



Installation and Initial Configuration

This chapter describes how to initially install and configure your Cisco 3350 Mobility Services Engine.

This chapter contains these sections:

- [Required Tools and Information, page 2-1](#)
- [Choosing a Physical Location for the Cisco 3350, page 2-3](#)
- [Unpacking the Mobility Services Engine, page 2-6](#)
- [Mounting the Cisco 3350 in a Rack, page 2-6](#)
- [Front and Rear Panel, page 2-9](#)
- [Connecting and Using the CLI Console, page 2-16](#)
- [Powering On the Mobility Services Engine, page 2-16](#)
- [Configuring the Mobility Services Engine, page 2-16](#)
- [Configuring an NTP Server, page 2-24](#)
- [Launching the Mobility Services Engine, page 2-25](#)
- [Verifying the Mobility Services Engine Software State, page 2-25](#)
- [Manually Stopping Mobility Services Engine Software, page 2-26](#)
- [Updating Mobility Services Engine Software, page 2-26](#)
- [Recovering a Lost Root Password, page 2-29](#)



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

Required Tools and Information

This section lists the required hardware, software and other information that you need to install and setup the mobility services engine.

Required Hardware

You need this equipment to install a mobility services engine in an EIA rack:

- A mobility services engine
- Network cables
- One rack unit (RU) in an EIA-standard rack
- Rack mounting kit (included in shipment)



Note If you are installing this unit in a threaded-hole rack, you must supply screws that fit the threaded-hole rack and the appropriate screwdriver or Torx driver for those screws.

CLI Console Requirements

You need this equipment to connect to the mobility services engine console:

- VT-100 terminal emulator on CLI console laptop, desktop, or palmtop



Note A null modem serial cable that provides a connection to the laptop, desktop, or palmtop is shipped with the mobility services engine.



Note

Please refer to the latest *Release Notes for Cisco 3300 Series Mobility Services Engine* for compatibility by release between the mobility services engine and Cisco WCS and controller releases at: http://www.cisco.com/en/US/products/ps9742/prod_release_notes_list.html

System Configuration Parameters

Obtain these parameters from your network administrator:

- A host name for the mobility services engine
- An IP address for the Ethernet-0 (eth0) port (mobility services engine back panel)
- A net mask for the eth0 IP address
- An IP address for the eth0 default gateway
- An IP address for the Ethernet-1 (eth1) port (mobility services engine back panel) (installation optional)
- A net mask for the eth1 IP address (only required if eth1 is installed)
- An IP address for the eth1 default gateway (only required if eth1 is installed)



Note

Either the Ethernet-0 or Ethernet-1 port can be used to transmit location updates to Cisco WCS. However, the Ethernet-0 port is generally configured to communicate with Cisco WCS and the Ethernet-1 port is generally used for out-of-band management. Both ports are configured as part of the installation script described in the “[Configuring the Mobility Services Engine](#)” section on page 2-16.

Choosing a Physical Location for the Cisco 3350

For maximum safety and reliability, mount the mobility services engine using the following guidelines.

General Precautions

To reduce the risk of personal injury or damage to the mobility services engine:

- Place the product away from radiators, heat registers, stoves, amplifiers, or other products that produce heat.
- Never use the product in a wet location.
- Avoid inserting foreign objects through openings in the product.
- To reduce risk of injury from electric shock hazards, do not open the product enclosure.

Laser Devices

Laser devices are used within the DVD of the mobility services engine. The DVD has no defined use on the customer site.

To reduce the risk of exposure to hazardous radiation:

- Do not try to open the laser device enclosure. There are no user-serviceable components inside.
- Do not operate controls, make adjustments, or perform procedures to the laser device other than those specified herein.
- Allow only Cisco authorized service technicians to repair the laser device.

Space and Airflow Requirements

Install the mobility services engine in a EIA-standard rack. One rack unit is required for each mobility services engine.

Ensure that you can reach the mobility services engine and all cables.

- Ensure that the mobility services engine is within 328 ft (100 m) equivalent distance to any equipment connected to the 10/100/1000BASE-T ports.
- Ensure that the power cord can reach a 110 or 220 VAC grounded electrical outlet.

Ensure that there is sufficient room at the back of the mobility services engine for all cables and connectors.

- Leave a minimum clearance of 63.5 cm (25 in.) in front of the rack.
- Leave a minimum clearance of 76.2 cm (30 in.) behind the rack.
- Leave a minimum clearance of 121.9 cm (48 in.) from the back of the rack to the back of another rack or row of racks



Caution

To prevent improper cooling and damage to the equipment, do not block the ventilation openings.

**Caution**

Always use blanking panels to fill empty vertical spaces in the rack. This arrangement ensures proper airflow. Using a rack without blanking panels results in improper cooling that can lead to thermal damage.

**Caution**

When selecting a rack to use, observe the following additional requirements to ensure adequate airflow and to prevent damage to the equipment: (1) Front and rear doors—If the 42U rack includes closing front and rear doors, you must allow 5,350 sq. cm (830 sq. in.) of holes evenly distributed from top to bottom to permit adequate airflow (equivalent to the required 64 percent open area for ventilation). (2) Side—The clearance between the installed rack component and the side panels of the rack must be a minimum of 7 cm (2.75 in.in.).

Temperature Requirements

To ensure continued safe and reliable equipment operation, install or position the system in a well ventilated, climate-controlled environment.

Ensure that the ambient operating temperature remains between 0 and 40° C (32 and 104° F), taking into account the elevated temperatures that occur when equipment is installed in a rack.

**Caution**

To reduce the risk of damage to the equipment when installing third-party options: (1) Do not permit optional equipment to impede airflow around the mobility services engine or to increase the internal rack temperature beyond the maximum allowable limits. (2) Do not exceed the manufacturer's TMRA.

Power Requirements

Installation of this equipment must comply with local and regional electrical regulations governing the installation of information technology equipment by licensed electricians. This equipment is designed to operate in installations covered by NFPA 70, 1999 Edition (National Electric Code) and NFPA-75, 1992 (code for Protection of Electronic Computer/Data Processing Equipment). For electrical power ratings on options, refer to the product rating label or the user documentation supplied with that option.

