wavelink®

MOBILE MANAGER™

Version 1.5 Users Guide

Enterprise Edition

Revised 11/8/02

Wavelink Corporation

11332 NE 122nd Way
Suite 300
Kirkland, Washington 98034
Telephone: (425) 823-0111
Web site: www.wavelink.com

E-mail: info@wavelink.com

The software is provided strictly on an “as is” basis. All software, including firmware, furnished to the user is on a licensed basis. Wavelink Corporation grants to the user a non-transferable and non-exclusive license to use each software or firmware program delivered hereunder (licensed program). Except as noted below, such license may not be assigned, sublicensed, or otherwise transferred by the user without prior written consent of Wavelink Corporation. No right to copy a licensed program in whole or in part is granted, except as permitted under copyright law. The user shall not modify, merge, or incorporate any form or portion of a licensed program with other program material, create a derivative work from a licensed program, or use a licensed program in a network without written permission from Wavelink Corporation. The user agrees to maintain Wavelink Corporation’s copyright notice on the licensed programs delivered hereunder, and to include the same on any authorized copies it makes, in whole or in part. The user agrees not to decompile, disassemble, decode, or reverse engineer any licensed program delivered to the user or any portion thereof.

Wavelink Corporation reserves the right to make changes to any software or product to improve reliability, function, or design.

Wavelink Corporation does not assume any product liability arising out of, or in connection with, the application or use of any product, circuit, or application described herein.

Symbol™, Spectrum One™, and Spectrum24™ are registered trademarks of Symbol Technologies, Inc. Wavelink™, Wavelink Symbol Client™ are registered trademarks of Wavelink Corporation. Cisco-Aironet™ is a registered trademark of Cisco Systems. Intel™ is a registered trademark of Intel Corporation. Ericsson™ is a registered trademark of Ericsson. 3COM™ is a registered trademark of 3COM Corporation. Nortel™ is a registered trademark of Nortel Networks Limited. Unicenter™ is a registered trademark of Computer Associates.

Table of Contents

Chapter 1: Introduction

This user documentation is a complete guide to the functions and components of the Wavelink Mobile Manager Enterprise Edition. This document presents:

- An introduction to the Enterprise Administrator of the Mobile Manager and conceptual information about the Mobile Manager's structure
- Detailed information on the components of the Mobile Manager Enterprise Edition
- Techniques and recommendations for creating a secure wireless network environment

This introduction defines the assumptions and conventions of this document, and provides an overview of the Mobile Manager Enterprise Edition product.

About This Document

This user documentation provides assistance to anyone who manages an enterprise-wide wireless network with the Mobile Manager product.

Document Assumptions

This document makes the following assumptions:

- You have a general understanding of the basic operational characteristics of your network operating systems.
- You have a general understanding of basic hardware configuration, such as how to install a network adapter.
- You have a working knowledge about operating your wireless networking hardware, such as Access Points and mobile devices. (See the appropriate documentation included with your wireless hardware for more information.)
- You have administrative access to your network.

Document Conventions

This document uses the following typographical conventions:

Courier New

Any time you interact with an option, such as a button, or type specific information into a text box, such as a file name, that option appears in the `Courier New` text style. This text style is also used for any keyboard commands that you might need to press.

Examples:

Click `Next` to continue.

Press `CTRL+ALT+DELETE`.

Bold

Any time this document refers to an option, such as descriptions of different options in a dialog box, that option appears in the **Bold** text style.

Examples:

Click `Open` from the **File** Menu.

The **Auto-Add** button automatically adds IP addresses to your IP address pool.

Italics

Any time this document refers to another section within the document, that section appears in the *Italic* text style. This style is also used to refer to the titles of dialog boxes.

Example:

See the *Installation* section for more information.

The *Access Point Profiles* dialog box.

About the Mobile Manager

The Mobile Manager is the premier remote deployment, management, and security tool for enterprise-wide wireless networks. With the Mobile

Manager, you can automatically install, discover, and manage your wireless network.

Key features of the Mobile Manager include:

- Comprehensive device management
- Enterprise-wide wireless network management
- Security and Access Control
- Multiple vendor support
- Agent-based administration
- Profile-based configuration
- Automatic IP assignment
- Automatic software maintenance
- Automatic alert notification
- Site administration

The following sections discuss these features in more detail.

Comprehensive Device Management

With the Mobile Manager, you have single solution that provides you with full management capabilities of both the Access Points and mobile devices on your network. Network maintenance tasks such as device configurations, software updates, and alert resolutions are accomplished using a single management console—the Enterprise Administrator. This comprehensive solution employs two software components—called Agents—that can either be deployed on multiple systems throughout your network, or on a single, centrally-accessible server.

Enterprise-wide Wireless Network Management

The Mobile Manager puts your entire wireless network at your fingertips. With the Mobile Manager, you can manage wireless network components regardless of your location. You can also monitor wireless network performance, allowing you to see which sites are operating at peak efficiency and which ones require attention. In addition, the Mobile Manager allows you to seamlessly move between a global perspective of your network to specific Access Points located at a site.

Security and Access Control

With the Mobile Manager, you can apply robust security and access control features that can prevent unauthorized devices from interfering with the wireless network. These features include the Very Large Access Control List, which uses a list of approved MAC addresses to allow mobile device access to the network, and automatic WEP rotation, an extremely secure way of encrypting wireless transmissions.

Multiple Vendor Support

Unlike other wireless network management tools, the Mobile Manager supports a variety of Access Point manufacturers. This support offers you the flexibility to deploy and integrate Access Points regardless of their hardware type.

Currently, the Mobile Manager supports the following Access Point manufacturers:

- 3COM
- Cisco-Aironet
- Ericsson
- Intel
- Nortel
- Symbol

One of the main advantages to the Mobile Manager is that it provides a common interface for Access Point configuration. For example, you configure a Cisco-Aironet Access Point using the same methods used to configure a Symbol Access Point.

NOTE While the Mobile Manager provides a common interface for Access Point configuration, it is important to note that different Access Point properties and statistics exist for different Access Point types.

If you deploy a wireless network using multiple Access Point types, it is important to remember the following:

- 3COM, Ericsson, Intel, Nortel, and Symbol Access Points share a common set of configuration properties. Cisco-Aironet Access Points have a unique set of properties that are not shared with these manufacturers.
- The Mobile Manager captures specific statistics for Cisco-Aironet Access Points. These statistics are different from the ones captured for 3COM, Ericsson, Intel, Nortel, and Symbol Access Points.

See *Configuring Enterprise Profiles* on page 112 for more information about the different properties and statistics associated with Access Point manufacturers.

Agent-based Administration

At the core of the Mobile Manager is the Agent. An Agent is a server-based application that actively monitors for Access Point broadcasts. Agents can be either be deployed on multiple locations throughout your network, or on a single, centrally-accessible server. The Mobile Manager uses Agents to implement its unique AutoDiscovery technology. AutoDiscovery recognizes new Access Points automatically and creates a direct administrative interface to each Access Point on your network.

You manage Agents on an enterprise level with the Enterprise Administrator. The Enterprise Administrator is an application that connects with multiple Agents located across your network. When active, the Enterprise Administrator connects to the Enterprise Manager component. This component is responsible for managing your remote Agents through an automatic and scheduled deployment of Access Point profiles. The Enterprise Manager also monitors the network through traps sent to the Fault Manager component—the component responsible for managing wireless network alerts.

Profile-based Configuration

One of the most beneficial features of the Mobile Manager is its profile-based configuration. Profile-based configuration means you can create templates of configuration settings and then assign these templates to specific Access Points. As a result, you can update or modify multiple Access Point configurations simultaneously, instead of changing each one manually.

Once an Access Point is assigned to a profile, that Access Point retains its configuration values until you alter it directly with the Mobile Manager. Even if you alter an Access Point's configuration values without the Mobile Manager—for example, by using a serial connection or a Telnet session—the Agent, when it next queries the Access Point, automatically restores the Access Point to the configuration values you established in the Access Point's assigned profile.

In the Mobile Manager Enterprise Edition, profiles are assigned to groups within your network infrastructure. Each group is a user-defined collection of sites—logical locations within your network where one or more Agents reside. You can create one profile for each Access Point hardware type deployed within each group.

NOTE Once you create a profile for a specific type of Access Point within a group, that profile is applied to every Access Point of that type, unless it already belongs to another profile.

Profiles help you improve wireless network security. For example, when you create a profile, you can create an Access Control List that contains only specific mobile devices. Access Points with this profile prevent unauthorized mobile devices from accessing the wireless network. You can also improve wireless network security by creating profiles for Access Point hardware that you do not use within your network. In this scenario, you create a profile for the Access Point type that enables the Access Control option for that profile, but leaves the actual Access Control List blank. Any mobile device that attempts to communicate with an Access Point with this profile is denied access to the network, because the MAC address for the mobile device cannot be found within the Access Point's Access Control List. This security feature helps to prevent rogue Access Points from communicating with the rest of your network.

Automatic IP Assignment

Another advantage to the Mobile Manager is automatic IP assignment. With the Enterprise Administrator, you can create a pool of IP addresses that Access Points can use. These IP addresses are created using the subnet mask of your network. When an Agent on a particular network site receives these IP addresses, it replaces the subnet mask with the subnet octets for its specific network segment.

Automatic Software Maintenance

With the Mobile Manager, you have the option of employing automatic software maintenance for the mobile devices that access your network. Tasks such as software updating are accomplished “over-the-air” and can be customized to target specific groups of mobile devices. These updates can also occur simultaneously, allowing you to send an application to multiple mobile devices at once.

Alert Profiles

The Mobile Manager helps you stay informed of wireless network problems with alert profiles. With alert profiles, the Mobile Manager sends you an e-mail whenever a wireless alert event occurs on your network.

The Mobile Manager divides alerts into two categories. The first category consists of SNMP events, such as when the Mobile Manager discovers a new Access Point on the network. The second category of alerts consists of exceeded statistical thresholds. These alerts are site-specific and occur whenever the value for an Access Point’s statistic falls outside an allowed minimum or maximum range.

Site Administration

The Mobile Manager Enterprise Edition provides you with the ability to manage your wireless network at a local, or site level.

To help you manage wireless components at a site, the Mobile Manager Enterprise Edition includes the site editions of the Mobile Manager and Avalanche. The site edition of Mobile Manager allows you to configure and maintain Access Points. The site edition of Avalanche allows you to manage the software deployed to your mobile devices.

See the *Mobile Manager Users Guide* and the *Avalanche Users Guide* for more information on how to manage your wireless network at a site level.

Additional Mobile Manager Features

Other features in the Mobile Manager include:

- Detailed access to wireless network statistics
- Online, comprehensive status reports for each site
- Enhanced logging filters
- Full remote administration of the entire wireless network
- Easy-to-use graphical user interface
- Remote updates of Access Point firmware

Components of Mobile Manager

The Mobile Manager consists of the following components:

Agents

Agents manage the wireless network. The Mobile Manager contains two Agents. The Mobile Manager Agent remotely configures and manages Access Points. The Avalanche Agent manages software updates to mobile devices.

Enterprise Administrator

The Enterprise Administrator allows you to control wireless network configuration on an enterprise-wide level. With the Enterprise Administrator, you can organize wireless network layout and implement Access Point profiles for different sites within your organization.

Enterprise Manager

The Enterprise Manager is a service component that allows the Enterprise Administrator to communicate with Agents across your network. Typically, this component is run as a service on your host system; however, you can also run it manually from the **Start** menu.

Fault Manager
The Fault Manager is similar to the Enterprise Administrator, but controls the communication of network events (such as network alerts) between Agents and the Enterprise Administrator.

License Server
The License Server is responsible for distributing licenses to any sites that you add to your network.

Uninstall
The Uninstall components allows you to uninstall the components of the Mobile Manager Enterprise Edition.

About Wavelink Avalanche

The Mobile Manager also allows you to incorporate features available from Wavelink Avalanche. Wavelink Avalanche is a mobile device configuration solution that provides remote, over-the-air software synchronization.

NOTE The Mobile Manager Enterprise Edition allows for flexible implementation of its features. Consequently, using the features of Wavelink Avalanche is completely optional.

Avalanche uses "push/pull" technology to install, update, and manage the software and configurations of wireless and other mobile devices. The Wavelink Avalanche system includes three primary components:

Avalanche Agent
The Avalanche Agent performs the actual management functions on the LAN or WAN, such as deploying software updates to mobile devices.

Avalanche Enabler
A software component that runs on each mobile device to allow management by the Enterprise Administrator.

Avalanche-enabled software packages
These packages include software such as Wavelink Telnet, Wavelink Studio Client software, and third party applications.

Avalanche Agent

The Avalanche Agent runs on any computer attached, either directly or through IP routing, to the networks where mobile devices reside. The Agent's network presence is not required for continued mobile device operation. When present, the Agent can reside anywhere on the LAN with the Access Points or across a WAN if connected by routers. As a result, you can perform upgrades from a corporate office rather than traveling to each branch location if the sites are connected to the network with the IP protocol.

Mobile devices attempt to connect to the Agent each time the Avalanche Enabler is activated (typically on reboot). When a mobile device connects to the Agent, either across the network or through a serial connection, the Agent determines whether an update is available and immediately starts the software upgrade. Once the new software is enabled and the Enabler activates on the mobile device, no additional user intervention is required to start the software update.

To determine appropriate software for each specific mobile device, the Avalanche Agent relies on a structure based on the following logical components:

- **Software Packages**. Software packages represent a collection of application files associated with a single product such as the Wavelink TN Clients or third party Avalanche-enabled software packages. All files in the package download automatically to the mobile device.

- **Software Collections**. Software collections contain one or more software packages. You can configure each software collection so that the packages it contains apply only to certain mobile devices.

Software Packages

An Avalanche software package is the collection of files that reside on the remote device for a particular application. This includes any support utilities used to configure or manage the application from the Enterprise Administrator. After the initial loading of a software package into the Enterprise Administrator, the Avalanche Agent handles all further package maintenance.

NOTE Software packages under Avalanche are not hex images and do not require re-burning a device's NVM image as with older software.

NOTE For Symbol devices, the "LWP" hex image, used for device support, is not required nor used. Instead, the system drivers (which LWP supplied to legacy systems) are provided by the Avalanche Enabler and can be updated over a wireless connection, as needed, using an Enabler Update kit.

NOTE It is recommended that LWP be removed from the flash drive. You can resolve this issue either by flashing the mobile device or, for Symbol 3000 devices, by using the 1.59-02 or newer version of the Enabler.

Avalanche software packages have a number of features which make them powerful and easy to use, such as:

- **Target Selection Criteria**. This feature limits distribution of the package to specific mobile devices. The selection criteria can encompass many device characteristics, including mobile device models, physical characteristics, IP and/or MAC addresses, etc. You can use operators to apply your own restrictions in addition to these, but you will not be able to circumvent any restrictions placed in the package definition itself.

- **Wireless download**. Packages download over the wireless network.

Each software package represents an independent application environment within the mobile device. Any configuration utilities that change application settings are typically modified through the Enterprise Administrator, simplifying application management. Each software package is usually pre-assigned with default selection criteria. For example, in a Symbol environment, a 6840 Telnet Client software package has a pre-assigned selection criteria that restricts it to 6840 mobile devices. No other mobile devices can receive this software package. Software packages can also target a complete series of mobile devices. The ATI3000 software package, for example, targets the entire 3000 series line of mobile devices.

Avalanche supports the full Wavelink product line for the Telnet Emulation Clients. This includes 5250, 3270, VT and HP clients for both TN (standalone) and NC (through a Wavelink gateway) environments. Avalanche-enabled packages are also available for the Wavelink Studio Clients.

Software Collections

A software collection is a logical grouping of software packages that the Avalanche Agent manages and maintains. You can create new collections or copy software from collection to collection as needed.

You can apply different selection criteria to each software collection. Selection criteria for a software collection places limits on the distribution of software packages in addition to the limits built into the package when it was created. The ability to define selection criteria for a software collection provides you with a high level of control over which packages download to which devices.

Software collections allow you to manage software packages in a variety of ways. In many cases, it is best to place all the packages into one global collection, but in other cases it might be helpful to separate the packages. For example, you could configure two software collections to target different classes of devices. You could then copy a package from one collection to the other and configure the package differently in each collection.

Avalanche Enabler

The Avalanche Enabler is the agent that you initially load onto a mobile device to allow the Avalanche Agent to manage it. In DOS devices, this also includes all of the drivers and other infrastructure needed to boot the device and connect it to the wireless network. For most device types, you must initially load the Enabler using a serial connection, though you can easily apply any updates to the Enabler using a wireless connection.

In addition to providing software and configuration updates, the Enabler manages the software applications loaded onto the mobile device. The Enabler displays a menu that provides users with an easy way to access applications.

Additional Information

The following resources are available to provide you with additional information about the Mobile Manager:

- The Wavelink Web site, www.wavelink.com
- The Mobile Manager Users Guide, which covers information regarding wireless network administration at a local, or site, level

- The Avalanche Manager Users Guide, which covers information regarding wireless mobile device software updates at a local, or site, level

Chapter 2: Installation

The Mobile Manager is designed to operate on a wide variety of network configurations. However, certain requirements must be met to ensure optimal performance.

This section lists the hardware and software requirements of the Mobile Manager and how to install it on your network. Complete installation information is available in the following topics:

- Requirements
- Getting Started
- Installing Mobile Manager
- Activating the Mobile Manager

Requirements

This section lists the hardware, software, and firmware requirements that the Mobile Manager requires for best performance.

Hardware Requirements

The Mobile Manager requires the following hardware components to operate effectively:

Mobile Manager Component	Required	Recommended
Enterprise Administrator	Pentium 450 Mhz, 128 MB RAM	Pentium 700 Mhz, 256 MB RAM
Enterprise Edition Components	Pentium 450 Mhz, 128 MB RAM	Pentium 700 Mhz, 256 MB RAM
Mobile Manager Agent	Pentium 233 Mhz 128MB RAM (plus 2 MB per Access Point managed)	Pentium 600 Mhz, 128MB RAM (plus 2 MB per Access Point managed)
Avalanche Agent	Pentium 133 Mhz 64 MB RAM	Pentium 233 Mhz 128 MB RAM

Table 2-1: *Hardware Requirements for Mobile Manager Enterprise Edition Components*

Software Requirements

The Mobile Manager requires one of the following operating systems to run effectively:

- Windows NT, service pack 6
- Windows 2000, service pack 2

NOTE To deploy your configuration settings to your wireless components, you must install an Agent on the subnet where those components reside.

Access Point Firmware Requirements

The Mobile Manager supports the following firmware versions:

Hardware	Firmware
3COM Airconnect 11Mbps	02.20-04
Cisco 340/350	AP 11.07 AP 11.07a AP 11.08T AP 11.08T1 AP 11.10T AP 11.10T1 AP 11.21
Cisco 350 Bridge	AP 11.07 AP 11.07a AP 11.08T AP 11.08T1 AP 11.10T AP 11.10T1 AP 11.21
Cisco 1200	AP 11.40 AP 11.41T AP 11.42T

Table 2-2: *Supported Firmware for Mobile Manager Enterprise Edition*

Hardware	Firmware
Ericsson WLAN DSSS A11	02.20-04
Intel Pro 2011	02.20-04
Intel Pro 2011B	03.00-19 03.51-20
Nortel e-mobility 802.11 DS	02.20-04
Symbol AP-2411	03.10-20 04.00-25
Symbol AP-3020, 3021	04.00-30c 04.01-25 04.02-12 04.02-19
Symbol AP-4111, 4121	02.20-04 02.21-00 02.51-23 02.52-13
Symbol AP-4131	03.50-10 03.50-18

Table 2-2: *Supported Firmware for Mobile Manager Enterprise Edition*

For updated information on supported firmware versions, see the release notes included with your Mobile Manager installation.

NOTE Current firmware support for Cisco-Aironet is limited to version 11.x and higher. If your Access Points use firmware 11.06, it is highly recommended that you update to version 11.08. See your hardware documentation for information on how to upgrade the firmware for Cisco-Aironet Access Points.

Supported Client Software

Wavelink Avalanche supports all Wavelink emulation products, including 5250, 3270, VT and HP emulations for both TN (standalone) and NC (through a Wavelink gateway) environments.

In addition, Wavelink Avalanche supports all Wavelink Studio Clients that run on supported devices.

Supported Devices

Wavelink currently supports most DOS-based mobile devices in addition to Palm OS and Windows CE/Pocket PC devices.

As new mobile devices are supported by Wavelink, they will automatically include support for Avalanche, with the rare exception of mobile devices that lack any dynamic storage ability. Check the Wavelink Web site, www.avelink.com for the most up to date list of supported devices.

Getting Started

After you have met the hardware and software requirements of Mobile Manager, you must acquire the necessary files and executables and install them on your network. These files are available from the Mobile Manager CD-ROM.

Installing Mobile Manager

This section covers a complete installation process of the Mobile Manager.

NOTE If you stop the installation process at any time, you must use the uninstall utility to remove any partially-installed components before you attempt to re-install.

To install Mobile Manager:

1 Insert the Mobile Manager CD into your CD-ROM drive. If your CD-ROM supports the auto-run feature, the installation menu automatically appears on your desktop.

If your CD-ROM does not support the auto-run feature, you can manually start the CD-ROM installation menu by running the file `mme_1000.exe` from the root of the CD-ROM.

NOTE At any time, you can cancel the installation process by clicking either `Cancel Setup` or `Exit Setup`.

The *Introduction* dialog box appears.

2 Click `Next` to continue the installation process.

The *License Agreement* dialog box appears.

3 Read through the license agreement carefully.

4 If you agree with the terms in the license agreement, select the **I accept the terms of the License Agreement** option and click `Next`.

The *Choose Product Features* dialog box appears.

5 Select an installation type.

If you want to install all of the Mobile Manager components, click the **Server & Administrator Console** icon.

If you want to install only the server components of Mobile Manager, click the **Server** icon.

If you want to install only the Enterprise Administrator, click the **Administrator** icon.

6 Click `Next`.

The *Choose Install Folder* dialog box appears.

7 Click `Next` to accept the default installation folder, or click `Choose` to navigate to a folder of your choice. After you click `Choose`, click `Next` to continue the installation process.

The *Choose Shortcut Folder* dialog box appears. This dialog box allows you to create a folder that contains shortcuts to the different Mobile Manager components.

8 Select a shortcut folder location, then click `Next`.

The *MySQL Database* dialog box appears.

9 Select if you want to install MySQL along with the Mobile Manager and click `Next`.

The setup program checks to see if MySQL is installed on your system. MySQL is the database Mobile Manager uses to help you manage your wireless network.

10 Click `Next`.

The *Administrative User* dialog box appears.

11 Type the name of the user that will have administrative rights to the Mobile Manager Enterprise Edition in the **User Name** text box.

12 Type the password for the administrative user account in the **Password** text box.

13 Confirm the password for this account by re-typing it in the **Confirm Password** text box.

14 Enable the **Enable Encryption** check box to enable encryption between the Enterprise Administrator and Mobile Manager server components, such as the Enterprise Manager and the Fault Manager.

The C*hoose Java Virtual Machine* dialog box appears. Because Mobile Manager components are Java-based, you must have a Java Virtual Machine to run these components.

15 If a Java Virtual Machine is not currently installed on your system, select the **Install a Java VM specifically for this application** option.

If you prefer to use an existing Java Virtual Machine, select the **Choose a Java VM already installed on this system** option, and then select the desired Java Virtual Machine.

NOTE You must use a Java VM that complies with the Java 2 Runtime Environment, standard edition, version 1.3 or later.

---

16 Click `Next`.

The *Pre-Installation Summary* dialog box appears, displaying the parameters you have set for this installation.

17 Click `Install`.

The Mobile Manager is installed on your system.

18 Click `Done`.

The Setup program configures several internal components to run on your system.

Once the installation is complete, you are immediately prompted to activate this installation of Mobile Manager for your network.

Activating the Mobile Manager

After the Mobile Manager is installed on your host system, you must activate it with a valid license code. This code uses a technique called nodelocking, in which the Mobile Manager is licensed only for a specific computer, or node, on your network.

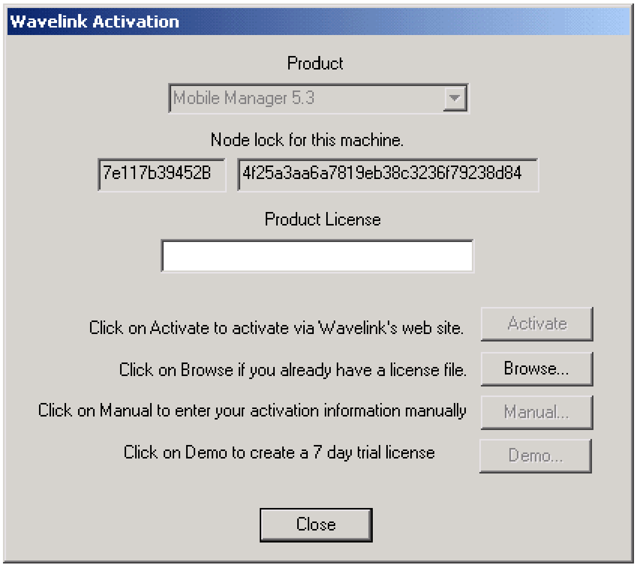
NOTE A node is defined as several specific system attributes that, in combination, uniquely distinguish it from any other system in your organization.

When you activate the Mobile Manager, a license file called `wavelink.lic` is installed on your system, which provides the information the product needs to operate. How you acquire this file depends on whether the system hosting the Mobile Manager has Internet access. If the system has Internet access, you can acquire the license file automatically. If the system does not have Internet access, there are alternate methods of receiving your license code.

To activate the Mobile Manager:

1 Install the Mobile Manager as described in *Installing Mobile Manager* on page 22.

  When the installation process copies all of the necessary files, the *Wavelink Activation* dialog box appears.



Wavelink Activation

Product

Mobile Manager 5.3

Node lock for this machine.

7e117b39452B 4f25a3aa6a7819eb38c3236f79238d84

Product License

Click on Activate to activate via Wavelink's web site.

Click on Browse if you already have a license file.

Click on Manual to enter your activation information manually

Click on Demo to create a 7 day trial license

Figure 2-1. *The Activation Dialog Box*

2 Type your license number for this installation in the **Product License** text box.

3 Select an activation type.

If the Mobile Manager resides on a system that has Internet access, click `Activate`. When you click `Activate`, the Mobile Manager connects with a secure Wavelink Web site. Once a connection is established, your license and nodelock are verified and a license file is sent to your host system. A new dialog box appears, specifying your licensing information and asking if you want to save this information for this installation. Click `Yes` to save the license file and activate your installation.

If you already have a license file that you want to use, click `Browse`. When you click `Browse`, a dialog box appears that allows you to navigate to the location of the license file. The Mobile Manager then uses this file to activate its services.

If you are receiving your authorization information from a Wavelink customer service representative, click `Manual`. When you click `Manual`, the *Manual Entry* dialog box appears. This dialog box allows you to type in the information provided by your customer service representative. Once you enter this information, click `Apply`. The Mobile Manager then generates a license file and is activated for its host system.

If, for any reason, you are unable to use the **Activate**, **Manual**, or **Browse** buttons to activate your product install, you can generate a temporary license by clicking the **Demo** button after you type a valid license number into the Product License text box. Once you click this button, the *Activation* dialog box creates a specialized Wavelink.lic license file. This file allows you to use an unrestricted installation of the Wavelink product for up to seven days. After seven days, you must either activate the installation permanently by using the **Activate** or **Manual** buttons.

The Mobile Manager is now authorized for use on your host system. It is important to remember that the new Wavelink licensing process ties the Mobile Manager install to a specific computer on your network. If a situation occurs that requires you to re-install the Mobile Manager on a different system, please contact your Wavelink customer service representative so they can unlock your license from that system, allowing you to re-install the product on a new one.

Chapter 3: Enterprise Administrator

You primarily interact with your wireless network using the Enterprise Administrator. The Enterprise Administrator allows you to control global characteristics of your wireless network. These characteristics include creating Access Point profiles, assigning IP addresses, managing software, and monitoring network performance. With the Enterprise Administrator, you can also compile reports of network activity over set periods of time, which you can use to further optimize your network to meet the demands of your organization.

As you manage your wireless network, the Enterprise Administrator works with server-based components of the Mobile Manager product, called Agents. These Agents are responsible for sending instructions to and receiving data from wireless devices. The Mobile Manager includes two types of Agents: Mobile Manager Agents and Avalanche Agents. From the Enterprise Administrator, you can deploy one or both of these Agents anywhere within your network. See *Chapter 12: Deploying Agents* on page 143 for more information on deploying Agents to manage your wireless network.

To streamline wireless network management, the Enterprise Administrator allows you to categorize Agents into sites and groups. A site is defined as a location within your network that hosts at least one Agent. A group is defined as a collection of sites that share similar traits. You can create as many or as few groups as you need to manage your wireless network. See *Chapter 4: Managing Sites and Groups* on page 43 for more information on how you can use sites and groups to organize wireless network components.

This section contains the following topics:

- Starting the Enterprise Administrator
- Understanding Enterprise Administrator Views
- Setting Enterprise Administrator Preferences

Starting the Enterprise Administrator

The Enterprise Administrator allows you to configure and manage your wireless network on an enterprise-wide basis.

To start the Enterprise Administrator:

1 Click `Start` from the desktop.

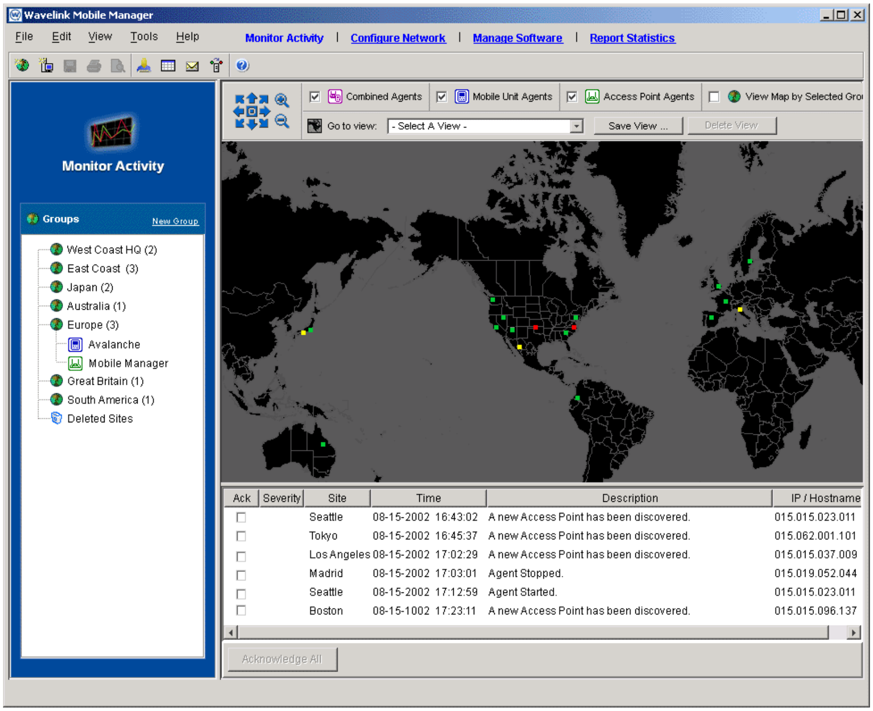
2 Select `Programs`.

3 Select `Wavelink Mobile Manager`.

4 Select `Enterprise`.

5 Select `Administrator`.

The Enterprise Administrator appears.



