



**Version 1.7.6 User's Guide  
Enterprise Edition**

*Revised 10/19/05*

11335 NE 122nd Way  
Suite 300  
Kirkland, Washington 98034  
Telephone: (425) 823-0111  
Web site: [www.wavelink.com](http://www.wavelink.com)

E-mail: [info@wavelink.com](mailto:info@wavelink.com)

No part of this publication may be reproduced or used in any form without permission in writing from Wavelink Corporation. This includes electronic or mechanical means, such as photocopying, recording, or information storage and retrieval systems. The material in this manual is subject to change without notice.

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™ 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. Unicenter™ is a registered trademark of Computer Associates. Proxim™ is a registered trademark of Proxim Inc. Dell™ is a registered trademark of Dell, Inc.

# Table of Contents

<b>Chapter 1: Introduction</b>	<b>7</b>
About This Document	7
Document Assumptions	7
Document Conventions	8
Managing Networks with Mobile Manager	8
Components of Mobile Manager	9
Location Management: Sites and Groups	9
Site-level Tools	10
<b>Chapter 2: Installation</b>	<b>11</b>
Before You Begin	11
Understanding Your Network Layout	11
Locating Access Points	12
Network Segmentation	12
Internet Connectivity	12
Partitioning Your Licenses	13
Wireless Device Access	13
Requirements	14
Hardware Requirements	14
Software Requirements	16
Firmware Requirements	16
Supported Client Software	16
Supported Devices	17
Determining Agent Placement	17
Centralized Agent Installation	17
Distributed Agent Installation	19
Installing Mobile Manager Enterprise	20
Activating Mobile Manager Enterprise	22
Installing Mobile Device Enablers	25
Downloading the Enabler	27
Downloading Hex Files	27
Configuring the Enabler	33
<b>Chapter 3: Enterprise Management Console</b>	<b>35</b>
Starting the Enterprise Management Console	35
Understanding Enterprise Management Console Views	37
Monitor Activity View	37
Configure Network View	42
Report Statistics View	45
Groups Window	46
Search	47
Setting Enterprise Management Console Preferences	48
Selecting the Location of Network Services	49

Configuring the Alarm Browser .....	50
Controlling Site Communication .....	51
User Accounts .....	53
Creating User Accounts .....	55
Editing User Accounts .....	57
Deleting User Accounts .....	57
Viewing Account Status .....	58
Changing Account Passwords .....	58
Deploying User Accounts .....	59
Using the Task Scheduler .....	70
Adding Tasks .....	71
Editing Tasks .....	73
Deleting Tasks .....	74
Running Tasks Immediately .....	75
Viewing Task Progress .....	76
Rescheduling Tasks .....	77
Deleting Completed Tasks .....	78
<b>Chapter 4: Managing Locations</b> .....	<b>81</b>
Sites .....	82
Creating Sites .....	82
Importing Sites .....	130
Deleting Agents .....	138
Deleting Sites .....	146
Configuring an HTTP Proxy .....	147
Groups .....	149
Adding Sites to Groups .....	150
Configuring Components at the Site Level .....	151
Accessing Site Tools .....	151
Site Management and the Enterprise Management Console .....	151
Deleting Groups .....	152
<b>Chapter 5: Managing Access Points</b> .....	<b>153</b>
Defining Device Access Privileges .....	154
Cisco IOS Access Privileges .....	157
Creating Access Point Profiles .....	160
Configuring Profiles .....	162
Modifying Profiles .....	165
Deleting Profiles .....	165
Refreshing Profiles .....	166
Determining Which Access Point Properties to Use .....	166
Scheduling Profiles .....	171
Applying Access Point Settings .....	174
Updating Access Point Firmware .....	186
Types of Firmware Support .....	186
Creating Firmware Packages .....	187

---

Deploying Firmware Packages .....	192
<b>Chapter 6: Managing Network Settings</b>	<b>205</b>
Assigning ESS IDs .....	205
Managing IP Addresses .....	207
Overview of Assigning IP Addresses .....	207
Assigning IP Addresses .....	208
Removing IP Addresses .....	212
Modifying Subnet Masks and Gateway IP Addresses .....	212
Assigning a Mobile Device Agent to Mobile Devices .....	215
Deploying Network Settings .....	217
Deploying Settings for All Devices .....	217
Deploying Access Point Settings .....	227
Deploying Mobile Device Settings .....	238
<b>Chapter 7: Managing Mobile Devices</b>	<b>251</b>
Managing Software .....	252
Creating Software Collections .....	253
Installing Software Packages .....	257
Defining Selection Criteria .....	265
Building Selection Criteria .....	269
Enabling Collections and Packages .....	277
Disabling Collections and Packages .....	278
Deleting Packages and Collections .....	280
Refreshing the Software Collections Manager .....	281
Synchronizing Mobile Device Software .....	282
Adding Synchronization Events .....	283
Excluding Dates and Times .....	292
Setting Maximum Simultaneous Updates .....	292
Deleting Orphaned Packages .....	293
Automatic Synchronization .....	294
Managing Licenses .....	294
Setting COM Ports .....	295
Authenticating Mobile Devices .....	295
Deploying Settings to Mobile Devices .....	297
<b>Chapter 8: Managing Security Settings</b>	<b>309</b>
Building Access Control Lists .....	311
Adding MAC Addresses .....	312
Modifying Very Large Access Control List Entries .....	314
Removing Very Large Access Control List Entries .....	316
Importing and Exporting Access Control List Files .....	318
Deploying Access Control Lists .....	322
Wired Equivalent Privacy (WEP) .....	330
Types of WEP Key Deployments .....	331
Configuring WEP Keys .....	331

Automatic WEP Rotation . . . . .	332
Configuring Automatic WEP Rotation . . . . .	333
Stopping Automatic WEP Rotation . . . . .	337
Automatic WEP Rotation and Cisco IOS VLANs . . . . .	340
Automatic WEP Rotation and Proxim VLANs . . . . .	342
Extensible Authentication Protocol (EAP) . . . . .	344
Enabling EAP Accounting . . . . .	347
Advanced Security Options . . . . .	348
Advanced Radio Properties . . . . .	350
Deploying Security Settings . . . . .	351
Deploying Security Settings for All Devices . . . . .	351
Deploying Security Settings to Access Points . . . . .	361
Deploying Security Settings to Mobile Devices . . . . .	372
<b>Chapter 9: Managing Alerts</b> . . . . .	<b>385</b>
Alert Profiles . . . . .	385
Creating an E-mail Address List . . . . .	386
Importing E-mail Addresses . . . . .	387
Deleting E-mail Addresses . . . . .	388
Creating Proxy Pool . . . . .	388
Deleting Proxies . . . . .	390
Creating Enterprise Alert Profiles . . . . .	390
Modifying Enterprise Alert Profiles . . . . .	393
Deleting Enterprise Alert Profiles . . . . .	393
Statistical Alerts . . . . .	394
Configuring New Statistical Alerts . . . . .	394
Editing Statistical Alerts . . . . .	398
Deleting Statistical Alerts . . . . .	398
Using the Alarm Browser . . . . .	399
Setting the Destination IP Address for Network Alerts . . . . .	399
Site Alert Filter Manager . . . . .	408
Performing Database Maintenance . . . . .	414
<b>Chapter 10: Reporting Network Data</b> . . . . .	<b>425</b>
Gathering Statistics . . . . .	426
Generating Reports . . . . .	436
<b>Appendix A: Installing Mobile Device Enablers</b> . . . . .	<b>439</b>
Loading the Enabler on a Series 3000 Device . . . . .	439
Loading the Enabler on a Series 7000 Device . . . . .	442
Loading the Enabler on Palm OS Devices . . . . .	446
Loading the Enabler on WinCE/PocketPC Devices . . . . .	450
Loading the Enabler on Series 4000/5000 Devices . . . . .	456
Loading the Enabler on Windows . . . . .	457
Future Releases . . . . .	458

---

<b>Appendix B: Country Codes for Importing Sites</b>	<b>459</b>
<b>Appendix C: Local Deployment Enhancement</b>	<b>469</b>
Important Notes about the Package Wizard .....	469
Editing the Local Deployment Batch File. ....	470
<b>Appendix D: Functions Available</b>	<b>475</b>





# Chapter 1: Introduction

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

- An introduction to the Enterprise Management Console of Mobile Manager Enterprise and conceptual information about Mobile Manager's structure
- Detailed information on the components of Mobile Manager Enterprise
- 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 Mobile Manager Enterprise product.

## About This Document

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

## Managing Networks with Mobile Manager

Wavelink Mobile Manager is a multiple-vendor solution for organizations seeking to deploy, configure and maintain an enterprise-wide wireless

network. This section describes several basic fundamentals of Mobile Manager, including:

- [Components of Mobile Manager](#)
- [Location Management: Sites and Groups](#)
- [Site-level Tools](#)

## Components of Mobile Manager

Mobile Manager is an integrated system of several components, which together allow you to manage your wireless network quickly and efficiently.

The primary components of Mobile Manager include:

- **Enterprise Management Console.** The Enterprise Management Console is your interface to wireless network components. With the Enterprise Management Console, you can manage and maintain everything from access point settings to mobile device software.
- **Agents.** Agents are server-side software that are responsible for communicating information to and from the Enterprise Management Console and wireless components. Mobile Manager contains two types of Agents: an access point Agent and a mobile device Agent. These Agents must be installed at each location that you want to manage.
- **Enablers.** Mobile devices require an additional component, called an Enabler, if you want to manage them with Mobile Manager. An Enabler is software installed on each mobile device that informs the mobile device of the mobile device Agent. With the Enabler installed, the mobile device can receive configuration instructions that you create in the Enterprise Management Console.

## Location Management: Sites and Groups

One of the key aspects of Mobile Manager is location management. A location is defined as any area within your network that contains wireless components that you want to manage.

Mobile Manager divides locations into two categories: sites and groups. A site is the most basic component of the Enterprise Management Console. 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.

---

**NOTE** The number of wireless components managed at a site depends on the communication range of the Agents installed at that site. Traditionally, this range has been defined as a single subnet on your network; however, depending on your network architecture, you can configure an Agent to communicate past a given subnet. This type of configuration takes place at the site level, using one of Mobile Manager’s site tools. See the *Mobile Manager User’s Guide* or the *Avalanche Manager’s User Guide* for more information.

---

Mobile Manager Enterprise 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 Management Console applies the configurations to every site within that group.

### **Site-level Tools**

Although you manage most aspects of your wireless network using the Enterprise Management Console, specific sites within the network might require additional configurations. These sites can be managed by accessing one of Mobile Manager’s site tools. There are two site tools available:

- **Mobile Manager Administrator.** The Administrator is a site-level tool designed to manage access points at a specific site.
- **Avalanche Management Console.** The Avalanche Management Console is the site-level tool that manages mobile device software and other settings.

## Chapter 2: Installation

Mobile Manager Enterprise 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 Mobile Manager Enterprise and how to install it on your network. Complete installation information is available in the following topics:

- Before You Begin
- Requirements
- Installing Mobile Manager Enterprise
- Activating Mobile Manager Enterprise

### Before You Begin

This section covers the recommended tasks you should complete before you install Mobile Manager on your network. While these tasks are not mandatory they can greatly streamline the installation process, allowing you to begin managing your wireless network faster.

To [install](#) Mobile Manager, it is recommended that you follow these steps:

- 1 [Understand](#) your network layout.
- 2 [Identify and enable](#) passwords on access points.
- 3 Obtain the correct [hardware and firmware](#).
- 4 Determine [placement](#) of Mobile Manager Agent services.
- 5 [Install](#) Mobile Manager.
- 6 [Activate](#) your Mobile Manager licenses.

### Understanding Your Network Layout

Perhaps the most crucial aspect of installing Mobile Manager is understanding your network layout before you start the installation process.

For the purposes of Mobile Manager, understanding your network layout is defined as knowing the following: the [location](#) of your access points, the [network segments](#), or subnets, that comprise your overall network, and the [Internet connectivity](#) of the system on which you install Mobile Manager Agents.

## Locating Access Points

Before you [install](#) Mobile Manager, take the time to locate where your access points are within your network. By knowing where these devices are beforehand, you can identify other network devices—such as switches or routers—that might affect wireless network management. With this information, you can then [determine](#) if you want to install the Agent on the same side of the switch or router as the access points—allowing you to take advantage of Mobile Manager’s broadcast-based discovery process—or on the opposite side, in which case you use Mobile Manager’s IP range discovery process.

---

**NOTE** Discovery processes are the main means by which Mobile Manager Agent discovers access points on the network. These processes are discussed in detail in the *Mobile Manager User’s Guide*.

---

## Network Segmentation

The larger a network is, the more likely it is divided into multiple segments, or subnets. These segments allow for easier administration of network components.

When you [install](#) Mobile Manager, it is important to know beforehand which network segments contain access points. This information is especially necessary if a switch or router exists between the Agent and the access points it is intended to manage. Once you know what network segments are part of the wireless network, you can [determine](#) if you can install the Agent centrally or if a per-subnet installation might be more efficient.

## Internet Connectivity

During typical operations, Mobile Manager does not require a connection to the Internet. The one exception is when you are [licensing](#) the installation of Mobile Manager Agent. At this time, the installation process must acquire an activation code which is locked to the specific system on which the Agent is installed.

The default method for acquiring this activation code is by accessing a secure Wavelink Web site through an Internet connection. If an Internet connection is unavailable, you can receive this code from a Wavelink Customer Service Representative.

---

**NOTE** The Wavelink license activation process is discussed in more detail in *Activating Mobile Manager Enterprise* on page 16.

---

## Partitioning Your Licenses

Mobile Manager allows you to [install](#) Agents on multiple locations within your network. This type of installation is called a distributed install and is described in more detail in the *Determining Agent Placement* on page 17 section.

To install multiple Agents on your network, you must partition your license. Partitioning means you segment your initial license into smaller groups of licenses, which you can then assign to different Agents on your network.

To partition your license, visit [www.wavelink.com/activation/partition](http://www.wavelink.com/activation/partition) and follow the instructions on this site. You can partition your licenses into as many groups as your need for your network.

You can only partition inactive licenses; consequently, it is recommended that you partition your licenses before you install Mobile Manager.

## Wireless Device Access

Access points are essentially highly-specialized computers and, as a result, they have their own authentication systems to ensure that they are modified only by authorized personnel. You must supply this information to Mobile Manager when you are attempting to identify and modify access points on the network; without this information, the access point will not allow Mobile Manager to make changes.

The types of authorizations include:

- SNMP Read-Only Community Name
- SNMP Read/Write Community Name
- Telnet user name (Cisco IOS only)

- Telnet passwords
- HTTP user name and password

The authorization required varies depending on the type of hardware being queried by the access point. Frequently a component requires more than one authorization type—for example, an Agent might need both an HTTP user name and an SNMP Read/Write name to correctly configure an access point.

---

**NOTE** See *Defining Device Access Privileges* on page 146 for additional information on access point authorization requirements.

---

Your access point documentation contains information on its default authorization names and passwords. Contact your system administrator if you are unsure of whether additional names and passwords might be necessary.

## Requirements

This section lists the [hardware](#), [software](#), and [firmware](#) requirements that Mobile Manager Enterprise requires for best performance.

### Hardware Requirements

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

	Required Hardware	Recommended Hardware
Enterprise Management Console	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

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

The following table lists the minimum requirements for each site that contains an access point Agent.



**NOTE** The optimal requirements for Mobile Manager depends on a number of factors, such as the number of access points you want to manage and your overall network topology.

Wavelink Corporation is not responsible for any system modifications you decide are necessary to improve the performance of Mobile Manager on your network.

Number of Access Points to Manage	Minimum Requirements
<20	Pentium III 500 Mhz 256MB RAM 500MB hard disk space
20 - 100	Pentium III 1.0 GHz 512MB RAM 500MB hard disk space
100 - 500	Pentium 4 1.0 GHz (Dual processors recommended) 2GB RAM 500MB hard disk space
500+	Pentium 4 1.0 GHz (Dual processors) 2GB RAM 500MB hard disk space

**Table 2-2:** Hardware Requirements for Mobile Manager Components

The following table lists the minimum requirements for each site that contains a mobile device Agent.

	Required Hardware	Recommended Hardware
Avalanche Management Console	Pentium III 550 MHz or faster processor 256 MB RAM 512 MB 200 MB hard disk space	Pentium IV 1.4 GHz 512 MB RAM 200 MB hard disk space
Mobile Device Agent	Pentium III 550 MHz or faster processor 256 MB RAM 512 MB 200 MB hard disk space	Pentium IV 1.4 GHz 512 MB RAM 200 MB hard disk space

**Table 2-3:** Hardware Requirements for Mobile Manager Enterprise Components

## Software Requirements

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

- Windows 2000 (Service Pack 2 or later)
- Windows XP

---

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

This Agent must be a Mobile Manager 5.6 Agent. You cannot manage older Agents with Mobile Manager Enterprise 1.7; however, you can upgrade them.

---

---

**NOTE** Windows NT is no longer supported.

---

## Firmware Requirements

To support as many access points as possible, Mobile Manager interacts with access points in one of two ways: either in [full support mode](#) or in [compatibility mode](#). Mobile Manager selects which mode to use based on whether it can recognize the firmware version installed on an access point. In full support mode, the Agent is able to retrieve and set the vast majority of options for that access point. In compatibility mode, the Agent attempts to use existing access point property files stored in the Agent to retrieve and set as many of the access point's options as possible.

---

**NOTE** See your release notes or contact your Wavelink sales representative to determine the firmware your version of Mobile Manager supports.

---

## 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.

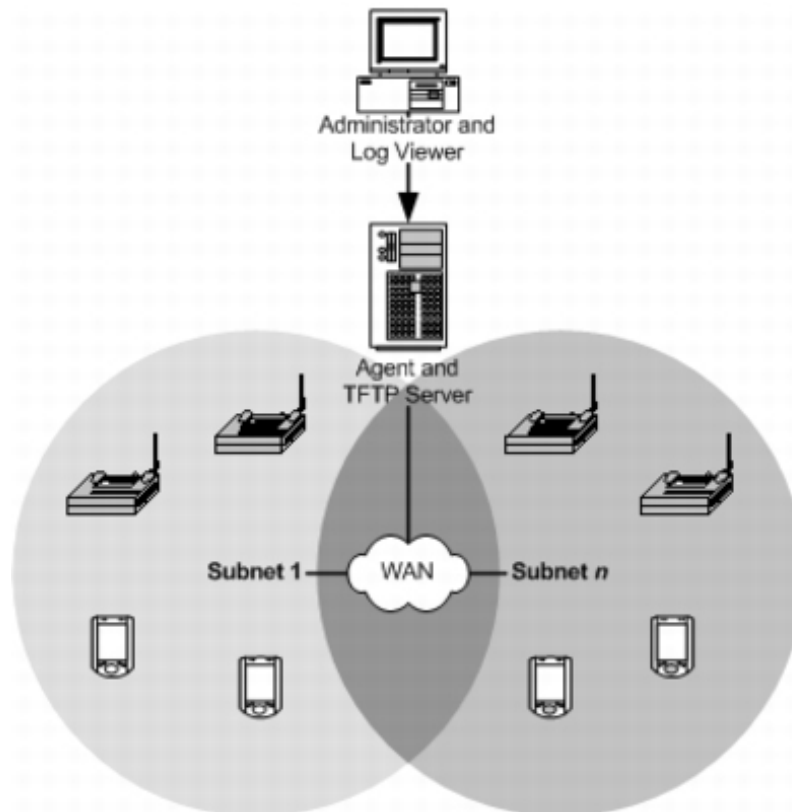
As new mobile devices are supported by Wavelink, they will automatically include support for Avalanche, with the rare exception of mobile devices that lack any dynamic storage ability. Check the Wavelink Web site, [www.wavelink.com](http://www.wavelink.com) for the most up to date list of supported devices.

## **Determining Agent Placement**

Determining where to space your Mobile Manager Agents is a very important task. The ability to manage your wireless network depends on Agents being able to locate and communicate with your access points. Currently, there are two primary methods of installing Agents: [centralized](#) and [distributed](#).

### **Centralized Agent Installation**

In centralized Agent [installs](#), a single Agent is responsible for managing all of the access points on the network. Centralized Agent installs are typically found in environments where specific sites within a network might be unable to support their own Agents. An example of this environment is a collection of retail stores. While the headquarters for these stores can support a Mobile Manager Agent, it might be unfeasible for each individual store to have its own Agent. In this case, installing the Agent centrally is an ideal solution.



**Figure 2-1.** *A Centralized Installation of Mobile Manager (Simplified)*

If you determine that a centralized Agent installation is the best choice for your wireless network, it is important to remember the following:

- You must know the network subnets to ensure the Agent knows where to listen for access point broadcasts.
- You must know what switches and routers reside between the Agent and access points (this is particularly helpful should any troubleshooting be necessary).
- You must have a general understanding of the overall performance of the wireless network, to ensure that specific time-based features (such as WEP key rotation) are configured correctly.

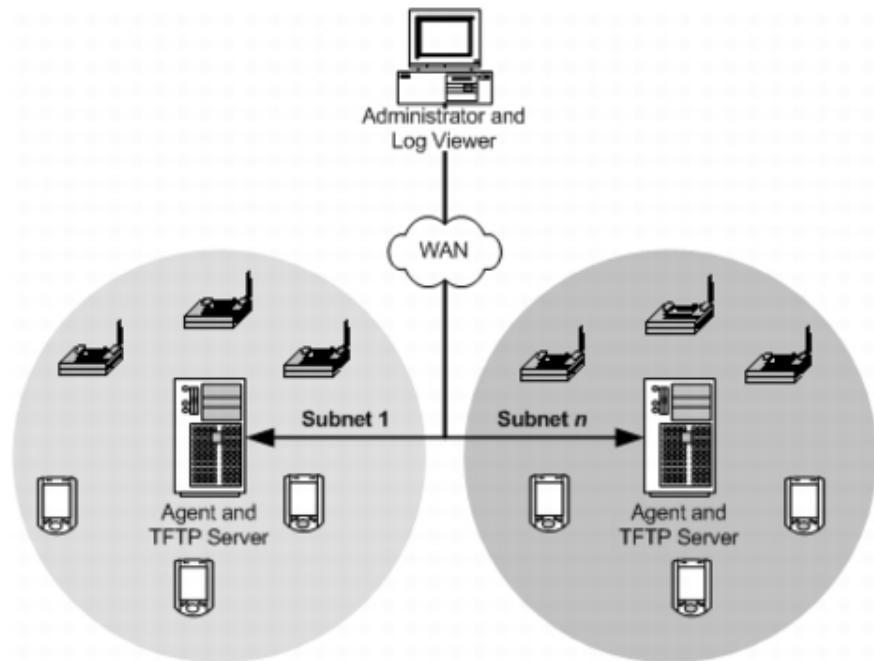
## Distributed Agent Installation

In distributed Agent [installs](#), an Agent resides on each network subnet. These Agents are responsible for managing on a per-subnet basis. Often, distributed Agent installations of Mobile Manager are found in environments where wireless network uptime is critical to business operations. For example, if a company has multiple locations across the country, connectivity between each site might depend on factors outside the company's control—such as weather, the performance of third-party services, and so on. In these situations, installing an Agent on each subnet provides a more robust environment in which wireless network downtime is minimized.

If you determine that a distributed Agent installation is the best choice for your wireless network, it is important to remember the following:

- Because you are installing multiple Agents on multiple systems, it might take more time to completely install and optimize Mobile Manager for your network.
- Each Agent must be licensed and nodelocked to a unique system; consequently, you must partition your license before installation.
- You must ensure that when you upgrade your Mobile Manager, you upgrade all Agents across the network.

Posted by: Carrie Fan | July 7, 2005 11:17 PM (#9 of 10)



**Figure 2-2.** *A Distributed Installation of Mobile Manager (Simplified)*

## Installing Mobile Manager Enterprise

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

---

**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 Enterprise:

- 1 Download the self-extracting zip file from the [Wavelink Web site](#).
- 2 Double-click the file to start the installation process.

---

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

---

The *Introduction* dialog box appears.

- 3 Click `Next` to continue the installation process.

The *License Agreement* dialog box appears.

- 4 Read through the license agreement carefully.
- 5 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 Install Folder* dialog box appears.

- 6 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 Enterprise components.

- 7 Select a shortcut folder location, then click `Next`.

The *Choose Product Features* dialog box appears.

- 8 Select an installation type.

If you want to install all of Mobile Manager Enterprise components, click the **Server & Administrator Console** icon. Select this installation if you want to run the Enterprise Management Console and all Mobile Manager Enterprise server components from the selected computer.

If you want to install only the server components of Mobile Manager Enterprise, click the **Server** icon. Select this installation if you want to install the server components of Mobile Manager Enterprise, but you plan to install the Enterprise Management Console on a separate computer.

If you want to install only the Enterprise Management Console, click the **Administrator** icon. Select this installation if you plan to install the server components of Mobile Manager Enterprise on a separate computer.

- 9 Click `Next`.

The *Administrative User* dialog box appears.

- 10 Type the name of the user that will have administrative rights to Mobile Manager Enterprise in the **User Name** text box.
- 11 Type the password for the administrative user account in the **Password** text box.
- 12 Confirm the password for this account by re-typing it in the **Confirm Password** text box.
- 13 Enable the **Enable Encryption** check box to enable encryption between the Enterprise Management Console and Mobile Manager Enterprise server components, such as the Enterprise Manager and the Fault Manager.
- 14 Click `Next`.

The *Select Host IP Address* dialog box appears.

- 15 Select the IP address for the network adapter through which remote administrators can connect to the Agent.
- 16 Click `Next`.

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

- 17 Click `Install`.

Mobile Manager Enterprise 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 Enterprise for your network.

## **Activating Mobile Manager Enterprise**

After you install Mobile Manager, you are asked to activate it with a valid license code. This code uses a technique called nodelocking, in which Mobile



Manager is licensed only for a specific computer, or node, on your network. A node is defined as several specific system attributes that, in combination, uniquely distinguish it from any other system in your organization.

---

**NOTE** If you plan on installing multiple Agents on your network, you must partition your Wavelink license. See *Before You Begin* on page 11 of this document for more information.

---

When you activate 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 Mobile Manager has Internet access. If the system has Internet access, you can acquire the license file. If the system does not have Internet access, you can receive this file from a Wavelink Customer Service Representative.

---

**NOTE** You are not required to activate Mobile Manager to complete the installation process.

After you install Mobile Manager, you must activate it to be able to manage your wireless network. See *Activating Mobile Manager Enterprise* on page 16 for more information on activating Mobile Manager after it has been installed.

---

**To activate Mobile Manager:**

- 1 Follow the steps as described in *Installing Mobile Manager Enterprise* on page 20.
- 2 After the installation process is complete, click `Next` in the *Configuration Setup Complete* dialog box.

The *Product License* dialog box appears.

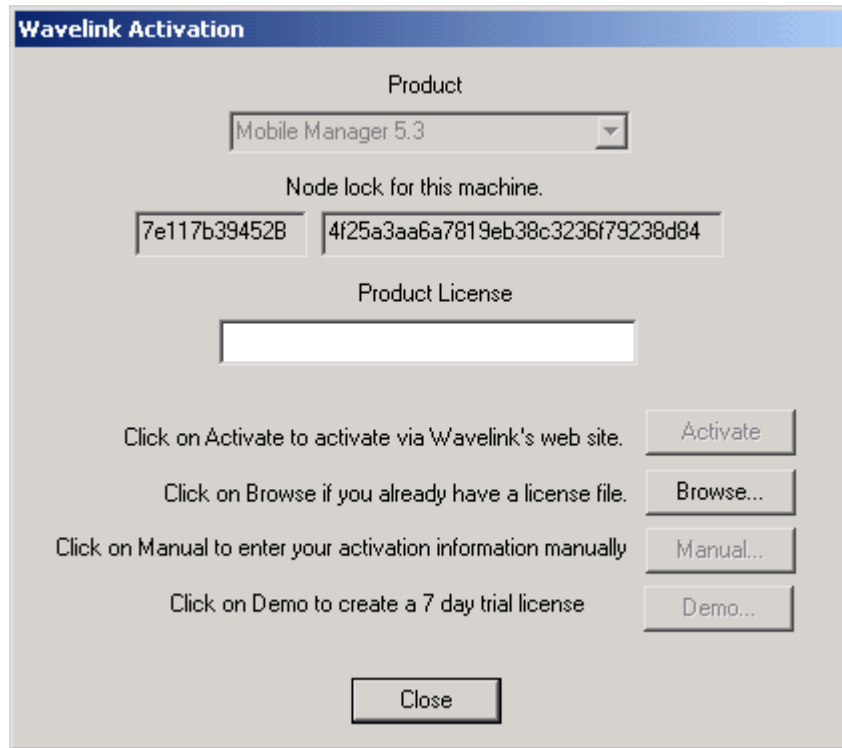
- 3 Enable the **Activate the product or add more licenses** checkbox and click `Next`.

The *Wavelink Activation* dialog box appears.

---

**NOTE** You can also access this dialog box from the **Start** menu after the installation.

---



**Figure 2-3.** *The Wavelink Activation Dialog Box*

- 4 Type your license number for this installation in the **Product License** text box.
- 5 Select an activation type.

If Mobile Manager resides on a system that has Internet access, click **Activate**. When you click **Activate**, 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 accept 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. Mobile Manager then uses this file to activate its services.

If you are installing Mobile Manager for demonstration purposes, click **Demo**. The **Demo** button authorizes Mobile Manager to manage up to 2 access points for 30 days.

Mobile Manager Enterprise is now authorized for use on your host system. It is important to remember that the new Wavelink licensing process ties Mobile Manager Enterprise install to a specific computer on your network. If a situation occurs that requires you to re-install Mobile Manager Enterprise 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.

## Installing Mobile Device Enablers

A Mobile Device Enabler is software that allows mobile devices to communicate with the Avalanche Manager. After the initial installation of the Enabler on a mobile device, future Enabler upgrades can occur over a wireless connection through the Avalanche Manager.

You must use the correct Enabler file, based on the device type and other factors. The naming convention for the Avalanche Enabler file is:

`[Component][Platform][OS][Radio][Version].[Extension]`

Where

- *Component* is always `WLEnabler`
- *Platform* represents a device type and platform, such as `S75`
- *OS* represents the operating system, such as `DOS`
- *Radio* represents the network type, such as `802.11B`
- *Version* represents the Enabler version number, such as `1.31`
- *Extension* represents the file extension, such as `.hex` for DOS Enablers

An example of an enabler file that uses this convention is `WLEnabler_S75_DO_8B_1_3_1.hex`, which represents the 7546 DOS Enabler, version 1.31, for 802.11B networks.

The following table shows the possible values for the platform/device, the operating system, the radio, and the file extensions in the Enabler file name.

S3K - Symbol 1K, 3K, 6K	DO -DOS	SP - Pre 802.11	.hex - for DOS
S40 - Symbol 4000	CE -CE 2.11	80 - 802.11	.exe - for Win CE
S72 - Symbol 7200	PP - PPC 3.0	8B - 802.11B	.prc - for Palm
S75 - Symbol 7500	PL - Palm	All - All radios	
S17 - Symbol 1700	W -Windows		
S27 - Symbol 2700			
S79 - Symbol 7900			
S81 - Symbol 8100			
S28 - Symbol 2800			
I50 - Intermec 5020			
WPC - Windows PC			

**Table 2-4:** *Enabler File Names*

**NOTE** For Symbol 3000 Series devices, the hex files provide a radio driver but do not update the mobile device's radio firmware. If the firmware needs to be updated, both the RF update software package (`RF3_vxx.exe`, where `xx` represents the version number) and the Avalanche Enabler should be downloaded. The RF update package contains the most recent radio drivers and firmware. Two RF update kits are available for 3000 Series mobile devices. One is for the "spring" and 802.11 protocols, the other is for the 11Mb (802.11b) protocol. Due to incompatibilities between different versions of radio drivers and firmware released by the hardware vendors, it is possible to select the

correct driver based on the RF protocol and still have communication problems due to older firmware in your mobile device. Applying a Wavelink RF update kit assures that compatible versions are used.

When the RF update software package is used with a serial connection, either `Ava3-spr.hex` or `Ava3-802.hex` can be used regardless of the firmware type found in the mobile device.

---

For Enablers that ship with Wavelink Avalanche, such as the Symbol Series 3000 devices, you can find the Enabler file in the `\Client` subdirectory in the location where you installed the Avalanche Manager (this defaults to `C:\Program Files\Wavelink\Avalanche\Client`).

For Enablers that do not ship with Wavelink Avalanche, you must download the Enabler from the Wavelink Web site.

### **Downloading the Enabler**

The installation of the Avalanche Enabler is OS- or device-specific. For information on loading the Enabler for a specific OS or device type, see the following sections in *Appendix A: Installing Mobile Device Enablers* on page 439:

- *Loading the Enabler on a Series 3000 Device* on page 439
- *Loading the Enabler on a Series 7000 Device* on page 442
- *Loading the Enabler on Palm OS Devices* on page 446
- *Loading the Enabler on WinCE/PocketPC Devices* on page 450
- *Loading the Enabler on Series 4000/5000 Devices* on page 456
- *Loading the Enabler on Windows* on page 457

### **Downloading Hex Files**

This section contains instructions for using the hex file download utility included with Wavelink Avalanche. You can use this utility to download the Enabler file and other hex files (.hex) to DOS-based devices over a serial connection.

---

**NOTE** Before you use the hex file download utility, see *Installing Mobile Device Enablers* on page 25 to obtain the name of the required Enabler file. You must also prepare your mobile device for a hex file download before using the hex file utility. See *Downloading the Enabler* on page 27 for more information.

---

The topics included in this section include:

- Using the Hex File Download Utility
- Simultaneous Hex File Downloads
- Configuring the Enabler

### **Using the Hex File Download Utility**

Use the hex file download utility to download the Enabler file to DOS-based devices over a serial connection. Before you can download the Enabler file, you must prepare the mobile device for downloading. See *Appendix A: Installing Mobile Device Enablers* on page 439 for more information about preparing a DOS-based device for downloading.

---

**NOTE** This section applies only to supported DOS devices that require the downloading of hex files over a serial connection. See *Appendix A: Installing Mobile Device Enablers* on page 439 for more information about downloading the Enabler on other devices.

---

### **To download the Enabler:**

- 1** Launch the Avalanche Management Console.
- 2** Connect to the Avalanche Manager Agent.

You can connect to the default Agent, localhost, by selecting `Connect to Agent` from the **Agent** menu. To connect to another local or remote Agent, see the *Avalanche Manager User's Guide* for more information.

- 3** Verify that a COM port is available for use.

To check the status on a COM port, double-click a COM port in the Tree View and read the information that appears in the Status branch. These COM ports are located below the Serial Ports branch. The status for an

available COM port is `Listening`.

If the Avalanche Manager Agent did not automatically detect the COM ports during the installation, see the *Avalanche Manager User's Guide* before attempting a serial download.

---

**NOTE** COM ports used by other software programs or hardware peripherals should be removed from the list of available serial ports.

---

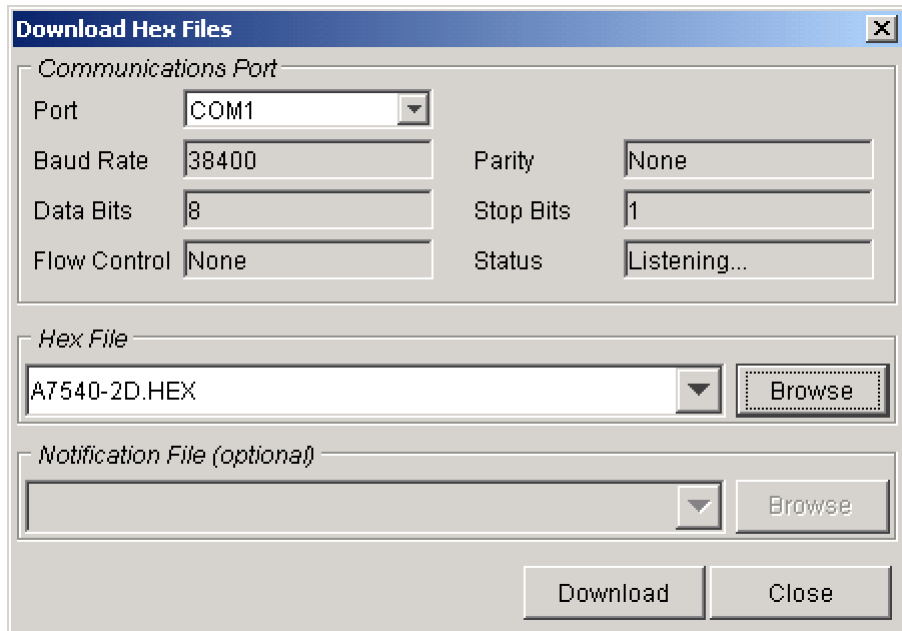
---

**NOTE** The Avalanche Manager Agent must reside on the system with the serial port connections. However, you can manage the Agent either from a local or remote Management Console. To manage the Agent from a remote console, you must connect to the Agent from the console using a routable IP address.

---

- 4 Launch the hex file download utility by selecting `Download Hex Files` on the **Tools** menu.

The *Download Hexfiles* dialog box appears.



**Figure 2-4.** The Download Hexfiles Dialog Box

- 5 In the **Port** list, select the desired COM port.
- 6 Verify that the port status is `Listening...` The **Status** box displays the port status.

---

**NOTE** If the default settings in the **Communications Port** group box do not match the mobile device, it is recommended that you use `Winhex.exe` or `Sendhex.exe` to download the Enabler.

---

- 7 In the **Hexfiles** group box of the *Download Hexfiles* dialog box, click `Browse` to browse for the location of the hex file.



---

**NOTE** For Series 7000 DOS devices, you must download the partition file that matches the device's flash type before downloading the Enabler. See *Loading the Enabler on a Series 7000 Device* on page 418 to determine the name of the required partition file. Follow steps 5 and 6 to download the partition file. Then repeat steps 5 and 6 to download the Enabler file.

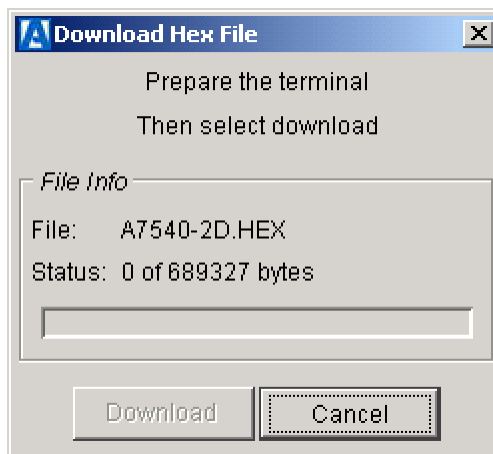
---

8 When you select a hex file, a message box appears asking you to confirm whether you want to upload the selected file to the Avalanche Manager Agent. The warning appears because this action might involve the transfer of large files.

9 Click **Yes**.

10 Click **Download**.

The following dialog box appears.



**Figure 2-5.** *The Download Hex File Dialog Box*

11 Click **Download**.

---

**NOTE** If the **Download** button is disabled, verify that the mobile device is prepared to receive data. See *Appendix A: Installing Mobile Device Enablers* on page 439 for more information.

---

The download utility installs the Enabler file on the mobile device. When the Enabler file has been fully installed, the status line shows the following message: Download completed successfully.

---

**NOTE** Do not take the mobile device out of its cradle during download.

---

Cold boot the mobile device after download. Instructions on how to cold boot are included in table 2-5 below.

	<b>Cold Boot Sequence</b>
46-key LRT 3840 46-key PDT 3140 47-key PDT 3540 46-key PDT 6840 46-key PDT 6140	Power off the mobile device. Hold A+B+D. Press and release PWR. Release A+B+D.
54-key VRC 3940 54-key VRC 6940	Power off the mobile device. Hold F1+F4+ENTER. Press and release ON/OFF. Release F1+F4+ENTER.
35-key PDT 3140 35-key PDT 6140	Power off the mobile device. Hold SPACE+FUNC+UP ARROW. Press and release ON/OFF. Release SPACE+FUNC+UP ARROW.
27-key WSS 1040	Power off the mobile device. Hold RIGHT ARROW+ENTER Press and release PWR. Release RIGHT ARROW+ENTER
7000 Series	Power off the mobile device. Hold PWR. After approximately 15 seconds, the mobile device will cold boot.

**Table 2-5:** Cold Boot Sequences for DOS-based Devices

After cold booting, the Avalanche Enabler loading process is complete.

### **Simultaneous Hex File Downloads**

The Avalanche Manager supports the ability to download hex files to more than one cradle from multiple serial ports simultaneously.

---

**NOTE** This section applies only to supported DOS devices that require the downloading of hex files over a serial connection.

---

**To perform a simultaneous download:**

- 1 Follow the procedure described in *Downloading Hex Files* on page 21 until the `Prepare Terminal...` message appears in the *Download Hex Files* dialog box.
- 2 Before downloading the first hex file, browse to choose another hex file or the same hex file being downloaded.
- 3 Select a different COM port (for example, select COM2 if the first hex file is associated with COM1).
- 4 In the *Download Hexfiles* dialog box, click `Download`.

Another dialog box showing the `Prepare Terminal...` message appears. This dialog box is associated with the new COM port.

- 5 At this point, verify that the mobile device is prepared to receive the installation files. See *Downloading the Enabler* on page 27 for more information.
- 6 Click `Download`.

The Enabler begins loading into the mobile device's non-volatile memory (NVM) drive. Once the installation is complete, activate the Enabler on the mobile device.

**Configuring the Enabler**

Before you can connect to the wireless network, you must configure the networking parameters of the Avalanche Enabler. You can configure IP addresses, ESS IDs, WEP encryption, and other network parameters on the mobile device either manually or through the Management Console.

- To configure the mobile device through the Management Console, create a network profile. Changes made to configuration through a network profile download to the device the next time the Enabler activates (typically on reboot). See the *Avalanche Manager User's Guide* for information about creating a profile.

---

**NOTE** Before you can download a network profile to a mobile device, you must connect to the Avalanche Manager Agent. You can connect to the default Agent, localhost, by selecting `Agents > localhost` from the **Administration** menu. To connect to another local or remote Agent, see the *Avalanche Manager User's Guide* for more information.

---

- To configure the network parameters manually, see the appropriate client documentation.

## Chapter 3: Enterprise Management Console

You primarily interact with your wireless network using the Enterprise Management Console. The Enterprise Management Console allows you to control global characteristics of your wireless network. These characteristics include [creating access point profiles](#), [assigning IP addresses](#), and [monitoring network performance](#). With the Enterprise Management Console, 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 Management Console works with server-based components of Mobile Manager Enterprise product, called Agents. These Agents are responsible for sending instructions to and receiving data from wireless devices. Mobile Manager Enterprise includes two types of Agents: access point Agents and mobile device Agents. From the Enterprise Management Console, you can deploy one or both of these Agents anywhere within your network.

To streamline wireless network management, the Enterprise Management Console 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 Locations* on page 73 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 Management Console
- Understanding Enterprise Management Console Views
- Setting Enterprise Management Console Preferences

### Starting the Enterprise Management Console

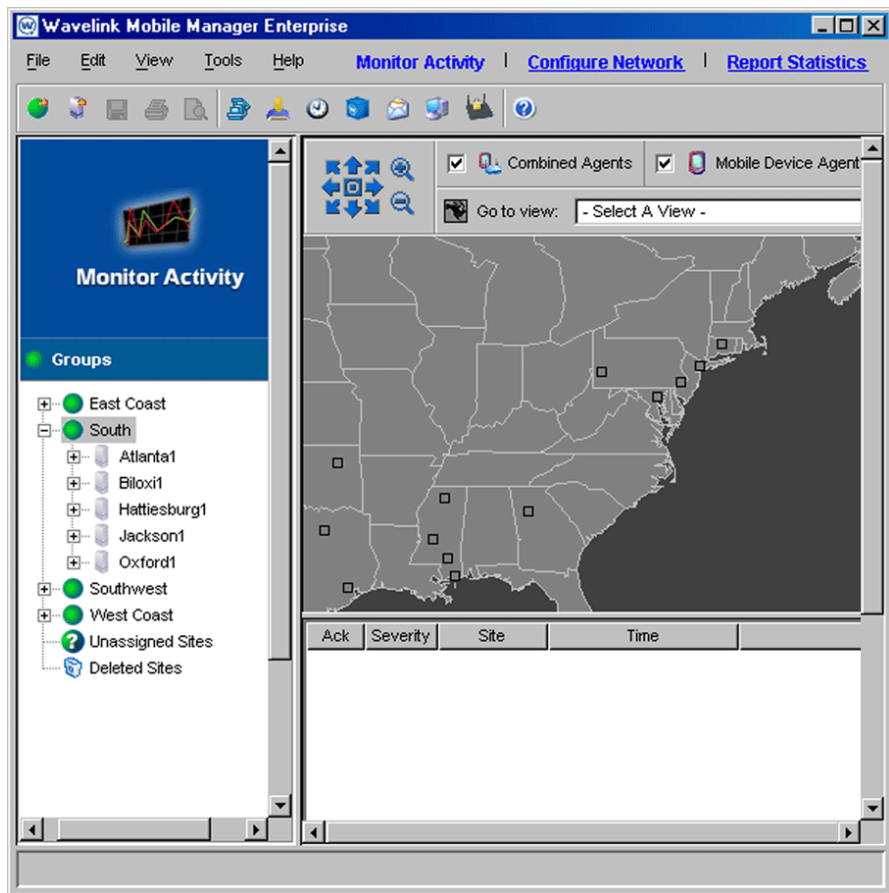
The Enterprise Management Console allows you to configure and manage your wireless network on an enterprise-wide basis.

#### **To start the Enterprise Management Console:**

- 1 Click `start` from the desktop.

- 2 Select Programs.
- 3 Select Wavelink Mobile Manager.
- 4 Select Enterprise.
- 5 Select Console.

The Enterprise Management Console appears.



**Figure 3-1.** *The Enterprise Management Console*

## Understanding Enterprise Management Console Views

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

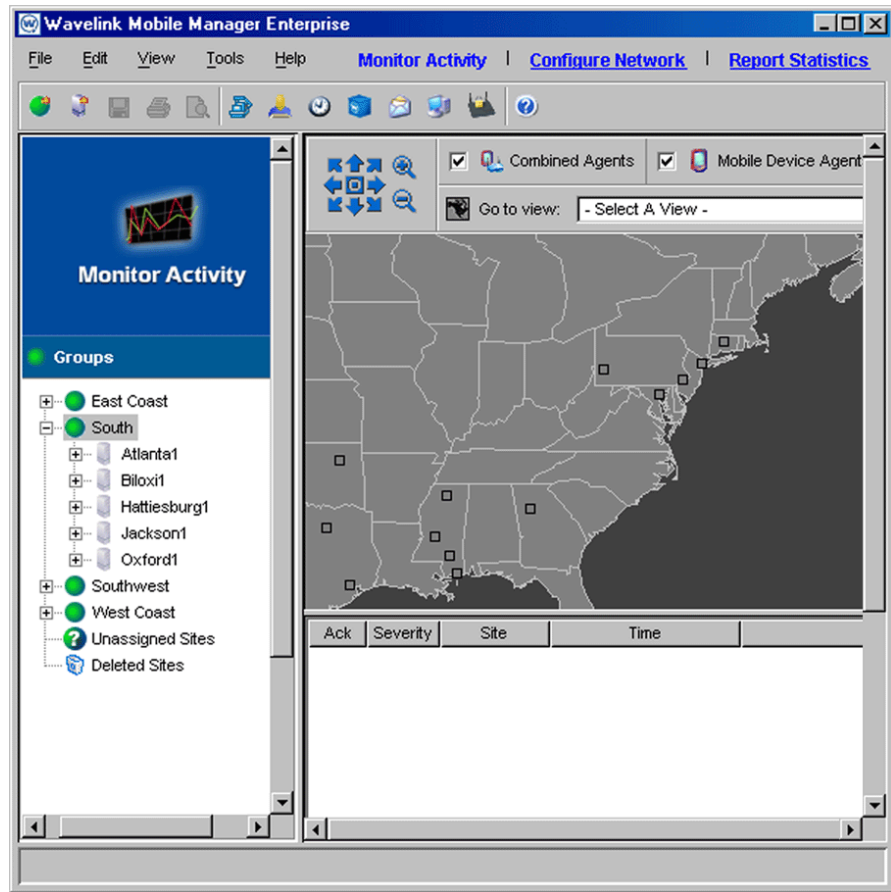
### Monitor Activity View

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 Management Console.
- 2 Click `Monitor Activity` from the toolbar.

The Monitor Activity view appears.



**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 Management Console 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:

<b>Combined Agents</b>	Displays sites that contain both a mobile device Agent and an access point Agent.
<b>Mobile Device Agents</b>	Displays sites that contain only a mobile device Agent.
<b>Access Point Agents</b>	Displays sites that contain only an access point Agent.
<b>View Map By Selected Group</b>	Displays only those sites that belong to the group selected in the <a href="#">Groups</a> window.

The Map pane also provides color-coding to identify components and to provide notifications of network health. The color codes for the components that appear in the map is as follows:

<b>Purple</b>	Indicates a site with combined Agents (mobile device and access point Agents)
<b>Blue</b>	Indicates a site with only a mobile device Agent
<b>Dark Green</b>	Indicates a site with only an access point Agent
<b>Yellow</b>	Indicates a site with one or more warning-level alarms (but no critical alarms).
<b>Red</b>	Indicates a site with one or more critical alarms.

When a site generates a warning or critical alarm, the icon in the Map pane flashes yellow or red, based on the highest severity level in its alarm list. The flashing stops when you acknowledge the alert in the Alarm Browser. The icon

returns to its base color when all warnings and critical alerts for the site have been cleared from the Alarm Browser.

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:

<b>Ack</b>	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.
<b>Severity</b>	Indicates the severity of the alert. Severity levels include Critical, Warning, and Informational.
<b>Site</b>	The name of the site that generated the alert.
<b>Time</b>	The time and date when the alert occurred.
<b>Description</b>	A brief description of the alert.
<b>IP Address/Hostname</b>	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.

### **Saving Views**

You also have the option of 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.

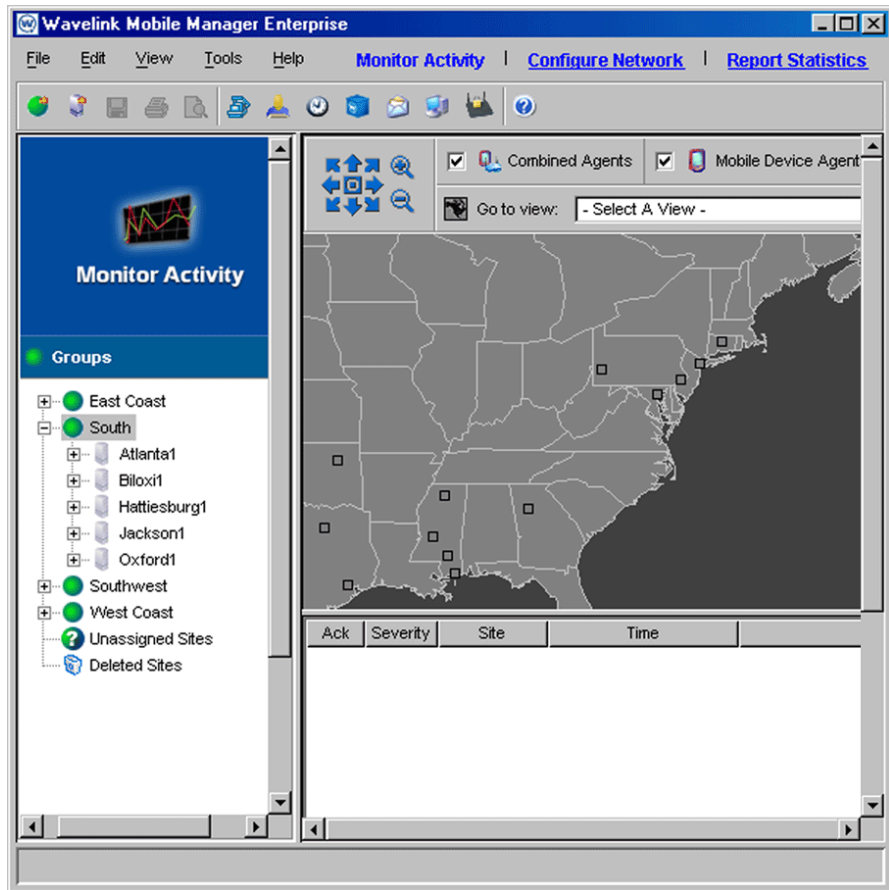
### **Modifying Colors**

You can also modify the colors displayed in the Monitor Activity view.

**To modify the colors in the Monitor Activity view:**

- 1 Open the Enterprise Management Console.
- 2 Click `Monitor Activity` from the toolbar.

The Monitor Activity view appears.



**Figure 3-3.** *The Monitor Activity View*

- 3 Select `Customize` from the **Tools** menu.

The Customize dialog box appears.



**Figure 3-4.** *The Customize Dialog Box*

- 4 Modify the colors associated with the Monitor Activity view as needed.
- 5 Click **OK**.

### **Configure Network View**

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

- Configure access point [profiles](#)
- Manage [IP addresses](#)

- Create [alert profiles](#)

With the Enterprise Management Console, you do not configure individual wireless network components, such as access points. Instead, Mobile Manager Enterprise allows you to organize these components into [sites](#) and combine those sites into [groups](#). Mobile Manager Enterprise applies any modifications you make to your network in the Enterprise Management Console to these groups.

---

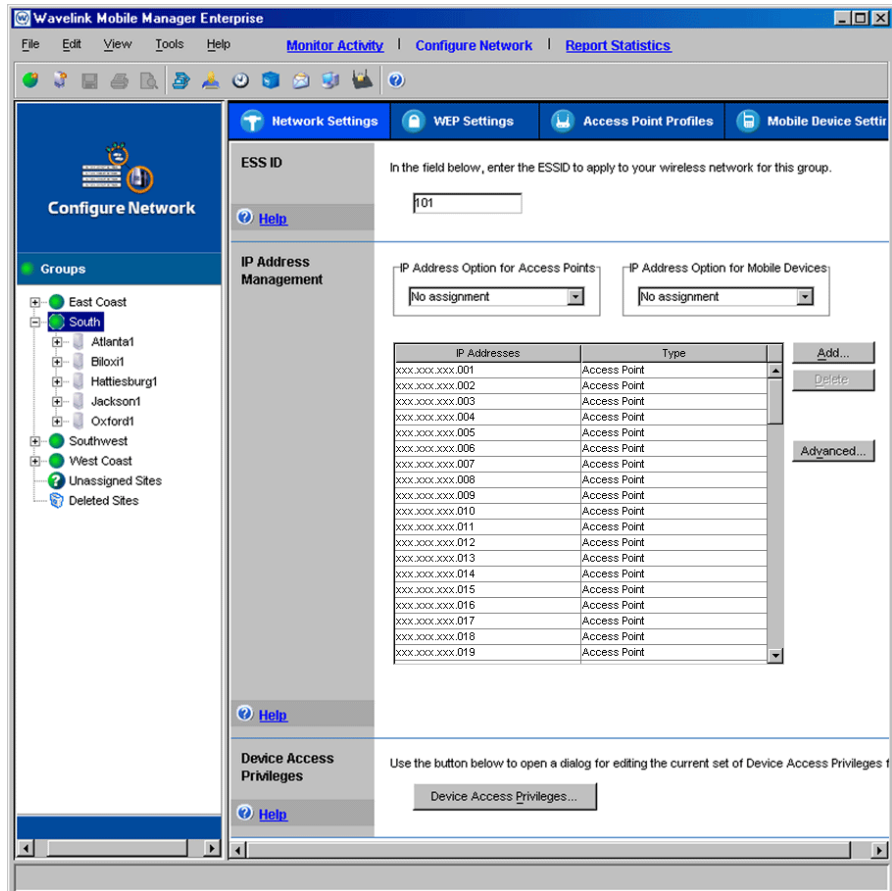
**NOTE** To modify wireless network components at the site level, see *Mobile Manager Users Guide*.

---

**To access the Configure Network view:**

- 1 Open the Enterprise Management Console.
- 2 Click `Configure Network` from the toolbar.

The Configure Network view appears.



**Figure 3-5.** *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:

<b>Network settings</b>	Defines network settings, such as IP addresses and ESSIDs.
<b>Security settings</b>	Defines security settings, such as WEP.
<b>Access Point Profiles</b>	Defines templates of configuration settings, called profiles, that are applied to access points on your network.
<b>Alert Profiles</b>	Defines alert profiles, which can notify you when a specific alert occurs on the network.

## 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 Management Console.
- 2 Click `Report Statistics` from the toolbar.

The Report Statistics view appears.

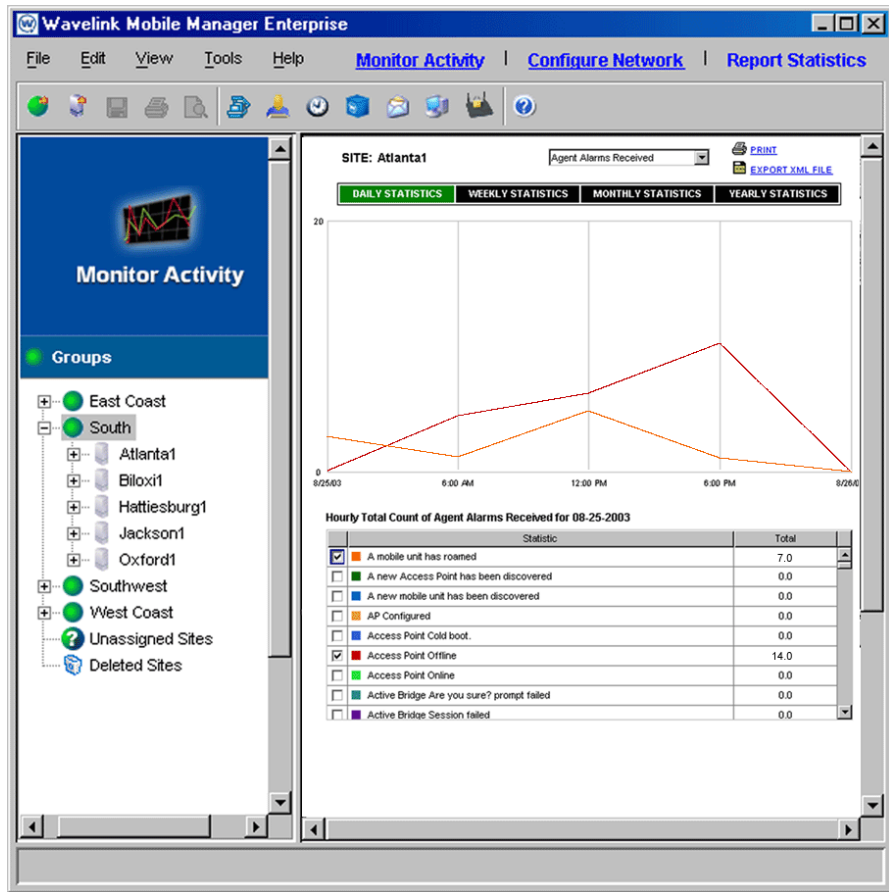
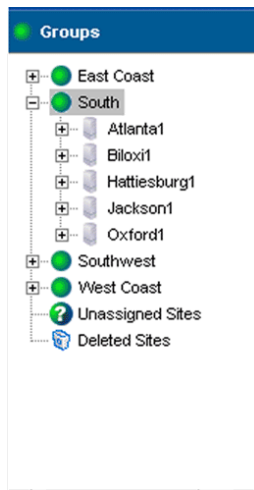


Figure 3-6. The Report Statistics view

## Groups Window

All of the Enterprise Management Console views provide access to the Groups window. This window, located on the left side of the Enterprise Management Console, 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 Locations* on page 73 for more information on how you use groups to manage your wireless network.



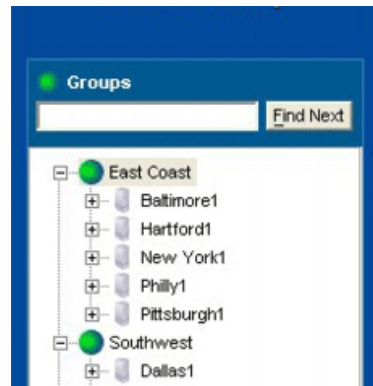


**Figure 3-7.** *The Groups Window*

## Search

The left-hand pane in the Enterprise Management Console shows you all your groups and sites in a tree view. When you have a large number of groups or sites, it may become more difficult to navigate to a desired group or site by scrolling and clicking through the tree.

In this case, the search function is helpful: Just type in the name of the group or site in the text field just above the tree view, then click the `Find Next` button just to its right. The highlight will move to the first group or site whose name begins with the text you entered. The search is not case sensitive. If there are multiple matches, just keep clicking the `Find Next` button until you have reached the group or site you were looking for.



**Figure 3-8.** Search Field

The Search function is also available in the *Scheduled Task Wizard*: On the Select Task Destinations panel, the same Search text field and button are shown just above the tree view. Again, enter a full or partial name and click 'Find Next' until the highlight shows the group or site you are interested in.

The Search function finds sites regardless of whether the containing group is expanded or collapsed.

## Setting Enterprise Management Console Preferences

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

- The [location](#) of the host system support Mobile Manager Enterprise 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 Management Console [communicates](#) with the sites on your network

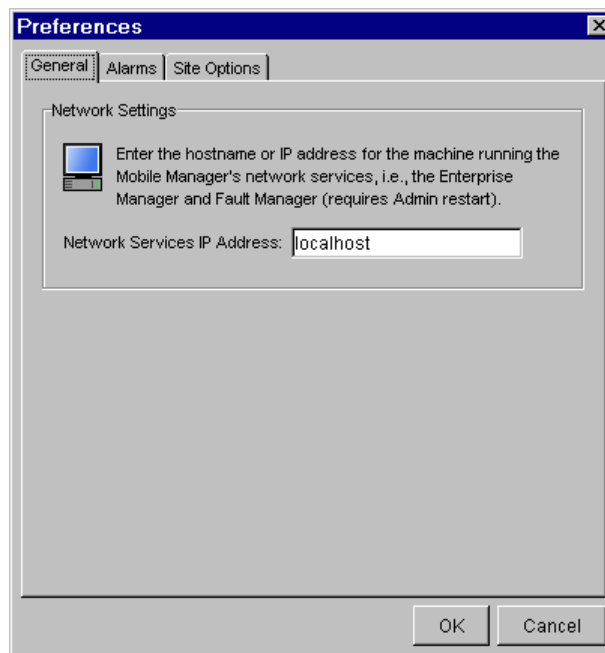
The following sections describe these preferences in detail.

## Selecting the Location of Network Services

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

To select the location of Mobile Manager Enterprise network services:

- 1 Select `Preferences` from the **File** menu.  
The *Preferences* dialog box appears.
- 2 Click the General tab.



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

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

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

## **Configuring the Alarm Browser**

The Enterprise Management Console 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 Management Console 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.



**Figure 3-10.** *The Alarms Tab of the Preferences Dialog Box*

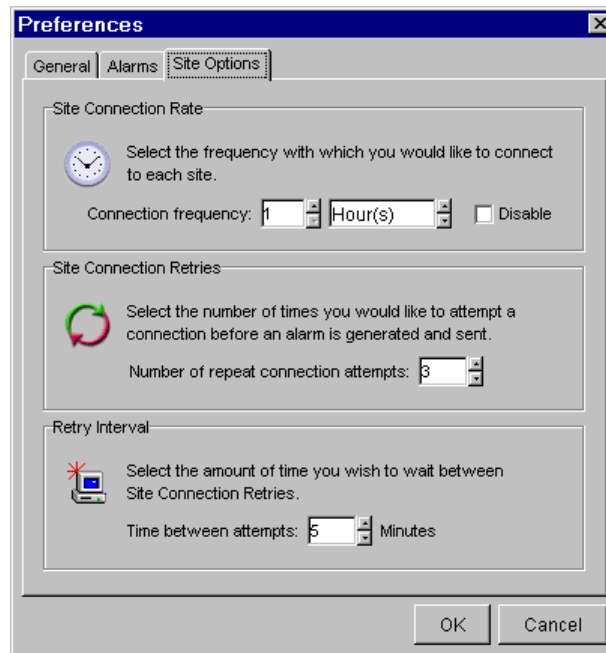
- 3 Type how many days an alert remains in the Alarm Browser in the **Remove alarms from the alarm browser after** text box.
- 4 Click **OK**.

## Controlling Site Communication

From the Enterprise Management Console you are able to access detailed information about your wireless network at a site level. You can control how the Enterprise Management Console 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



**Figure 3-11.** *The Site Options Tab of the Preferences Dialog Box*

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

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

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

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

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

- 6 Click **OK**.

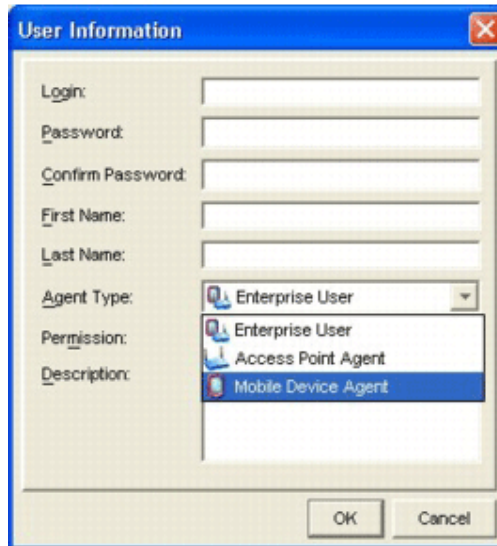
## User Accounts

When you install Mobile Manager Enterprise, 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:

<b>Administrative</b>	Full permissions to manage wireless devices, including profiles, IP address assignments, and access point configurations. Also has permission to create or modify user accounts.
<b>Read/Write</b>	Full permissions to manage wireless devices, including profiles, IP address assignments, and access point configurations, but cannot create or modify user accounts.
<b>Read Only</b>	Read-only access to wireless devices through the Administrator.

Each account also has an Agent Type, which determines access to groups of functionality for the entire enterprise, for the access points, or for mobile devices. The Enterprise User has access rights to both access points and mobile devices.

Please see Appendix D for a complete list of functions available based on Agent Type and Permission.



**Figure 3-12.** *User Information Dialog Box*

Accounts are created for enterprise-wide components of Mobile Manager Enterprise, such as the Enterprise Management Console, are also [distributed](#) to all the sites on your wireless networks. Consequently, a user that has read/write permissions for the Enterprise Management Console 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 Accountss
- Editing User Accounts
- Deleting User Accounts
- Viewing Account Status
- Changing Account Passwords
- Deploying User Accounts



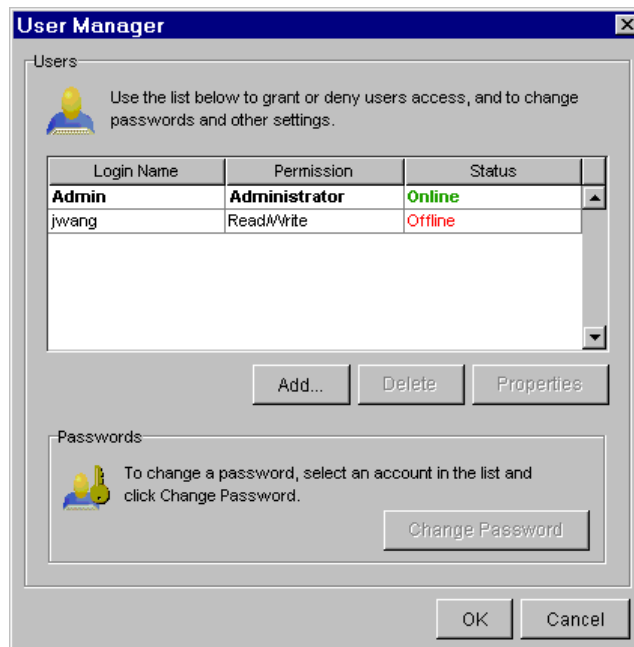
## Creating User Accounts

The user account you first create when you activate Mobile Manager Enterprise 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.

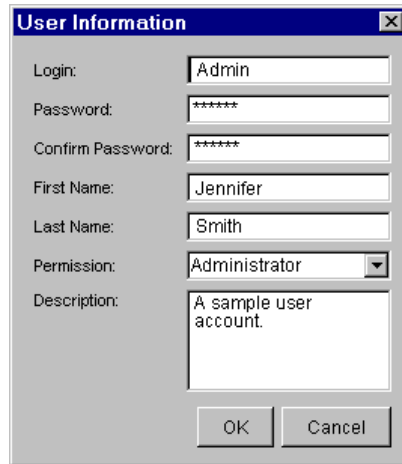
The *User Manager* dialog box appears.



**Figure 3-13.** *The User Manager Dialog Box*

- 2 Click **Add**.

The *User Information* dialog box appears.

A screenshot of a 'User Information' dialog box. The dialog has a title bar with 'User Information' and a close button. It contains several input fields: 'Login' with 'Admin', 'Password' with '\*\*\*\*\*', 'Confirm Password' with '\*\*\*\*\*', 'First Name' with 'Jennifer', 'Last Name' with 'Smith', 'Permission' with a dropdown menu showing 'Administrator', and 'Description' with a text area containing 'A sample user account.'. At the bottom are 'OK' and 'Cancel' buttons.

**Figure 3-14.** *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 Management Console. 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.

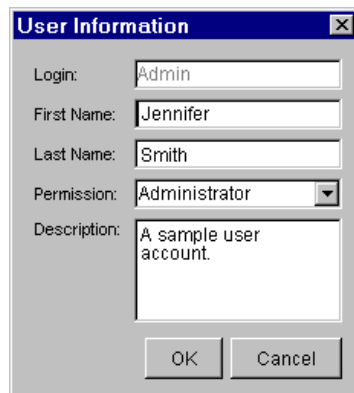
### To edit a user account:

- 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



**Figure 3-15.** *The User Information Dialog Box*

- 3 Edit the account as necessary.
- 4 Click `OK`.

The edited account is now available for the Enterprise Management Console. 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 Management Console. 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 Enterprise 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.

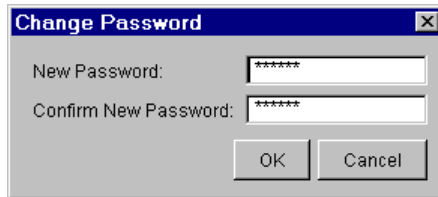
**To change an account password:**

- 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.



**Figure 3-16.** *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 Management Console. It is also **distributed** to any known sites on the network.

## Deploying User Accounts

Because user accounts greatly affect who can manage the wireless network, Mobile Manager immediately sends any changes you make to these accounts to all sites within a designated group.

---

**NOTE** The size of the files sent to update user accounts are very small, and do not impact site performance.

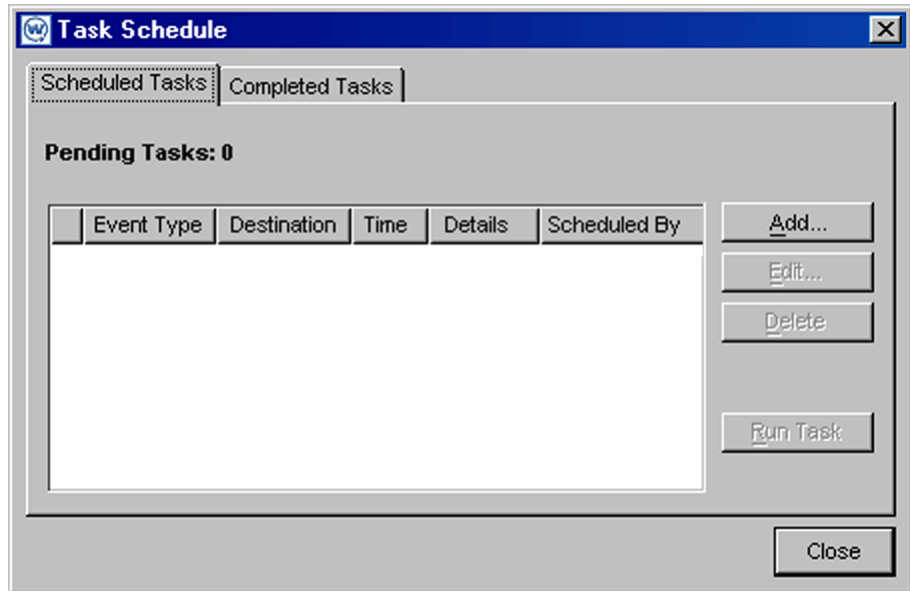
---

In the event that Mobile Manager was unable to deploy user accounts—for example, because the host system of the Enterprise Management Console was unable to connect to the network—you can manually schedule an event to deploy the accounts.

### To send user accounts to sites:

- 1 Select **Task Schedule** from the **Tools** menu.

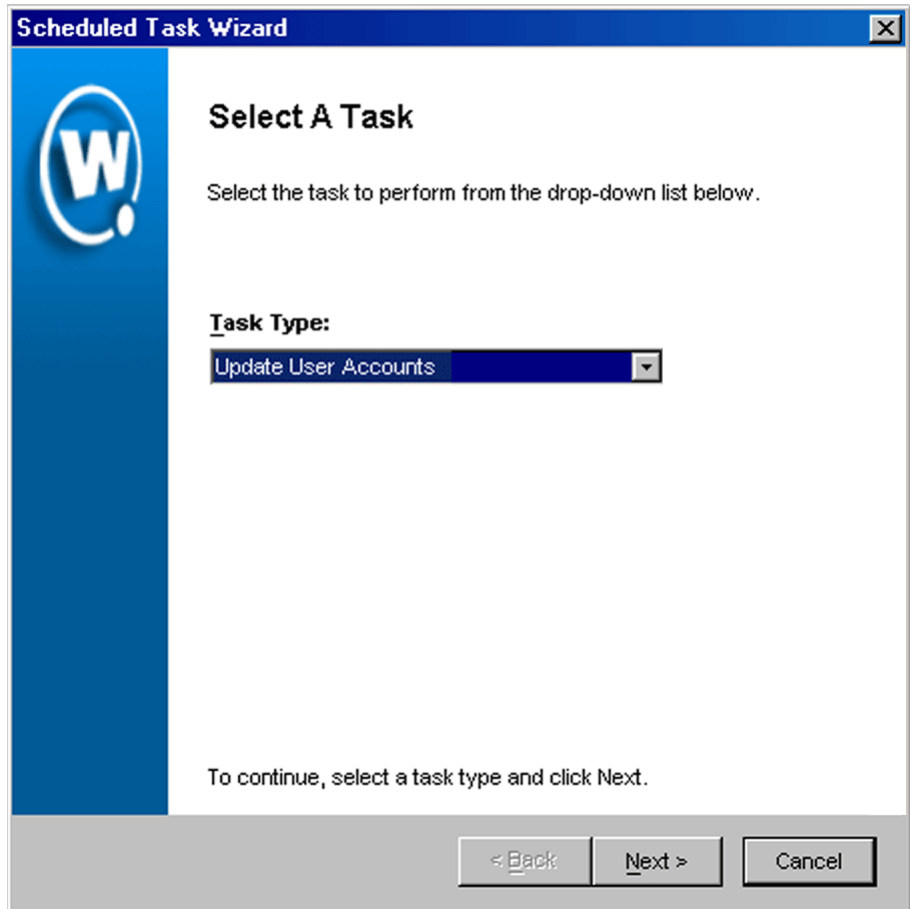
The *Task Schedule* dialog box appears.



**Figure 3-17.** *The Task Schedule Dialog Box*

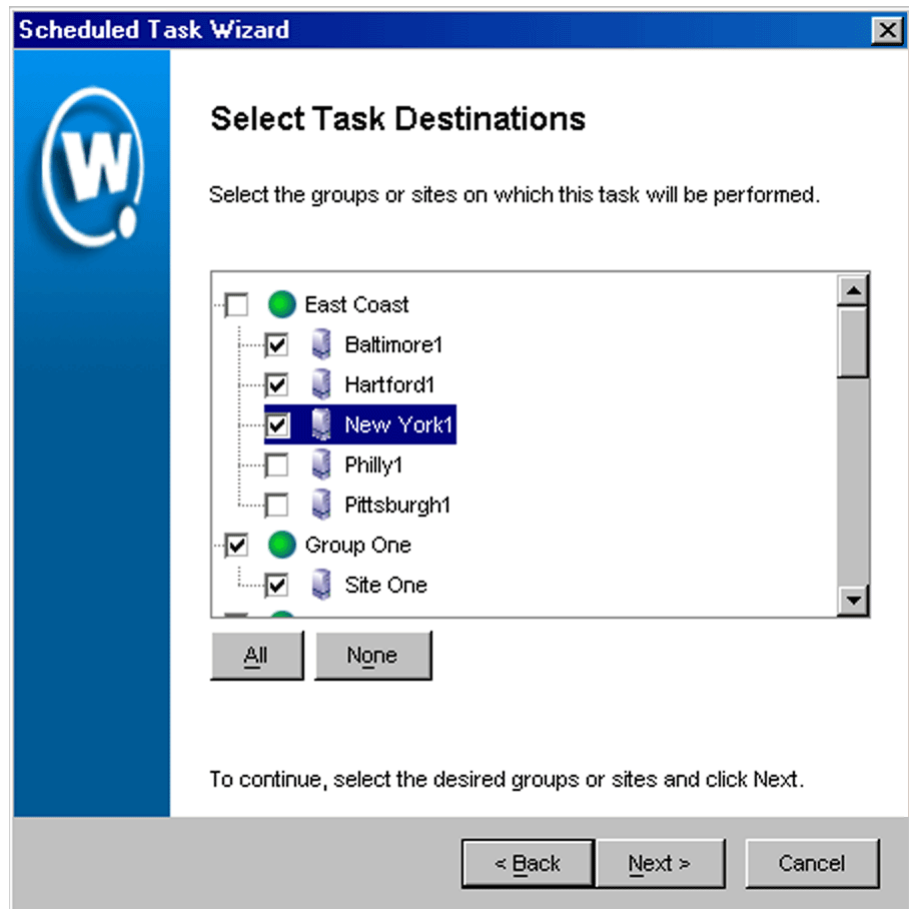
2 Click Add.

The *Select A Task* dialog box appears.



**Figure 3-18.** *The Select a Task Dialog Box*

- 3 Select `Update User Accounts` from the **Task Type** list and click `Next`.  
The *Select Task Destination* dialog box appears.



**Figure 3-19.** *The Select Task Destination Dialog Box*

- 4 Select the groups or sites by enabling the checkbox next to the group or site name. You can also select all groups by clicking `All`.
- 5 Click `Next`.

The *Select Settings to Deploy* dialog box appears.

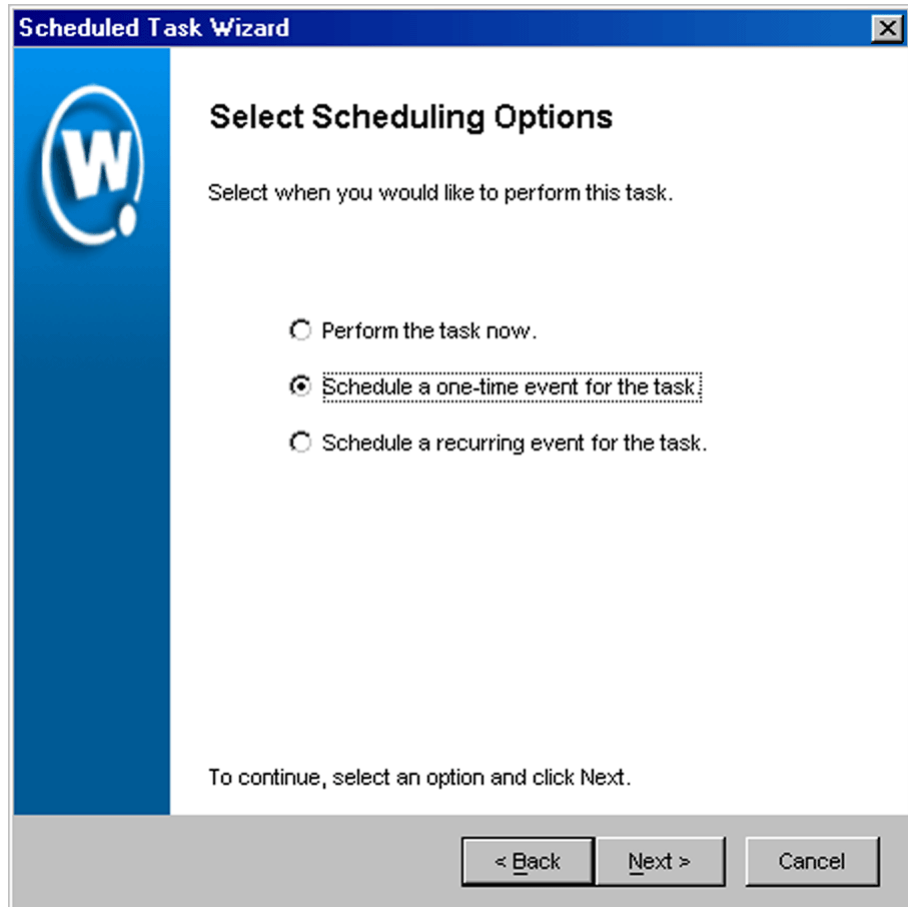




**Figure 3-20.** *The Select Settings to Deploy Dialog Box*

- 6 If you are only changing the ESS ID, IP addresses, or security settings, select the **Update Network Settings and Security Settings only** option.
- 7 If you are changing ESS ID, IP addresses, security settings, or access point profiles, select the **Update Network and Security Settings and synchronize Access Point Profiles** option.
- 8 Click **Next**.

The *Select Scheduling Options* dialog box appears.



**Figure 3-21.** *The Select Scheduling Options Dialog Box*

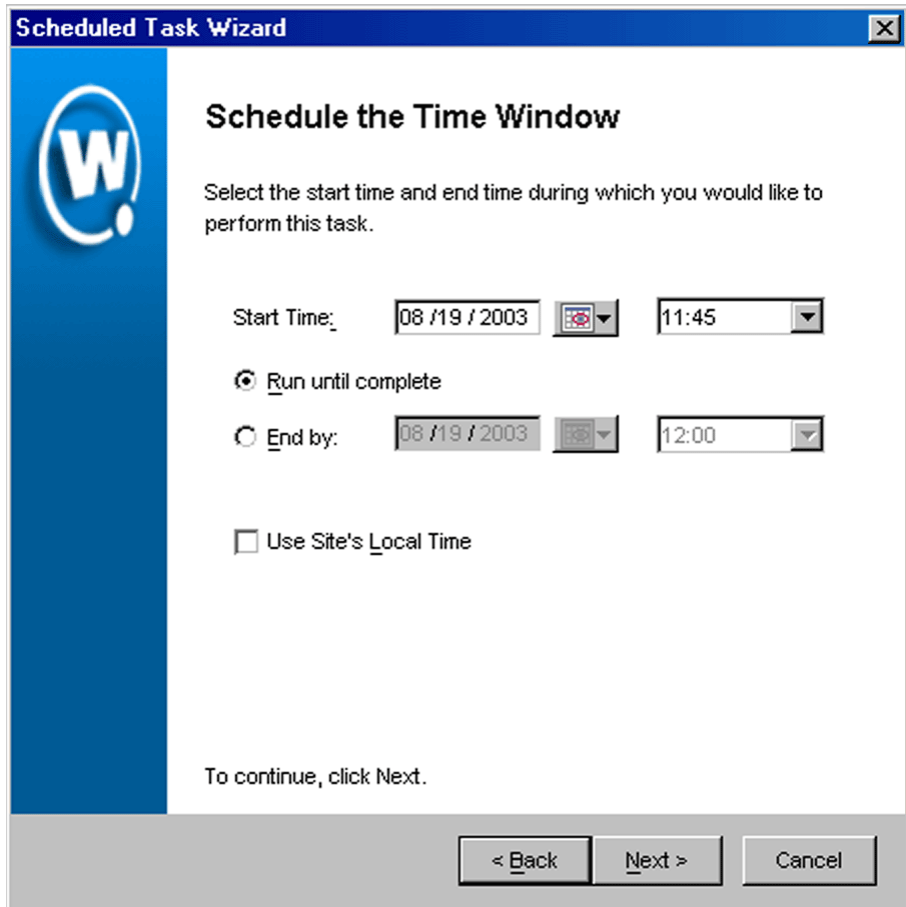
**9** Determine when the event will occur.

