



Installation and Initial Configuration

This chapter describes how to initially install and configure your Cisco 3365 Mobility Services Engine.

This chapter contains these sections:

- [Unpacking and Inspecting the Cisco MSE 3365, page 2-2](#)
- [Preparing for Cisco MSE 3365 Installation, page 2-2](#)
- [Installing the Cisco MSE 3365 in a Rack, page 2-4](#)
- [Initial Setup, page 2-11](#)
- [NIC Modes, page 2-17](#)
- [Configuring the Mobility Services Engine, page 2-17](#)
- [Manually Stopping Mobility Services Engine Software, page 2-23](#)
- [Manually Restarting a Running Mobility Services Engine, page 2-24](#)
- [Updating Mobility Services Engine Software, page 2-24](#)
- [Recovering a Lost Root Password, page 2-26](#)



Note

For configuration details beyond initial installation, refer to the appropriate mobility services configuration guide at:

http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

Rack Warnings



Warning

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety: (1) This unit should be mounted at the bottom of the rack if it is the only unit in the rack. (2) When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack. (3) If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack. Statement 1006.



Caution

To reduce the risk of personal injury or equipment damage when unloading a rack, at least two people are needed to safely unload the rack from the pallet.

**Caution**

To prevent damage, ensure that water or excessive moisture cannot get into the mobility services engine.

Unpacking and Inspecting the Cisco MSE 3365

**Caution**

When handling internal Cisco MSE 3365 components, wear an ESD strap and handle modules by the carrier edges only.

**Tip**

Keep the shipping container, in case the Cisco MSE 3365 requires shipping in the future.

**Note**

The chassis is thoroughly inspected before shipment. If any damage occurred during transportation or any items are missing, contact your customer service representative immediately.

To unpack the Cisco MSE 3365, follow these steps.

-
- Step 1** Remove the Cisco MSE 3365 from its cardboard container and save all packaging material.
- Step 2** Check for damage and report any discrepancies or damage to your customer service representative. Have the following information ready:
- Invoice number for shipper (see the packing slip)
 - Serial number of the damaged unit
 - Description of the damage
 - Effect of damage on the installation.
-

Preparing for Cisco MSE 3365 Installation

This section provides information about preparing for Cisco MSE 3365 installation, and it includes the following topics:

- [Installation Guidelines, page 2-3](#)
- [Rack Requirements, page 2-3](#)
- [Equipment Requirements, page 2-4](#)
- [Slide Rail Adjustment Range, page 2-4](#)

Installation Guidelines



Warning

To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 40° C (104° F).

Statement 1047



Warning

The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.

Statement 1019



Warning

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 250 V, 15 A.

Statement 1005



Warning

Installation of the equipment must comply with local and national electrical codes.

Statement 1074



Caution

To ensure proper airflow it is necessary to rack the MSE 3365 using rail kits. Physically placing the units on top of one another or “stacking” without the use of the rail kits blocks the air vents on top of Cisco MSE 3365, which could result in overheating, higher fan speeds, and higher power consumption. We recommend that you mount your Cisco MSE 3365 on rail kits when you are installing them into the rack because these rails provide the minimal spacing required between the MSE 3365s. No additional spacing between Cisco MSE 3365s is required when you mount the units using rail kits.



Caution

Avoid UPS types that use ferroresonant technology.

When you are installing an MSE 3365, use the following guidelines:

- Plan your site configuration and prepare the site before installing the Cisco MSE 3365.
- Ensure that there is adequate space around Cisco MSE 3365 to allow for servicing the MSE 3365 and for adequate airflow. The airflow in the Cisco MSE 3365 is from front to back.
- Ensure that the air-conditioning meets the thermal requirements listed in the Cisco MSE 3365 Specifications.
- Ensure that the cabinet or rack meets the requirements listed in the “Rack Requirements” section.
- Ensure that the site power meets the power requirements listed in the Cisco MSE 3365 Specifications. If available, you can use an uninterruptible power supply (UPS) to protect against power failures.

Rack Requirements

This section provides the requirements for standard open racks:

The rack must be of the following type:

- A standard 19-in. (48.3-cm) wide, four-post EIA rack, with mounting posts that conform to English universal hole spacing, per section 1 of ANSI/EIA-310-D-1992.
- The rack post holes can be square 0.38-inch (9.6 mm), round 0.28-inch (7.1 mm), #12-24 UNC, or #10-32 UNC when you use the supplied slide rails.
- The minimum vertical rack space per Cisco MSE 3365 must be one RU, equal to 1.75 in. (44.45 mm).

Equipment Requirements

The slide rails shipped with the Cisco MSE 3365 do not require tools for installation.

Slide Rail Adjustment Range

The slide rails shipped with the Cisco MSE 3365 have an adjustment range of 24 to 36 inches (610 to 914 mm).

Installing the Cisco MSE 3365 in a Rack

This section contains the following sections:

- [Installing the Slide Rails, page 2-4](#)
- [Installing the Cable Management Arm \(Optional\), page 2-7](#)
- [Reversing the Cable Management Arm \(Optional\), page 2-8](#)

Installing the Slide Rails

This section describes how to install the Cisco MSE 3365 in a rack using the rack kits that are sold by Cisco.



Warning

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

This unit should be mounted at the bottom of the rack if it is the only unit in the rack.

When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.
Statement 1006

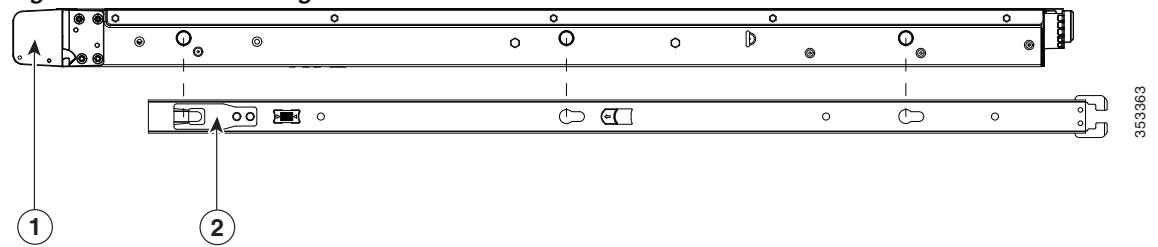
Step 1

Attach the inner rails to the sides of the Cisco MSE 3365:

1. Align an inner rail with one side of the Cisco MSE 3365 so that the three keyed slots in the rail align with the three pegs on the side of the Cisco MSE 3365 (see Figure 2-1).
2. Set the keyed slots over the pegs, and then slide the rail toward the front to lock it in place on the pegs. The front slot has a metal clip that locks over the front peg.