Ack	Severity	Site	Time	Description	IP / Hostname
☐		Seattle	08-15-2002 16:43:02	A new Access Point has been discovered.	015.015.023.011
☐		Tokyo	08-15-2002 16:45:37	A new Access Point has been discovered.	015.062.001.101
☐		Los Angeles	08-15-2002 17:02:29	A new Access Point has been discovered.	015.015.037.009
☐		Madrid	08-15-2002 17:03:01	Agent Stopped.	015.019.052.044
☐		Seattle	08-15-2002 17:12:59	Agent Started.	015.015.023.011
☐		Boston	08-15-1002 17:23:11	A new Access Point has been discovered.	015.015.096.137

Figure 3-1. *The Enterprise Administrator*

Understanding Enterprise Administrator Views

The Enterprise Administrator consists of four main components, or views: the Monitor Activity view, the Configure Network view, the Manage Software view, and the Report Statistics view. These views provide you with different information regarding wireless network configuration and activity. In addition, the Enterprise Administrator contains the Groups window, which provides a tree view of the groups and sites within your wireless network.

Monitor Activity View

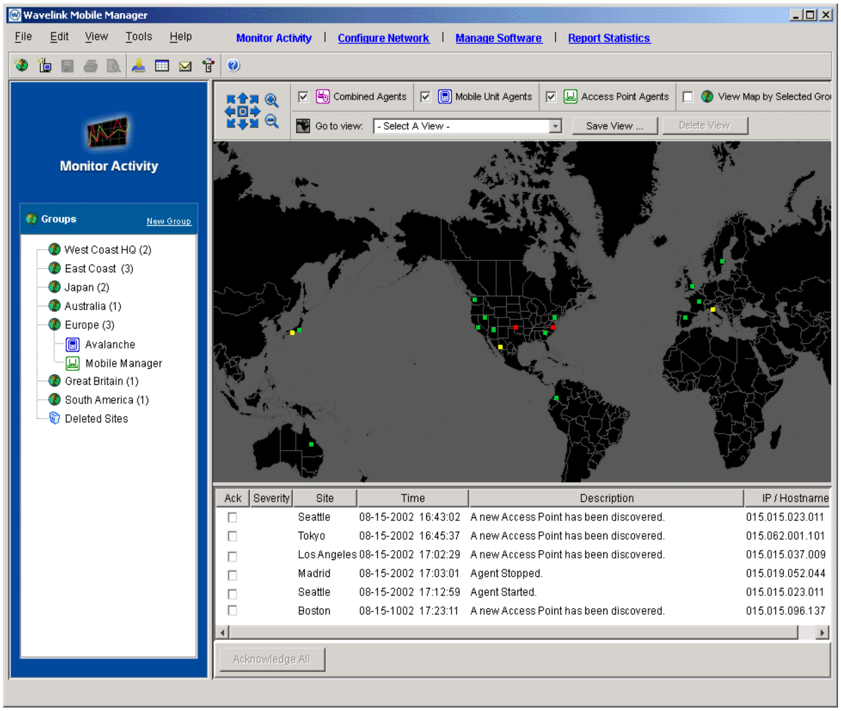
The Monitor Activity view provides you with a real-time view of the health of your wireless network. With the Monitor Activity view, you can tell at a glance which sites on your network are operating normally and which require attention.

To access the Monitor Activity view:

1 Open the Enterprise Administrator.

2 Click `Monitor Activity` from the toolbar.

The Monitor Activity view appears.



Ack	Severity	Site	Time	Description	IP / Hostname
□		Seattle	08-15-2002 16:43:02	A new Access Point has been discovered.	015.015.023.011
□		Tokyo	08-15-2002 16:45:37	A new Access Point has been discovered.	015.062.001.101
□		Los Angeles	08-15-2002 17:02:29	A new Access Point has been discovered.	015.015.037.009
□		Madrid	08-15-2002 17:03:01	Agent Stopped.	015.019.052.044
□		Seattle	08-15-2002 17:12:59	Agent Started.	015.015.023.011
□		Boston	08-15-1002 17:23:11	A new Access Point has been discovered.	015.015.096.137

Figure 3-2. *The Monitor Activity view*

The Monitor Activity view consists of two panes: the Map pane and the Alarm Browser. The Map pane provides a geographical overview of the health of your network.

You display different portions of the map by using the navigation arrows. You can also center the map on its default location by using the center button within these arrows. In addition, the magnifying glass icons allow you to zoom in and out of different areas on the map.

NOTE You can zoom in on specific areas by clicking within the map and dragging the pointer across the desired region. A square appears around the region. When you release the mouse button, the Enterprise Administrator refreshes the map to display a closer view of the selected area.

With the Map pane, you can apply filters so that only specific wireless components appear within the map. These filters are activated by the checkboxes located next to the map's navigation arrows. The filters you can apply include:

Combined Agents	Displays sites that contain both an Avalanche Agent and a Mobile Manager Agent.
Mobile Unit Agents	Displays sites that contain only an Avalanche Agent.
Access Point Agents	Displays sites that contain only a Mobile Manager Agent.
View Map By Selected Group	Displays only those sites that belong to the group selected in the Groups window.

You also have the option saving specific views within the Map pane. This feature allows you to immediately display a relevant section of your wireless network.

To save a view within the Map pane:

1 Configure the Map pane by using the navigation arrows and zooming in on the relevant geographic area.

2 Click `Save View`.

3 Type the name of the view in the dialog box that appears.

The view is now saved on the system hosting the Enterprise Manager. To access a saved view, select the view from the **Go to View** list.

Directly below the Map pane is the Alarm Browser. This pane displays the alerts that occur on your wireless network in a table format. This table provides the following information about each alert:

Ack
Allows you to acknowledge that you have seen the alert. When you acknowledge an alert, the site with that alert stops flashing in the Map pane.

Severity
Indicates the severity of the alert.

Site
The name of the site that generated the alert.

Time
The time and date when the alert occurred.

Description
A brief description of the alert.

IP Address/Hostname
The IP address and hostname of the Agent on the site that generated the alert.

You can sort this table by clicking a specific column heading.

Configure Network View

The Configure Network view allows you to modify network settings on both Access Points and mobile devices on on an enterprise-wide level. From this view, you manage the following administrative tasks:

- Configure Access Point profiles
- Manage IP addresses
- Build Very Large Access Control Lists
- Create alert profiles

With the Enterprise Administrator, you do not configure individual wireless network components, such as Access Points. Instead, the Mobile Manager allows you to organize these components into sites and combine those sites into groups. The Mobile Manager applies any modifications you make to your network in the Enterprise Administrator to these groups.

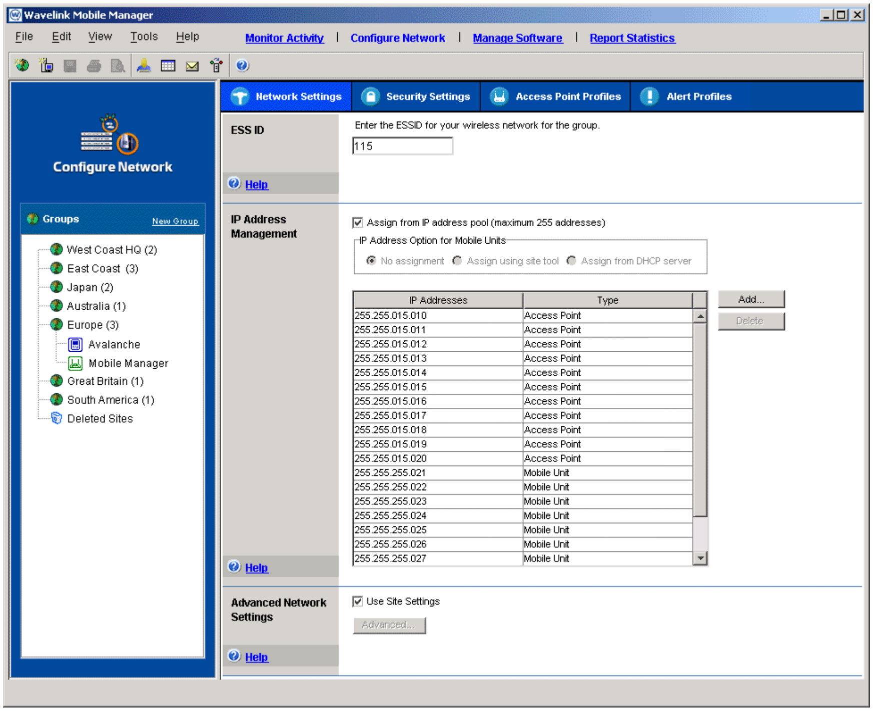
NOTE To modify wireless network components at the site level, see the *Mobile Manager Users Guide*.

To access the Configure Network view:

1 Open the Enterprise Administrator.

2 Click `Configure Network` from the toolbar.

The Configure Network view appears.



ESS ID

Enter the ESSID for your wireless network for the group.

115

IP Address Management

☑ Assign from IP address pool (maximum 255 addresses)

IP Address Option for Mobile Units

● No assignment ○ Assign using site tool ○ Assign from DHCP server

IP Addresses	Type
255.255.015.010	Access Point
255.255.015.011	Access Point
255.255.015.012	Access Point
255.255.015.013	Access Point
255.255.015.014	Access Point
255.255.015.015	Access Point
255.255.015.016	Access Point
255.255.015.017	Access Point
255.255.015.018	Access Point
255.255.015.019	Access Point
255.255.015.020	Access Point
255.255.255.021	Mobile Unit
255.255.255.022	Mobile Unit
255.255.255.023	Mobile Unit
255.255.255.024	Mobile Unit
255.255.255.025	Mobile Unit
255.255.255.026	Mobile Unit
255.255.255.027	Mobile Unit

Advanced Network Settings

☑ Use Site Settings

Figure 3-3. *The Configure Network view*

The Configure Network view contains four tabs. Each tab controls a specific aspect of Access Point configuration.

NOTE Any configurations made in the Configure Network view apply only to a specific group. As a result, you must select a group before you can modify a pane within the Configure Network view.

The tabs within the Configure Network view are as follows:

Network settings Defines network settings, such as IP addresses and ESSIDs.

Security settings Defines security settings, such as WEP.

Access Point Profiles Defines templates of configuration settings, called profiles, that are applied to Access Points on your network.

Alert Profiles Defines alert profiles, which can notify you when a specific alert occurs on the network.

Manage Software View

The Manage Software view provides you with the ability to add, modify, delete, and deploy software to your mobile devices. You can also define selection criteria which determines which mobile devices receive specific software.

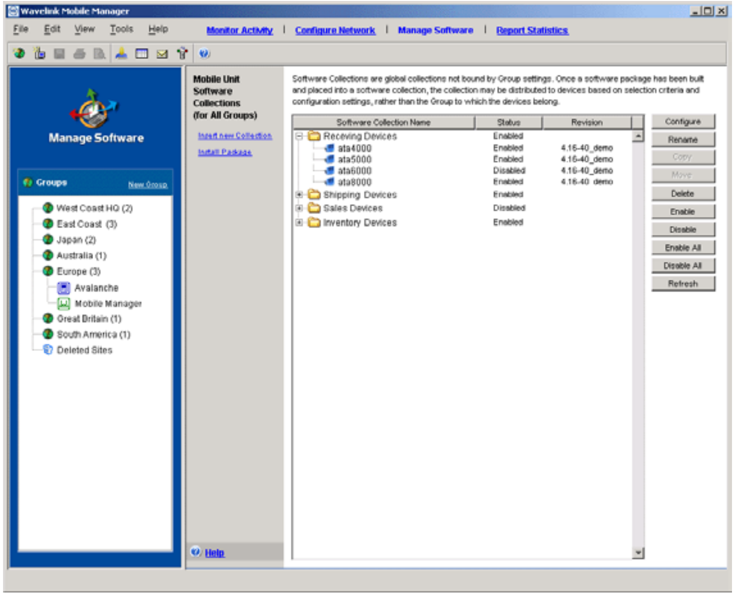
Mobile device software falls into two categories within the Manage Software view: packages and collections. A software package is a collection of application files associated with a single mobile device. When a software package is deployed to a mobile device, that device receives all of these files, ensuring that it can use the application effectively. A software collection contains one or more software packages. You can configure each software collection so that the packages it contains apply only to certain mobile devices.

To access the Manage Software view:

1 Open the Enterprise Administrator

2 Click `Manage Software` from the toolbar.

The Manage Software view appears.



Software Collections are global collections not bound by Group settings. Once a software package has been built and placed into a software collection, the collection may be distributed to devices based on selection criteria and configuration settings, rather than the Group to which the devices belong.

Software Collection Name	Status	Revision
Receiving Devices	Enabled	
ata4000	Enabled	4.16-40_demo
ata5000	Enabled	4.16-40_demo
ata6000	Disabled	4.16-40_demo
ata8000	Enabled	4.16-40_demo
Shipping Devices	Enabled	
Sales Devices	Disabled	
Inventory Devices	Enabled	

Figure 3-4. *The Manage Software View*

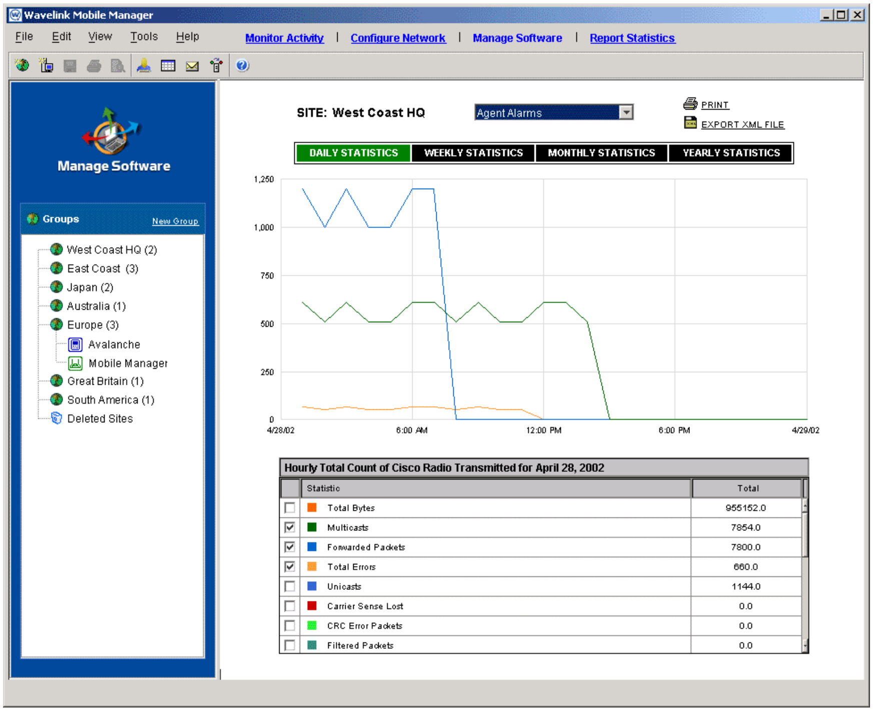
Report Statistics View

From the Report Statistics view, you can generate reports on wireless network performance based on a variety of statistical filters and event types. You can also print reports or export them into an XML file.

To access the Report Statistics view:

1. Open the Enterprise Administrator.
2. Click `Report Statistics` from the toolbar.

   The Report Statistics view appears.



SITE: West Coast HQ   Agent Alarms

Hourly Total Count of Cisco Radio Transmitted for April 28, 2002

	Statistic	Total
□	🟧 Total Bytes	955152.0
☑	🟩 Multicasts	7854.0
☑	🟦 Forwarded Packets	7800.0
☑	🟧 Total Errors	660.0
□	🟦 Unicasts	1144.0
□	🟥 Carrier Sense Lost	0.0
□	🟩 CRC Error Packets	0.0
□	🟩 Filtered Packets	0.0

Figure 3-5. *The Report Statistics view*

Groups Window

All of the Enterprise Administrator views provide access to the Groups window. This window, located on the left side of the Enterprise Administrator, allows you to organize sites that share common characteristics into groups. You can then assign configuration settings to these groups, instead of configuring each site individually. See *Chapter 4: Managing Sites and Groups* on page 43 for more information on how you use groups to manage your wireless network.

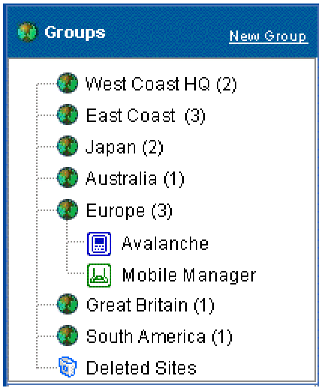


Figure 3-6. *The Groups Window*

Setting Enterprise Administrator Preferences

The Enterprise Administrator continually displays information pertaining to wireless network performance. You can customize the Enterprise Administrator to best suit your wireless network management needs. To customize the Enterprise Administrator, select `Preferences` from the **File** menu. This option allows you to change the following aspects of the Enterprise Administrator:

- The location of the host system support the Mobile Manager Enterprise Edition components (such as the Enterprise Manager and Fault Manager)
- The length of time that alerts remain in the Alarm Browser of the Monitor Activity view
- The rules that govern how the Enterprise Administrator communicates with the sites on your network

The following sections describe these preferences in detail.

Selecting the Location of Network Services

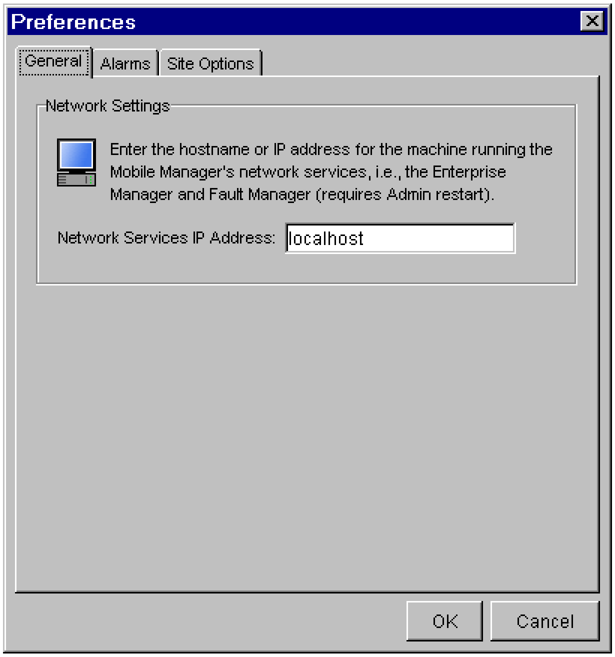
The Mobile Manager Enterprise Edition is designed to operate across an enterprise-wide wireless network. Consequently, the system running the Enterprise Administrator might not be the system that is running the network services of the Mobile Manager, such as the Enterprise Manager and Fault Manager. The Enterprise Administrator depends on these components to receive up-to-date information on your wireless network.

To select the location of Mobile Manager network services:

1 Select `Preferences` from the **File** menu.

The *Preferences* dialog box appears.

2 Click the General tab.



Enter the hostname or IP address for the machine running the Mobile Manager's network services, i.e., the Enterprise Manager and Fault Manager (requires Admin restart).

Network Services IP Address: localhost

Figure 3-7. *The General Tab of the Preferences Dialog Box*

3 Type the system name or IP address of the system running the Mobile Manager network services in the **Network Services IP Address** text box.

4 Click `OK`.

When you next restart the Enterprise Administrator, it will automatically attempt to connect to the network services that reside on the system you specified.

Configuring the Alarm Browser

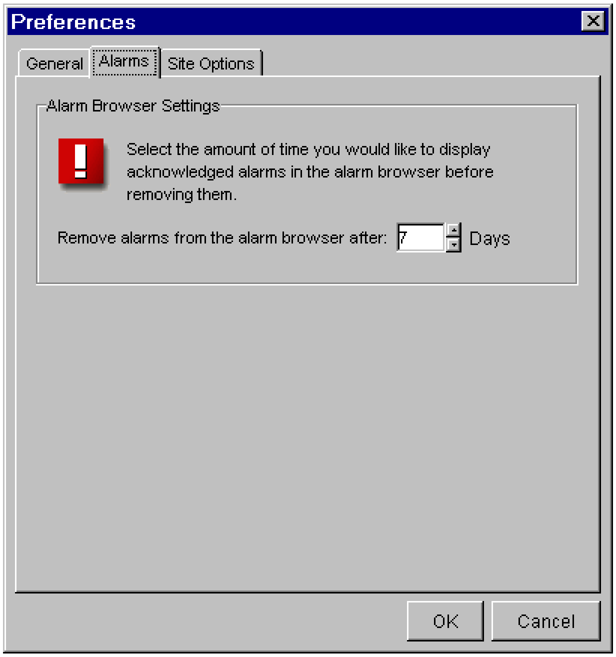
The Enterprise Administrator provides you with the Alarm Browser of the Monitor Activity view so you can quickly learn of network performance alerts. You can configure the Enterprise Administrator to remove acknowledged alerts after a defined period of time.

To configure when alerts are removed from the Alarm Browser:

1 Select `Preferences` from the **File** menu.

The *Preferences* dialog box appears.

2 Click the Alarms tab.



Select the amount of time you would like to display acknowledged alarms in the alarm browser before removing them.

Remove alarms from the alarm browser after: 7 Days

Figure 3-8. *The Alarms Tab of the Preferences Dialog Box*

3 Type how many days an alert remains in the Alarm Browser in the **Remove alarms from the alarm browser after** text box.

4 Click `OK`.

Controlling Site Communication

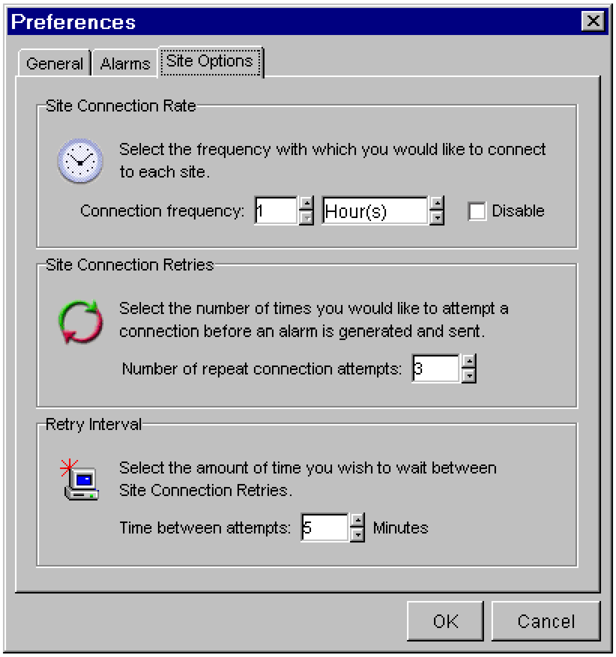
From the Enterprise Administrator you are able to access detailed information about your wireless network at a site level. You can control how the Enterprise Administrator communicates with the sites on your network with the Site Options tab of the *Preferences* dialog box.

To control site communication:

1 Select `Preferences` from the **File** menu.

The *Preferences* dialog box appears.

2 Click the Site Options tab.



Site Connection Rate

Select the frequency with which you would like to connect to each site.

Connection frequency: 1 Hour(s) □ Disable

Site Connection Retries

Select the number of times you would like to attempt a connection before an alarm is generated and sent.

Number of repeat connection attempts: 3

Retry Interval

Select the amount of time you wish to wait between Site Connection Retries.

Time between attempts: 5 Minutes

Figure 3-9. *The Site Options Tab of the Preferences Dialog Box*

3 Select how frequently you want the Enterprise Administrator to verify site status from the **Connection Frequency** text boxes.

If you do not want the Enterprise Administrator to verify site status, enable the **Disable** checkbox.

4 Select how many times the Enterprise Administrator attempts to verify site status from the **Number of repeat connection attempts** text box.

If the Enterprise Administrator cannot verify site status within the specified number of attempts, it generates an alert.

5 Select how much time the Enterprise Administrator waits between connection retries in the **Time between attempts** text box.

6 Click `OK`.

Chapter 4: Managing Sites and Groups

To streamline wireless network management, the Enterprise Administrator allows you to categorize Agents into sites and groups. A site is the most basic component of the Enterprise Administrator. Each site contains at least one Agent that communicates with specific wireless components. Because these sites are based on Agents, you can define a site in a way that best suits your network administration processes—for example, you can organize sites by location or by network role.

The Mobile Manager further streamlines wireless network management by allowing you to create one or more collections of sites, called groups. Each site within a group contains a set of similar characteristics such as geographic location or role within your organization's structure. When you configure a group, the Enterprise Administrator applies the configurations to every site within that group.

You control how many groups your organization uses and how many sites belong to each group. You can create as many or as few groups as your network management processes demand.

This section contains the following topics:

- Adding Sites
- Modifying Sites
- Deleting and Restoring Sites
- Locating Sites
- Relocating Sites
- Configuring Components at the Site Level
- Adding Groups
- Renaming Groups
- Deleting Groups
- Adding Sites to Groups
- Removing Sites from Groups

Adding Sites

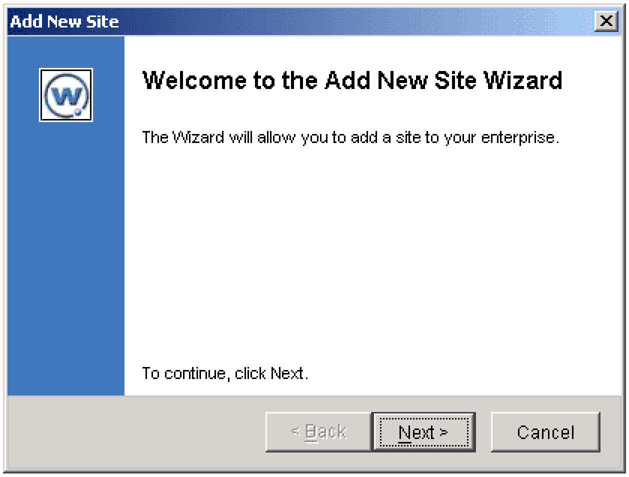
To track and display sites, you must first add those sites to the Enterprise Administrator. Once you add these sites, you can use the different views of the Enterprise Administrator to ensure that each site functions correctly.

NOTE The Enterprise Administrator is designed to apply configuration settings to groups of sites. To configure an individual site from the Enterprise Administrator, you can do so by creating a group that contains only that site and applying settings to that group.

To add a site:

1 Select `Add New Site` from the **Tools** menu.

The Add Site Wizard launches.



Welcome to the Add New Site Wizard

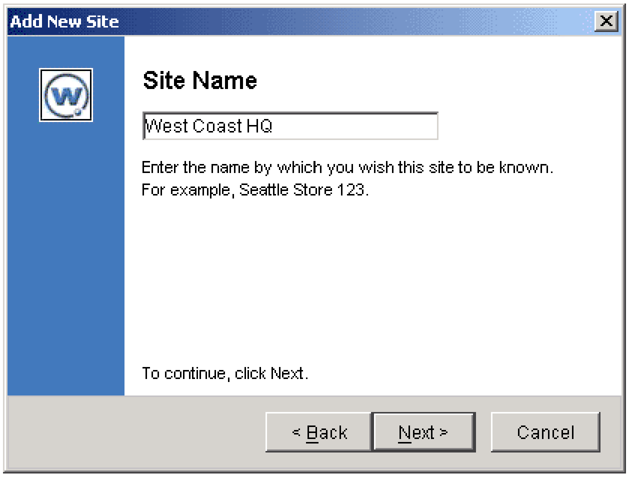
The Wizard will allow you to add a site to your enterprise.

To continue, click Next.

Figure 4-1. *The Welcome Dialog Box*

2 Click `Next`.

The *Site Name* dialog box appears.



West Coast HQ

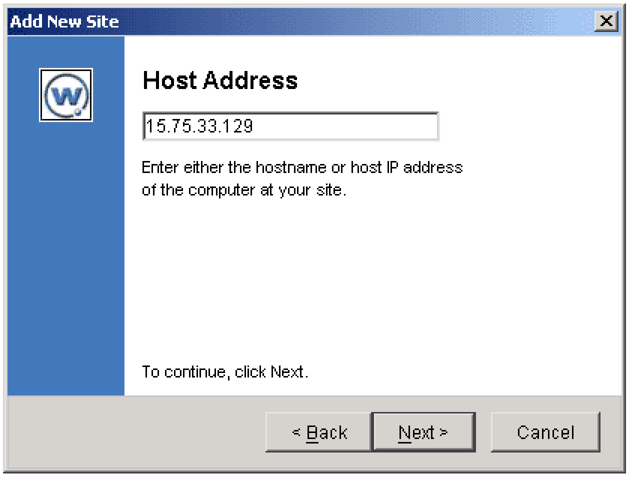
Enter the name by which you wish this site to be known.
For example, Seattle Store 123.

To continue, click Next.

Figure 4-2. *The Site Name Dialog Box*

3 Type a unique name of the new site in the **Site Name** text box and click `Next`.

The *Host Address* dialog box appears.



15.75.33.129

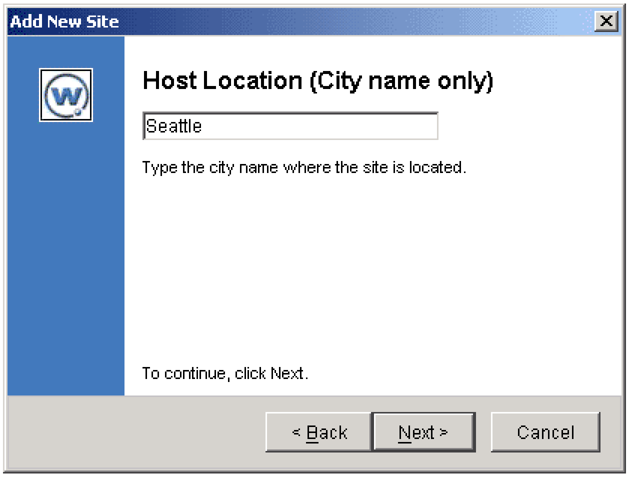
Enter either the hostname or host IP address
of the computer at your site.

To continue, click Next.

Figure 4-3. *The Host Address Dialog Box*

4 Type the hostname or IP address for the system that hosts (or will host) the Mobile Manager Agent in the **Host Address** text box and click `Next`.

The *Host Location (City Name Only)* dialog box appears.



Add New Site

Host Location (City name only)

Seattle

Type the city name where the site is located.

To continue, click Next.

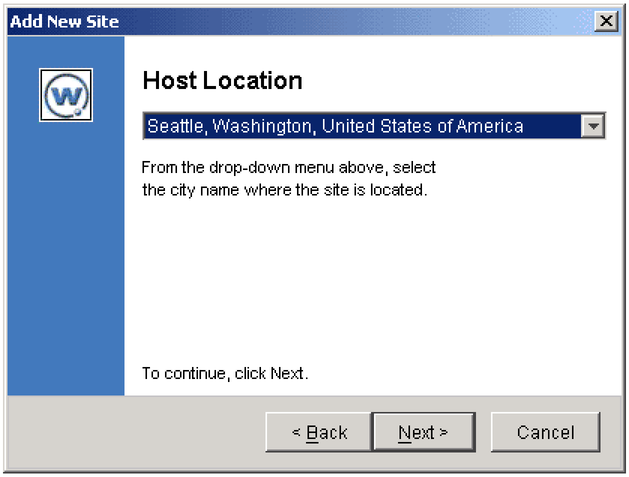
Figure 4-4. *The Host Location (City Name Only) Dialog Box*

5 Type the name of the city where this site resides in the **Host Location (City Name Only)** text box.

The information you provide in this dialog box allows the Mobile Manager to search its database for the city information.

6 Click `Next`.

If the Mobile Manager was able to locate the city, the *Host Location* dialog box appears.


Add New Site

Host Location

Seattle, Washington, United States of America

From the drop-down menu above, select the city name where the site is located.

To continue, click Next.

