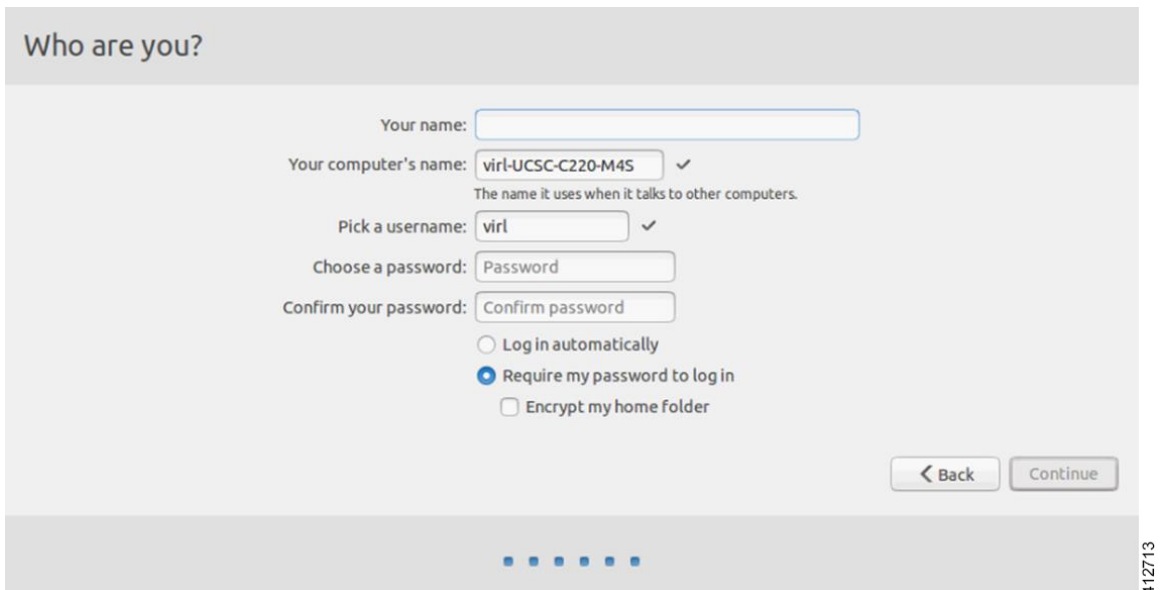


**Step 7** In the **Where are you?** window, enter the applicable time zone, and click **Continue**.

**Step 8** In the **Keyboard Layout** window, choose the applicable locale-specific keyboard layout to use by clicking the corresponding option from the **Choose your keyboard layout** list, and click **Continue**.

**Step 9** In the **Who are you?** window, enter values for the fields exactly as described here:

**Figure 18: Who are you? Window**



- In the **Your name** field, enter the value **cml** or a name of your choice.
- In the **Your computer's name** field, enter the value: **cml**



- In the **Pick a username** field, enter the value: **virl**
- In the **Choose a password** field, enter the value: **VIRL**
- In the **Confirm your password** field, enter the value: **VIRL**
- Uncheck the **Log in automatically** radio button if it is selected.
- Select the **Require my password to log in** radio button.
- Uncheck the **Encrypt my home folder** check box if it is selected.

**Caution** No variations on the these values are permitted.

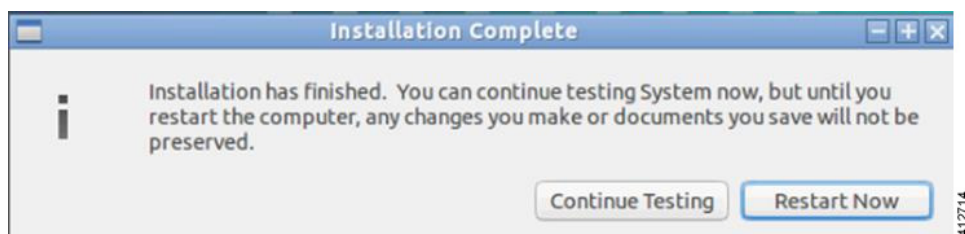
**Note** Ensure that the computer host name is set to **cml**. Failure to set the computer name to cml will prevent the OpenStack services from installing correctly and the installation will fail. If desired, a different host name can be set later as described in the Customization section.

Click **Continue** to start the installation. This initiates the image transfer process and copies the files to the UCS Server.