3. Install the second inner rail to the opposite side of the Cisco MSE 3365.

Figure 2-1 Attaching Inner Rail to Side of Cisco MSE 3365

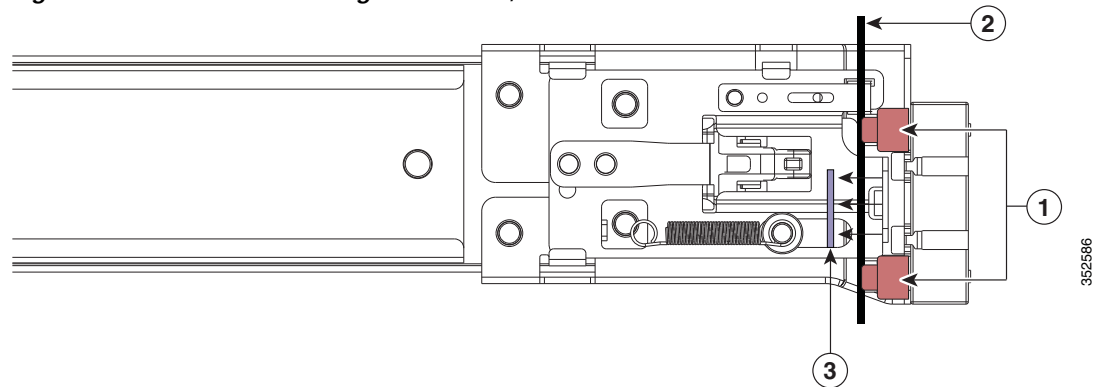


1	Front of Cisco MSE 3365	2	Locking clip on inner rail
---	-------------------------	---	----------------------------

- Step 2** Open the front securing plate on both slide-rail assemblies. The front end of the slide-rail assembly has a spring-loaded securing plate that must be open before you can insert the mounting pegs into the rack-post holes (see [Figure 2-2](#)).

On the *outside* of the assembly, push the green arrow button toward the rear to open the securing plate.

Figure 2-2 Front Securing Mechanism, Inside of Front End



1	Front mounting pegs	3	Securing plate shown pulled back to open position
2	Rack post		

- Step 3** Install the outer slide rails into the rack:

- a. Align one slide-rail assembly front end with the front rack-post holes that you want to use.

The slide rail front-end wraps around the outside of the rack post and the mounting pegs enter the rack-post holes from the outside-front (see [Figure 2-2](#)).



Note The rack post must be between the mounting pegs and the *open* securing plate.

- b. Push the mounting pegs into the rack-post holes from the outside-front.

- c. Press the securing plate release button, marked PUSH. The spring-loaded securing plate closes to lock the pegs in place.
- d. Adjust the slide-rail length, and then push the rear mounting pegs into the corresponding rear rack-post holes. The slide rail must be level front-to-rear.

The rear mounting pegs enter the rear rack-post holes from the inside of the rack post.

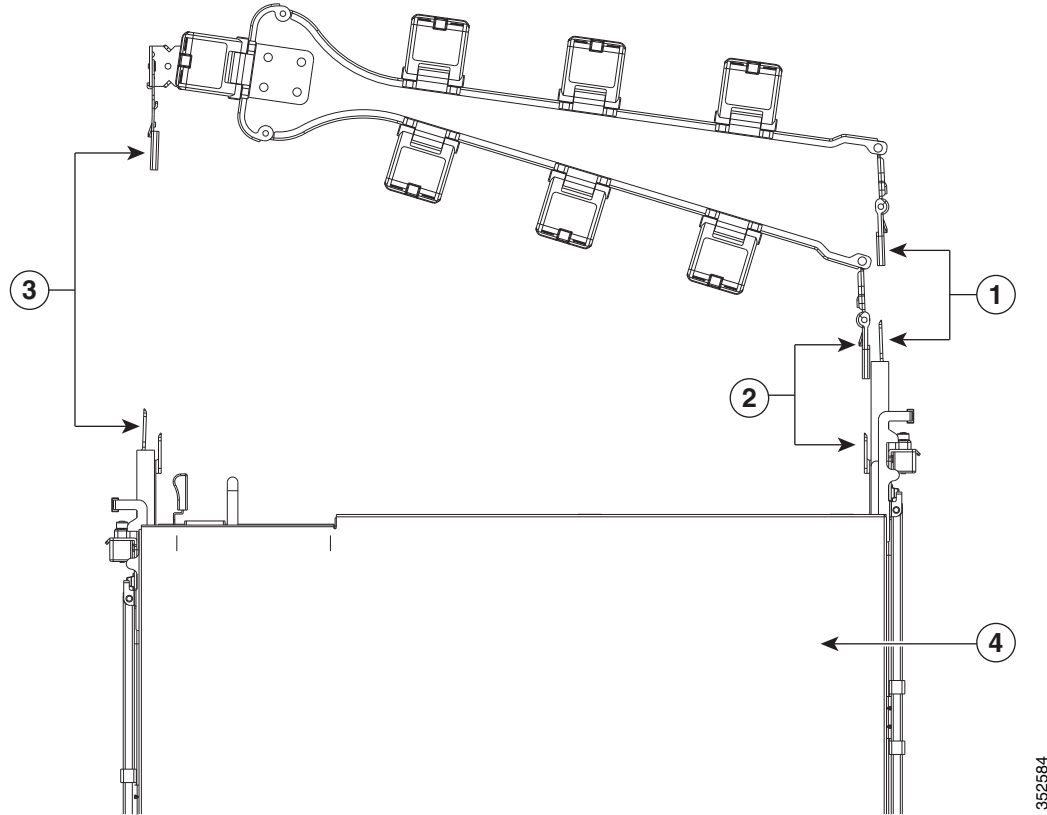
- e. Attach the second slide-rail assembly to the opposite side of the rack. Ensure that the two slide-rail assemblies are at the same height with each other and are level front-to-back.
- f. Pull the inner slide rails on each assembly out toward the rack front until they hit the internal stops and lock in place.