Figure 4-5. *The Host Location Dialog Box*

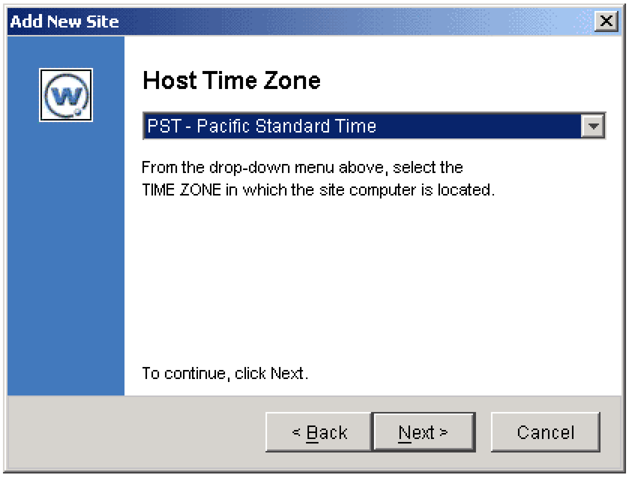
The **Host Location** list in this dialog box should already display the city name you entered in the *Host Location (City Name Only)* dialog box. If the Mobile Manager discovers several cities with the same name, you can select the appropriate city from the **Host Location** list.

If the Mobile Manager was unable to locate the city, the *Unable to Locate Host* dialog box appears. This dialog box allows you to check the city name you entered, or to continue adding the site.

NOTE If you continue adding the site when the *Unable to Locate Host* dialog box appears, you can relocate the site at a later time. See *Relocating Sites* on page 54 for more information.

7 Click `Next`.

The *Host Time Zone* dialog box appears.



Add New Site

Host Time Zone

PST - Pacific Standard Time

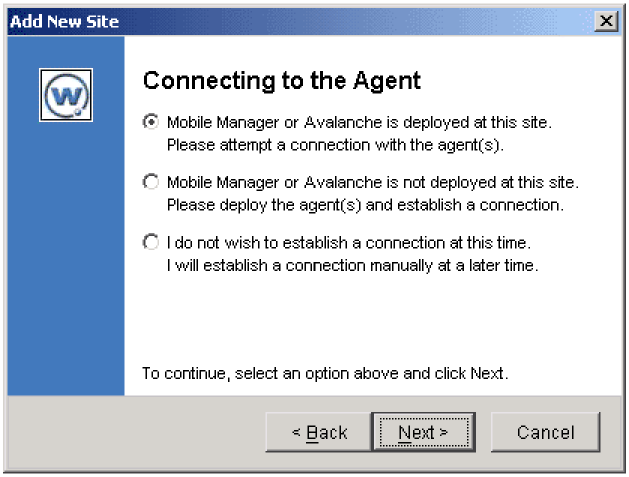
From the drop-down menu above, select the TIME ZONE in which the site computer is located.

To continue, click Next.

Figure 4-6. *The Host Time Zone Dialog Box*

8 Select the appropriate time zone for this site from the **Host Time Zone** list and click `Next`.

The *Connecting to the Agent* dialog box appears.



Add New Site

Connecting to the Agent

● Mobile Manager or Avalanche is deployed at this site. Please attempt a connection with the agent(s).

○ Mobile Manager or Avalanche is not deployed at this site. Please deploy the agent(s) and establish a connection.

○ I do not wish to establish a connection at this time. I will establish a connection manually at a later time.

To continue, select an option above and click Next.

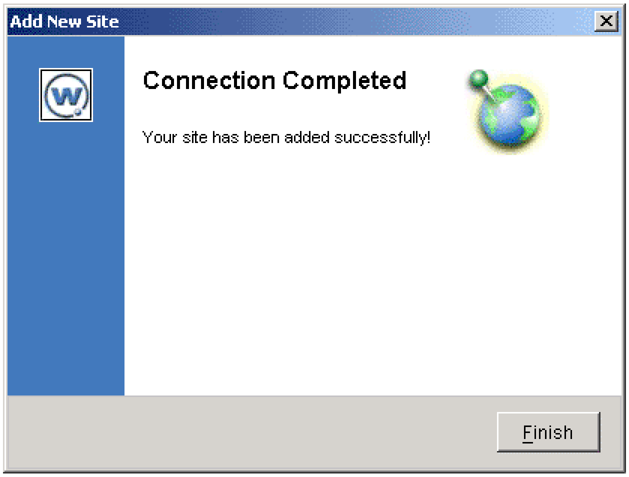
Figure 4-7. *The Connecting to the Agent Dialog Box*

9 Select the appropriate option from the dialog box and click `Next`.

If you opted to deploy an Agent to the new site, continue adding the site by following the steps listed in *Chapter 12: Deploying Agents* on page 143.

If an Agent already resides at the new site, the Mobile Manager attempts to connect to the Agents and displays. The results of this connection attempt appear in a *Connection Status* dialog box. Click `Next` from this dialog box to access the *Connection Completed* dialog box, signifying that the new site has been added to the Enterprise Administrator.

If you are not deploying an Agent at this time, the *Connection Completed* dialog box appears immediately.



Your site has been added successfully!

Figure 4-8. *The Connection Completed Dialog Box*

10 Click `Finish` to close the Add Site Wizard.

To add this new site to a group on your network, see *Adding Sites to Groups* on page 58.

Modifying Sites

If the identifiable information on a site changes—such as its IP address or its name—you can modify that site directly with the Enterprise Administrator.

To modify a site:

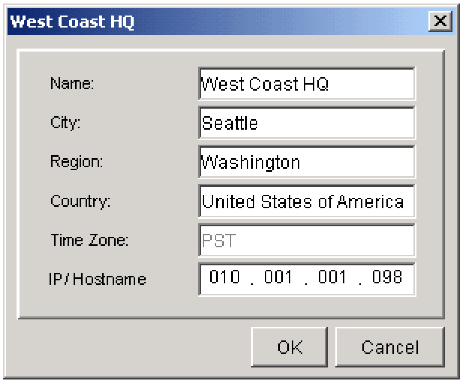
1 Open the Monitor Activity view of the Enterprise Administrator.

2 Right-click the site within the Maps pane.

If the site is a part of a group, you can also right-click the site from the Groups window.

3 Select `Properties` from the menu that appears

A dialog box appears, displaying information about the selected site.



Name: West Coast HQ

City: Seattle

Region: Washington

Country: United States of America

Time Zone: PST

IP / Hostname 010 . 001 . 001 . 098

Figure 4-9. *A Sample Modify Site Dialog Box*

Within this dialog box, you can modify the following site properties:

- Name
- City
- Region
- Country
- IP/Hostname

4 Modify the site information as necessary.

5 Click `OK` to close the dialog box and return to the Enterprise Administrator.

Deleting and Restoring Sites

Deleting sites from the Enterprise Administrator requires a degree of caution. This caution is warranted because not only are deleted sites unavailable to anyone using the Enterprise Administrator, but all historical data about that site are permanently deleted.

To help you delete unwanted sites from the Enterprise Administrator, the Groups window contains a group called Deleted Sites. When you first delete a site from a group, that site moves from its previous group to the Deleted Sites group. Consequently, you can still generate historical reports about that site. Once you delete a site from the Deleted Sites group, all information about that site is permanently removed from the Mobile Manager.

To move a site to the Deleted Sites group:

1. Open the Enterprise Administrator.
2. Right-click the desired site from the Groups window.
3. Select `Delete` from the menu that appears.

   A dialog box appears, asking you to confirm your decision to delete the site.
4. Click `Yes`.

The Mobile Manager removes the site from its group and the Map pane, and adds it to the Delete Sites group.

To restore a site from the Delete Sites group:

1. Open the Enterprise Administrator.
2. Right-click the desired site from the Deleted Sites group in the Groups window.
3. Select `Restore` from the menu that appears.

The site is now available to be added back to a group on your network. See *Adding Sites to Groups* on page 58 for more information.

To permanently delete a site from your network:

NOTE Once you delete a site, all data associated with that site is permanently removed and cannot be recovered.

---

1. Open the Enterprise Administrator.
2. Right-click the desired site from the Deleted Sites group in the Groups window.
3. Select `Delete` from the menu that appears.

   A dialog box appears, asking you to confirm that you want to permanently delete the site.
4. Click `Yes`.

The Mobile Manager permanently deletes the site from your network.

Locating Sites

As you manage your wireless network, you might find it necessary to locate a specific site to make changes or verify settings. You can locate sites using either the Groups window or the Monitor Activity view.

To locate a site within the Groups window:

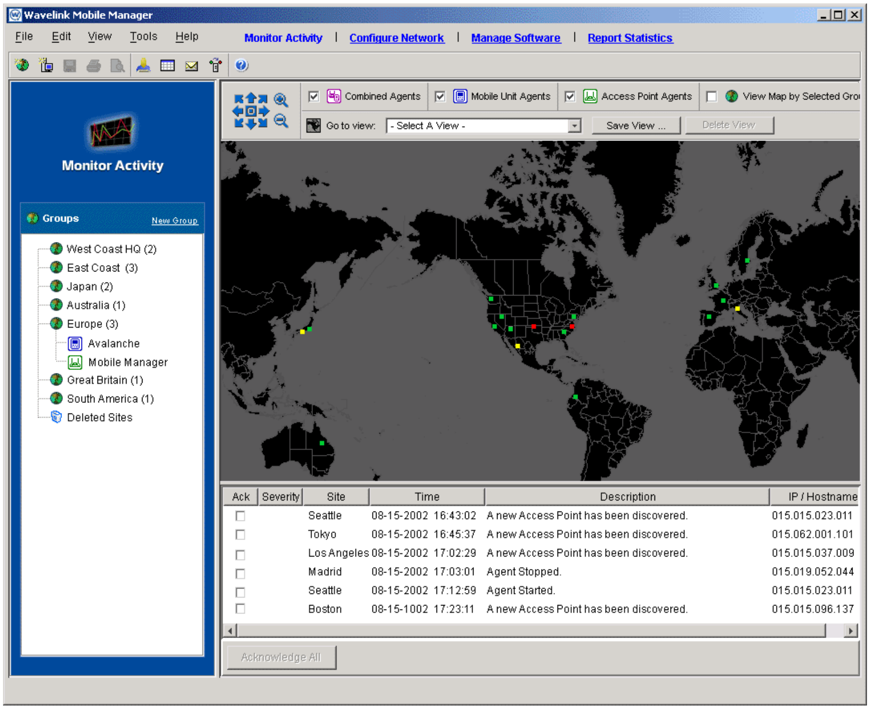
1. Locate the site's group within the Groups window.
2. Click the [+] icon next to the group.

   The sites assigned to that group appear beneath the group.
3. Select the desired site.

To locate a site within the Monitor Activity view:

1. Click `Monitor Activity` from the Enterprise Administrator's toolbar.

   The Monitor Activity view appears.



Ack	Severity	Site	Time	Description	IP / Hostname
☐		Seattle	08-15-2002 16:43:02	A new Access Point has been discovered.	015.015.023.011
☐		Tokyo	08-15-2002 16:45:37	A new Access Point has been discovered.	015.062.001.101
☐		Los Angeles	08-15-2002 17:02:29	A new Access Point has been discovered.	015.015.037.009
☐		Madrid	08-15-2002 17:03:01	Agent Stopped.	015.019.052.044
☐		Seattle	08-15-2002 17:12:59	Agent Started.	015.015.023.011
☐		Boston	08-15-1002 17:23:11	A new Access Point has been discovered.	015.015.096.137

Figure 4-10. *The Monitor Activity view*

2 Locate the geographic region for the site in the Map pane.

If the Map pane does not display the site's geographic region, use the navigation arrows located in the top-left corner of the Map window to manipulate the map until the correct region appears.

3 If necessary, use the zoom buttons located next to the navigation arrows to control the magnification of the Map window.

4 Select the desired site.

Each site on the network appears as either a gray, green, yellow, or red square. The name of each site appears when you place the mouse pointer over it.

If multiple sites reside within the same geographical area, they appear as a single square in the Map pane. In this situation, when you place the mouse over the square, the Map pane lists the sites represented by that location.

To locate a site from within a group of sites:

1 Click `Monitor Activity` from the Enterprise Administrator's toolbar.

The Monitor Activity view appears.

2 Locate the square that represents multiple sites.

If you are unsure as to which square represents multiple sites, locate the general geographic region for the site. Place your mouse over each square. If the square represents only one site, the name of that site appears over the square. If the square represents more than one site, a list of those sites within that location appears.

3 Right-click the square.

A menu appears that displays the different sites available. You can then select the site to access more information about it.

Relocating Sites

Occasionally, you might need to relocate a site in the Maps pane. The Mobile Manager makes it easy for you to quickly move a site from one location to another without disrupting communications between the Enterprise Administrator and the site.

To relocate a site:

1 Click `Monitor Activity` from the Enterprise Administrator's toolbar.

The Monitor Activity view appears.

2 Right-click on the site that you want to relocate.

3 Select `Relocate` from the menu that appears.

The site attaches to the mouse pointer, allowing you to move it to a new location in the Maps pane.

4 Click the location in the Maps pane to which you want to move the site.

The site detaches from the mouse pointer and remains fixed on the new location.

Configuring Components at the Site Level

Although you manage much of your wireless network with the Enterprise Administrator, certain sites might require additional configuration or management. To accommodate this need, you can access two tools from the Enterprise Administrator: the Mobile Manager Site Administrator, and the Avalanche Management Console. These tools allow you to fine-tune your wireless network by configuring your wireless network components and mobile device software at the site level.

Accessing Site Tools

You can access site tools in one of the following ways:

- Double-click a Mobile Manager or an Avalanche node in the group tree
- Right-click a site node in the group tree, then select `Site Tool` from the menu that appears
- Right-click a site in the map, then select `Connect To Service` in the popup menu
- Select a site, then select `Site Tool` from the **Tools** menu

In all cases, you must select whether you want to open the Mobile Manager Site Administrator, or the Avalanche Management Console. After you make your selection, the site tool appears in a separate window on your desktop.

NOTE When you close the Enterprise Administrator, the Mobile Manager Site Administrator automatically closes; however, the Avalanche Management Console will remain open.

See the *Mobile Manager Users Guide* and the *Avalanche Manager Users Guide* for more information on the features of the Administrator application.

Site Management and the Enterprise Administrator

To ensure that your wireless network is managed correctly, it is important to understand the relationship between the configurations established using the Enterprise Administrator, and those established using a site tool such as the Mobile Manager Site Administrator or the Avalanche Management Console. Because the Enterprise Administrator is designed to distribute wireless device settings across your entire network, it can conflict with settings applied to a specific site. These conflicts can be easily avoided, however, by using the following guidelines when applying device configurations at the site level:

- Software collections created in the Enterprise Administrator will override any software collections of the same name on the site level. By verifying that software collections specific to a single site has a unique name, you can ensure that the Enterprise Administrator will not override it.
- IP addresses can be assigned either by the Enterprise Administrator or by a site tool, but not both. Consequently, you must decide before you assign IP addresses if you want to manage them centrally or at the site level.
- WEP and WEP rotation settings assigned at the enterprise level will override any corresponding settings at the site level.
- The Enterprise Administrator is designed to apply configuration settings to groups of sites. To configure an individual site from the Enterprise Administrator, you can do so by creating a group that contains only that site and applying settings to that group.

Adding Groups

You can add as many groups to the Enterprise Administrator as necessary to mange your wireless network effectively.

NOTE The Enterprise Administrator is designed to apply configuration settings to groups of sites. To configure an individual site from the Enterprise Administrator, you can do so by creating a group that contains only that site and applying settings to that group.

To add a group:

1. Select `New Group` from the **File** menu.

   Alternatively, you can right-click within the Groups window and select `New Group` from the menu that appears.

   A new group appears within the Groups window.

2. Type the name of the new group.

3 Press `Enter`.

Renaming Groups

Typically, the name of the group indicates the types of sites it contains. For example, a group named “Seattle” would contain sites located in the Seattle area.

If you decide to rename a group, you can do so at any time.

To rename a group:

1 Right-click the group from the Groups window.

2 Select `Rename` from the menu that appears.

A cursor appears within the group name, allowing you to edit it as needed.

3 Rename the group.

4 On your keyboard, press `Enter`.

Deleting Groups

You can delete obsolete groups from the Enterprise Administrator at any time.

A site associated with a group automatically returns to the *Add Sites to Group* dialog box when you delete that group.

NOTE Deleting a group is permanent and cannot be undone without recreating the entire group.

To delete a group:

1 Right-click the group from the Groups window.

2 Select `Delete` from the menu that appears.

A dialog box appears, asking you to confirm that you want to delete the group.

3 Click `Yes` to delete the group.

Adding Sites to Groups

One of the benefits to creating groups within the Enterprise Administrator is that you can add sites to those groups. As a result, when you make changes to a group's configuration settings, those changes can be applied to all sites assigned to that group.

You can add as many sites to a group as needed.

To add a site to a group:

1 Select the group from the Groups window.

2 Select `Add Site to Group` from the **File** menu.

The *Add Site To Group* dialog box appears.

3 Select the one or more sites for the group by enabling the appropriate check box in the Select column.

4 Click `Add`.

The selected sites now appear under the selected group.

Removing Sites from Groups

As you manage your wireless network, you might decide that certain sites do not belong with the group to which they are assigned. When this situation occurs, you can remove those sites from the group.

NOTE When you remove a site from a group, the site retains the configuration values set for the group until you either assign the site to a new group or manually modify it.

To remove a site from a group:

1 Right-click the site from within the Groups window.

2 Select `Unassign Site` from the menu that appears.

The Enterprise Administrator removes the site from the group and adds it to the list found in the *Add Site To Group* dialog box.

Chapter 5: Managing Network Settings

The Configure Network view of the Enterprise Administrator includes the Network Settings tab. This tab contains options that apply to all wireless devices on your network, regardless of hardware type.

With the Network Settings tab, you can configure the following parameters for your wireless devices:

- ESS IDs
- IP address assignments

This section contains the following topics:

- Assigning ESS IDs
- Managing IP Addresses
- Deploying Network Settings

Assigning ESS IDs

For mobile devices and Access Points to communicate, they must share a common ESS ID. An ESS ID is a unique identifier that used to organize mobile device-to-Access Point associations. This identifier helps prevent mobile devices that might belong to other wireless networks from accidentally associating with Access Points within your organization.

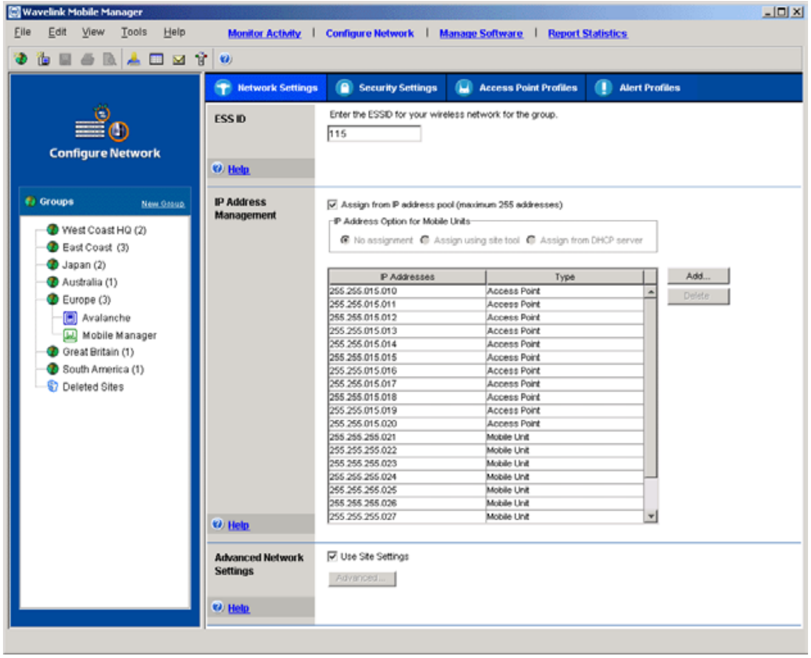
To assign an ESS ID:

1. Select a group from the Groups window.

   The ESS ID that you assign will apply to all mobile devices and Access Points managed within the selected group.

2. Select `Configure Network`.

3. Click the Network Settings tab.



ESS ID

Enter the ESSID for your wireless network for the group.

115

IP Address Management

☑ Assign from IP address pool (maximum 255 addresses)

IP Address Option for Mobile Units

● No assignment ○ Assign using site tool ○ Assign from DHCP server

IP Addresses	Type
255.255.015.010	Access Point
255.255.015.011	Access Point
255.255.015.012	Access Point
255.255.015.013	Access Point
255.255.015.014	Access Point
255.255.015.015	Access Point
255.255.015.016	Access Point
255.255.015.017	Access Point
255.255.015.018	Access Point
255.255.015.019	Access Point
255.255.015.020	Access Point
255.255.255.021	Mobile Unit
255.255.255.022	Mobile Unit
255.255.255.023	Mobile Unit
255.255.255.024	Mobile Unit
255.255.255.025	Mobile Unit
255.255.255.026	Mobile Unit
255.255.255.027	Mobile Unit

Advanced Network Settings

☑ Use Site Settings

Figure 5-1. *The Network Settings Tab of the Configure Network View*

4 Type the identifier that you want to use in the text box located within the ESS ID pane.

5 Select `Save Group` from the **File** menu.

The Mobile Manager will assign the new ESS ID to wireless devices during the next network settings deployment event. See *Deploying Network Settings* on page 70 for more information on deploying network settings.

Managing IP Addresses

The Enterprise Administrator allows you to control what IP addresses are available to a specific group. These IP addresses are based on the subnet mask established on the site level. By using the subnet mask, you can add or remove IP addresses regardless of the IP address of each subnet within a group.

Overview of Assigning IP Addresses

With the Enterprise Administrator, you create ranges of IP addresses that are available to each Agent on the network. These ranges are a combination of the group's subnet mask, which typically consists of one or more octets in the IP address, and the defined range, which typically consists of at least the last octet in the IP address. After you create a range of IP addresses for a group, each Agent within that group receives the defined range and replaces the subnet mask octets with octets appropriate to that Agent's subnet.

For example, a group consists of two sites. The first site has a subnet of 128.52.7.0. The second site has subnet of 125.103.18.0. If you create an IP address range between 1 and 3, the IP Address list displays the following:

```
255.255.255.1

255.255.255.2

255.255.255.3
```

When these IP address masks are deployed to the group, each Agent on the site configures the IP addresses to match its subnet. In this example, the first site would create the following:

```
128.52.7.1

128.52.7.2

128.52.7.3
```

The Agent on the second site in the group would use the same IP address range to create the following:

```
125.103.18.1

125.103.18.2

125.103.18.3
```

This method allows you to create a large number of IP addresses without requiring you to track the various subnets on the network.

Configuring IP Addresses for Mobile Devices

Within the IP Address Management pane, you have several methods of configuring IP addresses for mobile devices. The exact method you select depends on the configuration of your overall wireless network.

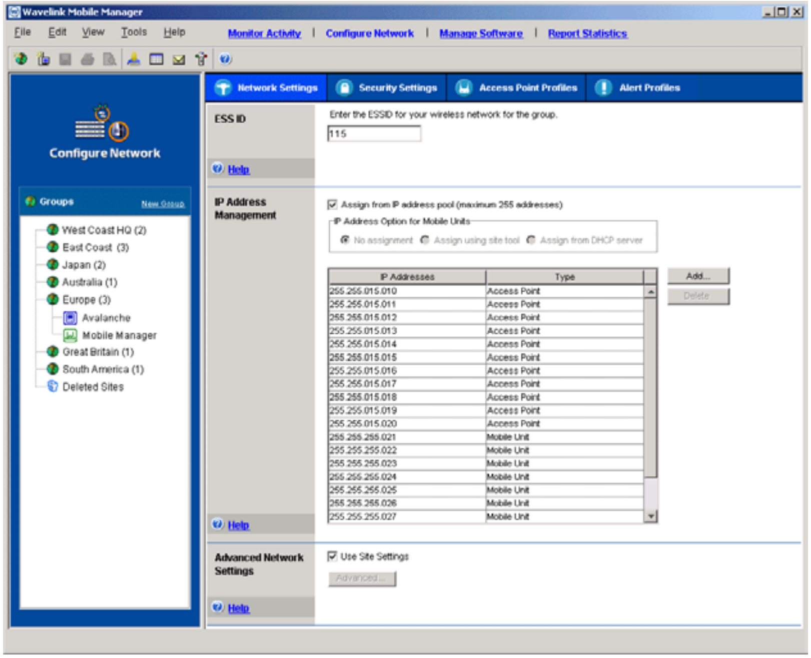
The options available for assigning IP addresses to mobile devices are:

- Using an IP address pool from the Enterprise Administrator, indicated by enabling the **Assign from IP Address Pool** checkbox
- Assigning at the device level, indicated by selecting the **No Assignment** option
- Using the Avalanche Management Console at the site level, indicated by selecting the **Assign Using Site Tool** option
- Using a DHCP server, as indicated by selecting the **Assign from DHCP Server** option

Adding IP Addresses

The Enterprise Administrator allows you to add multiple IP addresses to a group at the same time.

IP addresses generated using the Enterprise Administrator are IP address masks, which are turned into actual IP addresses on a per-Agent basis. If you remove an IP address mask from the Enterprise Administrator, each affected Agent removes the corresponding IP address from its IP address pool. See *Overview of Assigning IP Addresses* on page 63 for information on how the Enterprise Administrator deploys IP addresses on an enterprise-wide level.



ESS ID

Enter the ESSID for your wireless network for the group.

115

IP Address Management

☑ Assign from IP address pool (maximum 255 addresses)

IP Address Option for Mobile Units

● No assignment ○ Assign using site tool ○ Assign from DHCP server

IP Addresses	Type
255.255.015.010	Access Point
255.255.015.011	Access Point
255.255.015.012	Access Point
255.255.015.013	Access Point
255.255.015.014	Access Point
255.255.015.015	Access Point
255.255.015.016	Access Point
255.255.015.017	Access Point
255.255.015.018	Access Point
255.255.015.019	Access Point
255.255.015.020	Access Point
255.255.255.021	Mobile Unit
255.255.255.022	Mobile Unit
255.255.255.023	Mobile Unit
255.255.255.024	Mobile Unit
255.255.255.025	Mobile Unit
255.255.255.026	Mobile Unit
255.255.255.027	Mobile Unit

Advanced Network Settings

☑ Use Site Settings

Figure 5-2. *The Network Settings Tab of the Configure Network View*

NOTE The subnet mask for a group determines how many octets you can customize when creating a range of IP addresses. For example, if a subnet mask uses the first three octets, you can use only the last octet to create IP addresses.

To add a range of IP addresses:

1 Select a group from the Groups window.

The IP addresses that you create will apply to all mobile devices and Access Points managed within the selected group.

2 Select `Configure Network`.

3 Click the Network Settings tab.

4 Enable the **Assign from IP Address Pool** checkbox.

This checkbox is located within the IP Address Management pane.

5 Click `Add`.

The *IP Range* dialog box appears. This dialog box contains two editable text boxes—a **Start** text box and an **End** text box—which allows you to create a range of IP addresses. Each text box is subdivided into four sections—one for each IP address octet.

The exact number of octets that you can modify depends on other settings within the Enterprise Administrator. By default, the Enterprise Administrator does not know the exact octets for the subnets with a group of sites. Consequently, you can modify any of the octets in the **Start** and **End** text boxes—however, any IP addresses that you create that do not match the subnet at a site are ignored by the Agent.

If you decide to set the subnet mask for a group from the Enterprise Administrator, you can only create IP addresses using the octets that correspond to the open octets for the designated subnet mask. See *Modifying Subnet Masks and Gateway IP Addresses* on page 67 for more information.

6 Type the starting address for the IP address range in the **Start** text box.

To add an IP address, click within each octet and type a valid number.

7 Type the ending number for the IP address range in the **End** text box.

To add an IP address, click within each octet and type a valid number.

NOTE You can add a single IP address to the IP address pool by entering the same value in the **Start** and **End** text boxes.

8 Select whether you want these IP addresses to apply to Access Points or mobile devices.

9 Click `OK`.

10 Select `Save Group` from the **File** menu.

The Enterprise Administrator creates a range of IP addresses. These IP addresses consist of the subnet mask for the group plus a number that falls within the range you established. When these IP addresses are distributed to sites, the Agents at those sites automatically replace the subnet mask octets with octets that match the actual subnet for the Agent.

Removing IP Addresses

You can remove an IP address from a group when that address is no longer necessary. However, IP addresses generated using the Enterprise Administrator are IP address masks, which are turned into actual IP addresses on a per-Agent basis. If you remove an IP address mask from the Enterprise Administrator, each affected Agent removes the corresponding IP address from its IP address pool.

For example, if you removed the IP address `255.255.255.43` from a group's IP address pool, all Agents would remove an IP address using `43` as its last octet.

To remove an IP address:

1. Select a group from the Groups window.

   The IP addresses that you create will apply to all mobile devices and Access Points managed within the selected group.

2. Select `Configure Network`.

3. Click the Network Settings tab.

4. Select one or more IP addresses from the IP Address Management pane.

5. Click `Delete`.

6. Select `Save Group` from the **File** menu.

The Enterprise Administrator removes the IP address from the IP address pool.

Modifying Subnet Masks and Gateway IP Addresses

The Enterprise Administrator allows you to modify the subnet mask and gateway IP address for a group. These settings override their corresponding settings at the site level.

NOTE Because subnet masks and gateway IP addresses frequently vary from site to site, it is recommended that you modify these settings from the Enterprise Administrator only if every site within a selected group uses the same network configuration.

Typically, it is recommended that you allow subnet masks and gateway IP addresses to be set at the site level. If you decide you want to set subnet masks using the Enterprise Administrator, the IP addresses that you can add to an IP address pool is restricted by the subnet mask you create. See *Adding IP Addresses* on page 64 for more information.

To use site settings for subnet masks and gateway IP addresses:

1 Select a group from the Groups window.

The IP addresses that you create will apply to all mobile devices and Access Points managed within the selected group.

2 Select `Configure Network`.

3 Click the Network Settings tab.

4 Enable the **Use Site Settings** checkbox.

5 Select `Save Group` from the **File** menu.

To modify a subnet mask or gateway IP address:

1 Select a group from the Groups window.

The IP addresses that you create will apply to all mobile devices and Access Points managed within the selected group.

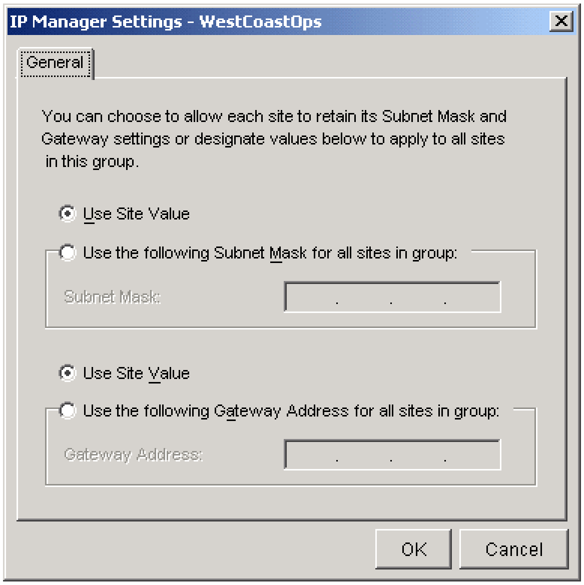
2 Select `Configure Network`.

3 Click the Network Settings tab.

4 Click `Advanced`.

This button is located in the Advanced Network Settings pane. If this button is disabled, you can enable it by disabling the **Use Site Settings** checkbox.

The *Advanced Network Settings* dialog box appears.



IP Manager Settings - WestCoastOps

General

You can choose to allow each site to retain its Subnet Mask and Gateway settings or designate values below to apply to all sites in this group.

● Use Site Value

○ Use the following Subnet Mask for all sites in group:

Subnet Mask: . . .

● Use Site Value

○ Use the following Gateway Address for all sites in group:

Gateway Address: . . .