If you want the event to occur immediately, select the **Perform the task now** option.

If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

If you want the event to occur on a regular basis, select the **Schedule a recurring event** for this task option.

- 10 Click **Next**.
- 11 If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.



**Figure 3-22.** *The Schedule the Time Window Dialog Box*

Within this dialog box, you can set the following parameters for the event:

- Select the start date and time for the event.
- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete**

option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.
- 12** If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

**Scheduled Task Wizard**

## Configure Task Recurrence

Use the controls below to configure the recurrence settings

**Task time**

Start Time: 00:00  Run until complete  Use Site's Local Time  
 End by: 00:00

**Recurrence pattern**

Daily  Weekly  Monthly

Recur every 1 week(s) on:

Sunday  Monday  Tuesday  Wednesday  
 Thursday  Friday  Saturday

**Range of recurrence**

Start: 08 / 19 / 2003  No end date  
 End by: / /

To continue, click Next.

< Back    Next >    Cancel

**Figure 3-23.** The Configure Task Recurrence Dialog Box

Within this dialog box, you can set the following parameters for this event:

- Select the start time for the event.
- Determine when you want the event to stop. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

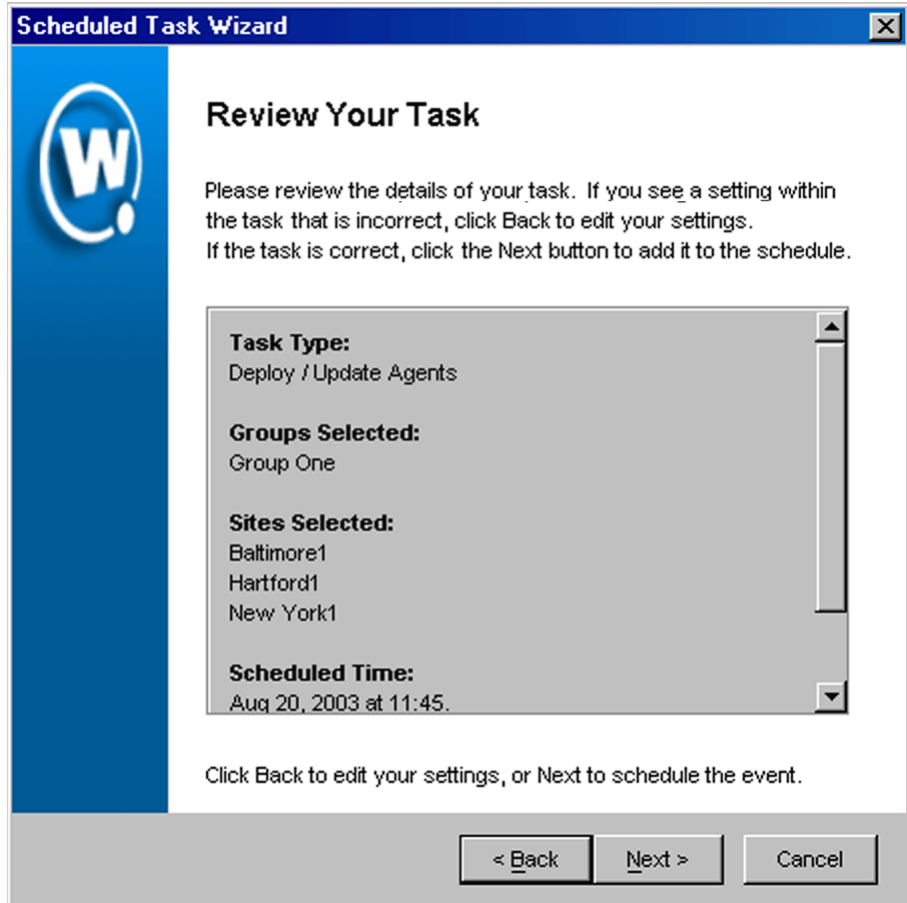
---

**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

**13** Click *Next*.

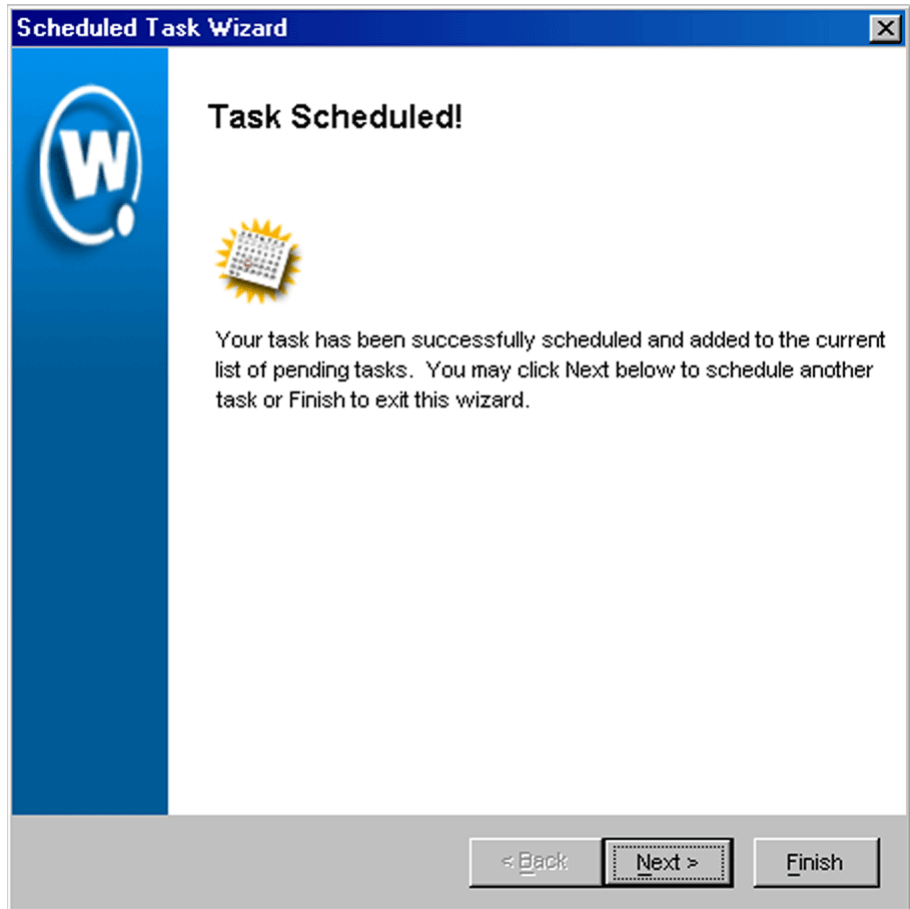
The *Review Your Task* dialog box appears.



**Figure 3-24.** *The Review Your Task Dialog Box*

**14** Review your the task to ensure that it is correct and click `Next`.

The *Task Scheduled* dialog box appears.



**Figure 3-25.** *The Task Scheduled Dialog Box*

- 15 Click `Next` to schedule a new event, or click `Finish` to return to the *Task Schedule* dialog box.

## Using the Task Scheduler

The Task Scheduler is a powerful component of Mobile Manager Enterprise that enables you to schedule network management activities for your sites and groups.



When you configure an aspect of your wireless network using the Enterprise Management Console, those configurations are not immediately sent to the rest of your network. Instead, you schedule specific times during which the new configurations are sent. Scheduling events provides several advantages, including:

- the ability to specify which sites or group receive the changes
- the ability to implement changes during periods of low network activity

To access the Task Scheduler, select `Task Schedule` from the **Tools** menu, or click the clock icon on the menu toolbar. The Task Schedule dialog box appears. This dialog box contains two tabs. The first tab, `Scheduled Tasks`, shows a list of tasks that have yet to be implemented. The second tab, `Completed Tasks`, shows a list of tasks that are either in process, or are already complete.

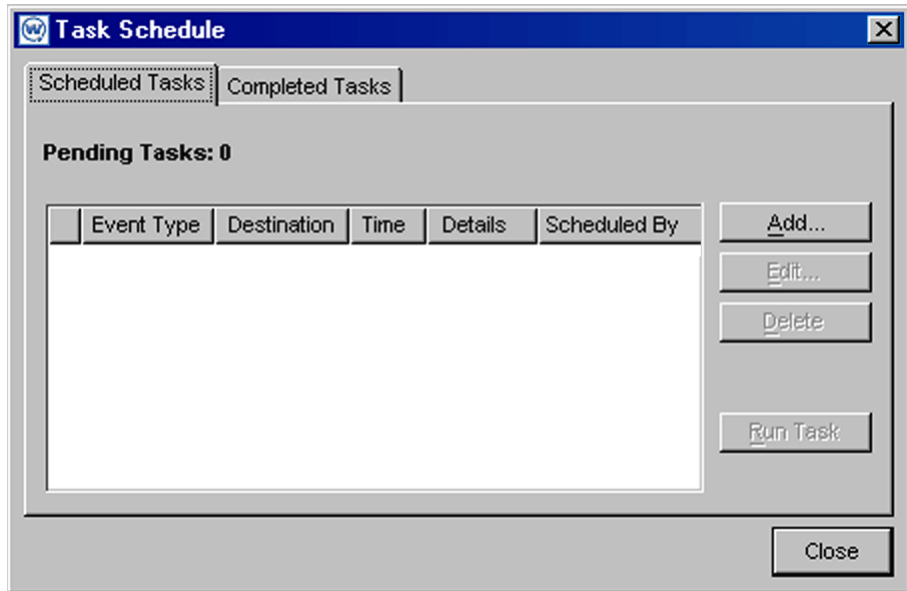
## **Adding Tasks**

You can add as many tasks as necessary to the Task Scheduler.

### **To add a task to the Task Scheduler:**

- 1 Select `Task Schedule` from the **Tools** menu.

The *Task Schedule* dialog box appears.



**Figure 3-26.** *The Task Schedule Dialog Box*

- 2 Select the Scheduled Tasks tab.
- 3 Click Add.

When you click the Add button, the Scheduled Task Wizard launches. This wizard allows you to select and configure the task as needed. The types of tasks you can create are:

- Synchronize Group Settings Between Agents, which is described in *Deploying Settings for All Devices* on page 217.
- Deploy Access Point Settings, which is described in *Deploying Access Point Settings* on page 227.
- Deploy Mobile Device Settings, which is described in *Deploying Mobile Device Settings* on page 238.
- Update Very Large Access Control List, which is described in *Deploying Access Control Lists* on page 322

- Update Access Point Firmware, which is described in *Deploying Firmware Packages* on page 192.
- Deploy/Update Agents, which is described in *Deploying Sites* on page 121.
- Retrieve Access Point Statistics, which is described in *Gathering Statistics* on page 426.
- Update User Accounts, which is described in *Deploying User Accounts* on page 59.
- Set Destination IP Address for Network Alerts, which is described in *Setting the Destination IP Address for Network Alerts* on page 399.
- Perform Database Maintenance, which is described in *Performing Database Maintenance* on page 414.
- Uninstall Agents, which is described in *Deleting Agents* on page 138.

See the appropriate section for complete information on how to configure the needed task.

---

**NOTE** When you place the cursor over an entry in the *Scheduled Tasks* dialog box, a tool tip appears, displaying all of the information for that entry.

In addition, you can modify the size of each column to suit your preferences.

---

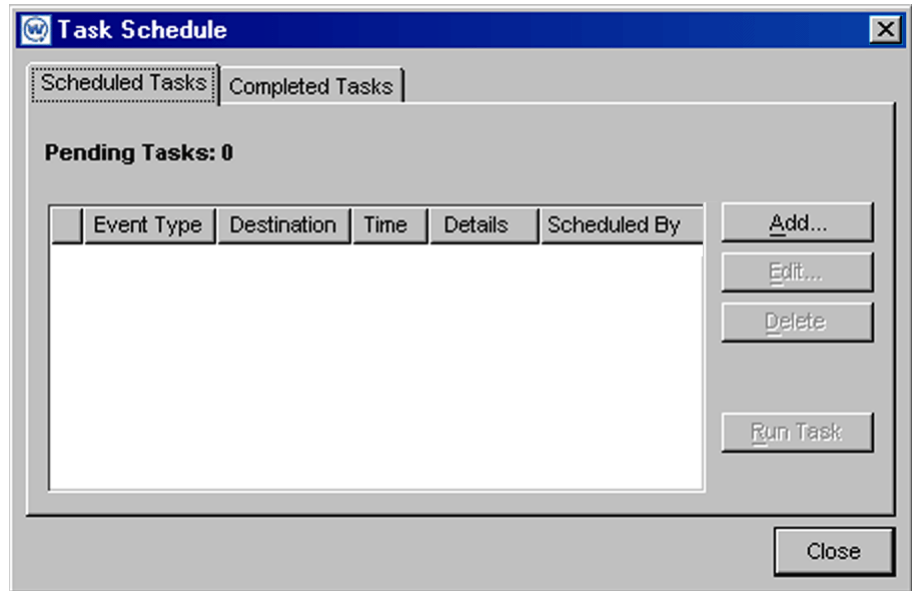
## Editing Tasks

From the Task Scheduler, you can edit existing tasks on an as-needed basis.

### To edit a task:

- 1 Select `Task Schedule` from the **Tools** menu.

The *Task Schedule* dialog box appears.



**Figure 3-27.** *The Task Schedule Dialog Box*

- 2 Select the Scheduled Tasks tab.
- 3 Select the appropriate task.
- 4 Click `Edit`.

The Scheduled Task Wizard launches, allowing you to edit the task.

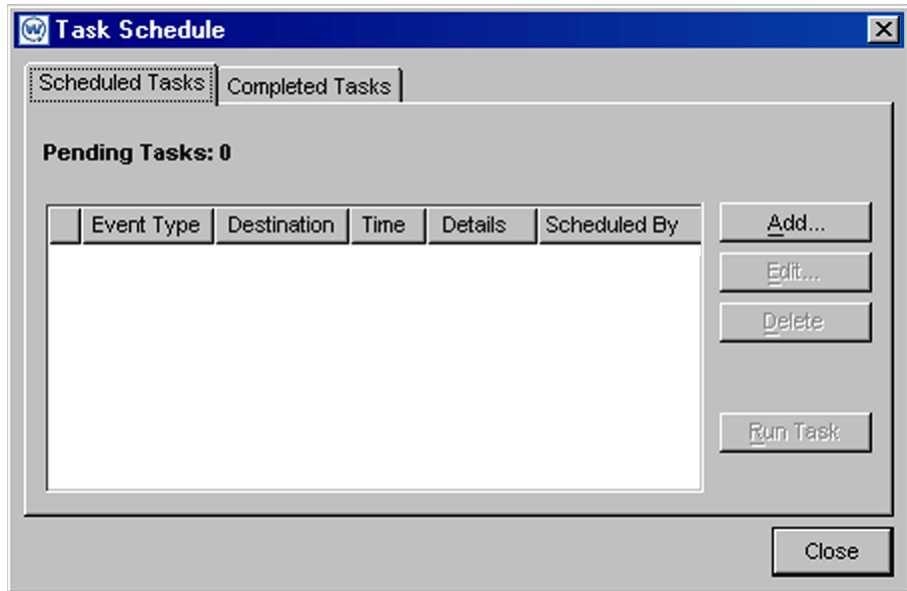
## Deleting Tasks

If you decide that a task should not be implemented, you can delete it from the Task Scheduler.

### To delete a task:

- 1 Select `Task Schedule` from the **Tools** menu.

The *Task Schedule* dialog box appears.



**Figure 3-28.** *The Task Schedule Dialog Box*

- 2 Select the Scheduled Tasks tab.
- 3 Select the appropriate task.
- 4 Click `Delete`.

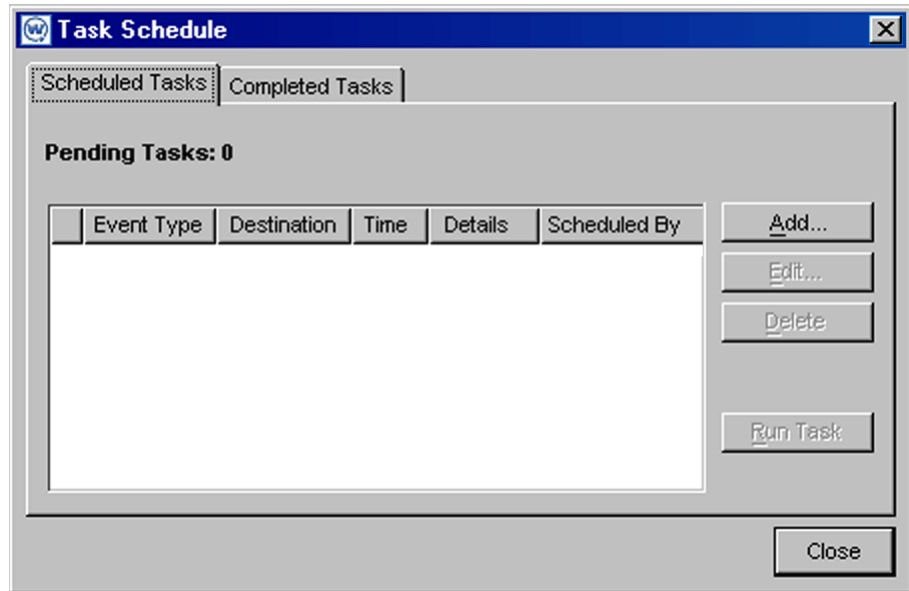
### Running Tasks Immediately

When you schedule a task, you typically assign a date in the future, at which time Mobile Manager Enterprise will complete the task. However, under certain circumstances you might want to run a task as soon as you have finished scheduling it. For these purposes, you can use the **Run Task** option.

#### To run a task immediately:

- 1 Select `Task Schedule` from the **Tools** menu.

The *Task Schedule* dialog box appears.



**Figure 3-29.** *The Task Schedule Dialog Box*

- 2 Select the Scheduled Tasks tab.
- 3 Select the appropriate task.
- 4 Click Run Task.

---

**NOTE** When you use the **Run Task** option, the task remains in the Task Scheduler. Mobile Manager will still run the task based on its assigned time schedule unless you delete the task. See *Deleting Tasks* on page 74 for more information on how to delete a task.

---

## Viewing Task Progress

Tasks can take varying lengths of time to complete. This variation is due to a number of factors, such as the amount of data being sent to a site (for example, with a firmware update) or network connection speeds.

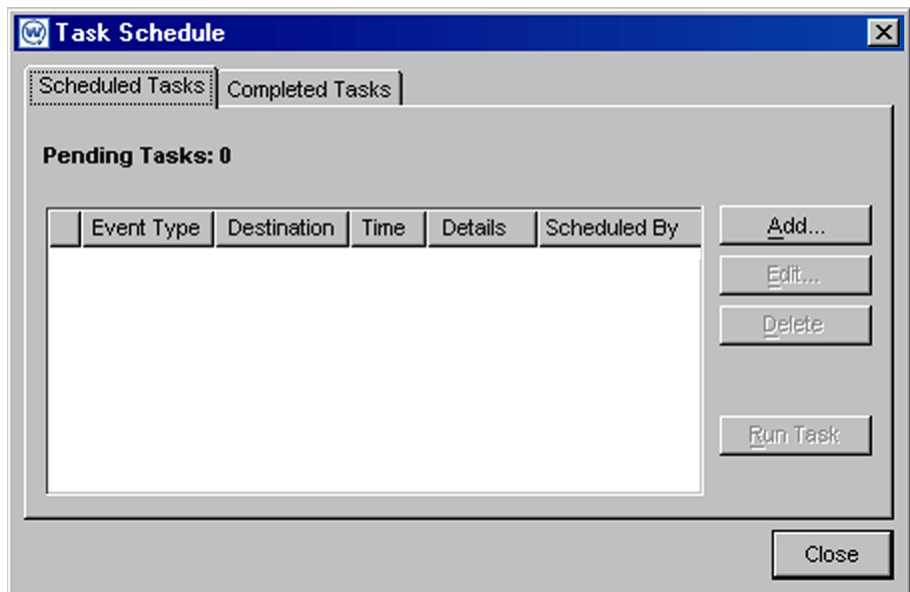
When Mobile Manager Enterprise begins to implement a task, that task appears in the Completed Task tab of the Task Scheduler. Tasks that are in process but not yet complete have a series of dots preceding their entry in the

Completed Tasks tab. In addition, the Details column within this tab tells you how many sites have been successfully updated with the task and how many have failed.

**To view task progress:**

- 1 Select `Task Schedule` from the **Tools** menu.

The *Task Schedule* dialog box appears.



**Figure 3-30.** *The Task Schedule Dialog Box*

- 2 Select the Completed Tasks tab.
- 3 View the information for the appropriate task.

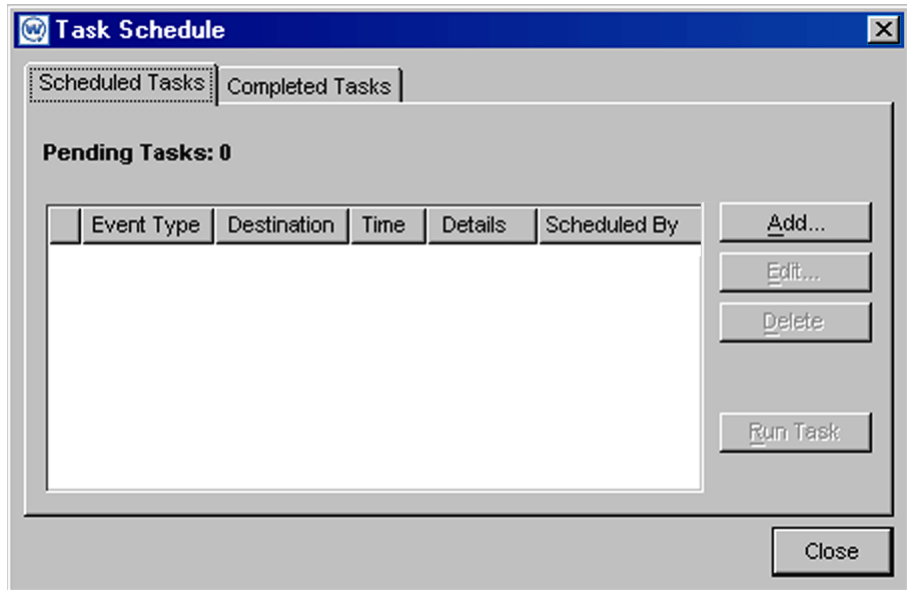
## Rescheduling Tasks

After a task has completed, you can elect to reschedule that task to occur again at a future date.

**To reschedule a task:**

- 1 Select `Task Schedule` from the **Tools** menu.

The *Task Schedule* dialog box appears.



**Figure 3-31.** *The Task Schedule Dialog Box*

- 2 Select the Completed Tasks tab.
- 3 Select the task you want to reschedule
- 4 Click Reschedule.

The Scheduled Task Wizard launches, allowing you to re-assign a date and time to the task.

Rescheduled tasks appear as a new entry in the Scheduled Tasks tab of the Task Scheduler; however, the original task remains in the Completed Tasks tab.

## Deleting Completed Tasks

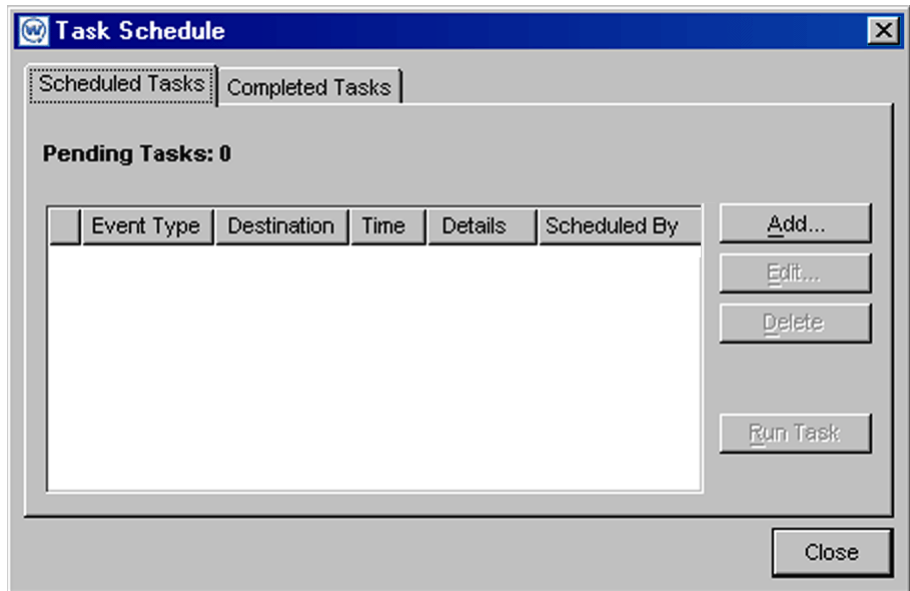
You can delete tasks from the Completed Task list at any time.

### To delete a completed task:

- 1 Select `Task Schedule` from the **Tools** menu.



The *Task Schedule* dialog box appears.



**Figure 3-32.** *The Task Schedule Dialog Box*

- 2 Select the Completed Tasks tab.
- 3 Select the task.
- 4 Click Delete.



## Chapter 4: Managing Locations

One of the primary tasks you accomplish with Mobile Manager is location management. A location is defined as any area within your network that contains wireless components that you want to manage.

Mobile Manager divides locations into two categories: sites and groups. A site is the most basic component of the Enterprise Management Console. 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.

---

**NOTE** The number of wireless components managed at a site depends on the communication range of the Agents installed at that site. Traditionally this range has been defined as a single subnet on your network; however, depending on your network architecture, you can configure an Agent to communicate past a given subnet. This type of configuration takes place at the site level, using one of Mobile Manager's site tools. See the *Mobile Manager User's Guide* or the *Avalanche Manager's User Guide* for more information.

---

Mobile Manager Enterprise 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 Management Console 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 describes how to manage both sites and groups. Once you create the necessary sites and groups for your network, you can manage them by configuring access point and mobile device properties as needed. See *Chapter 5: Managing Access Points* on page 153 and *Chapter 7: Managing Mobile Devices* on page 251 for more information.

## Sites

A site is any location that contains wireless components that are managed by an access point Agent, a mobile device Agent, or both. A site can be a unique physical entity, such as a warehouse, or a subsection of an entity, such as the third floor of an office building.

The number of wireless components managed at a site depends on the communication range of the Agents installed at that site. Traditionally, this range has been defined as a single subnet on your network; however, depending on your network architecture, you can configure an Agent to communicate past a given subnet.

To ensure that all wireless devices are managed at a particular site, you can do one of the following:

- Configure your network hardware to allow access point and mobile device broadcasts to reach the Agents
- Use the site-based tools included with Mobile Manager to configure the Agent to manage multiple subnets
- Segment the location into multiple sites by installing the appropriate Agents at each subnet

### Creating Sites

In most cases, the location you want to manage with Mobile Manager does not contain an Agent. As a result, you must create a new site by deploying one or more Agents to that location.

If the location already contains one or more Agents, you do not need to create a new site. However, you must ensure that the Agent installed at the site is compatible with the Enterprise Management Console. See *Requirements* on page 14 for more information.

Creating a site involves three processes:

- Creating a collection of files that define Agent behavior, called a deployment package
- Adding the site within the Enterprise Manage Console
- Deploying that package to the desired location

## **Creating Deployment Packages**

A deployment package is a collection of files that define Agent behavior. You can create deployment packages for [access points only](#), [mobile devices only](#), or [both](#).

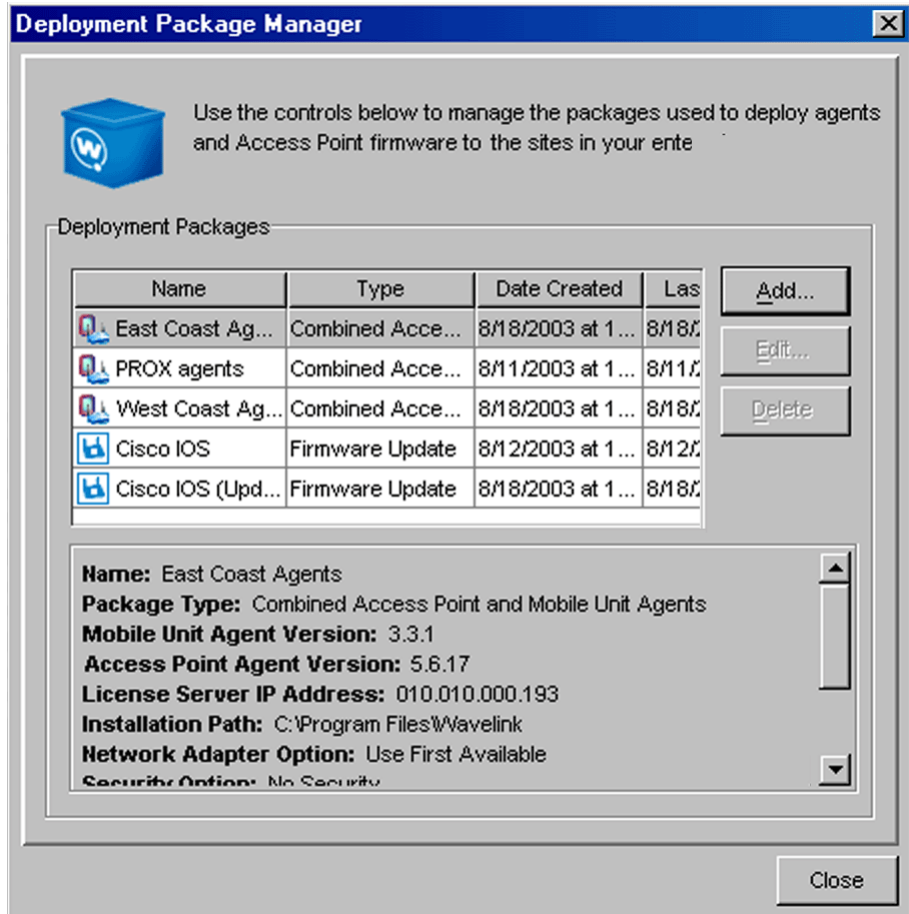
### **Deployment Packages for Access Points**

This section describes how to create a deployment package that will manage only the access points at a specific location.

#### **To create a deployment package for access points:**

- 1 Select Deployment Packages from the **Tools** menu.

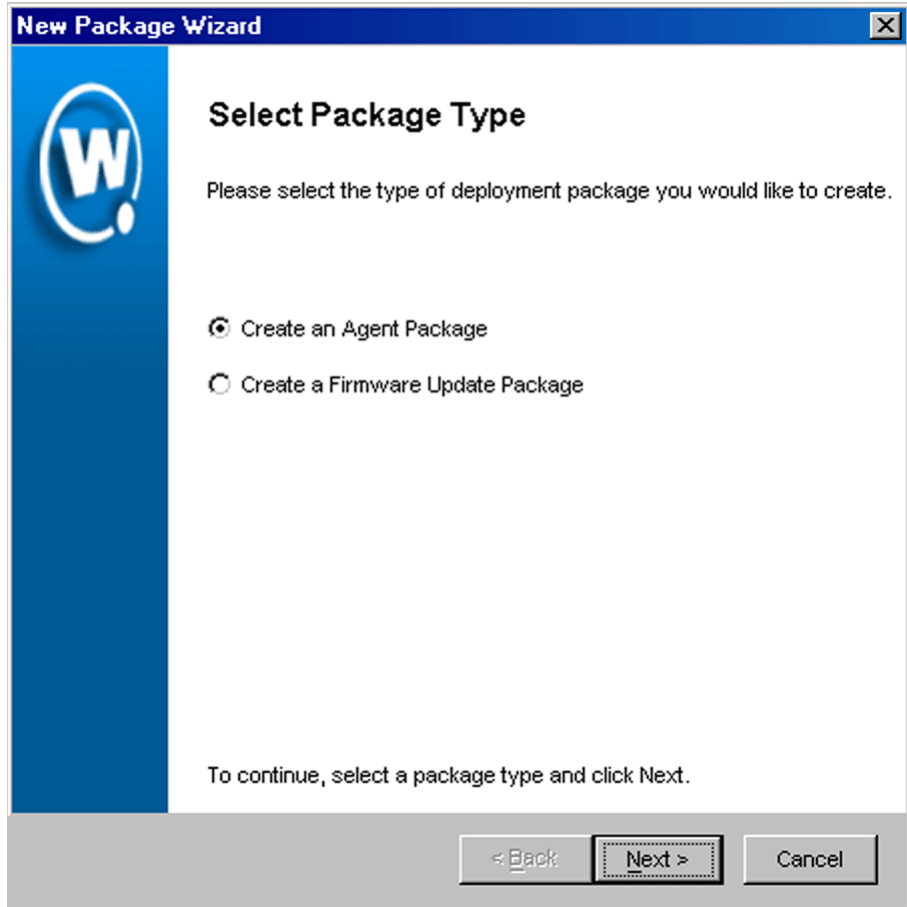
The *Deployment Package Manager* dialog box appears.



**Figure 4-1.** The Deployment Package Manager Dialog Box

- 2 Click Add.

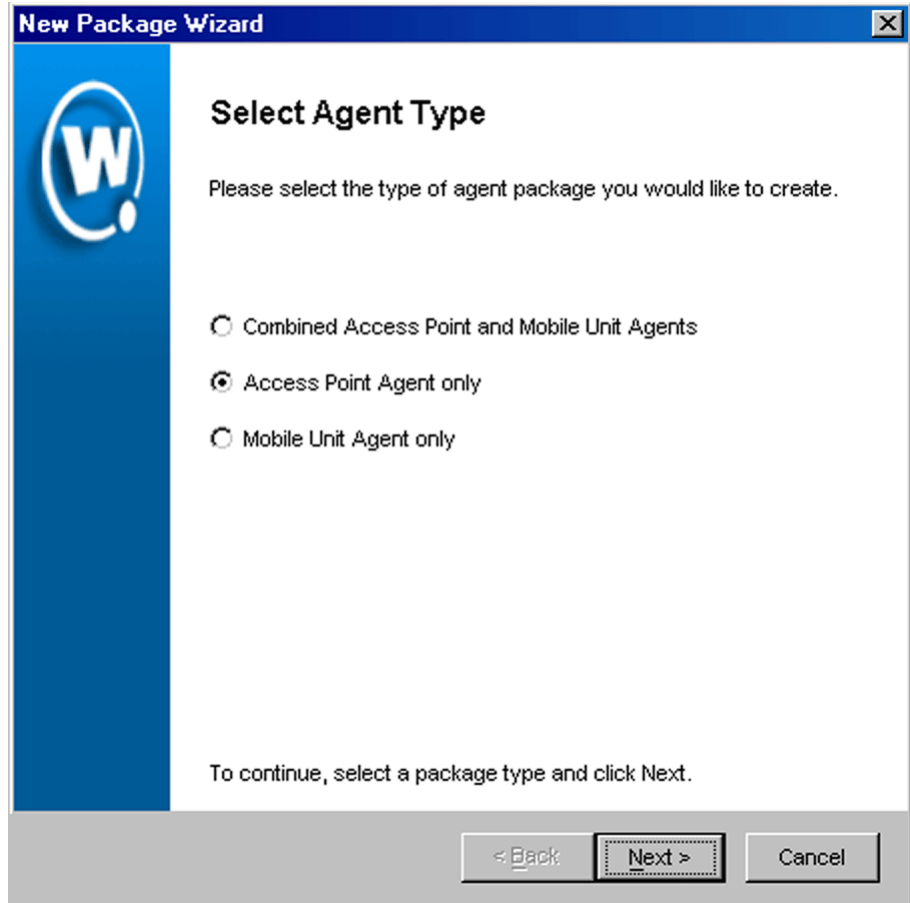
The *Select Package Type* dialog box appears.



**Figure 4-2.** *The Select Package Type Dialog Box*

**3** Select the **Create an Agent Package** option and click **Next**.

The *Select Agent Type* dialog box appears.



**Figure 4-3.** *The Select Agent Type Dialog Box*

- 4 Select one of the Access Point Agent choices and click on **Next**.

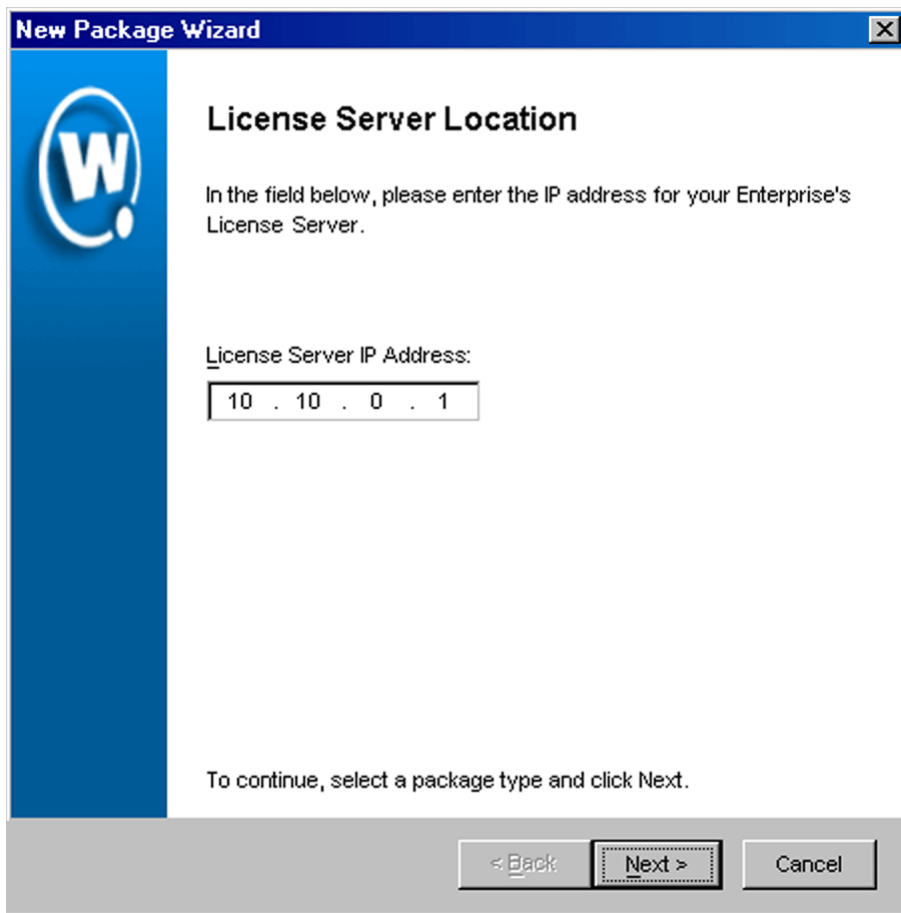
**Access Point Agent only** deploys a full-function Access Point Agent to a site that may or may not yet have an Access Point Agent. You will be able to control numerous deployment choices on the subsequent wizard panels. Continue with step 5 in this topic.

If you only want to update an existing Access Point Agent to the latest version of Mobile Manager, without changing any settings or deploying any firmware files, you can pick **Lightweight Access Point Agent Update**, as long as the existing Access Point Agent is at least version 5.7.1. The resulting deployment



package will be much smaller in size, only about 9MB, so this is particularly advantageous for low bandwidth networks.

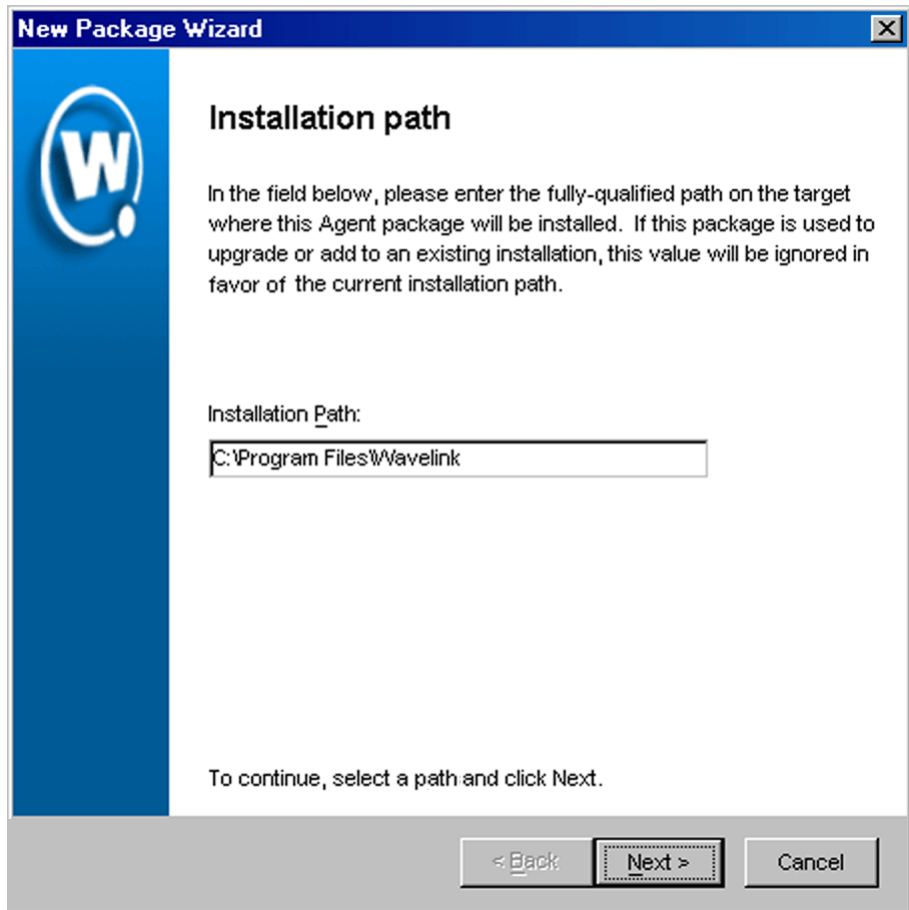
If you select the **Lightweight Access Point Agent Update** choice and click on **Next**, you will immediately advance to the final panel in the deployment Wizard, where you enter the package name. Please skip ahead to step 12 in this topic.



**Figure 4-4.** *The License Server Location Dialog Box*

- 5 Type the IP address of the license server for Mobile Manager and click Next. This IP address is typically the same as the location of Mobile Manager back-end components.

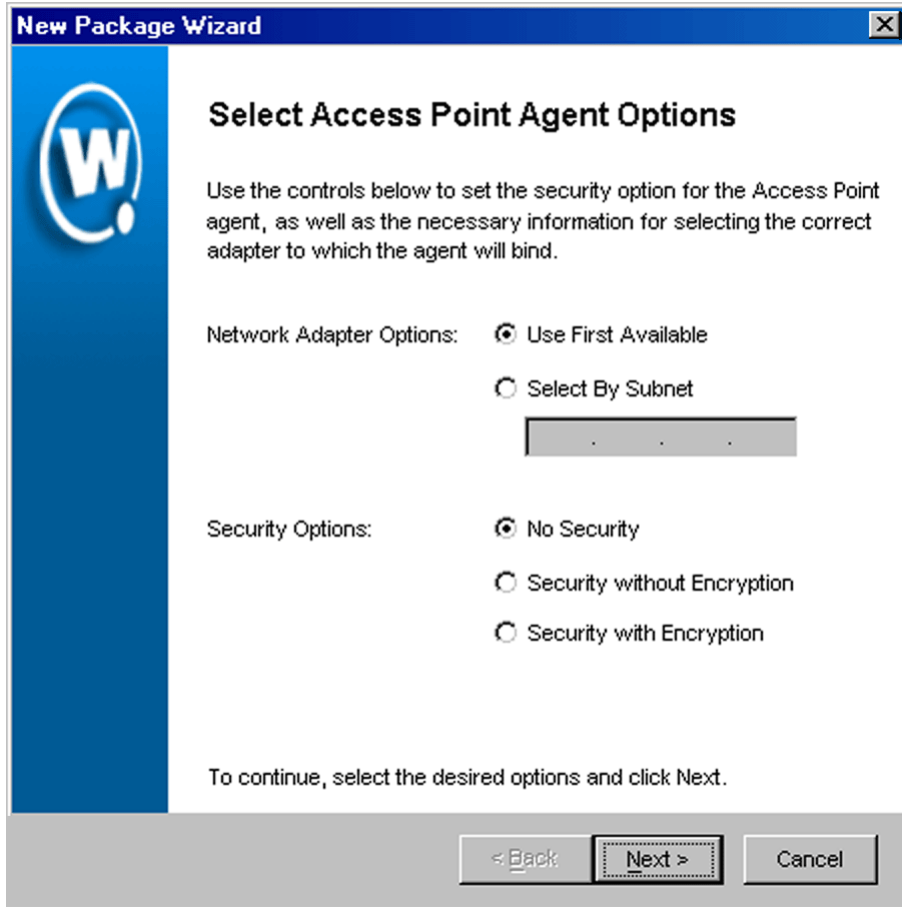
The *Installation Path* dialog box appears.



**Figure 4-5.** *The Installation Path Dialog Box*

- 6 Type the full path where the package is installed on any remote system in the *Installation Path* dialog box, for example, C:\Program Files\Wavelink, and click Next.

The *Select Access Point Agent Options* dialog box appears.



**Figure 4-6.** *The Select Access Point Agent Options Dialog Box*

#### 7 Determine how the access point Agent selects a network adapter.

If you want the Agent to select the first available network adapter, select the **First Available** option. This option is recommended if the system that will host the Agent only has one network adapter.

If you want the Agent to select an adapter based on a specific subnet, select the **Select by Subnet** option and then type the subnet address in the text box. For example, if the adapter resides on subnet 172.15.6.0, you would type 172.15.6.0 in this text box.

**8** Determine the security options for the Agent and console.

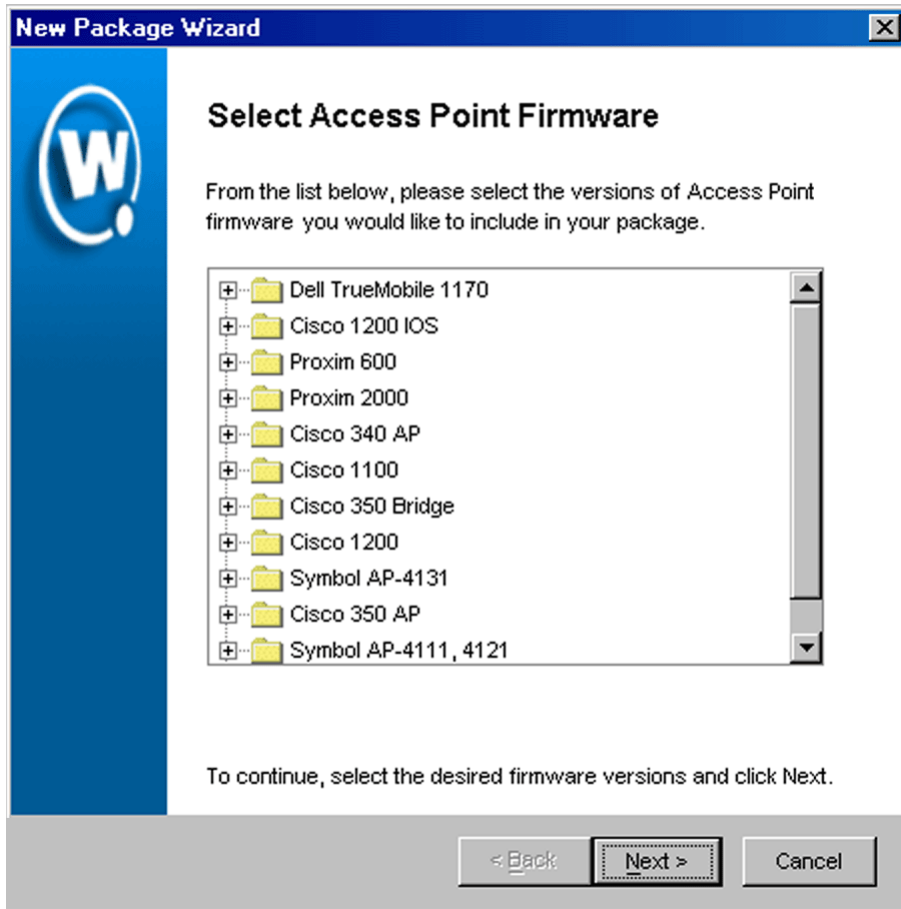
If you want the Agent to operate without any security measures, select the **No Security** option.

If you want the Agent to require a user name and password, select the **Security without Encryption** option.

If you want the Agent to require a user name and password and encrypt communications between management consoles and the Agent, select the **Security with Encryption** option.

**9** Click `Next`.

The *Select Access Point Firmware* dialog box appears. This dialog box contains a collection of folders, with each folder representing a specific type of access point.



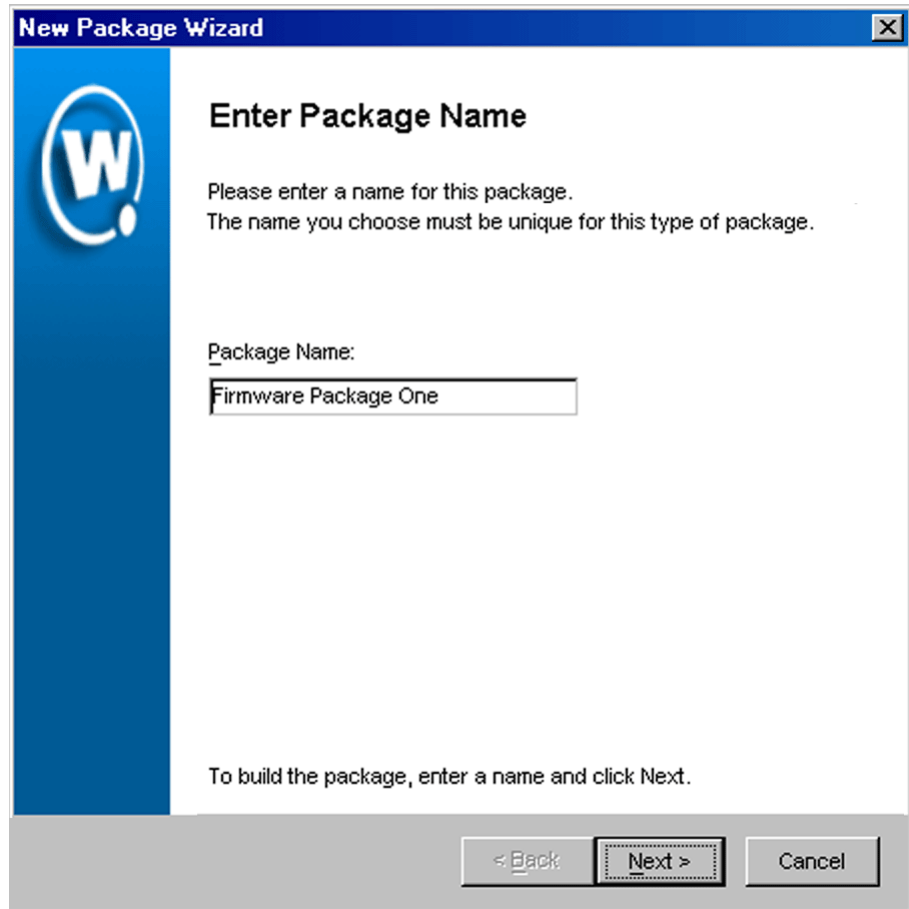
**Figure 4-7.** *The Select Access Point Firmware Dialog Box*

**10** Select the firmware versions this Agent will support.

To select firmware, open the appropriate folder within the dialog box. A list of available firmware versions appears. Select a firmware version by enabling the checkbox next to the firmware name. You can select as many firmware versions, from as many folders, as needed.

**11** Click *Next*.

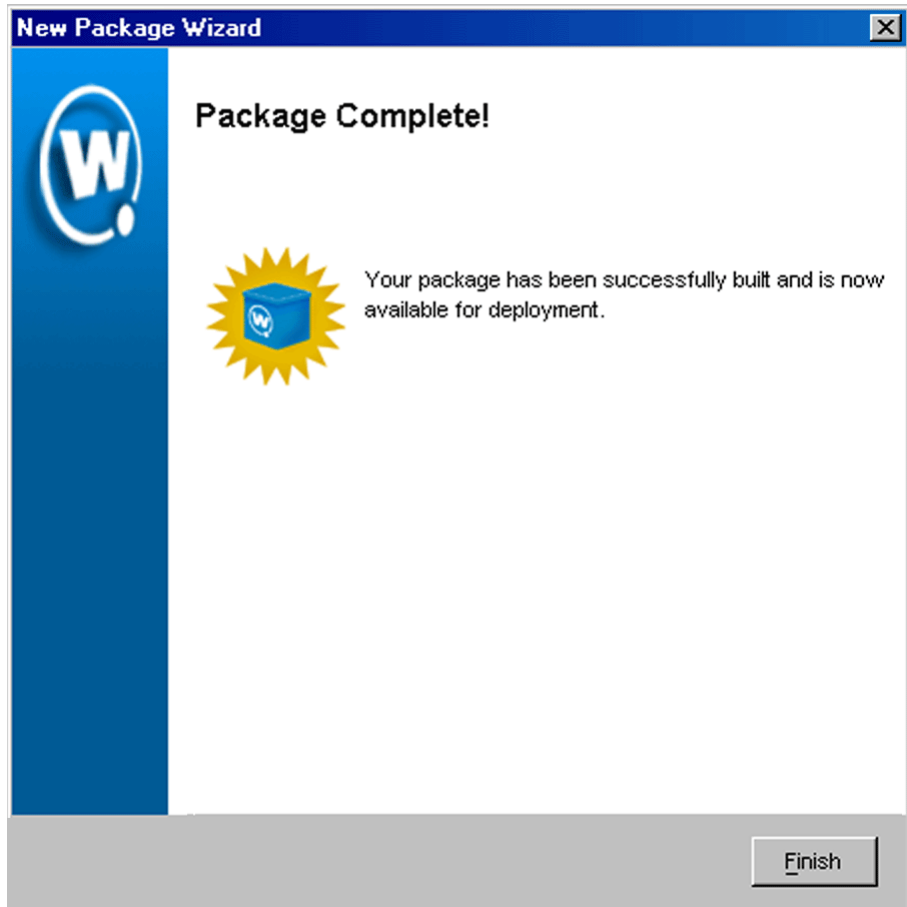
The *Enter Package Name* dialog box appears.



**Figure 4-8.** *The Enter Package Name Dialog Box*

- 12** Type a name for the package in the **Package Name** text box and click **Next**.

Mobile Manager begins to create the deployment package. When it is finished, a *Package Complete* dialog box appears.



**Figure 4-9.** *The Package Complete Dialog Box*

**13** Click `Finish`.

Mobile Manager returns you to the *Deployment Package Manager* dialog box. You can now create a new package, edit a package, or delete a package as needed.

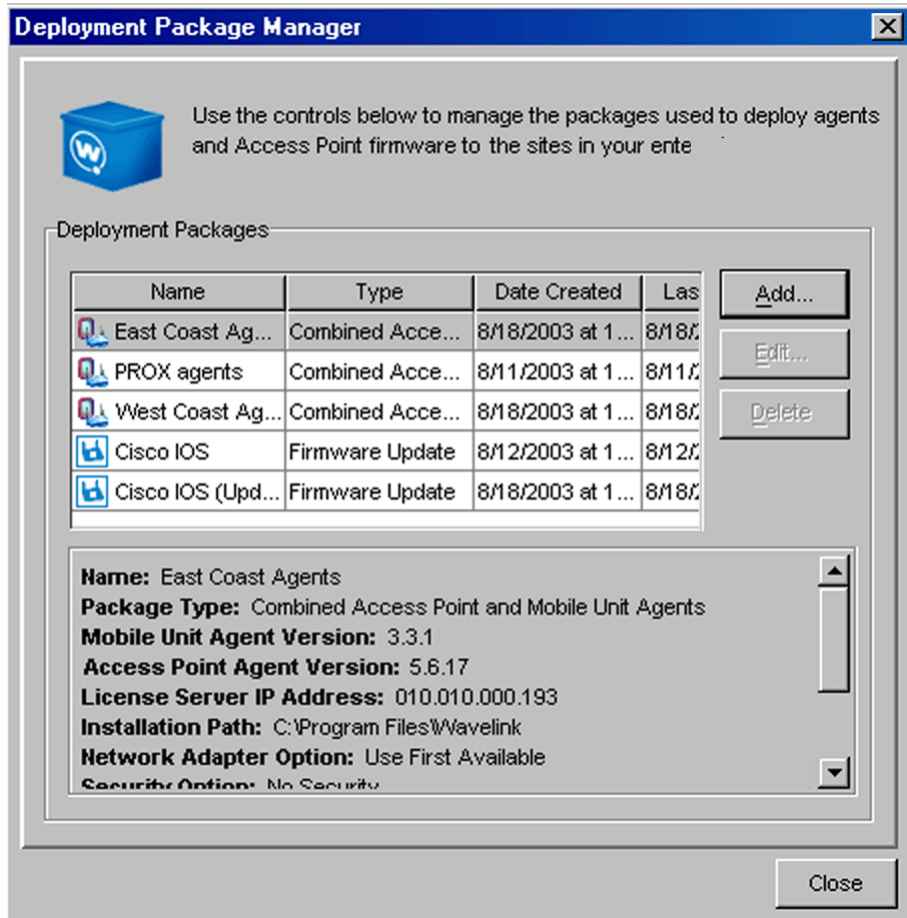
### **Deployment Packages for Mobile Devices**

This section describes how to create a deployment package that will manage only the mobile devices at a specific location.

**To create a deployment package for mobile devices:**

- 1 Select Deployment Packages from the **Tools** menu.

The *Deployment Package Manager* dialog box appears.



**Figure 4-10.** *The Deployment Package Manager Dialog Box*

- 2 Click Add.

The *Select Package Type* dialog box appears.

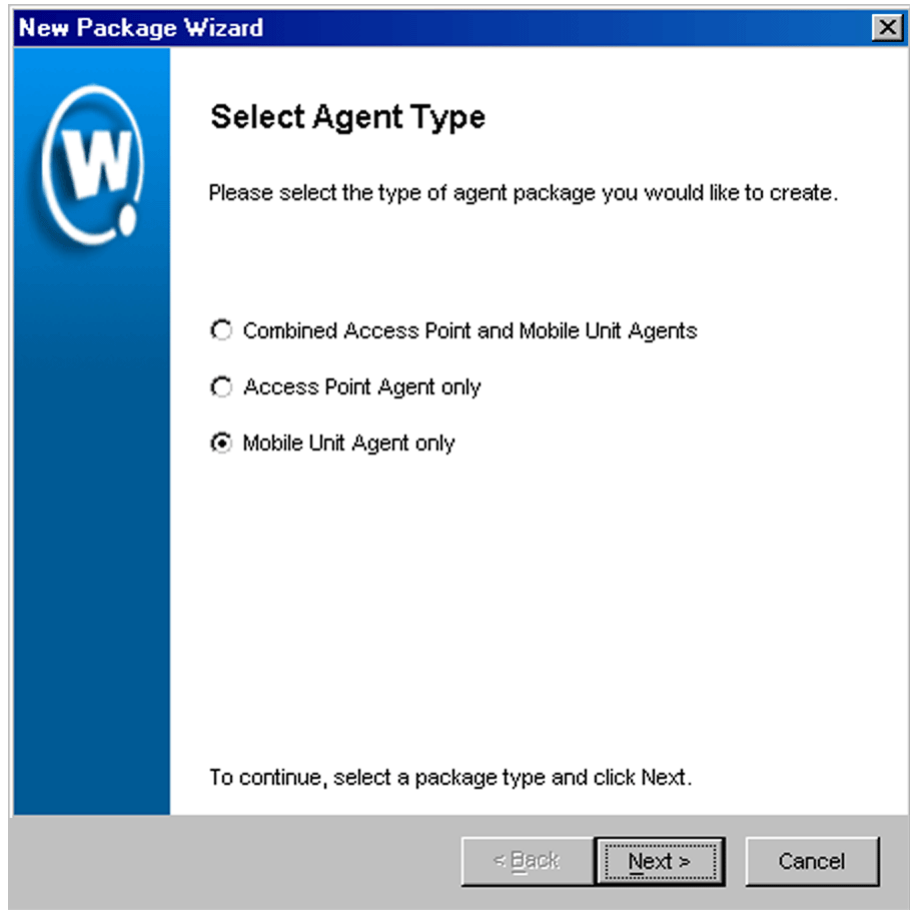




**Figure 4-11.** *The Select Package Type Dialog Box*

**3** Select the **Create an Agent Package** option and click **Next**.

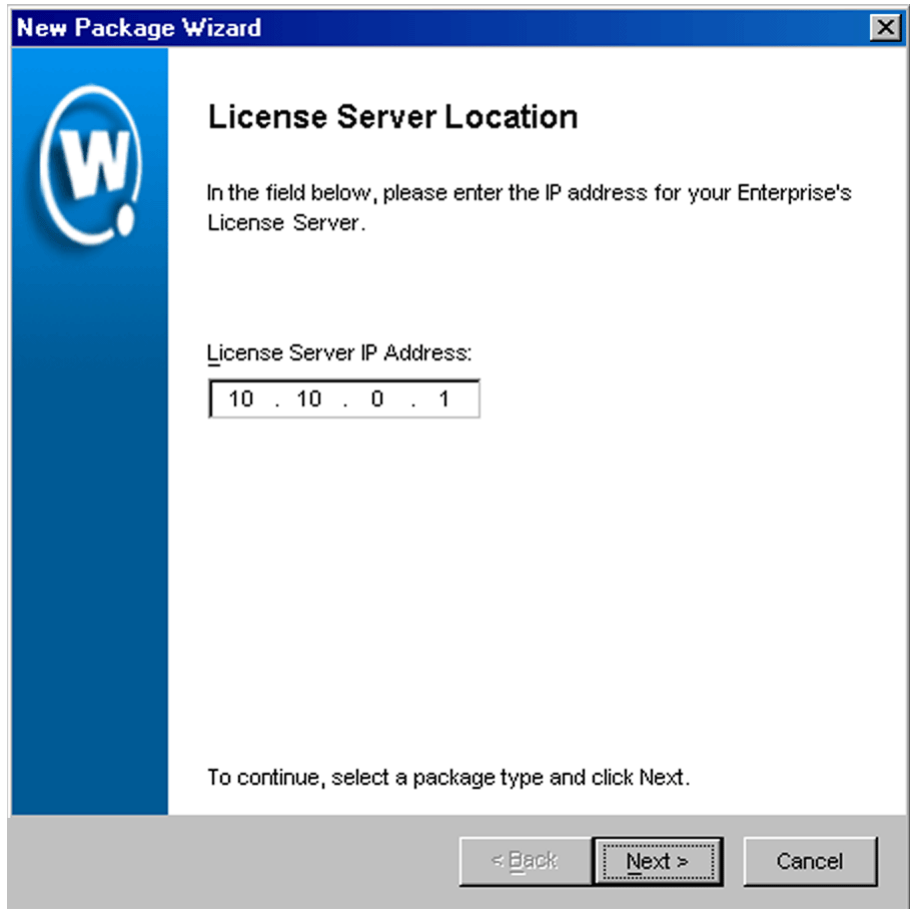
The *Select Agent Type* dialog box appears.



**Figure 4-12.** *The Select Agent Type Dialog Box*

- 4 Select the **Mobile Unit Agent Only** option and click Next.

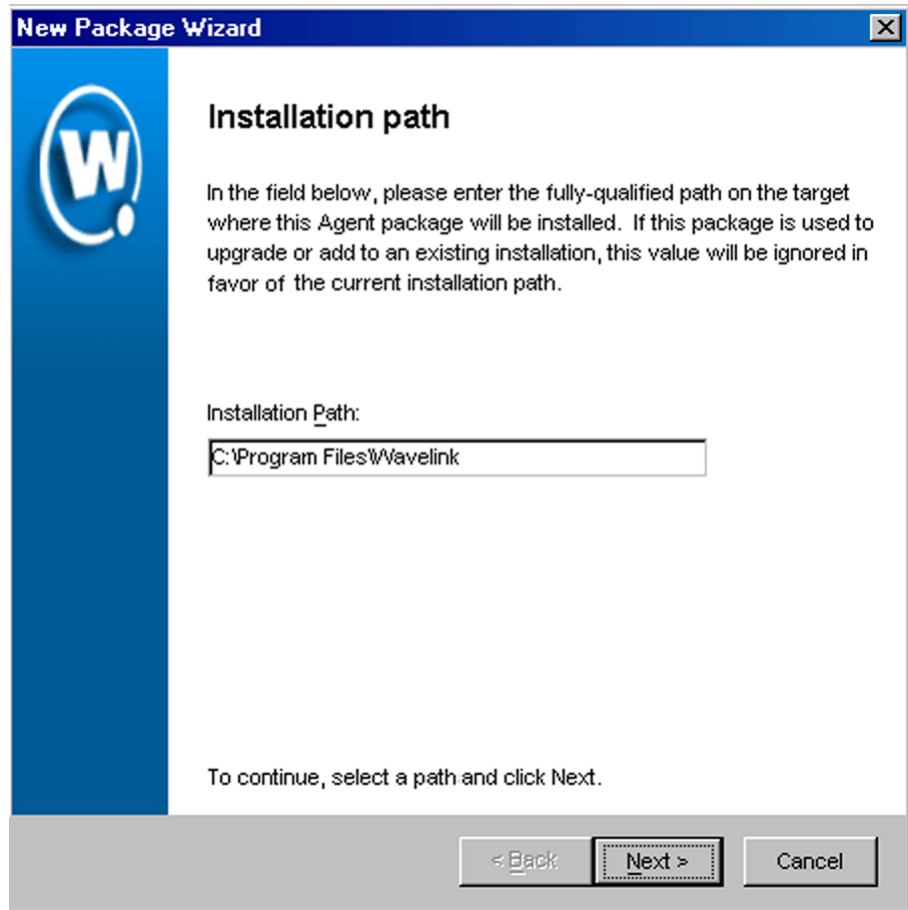
The *License Server Location* dialog box appears.



**Figure 4-13.** *The License Server Location Dialog Box*

- 5 Type the IP address of the license server for Mobile Manager and click Next. This IP address is typically the same as the location of Mobile Manager back-end components.

The *Installation Path* dialog box appears.



**Figure 4-14.** *The Installation Path Dialog Box*

- 6 Type the full path where the package is installed on any remote system in the *Installation Path* dialog box, for example, C:\Program Files\Wavelink, and click *Next*.

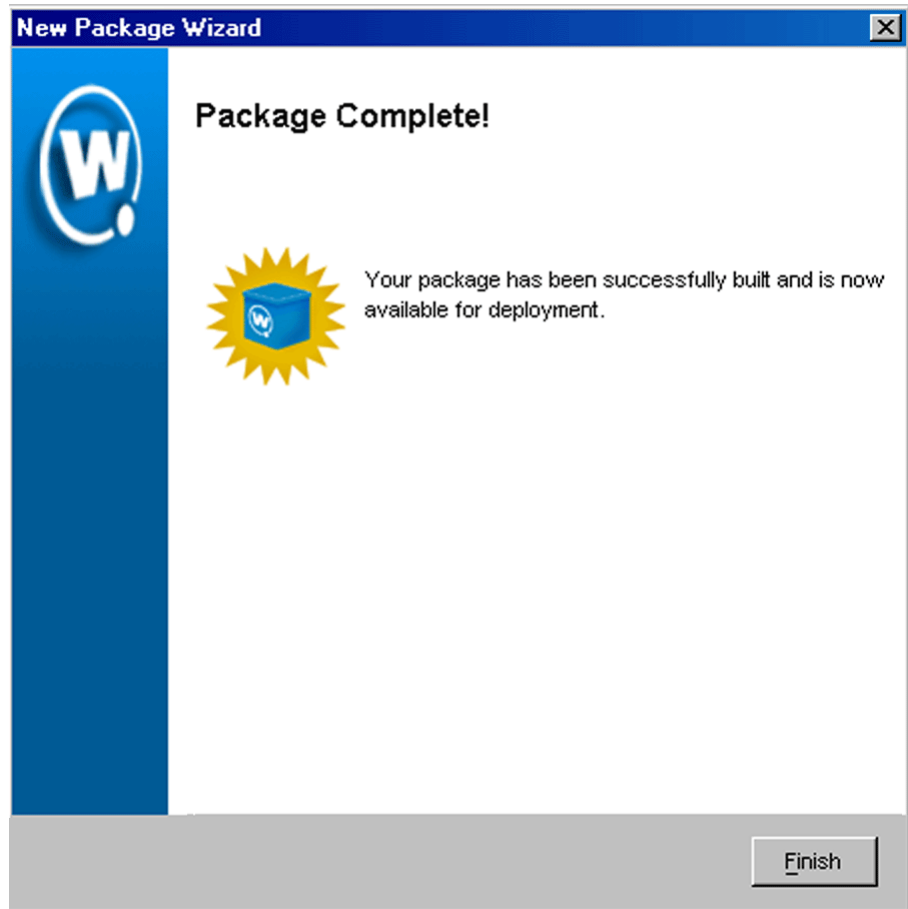
The *Enter Package Name* dialog box appears.



**Figure 4-15.** *The Enter Package Name Dialog Box*

- 7 Type a name for the package in the **Package Name** text box and click **Next**.

Mobile Manager begins to create the deployment package. When it is finished, a *Package Complete* dialog box appears.



**Figure 4-16.** *The Package Complete Dialog Box*

8 Click `Finish`.

Mobile Manager returns you to the *Deployment Package Manager* dialog box. You can now create a new package, edit a package, or delete a package as needed.

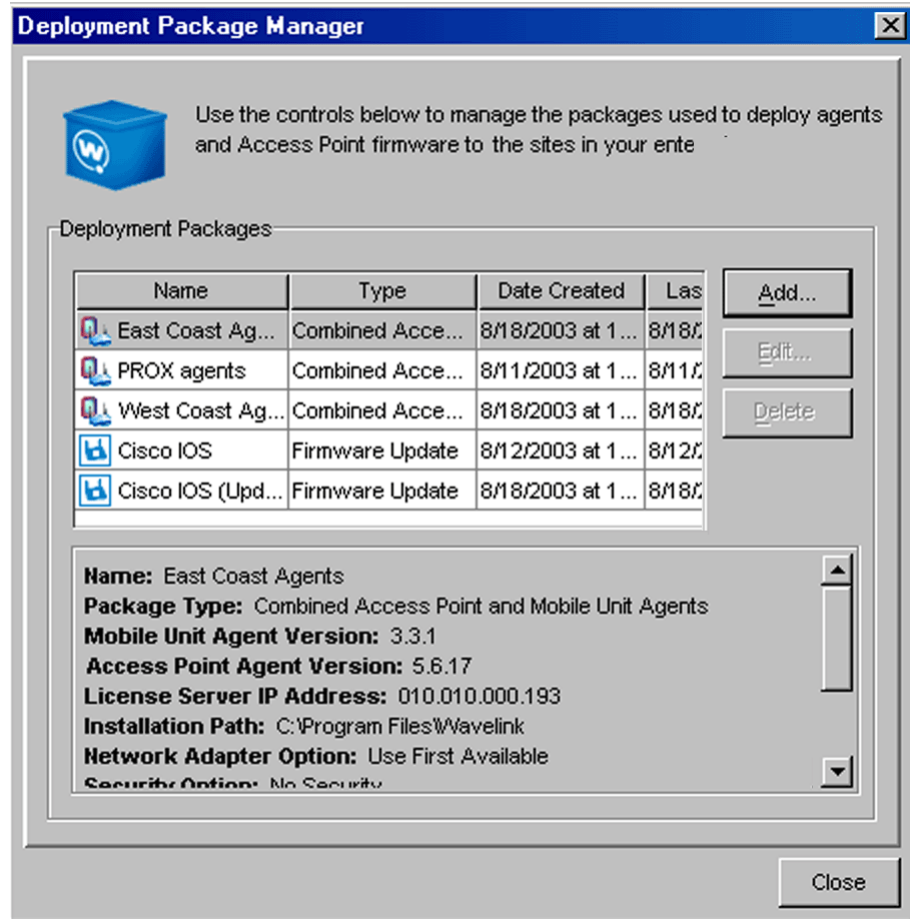
### **Deployment Packages for All Devices**

This section describes how to create a deployment package that will manage all devices—access points and mobile devices—at a specific location.

**To create a deployment package for all devices:**

- 1 Select Deployment Packages from the **Tools** menu.

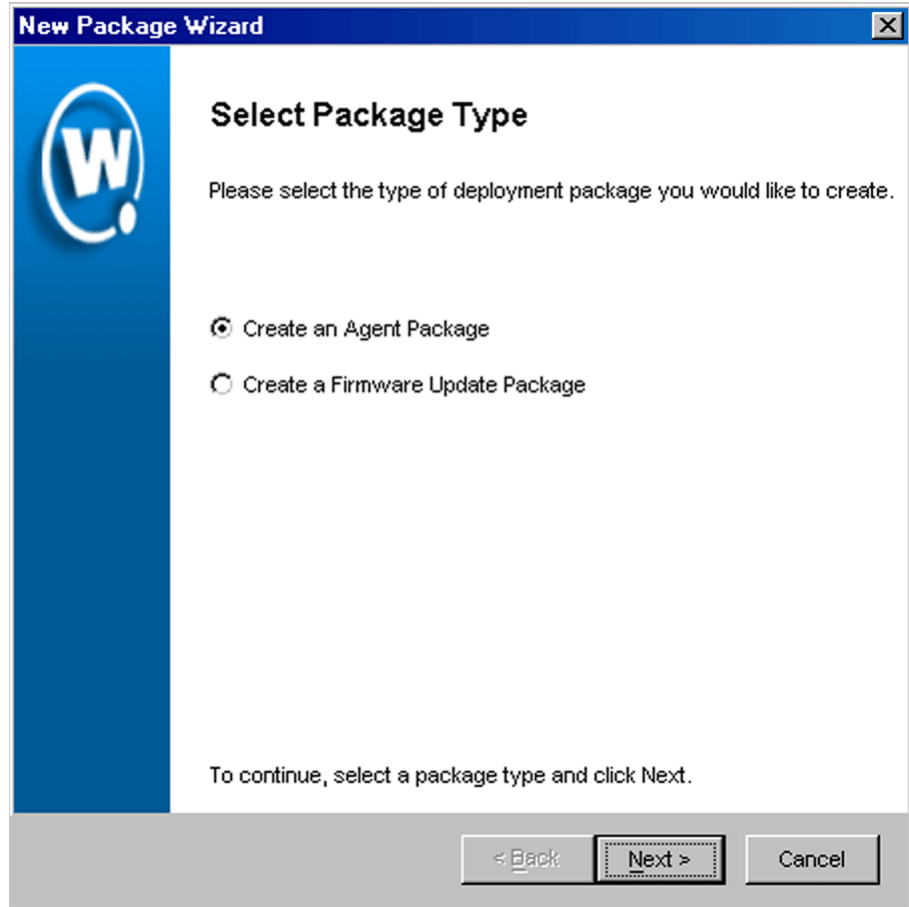
The *Deployment Package Manager* dialog box appears.



**Figure 4-17.** *The Deployment Package Manager Dialog Box*

- 2 Click Add.

The *Select Package Type* dialog box appears.



**Figure 4-18.** *The Select Package Type Dialog Box*

- 3 Select the **Create an Agent Package** option and click **Next**.

The *Select Agent Type* dialog box appears.

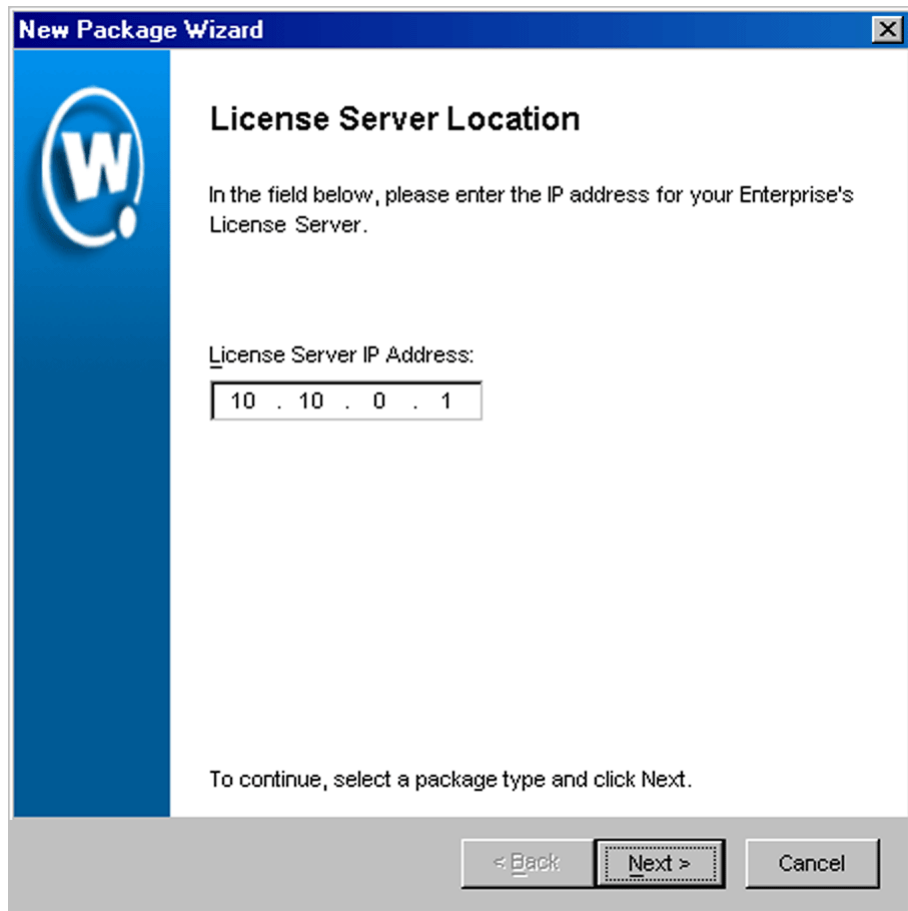




**Figure 4-19.** *The Select Agent Type Dialog Box*

- 4 Select the **Combined Access Point and Mobile Unit Agents** option and click **Next**.

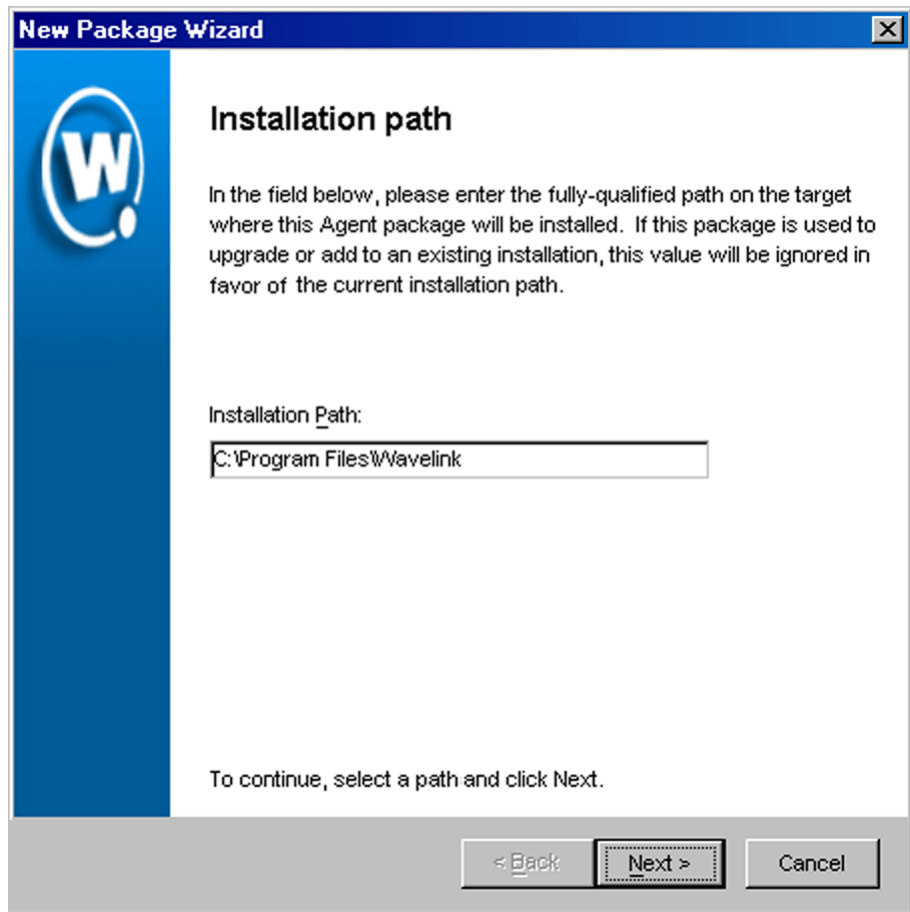
The *License Server Location* dialog box appears.



**Figure 4-20.** *The License Server Location Dialog Box*

- 5 Type the IP address of the license server for Mobile Manager and click Next. This IP address is typically the same as the location of Mobile Manager back-end components.

The *Installation Path* dialog box appears.



**Figure 4-21.** *The Installation Path Dialog Box*

- 6 Type the full path where the package is installed on any remote system in the *Installation Path* dialog box, for example, C:\Program Files\Wavelink, and click *Next*.

The *Select Access Point Agent Options* dialog box appears.



**Figure 4-22.** *The Select Access Point Agent Options Dialog Box*

**7** Determine how the access point Agent selects a network adapter.

If you want the Agent to select the first available network adapter, select the **First Available** option.

If you want the Agent to select an adapter based on a specific subnet, select the **Select by Subnet** option and then type the subnet address in the text box.

**8** Determine the security options for the Agent.

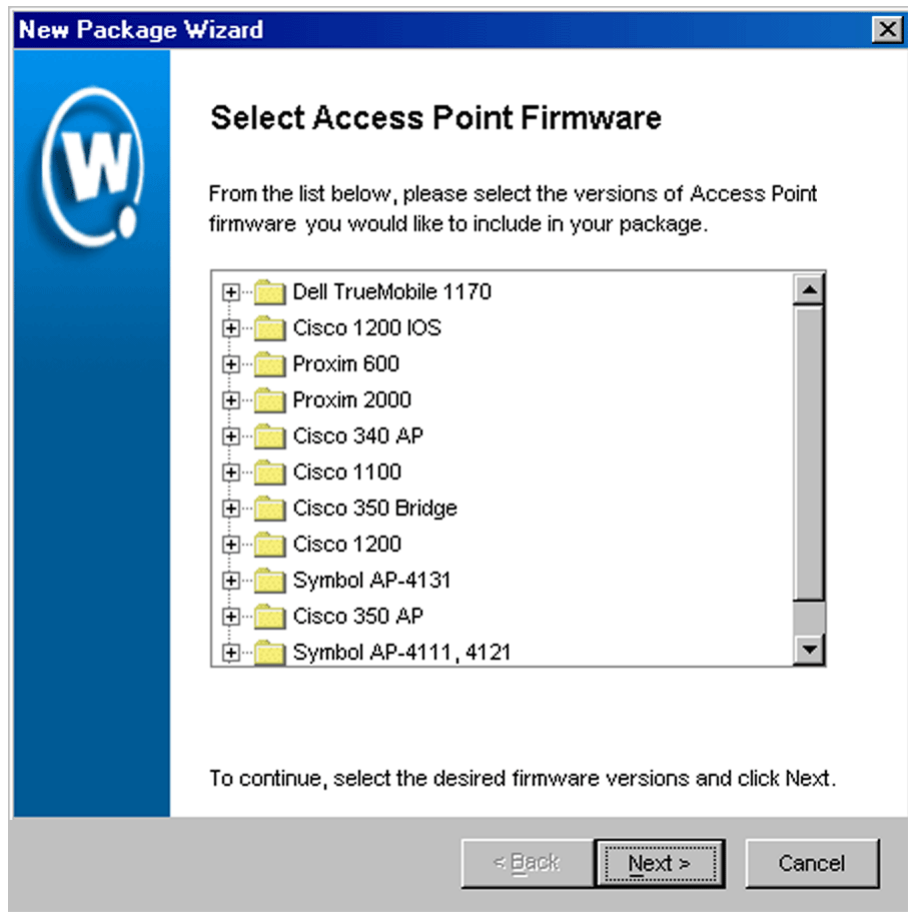
If you want the Agent to operate without any security measures, select the **No Security** option.