**Caution**

Protect the mobility services engine from power fluctuations and temporary interruptions with a regulating uninterruptible power supply (UPS). This device protects the hardware from damage caused by power surges and voltage spikes and keeps the system in operation during a power failure.

When installing more than one mobility services engine, you may need to use additional power distribution devices (PDUs) to safely provide power to all devices. Observe the following guidelines:

- Balance the mobility services engine power load between available AC supply branch circuits.
- Do not allow the overall system AC current load to exceed 80 percent of the branch circuit AC current rating.
- Do not use common power outlet strips for this equipment.
- Provide a separate electrical circuit for the mobility services engine.

Power Supplies on the Mobility Services Engine

The mobility services engine has two power supplies.



This unit might have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028



Verify that the external power source connected to the mobility services engine matches the type of power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your Cisco authorized reseller or local power company.

Batteries

The mobility services engine might include a real-time clock battery or coin cell battery that might contain perchlorate and might require special handling when recycled or disposed of in California.

Refer to the following link for disposal information.

<http://www.dtsc.ca.gov/hazardouswaste/perchlorate>



Do not dispose of batteries with the general household waste. Recycle them using the public collection system.

Electrical Grounding Requirements

The mobility services engine must be grounded properly for proper operation and safety. In the United States, you must install the equipment in accordance with NFPA 70, 1999 Edition (National Electric Code), Article 250, as well as any local and regional building codes. In Canada, you must install the equipment in accordance with Canadian Standards Association, CSA C22.1, Canadian Electrical Code. In all other countries, you must install the equipment in accordance with any regional or national electrical wiring codes, such as the International Electrotechnical Commission (IEC) Code 364, parts 1 through 7.

Furthermore, you must verify that all power distribution devices used in the installation, such as branch wiring and receptacles, are listed or certified grounding-type devices. Because of the high ground-leakage currents associated with multiple systems connected to the same power source, Cisco recommends the use of a PDU that is either permanently wired to the building's branch circuit or includes a nondetachable cord that is wired to an industrial-style plug, NEMA locking-style plugs or those complying with IEC 60309 are considered suitable for this purpose. Using common power outlet strips for the mobility services engine is not recommended.

Rack Warnings



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 the Mobility Services Engine

Follow these steps to unpack the mobility services engine.

-
- Step 1** Open the shipping container and carefully remove the contents.
 - Step 2** Return all packing materials to the shipping container and save it.
 - Step 3** Ensure that all items listed in the “**Package Contents**” section are included in the shipment.
 - Step 4** Check each item for damage. If any item is damaged or missing, notify your authorized Cisco sales representative.
-

Package Contents

Each mobility services engine package contains the following items:

- One Cisco 3350 Mobility Services Engine
- One rack mount kit
- Power cords
- DB9-RJ45 cable for console connection
- RJ45-DB9 adapter
- This guide, the *Cisco 3350 Mobility Services Engine Getting Started Guide*

Mounting the Cisco 3350 in a Rack

**Warning**

Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030

**Caution**

This mobility services engine is very heavy (37 lbs, 17 kgs).

To reduce the risk of personal injury or damage to the equipment:

- Observe local occupational health and safety requirements and guidelines for manual material handling.
- Get help to lift and stabilize the mobility services engine during installation or removal is recommended, especially when the system is not fastened to the rails.
- Use caution when installing the mobility services engine in or removing it from the rack; it is unstable when not fastened to the rails.
- Always plan the rack installation so that the heaviest item is on the bottom of the rack. Install the heaviest item first, and continue to populate the rack from the bottom to the top.



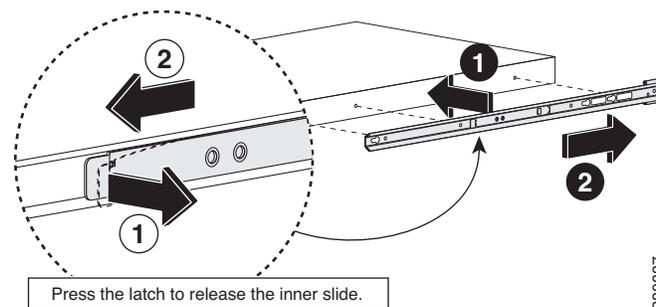
Note

- The mobility services engine comes with a rack mount rail kit that can be installed in a square-hole rack, round-hole rack, or a threaded-hole rack.
- You must provide the threaded-hole screws to secure the mounting rails to the rack. Threaded-hole screws are not shipped with the system.

Installing the Rail Kit Into a Threaded-Hole, Square-Hole or Round-Hole Rack

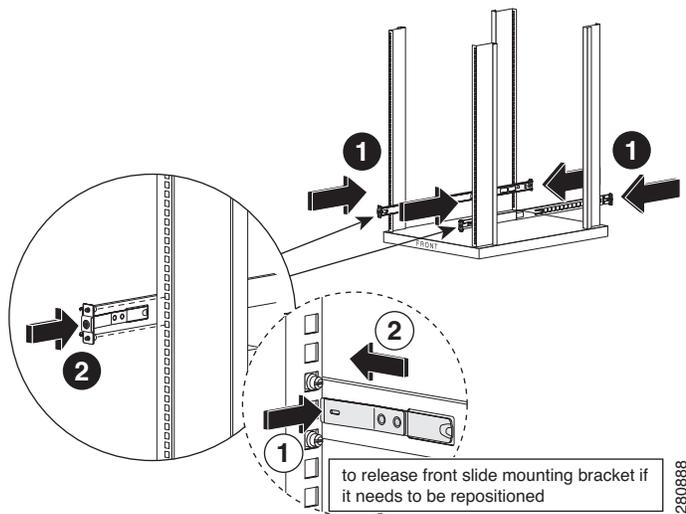
- Step 1** Release the inner slide of the mounting rail and attach it to the side of the mobility services engine (Figure 2-1). The numbers within the illustrations indicate the order of the action.