Figure 5-3. *The IP Manager Settings Dialog Box*

5 If you want the group to use the subnet mask defined at the site level, enable the **Use Site Value** option.

If you want to define a subnet mask, enable the **Use the Following Subnet Mask for All Sites In Group** option, then type the subnet mask address in the **Subnet Mask** text box.

6 If you want the group to use the gateway IP address defined at the site level, enable the **Use Site Value** option.

If you want to define a gateway IP address, enable the **Use the Following Gateway Address for All Sites In Group** option, then type the gateway IP address in the **Gateway Address** text box.

7 Click `OK`.

8 Select `Save Group` from the **File** menu.

Deploying Network Settings

After you have configured the network settings for a group, you can deploy those settings by using one or more deployment events. If your settings affect Access Points, you use the Deploy Settings to Mobile Manager event. If your settings affect mobile devices, you use the Deploy Settings to Avalanche event.

See *Chapter 13: Deploying Configurations* on page 161 for more information on how to create deployment events.

Chapter 6: Managing Device Software

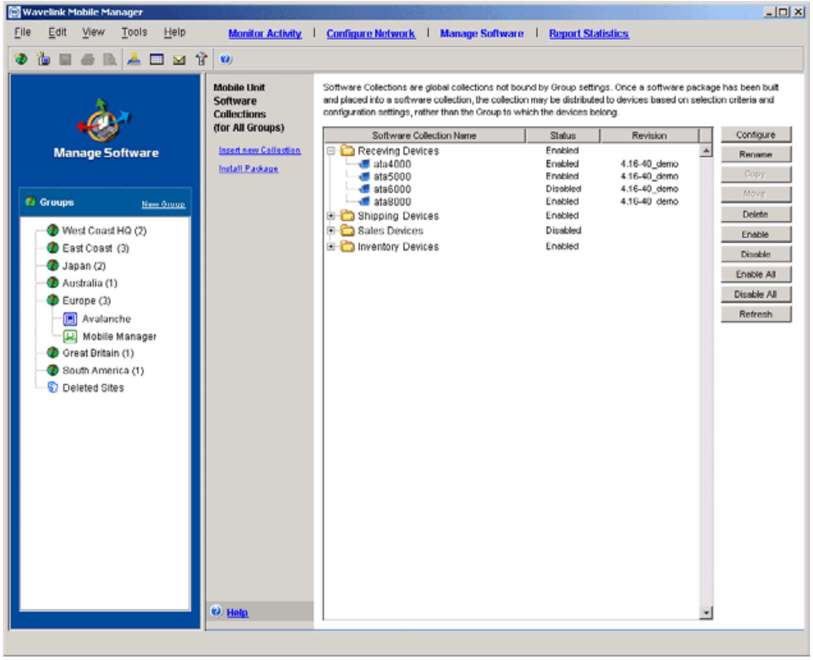
One of the significant challenges when managing a wireless network is determining an effective way to configure, update, and maintain the software installed on mobile devices. Given the level of customization that most wireless applications entail and the wide distribution of mobile device hardware, ensuring that each device has the most up-to-date software is frequently a time- and resource-consuming task. When a wireless network spans an entire enterprise, this challenge becomes both more difficult and more crucial to solve.

The Manage Software view allows you to manage your wireless software in a timely and efficiently. Within this view, you can centrally manage the software that is installed on the mobile devices within your network. Some of the tasks you can accomplish with the Manage Software view include:

- **Install software packages**. A software package is a collection of application files associated with a single mobile device. When a software package is deployed to a mobile device, that device receives all of these files, ensuring that it can use the application effectively.

- **Create software collections**. A software collection contains one or more software packages. You can configure each software collection so that the packages it contains apply only to certain mobile devices.

- **Define selection criteria**. The Manage Software view allows you to define specific criteria for each software collection. By defining these criteria, you can instruct the Mobile Manager to deploy a software package only to specific types of mobile devices.



Software Collections are global collections not bound by Group settings. Once a software package has been built and placed into a software collection, the collection may be distributed to devices based on selection criteria and configuration settings, rather than the Group to which the devices belong.

Software Collection Name	Status	Revision
Receving Devices	Enabled	
ata4000	Enabled	4.16-40_demo
ata5000	Enabled	4.16-40_demo
ata6000	Disabled	4.16-40_demo
ata8000	Enabled	4.16-40 demo
Shipping Devices	Enabled	
Sales Devices	Disabled	
Inventory Devices	Enabled	

Figure 6-1. *The Manage Software View*

This section describes how to install software packages, create software collections, define which mobile devices receive which software, and how to deploy software out to your mobile devices.

NOTE Unlike other configuration settings within the Enterprise Administrator, such as creating an Access Point profile or defining an Access Control List, the settings you assign in the Manage Software view apply to all groups within the Enterprise Administrator.

This section contains the following topics:

- Software Packages
- Software Collections
- Activating Software
- Deleting Packages and Collections

- Refreshing the Manage Software View
- Deploying Software

Software Packages

A software package is a collection of application files associated with a single mobile device. When a software package is deployed to a mobile device, that device receives all of these files, ensuring that it can use the application effectively. Software packages are organized into groups, called software collections, that allow you to determine which mobile devices receive specific applications. See *Software Collections* on page 76 for more information on managing software collections.

This section includes information on managing software packages, including:

- Installing packages
- Moving packages between software collections
- Copying packages from one collection to another
- Configuring packages

Installing Packages

Software packages are available for download from the Wavelink Web site, www.wavelink.com. The exact packages you need to install depends on the needs of your organization—your Wavelink sales representative can assist you in finding the packages you need. Once you download a software package, you can install it using the Enterprise Administrator.

NOTE Before you install a package, you must have a software collection that will contain it. See *Software Collections* on page 76 for more information.

When you first install a software package, it appears as disabled within the Manage Software view. Before you deploy the package to your network, you must enable it. See *Activating Software* on page 89 for more information.

To install a package:

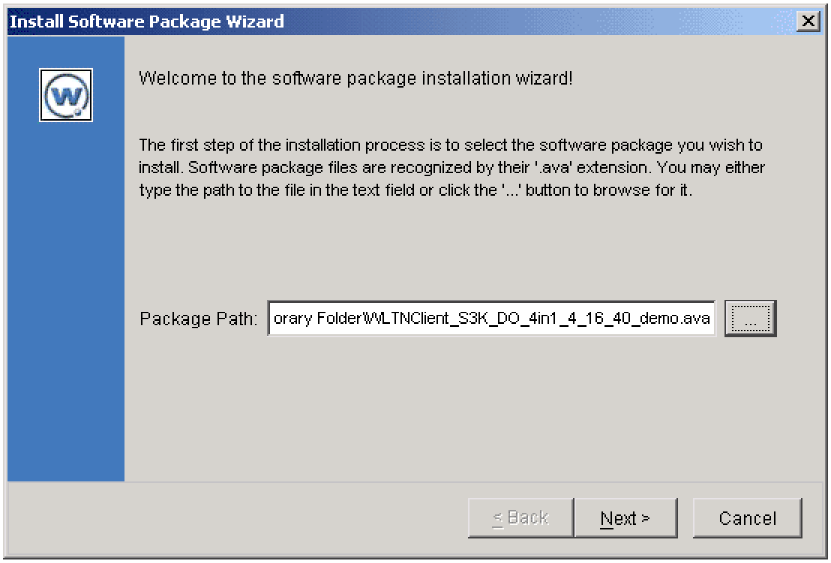
1 From the Enterprise Administrator, select `Manage Software`.

2 If you have yet to create a software collection for the software package, create that collection.

See *Creating Collections* on page 76 for more information.

3 Select `Install Package`.

The Install Software Package Wizard starts.



Install Software Package Wizard

Welcome to the software package installation wizard!

The first step of the installation process is to select the software package you wish to install. Software package files are recognized by their '.ava' extension. You may either type the path to the file in the text field or click the '...' button to browse for it.

Package Path: orary Folder\WLTNClient_S3K_DO_4in1_4_16_40_demo.ava

Figure 6-2. *The Install Software Package Wizard Dialog Box*

4 Type the path to the software package in the **Package Path** text box and click `Next`..

You can also navigate to the package by clicking `[...]`.

5 Select a software collection for the package and click `Next`.

The package is installed into the selected collection.

6 Click `Finish`.

Moving Packages

You can use the Enterprise Administrator to move a software package from one collection to another.

To move a package:

1. From the Enterprise Administrator, select `Manage Software`.
2. Select a software package.
3. Click `Move`.

   The *Copy or Move Package* dialog box appears.
4. Select the software collection that will receive the package and click `OK`.

Copying Packages

Depending on your network configuration, a software package can be applicable to multiple software collections. You can use the Enterprise Administrator to copy these packages from one collection to another.

To move a package:

1. From the Enterprise Administrator, select `Manage Software`.
2. Select a software package.
3. Click `Copy`.

   The *Copy or Move Package* dialog box appears.
4. Select the software collection that will receive the package and click `OK`.

Configuring Packages

You can access the configurable options for a package directly from the Manage Software view. The exact options available to you vary depending on the type of package that you have installed.

To configure a package:

1. From the Enterprise Administrator, select `Manage Software`.
2. Select a software package.
3. Click `Configure`.

   A dialog box appears, allowing you to configure the software package.

See the documentation for your client software for more information on configuration options.

Software Collections

A software collection contains one or more software packages. You can configure each software collection so that the packages it contains apply only to certain mobile devices.

Creating Collections

At least one collection is required before you install a software package.

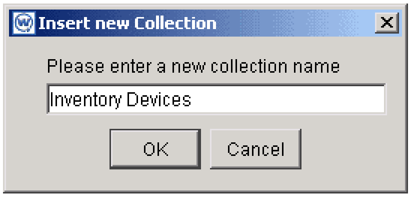
When you first create a software collection, it appears as disabled within the Manage Software view. Before you deploy the collection to your network, you must enable it. See *Activating Software* on page 89 for more information.

To create a collection:

1 From the Enterprise Administrator, select `Manage Software`.

2 Select `Insert New Collection`

The *Insert New Collection* dialog box appears.



Inventory Devices

Figure 6-3. *The Insert New Collection Dialog Box*

3 Type a name for the collection in the text box and click `OK`.

Configuring Collections

A set of rules called selection criteria define which mobile devices receive designated updates. The selection criteria determines which mobile devices can receive the software packages contained in the collection. Additional selection criteria is typically associated with the software packages themselves, further restricting the distribution of the package, but package criteria is built-in to the package at the time of its creation.

NOTE The selection criteria associated with a particular software package is set by Wavelink or the third-party application developer and, once created, the criteria associated with a package cannot be modified.

A selection criteria string is a single expression (much like a mathematical expression) that takes a set of variables corresponding to different aspects of a mobile device and compares them to fixed values. The syntax includes parentheses and boolean operators to allow flexible combination of multiple variables.

By default, the selection criteria string for a software collection is empty, which allows all packages within the collection to download to all mobile devices. You can modify this criteria at any time.

You can use the selection criteria wizard to build a valid selection criteria string. You can also use the selection criteria wizard to test the selection criteria string on specific mobile devices that appear in the List View of the Management Console.

NOTE Selection criteria for a software collection are applied to all sites containing that collection. It is highly recommended that you verify that the selection criteria is applicable to all sites with that collection before you implement it.

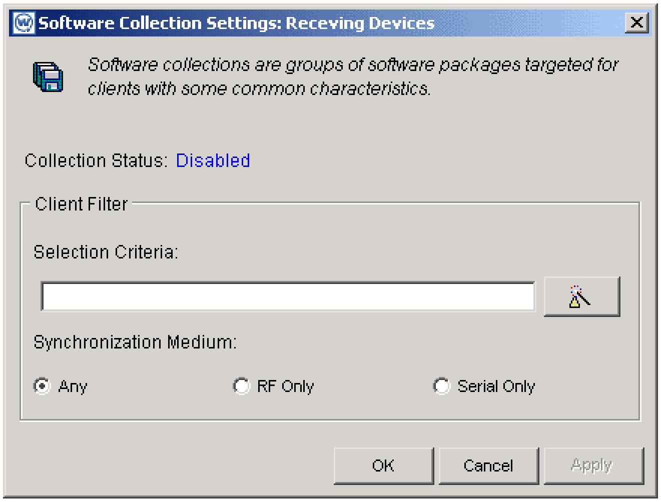
To open the Selection Criteria Wizard for a software collection:

1 From the Enterprise Administrator, select `Manage Software`.

2 Select a software collection.

3 Select `Configure`.

The *Software Collection Settings* dialog box appears.



Software Collection Settings: Receving Devices

Software collections are groups of software packages targeted for clients with some common characteristics.

Collection Status: Disabled

Client Filter

Selection Criteria:

Synchronization Medium:

● Any ○ RF Only ○ Serial Only

Figure 6-4. *The Software Collection Settings Dialog Box*

4 Set the desired synchronization option in the **Synchronization Medium** group box.

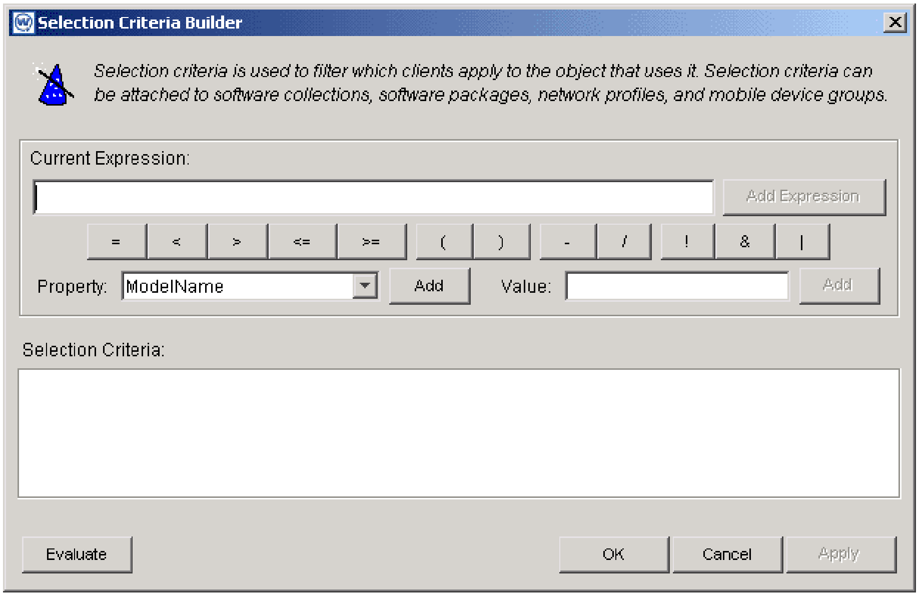
If you want to restrict the software updates associated with the current profile to wireless only, enable the **RF Only** option.

If you want to restrict the software updates associated with the current profile to serial only, enable the **Serial Only** option.

If you want to allow both types of synchronization, enable the **Any** option.

5 Click the **Selection Criteria Wizard** icon.

The *Selection Criteria Builder* dialog box appears.



Selection criteria is used to filter which clients apply to the object that uses it. Selection criteria can be attached to software collections, software packages, network profiles, and mobile device groups.

Property: ModelName

Figure 6-5. *The Selection Criteria Builder Dialog Box*

In this dialog box, you can build the selection criteria string by selecting or typing string elements one element at a time. The string elements include:

- Selection variables such as `ModelName` or `KeyboardName`. These variables determine the type of restriction placed on the package or profile. For example, by using a `ModelName` variable, you can restrict the package or profile to a specific class of mobile devices, based on their model numbers.

NOTE Client properties such as the Terminal ID also function like selection variables. Currently, the selection criteria wizard supports the use of the Terminal ID property only. Additional properties will be supported in future releases.

- Operators such as Eq (=), And (&), and Or (|) that are used to assign a value to a selection variable or to combine multiple variables.

NOTE Parentheses are required when multiple operators are involved. Nesting of parentheses is also allowed.

- Actual values that are assigned to a selection variable. For example, if you assign a value of 3840 to a `ModelName` variable by building the string, ModelName = 3840, then you will restrict packages or profiles to model 3840 mobile devices.

To build the selection criteria string:

1 In the *Selection Criteria Builder* dialog box, select the elements to add to the selection criteria string from the options at the top of the dialog box.

Elements are added in order, from left to right. When you add an element, it appears as the proposed selection criteria in the **Current Expression** text box.

To add a selection variable or property, select the element from the **Property** drop-down list and click `Add`. See *Selection Variables and Properties* on page 81 for a description of the valid selection variables.

To add an operator to the selection criteria string, click the button containing the desired operator. See *Operators* on page 86 for more information.

NOTE Parentheses are not required unless more than one operator is included in the string.

To add a comparison value to the selection criteria string, type it in the **Value** text box and click `Add`. The range of possible values are dependent on the specific selection variable in use. See *Selection Variables and Properties* on page 81 for additional information.

2 Click `Add Expression`.

The selection criteria string appears in the Selection Criteria text box.

3 For each additional element you want to add to the selection criteria string, repeat the preceding steps.

NOTE Due to the potential complexity of long selection criteria strings, it is recommended that you limit the selection criteria to 20 selection variables or less.

4 Click `OK`.

5 Select how you want the Mobile Manager to synchronize the software within this collection on mobile devices.

You can select one of three options: **Any**, which allows the Mobile Manager to use both serial and wireless connections to update software; **RF Only**, which instructs the Mobile Manager to use only wireless connections; and **Serial Only**, which instructs the Mobile Manager to use only serial connections.

6 Click `Apply`.

To test the selection criteria string:

1 Open the *Selection Criteria Builder* dialog box.

2 Verify that a selection criteria string appears in the **Selection Criteria** text box.

3 Click `Evaluate`.

The Mobile Manager checks the selection criteria for any syntactical errors. If an error occurs, a dialog box appears, informing you that you must modify the expression.

Selection Variables and Properties

The selection criteria is based on the use of selection variables and client properties.

NOTE Currently, the Terminal ID is the only client property that can be used in the selection criteria.

You can place numbers and strings directly in the selection criteria string, with or without quotes. Selection variable names are not case sensitive, but the values are case sensitive.

For example, the following selection criteria strings are all valid:

```
modelname=6840
ModelName=6840
ModelName = 6840
ModelName="6840"
```

The following selection criteria strings are valid:

```
series = S
Series = S
```

while the following are not:

```
series = s
Series = s
```

Selection variables and client properties for the selection criteria string are as follows:

`IP`

IP address of the mobile device.

Enter all IP addresses using dotted notation. IP addresses can be compared in three ways:

- Direct comparison with a single IP address. For example, `IP = 10.1.1.1.`
- Comparison with an arbitrary address range. For example, `IP = 10.1.1.5 - 10.1.1.15` (This can also be written as `IP = 10.1.1.5 - 15`.)
- Comparison with a subnet number. This is done by supplying the network number along with the netmask or CIDR value. For example, `IP = 10.1.1.0/255.255.255.0`. Using CIDR notation, this can also be written as `IP = 10.1.1.0/24`.

`MAC`

MAC address of the mobile device.

Enter any MAC Addresses as a string of hexadecimal digits. Dashes or colons between octets are optional. For convenience, you can shorten the address by entering just the rightmost portion (any number of digits, up to 12.) For example:

```
MAC = 00:A0:F8:85:E8:E3
```

Or:

```
MAC = 00A0F885E8E3
```

`ModelName`

The standard model name for a device. This name is often a number but it can be alphanumeric as well. Examples include 6840, 3940, 4040. If the model number is unknown, it appears in one of the views when the mobile device is selected.

The following models are supported:

1040	1740	1746
1840	1846	2740
2840	3140	3143
3540	3840	3843
3940	4040	5040
6140	6143	6840
6843	6940	7240
7540	7940	8140
8940	PTC960	TR1200
VT2400	WinPC	WT2200

Example:

```
Modelname = 6840
```

```
Modelname=3840
```

Spaces around the equal sign is optional.

`KeyboardName`

A string depicting which style of keyboard the mobile device is using (46key, 35key etc.) This variable is not applicable for CE devices.

Example:

```
KeyboardName = 35Key
```

`Series`

The general series of a device. This is a single letter: ‘3’ for Symbol ‘3000’ series mobile devices, ‘7’ for Symbol ‘7000’ series mobile devices, etc.

The following values are supported:

3 = DOS 3000 series

P = DOS 4000 and 5000 series

7 = DOS 7000 series

T = Telxon

C = CE

P = Palm

W = Windows

Example:

```
Series = 3
```

`ModelCode`

A number set by the device manufacturer and used internally by the BIOS to identify the hardware.

The following values are supported:

1 = LRT 38xx/LDT 38xx

2 = VRC39xx/69xx

3 = PDT 31xx /35xx

4 = WSS1000

5 = PDT 6800

6 = PDT 6100

Example:

```
ModelCode <= 2
```

`KeyboardCode`

A number set by the device manufacturer and used internally by the BIOS to identify the keyboard type. This variable is available only for DOS 3000 series mobile devices.

The following values are supported:

0 = 35 key

1 = More than 35 keys/WSS1000

2 = Other terminals with less than 35 keys.

Example:

```
KeyboardCode < 2
```

`Rows`

The number of display rows the mobile device supports. This variable supports values from 1 to 25.

Example:

```
Rows = 6
```

`Columns`

The number of display columns the mobile device supports. This variable supports values from 1 to 80.

Example:

```
Columns = 21
```

`Terminal ID`

This client property is the unique ID for the mobile device that the Avalanche Manager generates. The values assigned by the Mobile Manager start from 1 and increase incrementally.

Example:

```
Terminal ID = 5
```

Operators

All selection criteria strings are evaluated from left to right, without operator precedence. When more than one operator is involved, you must include parentheses in order for the selection criteria string to be evaluated properly.

For example:

```
(ModelName=3840) or ((ModelName=6840) and (KeyboardName=
46Key))
```

NOTE Spaces around operators are optional.

The preceding selection criteria string states that either 3840 mobile devices regardless of keyboard type or 46Key 6840 mobile devices will receive the software package.

The following operators can be used along with any number of parentheses to combine multiple variables.

`Not (!)` Unary operator that negates the boolean value that follows it.

In the following example, all mobile devices with 20 rows receive the software packages within the collection except for those with 35Key keyboards.

```
! (KeyboardName = 35Key) & (Rows = 20)
```

`And (&)` Binary operator that results in TRUE if and only if the expressions before and after it are also both TRUE.

Example:

```
(ModelName=3840) | ((ModelName=6840) &
(KeyboardName= 46Key))
```

`Or (|)` Binary operator that results in TRUE if either of the expressions before and after it are also TRUE.

In this example, either 6840 or 3840 mobile devices can receive the software packages.

```
(ModelName =6840) | (ModelName = 3840)
```

Eq (=)

Binary operator that results in TRUE if the two expressions on either side of it are equivalent.

Example:

ModelName = 6840

>

Binary operator that results in TRUE if the expression on the left is greater than the expression on the right.

Example:

Rows > 15

<

Binary operator that results in TRUE if the expression on the left is less than the expression on the right.

Example:

Rows < 5

>=

Binary operator that results in TRUE if the expression on the left is greater than or equal to the expression on the right.

Example:

Rows >= 10

<=

Binary operator that result in TRUE if the expression on the left is less than or equal to the expression on the right.

Example:

Rows <= 20

Renaming Collections

You have the option to rename a software collection at any time.

To rename a collection:

1 From the Enterprise Administrator, select Manage Software.

2 Select a software collection.

3 Click Rename.

The *Rename Collection* dialog box appears.

4 Type a new name for the collection and click `OK`.

Activating Software

By default, software collections and software packages are disabled when you first create them. This setting allows you to adjust any configurations you want to make before the Mobile Manager deploys the software to mobile devices.

Enabling Collections and Packages

When a software collection or package is ready for deployment, you must use the **Enable** option to activate it.

To enable a single software collection or package:

1 From the Enterprise Administrator, select `Manage Software`.

2 Select a software package or collection.

3 Click `Enable`.

To enable all software collections or packages:

1 From the Enterprise Administrator, select `Manage Software`.

2 Click `Enable All`.

Disabling Collections and Packages

Disabling a collection or package prevents the Mobile Manager from deploying updates of it to mobile devices.

To disable a single software collection or package:

1 From the Enterprise Administrator, select `Manage Software`.

2 Select a software package or collection.

3 Click `Disable`.

To disable all software collections or packages:

1 From the Enterprise Administrator, select `Manage Software`.

2 Click Disable All.

Deleting Packages and Collections

In the event that a package or collection becomes obsolete, you can remove it entirely from the Manage Software view.

To delete a package or collection:

1 From the Enterprise Administrator, select Manage Software.

2 Select a software package or collection.

3 Click Delete.

Refreshing the Manage Software View

Although the Manage Software view is periodically updated by the Mobile Manager, you have the option of refreshing it manually. This feature is useful if multiple individuals have access to the Enterprise Administrator.

To refresh the Manage Software view:

1 From the Enterprise Administrator, select Manage Software.

2 Click Refresh.

Deploying Software

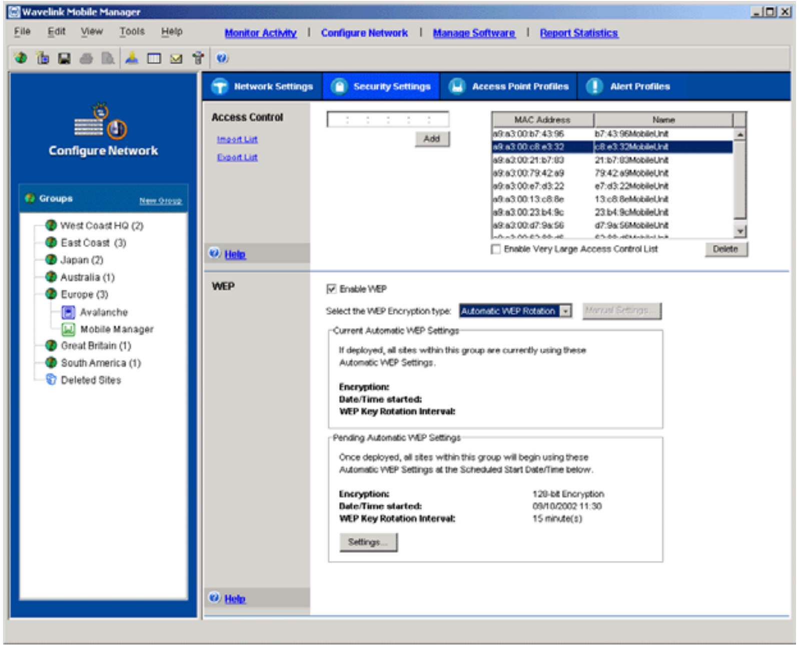
After you have configured the software packages and collections for mobile devices, you can deploy those settings by using the Deploy Settings to Avalanche event.

See *Chapter 13: Deploying Configurations* on page 161 for more information on how to create deployment events.

Chapter 7: Managing Security Settings

Security settings are an integral part of any wireless network setup. Because both Access Points and mobile devices constantly broadcast information, it is important to ensure that only authorized devices receive and transmit data across your network.

The Enterprise Administrator provides you with the means to configure two primary methods of restricting wireless communications. The first method is creating an Access Control List. This list consists of mobile device MAC addresses. Only devices whose MAC addresses appear in the Access Control List are allowed to associate with an Access Point. The second method is Wired Equivalent Privacy, or WEP. WEP is an encryption technology that helps prevent unauthorized access to wireless communications. There are two types of WEP implementations available: static WEP, which is the original method used, and the Wavelink-designed automatic WEP rotation, a more robust WEP implementation that thoroughly protects wireless data over the air.



MAC Address	Name
a9:a3:00:b7:43:96	b7:43:96MobileUnit
a9:a3:00:c8:e3:32	c8:e3:32MobileUnit
a9:a3:00:21:b7:83	21:b7:83MobileUnit
a9:a3:00:79:42:a9	79:42:a9MobileUnit
a9:a3:00:e7:d3:22	e7:d3:22MobileUnit
a9:a3:00:13:c8:8e	13:c8:8eMobileUnit
a9:a3:00:23:b4:9c	23:b4:9cMobileUnit
a9:a3:00:d7:9a:56	d7:9a:56MobileUnit

□ Enable Very Large Access Control List

Delete

☑ Enable WEP

Select the WEP Encryption type: Automatic WEP Rotation

Manual Settings...

Current Automatic WEP Settings

If deployed, all sites within this group are currently using these Automatic WEP Settings.

Encryption:
Date/Time started:
WEP Key Rotation Interval:

Pending Automatic WEP Settings

Once deployed, all sites within this group will begin using these Automatic WEP Settings at the Scheduled Start Date/Time below.

Encryption: 128-bit Encryption
Date/Time started: 09/10/2002 11:30
WEP Key Rotation Interval: 15 minute(s)

Settings...

Figure 7-1. *The Security Settings Tab of the Configure Network View*

This section contains the following information:

- Building Access Control Lists
- Wired Equivalent Privacy (WEP)
- Automatic WEP Rotation
- Extensible Authentication Protocol (EAP)
- Advanced Security Options
- Deploying Security Settings

Building Access Control Lists

Access Points support a feature called the Access Control List. This list contains the MAC addresses of mobile devices that are allowed to access your wireless network. Only those mobile devices that are on an Access Control List can communicate with your network through an Access Point.

While Access Control Lists can provide a great deal of security for an Access Point, they are limited in the number of MAC addresses they can contain. As a result, their use can be restrictive in enterprise-wide environments that consist of thousands of mobile devices.

To address this issue, the Mobile Manager supports the Very Large Access Control List, which can support an unlimited number of MAC addresses. This list is identical to the Access Control List, but is supported by the Agent as opposed to an individual Access Point. With the Very Large Access Control List enabled for a group, the Access Points refer to the Agent to know which mobile devices are allowed access to the network.

If security is a high priority within your organization, it is highly recommended that you configure the Very Large Access Control List for each group within your wireless network. When you add one or more MAC addresses to a group’s Very Large Access Control List, the Access Points within that group check the MAC address of each mobile device against the MAC addresses listed in the Agent’s Very Large Access Control List. If the Access Point finds a match, it allows the mobile device to connect to the network. If the Access Point does not find a match, it refuses to communicate with the mobile device.

NOTE Mobile devices connecting to a Cisco-Aironet Access Point can connect regardless of whether their MAC addresses are listed in the Access Point's Access Control List. However, the Access Point does not forward any information to the network unless the mobile device is listed in the Access Control List.

By default, the Very Large Access Control List for a group is disabled, allowing any mobile device to connect to Agents within that group.

NOTE You can configure the Access Point-supported Access Control Lists at the site level. See the *Mobile Manager Users Guide* for more information.

Adding MAC Addresses

The Enterprise Administrator allows you to add as many mobile device MAC addresses to a group's Very Large Access Control List as your network demands.

To add a MAC address:

1 Select a group from the Groups window.

The Access Control List that you create will apply to all mobile devices and Access Points managed within the selected group.

2 Select `Configure Network`.

3 Click the Security Settings tab.

4 Enable the **Enable Very Large Access Control List** checkbox.

5 Type a MAC address in the text box located in the Access Control pane.

6 Click `Add`.

The MAC address appears in the table.

This list contains two columns, MAC Address and Name.

7 Select `Save Group` from the **File** menu.

NOTE When you add a new MAC address to a Very Large Access Control List, the Enterprise Administrator automatically assigns the address a default name.

Modifying Very Large Access Control List Entries

After you build a Very Large Access Control List for a group, you can modify its entries by changing their MAC addresses or device names.

To modify the name of an Access Control List entry:

1 Select a group from the Groups window.

The Access Control List that you create will apply to all mobile devices and Access Points managed within the selected group.

2 Select `Configure Network`.

3 Click the Security Settings tab.

4 Select an entry from the Very Large Access Control List.

5 Double-click the name for the entry.

A cursor appears within the name entry, allowing you to type a new device name.

6 Type the new name.

The Very Large Access Control List table updates to display your changes.