Installing the Cable Management Arm (Optional)

**Note**

The CMA is reversible left to right. To reverse the CMA, see [Reversing the Cable Management Arm \(Optional\)](#), page 2-8 before installation.

-
- Step 1** With the Cisco MSE 3365 pushed fully into the rack, slide the CMA tab of the CMA arm that is farthest from the MSE 3365 onto the end of the stationary slide rail that is attached to the rack post (see [Figure 2-3](#)). Slide the tab over the end of the rail until it clicks and locks.
 - Step 2** Slide the CMA tab that is closest to the Cisco MSE 3365 over the end of the inner rail that is attached to the Cisco MSE 3365 (see [Figure 2-3](#)). Slide the tab over the end of the rail until it clicks and locks.
 - Step 3** Pull out the width-adjustment slider that is at the opposite end of the CMA assembly until it matches the width of your rack (see [Figure 2-3](#)).
 - Step 4** Slide the CMA tab that is at the end of the width-adjustment slider onto the end of the stationary slide rail that is attached to the rack post (see [Figure 2-3](#)). Slide the tab over the end of the rail until it clicks and locks.
 - Step 5** Open the hinged flap at the top of each plastic cable guide and route your cables through the cable guides as desired.

Figure 2-3 *Attaching the Cable Management Arm to the Rear of the Slide Rails*

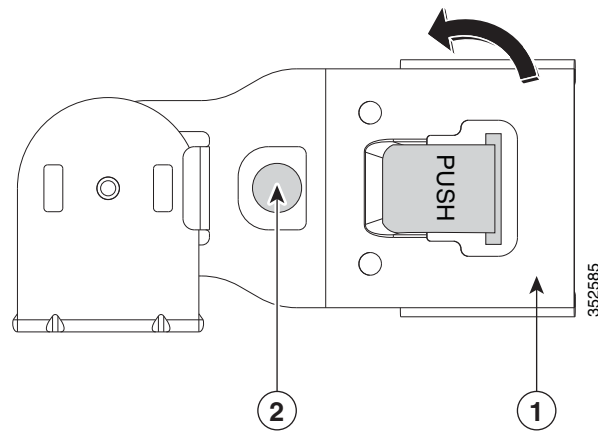
352584

1	CMA tab on arm farthest from the Cisco MSE 3365 and end of stationary outer slide rail	3	CMA tab on width-adjustment slider and end of stationary outer slide rail
2	CMA tab on arm closest to the Cisco MSE 3365 and end of inner slide rail attached to the Cisco MSE 3365	4	Rear of the Cisco MSE 3365

Reversing the Cable Management Arm (Optional)

- Step 1** Rotate the entire CMA assembly 180 degrees. The plastic cable guides must remain pointing upward.
- Step 2** Flip the tabs at the end of each CMA arm so that they point toward the rear of the Cisco MSE 3365.
- Step 3** Pivot the tab that is at the end of the width-adjustment slider. Depress and hold the metal button on the outside of the tab and pivot the tab 180 degrees so that it points toward the rear of the Cisco MSE 3365.

Figure 2-4 *Reversing the CMA*



1	CMA tab on end of width-adjustment slider	2	Metal button for rotating
---	---	---	---------------------------

Step 4 Insert the Cisco MSE 3365 into the slide rails.



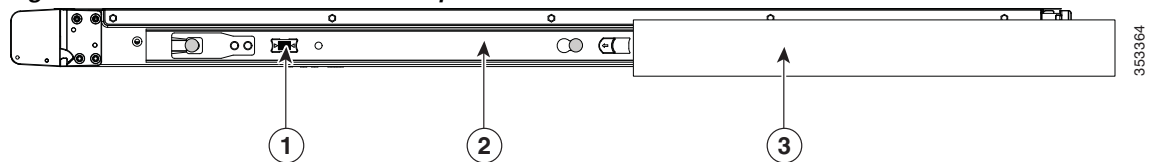
Caution

Cisco MSE 3365 weighs 38 lbs (17.20 kilograms). We recommend that you use a minimum of two people or a mechanical lift when lifting the Cisco MSE 3365. Attempting this procedure alone could result in personal injury or equipment damage.

- a. Align the rear of the inner rails that are attached to the Cisco MSE 3365 sides with the front ends of the empty slide rails on the rack.
- b. Push the inner rails into the slide rails on the rack until they stop at the internal stops.

Step 5 Slide the release clip toward the rear on both inner rails, and then continue pushing the Cisco MSE 3365 into the rack until its front slam latches engage with the rack posts.

Figure 2-5 Inner Rail Release Clip



1	Inner rail release clip	3	Outer rail attached to rack post
2	Inner rail attached to the Cisco MSE 3365 and inserted into outer rail		

Step 6 (Optional) Secure the Cisco MSE 3365 in the rack more permanently by using the two screws that are provided with the slide rails. Perform this step if you plan to move the rack with the Cisco MSE 3365 installed.

Step 7 With the Cisco MSE 3365 fully pushed into the slide rails, open the hinged slam latch lever on the front of the Cisco MSE 3365 and insert the screw through the hole that is under the lever. The screw threads into the static part of the rail on the rack post and prevents the Cisco MSE 3365 from being pulled out. Repeat for the opposite slam latch.

Initial Setup

Connecting and Powering On the Cisco MSE 3365 (Standalone Mode)

Cisco MSE 3365 can be setup using one of the following methods. You can use any procedure that meets your requirements. However, setting up the Cisco MSE 3365 for remote setup provides the most flexible option.

- Local setup—Use this procedure if you want to connect a keyboard and monitor the system for setup.
 - Use the KVM cable provided with the Cisco MSE 3365 or the ports on the rear of the Cisco MSE 3365. See [Local Connection Using KVM, page 2-11](#).
 - Use the local connection using Serial Console Interface. See [Local Connection using Serial Console, page 2-11](#).
- Remote setup—Use this procedure if you want to perform setup through your dedicated management LAN. See [Remote Connection Procedure, page 2-12](#).

Local Connection Using KVM

-
- | | |
|---------------|---|
| Step 1 | Attach a power cord to each power supply unit (PSU) in your Cisco MSE 3365, and then attach each power cord to a grounded AC power outlet. See Physical Specifications, page A-1 for power specifications.

