Meru System Director

Getting Started Guide

Release 6.0-2.0

Ocotober 2013

Document Number: 882-30050 Rev A Rel 6.0-2.0 Ver 1 Getting Started

END USER SOFTWARE LICENSE AGREEMENT

IMPORTANT:

THIS END USER SOFTWARE LICENSE AGREEMENT (THIS "AGREEMENT") IS A LEGAL AGREEMENT BETWEEN THE END USER ("CUSTOMER") OF THE SOFTWARE ACCOMPANYING THIS AGREEMENT (THE "SOFTWARE") AND MERU NETWORKS, INC. ("MERU"). THIS AGREEMENT GOVERNS CUSTOMER'S USE OF, AND THE TERM "SOFTWARE INCLUDES, ANY AND ALL COMPUTER SOFTWARE, ANY PRINTED OR ELECTRONIC DOCUMENTATION, OR OTHER CODE, WHETHER ON A DISK, IN ANY MEMORY DEVICE, EMBEDDED IN A SEMICONDUCTOR, DOWNLOADED OR ON ANY OTHER MEDIA PROVIDED TO CUSTOMER BY MERU NETWORKS, INC. ("MERU") OR ITS AUTHORIZED RESELLER ("RESELLER") AS PART OF A MERU PRODUCT ("MERU PRODUCT") OR AS A STAND-ALONE PRODUCT. CUSTOMER MUST READ THIS AGREEMENT CAREFULLY BEFORE INSTALLING OR OTHERWISE USING THE SOFTWARE. BY INSTALLING, DOWNLOADING, EMBEDDING OR OTHERWISE USING THE SOFTWARE, CUSTOMER AGREES TO BE BOUND BY THE TERMS OF THIS AGREEMENT. THIS AGREEMENT PROVIDES A LICENSE TO USE THE SOFTWARE AND CONTAINS WARRANTY DISCLAIMERS AND LIABILITY LIMITATIONS. BY USING THE SOFTWARE IN ANY WAY, INCLUDING BUT NOT LIMITED TO, REQUESTING A LICENSE KEY FROM MERU, CUSTOMER CONFIRMS ITS ACCEPTANCE OF, AND AGREEMENT TO BE BOUND BY, THE TERMS OF THIS AGREEMENT. IF CUSTOMER DOES NOT AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT, THEN CUSTOMER MUST: (I) ERASE ALL ASPECTS OF THE SOFTWARE FROM ITS COMPUTERS; (II) NOT REQUEST FROM MERU OR ANYONE ELSE A LICENSE KEY THAT WOULD ALLOW OPERATION OF THE SOFTWARE; AND (III) NOT OPERATE THE SOFTWARE IN ANY MANNER.

Article 1. License

1.1. Grant. Subject to Customer's compliance with the terms and conditions in this Agreement, Meru grants Customer a non-exclusive, non-transferable royalty-free license to use the Software exclusively in connection with the Meru Product on which it has been embedded or for which it has been offered, and to use all written materials accompanying the Software (the "Documentation").

1.2. Ownership of Software and Confidentiality.

(a).The Software is licensed, not sold, to Customer by Meru. CUSTOMER MAY OWN THE MEDIA ON WHICH THE SOFTWARE IS PROVIDED, BUT MERU AND/OR MERU'S LICENSOR(S) RETAIN TITLE TO THE SOFTWARE. Customer acknowledges that the Software and Documentation are protected, among other ways, by federal copyright law and international treaties and that they constitute confidential information of Meru, protected also by this Agreement. The organization, structure, sequence, logic and source code of the Software are valuable trade secrets of Meru and its licensors. Except for those rights expressly granted by this Agreement to Customer, Meru or its licensors retain and shall own all rights, title and interests in and to the Software, and Customer shall have no right, title or interest in or to any of, the Software or Documentation, including without limitation, the intellectual property rights comprising or related to the Software and Documentation.

(b).Customer shall keep the Software and Documentation confidential and shall take all reasonable precautions to preserve its confidentiality, including where applicable, having all of its employees and subcontractors execute confidentiality agreements that cover the Software and Documentation. Customer shall take all steps reasonably necessary to ensure that no person or entity has unauthorized access to the Software or Documentation.

1.3. Permitted Uses. This Agreement allows Customer to use the Software solely as embedded in the Meru Product on which the Software has been installed, for execution on, or (where the applicable documentation permits installation on non-Meru equipment)

for communication with Meru Product owned or leased by the Customer and in accordance with Meru's documentation. Notwithstanding the restrictions set out above in Section 1.2, Customer may make one copy of any Software that is offered separate from, not embedded in, a Meru Product, in a machine-readable form for back-up purposes only, subject to Customer including on the copy all copyright, trademark and other proprietary rights notices, as contained on the original version. Customer may copy the Documentation in a reasonable number for employees using the Software, subject to Customer including on each copy all copyright, trademark and other proprietary rights notices, as contained in the original version of the Documentation.

1.4. Restrictions on Use. Customer may not, nor may Customer permit any third party to: (a) decompile, reverse engineer, disassemble, or otherwise attempt to derive, reconstruct or discover any humanly readable form of the Software source code; (b) modify, translate, copy, reproduce, disclose, or create derivative works of the Software or Documentation; (c) allow access to the Software or Documentation by any third party other than agents and representatives working on Customer's behalf; or (d) rent, lease, loan, distribute, assign or transfer the Software unless expressly permitted in writing by Meru or by this Agreement. Customer may not disclose, provide, or otherwise make available any trade secret and/or copyrighted material, including without limitation, the specific design and structure of individual programs or trade secrets, contained within or related to the Software to any third party without Meru's prior written consent. Additionally, Customer shall keep any result of any benchmark or other evaluation of the Software confidential and shall not publish any result of any such result without Meru's prior written consent. Customer will implement reasonable security measures to protect such trade secrets and copyrighted materials. Customer shall not under any circumstance, and shall not permit any third party to, prepare any error correction, modification or derivative work of the Software or Documentation or remove deface or obscure any product identification, copyright, trademark, suppliers' proprietary rights notices, or other notice on or in the Software or on output generated by the Software or the Documentation.

Article 2. Termination. This Agreement is effective until terminated. Customer's rights under this Agreement will terminate automatically without notice from Meru if Customer violates any of the restrictions in Article 1 or breaches any term(s) of this Agreement. Upon termination, Customer must destroy all copies of the Software in Customer's possession or control. Customer acknowledges and agrees that any unauthorized use, transfer, sublicensing or disclosure of the Software may cause irreparable injury to Meru, and under such circumstances, Meru shall be entitled to equitable relief, without posting bond or other security, including but not limited to, preliminary and permanent injunctive relief.

Article 3. Disclaimer of Warranty.

3.1. **TO THE MAXIMUM EXTENT PERMITTED BY LAW, MERU AND MERU 'S LICENSOR(S) (FOR THE PURPOSES OF ARTICLES 3 AND 4, MERU AND MERU 'S LICENSOR(S) SHALL BE COLLECTIVELY REFERRED TO AS "MERU ") PROVIDES THE SOFTWARE AND DOCUMENTATION "AS IS" AND "WITHOUT WARRANTY", AND WITH RESPECT TO THE SOFTWARE AND ANY DOCUMENTATION, MERU HEREBY SPECIFICALLY EXCLUDES AND DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY, AND FITNESS FOR A PARTICULAR USE AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED BY LAW, STATUTE OR COURSE OF DEALING, AND MERU SPECIFICALLY EXCLUDES ALL REPRESENTATIONS AND WARRANTIES, WHETHER STATUTORY OR OTHERWISE, WITH RESPECT TO NON-INFRINGEMENT OF ANY NATURE OF THE RIGHTS OF ANY THIRD PARTY.**

3.2. SPECIFICALLY, MERU DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET CUSTOMER'S REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. FURTHERMORE, MERU DOES NOT WARRANT OR MAKE ANY REPRESENTATION REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE OR RELATED DOCUMENTATION IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY MERU OR MERU AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY.

3.3. Meru does not warrant that the Software or any Appliance will be free of vulnerability to intrusion, virus attack or hacker attacks. The Software is not fault-tolerant nor designed or intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air

traffic control, weapons systems, direct life-support machines or any other application in which the failure of the Software could lead directly to death, personal injury, or severe physical or property damage (collectively, "**High Risk Activities**"). Meru expressly disclaims any express or implied warranty of fitness for High Risk Activities.

Article 4. Limitation of Liability.

4.1. **CUSTOMER ASSUMES THE ENTIRE RISK AS TO RESULTS AND PERFORMANCE OF THE SOFTWARE. TO THE MAXIMUM EXTENT PERMITTED UNDER LAW, UNDER NO CIRCUMSTANCE SHALL MERU BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF ANY KIND OR NATURE WHATSOEVER ARISING OUT OF OR IN ANY WAY RELATED TO THIS AGREEMENT OR THE SOFTWARE**. Such limitation of damages includes, but is not limited to, lost good will, lost profits, loss of data or software, work stoppage or impairment of other goods, regardless of the legal theory on which the claim is brought, even if Meru has been advised of the possibility of such damage or if such damage could have been reasonably foreseen, and notwithstanding any failure of essential purpose of any exclusive remedy provided in this Agreement.

4.2. **IN NO EVENT SHALL MERU'S TOTAL LIABILITY IN CONNECTION WITH THIS AGREEMENT OR THE SOFTWARE, WHETHER BASED ON CONTRACT, WARRANTY, TORT, INCLUDING NEGLIGENCE, STRICT LIABILITY OR OTHERWISE, EXCEED (i) THE AMOUNT TO MERU FOR THE SOFTWARE LICENSE, OR (ii) IF NO SEPARATE FEE WAS PAID FOR THE SOFTWARE LICENSE, THE AMOUNTS PAID FOR THE MERU PRODUCT IN WHICH THE SOFTWARE IS EMBEDDED. IN NO CASE SHALL MERU BE LIABLE FOR THE COST OF PROCUREMENT OF ANY SUBSTITUTE PRODUCT, SOFTWARE OR SERVICE.**

4.3. Customer acknowledges that its agreement to the limitations of liability set out in this article is a crucial part of its consideration for the rights under the license grant.

Article 5. U.S. Government Rights. If Customer is the U.S. Government, Customer acknowledges that it obtains only those rights customarily provided to commercial end use customers. For U.S. governmental entities, this commercial license is provided in accordance with FAR 12.211 (Technical Data) and 12.212 (Computer Software) and, for Department of Defense purchasers, DFAR 252.227-7015 (Technical Data – Commercial Items) and DFAR 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation). Use, duplication or disclosure by the U.S. Government is subject to the restrictions set forth in FAR 52.227-14(g), Rights in Data—General (June 1987) and FAR 52.227-19, Commercial Computer Software—Restricted Rights (June 1987), or if under Department of Defense, DFAR 252.227-7015(b), Technical Data—Commercial Items (June 2004) and DFAR 227.7202-3(a) June 2005) in accordance with this Agreement. If Customer is a governmental entity that has a need for rights not addressed above in this Article 5, it must negotiate a separate agreement with Meru. Customer acknowledges that the Software source code is unpublished and that all rights are reserved under the copyright laws of the United States. Any use, modification, reproduction, display or disclosure of the Software or any documentation by the United States Government shall be governed by the terms of this Agreement.

Article 6. Export. The Software may be subject to the United States laws and regulations related to the export of technical data and products produced from such data. Customer shall not, without fully complying with all applicable laws and regulations, including all United States laws and regulations with respect to export, export any Software or any Appliance, allow any Software to be exported or transfer any Software to any person or entity that engages in the research or production of military devices, armaments or any instruments of warfare, including biological, chemical and nuclear warfare.