7 Select `Save Group` from the **File** menu.

Removing Very Large Access Control List Entries

You can remove a mobile device’s MAC address from a Very Large Access Control List at any time, preventing that device from connecting to Access Points within that group.

To remove a Very Large Access Control List entry:

1 Select a group from the Groups window.

The Access Control List that you create will apply to all mobile devices and Access Points managed within the selected group.

2 Select `Configure Network`.

3 Click the Security Settings tab.

4 Select the entry you want to remove.

5 Click `Delete`.

The Enterprise Administrator deletes the entry from the Very Large Access Control List.

6 Select `Save Group` from the **File** menu.

Importing and Exporting Access Control List Files

You can import and export Very Large Access Control List entries using comma-delimited text files (either .csv or .txt files). These import and export commands allow you to apply the same Very Large Access Control List to multiple groups or save records of entries for backup purposes.

To export a Very Large Access Control List file:

1 Select a group from the Groups window.

The Access Control List that you create will apply to all mobile devices and Access Points managed within the selected group.

2 Select `Configure Network`.

3 Click the Security Settings tab.

4 Click `Export` from the Very Large Access Control List pane.

A standard *Save* dialog box appears.

5 Navigate to where you want to save the Very Large Access Control List text file.

This file must be either a .csv or .txt file.

6 Click `Save`.

If you want to import a Very Large Access Control List file, you must ensure that the comma-delimited text file is in the correct format. This format is as follows:

```
[MAC Address], [Device Name]
```

Where

- *MAC Address* is the MAC address of approved wireless device
- *Device Name* is a name that identifies the wireless device

NOTE The preceding format is required for both .txt and .csv files. You can add as many MAC addresses as necessary to the comma-delimited file, as long as each entry complies to this format.

To import a Very Large Access Control List file:

1 Select a group from the Groups window.

The Access Control List that you create will apply to all mobile devices and Access Points managed within the selected group.

2 Select `Configure Network`.

3 Click the Security Settings tab.

4 Click `Import` from the Very Large Access Control List pane.

A standard *Open* dialog box appears.

5 Locate and select the text file.

6 Click `Open`.

The Very Large Access Control List pane updates to display the added entries.

7 Select `Save Group` from the **File** menu.

Wired Equivalent Privacy (WEP)

WEP, or Wired Equivalent Privacy, is a protocol for encrypting wireless network communications. You secure your wireless network by assigning either a 40- or 128-bit WEP key. This WEP key is shared between Access Points and mobile devices, allowing them to securely communicate with each other.

NOTE The Mobile Manager only tracks the WEP keys that were assigned to Access Points through the Administrator. Consequently, WEP keys displayed in the Administrator might not match the keys for an Access Point if you modified them from outside of the Mobile Manager.

Types of WEP Key Deployments

The Mobile Manager offers you two methods of deploying WEP keys to your Access Points. First, you can deploy static WEP keys. This type of deployment is the typical method thought of when an organization opts to include WEP as a part of their security processes. However, this method has been shown through numerous studies to be highly vulnerable to decryption.

To prevent unauthorized individuals from decrypting WEP transmissions, the Mobile Manager includes a unique method of deployment: automatic WEP rotation. By deploying the automatic WEP rotation feature, the Mobile Manager rotates and modifies WEP keys on a regular basis, which prevents an attacker from discovering a WEP key and accessing your data.

NOTE Automatic WEP rotation is only available through an Access Point profile. See *Automatic WEP Rotation* on page 99 for more information.

Configuring WEP Keys

The following steps assist you in creating static WEP keys for your wireless network. If you want to use the Mobile Manager's automatic WEP rotation feature, see *Automatic WEP Rotation* on page 99.

To configure WEP keys:

1 Select a group from the Groups window.

The Access Control List that you create will apply to all mobile devices and Access Points managed within the selected group.

2 Select `Configure Network`.

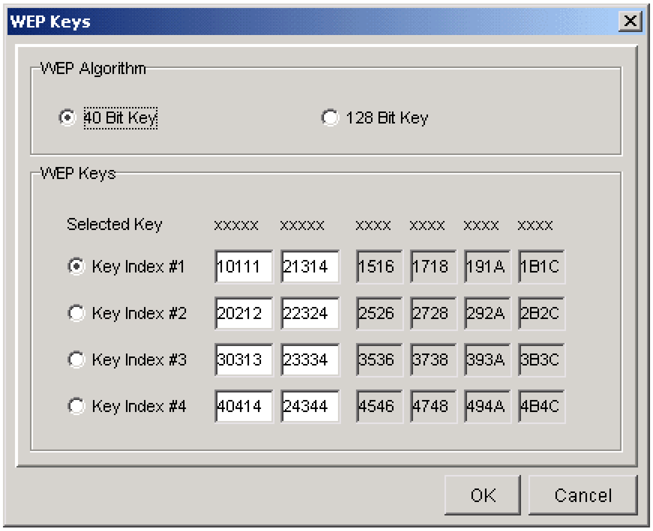
3 Click the Security Settings tab.

4 Enable the **Enable WEP** checkbox.

5 Select `Static WEP` from the **Select the WEP Encryption Type** list.

6 Click `Static Settings`.

The *WEP Keys* dialog box appears.



WEP Keys

WEP Algorithm

● 40 Bit Key ○ 128 Bit Key

WEP Keys

Selected Key	xxxxx	xxxxx	xxxx	xxxx	xxxx	xxxx
● Key Index #1	10111	21314	1516	1718	191A	1B1C
○ Key Index #2	20212	22324	2526	2728	292A	2B2C
○ Key Index #3	30313	23334	3536	3738	393A	3B3C
○ Key Index #4	40414	24344	4546	4748	494A	4B4C

Figure 7-2. *The WEP Keys Dialog Box*

7 Select either the **40 bit** or **128 bit** option.

8 Select one of the four default keys.

To change the value for one of the hex digits in a key, type a new value (between 0-9 and A-F) in the appropriate text box. For example, you could change `10111` to `101F1`. You can change as many digits as necessary to build your WEP key.

9 Click `OK`.

10 Select `Save Group` from the **File** menu.

NOTE You must ensure that any mobile devices that need to connect to an Access Point share the same WEP key as that Access Point. If the keys do not match, the mobile device cannot communicate with the Access Point.

To set the WEP key for a mobile device, refer to the client documentation for that device.

Automatic WEP Rotation

Recent studies have demonstrated significant vulnerabilities in the current implementation of WEP. These vulnerabilities greatly reduce the viability of WEP in securely encrypting wireless transmissions. While new wireless standards are forthcoming to help fortify WEP’s effectiveness, these standards require new hardware that can support the new protocols.

To address the need for wireless data encryption, the Mobile Manager provides a unique feature: automatic WEP rotation. This feature offers two advantages to a wireless network: first, it modifies WEP implementation to dramatically increase the security of wireless transmissions; second, it is designed to work with both current and future wireless communication standards.

NOTE Step-by-step instructions on configuring automatic WEP rotation can be found in the Configuring Automatic WEP Rotation section.

Automatic WEP rotation fortifies WEP implementation on several levels. First, while current WEP implementation uses a single, static WEP key, automatic WEP rotation employs four keys which are rotated at specified intervals. These keys are known by both access points and mobile devices. An intruder attempting to decrypt transmissions using automatic WEP rotation must first determine that multiple keys are in use. To make decrypting WEP keys more difficult, the keys used by access points and mobile devices are staggered. Staggering the WEP keys means that the key sent by an access point is different from the one sent by a mobile device. Because both access points and mobile devices know which keys are authorized, they can communicate securely without using a shared key.

Second, automatic WEP rotation continually rotates old WEP keys out of the approved list of keys, replacing them with new ones. Each rotation interval not only changes the WEP key transmitted by a wireless device; it also changes one of the WEP keys in the WEP key list. Because these WEP keys are staggered, two out of four possible WEP keys are in use at any given time. During each key rotation, one of the unused WEP keys is replaced by a newly-generated key. By setting an appropriate rotation interval (which can vary depending on average wireless network activity), an IT professional can completely prevent an intruder from decrypting wireless transmissions.

The third method automatic WEP rotation uses to secure wireless transmissions is by helping IT professionals generate unique keys. Because automatic WEP rotation requires consistently changing keys, it employs a specific algorithm to create new keys. This algorithm removes the burden of creating new keys from the IT professional. The combination of constant automatic WEP rotation, continual key replacement, and unique key generation creates a secure system in which an organization's wireless transmissions are impervious to decrypting.

Configuring Automatic WEP Rotation

To implement automatic WEP rotation, you use the Security Settings tab located in the Configure Network view.

For mobile devices to employ automatic WEP rotation effectively, they must have the following Avalanche Enablers installed:

DOS	Version 1.61-00 or later
TN	Version 4.16-40 or later
CE	Contact your Wavelink sales representative.

To configure automatic WEP rotation:

1. Select a group from the Groups window.

   The WEP rotation parameters that you set will apply to all mobile devices and Access Points managed within the selected group.

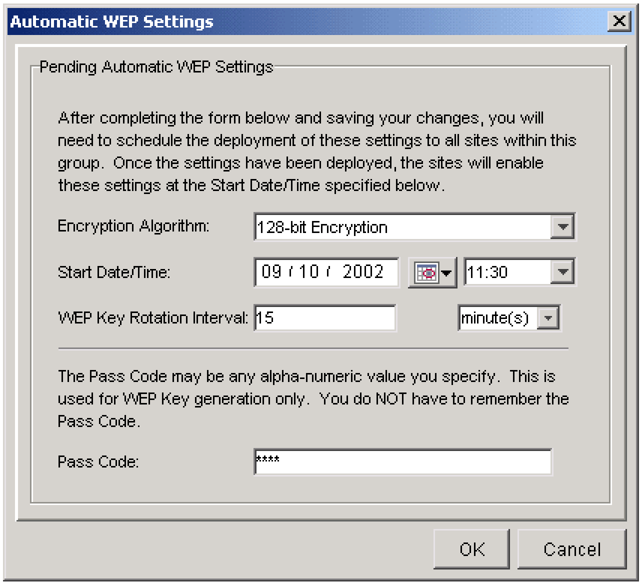
2. Select `Configure Network`.

3. Click the Security Settings tab.

4. Enable the **Enable WEP** checkbox.

5 Select `Automatic WEP Rotation` from the **Select the WEP Encryption Type** list.

The *Automatic WEP Settings* dialog box appears.



Automatic WEP Settings

Pending Automatic WEP Settings

After completing the form below and saving your changes, you will need to schedule the deployment of these settings to all sites within this group. Once the settings have been deployed, the sites will enable these settings at the Start Date/Time specified below.

Encryption Algorithm: 128-bit Encryption

Start Date/Time: 09 / 10 / 2002 11:30

WEP Key Rotation Interval: 15 minute(s)

The Pass Code may be any alpha-numeric value you specify. This is used for WEP Key generation only. You do NOT have to remember the Pass Code.

Pass Code: ****

Figure 7-3. *The Automatic WEP Settings Dialog Box*

6 Determine the size of the WEP keys you want to use by selecting either the 40-bit Encryption or 128-bit Encryption from the **Encryption Algorithm** list.

7 Type the start time when you want to initiate automatic WEP rotation in the **Start Date/Time** text boxes.

There are two **Start Time** text boxes. The first allows you to type the start date (including month, day, and year). The second allows you to select the start time (including hours and minutes).

8 Type the frequency of WEP key rotations in the **Rotation Interval** text box, and select whether this value indicates minutes, hours, days or weeks.

The value in this text box determines when the Mobile Manager rotates and replaces WEP keys. For example, if you type `15` in this text box, WEP keys are rotated for each Access Point every 15 minutes and an existing WEP key is replaced by a newly-generated one.

NOTE The minimum value for a WEP key rotation is 5 minutes.

9 Type a pass code into the **Pass Code** text box.

A pass code is like a password that is incorporated into the algorithm used to create WEP keys. This pass code allows you to deploy unique WEP keys to your Access Points without having to create and update multiple WEP keys manually.

10 Click `OK`.

11 Select `Save Group` from the **File** menu.

You can now use this automatic WEP rotation setup for your Access Point profiles. The settings you selected now appear in the WEP pane in the Pending Automatic WEP Settings box. When these settings are deployed, the values move to the Current Automatic WEP Settings box.

Extensible Authentication Protocol (EAP)

Cisco-Aironet Access Points support an additional protocol, called the Extensible Authentication Protocol, or EAP. This protocol works in conjunction with a RADIUS server on your network to authenticate mobile devices. Because this protocol works with a RADIUS server, wireless communications can be made more secure than static WEP key implementations. See your Cisco-Aironet Access Point documentation for detailed information on these options.

NOTE These options are only available within an Access Point profile.

To configure EAP for your wireless network:

1 Select a group from the Groups window.

2 Select `Configure Network`.

3 Click the Access Point Profiles tab.

4 Select the Cisco Access Point profile for which you are configuring EAP.

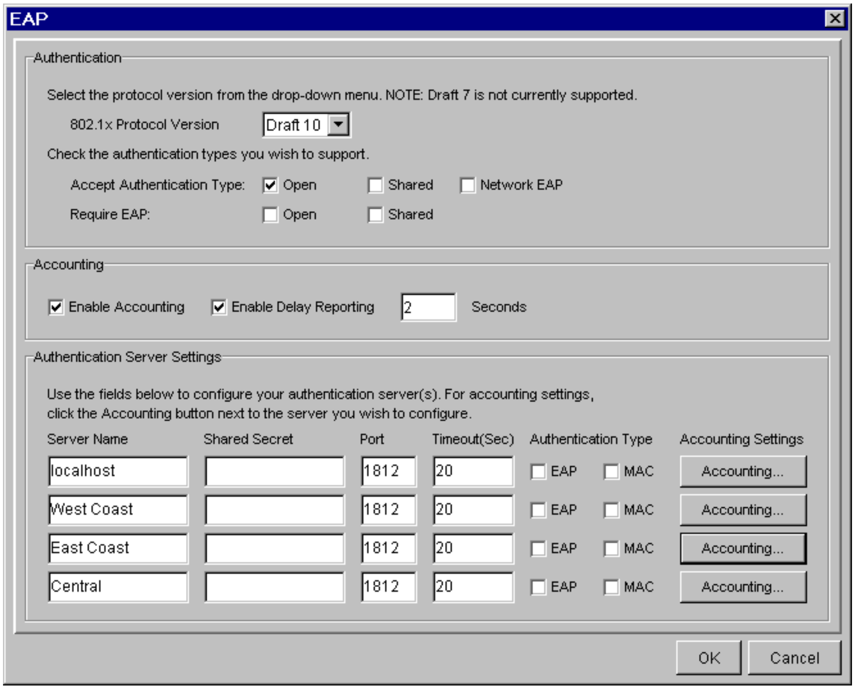
The *Access Point Profile* dialog box appears.

5 Click `Security`.

The Security Settings dialog box appears.

6 Click `EAP Settings`.

The *EAP* dialog box appears.



EAP

Authentication

Select the protocol version from the drop-down menu. NOTE: Draft 7 is not currently supported.

802.1x Protocol Version: Draft 10

Check the authentication types you wish to support.

Accept Authentication Type: ☑ Open □ Shared □ Network EAP

Require EAP: □ Open □ Shared

Accounting

☑ Enable Accounting ☑ Enable Delay Reporting 2 Seconds

Authentication Server Settings

Use the fields below to configure your authentication server(s). For accounting settings, click the Accounting button next to the server you wish to configure.

Server Name	Shared Secret	Port	Timeout(Sec)	Authentication Type		Accounting Settings
localhost		1812	20	□ EAP	□ MAC	Accounting...
West Coast		1812	20	□ EAP	□ MAC	Accounting...
East Coast		1812	20	□ EAP	□ MAC	Accounting...
Central		1812	20	□ EAP	□ MAC	Accounting...

Figure 7-4. *The EAP Dialog Box*

7 Select a protocol version appropriate for your network from the **802.1x Protocol Version** list.

The protocol version you select must be consistent between your Access Points and mobile devices. Different mobile devices support different draft versions of the EAP protocol, depending on their firmware type. See your mobile device documentation to determine the correct draft version.

NOTE The latest Cisco documentation known to Wavelink reports that firmware 4.25 and later supports draft 10.

Access Points compliant with Draft 7 do not support EAP. Consequently, you should not need to select this option.

8 Select the authentication type you want to support from one of the **Accept Authentication Type** checkboxes.

You can select from either open or shared authentication. Open authentication allows any mobile device to authenticate and attempt to connect with your network. This authentication type does not require a RADIUS server, and only mobile devices that have a WEP key that matches the designated Access Point can access your network.

Shared authentication provides a key that is shared between mobile devices and Access Points. This type of authentication, however, is vulnerable to unauthorized monitoring because the challenge text string sent from the Access Point is unencrypted.

You can also enable the **Network EAP** checkbox. This option allows EAP-enabled mobile devices to authenticate through an Access Point.

9 If you want to require EAP for either Open or Shared authentication, select one of the **Require EAP** checkboxes. These options instruct the Mobile Manager to block mobile devices that do not use EAP for authentication.

10 Enable the **Enable Accounting** checkbox to record data on attempts to access your network.

11 Enable the **Enable Delay Reporting** checkbox to delay the reporting of accounting events by a specified number of seconds.

To specify the delay time, type a number of seconds in the **Seconds** text box.

12 Type the name or IP address of a RADIUS server in a **Server Name** text box.

NOTE The accounting server and authentication server must have the same IP address.

13 Type the shared secret your RADIUS server uses in a Shared Secret text box.

The shared secret on the Access Point must match the one on the RADIUS server for authentication to occur.

14 Type the port number your RADIUS server uses for authentication in a **Auth Port** text box.

Typically, the default authentication port number for these servers is port 1812; however, it is recommended you check the documentation for your server to verify that you use the correct port number.

15 Type the number of seconds the Access Point can wait before authentication fails in a Timeout text box.

16 Enable either the **EAP** or **MAC** check box, depending on how you authenticate wireless communications.

If you select EAP, the Access Points use EAP to authenticate mobile devices. If you select MAC, Access Points use the MAC address of the mobile device.

17 Click `Accounting` to set the accounting settings for this RADIUS server.

See *Enabling EAP Accounting* on page 105 for more information on EAP accounting options.

18 Click `OK`.

Enabling EAP Accounting

If you implement EAP for a Cisco-Aironet profile, you can also activate RADIUS accounting. RADIUS accounting allows you to store information about wireless connection activity.

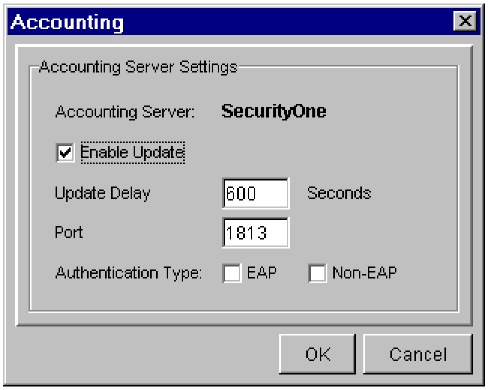
To enable EAP Accounting:

1 Open a profile for which you have enabled EAP.

See *Extensible Authentication Protocol (EAP)* on page 102 for more information on enabling EAP for a profile.

2 Click `Accounting` for the RADIUS server for which you want to enable accounting.

The *Accounting* dialog box appears.



Accounting

Accounting Server Settings

Accounting Server: SecurityOne

☑ Enable Update

Update Delay 600 Seconds

Port 1813

Authentication Type: □ EAP □ Non-EAP

Figure 7-5. *The Accounting Dialog Box*

3 If you want the Access Point to send period accounting updates to the RADIUS server, enable the **Enable Update** checkbox.

4 When you enable the **Enable Update** checkbox, type the number of seconds you want to pass between each Access Point update in the **Update Delay** text box.

5 Type the port number your RADIUS server uses for accounting in the **Port** text box.

6 Enable either the **EAP** or **Non-EAP** check box, depending on how you authenticate the accounting of users attempting to access your network.

7 Click `OK`.

Advanced Security Options

Cisco-Aironet Access Points contain additional security features that you can use to further strengthen your wireless network against unauthorized access. These features work in conjunction with existing WEP key settings; however, you are not required to implement them if they do not conform with the security requirements of your wireless network.

To configure advanced security options:

1 Select a group from the Groups window.

2 Select `Configure Network`.

3 Click the Access Point Profiles tab.

4 Select the Cisco Access Point profile for which you are configuring EAP.

The *Access Point Profile* dialog box appears.

5 Click `Security`.

The Security Settings dialog box appears.

6 Click `Advanced Settings`.

The Advanced Radio tab of the *Access Point Properties* dialog box appears.

7 Click `Advanced Settings`.

The Advanced Radio tab of the *Access Point Properties* dialog box appears.

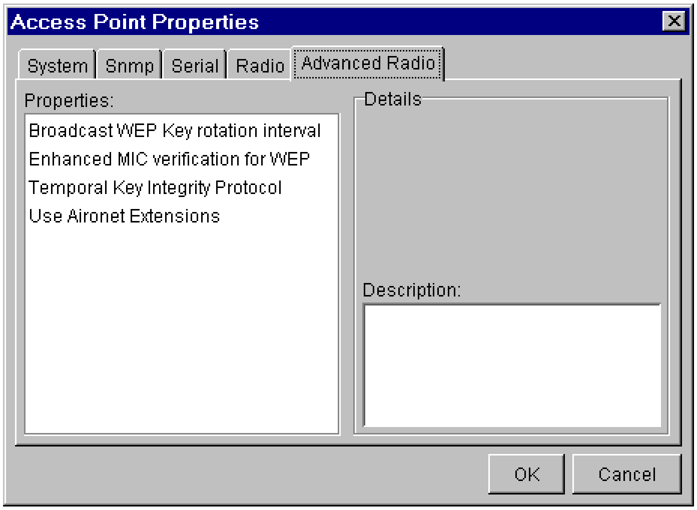


Figure 7-6. *The Advanced Radio Tab of the Access Point Properties Dialog Box*

8. Select an option from the Properties list.

   A configurable option (such as a checkbox) appears in the Details section of the *Access Point Properties* dialog box.

9. Configure the property as needed.

   See *Advanced Radio Properties* for descriptions about each of these properties.

10. Click `OK` when you are finished configuring the advanced radio properties.

Advanced Radio Properties

The following list describes the advanced radio properties of Cisco-Aironet Access Points and how you can use them to further fortify your network against intrusion.

NOTE See your Cisco-Aironet Access Point documentation for detailed information on these options.

Use Aironet Extensions

The **Use Aironet Extensions** checkbox enables the use of the Enhanced MIC for WEP, Temporal Key Integrity Protocol, and Broadcast WEP Key Rotation Interval features.

Enhanced MIC Verification for WEP

MIC, an abbreviation for Message Integrity Check, is a security feature that adds a message digest to each transmission between Access Points and mobile devices. This message digest prevents attacks that intercept a transmission, alter it, and re-insert it back into your network.

Temporal Key Integrity Protocol	Even with WEP keys in place, a part of each wireless packet sent across your network, called the initialization vector, remains unencrypted. An intruder can potentially use this initialization vector to discover your WEP keys. When you enable a Temporal Key Integrity Protocol, you remove the predictability that an intruder needs to locate and exploit an initialization vector. To enable this feature, select Cisco from the **Temporal Key Integrity Protocol** list.
Broadcast WEP Key Rotation Interval	This feature creates a dynamically changing WEP key. After you set up the WEP keys for your network, you can use this option to rotate between each key at a specific interval. This option is ideal if your Cisco-Aironet Access Points do not support the **Temporal Key Integrity Protocol** option. To use this feature, type the rotation interval, in seconds, in the **Broadcast WEP Key Rotation Interval** text box.

Deploying Security Settings

After you have configured the network settings for a group, you can deploy those settings by using the following deployment events:

- Deploy Settings to Mobile Manager
- Deploy Settings to Avalanche

These events ensure that both the Mobile Manager and Avalanche Agents receive the correct security information.

See *Chapter 13: Deploying Configurations* on page 161 for more information on how to create deployment events.

Chapter 8: Managing Access Point Profiles

The Mobile Manager Enterprise Edition streamlines Access Point configuration and management by allowing you to create a profile for each type of Access Point on your network.

In the past, organizations have been challenged with finding an efficient means of configuring Access Points. These challenges existed for several reasons. First, prior to the Mobile Manager, Access Points were only configurable one at a time, by initiating a Telnet session or creating a serial connection directly to that Access Point. Because most Access Points are installed in locations that are optimized for wireless coverage—such as ceilings—locating and configuring individual Access Points was both time-consuming and difficult. Second, Access Points are highly specialized network devices and are not designed for untrained user interaction. Configuring an Access Point can be difficult without the proper level of technical experience.

Access Point profiles remove these challenges by providing you with a straightforward interface to Access Point settings, and by pushing these settings to multiple Access Points on your network simultaneously. The Mobile Manager also monitors the network to verify that Access Point configurations remain unchanged. If the Mobile Manager finds an Access Point's configuration has changed, it resets the Access Point back to the settings defined in its profile. In addition, the Mobile Manager routinely checks for new Access Points on the network. When a new Access Point is discovered, the Mobile Manager determines its hardware type and assigns it to the appropriate Access Point profile.

NOTE Access Point profiles apply only to one group within the Enterprise Administrator. You cannot assign a single profile to multiple groups.

There are two types of Access Point profiles: enterprise profiles and normal profiles. Normal profiles are created using the Mobile Manager Administrator and operate at the site level. Enterprise profiles are created using the Enterprise Administrator and operate across your enterprise. Enterprise profiles are treated as default profiles, and are applied to any non-profiled Access Points when they are deployed to a specific site.

NOTE If a site already contains a default profile, the enterprise profile takes precedence. The site's default profile remains, but the Agent no longer uses it as the default profile.

See the *Mobile Manager Users Guide* for more information on creating Access Point profiles at the site level.

This section contains the following topics:

- Configuring Enterprise Profiles
- Determining Which Access Point Properties to Use
- Creating a Sample Profile
- Deploying Enterprise Profiles

Configuring Enterprise Profiles

Once you organize your network sites into groups, you can assign enterprise profiles to each group. The Enterprise Administrator takes the configuration values for each profile assigned to a group and applies them to the sites associated with that group. As a result, you can configure multiple sites on your network at one time.

This section focuses on how to create, modify, and delete enterprise profiles. It also provides information on how to refresh the Profile list so you retain an accurate view of the profiles for a specific group.

Creating Enterprise Profiles

Enterprise profiles apply only to one specific group. Each group can have one enterprise profile per Access Point hardware type. These hardware types are as follows:

- 3COM Airconnect 11 Mbps
- Cisco 1200
- Cisco 340/350

- Cisco 350 Bridge
- Ericsson WLAN DSSS A11
- Intel Pro 2011
- Intel Pro 2011B
- Nortel e-Mobility 802.11 DS
- Symbol AP-2411
- Symbol AP-3020, 3021
- Symbol AP-4111, 4121
- Symbol AP-4131

You can create enterprise profiles to be as basic or as detailed as your wireless network demands.

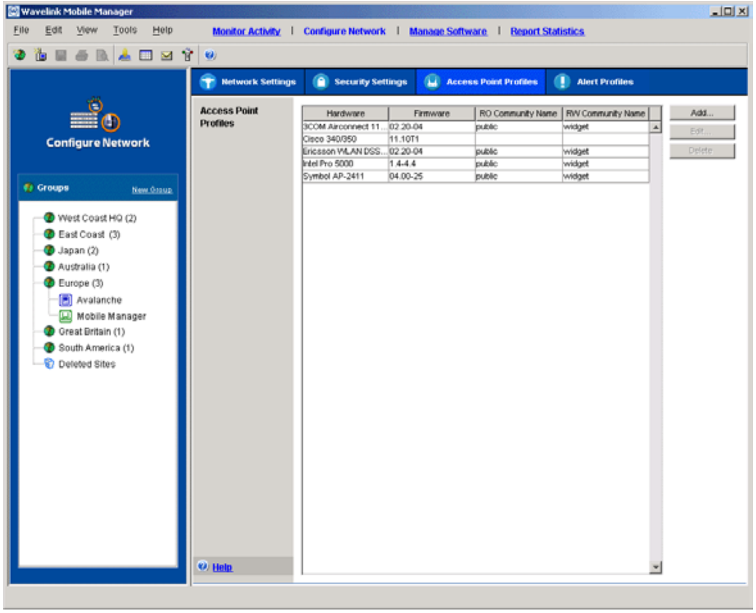
To create a basic enterprise profile:

1 Select a group from the Groups window.

The profile that you create will apply to all Access Points managed within the selected group.

2 Select `Configure Network`.

3 Click the Access Point Profiles tab.

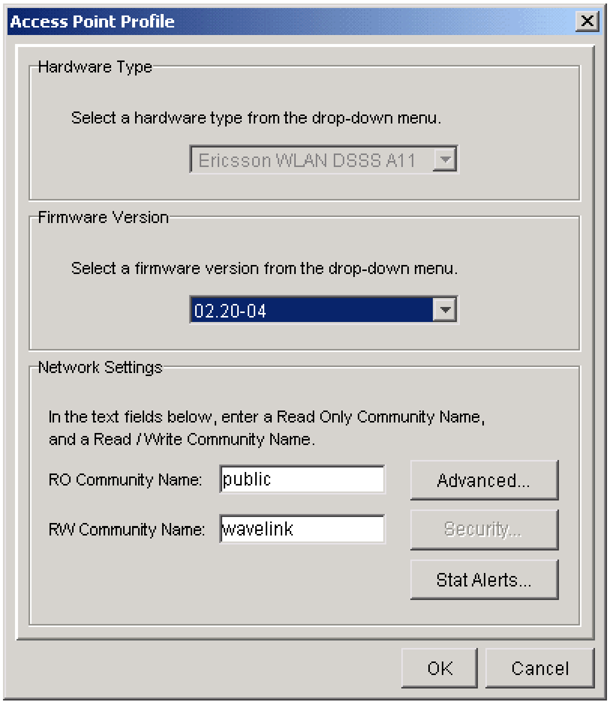


Hardware	Firmware	RO Community Name	RW Community Name
3COM Airconnect 11...	02.20-04	public	widget
Cisco 340/350	11.10T1		
Ericsson WLAN DSS...	02.20-04	public	widget
Intel Pro 5000	1.4-4.4	public	widget
Symbol AP-2411	04.00-25	public	widget

Figure 8-1. *The Access Point Profiles Tab of the Configure Network View*

4 Click `Add`.

The *Access Point Profile* dialog box appears.



Access Point Profile

Hardware Type

Select a hardware type from the drop-down menu.

Ericsson WLAN DSSS A11

Firmware Version

Select a firmware version from the drop-down menu.

02.20-04

Network Settings

In the text fields below, enter a Read Only Community Name, and a Read / Write Community Name.

RO Community Name: public

RW Community Name: wavelink

Figure 8-2. *The Access Point Profile Dialog Box*

5 Select a hardware type from the **Hardware Type** list.

6 Select a firmware from the **Firmware Version** list.

7 Type the read-only community name in the **RO Community Name** text box.

8 Type the read/write community name in the **RW Community Name** text box.

9 To configure additional Access Point properties, click `Advanced`.

See the *Mobile Manager Users Guide* for more information on the properties available for your Access Points.

10 To assign security settings to this profile, click `Security`.

See *Chapter 7: Managing Security Settings* on page 91 for more information on creating WEP keys for your Access Points.

11 To create one or more statistical alerts for this profile, click `Stat Alerts`.

See *Chapter 14: Statistical Alerts* on page 171 for more information on creating a statistical alert.

12 Click `OK`.

The new enterprise profile appears in the Access Point Profiles tab.

Modifying Enterprise Profiles

You can modify enterprise profiles as your network demands.

NOTE You must deploy enterprise profiles to apply their settings to individual Access Points. Modified profiles are not implemented on your network until they are deployed. See *Chapter 13: Deploying Configurations* on page 161 for more information on profile deployment.