Wait for approximately two minutes to let the server boot in standby power during the first bootup. You can verify system power status by looking at the system Power Status LED on the front panel (see External Features Overview, page 1-1). The system is in standby power mode when the LED is amber. |
| Step 2 | Connect a USB keyboard and VGA monitor to the Cisco MSE 3365 using one of the following methods: <ul style="list-style-type: none">• Connect a USB keyboard and VGA monitor to the corresponding connectors on the rear panel (see External Features Overview, page 1-1).• Connect the KVM cable to the KVM connector on the front panel (see External Features Overview, page 1-1 for the connector location). Connect your USB keyboard and VGA monitor to the corresponding ports on the KVM connector. |
| Step 3 | Power up the Cisco MSE 3365 and watch the on-screen prompts. The Cisco MSE progresses through the boot-up procedure and then finally prompts for user login. At this time, you can use the default credentials (root/password) to login and configure the Cisco MSE. Note that in this mode, you may not be able to see every output coming from the Cisco MSE because limited output is sent to the directly connected monitor. |
-

Local Connection using Serial Console

In this mode, all operations are performed through the serial console interface.

-
- | | |
|---------------|---|
| Step 1 | Connect a serial console cable (DB9 assembly) to the serial port on the KVM cable. The KVM cable is attached to the KVM connector on the front of the Cisco MSE 3365 (see Figure 1-1). |
|---------------|---|

- Step 2** Connect the other end of the serial console cable to a terminal emulator application. Set the terminal emulator to:
- 9600 baud
 - 8 data bits
 - no flow control
 - 1 stop bit
 - no parity
- Step 3** Power up the Cisco MSE 3365 and watch the output on the serial console. Finally, when prompted, login and proceed with Cisco MSE 3365 setup.

**Note**

You may also use the serial port on the rear of the unit for serial console access, instead of the port on the KVM cable. However, the serial port on the rear of the MSE 3365 is a RJ-45 connector and not a DB 9-connector (see [Figure 1-2](#)).

Remote Connection Procedure

In this setup, the Cisco Integrated Management Controller (CIMC) is used to access the Cisco MSE 3365. A dedicated IP address is assigned to the CIMC and the management port on the rear of the unit is used for CIMC access.

- Step 1** Attach a power cord to each power supply unit (PSU) in your Cisco MSE 3365, and then attach the other end of the power cord to a grounded AC power outlet. See [Physical Specifications, page A-1](#) for power specifications.

Wait for approximately two minutes to let the Cisco MSE 3365 boot in standby power during the first bootup.

You can verify system power status by looking at the system Power Status LED on the front panel (see [External Features Overview, page 1-1](#)). The system is in standby power mode when the LED is amber.

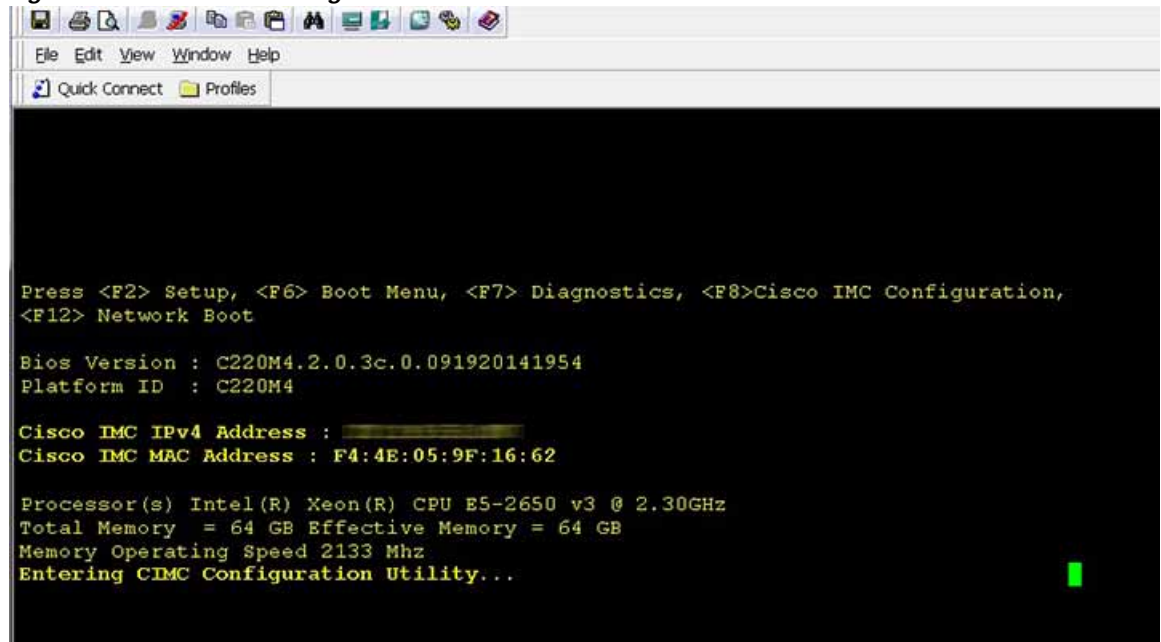
- Step 2** Plug your management Ethernet cable into the dedicated management port on the rear panel (see [External Features Overview, page 1-1](#)).

**Note**

The management port (and the management port IP address) should not be confused with the Cisco MSE 3365 IP address. The management port is strictly used for setup and monitoring of the Cisco 3365 and not for regular MSE traffic flow.