Article 7. Governing Law. This Agreement will be governed by and construed in accordance with the laws of the State of California, U.S.A., without reference to its conflict of law principles, and the United Nations Convention on Contracts for the International Sale of Goods does not apply. Except for actions for injunctive relief for a violation of intellectual property rights or confidentiality obligations, any action by either party with respect to this Agreement or the Software must be brought in the state or federal courts sitting in Santa Clara County, California, and each party submits to the personal jurisdiction of such courts.

Article 8. **Injunctive Relief**. Customer acknowledges that its violation of any restriction set out in Article 1 or of any obligation set out under Article 2 may cause irreparable harm to Meru and upon any such violation, Meru shall be entitled to seek equitable relief without posting any bond or other security.

Article 9. **Entire Agreement; Waiver; Modifications; Severability**. This Agreement constitutes the entire agreement between the parties with respect to the subject matter of this Agreement and supersedes and replaces all prior or contemporaneous understandings or agreements, written or oral, with respect to such subject matter. No modification or amendment of this Agreement or any waiver of any right under this Agreement shall be effective unless in writing and signed by an authorized representative of the party to be charged. Any waiver of any breach of any provision of this Agreement shall not be construed as a waiver of any continuing or succeeding breach of such provision or a waiver or modification of the provision. If a court of competent jurisdiction finds any provision of this Agreement invalid or unenforceable, that provision will be amended to achieve as nearly as possible the same economic effect as the original provision and the remainder of this Agreement will remain in full force. Failure of a party to enforce any provision of this Agreement shall not constitute and shall not be construed as a waiver of such provision or of the right to enforce such provision. CUSTOMER ACKNOWLEDGES THAT IT IS NOT RELYING UPON ANY ORAL REPRESENTATION BY Meru OF ANY NATURE, INCLUDING WITH RESPECT TO ANY WARRANTY.

Contents

Chapter 1
Initial Setup

This chapter describes how to set up a simple WLAN with a minimum configuration via either of two methods: commands entered via a terminal session in the Command Line Interface (CLI) or via the EzSetup Wizard portion of the WebUI. The first path, configuration via the CLI, is described in **Setup Via CLI**. To perform configuration via the EzSetup wizard, refer to **Configuration Via the WebUI Wizard**.

If you need help while using the WebUI, use the WebUI Help system. It supplies the information for learning how to use the configuration, maintenance, and management pages. An overview of the Help system is available by clicking the Help link on the WebUI opening page, located in the right side navigational pane. Specific help for the active view is available on each WebUI page by clicking the Help link.

This chapter contains the following sections:

Before You Start

Before you set up your WLAN, ensure you have met the following prerequisites:

- Consult the System Director Release Notes for the latest features, bug fixes, and known issues.
- You have installed the controller, as described in the *Meru Controller Install Guide*.
- You have installed the access points, as described in the *Meru Access Point Install Guide*.
- You have a Null modem cable (serial cable with DB-9 female connectors or RJ-45 connectors, depending on your controller model) on hand for attaching to the console port of the controller.
- You have a PC or laptop with terminal session software.
- You have site's IP configuration settings for your controller—ask your local network administrator for the following network settings, as needed for your configuration, and write them in the spaces provided here:
  - IP address and netmask for the controller _____
  - DHCP server address _____
  - gateway server address _____
  - DNS server addresses _____
  - network domain name _____
  - primary and secondary RADIUS Server addresses _____
  - syslog server address_____
  - SIP server _____

Connecting to the Controller

Make sure you know the locations of the following ports—see the following figures:

- Primary Ethernet port connector (G1 or LAN1) to connect to the Ethernet switch
- RS-232 serial or Console port connector for initial connection to the PC or laptop
- Power cord inlet connector
- Power On/Off switch

Figure 1: MC1550 Rear Panel

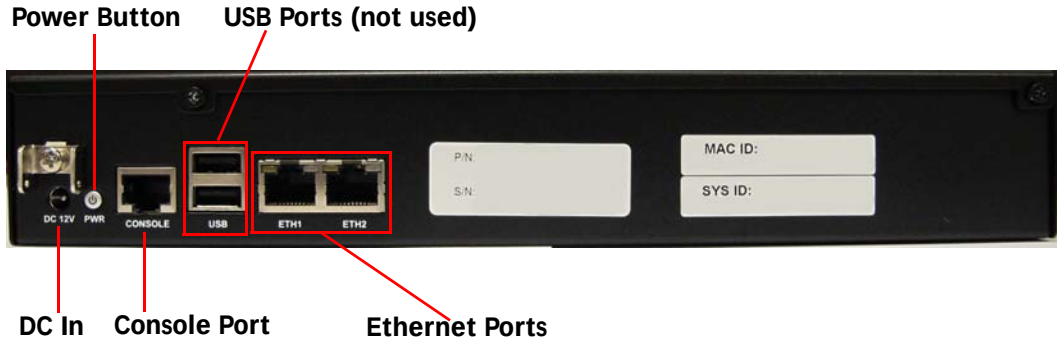


Figure 2: MC1500 Front Panel

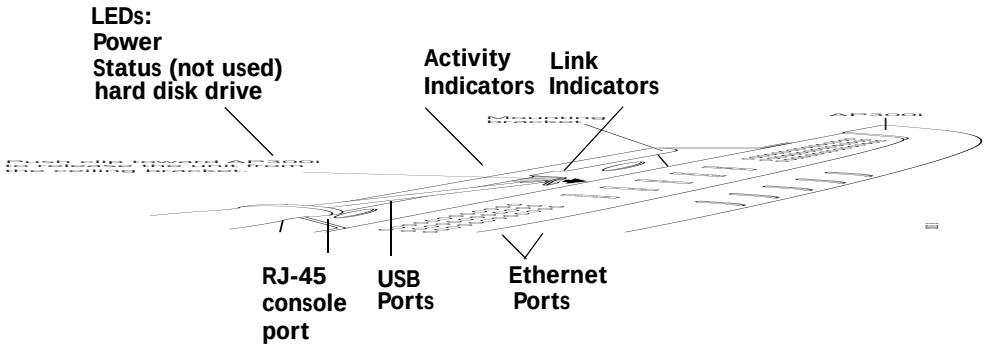


Figure 3: MC3200 and MC4200 Front Panel

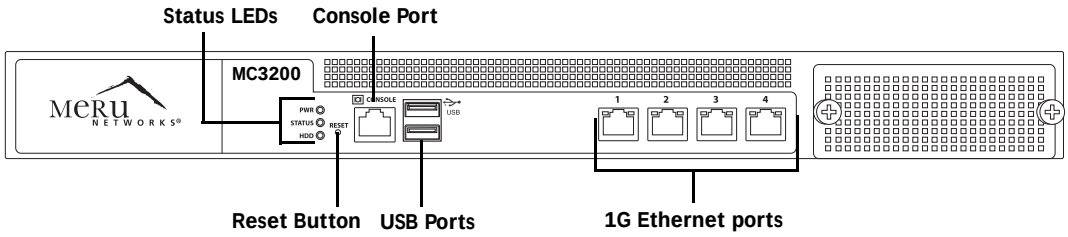
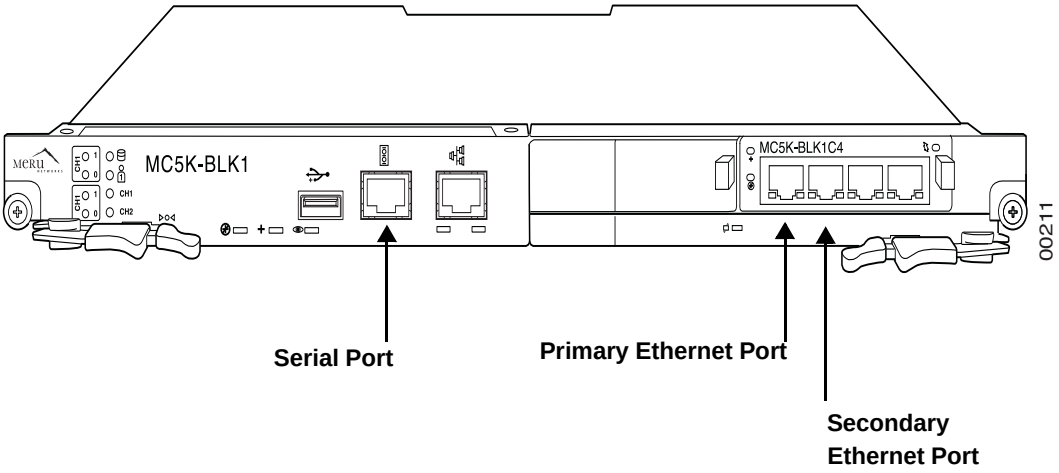


Figure 4: MC5000 Controller Blade



Initial Setup for a Controller

As stated in the opening to this chapter, the initial configuration procedure can be performed via either the CLI or the WebUI based on the user's preference. Follow the steps provided for the section below that corresponds to your preference.

Note: Prior to performing initial software setup, it is recommended that users consult the *Meru Controller Installation Guide* for instructions on physically installing the controller.

Setup Via CLI

Initial setup of a controller requires a serial connection to a PC or laptop to configure the controller network identification settings. After that, the controller management interface can be accessed through the network via an SSH2 connection for using the CLI or secure HTTP connection from the WebUI.

1. Before applying power to the controller, make sure the controller is connected to an Ethernet switch.

2. Set up a serial connection from the PC or laptop to the controller. *For the initial controller configuration, you must connect to the controller using the serial port.*

   Plug the Null modem serial cable into the controller serial port and the other end into the serial port of the PC or laptop.

3. On the PC or laptop, set up an ANSI or VT100 compatible terminal session with the following settings:
   - Baud—115200
   - Data—8 bits
   - Parity—None
   - Stop Bit—1
   - Flow Control—None

Caution! Only one terminal session is supported at a time. Making multiple serial connections causes signalling conflicts, resulting in damage or loss of data.

4. Plug the controller into the AC power source. Note that some controller models require more than one AC connection.

Note: If the controller has two AC plugs on the back but boots up when only one is connected, it may sound an alarm noise. To disable this sound, press the red button on the back of the controller.

5. If the controller does not turn on automatically, press the controller Power On/Off switch. When the controller boots for the first time, it shows a series of informational messages and then presents the default login prompt. Ignore all messages until the default login prompt appears.
6. Log in with the user name as **admin**, password **admin**:

```
default login: admin
Password:
```

7. Type **setup** and press Enter to access the initial configuration script:

Note: The **setup** script can be canceled during any step by typing “quit” at the prompt. Note, however, that this operation will result in the loss of **all** settings entered during setup.

```
default(15)# setup
Begin system configuration ...
Country code configuration for this machine.
The country code is currently set to US
Would you like to change it [yes/no/quit]?
```

8. Note that this option will only appear for international controller models; US controllers automatically default to the US region and cannot be changed. If you are setting up the controller outside of the United States, answer **yes** or **y** to display a listing of supported country codes.

Note: Note the country code that represents your county (for example, **JP** for Japan, **IN** for India, **TW** for Taiwan, and so forth). At the following prompts, configure the code for your country.

```
Would you like to change it [yes/no/quit]? y
Please enter the new country code, or q to quit: JP
Host Name configuration for this machine
```

9. Type the hostname for the controller (the hostname must be less than 32 characters and cannot start with integers or contain all integers). In the following example, we choose the hostname **`controller`** for our controller:

```
Please enter host name, or q to quit: controller
Is controller correct [yes/no/quit]?: y
```

10. Change the default admin password to prevent any security breaches:

```
Currently default password is used for admin
Would you like to change the password [yes/no/quit]?: yes
Changing password for user admin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Note: If you enter **no** when asked about changing the password, the default password (**admin**) will be retained and you may proceed to Step 11. However, it is strongly recommended that users change to a more secure password for security purposes. Note that if a weak password is entered, the system will state that it is “bad”. If you wish to continue using the weak password, simply re-enter it and the system will proceed with setup.

11. Enable the guest user (if desired). If you enter **no** at this prompt, you may proceed directly to Step 13, below.