To modify an enterprise profile:

1 Select a group from the Groups window.

2 Select `Configure Network`.

3 Click the Access Point Profiles tab.

4 Click `Edit`.

5 Modify the profile as needed.

Deleting Enterprise Profiles

If a profile is no longer necessary for a particular group, you can delete that profile from the group. Any Access Point that belongs to a deleted profile retains that profile's settings until you either assign it a new profile or modify it manually.

NOTE Deleting a profile is permanent and cannot be undone without recreating the entire profile.

In addition, deleted profiles remain at each site until they are removed manually.

To delete an enterprise profile:

1 Select a group from the Groups window.

2 Select `Configure Network`.

3 Click the Access Point Profiles tab.

4 Select `Delete` from the menu that appears.

Refreshing the Profile List

If you installed the Enterprise Administrator on multiple systems, the Profile list is refreshed each time you launch the Enterprise Administrator to ensure that you view the most current information. If you want to refresh the profile list manually, you can do so at any time.

To manually refresh the Profile list:

1 Select a group from the Groups window.

2 Select `Configure Network`.

3 Click the Access Point Profiles tab.

4 Right-click within the list of profiles.

5 Select `Refresh Profile List` from the menu that appears.

Determining Which Access Point Properties to Use

The types of properties available to your profiles depends on the Access Point manufacturer. While the manufacturers that the Mobile Manager supports all share similar capabilities, the properties that control those capabilities vary from one manufacturer to another. Despite these differences between Access Point types, there are several principles you can use to create Access Point profiles that benefit your network.

A well-designed Access Point profile:

- Controls how Access Points are configured
- Activates security features
- Captures relevant statistical data

The following sections discuss these principles in more detail.

Controlling How Access Points Are Configured

Depending on the manufacturer, Access Points are configurable using one of several methods. These methods are:

- Serial connection
- Telnet session
- Web browser
- Mobile Manager

You can activate or deactivate using an Access Point profile using any of these methods. For example, to prevent Access Point configuration by Telnet session, you disable the **Enable Telnet** property.

NOTE Do not disable the Web interface to Cisco-Aironet Access Points. Doing so prevents the Agent from managing them.

When you create your profiles, it is recommended that you consider which methods you want enabled on your Access Points. For example, if you wanted to ensure that Access Points can only be configured through the Enterprise Administrator, you would deactivate the properties relating to serial connections and Telnet sessions. Once these properties are deactivated, you can only modify an Access Point through the Enterprise Administrator.

Activating Access Point Security Features

Access Points contain several security features that help prevent unauthorized access to your wireless network. The features that have the greatest impact on your wireless network security are the Very Large Access Control List and WEP keys.

A well-defined Access Point profile incorporates these security features to reduce the risk of unauthorized network access. Two ways you can implement these features are:

1 Build and maintain a Very Large Access Control List.

You can add and remove MAC address from an Access Point profile by using the Very Large Access Control List pane of the Enterprise Administrator's Configure Network view. See *Building Access Control Lists* on page 92 for more information.

2 Assign WEP keys or other security protocols to the profile.

WEP, or Wired Equivalent Privacy, is a protocol for securing wireless network communications. You secure your wireless network by assigning a WEP key to an Access Point. This key encrypts transmissions between a mobile device and an Access Point. See *Chapter 7: Managing Security Settings* on page 91 for more information on WEP and other security protocols.

It is highly recommended that you implement all of these security features to maintain the integrity of your wireless network. See the *Chapter 7: Managing Security Settings* on page 91 for more information on wireless network security and Mobile Manager.

Capturing Network Events

As you deploy profiles across your enterprise, you might find it useful to capture specific events that occur on your network. You can use your Access Point profiles to track and store these events, allowing you to review their occurrences and further tune your wireless network for better performance.

Most of these statistical settings are controlled in the SNMP tab of the *Access Points Properties* dialog box.

To access the SNMP tab:

1 Select a group from the Groups window.

The profile that you create will apply to all Access Points managed within the selected group.

2 Select `Configure Network`.

3 Click the Access Point Profiles tab.

4 Select a profile from the Profiles pane and click `Edit`.

If you have not created a profile yet, click `Add`.

The *Access Point Profile* dialog box appears.

5 Click `Advanced`.

The *Access Point Profiles* dialog box appears.

6 Click the SNMP tab.

The types of events (also known as traps) that you can capture depends on the firmware and manufacturer you selected for this profile. See the appropriate MIB documentation for more information on the different statistics you can capture.

Creating a Sample Profile

This section takes the principles discussed in *Determining Which Access Point Properties to Use* on page 117 and applies it to a sample enterprise profile. If you have not created an enterprise profile before, you can follow the steps in this sample to experience firsthand how easy it is to configure Access Point with the Mobile Manager.

NOTE Do not deploy this profile unless it is appropriate for your network.

This sample profile is designed for 11MB Access Points. For security purposes, this profile disables Access Point configuration by Telnet session or serial connection, allowing only individuals authorized to use the Enterprise Administrator to modify Access Point settings.

NOTE Because security settings are unique to each organization, these features are not covered in this sample profile.

To create a sample profile:

1 Select a group from the Groups window.

The profile that you create will apply to all Access Points managed within the selected group.

2 Select `Configure Network`.

3 Click the Access Point Profiles tab.

4 Click `Add`.

The *Access Point Profile* dialog box appears.

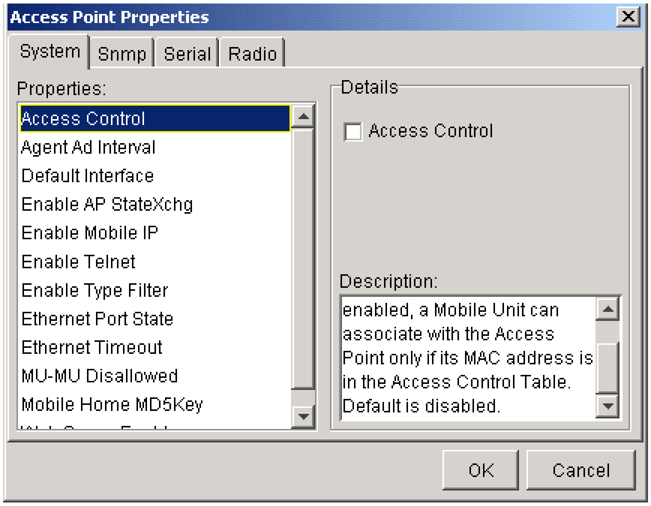
5 Select an Access Point hardware type from the **Hardware Type** list.

6 Select a firmware version from the **Firmware Version** list.

7 In the **RW Community Name** field, type `Mobile Manager`.

8 Click `Advanced`.

The *Access Point Profiles* dialog box appears.



Access Control
Agent Ad Interval
Default Interface
Enable AP StateXchg
Enable Mobile IP
Enable Telnet
Enable Type Filter
Ethernet Port State
Ethernet Timeout
MU-MU Disallowed
Mobile Home MD5Key

□ Access Control

enabled, a Mobile Unit can associate with the Access Point only if its MAC address is in the Access Control Table. Default is disabled.

Figure 8-3. *The Access Point Properties Dialog Box*

9 Click the System tab.

10 From the **Properties** list, select `Enable Telnet`.

A checkbox appears in the Details section. This checkbox allows you to enable or disable the ability to Telnet into the Access Point.

11 Disable the **Enable Telnet** checkbox.

12 Click the Serial tab.

13 From the **Properties** list, select `Serial Port Use`.

A checkbox appears in the Details section. This checkbox allows you to enable or disable the ability to use the configure the Access Point through a serial connection.

14 Disable the **Serial Port Use** checkbox.

15 Click `Apply`.

16 Click `OK` to return to the *Access Point Profile* dialog box.

17 Click `OK` to return to the Configure Network view.

You have now created a hardware-specific profile for 11MB Access Points for a group of sites in your wireless network. If you want to continue modifying this profile to match the needs of your network, it is recommended you:

- Change the ESS ID and SNMP Community Name properties
- Assign IP addresses to the profile
- Add MAC addresses to the Very Large Access Control List

Accomplishing these tasks is covered in *Configuring Enterprise Profiles* on page 112. Additional information can also be found in *Chapter 5: Managing Network Settings* on page 61 and *Chapter 7: Managing Security Settings* on page 91.

Deploying Enterprise Profiles

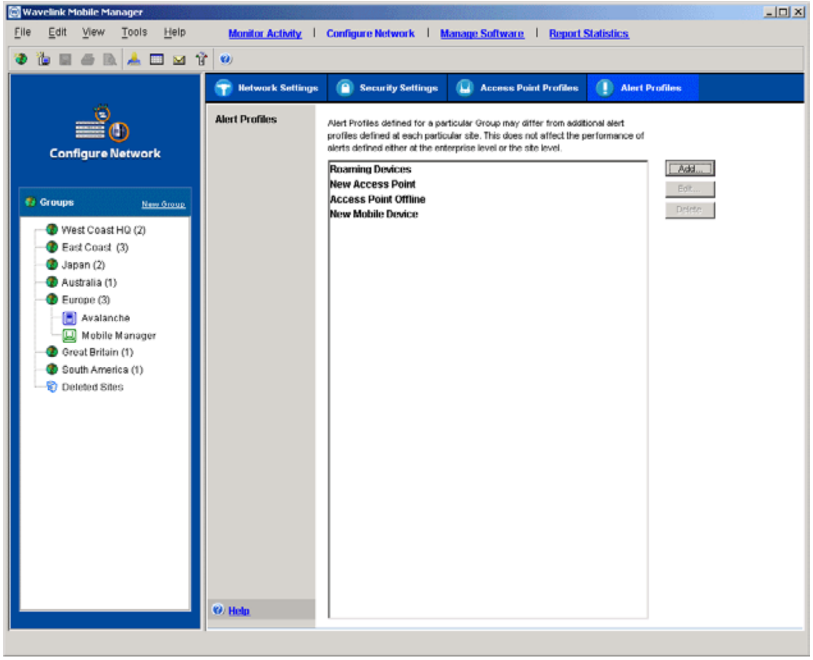
After you have created one or more enterprise profiles for a group, you can deploy those profiles by using the Deploy Settings to Mobile Manager deployment event.

See *Chapter 13: Deploying Configurations* on page 161 for more information on how to create deployment events.

Chapter 9: Managing Alert Profiles

One of the key requirements to any network management tool is its ability to quickly inform you of network alerts and provide you with an efficient means of responding to those alerts. The Mobile Manager fulfills this requirement by allowing you to create alert profiles.

There are two types of alert profiles: enterprise alert profiles and normal alert profiles. Normal alert profiles are created using the Mobile Manager Administrator and operate at the site level. Enterprise alert profiles are created using the Enterprise Administrator and operate across your enterprise. Unlike Access Point profiles, which have a hierarchal relationship, alert profiles at the site and enterprise levels co-exist equally.



Alert Profiles defined for a particular Group may differ from additional alert profiles defined at each particular site. This does not affect the performance of alerts defined either at the enterprise level or the site level.

Roaming Devices
New Access Point
Access Point Offline
New Mobile Device

Figure 9-1. *The Alert Profiles Tab of the Configure Network View*

With alert profiles, you decide what alerts demand your immediate attention. You can also create a list of e-mail addresses that the Enterprise Administrator uses to inform you when a specified alert occurs. In addition, the Enterprise Administrator allows you to set one or more proxies (such as CA Unicenter). When you set a proxy for an alert profile, the Enterprise

Administrator automatically forwards the alert to the proxy's IP address, enabling you to integrate the Mobile Manager with your existing network management tools.

You configure most options related to wireless network alerts from the Alert Profiles pane of the Enterprise Administrator's Configure Network view. Information on viewing reports on wireless network alerts can be found in *Chapter 11: Reporting Network Data* on page 139.

This section contains the following topics:

- Creating an E-mail Address List
- Creating Proxy Pool
- Creating Enterprise Alert Profiles

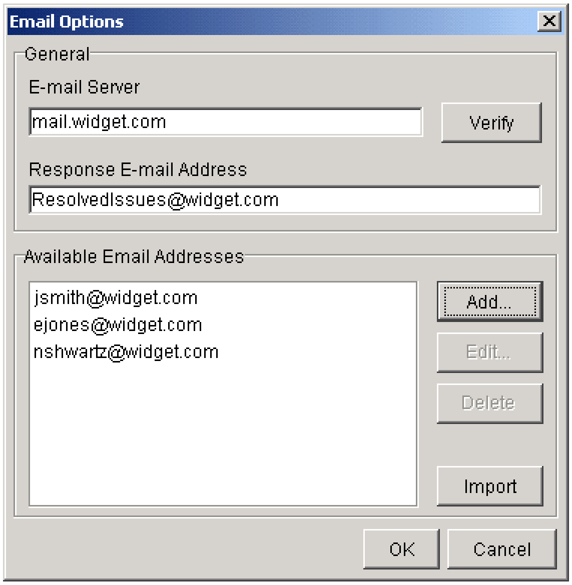
Creating an E-mail Address List

If you want the Enterprise Administrator to notify you of an alert by e-mail, you must create an e-mail address list. E-mail address lists are available to all groups within the Enterprise Administrator.

To create an e-mail address list:

1 Select `E-mails` from the **Tools** menu.

The *E-mail Options* dialog box appears.



E-mail Server: mail.widget.com

Response E-mail Address: ResolvedIssues@widget.com

jsmith@widget.com
ejones@widget.com
nshwartz@widget.com

Figure 9-2. *The E-mail Options Dialog Box*

This dialog box allows you to add e-mail addresses, import an e-mail address list, and delete obsolete addresses.

2 Type the name of the SMTP e-mail server in the **E-mail Server** text box, such as `mail.company.com`.

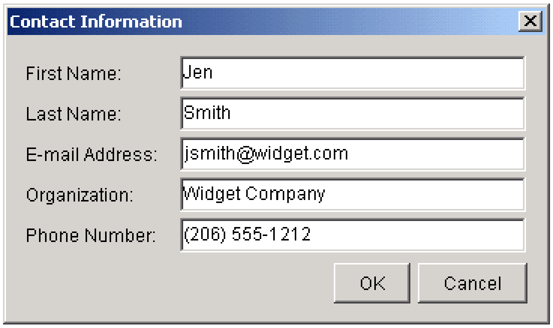
To verify the validity of the e-mail server, click `Verify`. The Mobile Manager attempts to contact the e-mail server, and displays a dialog box informing you if it was successful or not.

3 Type an e-mail address in the **Response e-mail address** text box, such as `itdept@company.com`.

Any replies to alert notification e-mails are sent to this e-mail address.

4 Add any e-mails addresses to which you want alert notification e-mails sent, such as `jens@company.com`.

To add an e-mail address, click `Add`. The *Contact Information* dialog box appears. Type the appropriate information in this dialog box.



First Name: Jen
Last Name: Smith
E-mail Address: jsmith@widget.com
Organization: Widget Company
Phone Number: (206) 555-1212

Figure 9-3. *The Contact Information Dialog Box*

5 Click `OK`.

The address appears in the **Available e-mail address** list.

6 Repeat 4 and 5 until you are finished adding e-mail addresses.

7 Click `OK`.

Importing E-mail Addresses

You can add e-mail addresses to the e-mail address list by importing a comma-delimited .csv file that was exported from Outlook.

To import e-mail addresses:

1 Select `E-mails` from the **Tools** menu.

The *E-mail Options* dialog box appears.

2 Click `Import`.

An *Open* dialog box appears.

3 Select the .csv file that contains the e-mail addresses that you want to import.

4 Click `OK`.

The e-mail addresses contained in the text file appear in the **Available E-mail Addresses** list.

Deleting E-mail Addresses

If you need to delete an e-mail address from an e-mail address list, you can do so at any time.

To delete an e-mail address:

1 Select `E-mails` from the **Tools** menu.

The *E-mail Options* dialog box appears.

2 Select the e-mail address from the **Available E-mail Addresses** list.

3 Click `Delete`.

The Enterprise Administrator removes the e-mail address from the list.

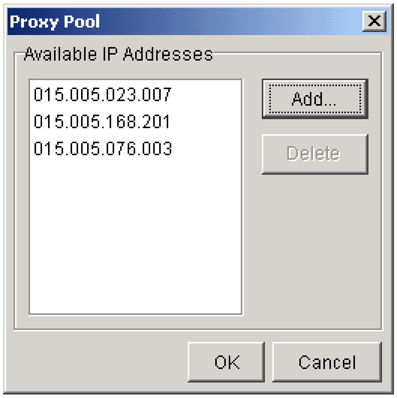
Creating Proxy Pool

The Enterprise Administrator provides you with the ability to send alert profiles to a proxy (for example, CA Unicenter). To use proxies with alert profiles you must create a proxy pool. Proxies are available to all groups within the Enterprise Administrator.

To add a proxy to a proxy pool:

1 Select `Proxies` from the **Tools** menu.

The *Proxy Pool* dialog box appears.



015.005.023.007
015.005.168.201
015.005.076.003

Figure 9-4. *The Proxy Pool Dialog Box*

2 Click `Add`.

The *Add Proxy Address* dialog box appears.

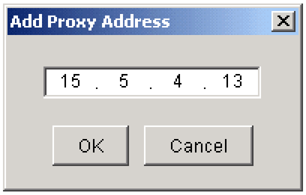


Figure 9-5. *The Add Proxy Address Dialog Box*

3 Type the IP address of the proxy.

4 Click `OK` to return to the *Proxy Pool* dialog box.

The IP address of the new proxy appears in the `Available Proxy Addresses` list.

5 Click `OK`.

Deleting Proxies

If you need to delete a proxy from a proxy pool, you can do so at any time.

To delete a proxy:

1 Select `Proxies` from the **Tools** menu.

The *Proxy Pool* dialog box appears.

2 Select the IP address of the desired proxy from the **Available Proxy Addresses** list.

3 Click `Delete`.

The Mobile Manager deletes the proxy from the list.

Creating Enterprise Alert Profiles

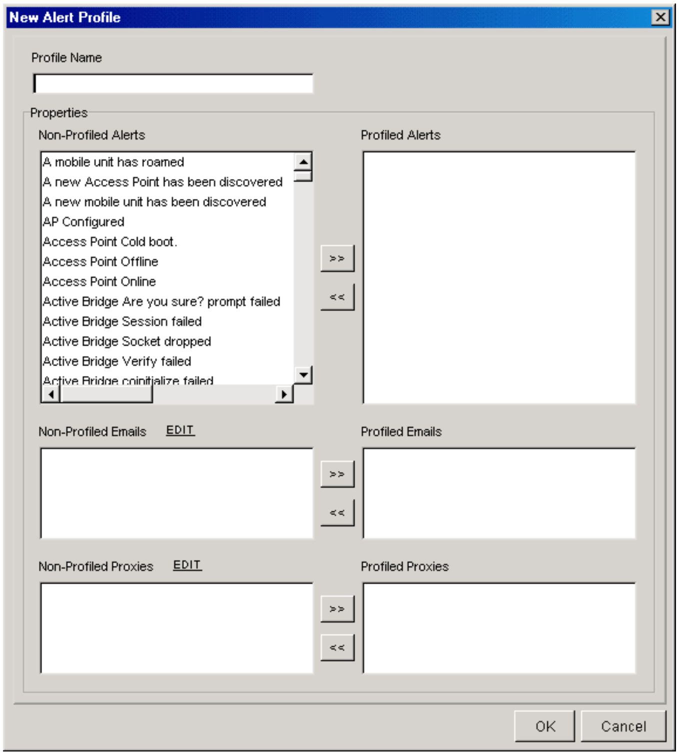
Once you add e-mail addresses to an e-mail address list or add proxies to a proxy pool, you can create enterprise alert profiles. With an enterprise alert profile, you assign Mobile Manager alerts to one or more e-mail addresses or proxies. When these alerts occur, Mobile Manager immediately either sends an e-mail to the selected addresses or forwards the alert to the proxy computer.

NOTE If you do not assign an alert to a profile, you can still access information about the alert through the Monitor Activity and Report Statistics views.

To create an enterprise alert profile:

1. Select a group from the Groups window.
2. Select `Configure Network`.
3. Click the Alert Profiles tab.
4. Click `Add`.

   The *Notification* dialog box appears.



A mobile unit has roamed
A new Access Point has been discovered
A new mobile unit has been discovered
AP Configured
Access Point Cold boot.
Access Point Offline
Access Point Online
Active Bridge Are you sure? prompt failed
Active Bridge Session failed
Active Bridge Socket dropped
Active Bridge Verify failed
Active Bridge coinitialize failed

Figure 9-6. *The Notification Dialog Box*

5 Type a name for the enterprise alert profile in the **Profile Name** text box.

6 Select one or more alerts from the **Non-Profiled Alerts** list and click [>].

The alert moves to the **Profiled Alerts** list.

7 If you want the Enterprise Administrator to inform you of the alert by e-mail, select one or more e-mail addresses from the **Non-Profiled E-mails** list and click [>].

NOTE You can modify e-mail addresses from the *Notifications* dialog box by clicking the **Edit** link located next to the **Non-Profiled E-mails** list.

The e-mail address moves to the **Profiled E-mails** list.

8 If you want the Enterprise Administrator to send the alert to a proxy, select one or more IP addresses from the **Non-Profiled Proxies** list and click [>].

NOTE You can modify e-mail addresses from the *Notifications* dialog box by clicking the **Edit** link located next to the **Non-Profiled Proxies** list.

The proxy moves to the **Profiled Proxies** list.

9 Click `OK` to save your changes and return to the Enterprise Administrator.

Modifying Enterprise Alert Profiles

You can make modifications to an enterprise alert profile at any time. Any changes you make to an enterprise alert profile take effect immediately.

To modify an enterprise alert profile:

1 Select a group from the Groups window.

2 Select `Configure Network`.

3 Click the Alert Profiles tab.

4 Select an enterprise alert profile.

5 Click `Edit`.

The *Notifications* dialog box appears.

6 Edit the notification as necessary.

7 Click `OK` to save your changes and return to the Enterprise Administrator.

Deleting Enterprise Alert Profiles

If you determine that an enterprise alert profile is unnecessary, you can delete it from the Enterprise Administrator.

To delete an enterprise alert profile:

1 Select a group from the Groups window.

2 Select `Configure Network`.

3. Click the Alert Profiles tab.
4. Select an enterprise alert profile.
5. Click `Delete`.

The Enterprise Administrator deletes the enterprise alert profile.

Chapter 10: Managing Users

When you install the Mobile Manager Enterprise Edition, you create an administrative user account. This account allows you to restrict administration of your wireless network. With this account, you can create new accounts, each of which can have several different levels of permissions. The different permission levels for these accounts are as follows:

Administrative Full permissions to manage wireless devices, including profiles, IP address assignments, and Access Point configurations. Also has permission to create or modify user accounts.

Read/Write Full permissions to manage wireless devices, including profiles, IP address assignments, and Access Point configurations, but cannot create or modify user accounts.

Read Only Read-only access to wireless devices through the Administrator.

Accounts are created for enterprise-wide components of the Mobile Manager, such as the Enterprise Administrator, are also distributed to all the sites on your wireless networks. Consequently, a user that has read/write permissions for the Enterprise Administrator also has read/write permissions for any site on the network. When you add a new site, that site automatically receives all the user account information established for your wireless network.

This section contains the following topics:

- Creating User Accounts
- Editing User Accounts
- Deleting User Accounts
- Viewing Account Status
- Changing Account Passwords
- Deploying User Accounts

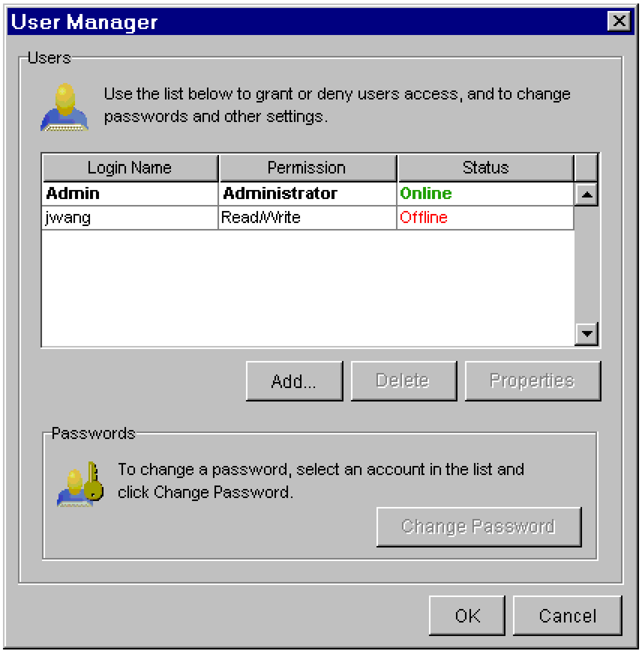
Creating User Accounts

The user account you first create when you activate the Mobile Manager security controls is an administrative account by default. With this account, you have the ability to create new accounts.

To create a new account:

1 Select `User Manager` from the **Tools** menu.

The *User Manager* dialog box appears.



User Manager

Users

Use the list below to grant or deny users access, and to change passwords and other settings.

Login Name	Permission	Status
Admin	**Administrator**	**Online**
jwang	Read/Write	Offline

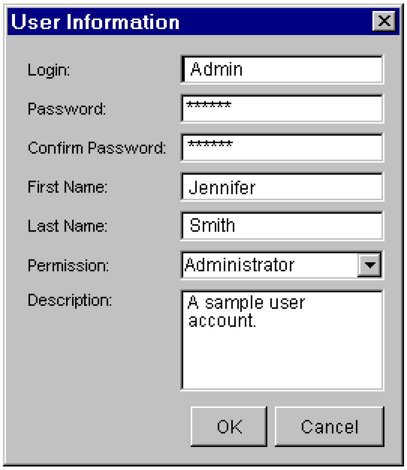
Passwords

To change a password, select an account in the list and click Change Password.

Figure 10-1. *The User Manager Dialog Box*

2 Click `Add`.

The *User Information* dialog box appears.



User Information

Login: Admin

Password: ******

Confirm Password: ******

First Name: Jennifer

Last Name: Smith

Permission: Administrator

Description: A sample user account.

Figure 10-2. *The User Information Dialog Box*

3 Type the login name for the account in the **Login** text box.

4 Type the password for this account in the **Password** text box.

5 Confirm the password by re-typing it in the **Confirm Password** text box.

6 Type the first name for the individual using the account in the **First Name** text box.

7 Type the last name for the individual using the account in the **Last Name** text box.

8 Select the level of permissions for this account from the **Permission** list.

You can select from administrative, read/write, and read only.

9 Type a description for the account in the **Description** text box.

10 Click `OK`.

The new account is now available for the Enterprise Administrator. It is also distributed to any known sites on the network.

Editing User Accounts

If you have a user account with administrative permissions, you have the ability to edit user accounts. For example, you can change the password or permissions level for the account.

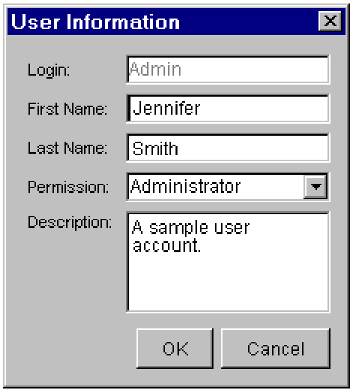
To edit a user account:

1 Select `User Manager` from the **Tools** menu.

The *User Manager* dialog box appears.

2 Select a user and click `Properties`.

The *User Information* dialog box appears.



Login: Admin
First Name: Jennifer
Last Name: Smith
Permission: Administrator
Description: A sample user account.

Figure 10-3. *The User Information Dialog Box*

3 Edit the account as necessary.

4 Click `OK`.

The edited account is now available for the Enterprise Administrator. It is also distributed to any known sites on the network.

Deleting User Accounts

If you have a user account with administrative permissions, you have the ability to delete user accounts.

To delete a user account:

1 Select `User Manager` from the **Tools** menu.

  The *User Manager* dialog box appears.

2 Select a user from the list.

3 Click `Delete`.

The deleted account is now removed from the Enterprise Administrator. It is also removed from any known sites on the network.

Viewing Account Status

Any user that has access to an Agent can view the status of other Mobile Manager users. To view the status of a user, select `User Manager` from the **Tools** menu to open the *User Manager* dialog box. From this dialog box, users can determine which accounts are currently online, and the level of permission for each account.

NOTE If a user does not have administrative permissions for the Agent, the **Add**, **Edit**, and **Delete** buttons in the *User Manager* dialog box do not appear.

Changing Account Passwords

All users, regardless of their level of permission, have the ability to change the password for their account.

To change an account password:

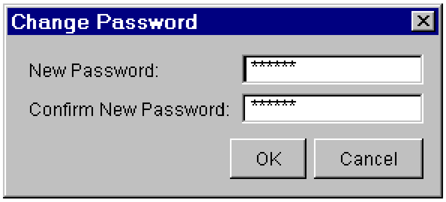
1 Select `User Manager` from the **Tools** menu.

  The *User Manager* dialog box appears.

2 Select a user.

3 Click `Change Password`.

  The *Change Password* dialog box appears.



Change Password

New Password: *******

Confirm New Password: *******

Figure 10-4. *The Change Password Dialog Box*

4 Type the new password in the **New Password** text box.

5 Confirm the new password by re-typing it in the **Confirm New Password** text box.

6 Click `OK`.

The new password information is now available for the Enterprise Administrator. It is also distributed to any known sites on the network.

Deploying User Accounts

By default, the Mobile Manager Enterprise Edition automatically deploys new or modified user accounts to all sites on your wireless network. However, if the Mobile Manager was unable to deploy user accounts—for example, because the host system of the Enterprise Administrator was unable to connect to the network—you can use the Update User Accounts (Mobile Manager Only) deployment event to distribute user accounts manually.

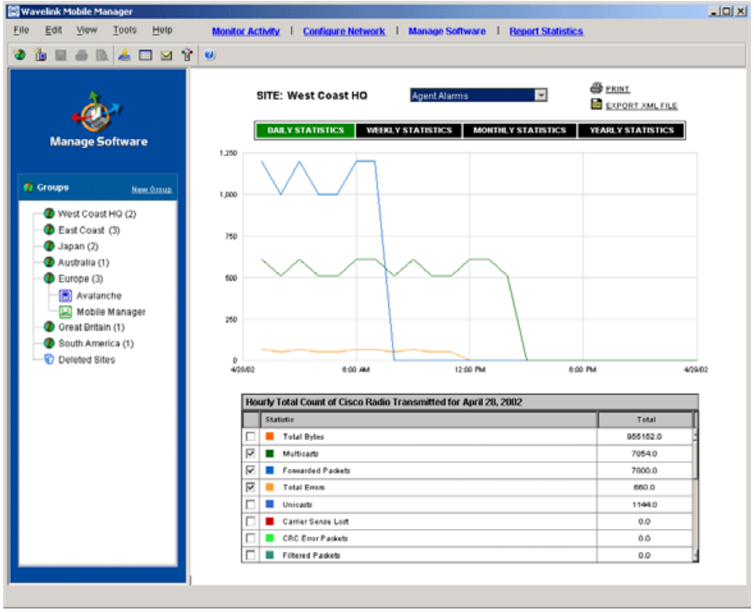
See *Chapter 13: Deploying Configurations* on page 161 for more information on deployment events.

Chapter 11: Reporting Network Data

Efficient network management hinges on having accurate and timely information on current network performance. With this information, you are better able to optimize your network.

To assist you with tracking wireless network performance, the Enterprise Administrator includes the Report Statistics view. This view allows you to create graphs and reports on both statistical data, such as how many Ethernet packets were sent, and Agent alerts, such as when an Agent discovers a new Access Point on its subnet. By using the Report Statistics view, you can continually monitor the performance of your wireless network, and make adjustments to ensure that the network meets the needs of your organization.