**Note**

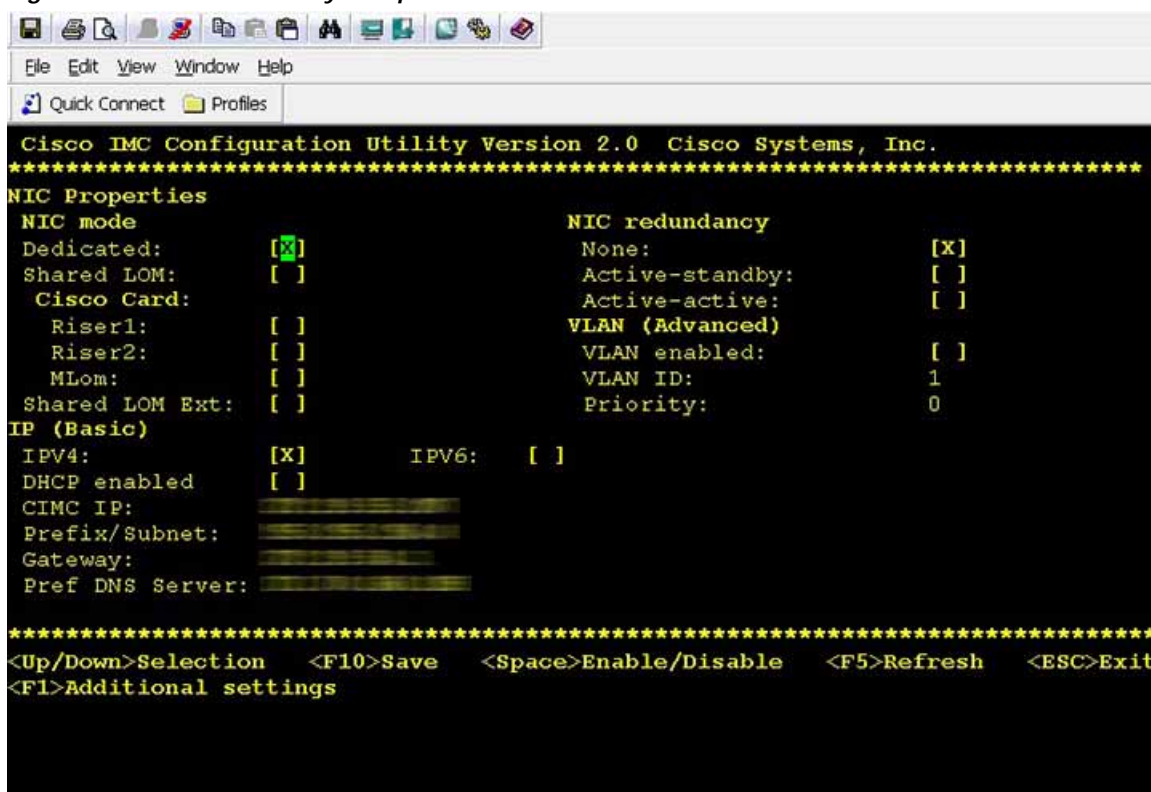
Just to perform the one-time CIMC setup, connect a keyboard and monitor (or use the serial console connection) and then power up the Cisco MSE 3365. As the Cisco MSE 3365 boots up, press F8 and enter the CIMC configuration mode (see [Figure 2-6](#)).

Figure 2-6 CIMC Configuration Mode

CIMC Configuration Utility Setup

- Step 1** Once you are in the Cisco Integrated Management Controller (CIMC) configuration screen, you need to assign an IP address for the CIMC management port and configure the attributes (see [Figure 2-7](#)).

Figure 2-7 CIMC Utility Setup



Cisco MSE 3365 ships with NIC mode as Dedicated, meaning that only the management port is used for CIMC communication.

For quick and simple access to CIMC, just configure the IP address, gateway, and subnet mask. No other configuration is required.

The static IPv4 and IPv6 settings include the following:

- The Cisco Integrated Management Controller (CIMC) IP address.
- The prefix/subnet.

For IPv6, valid values are 1–127.

- The gateway.

For IPv6, if you do not know the gateway, you can set it as none by entering :: (two colons).

- The preferred DNS server address.

For IPv6, you can set this as none by entering :: (two colons).

Step 2 (Optional) Use this utility to make VLAN settings.

Step 3 Press **F1** to go to the second settings window, then continue with the next step.

From the second window, you can press **F2** to switch back to the first window.

Step 4 (Optional) Set a hostname for the server.

Step 5 (Optional) Enable dynamic DNS and set a dynamic DNS (DDNS) domain.

Step 6 (Optional) If you check the Factory Default check box, the server reverts to the factory defaults.

Step 7 (Optional) Set a default user password.

Step 8 (Optional) Enable auto-negotiation of port settings or set the port speed and duplex mode manually.



Note Auto-negotiation is applicable only when you use the Dedicated NIC mode. Auto-negotiation sets the port speed and duplex mode automatically based on the switch port to which the server is connected. If you disable auto-negotiation, you must set the port speed and duplex mode manually.

Step 9 (Optional) Reset port profiles and the port name.

Step 10 Press **F5** to refresh the settings that you made. You might have to wait about 45 seconds until the new settings appear and the message, “Network settings configured” is displayed before you reboot the server in the next step.

Step 11 Press **F10** to save your settings and reboot the server.



Note If you chose to enable DHCP, the dynamically assigned IP and MAC addresses are displayed on the console screen during bootup.

Cisco Integrated Management Controller

Use a browser and the IP address of the Cisco Integrated Management Controller (CIMC) to connect to the Cisco Integrated Management Controller (CIMC) interface. The IP address is based upon the settings that you made (either a static address or the address assigned by your DHCP server).



Note The default username for the server is *admin*. The default password is *password*.

Once the CIMC dedicated IP address is configured and the changes are saved, you can access the CIMC interface using a web browser. You must connect to <https://CIMC-IP/> and login with the default credentials (admin/password).

From the CIMC web interface, you can launch the KVM console and gain access to the serial console and interact with the MSE 3365.

Accessing the CIMC Interface over SSH

You can also use an ssh session to access the Cisco Integrated Management Controller (CIMC) serial console. This is called Serial-Over-LAN (SOL).

Follow these steps to enable SOL:

Step 1 SSH ip-address-of-cimc-l admin

Step 2 Login using the credentials of CIMC

Step 3 Once you are connected to CIMC through ssh, enter the following commands:

- `# scope sol`
- `Server /sol #set enabled yes`

- Server /sol *# **set baud-rate 115200**
- Server /sol *# **commit**
- Server /sol # **show**
Enabled Baud Rate(bps)

yes 115200

Now you should be able to connect to SOL. You must perform the above steps only once.

Step 4 To connect to the serial console, enter the following command:

```
Server# connect host
```

Now you are on the serial console of the Cisco MSE 3365.

NIC Modes

The Cisco MSE 3365 has the following NIC mode setting:

- **Dedicated**—The dedicated management port is used to access Cisco Integrated Management Controller (CIMC). This is the default mode the Cisco MSE 3365 is shipped with. You must configure the IP address for CIMC access.

Configuring the Mobility Services Engine

Minimal configuration is done for the mobility services engine as part of installation using the console. All configuration beyond the initial setup using the automatic installation is done with Cisco Prime Infrastructure.



Note

You must change the default root password during initial configuration of the mobility services engine to ensure optimum network security.

- You are prompted to change the password during the automatic setup script.
- You can also change the password using the Linux command, **passwd**.