A status window indicates the progress of the installation. Once the file transfer has completes, the system detects the running hardware; applies necessary adaptations, and performs a post-install cleanup.

**Step 10** The **Installation Complete** notification indicates a successful installation. Click **Restart Now** to effect a reboot using the installed image.

**Figure 19: Installation Complete Window**



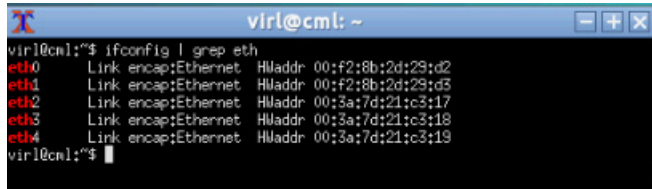
**Step 11** If you choose **Install Option 2: install - start the VIRL installer directly**, this bypasses booting a transient instance of the server and immediately starts the installation. Steps 3 -10 are performed as described above.

## 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.

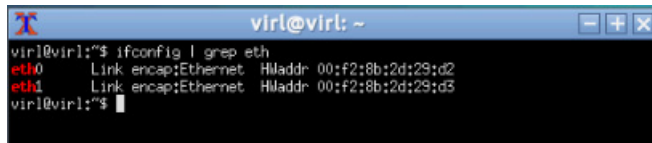
**Figure 20: List of Five Interfaces**



```
virt@cml: ~  
virt@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  
virt@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 21: List of Two Interfaces Only**



```
virt@virt: ~  
virt@virt:~$ 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  
virt@virt:~$
```

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 22: 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
  
```

412717

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:

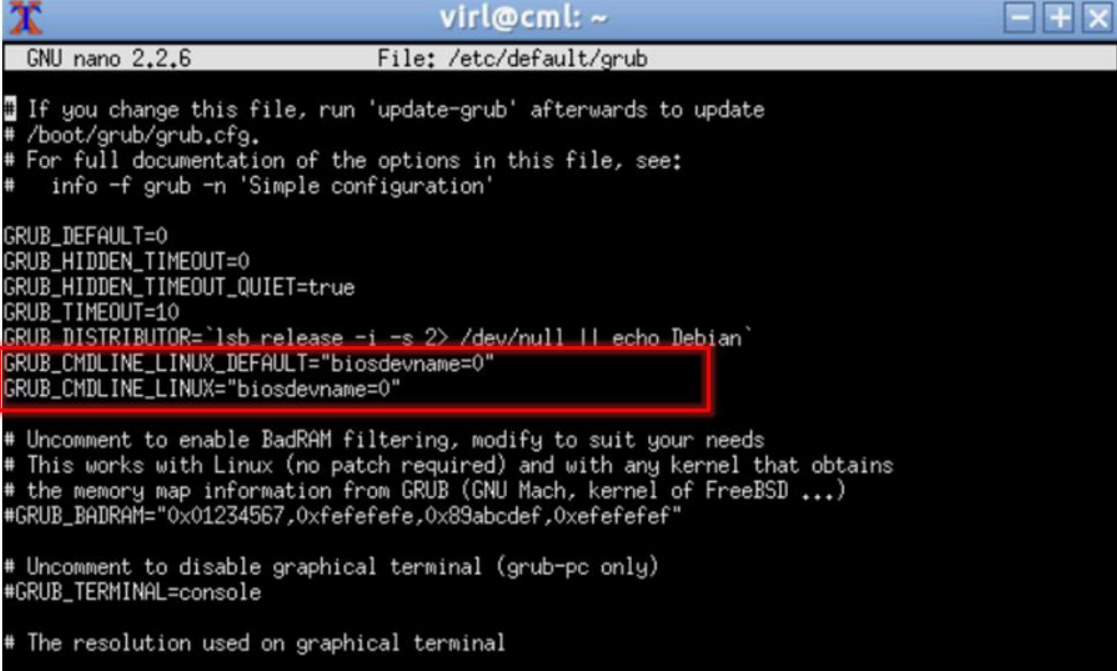
```

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 23: 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) Configure Static IP

In accordance with best practices and to account for a possible lack of DHCP services, it is recommended that the eth0 interface be configured with a static IP address, as follows:

**Step 1** Start the virtual machine and log in using the username virl and the password VIRL.

**Note** The Ubuntu Software Updater may start automatically upon login. It is safe to close the Updater and continue with the installation.

- Step 2** Click the **xterm** icon to open a terminal window.
- Step 3** Change to the network interfaces configuration directory: `cd /etc/network`
- Step 4** Open the interfaces configuration file for editing: `sudo nano interfaces`
- Step 5** Change the eth0 addressing method to static: `iface eth0 inet static`
- Step 6** Provide the static IP address: `address n.n.n.n`
- Step 7** Provide the static IP address netmask: `netmask mmm.mmm.mmm.mmm`
- Step 8** Provide the default IP gateway address: `gateway g.g.g.g`  
**Note** If no default IP gateway address is provided, do not configure any DNS name-server addresses unless they are reachable on the local subnet. Doing otherwise will lead to unpredictable behavior as various Cisco Modeling Labs services fruitlessly attempt to resolve names.
- Step 9** Provide valid reachable DNS name-server addresses: `dns-nameservers a.a.a.a b.b.b.b`
- Step 10** Enter Ctrl-X to exit.
- Step 11** Enter Y and Enter to confirm saving the interfaces file and exit.
- Step 12** Enter `sudo reboot now` to reboot the virtual machine in preparation for the remaining installation steps.

## (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:

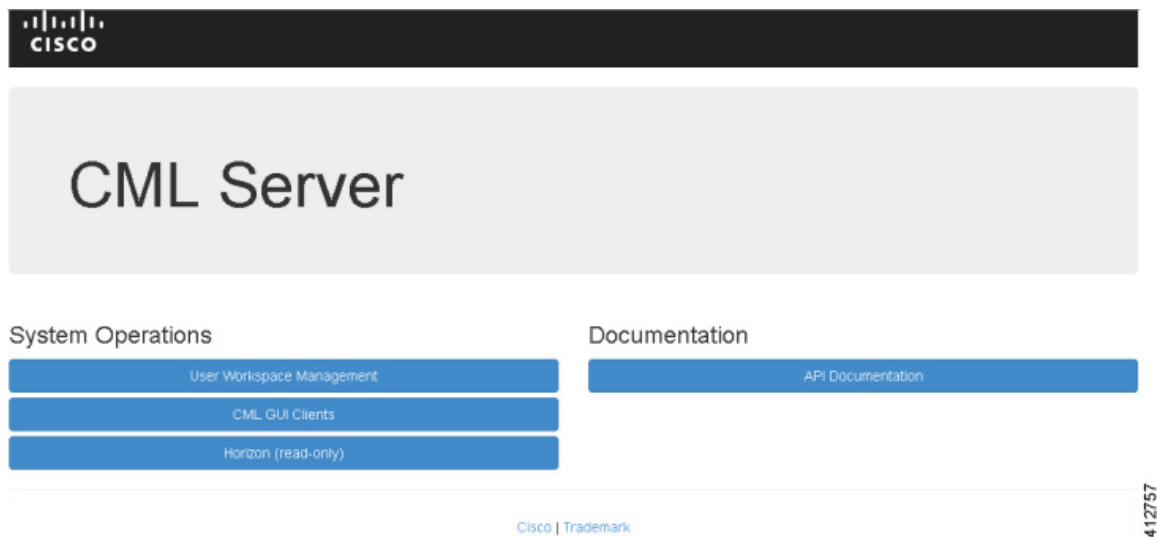
- 
- Step 1** In the KVM Console window, click **Macros** on the menu bar.
  - Step 2** From the drop-down menu, choose the **Macros > Static Macros > Ctrl-Alt-F > Ctrl-Alt-F2**, followed by **<Enter>** to switch the vConsole to a command line interface (CLI). If necessary, login with `virl/VIRL`.
  - 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`
-

# Start 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.)

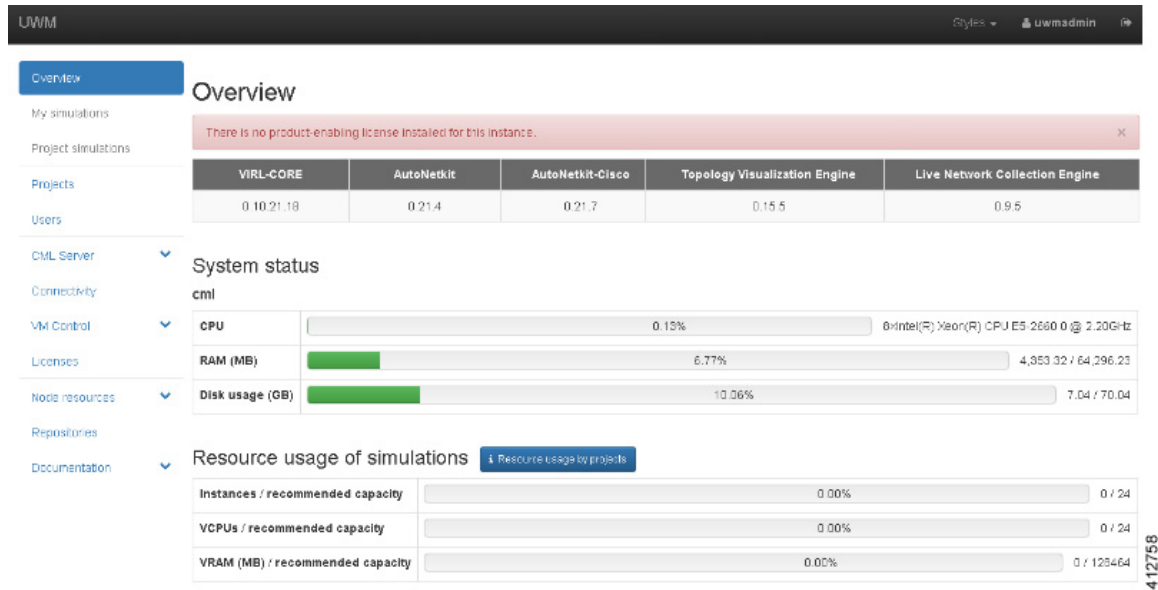
*Figure 24: CML Server Main Menu*





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

**Figure 25: 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 26: System Configuration Controls**

The screenshot displays the 'System Configuration Controls' interface. On the left, a navigation sidebar is visible with 'CML Server' expanded to 'System Configuration'. The main content area shows various configuration parameters for the system. The 'System' tab is selected, and an 'Apply Changes' button is present in the top right. The configuration fields are as follows:

Parameter	Value
Hostname	cml
Domain Name	cisco.com
NTP Server	ntp.esl.cisco.com
Ramdisk enabled	<input type="checkbox"/>
VNC enabled	<input type="checkbox"/>
VNC password	letmein
Primary Ethernet port	eth0
Use DHCP on primary Ethernet port?	<input type="checkbox"/>
Static IP address	172.23.81.101
Primary port network	172.23.81.64
Primary port netmask	255.255.255.192
Primary port gateway	172.23.81.65

**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	Enable this option if you have at least 16 GB free RAM, 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.

Parameter	Default	Description
VNC Password	letmein	Enter the password for the VNC server.