With the Enterprise Administrator, you create reports on a per-site basis. Consequently, you can customize your reporting processes to match the specific needs of the groups within your wireless network.



SITE: West Coast HQ

Agent Alarms

Hourly Total Count of Cisco Radio Transmitted for April 28, 2002

	Statistic	Total
□	🟧 Total Bytes	955152.0
☑	🟩 Multicasts	7054.0
☑	🟦 Forwarded Packets	7000.0
☑	🟧 Total Errors	660.0
□	🟦 Unicasts	1144.0
□	🟥 Carrier Sense Lost	0.0
□	🟩 CRC Error Packets	0.0
□	🟩 Filtered Packets	0.0

Figure 11-1. *The Report Activity View*

This section contains the following topics:

- Gathering Statistics

- Generating Reports
- Deploying the Default Alert Profile

Gathering Statistics

If you want to view the statistical data of a group within your wireless network, you must instruct your Agents to send that data to the Enterprise Administrator. The Agents automatically send only data relevant to the Access Points on their subnets. For example, an Agent that manages Cisco-Aironet Access Points sends data relevant to that type of Access Point; it does not send information about Access Points from other manufacturers, such as Symbol.

Gathering statistics requires deploying a Gather Statistics deployment event. See *Chapter 13: Deploying Configurations* on page 161 for more information.

Generating Reports

After the Enterprise Administrator gathers information on Agent alerts or Access Point statistics, you can use the Report Statistics view to display as much or as little of that information as you need.

To generate a report:

1. Click `Report Statistics` from the Enterprise Administrator toolbar to access the Report Statistics view.
2. Select a site that has data that you want to view from the Groups window.
3. Select a category of alerts or events from which you want to select from the list at the top of the Report Statistics view.

   The categories available to you range from Agent alerts to firmware-specific events. These categories vary depending on the components of your wireless network.
4. Click `Daily Statistics`, `Weekly Statistics`, `Monthly Statistics`, or `Yearly Statistics` to set the range of data you want to view.
5. Select the types of alerts and events you want to view from the list at the bottom of the Report Statistics view.

To select an alert or event, enable the check box next to the event's description.

The Report Statistics view displays a graph of the different alerts or events that you selected. You can then print the report or export it into an XML file by selecting the **Print** or **Export XML File** links, respectively.

Deploying the Default Alert Profile

Before you can use the Report Statistics view to display information regarding Agent alerts, such as when an Agent discovers a new Access Point, you must first inform those Agents to forward those alerts to the Enterprise Administrator. You instruct Agents to forward alerts by deploying the default alert profile to those Agents. This profile informs the Agent of the IP address of the Enterprise Administrator. The Agent then uses this IP address to inform you of any Agent alerts that it encounters.

The default alert profile is automatically deployed with the addition of each site to the Enterprise Administrator. However, if the site was unable to receive the default alert profile—for example, because of a loss of Internet connection—you can deploy the default alert profile manually by using the Deploy Default Alert Profile event.

See *Chapter 13: Deploying Configurations* on page 161 for more information on how to create deployment events.

Chapter 12: Deploying Agents

The Mobile Manager uses Agents to track and manage wireless devices across your network. The Enterprise Administrator defines each site on your network as a collection of wireless devices managed by a specific Mobile Manager Agent.

When you add a new site into the Enterprise Administrator, you have the option of remotely deploying an Agent to that site. This section describes how to remotely deploy an Agent using the Add Site Wizard. It also provides you with information on how to deploy an Agent through a command-line interface.

NOTE To deploy an Agent to a remote system, you must be logged into your local system with an account that has administrative access to both your local system and the remote system. In addition, you must have administrative access to the Enterprise Administrator.

This section contains the following topics:

- Add Site Wizard
- Deploying Agents without the Administrator

Add Site Wizard

When you create a new site in the Enterprise Administrator, you can elect to deploy an Agent to that location. This option allows you to create a new site without pre-installing any software.

NOTE This process does not deploy a DHCP server to the new site. If your enterprise profiles require a DHCP server, you must ensure that one is already running at the new site.

Deploying Mobile Manager Agents to a Site

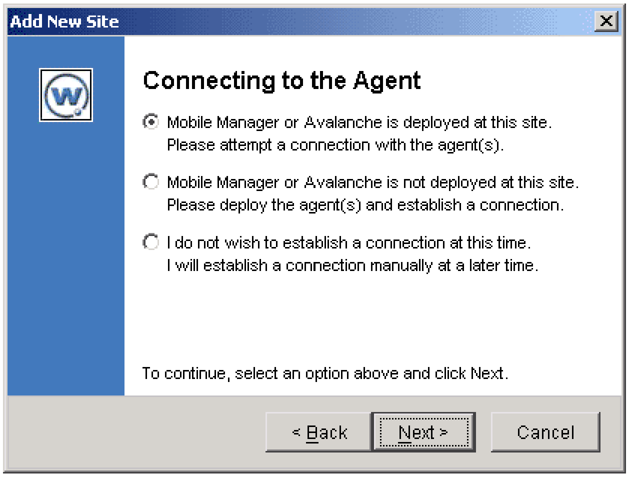
This section describes how you can deploy a new Mobile Manager Agent to a remote site.

NOTE The steps provided in this section also apply if you are installing both a Mobile Manager Agent and an Avalanche Agent at the new site.

To deploy an Agent to an individual site:

1 Follow the steps for creating a new site as described in *Adding Sites* on page 44.

2 When the *Connecting to the Agent* dialog box appears, select the option that allows you to deploy a new Agent to the site.



Add New Site

Connecting to the Agent

● Mobile Manager or Avalanche is deployed at this site.
Please attempt a connection with the agent(s).

○ Mobile Manager or Avalanche is not deployed at this site.
Please deploy the agent(s) and establish a connection.

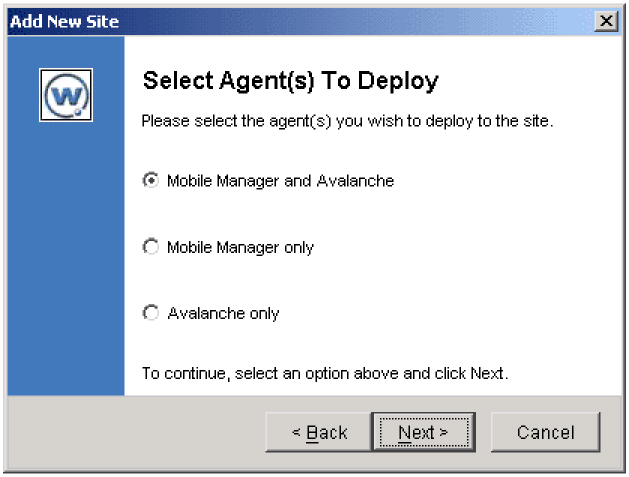
○ I do not wish to establish a connection at this time.
I will establish a connection manually at a later time.

To continue, select an option above and click Next.

Figure 12-1. *The Connecting to the Agent Dialog Box of the Add New Site Wizard*

3 Click `Next`.

A *Select Agent(s) To Deploy* dialog box appears.



Add New Site

Select Agent(s) To Deploy

Please select the agent(s) you wish to deploy to the site.

● Mobile Manager and Avalanche

○ Mobile Manager only

○ Avalanche only

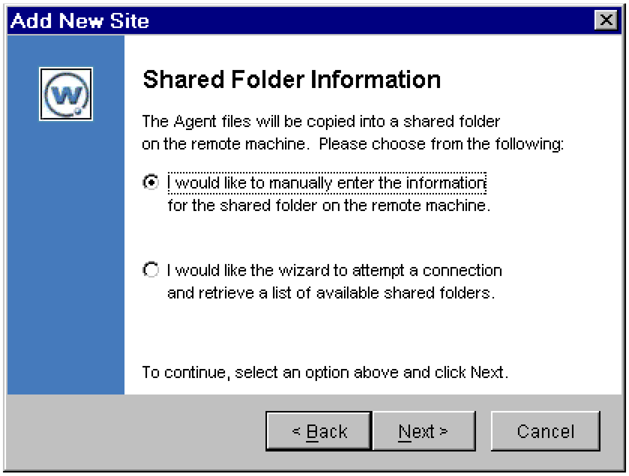
To continue, select an option above and click Next.

Figure 12-2. *The Select Agent(s) To Deploy Dialog Box*

4 Select the **Mobile Manager Only** option and click `Next`.

NOTE If you want to deploy both Agents to the site, select the **Mobile Manager and Avalanche** option.

A *Shared Folder Information* dialog box appears.



Add New Site

Shared Folder Information

The Agent files will be copied into a shared folder on the remote machine. Please choose from the following:

● I would like to manually enter the information for the shared folder on the remote machine.

○ I would like the wizard to attempt a connection and retrieve a list of available shared folders.

To continue, select an option above and click Next.

Figure 12-3. *A Shared Folder Information Dialog Box*

Select the appropriate option to launch a dialog box which either lets you manually type the shared folder information for the host system, or select from a list of retrieved shared folders.

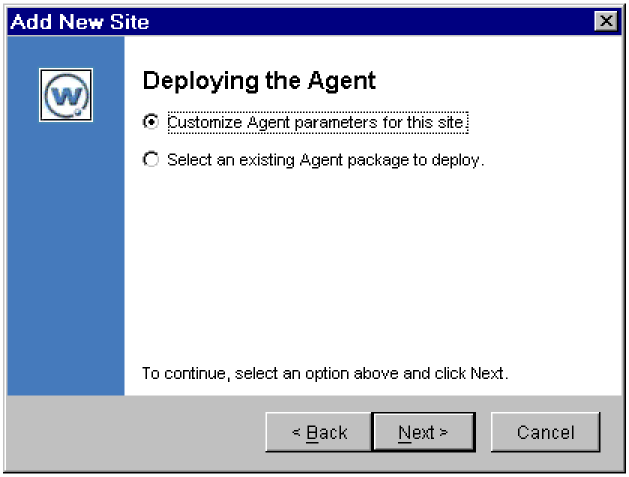
NOTE If you want the wizard to retrieve a list of available shared folders, a dialog box appears, requesting that you type the login name and password of an administrative account for the remote system.

Also, this option does not locate shared folders with names exceeding 12 characters.

---

5 After you select the shared folder, click `Next`.

A *Deploying the Agent* dialog box appears.



Add New Site

Deploying the Agent

● Customize Agent parameters for this site

○ Select an existing Agent package to deploy.

To continue, select an option above and click Next.

Figure 12-4. *A Second Deploying the Agent Dialog Box*

6 If you have previously deployed an Agent to another site, you can select the **Select an existing Agent package to deploy** option. A dialog box appears, which allows you to select the Agent package you want to use.

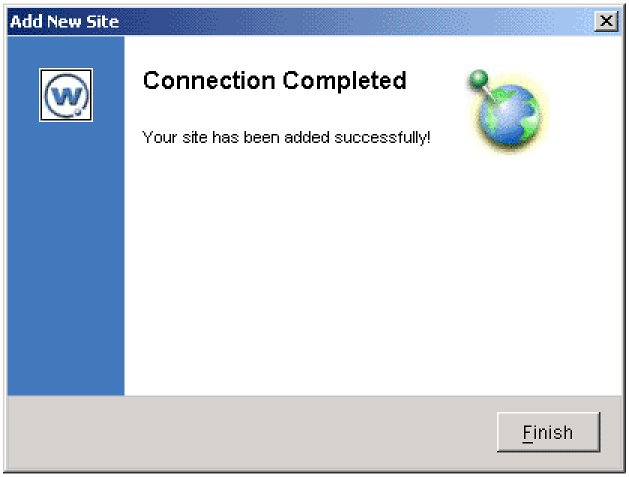
If you have not deployed an Agent before, or you want to create a new Agent deployment package, select the **Customize Agent parameters for this site** option.

7 If you selected the **Customize Agent parameters for this site** option, see *Creating an Agent Package* on page 152 to create an Agent package for this site.

If you selected the **Select an existing Agent package** option to deploy option, click `Next`. The Add Site Wizard displays a dialog box that allows you to select the Agent package.

8 Select a package and click `Next`.

The Mobile Manager attempts to deploy the package to the remote site. Once the deployment is successful, the *Connection Completed* dialog box appears.



Connection Completed

Your site has been added successfully!

Figure 12-5. *The Connection Completed Dialog Box*

9 Click `Finish`.

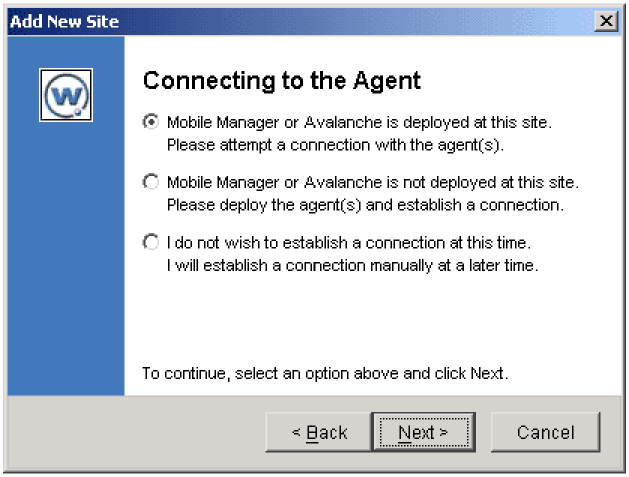
Deploying Avalanche Agents to a Site

This section describes how you can deploy a new Avalanche Agent to a remote site.

To deploy an Agent to an individual site:

1 Follow the steps for creating a new site as described in *Adding Sites* on page 44.

2 When the *Connecting to the Agent* dialog box appears, select the option that allows you to deploy a new Agent to the site.



Add New Site

Connecting to the Agent

● Mobile Manager or Avalanche is deployed at this site. Please attempt a connection with the agent(s).

○ Mobile Manager or Avalanche is not deployed at this site. Please deploy the agent(s) and establish a connection.

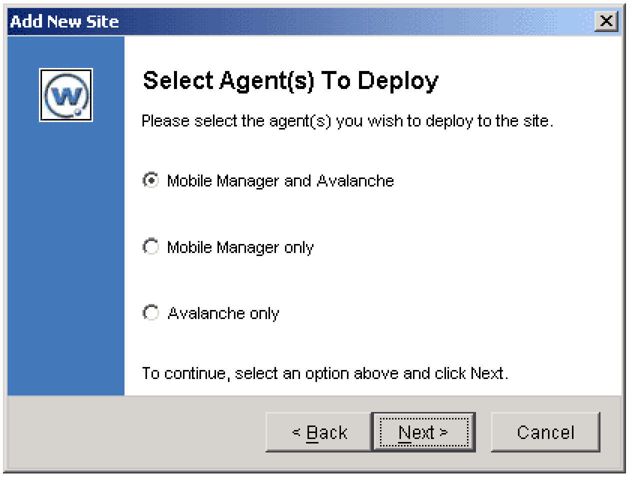
○ I do not wish to establish a connection at this time. I will establish a connection manually at a later time.

To continue, select an option above and click Next.

Figure 12-6. *The Connecting to the Agent Dialog Box of the Add New Site Wizard*

3 Click `Next`.

A *Select Agent(s) To Deploy* dialog box appears.



Add New Site

Select Agent(s) To Deploy

Please select the agent(s) you wish to deploy to the site.

● Mobile Manager and Avalanche

○ Mobile Manager only

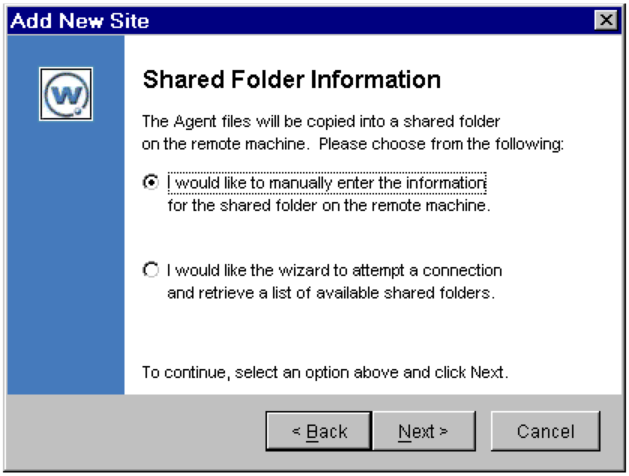
○ Avalanche only

To continue, select an option above and click Next.

Figure 12-7. *The Select Agent(s) To Deploy Dialog Box*

4 Select the **Avalanche Only** option and click `Next`.

A *Shared Folder Information* dialog box appears.



Shared Folder Information

The Agent files will be copied into a shared folder on the remote machine. Please choose from the following:

● I would like to manually enter the information for the shared folder on the remote machine.

○ I would like the wizard to attempt a connection and retrieve a list of available shared folders.

To continue, select an option above and click Next.

Figure 12-8. *A Shared Folder Information Dialog Box*

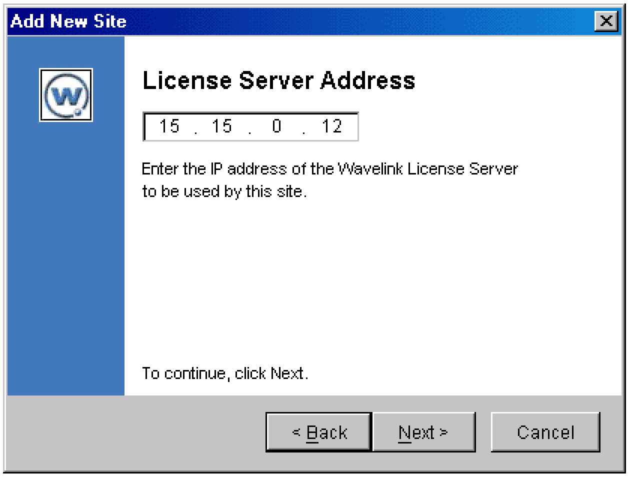
Select the appropriate option to launch a dialog box which either lets you manually type the shared folder information for the host system, or select from a list of retrieved shared folders.

NOTE If you want the wizard to retrieve a list of available shared folders, a dialog box appears, requesting that you type the login name and password of an administrative account for the remote system.

Also, this option does not locate shared folders with names exceeding 12 characters.

5 After you select the shared folder, click `Next`.

The *License Server Address* dialog box appears.



Add New Site

License Server Address

15 . 15 . 0 . 12

Enter the IP address of the Wavelink License Server to be used by this site.

To continue, click Next.

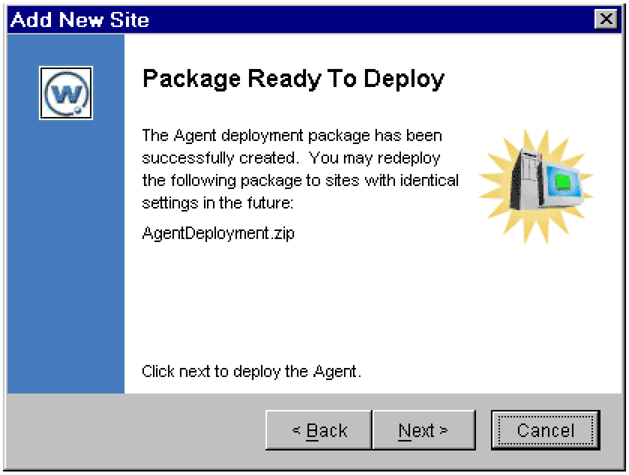
Figure 12-9. *The License Server Address Dialog Box*

6 Type the IP address of the system hosting your license server in the **License Server Address** text box.

Contact your Wavelink sales representative for more information on your license server and the Wavelink licensing process.

7 Click `Next`.

The *Package Ready for Deployment* dialog box appears.



Add New Site

Package Ready To Deploy

The Agent deployment package has been successfully created. You may redeploy the following package to sites with identical settings in the future:

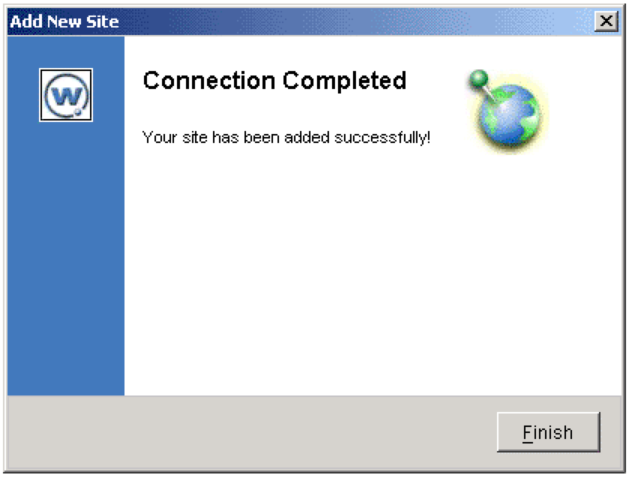
AgentDeployment.zip

Click next to deploy the Agent.

Figure 12-10. *The Package Ready to Deploy Dialog Box*

8 Click `Next`.

The Mobile Manager attempts to deploy the package to the remote site. Once the deployment is successful, the *Connection Completed* dialog box appears.



Add New Site

Connection Completed

Your site has been added successfully!

Figure 12-11. *The Connection Completed Dialog Box*

9 Click `Finish`.

Creating an Agent Package

When the Mobile Manager deploys an Agent to a remote site, it creates an Agent package, which contains the files the Agent needs to operate. Once you create an Agent package, you can reuse it on other remote systems, as long as the parameters you selected for the package remain applicable. For example, the adapter index value must match the specific network card for each remote system.

NOTE See *Add Site Wizard* on page 143 for information on how to deploy a previously-created Agent package to a new site.

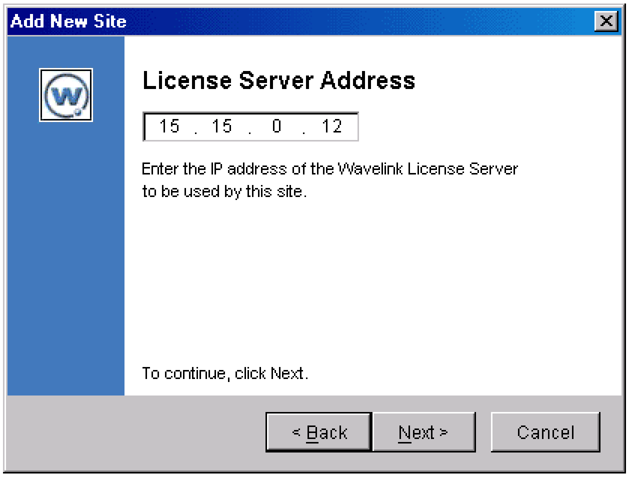
If you do not have an Agent package, or if you need to create a new one, the Add Site Wizard of the Enterprise Administrator allows you to create a new package.

To create an Agent package:

1 Follow the steps for creating a new site as described in *Adding Sites* on page 44, then follow the steps listed in *Add Site Wizard* on page 143.

2 From the *Deploying the Agent* dialog box, select the **Customize Agent parameters for this site** option and click `Next`.

The *License Server Address* dialog box appears.



Add New Site

License Server Address

15 . 15 . 0 . 12

Enter the IP address of the Wavelink License Server to be used by this site.

To continue, click Next.

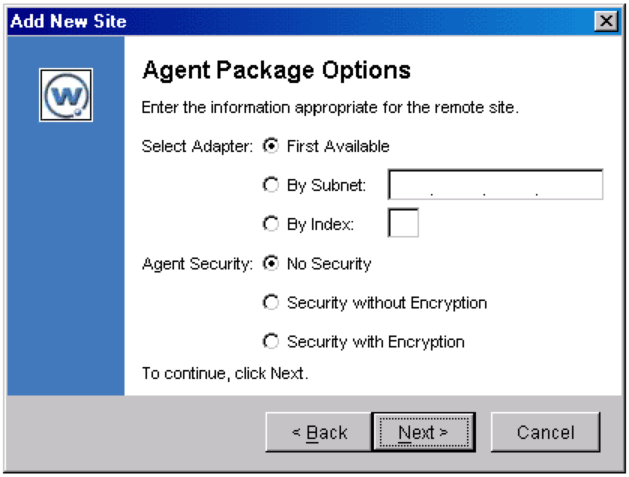
Figure 12-12. *The License Server Address Dialog Box*

3 Type the IP address of the system hosting your license server in the **License Server Address** text box.

Contact your Wavelink sales representative for more information on your license server and the Wavelink licensing process.

4 Click `Next`.

The *Agent Package Options* dialog box appears.



Add New Site

Agent Package Options

Enter the information appropriate for the remote site.

Select Adapter: ● First Available

○ By Subnet: . . .

○ By Index:

Agent Security: ● No Security

○ Security without Encryption

○ Security with Encryption

To continue, click Next.

Figure 12-13. *The Agent Package Options Dialog Box*

5 Select how you want the Agent to determine which network adapter card to use from the **Select Adapter** options.

To use the first network adapter card available on the system hosting the Agent, select the **First Available** option.

To use a network adapter card based on a subnet mask, select the **By Subnet** option and type the subnet mask for the network adapter card. For example, if the network adapter card was on a subnet `15.23.7.x` and the actual IP address for the card was `15.23.7.5`, you would type `15.23.7.0` in the **By Subnet** text box.

NOTE Do not use an actual IP address when using the **By Subnet** option. Using an actual IP address will prevent the Agent from communicating with the network.

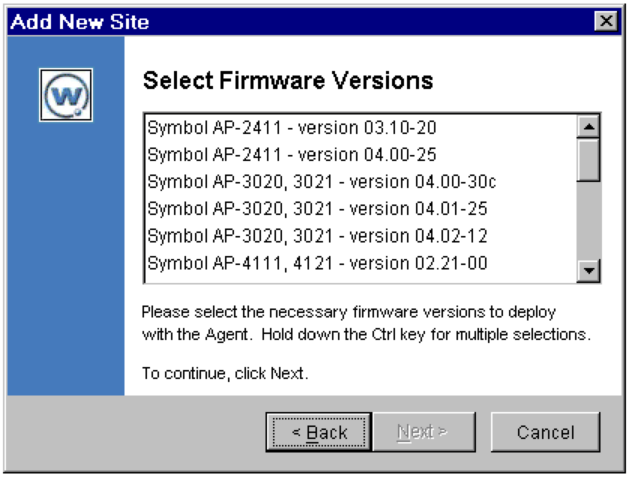
To assign a network adapter card by its index in the Windows registry, select the **By Index** option and type the index number.

6 Select one of the Agent Security options to set the security level for the Agent.

You can select from three security options when you deploy the Agent: **No Security**; **Security without Encryption**, which only prompts for a user name and password; and **Security with Encryption**, which prompts for a user name and password, as well as encrypts communication between the Enterprise Administrator and the Agent.

7 Click `Next`.

The *Select Firmware Versions* dialog box appears.



Add New Site

Select Firmware Versions

Symbol AP-2411 - version 03.10-20
Symbol AP-2411 - version 04.00-25
Symbol AP-3020, 3021 - version 04.00-30c
Symbol AP-3020, 3021 - version 04.01-25
Symbol AP-3020, 3021 - version 04.02-12
Symbol AP-4111, 4121 - version 02.21-00

Please select the necessary firmware versions to deploy with the Agent. Hold down the Ctrl key for multiple selections.

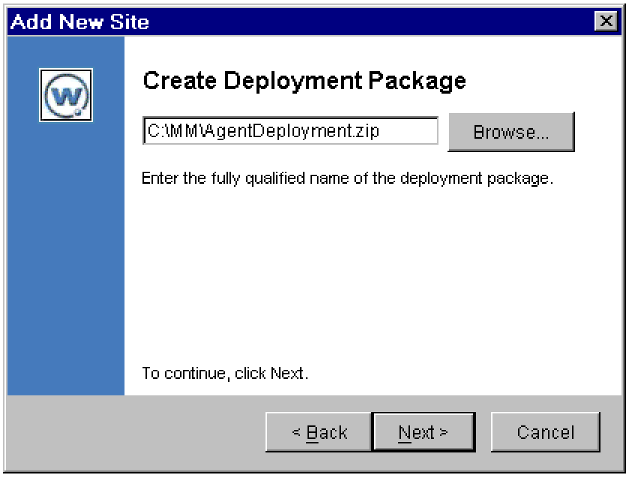
To continue, click Next.

Figure 12-14. *The Select Firmware Versions Dialog Box*

NOTE The more firmware versions you select, the larger the Agent package becomes and the longer it might take to deploy the Agent. If you are deploying an Agent using a slow connection, it is recommended that you select only those firmware versions that are required for your network.

8 Select one or more firmware versions and click `Next`.

The *Create Deployment Package* dialog box appears.



Add New Site

Create Deployment Package

C:\MM\AgentDeployment.zip

Enter the fully qualified name of the deployment package.

To continue, click Next.

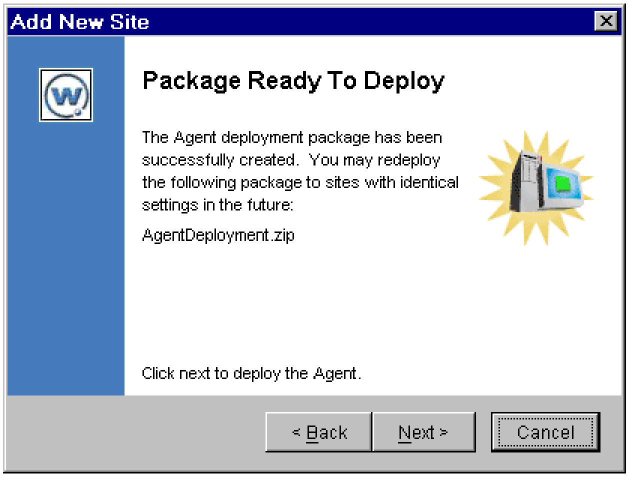
Figure 12-15. *The Create Deployment Package Dialog Box*

9 Type the fully qualified name for the Agent package and click `Next`.

NOTE The name for the Agent package must end with the .zip extension.

The Mobile Manager begins to create the Agent package. During this time, a *Preparing Package for Deployment* dialog box appears, displaying the progress of creating the new package.

After the Mobile Manager creates the Agent package, the *Package Ready for Deployment* dialog box appears.



Add New Site

Package Ready To Deploy

The Agent deployment package has been successfully created. You may redeploy the following package to sites with identical settings in the future:

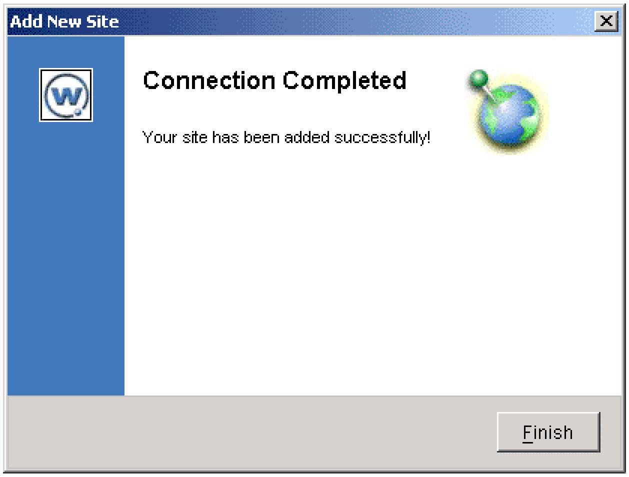
AgentDeployment.zip

Click next to deploy the Agent.

Figure 12-16. *The Package Ready to Deploy Dialog Box*

10 Click `Next`.

The Mobile Manager attempts to deploy the package to the remote site. Once the deployment is successful, the *Connection Completed* dialog box appears.



Add New Site

Connection Completed

Your site has been added successfully!

Figure 12-17. *The Connection Completed Dialog Box*

11 Click `Finish`.

Deploying Agents without the Administrator

The Add Site Wizard of the Enterprise Administrator provides you with an efficient means of deploying an Agent to a new site on your network. You also have the option of using a batch process to deploy multiple Agents to several locations on your network.