If you want the Agent to require a user name and password, select the **Security without Encryption** option.

If you want the Agent to require a user name and password and encrypt communications between management consoles and the Agent, select the **Security with Encryption** option.

**9** Click `Next`.

The *Select Access Point Firmware* dialog box appears. This dialog box contains a collection of folders, with each folder representing a specific type of access point.



**Figure 4-23.** *The Select Access Point Firmware Dialog Box*

**10** Select the firmware versions this Agent will support.

To select firmware, open the appropriate folder within the dialog box. A list of available firmware versions appears. Select a firmware version by enabling the checkbox next to the firmware name. You can select as many firmware versions, from as many folders, as needed.

**11** Click Next.

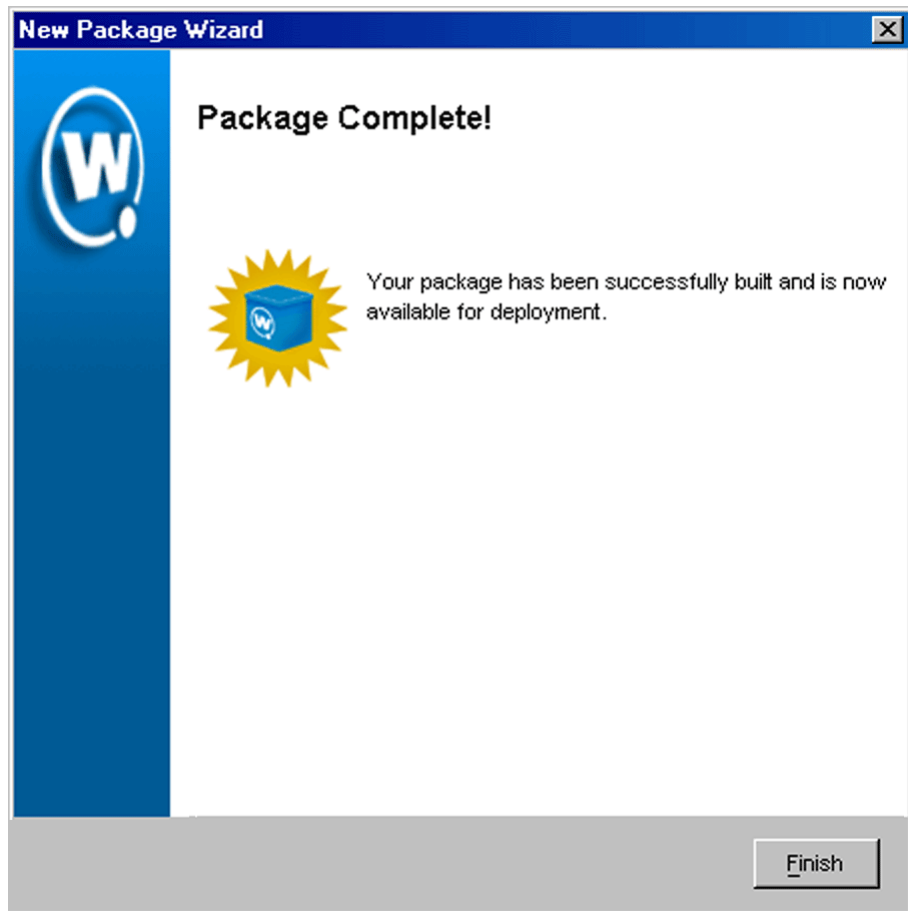
The *Enter Package Name* dialog box appears.



**Figure 4-24.** *The Enter Package Name Dialog Box*

- 12 Type a name for the package in the **Package Name** text box and click **Next**.

Mobile Manager begins to create the deployment package. When it is finished, a *Package Complete* dialog box appears.



**Figure 4-25.** *The Package Complete Dialog Box*

**13** Click *Finish*.

Mobile Manager returns you to the *Deployment Package Manager* dialog box. You can now create a new package, edit a package, or delete a package as needed.

**Adding Sites to the Enterprise Management Console**

Before you can send a deployment package to a site, you must add that site to the Enterprise Management Console. This process involves naming the site and identifying its IP address and location.



**To add a site to the Enterprise Management Console:**

- 1 From the **File** menu, select **New** and then select **Site**.

The *Enter Site Name* dialog box appears.



**Figure 4-26.** *The Enter Site Name Dialog Box*

- 2 Type the name of the site in the **Site Name** text box and click **Next**.

The *Enter Hostname or IP Address* dialog box appears.



**Figure 4-27.** *The Enter Hostname or IP Address Dialog Box*

- 3 Type the host name or the IP address of the system which contains (or will contain) an Agent in the **Site Hostname or IP address** text box and click Next.

The *Enter Site City Name* dialog box appears.



The screenshot shows a dialog box titled "New Package Wizard" with a blue header bar. On the left side, there is a blue vertical bar containing a white circular logo with a stylized "W" and a speech bubble. The main content area is white and contains the following text:

### Enter Site City Name

In the field below, please enter the name of the city in which this site will be located. Please enter the city name only. By clicking next, you will initiate a search of our database for this city and will be asked to choose the correct one from the results.

Site City Name:

Check here to bypass this search

To continue, enter the appropriate information and click Next.

At the bottom right, there are three buttons: "< Back" (disabled), "Next >" (active, highlighted with a dashed border), and "Cancel" (disabled).

**Figure 4-28.** *The Enter Site City Name Dialog Box*

- 4 Type the name of the city where the site resides in the **Site City Name** text box.

Mobile Manager will search its database to find all cities that have the name you specified. If you do not want Mobile Manager to search its database, enable the **Check here to bypass this search** checkbox.

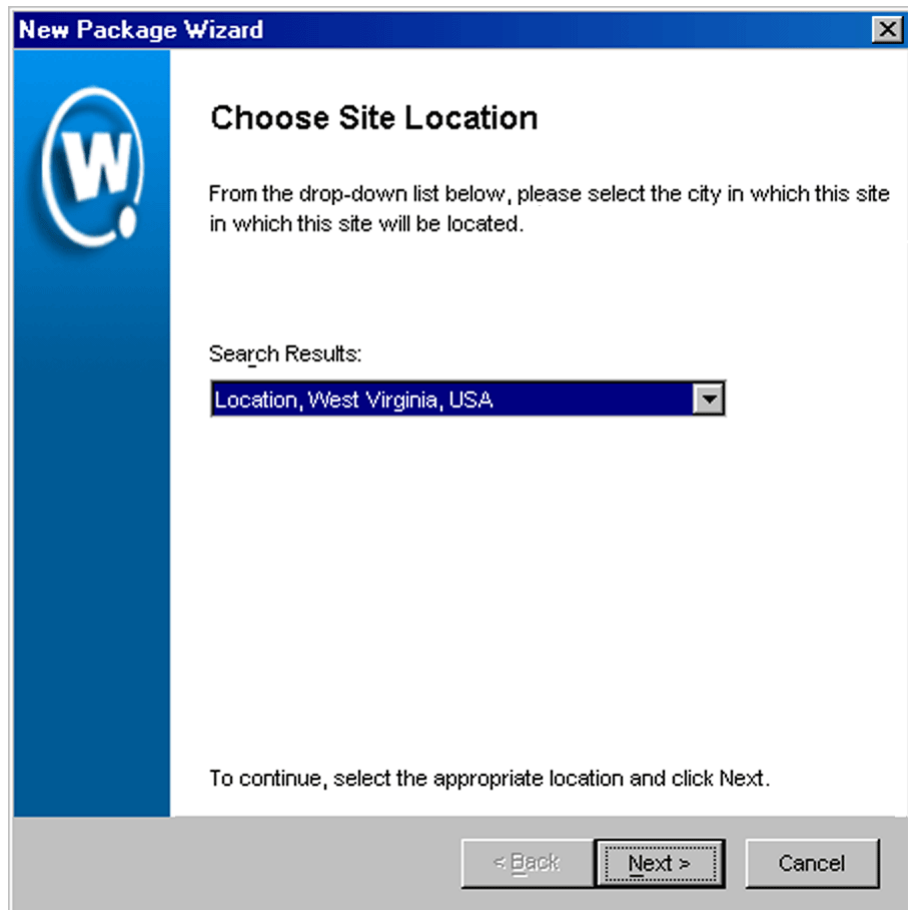
---

**NOTE** Mobile Manager connects to a database at the Wavelink Corporation Web site. If you are using an HTTP proxy for external Web site connections, see *Configuring an HTTP Proxy* on page 138 to enable the city search feature.

---

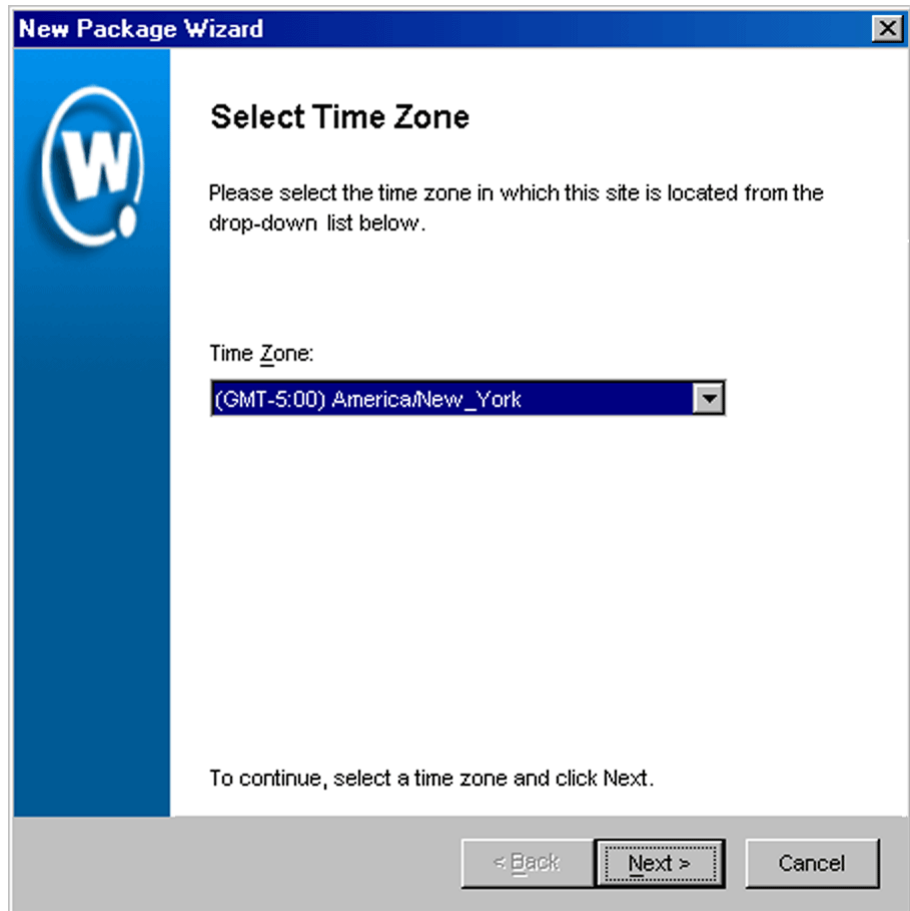
- 5 Click **Next**.

The *Choose Site Location* dialog box appears.



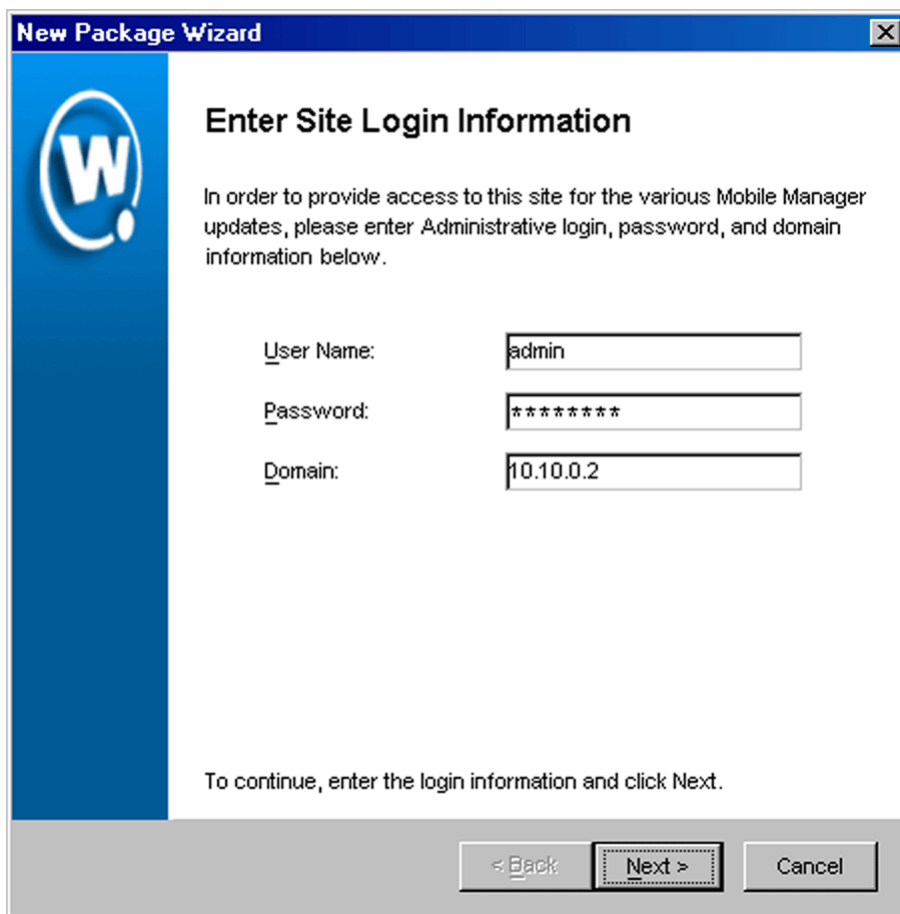
**Figure 4-29.** *The Choose Site Location Dialog Box*

- 6 Select the appropriate city from the **Search Results** list and click **Next**.  
The *Select Time Zone* dialog box appears.



**Figure 4-30.** *The Select Time Zone Dialog Box*

- 7 Select the time zone for the city and click **Next**.  
The **Enter Site Login Information** dialog box appears.



The screenshot shows a Windows-style dialog box titled "New Package Wizard" with a close button in the top right corner. On the left side, there is a blue vertical bar containing a white circular logo with a stylized "W". The main area of the dialog has the title "Enter Site Login Information" and a paragraph of text: "In order to provide access to this site for the various Mobile Manager updates, please enter Administrative login, password, and domain information below." Below this text are three input fields: "User Name:" with the value "admin", "Password:" with "\*\*\*\*\*", and "Domain:" with "10.10.0.2". At the bottom of the dialog, there is a grey bar containing three buttons: "< Back", "Next >" (which is highlighted with a dashed border), and "Cancel".

**Figure 4-31.** *The Enter Site Login Information Dialog Box*

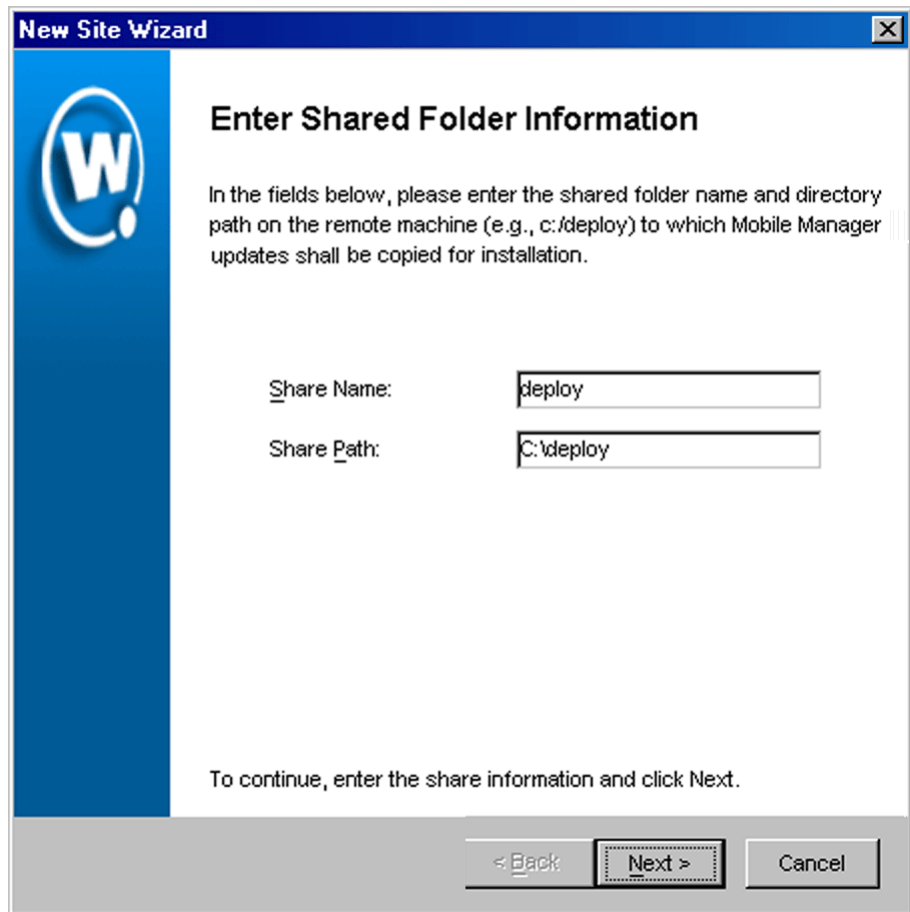
- 8 Type the user name and password for the system on which the Agent resides (or will reside) and click **Next**.

---

**NOTE** This user name and password must have administrative access to the system.

---

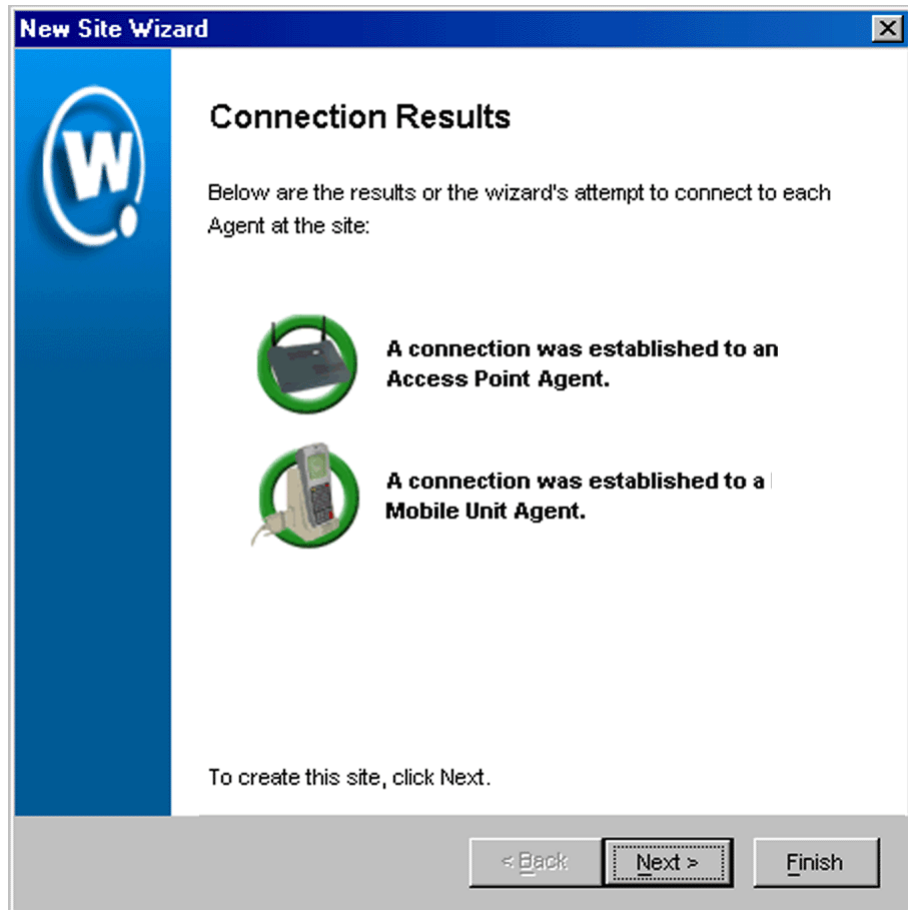
The *Enter Shared Folder Information* dialog box appears.



**Figure 4-32.** *The Enter Shared Folder Information Dialog Box*

- 9 Type the name of the shared folder where Mobile Manager updates are installed in the **Share Name** text box.
- 10 Type the directory path where Mobile Manager updates are installed on this remote system in the **Share Path** text box. This path is not the network path (such as `\\system1\deploy\`), but is the local path to the shared folder (such as `c:\deploy\`).
- 11 Click **Next**.

Mobile Manager attempts to contact the site to verify that all the information is correct. After a few moments, the *Connection Results* dialog box appears.



**Figure 4-33.** *The Connection Results Dialog Box*

**12** Click **Next**.

The *Site Created* dialog box appears.





**Figure 4-34.** *The Site Created Dialog Box*

**13** Click *Finish*.

The site now appears in the Unassigned Sites group within the Groups window of the Enterprise Management Console. You can now deploy Agents to the site, or modify the site as needed.

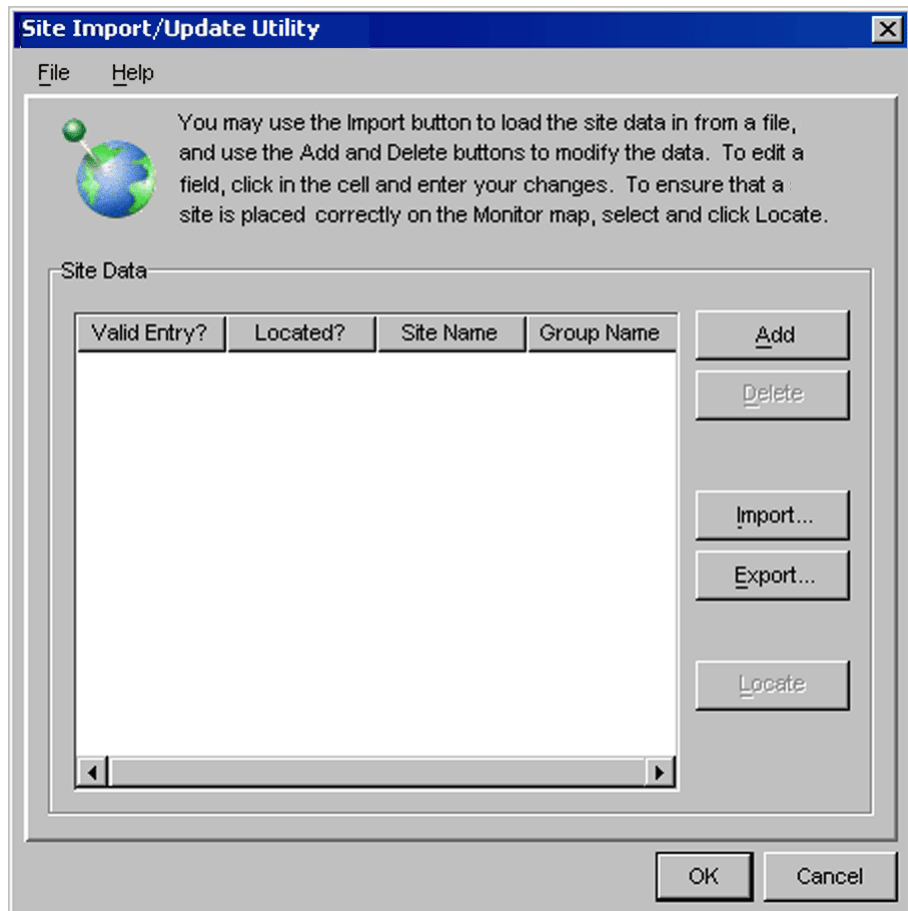
**Adding Sites through the Site Import/Update Utility**

You can also add sites through the Site Import/Update Utility.

**To add a site using the Site Import/Update Utility:**

- 1 From the **File** menu, select Import/Update Site Data.

The *Site Import/Update Utility* dialog box appears.



**Figure 4-35.** *The Site Import/Update Utility Dialog Box*

- 2 Click Add.

A new entry appears in the **Site Data** list.

- 3 For each field in the entry, type the appropriate information for the site.

Mobile Manager Enterprise attempts to verify that the site is being added correctly. When it detects that the site has enough correct information, a green checkmark appears in the **Valid Entry?** column.

### **Deploying Sites**

After you create one or more deployment packages and add one or more sites to the Enterprise Management Console, you can deploy a site using the Enterprise Management Console. Deploying a site is defined as sending a deployment package to a specific location within your network.

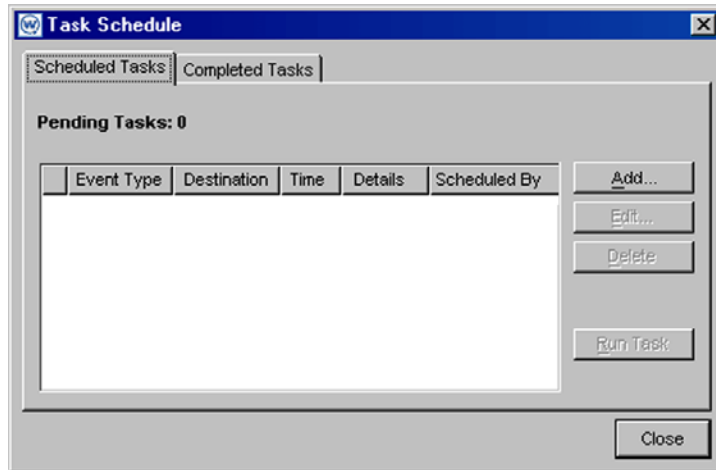
You send a deployment package to a location by scheduling an event within the Enterprise Management Console. An event is an action during which Mobile Manager sends information to or receives information from a given location.

This section describes how to send a deployment package to a location on your network, resulting in the creation of a new site that you can manage with the Enterprise Management Console.

#### **To deploy a site:**

- 1** If you have not already done so, create a deployment package as described in *Creating Deployment Packages* on page 75.
- 2** Select **Task Schedule** from the **Tools** menu.

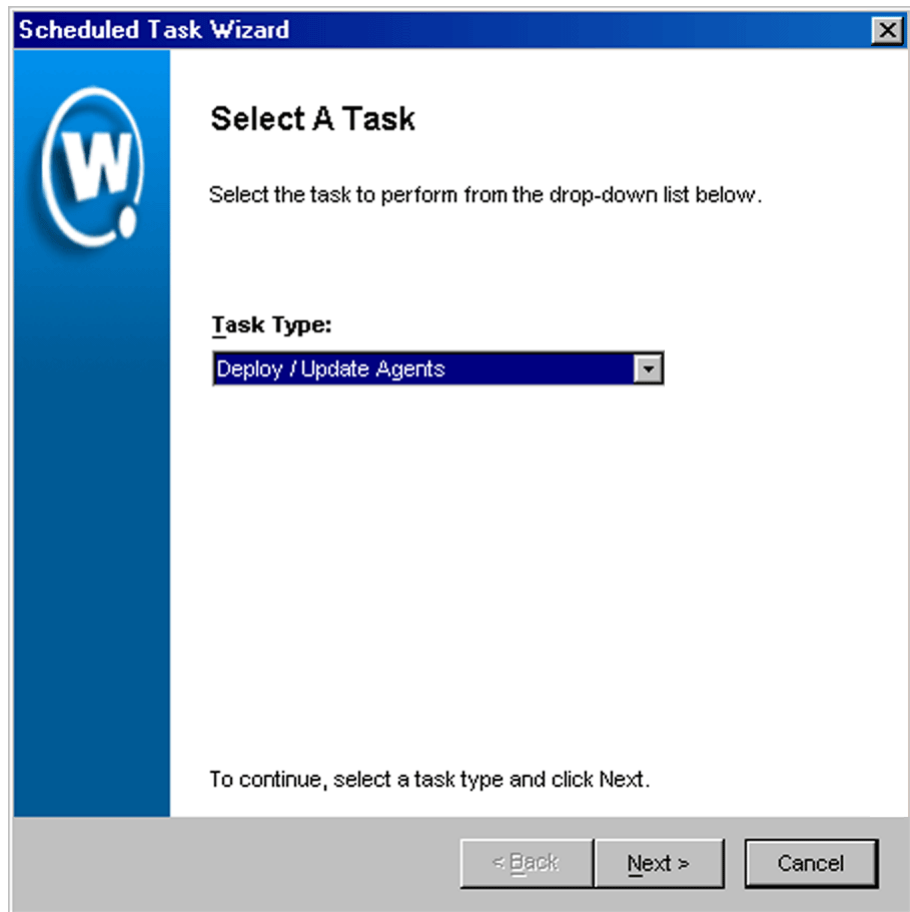
The *Task Schedule* dialog box appears.



**Figure 4-36.** *The Task Schedule Dialog Box*

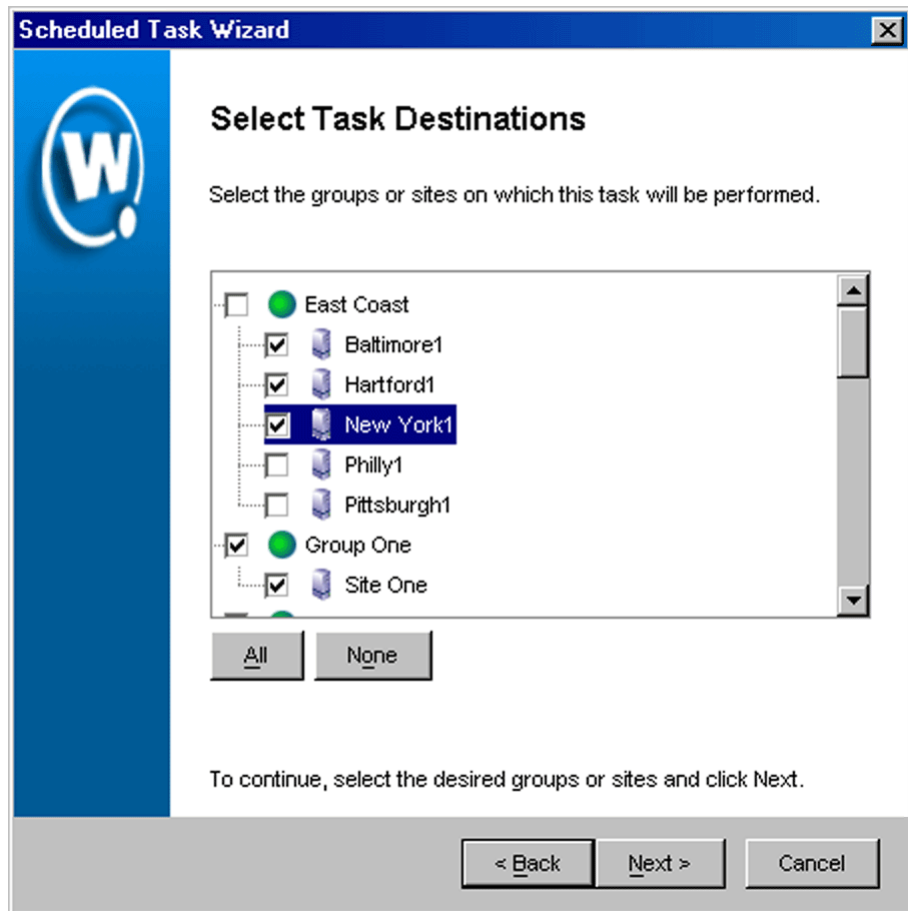
**3** Click Add.

The *Select A Task* dialog box appears.



**Figure 4-37.** *The Select A Task Dialog Box*

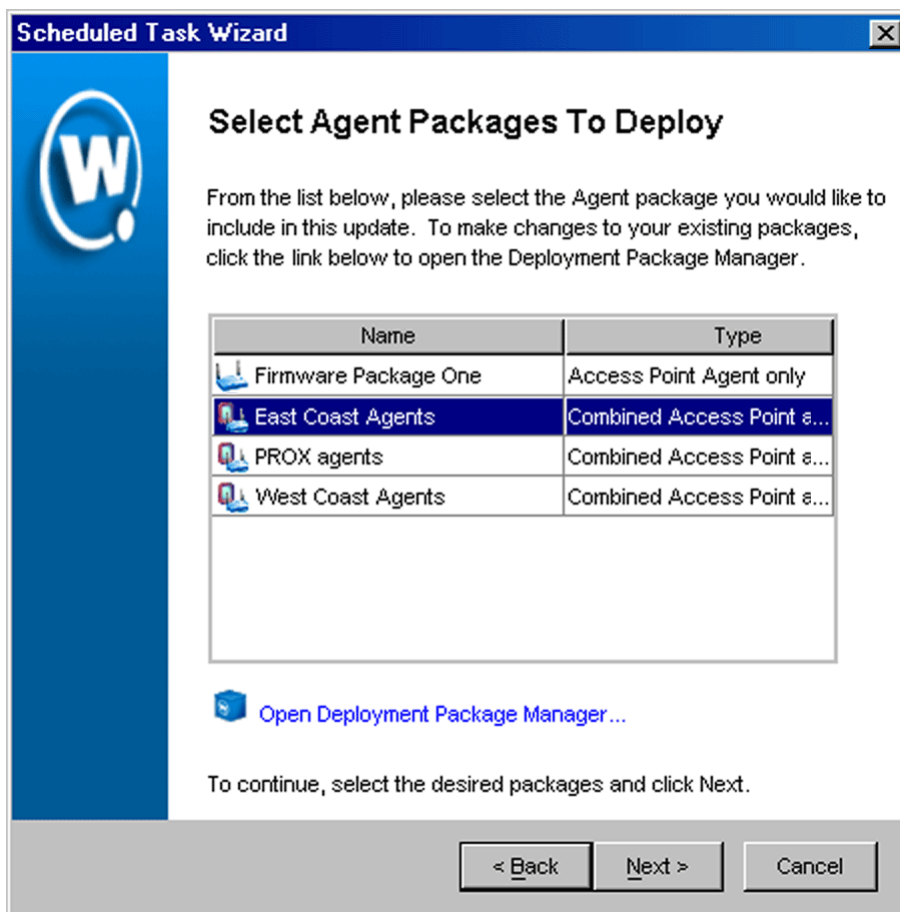
- 4 Select Deploy/Update Agents from the **Task Type** list and click Next.  
The *Select Task Destination* dialog box appears.



**Figure 4-38.** *The Select Task Destination Dialog Box*

- 5 Select the groups or sites by enabling the checkbox next to the group or site name. You can also select all groups by clicking All.
- 6 Click Next.

The *Select Agent Packages to Deploy* dialog box appears.

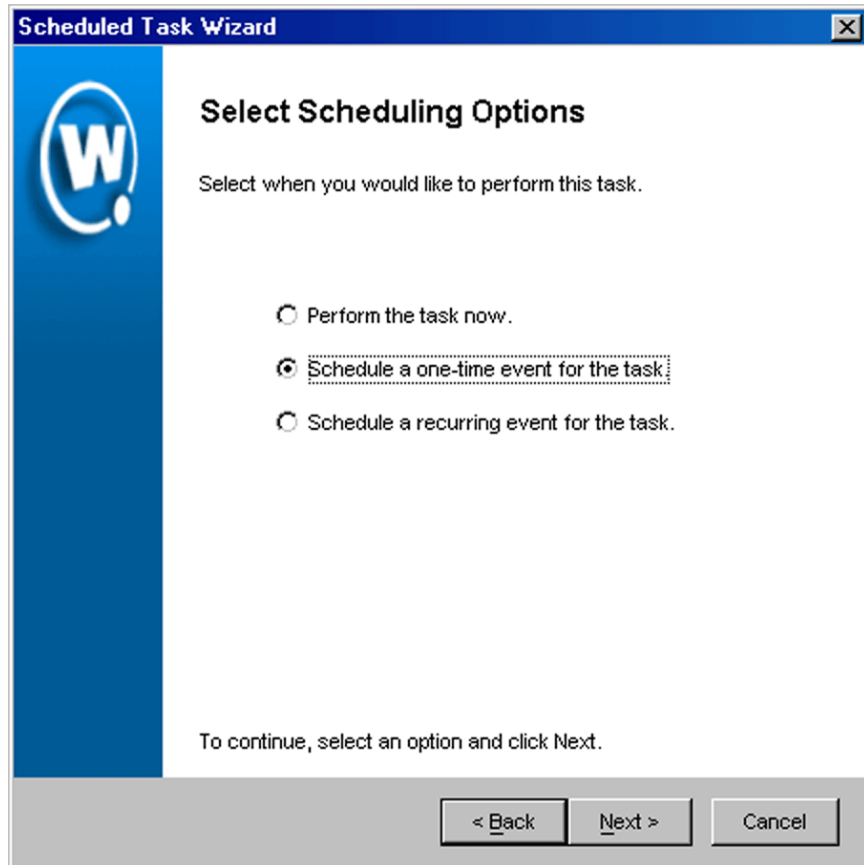


**Figure 4-39.** The Select Agent Packages to Deploy Dialog Box

7 Select an Agent package and click Next.

**NOTE** If you have not created a deployment package, you can do so at this time by clicking the **Open Deployment Package Manager** link at the bottom of the dialog box. See *Creating Deployment Packages* on page 75 for more information on creating deployment packages.

The *Select Scheduling Options* dialog box appears.



**Figure 4-40.** *The Select Scheduling Options Dialog Box*

**8** Determine when the event will occur.

If you want the event to occur immediately, select the **Perform the task now** option.

If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

---

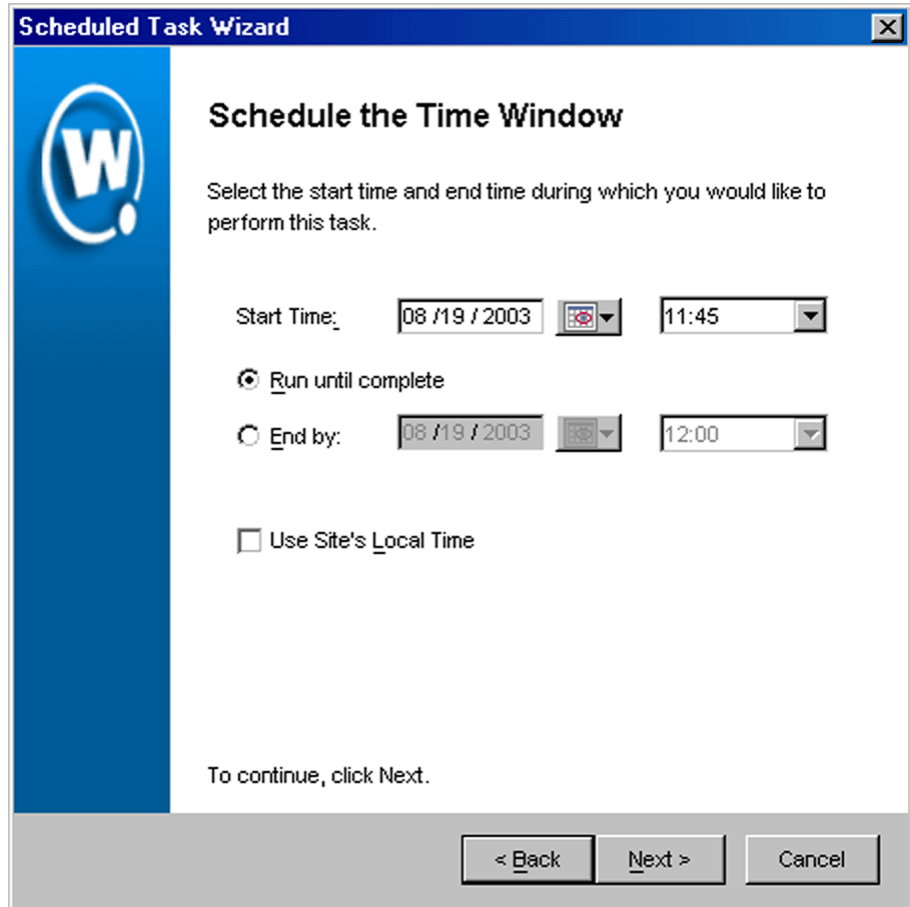
**NOTE** For scheduling deployment packages, it is not recommended that you select the **Schedule a recurring event for the task** option.

---



9 Click **Next**.

If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.



The image shows a screenshot of the 'Scheduled Task Wizard' dialog box, specifically the 'Schedule the Time Window' step. The dialog has a blue header with the title 'Scheduled Task Wizard' and a close button. On the left side, there is a blue vertical bar with a white circle containing a 'W' logo. The main content area has the title 'Schedule the Time Window' and the instruction 'Select the start time and end time during which you would like to perform this task.' Below this, there are two rows of time selection controls. The first row is for the 'Start Time', with a date field set to '08 /19 /2003', a dropdown arrow, and a time field set to '11:45'. The second row is for the 'End by' time, with a date field set to '08 /19 /2003', a dropdown arrow, and a time field set to '12:00'. There are two radio buttons: 'Run until complete' (which is selected) and 'End by:'. Below these is a checkbox labeled 'Use Site's Local Time' which is unchecked. At the bottom of the dialog, there is a grey bar containing three buttons: '< Back', 'Next >', and 'Cancel'. The text 'To continue, click Next.' is located above the 'Next >' button.

**Figure 4-41.** *The Schedule the Time Window Dialog Box*

10 Select the start date and time for the event.

11 Determine when you want the event to end.

If you want the event to end only after the deployment is complete, select the **Run until complete** option.

If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

---

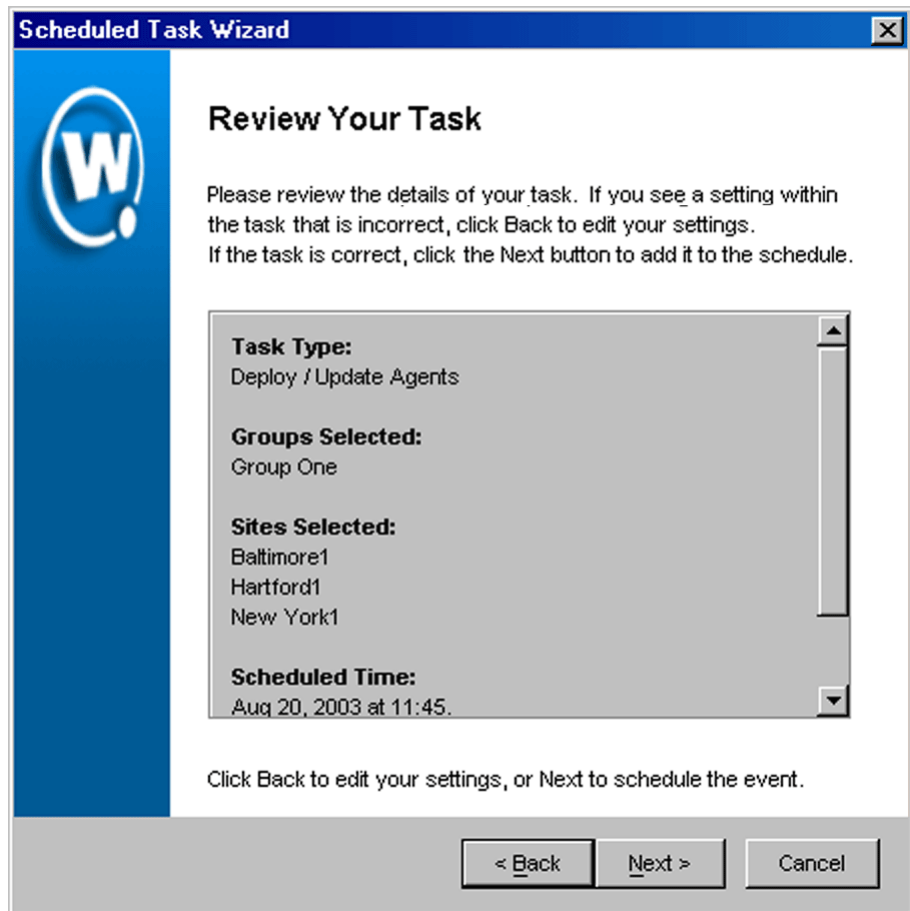
**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

**12** If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

**13** Click **Next**.

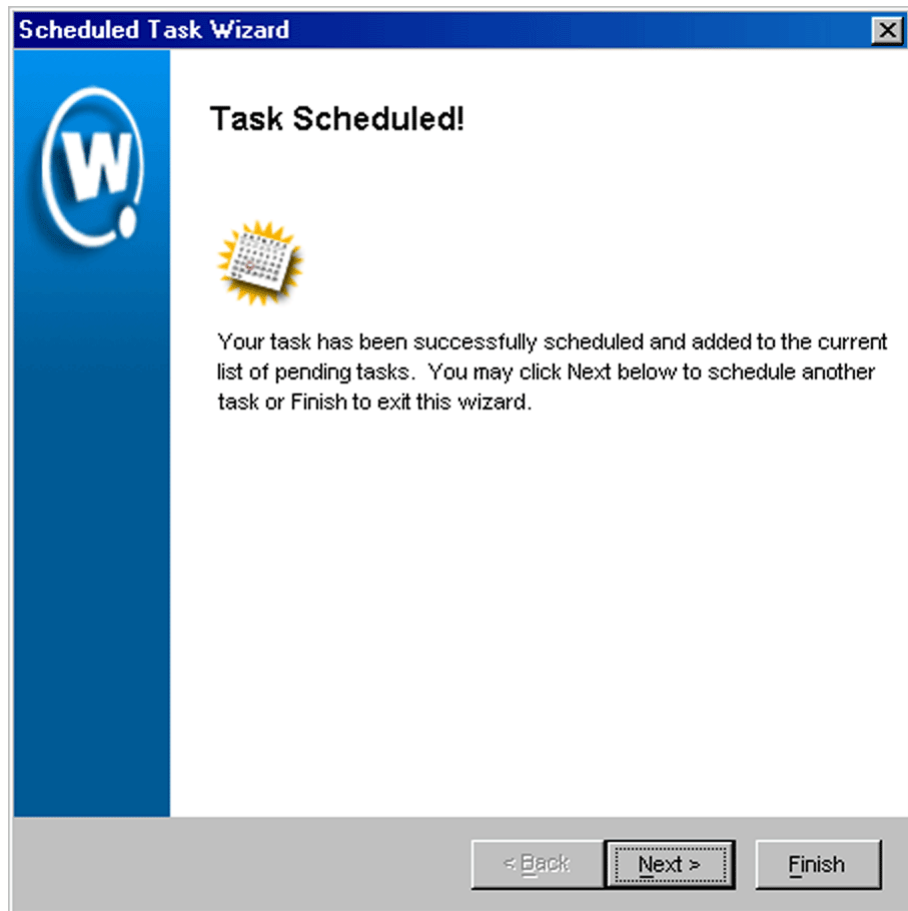
The *Review Your Task* dialog box appears.



**Figure 4-42.** *The Review Your Task Dialog Box*

**14** Review your the task to ensure that it is correct and click Next.

The *Task Scheduled* dialog box appears.



**Figure 4-43.** *The Task Scheduled Dialog Box*

- 15 Click **Next** to schedule a new event, or click **Finish** to return to the *Task Schedule* dialog box.

## Importing Sites

In situations where you want to create a large number of sites simultaneously, you can create a list of sites and import the list into the Enterprise Management Console. You can then send the appropriate deployment packages to these sites.

A list of sites can be any comma-separated value (CSV) file. Each line within the file contains the information needed for Mobile Manager to recognize the site. The information each line must contain is as follows:

<b>Site Name</b>	The name of the site.
<b>Group Name</b>	The group in the Enterprise Management Console that will contain the site.
<b>Site Address</b>	The IP address of the site.
<b>City</b>	The city where the site is located.
<b>State/Region</b>	The state or region where the site is located.
<b>Country</b>	The country where the site is located.

---

**NOTE** Country is defined by using a specific country code.

---

<b>Time Zone</b>	The time zone where the site is located.
<b>User Name</b>	The user name of an administrative account for the system where the Agent resides at the site.
<b>Password</b>	The password of an administrative account for the system where the Agent resides at the site.
<b>Domain</b>	The domain for the site.
<b>Share Name</b>	The name of the shared folder where Mobile Manager updates are installed.
<b>Shared Path</b>	The local path for the remote system where Mobile Manager updates are installed.

If information for a site is unavailable—for example, if the site does not yet have a group name—you do not have to include it in your list of sites. However, you must still include a comma where the information would be for each line. The following is an example of how to omit the group name:

```
Store1,,10.0.0.27,Seattle,<rest of line entries>
```

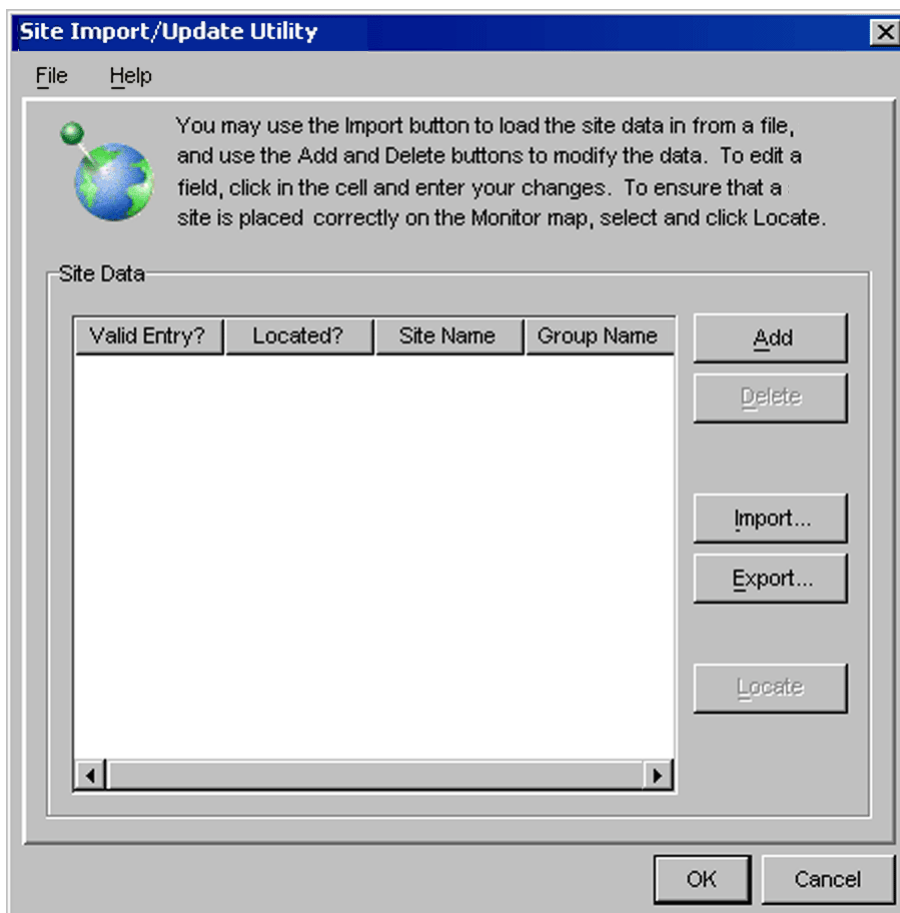
The “extra” comma after Store1 indicates where the group name would normally reside. Without this comma, the Enterprise Management Console will not read the site list file correctly.

After you create a list of sites, you can import that list into the Enterprise Management Console.

**To import a list of sites:**

- 1 Select `Import Site Data` from the **File** menu.

The *Site Import Utility* dialog box appears.



**Figure 4-44.** *The Site Import Utility Dialog Box*

- 2 Within this dialog box, click the **File** menu, then select `Import`, followed by `From Site Data`.

An *Open* dialog box appears, allowing you to navigate to the file containing your site data.

- 3 Navigate to the file and click *Open*.

Mobile Manager imports the list of sites into the *Site Import Utility* dialog box. This dialog box contains several columns, listing the same information contained in the CSV file of the sites. In addition, there are two additional columns. The first column, **Valid Entry?**, shows if the criteria defining the site is valid. The second column, **Located?**, shows if Mobile Manager was able to locate the site.

You can edit any entry in this utility by clicking in the column that contains the data you want to change.

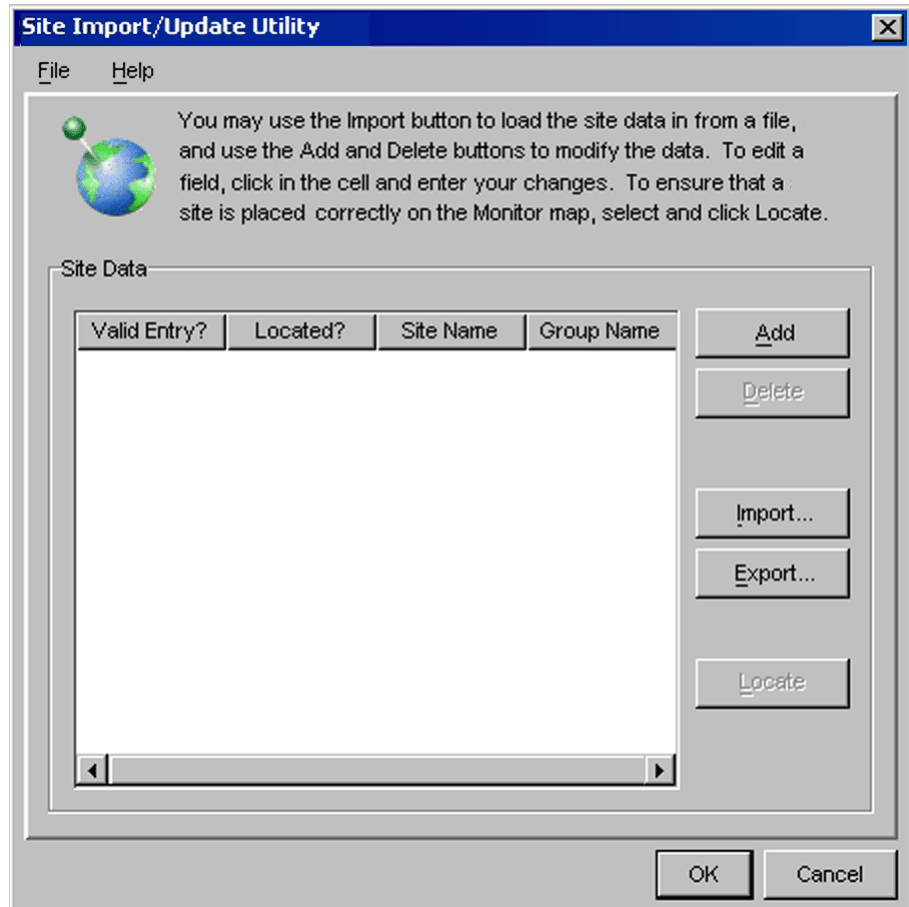
### **Importing Existing Site Data**

You can also import existing site data into the *Site Import/Update Utility* dialog box. This feature allows you to collect existing site data and either update information from within the *Site Import/Update Utility* dialog box, or by exporting the data into a text file for editing.

#### **To import existing site data:**

- 1 From the **File** menu, select *Import/Update Site Data*.

The *Site Import/Update* dialog box appears.



**Figure 4-45.** *The Site Import/Update Utility Dialog Box*

- 2 Within this dialog box, click the **File** menu, then select **Import**, followed by **From Site Data**.

The *Site Import/Update* dialog box updates with entries based on your existing sites.

### **Exporting Site Data**

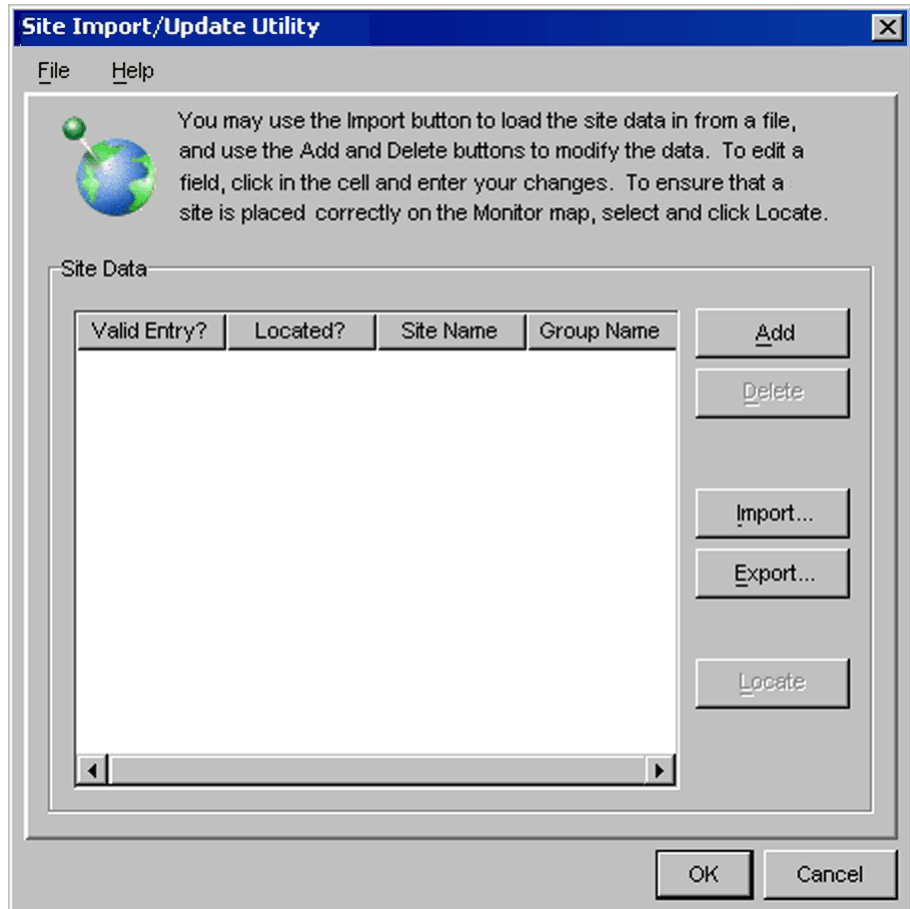
You can export site data to a text file. Using this file, you can then use a separate application, such as a spreadsheet, to modify the contents of the file and then re-import the data back into Mobile Manager Enterprise.



**To export site data:**

- 1 From the **File** menu, select `Import/Update Site Data`.

The *Site Import/Update* dialog box appears.



**Figure 4-46.** *The Site Import/Update Utility Dialog Box*

- 2 Within this dialog box, click the **File** menu, then select `Export`.

A *Save* dialog box appears, allowing you to set the name and destination of the new file.

- 3 Select a location for the file, name it, and click **Save**.

### **Locating Sites**

By default, sites that you import into the *Site Import Utility* dialog box are not verified by Mobile Manager. If you want Mobile Manager to verify a site, you can do so by using the **Locate** button.

#### **To locate a site:**

- 1 Select one or more sites from the **Site Data** list in the *Site Import Utility* dialog box.
- 2 Click **Locate**.

Mobile Manager attempts to locate the site. If the attempt is successful, a green checkmark will appear in the **Located?** column for the site entry. If the attempt does not succeed, an alert dialog box appears, explaining why the site could not be found.

---

**NOTE** Mobile Manager connects to a database at the Wavelink Corporation Web site to while trying to locate sites. If you are using an HTTP proxy for external Web site connections, see *Configuring an HTTP Proxy* on page 147 to enable the site location feature.

---

### **Modifying Sites**

You can modify a site at any time.

#### **To modify a site:**

- 1 Right-click the site and select **Properties** from the menu that appears.

A dialog box appears, displaying all of the relevant information about that site. This information includes configurable options, such as the site name, as well as version and licensing information for the Agents installed at the site.

**SPOK1**



---

City:

Region:

Country:

Time Zone:

IP / Hostname:

User Name:

Password:

Domain:

Share Name:

Share Path:

---

Access Point Agent Version: **Unknown**

 Licensed Access Points: **10**

Mobile Unit Agent Version: **Unknown**

 Licensed Mobile Units (Wavelink): **10**

 Licensed Mobile Units (Manufacturer): **10**

**Figure 4-47.** *The Site Information Dialog Box*

- 2 Edit the information as needed.
- 3 Click OK.

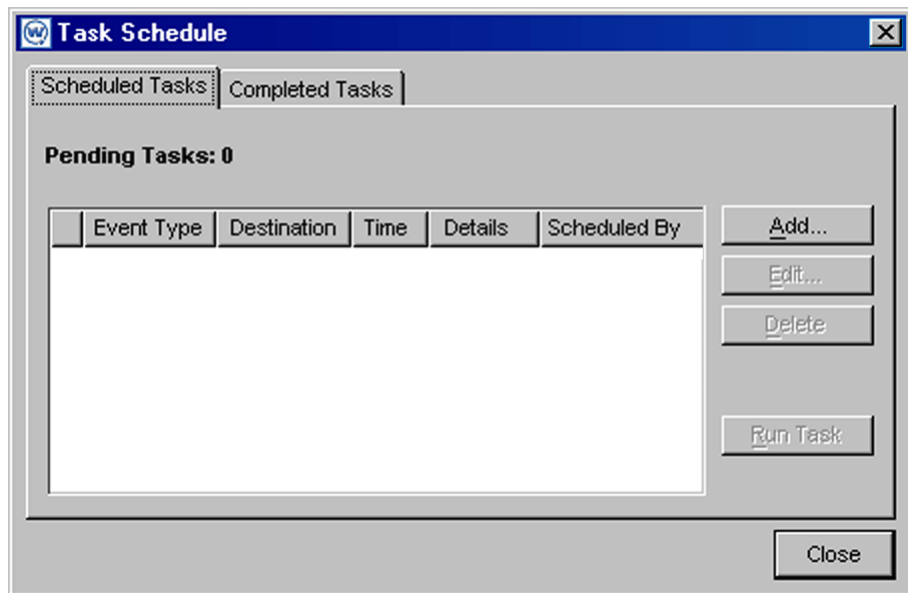
## Deleting Agents

You can remove an Agent from a site at any time.

### To delete an Agent:

- 1 Select **Task Schedule** from the **Tools** menu.

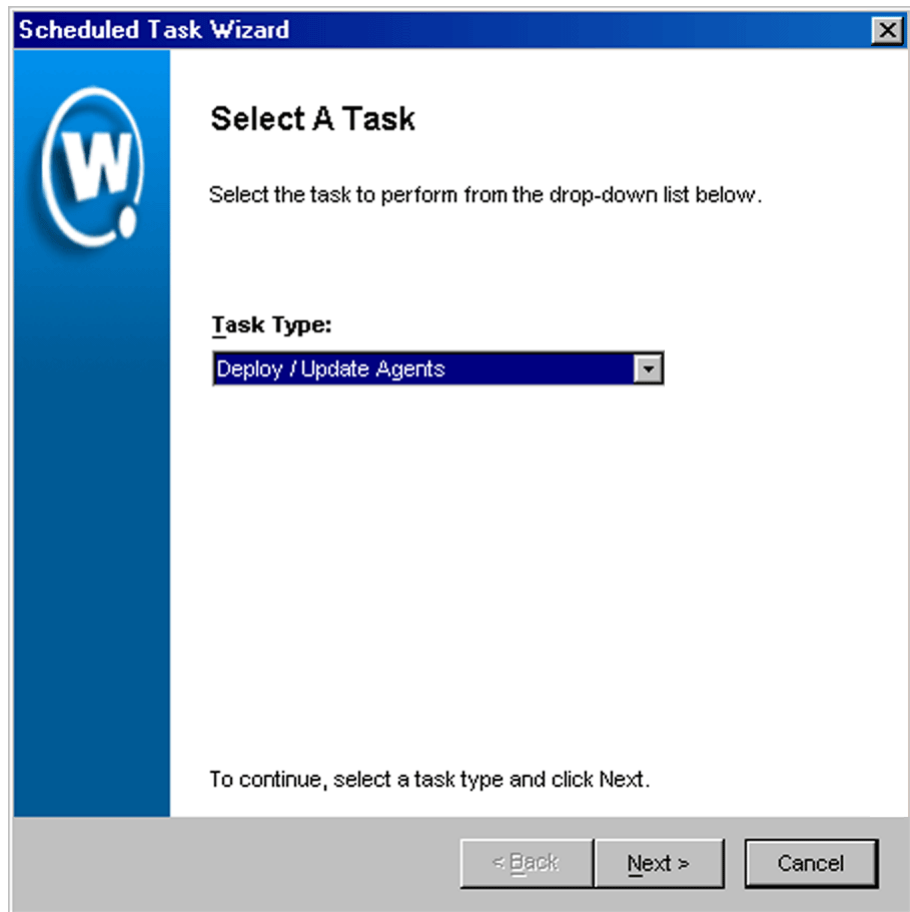
The *Task Schedule* dialog box appears.



**Figure 4-48.** *The Task Schedule Dialog Box*

- 2 Click **Add**.

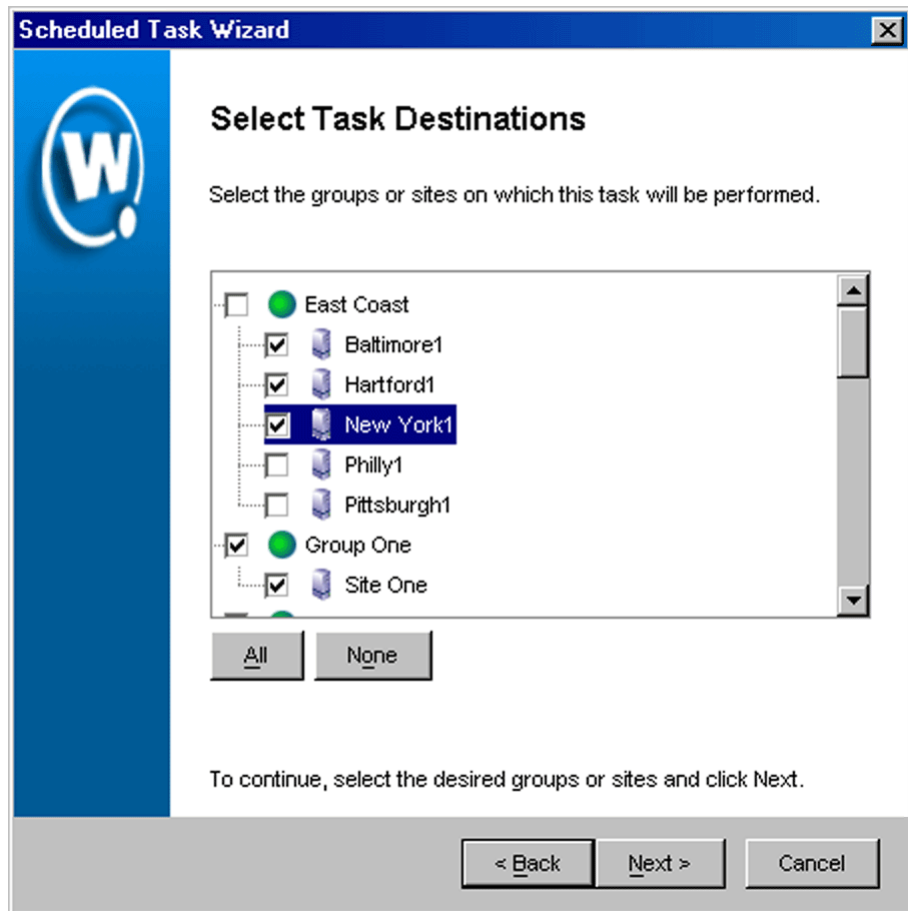
The *Select A Task* dialog box appears.



**Figure 4-49.** *The Select a Task Dialog Box*

- 3 Select `Uninstall Agents` from the **Task Type** list and click **Next**.

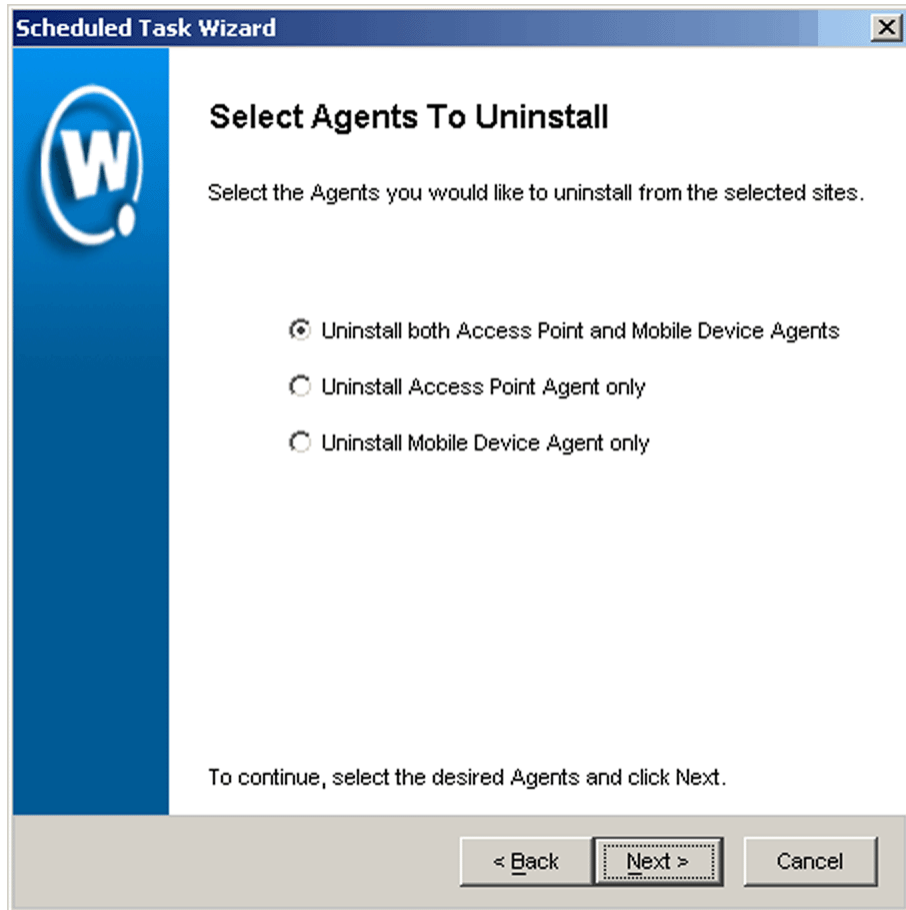
The *Select Task Destination* dialog box appears.



**Figure 4-50.** *The Select Task Destination Dialog Box*

- 4 Select the groups or sites by enabling the checkbox next to the group or site name. You can also select all groups by clicking **All**.

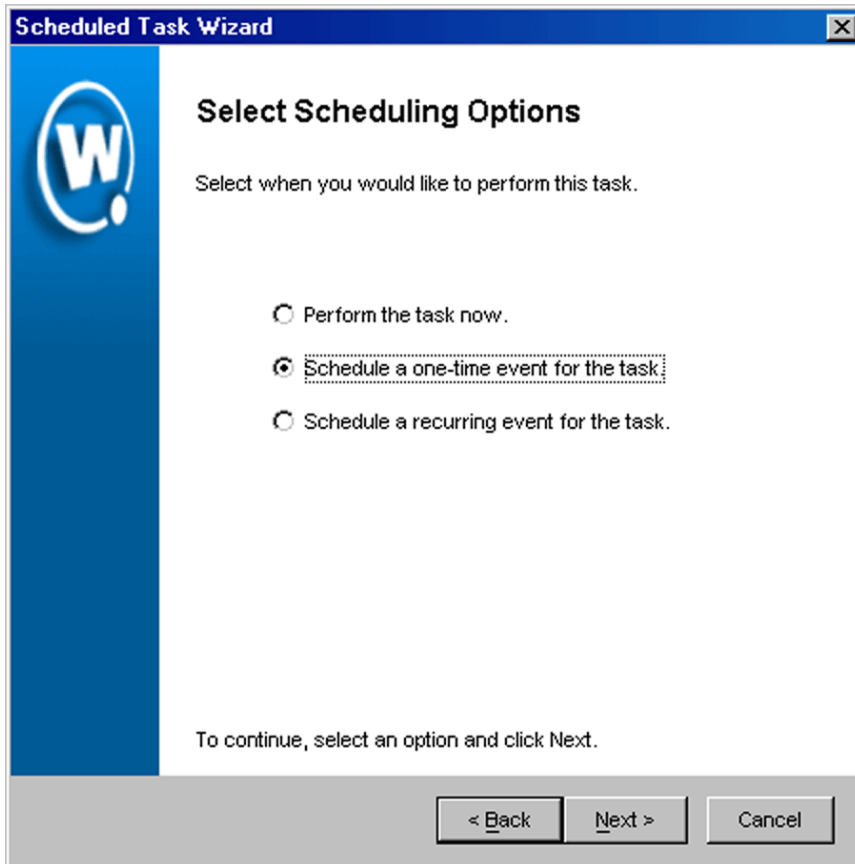
The *Select Agents to Uninstall* dialog box appears.



**Figure 4-51.** *The Select Agents to Uninstall Dialog Box*

- 5 Select whether to uninstall either the access point Agent, the mobile device Agent, or both.

The *Select Scheduling Options* dialog box appears.



**Figure 4-52.** *The Select Scheduling Options Dialog Box*

**6** Determine when the event will occur.

If you want the event to occur immediately, select the **Perform the task now** option.

If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

---

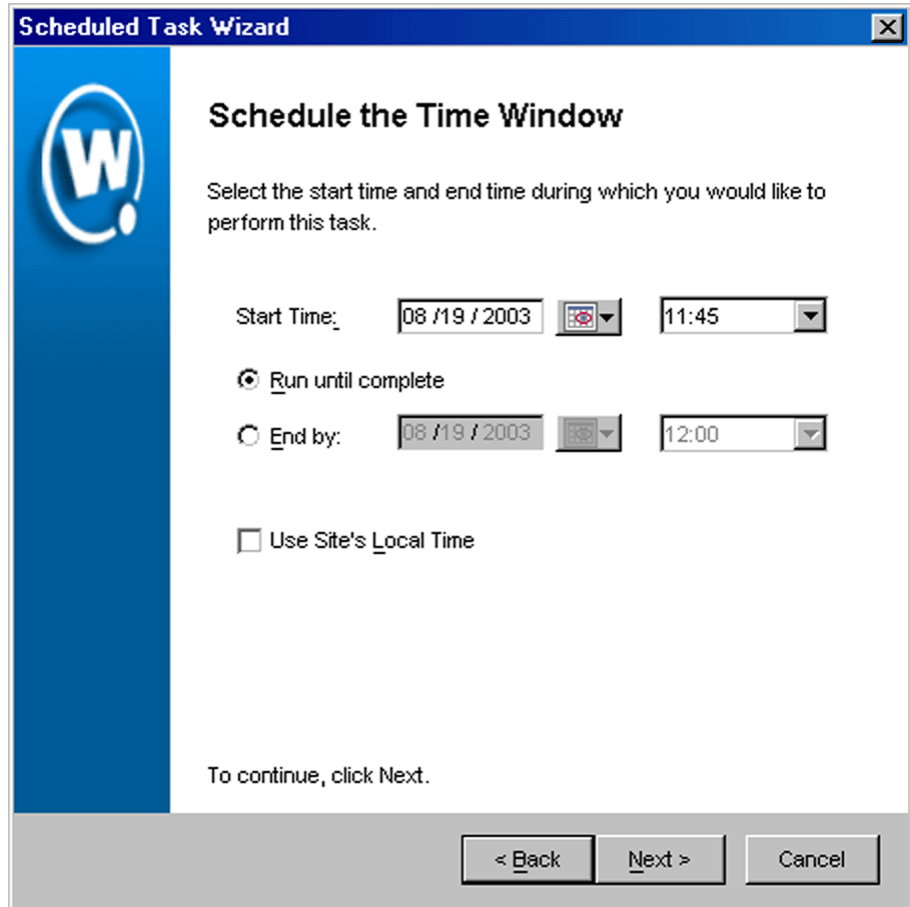
**NOTE** For scheduling deployment packages, it is not recommended that you select the **Schedule a recurring event for the task** option.

---



7 Click **Next**.

If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.



The image shows a screenshot of the 'Scheduled Task Wizard' dialog box, specifically the 'Schedule the Time Window' step. The dialog has a blue header with the title 'Scheduled Task Wizard' and a close button. On the left side, there is a blue vertical bar with a white 'W' logo. The main content area is white and contains the following elements:

- Schedule the Time Window** (Section Header)
- Select the start time and end time during which you would like to perform this task.
- Start Time:** A date field containing '08 /19 /2003', a dropdown arrow, and a time field containing '11:45' with a dropdown arrow.
- Run until complete**
- End by:** A date field containing '08 /19 /2003', a dropdown arrow, and a time field containing '12:00' with a dropdown arrow.
- Use Site's Local Time**
- To continue, click Next.
- Navigation buttons at the bottom: '< Back', 'Next >', and 'Cancel'.

**Figure 4-53.** *The Schedule the Time Window Dialog Box*

8 Select the start date and time for the event.

9 Determine when you want the event to end.

If you want the event to end only after the deployment is complete, select the **Run until complete** option.

If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

---

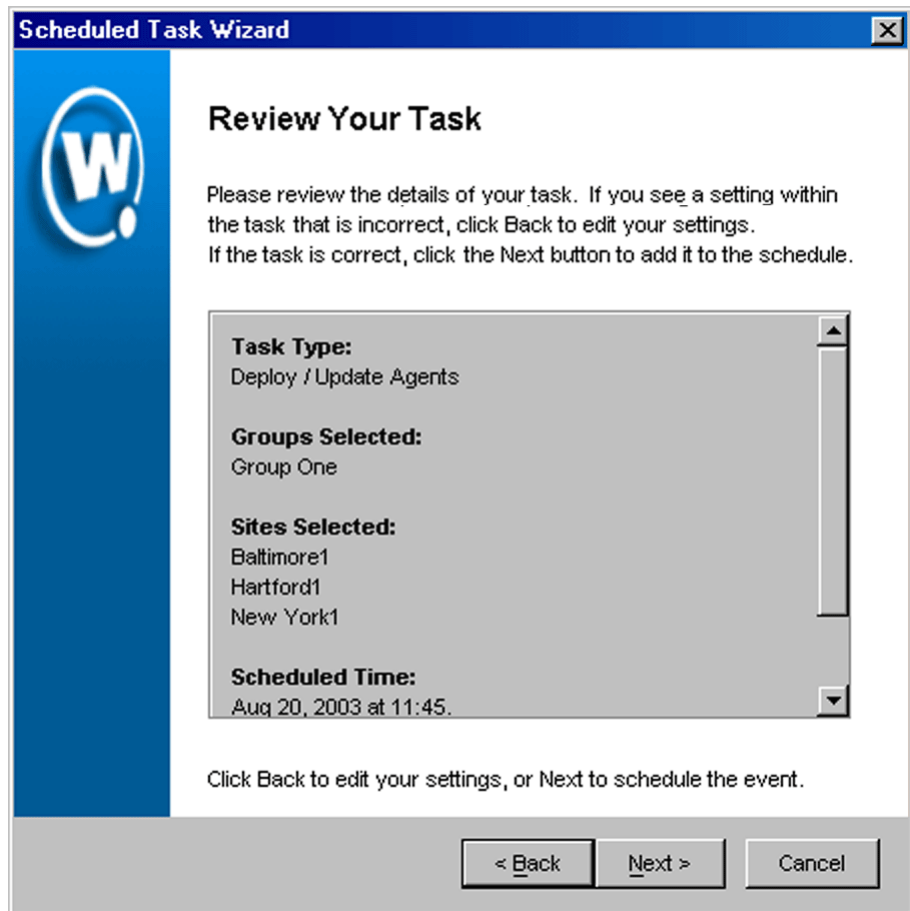
**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

**10** If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

**11** Click **Next**.

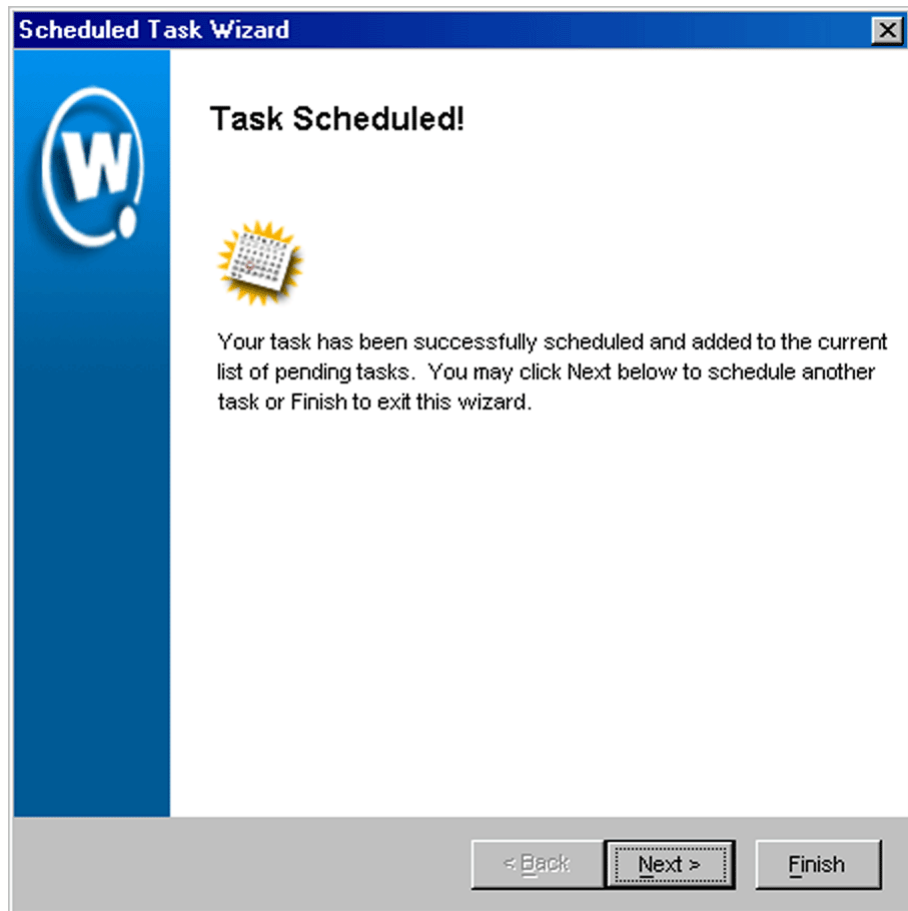
The *Review Your Task* dialog box appears.



**Figure 4-54.** *The Review Your Task Dialog Box*

**12** Review your the task to ensure that it is correct and click Next.

The *Task Scheduled* dialog box appears.



**Figure 4-55.** *The Package Complete Dialog Box*

- 13 Click **Next** to schedule a new event, or click **Finish** to return to the Task Schedule dialog box.

When this event occurs, Mobile Manager will remove the Agents from the site. You can then either install new Agents, or delete the site.

## **Deleting Sites**

If a site becomes unnecessary, you can delete it from the Enterprise Management Console.

To retain historical data, Mobile Manager does not immediately remove sites that you have decided to delete. Instead, these sites move to the Deleted Devices folder, and cease to receive any new configuration values from the Enterprise Management Console. You can then access historical data about the site at a later date.

---

**NOTE** If you want to completely remove the site, including any Agents installed, you must first uninstall the Agents from site.

---

You can delete a site using one of the following methods:

- Selecting the site from the Groups window and pressing the Delete key
- Dragging the site into the Deleted Sites group
- Right-clicking the site and selecting Delete from the menu that appears

To completely delete the site, including all historical data, select the site from within the Deleted Devices group and use one of the methods described in the preceding list.