Figure 2-1 Attach Inner Sliding Rail to Mobility Services Engine



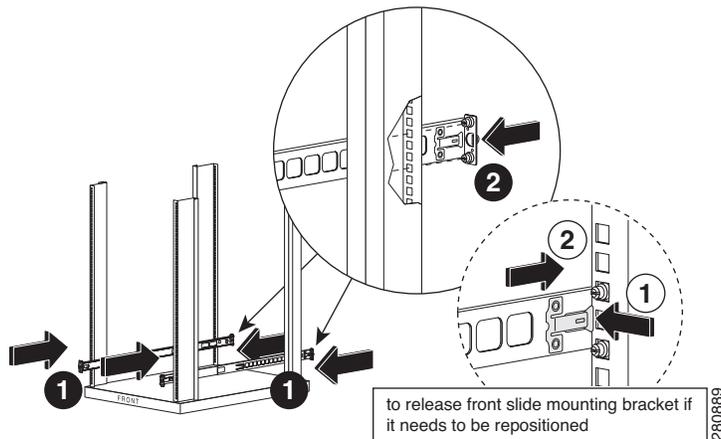
- Step 2** Attach the outside rail to the front of the rack structure where the mobility services engine is going to be installed (Figure 2-2). The numbers within the illustrations indicate the order of the action.

Figure 2-2 Attach Outer Rail to Front of Rack



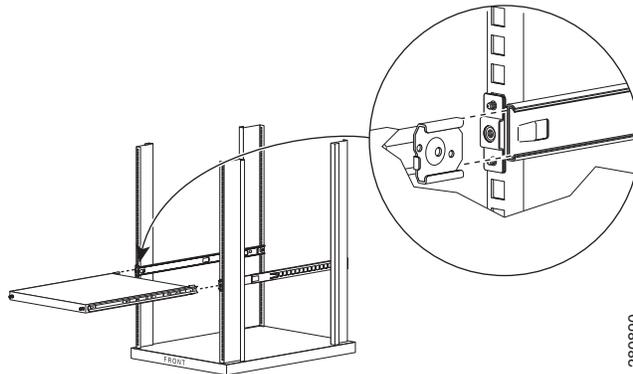
Step 3 Attach the outside rail to the back of the rack structure where the mobility services engine is going to be installed (Figure 2-3). The numbers within the illustrations indicate the order of the action.

Figure 2-3 *Attach Outer Rail to Back of Rack*



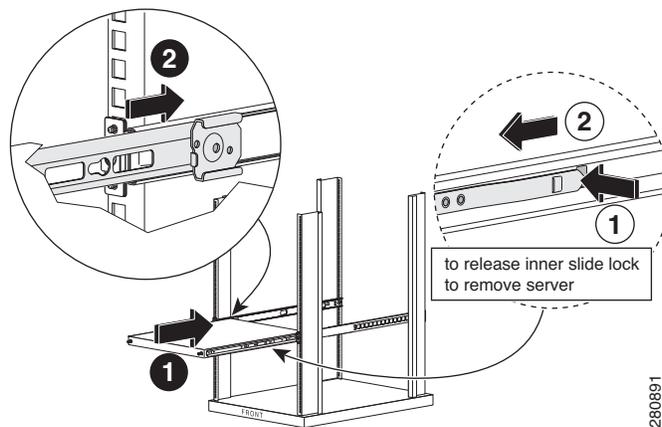
Step 4 Attach inner slide rail with mobility service engine to the outside rail that is mounted on the rack (Figure 2-4).

Figure 2-4 *Attach Inner Rail to Outer Rail*



Step 5 Slide the attached inner rail and the mobility services engine to the rear of the rack (Figure 2-5). The numbers within the illustrations indicate the order of the action.

Figure 2-5 Slide System and Inner Rail to Rear of Rack



Front and Rear Panel

Front Panel

Figure 2-6 shows a full view of the front panel of the Cisco 3350 Mobility Services Engine.

Figure 2-7 shows a detailed section of the Cisco 3350 front panel.

Table 2-1 identifies Cisco 3350 front panel components and their function.

Figure 2-6 Cisco 3350 Front Panel

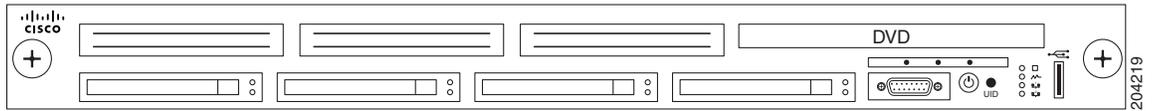


Figure 2-7 Close Up of Cisco 3350 Front Panel

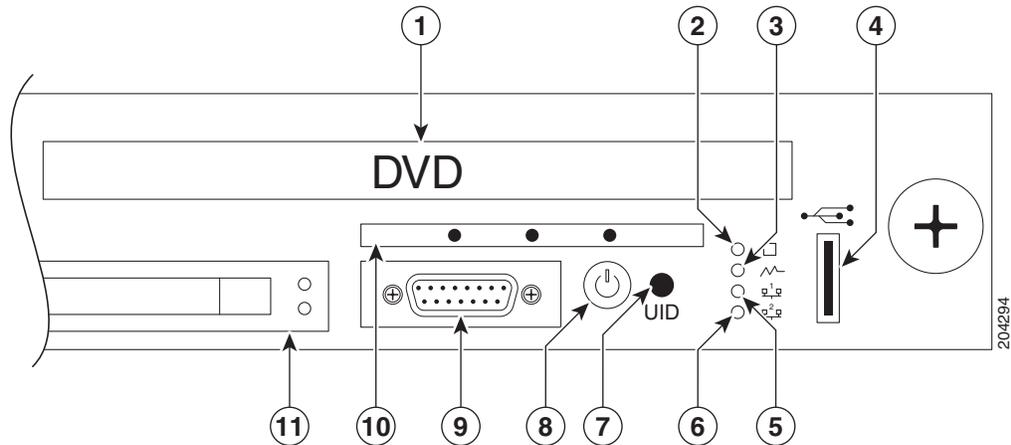


Table 2-1 Front Panel Components

Number	Component	Description or LED Status
1	DVD drive	No customer use. All system software is downloaded using Cisco WCS.
2	System LED	Green means that the system health is normal. Amber means that system health is degraded. For specific system information, pull out the diagnostic card from the front panel. Refer to the “Diagnostic Card” section on page 2-12. Red means that system health is critical. To identify the component in a critical state, pull out the diagnostic card from the front panel. Refer to the “Diagnostic Card” section on page 2-12. Off means that system health is normal (when in standby mode).
3	Power Supply LED	Green means that power supply health is normal. Amber means that power redundancy failure occurred. Off means that power supply health is normal when in standby mode.
4	USB slot	Reserved for future use.