NOTE Before you initiate a remote deployment of Agents, you must have administrative access to both the local system from which you are deploying the Agents, and any remote systems to which you want to install an Agent.

Deploying an Agent without the Administrator requires three files:

- Deploy.exe, which deploys the Agent and its files
- Iserv.exe, which starts the Agent once it is installed
- unzip32.dll, which unzips the Agent deployment package

These files are located in the Administrator folder of the Mobile Manager Enterprise Edition working directory. You must also have an Agent deployment package, which contains all of the files needed to install and run an Agent on your network. This package is best created by following the steps listed in *Creating an Agent Package* on page 152.

NOTE This process does not deploy a DHCP server to the new site. If your enterprise profiles require a DHCP server, you must ensure that one is already running at the new site.

You use the Deploy.exe application to deploy an Agent. This application requires a specific set of command-line parameters to operate effectively. The available parameters are as follows:

/o The type of Agent to be deployed. Values are 0 for Mobile Manager only, 1 for Avalanche only, and 2 for both Agents.

Example: `/o1`

/c The computer name or IP address for the remote system to which the Agent is installed.

Example: `/c15.23.51.87`

/a The adapter options (for Mobile Manager Agents only). Values are -s for subnet of network card to which the Agent will bind, -a for the index of the network card, or -f for the first network card in found in the directory.

Example: `/a-s15.23.0.0`

/i The name of the file distributed to the remote system. This file is typically a ZIP file and can be either a fully qualified filename or a relative filename. If the value is a relative filename, the full file path is formed by appending the filename to the "local path" specified by the /x parameter.

Example: `/iC:\projects\deploy.zip`

/j If deploying Avalanche, this parameter contains the name of the ZIP file containing the Avalanche service.

Example: `/jAvalancheDeploy.zip`

/m The drive letter used locally when mapping to the remote system. If this parameter is left blank, deployment uses the first available drive letter.

Example: `/mC`

/s

The share name on the remote system. This parameter is combined with the /c parameter to designate the destination of the Agent.

Example: `/sdeploy`

/d

The path on the remote where the remote will execute its install service, IServ.exe.

Example: `/dC:\deploy`

/u

The name of the DLL that unzips the remote. The name used is unzip32.dll.

Example: `/uunzip32.dll`

/x

The path on the local system where the IServe.exe and unzip32.dll files are located. If the /i parameter does not contain a fully qualified file path, the value in this parameter is assumed to be the location of the Agent files.

Example: `/xC:\projects`

/w

The parent Wavelink path on the remote system.

Example: `/wc:\Program Files\Wavelink`

/q

The path for installing Mobile Manager. This path is relative to the parent Wavelink directory defined by the /w parameter.

Example: `/qMM\Program`

/r

The path for installing Avalanche. This path is relative to the parent Wavelink directory defined by the /w parameter.

Example: `/rAvalanche/Service`

Once the Deploy.exe application executes, it displays a numeric indicator of whether the deployment was successful. If the application returns a 0, the deployment succeeded. If the application returns any other number, an error occurred at some point during the process. The definition of these errors is designated by the Windows System Error Codes.

NOTE The IServ.exe application does not return information back to the local system; the only way to verify that the Agent has started correctly is by connecting to it through the Enterprise Administrator.

Batch Deployment of Agents

You can use the Deploy.exe, IServ.exe, unzip32.dll files, along with an Agent deployment package, to conduct a batch install of Agents to your network. This process requires that you create a script that automates the installation process.

Because the process for creating a batch install varies according to your network setup, this document does not describe how to conduct a batch install. If you require assistance with this process, please contact your Wavelink sales representative.

Chapter 13: Deploying Configurations

The Enterprise Administrator allows you to control when group configuration settings are deployed to on the wireless network. This feature allows you to ensure that configurations occur only during periods of low network activity.

Often wireless devices might become unavailable when they receive new configuration settings. These devices become unavailable because their firmware requires a reset to save the new changes. Consequently, correct deployment of configuration settings is essential to allow mobile device users access to the network when they need it.

NOTE Deploying group configuration settings can significantly affect network performance and mobile device access. It is recommended that you only deploy settings during periods of low network activity.

This section contains the following topics:

- Types of Deployment Events
- One-time Versus Recurring Deployment Events
- Creating One-Time Deployment Events
- Creating Recurring Deployment Events
- Deploying Profiles Immediately
- Deleting Deployment Events

Types of Deployment Events

The Mobile Manager includes several types of deployment events, allowing you to customize setting deployments to best suit the needs of the wireless network.

The types of deployment events include:

Deploy Default Alert Profile Instructs the Mobile Manager to deploy the default alert profile. This profile informs the Agent of the IP address of the Enterprise Administrator

Deploy Settings to Avalanche Instructs the Mobile Manager to deploy settings to the Avalanche Agent.

Deploy Settings to Mobile Manager Deploys settings to the Mobile Manager Agent.

Gather Mobile Manager Statistics Instructs the Mobile Manager to gather statistical data from Mobile Manager Agents within a group.

Update User Accounts (Mobile Manager Only) Updates the Mobile Manager Agents with new or changes user account information.

One-time Versus Recurring Deployment Events

You can deploy settings to groups using one-time or recurring events. A one-time event, as the name implies, occurs only once on a specific date. A recurring event occurs repeatedly on multiple days and times.

When a deployment event occurs, the Mobile Manager sends the information related to that event to multiple sites within the selected group. As each site successfully updates, the Mobile Manager begins updating another site within the group, until either all sites are updated or the deployment event ends. After a deployment event ends, you can access the Alarm Browser of the Monitor Activity view to see which sites received the complete update.

NOTE Once the Mobile Manager starts sending event information to a site on your network, it continues the deployment process until it is completed—even if the deployment event's end time is reached.

Consider the following example. An organization is using the Mobile Manager Enterprise Edition to manage a group of 60 sites. These sites are to receive a new Access Point profile through a deployment event that starts at 10:00pm and ends at 12:00am. When the events starts at 10:00pm, the Mobile Manager sends the new profile to the sites. At 12:00am, when the deployment event ends, the Mobile Manager is still in the process of updating 10 sites.

Even though the deployment event's end time has been reached, the Mobile Manager continues to update these 10 sites until they completely receive the new profile. However, any remaining sites within the group do not get updated. If this deployment event was a one-time event, those remaining sites would not get updated until a new deployment event was created. If this deployment event was a recurring event, the Mobile Manager gives those remaining sites top priority to receive the new profile when the deployment event next occurs.

Creating One-Time Deployment Events

Whether you use a recurring or one-time deployment event depends on the role of profiled Access Points on your network. If these Access Points retain their configurations for extended periods of time, a one-time deployment event is appropriate.

NOTE Deploying Access Point profiles can significantly affect network performance and mobile device access. It is recommended that you only deploy profiles during periods of low network activity.

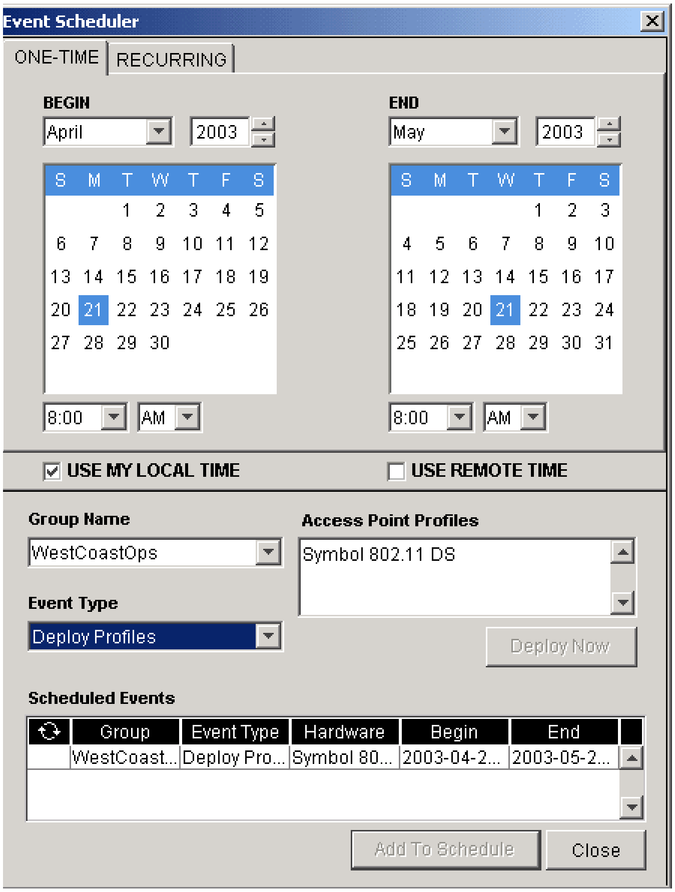
If you want to gather statistics for a group of Access Points, you might want to establish a recurring deployment event. See *Creating Recurring Deployment Events* on page 165 for more information.

To set a one-time deployment event:

1 Select `Event Schedule` from the **Tools** menu.

The *Event Scheduler* dialog box appears.

2 Click the One-Time tab.



Event Scheduler

ONE-TIME | RECURRING

BEGIN: April 2003

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

8:00 AM

END: May 2003

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

8:00 AM

☑ USE MY LOCAL TIME ☐ USE REMOTE TIME

Group Name: WestCoastOps

Access Point Profiles: Symbol 802.11 DS

Event Type: Deploy Profiles

Deploy Now

Scheduled Events

	Group	Event Type	Hardware	Begin	End
	WestCoast...	Deploy Pro...	Symbol 80...	2003-04-2...	2003-05-2...

Add To Schedule | Close

Figure 13-1. *The One-Time tab of the Event Scheduler Dialog Box*

3 Select the starting date for the event by using the calendar and lists located in the Begin section.

You must set the month, year, day, and time for a starting date.

4 Select the ending date for the event by using the calendar and lists located in the End section.

You must set the month, year, day, and time for an ending date.

5 Enable the **Use My Local Time** check box if you want to deploy the event using the time zone for the system hosting the Enterprise Manager.

Enable the **Use Remote Time** check box if you want to deploy the event using the time zones for the Agents affected by the deployment event.

NOTE If you enable the **Use Remote Time** check box for a group that has Agents in multiple time zones, the deployment event occurs multiple times—once for each time zone.

---

6. Select the group receiving the profile deployment from the **Group Name** list.
7. Select the profiles you want to deploy from the **Access Point Profiles** list.
8. Select an event from the **Event Type** list.
9. Click `Add to Schedule` to activate the deployment event.

   The event appears in the Scheduled Events list located at the bottom of the *Event Scheduler* dialog box.

NOTE If you select multiple profiles for an event, each profile receives its own entry in the Scheduled Events list.

---

10. Click `OK` to return to the Enterprise Administrator.

Creating Recurring Deployment Events

If you want to deploy a profile over a series of days, as opposed to one specific date, you can use a recurring deployment event. Recurring events are useful if you have a very large number of sites that need to receive a new profile.

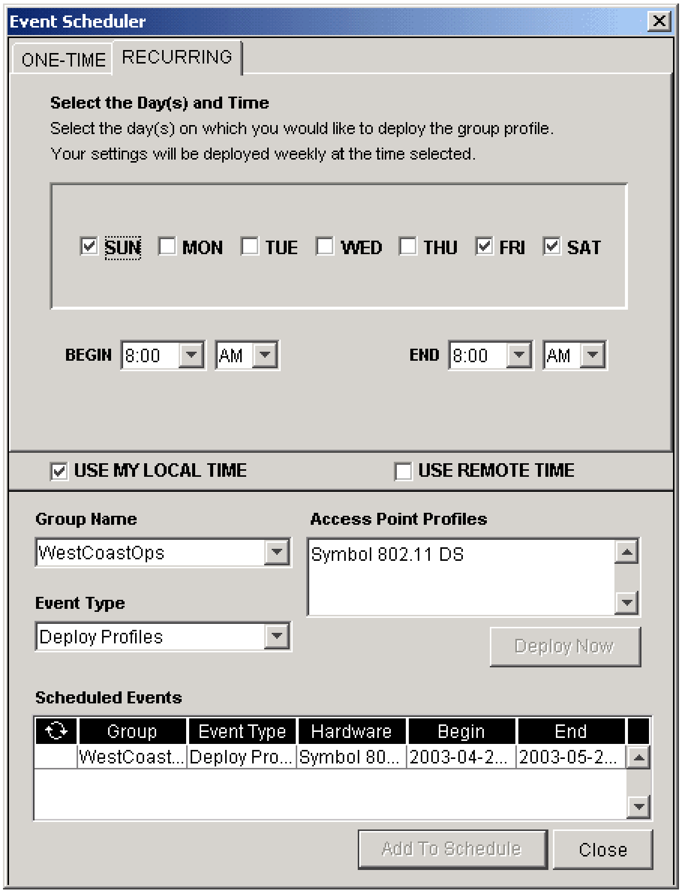
NOTE Deploying Access Point profiles can significantly affect network performance and mobile device access. It is recommended that you only deploy profiles during periods of low network activity.

To set a recurring deployment event:

1. Select `Events Schedule` from the **Tools** menu.

The *Event Scheduler* dialog box appears.

2 Click the Recurring tab.



Event Scheduler

ONE-TIME | RECURRING

Select the Day(s) and Time

Select the day(s) on which you would like to deploy the group profile. Your settings will be deployed weekly at the time selected.

☑ SUN □ MON □ TUE □ WED □ THU ☑ FRI ☑ SAT

BEGIN 8:00 AM END 8:00 AM

☑ USE MY LOCAL TIME □ USE REMOTE TIME

Group Name: WestCoastOps

Access Point Profiles: Symbol 802.11 DS

Event Type: Deploy Profiles

Scheduled Events

	Group	Event Type	Hardware	Begin	End
	WestCoast...	Deploy Pro...	Symbol 80...	2003-04-2...	2003-05-2...

Figure 13-2. *The Recurring Tab of the Event Scheduler Dialog Box*

3 Select the days you want the event to occur by enabling the check box next to the desired days.

4 Select the starting time for the event by using the lists in the Begin section.

5 Select the ending time for the event by using the lists in the End section.

6 Enable the **Use My Local Time** check box if you want to deploy the event using the time zone for the system hosting the Enterprise Manager.

Enable the **Use Remote Time** check box if you want to deploy the event using the time zones for the Agents affected by the deployment event.

NOTE If you enable the **Use Remote Time** check box for a group that has Agents in multiple time zones, the deployment event occurs multiple times—once for each time zone.

7 Select the group receiving the profile deployment from the **Group Name** list.

8 Select the profiles you want to deploy from the **Access Point Profiles** list.

9 Select an event from the **Event Type** list.

10 Click `Add to Schedule` to activate the deployment event.

The event appears in the Scheduled Events list located at the bottom of the *Event Scheduler* dialog box.

NOTE If you select multiple profiles for an event, each profile receives its own entry in the Scheduled Events list.

11 Click `OK` to return to the Enterprise Administrator.

If you create a recurring deployment event for a profile, it is recommended that you remove the event after all sites receive the new profile. Otherwise, the Mobile Manager will continue to send the profile during each occurrence of the deployment event, which can take up unnecessary bandwidth for your network.

NOTE When you place your mouse over a recurring event in the Schedule Events list, a tooltip appears indicated the days on which that event occurs.

Deploying Profiles Immediately

On occasion, you might need to deploy a profile immediately. For example, you might decide to re-assign Access Points within a group to a new profile to solve a network problem or improve network traffic. You can accomplish this task by using Mobile Manager's Deploy Now feature.

Depending on the number of Access Points within a group and their location within your enterprise, profile deployment can take several minutes to several hours to accomplish. During that time, Access Points are frequently reset, possibly preventing mobile device users from accessing the network.

NOTE Deploying Access Point profiles can significantly affect network performance and mobile device access. It is highly recommended that you only deploy profiles during periods of low network activity.

To deploy a profile immediately:

1 Select `Event Schedule` from the **Tools** menu.

   The *Event Scheduler* dialog box appears.

2 Click either the One-Time or Recurring tab.

3 Select the group receiving the profile deployment from the **Group Name** list.

4 Select the profiles you want to deploy from the **Access Point Profiles** list.

5 Select `Deploy Profiles` from the **Event Type** list.

6 Click `Deploy Now`.

   A dialog box appears, asking you to confirm that you want to deploy the selected profiles.

7 Click `Yes`.

The Enterprise Administrator deploys the new or updated profiles to the assigned Agents.

Deleting Deployment Events

As your enterprise network changes with time, deployment events can become obsolete. Also, other network concerns might arise that take priority over profile deployment. When these and other situations occur, you can delete a deployment event.

To delete a deployment event:

1 Select `Profile Deployment Schedule` from the **Tools** menu.

  The *Event Scheduler* dialog box appears.

2 Right-click the event you want to delete from the **Scheduled Events** list.

3 Select `Remove From Schedule` from the menu that appears.

  A dialog box appears, asking you to confirm that you want to delete the event.

4 Click `Yes` to delete the event.

Close the dialog box to return to the Enterprise Administrator.

Chapter 14: Statistical Alerts

Statistical alerts are alerts the Mobile Manager generates based on Access Point statistics contained in the SNMP MIB.

Statistical alerts differ from other network alerts in two ways:

- The Agent only generates statistical alerts during specific time periods
- Statistical alerts are configurable

NOTE You can only configure statistical alerts if you use Access Point profiles.

When you create a statistical alert, you instruct the Agents at each site to monitor a specific statistical value of your Access Points. The Agent checks this value each time it verifies the profile settings for those Access Points. You can also modify or delete these alerts at any time.

This section contains the following topics:

- Configuring New Statistical Alerts
- Editing Statistical Alerts
- Deleting Statistical Alerts
- Descriptions of Statistical Alert Properties

Configuring New Statistical Alerts

Configuring a new statistical alert involves the following steps:

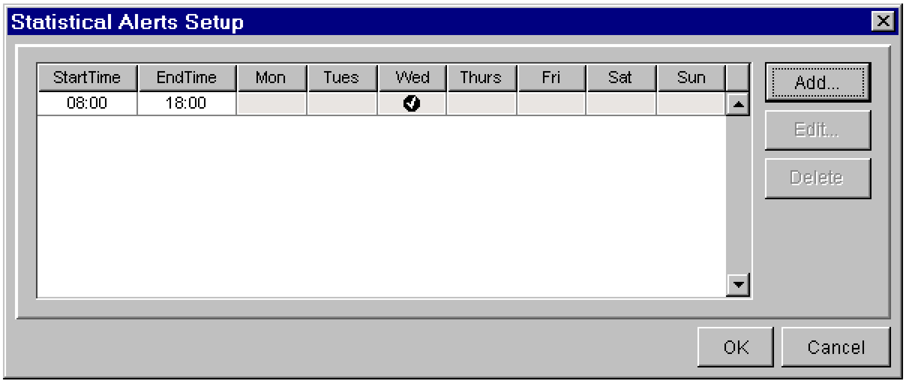
1. Add a new alert.
2. Determine when the Mobile Manager monitors this alert.
3. Configure all appropriate radio values.
4. Configure all appropriate Ethernet values.
5. Save the new alert.

These steps are described further in the following sections.

To add a new alert:

1 From the *Access Point Profile* dialog box, click `Stat Alerts`.

The *Statistical Alerts Setup* dialog box appears.



Statistical Alerts Setup

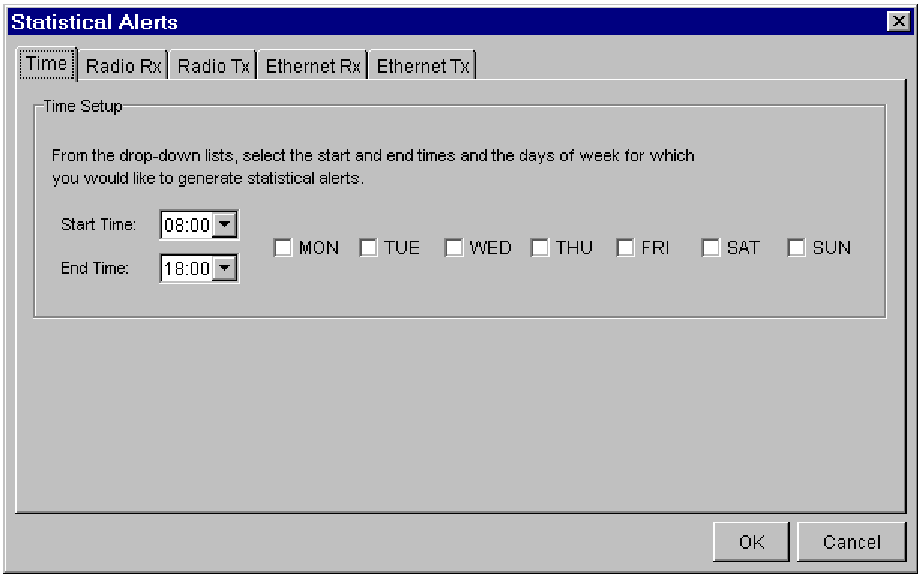
StartTime	EndTime	Mon	Tues	Wed	Thurs	Fri	Sat	Sun
08:00	18:00			✓				

Figure 14-1. *The Statistical Alerts Setup Dialog Box*

The days and times that the Agent checks for each statistical alert appears in this dialog box. These alerts apply to all Access Points associated with the current Access Point profile.

2 Click `Add`.

A new dialog box appears.



From the drop-down lists, select the start and end times and the days of week for which you would like to generate statistical alerts.

Start Time: 08:00

End Time: 18:00

□ MON □ TUE □ WED □ THU □ FRI □ SAT □ SUN

Figure 14-2. *The Time Tab of the Statistical Alerts Dialog Box*

To determine when the Mobile Manager monitors this alert:

1 Click the Time tab.

2 Select the time you want the Agent to start checking for the alert from the **Start Time** list.

3 Select the time you want the Agent to stop checking for the alert from the **End Time** list.

4 Select the days you want the Agent to check for this alert by enabling the checkbox next to each day.

To configure radio properties for the alert:

1 Click the Radio tab.

NOTE For Cisco-Aironet Access Points, click either the Radio Rx or the Radio Tx tab.

2 Edit the minimum and maximum values for each option you want the Agent to check.

A minimum value of 0 means the Agent does not generate an alert based on the minimum value for that option.

A maximum value of 2147483647 means the Agent does not generate an alert based on the maximum value for that option.

See *Descriptions of Statistical Alert Properties* on page 176 for more information on the options in this screen.

3 Click the Radio 2 tab.

NOTE For Cisco-Aironet Access Points, click either the Radio Rx or the Radio Tx tab.

---

4 Edit the minimum and maximum values for each option you want the Agent to check.

A minimum value of 0 means the Agent does not generate an alert based on the minimum value for that option.

A maximum value of 2147483647 means the Agent does not generate an alert based on the maximum value for that option.

See *Descriptions of Statistical Alert Properties* on page 176 for more information on the options in this screen.

To configure Ethernet properties for the alert:

1 Click the Ethernet tab.

NOTE For Cisco-Aironet Access Points, click either the Ethernet Rx or the Ethernet Tx tab.

---

2 Edit the minimum and maximum values for each option for which you want the Agent to check.

A minimum value of 0 means the Agent does not generate an alert based on the minimum value for that option.

A maximum value of 2147483647 means the Agent does not generate an alert based on the maximum value for that option.

See *Descriptions of Statistical Alert Properties* on page 176 for more information on the options in this screen.

To save the new alert:

1 Once you configure the different radio and Ethernet options for the alert, click `Apply`.

2 To return to the Administrator, click `OK`.

Editing Statistical Alerts

You can edit a statistical alert at any time.

To edit a statistical alert:

1 From the *Access Point Profiles* dialog box, click `Stat Alerts`.

2 Select an alert from the list.

3 Click `Edit`.

4 Edit the alert as necessary.

5 Click `Apply`.

Deleting Statistical Alerts

You can remove a statistical alert at any time.

To remove a statistical alert:

1 From the *Access Point Profiles* dialog box, click `Stat Alerts`.

2 Select an alert from the list.

3 Click `Delete`.

Descriptions of Statistical Alert Properties

This section describes the different alert properties that you can configure for statistical alerts through the tabs on the *Statistical Alerts* dialog box.

Radio Properties (3COM, Ericsson, Intel, Nortel, and Symbol)

The following are properties available for 3COM, Ericsson, Intel, Nortel, and Symbol Access Points.

Associated Mobile Devices Number of mobile devices currently associated with this Access Point.

Broad/Multicasts Octets Rcvd Number of broadcast/multicast bytes that have been successfully received.

Broad/Multicasts Octets Sent Number of broadcast/multicast bytes that have been successfully transmitted.

Broad/Multicasts Pkts Rcvd Number of broadcast/multicast packets that have been successfully received.

Broad/Multicasts Pkts Sent Number of broadcast/multicast packets that have been successfully transmitted.

Data Octets Rcvd Number of data bytes that have been successfully received.

Data Octets Sent Number of data bytes that have been successfully transmitted.

Data Pkts Rcvd Number of data packets that have been successfully received.

Data Pkts Sent Number of data packets that have been successfully transmitted.

Encrypted Pkts Rcvd Number of encrypted packets that have been successfully received.

Encrypted Pkts Sent Number of encrypted packets that have been successfully transmitted.

Pkts With Collisions Number of packets that suffered at least one collision.

Pkts With Max Collisions Number of packets that suffered the maximum number of collisions.

Pkts Without Collisions Number of packets without collisions.

Rcvd CRC Errors Number of packets that were received but had CRC errors.

Rcvd Duplicate Pkts Number of packets that were received but were duplicates of packets previously received. This is usually an indication that the sending unit did not receive an acknowledgement.

S Broad/Multicasts Pkts Rcvd Number of system broadcast/multicast packets (includes beacons) that have been successfully received.

S Broad/Multicasts Pkts Sent Number of system broadcast/multicast packets (includes beacons) that have been successfully transmitted.

Successful Fragment Pkts Number of packets that were fragmented and for which all fragments were acknowledged.

Successful Reassembles Number of packets that were reassigned and successfully reassembled.

System Pkts Rcvd Number of system packets (includes probe operations packets) that have been successfully received.

System Pkts Sent Number of system packets (includes probe operations packets) that have been successfully transmitted.

Total Collisions Number of collisions that have occurred on the interface. A collision on the RF interface means that an ACK was not received or that a RTS was not answered by a CTS.

Total Fragments Rcvd Number of packets fragments that have been received.

Total Fragments Sent Number of packets fragments that have been sent.

Unsuccessful Fragment Pkts Number of packets that were fragmented but for which one or more fragments were not acknowledged.

Unsuccessful Reassembles Number of packets that were unsuccessfully reassembled.

Radio Received Properties (Cisco-Aironet Only)

The following are properties available for Cisco-Aironet Access Points.

CRC Errors Number of cyclic redundancy check (CRC) errors that were detected in a received packet.

Discarded Packets Number of packets that were discarded because the Access Point had a temporary overload of packets to handle.

Duplicate Packets Number of packets that were received twice because an acknowledgment got lost and then the sender retransmitted the packet.

Filtered Packets Number of packets discarded due to an applied filter.

Forwardable Packets Number of Ethernet packets forwardable from the Ethernet interface to other interfaces.

Lifetime Exceeded Number of packets discarded because they were too old.

Multicast Packets Number of packets received that were sent as a transmission to a set of nodes.

Overrun Packets Number of packets that were discarded because the Access Point had an overload of packets to handle.

Total Bytes Total bytes received.

Total Errors Total errors received.

Unicast Packets Number of packets received using point-to-point communication.

WEP Errors Number of encryption errors.

Radio Transmitted Properties (Cisco-Aironet Only)

The following are additional radio properties available for Cisco-Aironet Access Points.

Cancelled AID Packets dropped by a repeater because it roamed to a different parent during a retransmission attempt. The AID (association ID) is assigned by an Access Point to a station with which it is associated.

Cancelled Assoc. Lost Packets dropped due to a station's loss of association with the Access Point or a repeater's loss of association with its parent.

Discarded Packets Number of packets that were discarded because the Access Point had a temporary overload of packets to handle.

Filtered Packets Number of packets discarded due to an applied filter.

Forwardable Packets Number of Ethernet packets forwardable from the Ethernet interface to other interfaces.

Lifetime Exceeded Number of packets discarded because they were too old.

Max Retry Packets Number of times request to send (RTS) reached the maximum retry number.

Multicast Packets Number of packets received that were sent as a transmission to a set of nodes.

Total Bytes Total bytes transmitted.

Total Errors Total errors transmitted.

Total Retries Total number of retries occurring for each port.

Unicast Packets Number of packets sent using point-to-point communication.

Ethernet Properties (3COM, Ericsson, Intel, Nortel, and Symbol)

The following are properties available for 3COM, Ericsson, Intel, Nortel, and Symbol Access Points.

Broad/Multicasts Transmitted Number of Ethernet broadcasts/multicasts successfully transmitted.

Packets Discarded (bad crc) Number of packets discarded due to CRC errors.

Packets Discarded (no buffer) Number of packets discarded due to lack of available buffers in the Access Point.

Packets Filtered by Type Number of packets discarded due to type or address filters applied.

Packets Forwarded Number of Ethernet packets forwarded from the Ethernet interface to other interfaces.

Packets Sent Number of packets sent by this Ethernet port.

Packets Unknown Destination Number of packets discarded due to unknown destination (for example, no database entry).

Packets with >1 Collision Number of packets that suffered more than one collision.

Packets with 1 Collision Number of packets that suffered at least one collision.

Packets with Late Collisions Number of packets that suffered late collisions.

Packets with Max Collisions Number of packets that suffered more than the maximum number of collisions.

Pkts Seen Number of packets that have been seen on the Ethernet interface. Most of these packets are for stations other than those associated with this Access Point.

Transmits Deferred (too busy) Number of times the Access Point had to defer transmit requests on Ethernet due to busy medium.

Unicasts Received Number of unicasts received.

Ethernet Received Properties (Cisco-Aironet Only)

The following are properties available for Cisco-Aironet Access Points.

CRC Errors Number of cyclic redundancy check (CRC) errors that were detected in a received packet.

Discarded Packets Number of packets that were discarded because the Access Point had a temporary overload of packets to handle.

Duplicate Packets Number of packets that were received twice because an acknowledgment got lost and then the sender retransmitted the packet.

Filtered Packets Number of packets discarded due to an applied filter.

Forwardable Packets Number of Ethernet packets forwardable from the Ethernet interface to other interfaces.

Lifetime Exceeded Number of packets discarded because they were too old.

Multicast Packets Number of packets received that were sent as a transmission to a set of nodes.

Overrun Packets Number of packets that were discarded because the Access Point had a temporary overload of packets to handle.

Total Bytes Total bytes received.

Total Errors Total errors received.

Unicast Packets Number of packets received using point-to-point communication.

WEP Errors Number of encryption errors.

Ethernet Transmitted Properties (Cisco-Aironet Only)

The following are additional Ethernet properties available for Cisco-Aironet Access Points.

Cancelled AID Packets dropped by a repeater because it roamed to a different parent during a retransmission attempt. The AID (Association ID) is assigned by an Access Point to a station with which it is associated.

Cancelled Assoc. Lost Packets dropped due to a station's loss of association with the Access Point or a repeater's loss of association with its parent.

Discarded Packets Number of packets that were discarded because the Access Point had a temporary overload of packets to handle.

Filtered Packets Number of packets discarded due to an applied filter.

Forwardable Packets Number of Ethernet packets forwardable from the Ethernet interface to other interfaces.

Lifetime Exceeded Number of packets discarded because they were too old.

Max Retry Packets Number of times Request to Send (RTS) reached the maximum retry number.

Multicast Packets Number of packets received that were sent as a transmission to a set of nodes.

Total Bytes Total bytes transmitted.

Total Errors Total errors transmitted.

Total Retries Total number of retries occurring for each port.

Unicast Packets Number of packets sent using point-to-point communication.

Index