```
Currently guest user is disabled
Would you like to enable user guest [yes/no/quit]?: no
```

12. Change the default guest password to prevent any security breaches (if enabled in Step 11 above):

```
Currently default password is used for guest
Would you like to change the password [yes/no/quit]?: no
IP Configuration for this machine
```

Note: If you enter **no** when asked about changing the password, the default password (**admin**) will be retained and you may proceed to Step 13. However, it is strongly recommended that users change to a more secure password for security purposes.

13. Configure IP addressing for the controller.

At this stage, we will assign a static IP address and a netmask to the controller, as well as a gateway address, so a telnet or browser connection can be made. Use the addresses obtained from your administrator, as noted in “Before You Start” on page 2.

```
Would you like to configure networking? y
Would you like your controller to use Dynamic IP configuration
(DHCP)[yes/no/quit]: n

Please enter the IP configuration for this machine.
Each item should be entered as an IP version 4 style address in
dotted-decimal notation (for example, 10.20.30.40)

Enter IP address, or q to quit: nnn.nnn.nnn.nnn
Is nnn.nnn.nnn.nnn correct [yes/no/quite]? y

Enter netmask, or q to quit: nnn.nnn.nnn.nnn
Is nnn.nnn.nnn.nnn correct [yes/no/quit]? y

Enter default gateway (IP), or q to quit: nnn.nnn.nnn.nnn
Is nnn.nnn.nnn.nnn correct [yes/no/quit]? y
```

14. For the initial start-up, if your controller is to be on a different subnet from the APs (Layer 3 configuration), enter the appropriate DNS server information for your WLAN.

Note: **Note:** Be sure to update your DNS servers with the name for this controller (wlan-controller).

```
Would you like to configure a Domain Name Server [yes/no/quit]? y
Domain Name Server (DNS) configuration for this machine.
Enter one or more DNS name servers.
For this prompt only use q when finished entering name servers.

Enter Name Server IP Address, or q to quit: admin#nnn.nnn.nnn.nnn
```

15. If needed, you will also be prompted to enter your controller’s domain name.
16. If desired, you can specify your controller’s index number at this point. This can be helpful when multiple controllers are active on a single deployment.
17. You are now prompted to set the time zone. You can set it now or later, using the **timezone** command.

```
The time is now Wed Aug 17 12:27:13 UTC 2005
Would you like to change the time zone for this machine [yes/no/quit]?:
y
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) none - I want to specify the time zone using the Posix TZ format.
   #? 2
   Please select a country.
   1) Anguilla              18) Ecuador              35) Paraguay
   2) Antigua & Barbuda     19) El Salvador          36) Peru
   3) Argentina             20) French Guiana        37) Puerto Rico
   4) Aruba                 21) Greenland            38) St Kitts & Nevis
   5) Bahamas               22) Grenada              39) St Lucia
   6) Barbados              23) Guadeloupe           40) St Pierre &
   Miquelon
   7) Belize                24) Guatemala            41) St Vincent
   8) Bolivia               25) Guyana               42) Suriname
   9) Brazil                26) Haiti                43) Trinidad &
   Tobago
   10) Canada                27) Honduras             44) Turks & Caicos
   Is
   11) Cayman Islands        28) Jamaica              45) United States
   12) Chile                 29) Martinique           46) Uruguay
   13) Colombia              30) Mexico               47) Venezuela
   14) Costa Rica            31) Montserrat           48) Virgin Islands
   (UK)
   15) Cuba                  32) Netherlands Antilles 49) Virgin Islands
   (US)
   16) Dominica              33) Nicaragua
   17) Dominican Republic    34) Panama
   #? 45
   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 - Crawford County
 7) Eastern Time - Indiana - Starke County
 8) Eastern Time - Indiana - Switzerland County
 9) Central Time
10) Central Time - Indiana - Daviess, Dubois, Knox, Martin, Perry &
   Pulaski Counties
11) Central Time - Indiana - Pike County
12) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee
   Counties
13) Central Time - North Dakota - Oliver County
14) Central Time - North Dakota - Morton County (except Mandan area)
15) Mountain Time
16) Mountain Time - south Idaho & east Oregon
17) Mountain Time - Navajo
18) Mountain Standard Time - Arizona
19) Pacific Time
20) Alaska Time
21) Alaska Time - Alaska panhandle
22) Alaska Time - Alaska panhandle neck
```



```
23) Alaska Time - west Alaska
24) Aleutian Islands
25) Hawaii
#? 19

   The following information has been given:

          United States
          Pacific Time

   The name of the time zone is 'America/Los_Angeles'.
   Is the above information OK?
   1) Yes
   2) No
   #? 1
```

The following command is the alternative way of selecting the same time zone

```
     timezone set America/Los_Angeles
Set system time for this machine.
```

18. As well, you can synchronize the system time with a Network Time Protocol server so that the controller time is extremely accurate, or set the time from the CLI with the **calendar set** command.

```
Synchronize time with a Network Time Protocol (NTP) server
[yes/no/quit]?: n
You can use the "calendar set" option of the cli to set the time
```

Note: If you enter **yes** when asked about using a NTP server, you will be required to enter the server's DNS name or IP address.

19. The system asks for permission to reboot. Tell it to reboot, when prompted:

```
System Configuration completed.
Do you want to commit your changes and reboot? [yes/no/quit] yes
Broadcast message from root (Wed Aug 17 11:30:32 2005):
The system is going down for reboot NOW!
```

After approximately 5-10 minutes, the controller restarts.

20. If you have not yet connected your test station the Ethernet switch (used for setting up your test network) to the upstream network, connect it now.

21. Verify that you can connect to the controller using the Web UI or the CLI.

- To start the WebUI, open a browser window and provide the IP address of the Controller you have just configured (**http://***nnn.nnn.nnn.nnn*).
- To use the CLI, start a SSH2 session using the IP address of the controller.

22. Start the licensing process:

Each Controller requires a license in order to support an AP deployment. To permanently license the number of APs or Radio Switches that you have purchased, or to add optional features, you need a license key file from Meru for those items.

To request a license key file, follow these steps for each controller you are licensing:

a. Locate the License Certificate that was included in the Controller shipping carton (or sent via email) for the controller or feature you are licensing. The certificate identifies the feature or controller by orderable model number, serial number, and system ID. It also includes an Entitlement Identification Number that is used for licensing the item.

Note: If your controller did not include a License Certificate, or if you wish to obtain an evaluation License Certificate, contact your sales account manager or authorized reseller. They will process your order for a permanent license certificate or an evaluation license certificate, as desired.

b. Open an Internet browser and navigate to **http://support.merunetworks.com**.

c. Log into your Meru Support account using the **login** link (if you have not registered an account already, do so using the **Register** link).

d. From the support page, click **Activate your Licenses** and follow the instructions provided.

e. Access your controller's web UI and navigate to **Maintenance>Add License**.

f. Browse to your downloaded license file and click **Import License**.

23. Plug the access points into the layer 2 or layer 3 switch.

Access Points can obtain their power from a standard Power over Ethernet (PoE) device. The power can be supplied by a PoE-compatible network switch or PoE power injector installed between the switch and the AP. See the Access Point Installation Guide specific to your AP model in order to determine its ideal power specifications.

24. Verify that each access point receives power. If the access point is receiving power, the power LED glows green. Refer to the *Meru Access Point and Radio Switch Installation Guide* for a complete description of LED status codes.

Your network is now operating.

Configuration Via the WebUI Wizard

System Director versions 5.2 and later provide support for an easy-to-use "EzSetup Wizard" in the WebUI that walks you through all the configuration options typically performed using the **setup** script described earlier in this chapter. The EzSetup

Wizard is intended for new users setting up a relatively small deployment; while it can be used for installations of any scale, the idea is to get a simple WLAN up and running with a few APs connected. From there, users can extend the scope of the network as needed using the additional configuration features in the WebUI.

The following materials will be needed for setup:

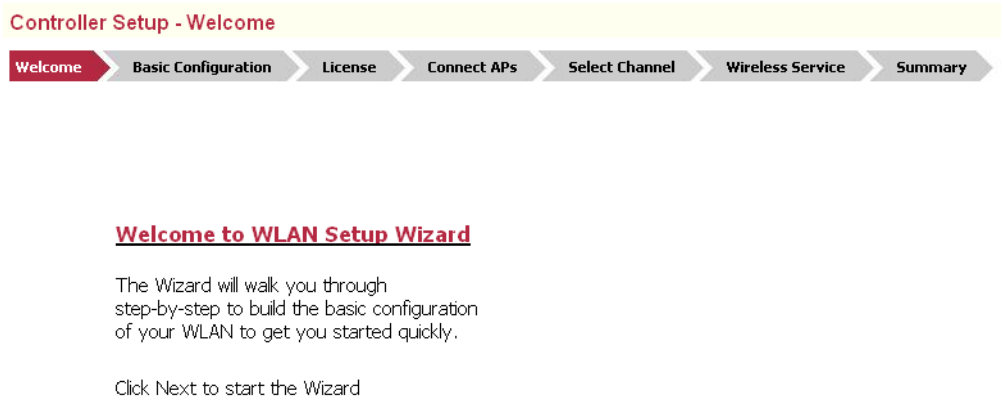
- Controller
- AP(s)
- Laptop (must be on the 192.168.1.x subnet)
- Ethernet Switch (and cables required to connect everything to it)

Accessing the Wizard Interface

The EzSetup page is automatically launched when the controller boots up. To access it, connect all the devices to the switch and power up the controller. Then, follow the steps below:

1. Open a web browser on the laptop.
2. Navigate to **https://192.168.1.12**. This is the default IP address assigned to the controller (you will be able to change it during the setup process). A welcome screen will appear introducing you to the setup wizard.

Figure 5: Welcome Screen



Note: If a "Page cannot be displayed" message appears, the controller may not have finished booting up. Try refreshing after a minute or two.

3. Click **Next** to begin the setup process. The Basic Configuration screen appears.
4. Enter the required information as described in the following table. Note that all fields in the Basic Configuration screen are required.

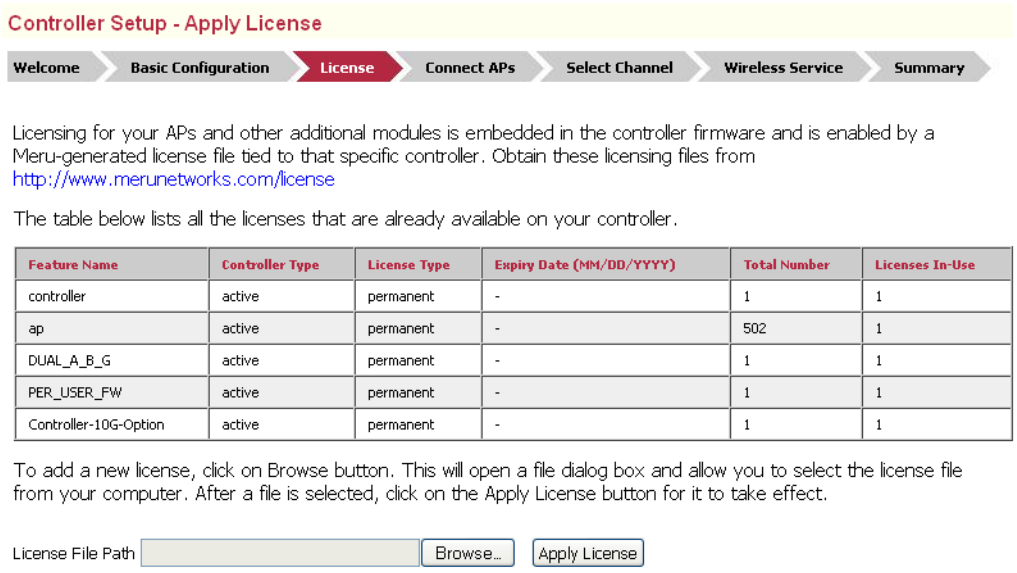
Table 1: Basic Configuration Options

Option	Description
Host Name	Enter the desired host name for your system.
Controller IP Method	Specify whether you wish to assign a static IP address to your system or have it obtain one automatically via DHCP.
Controller IP Address	*Note: This field only appears when the Controller IP Method is set to Static.* Enter the desired IP address for the controller.
Controller Subnet	*Note: This field only appears when the Controller IP Method is set to Static.* Enter the desired subnet for the controller. This is often in 255.255.255.0 format.
Controller Gateway	*Note: This field only appears when the Controller IP Method is set to Static.* Enter the desired gateway for the controller. This is often the first three fields of your controller's static IP address with the final field set to 1 (e.g., 192.168.14.1).
Country Code	Use this drop-down list to select the country in which your deployment resides. Note that this option is only available for international controller models.
Time Zone	Use this drop-down list to select the time zone in which the controller is active.
System Time	Specify whether the controller should use a Network Time Protocol (NTP) or use the time assigned manually.
Date/Time	If entering the time manually, click the **…** button to select today's date and time.
NTP Server Name/IP	If using an NTP server, enter its name or IP address.

5. Click **Next** to continue. This page will allow you to add any licenses you purchased with the controller (e.g., a license for the number of APs permitted). Follow the instructions provided on the screen to obtain your license files.
6. Once you have your licenses, click **Browse…** and browse to their location.

7. Click **Apply License** to upload the license file to the controller. Repeat for all license files needed. As each file is added, a license entry should display in the table on the screen.

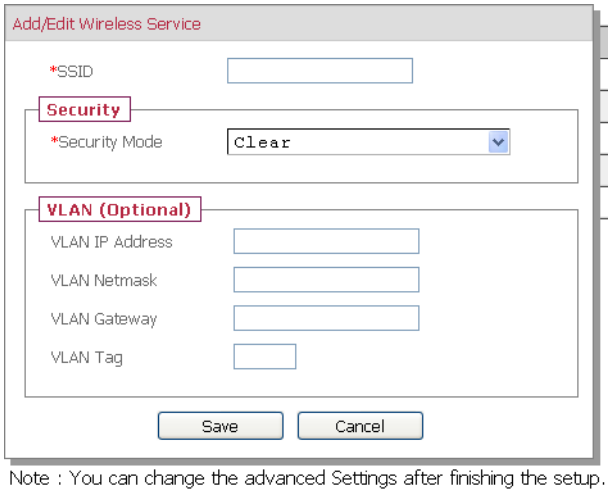
Figure 6: License Table



8. Once all the licenses have been added, click **Next** to proceed to AP detection.
9. If your APs are already connected via the switch (as instructed earlier in this section), they should automatically show up in the *Connected APs* table. Click **Next** to continue to channel selection.
10. The *Select Channel* screen allows you to specify the channel on which your APs will operate. Note that the available bands will vary depending on the licenses installed (i.e., an 802.11n license is required for some models of AP in order to utilize 802.11n frequencies).

    It is recommended that you click the **Start Scanning** button when first setting up a deployment; this option will allow the controller to scan the wireless environment and assess which channels would be ideal for your AP configuration.
11. Specify the band and channel options desired and click **Next**. This screen will allow you to create a basic wireless profile for the deployment.
12. Click **Add** to open the *Add/Edit Wireless Service* dialog.

Figure 7: Add/Edit Wireless Service



13. Enter the SSID desired for your wireless service. The SSID will be the name seen when you attempt to connect a wireless station to the network.
14. Use the **Security Mode** drop-down to select your security mechanism. Note that depending on the mode selected, you will need to enter additional information (i.e., if **Static WEP** is selected, you will need to enter a WEP Key used to connect to the network).
15. If desired, provide the VLAN configuration in the fields provided. This information is optional.
16. When all fields are configured correctly, click **Save** to save the profile. It will be displayed in the Wireless Service table.
17. Repeat steps 12-16 for additional wireless profiles, if desired. When finished, click **Next** to proceed.
18. The final screen provides a summary of your configuration options. If everything is configured correctly, click **Finish** to complete the wizard. The controller will reboot and apply the changes.