Table 2-1 Front Panel Components (continued)

Number	Component	Description or LED Status
5	NIC1 link/activity LED	Green means that a network link exists. Note NIC1 is identified as Ethernet-0 during the automatic installation script.
		Blinking green = Network link and activity exist.
		Off means that no link to the network exists. Note If power is off, the front panel LED is not active. Check the NIC1 LED on the rear panel. Refer to the “Rear Panel” section on page 2-14.
6	NIC2 link/activity LED	Green means that a network link exists. Note NIC2 is identified as Ethernet-1 during the automatic installation script.
		Blinking green means that a network link and activity exist.
		Off means that no link to the network exists. Note If power is off, the front panel LED is not active. Check the NIC2 LED on the rear panel. Refer to the “Rear Panel” section on page 2-14.
7	UID	Blue means that identification is activated. Flashing blue means that the system is being remotely managed. Off means that identification is deactivated.
8	Power On/Standby button and system power LED	Green means that the system is on.
		Amber means that the system is shut down, but power is still applied.
		Off means that the power cord is not attached, power supply failure has occurred, no power supplies are installed, facility power is not available, or power button cable is disconnected.
9	Video connector (DB-15)	Serial connection is recommended. Do not connect any equipment to this port.
10	Diagnostic card	Provides status on the power supplies, internal processors, DIMMS, memory, temperature and alarms. Refer to the “Diagnostic Card” section on page 2-12 for details.
11	Hard drive bay (1 of 4)	Do not remove a hard drive unless it is malfunctioning and you are directed by Cisco technical support to do so.

Diagnostic Card

Figure 2-8 shows details of the diagnostic card found on the front panel.

Table 2-2 summarizes the internal components of the mobility services engine that are tracked by the diagnostic card. Definitions of each of the LED states for those components are also summarized.


Note

This information is not currently summarized within Cisco WCS.

Figure 2-8 Diagnostic Card

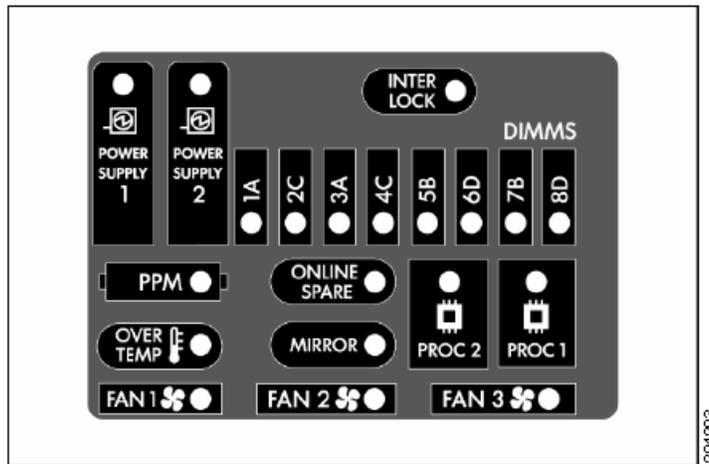


Table 2-2 Diagnostic Card LEDs

Component	LED Status
Power Supply 1 <i>or</i> 2 LED is Amber or Red.	<p>Red means that one or more of the following conditions might exist:</p> <ul style="list-style-type: none"> Processor in socket X has failed. Processor X is required yet not installed in the socket. Processor X is unsupported. <p>Amber means that the processor in socket X is in a pre-failure condition.</p>
Power Supply 1 <i>and</i> 2 LEDs are Red.	Red means that the processor types are mismatched.
Interlock	Red means that the PCI riser board assembly is not seated properly.

Table 2-2 Diagnostic Card LEDs (continued)

Component	LED Status
DIMMs, one slot	<p>Red means that one or more of the following conditions may exist:</p> <ul style="list-style-type: none"> • FBDIMM in slot X has failed. • FBDIMM in slot X is an unsupported type, and no valid memory exists in another bank <p>Amber means that one or more of the following conditions may exist:</p> <ul style="list-style-type: none"> • FBDIMM in slot X has reached single-bit correctable error threshold. • FBDIMM in slot X is in a pre-failure condition. • FBDIMM in slot X is an unsupported type, but valid memory exists in another bank.
DIMMs, all slots	Red means that no valid or usable memory is installed in the system.
PPM	Red means that the Integrated Processor Power Module (PPM) has failed.
Online Spare	<p>Green means that protection is enabled.</p> <p>Blinking amber means that a memory configuration error.</p> <p>Amber means that a memory failure occurred.</p> <p>Off = No protection.</p>
Proc 1 <i>or</i> Proc 2 is Amber or Red	<p>Red = One or more of the following conditions may exist:</p> <ul style="list-style-type: none"> • Processor has failed. • Processor is required yet not installed in the socket. • Processor is unsupported. <p>Amber means that the processor in socket X is in a pre-failure condition.</p>
Proc 1 <i>and</i> Proc 2 are Amber or Red	Processor types are mismatched.
Over Temp	<p>Amber means that the health driver has detected a cautionary temperature level.</p> <p>Red means that the system has detected a critical temperature level.</p>

Table 2-2 Diagnostic Card LEDs (continued)

Component	LED Status
Mirror	Green means that protection is enabled for the memory.
	Blinking amber means that there is a memory configuration error.
	Amber means that a memory failure occurred.
	Off means that there is no protection.
Fan 1, 2, or 3	Amber means that a redundant fan has failed.
	Red means that the minimum fan requirements are not being met in one or more of the fan modules. One or more fans have failed or are missing.