## Configuring an HTTP Proxy

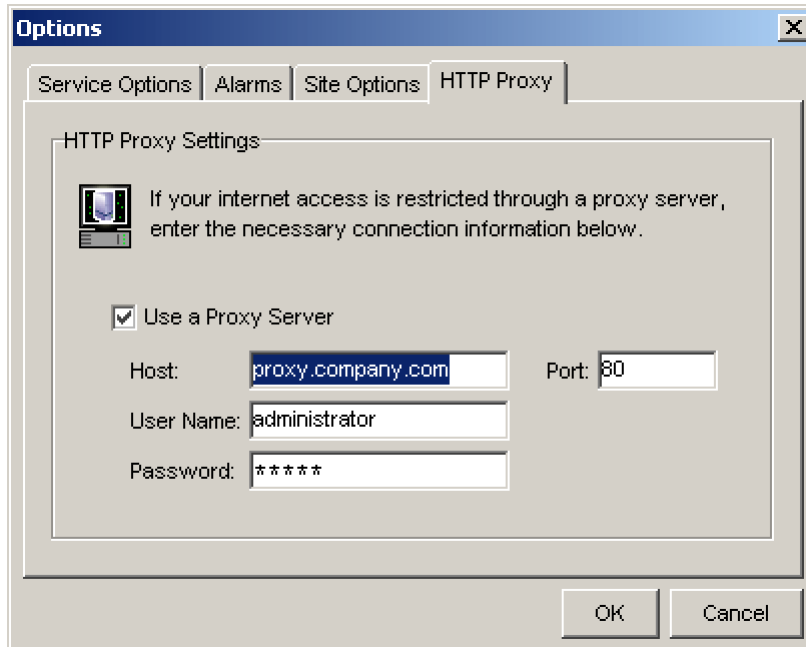
When you add a site to the Enterprise Manager and specify a city, Mobile Manager performs a city search to find all cities that have the name you specified. To perform the search, Mobile Manager connects to a database at the Wavelink Corporation Web site. If you are using a HTTP proxy for external Web site connections, you must configure HTTP proxy settings to enable the city search.

### To configure HTTP proxy settings:

- 1 Click **Options** from the **File** menu.

The *Options* dialog box appears.

- 2 Select the HTTP Proxy tab.



**Figure 4-56.** *The HTTP Proxy Dialog Box*

- 3** Enable the **Use a Proxy Server** checkbox.
- 4** In the **Host** text box, type either the IP address or host name of the proxy.
- 5** Optionally enter a port number in the **Port** text box.  
  
If no port is entered, the port will default to port 80.
- 6** If you are using Basic Authentication for the HTTP proxy type the username and password in the **User Name** and **Password** text boxes. Otherwise, leave these options blank.
- 7** Click OK to save your changes.

When you next run the New Site Wizard or use the Locate feature in the Import/Export Site utility, the proxy server settings configured in this dialog box will be used.

To disable the use of a proxy, disable the **Use a Proxy Server** checkbox in the *Options* dialog box. When you click OK, this erases your proxy settings from

the database. If you then re-open this dialog box, all of the values will be blank.

## Groups

A group is a collection of sites that share a set of similar characteristics such as geographic location or role within your organization's structure. When you define settings for access points or mobile devices, Mobile Manager applies those settings on a per-group basis. You can add as many groups to the Enterprise Management Console as necessary to manage your wireless network effectively.

---

**NOTE** To configure an individual site from the Enterprise Management Console, you can do so by creating a group that contains only that site and applying settings to that group, or by accessing one of the site tools included with Mobile Manager: the Mobile Manager Administrator or the Avalanche Management Console.

---

### To add a group:

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

-or-

Right-click within the Groups window and select **New Group** from the menu that appears.

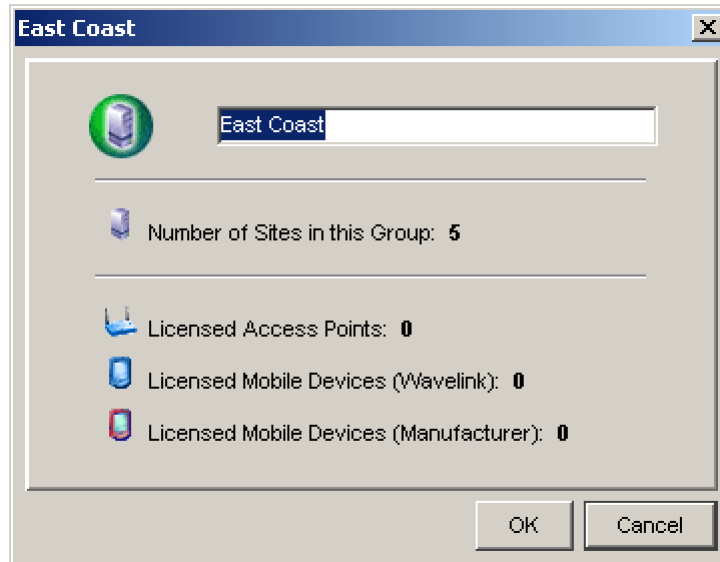
A new group appears within the Groups window.

- 2 Type the name of the new group.

### To view group properties:

- 1 Select a group within the Groups window.
- 2 Select **Properties** from the **File** menu.

The *Group Properties* dialog box appears.



**Figure 4-57.** *The Group Properties dialog box*

In this dialog box, you can view license information associated with a site, the number of sites in the group, and rename the group if desired.

## Adding Sites to Groups

One of the benefits to creating groups within the Enterprise Management Console 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 a site to a group using one of the following methods:

- Drag the site from the Unassigned Sites group to the new group
- Right-click the site, select Move To from the menu that appears, and select the new group



## Configuring Components at the Site Level

Although you manage much of your wireless network with the Enterprise Management Console, certain sites might require additional configuration or management. To accommodate this need, you can access two tools from the Enterprise Management Console: Mobile Manager 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 an access point or a mobile device node in the group tree
- Right-click a site node in the group tree, then select Connect to Site from the menu that appears
- Right-click a site in the map, then select Connect To Site in the popup menu
- Select a site, then select Connect to Site from the **Tools** menu

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

See *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 Management Console

To ensure that your wireless network is managed correctly, it is important to understand the relationship between the configurations established using the Enterprise Management Console, and those established using a site tool such as Mobile Manager Site Administrator or the Avalanche Management Console. Because the Enterprise Management Console 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 Management Console 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 Management Console will not override it.
- IP addresses can be assigned either by the Enterprise Management Console 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 Management Console is designed to apply configuration settings to groups of sites. To configure an individual site from the Enterprise Management Console, you can do so by creating a group that contains only that site and applying settings to that group.

## Deleting Groups

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

A site associated with a group automatically returns to the Unassigned Sites group 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.

## Chapter 5: Managing Access Points

One of the primary tasks for which you use Mobile Manager is to manage the access points on the network. Within the Enterprise Management Console, access point settings are divided into several groups:

- **Group-based settings.** These settings apply to all access points within a specific group that you select from the Groups window. Group-based settings include the ESS ID and IP address assignments. Because the process for configuring these settings applies to both access points and mobile devices, their use is described in *Chapter 6: Managing Network Settings* on page 205.
- **Device access privileges.** These settings are the user names and passwords that provide Mobile Manager with the authorization needed to configure specific access points.
- **Profile-based settings.** These settings apply to a specific set of access points within a given group. Profiles allow you to create collections of access point settings that you can simultaneously apply to multiple access points.
- **Firmware updates.** Firmware is the software that determines the features an access point supports. If you want to manage a new type of access point, you will likely need to update the access point Agent with additional firmware.
- **Security settings.** These settings apply to all access points within your network, regardless of their group. These settings are primarily security-based and include settings such as the Access Control List and WEP. Because these settings focus on securing your wireless network, their use is described in *Chapter 8: Managing Security Settings* on page 309.

This section covers the following topics:

- Defining Device Access Privileges
- Creating Access Point Profiles
- Scheduling Profiles
- Applying Access Point Settings
- Updating Access Point Firmware

## Defining Device Access Privileges

To manage wireless network components—including access points, switches, and routers—an Agent must have the correct authorization. The type of authorization required varies, depending on which protocol the Agent uses to configure the component. These types of authorizations are as follows:

- SNMP Read-Only Community Name
- SNMP Read/Write Community Name
- Telnet passwords
- HTTP user name and password

The authorization required varies depending on the type of hardware being queried by the access point. Frequently, a component requires more than one authorization type—for example, an Agent might need both an HTTP user name and an SNMP Read/Write name to correctly configure an access point. The following table lists the authorization required for each hardware type:

	Authorization
Switches	SNMP Read-Only Community Name
Cisco-Aironet 350/1200 Series access points	SNMP Read/Write Community Name HTTP user name and password
Cisco-Aironet (IOS)	SNMP Read/Write Community Name Telnet Password HTTP user name and password
Symbol access points	SNMP Read/Write Community Name SNMP Read-Only Community Name HTTP user name and password
Proxim access points	SNMP Read-Only Community Name SNMP Read/Write Community Name
Dell access points	SNMP Read-Only Community Name SNMP Read/Write Community Name

**Table 5-1:** Authorization Required for Component Queries

---

**NOTE** If you find that an Agent is unable to query a component, it is recommended that you first look at whether the Agent has the proper authorization information for that component.

---

The Agent supports multiple authorizations for each protocol type. For example, networks frequently have multiple SNMP read/write user names. In this situation, when you define device access privileges for the Agent, you can create a list of SNMP read/write user names. When the Agent attempts to query an access point, it moves through the list of SNMP read/write user names until it finds one the access point will accept. If all attempts to communicate with an access point fail, the Agent will generate an alert.

---

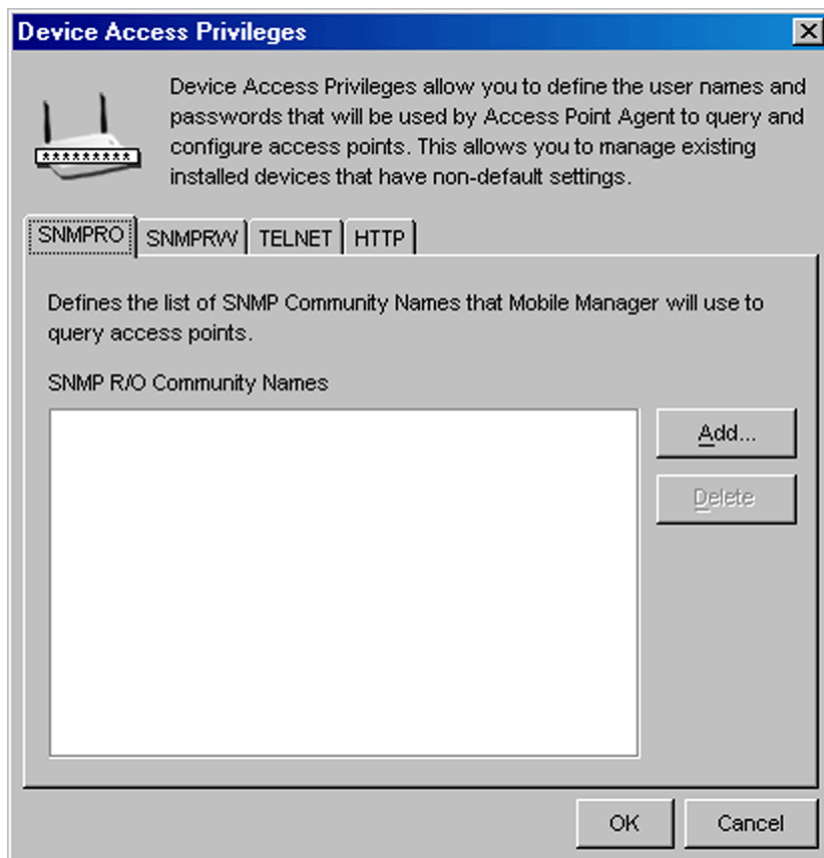
**NOTE** To apply new device access privileges to a group, you must send the information to the Agents within that group. See *Applying Access Point Settings* on page 174 for more information.

---

**To define device access privileges:**

- 1 Select a group from the Groups window.
- 2 Click `Configure Network`.
- 3 Click the `Network Settings Tab`.
- 4 Click `Define Access Privileges`, located at the bottom of the `Network Settings` tab.

The *Device Access Privileges* dialog box appears.



**Figure 5-1.** *The Device Access Privileges Dialog Box*

- 5** To add an SNMP read-only user name, select the SNMP R/O tab and click Add. A dialog box appears, allowing you to type a new SNMP read-only user name.
- 6** To add an SNMP read/write user name, select the SNMP R/W tab and click Add. A dialog box appears, allowing you to type a new SNMP read/write user name.
- 7** To add a Telnet password, select the Telnet tab and click Add. A dialog box appears, allowing you to type a new Telnet password.
- 8** To add an HTTP account, select the HTTP tab and click Add. A dialog box will appear, allowing you to enter a user name and password for the

account. Each account must be assigned to a specific hardware manufacturer, such as Cisco or Symbol.

In addition, you can enable the **Make This User a Cisco AP Administrator** checkbox to designate the new account as a Cisco AP administrator, which is necessary if you want the account to be authorized to make changes to Cisco-Aironet and Cisco IOS access point configurations. When you enable this checkbox, Mobile Manager will push this account to your Cisco-Aironet and Cisco IOS access points.

---

**NOTE** To manage Cisco-Aironet access points with the Mobile Manager Administrator, you must have both an HTTP account that has administrative privileges and an authorized SNMP Read/Write user name. HTTP access must be enabled on the access point.

---

---

**NOTE** To manage Cisco IOS access points with the Mobile Manager Administrator, you must have both an HTTP account that has administrative privileges and an authorized SNMP Read/Write user name. You might also need to add a Telnet user if the Enable password is not the default. Telnet access must be enabled on the access point.

---

9 Click **Apply**.

10 Click **OK**.

## **Cisco IOS Access Privileges**

For Cisco access points that use IOS, the following information is required to authorize Mobile Manager to manage the access point:

- Telnet user name and password
- Telnet Enable password

By default, the Telnet user name, password, and Enable password for Cisco IOS access points is Cisco. If you enabled security for managing access points with Mobile Manager, this default Telnet information is removed to prevent unauthorized use of the access point.

Mobile Manager will enable SNMP on the access point provided it can enter Enable mode. By default, SNMP is disabled and no SNMP read/write user exists.

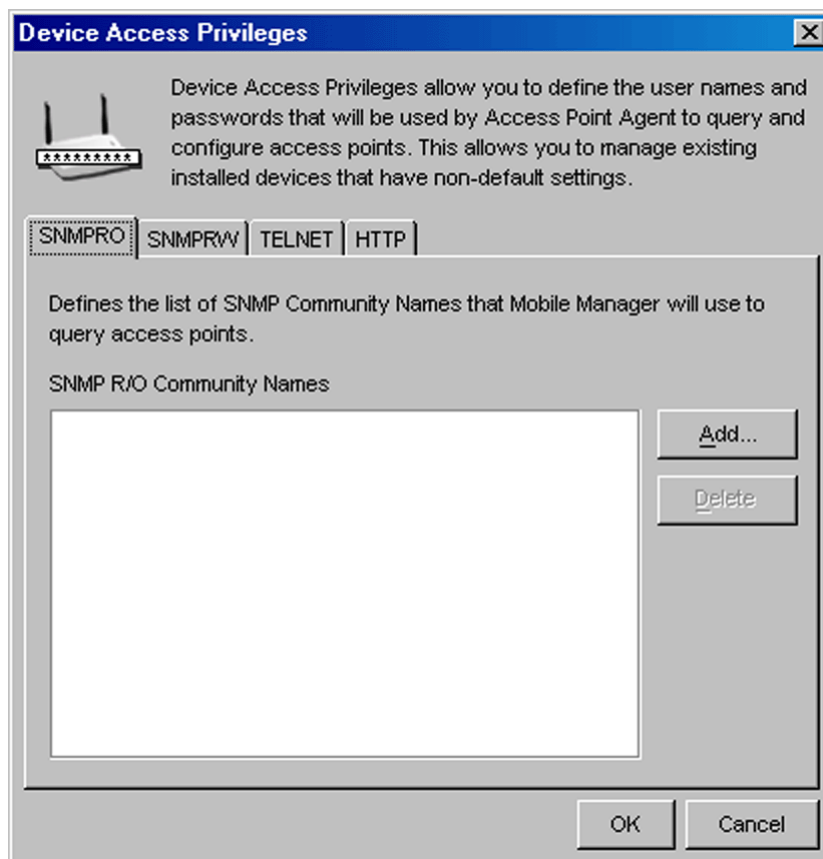
If you installed Mobile Manager with security disabled, Mobile Manager will add a public SNMP read/write user. If you installed Mobile Manager with security enabled, Mobile Manager will add a SNMP read/write user with the same value as the Telnet user name. Mobile Manager will remove the public SNMP read/write user any time you enable its security features.

**To define Cisco IOS access privileges:**

- 1 Select a group from the Groups window.
- 2 Click `Configure Network`.
- 3 Click the `Network Settings Tab`.
- 4 Click `Define Access Privileges`, located at the bottom of the `Network Settings` tab.

The *Device Access Privileges* dialog box appears.





**Figure 5-2.** *The Device Access Privileges Dialog Box*

- 5 If you modified the Cisco IOS access point so that its Telnet Enable password is not "Cisco," select the Telnet tab and click **Add**. A dialog box appears, allowing you to type the Telnet Enable password that Mobile Manager requires to access the Cisco IOS access point.
- 6 Click the HTTP tab and click **Add**. A dialog box appears, allowing you to add an HTTP user name and password. For Cisco IOS access points, this information is used as follows:
  - HTTP user name is used as the Telnet user name
  - HTTP password is used as the Telnet and Telnet Enable passwords.

- 7 Enable the **Make This User a Cisco AP Administrator** checkbox to make the new account a Cisco AP administrator.

---

**NOTE** If you have a mixed environment of VxWorks and IOS access points, this account will be used for both types of access points.

---

- 8 Click `Apply`

When you create Cisco IOS access privileges, it is helpful to remember the following:

- Mobile Manager will automatically add a Cisco/Cisco HTTP user. This user exists to manage any access point that is in its factory default state. It is recommended that you do not delete these entries—doing so can result in Mobile Manager being unable to manage the access points. You can always add this user back if you have problems accessing the access point.
- If the SNMP Read/Write name is left at its default value, public, then Mobile Manager replaces it with the HTTP user name you defined.
- If you connect to the access points using a Web browser, the user name field in the Web browser authentication dialog box corresponds to the access point's Telnet user name. Similarly, the password field corresponds to the Telnet Enable password.

## Creating Access Point Profiles

An access point profile is a collection of access point settings that you can simultaneously apply to multiple access points. Mobile Manager not only applies these settings to access points—it also enforces these settings, preventing unauthorized modifications.

Previously, organizations have been challenged with finding an efficient means of configuring access points. These challenges existed for several reasons. First, prior to 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. If Mobile Manager Enterprise finds an access point's configuration has changed, it resets the access point back to the settings defined in its profile. In addition, Mobile Manager routinely checks for new access points on the network. When a new access point is discovered, the access point Agent determines its hardware type and assigns it to the appropriate access point profile, if one is available.

---

**NOTE** Access point profiles apply only to one group within the Enterprise Management Console. You cannot assign a single profile to multiple groups; however, you can copy a profile from one group to another.

---

There are two types of access point profiles: regular profiles and default profiles. Regular profiles are applied only to the access points that you specify. You can have as many regular profiles as your network needs demand. Default profiles are profiles that Mobile Manager applies to any non-profiled or newly-discovered access points within a group. Unlike regular profiles, you can only have one default profile per type of access point.

---

**NOTE** If a site contains a default profile that was created at the site level, the profile created with the Enterprise Management Console has precedence. The site's default profile remains, but the Agent at that site ceases using it as the default profile.

---

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

This section contains the following topics:

- Configuring Profiles
- Modifying Profiles
- Deleting Profiles
- Refreshing Profiles

- Determining Which Access Point Properties to Use

## Configuring Profiles

Once you organize your network sites into groups, you can assign profiles to each group. The Enterprise Management Console 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](#) 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 Profiles

Enterprise profiles apply only to one specific [group](#); however you can copy a profile from one group to another. Profiles can be created for any hardware type that Mobile Manager supports. These hardware types are as follows:

- Cisco 1100
- Cisco 1200
- Cisco 340/350
- Cisco 350 Bridge
- Dell TrueMobile 1170
- Symbol AP-3020, 3021
- Symbol AP-4111, 4121
- Symbol AP-4131
- Proxim 600
- Proxim 2000

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

---

**NOTE** To apply profiles to a group, you must send the information to the Agents within that group. See *Applying Access Point Settings* on page 174 for more information.

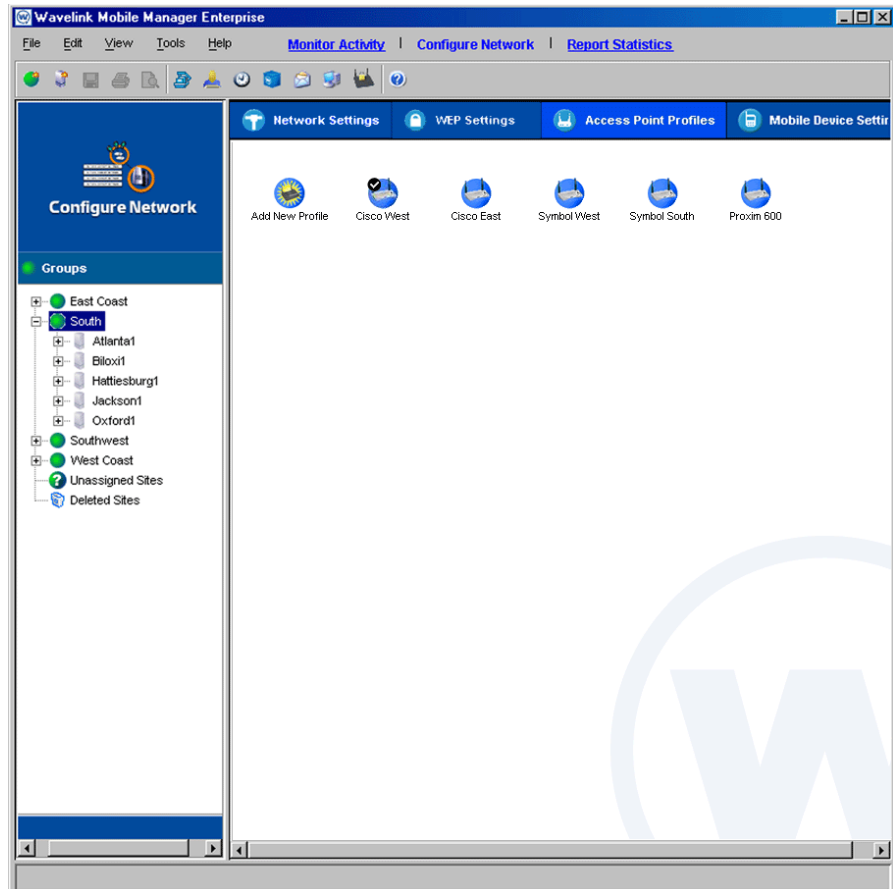
---

#### To create a profile:

- 1 Select a group from the Groups window.

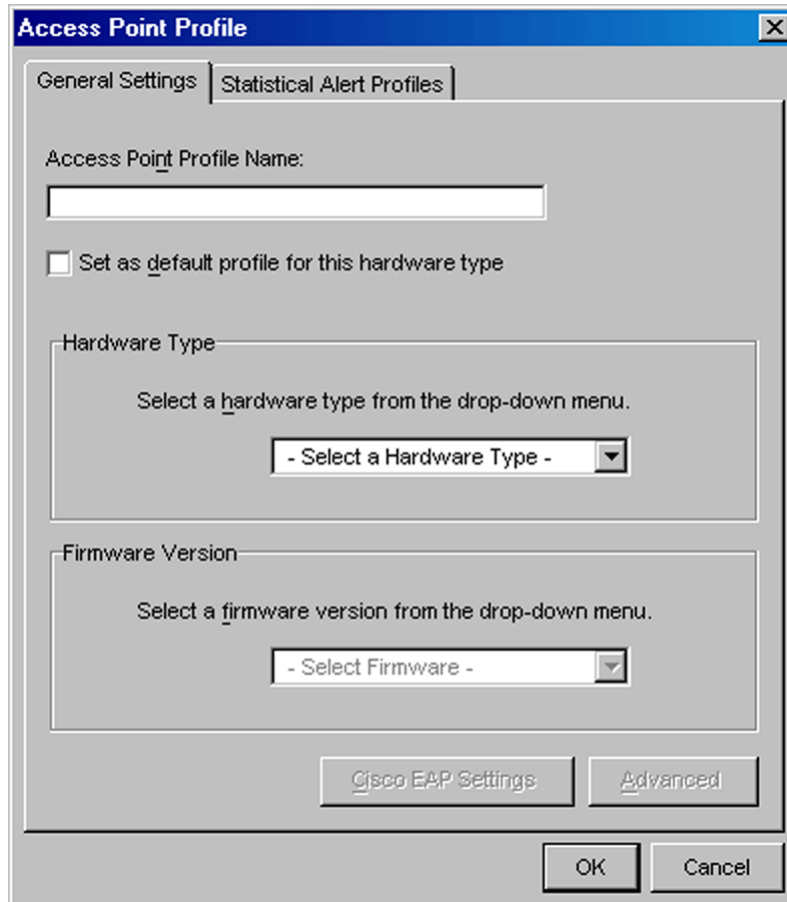
The profile that you create will apply to all access points managed within the selected group.

- 2 Select **Configure Network**.
- 3 Click the **Access Point Profiles** tab.



**Figure 5-3.** *The Access Point Profiles Tab of the Configure Network View*

- 4 Double-click the **Add New Profile** icon.  
The *Access Point Profile* dialog box appears.



**Figure 5-4.** *The Access Point Profile Dialog Box*

- 5 Type a name for the profile in the **Access Point Profile Name** text box.
- 6 If you want this profile to be a default profile, enable the **Set as default profile for this hardware type** checkbox.
- 7 Select a hardware type from the **Hardware Type** list.
- 8 Select a firmware from the **Firmware Version** list.
- 9 To configure additional access point properties, click **Advanced**.

See *Mobile Manager Users Guide* for more information on the properties available for your access points.

10 Click `OK`.

The new profile appears in the Access Point Profiles tab.

## Modifying Profiles

You can modify profiles as your network demands.

---

**NOTE** To apply profiles to a group, you must send the information to the Agents within that group. See *Applying Access Point Settings* on page 174 for more information.

---

### To modify a profile:

- 1 Select a group from the Groups window.
- 2 Select `Configure Network`.
- 3 Click the Access Point Profiles tab.
- 4 Right-click the profile and select `Properties` from the menu that appears.
- 5 Modify the profile as needed.

## Deleting 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 the site is synchronized with the Enterprise Management Console.

---

**To delete a profile:**

- 1 Select a group from the Groups window.
- 2 Select `Configure Network`.
- 3 Click the Access Point Profiles tab.
- 4 Right-click the profile and select `Delete` from the menu that appears.

**Refreshing Profiles**

If you installed the Enterprise Management Console on multiple systems, the profile list is refreshed each time you launch the Enterprise Management Console 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 Access Point Profiles tab.
- 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 Mobile Manager Enterprise 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.

---

**NOTE** You can view supported properties and property descriptions for different access points in the Administrator in the *Advanced Properties* dialog box for a profile.

---

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 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 want to ensure that access points can only be configured through the Enterprise Management Console, you can 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 Management Console.

### **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 Management Console's Configure Network view. See *Building Access Control Lists* on page 291 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 8: Managing Security Settings* on page 289 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 8: Managing Security Settings* on page 309 for more information on wireless network security and Mobile Manager Enterprise.

### **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 folder of the *Access Points Properties* dialog box.

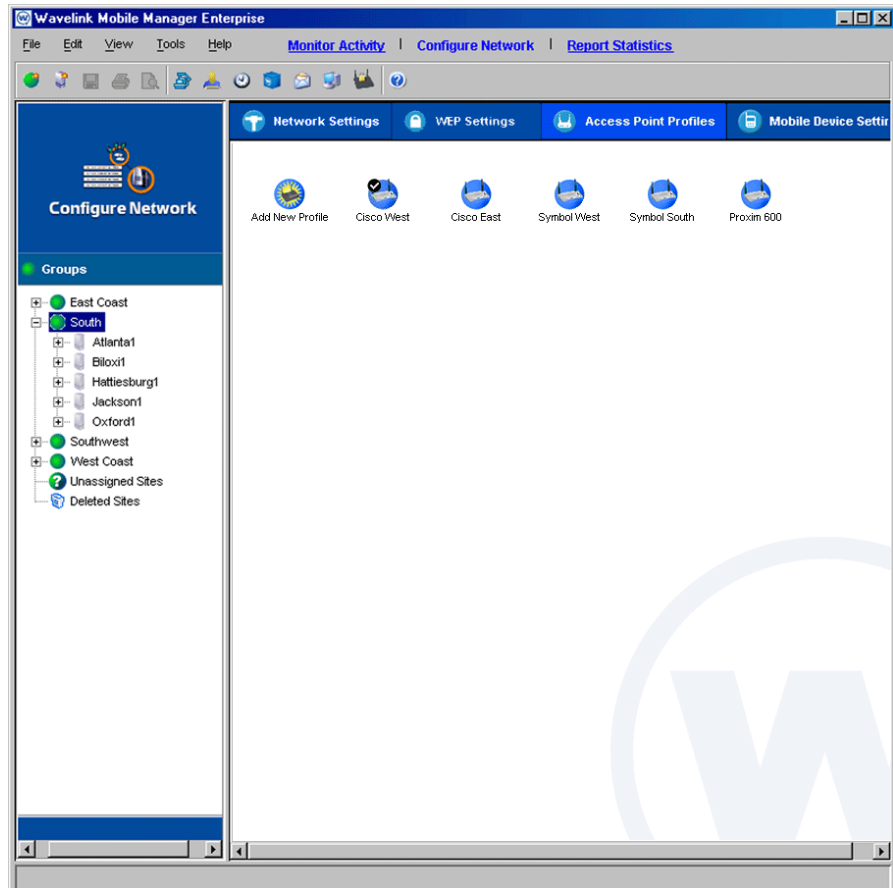
#### **To access the SNMP folder:**

- 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.

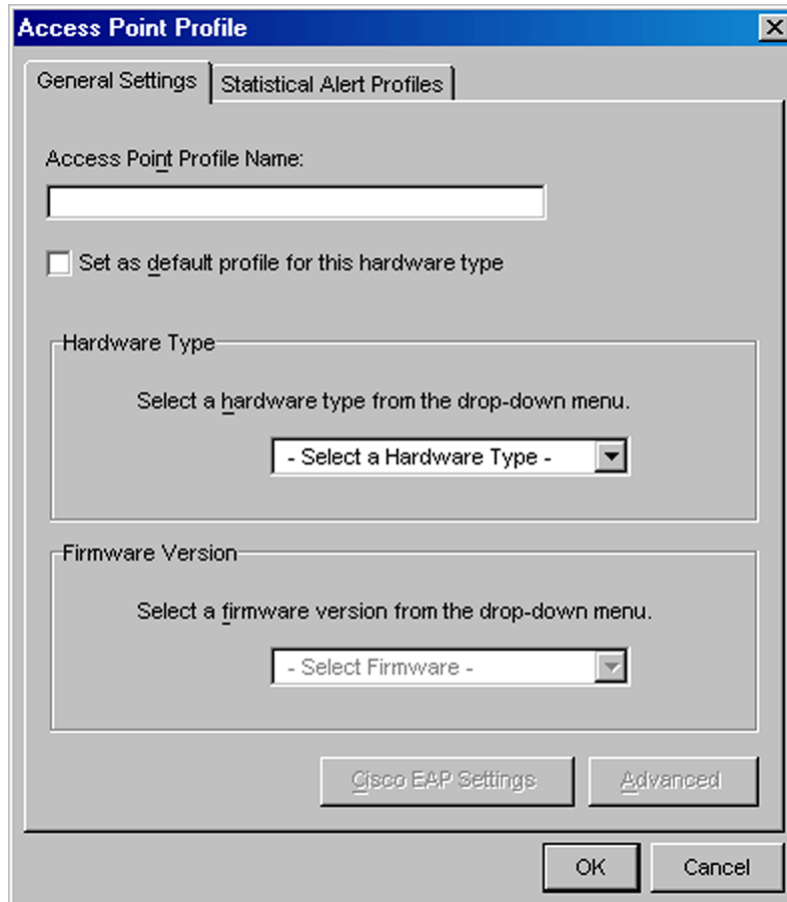


**Figure 5-5.** The Access Point Profiles Tab of the Configure Network View

**4** Select a profile and click `Edit`.

If you have not created a profile yet, double-click the **Add New Profile** icon.

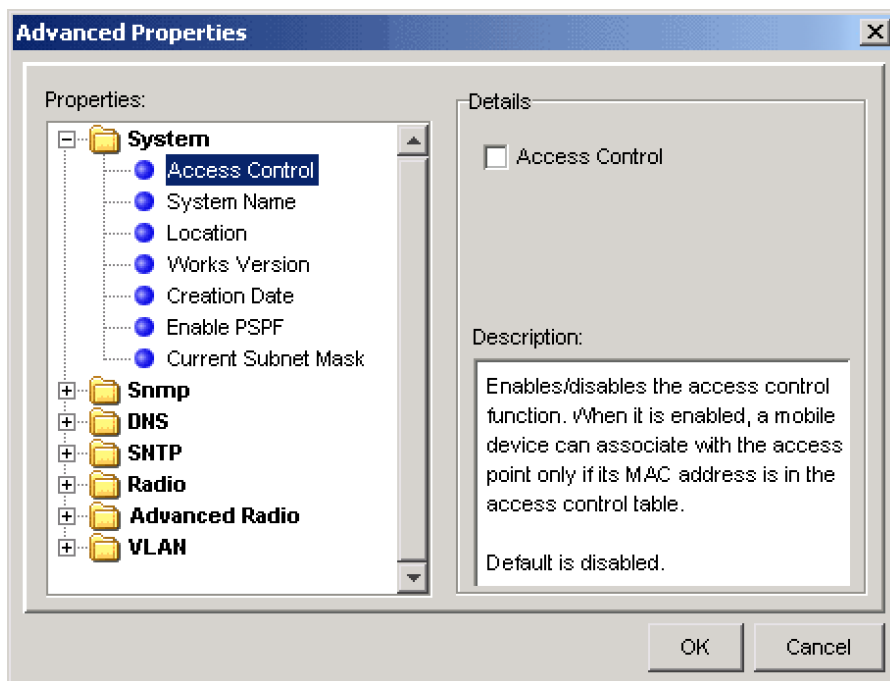
The *Access Point Profile* dialog box appears.



**Figure 5-6.** *The Access Point Profile Dialog Box*

- 5 Click *Advanced*.

The *Advanced Properties* dialog box appears.



**Figure 5-7.** *The Advanced Properties Dialog Box*

**6** Click the SNMP folder.

The types of events (also known as traps) that you can capture depend 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.

## Scheduling Profiles

In addition to creating profiles, you also have the option to schedule profiles at the agent level. When you schedule a profile, you define a time and date when you want the profile to apply to a given set of access points/wireless switches at the access point site agents directly. This is helpful if you do not want to have the Enterprise Console perform the scheduled operation. Currently, if you define a default profile for a Cisco 1130- AP and use the Enterprise Task Scheduler, it pushes the default profile to the defined sites at the Enterprise Scheduler's the scheduled time. As soon as the profile arrives

at the site, it will apply immediately. The new agent profile scheduler provides another layer of control that allows you to push down the profile, but keeps the profile in an inactive state at the site until the profile scheduled time arrives.

Once you schedule a profile, the scheduled profile needs to be pushed to the defined sites using the Task Scheduler. If the defined profile is a default profile it arrives at the site and remains in a pending state until the scheduled time arrives. Once the scheduled time has arrived, the profile applies to all access points/wireless switches at the site that meet the hardware type of the defined profile.

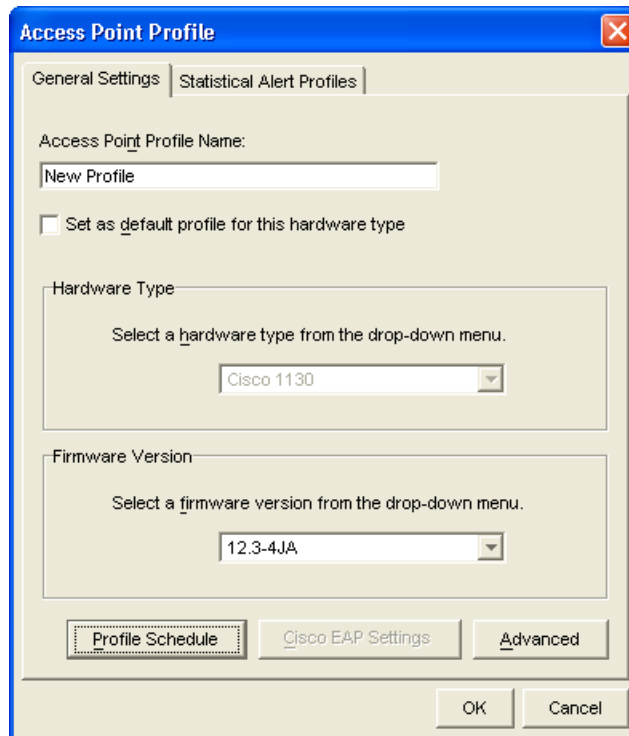
If the defined profile is not a default profile, it remains available at the site agent, but does not apply to any devices. You have the option to launch the detailed view for the applicable sites and then manually apply the defined profiles to individual or a group of devices. The profile remains pending until the scheduled time arrives. Once the schedule time arrives, the profile will be applied.

Once the scheduled profile is applied, an alert is generated for each applicable AP informing the user that the scheduled profile was applied.

**To schedule a profile:**

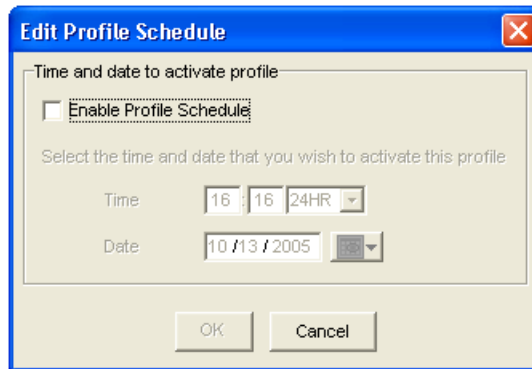
- 1** Select a group from the Groups window.
- 2** Select `Configure Network`.
- 3** Click the Access Point Profiles tab.
- 4** Double-click the **Add New Profile** icon.

The *Access Point Profile* dialog box appears.



**Figure 5-8.** Access Point Profile

- 5 Type a name for the Profile in the **Access Point Profile Name** text box.
- 6 If you want this profile to be the default profile, enable the **Set as default Profile for this hardware type** check box.
- 7 Select a hardware type from the **Hardware Type** list.
- 8 Select a firmware from the **Firmware Version** list.
- 9 Click Profile Schedule.



**Figure 5-9.** *Edit Profile Schedule*

- 10 Select the **Enable Profile Schedule** check box.
- 11 Configure the **Time** and **Date** for the profile to apply to the set of access points/wireless switches.

## Applying Access Point Settings

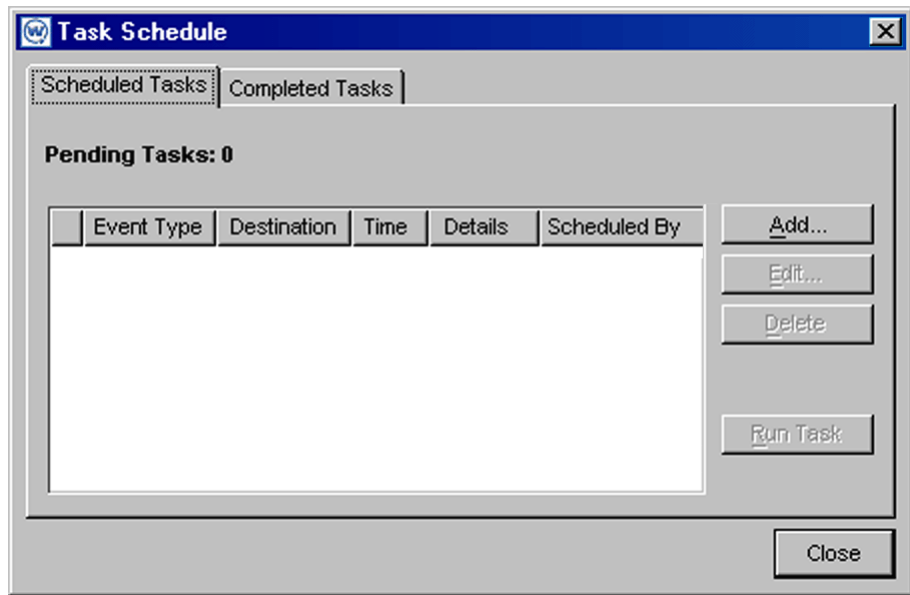
Any time you create or modify settings for a group's access points—whether it is changing an ESS ID or creating a new profile—you must send those settings to the Agents within the group for the modification to take effect.

### To apply access point settings to a group:

- 1 Select **Task Schedule** from the **Tools** menu.

The *Task Schedule* dialog box appears.

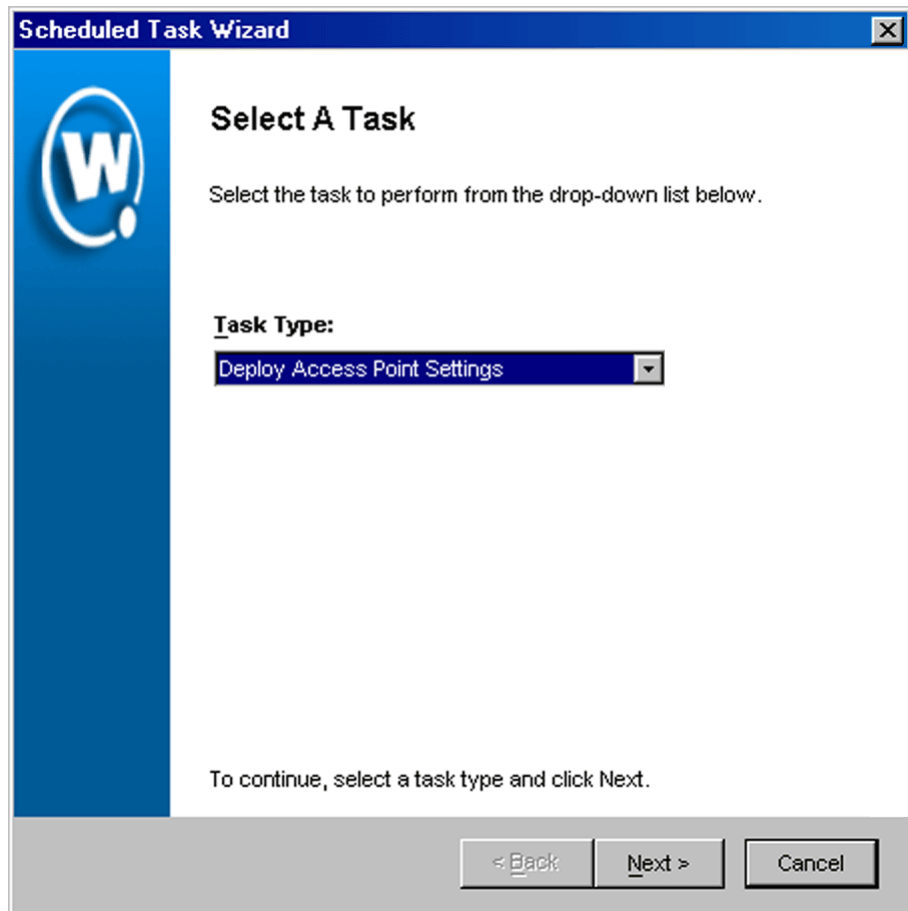




**Figure 5-10.** *The Task Schedule Dialog Box*

- 2 Click Add.

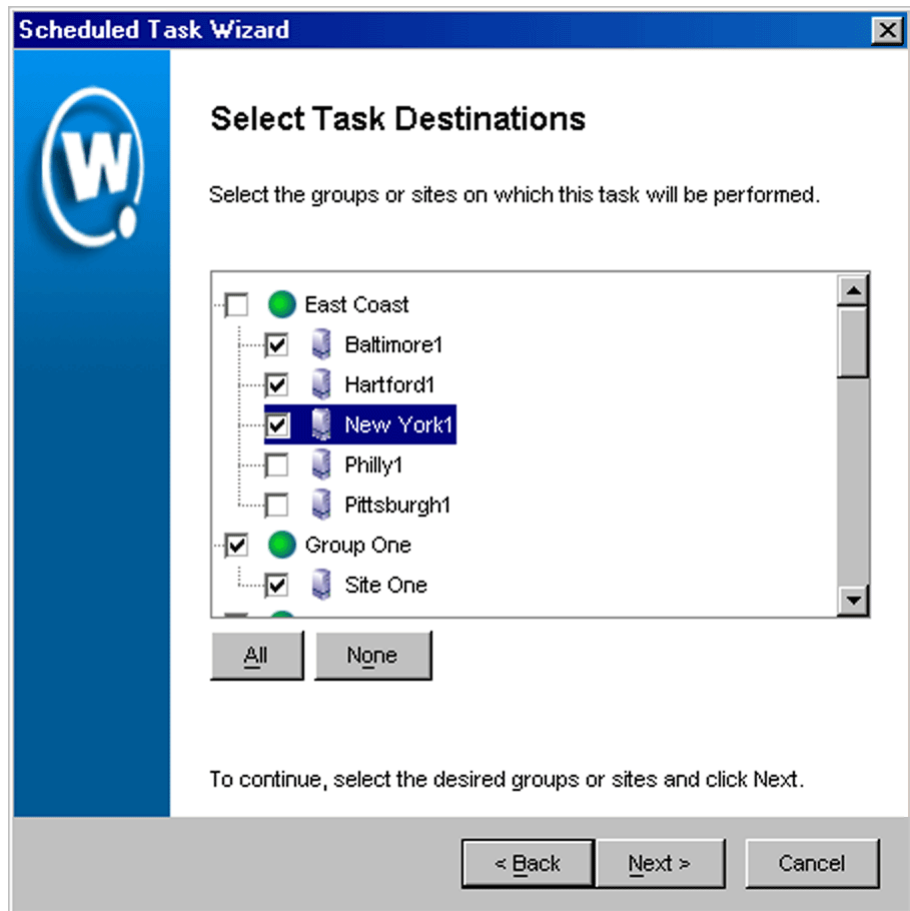
The *Select A Task* dialog box appears.



**Figure 5-11.** *The Select A Task Dialog Box*

- 3 Select `Deploy Access Point Settings` from the **Task Type** list and click `Next`.

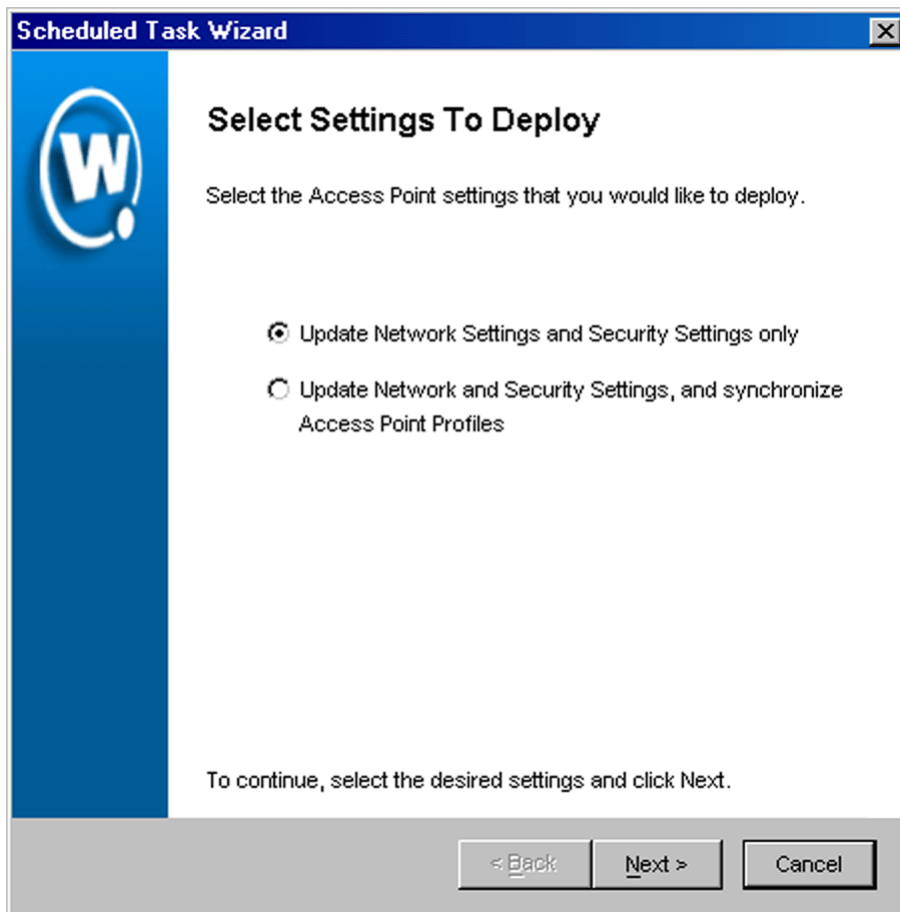
The *Select Task Destination* dialog box appears.



**Figure 5-12.** *The Select Task Destination Dialog Box*

- 4 Select the groups or sites by enabling the checkbox next to the group or site name. You can also select all groups by clicking `All`.
- 5 Click `Next`.

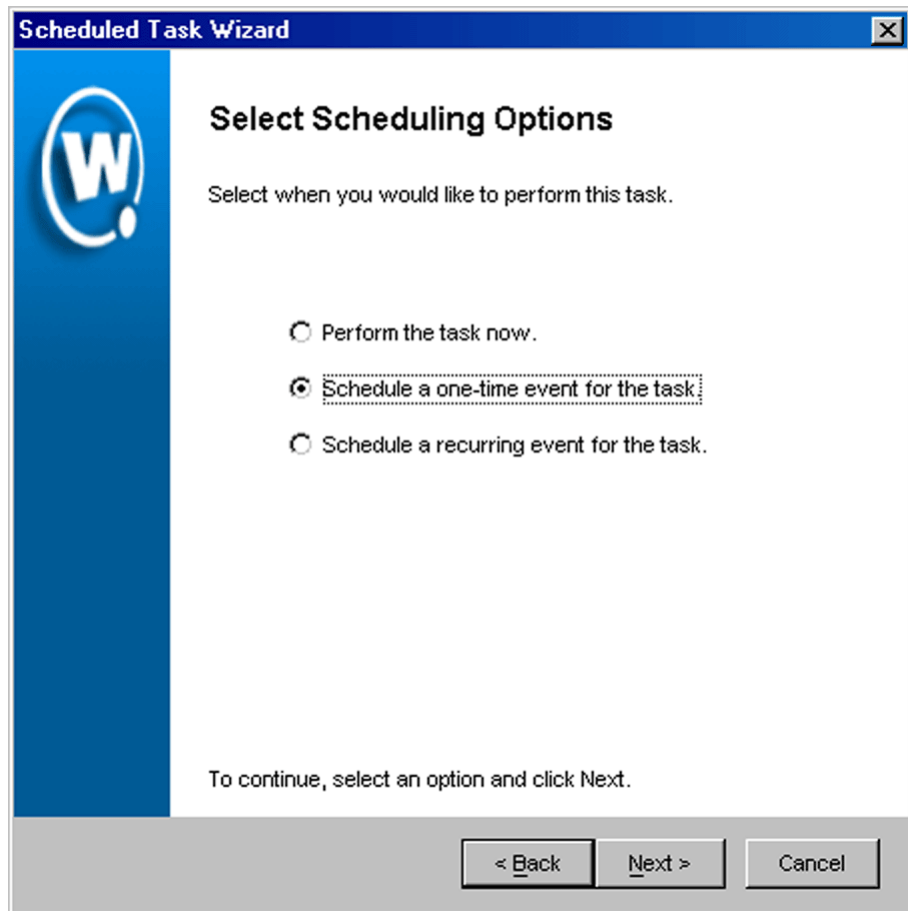
The *Select Settings to Deploy* dialog box appears.



**Figure 5-13.** *The Select Settings to Deploy Dialog Box*

- 6** If you are only changing the ESS ID, IP addresses, or security settings, select the **Update Network Settings and Security Settings only** option.
- 7** If you are changing ESS ID, IP addresses, security settings, or access point profiles, select the **Update Network and Security Settings and synchronize Access Point Profiles** option.
- 8** Click **Next**.

The *Select Scheduling Options* dialog box appears.



**Figure 5-14.** *The Select Scheduling Options Dialog Box*

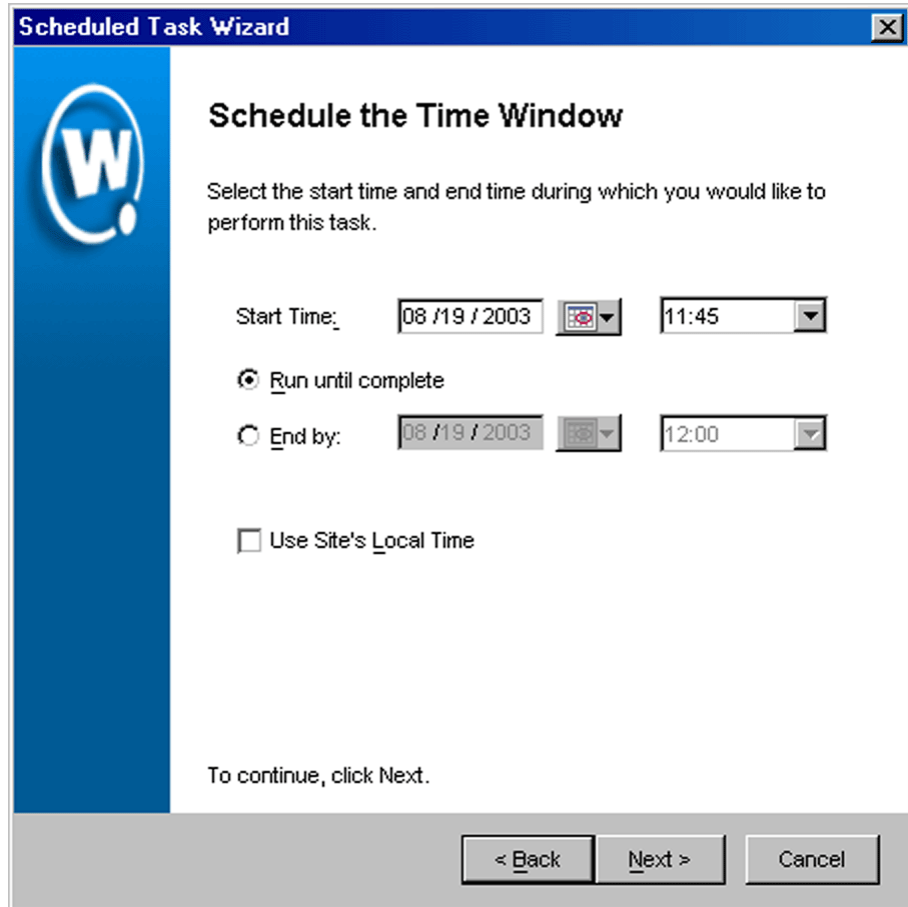
**9** Determine when the event will occur.

If you want the event to occur immediately, select the **Perform the task now** option.

If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

If you want the event to occur on a regular basis, select the **Schedule a recurring event** for this task option.

- 10 Click **Next**.
- 11 If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.



**Figure 5-15.** *The Schedule the Time Window Dialog Box*

Within this dialog box, you can set the following parameters for the event:

- Select the start date and time for the event.
- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete**

option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.
- 12** If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

**Scheduled Task Wizard**

## Configure Task Recurrence

Use the controls below to configure the recurrence settings

**Task time**

Start Time: 00:00  Run until complete  Use Site's Local Time  
 End by: 00:00

**Recurrence pattern**

Daily Recur every 1 week(s) on:  
 Weekly  Sunday  Monday  Tuesday  Wednesday  
 Monthly  Thursday  Friday  Saturday

**Range of recurrence**

Start: 08 / 19 / 2003  No end date  
 End by: / /

To continue, click Next.

< Back    Next >    Cancel

**Figure 5-16.** *The Configure Task Recurrence Dialog Box*

Within this dialog box, you can set the following parameters for this event:

- Select the start time for the event.
- Determine when you want the event to stop. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.



- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

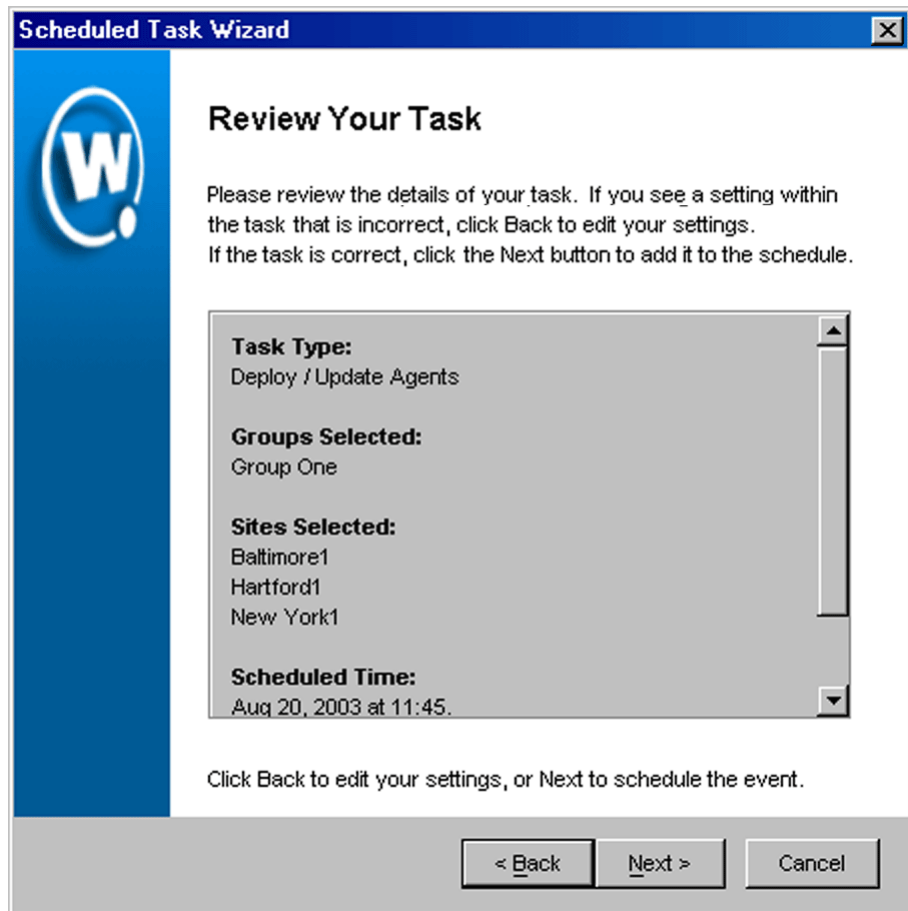
---

**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

**13** Click *Next*.

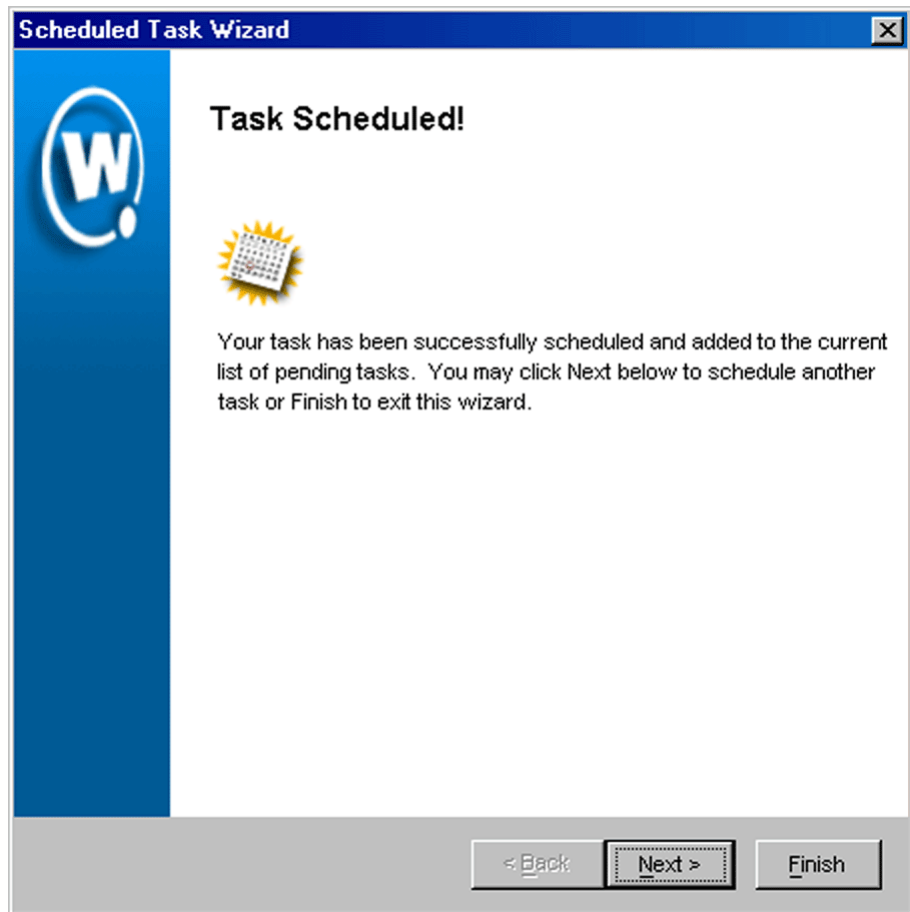
The *Review Your Task* dialog box appears.



**Figure 5-17.** *The Review Your Task Dialog Box*

**14** Review your the task to ensure that it is correct and click `Next`.

The *Task Scheduled* dialog box appears.



**Figure 5-18.** *The Task Scheduled Dialog Box*

- 15 Click `Next` to schedule a new event, or click `Finish` to return to the *Task Schedule* dialog box.

---

**NOTE** To update an Access Control List, you must follow the steps described in *Deploying Access Control Lists* on page 322.

---

## Updating Access Point Firmware

Firmware is the software installed on access points that determines what sort of properties and features that an access point supports. Mobile Manager supports a wide range of firmware for many different types of access points.

When you first deploy an access point Agent to a site, you specify a selection of firmware that the Agent supports. If you want to expand this selection, you can do so at any time by updating the access point firmware at the site.

This section covers the following topics:

- Types of Firmware Support
- Creating Firmware Packages
- Deploying Firmware Packages

### Types of Firmware Support

To support as many firmware versions as possible, Mobile Manager interacts with access points in one of two ways: either in [full support mode](#) or in [compatibility mode](#). Mobile Manager selects which mode to use based on whether it can recognize the firmware version installed on an access point. If neither mode is available for the firmware, the Mobile Manager does not manage the access point until the firmware version is changed.

Using the full support and compatibility modes provides you with a great deal of flexibility when determining what firmware versions you want to install on your access points. These modes also reduce the risk of access points going unengaged because their firmware type was not recognized.

#### Full Support Mode

If the firmware version installed on an access point matches a firmware version known to the Mobile Manager Agent, the Agent can communicate with that access point in full support mode. In full support mode, the Agent is able to retrieve and set a vast majority of properties for that access point. This mode is the standard mode the Agent uses to manage access points.

#### Compatibility Mode

If the Agent is unable to recognize the firmware installed on the access point, it attempts to communicate with it in compatibility mode. In compatibility

mode, the Agent relies on existing firmware property files to retrieve and set as many of the access point's properties as possible.

When the Agent detects an access point that has an unrecognized firmware version, the Agent compares that firmware against a list of defined firmware ranges. Each firmware range corresponds to a firmware version that the Agent fully supports. If the unrecognized firmware falls within one of these ranges, the Agent manages the access point using the corresponding fully-supported firmware. If the unrecognized firmware does not fall within a firmware range, the Agent uses a pre-defined firmware version to manage the access point.

---

**NOTE** The Agent uses alternative firmware versions only as a basis to manage access points with unrecognized firmware; the Agent does not update the actual firmware of the access point unless you specifically instruct it to do so.

---

See your Mobile Manager release notes for the specific firmware ranges the Agent uses to manage access points with unrecognized firmware.

The following table illustrates how the Agent selects a matching property file:

	Fully-supported Firmware	Compatible Firmware Range
Cisco-Aironet 350	12.01T1	<b>12.01T1 - 12.99</b>
Symbol T3	03.50-18	<b>03.50-00 - 03.50-99</b>

**Table 5-2:** *Firmware Version Matches for Compatibility Mode Support (Samples)*

The following example uses the information in table 5-2 to demonstrate how the Agent manages access points with unrecognized firmware. A Cisco-Aironet access point is installed on a network that used firmware version 12.02T1. The Agent discovers this access point, and identifies that it cannot recognize the firmware version. The Agent then checks to see if firmware 12.02T1 falls within a firmware range. It finds that if a firmware version falls between 12.01T1 and 12.99, it should use firmware version 12.01T1 to manage the access point. Consequently, the Agent begins to manage the new access point based on the 12.01T1 firmware.

## Creating Firmware Packages

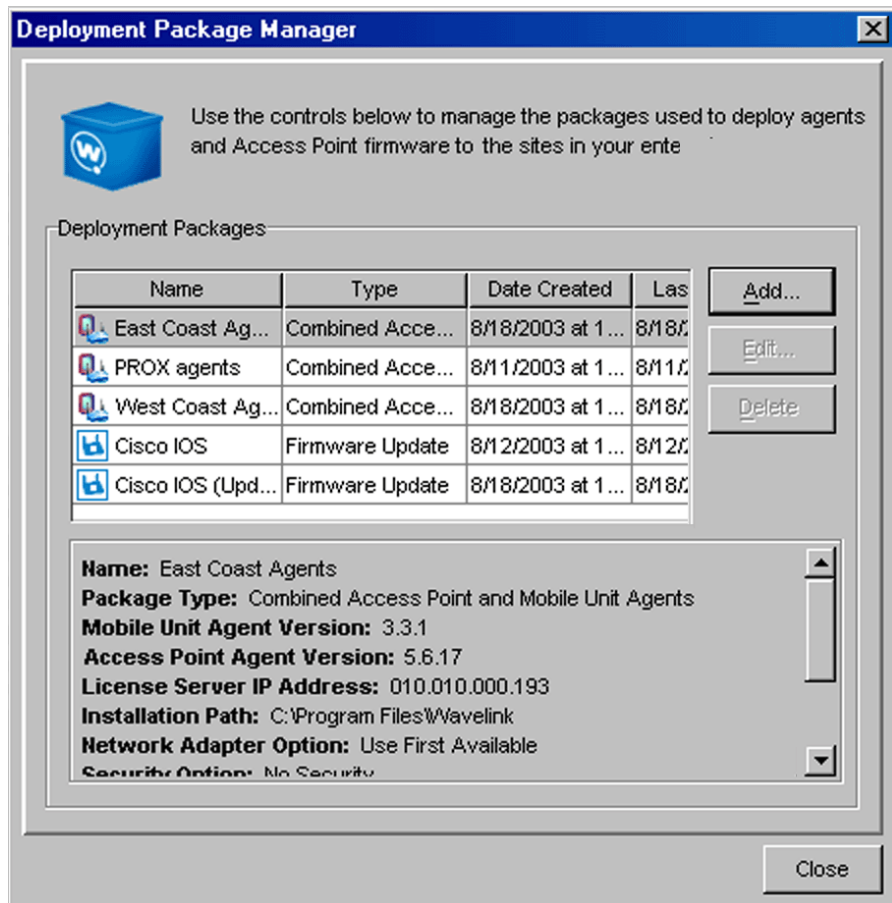
A firmware package is a collection of files that allow an Agent to support the software installed on access points. You can create a firmware package to contain as many firmware versions as you need; however, it is important to

remember that the larger the firmware package, the longer it takes to send to a given site.

**To create a firmware package:**

- 1 Select `Deployment Packages` from the **Tools** menu.

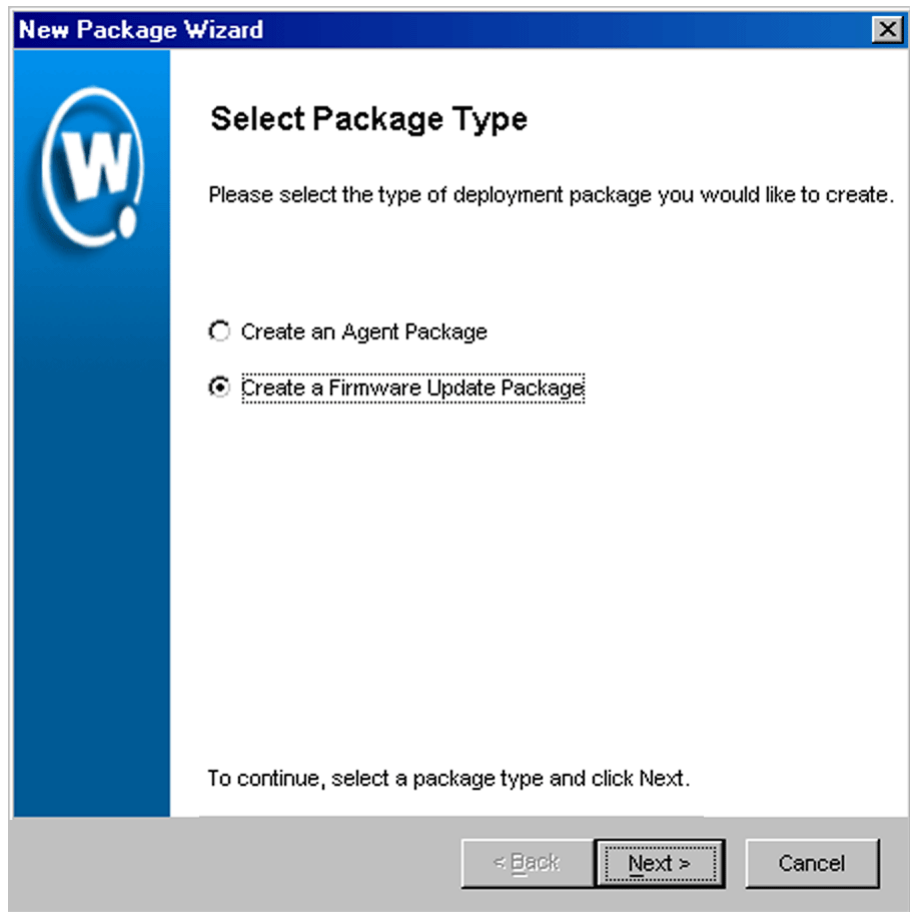
The *Deployment Package Manager* dialog box appears.



**Figure 5-19.** *The Deployment Package Manager Dialog Box*

- 2 Click `Add`.

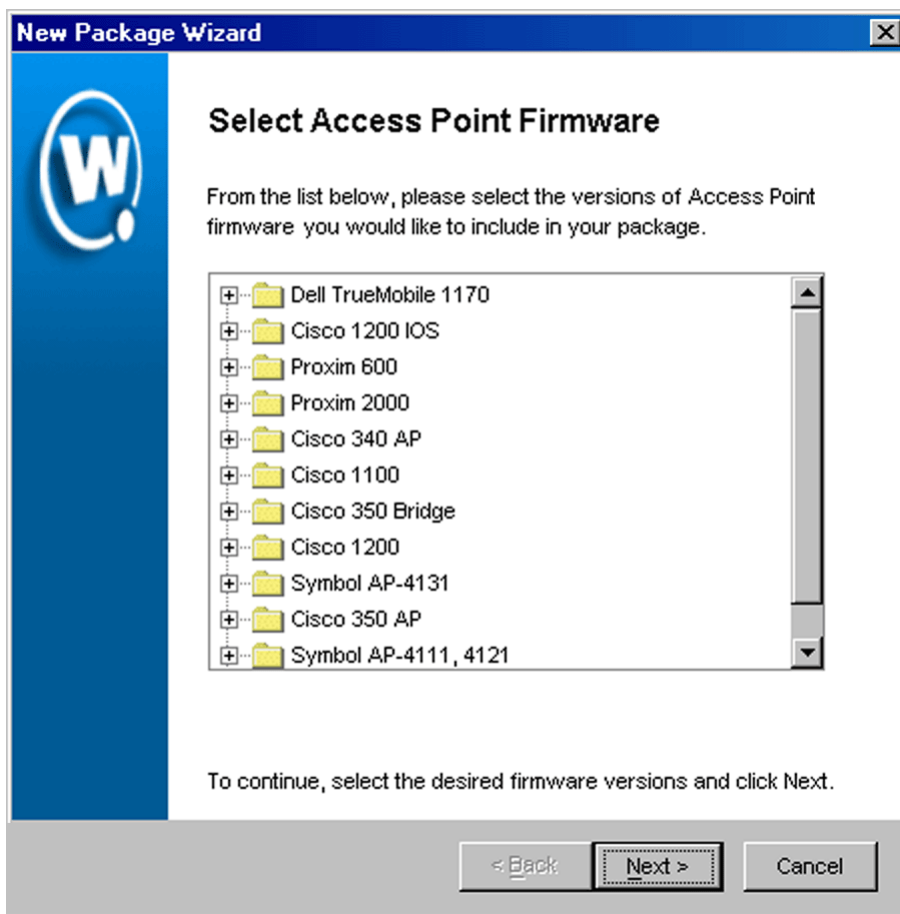
The *Select Package Type* dialog box appears.



**Figure 5-20.** *The Select Package Type Dialog Box*

- 3 Select the **Create a Firmware Update Package** option and click **Next**.

The *Select Access Point Firmware* dialog box appears. This dialog box contains a collection of folders, with each folder representing a specific type of access point.



**Figure 5-21.** *The Select Access Point Firmware Dialog Box*

**4** Select the firmware versions this Agent will support.

To select firmware, open the appropriate folder within the dialog box. A list of available firmware versions appears. Select a firmware version by enabling the checkbox next to the firmware name. You can select any number of firmware versions from each folder.

**5** Click `Next`.

The *Enter Package Name* dialog box appears.

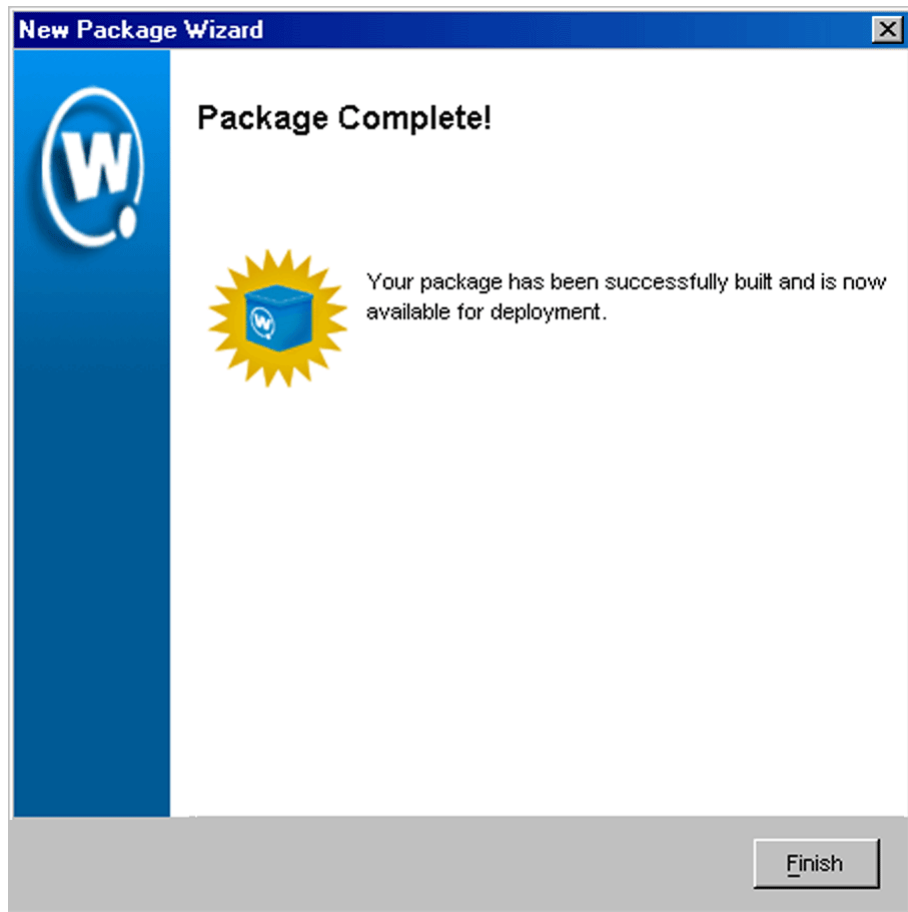




**Figure 5-22.** *The Enter Package Name Dialog Box*

- 6 Type a name for the package in the **Package Name** text box and click **Next**.

Mobile Manager begins to create the deployment package. When it is finished, a *Package Complete* dialog box appears.



**Figure 5-23.** *The Package Complete Dialog Box*

7 Click `Finish`.

Mobile Manager returns you to the *Deployment Package Manager* dialog box. You can now create a new package, edit a package, or delete a package as needed.

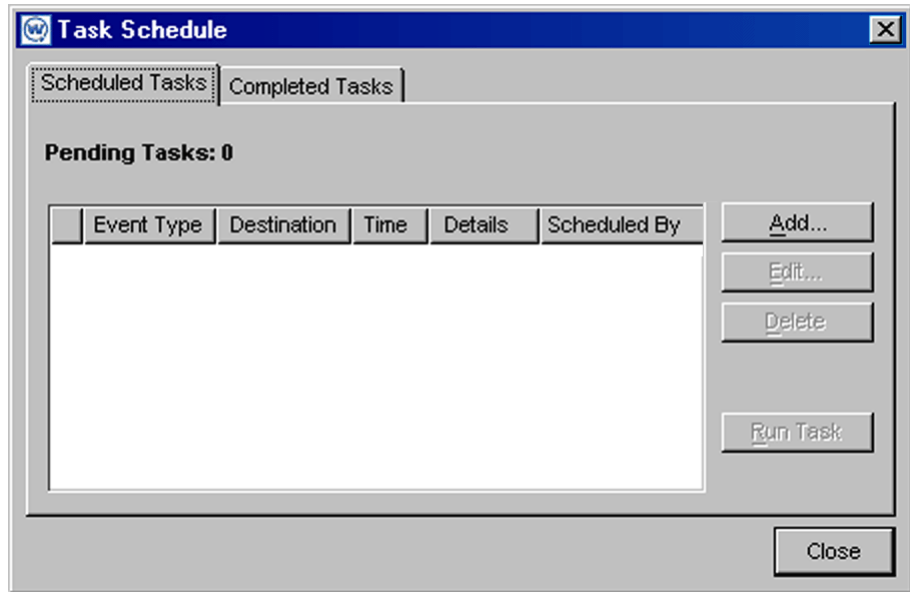
## **Deploying Firmware Packages**

Once you create a firmware package, you must deploy it to your sites and groups.

**To deploy firmware packages:**

- 1 Select `Task Schedule` from the **Tools** menu.

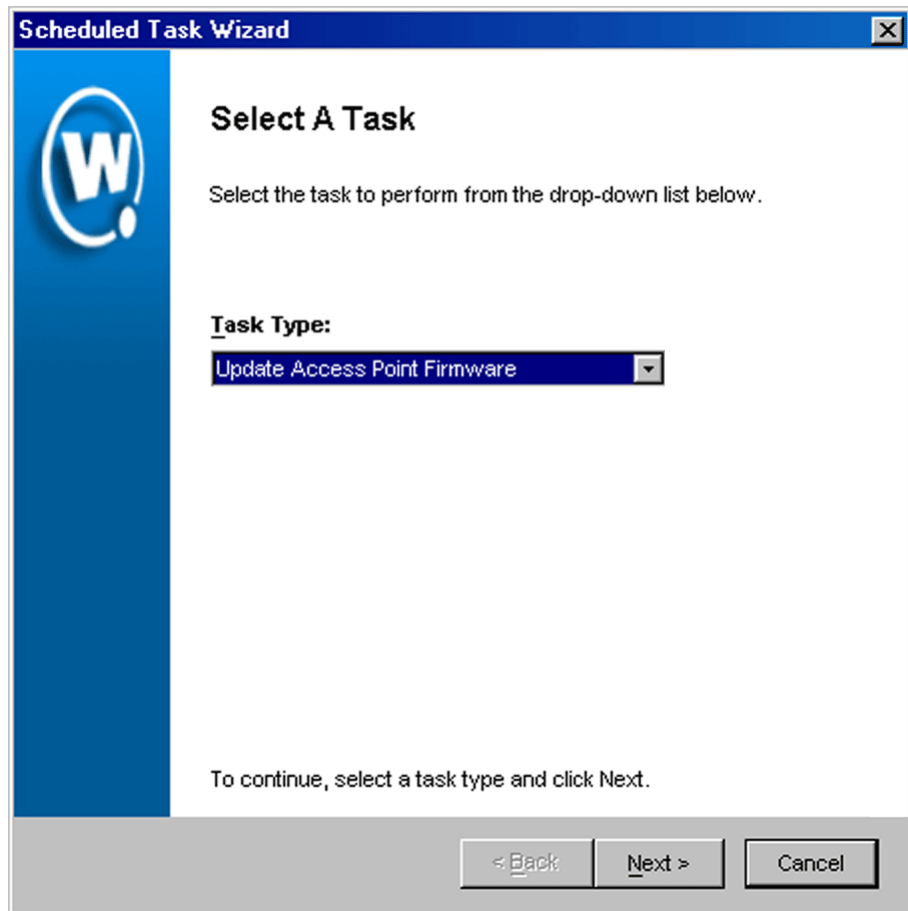
The *Task Schedule* dialog box appears.



**Figure 5-24.** *The Task Schedule Dialog Box*

- 2 Click `Add`.

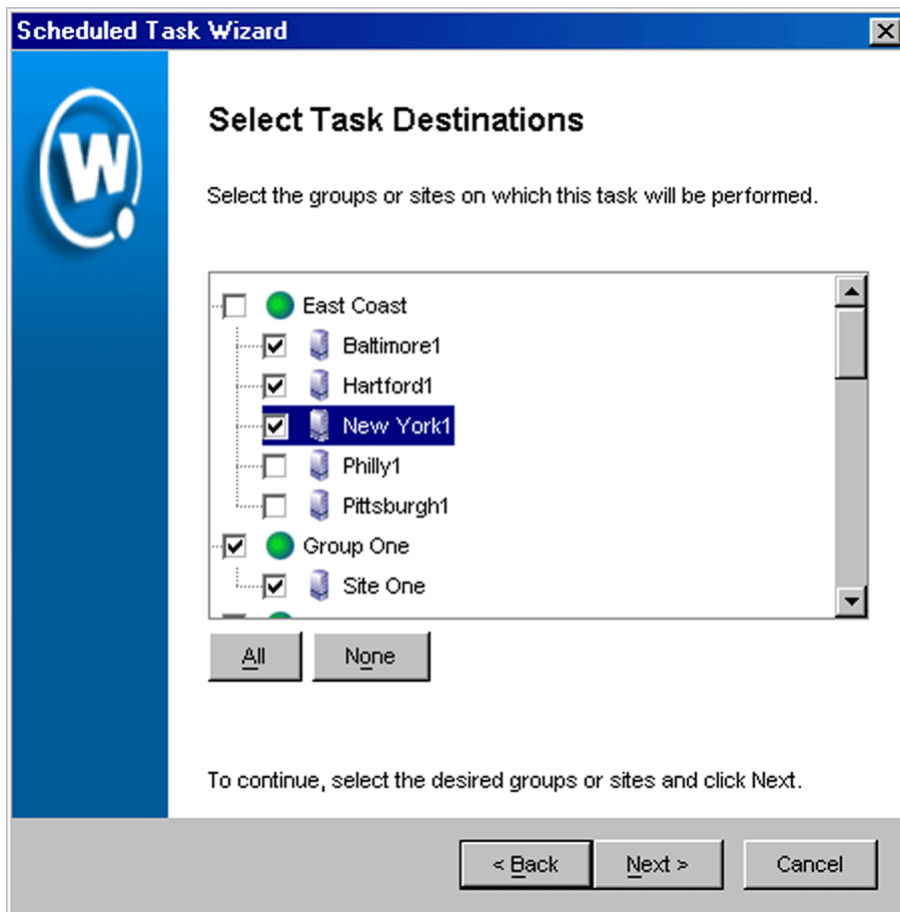
The *Select A Task* dialog box appears.