- Step 5** The first time you power up the Cisco MSE 3365, you will be prompted to run the setup script and configure the Cisco MSE

```
-----
Cisco Mobility Services Engine
```

```
mse login: root
password: password
Last login: Mon Mar 9 04:11:50 on tty1
```

[Configuration starts as soon as you log in]

```
Would you like to setup initial parameters using menu options (yes/no) [yes]:
```

[Press Enter to use the default values (yes) to use the Menu options]

```
Please select a configuration option below and enter the
requested information. You may exit setup at any time by
typing <Ctrl+C>.
```

```
You will be prompted to choose whether you wish to configure a
parameter, skip it, or reset it to its initial default value.
Skipping a parameter will leave it unchanged from its current
value.
```

```
Please note that the following parameters are mandatory and must be configured at least
once.
```

```
-> Hostname
-> Network interface eth0
-> Timezone settings
-> Root password
-> NTP settings
```

-> Prime Infrastructure password

You must select option 24 to verify and apply any changes made during this session.

PRESS <ENTER> TO CONTINUE:

Configure MSE:

- | | |
|---------------------------------------|--------------------------------------|
| 1) Hostname * | 13) Remote syslog setting |
| 2) Network Interface eth0 settings * | 14) Host access control settings |
| 3) Timezone settings * | 15) Audit rules |
| 4) Root password * | 16) Login banner |
| 5) NTP settings * | 17) System console restrictions |
| 6) Prime Infrastructure configuration | 18) SSH root access |
| 7) Display current configuration | 19) Single user password check |
| 8) Domain | 20) Login and password settings |
| 9) High availability role | 21) GRUB password |
| 10) Network interface eth1 settings | 22) Root access control |
| 11) DNS settings | 23) Auto start MSE on system boot up |
| 12) Future restart time | 24) ## Verify and apply changes ## |



Note

It is highly recommended that all relevant items be configured during initial setup to ensure optimum operation of the mobility services engine in your network. The hostname and either the Ethernet-0 (eth0) or the Ethernet-1 (eth1) port must always be configured during the automatic installation.

You can rerun the automatic installation script at any time to add or change parameters using this command:

```
[root@mse]# /opt/mse/setup/setup.sh.
```

There is no need to re-enter values that you do not want to change during one of these updates.



Note

If you do not want to configure an item, enter **skip** and you are prompted for the next configuration step. Any setting skipped is retained and not modified.



Note

Minimal configuration is done for the mobility services engine as part of installation using the console. All configurations beyond the initial setup using the automatic installation is done with the Cisco Prime Infrastructure.

Step 6 Configure the hostname

Please enter your choice [1 - 24]: **1**

Current Hostname=[mse]

Configure Hostname? (Y)es/(S)kip/(U)se default [Skip]: **y**

The host name should be a unique name that can identify the device on the network. The hostname should start with a letter, end with a letter or number, and contain only letters, numbers, and dashes.

Enter a Host name [mse]:

Step 7 Configure eth0 network settings

```

Please enter your choice [1 - 24]: 2

Current eth0 interface IP address=[10.0.0.1]
Current eth0 interface netmask=[255.0.0.0]
Current IPv4 gateway address=[172.20.104.123]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:y

Enter an IP address for first ethernet interface of this machine.

Enter eth0 IP address [10.0.0.2]:

Enter the network mask for IP address 172.21.105.126

Enter network mask [255.255.255.224]:

Enter the default gateway address for this machine.

Note that the default gateway must be reachable from
the first ethernet interface.

Enter default gateway address [172.20.104.123]:

```

Step 8 Configure the DNS Settings:

```

Please enter your choice [1 - 24]: 11

Domain Name Service (DNS) Setup

Enable DNS (yes/no) [no]: y
Default DNS server 1=[8.8.8.8]
Enter primary DNS server IP address:
DNS server address must be in the form #.#.#.#, where # is 0 to 255 or hexadecimal :
separated v6 address

Enter primary DNS server IP address [8.8.8.8]:
Enter backup DNS server IP address (or none) [none]:

```

Step 9 Configure the Timezone settings:**Note**

UTC must be used when you are configuring for wIPS. For other services, you must use the same time zone as the controllers.

```

Please enter your choice [1 - 24]: 3

Current Timezone=[America/New_York]
Configure Timezone? (Y)es/(S)kip/(U)se default [Skip]: y

Enter the current date and time.

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
11) UTC - I want to use Coordinated Universal Time.

```

#? 2

Please select a country.

- | | |
|------------------------|-----------------------------|
| 1) Anguilla | 27) Honduras |
| 2) Antigua & Barbuda | 28) Jamaica |
| 3) Argentina | 29) Martinique |
| 4) Aruba | 30) Mexico |
| 5) Bahamas | 31) Montserrat |
| 6) Barbados | 32) Netherlands Antilles |
| 7) Belize | 33) Nicaragua |
| 8) Bolivia | 34) Panama |
| 9) Brazil | 35) Paraguay |
| 10) Canada | 36) Peru |
| 11) Cayman Islands | 37) Puerto Rico |
| 12) Chile | 38) St Barthelemy |
| 13) Colombia | 39) St Kitts & Nevis |
| 14) Costa Rica | 40) St Lucia |
| 15) Cuba | 41) St Martin (French part) |
| 16) Dominica | 42) St Pierre & Miquelon |
| 17) Dominican Republic | 43) St Vincent |
| 18) Ecuador | 44) Suriname |
| 19) El Salvador | 45) Trinidad & Tobago |
| 20) French Guiana | 46) Turks & Caicos Is |
| 21) Greenland | 47) United States |
| 22) Grenada | 48) Uruguay |
| 23) Guadeloupe | 49) Venezuela |
| 24) Guatemala | 50) Virgin Islands (UK) |
| 25) Guyana | 51) Virgin Islands (US) |
| 26) Haiti | |

#? 47

Please select one of the following time zone regions.