Rear Panel

Figure 2-9 shows details of the rear panel for the Cisco 3350 Mobility Services Engine.

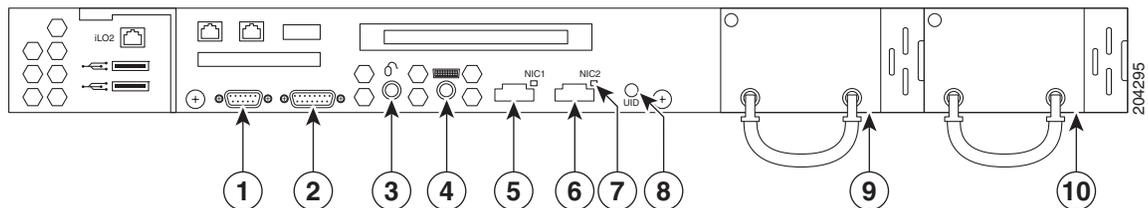
Table 2-3 identifies Cisco 3350 back panel components and their function.

Table 2-4 summarizes pin assignment for the DB9 cable.



Note

Items not labeled in Figure 2-9 are not currently assigned an active role on the system.

Figure 2-9 Cisco 3350 Mobility Services Engine Rear Panel**Table 2-3** Back Panel Components

Number	Description
1	DB9 serial connector for console. See pinouts in Table 2-4.
2	DB15 connector.
3	Mouse connector.
4	Keyboard connector.
5	NIC 1 (Ethernet-0) connector and LED. <ul style="list-style-type: none"> Green LED indicates link exists. Off (unlit) LED indicates no link.

Table 2-3 Back Panel Components (continued)

Number	Description
6	NIC 2 (Ethernet-1) connector and LED. <ul style="list-style-type: none"> Green LED indicates link exists. Off (unlit) LED indicates no link.
7	NIC 2 link status LED (same function as LED for NIC 1)
8	UID button and LED. <ul style="list-style-type: none"> Blue means that identification is activated. Blinking blue means that the system is being managed remotely. Off (unlit) means that identification is deactivated.
9	Power Supply 2. <ul style="list-style-type: none"> Green means normal operation. Off means that the system is off or the power supply has failed.  <p>Warning This unit might have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028</p>
10	Power Supply 1. <ul style="list-style-type: none"> Green means normal operation. Off means that the system is off or the power supply has failed.  <p>Warning This unit might have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028</p>

Table 2-4 Pin Assignments for DB9 Pinout

Pin	Assignments	Description
1	DCD	Data Carrier Detect
2	RD	Receive Data
3	TD	Transmit Data
4	DTR	Data Terminal Ready
5	SG	Signal Ground
6	DSR	Data Set Ready
7	RTS	Request to Send
8	CTS	Clear to Send
9	Ring	Ring Indicator

Connecting and Using the CLI Console

For initial system configuration, use the command-line interface (CLI) console. The CLI console connects to the mobility services engine back-panel DB9 console port. [Figure 2-9](#) shows the console port on the back panel of the mobility services engine. Back panel components are described in [Table 2-3](#). Console port pinouts are shown in [Table 2-4](#).

**Note**

Use either a Crossover serial cable or Null modem cable to connect the console ports.

Use these terminal emulator settings for the CLI console session:

- 9600 baud
- 8 data bits
- no flow control
- 1 stop bit
- no parity

Powering On the Mobility Services Engine

When you apply AC power to a mobility services engine, the bootup script initializes the operating system and its stored configurations. You are prompted to enter a user ID and password and enter key configuration details.

Follow these steps to power up the mobility services engine.

Step 1 Plug an AC power cord into the back of the power supplies of the mobility services engine ([Figure 2-9](#)), and connect the other end to a grounded 100 to 240 VAC 50/60 Hz electrical outlet.

The end of the power cord that plugs into the mobility services engine conforms with the IEC 320 standard.

Step 2 Use the front-panel Power On/Standby button to turn the mobility services engine on ([Figure 2-7](#)).

Step 3 At the login prompt, enter the mobility services engine operating user ID and password. The default user ID is *root* and the default password is *password*.

The user ID and password are case sensitive.

You are now logged into the mobility services engine operating system.

Continue to the [“Configuring the Mobility Services Engine”](#) section on page 2-16.

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 can be done with Cisco WCS. For details on automatic installation refer to the [“Automatic Installation Script”](#) section on page 2-17.

**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**.

Automatic Installation Script

**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.

**Note**

You can rerun the automatic installation script at any time to add or change parameters. There is no need to reenter values that you do not want changed 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.

The automatic installation script that displays to the screen is shown below along with descriptive text.

Example text: Indicates the installation script that displays to the console.

Body text: Provides additional information to the user about steps within the script.

Enter the login *root*.

```
localhost.localdomain login:
```

Enter the password *password*.

```
Password:
```

```
Setup parameters via Setup Wizard (yes/no) [yes]:
```

Enter **yes** if you want to use the setup wizard or **No** if you want to manually set the parameters. Only experienced Linux system administrators should opt to configure the system using the setup script. The option in square brackets is the default. You can press **Enter** to choose that default.

When you enter **Yes** the following displays on the console.

```
Welcome to the mobility services engine setup.  
Please enter the requested information. At any prompt,  
enter ^ to go back to the previous prompt. You may exit 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.
```

Changes made will only be applied to the system once all the information is entered and verified.

```
Current hostname=[localhost]
Configure hostname? (Y)es/(S)kip/(U)se default [Yes]: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 [localhost]: mse-nyc
```

Enter a domain name for the network domain to which this device belongs. The domain name should start with a letter, and it should end with a valid domain name suffix such as *.com*. It must contain only letters, numbers, dashes, and dots.

```
Current domain=[localdomain]
Configure domain name? (Y)es/(S)kip/(U)se default [Yes]: Y
```

```
Enter a domain name [localdomain]: cisco.com
```

```
Current IP address=[209.165.201.25]
Current eth0 netmask=[255.255.255.224]
Current gateway address=[209.165.201.1]
Enter eth0 IP address [209.165.201.25]:
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]: Y
```

Enter **Yes** if you want to provide information for Ethernet-0 (eth0) interface.