After the reboot has completed, your configured wireless network should be available. Use a wireless station to attempt to connect to it and verify that the configuration is complete.

Controller Configuration, Additional Settings

This section shows how to configure additional settings for the controller. It is of particular use when setup was performed via CLI; note that some of these configurations may already have been performed if you set up the controller with the EzSetup Wizard.

This section covers the following configurations:

- Controller identification and contact information
- DHCP addresses and settings
- Domain Name Server setting
- System time and NTP settings
- RADIUS server addresses and settings

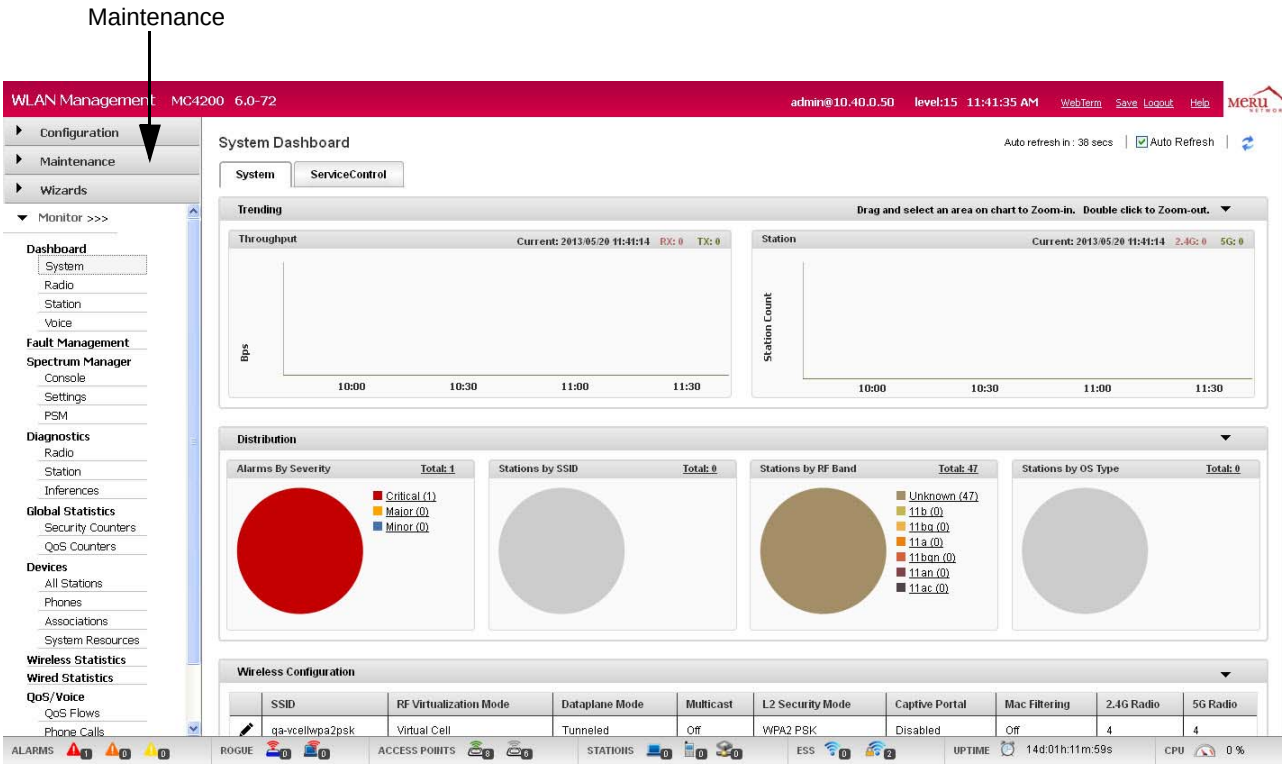
The easiest way to change these settings is through the WebUI, which will be the method described in the remainder of this chapter.

Choose a network architecture that supports how your APs are attached to your controller: the Controller and APs can be on the same subnet (Layer 2) or a different subnet (Layer 3).

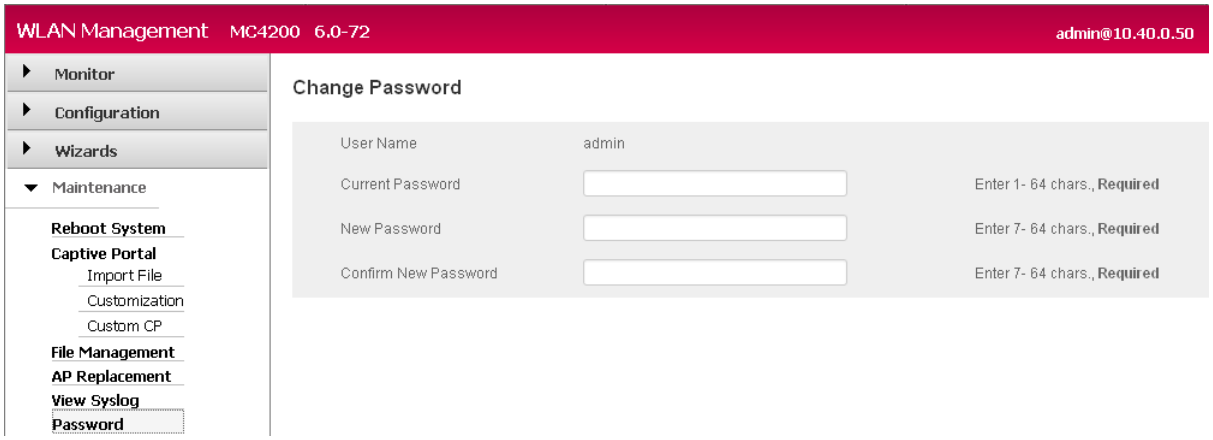
1. Be sure you have obtained the following network parameters from your network administrator:
   - IP numbers for the local domain name servers
   - Name of the local domain
   - Settings for the primary and secondary Radius servers
2. Open a web browser and connect to the controller, using the IP address you configured with the **setup** command (or example, **http://***nnn.nnn.nnn.nnn*).

   If any security or certificate warning windows display, click the Yes or Continue to web page to proceed (this step may vary depending on the web browser in use).
3. The Web Management Interface login dialog pop-up displays. Enter the username **admin** and your password (or the default password of **admin** if you did not change it during setup) to continue.

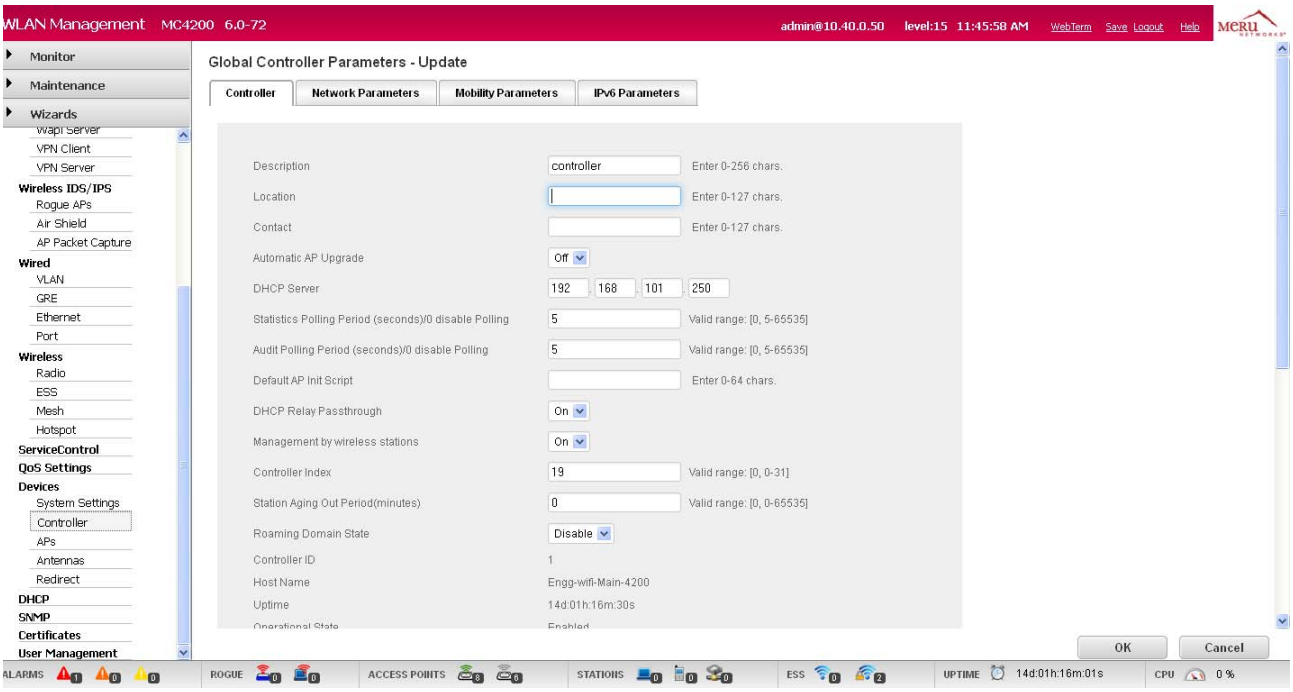
   The WLAN Management home page opens with the Monitor portion of the interface, displaying the Dashboard charts.



4. For security reasons, the default password should be changed. If you did not change it during the **setup** program, do so now. Click **Maintenance** and under the Password area, click **Change Password**.
   a. In the User Name text box, type in the user name **admin**.
   b. In the Current Password text box, type **admin**.
   c. In the New Password text box, enter a new password (from 1 to 256 characters).
   d. In the Re-type New Password text box, retype your password for validation.
   e. Click **OK** to save changes. You will be prompted to confirm the change.
   f. Click **OK** again to confirm the new password, at which point the Change Password screen is displayed again.
   g. Test the new password by clicking **Logout** in the top-right portion of the screen and log back in using the new credentials.



5. In the left panel, click **Configuration** and under the Devices heading, click **Controller** to open the Global Controller Parameters window.



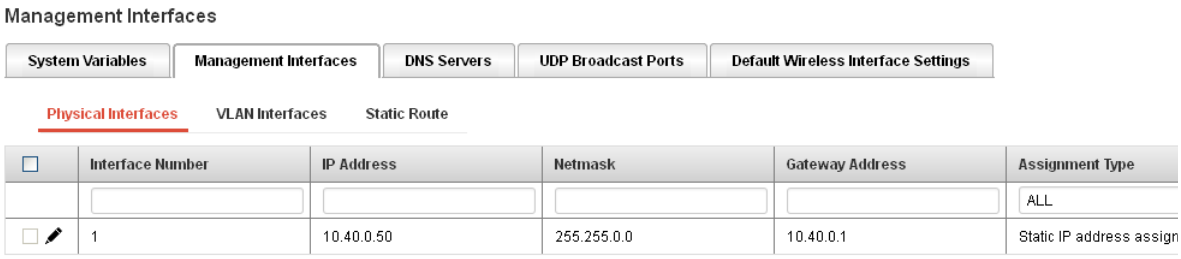
6. Add optional information for identifying the controller:
   - In the Description box, type a description for the controller. This is for your informational use only. The description can be up to 256 alphanumeric characters long.
   - In the Location box, type the location of the controller. This is for your informational use only. The location can be up to 127 alphanumeric characters long.
   - In the Contact box, type the name of the contact person or group for the controller. This is for your informational use only. The contact name can be up to 127 alphanumeric characters long.

— Click **OK** to save your changes.

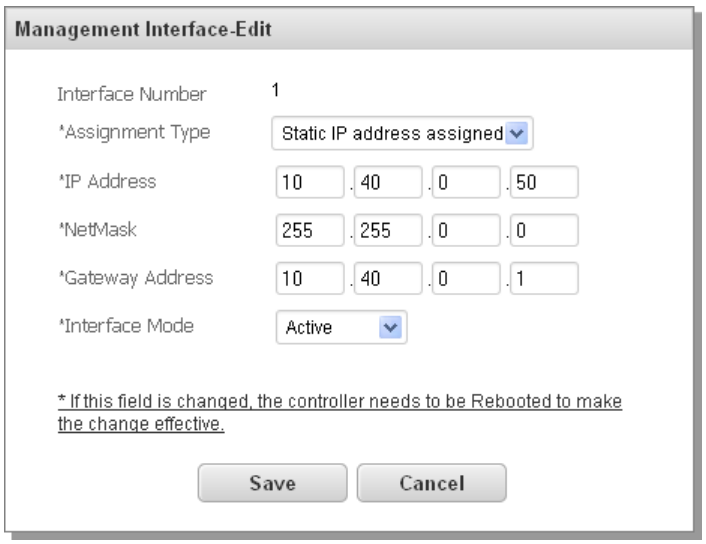
7. In the **setup** program, you gave the controller a static IP address so you could easily reach it. You can change that now if you wish. You can assign a different IP address or you can change the address to a dynamic IP address to be assigned by the DHCP server. If you do not wish to change the IP address, skip to the step to save the configuration (step 9).

   To change the IP address or configure a Dynamic IP address for the controller:

   a. Under the Devices heading on the left panel, click **System Settings>Management Interfaces tab** to open the IP Address table.



   b. Click the check box to activate the first Controller IP address listing and click the pencil next to the box (or **Settings** at the bottom of the window). The IP Addresses - Update window displays:



   — To change the static IP address, type a new address in the IP Address boxes, type in a Netmask and Gateway address to complete the configuration.

   — To change to dynamic IP addressing, click the Assignment Type drop-down list, select DHCP.

   c. Click **OK**.

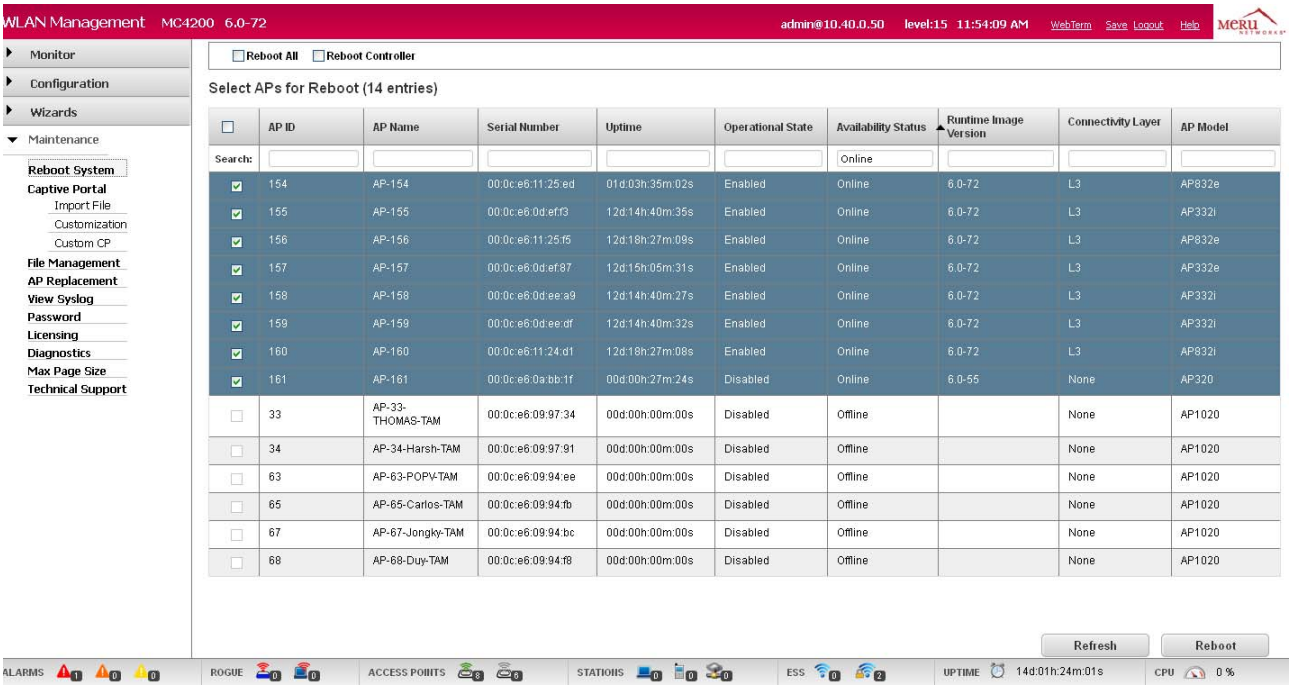
   d. Click the **Controller** link on the left panel to return to the Global Controller Parameters window.

8. If you have set the Assignment type to DHCP, change the address in the DHCP Server text boxes to a specific DHCP Server address. Note that this practice is not recommended, as it means that if the DHCP server is rendered inoperable, the entire wireless network could be disabled.

   By default, the DHCP server is set to 127.0.0.1, which allows successful passing of client DHCP requests as soon as the controller is plugged into the network. If the DHCP server is set to 255.255.255.255, broadcasts are sent on the System Director interface, rather than unicast requests being sent to a specific DHCP server.

9. Click **Save** on the top right corner of this window to save your changes. Click **OK** on the warning message that is displayed to confirm the change.

10. Click **Maintenance** in the left pane to open the Maintenance module.



11. Click the **Reboot Controller** checkbox at the top of the page and then click **Reboot** at the bottom of the window to reboot the controller.

Once the controller reboots, you can continue with the next section to configure a simple wireless network with basic settings for security and voice.

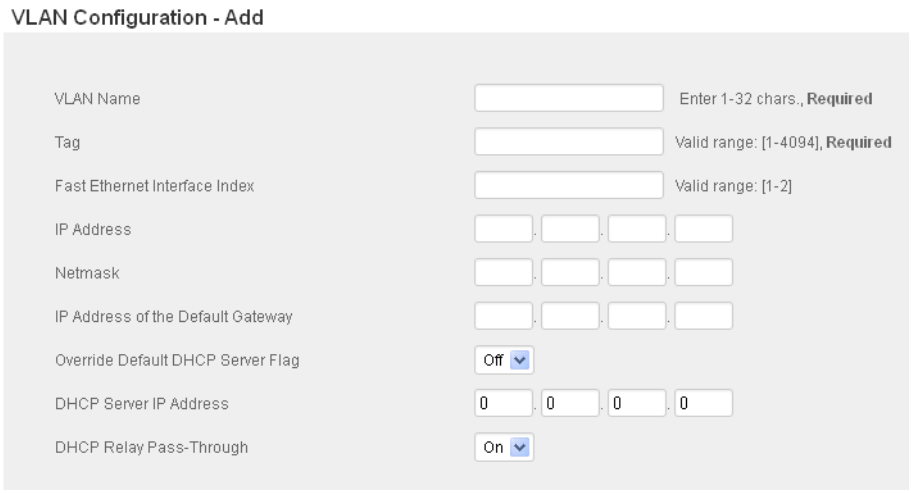
Create an ESS Profile with VLAN

By default, the factory-shipped settings do not include an ESS for client connection so you need to create one. To create the ESS connected to a port with a single VLAN, first configure a Security Profile and then create an ESS Profile that references the Security Profile. To do this, follow these steps:

1. If you have not already done so, open a browser and connect to the controller using the WebUI.
2. On the left side of the window, click **Configuration > Quick Start**.

Note: If you do not wish to create a VLAN for your network, you may proceed directly to Step 6 below.

3. Click the **VLAN** tab from the horizontal tab listing across the top of the page.
4. Click **Add** and fill in the required information for the new VLAN. See the example below.

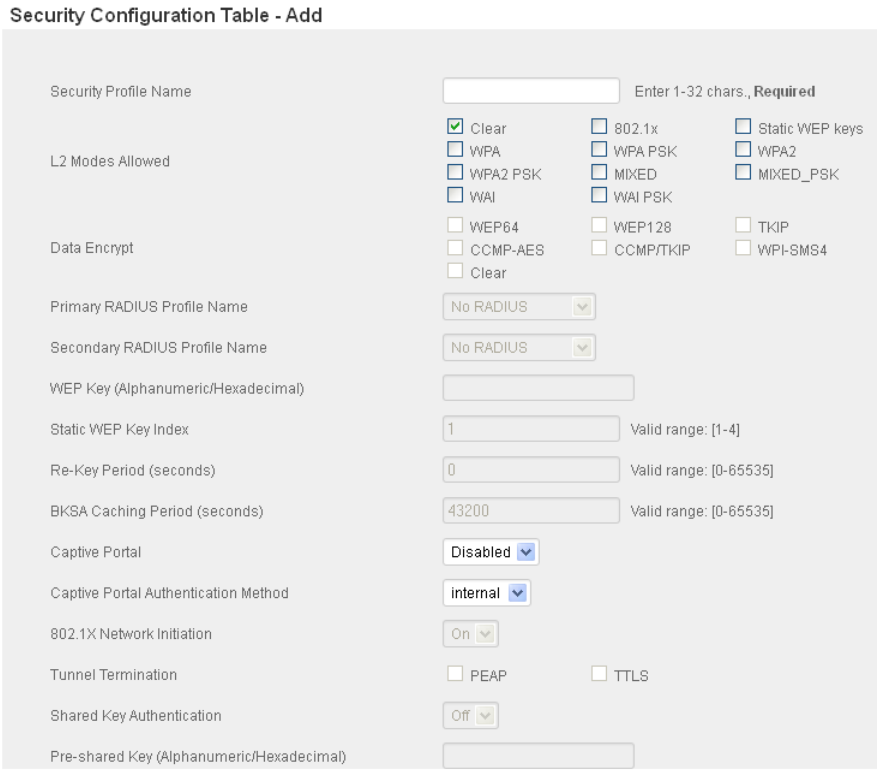


5. Click **OK** to save the VLAN and return to the Quick Start page.
6. Click the **Security Profile** tab to start configuring a Security Profile.
7. At the bottom of the Security Profile Table window that displays, click **Add**. The Security Profile - Add page displays. For this process, the default security profile may be used, but users are encouraged to go through the process of creating one just to get familiar with the steps.

Note:

Primary and Secondary RADIUS Profile Configuration

If your Security Profile is based on RADIUS Server User Authentication, you need to create at least a Primary RADIUS Profile before the profile will display in the drop-down list (proceed to the section "**Configuring RADIUS Profiles"** now and then continue with Security Profile configuration.)



8. Using the Security Profile Table - Add window, configure the settings for a new profile. **Table 2** summarizes the settings for some common security profiles, based on the L2 Mode that is selected. **Note** that optional settings are italicized.

Table 2: Security Profile Configuration Settings

L2 Mode	Encryption	RADIUS Server	Key Settings	Captive Portal
Clear (default profile) Click **Cancel** to exit				WebAuth
802.1X	WEP128 or WEP64	Primary Secondary (Configure using the Radius Profile tab)	*Rekey Period* *Key Rotation*	
WPA2/Mixed (WPA2-Enterprise)	CCMP-AES	Primary Secondary (Configure using the Radius Profile tab)		
WPA (WPA-Enterprise)	TKIP	Primary Secondary (Configure using the Radius Profile tab)	*Key Rotation*	
WPA2-PSK (WPA2-Personal)	COMP-AES		Pre-shared Key	
WPA-PSK/Mixed (WPA-Personal)	TKIP		Pre-shared Key	