- 1) Eastern Time
- 2) Eastern Time - Michigan - most locations
- 3) Eastern Time - Kentucky - Louisville area
- 4) Eastern Time - Kentucky - Wayne County
- 5) Eastern Time - Indiana - most locations
- 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
- 7) Eastern Time - Indiana - Pulaski County
- 8) Eastern Time - Indiana - Crawford County
- 9) Eastern Time - Indiana - Pike County
- 10) Eastern Time - Indiana - Switzerland County
- 11) Central Time
- 12) Central Time - Indiana - Perry County
- 13) Central Time - Indiana - Starke County
- 14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
- 15) Central Time - North Dakota - Oliver County
- 16) Central Time - North Dakota - Morton County (except Mandan area)
- 17) Mountain Time
- 18) Mountain Time - south Idaho & east Oregon
- 19) Mountain Time - Navajo
- 20) Mountain Standard Time - Arizona
- 21) Pacific Time
- 22) Alaska Time
- 23) Alaska Time - Alaska panhandle
- 24) Alaska Time - Alaska panhandle neck
- 25) Alaska Time - west Alaska
- 26) Aleutian Islands
- 27) Hawaii

#? 21

The following information has been given:

United States
Pacific Time

```
Therefore TZ='America/Los_Angeles' will be used.
Local time is now:      Sun Apr  6 18:45:27 PDT 2014.
Universal Time is now:  Mon Apr  7 01:45:27 UTC 2014.
Is the above information OK?
1) Yes
2) No
#? 1
```

Step 10 Configure the Root password:

Note If you do not set the root password, a warning message is displayed when you apply the settings.

```
Please enter your choice [1 - 24]: 4
```

```
Root password has not been configured
Configure root password? (Y)es/(S)kip/(U)se default [Skip]:
Changing password for user root.
```

```
You can now choose the new password.
```

A valid password should be a mix of upper and lower case letters, digits, and other characters. You can use an 8 character long password with characters from all of these classes. An upper case letter that begins the password and a digit that ends it do not count towards the number of character classes used.

```
Enter new password:
```

Step 11 Configure the NTP Setup

```
Please enter your choice [1 - 24]: 5
```

```
Network Time Protocol (NTP) Setup.
```

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

```
NTP is currently disabled.
```

```
Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: y
```

```
Enter whether or not you would like to set up the
Network Time Protocol (NTP) for this machine.
```

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

```
Enable NTP (yes/no) [no]: y
```

```
Default NTP server 1=[time.nist.gov]
```

```
Enter NTP server name or address:
```

```
NTP server address must be in the form #.#.#.3, where # is 0 to 255 hexadecimal :
separated v6 address.
```

```
Enter NTP server name or [time.nist.gov]:
```

```
Enter another NTP server IP address (or none) [none]:
```

```
Configure NTP Authentication ? (Y)es/(S)kip/(U)se default [Skip]: y
```

```
Enter NTP Auth key Number [1]:
```

```
Enter NTP Auth key Value (String) [Secret]:
```

```
Do you want to continue (yes/no) [no]: y
```

Step 12 Configure the Prime Infrastructure password:



Note If you do not set the password, a warning message appears when you apply the settings. The default PI communication password is *admin*.

Please enter your choice [1 - 24]: **6**

Cisco Prime Infrastructure communication password has not been configured.
Configure Prime Infrastructure password? (Y)es/(S)kip/(U)se default [Yes]:

Enter a password for the admin user.

The admin user is used by the Prime Infrastructure and other northbound systems to authenticate their SOAP/XML session with the server. Once this password is updated, it must correspondingly be updated on the NCS page for MSE General Parameters so that the Prime Infrastructure can communicate with the MSE.

Enter Prime Infrastructure password:

Step 13 Verify the setup information and apply the changes:

Please enter your choice [1 - 24]: **24**

Please verify the following setup information.

-----BEGIN-----

```

Hostname=mse8-0
Eth0 IP address= , Eth0 network mask=255.255.254.0
Time zone=America/Los_Angeles
Enable DNS=yes, DNS servers=8.8.8.8
Enable NTP=yes, NTP servers=time.nist.gov
Time zone=America/Los_Angeles
Root password is changed.
Cisco Prime Infrastructure password is changed.

```

-----END-----

You may enter "yes" to proceed with configuration, "no" to make more changes.

Configuration Changed

Is the above information correct (yes or no): **yes**

Checking mandatory configuration information...

Setup will now attempt to apply the configuration.

Restarting network services with new settings.
Shutting down interface eth0:

The system is minimally configured right now. It is strongly recommended that you run the setup script under /opt/mse/setup/setup.sh command to configure all appliance related parameters immediately after installation is complete.

PRESS <ENTER> TO EXIT THE INSTALLER:

[root@mse8-0 installers]# reboot

Stopping MSE Platform

Flushing firewall rules: [OK]

Setting chains to policy ACCEPT: nat filter [OK]

```

Unloading iptables modules:                                [ok]

Broadcast message from root (pts/0) (Tue Apr29 14:15:27:2014):

The system is going down for reboot NOW:

```

**Note**

The next time you log in using root, only the Linux shell prompt appears and not the setup script. You can rerun the setup script at any time to change settings by logging in as *root* and running **/opt/mse/setup/setup.sh**.

- Step 14** Log in and configure the MSE to automatically launch after boot up.

```

Cisco Mobility Service Engine
mse8-0 login:
Password:

```

- Step 15** To configure the MSE to automatically launch after boot up, enter the following command:

```
[root@mse8-0]# chkconfig msed on
```

**Note**

You can also enable the Cisco MSE to start automatically after boot up using Option 23 in the setup script wizard.

- Step 16** To verify the status of MSE software, enter the following command:

```
[root@mse8-0] # service msed status
```

- Step 17** Reboot using the following command:

```
[root@mse8-0]# reboot
```

- Step 18** To start the MSE service manually, enter the following command:

```
[root@mse8-0]# service msed start
```

The setup script generates a log file that can be found at **/opt/mse/setup/setup.log**.

Manually Stopping Mobility Services Engine Software

The mobility services engine software automatically runs after initial configuration and after each reboot.

Follow these steps to manually stop and restart the software:

- Step 1** To stop the software, enter **/etc/init.d/msed stop** or use the **service msed stop** command.
- Step 2** To check status, enter **/etc/init.d/msed status** or use the **service msed status** command.
- Step 3** To start the software, enter **/etc/init.d/msed start** or use the **service msed start** command.

Manually Restarting a Running Mobility Services Engine

To restart a running mobility services engine, enter `/etc/init.d/msed restart`.

Updating Mobility Services Engine Software

You can update the mobility services engine using the Cisco Prime Infrastructure by manually downloading the software using a console port connected to the mobility services engine.