Note A network administrator can provide you with the IP address, network mask, and default gateway address for the prompts that follow.

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

```
Enter eth0 IP address [209.165.201.25]:
Enter the network mask for IP address 209.165.201.25.
Enter network mask [255.255.255.224]:
```

Enter a default gateway address for this machine.
Note that the default gateway must be reachable from the first ethernet interface

```
Enter default gateway address [209.165.201.1]:
```

```
The second ethernet interface is currently disabled for this machine.
Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

Enter **Yes** if you want to provide information for a second ethernet (eth1) interface.



Note Entry of a second ethernet interface (eth1) can be skipped by entering **skip**.

Enter an IP address for the second ethernet interface (eth1) on this machine.

```
Enter eth1 IP address [none]:
```

Enter the network mask for the IP address you specified.

```
Enter network mask [255.0.0.0]:
```



Note If you entered an IP address and mask for the second interface (eth1) of this machine, you are given the opportunity to define up to two static routing entries for that interface. Static routes are typically used in lab environments to mimic out-of-band networks and are not recommended for implementation within your network unless you have extensive experience in their use.



Note If you do not want to configure any static routes, enter **none** at the network address prompt seen below. You will not be prompted for the network mask and gateway address.



Note If you want to configure only one route, you can enter **none** when you are prompted for the second network address. You will not be prompted for the network mask and gateway address for the second route.

Enter the network address to define a static route for eth1.

```
Enter network [none]:
```

Enter the network mask for the network address you entered above.

```
Enter network mask [255.0.0.0]:
```

Enter a gateway address for the network address and network mask you provided.

```
Enter gateway address:
```

Enter DNS information.

```
Domain Name Service (DNS) Setup
DNS is currently enabled.
No DNS servers currently defined
Configure DNS related parameters? (Y)es/(S)kip/(U)se default [Skip]:Y
```

```
Enable DNS (yes/no) [yes]: Yes
Enter primary DNS server IP address: 209.165.201.20
Enter backup DNS server IP address (or none) [none]:
```

Enter time zone information.



Note Communications between the mobility services engine, Cisco WCS and the controller are in universal time code (UTC). Local time zones are configured on the mobility services engine to assist network operations center personnel in locating events within logs. Configuring NTP on each system provides devices with the UTC time.

```
Current timezone=[America/Los_Angeles]
Configure timezone? (Y)es/(S)kip/(U)se default [Skip]:
```

Enter NTP server information.



Note The mobility services engine and its associated controllers must be mapped to the same NTP server and the same Cisco WCS server. An NTP server is required to automatically synchronize time between the controller, Cisco WCS and the mobility services engine.

```
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]: **yes**

Enter NTP server name or address: 1.ntp.es1.cisco.com

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

A login banner appears when a user logs in through the console or SSH. This example shows the default banner. You can change the text that appears in this banner in the steps below. The banner is usually used to warn users that they are entering a private system.

Current Login Banner = [Warning!]

Configure login banner (Y)es/(S)kip/(U)se default [Skip]:

Enter text to be displayed as login banner. Enter a single period on a line to terminate.

Login banner [Warning!]:

Cisco Mobility Service Engine.

Remote root login is currently disabled.

Enter **Y** in the step below to configure and enable remote root login (access) from the console.



Note If you enable *remote root access*, serial and SSH connections are supported. Local monitor and keyboard access is denied.



Note If you disable *remote root access*, then both the local monitor and keyboard work along with the serial connection. SSH access is disabled.

Configure remote root access? (Y)es/(S)kip/(U)se default [Skip]: **N**

Enter whether or not you would like to allow remote root login via secure shell for this machine.

Enable remote root login (yes/no) [no]: **N**

SSH root access is currently enabled.

Configure ssh access for root (Y)es/(S)kip/(U)se default [Skip]: **N**

Enter whether or not you would like to enable ssh root login. If you disable this option, only console root login will be possible.

Enter **yes** (below) to allow remote login through SSH v2 (ssh root login) in addition to console login. Choose **no** to allow *root* login only from the console.

Enable ssh root access (yes/no): **yes**



Note If you forget the *ssh root* login password, you can enter into *single user mode* and change the password. To prevent unauthorized access, a password for the *single user mode* can be defined.

```
Single user mode password check is currently enabled.
Configure single user mode password check (Y)es/(S)kip/(U)se default [Skip]: Y
The single user mode is usually used for recovery
operations. For example, when the root password is
forgotten, you can log into single user mode and reset
the root password.
*****
!!WARNING!!
-----
If single user mode password check is enabled and
the root password is forgotten, the appliance
will be unusable as it cannot be logged into
successfully. Do not enable this option unless it
is required. (Press ^ to go back to previous step.)
*****
```

**Caution**

If you forget the *single user mode* password, you cannot login and you will need to contact TAC to arrange for an RMA.

```
Enable password check for single user mode login (yes/no) [yes]: yes
```

Enter the desired value for each of the password parameters or hit **Enter** to accept the default parameter value.



Note These parameter settings apply to ALL passwords that you enable and set during the installation script.

```
Login and password strength related parameter setup
Maximum number of days a password may be used : 60
Minimum number of days allowed between password changes : 1
Minimum acceptable password length : 9
Login delay after failed login : 5
Checking for strong passwords is currently enabled.
```

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

Enter login and password related parameters.

```
Maximum number of days a password may be used(1-99999, 99999 means no expiry) [60]:
Minimum number of days a password may be used(0-99999, 0 means no minimum) [1]:
Minimum acceptable password length(8-10) [9]:
Login delay in seconds after failed login(0-15) [5]
Enable strong password checking? [yes/no] [yes]:
```

Enter **Y** to enable and define a *root* (superuser) password. Press Enter to skip this step.

```
Configure root password? (Y)es/(S)kip/(U)se default [Skip]: Y
```

Enter a password for the superuser.

Enter a password for the superuser and confirm it by typing it again. Your typing is not visible.

```
Enter root password:
Confirm root password:
```

You can also configure a *strong* (GRand Unified Bootloader (GRUB)) password. A strong password must have a minimum of 9 characters and must include: two lowercase letters, two digits and two special characters (such as \$ and #). An error message displays if you enter an inadequate password.