**Figure 5-25.** *The Select a Task Dialog Box*

- 3 Select Update Access Point Firmware from the **Task Type** list and click Next.

The *Select Task Destination* dialog box appears.



**Figure 5-26.** *The Select Task Destination Dialog Box*

- 4 Select the groups or sites by enabling the checkbox next to the group or site name. You can also select all groups by clicking `All`.
- 5 Click `Next`.

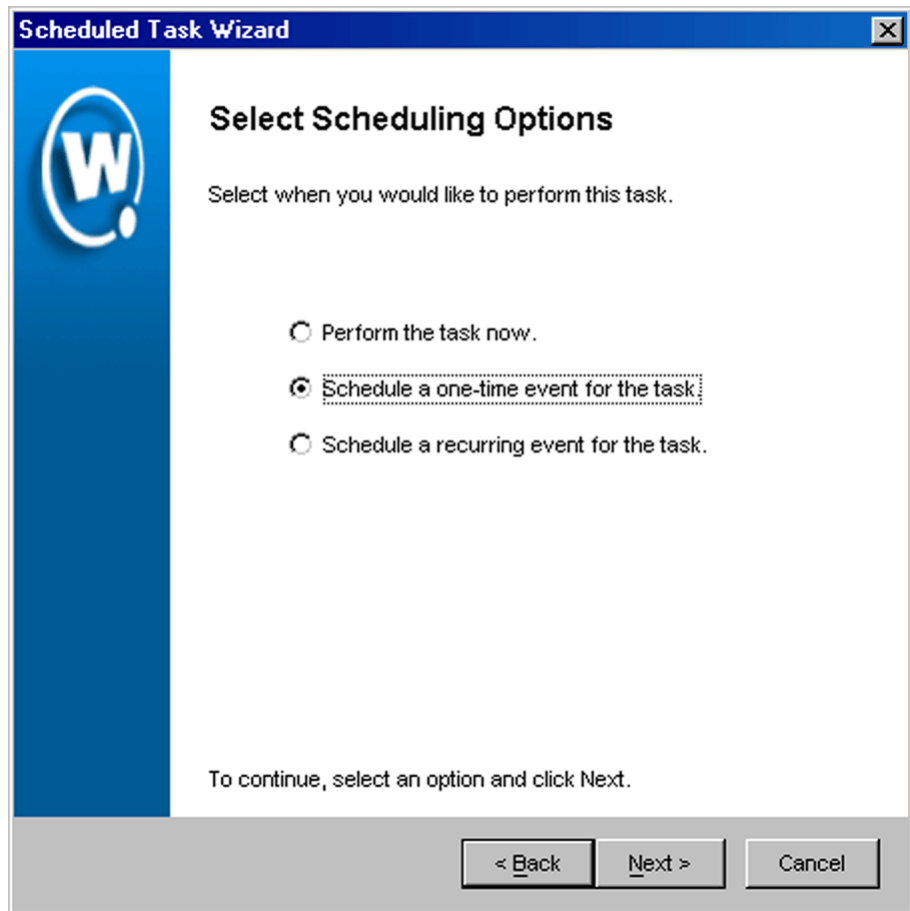
The *Select Firmware Packages to Deploy* dialog box appears.



**Figure 5-27.** *The Select Firmware Packages to Deploy Dialog Box*

- 6** Select the firmware packages you want to deploy by enabling the checkbox next to the name of the firmware package.
- 7** Click `Next`.

The *Select Scheduling Options* dialog box appears.



**Figure 5-28.** *The Select Scheduling Options Dialog Box*

**8** Determine when the event will occur.

If you want the event to occur immediately, select the **Perform the task now** option.

If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

If you want the event to occur on a regular basis, select the **Schedule a recurring event** for this task option. This option is not necessary if the firmware package is not expected to change.

9 Click **Next**.

10 If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.

**Scheduled Task Wizard**

### Schedule the Time Window

Select the start time and end time during which you would like to perform this task.

Start Time: 08 /19 /2003 11:45

Run until complete

End by: 08 /19 /2003 12:00

Use Site's Local Time

To continue, click Next.

< Back Next > Cancel

**Figure 5-29.** *The Schedule the Time Window Dialog Box*

Within this dialog box, you can set the following parameters for the event:



- Select the start date and time for the event.
  - Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.
  - If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.
- 11** If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

**Scheduled Task Wizard**

## Configure Task Recurrence

Use the controls below to configure the recurrence settings

**Task time**

Start Time: 00:00  Run until complete  Use Site's Local Time  
 End by: 00:00

**Recurrence pattern**

Daily Recur every 1 week(s) on:  
 Weekly  Sunday  Monday  Tuesday  Wednesday  
 Monthly  Thursday  Friday  Saturday

**Range of recurrence**

Start: 08 / 19 / 2003  No end date  
 End by: / /

To continue, click Next.

< Back Next > Cancel

**Figure 5-30.** The Configure Task Recurrence Dialog Box

Within this dialog box, you can set the following parameters for this event:

- Select the start time for the event.
- Determine when you want the event to stop. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

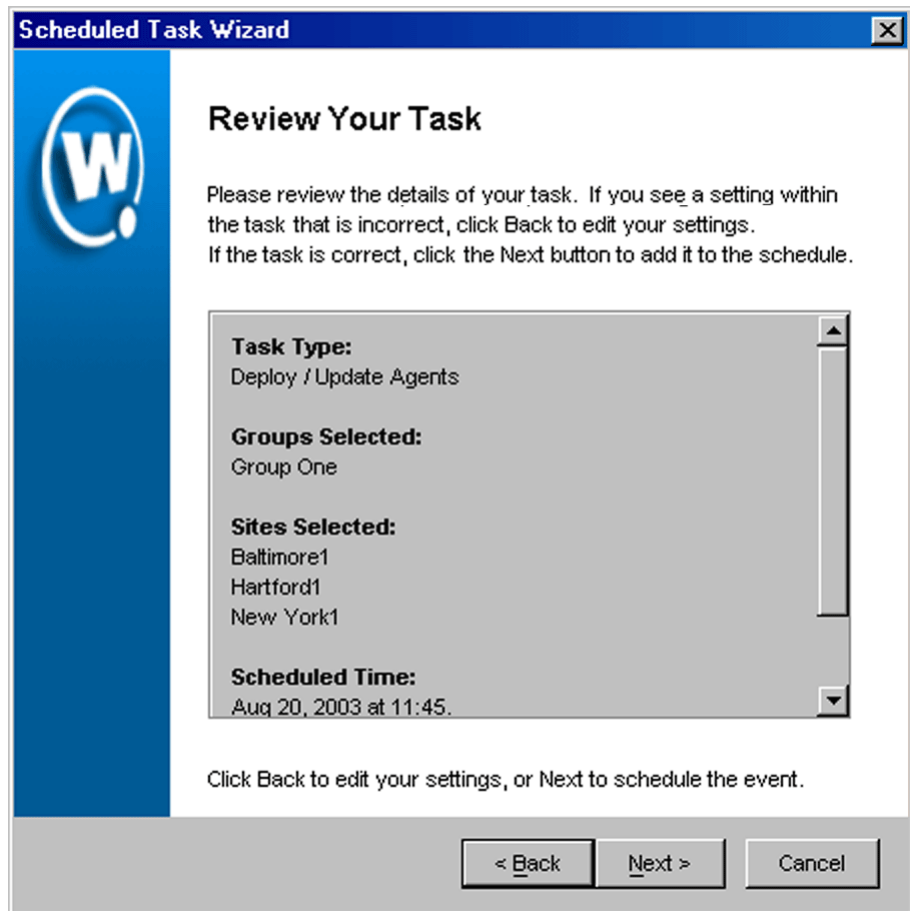
---

**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

**12** Click *Next*.

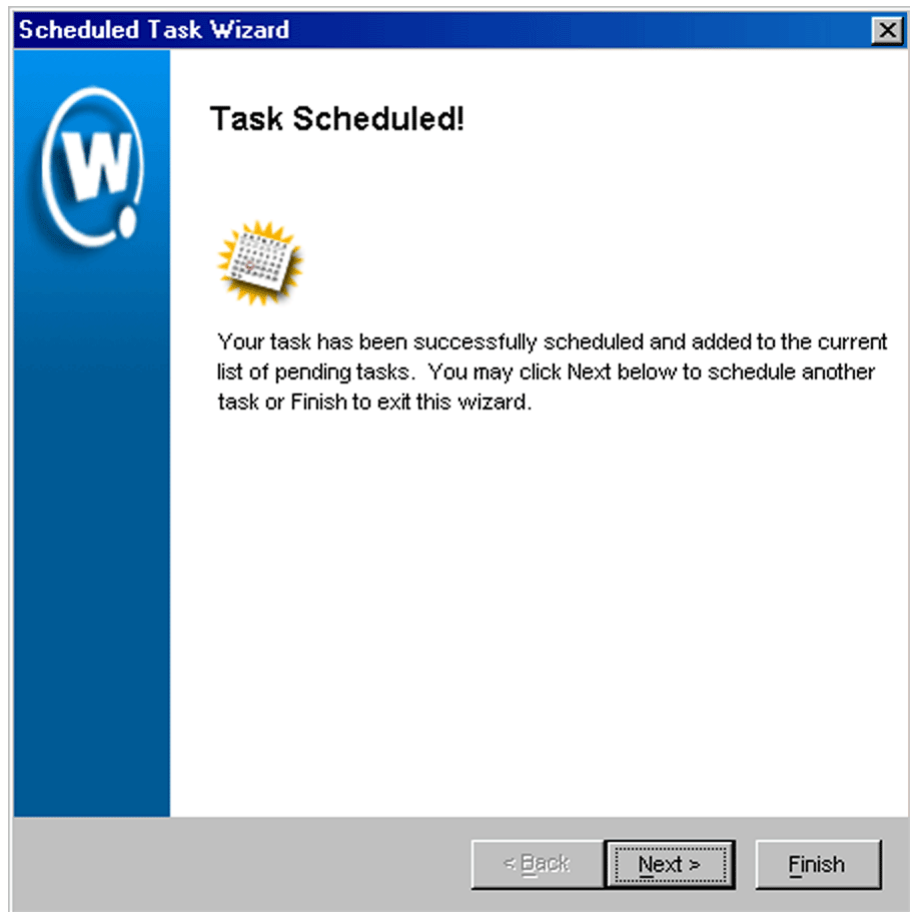
The *Review Your Task* dialog box appears.



**Figure 5-31.** *The Review Your Task Dialog Box*

**13** Review your the task to ensure that it is correct and click `Next`.

The *Task Scheduled* dialog box appears.



**Figure 5-32.** *The Task Scheduled Dialog Box*

- 14 Click `Next` to schedule a new event, or click `Finish` to return to the *Task Schedule* dialog box.



## Chapter 6: Managing Network Settings

The Configure Network view of the Enterprise Management Console 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.** ESS IDs are unique identifiers that organize mobile device-to-access point associations. These identifiers serve two purposes: (1) to provide you a means of categorizing subsections of your wireless network, and (2) to help prevent mobile devices that might belong to other wireless networks from accidentally associating with access points within your organization.
- **IP addresses.** The Network Settings tab provides you with tools to add, modify, and delete IP address assignments to both access points and mobile devices.

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 organizes mobile device-to-access point associations. This identifier serves two purposes: (1) to provide you a means of categorizing subsections of your wireless network, and (2) to help 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.

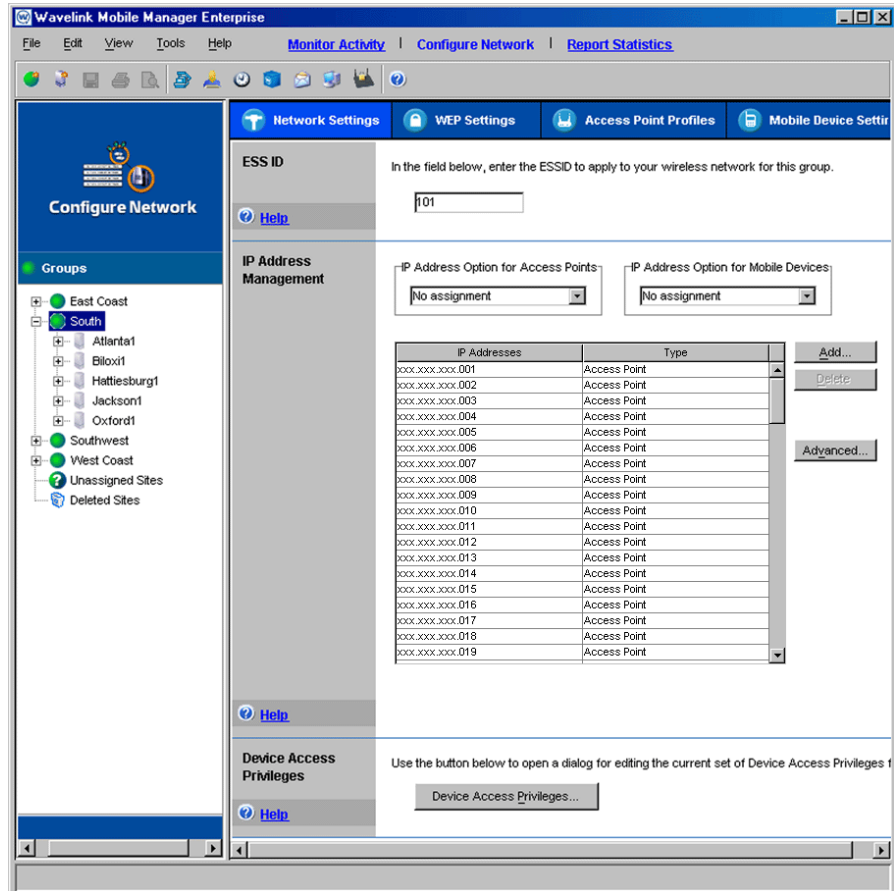


Figure 6-1. The Network Settings Tab of the Configure Network View

- 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.



Mobile Manager Enterprise will assign the new ESS ID to wireless devices during the next network settings deployment event. See *Deploying Network Settings* on page 217 for more information on deploying network settings.

## Managing IP Addresses

The Enterprise Management Console 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.

Before you begin creating IP addresses for your enterprise wireless network, it is recommended that you review the following section, *Overview of Assigning IP Addresses* on page 207. This section describes how Mobile Manager Enterprise assigns IP addresses to the multiple sites within a given group.

After you are familiar with how Mobile Manager Enterprise assigns IP addresses to wireless components, you can read the section *Assigning IP Addresses* on page 208 for complete instructions on assigning IP addresses to access points and mobile devices.

### Overview of Assigning IP Addresses

With the Enterprise Management Console, 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.

---

**NOTE** The following section, *Assigning IP Addresses*, provides complete instructions for assigning IP address to access points and mobile devices.

---

## **Assigning IP Addresses**

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

The options available for assigning IP addresses to access points are:

- Using an [IP address pool](#) from the Enterprise Management Console, indicated by enabling the **Assign from IP Address Pool** checkbox
- Using a DHCP server, as indicated by selecting the **Assign from DHCP Server** option
- Assigning at the device level, indicated by selecting the **No Assignment** option

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

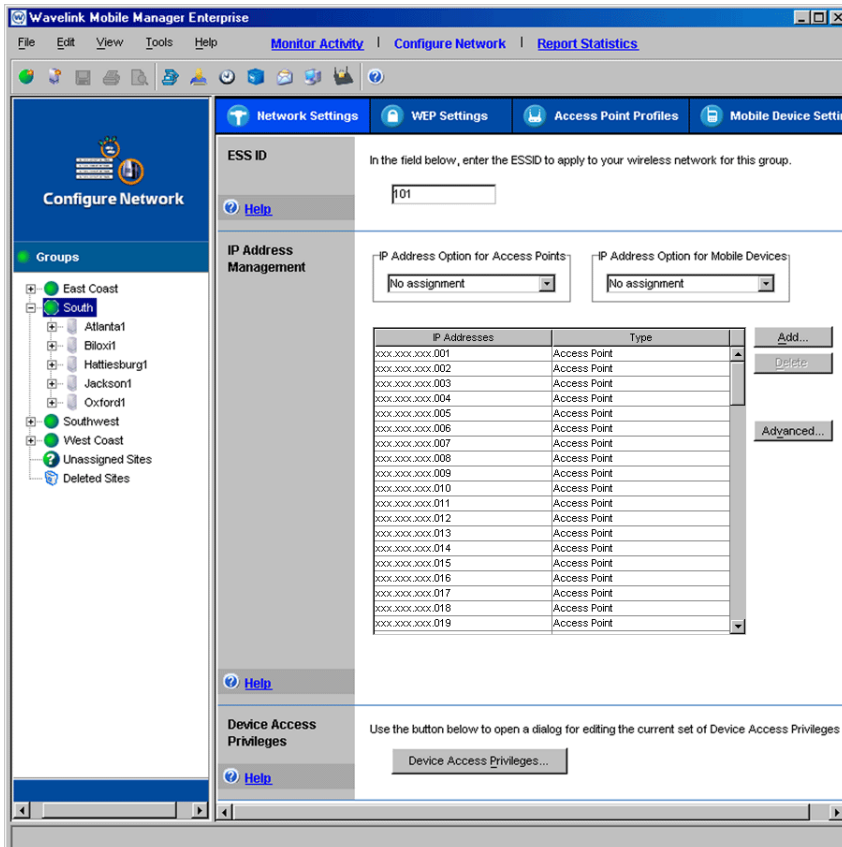
- Using an **IP address pool** from the Enterprise Management Console, indicated by enabling the **Assign from IP Address Pool** checkbox
- Using the Avalanche Management Console at the site level, indicated by selecting the **Assign Using Site Tool** option
- Assigning at the device level, indicated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

IP addresses generated using the Enterprise Management Console 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 Management Console, each affected Agent removes the corresponding IP address from its IP address pool. See *Overview of Assigning IP Addresses* on page 207 for information on how the Enterprise Management Console deploys IP addresses on an enterprise-wide level.

---

**NOTE** To assign newly-added IP addresses to access points or mobile devices, you must ensure that the relevant devices are configured to receive IP addresses from an IP address pool.

---



**Figure 6-2.** 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 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 Management Console. By default, the Enterprise Management Console 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 Management Console, 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 198 for more information.

- 5 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.
- 6 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.

---

- 7 Select whether you want these IP addresses to apply to access points or mobile devices.
- 8 Click `OK`.
- 9 Select `Save Group` from the **File** menu.

The Enterprise Management Console 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 Management Console 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 Management Console, 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 Management Console removes the IP address from the IP address pool.

## Modifying Subnet Masks and Gateway IP Addresses

The Enterprise Management Console 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 Management Console 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 Management Console, the IP addresses that you can add to an IP address pool is restricted by the subnet mask you create. See *Assigning IP Addresses* on page 208 for more information.

**To modify a subnet mask or gateway IP address:**

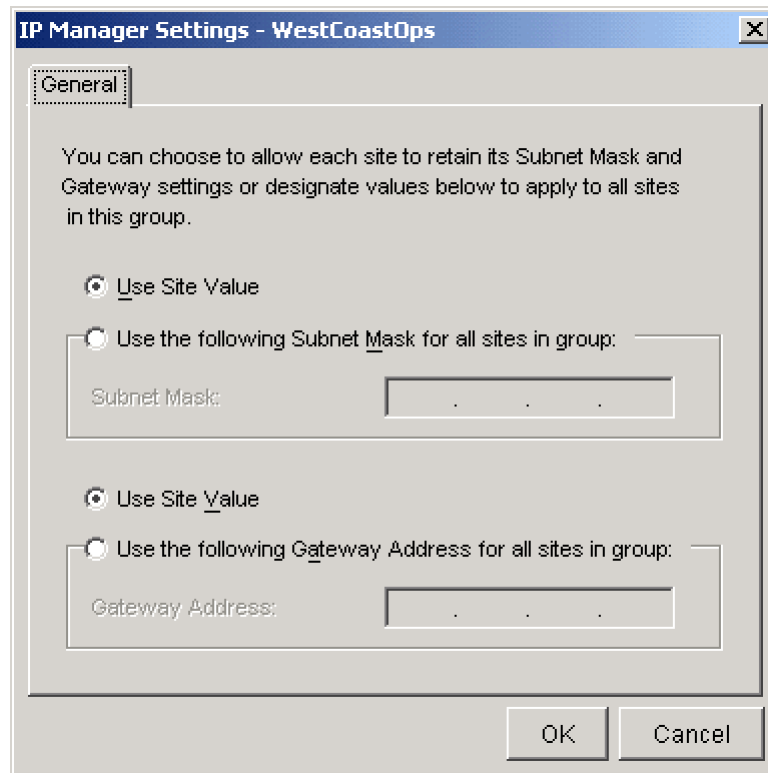
- 1 Select a group from the Groups window.

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 IP Address Management pane.

The *Advanced Network Settings* dialog box appears.



**Figure 6-3.** *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. This option instructs the access point Agent to use the settings assigned to the network card to which it binds. It also instructs the mobile device Agent to use the settings assigned to the first network card on the system on which the Agent is installed.

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. This option instructs the access point Agent to use the settings assigned to the network card to which it binds. It



also instructs the mobile device Agent to use the settings assigned to the first network card on the system on which the Agent is installed.

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.

### **Assigning a Mobile Device Agent to Mobile Devices**

The Enterprise Management Console allows you to modify the mobile device Agent IP address for all mobile devices in a group. This IP address is stored on each mobile device and determines which Agent the device tries to associate with. These settings override their corresponding settings at the site level.

Unless you are using one mobile device Agent for all sites in the group, it is recommended that you allow the mobile device Agent IP address to be set at the site level.

#### **To modify the mobile device Agent IP address:**

- 1 Select a group from the Groups window.

The mobile device Agent IP address that you create will apply to all mobile devices managed within the selected group.

- 2 Select `Configure Network`.
- 3 Click the **Network Settings** tab.
- 4 Click `Advanced`.

This button is located in the IP Address Management pane.

The *Advanced Network Settings* dialog box appears.

- 5 Select the **Mobile Device Settings** tab.

The following dialog box appears.

**Figure 6-4.** *The Mobile Device Settings Tab*

**6** Select an option for the assignment of the mobile device Agent IP address.

If you want the mobile devices in the group to use the mobile device Agent specified by the mobile device Agent at the site level, enable the **Use Site Value** option.

If you want to define a mobile device Agent IP address for all mobile devices in the group, enable the **Use the Following Agent for all your devices** option, then type the IP address or hostname in the **Agent IP/ Hostname** text box. Leave the text box blank if you do not want to supply the mobile devices with an Agent address.

- 7 Select an option for the assignment of the mobile device DNS settings.

If you want the mobile devices in the group to use the DNS settings defined at the site level (using the mobile device site tool), enable the **Use Site Value** option.

If you want to define DNS settings for all mobile devices in the group, enable the **Use the Following DNS Settings for all your devices** option, then configure the DNS name and the IP addresses for the primary, secondary, and tertiary DNS server. Leave text boxes blank if they are not needed.

- 8 Click **OK**.
- 9 Select **Save Group** from the **File** menu.

## Deploying Network Settings

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

- Deploying Settings for All Devices
- Deploying Access Point Settings
- Deploying Mobile Device Settings

### Deploying Settings for All Devices

Under most circumstances, you will want to deploy network settings to both access points and mobile devices simultaneously. Deploying settings simultaneously prevents any inconsistencies between the configurations for mobile devices and access points, which can hinder network performance.

When you deploy settings for all devices, you send the following information to each Agent within the selected sites or groups:

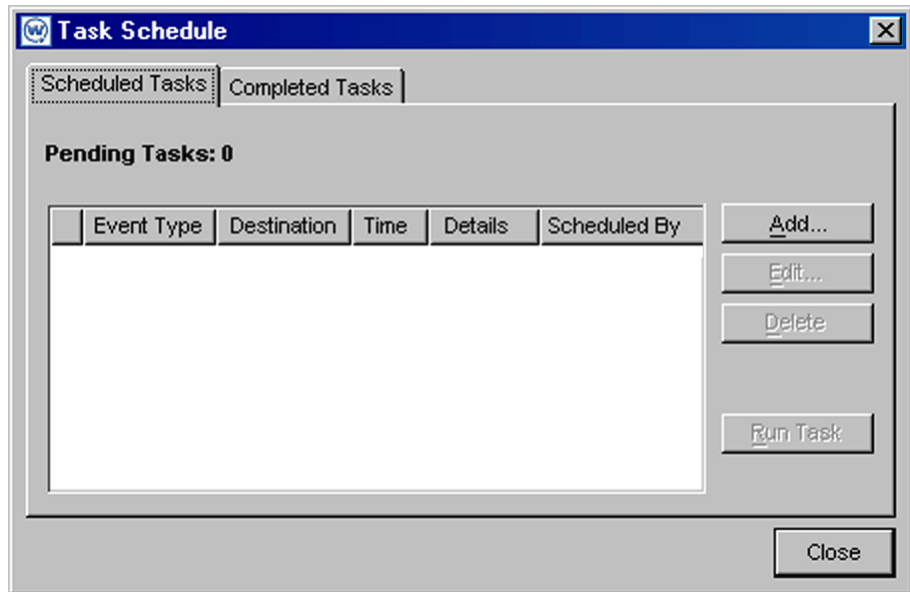
- ESS IDs
- IP addresses
- Mobile device information (such as when to release licenses)

- Device access privileges
- WEP settings

**To deploy settings for all devices:**

- 1 Select `Task Schedule` from the **Tools** menu.

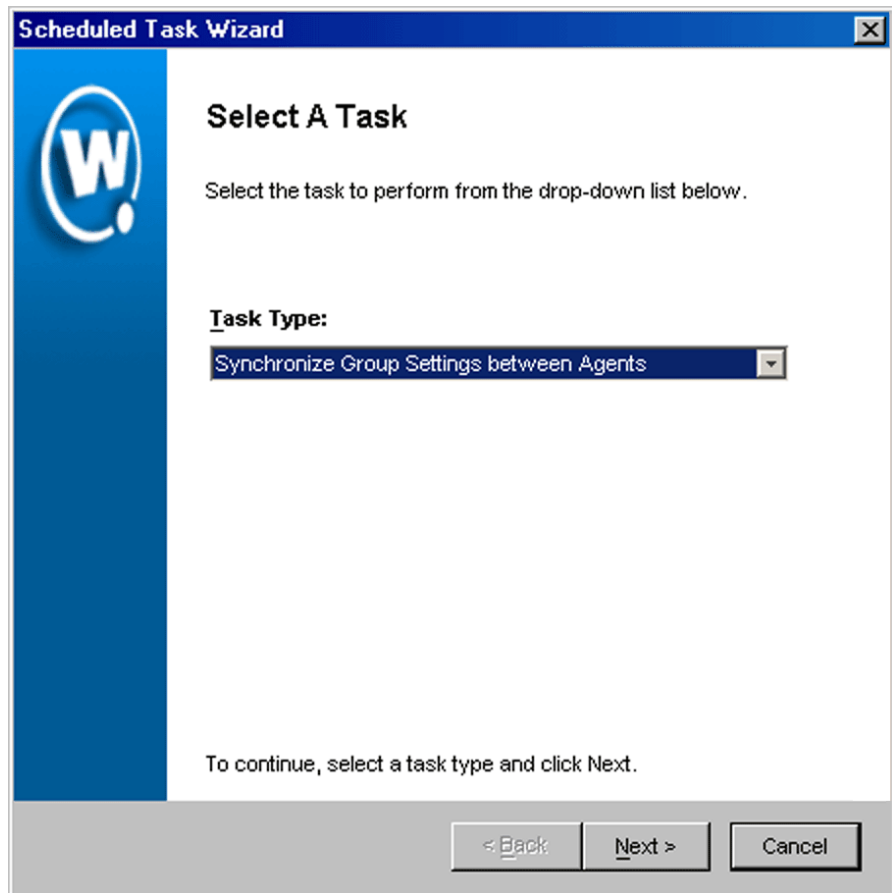
The *Task Schedule* dialog box appears.



**Figure 6-5.** *The Task Schedule Dialog Box*

- 2 Click `Add`.

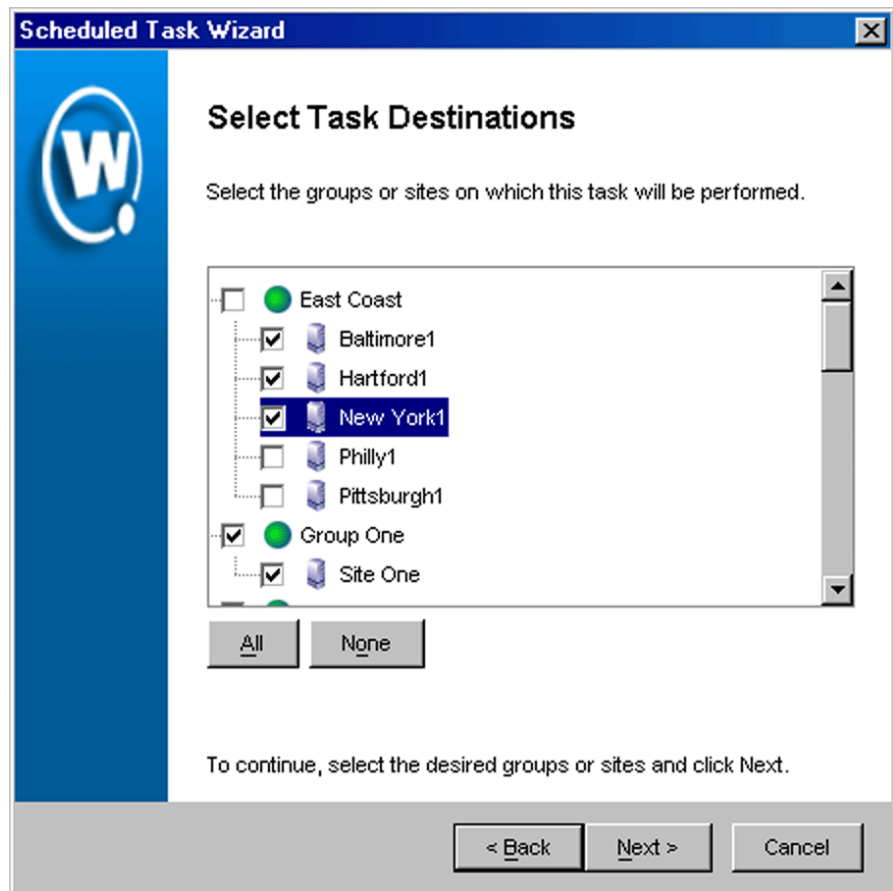
The *Select A Task* dialog box appears.



**Figure 6-6.** *The Select a Task Dialog Box*

- 3 Select **Synchronize Group Settings between Agents** from the **Task Type** list and click **Next**.

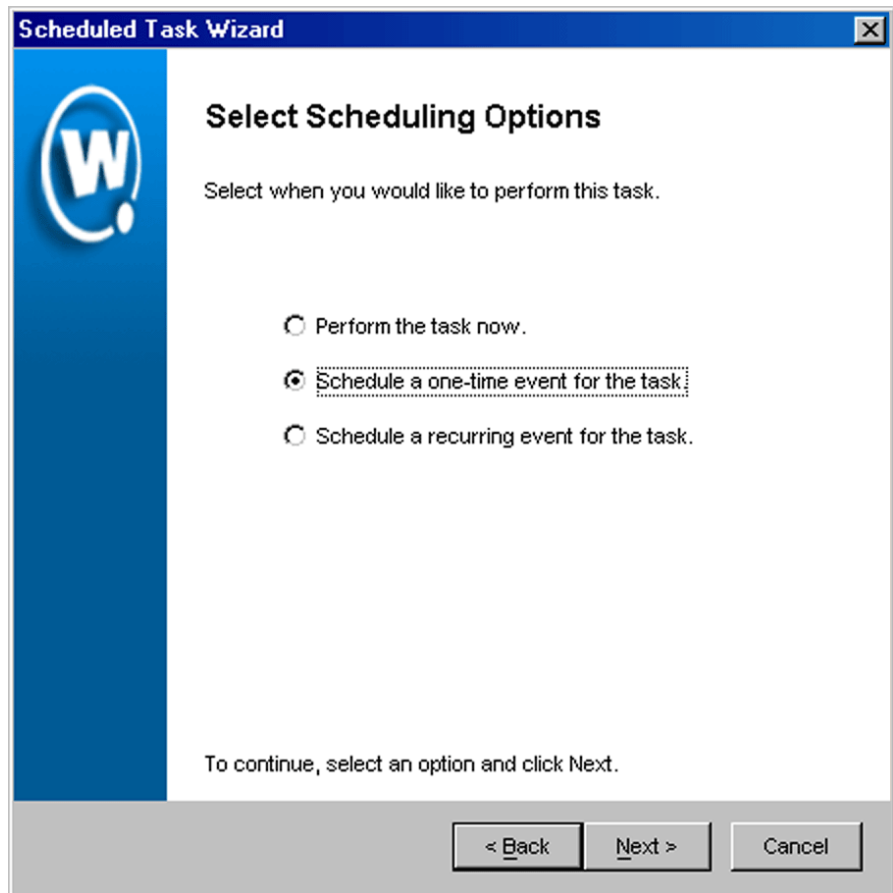
The *Select Task Destination* dialog box appears.



**Figure 6-7.** The Select Task Destination Dialog Box

- 4 Select the groups or sites by enabling the checkbox next to the group or site name. You can also select all groups by clicking `All`.
- 5 Click `Next`.

The *Select Scheduling Options* dialog box appears.



**Figure 6-8.** *The Select Scheduling Options Dialog Box*

**6** Determine when the event will occur.

If you want the event to occur immediately select the **Perform the task now** option.

If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

If you want the event to occur on a regular basis, select the **Schedule a recurring event** for this task option.

- 7 Click **Next**.
- 8 If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.

**Figure 6-9.** *The Schedule the Time Window Dialog Box*

Within this dialog box, you can set the following parameters for the event:

- Select the start date and time for the event.
- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete**



option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.
- 9** If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

**Scheduled Task Wizard**

## Configure Task Recurrence

Use the controls below to configure the recurrence settings

**Task time**

Start Time:   Run until complete  Use Site's Local Time  
 End by:

**Recurrence pattern**

Daily  Weekly  Monthly

Recur every  week(s) on:

Sunday  Monday  Tuesday  Wednesday  
 Thursday  Friday  Saturday

**Range of recurrence**

Start:   No end date  
 End by:

To continue, click Next.

< Back    Next >    Cancel

**Figure 6-10.** *The Configure Task Recurrence Dialog Box*

Within this dialog box, you can set the following parameters for this event:

- Select the start time for the event.
- Determine when you want the event to stop. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

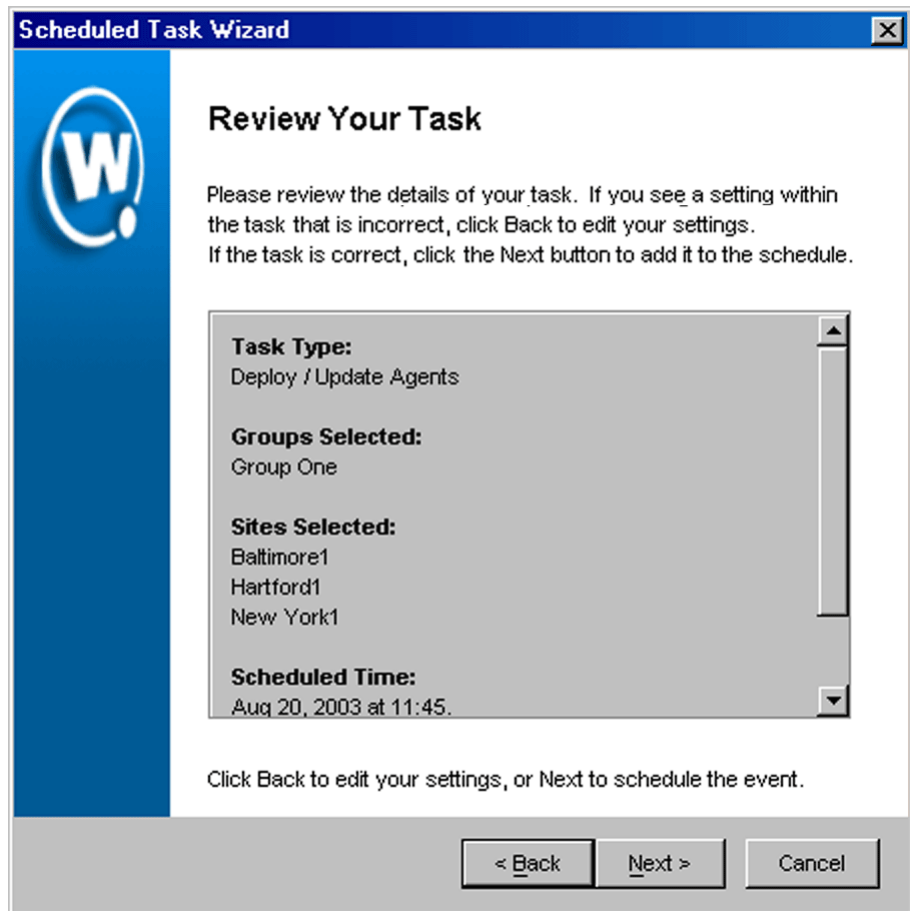
---

**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

**10** Click *Next*.

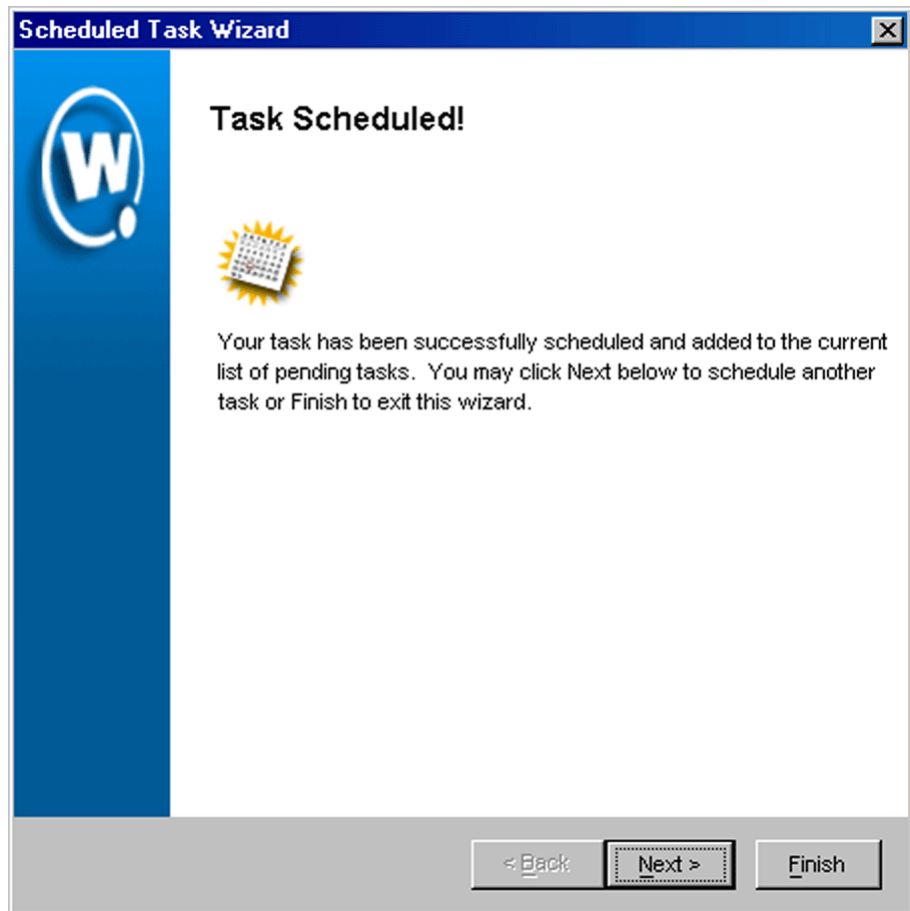
The *Review Your Task* dialog box appears.



**Figure 6-11.** *The Review Your Task Dialog Box*

**11** Review your the task to ensure that it is correct and click `Next`.

The *Task Scheduled* dialog box appears.



**Figure 6-12.** *The Task Scheduled Dialog Box*

- 12 Click `Next` to schedule a new event, or click `Finish` to return to the Task Schedule dialog box.

## Deploying Access Point Settings

This section describes how to apply network settings to the access points within a given group.

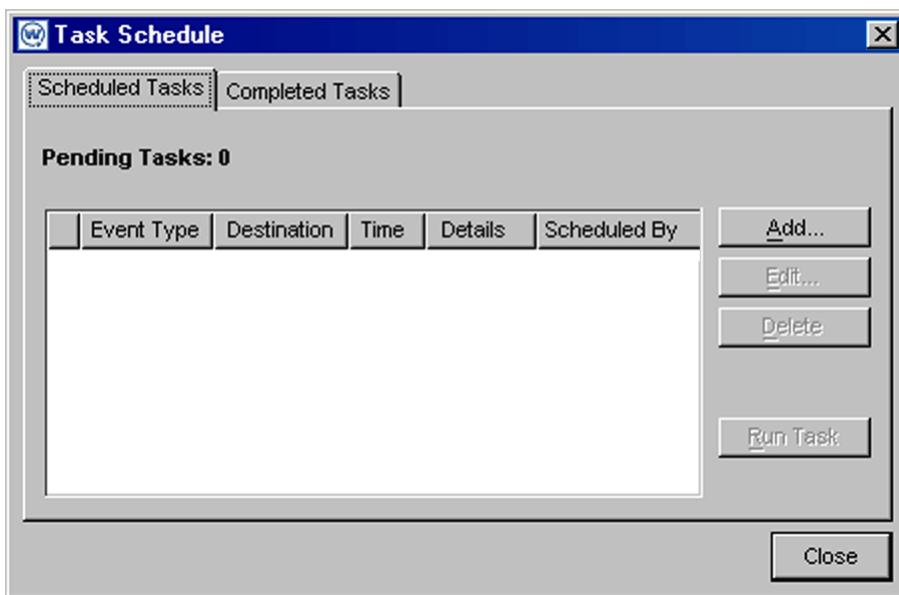
---

**NOTE** If you plan on deploying settings to both access points and mobile devices, it is highly recommended you follow the steps described in *Deploying Settings for All Devices* on page 217.

---

**To deploy access point settings:**

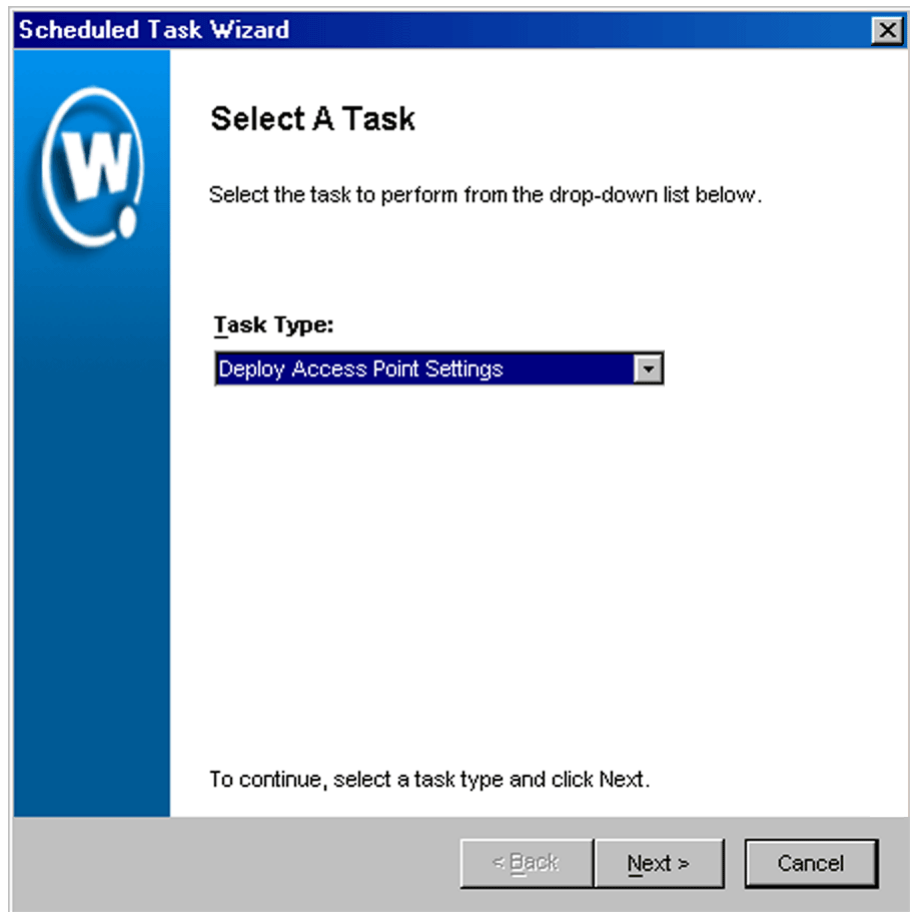
- 1 Select **Task Schedule** from the **Tools** menu.
- 2 The *Task Schedule* dialog box appears.



**Figure 6-13.** *The Task Schedule Dialog Box*

- 3 Click **Add**.

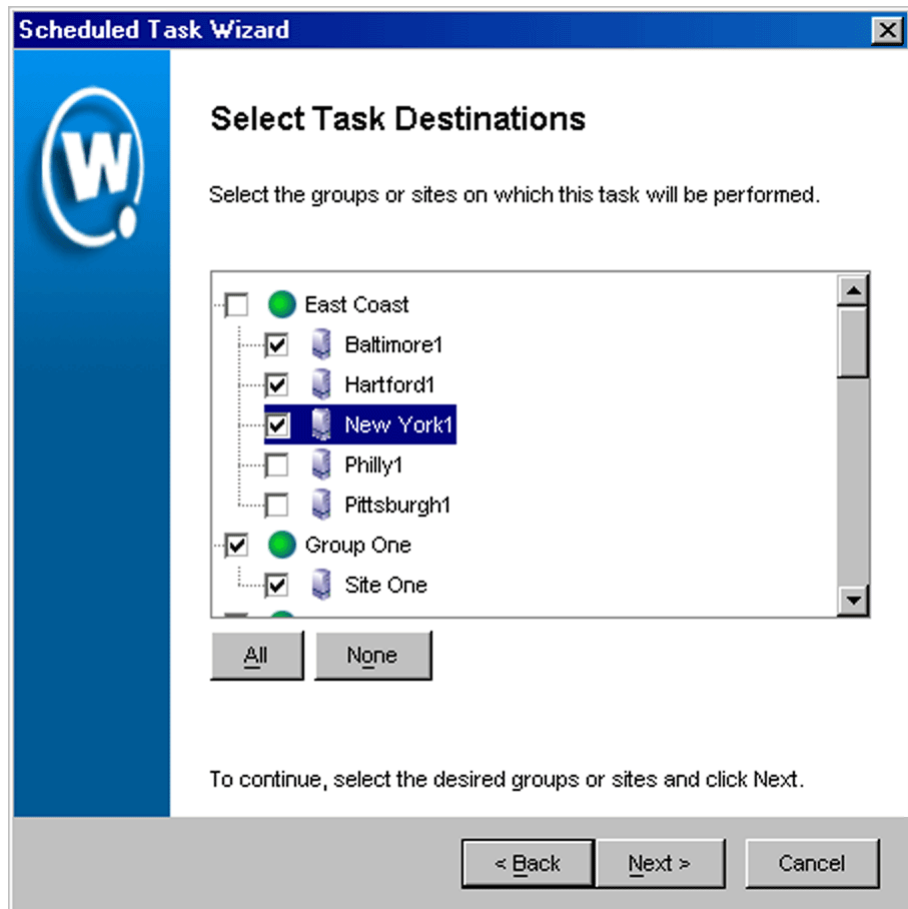
The *Select A Task* dialog box appears.



**Figure 6-14.** *The Select a Task Dialog Box*

- 4 Select **Deploy Access Point Settings** from the **Task Type** list and click **Next**.

The *Select Task Destination* dialog box appears.



**Figure 6-15.** *The Select Task Destination Dialog Box*

- 5 Select the groups or sites by enabling the checkbox next to the group or site name. You can also select all groups by clicking `All`.
- 6 Click `Next`.

The *Select Settings to Deploy* dialog box appears.

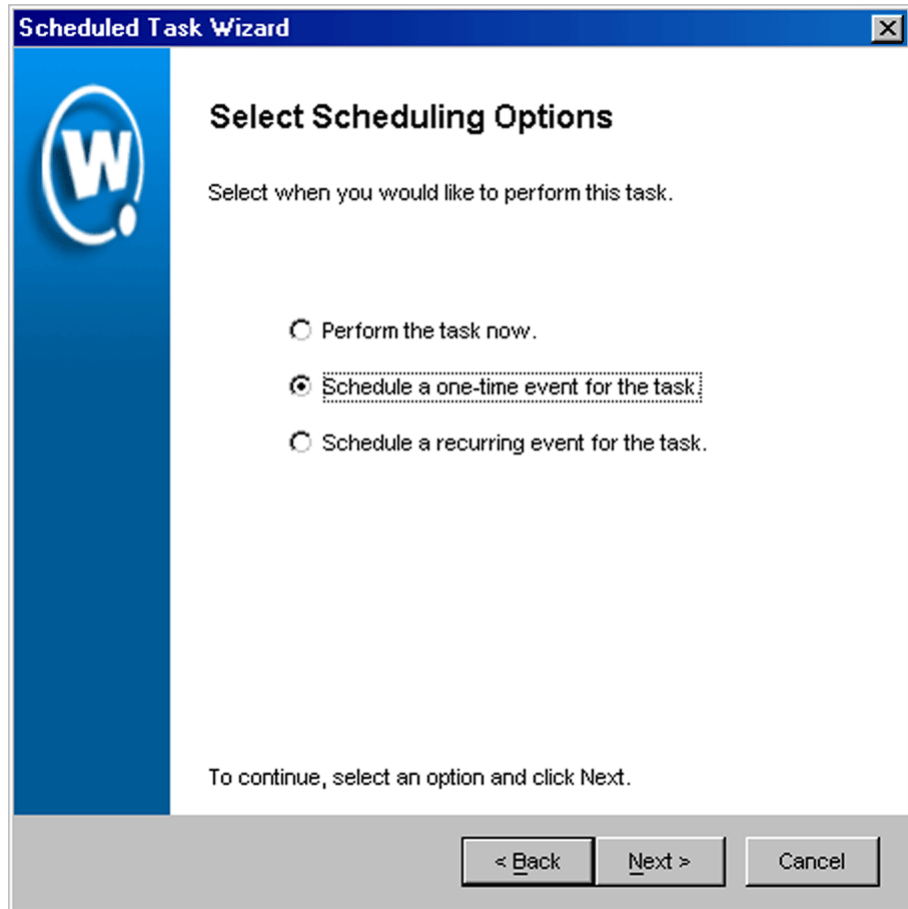




**Figure 6-16.** *The Select Settings to Deploy Dialog Box*

- 7 Select the **Update Network Settings and Security Settings only** option.
- 8 Click **Next**.

The *Select Scheduling Options* dialog box appears.



**Figure 6-17.** *The Select Scheduling Options Dialog Box*

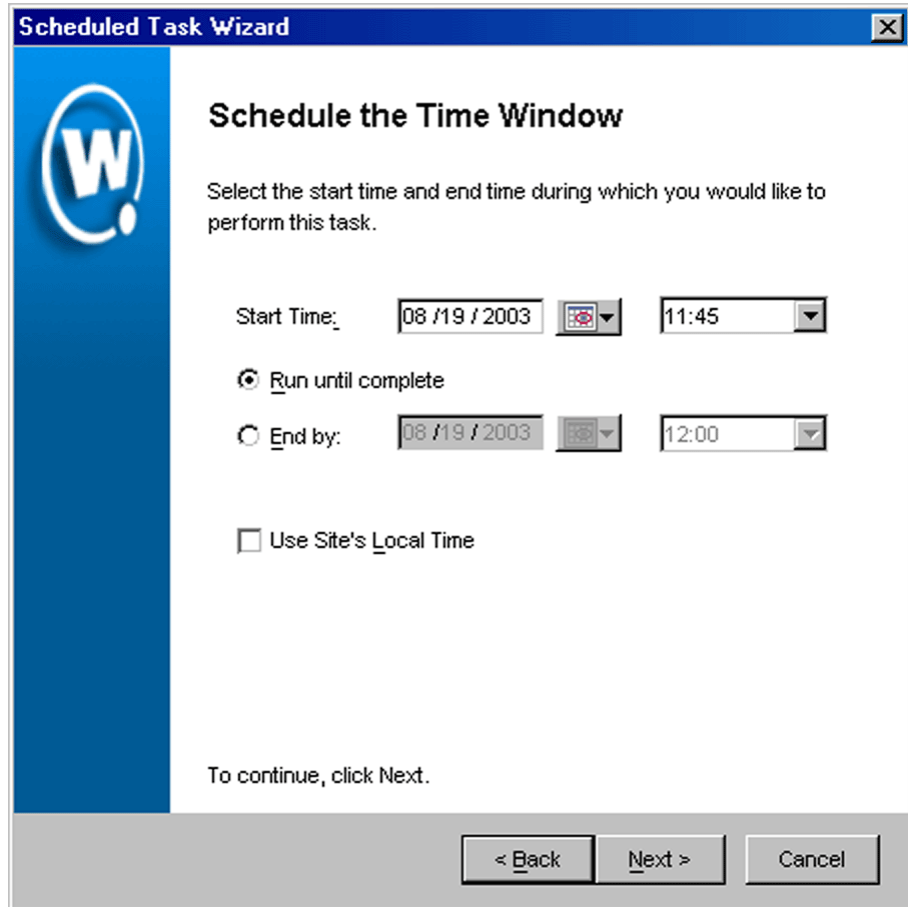
**9** Determine when the event will occur.

If you want the event to occur immediately, select the **Perform the task now** option.

If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

If you want the event to occur on a regular basis, select the **Schedule a recurring event** for this task option.

- 10 Click **Next**.
- 11 If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.

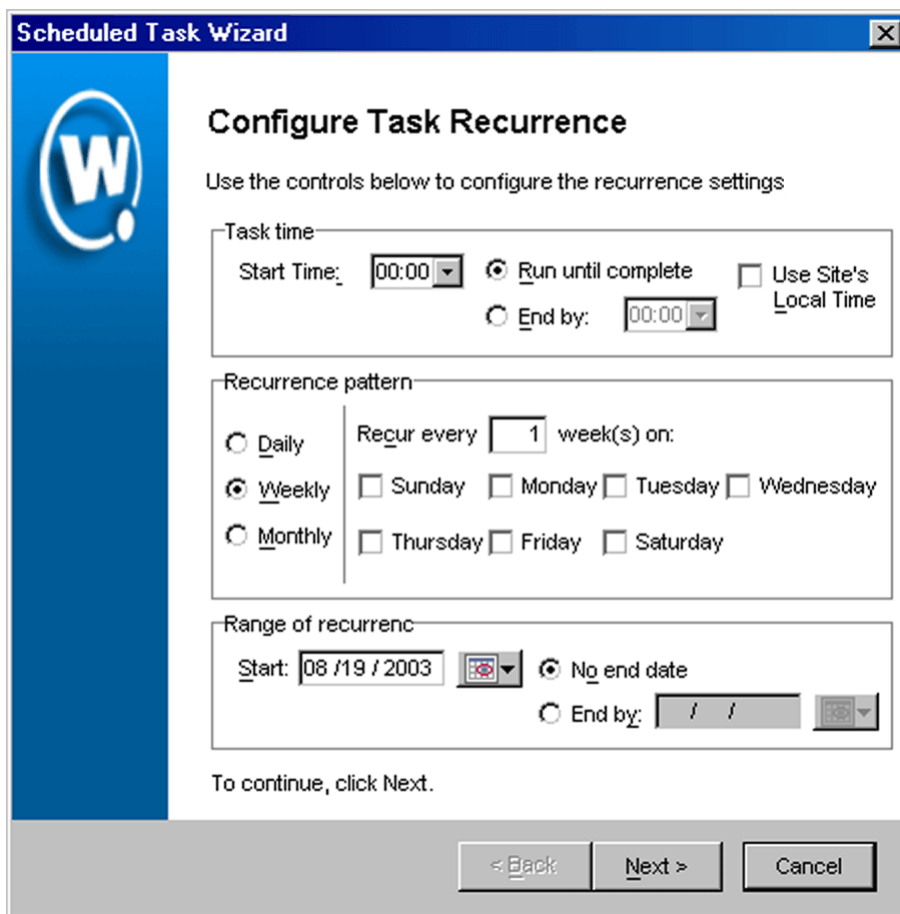


**Figure 6-18.** *The Schedule the Time Window Dialog Box*

Within this dialog box, you can set the following parameters for the event:

- Select the start date and time for the event.

- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.
  - If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.
- 12** If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.



**Figure 6-19.** The Configure Task Recurrence Dialog Box

Within this dialog box, you can set the following parameters for this event:

- Select the start time for the event.
- Determine when you want the event to stop. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

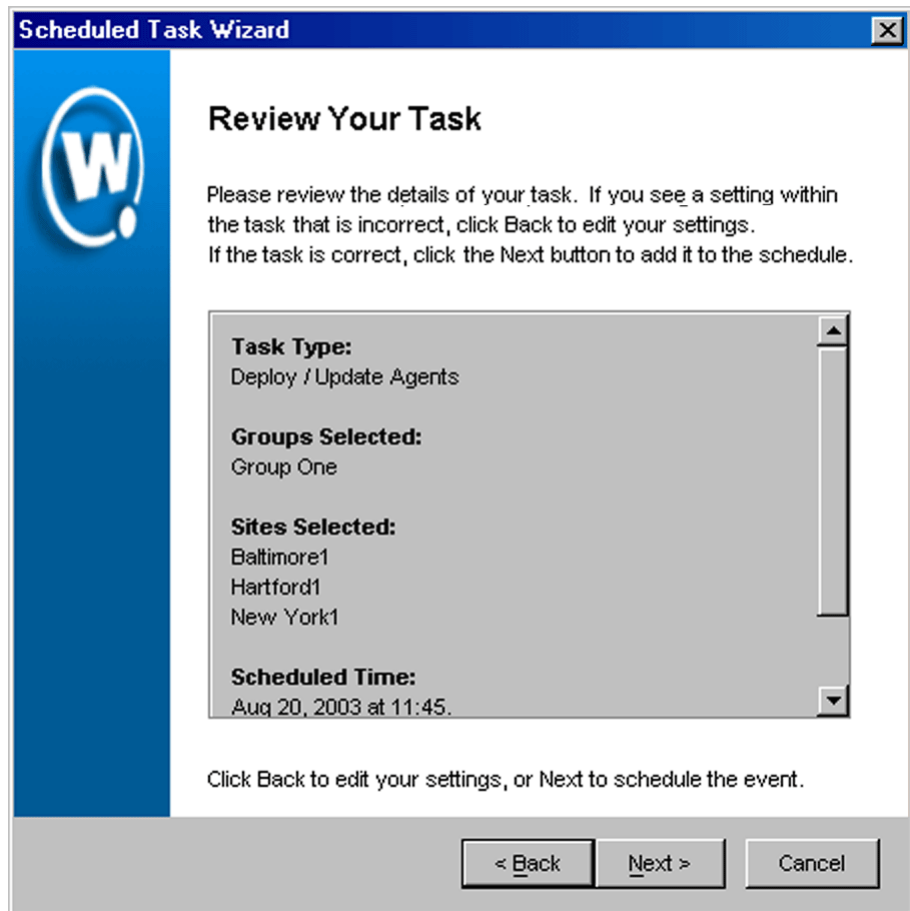
---

**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

**13** Click *Next*.

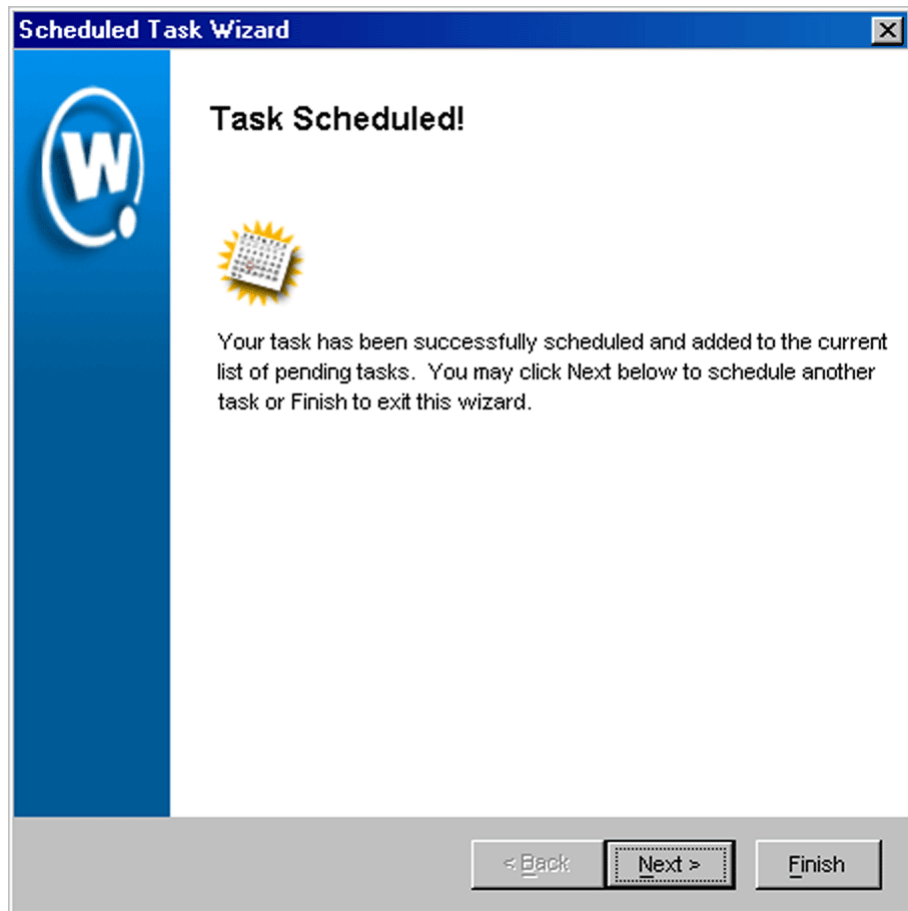
The *Review Your Task* dialog box appears.



**Figure 6-20.** *The Review Your Task Dialog Box*

**14** Review your the task to ensure that it is correct and click `Next`.

The *Task Scheduled* dialog box appears.



**Figure 6-21.** *The Task Scheduled Dialog Box*

- 15 Click `Next` to schedule a new event, or click `Finish` to return to the Task Schedule dialog box.

## Deploying Mobile Device Settings

This section describes how to apply network settings to the mobile devices within a given group.



---

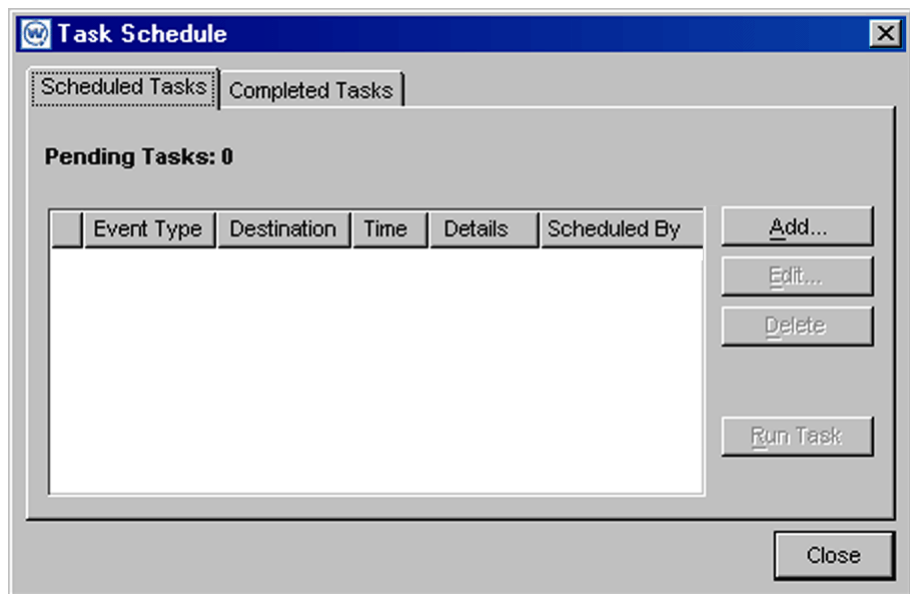
**NOTE** If you plan on deploying settings to both access points and mobile devices, it is highly recommended you follow the steps described in *Deploying Settings for All Devices* on page 217.

---

**To deploy mobile device settings:**

- 1 Select **Task Schedule** from the **Tools** menu.

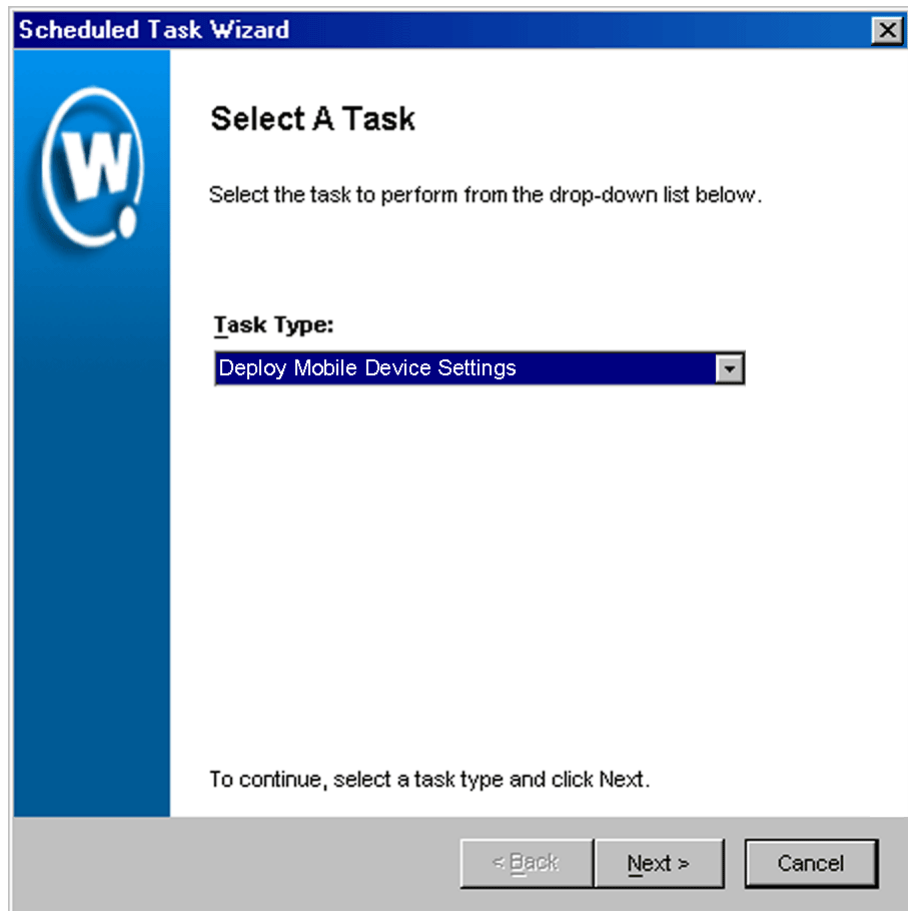
The *Task Schedule* dialog box appears.



**Figure 6-22.** *The Task Schedule Dialog Box*

- 2 Click **Add**.

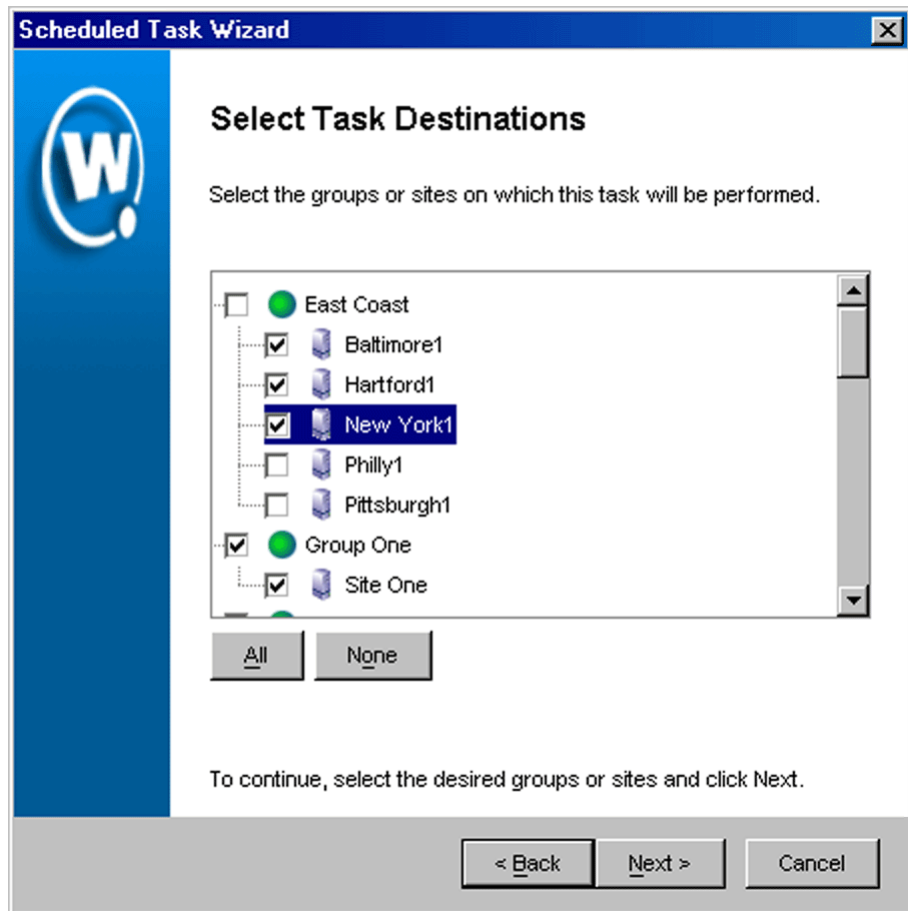
The *Select A Task* dialog box appears.



**Figure 6-23.** *The Select a Task Dialog Box*

- 3 Select **Deploy Mobile Device Settings** from the **Task Type** list and click **Next**.

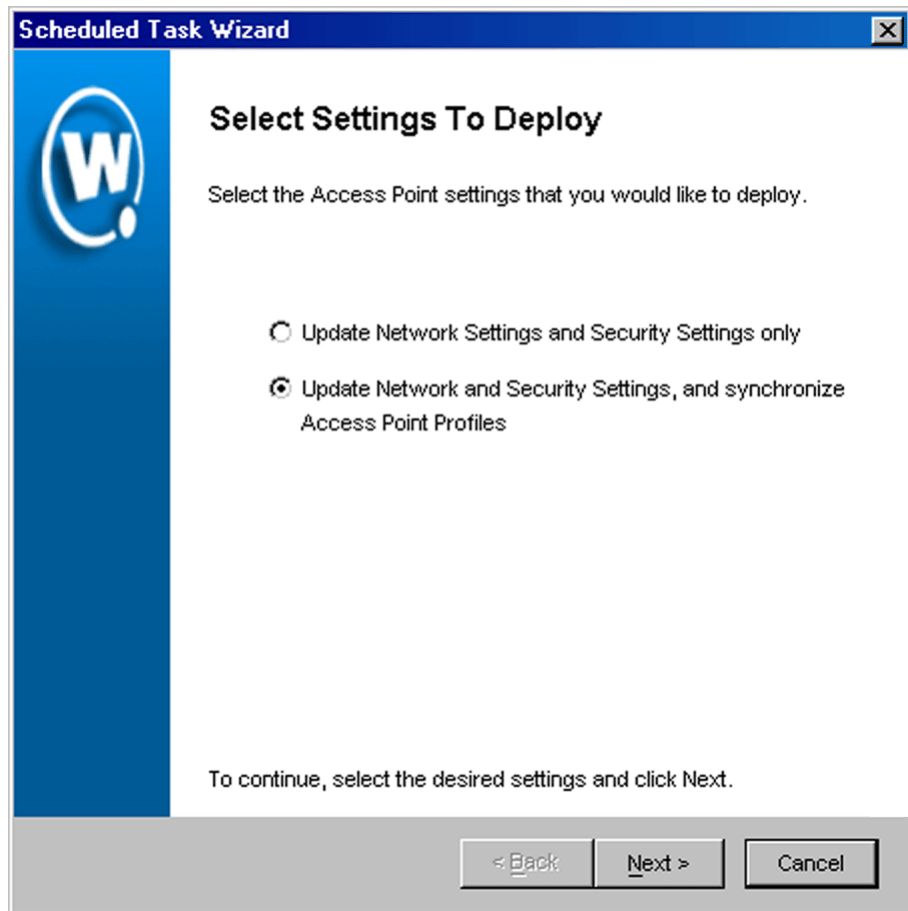
The *Select Task Destination* dialog box appears.



**Figure 6-24.** *The Select Task Destination Dialog Box*

- 4 Select the groups or sites by enabling the checkbox next to the group or site name. You can also select all groups by clicking `All`.
- 5 Click `Next`.

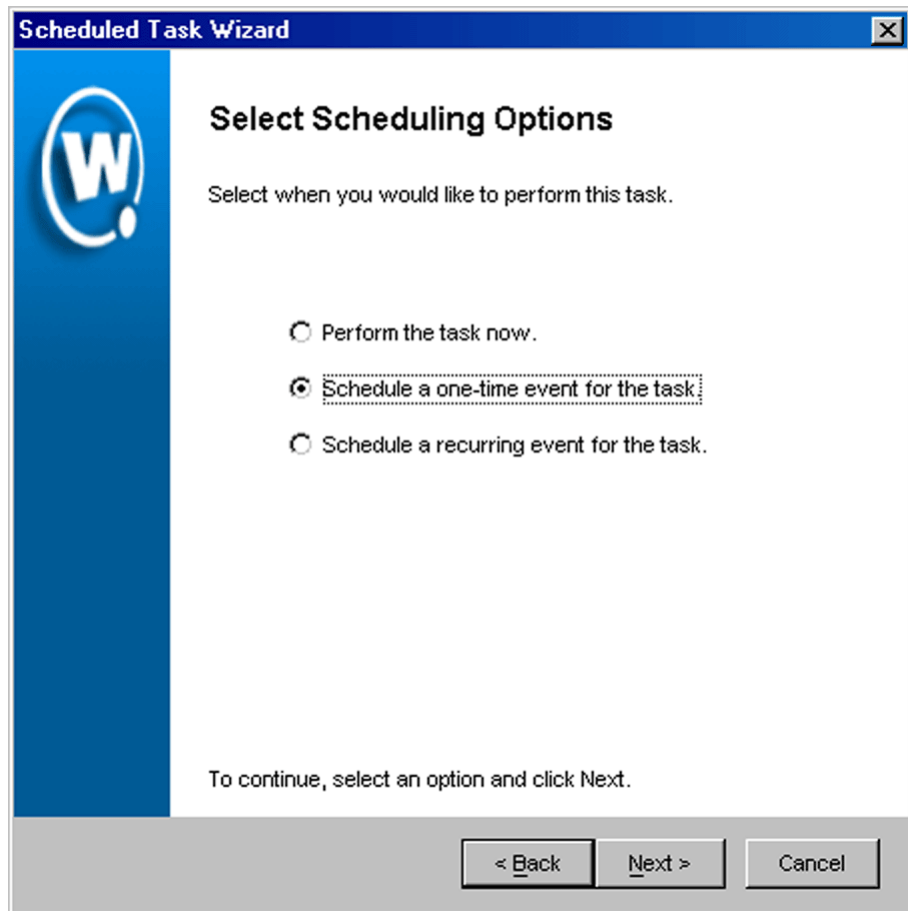
The *Select Settings to Deploy* dialog box appears.



**Figure 6-25.** *The Select Settings to Deploy Dialog Box*

- 6** Select the **Update Network Settings and Security Settings only** option.
- 7** Click **Next**.

The *Select Scheduling Options* dialog box appears.



**Figure 6-26.** *The Select Scheduling Options Dialog Box*

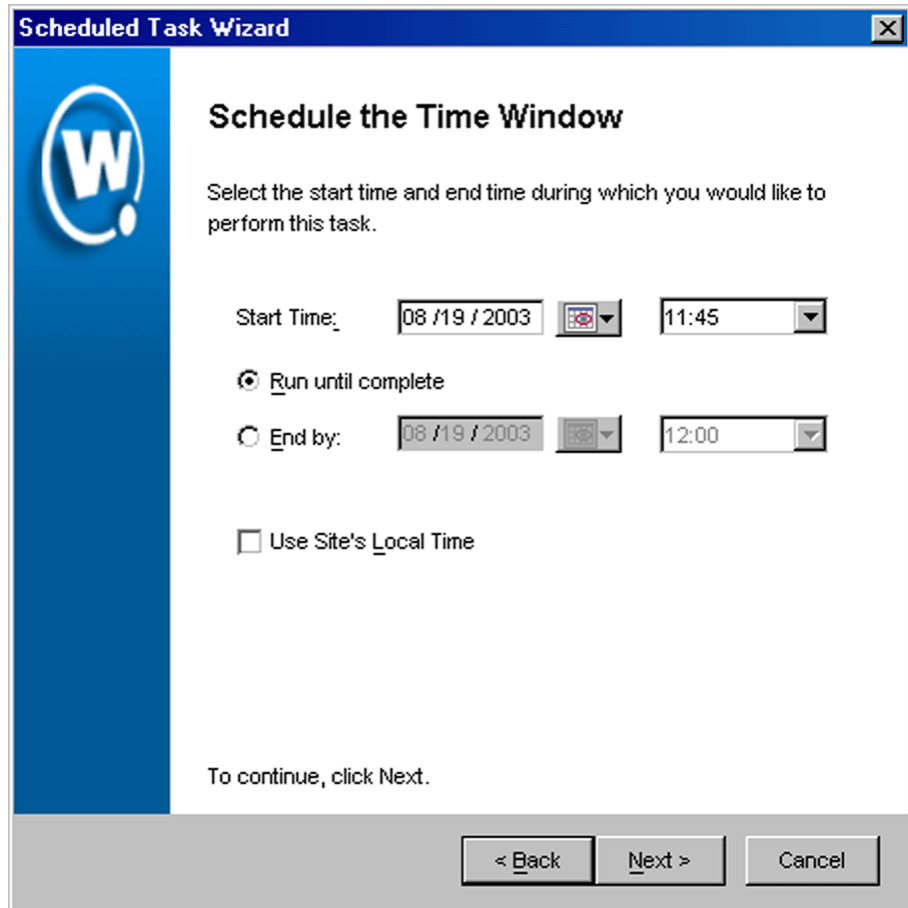
**8** Determine when the event will occur.

If you want the event to occur immediately, select the **Perform the task now** option.

If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

If you want the event to occur on a regular basis, select the **Schedule a recurring event** for this task option.

- 9 Click **Next**.
- 10 If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.



The screenshot shows a dialog box titled "Scheduled Task Wizard" with a close button in the top right corner. On the left side, there is a blue vertical bar containing a white circular logo with a stylized "W". The main content area is white and has the title "Schedule the Time Window". Below the title, there is a text instruction: "Select the start time and end time during which you would like to perform this task." The form contains several input fields and controls: "Start Time:" followed by a date field containing "08 /19 /2003", a calendar icon, and a time field containing "11:45"; a radio button labeled "Run until complete" which is selected; another radio button labeled "End by:" followed by a date field containing "08 /19 /2003", a calendar icon, and a time field containing "12:00"; and a checkbox labeled "Use Site's Local Time" which is not selected. At the bottom of the dialog box, there is a grey bar containing three buttons: "< Back", "Next >", and "Cancel".

**Figure 6-27.** *The Schedule the Time Window Dialog Box*

Within this dialog box, you can set the following parameters for the event:

- Select the start date and time for the event.

- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.
  - If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.
- 11** If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

**Scheduled Task Wizard**

### Configure Task Recurrence

Use the controls below to configure the recurrence settings

**Task time**

Start Time: 00:00  Run until complete  Use Site's Local Time

End by: 00:00

**Recurrence pattern**

Daily Recur every 1 week(s) on:

Weekly  Sunday  Monday  Tuesday  Wednesday

Monthly  Thursday  Friday  Saturday

**Range of recurrence**

Start: 08 / 19 / 2003  No end date

End by: / /

To continue, click Next.

< Back Next > Cancel

**Figure 6-28.** The Configure Task Recurrence Dialog Box

Within this dialog box, you can set the following parameters for this event:

- Select the start time for the event.
- Determine when you want the event to stop. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.



- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

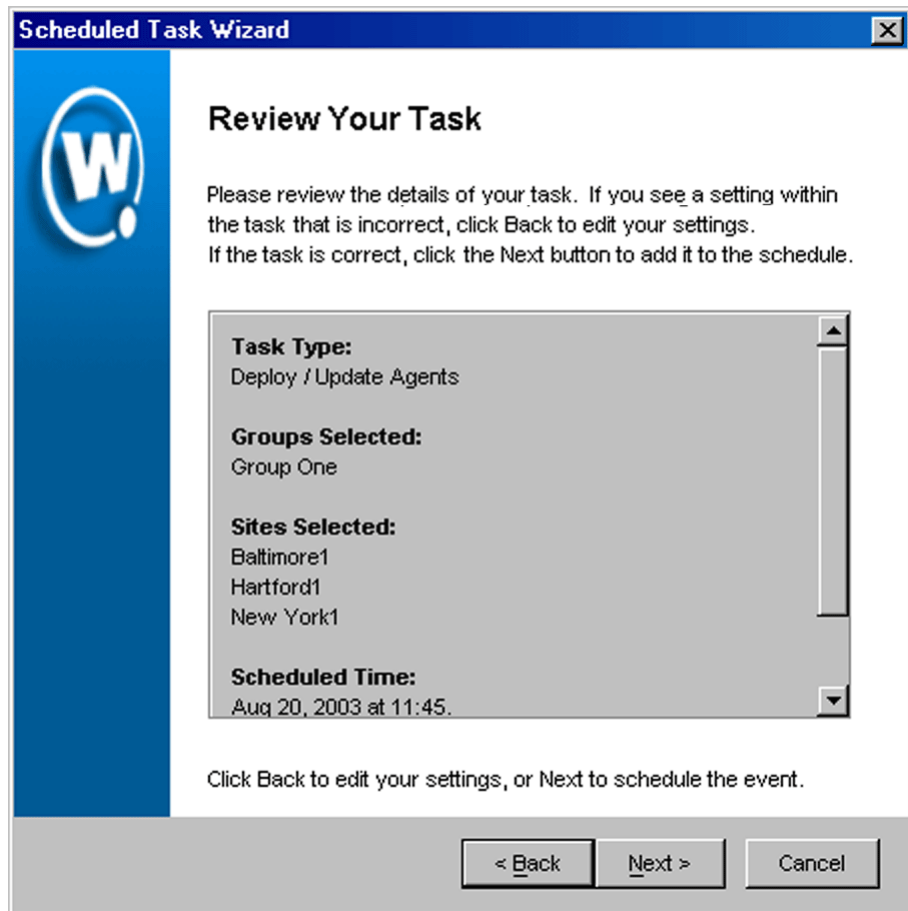
---

**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

**12** Click *Next*.

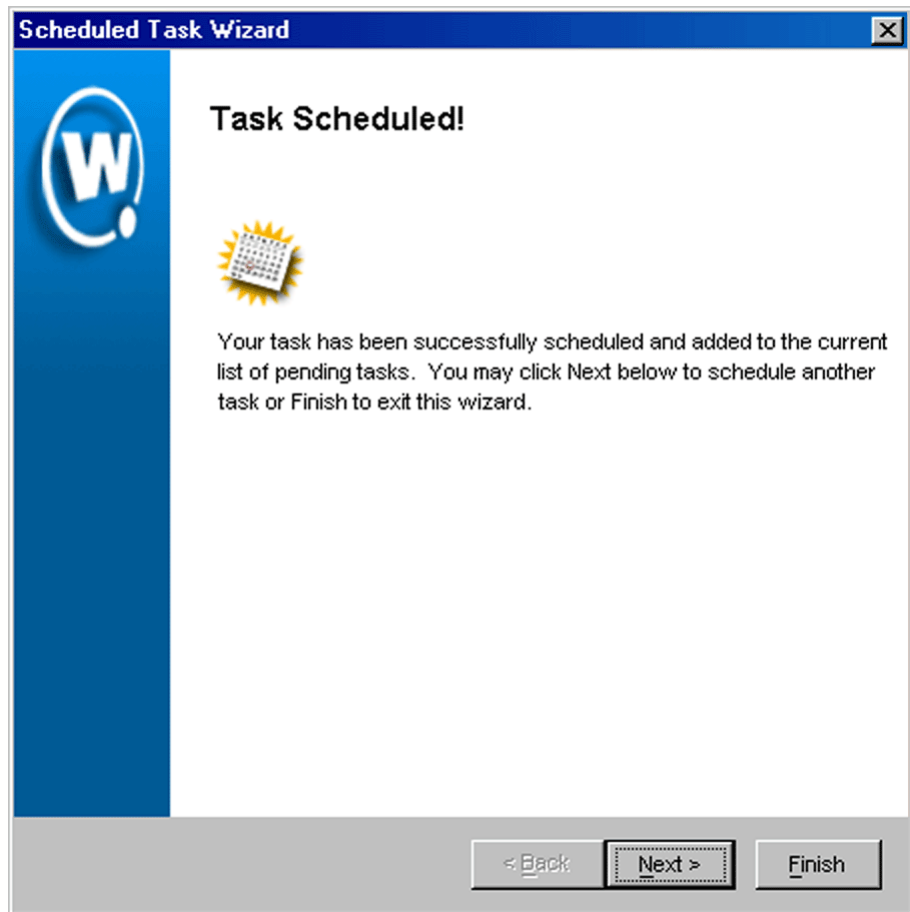
The *Review Your Task* dialog box appears.