Static WEP Keys	WEP128 or WEP64		WEP Key *Static WEP Key Index* *Shared Key Authentication*	

a. Enter a name for the security profile in the Security Profile Name text box.

b. In the L2 Modes Allowed area, select the type of security required for your ESS (use the setting from the table's L2 Mode). This determines what other options are active on the view.

c. Use the table to set the rest of the settings, based on the L2 mode you selected.

Static WEP Key Notes

— In the WEP Key text box, enter a key that is within the contraints of the WEP flavor you selected:

A **WEP64** key must be 10 hexadecimal digits (the hexadecimal string must be preceded with **0x**) or 5 printable alphanumeric characters. For example, **0x619B947A3D** is a valid hexadecimal value, and **wpass** is a valid alphanumeric string.

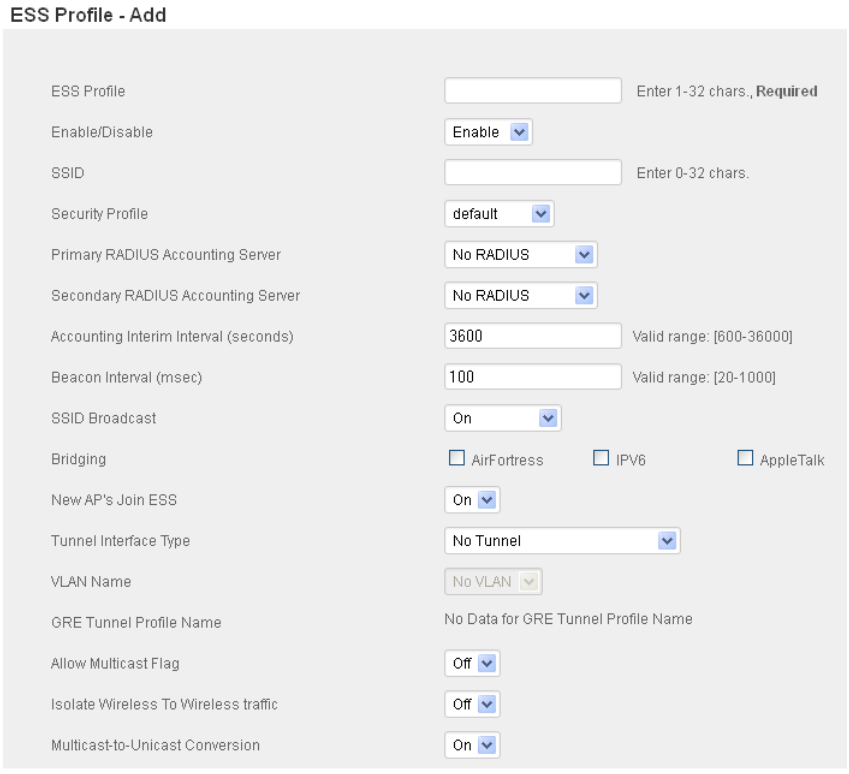
A **WEP128** key must 26 hexadecimal digits (the hexadecimal string must be preceded with **0x**) or 13 printable alphanumeric characters. For example, **0xB58CE2C2C75D73B298A36CDA6A** is a valid hexadecimal value, and **mypass8Word71** is a valid alphanumeric string.

WPA-PSK/WPA2-PSK Notes

In the Pre-shared Key box, enter a key. The key can be from 8 to 64 ASCII characters or 64 hex characters. Hex keys must be prefixed with **0x** or the key will not work.

d. Click **OK** when you have finished.
You are returned to the Security Profile Table, where your new profile entry displays.

9. Click the next tab in the tab row, **ESS Profile**, to configure the ESSID. The ESS Profile window displays. Click **Add** to open the The ESS Profile - Add window.



10. In the ESS Profile - Add window, configure the following settings:
    a. In the ESS Profile Name box, type the name of this profile, which can be the name of the extended service set ID, also known as an SSID, for the network.
    b. Add an SSID in the text entry box. The SSID is the name that will be broadcast on the wireless network, if broadcast is set to **On**. This field may also be left blank, in which case the ESS Profile Name will be used for the SSID.
    c. From the Security Profile Name drop-down list, select the name of the Security Profile you created in the previous step.
    d. In the Tunnel Interface Type list, select **Configured VLAN Only**.
    e. Select the VLAN you previously created from the VLAN Name list.
    f. Configure any other settings required by your ESS and then click **OK** when you have finished Your new ESS displays in the ESS Profile table.
11. To review your newly configured ESS information, click the checkbox next to your profile in the ESS Profile table, then click **View Details**.
    Your ESS Profile settings display in the ESS Profile - Details window. Click **OK** to exit. Click **OK** on the warning message that appears to confirm the changes.
12. Click **Save** at the upper right corner of the WLAN Management window to save your changes.

You have now configured an ESS for your wireless clients.

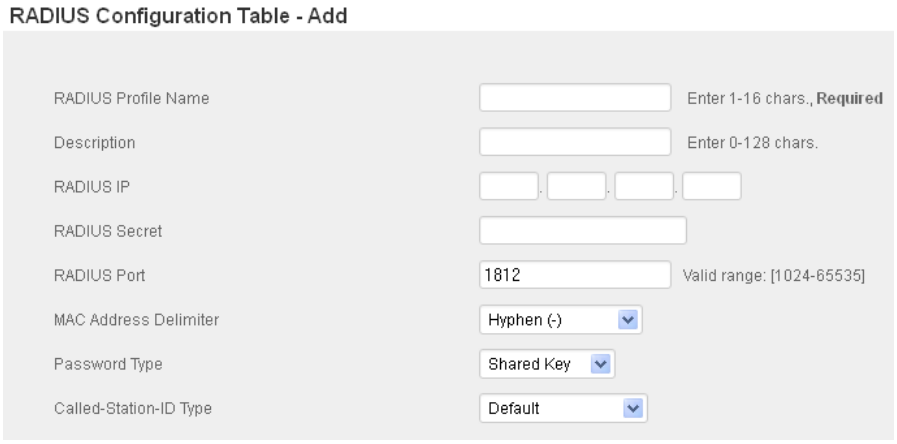
Some additional actions you may wish to perform at a later time:

- To remove an ESS, in the ESS Profile table, click the check box to the left of that profile, then click **Delete**.
- If you need to modify your settings, click the checkbox to the left of the profile and click **Settings** at the bottom of the screen. The ESS Profile - Update window displays.

Configuring RADIUS Profiles

To configure a Primary (or Secondary) RADIUS Server that can be selected from the Security Profile (RADIUS Authentication Server) or ESS Profile (RADUIS Accounting Server), follow these steps:

1. On the left side of the WebUI window, click **Configuration**.
2. Click the **Quick Start** link in the System Config area to open the System Config view.
3. Click the tab **RADIUS Profile** to open the RADIUS Profile Table view.
4. Click **Add**. The RADIUS Profile Table - Add page displays.

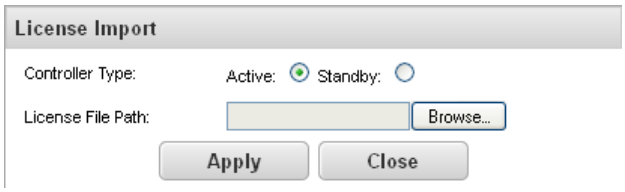


5. In the RADIUS Profile Name box, enter a name for the RADIUS Profile, using from 1 to 16 characters. This is a mandatory field. Note that spaces are not permitted in this field.
6. Enter an optional description of the profile in the Description field, using 1-128 characters.
7. In the RADIUS IP text boxes, add the IP address of the RADIUS server.
8. In the RADIUS Secret text box, add the shared secret that is configured for the RADIUS server. The key can be a maximum of 64 characters.
9. In the RADIUS Port text box, change the default port for authentication servers, 1812, to another port if the RADIUS server uses a non-default port or if the configuration is for a RADIUS Accounting Server, which uses port 1813 by default.
10. In the MAC Address Delimiter drop-down list, select the delimiter used on the RADIUS Server to separate MAC addresses.
    - **None**--No delimiter is used.
    - **Hyphen (-)**--A hyphen is used to delimit the fields (xx-yy-zz-aa-bb-cc)
    - **Single Hyphen (-)**--Only one hyphen is used to delimit fields (xxyyzz-aabbcc)
    - **Colon(:)** a colon is used to delimit fields (xx:yy:zz:aa:bb:cc)
11. In the Password Type drop-down list, select the type of password to be used for clients:
    - **Shared Key**--(RADIUS secret that is configured)
    - **MAC Address**--(client's MAC Address)
12. Click **OK** to complete the RADIUS server configuration and exit this window back to the RADIUS Profile Table. The RADIUS profile will now be available from the Security or ESS Profile page.

Completing Licensing

After you have obtained the License Key file from the email sent by Meru, use the following procedure to use the WebUI to complete the licensing of your purchased item. To obtain a license, use an Internet browser to navigate to **Meru's Support Portal**.

1. From the **Maintenance** menu, in the Licensing area, click the **Licensing** link. The Licensing window displays.
2. Click **Import** to display the License Import pop-up:



3. In Step 1, activate the radio button for the controller where the item is being licensed: **Active** or **Standby**.
4. In Step 2, type in the location of the license file that you received from Meru Licensing, or click **Browse** to locate the file.
5. Click **Apply** to import the license into the controller.

Viewing Licenses

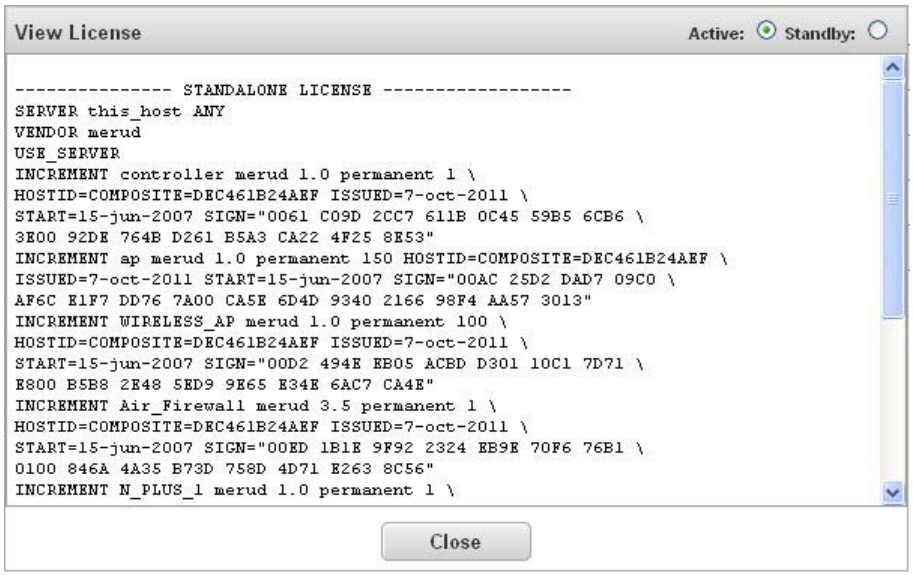
To see a listing of the controller, APs, and features that are permanently licensed, click the **Licensing** . The License Table window, similar to the following displays, showing the licensed hardware and optional software:

Licensing

The table below lists all the licenses that are already available on your controller.

Feature Name	Controller Type	License Type	Expiry Date (MM/DD/YYYY)	Total Number	Licenses In-Use
controller	active	permanent	-	1	1
ap	active	permanent	-	150	8
WIRELESS_AP	active	permanent	-	100	0
Air_Firewall	active	permanent	-	1	0
N_PLUS_1	active	permanent	-	1	0
PER_USER_FW	active	permanent	-	1	0
GRE_TUNNELS	active	permanent	-	1	0

To see the details of the imported licenses, click the **View** button at the bottom of the screen.



Powering Off the Controller

Should it become necessary to power off the controller, it is recommended you use the CLI command "**poweroff controller"** before switching the controller off with the Power On/Off switch. The command gracefully brings the controller down to a state where power can be removed using the power rocker switch. This process halts the system, and can take several minutes.

Caution! Failure to use the **poweroff controller** command before removing power from the controller can cause Flash card corruption and result in the controller becoming non-operational.

Where to Go from Here

You have successfully completed an initial WLAN configuration.

The remaining chapters in this guide present additional configuration tasks and show how to monitor the WLAN using the WebUI.

For complete configuration instructions, refer to the *Meru System Director Configuration Guide* and *Meru System Director Command Reference,* included in documentation set.

The documentation set includes:

- *Meru System Director Release Notes*
- *Meru Controller Install Guide*
- *Meru Access Point Install Guide*
- *Meru System Director Configuration Guide*
- *Meru System Director Command Reference*

Chapter 2
Monitoring Your Network

This chapter provides an introduction to monitoring and reviewing various aspects of your wireless LAN, including:

Testing Connectivity with ping

You can quickly test your network connectivity with the **ping** command. For example:

1. Ping the remote host with the IP address 10.12.101.1:

```
controller# ping 10.12.101.1
PING 10.12.101.1 (10.12.101.1) from 10.0.220.93 : 56(84) bytes of data.
64 bytes from 10.12.101.1: icmp_seq=1 ttl=255 time=0.958 ms
64 bytes from 10.12.101.1: icmp_seq=2 ttl=255 time=0.223 ms
64 bytes from 10.12.101.1: icmp_seq=3 ttl=255 time=2.17 ms
64 bytes from 10.12.101.1: icmp_seq=4 ttl=255 time=0.223 ms
64 bytes from 10.12.101.1: icmp_seq=5 ttl=255 time=0.229 ms
64 bytes from 10.12.101.1: icmp_seq=6 ttl=255 time=0.250 ms
```

2. Press **Ctrl-C** to stop the pinging. This displays a summary of the results:

```
--- 10.12.101.1 ping statistics ---
6 packets transmitted, 6 received, 0% loss, time 5023ms
rtt min/avg/max/mdev = 0.223/0.675/2.170/0.719 ms
```

Viewing Routing Information

You can view the IP addresses and status for all routers between the controller and a specified remote destination with the **traceroute** command. For example, to view this information for the route to a destination whose hostname is `OurServer`, type

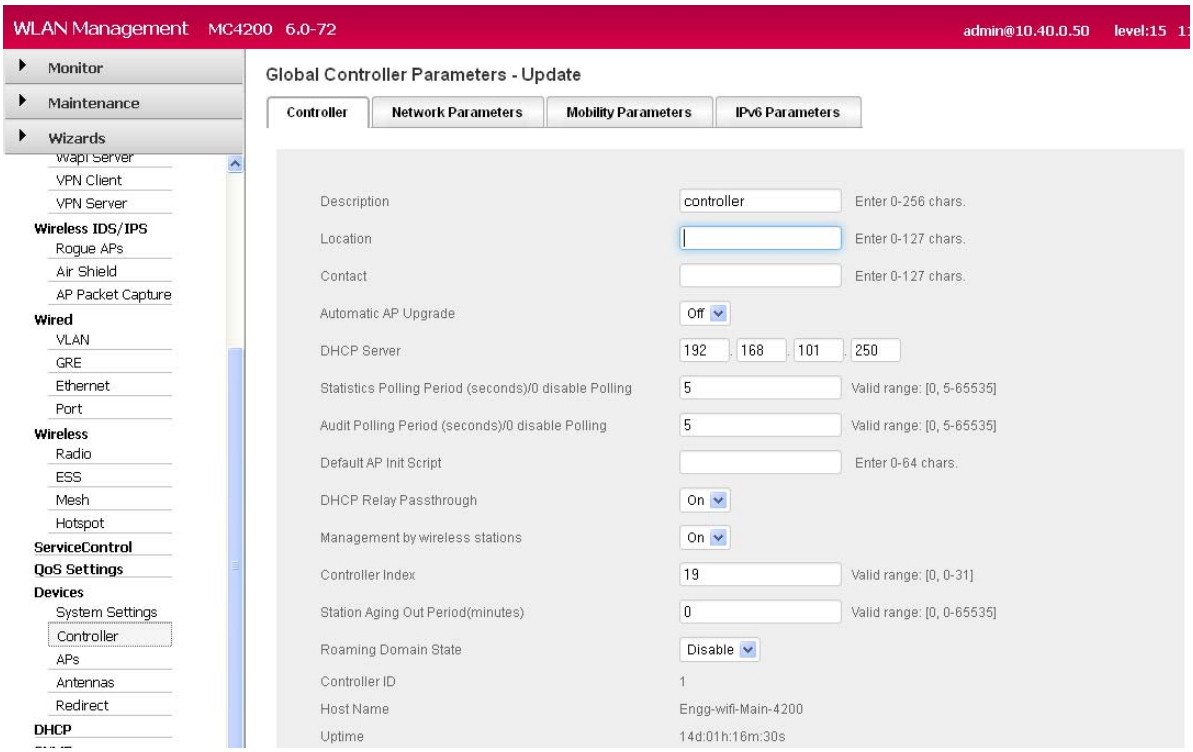
```
controller# traceroute OurServer