**Caution**

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

**Note**

If a *strong* password is not enabled, a password can be of any length.

**Note**

Passwords defined *before* a strong password is set are not affected by the *strong* password setting. Only those passwords that are set *after* the strong password is set are affected. For example, *strong* passwords will be required for passwords set later in this script such as the Cisco WCS communication password (as noted in example below) and as passwords expire.

```
GRUB password is not currently configured.
Configure GRUB password (Y)es/(D)isable/(S)kip/(U)se default [Skip]: Y
GRUB is the Linux bootloader. Setting a password for
the GRUB loader means that each time the appliance is
powered up, you will be prompted for the GRUB password
you configure here.
```

```
*****
!!WARNING!!
-----
```

```
If the GRUB password is forgotten, the appliance
will be unusable as it cannot be booted up
successfully. Do not configure this option unless it
is required. (Press ^ to go back to previous step.)
*****
```

Enter a password for the grub menu.

```
Enter GRUB Password:
Verify GRUB Password:
```

Password must be 9 characters long. Try again.

```
Enter GRUB Password:
Verify GRUB Password:
UP = 2, LO = 6, DIGIT = 3, PUNCT = 0
Password must contain 2 uppercase, 2 lowercase letters,
2 digits and 2 special characters. Try again.
```

```
Enter GRUB Password:
Verify GRUB Password:
```

Enter **Y** to enable and define a *Cisco WCS communication* password.

**Note**

This password does not define an individual user password for access to the Cisco WCS GUI. This password is used for SOAP/XML authentication between systems (such as mobility services engines) and Cisco WCS.

```
Configure WCS communication password? (Y)es/(S)kip/(U)se default [Skip]: Y
```

Enter a password for the admin user.
 The admin user is used by the WCS 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 WCS page for MSE General Parameters so that the WCS can communicate with the MSE.

Enter a password for Cisco WCS communication and confirm it by typing it again. Your typing is not visible.

Enter WCS communication password:
 Confirm WCS communication password:



Note It is recommended that you set a BIOS password to prevent unauthorized BIOS access.

All of the information that was entered into the install script appears on the screen.

Please verify the following setup information.

```
-----
Host name= mse-nyc
Domain=cisco.com
Eth0 IP address=209.165.201.25, Eth0 network mask=255.255.255.224
Default gateway=209.165.201.1
Enable DNS=yes, DNS servers=209.165.201.20
Enable NTP=yes, NTP servers=1.ntp.esl.cisco.com
Login banner =
Cisco Mobility Service Engine.
Enable Remote Root Login=no
Enable SSH root access=yes
Enable Single User Mode Password Check=no
Password/Login parameters :
Password min length=9
Password min days =1
Password max days =60
Failed login delay =5
Strong password checking=yes
Root password is changed.
GRUB password is changed.
WCS password is changed.
-----
```

```
You may enter "yes" to proceed with configuration, "no" to make
more changes, or "^" to go back to the previous step.
Is the above information correct (yes, no, or ^): yes
-----
```

```
Setup will now attempt to apply the configuration.
Applying hostname related parameters...
Generating /etc/hosts
Running hostname mse-nyc.cisco.com
Generating /etc/sysconfig/network
Updating /proc/sys/kernel/hostname
Applying eth0 related parameters...
Generating /etc/sysconfig/network-scripts/ifcfg-eth0
Applying DNS related parameters...
Generating /etc/resolv.conf
Restarting network services with new settings.
Shutting down interface eth0:
Shutting down loopback interface:
Setting network parameters:
Bringing up loopback interface:
Bringing up interface eth0:
Applying NTP related parameters...
```

```

Generating /etc/ntp.conf and /etc/ntp/step-tickers
Setting system clock from NTP.
11 Apr 15:56:59 ntpdate[15176]: step time server 209.165.201.22 offset -37.556823 sec
Synchronizing hardware clock
Generating /etc/sysconfig/clock
Applying remote root login related parameters...
Disabling single user mode login password check...

Setting password/login parameters....
Setting root password.
Changing password for user root.
passwd: all authentication tokens updated successfully.
Setting grub password...
Setting wcs password.
***Configuration successful***
We recommend you reboot the system to ensure changes are operational.
Reboot now? (yes/no) [yes]: yes
Some of your changes will only take effect after the next reboot.
Exiting setup script...
[root@sanity-lbs setup]#
Script done on Wed 30 Sept 2008 03:58:12 PM PDT

```

After the script configuration appears on the screen, you are asked to verify all the setup information you provided. You can enter **Yes** to proceed with the configuration, **No** to make more changes, or **^** to go back to the previous step.

Is the above information correct (yes, no, or ^):

If you enter **yes**, the configuration information is applied. Cisco recommends that you reboot the system when prompted to ensure that the changes are applied.

**Note**

The message “***Configuration successful***” appears on the screen when the configuration is complete.

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**.

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

Configuring an NTP Server

You can configure NTP servers to set up the time and date of the mobility services engine.

**Note**

You are automatically prompted to enable NTP and enter NTP server IP addresses as part of the automatic installation script. For more details on the automatic installation script, refer to the [“Configuring the Mobility Services Engine” section on page 2-16](#).

**Note**

If you need to add or change an NTP server installation after a mobility services engine install, rerun the automatic installation script. You can configure the NTP server without adjusting the other values by just tabbing through the script. To rerun the automatic script, log in as *root* and run **/opt/mse/setup/setup.sh**.

**Note**

For more information on the NTP configuration, consult the Linux configuration guide.