**Figure 6-29.** *The Review Your Task Dialog Box*

**13** Review your the task to ensure that it is correct and click `Next`.

The *Task Scheduled* dialog box appears.



**Figure 6-30.** *The Task Scheduled Dialog Box*

- 14 Click `Next` to schedule a new event, or click `Finish` to return to the Task Schedule dialog box.



## Chapter 7: Managing Mobile Devices

Mobile Manager allows you to manage the software and network settings of the mobile devices operating on the network. Within the Enterprise Management Console, mobile device settings are divided into several groups:

- **Group-based settings.** These settings apply to all mobile devices within a specific group that you select from the Groups window. Group-based settings include the ESS ID and IP address assignments. Because the process for configuring these settings applies to both access points and mobile devices, their use is described in *Chapter 6: Managing Network Settings* on page 205.
- **Software management.** Within the Enterprise Management Console, you can install new mobile device applications (called packages) create groups of those packages (called collections) and define the selection criteria that mobile device Agents will use to determine which mobile devices receive which software.
- **Software synchronization.** These settings determine when mobile device software is synchronized between the Enterprise Management Console and one or more mobile device Agents. Software synchronization refers to the process by which Mobile Manager verifies that the software versions managed by the Enterprise Management Console are the same as the software versions managed by individual mobile device Agents.
- **License management.** Licenses for mobile devices are frequently redistributed, providing a great deal of flexibility in managing licenses. Within the Enterprise Management Console, these settings focus on when mobile device licenses are released from an inactive mobile device, allowing that license to move to a new device.
- **COM port settings.** Because mobile devices are frequently connected to cradles when they are not in use, mobile device Agents use COM ports to automatically detect and manage cradled mobile devices. These settings allow you to decide which COM ports mobile device Agents are allowed to use.
- **Authentication.** Mobile Manager includes several different authentication methods to prevent unauthorized mobile devices from accessing your network. These settings are different from Access Control Lists and WEP settings, which are described in *Chapter 8: Managing Security Settings* on page 309.

- **Global settings.** These settings apply to all access points within your network, regardless of their group. These settings are primarily security-based and include settings such as the Access Control List and WEP. Because these settings focus on securing your wireless network, their use is described in *Chapter 8: Managing Security Settings* on page 309.

This section covers the following topics:

- Managing Software
- Synchronizing Mobile Device Software
- Managing Licenses
- Setting COM Ports
- Authenticating Mobile Devices

## Managing Software

The Enterprise Management Console allows you to manage the software installed on your mobile devices. Software management is divided into the following tasks:

- **Creating software collections.** A software collection contains one or more software packages — collections of application files associated with a single mobile device. You create software collections before you install software packages, because each software package must belong to a specific software collection.
- **Installing 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.
- **Defining selection criteria.** The Manage Software view allows you to define specific criteria for each software collection. By defining these criteria, you can instruct Mobile Manager Enterprise to deploy a software package only to specific types of mobile devices.
- **Enabling or Disabling software packages and collection.** By default, any packages you install or collections you create are disabled, to allow you the

opportunity to correctly configure them before sending them to your mobile device Agents. You can enable or disable packages and collections on an as-needed basis.

In addition to the preceding tasks, you can also delete unnecessary software packages and collections, as well as refresh the list of packages and collections to ensure the data you view is up-to-date.

---

**NOTE** Software management applies to all sites and groups.

---

## Creating Software Collections

A software collection contains one or more software packages—collections of application files associated with a single mobile device. You create software collections before you install software packages, because each software package must belong to a specific software collection.

Once you create a software collection, you can apply selection criteria to it. Selection criteria are specific parameters that determine what mobile devices can receive the software packages contained in the software collection.

---

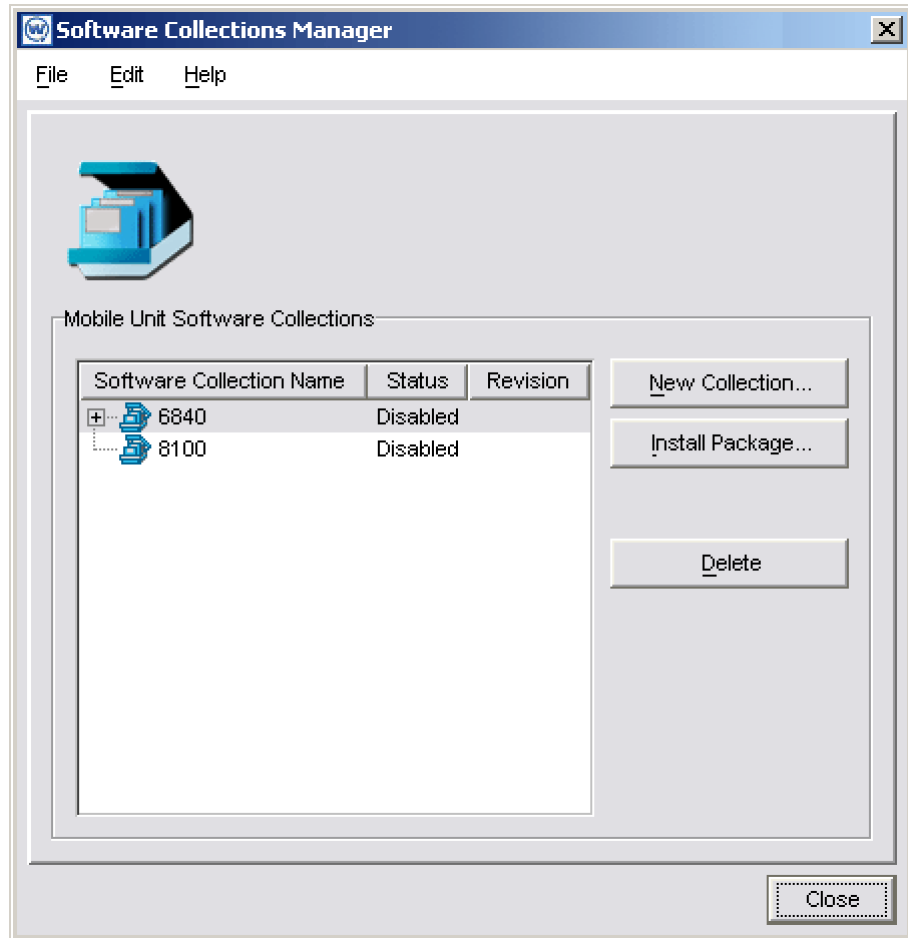
**NOTE** The settings described in this section are global, affecting all groups managed with the Enterprise Management Console.

---

### To create a software collection:

- 1 Select `Software Collections` from the **Tools** menu.

The *Software Collections Manager* dialog box appears.



**Figure 7-1.** *The Software Collections Manager Dialog Box*

- 2 Click **New Collection**.

The *Insert New Collection* dialog box appears.





**Figure 7-2.** *The Insert New Collection Dialog Box*

- 3 Type a name for the new collection and click **OK**.

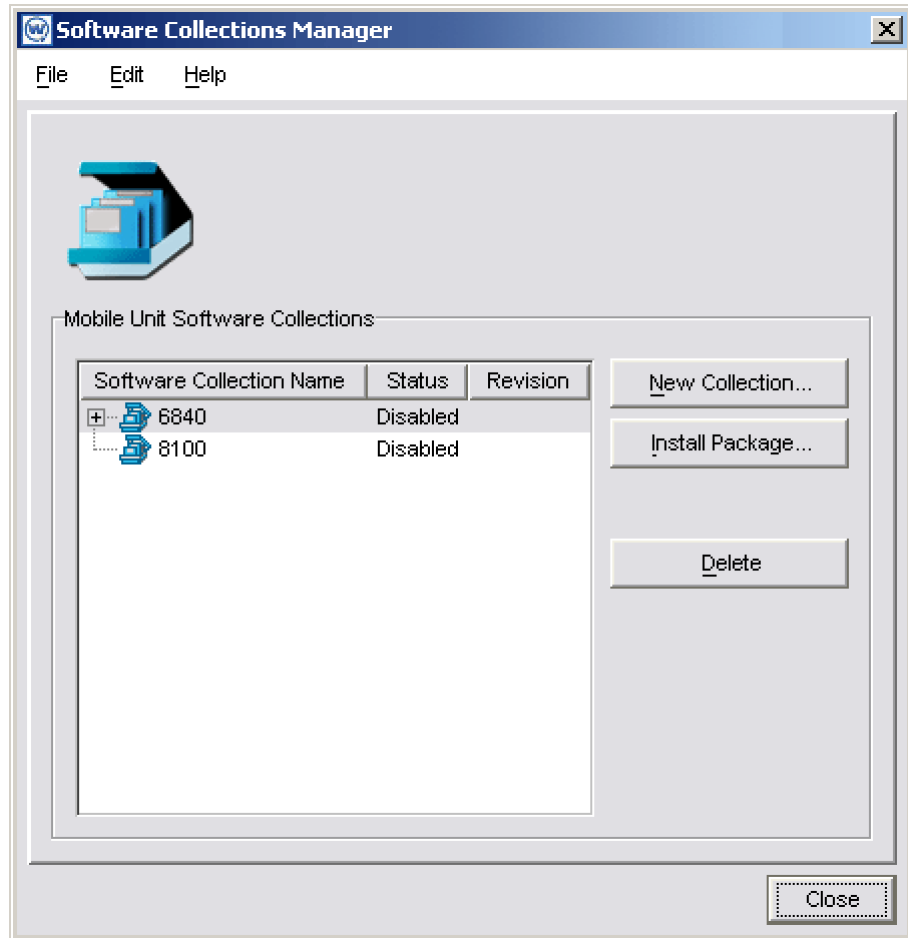
### **Renaming Collections**

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

#### **To rename a collection:**

- 1 Select **Software Collections** from the **Tools** menu.

The *Software Collections Manager* dialog box appears.



**Figure 7-3.** *The Software Collections Manager Dialog Box*

- 2 Select a software collection.
- 3 From the **File** menu of the *Software Manager Collection* dialog box, click *Rename*.

The *Rename Collection* dialog box appears.



**Figure 7-4.** *The Rename Collection Dialog Box*

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

## Installing 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.

---

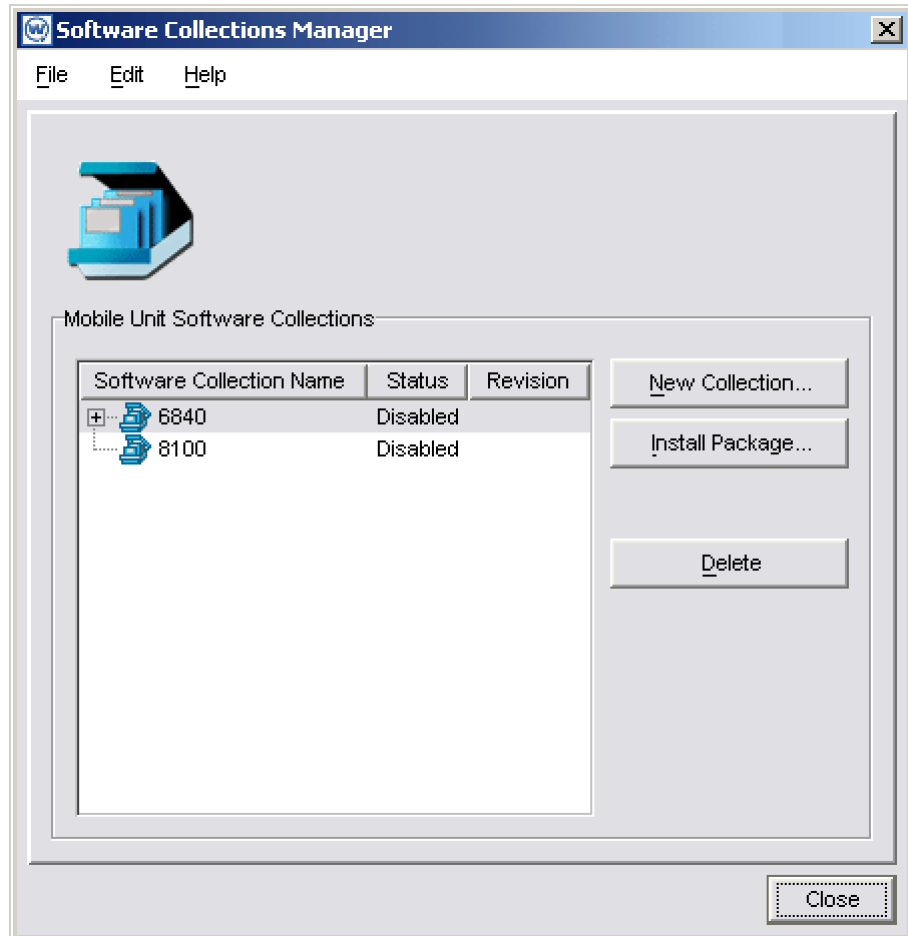
**NOTE** The settings described in this section are global, affecting all groups managed with the Enterprise Management Console.

---

### To install a software package:

- 1 Select `Software Collections` from the **Tools** menu.

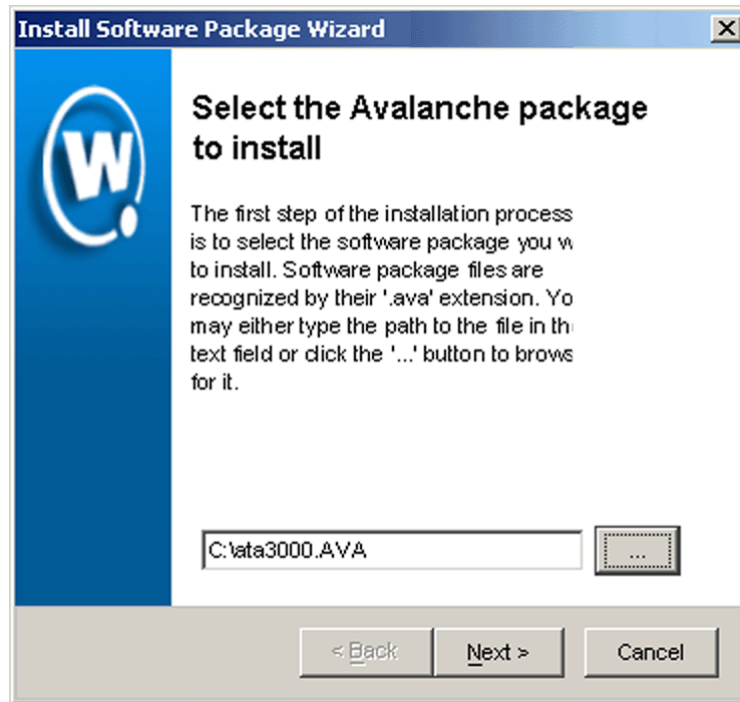
The *Software Collections Manager* dialog box appears.



**Figure 7-5.** *The Software Collections Manager Dialog Box*

2 Click Install Package.

The *Select Avalanche Package to Install* dialog box appears.



**Figure 7-6.** *The Select Avalanche Package to Install Dialog Box*

- 3 Type the path to the Avalanche package you want to install, or click [ . . . ] to browse to the file.

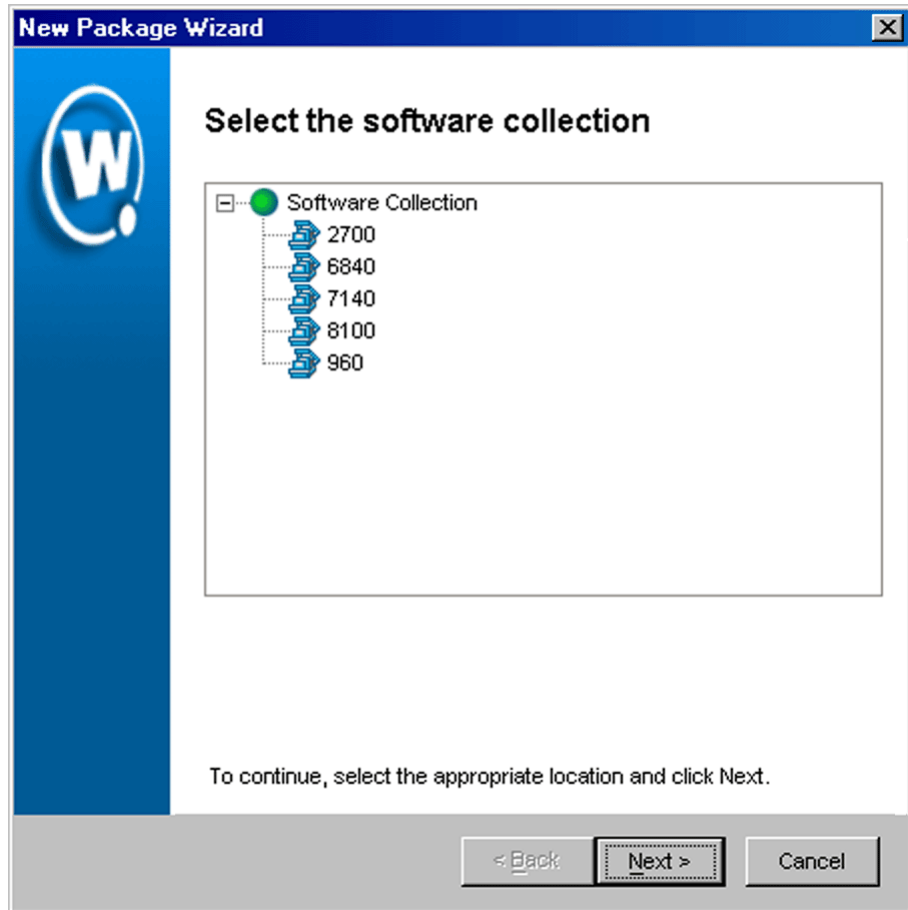
---

**NOTE** Avalanche packages use the.ava file extension.

---

- 4 Click Next.

The *Select the Software Collection* dialog box appears.



**Figure 7-7.** The Select the Software Collections Dialog Box

- 5 Select a software collection where the package will be installed.

---

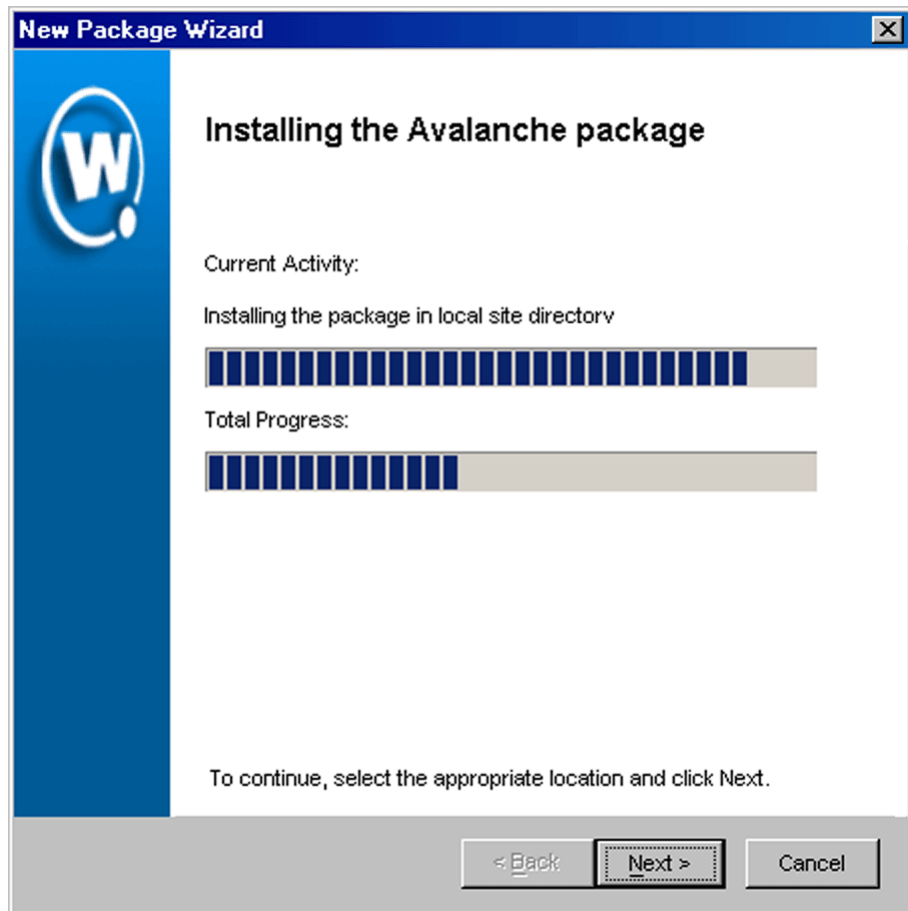
**NOTE** If you have not yet created a software collection, see *Creating Software Collections* on page 253.

---

To select a software collection, expand the **Software Collection** node, then select the appropriate collection from the list that appears.

- 6 Click **Next**.

The *Installing the Avalanche Package* dialog box appears.



**Figure 7-8.** *The Installing the Avalanche Package Dialog Box*

7 When the package installation is complete, click `Finish`.

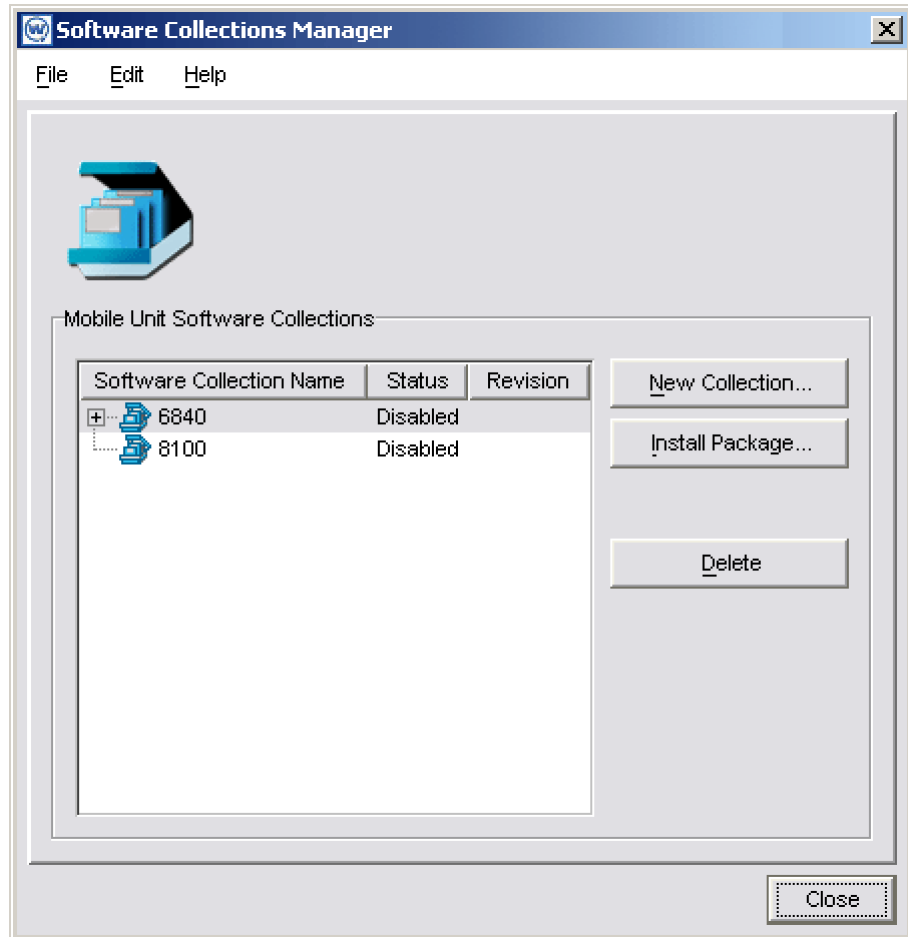
### **Moving Packages**

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

**To move a package:**

- 1 Select `Software Collections` from the **Tools** menu.

The *Software Collections Manager* dialog box appears.

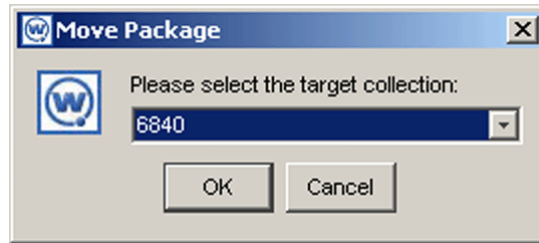


**Figure 7-9.** *The Software Collections Manager Dialog Box*

- 2 Select a software package.
- 3 From the **Edit** menu in the *Software Collections Manager* dialog box, select `Move`.



The *Move Package* dialog box appears.



**Figure 7-10.** *The Move Package Dialog Box*

- 4 Select the software collection that will receive the package and click `OK`.

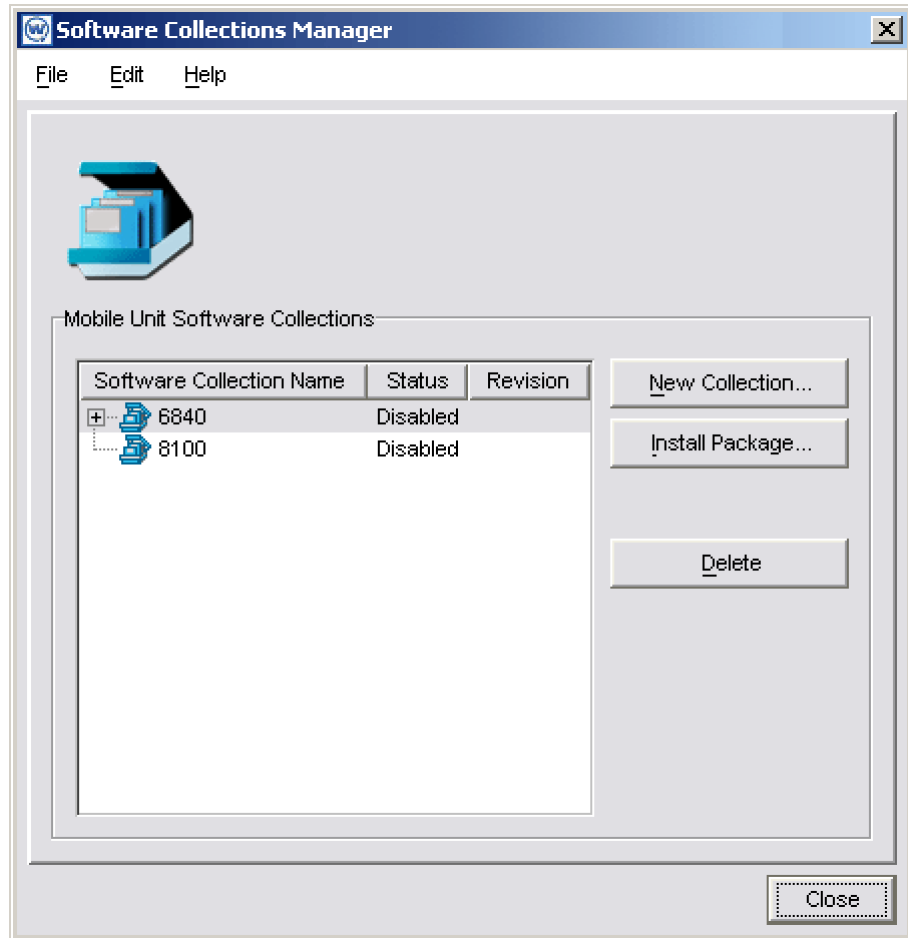
### **Copying Packages**

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

#### **To move a package:**

- 1 Select `Software Collections` from the **Tools** menu.

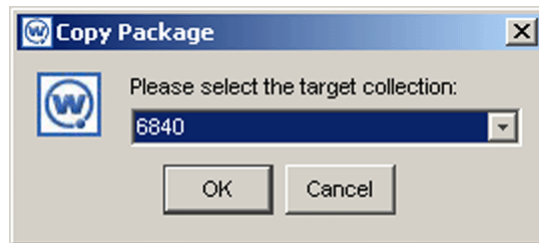
The *Software Collections Manager* dialog box appears.



**Figure 7-11.** *The Software Collections Manager Dialog Box*

- 2 Select a software package.
- 3 From the **Edit** menu in the *Software Collections Manager* dialog box, select Copy

The *Copy Package* dialog box appears.



**Figure 7-12.** *The Copy Package Dialog Box*

- 4 Select the software collection that will receive the package and click **OK**.

### **Configuring Packages**

You have the option of configuring several different properties related to software packages. These properties are divided into three categories:

- Host profiles
- Emulation parameters
- Localization

These options vary from software package to software package. See the *Avalanche Manager User's Guide* for more information.

### **Defining Selection Criteria**

Once you create a software collection, you can apply selection criteria to it. Selection criteria are specific parameters that determine what mobile devices can receive the software packages contained in the software collection.

---

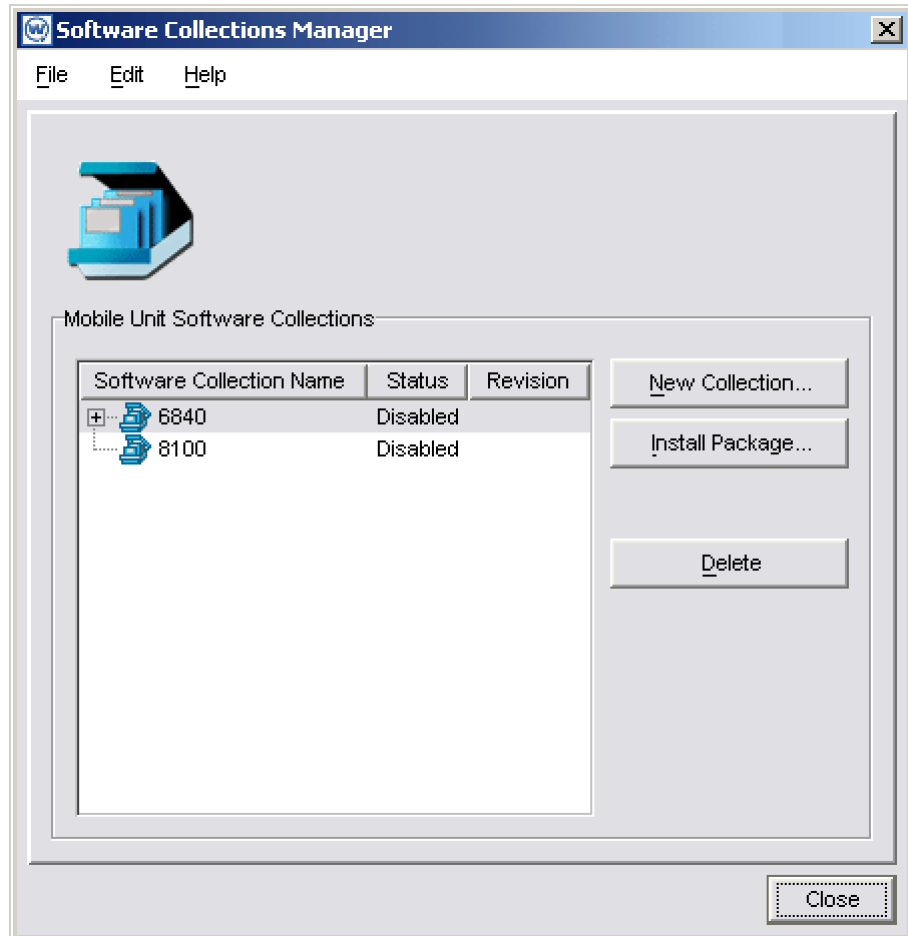
**NOTE** The settings described in this section are global, affecting all groups managed with the Enterprise Management Console.

---

#### **To define selection criteria:**

- 1 Select **Software Collections** from the **Tools** menu.

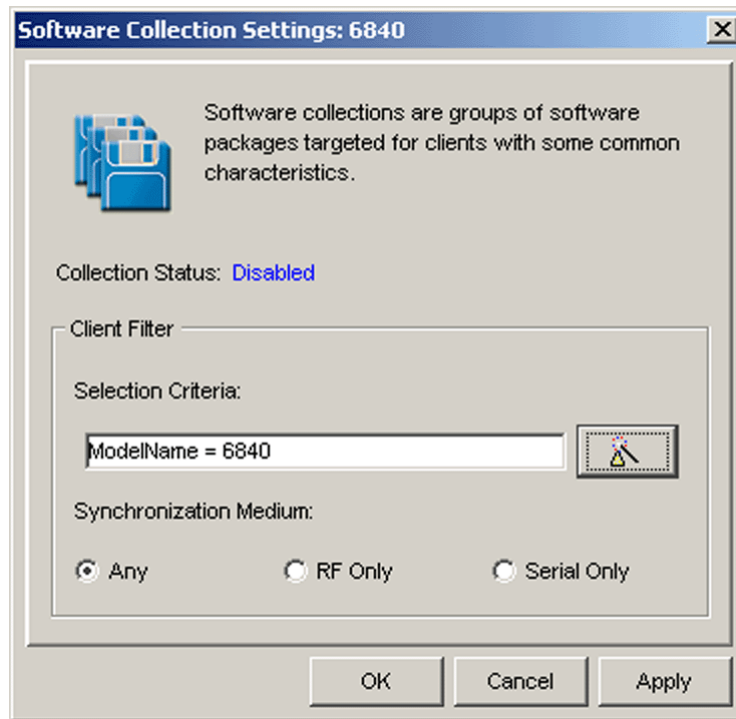
The *Software Collections Manager* dialog box appears.



**Figure 7-13.** *The Software Collections Manager Dialog Box*

- From the **Edit** menu within the *Software Collections Manager* dialog box, select **Configure**.

The *Software Collection Settings* dialog box appears.



**Figure 7-14.** *The Software Collections Settings Dialog Box*

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

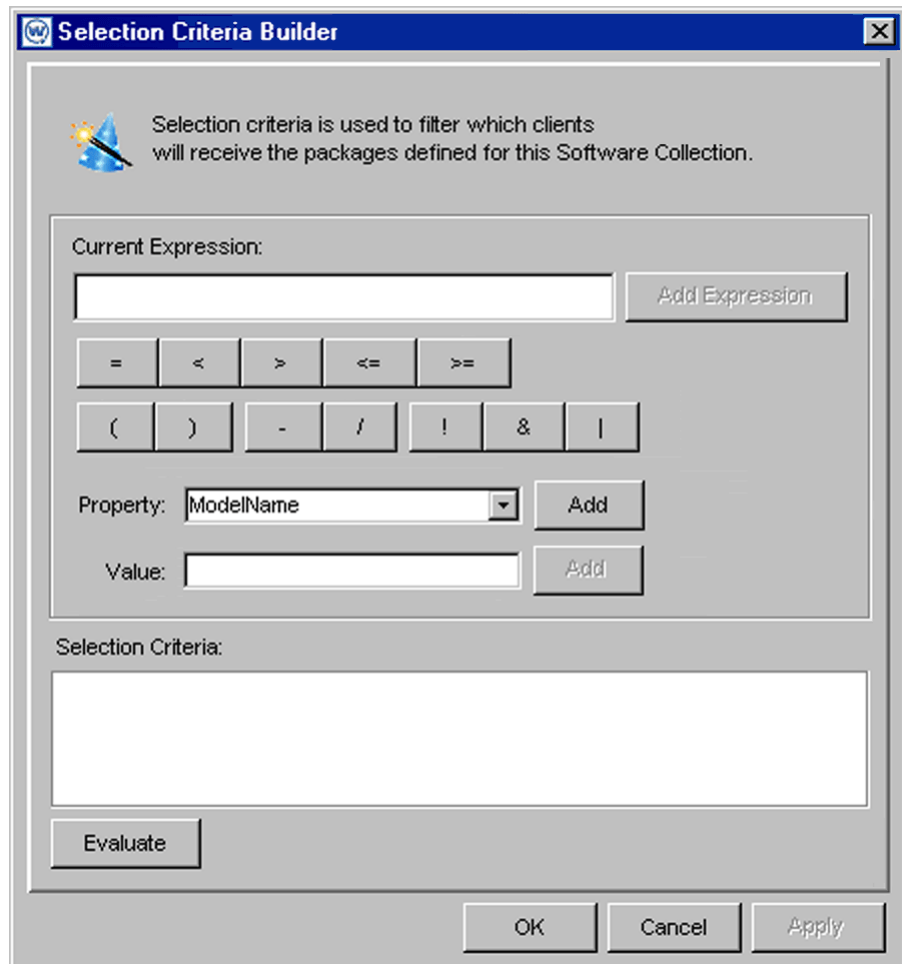
If you want to restrict the software updates associated with the current profile to wireless only, enable the **RF Only** option.

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.

- 4 Click the **Selection Criteria Wizard** icon.

The *Selection Criteria Builder* dialog box appears.



**Figure 7-15.** *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.

Detailed information on building selection criteria is available in *Building Selection Criteria* on page 269.

## Building Selection Criteria

- 1 Follow the steps for creating selection criteria as described in *Defining Selection Criteria* on page 265.
- 2 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* on page 271 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 275 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* on page 271 for additional information.

**3** Click `Add Expression`.

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

**4** 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.

---

**5** Click `OK`.

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

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

**7** 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`.



Mobile Manager Enterprise 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**

The selection criteria is based on the use of selection variables.

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 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 are 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	<p>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.</p> <p>The following values are supported:</p> <ul style="list-style-type: none"><li>0 = 35 key</li><li>1 = More than 35 keys/WSS1000</li><li>2 = Other terminals with less than 35 keys.</li></ul> <p>Example:</p> <pre>KeyboardCode &lt; 2</pre>
Rows	<p>The number of display rows the mobile device supports. This variable supports values from 1 to 25.</p> <p>Example:</p> <pre>Rows = 6</pre>
Columns	<p>The number of display columns the mobile device supports. This variable supports values from 1 to 80.</p> <p>Example:</p> <pre>Columns = 21</pre>
Terminal ID	<p>This client property is the unique ID for the mobile device that the Avalanche Manager generates. The values assigned by Mobile Manager Enterprise start from 1 and increase incrementally.</p> <p>Example:</p> <pre>Terminal ID = 5</pre>

### 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:  <code>ModelName = 6840</code>
>	Binary operator that results in TRUE if the expression on the left is greater than the expression on the right.  Example:  <code>Rows &gt; 15</code>
<	Binary operator that results in TRUE if the expression on the left is less than the expression on the right.  Example:  <code>Rows &lt; 5</code>
>=	Binary operator that results in TRUE if the expression on the left is greater than or equal to the expression on the right.  Example:  <code>Rows &gt;= 10</code>
<=	Binary operator that result in TRUE if the expression on the left is less than or equal to the expression on the right.  Example:  <code>Rows &lt;= 20</code>

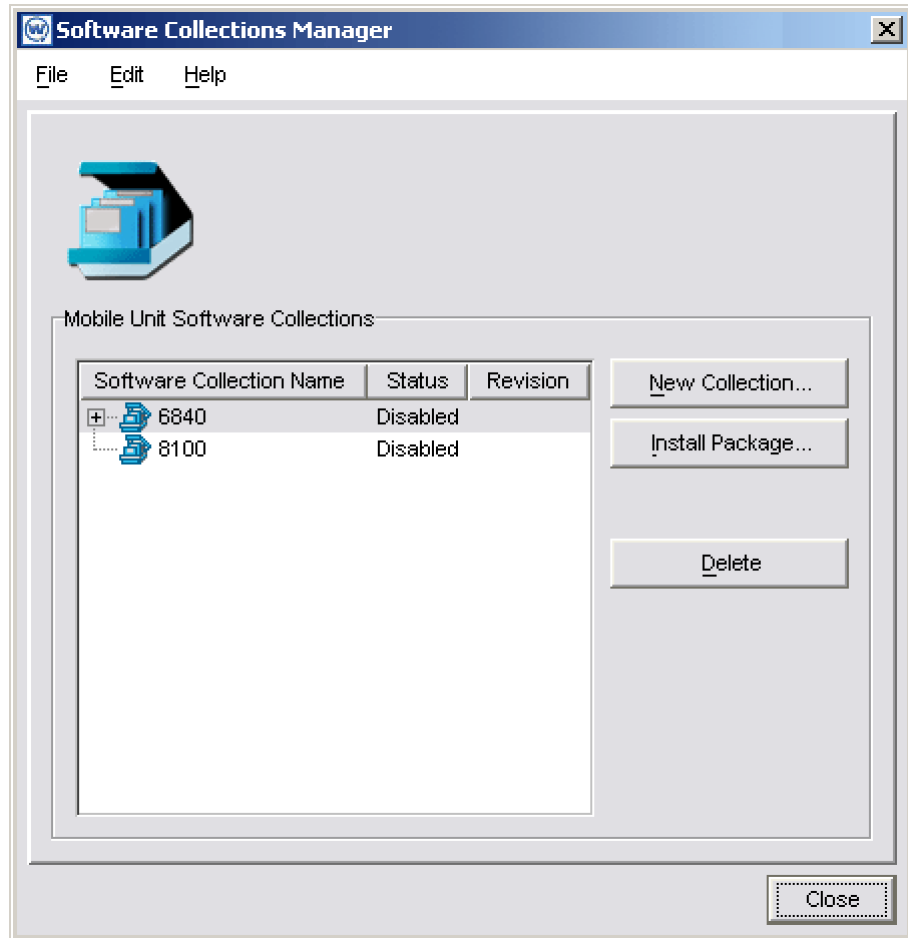
## Enabling Collections and Packages

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 Select `Software Collections` from the **Tools** menu.

The *Software Collections Manager* dialog box appears.



**Figure 7-16.** *The Software Collections Manager Dialog Box*

- 2 Select a software package or collection.
- 3 From the **Edit** menu of the *Software Collections Manager* dialog box, click **Enable**.

### **Disabling Collections and Packages**

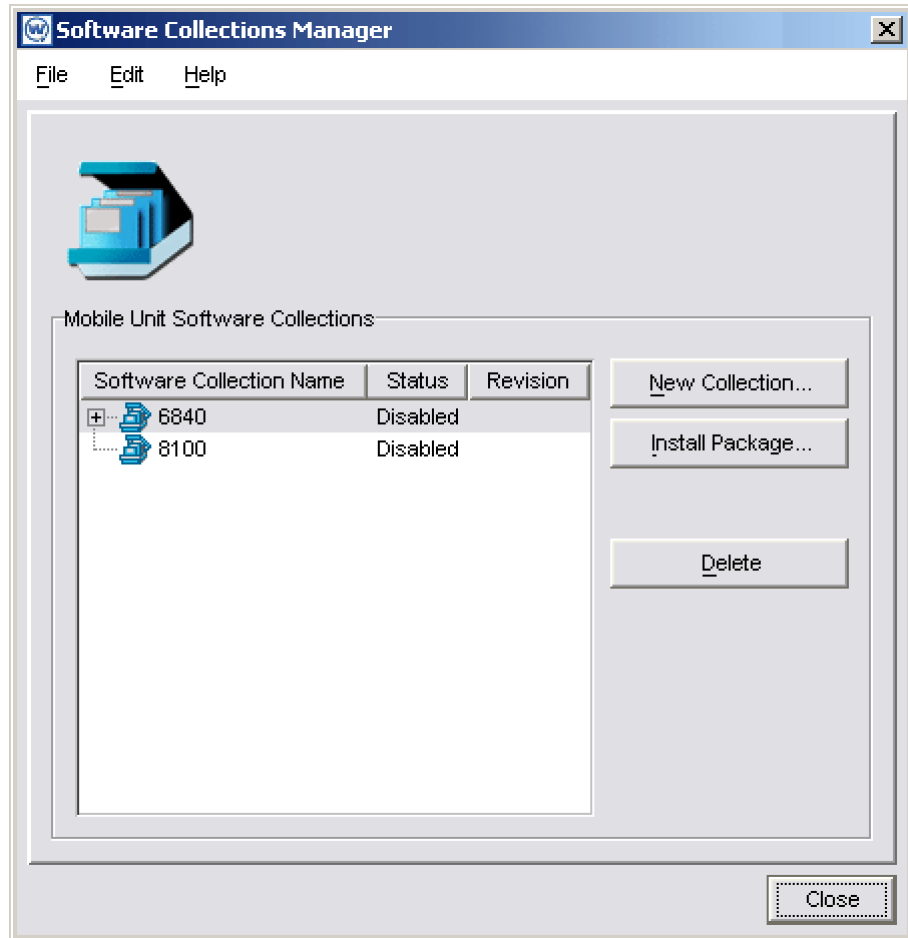
Disabling a collection or package prevents Mobile Manager Enterprise from deploying updates related to the collection or package to mobile devices.



**To disable a single software collection or package:**

- 1 Select `Software Collections` from the **Tools** menu.

The *Software Collections Manager* dialog box appears.



**Figure 7-17.** *The Software Collections Manager Dialog Box*

- 2 Select a software package or collection.
- 3 From the **Edit** menu of the *Software Collections Manager* dialog box, click `Disable`.

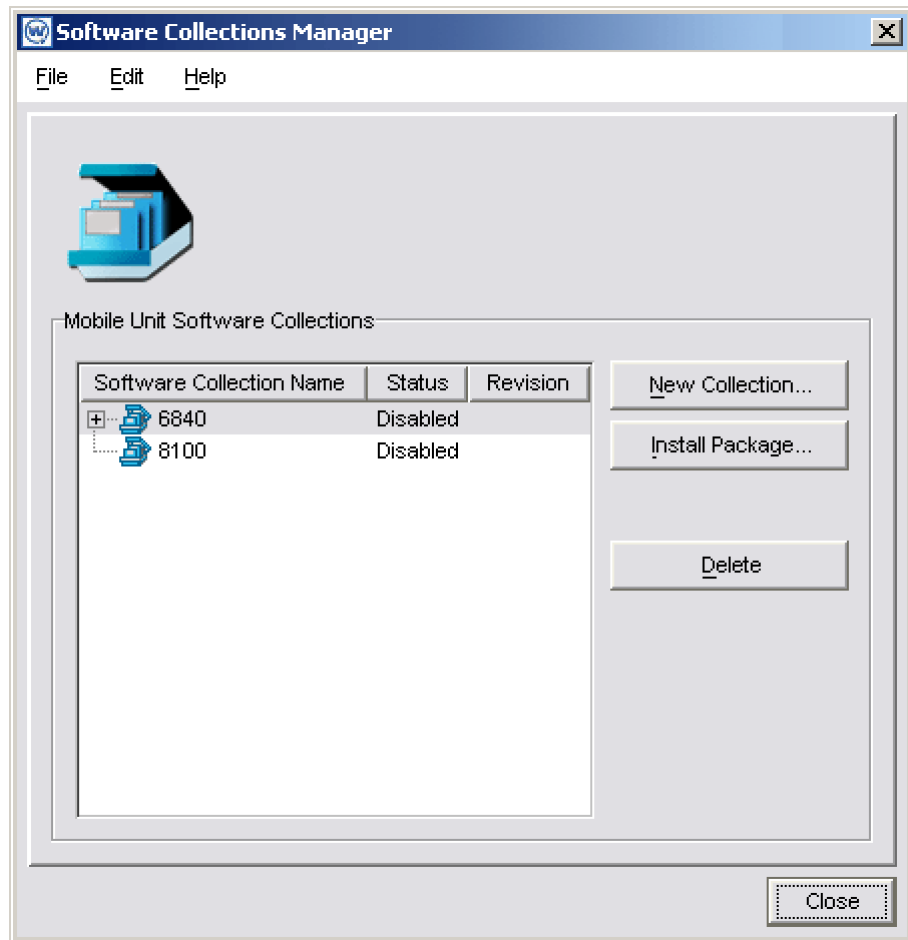
## Deleting Packages and Collections

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 Select `Software Collections` from the **Tools** menu.

The *Software Collections Manager* dialog box appears.



**Figure 7-18.** *The Software Collections Manager Dialog Box*

- 2 Select a software package or collection.
- 3 From the **Edit** menu of the *Software Collections Manager* dialog box, click **Delete**.

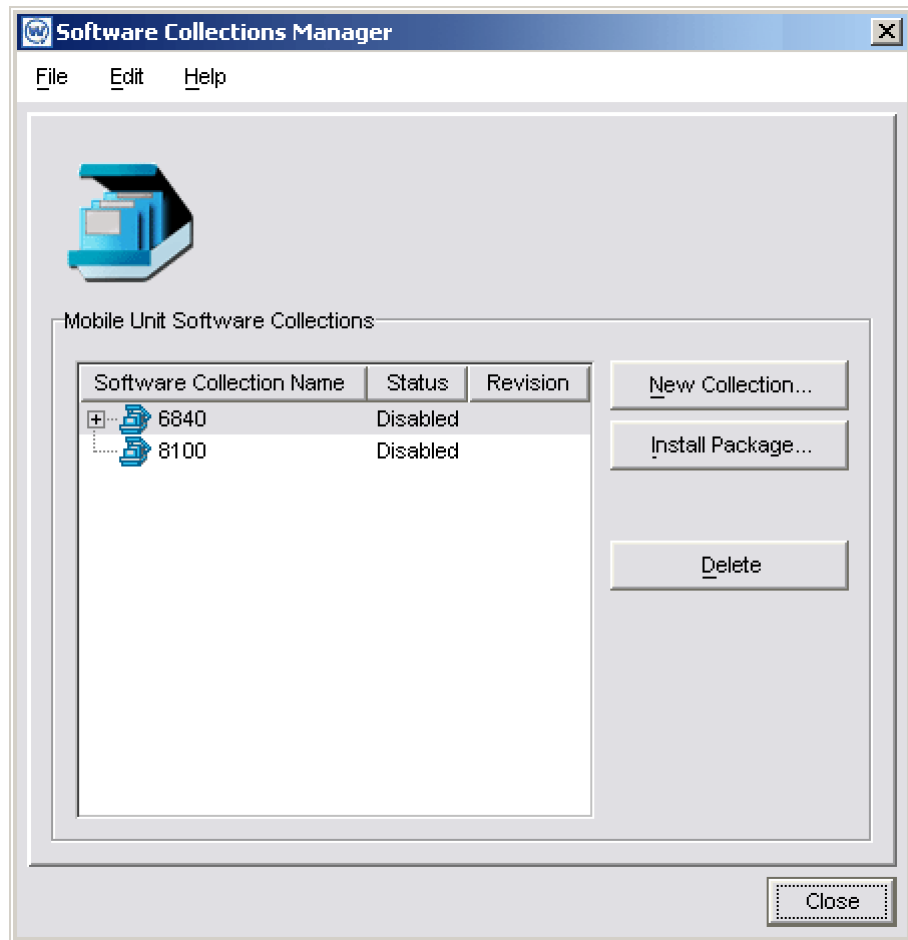
### **Refreshing the Software Collections Manager**

Although the Software Collections Manager dialog box is periodically updated by Mobile Manager, you have the option of refreshing it manually. This feature is useful if multiple individuals have access to the Enterprise Management Console, and you want to ensure that the Enterprise Management Console displays the latest information.

#### **To refresh the Software Collections Manager dialog box:**

- 1 Select *Software Collections* from the **Tools** menu.

The *Software Collections Manager* dialog box appears.



**Figure 7-19.** *The Software Collections Manager Dialog Box*

- From the **File** menu of the *Software Collections Manager* dialog box, click Refresh.

## Synchronizing Mobile 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. The Enterprise Management Console allows you

to manage your wireless software in a timely and efficient manner. Within this view, you can centrally manage the software installed on the mobile devices within your network.

Typically, you manage device software by adding one or more synchronization events within the Enterprise Management Console. A synchronization event defines the dates and times when software versions are updated on mobile device Agents. Occasionally, you might need to configure other aspects of software synchronization, including:

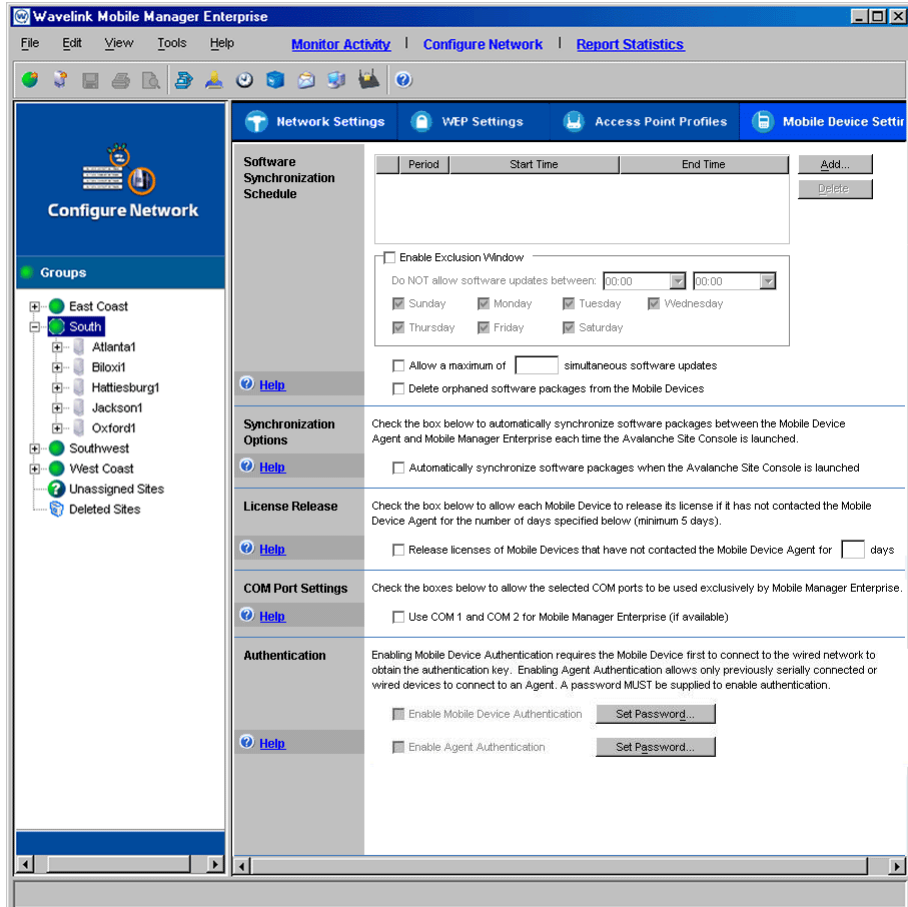
- Excluding certain days and times from software updates
- Setting a maximum number of simultaneous updates
- Deleting orphaned packages from mobile devices
- Automatically synchronizing software when a site tool is launched

### **Adding Synchronization Events**

A synchronization event is an event during which Mobile Manager updates and synchronizes the software applications managed in a group. You can create multiple synchronization events to correspond with the different software applications running at different sites.

#### **To add a synchronization event:**

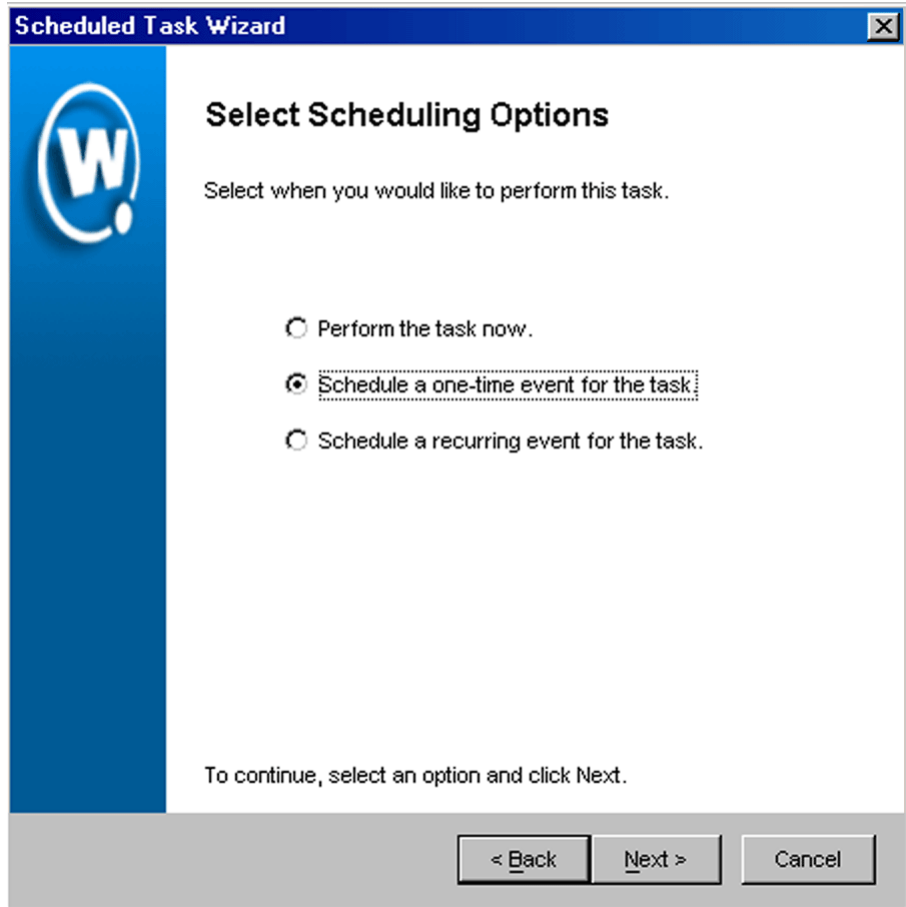
- 1** Select a group from the Groups window.
- 2** Click `Configure Network`.
- 3** Click the Mobile Unit Settings Tab.



**Figure 7-20.** The Mobile Device Settings Tab of the Configure Network View

4 In the Software Synchronization section, click Add .

The *Select Scheduling Options* dialog box appears.



**Figure 7-21.** *The Select Scheduling Options Dialog Box*

**5** Determine when the event will occur.

If you want the event to occur immediately, select the **Perform the task now** option.

If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

If you want the event to occur on a regular basis, select the **Schedule a recurring event** for this task option.

- 6 Click **Next**.
- 7 If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.

**Scheduled Task Wizard**

### Schedule the Time Window

Select the start time and end time during which you would like to perform this task.

Start Time: 08 /19 /2003 11:45

Run until complete

End by: 08 /19 /2003 12:00

Use Site's Local Time

To continue, click Next.

< Back Next > Cancel

**Figure 7-22.** *The Schedule the Time Window Dialog Box*

Within this dialog box, you can set the following parameters for the event:

- Select the start date and time for the event.



- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.
- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.
- 8** If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

**Scheduled Task Wizard**

## Configure Task Recurrence

Use the controls below to configure the recurrence settings

**Task time**

Start Time:   Run until complete  Use Site's Local Time  
 End by:

**Recurrence pattern**

Daily    Recur every  week(s) on:  
 Weekly     Sunday  Monday  Tuesday  Wednesday  
 Monthly     Thursday  Friday  Saturday

**Range of recurrence**

Start:    No end date  
 End by:

To continue, click Next.

< Back    Next >    Cancel

**Figure 7-23.** The Configure Task Recurrence Dialog Box

Within this dialog box, you can set the following parameters for this event:

- Select the start time for the event.
- Determine when you want the event to stop. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

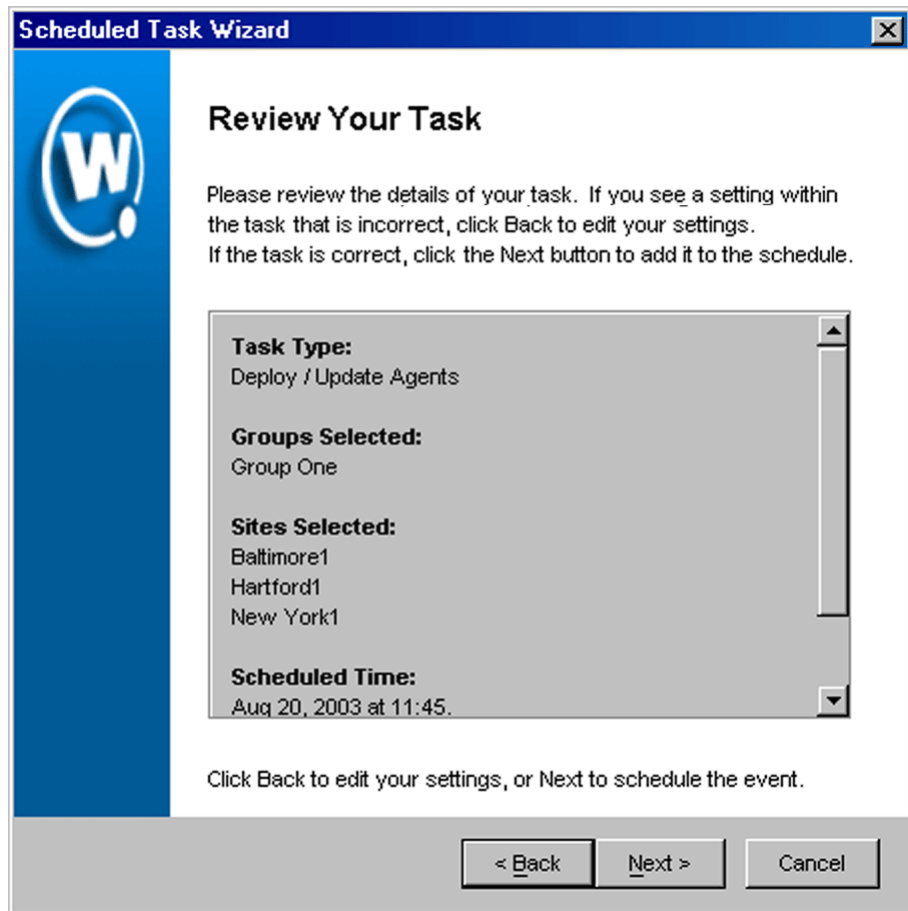
---

**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

- 9 Click *Next*.

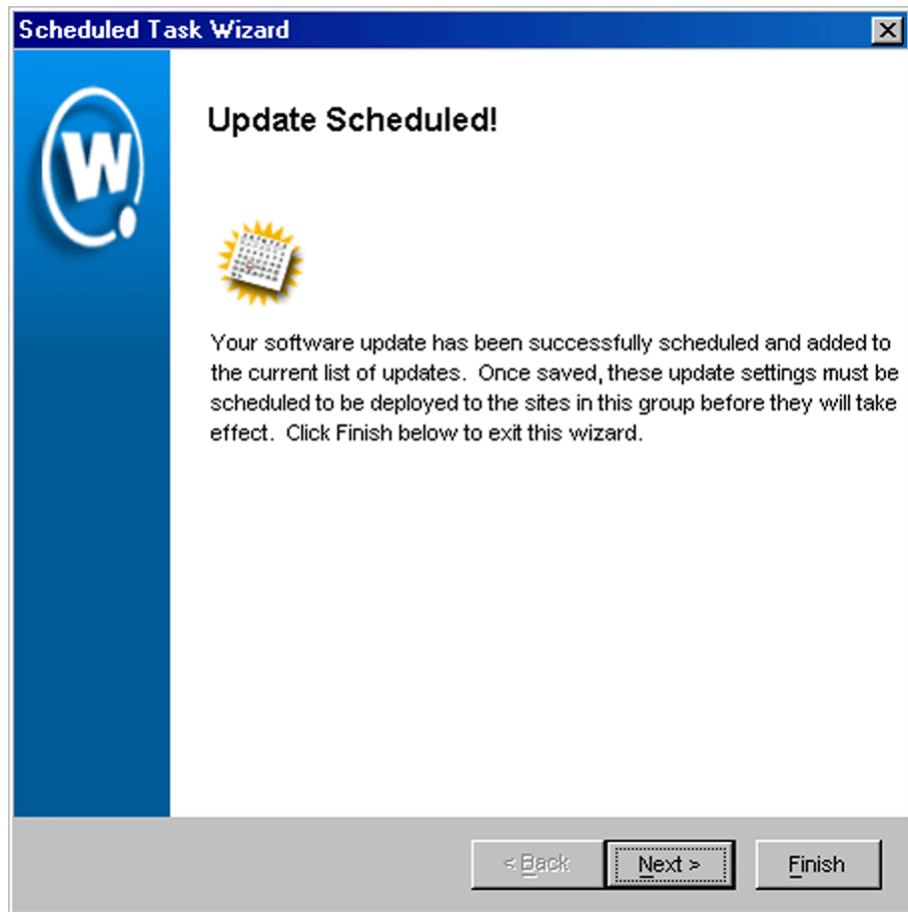
The *Review Your Task* dialog box appears.



**Figure 7-24.** *The Review Your Task Dialog Box*

**10** Review your the task to ensure that it is correct and click `Next`.

The *Update Scheduled* dialog box appears.



**Figure 7-25.** *The Update Scheduled Dialog Box*

- 11 Click **Next** to schedule a new event, or click **Finish** to return to the *Task Schedule* dialog box.

The event now appears in the list within the Software Synchronization Schedule section.

If you want to exclude certain times and dates from these update events, see *Excluding Dates and Times* on page 292.

## Excluding Dates and Times

When you create scheduling events for synchronizing mobile device software, you might want to exclude specific dates and times. For example, you might want to prevent Mobile Manager from trying to update software during hours when these devices are in use.

---

**NOTE** The dates and times you exclude from scheduling events apply to all events for that group—you cannot set specific exclusion dates and times for each event.

---

### To exclude dates and times from a scheduling event:

- 1 Select a group from the Groups window.
- 2 Click `Configure Network`.
- 3 Click the Mobile Unit Settings Tab.
- 4 Within the Software Synchronization Schedule section, Enable the **Enable Exclusion Window** checkbox.
- 5 Using the lists provided, select the start and end times between which software updates should not occur.
- 6 Select the days during which these start and end times apply by enabling the checkbox next to the day.

For example, if you want to prevent software updates from occurring from 7:00 am to 7:00 pm from Monday through Friday you would select 07:00 from the start time list, select 19:00 from the end time list, and enable the checkboxes for Monday, Tuesday, Wednesday, Thursday, and Friday.

## Setting Maximum Simultaneous Updates

Software updates require sending application package files to each mobile device. The amount of time needed to send these files depends on how large the application package files are. If you want to conserve network bandwidth, you can set a maximum number of simultaneous updates that can occur.

---

**NOTE** The maximum number of simultaneous updates that you allow applies to all events for a group.

---

**To set a maximum number of simultaneous updates:**

- 1 Select a group from the Groups window.
- 2 Click `Configure Network`.
- 3 Click the Mobile Unit Settings Tab.
- 4 Enable the **Allow a maximum of simultaneous software updates** checkbox.

Within the description of this checkbox, there is an additional text box where you can type the number of simultaneous updates that you want to allow.

- 5 Type the maximum number of simultaneous updates in this text box.

## **Deleting Orphaned Packages**

As you update and modify the software installed on mobile devices, you might find that these devices begin to acquire orphaned packages. Orphaned packages are parts of application files that no longer apply to applications on a mobile device.

Within the Enterprise Management Console, you can instruct the mobile device Agents for a group to delete any orphaned packages on their managed mobile devices.

**To delete orphaned packages:**

- 1 Select a group from the Groups window.
- 2 Click `Configure Network`.
- 3 Click the Mobile Unit Settings Tab.
- 4 Enable the **Delete orphaned software packages from the Mobile Units** option.

## Automatic Synchronization

Mobile Manager allows you to manage your sites in more detail by opening one of two site tools. For mobile devices, the tool that you use is the Avalanche Management Console.

You can configure a group so that each time an Avalanche Management Console is opened for a given site, the software packages managed at that site are synchronized with the software packages managed within the Enterprise Management Console.

To automatically synchronize software packages when the Avalanche Management Console opens:

- 1 Select a group from the Groups window.
- 2 Click `Configure Network`.
- 3 Click the Mobile Unit Settings Tab.
- 4 Enable the **Automatically synchronize software packages when the Avalanche Site Console is launched** option.

## Managing Licenses

Licenses for mobile devices are frequently redistributed, providing a great deal of flexibility in managing licenses. Within the Enterprise Management Console, you can configure mobile device Agents to release licenses from mobile devices that have not connected to the network within a specific number of days.

---

**NOTE** Settings for managing licenses are applied on a per-group basis.

---

### To release unused licenses:

- 1 Select a group from the Groups window.
- 2 Click `Configure Network`.
- 3 Click the Mobile Unit Settings Tab.



- 4 In the License Release section, enable the **Release licenses of Mobile Devices that have not contacted the Unit Agent for days** option.

Within the description of this checkbox, there is an additional text box where you can type the number of days before the mobile device Agents release unused licenses.

- 5 Type the number of days before the mobile device Agents release unused licenses in the text box.

## Setting COM Ports

Mobile devices that are new to the network cannot be configured a wireless connection; instead, they must be initially configured when they are physically connected to the network through a cradle. You can configure mobile device Agents to automatically listen for mobile devices using the COM ports on the remote system.

---

**NOTE** Settings for COM port are configured on a per-group basis.

---

### To establish COM port settings:

- 1 Select a group from the Groups window.
- 2 Click `Configure Network`.
- 3 Click the Mobile Unit Settings Tab.
- 4 In the COM Port Settings section, enable the **Use COM 1 and COM 2 for Mobile Manager Enterprise (if available)** option.

## Authenticating Mobile Devices

Along with Access Control Lists and WEP security measure, Mobile Manager provides additional authentication methods for mobile devices. These options require that a mobile device first connect to the network through a serial connection before being able to roam the network wirelessly.

---

**NOTE** Settings for authenticating mobile devices are configured on a per-group basis.

---

Mobile device authentication employs two options:

- **Enable Mobile Device Authentication.** This option forces mobile devices to connect to the network through a wired connection (such as a cradle) and receive an authentication key.
- **Enable Agent Authentication.** This option forces mobile devices to communicate with a single, known Agent. As with the Enable Mobile Device Authentication option, this option requires that mobile devices first connect to the network through a wired connection to receive information on which Agent with which they are allowed to communicate.

---

**NOTE** Both of these options require mobile devices to connect to the network through a wired connection to receive authentication information. Proper planning is essential to ensure that all devices can connect to the wired network when these options are enabled—otherwise, these devices might be unable to connect to the network.

---

**To authenticate mobile devices:**

- 1 Select a group from the Groups window.
- 2 Click `Configure Network`.
- 3 Click the Mobile Device Settings Tab.
- 4 If you want to force mobile devices to connect to the wired network and receive an authentication key before being allowed to roam the network wirelessly, you must set the following options in the Authentication section of the dialog box:
  - Set the administrative password for the mobile device Agent by clicking `Set Password` and entering a valid user password.
  - Enable the **Enable Mobile Device Authentication** checkbox.

- 5 If you want to restrict mobile devices to communicate only with a single, known Agent, you must set the following options in the Authentication section of the dialog box:
  - Set the administrative password for the access point Agent by clicking
  - Set `Password` and entering a valid user password.
  - Enable the **Enable Agent Authentication** checkbox

---

**NOTE** If a site environment involves mobile devices roaming from one Agent to another, it is highly recommended that you do **NOT** activate this option.

---

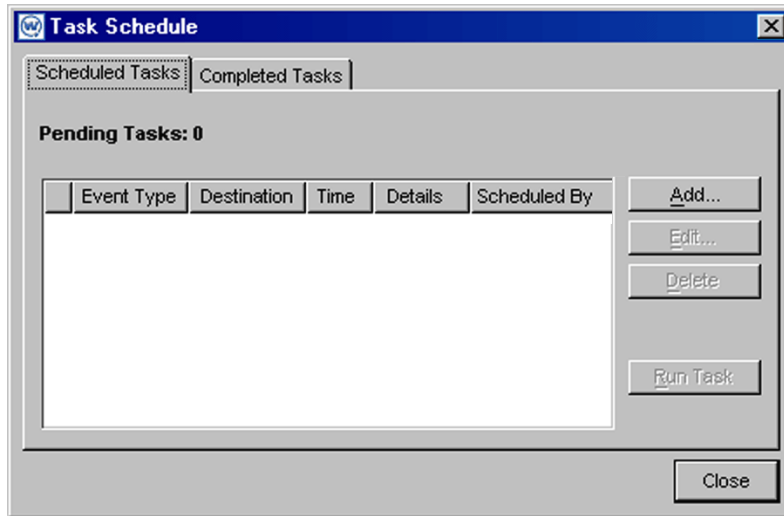
## Deploying Settings to Mobile Devices

This section describes how to apply network settings to the mobile devices within a given group.

### To deploy mobile device settings:

- 1 Select `Task Schedule` from the **Tools** menu.

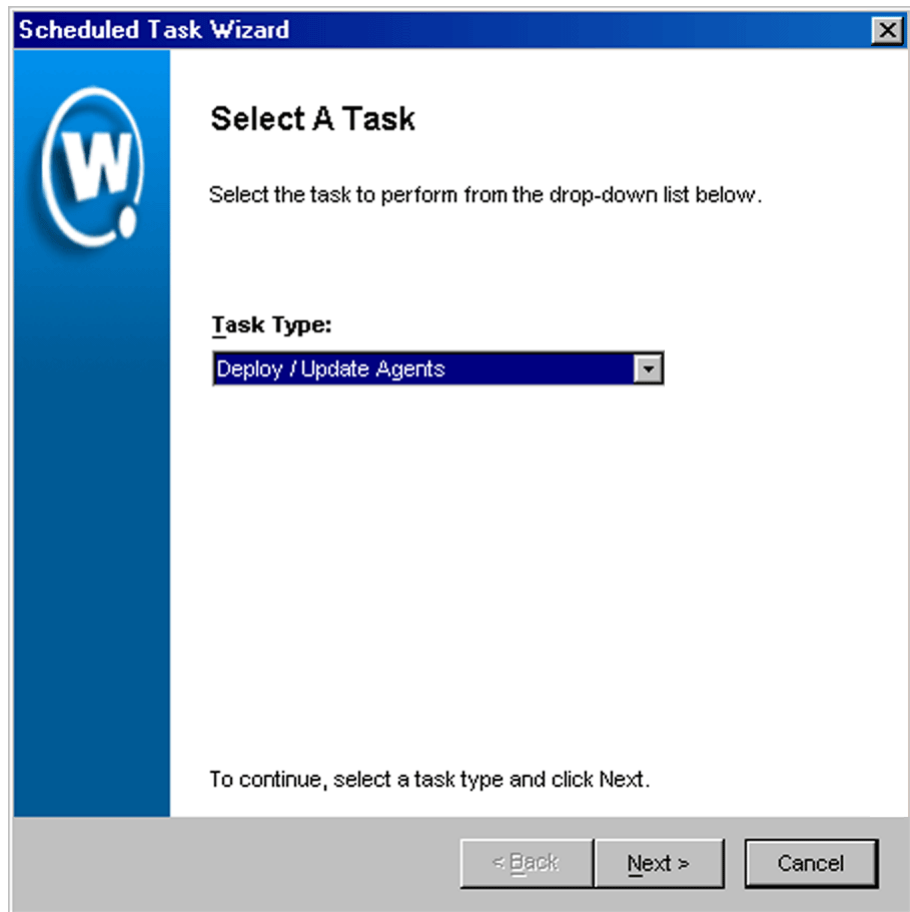
The *Task Schedule* dialog box appears.



**Figure 7-26.** *The Task Schedule Dialog Box*

2 Click Add.

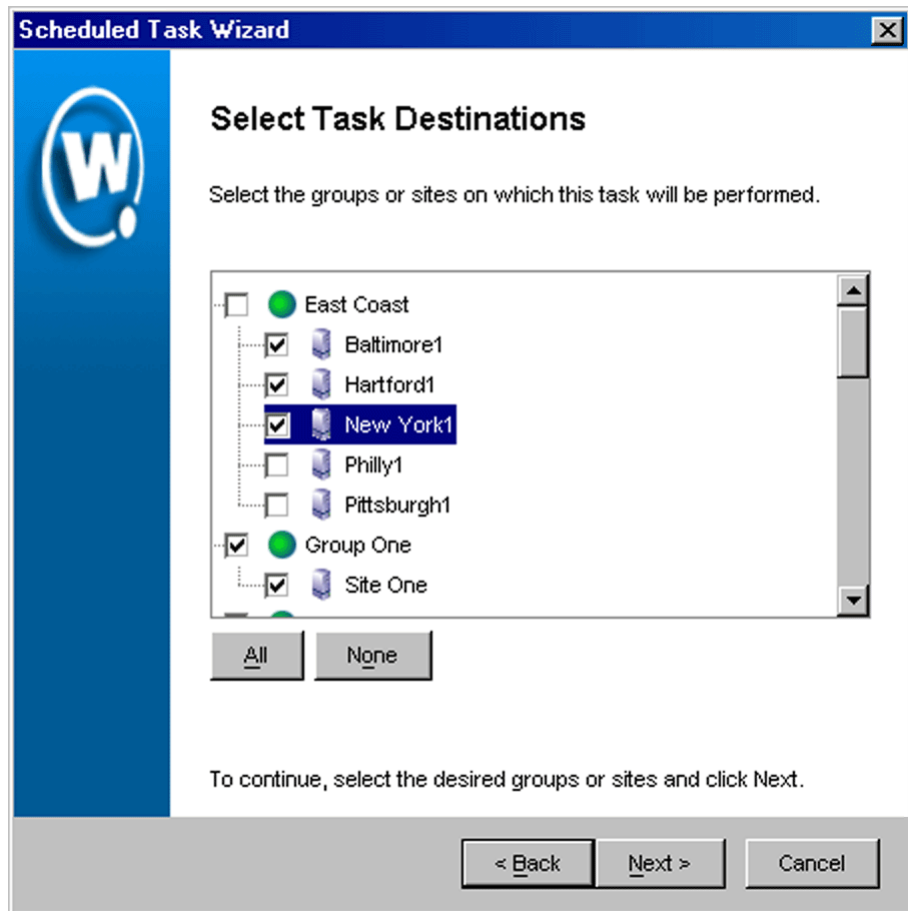
The Select A Task dialog box appears.



**Figure 7-27.** *The Select a Task Dialog Box*

- 3 Select `Deploy Mobile Device Settings` from the **Task Type** list and click `Next`.

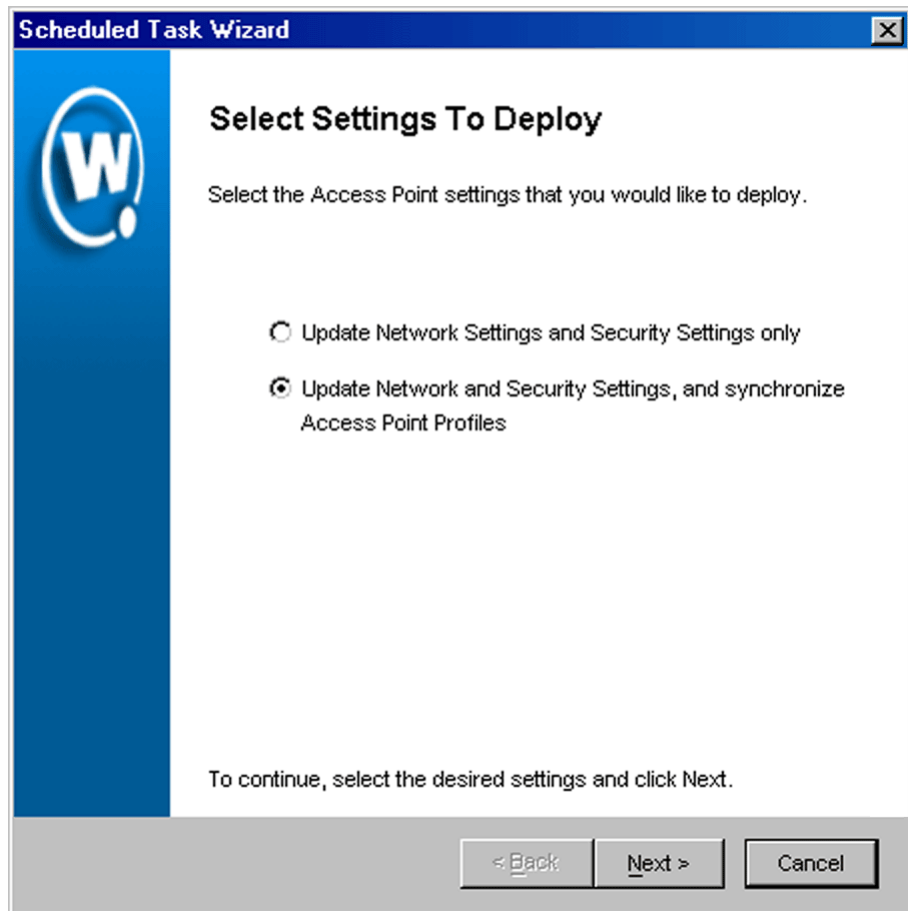
The *Select Task Destination* dialog box appears.



**Figure 7-28.** *The Select Task Destination Dialog Box*

- 4 Select the groups or sites by enabling the checkbox next to the group or site name. You can also select all groups by clicking All.
- 5 Click Next.

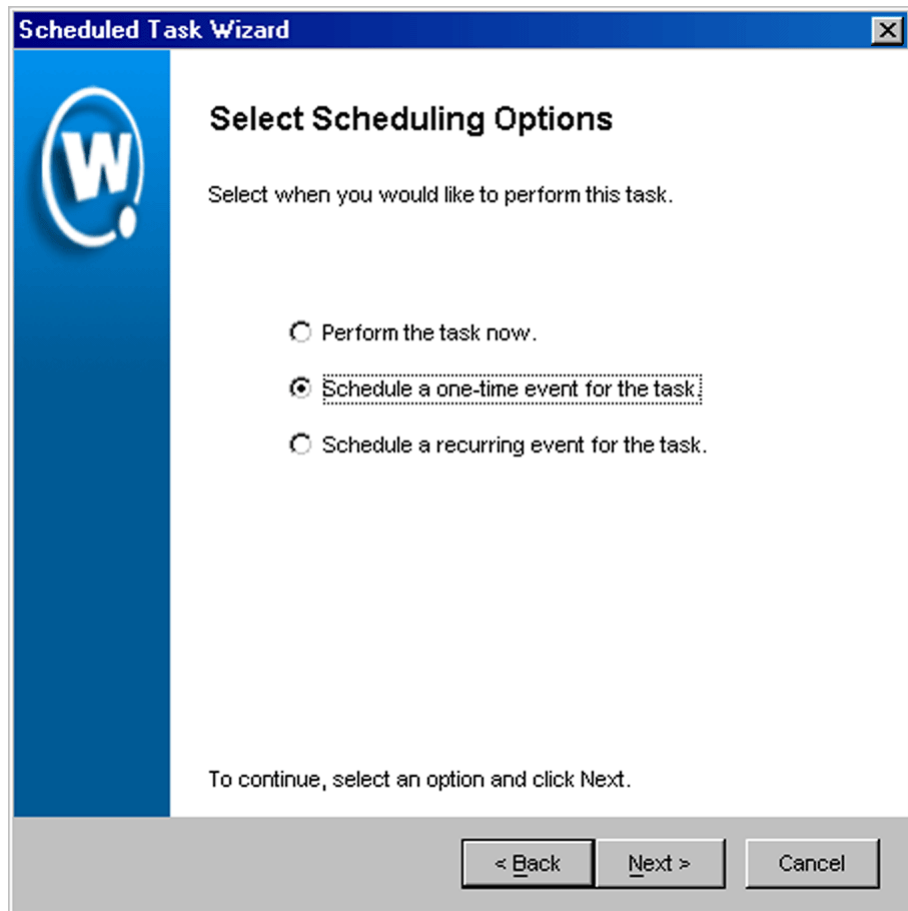
The *Select Settings to Deploy* dialog box appears.