traceroute to OurServer (10.0.12.1), 30 hops max, 38 byte packets
 1  mc1000 (10.19.1.1)  2997.354 ms !H  2999.525 ms !H  2999.944 ms !
```

Instead of a hostname, you can alternatively specify an IP address or a hostname with a domain name.

Viewing Controller Information

To obtain detailed Controller information:

- To check controller information on the Web UI, click **Configuration** and then click the **Controller** link under the Devices heading.



- To check controller information with the CLI, use the **show controller** command. You can see detailed configuration information and status information.

Viewing Access Point Information

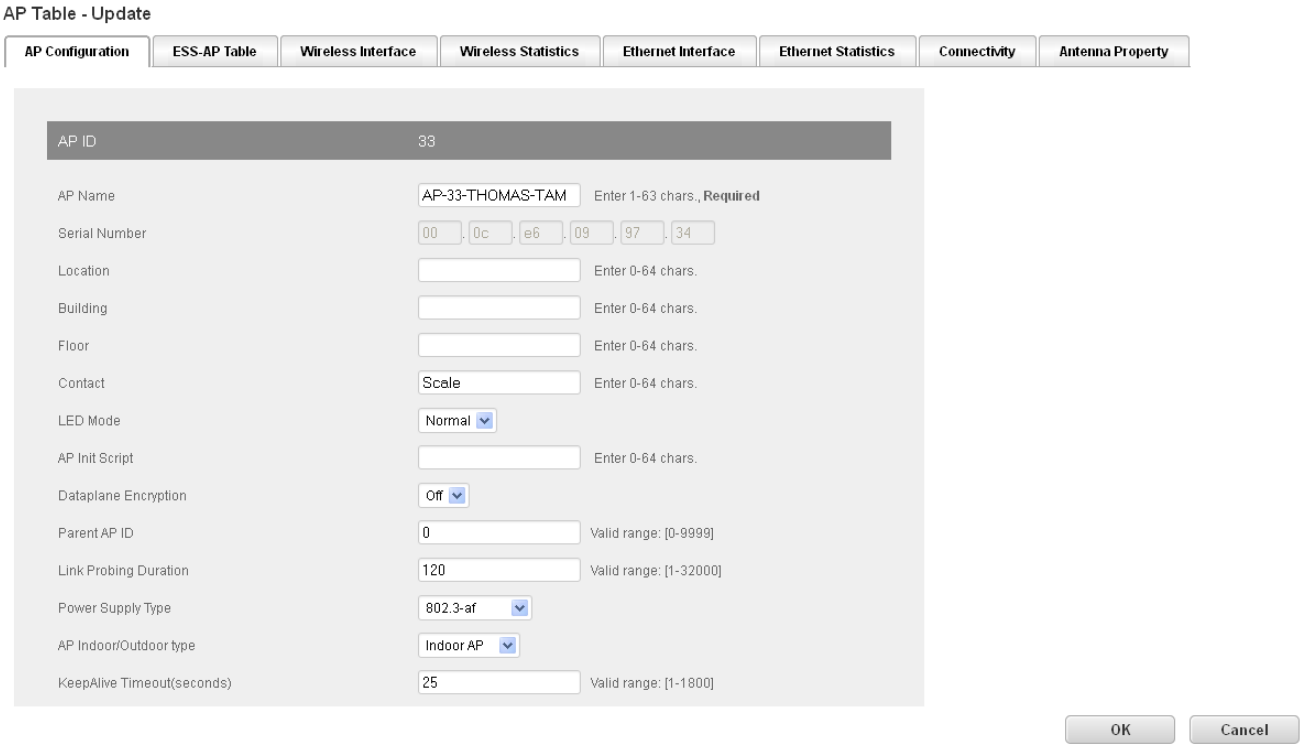
A wealth of access point configuration, monitoring, and statistic information is available in the Web UI.

To check configuration information for all APs, click **Configuration** in the left navigation pane, then click **APs** under the Devices heading.

AP Table (14 entries)

	AP ID	AP Name	Serial Number	Uptime	Operational State	Availability Status	Runtime Image Version	Connectivity
Search:								
	33	AP-33-THOMAS-TAM	00:0c:e6:09:97:34	00d:00h:00m:00s	Disabled	Offline		None
	34	AP-34-Harsh-TAM	00:0c:e6:09:97:91	00d:00h:00m:00s	Disabled	Offline		None
	63	AP-63-POPV-TAM	00:0c:e6:09:94:ee	00d:00h:00m:00s	Disabled	Offline		None
	65	AP-65-Carlos-TAM	00:0c:e6:09:94:fb	00d:00h:00m:00s	Disabled	Offline		None
	67	AP-67-Jongky-TAM	00:0c:e6:09:94:bc	00d:00h:00m:00s	Disabled	Offline		None
	68	AP-68-Duy-TAM	00:0c:e6:09:94:f8	00d:00h:00m:00s	Disabled	Offline		None
	154	AP-154	00:0c:e6:11:25:ed	01d:03h:48m:26s	Enabled	Online	6.0-72	L3
	155	AP-155	00:0c:e6:0d:ef:f3	12d:14h:53m:59s	Enabled	Online	6.0-72	L3

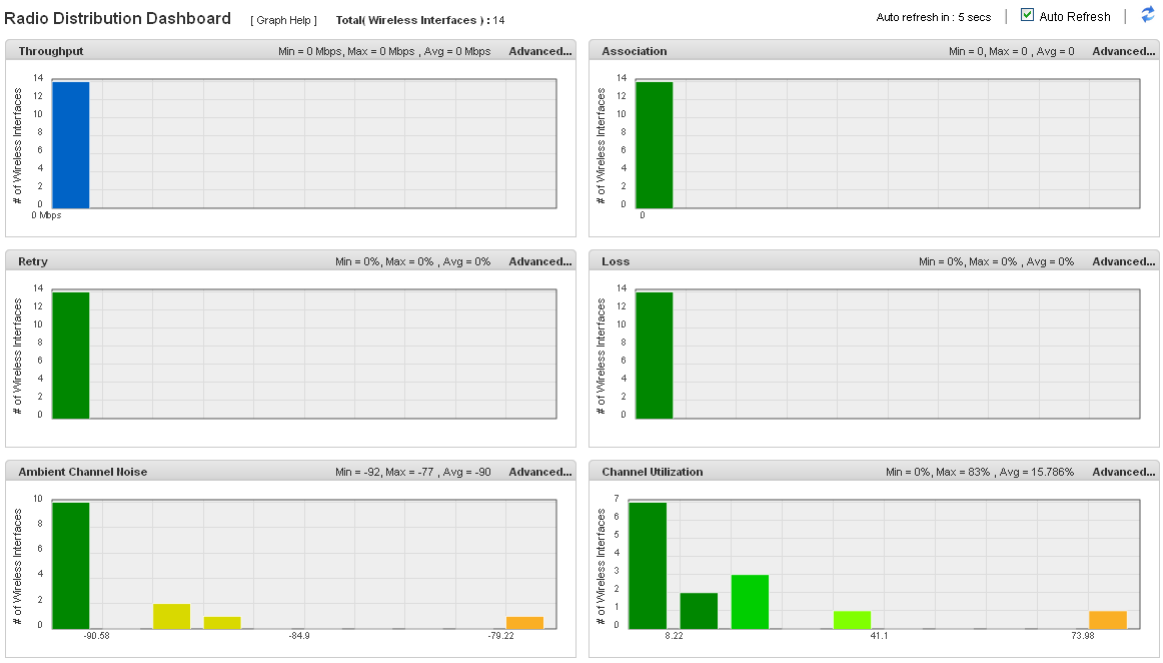
To drill down and obtain detailed interface information, wireless statistics, and other helpful information, click a checkbox to the left of the AP ID and click **Settings** . The AP Table - Update window displays. Notice the tabs across the top of the window that provide additional details for ESS-AP configuration, Wireless interfaces, Wireless statistics, Ethernet Interfaces, Ethernet Statistics, Connectivity, and Antenna Properties.



Monitoring APs

The opening page of the Web UI, the Dashboard, presents an overview of WLAN, AP and station activity. To revisit the opening page, click **Monitor** and the **System** link under the Dashboard heading.

The Dashboard presents the WLAN throughput and Station activity for the last 12 hours on a moving historical graph (the display ages every hour, with the new activity appearing on the right side of the chart).



The **Dashboard>Radio** charts provide a more comprehensive look at wireless activity over time including the following categories:

- Traffic throughput
- Association statistics
- Cumulative packet loss
- Retry information
- Channel noise
- Channel utilization
- Management traffic overhead

Viewing Mobile Station Information

The Meru Wireless LAN System automatically recognizes mobile stations that come within the service range.

To see station information, click **Monitor** and then the **All Stations** link under the Devices heading. The Station Table displays, showing all associated stations with MAC address, IP address type, the AP the station is associated with, L2/L3 state, authenticated user name, and VLAN tag info.

To drill down and obtain detailed information, statistics, and other helpful information, click a checkbox to the left of station's MAC address and click either the red arrow icon or **View Details**. This opens a page that displays advanced details about the selected station, including its MAC address, associated AP, security status, etc.

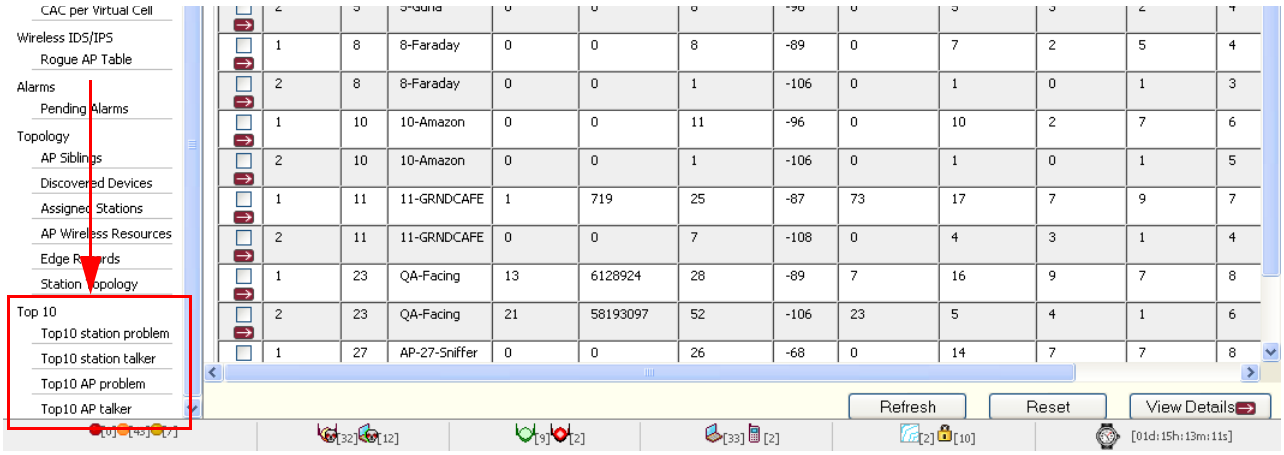
WLAN Monitoring

A wealth of WLAN statistics is accessed by clicking **Monitor**. The left navigation panel lists the different monitoring statistics that are gathered for the WLAN.

The monitored statistics include:

- **Dashboard**—A quick glance at pertinent statistics in a variety of categories.
- **Diagnostics**—Data that allows you to assess and monitor problems in the wireless network.
- **Global Statistics**—Includes Security counters and QoS counters.
- **Devices**—All Stations, Phones that are connected, and Associated stations per AP statistics
- **Wireless Radios—**802.11 statistics
- **Wired Ethernet—**Ethernet statistics
- **QoS/Voice**—QoS Flows, Phone Calls, CAC per AP and Virtual Cell
- **Wireless IDS/IPS**—Mechanisms for monitoring and eliminating rogue devices.
- **Alarms**—Pending Alarms

Clicking the **>>>** link at the top of the Monitor pane exposes Topology statistics and Top 10 categories (ten APs or stations with the most activity or problems). These options appear at the bottom of the left-hand pane (below **Pending Alarms**).


CAC per Virtual Cell
Wireless IDS/IPS
Rogue AP Table
Alarms
Pending Alarms
Topology
AP Siblings
Discovered Devices
Assigned Stations
AP Wireless Resources
Edge Rogues
Station Topology
Top 10
Top10 station problem
Top10 station talker
Top10 AP problem
Top10 AP talker
1 8 8-Faraday 0 0 8 -89 0 7 2 5 4
2 8 8-Faraday 0 0 1 -106 0 1 0 1 3
1 10 10-Amazon 0 0 11 -96 0 10 2 7 6
2 10 10-Amazon 0 0 1 -106 0 1 0 1 5
1 11 11-GRNDCAFE 1 719 25 -87 73 17 7 9 7
2 11 11-GRNDCAFE 0 0 7 -108 0 4 3 1 4
1 23 QA-Facing 13 6128924 28 -89 7 16 9 7 8
2 23 QA-Facing 21 58193097 52 -106 23 5 4 1 6
1 27 AP-27-Sniffer 0 0 26 -68 0 14 7 7 8
Refresh
Reset
View Details
[01d:15h:13m:11s]

Meru Networks, Inc.
894 Ross Drive
Sunnyvale, CA 94087
408-215-5300
www.merunetworks.com