**Note**

If MSE is unreachable on Cisco Prime Infrastructure soon after an upgrade, you must reboot the MSE using this command as root user on the MSE: `reboot`

**Note**

For the latest Cisco Prime Infrastructure and Cisco Mobility Services Engine compatibility and installation notes for a given release, refer to the appropriate release note at the following link: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

Before downloading and updating software on the mobility services engine, note the following:

- The mobility services engine (server) image is compressed. The software image automatically decompresses during its download from Cisco Prime Infrastructure.
- Approximately 5 minutes is required for the newly loaded mobility services engine software version to appear on the Cisco Prime Infrastructure. Choose **Services > Mobility Services** from the Cisco Prime Infrastructure user interface.

Downloading Software Using the Cisco Prime Infrastructure

To download software to a mobility services engine, follow these steps:

- Step 1** Verify that you can ping the mobility services engine from the Prime Infrastructure server or an external FTP server, whichever you are going to use for the application code download
- Step 2** Choose **Services > Mobility Services Engine**.
- Step 3** Click the name of the MSE to which you want to download software.
- Step 4** Choose **System > Maintenance > Download Software** from the left sidebar menu.
- Step 5** To download software, do one of the following:
- Step 6** To download software listed in the Prime Infrastructure directory, select the **Select from uploaded images to transfer into the Server** radio button. Choose a binary image from the drop-down list.
- Step 7** Prime Infrastructure downloads the binary image to the FTP server directory you specified during the Prime Infrastructure installation.
- Step 8** To use downloaded software available locally or over the network, select the **Browse a new software image to transfer into the Server** radio button, and click **Choose File**. Locate the file, and click **Open**.
- Step 9** Click **Download** to send the software to the `/opt/installers` directory on the MSE.
- Step 10** After the image is transferred to the MSE, log in to the MSE command-line interface.

Step 11 Run the installer image from the `/opt/installers` directory by entering the following command:
`/opt/installers/CISCO-MSE-L-K9-x-x-x-x-64bit.bin`

where, `x-x-x-x` is the version of the image you downloaded (for example, `CISCO-MSE-L-K9-8-0-110-10-64bit.bin`)

Step 12 To run the software, enter the **`/etc/init.d/msed start`** command.



Note

To stop the software, enter the **`/etc/init.d/msed stop`** command, and to check status, enter the **`/etc/init.d/msed status`** command.

Manually Downloading Software

If you do not want to automatically update the mobility services engine software using Cisco Prime Infrastructure, follow these steps to upgrade the software manually using a local (console) or remote (SSH) connection.

Step 1 Transfer the new mobility services engine image onto the hard drive.

- a. Log in as root and use the binary setting to send the software image from an external FTP server root directory.

The image format is similar to the following and changes with each release:

`CISCO-MSE-L-K9-x-x-x-x-64bit.bin.tar.gz`



Note

The mobility services engine image is compressed at this point.



Note

If you are using Cisco Prime Infrastructure as the ftp server, the default login name for stp server is `stp-user`.

Your entries should look like this example:

```
# cd /opt/installers
# ftp <FTP Server IP address>
Name: <login>
Password: <password>
binary
get CISCO-MSE-L-K9-x-x-x-x-64bit.bin.tar.gz
<CTRL-Z>
#
```

- b. Verify that the image (`CISCO-MSE-L-K9-x-x-x-x-64bit.bin.tar.gz`) is in the `MSE/opt/installers` directory.
- c. To decompress (unzip) the image file, enter the following command:

```
tar zxvf CISCO-MSE-L-K9-x-x-x-x-64bit.bin.tar.gz
```

The decompression yields 3 files:

`CISCO-MSE-L-K9-x-x-x-x-64bit.bin`

```
MSE_PUB.pem
```

```
signhash.bin
```

- d. Make sure that the CISCO-MSE-L-K9-x-x-x-x.bin.tar.gz file has execute permissions for the root user. If not, enter the following command:

```
chmod 755 CISCO-MSE-L-K9-x-x-x-x.bin
```

Step 2 Manually stop the MSE.

Step 3 Log in as root and enter the following command to start the installation procedure. Pay attention to the messages and answer prompts appropriately.

```
/opt/installers/CISCO-MSE-L-K9-x-x-x-x.bin
```

Step 4 Once the installation is complete, reboot the Cisco MSE:

```
# reboot
```

Recovering a Lost Root Password

To recover a lost or forgotten root password for a mobility services engine, follow these steps.



Note

You must be connected to the Cisco MSE 3365 through Serial Console connection (either direct Serial console or Serial Console over LAN). The procedure will not work if you are using the KVM console launched from the Cisco Integrated Management Controller (CIMC).

Step 1 When the GRUB screen comes up, press **Esc** to enter the boot menu.



Caution

If you forget the GRUB password, you cannot login and you will need to contact TAC to arrange for an RMA.

The following screen is displayed. See [\(Figure 2-8\)](#).

Figure 2-8 **Screen 1**

```

GNU GRUB  version 0.97  (620K lower / 1820600K upper memory)

-----
root (hd0,0)
kernel /vmlinuz-2.6.32-504.el6.x86_64 ro root=UUID=1f6be69b-3c7a-4328>
initrd /initramfs-2.6.32-504.el6.x86_64.img
-----

Use the ^ and v keys to select which entry is highlighted.
Press 'b' to boot, 'e' to edit the selected command in the
boot sequence, 'c' for a command-line, 'o' to open a new line
after ('O' for before) the selected line, 'd' to remove the
selected line, or escape to go back to the main menu.

```

- Step 2** Press **e** to edit.
- Step 3** Navigate to the line beginning with “kernel,” and press **e**.
- Step 4** At the end of the line, type a space followed by `single console =ttyS0`. See (Figure 2-9).

Figure 2-9 **Screen 2**

```

[ Minimal BASH-like line editing is supported.  For the first word, TAB
  lists possible command completions.  Anywhere else TAB lists the possible
  completions of a device/filename.  ESC at any time cancels.  ENTER
  at any time accepts your changes.]

<9b-3c7a-4328-94cb-58f3ec9ec5f1 single console=ttyS0

```

- Step 5** Press **Enter** to save this change.
- Step 6** Press **b** to begin boot sequence.
- Step 7** At the end of the boot sequence, a shell prompt appears.



Note The shell prompt does not appear if you set up a single-user mode password.

- Step 8** Enter the **passwd** command to change the root password.
- Step 9** Enter and confirm the new password.

Step 10 Restart the machine.



Note

Ensure that you remember the root password and only change the password if it is absolutely necessary.