**Figure 7-29.** *The Select Settings to Deploy Dialog Box*

- 6** Select the **Update Network Settings and Security Settings only** option.
- 7** Click **Next**.

The *Select Scheduling Options* dialog box appears.



**Figure 7-30.** *The Select Scheduling Options Dialog Box*

**8** Determine when the event will occur.

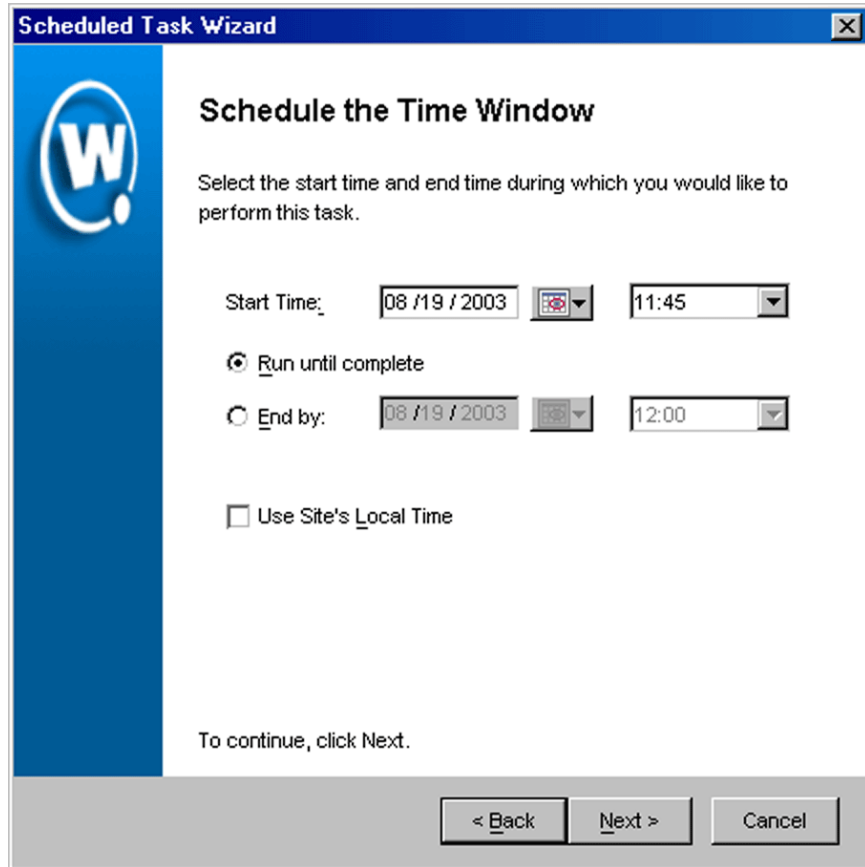
If you want the event to occur immediately, select the **Perform the task now** option.

If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

If you want the event to occur on a regular basis, select the **Schedule a recurring event** for this task option.



- 9 Click **Next**.
- 10 If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.



**Figure 7-31.** *The Schedule the Time Window Dialog Box*

Within this dialog box, you can set the following parameters for the event:

- Select the start date and time for the event.
- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select

the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.
- 11** If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

The screenshot shows a dialog box titled "Scheduled Task Wizard" with a sub-title "Configure Task Recurrence". The dialog box contains the following sections:

- Task time:**
  - Start Time: 00:00 (dropdown)
  - Run until complete
  - Use Site's Local Time
  - End by: 00:00 (dropdown)
- Recurrence pattern:**
  - Daily
  - Weekly: Recur every 1 week(s) on:
    - Sunday
    - Monday
    - Tuesday
    - Wednesday
    - Thursday
    - Friday
    - Saturday
  - Monthly
- Range of recurrence:**
  - Start: 08 / 19 / 2003 (calendar icon)
  - No end date
  - End by: / / (calendar icon)

At the bottom, it says "To continue, click Next." and there are three buttons: "< Back", "Next >", and "Cancel".

**Figure 7-32.** The *Configure Task Recurrence* Dialog Box

Within this dialog box, you can set the following parameters for this event:

- Select the start time for the event.
- Determine when you want the event to stop. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.
- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

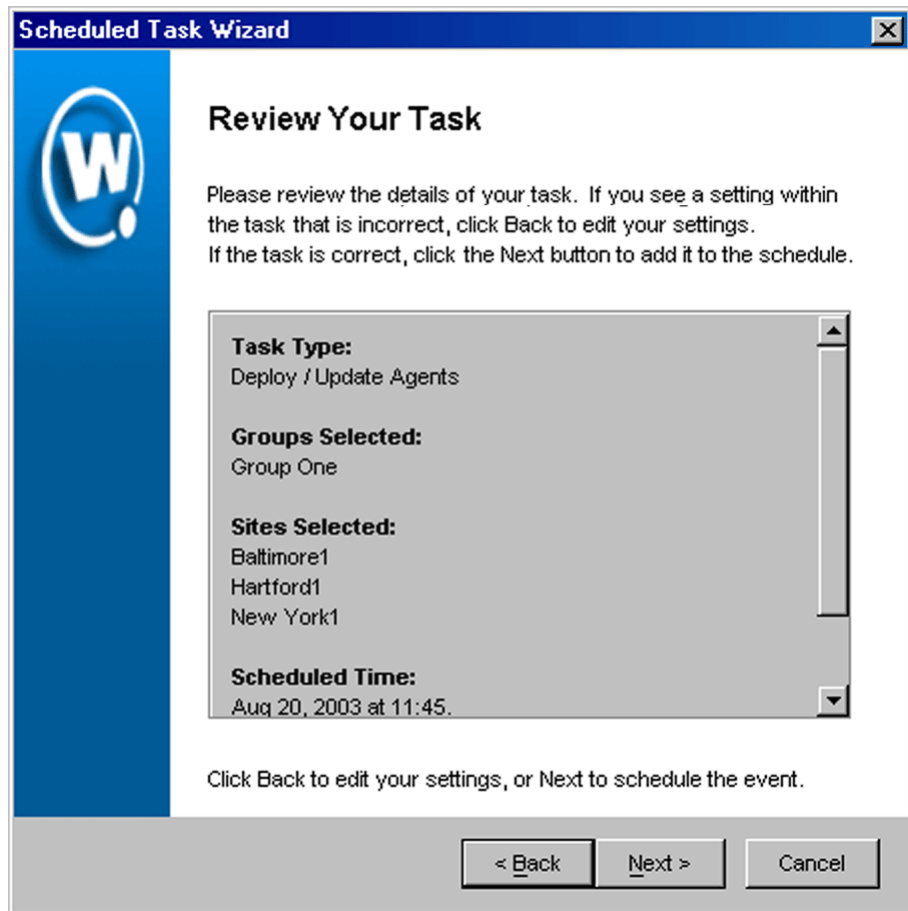
---

**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

**12** Click *Next*.

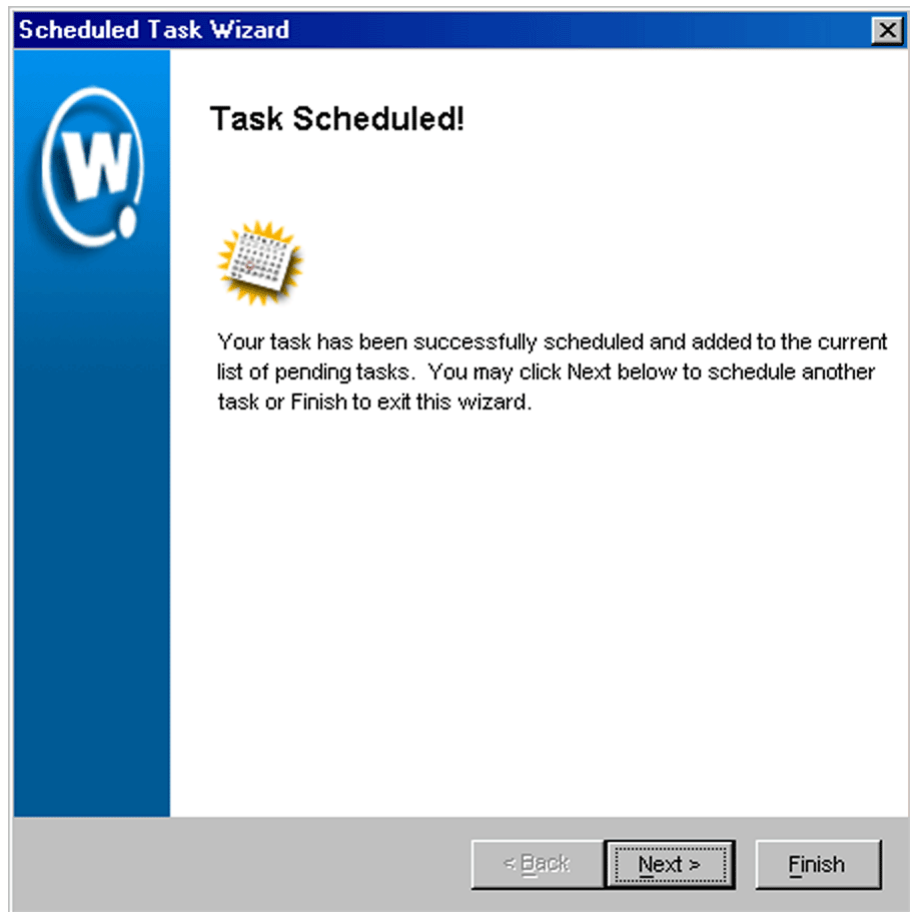
The *Review Your Task* dialog box appears.



**Figure 7-33.** *The Review Your Task Dialog Box*

**13** Review your the task to ensure that it is correct and click `Next`.

The *Task Scheduled* dialog box appears.



**Figure 7-34.** *The Task Scheduled Dialog Box*

- 14 Click `Next` to schedule a new event, or click `Finish` to return to the *Task Schedule* dialog box.



## Chapter 8: 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 Management Console provides you with the means to configure two primary methods of restricting wireless communications:

- **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.

---

**NOTE** Access Control Lists are set globally, and affect all sites managed with the Enterprise Management Console.

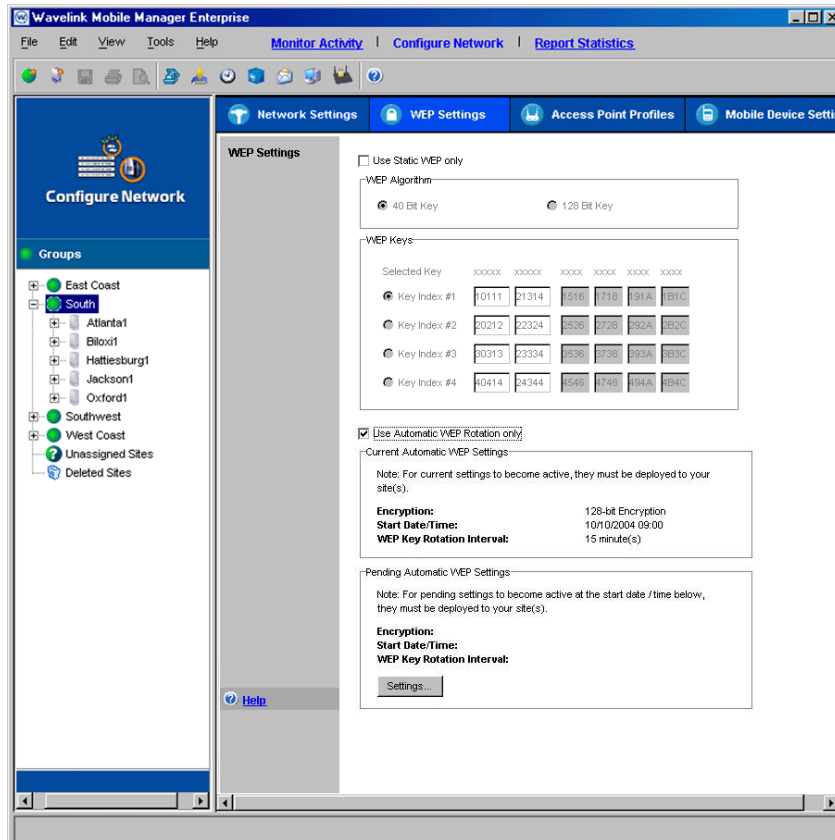
---

- **Wired Equivalent Privacy (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.
- **Extensible Authentication Protocol (EAP).** EAP is an additional protocol that increases the security of wireless transmissions. Currently EAP support is only available for Cisco access points.

---

**NOTE** WEP and EAP settings are set on a per-group basis.

---



**Figure 8-1.** The WEP 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, Mobile Manager Enterprise 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 Mobile [Manager Users Guide](#) for more information.

---

## Adding MAC Addresses

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

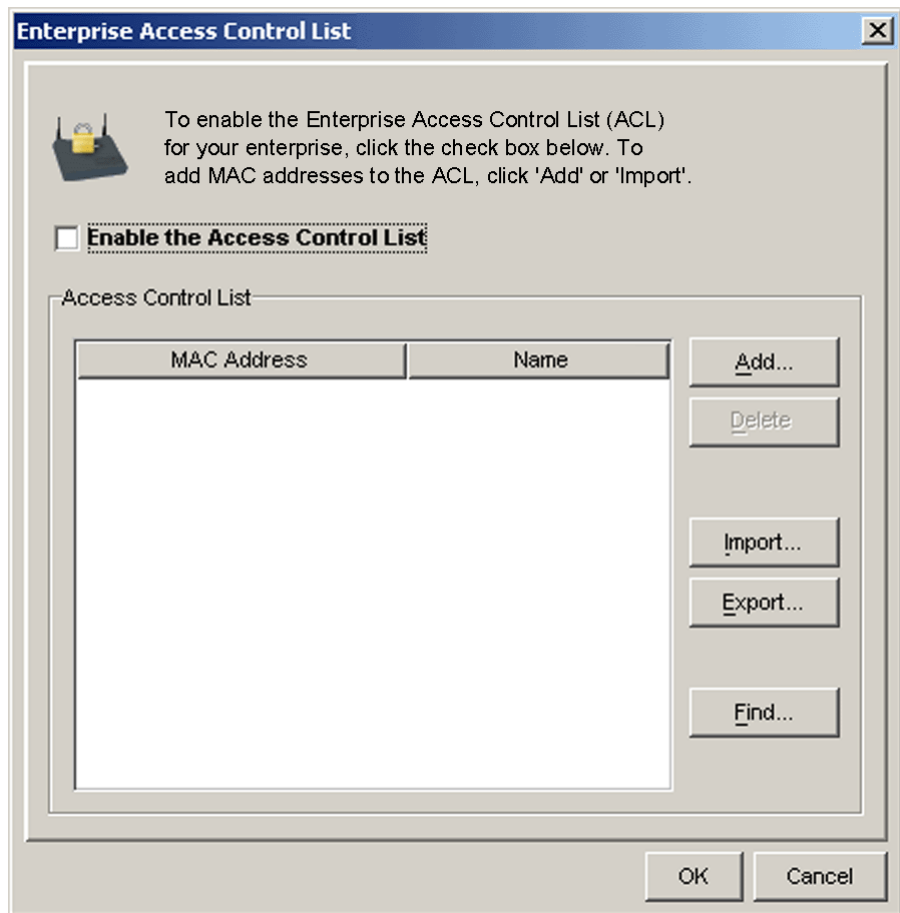
### To add a MAC address:

- 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 `Access Control List` from the **Tools** menu.

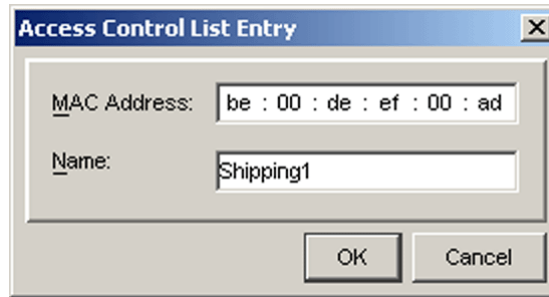
The *Enterprise Access Control List* dialog box appears.



**Figure 8-2.** *The Enterprise Access Control List Dialog Box*

- 3 Enable the **Enable Access Control List** checkbox.
- 4 Click Add.

The *Access Control List Entry* dialog box appears.



**Figure 8-3.** *The Access Control List Entry Dialog Box*

- 5 Type a MAC address in the **MAC Address** text box.
- 6 Type a name for the entry in the **Name** text box.
- 7 Click **OK** to return to the *Enterprise Access Control List* dialog box.

The MAC address appears in the **Access Control List** table.

- 8 Click **Add** again to add additional MAC addresses, or click **OK** to return to the Enterprise Management Console.

## **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.

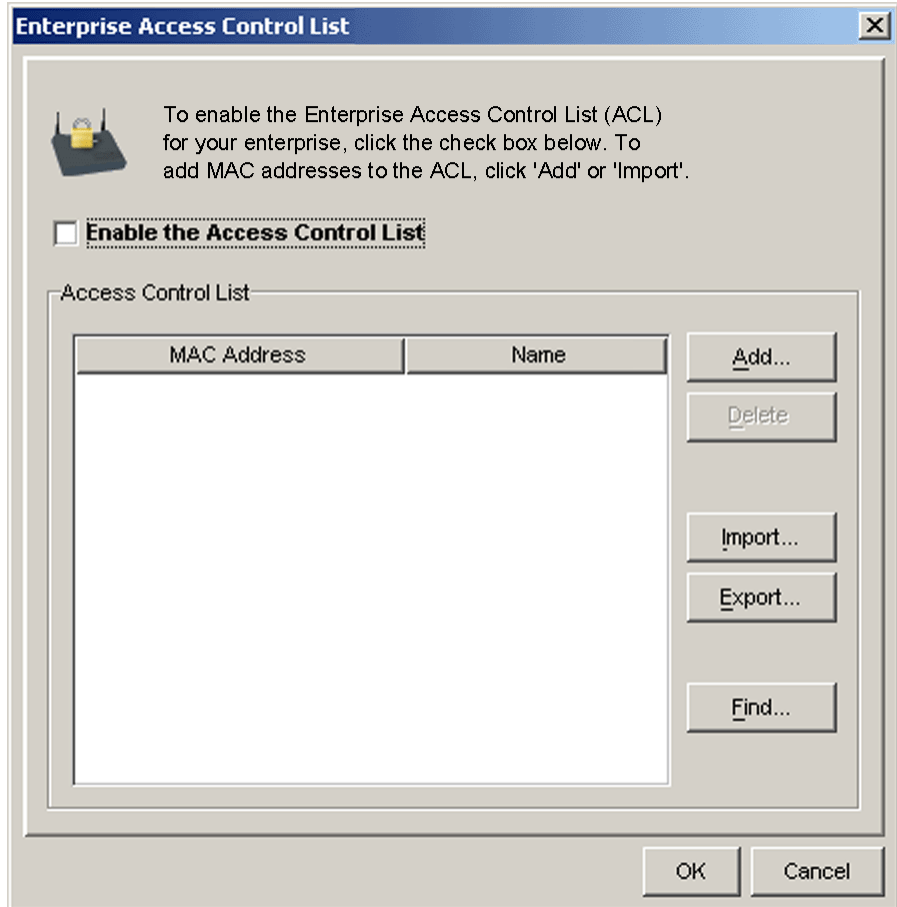
### **To modify the name of an Access Control List entry:**

- 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 **Access Control List** from the **Tools** menu.

The *Enterprise Access Control List* dialog box appears.



**Figure 8-4.** *The Enterprise Access Control List Dialog Box*

- 3 Select an entry from the Very Large Access Control List.
- 4 Right-click the appropriate entry and select Rename from the menu that appears.

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

- 5 Type the new name.

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

- 6 Click OK.

## **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.

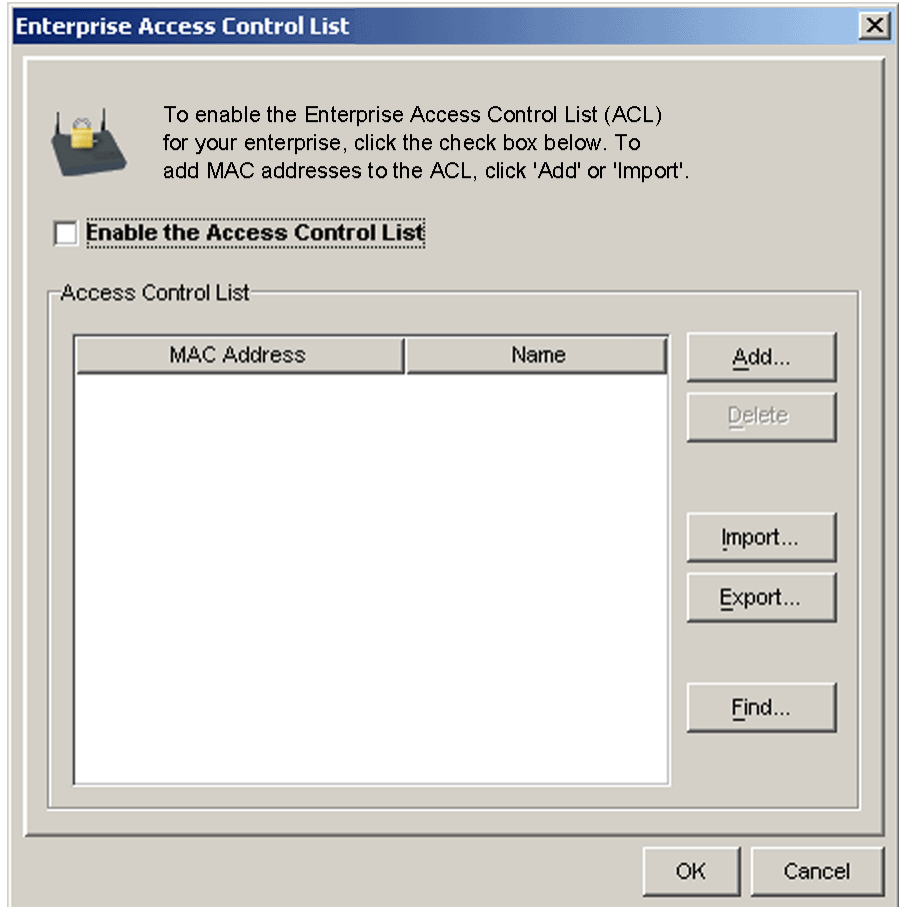
### **To remove a Very Large Access Control List entry:**

- 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 `Access Control List` from the **Tools** menu.

The *Enterprise Access Control List* dialog box appears.



**Figure 8-5.** *The Enterprise Access Control List Dialog Box*

**3** Select the entry you want to remove.

**4** Click `Delete`.

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

**5** 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:

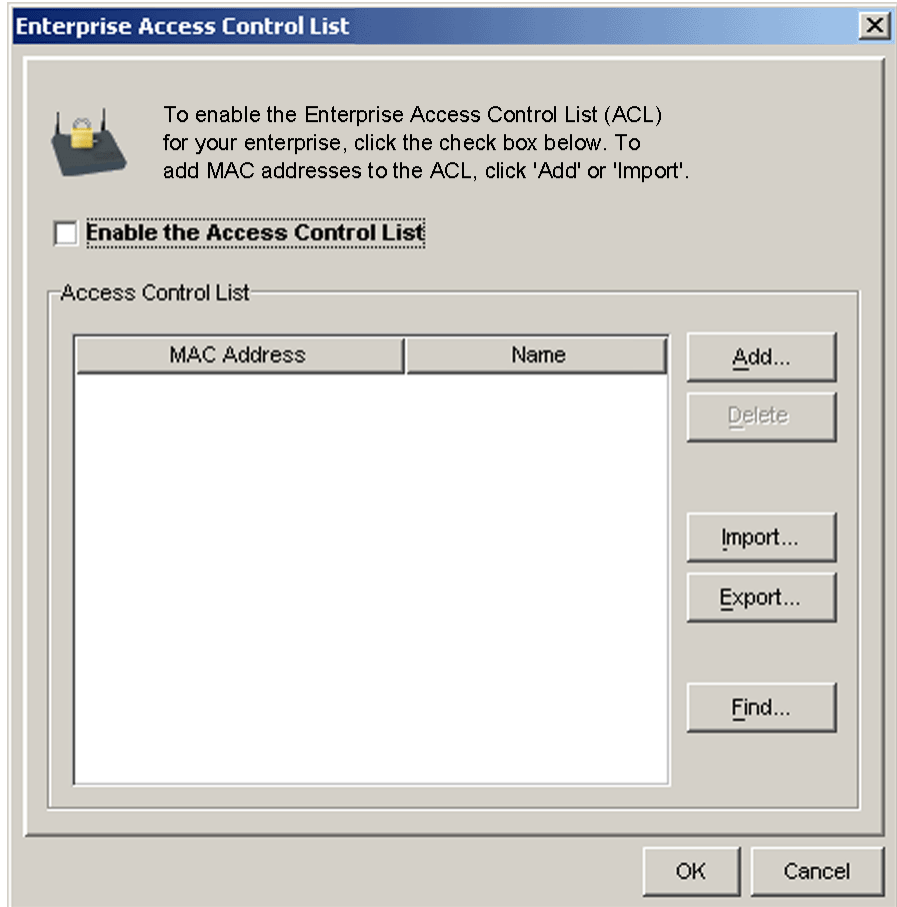
- 1 Select a group from the Groups window.

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

- 2 Select `Access Control List` from the **Tools** menu.

The *Enterprise Access Control List* dialog box appears.





**Figure 8-6.** The Enterprise Access Control List Dialog Box

- 3 Click **Export**.

A standard *Save* dialog box appears.

- 4 Navigate to where you want to save the Access Control List text file.

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

- 5 Click **Save**.

If you want to import an 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.

---

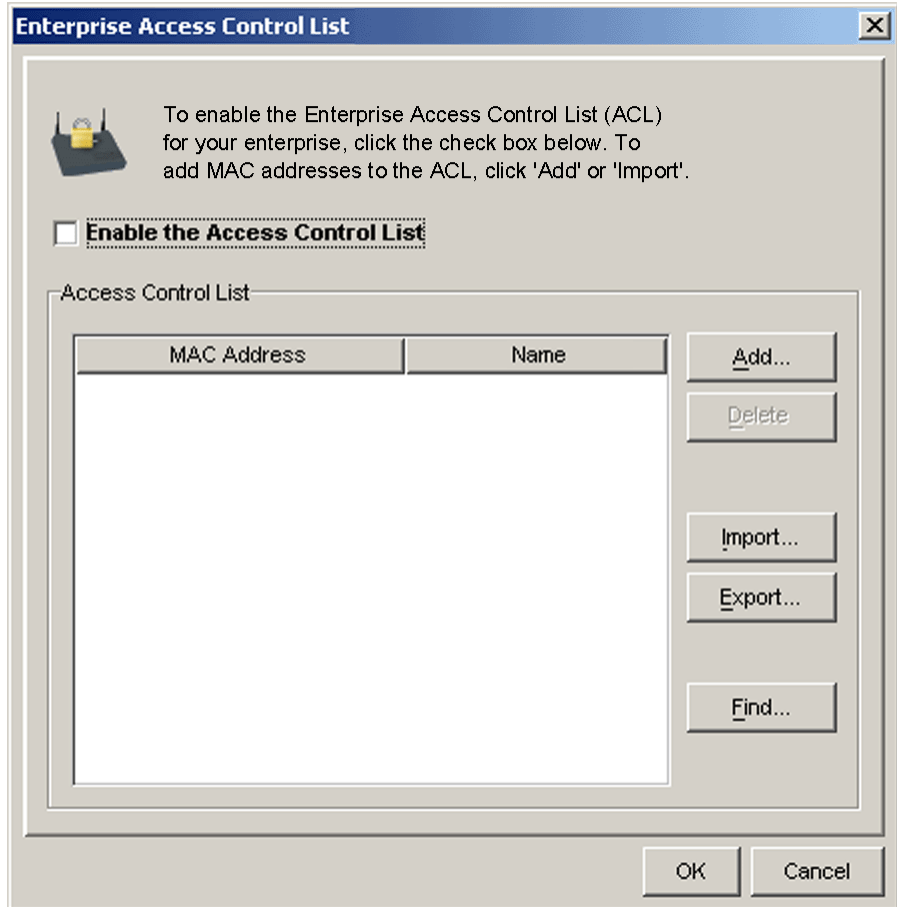
**To import an Access Control List file:**

- 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 Access Control List from the **Tools** menu.

The *Enterprise Access Control List* dialog box appears.



**Figure 8-7.** The Enterprise Access Control List Dialog Box

- 3 Click Import.

A standard *Open* dialog box appears.

- 4 Locate and select the text file.

- 5 Click Open.

The *Access Control List* dialog box updates to display the added entries.

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

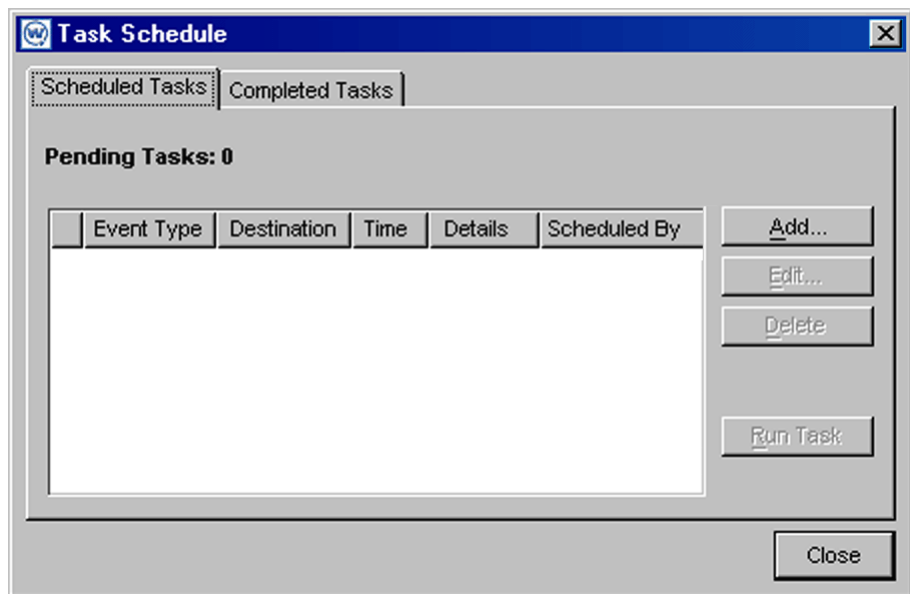
## Deploying Access Control Lists

After you create an Access Control List, you can deploy it to selected sites and groups.

### To deploy an Access Control List:

- 1 Select **Task Schedule** from the **Tools** menu.

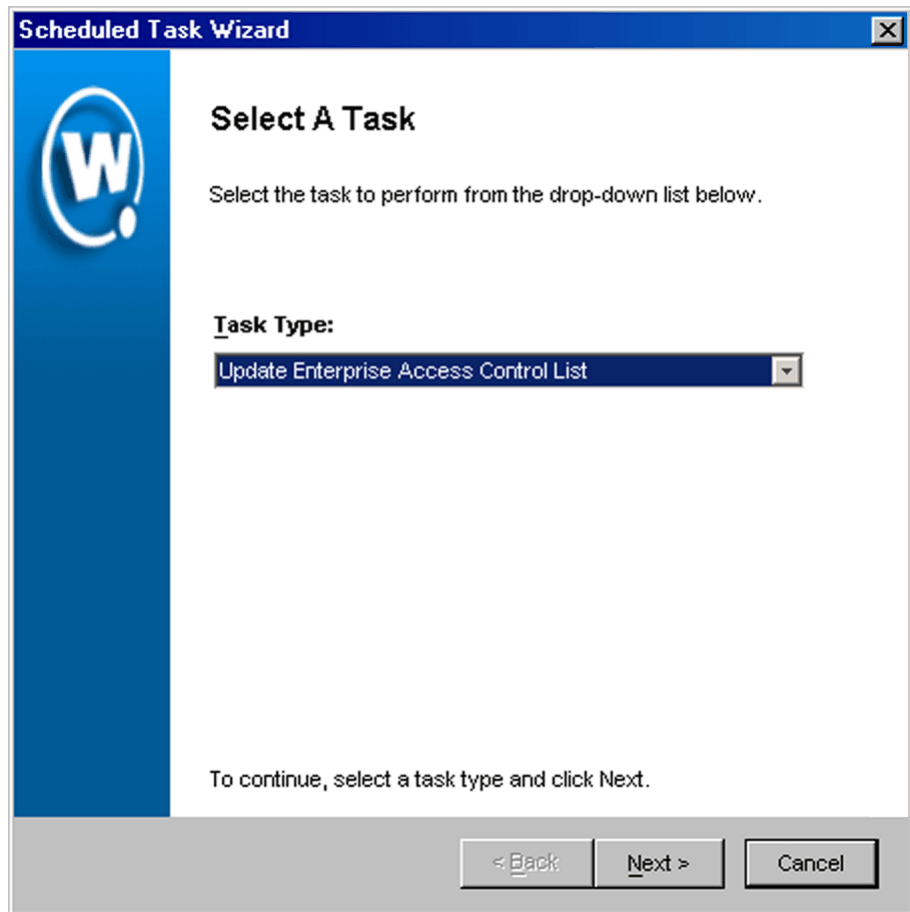
The *Task Schedule* dialog box appears.



**Figure 8-8.** The *Task Schedule* Dialog Box

- 2 Click **Add**.

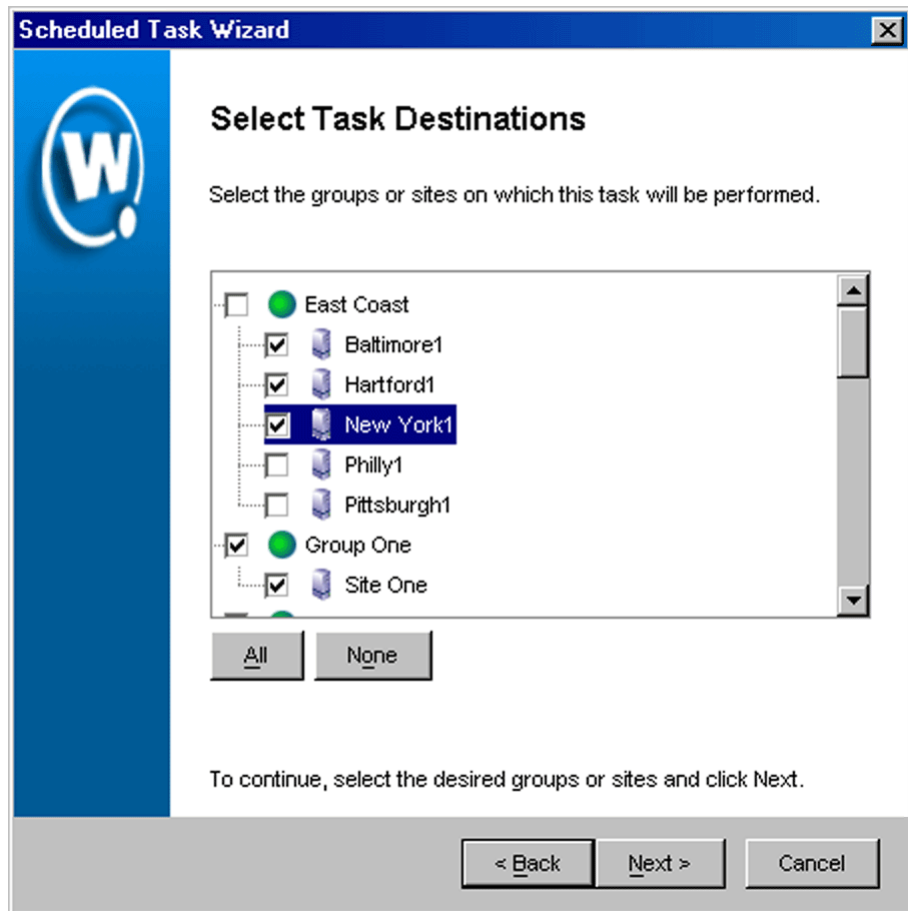
The *Select A Task* dialog box appears.



**Figure 8-9.** *The Select A Task Dialog Box*

- 3 Select Update Very Large Access Control List from the **Task Type** list and click Next.

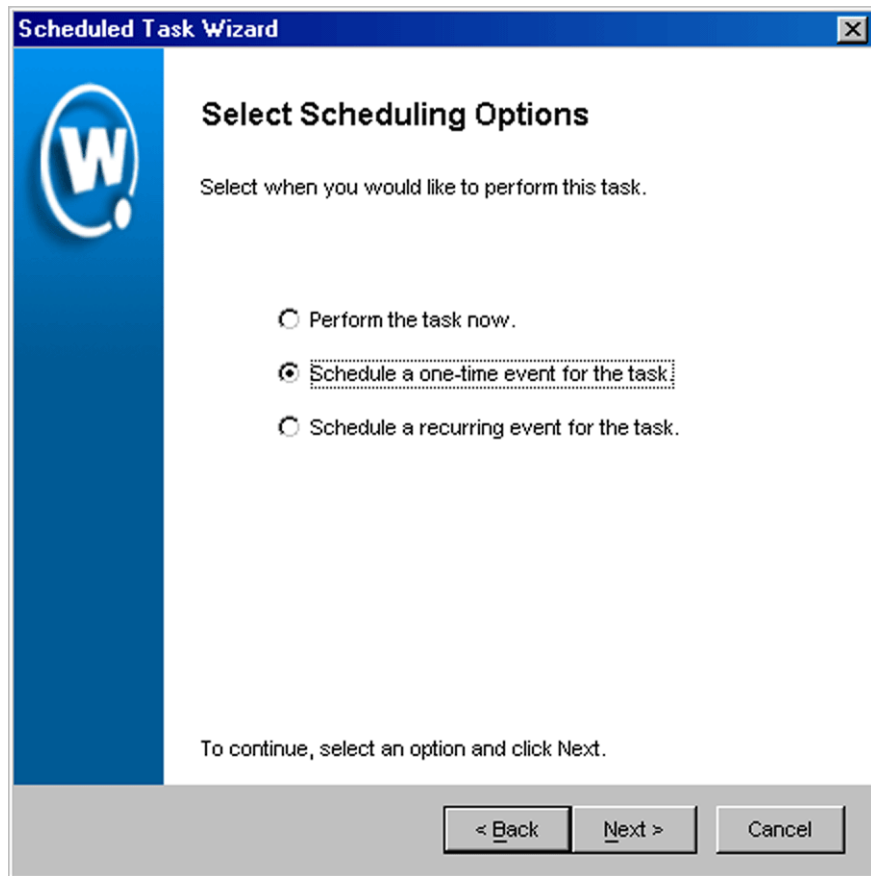
The *Select Task Destination* dialog box appears.



**Figure 8-10.** *The Select Task Destination Dialog Box*

- 4 Select the groups or sites by enabling the checkbox next to the group or site name. You can also select all groups by clicking **All**.
- 5 Click **Next**.

The *Select Scheduling Options* dialog box appears.



**Figure 8-11.** *The Select Scheduling Options Dialog Box*

**6** Determine when the event will occur.

If you want the event to occur immediately select the **Perform the task now** option.

If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

If you want the event to occur on a regular basis, select the **Schedule a recurring event** for this task option.

**7** Click **Next**.

- 8 If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.

**Scheduled Task Wizard**

### Schedule the Time Window

Select the start time and end time during which you would like to perform this task.

Start Time: 08 /19 / 2003 11:45

Run until complete

End by: 08 /19 / 2003 12:00

Use Site's Local Time

To continue, click Next.

< Back Next > Cancel

**Figure 8-12.** *The Schedule the Time Window Dialog Box*

Within this dialog box, you can set the following parameters for the event:

- Select the start date and time for the event.
- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the



event is not finished by this date and time, Mobile Manager will generate an alert.

- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.
- 9 If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

**Scheduled Task Wizard**

### Configure Task Recurrence

Use the controls below to configure the recurrence settings

**Task time**

Start Time: 00:00  Run until complete  Use Site's Local Time  
 End by: 00:00

**Recurrence pattern**

Daily  Weekly  Monthly

Recur every 1 week(s) on:

Sunday  Monday  Tuesday  Wednesday  
 Thursday  Friday  Saturday

**Range of recurrence**

Start: 08 / 19 / 2003  No end date  
 End by: / /

To continue, click Next.

< Back   Next >   Cancel

**Figure 8-13.** The *Configure Task Recurrence* Dialog Box

Within this dialog box, you can set the following parameters for this event:

- Select the start time for the event.
- Determine when you want the event to stop. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.
- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

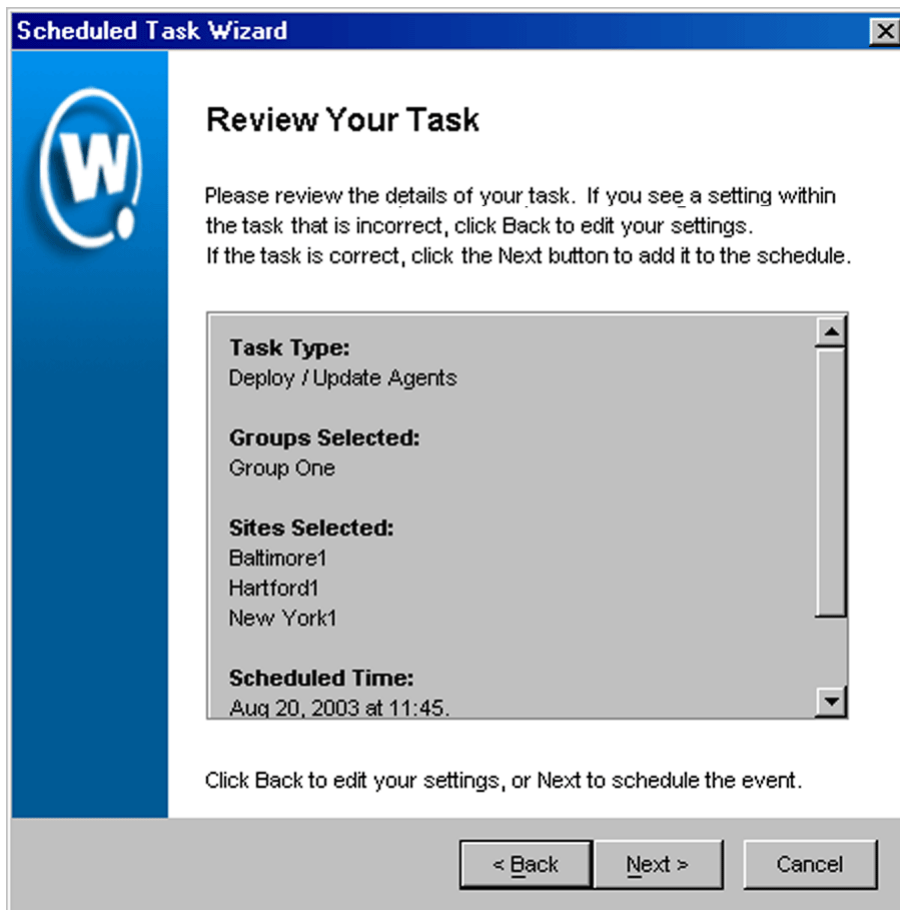
---

**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

**10** Click *Next*.

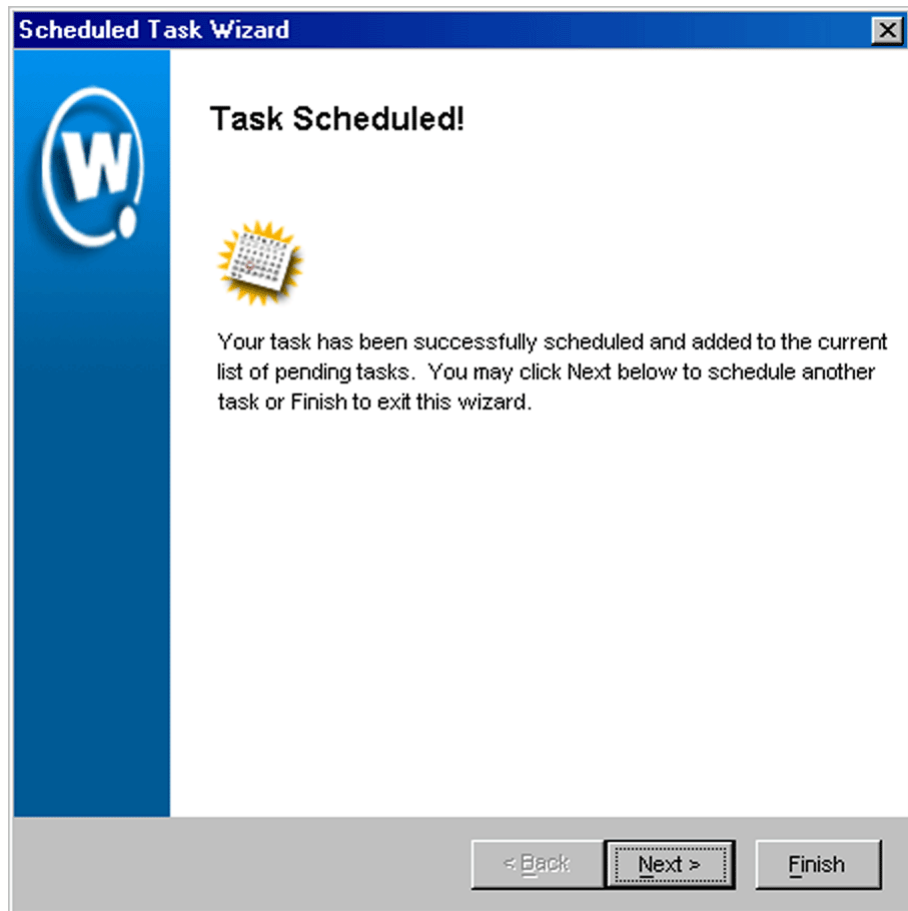
The *Review Your Task* dialog box appears.



**Figure 8-14.** *The Review Your Task Dialog Box*

**11** Review your the task to ensure that it is correct and click Next.

The *Task Scheduled* dialog box appears.



**Figure 8-15.** *The Task Scheduled Dialog Box*

- 12 Click **Next** to schedule a new event, or click **Finish** to return to the Task Schedule dialog box.

## 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** Mobile Manager Enterprise only tracks the WEP keys that were assigned to access points through the Enterprise Management Console. Consequently, WEP keys displayed in the console might not match the keys for an access point if you modified them from outside of Mobile Manager Enterprise.

---

## Types of WEP Key Deployments

Mobile Manager Enterprise 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, Mobile Manager Enterprise includes a unique method of deployment: automatic WEP rotation. By deploying the automatic WEP rotation feature, Mobile Manager Enterprise 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 332 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 Mobile Manager Enterprise's automatic WEP rotation feature, see *Automatic WEP Rotation* on page 332.

### 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 `WEP Settings` tab.
- 4 Enable the **Use Static WEP Only** checkbox.

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

6 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.

7 Click **OK**.

---

**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, Mobile Manager Enterprise 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.

---

**NOTE** Automatic WEP rotation settings are not recoverable. If the system hosting the access point Agent becomes unavailable (for example, due to a hardware crash), you must re-connect serially to each mobile device to ensure that WEP key settings are correctly synchronized.

---

## 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:**

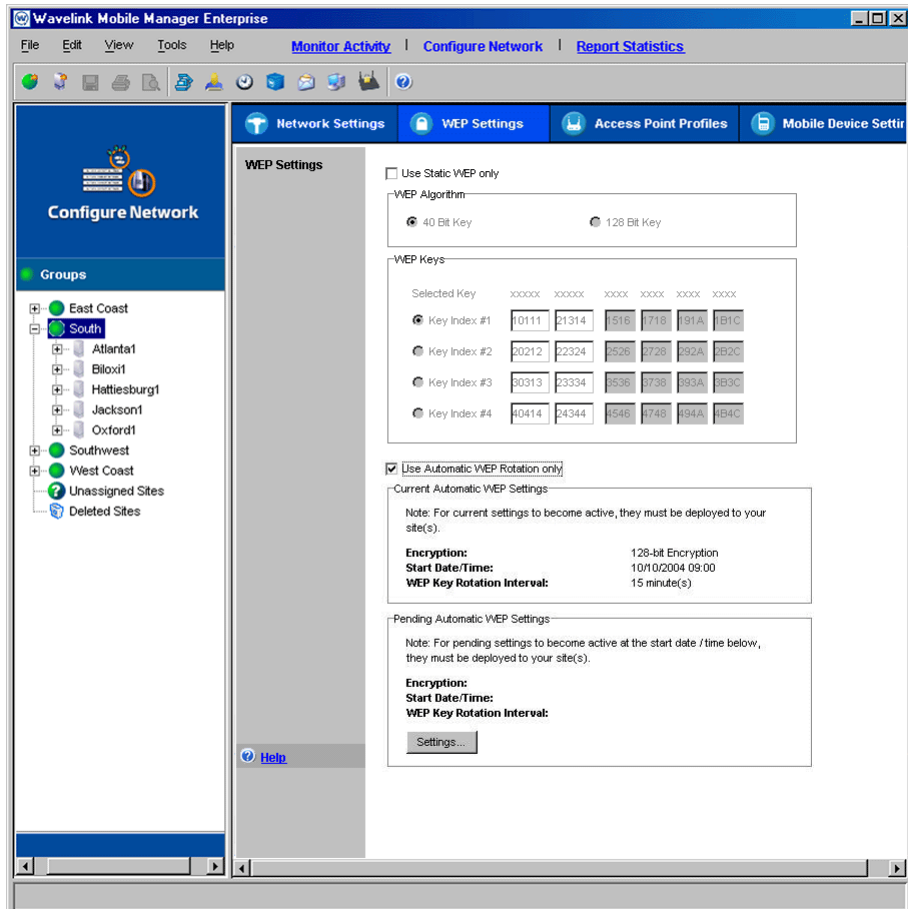
**1** Select a group from the Groups window.

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 `WEP Settings` tab.

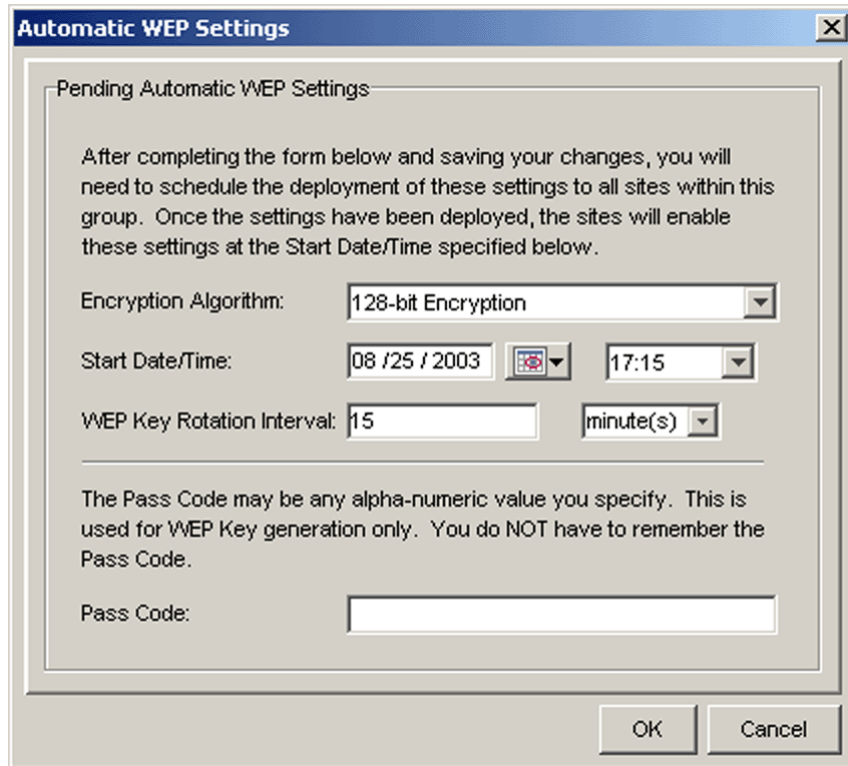




**Figure 8-16.** The WEP Settings Tab of the Configure Network View

**4** Enable the **Use Automatic WEP Rotation Only** checkbox.

The *Automatic WEP Settings* dialog box appears.



The image shows a dialog box titled "Automatic WEP Settings" with a close button (X) in the top right corner. The dialog box contains the following elements:

- A title bar: "Automatic WEP Settings" with a close button (X).
- A section header: "Pending Automatic WEP Settings".
- Instructional text: "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: A dropdown menu set to "128-bit Encryption".
- Start Date/Time: Two text boxes. The first contains "08 /25 / 2003" and has a calendar icon button to its right. The second contains "17:15".
- WEP Key Rotation Interval: A text box containing "15" and a dropdown menu set to "minute(s)".
- Pass Code instructions: "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: A text box for entering the pass code.
- Buttons: "OK" and "Cancel" buttons at the bottom right.

**Figure 8-17.** *The Automatic WEP Settings Dialog Box*

- 5 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.
- 6 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).

You can also use the **Calendar** button to select the start date.

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

The value in this text box determines when Mobile Manager Enterprise 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.

---

- 8 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.

- 9 Click **OK**.

You can now use this automatic WEP rotation setup for your access point profiles. The settings you selected will appear in the WEP pane in the **Pending Automatic WEP Settings** box. Once the start time passes, the values move to the **Current Automatic WEP Settings** box.

## Stopping Automatic WEP Rotation

If you decide that you no longer want to use automatic WEP key rotation, you must inform the access points and mobile devices.

---

**NOTE** For mobile devices, you must use Wavelink Avalanche to stop automatic WEP rotation.

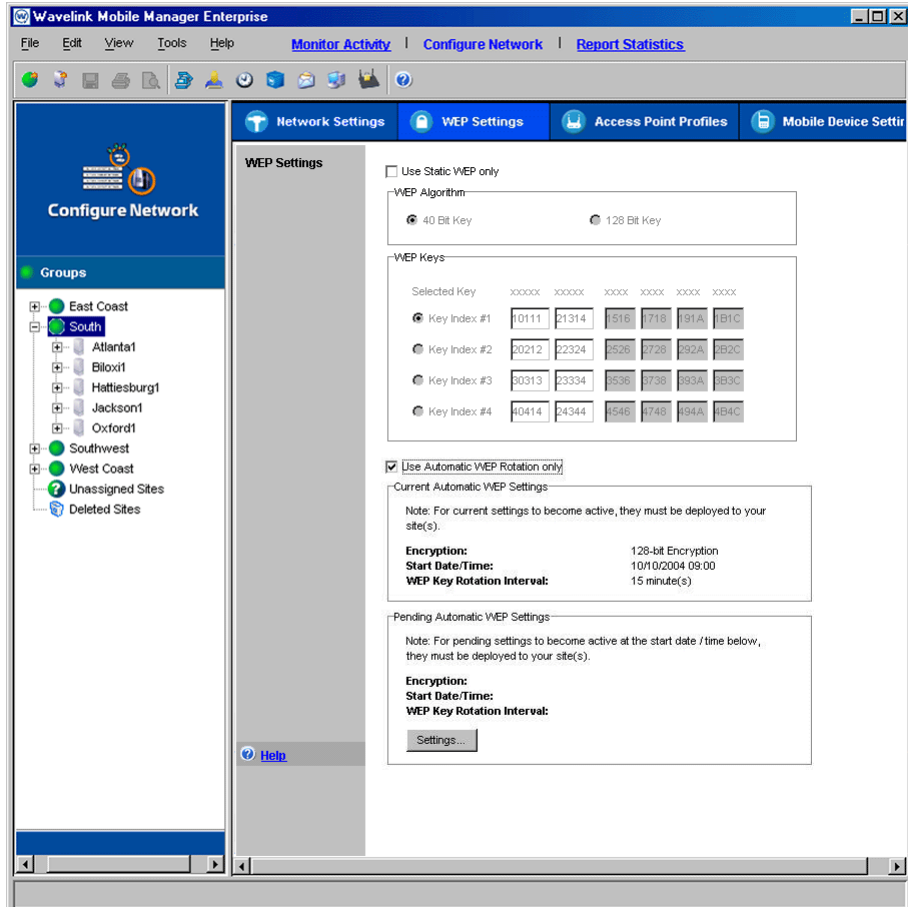
---

### To stop automatic WEP rotation for access points:

- 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.

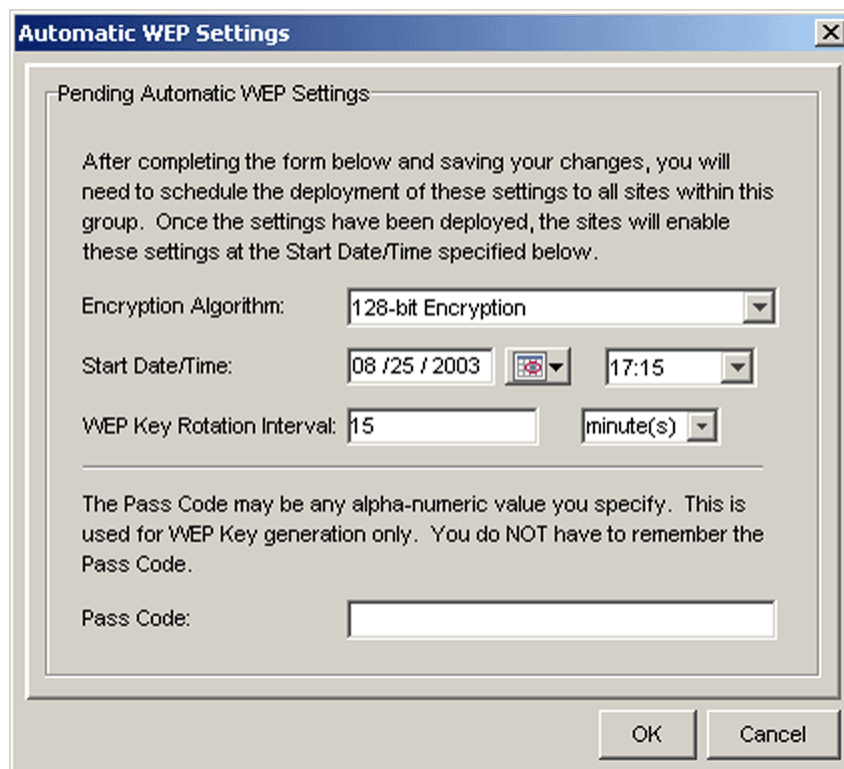
- 2 Select **Configure Network**.
- 3 Click the **WEP Settings** tab.



**Figure 8-18.** The WEP Settings Tab of the Configure Network View

- 4 Enable the **Use Automatic WEP Rotation Only** checkbox.
- 5 Click **Settings**.

The *Automatic WEP Settings* dialog box appears.



**Figure 8-19.** *The Automatic WEP Settings Dialog Box*

- 6 Ensure that the **Pending** option is selected.
- 7 Select **Stop Using Rotation** from the **WEP Algorithm** list.
- 8 Type the time when you want to stop using automatic WEP rotation in the **Start 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 type the start time (including hours and minutes).

---

**NOTE** The start time must be more than 48 hours later than the current time and date.

---

9 Click **Apply**.

10 Deploy your settings to the appropriate sites.

At the time you specify, the access points will stop using automatic WEP rotation.

### **Automatic WEP Rotation and Cisco IOS VLANs**

If you use VLANs with Cisco IOS access points, you have the option of using Mobile manager's automatic WEP rotation feature to protect those VLANs from unauthorized eavesdropping or intrusion. Automatic WEP rotation is a security enhancement available to organizations using both Mobile Manager and Avalanche.

---

**NOTE** Automatic WEP rotation is only available through an access point profile. If you are unfamiliar with access point profiles, see *Creating Access Point Profiles* on page 160. Also, information on automatic WEP rotation is available in *Automatic WEP Rotation* on page 332.

---

For automatic WEP rotation to work correctly both access points and mobile devices must be synchronized with the correct WEP settings. To ensure that these settings are synchronized, Mobile Manager requires a 48-hour timeframe to start or stop automatic WEP rotation, which starts after you deploy the new settings to the appropriate sites. This timeframe helps ensure that all affected mobile devices can receive the correct WEP rotation information.

#### **To configure VLANs of Cisco IOS access points to use automatic WEP rotation:**

1 Stop automatic WEP rotation, if it is enabled.

See *Stopping Automatic WEP Rotation* on page 337 for information on how to stop automatic WEP rotation.

You must allow 48 hours to completely stop automatic WEP rotation. This 48-hour period begins after you deploy the information to the appropriate sites.

2 Enable and configure WEP key rotation settings as needed.

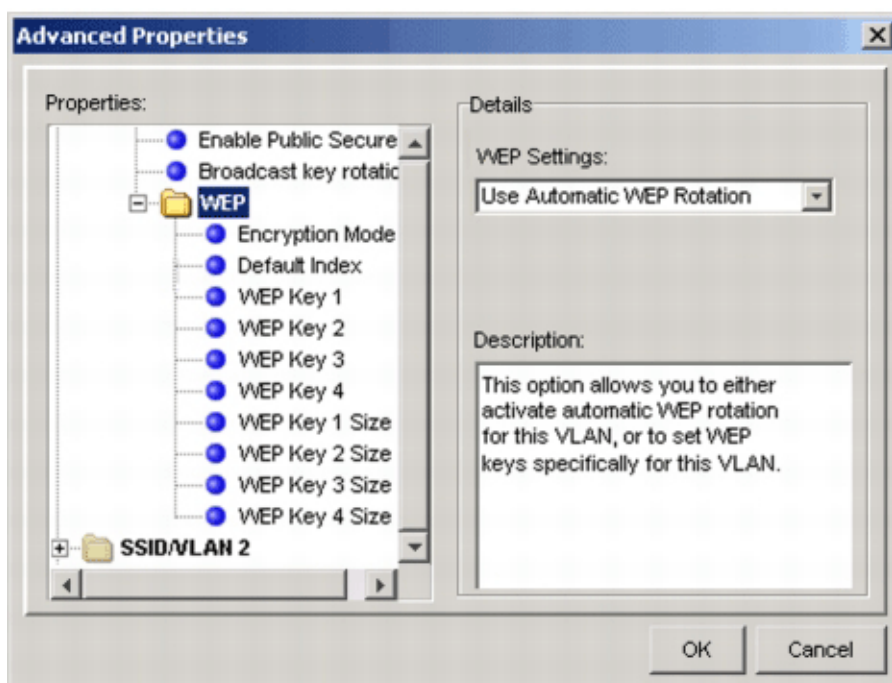
Information on configuring WEP key rotation is available in *Configuring Automatic WEP Rotation* on page 333.

You must allow 48 hours to completely start automatic WEP rotation. This 48-hour period begins after you deploy the information to the appropriate sites.

- 3 Create a profile for the access points for which you will configure one or more VLANs that use automatic WEP rotation.

To learn how to create an access point profile, see *Chapter 5: Managing Access Points* on page 153.

- 4 When you create the profile, select the WEP folder from the *Advanced Properties* dialog box for the VLAN.



**Figure 8-20.** The WEP Folder of the Advanced Properties Dialog Box

To access this folder, open the *Advanced Properties* dialog box for the access point profile. Within this folder, open the *SSID/VLAN Setup* folder, then the *SSID/VLAN* folder, and then the *VLAN* folder.

In the *Details* section of the dialog box, the **WEP Settings** list appears.

- 5 Select Use Automatic WEP Rotation from the **WEP Settings** list.
- 6 Click **OK**.
- 7 Deploy the settings to the appropriate sites.

### **Automatic WEP Rotation and Proxim VLANs**

If you use VLANs with Proxim access points, you have the option of using Mobile manager's automatic WEP rotation feature to protect those VLANs from unauthorized eavesdropping or intrusion. Automatic WEP rotation is a security enhancement available to organizations using both Mobile Manager and Avalanche.

---

**NOTE** Automatic WEP rotation is only available through an access point profile. If you are unfamiliar with access point profiles, see *Chapter 5: Managing Access Points* on page 153. Also, information on automatic WEP rotation is available in *Configuring Automatic WEP Rotation* on page 333.

---

For automatic WEP rotation to work correctly both access points and mobile devices must be synchronized with the correct WEP settings. To ensure that these settings are synchronized, Mobile Manager requires a 48-hour timeframe to start or stop automatic WEP rotation, which starts after you deploy the new settings to the appropriate sites. This timeframe helps ensure that all affected mobile devices can receive the correct WEP rotation information.

#### **To configure VLANs of Proxim access points to use automatic WEP rotation:**

- 1 Stop automatic WEP rotation, if it is enabled.

See *Stopping Automatic WEP Rotation* on page 337 for information on how to stop automatic WEP rotation.

You must allow 48 hours to completely stop automatic WEP rotation. This 48-hour period begins after you deploy the information to the appropriate sites.

- 2 Enable and configure WEP key rotation settings as needed.

Information on configuring WEP key rotation is available in *Configuring Automatic WEP Rotation* on page 333.

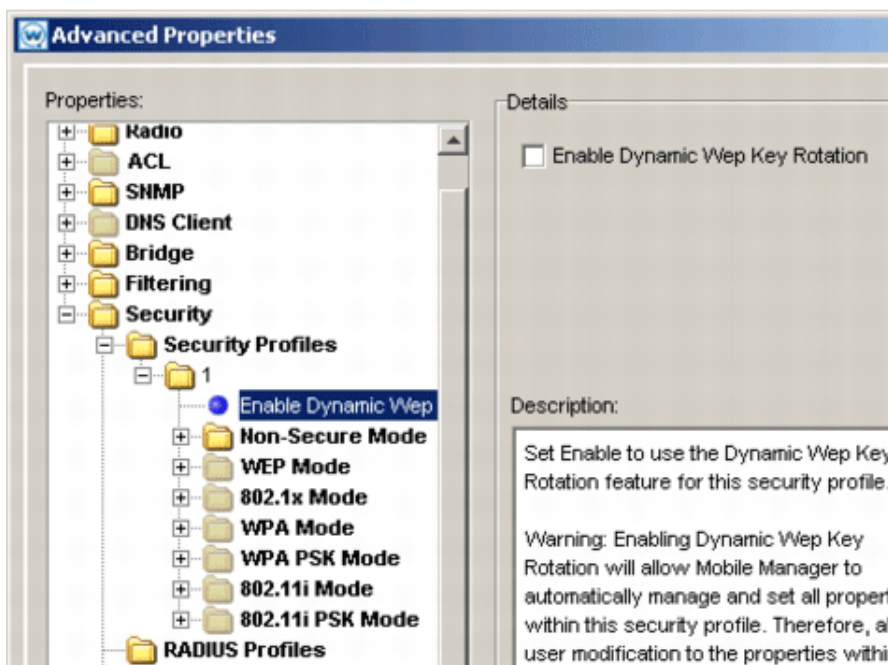


You must allow 48 hours to completely start automatic WEP rotation. This 48-hour period begins after you deploy the information to the appropriate sites.

- 3 Create a profile for the access points for which you will configure one or more VLANs that use automatic WEP rotation.

To learn how to create an access point profile, see *Chapter 5: Managing Access Points* on page 153.

- 4 If the profile is for Proxim 2000 access points, select the appropriate Wireless Interface folder from the *Advanced Properties* dialog box for the VLAN.



**Figure 8-21.** The Enable Auto WEP Rotation Option of the Advanced Properties Dialog Box

To access this folder, open the *Advanced Properties* dialog box for the access point profile. Within this folder, open the *Security* folder, then the *WEP* folder, and then the *Wireless Interface* folder.

---

**NOTE** If this folder is grayed out, select the folder and enable the **Enable** checkbox located in the Details section of the dialog box.

---

- 5 If the profile is for Proxim 600 access points, select the WEP folder from the *Advanced Properties* dialog box for the VLAN.

To access this folder, open the *Advanced Properties* dialog box for the access point profile. Within this folder, open the Security folder, and then the WEP folder.

---

**NOTE** If this folder is grayed out, select the WEP folder and enable the **Enable** checkbox located in the Details section of the dialog box.

---

- 6 Select the **Enable Auto WEP Rotation** option.

In the Details section of the dialog box, the **Enable Auto WEP Rotation** checkbox appears.

- 7 Enable the **Enable Auto WEP Rotation** checkbox.
- 8 Deploy the settings to the appropriate sites.

## 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.

---

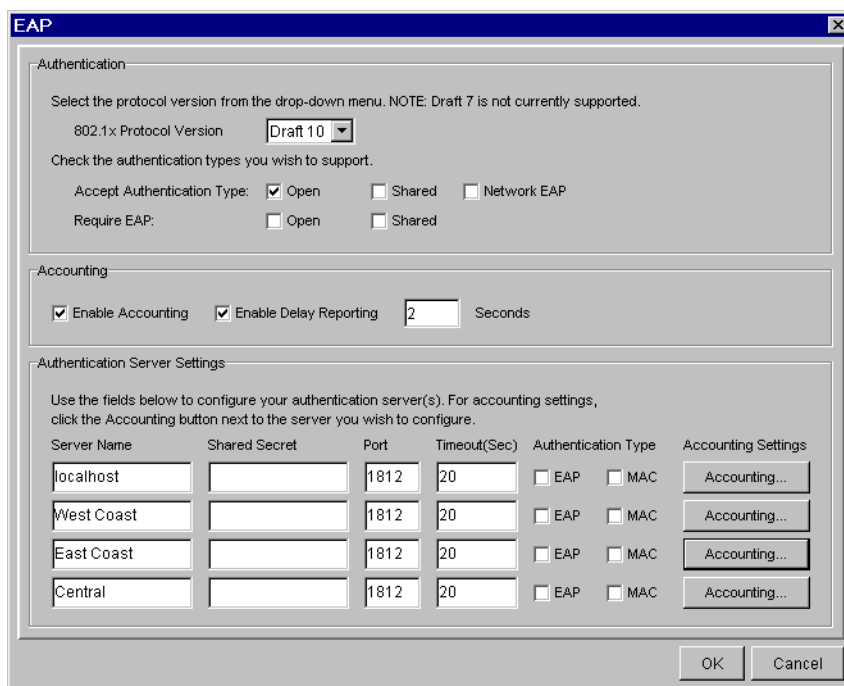
**NOTE** These options are only available within an access point profile.

---

### 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 `Cisco EAP Settings`.  
The *EAP* dialog box appears.



**Figure 8-22.** *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 Mobile Manager Enterprise 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 347 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.

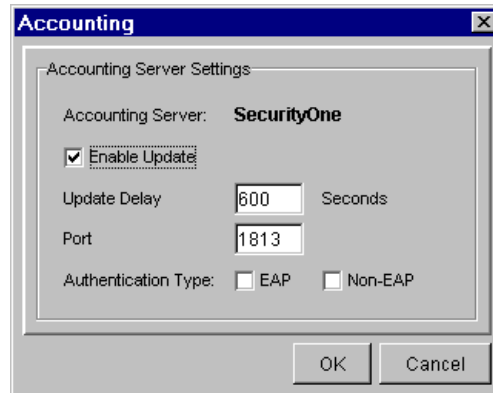
### To enable EAP Accounting:

- 1 Open a profile for which you have enabled EAP.

See *Extensible Authentication Protocol (EAP)* on page 344 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.



**Figure 8-23.** *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.

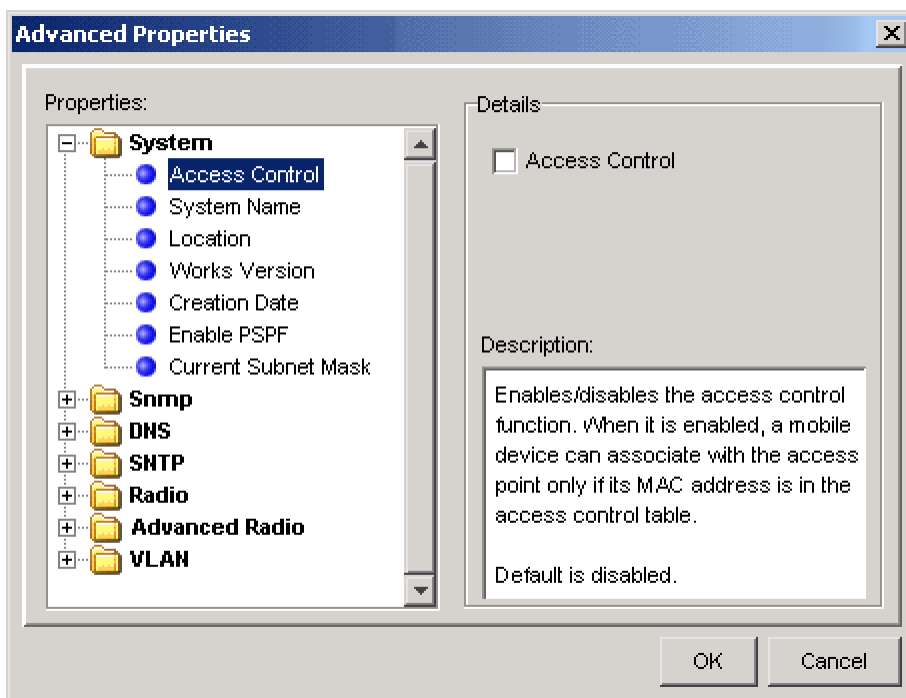
**To configure advanced security options:**

- 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 `Advanced`.

The *Advanced Properties* dialog box appears.



**Figure 8-24.** The *Advanced Properties* Dialog Box

- 6 Open the Advanced Radio folder.
- 7 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.

- 8 Configure the property as needed.

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

- 9 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 security settings for a group, you can deploy those settings by scheduling the following deployment events:

- Deploying Security Settings for All Devices
- Deploying Security Settings to Access Points
- Deploying Security Settings to Mobile Devices

### Deploying Security Settings for All Devices

Under most circumstances, you will want to deploy security settings to both access points and mobile devices simultaneously. Deploying settings simultaneously prevents any inconsistencies between the configurations for mobile devices and access points, which can hinder network performance.

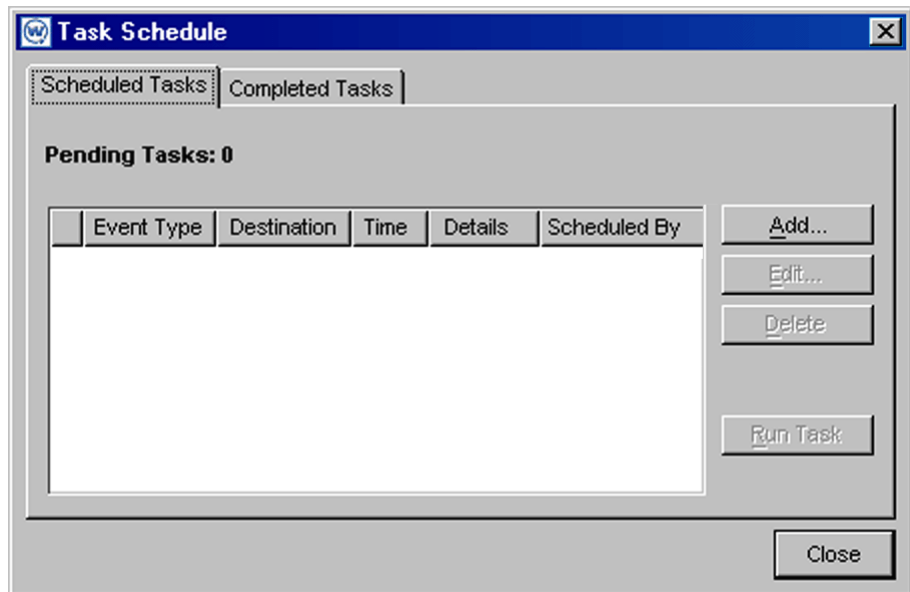
When you deploy settings for all devices, you send the following information to each Agent within the selected sites or groups:

- ESS IDs
- IP addresses
- Mobile device information (such as when to release licenses)
- Device access privileges
- WEP settings

**To deploy security settings for all devices:**

- 1 Select Task Schedule from the **Tools** menu.

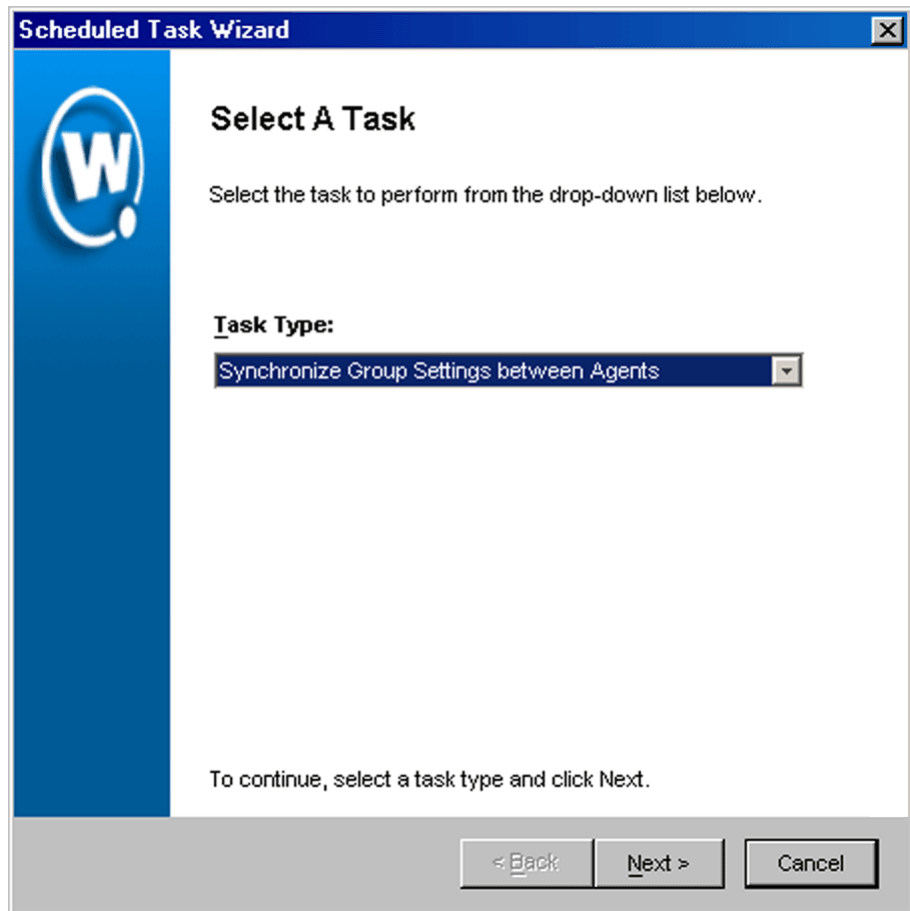
The *Task Schedule* dialog box appears.



**Figure 8-25.** *The Task Schedule Dialog Box*

- 2 Click Add.

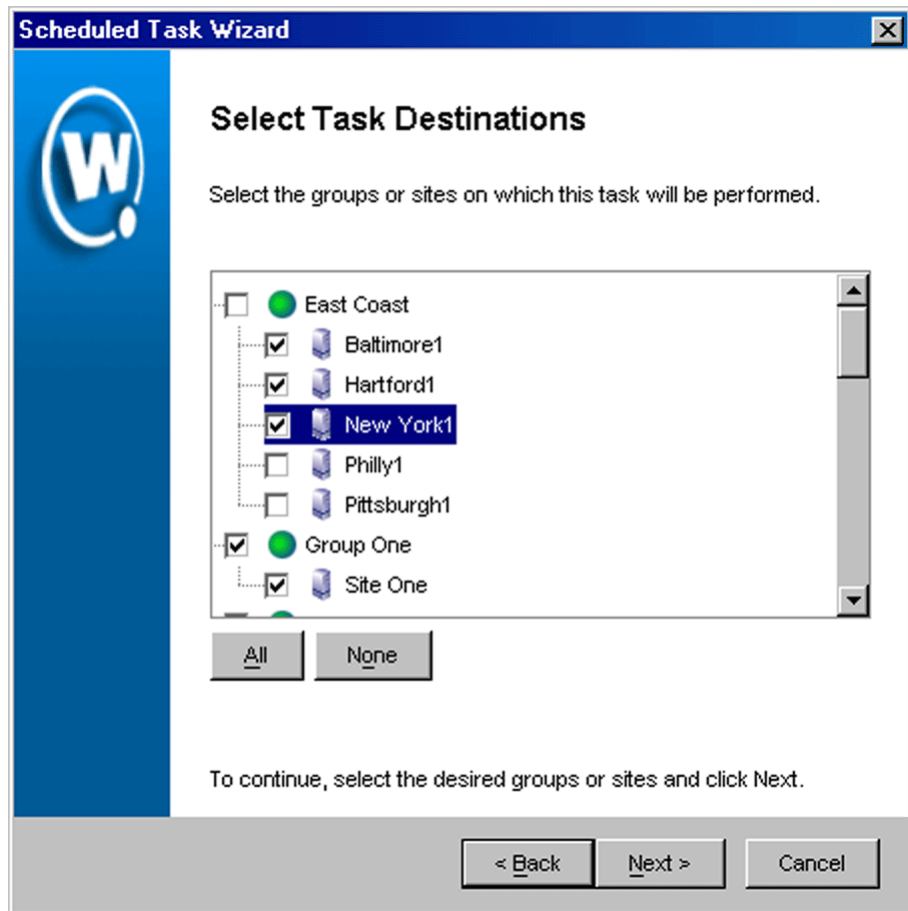
The *Select A Task* dialog box appears.



**Figure 8-26.** *The Select a Task Dialog Box*

- 3** Select *Synchronize Group Settings between Agents* from the **Task Type** list and click *Next*.

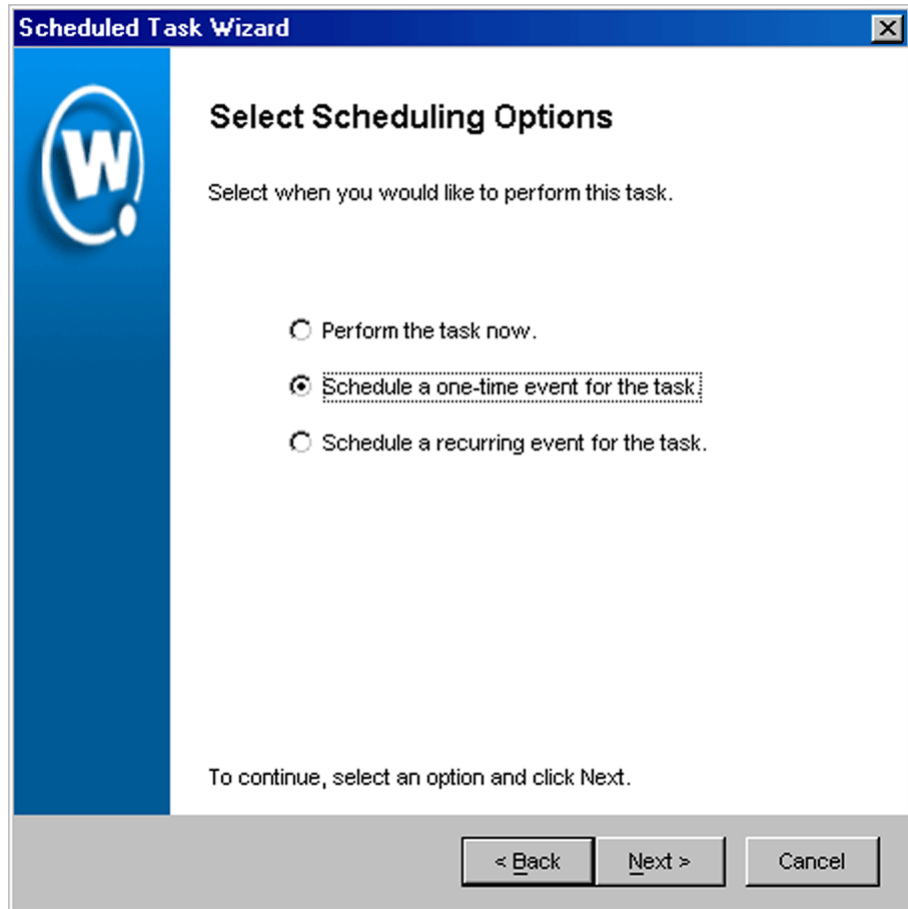
The *Select Task Destination* dialog box appears.