Primary Ethernet Port	eth0	Enter the primary ethernet port.
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://mkt.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.

Parameter	Default	Description
Flat Network Netmask	255.255.255.0	Enter the Flat network netmask.
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.

Parameter	Default	Description
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.
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 **VIRL Services** to configure the port numbers for VIRL services.

**Table 3: VIRL Services Configuration Parameters**

Parameter	Default	Description
VIRL Apache Server Port	80	Enter the number of the VIRL Apache server port.
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.
Nova Websocket VNC Port	19407	Enter the TCP port number for the websocket-based VNC console connections.

**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.
Docker Registry Port	19397	Enter the port number for the docker registry.

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

**Table 5: Resources Configuration Parameters**

Parameter	Default	Description
RAM Overcommit Value	2	Enter a value. The value range is 1 to 4. The value format is floating, such as 2.0. Overcommitting RAM allows you to run more virtual machines in the available memory. However, running more virtual machines reduces overall performance. We recommend that you change this value in small increments since setting a high initial value may result in the system becoming unresponsive.
Reset RAM Overcommit	Unchecked	Use this option to reset the RAM overcommit value to the default built-in value. The reset occurs after you have applied your changes.
vCPU Overcommit Value	3	Enter a value. The value range is 1 to 30. The value format is floating, such as 2.0. Overcommitting vCPU allows you to run more virtual machines in the available CPU capacity. However, running more virtual machines reduces overall performance. We recommend that you change this value in small increments since setting a high initial value may result in the system becoming unresponsive.
Reset vCPU Overcommit	Unchecked	Use this option to reset the vCPU overcommit value to the default built-in value. The reset occurs after you have applied your changes.
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 " <code>&lt;username&gt;:&lt;password&gt;</code> ".
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**. A summary of the changes is presented, showing the previous parameters settings and the new values being applied. Having confirmed that all changes are correct, click **Apply Changes** at the bottom of the page.

**Figure 27: Apply Changes Made**

The screenshot shows the UWM System Configuration page. The left sidebar contains navigation options: Overview, My simulations, Project simulations, Projects, Users, CML Server (expanded), System Configuration (selected), System Status, Connectivity, VM Control (expanded), Licenses, Node resources (expanded), Repositories, and Documentation (expanded). The main content area is titled "System Configuration" and shows a "Changes:" section with a table of updates:

Field	Current value	New value
Primary port gateway	N/A	192.168.1.1
Primary port netmask	N/A	255.255.255.0
Primary port network	N/A	192.168.1.0
Ramdisk enabled	False	True
Static IP address	N/A	192.168.1.68
Use DHCP on primary Ethernet port?	True	False
VNC enabled	False	True

Below the table is a "Changes impact:" section with a text area containing:

```

vinstall salt
vinstall rehost
  
```

A note states: "NOTE: You will need to reboot the CML Server after the changes." At the bottom, there are three buttons: "Go back to configuration", "Apply Changes", and "Cancel".

412759

A confirmation page verifies the configuration acceptance and schedules the listed update jobs.

**Figure 28: Confirmation of Changes Page**

The screenshot shows the UWM System Configuration page after applying changes. The left sidebar is the same as in Figure 27. The main content area is titled "System Configuration" and shows two green notification banners:

- Viri.ini was updated
- System configuration jobs were scheduled

Below the banners is a "Jobs in progress" section with a table:

Job	Status	Last update	Runtime	Success	Options
vinstall salt	● scheduled	2016-04-22 00:39:45	—	↑ N/A	Cancel
vinstall rehost	● scheduled	2016-04-22 00:39:45	—	↑ N/A	Cancel

A note states: "NOTE: You will have to reboot the CML Server after these jobs finish." Below the table is a "Refresh" button. At the bottom, a message says: "Please wait... You will be able to get back to system configuration once the above jobs finish and get confirmed."

412760



Click the **Refresh** button to display the current status of the scheduled **Jobs in progress**.

**Figure 29: List of Jobs in Progress**

Jobs in progress

Job	Status	Last update	Runtime
vinstall salt	● finished	2016-04-22 00:40:01	10s
vinstall rehost	● running	triggered at 2016-04-22 00:40:02	13m 1s...

412761

When complete, the status updates to **Finished**.

**Figure 30: Jobs Completed**

Jobs in progress

Job	Status	Last update	Runtime
vinstall salt	● finished	2016-04-22 00:40:01	10s
vinstall rehost	● finished	2016-04-22 00:56:10	16m 8s

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



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

412762

Click **OK** to return to the **System Configuration Controls** page, after confirmation that all scheduled jobs were completed and cleared. At this point, the Cisco Modeling Labs server must be rebooted.

**Figure 31: List of Jobs in Progress**

System Configuration Controls



412763

## Step 9

Return to the Cisco Modeling Labs virtual machine console and open an xterm window. Initiate a system reboot with the `sudo reboot now` command. Alternatively, double-click on the **2. REBOOT** icon on the desktop. When the system reboot has completed, return to the **User Workspace Management** interface to confirm the custom settings.

# 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 Overview page. The left sidebar contains navigation options: Overview (selected), My simulations, Project simulations, Projects, Users, CML Server, Connectivity, VM Control, Licenses, Node resources, Repositories, and Documentation. The main content area is titled 'Overview' and features a warning message: 'There is no product-enabling license installed for this instance.' Below this is a table of license keys:

VIRL-CORE	AutoNetkit	AutoNetkit-Cisco	Topology Visualization Engine	Live Network Collection Engine
0 10.21.18	0 21.4	0 21.7	0.15.5	0.9.5

Below the table is the 'System status' section for the 'cml' node, showing resource usage:

Resource	Usage	Capacity
CPU	0.13%	0 / 24
RAM (MB)	6.77%	4,353.32 / 64,296.23
Disk usage (GB)	10.26%	7.04 / 70.04

The 'Resource usage of simulations' section shows:

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

The page number 412758 is visible on the right side.

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 32: 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 33: 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

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. <b>Note</b> 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 34: 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 35: 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.