Launching the Mobility Services Engine

To configure a mobility services engine to automatically launch after bootup enter:

```
[root@mse-server1]# chkconfig msed on
```

To start the image manually, enter: `/etc/init.d/msed start`

Verifying the Mobility Services Engine Software State

You can verify the mobility services engine software state at any time. In the mobility services engine CLI interface, enter: `/etc/init.d/msed status`

If the mobility services engine is running, the command output looks like this example:

```
-----  
Server Config  
-----  
Product name: Cisco Mobility Service Engine  
Version: x.x.x.x  
Hw Version: none  
Hw Product Identifier: none  
Hw Serial Number: none  
Use HTTPS: true  
HTTPS Port: 443  
Use HTTP: false  
HTTP Port: 80  
Legacy HTTPS: false  
Legacy Port: 8001  
Session timeout in mins: 30  
DB backup in days: 0  
  
-----  
Server Monitor  
-----  
Start time: Wed Sept 30 15:24:36 EDT 2008  
Server current time: Fri May 30 19:08:15 EDT 2008  
Server timezone: America/New_York  
Server timezone offset: -18000000  
-----  
Service Engine (1):  
-----  
NAME: Location Service  
VERSION: x.x.x.x  
-----  
Location Service Monitor  
-----  
Log Modules: 262143  
Log Level: INFO  
Days to keep events: 2  
Keep absent data in mins: 1440  
Restarts: 1  
Used Memory (bytes): 129851856  
Allocated Memory (bytes): 3087007744  
Max Memory (bytes): 3087007744
```

```

DB virtual memory (kbytes): 0
DB virtual memory limit (bytes): 256000000
DB disk memory (bytes): 4128768
DB free size (kbytes): 2856
Active Elements: 0
Active Clients: 0
Active Tags: 0
Active Rogues: 0
Active Elements Limit: 18000
Active Sessions: 0
Clients Not Tracked due to the limiting: 0
Tags Not Tracked due to the limiting: 0
Rogues Not Tracked due to the limiting: 0
Total Elements Not Tracked due to the limiting: 0

```

If the mobility services engine is not running, the command output looks like this example:

```

com.aes.common.util.AesException: Failed to connect to server: http://localhost:8001
    at com.aes.client.AesClient.connect(AesClient.java:218)
    at com.aes.location.test.AesAbstractTest.init(AesAbstractTest.java:181)
    at
com.aes.location.test.admin.AesTestGetServerInfo.main(AesTestGetServerInfo.java:75)
    at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
    at sun.reflect.NativeMethodAccessorImpl.invoke(Unknown Source)
    at sun.reflect.DelegatingMethodAccessorImpl.invoke(Unknown Source)
    at java.lang.reflect.Method.invoke(Unknown Source)
    at com.zerog.lax.LAX.launch(DashoA8113)
    at com.zerog.lax.LAX.main(DashoA8113)
#

```

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`.
 - Step 2** To check status enter `/etc/init.d/msed status`.
 - Step 3** To start the software, enter: `/etc/init.d/msed start`.
-

Updating Mobility Services Engine Software

You can update the mobility services engine using the Cisco WCS or manually download the software using a console port connected to the mobility services engine.



Note

For the latest Cisco WCS and 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 WCS.
- Approximately 5 minutes is required for the newly loaded mobility services engine software version to appear on the Cisco WCS **Mobility > Mobility Service Engines** window.



Note In release 6.0, the path is **Services > Mobility Services**.



Note Cisco WCS queries for mobility services engine connectivity and database updates every 5 minutes by default.

Downloading Software Using Cisco WCS

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

-
- Step 1** Verify that you can ping the mobility services engine from Cisco WCS or an external FTP server, whichever you are going to use for the image download.
- Step 2** In Cisco WCS, choose **Mobility > Mobility Service Engines**.
-
- **Note** In release 6.0, the path is **Services > Mobility Services**.

- Step 3** Click the name of the mobility services engine to which you want to download software.
- Step 4** Choose **Maintenance** (left panel).
- Step 5** Choose **Download Software**.
- Step 6** To download software, do one of the following:
- To download software listed in the Cisco WCS directory, select **Select from uploaded images to transfer into the Server**. Then, choose a binary image from the drop-down menu.
Cisco WCS downloads the binary images listed in the drop-down menu into the FTP server directory you have specified during the Cisco WCS installation.
 - To use downloaded software available locally or over the network, select the **Browse a new software image to transfer into the Server** and click **Browse**. Locate the file and click **Open**.
- Step 7** Enter the time in seconds (between 1 and 1800) after which software download times out.
-
- **Note** This time out setting represents the total time allowed before a software download to a mobility services engine expires. It is not a FTP packet timeout setting.

- Step 8** Click **Download** to send the software to the `/opt/installers` directory on the mobility services engine.
- Step 9** After the image has been transferred to the mobility service engine, log in to the mobility services engine CLI and run the installer image from the `/opt/installers` directory by entering the *`Jimage-name`* command.
- Step 10** To run the software, enter `/etc/init.d/msed start`.

Step 11 To stop the software, enter `/etc/init.d/msed stop` and to check status enter `/etc/init.d/msed status`.

Manually Downloading Software

If you do not want to automatically update the mobility services engine software using Cisco WCS, 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.

An example software image file name is `CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz` and it changes with each release.



Note The mobility services engine image is compressed at this point.



Note The default login name for the FTP server is `ftp-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.gz
<CTRL-Z>
#
```

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

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

The decompression yields a `bin` file.

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

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

Step 2 To manually stop the mobility services engine, login as `root` and enter:

```
/etc/init.d/msed stop.
```

Step 3 To install the new mobility services engine image, enter:

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

Step 4 To start the new mobility services software, by enter:

```
/etc/init.d/msed start
```

**Caution**

Do not complete the next step, which uninstalls the script files, unless the system instructs you to do so. Removing the files unnecessarily erases your historical data.

Step 5 To uninstall the mobility services engine's script files, enter:

```
/opt/mse/uninstall
```

Recovering a Lost Root Password

If you lose or forget the root password for a mobility services engine, follow these steps:

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.

**Note**

The connection must be made over the console port, not by connecting a keyboard, mouse and monitor to the unit.

Step 2 Press **e** to edit.

Step 3 Navigate to the line beginning with "kernel," and press **e**.

At the end of the line enter a space and the number one (1). Press **Enter** to save this change.

Step 4 Press **b** to begin boot sequence.

At the end of the boot sequence, a shell prompt appears.



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

Step 5 You can change the root password by entering the **passwd** command.

Step 6 Enter and confirm the new password.

Step 7 Restart the machine.