**Figure 8-27.** *The Select Task Destination Dialog Box*

- 4 Select the groups or sites by enabling the checkbox next to the group or site name. You can also select all groups by clicking **All**.
- 5 Click **Next**.

The *Select Scheduling Options* dialog box appears.



**Figure 8-28.** *The Select Scheduling Options Dialog Box*

**6** Determine when the event will occur.

If you want the event to occur immediately, select the **Perform the task now** option.

If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

If you want the event to occur on a regular basis, select the **Schedule a recurring event** for this task option.

- 7 Click Next.
- 8 If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.

**Scheduled Task Wizard**

### Schedule the Time Window

Select the start time and end time during which you would like to perform this task.

Start Time: 08 /19 /2003 11:45

Run until complete

End by: 08 /19 /2003 12:00

Use Site's Local Time

To continue, click Next.

< Back Next > Cancel

**Figure 8-29.** The *Schedule the Time Window* Dialog Box

Within this dialog box, you can set the following parameters for the event:

- Select the start date and time for the event.

- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.
- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.
- 9 If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

**Scheduled Task Wizard** [X]

**Configure Task Recurrence**

Use the controls below to configure the recurrence settings

**Task time**

Start Time: 00:00  Run until complete  Use Site's Local Time  
 End by: 00:00

**Recurrence pattern**

Daily | Recur every 1 week(s) on:  
 Weekly  Sunday  Monday  Tuesday  Wednesday  
 Monthly  Thursday  Friday  Saturday

**Range of recurrence**

Start: 08 / 19 / 2003  No end date  
 End by: / /

To continue, click Next.

< Back    Next >    Cancel

**Figure 8-30.** The Configure Task Recurrence Dialog Box

Within this dialog box, you can set the following parameters for this event:

- Select the start time for the event.
- Determine when you want the event to stop. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.



- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

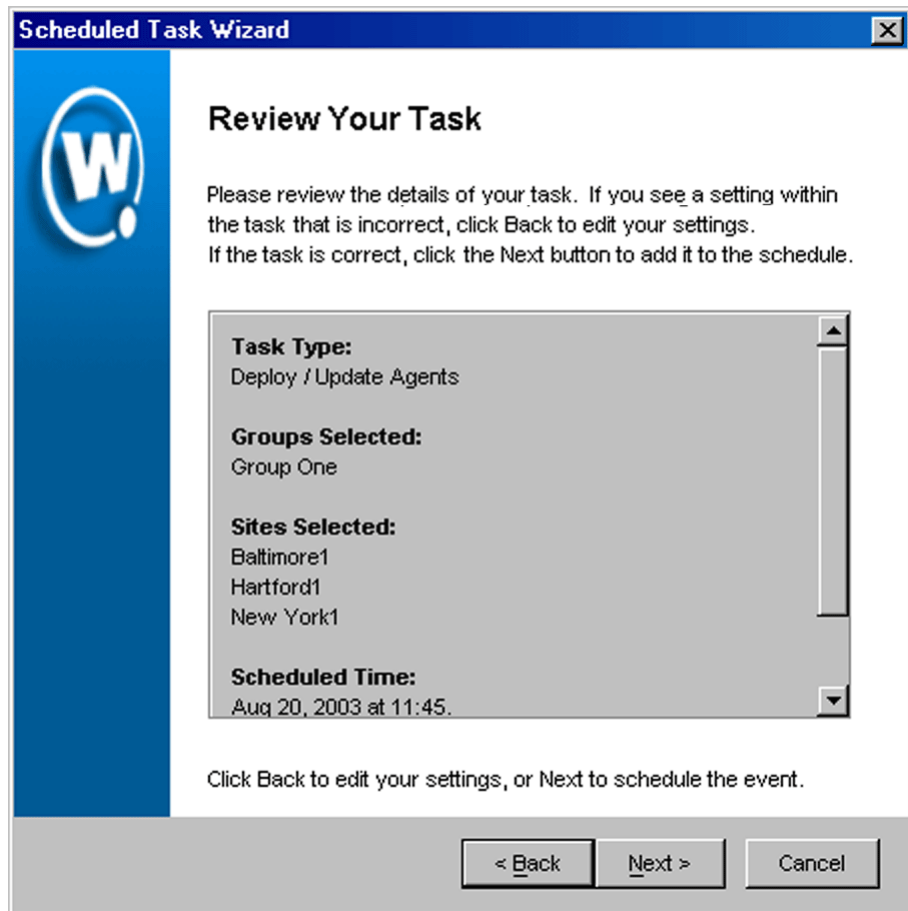
---

**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

**10** Click *Next*.

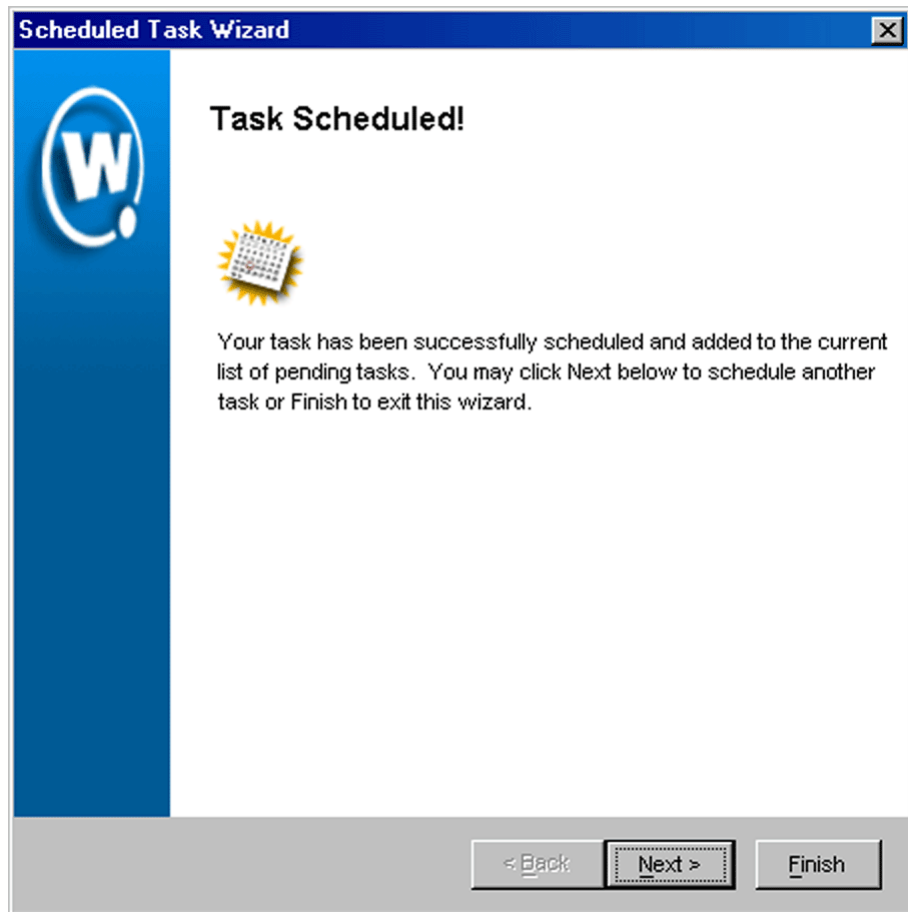
The *Review Your Task* dialog box appears.



**Figure 8-31.** *The Review Your Task Dialog Box*

**11** Review your the task to ensure that it is correct and click Next.

The *Task Scheduled* dialog box appears.



**Figure 8-32.** *The Task Scheduled Dialog Box*

- 12 Click `Next` to schedule a new event, or click `Finish` to return to the Task Schedule dialog box.

## Deploying Security Settings to Access Points

This section describes how to apply security settings to the access points within a given group.

---

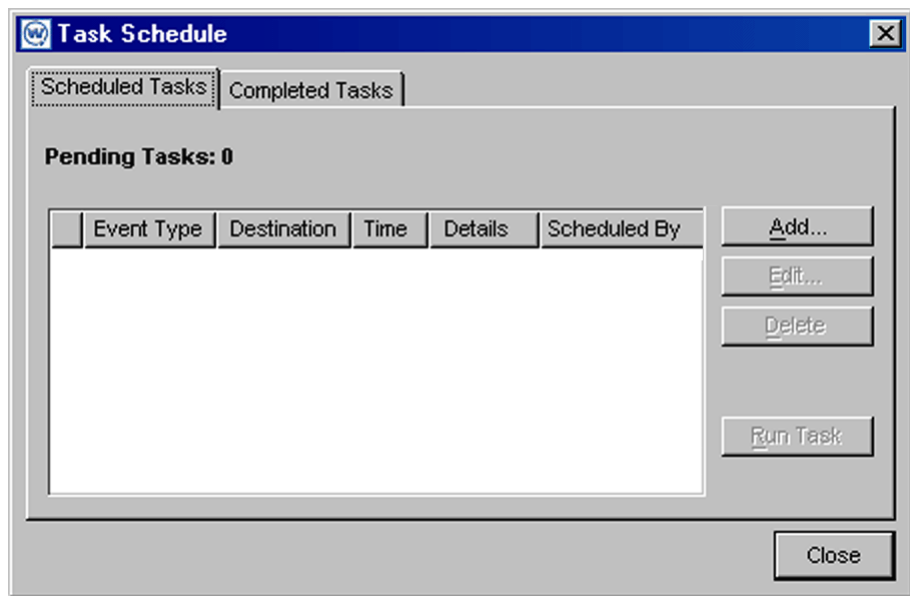
**NOTE** If you plan on deploying settings to both access points and mobile devices, it is highly recommended you follow the steps described in *Deploying Security Settings for All Devices* on page 351.

---

**To deploy security settings:**

- 1 Select **Task Schedule** from the **Tools** menu.

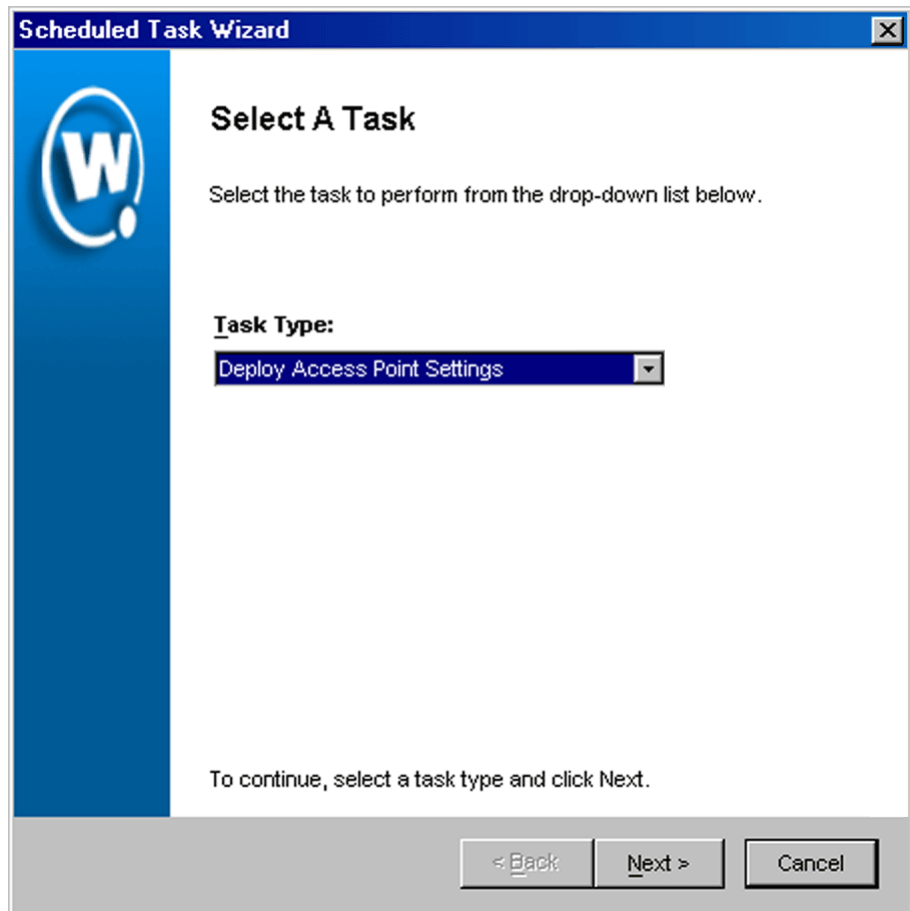
The *Task Schedule* dialog box appears.



**Figure 8-33.** *The Task Schedule Dialog Box*

- 2 Click **Add**.

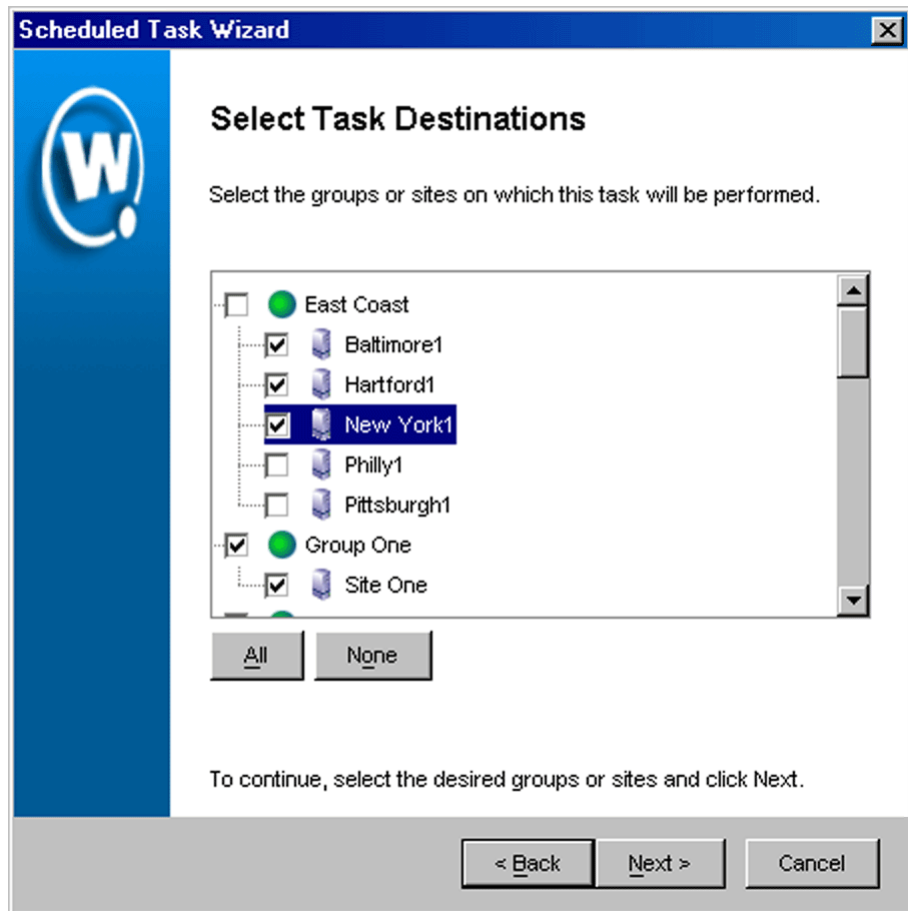
The *Select A Task* dialog box appears.



**Figure 8-34.** *The Select a Task Dialog Box*

- 3 Select `Deploy Access Point Settings` from the **Task Type** list and click `Next`.

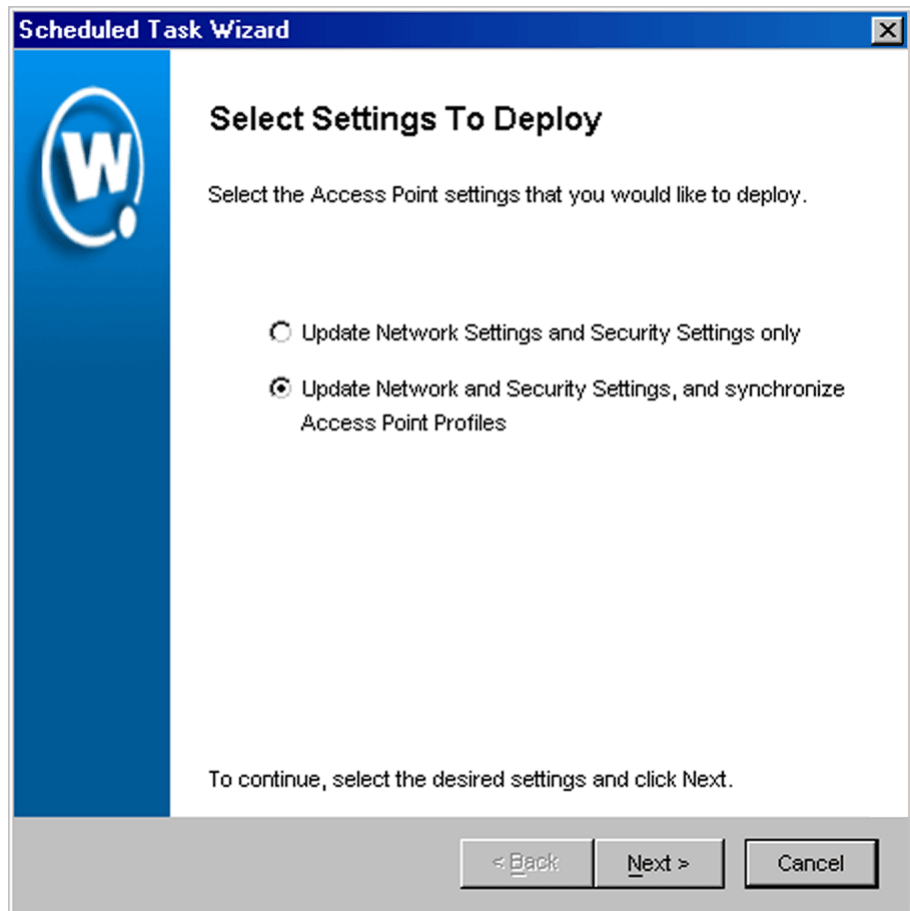
The *Select Task Destination* dialog box appears.



**Figure 8-35.** *The Select Task Destination Dialog Box*

- 4 Select the groups or sites by enabling the checkbox next to the group or site name. You can also select all groups by clicking **All**.
- 5 Click **Next**.

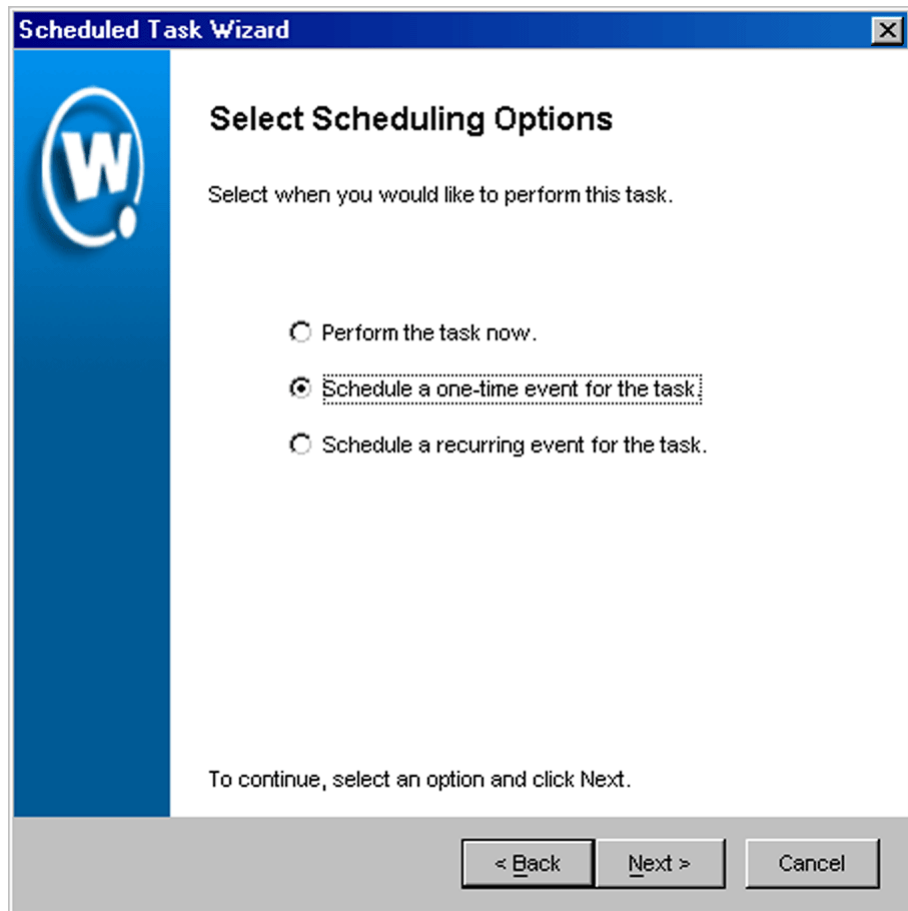
The *Select Settings to Deploy* dialog box appears.



**Figure 8-36.** *The Select Settings to Deploy Dialog Box*

- 6** Select the **Update Network Settings and Security Settings only** option.
- 7** Click **Next**.

The *Select Scheduling Options* dialog box appears.



**Figure 8-37.** *The Select Scheduling Options Dialog Box*

**8** Determine when the event will occur.

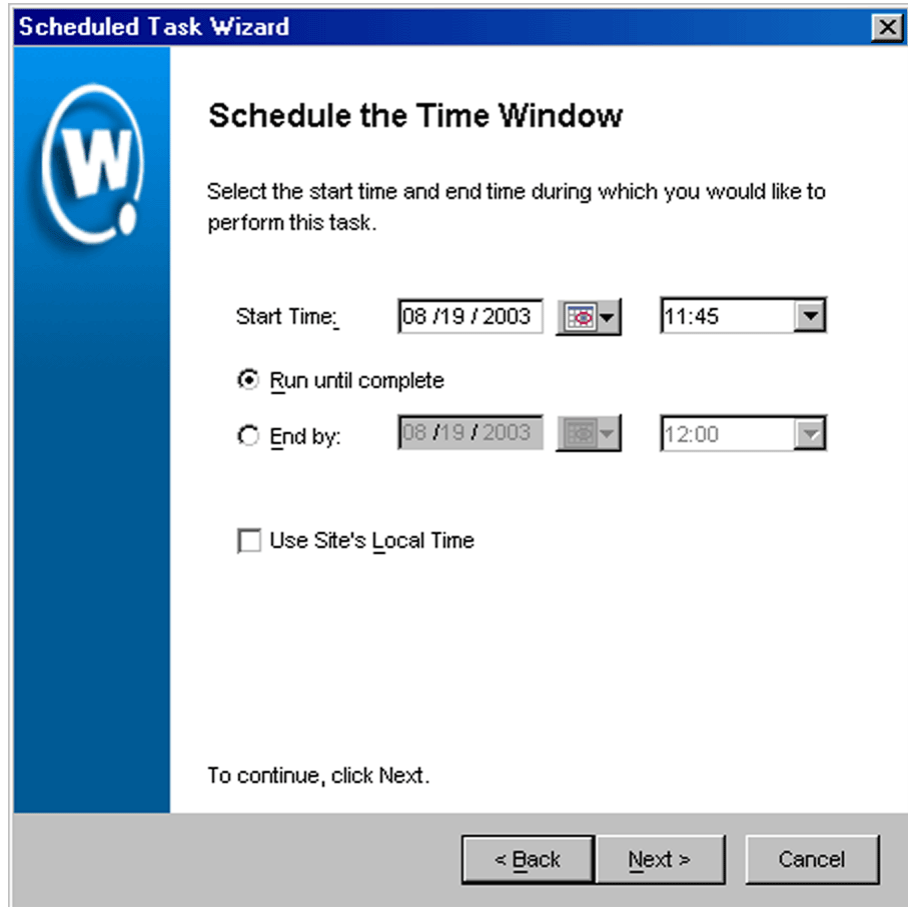
If you want the event to occur immediately, select the **Perform the task now** option.

If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

If you want the event to occur on a regular basis, select the **Schedule a recurring event** for this task option.



- 9 Click **Next**.
- 10 If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.



**Figure 8-38.** *The Schedule the Time Window Dialog Box*

Within this dialog box, you can set the following parameters for the event:

- Select the start date and time for the event.
- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete**

option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.
- 11** If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

**Scheduled Task Wizard**

### Configure Task Recurrence

Use the controls below to configure the recurrence settings

**Task time**

Start Time: 00:00  Run until complete  Use Site's Local Time  
 End by: 00:00

**Recurrence pattern**

Daily  Weekly  Monthly

Recur every 1 week(s) on:

Sunday  Monday  Tuesday  Wednesday  
 Thursday  Friday  Saturday

**Range of recurrence**

Start: 08 / 19 / 2003  No end date  
 End by: / /

To continue, click Next.

< Back Next > Cancel

**Figure 8-39.** The Configure Task Recurrence Dialog Box

Within this dialog box, you can set the following parameters for this event:

- Select the start time for the event.
- Determine when you want the event to stop. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

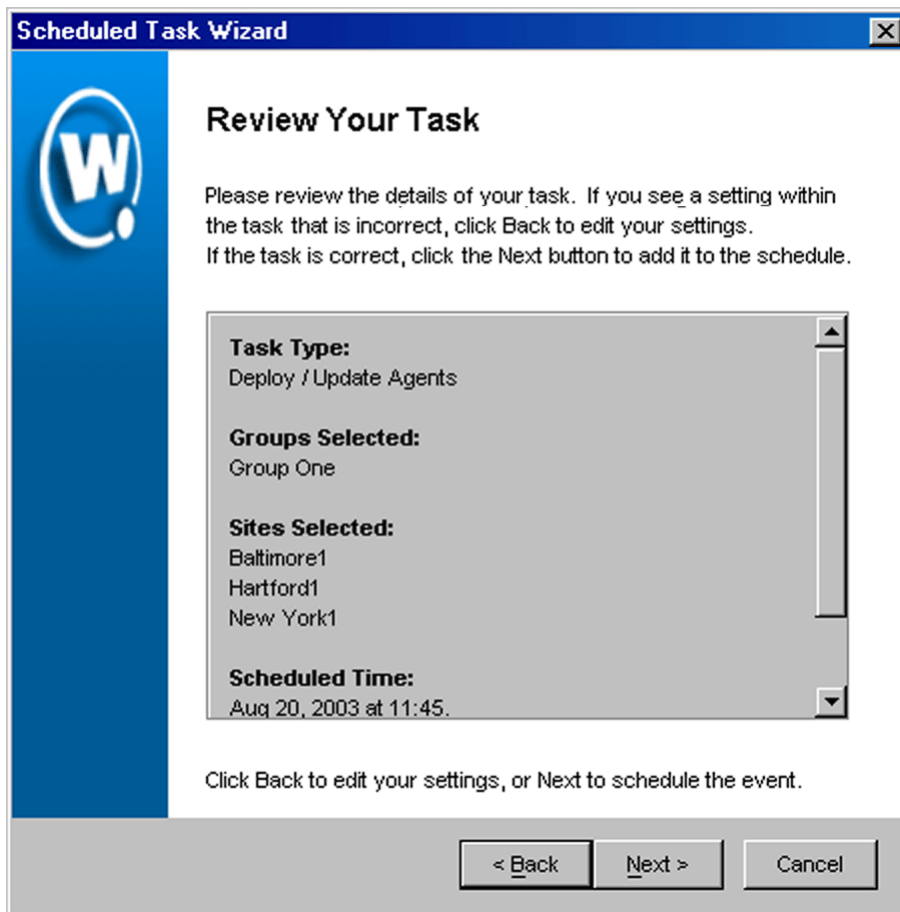
---

**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

**12** Click *Next*.

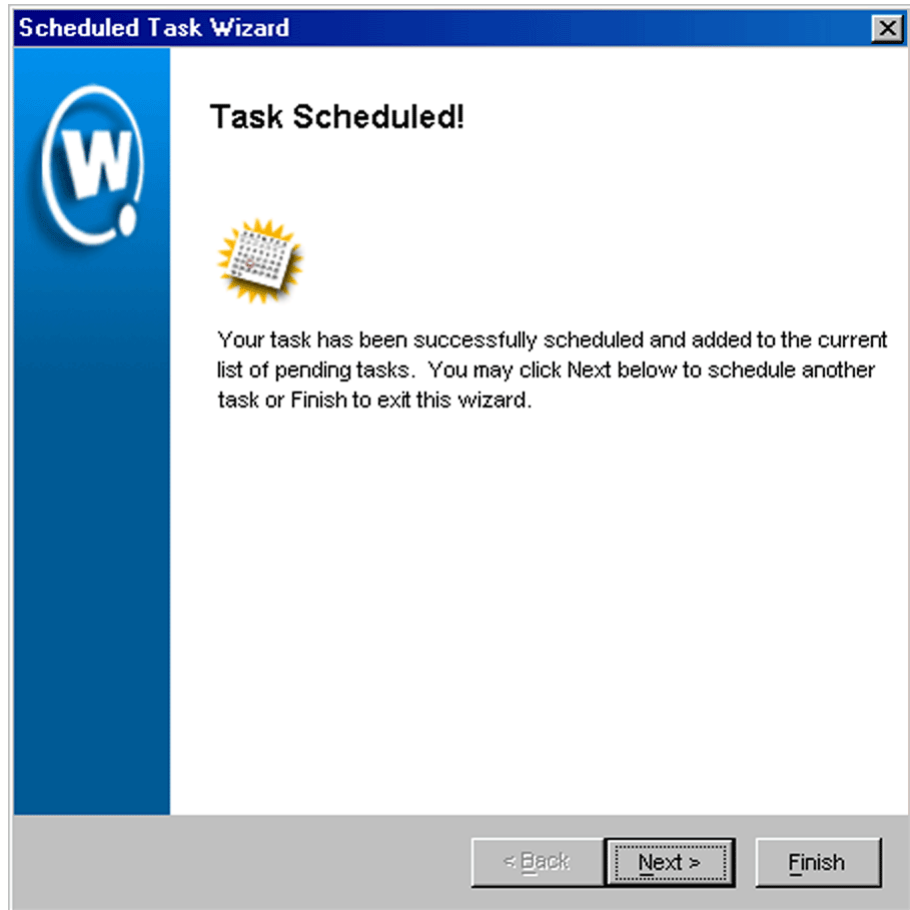
The *Review Your Task* dialog box appears.



**Figure 8-40.** *The Review Your Task Dialog Box*

**13** Review your the task to ensure that it is correct and click Next.

The *Task Scheduled* dialog box appears.



**Figure 8-41.** *The Task Scheduled Dialog Box*

- 14 Click `Next` to schedule a new event, or click `Finish` to return to the Task Schedule dialog box.

## **Deploying Security Settings to Mobile Devices**

This section describes how to apply security settings to the mobile devices within a given group.

---

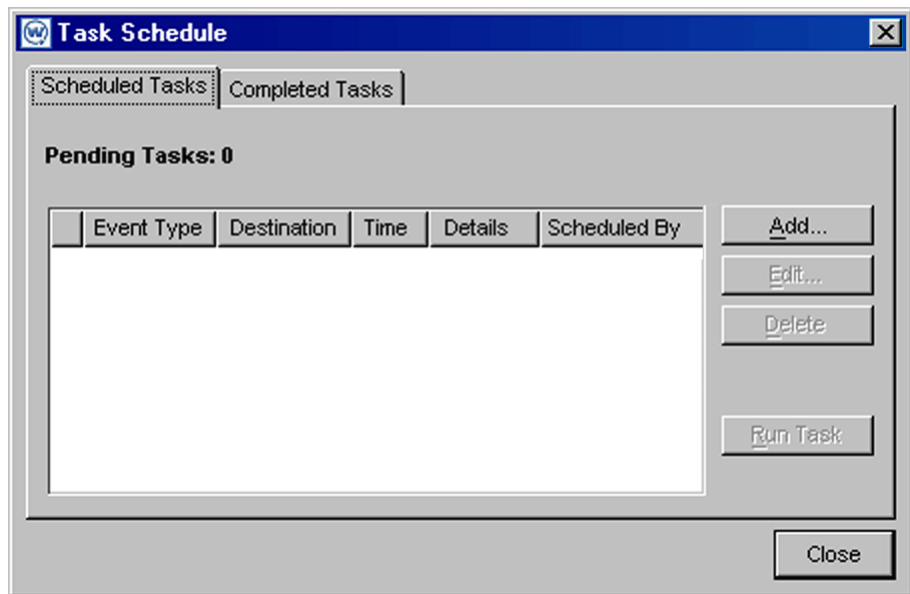
**NOTE** If you plan on deploying settings to both access points and mobile devices, it is highly recommended you follow the steps described in *Deploying Security Settings for All Devices* on page 351.

---

**To deploy security settings:**

- 1 Select Task Schedule from the **Tools** menu.

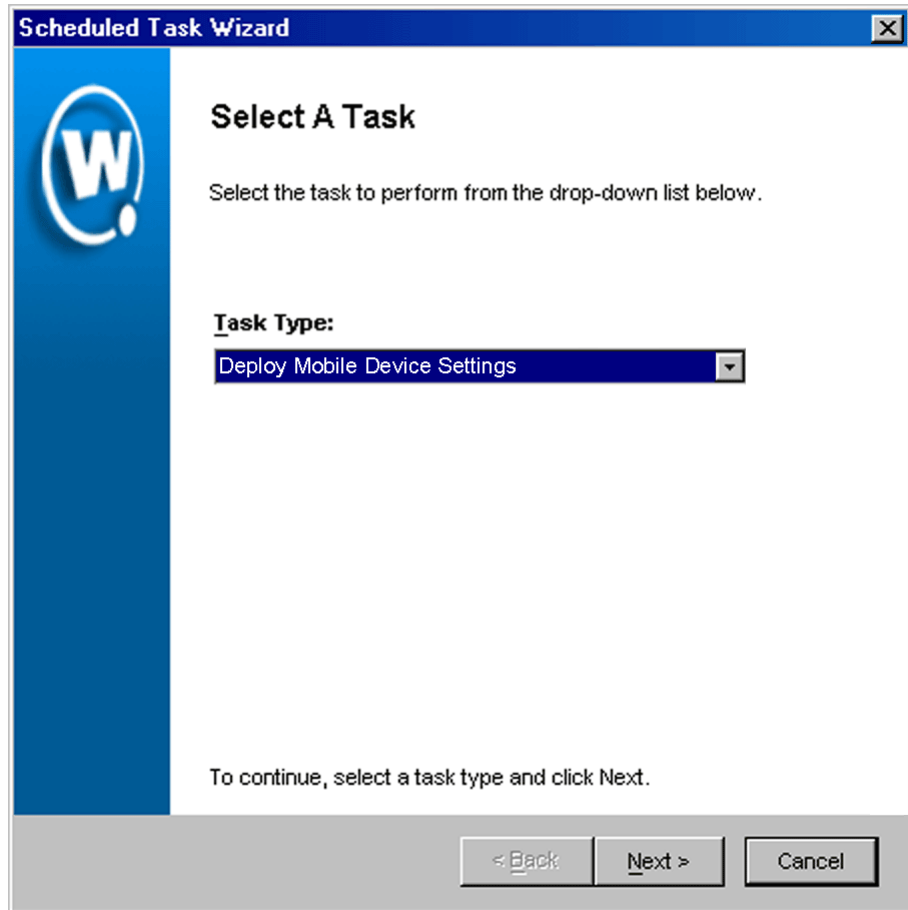
The *Task Schedule* dialog box appears.



**Figure 8-42.** *The Task Schedule Dialog Box*

- 2 Click Add.

The *Select A Task* dialog box appears.

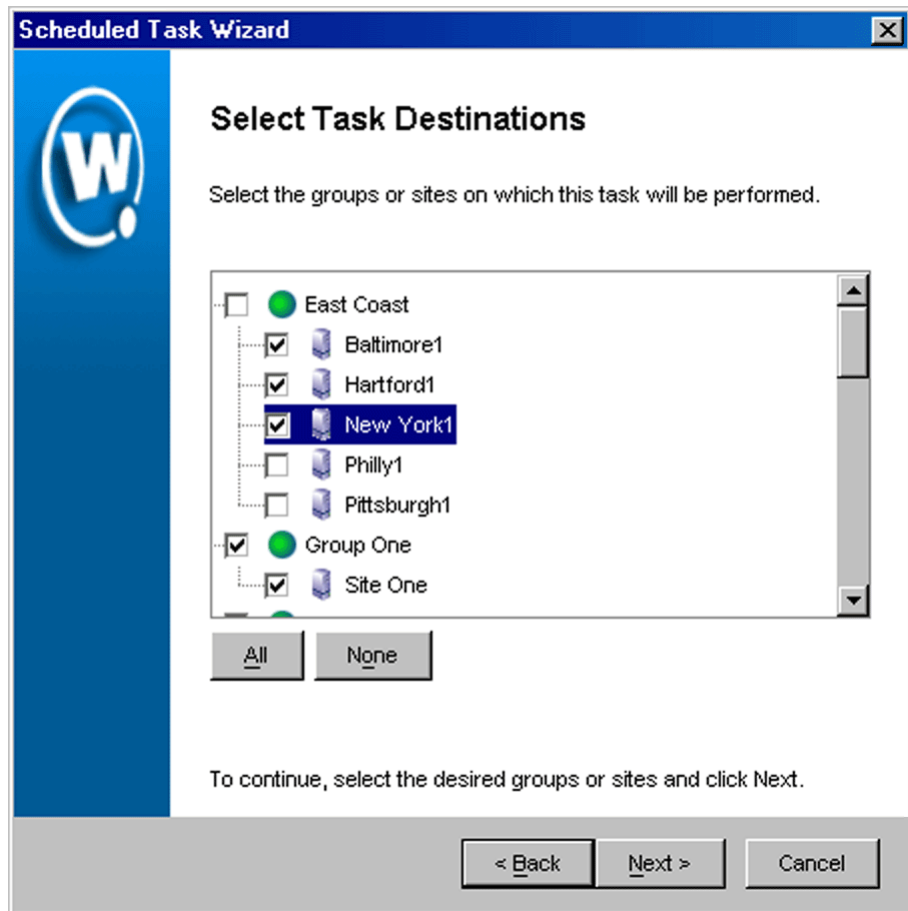


**Figure 8-43.** *The Select a Task Dialog Box*

- 3 Select Deploy Mobile Device Settings from the **Task Type** list and click Next.

The *Select Task Destination* dialog box appears.

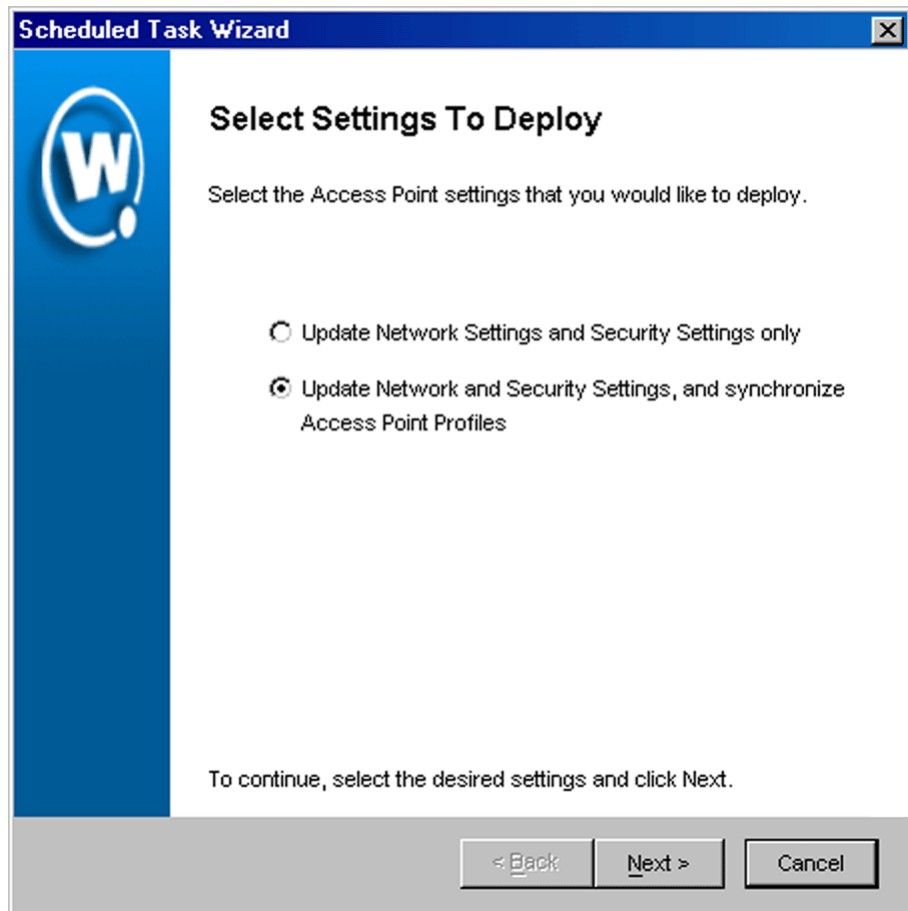




**Figure 8-44.** *The Select Task Destination Dialog Box*

- 4 Select the groups or sites by enabling the checkbox next to the group or site name. You can also select all groups by clicking **All**.
- 5 Click **Next**.

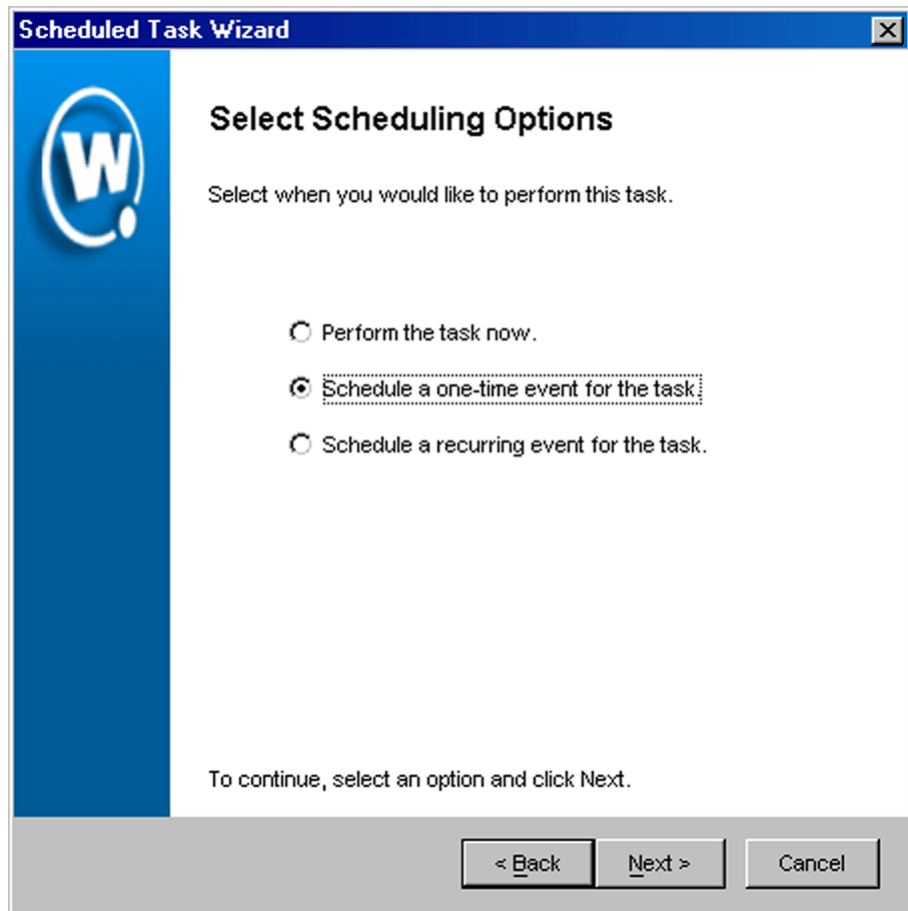
The *Select Settings to Deploy* dialog box appears.



**Figure 8-45.** *The Select Settings to Deploy Dialog Box*

- 6** Select the **Update Network Settings and Security Settings only** option.
- 7** Click **Next**.

The *Select Scheduling Options* dialog box appears.



**Figure 8-46.** *The Select Scheduling Options Dialog Box*

**8** Determine when the event will occur.

If you want the event to occur immediately, select the **Perform the task now** option.

If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

If you want the event to occur on a regular basis, select the **Schedule a recurring event** for this task option.

- 9 Click **Next**.
- 10 If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.

**Scheduled Task Wizard**

### Schedule the Time Window

Select the start time and end time during which you would like to perform this task.

Start Time: 08 /19 / 2003 11:45

Run until complete

End by: 08 /19 / 2003 12:00

Use Site's Local Time

To continue, click Next.

< Back Next > Cancel

**Figure 8-47.** The *Schedule the Time Window* Dialog Box

Within this dialog box, you can set the following parameters for the event:

- Select the start date and time for the event.
- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select

the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.
- 11** If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

**Scheduled Task Wizard**

## Configure Task Recurrence

Use the controls below to configure the recurrence settings

**Task time**

Start Time:   Run until complete  Use Site's Local Time  
 End by:

**Recurrence pattern**

Daily  Weekly  Monthly

Recur every  week(s) on:

Sunday  Monday  Tuesday  Wednesday  
 Thursday  Friday  Saturday

**Range of recurrence**

Start:    No end date  
 End by:

To continue, click Next.

< Back    Next >    Cancel

**Figure 8-48.** *The Configure Task Recurrence Dialog Box*

Within this dialog box, you can set the following parameters for this event:

- Select the start time for the event.
- Determine when you want the event to stop. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

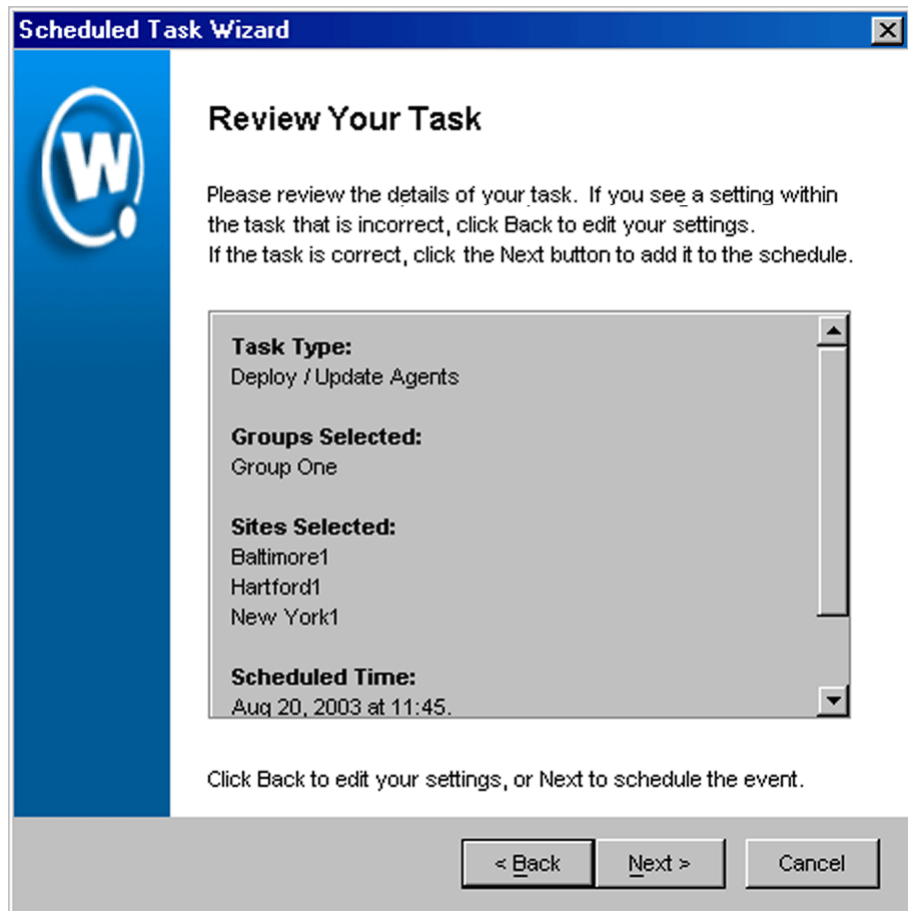
---

**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

**12** Click *Next*.

The *Review Your Task* dialog box appears.

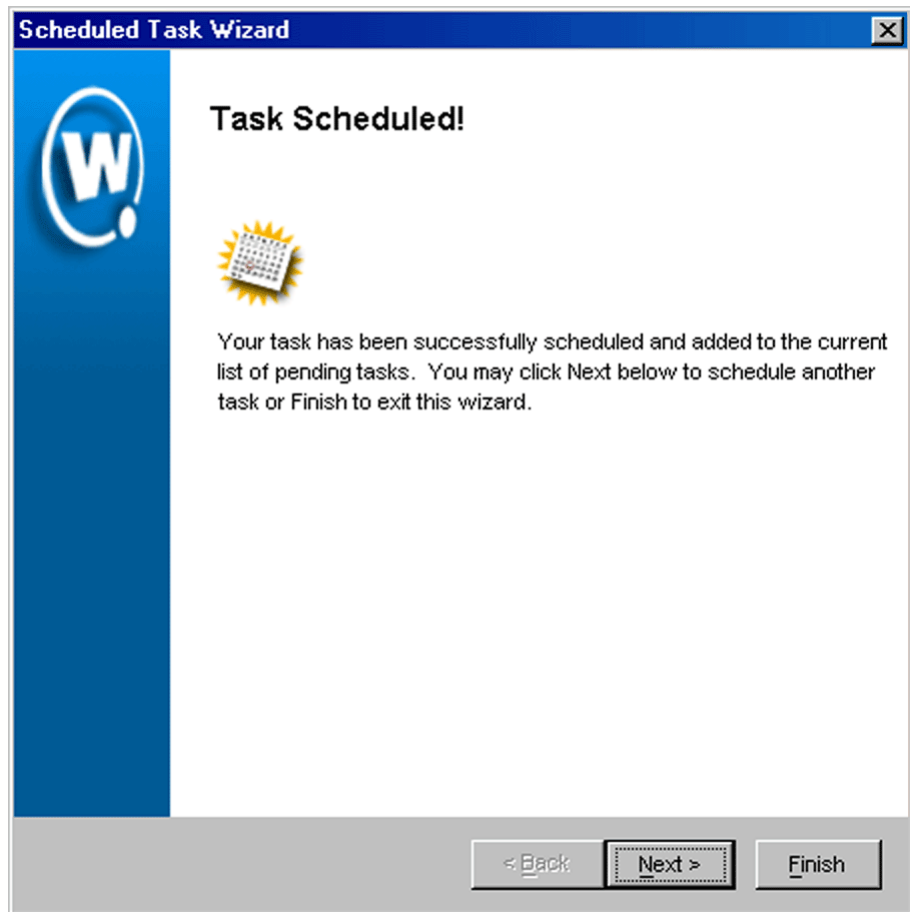


**Figure 8-49.** *The Review Your Task Dialog Box*

**13** Review your the task to ensure that it is correct and click Next.

The *Task Scheduled* dialog box appears.





**Figure 8-50.** *The Task Scheduled Dialog Box*

- 14 Click `Next` to schedule a new event, or click `Finish` to return to the Task Schedule dialog box.



## Chapter 9: Managing Alerts

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. Mobile Manager Enterprise fulfills this requirement by allowing you to manage two alert types:

- **Network alerts.** These alerts refer to activity that occurs on a wireless device. An example of a network alert is if an Agent goes offline, or if a new access point is discovered.
- **Statistical alerts.** These alerts refer to the performance capabilities of an access point or mobile device.

This section covers the following topics:

- Managing network alerts using alert profiles
- Managing statistical alerts
- Using the alarm browser

### Alert Profiles

With [alert profiles](#), you decide what alerts demand your immediate attention. Each alert profile uses one or more [e-mail addresses](#) to inform you when a specified alert occurs. In addition, the Enterprise Management Console allows you to set one or more [proxies](#) (such as CA Unicenter). When you set a proxy for an alert profile, the Enterprise Management Console automatically forwards the alert to the proxy's IP address, enabling you to integrate Mobile Manager Enterprise with your existing network management tools.

You configure most options related to wireless network alerts from the Alert Profiles tab of the Enterprise Management Console's [Configure Network view](#). Information on viewing reports on wireless network alerts can be found in *Chapter 10: Reporting Network Data* on page 425.

This section contains the following topics:

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

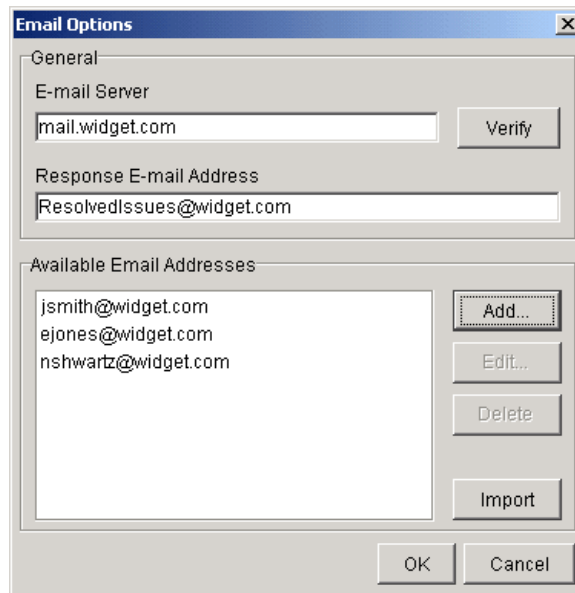
## Creating an E-mail Address List

If you want the Enterprise Management Console 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 Management Console.

### To create an e-mail address list:

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

The *E-mail Options* dialog box appears.



**Figure 9-1.** 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.

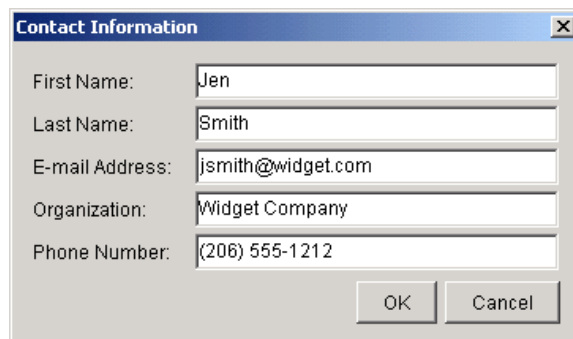
To verify the validity of the e-mail server, click **Verify**. Mobile Manager Enterprise attempts to contact the e-mail server, and displays a dialog box informing you if it was successful or not.

- 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.



**Figure 9-2.** *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 Management Console removes the e-mail address from the list.

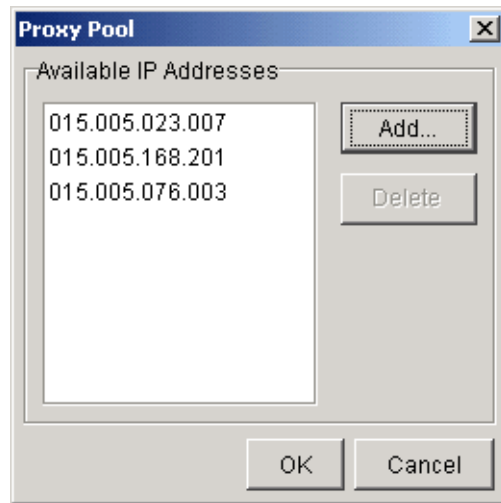
## Creating Proxy Pool

The Enterprise Management Console 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 Management Console.

### To add a proxy to a proxy pool:

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

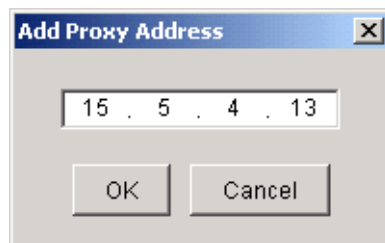
The *Proxy Pool* dialog box appears.



**Figure 9-3.** *The Proxy Pool Dialog Box*

- 2 Click Add.

The *Add Proxy Address* dialog box appears.



**Figure 9-4.** *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`.

Mobile Manager Enterprise 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 Enterprise alerts to one or more e-mail addresses or proxies. When these alerts occur, Mobile Manager Enterprise immediately either sends an e-mail to the selected addresses or forwards the alert to the proxy computer.

---

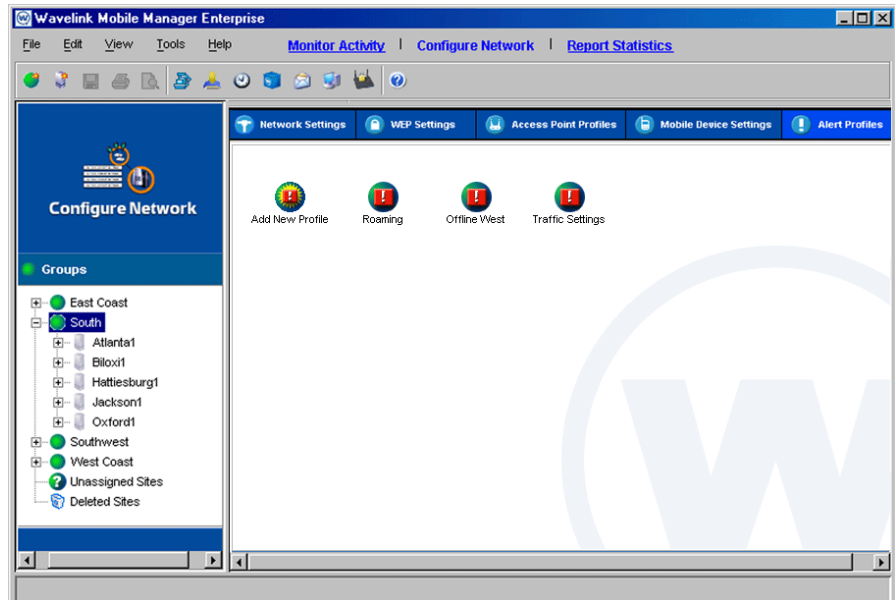
**NOTE** If you do not assign an alert to a profile, you can still access information about the alert through the [Monitor Activity](#) and [Report Statistics](#) views.

---

### To create an enterprise alert profile:

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

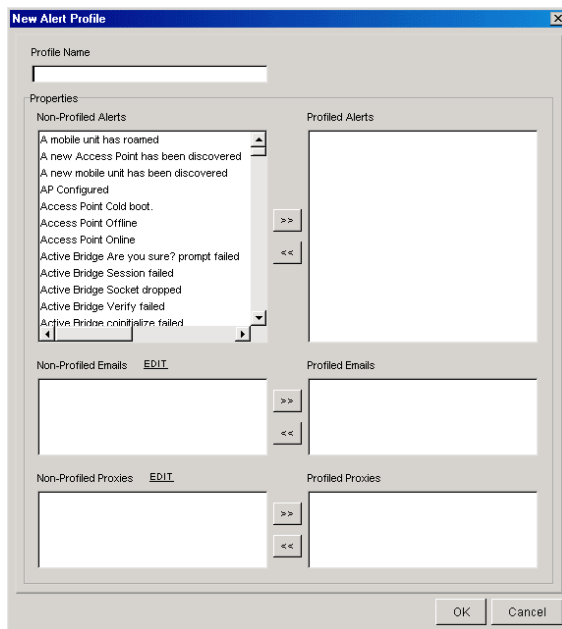




**Figure 9-5.** *The Alert Profiles Tab of the Configure Network View*

**4** Double click the **Add New Profile** icon.

The *New Alert Profile* dialog box appears.



**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 Management Console 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 Management Console 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 Management Console.

The new alert profile appears as its own icon in the Alert Profiles tab.

## 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 Double click the icon for the profile you want to edit.
- 5 Click `Edit`.

A dialog box appears.

- 6 Edit the profile as necessary.
- 7 Click **OK** to save your changes and return to the Enterprise Management Console.

## Deleting Enterprise Alert Profiles

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

### 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 Right-click the icon that represents the alert profile and select `Delete` from the menu that appears.

The Enterprise Management Console deletes the enterprise alert profile.

## Statistical Alerts

Statistical alerts are alerts Mobile Manager Enterprise 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](#)

## Configuring New Statistical Alerts

Configuring a new statistical alert involves the following steps:

- 1 Add a new alert.
- 2 Determine when Mobile Manager Enterprise monitors this alert.
- 3 Configure all appropriate radio values.

- 4 Configure all appropriate Ethernet values.
- 5 Save the new alert.

---

**NOTE** You can view supported statistics and statistics descriptions for different access points in the Administrator in the *Advanced Properties* dialog box for a profile or access point. See your hardware vendor's documentation or MIB for additional information.

---

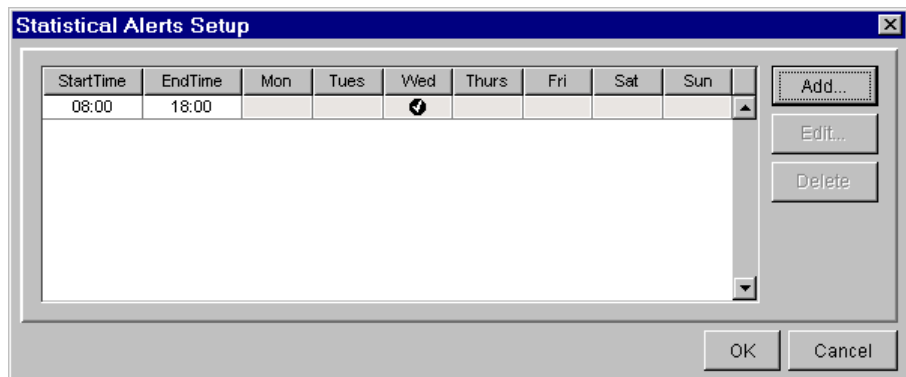
These steps are described further in the following sections.

**To add a new alert:**

- 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 `Statistical Alerts Profiles` tab.

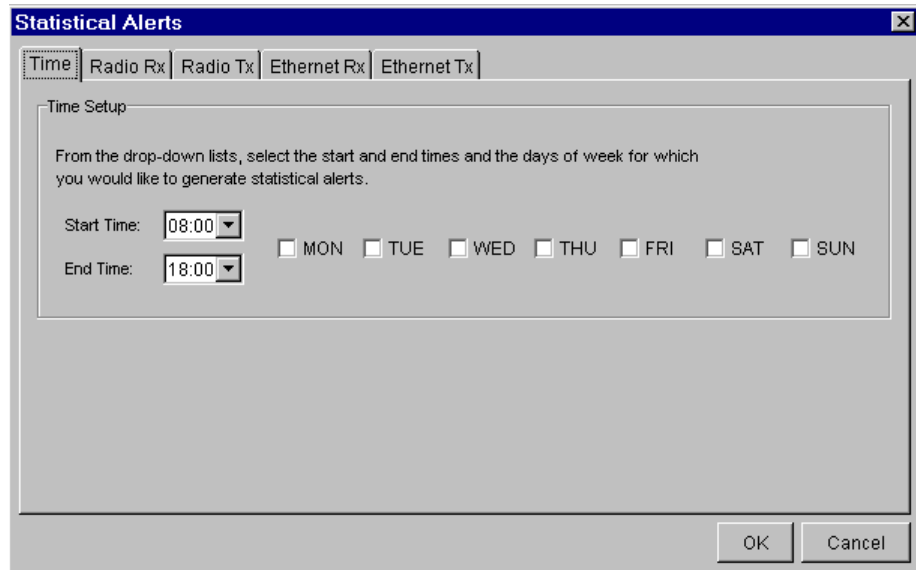


**Figure 9-7.** *The Statistical Alerts Setup Dialog Box*

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.

- 4 Click `Add`.

A new dialog box appears.



**Figure 9-8.** *The Time Tab of the Statistical Alerts Dialog Box*

**To determine when Mobile Manager Enterprise 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.

---

**NOTE** You can view supported statistics and statistics descriptions for different access points in the Administrator in the *Advanced Properties* dialog box for a profile or access point. See your hardware vendor's documentation or MIB for additional information.

---

- 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.

**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.

**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 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 `Statistical Alerts Profiles` tab.
- 4 Select an alert from the list.
- 5 Click `Edit`.
- 6 Edit the alert as necessary.
- 7 Click `Apply`.

## **Deleting Statistical Alerts**

You can remove a statistical alert at any time.

**To remove a statistical alert:**

- 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 `Statistical Alerts Profiles` tab.
- 4 Select an alert from the list.
- 5 Click `Delete`.

## Using the Alarm Browser

In the Monitor Activity view, there is a section called the Alarm Browser. This section provides you with a quick overview of the alerts that occur on your wireless network in a table format. This table provides the following information about each alert:

<b>Ack</b>	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.
<b>Severity</b>	Indicates the severity of the alert.
<b>Site</b>	The name of the site that generated the alert.
<b>Time</b>	The time and date when the alert occurred.
<b>Description</b>	A brief description of the alert.
<b>IP Address/Hostname</b>	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.

## Setting the Destination IP Address for Network Alerts

Each Agent on your network must know the IP address of the system hosting the Fault Manager, a component of Mobile Manager that is installed when you install the Enterprise Management Console. The Fault Manager is responsible for providing the Enterprise Management Console with alert information.

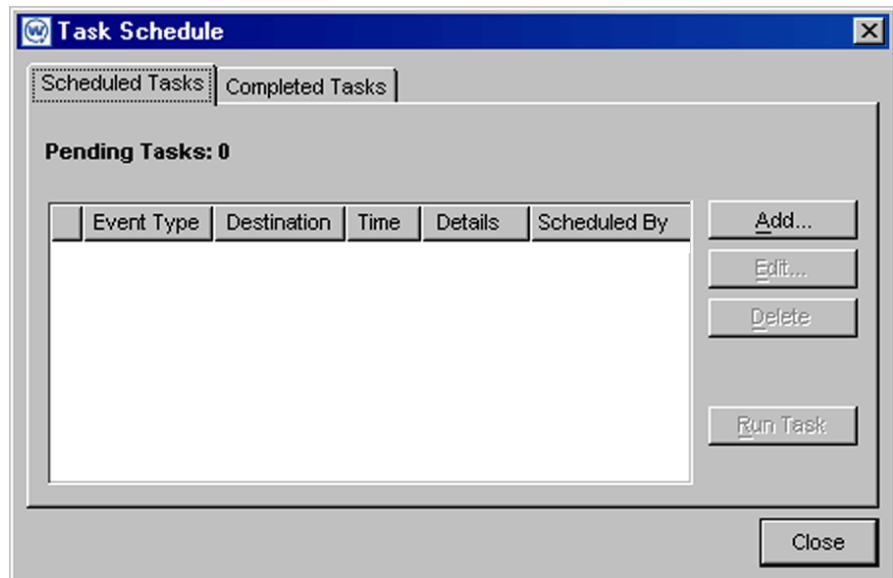
Typically, the IP address of this system is included when you deploy an Agent to a site; however, some circumstances require that you inform your Agents manually. An example of when this task is required is if you move the Enterprise Management Console to a new system.

To inform Agents of where to send network alerts, you schedule an event within the Enterprise Management Console. This event sends the IP address of the system hosting the Fault Manager to the selected sites or groups.

**To set the destination IP address for network alerts:**

- 1 Select **Task Schedule** from the **Tools** menu.

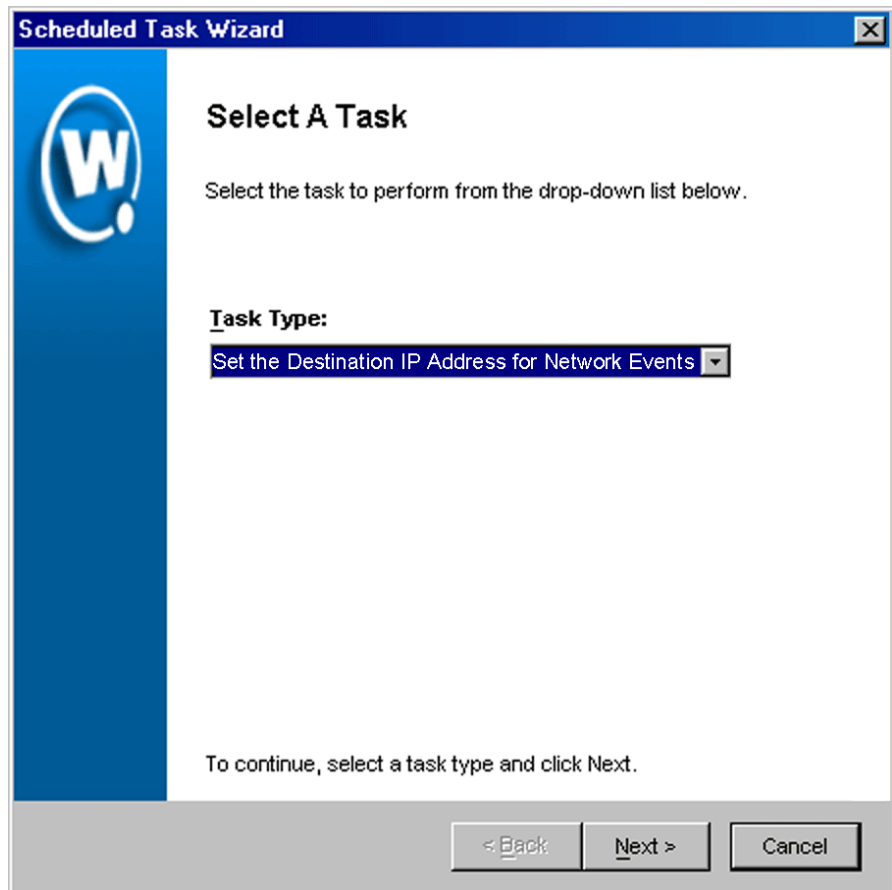
The *Task Schedule* dialog box appears.



**Figure 9-9.** The *Task Schedule* Dialog Box

- 2 Click **Add**.

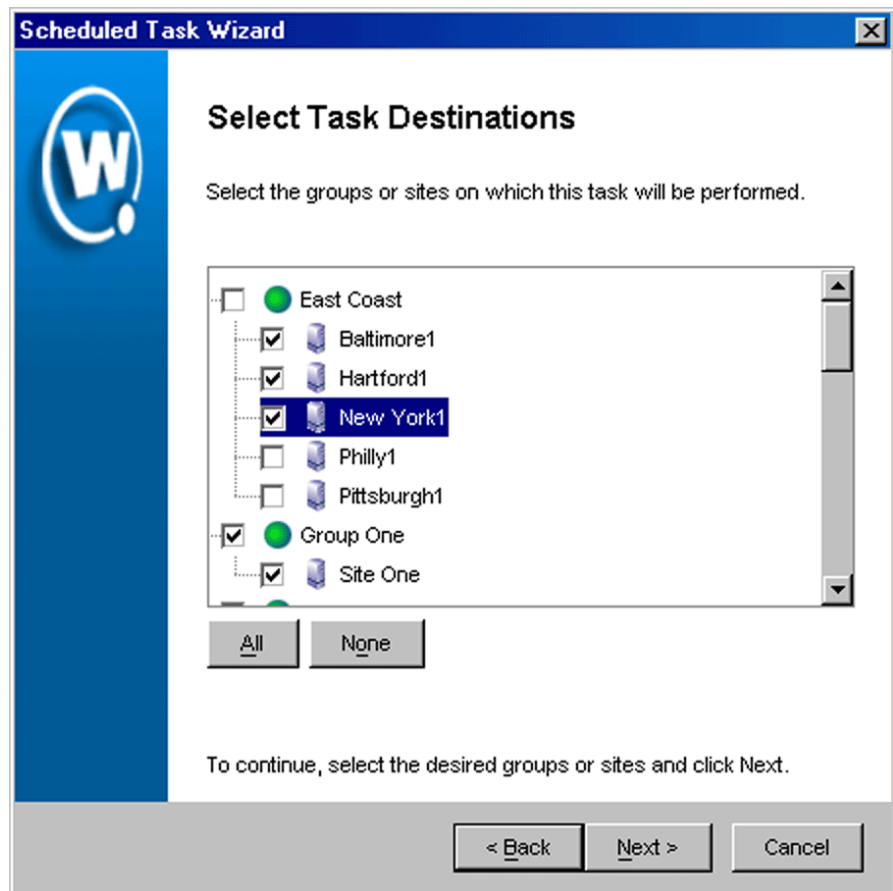
The *Select A Task* dialog box appears.



**Figure 9-10.** *The Select A Task Dialog Box*

- 3 Select Set the Destination IP Address for Network Alerts from the **Task Type** list and click Next.

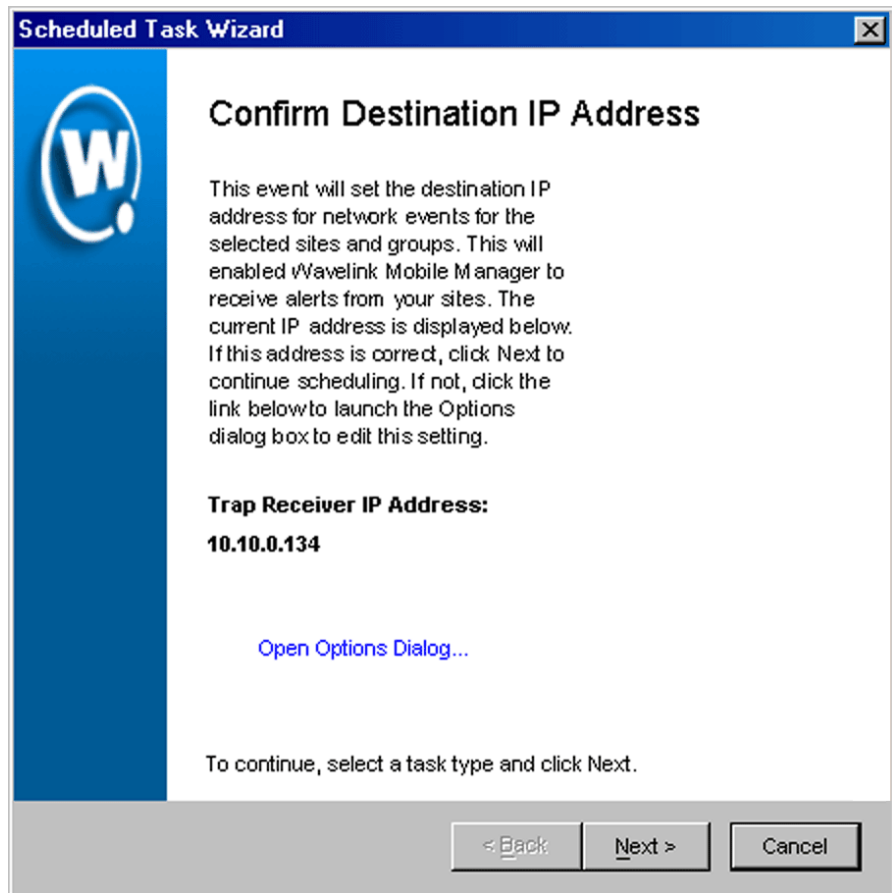
The *Select Task Destination* dialog box appears.



**Figure 9-11.** *The Select Task Destination Dialog Box*

- 4 Select the groups or sites by enabling the checkbox next to the group or site name. You can also select all groups by clicking All.
- 5 Click Next.

The *Confirm Destination IP Address* dialog box appears.

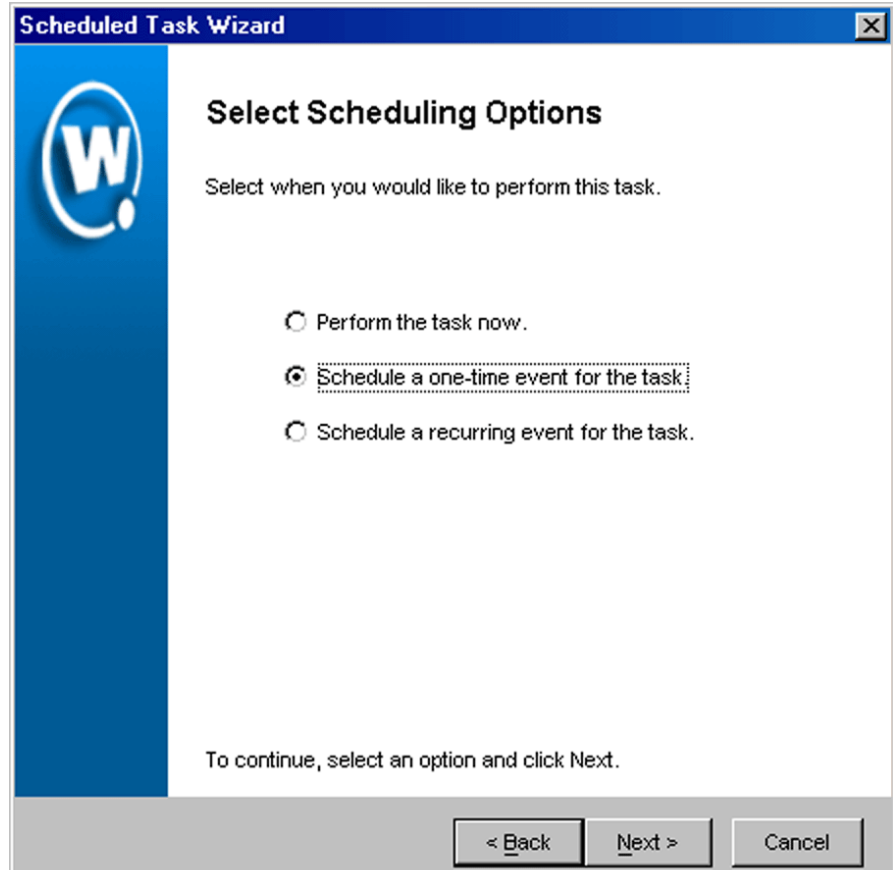


**Figure 9-12.** *The Select Settings to Deploy Dialog Box*

- 6 If the IP address within this dialog box is correct, click **Next**.

If the IP address is incorrect, click the **Open Options Dialog...** hyperlink. The *Options* dialog box appears, allowing you to set the destination IP address. Once you apply your changes and close the dialog box, click **Next**.

The *Select Scheduling Options* dialog box appears.



**Figure 9-13.** *The Select Scheduling Options Dialog Box*

**7** Determine when the event will occur.

If you want the event to occur immediately, select the **Perform the task now** option.

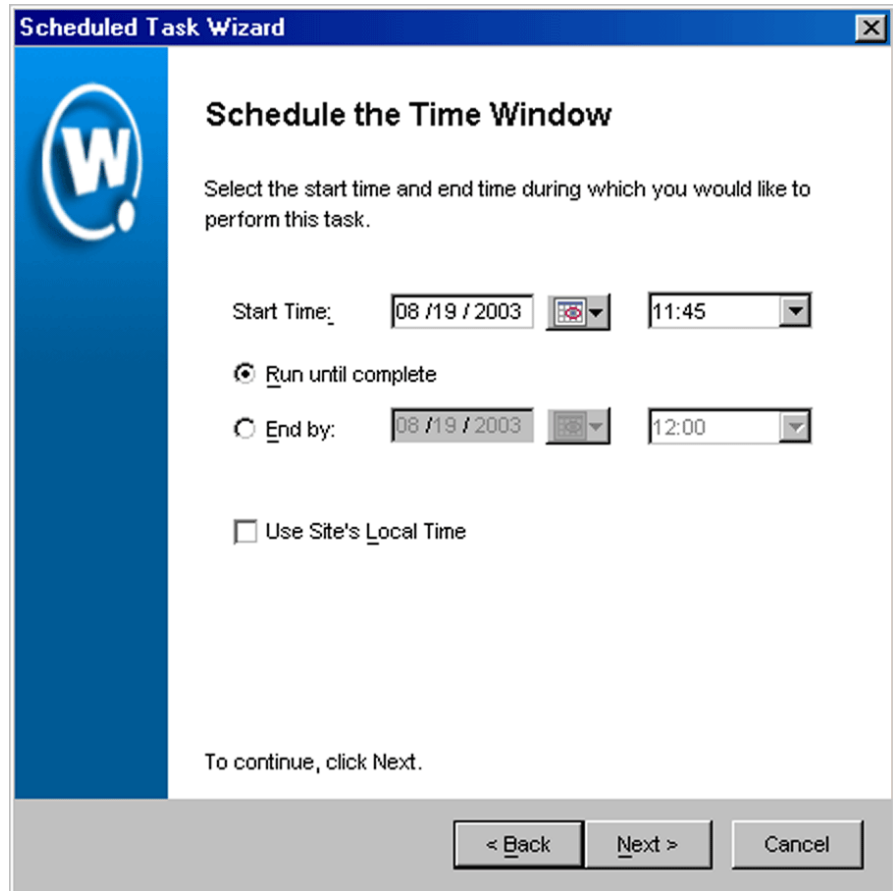
If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

---

**NOTE** For scheduling the destination IP address, it is not recommended that you select the **Schedule a recurring event for the task** option.

---

- 8 Click **Next**.
- 9 If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.



**Figure 9-14.** *The Schedule the Time Window Dialog Box*

Within this dialog box, you can set the following parameters for the event:

- Select the start date and time for the event.
- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete**

option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

---

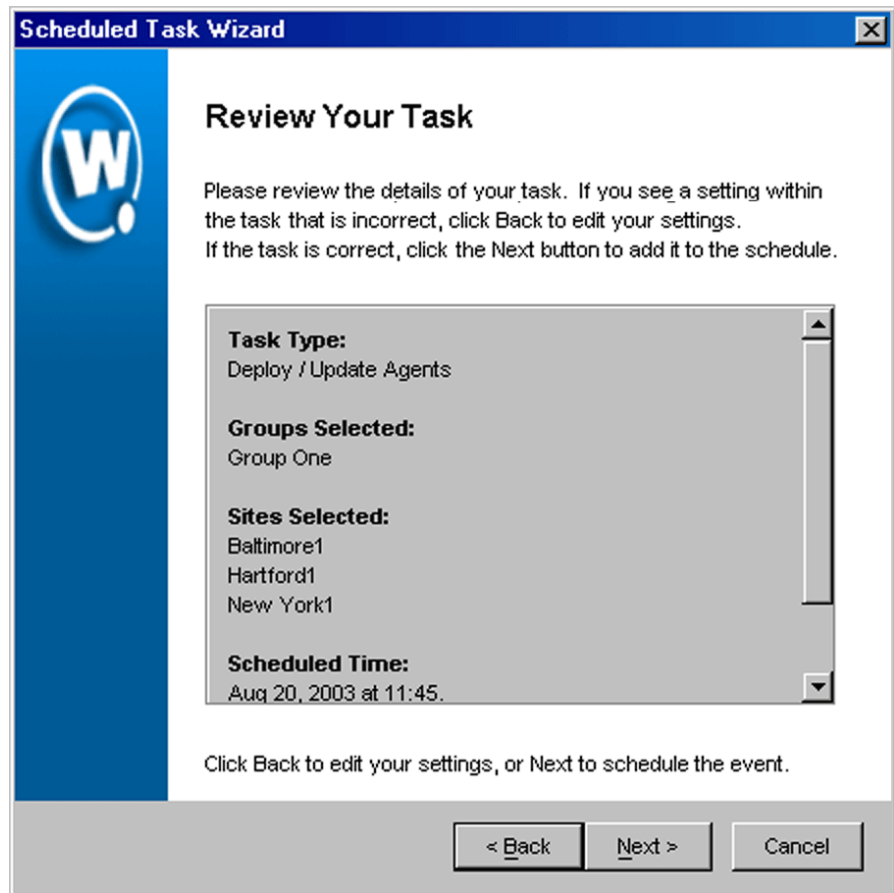
**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

**10** Click *Next*.

The *Review Your Task* dialog box appears.

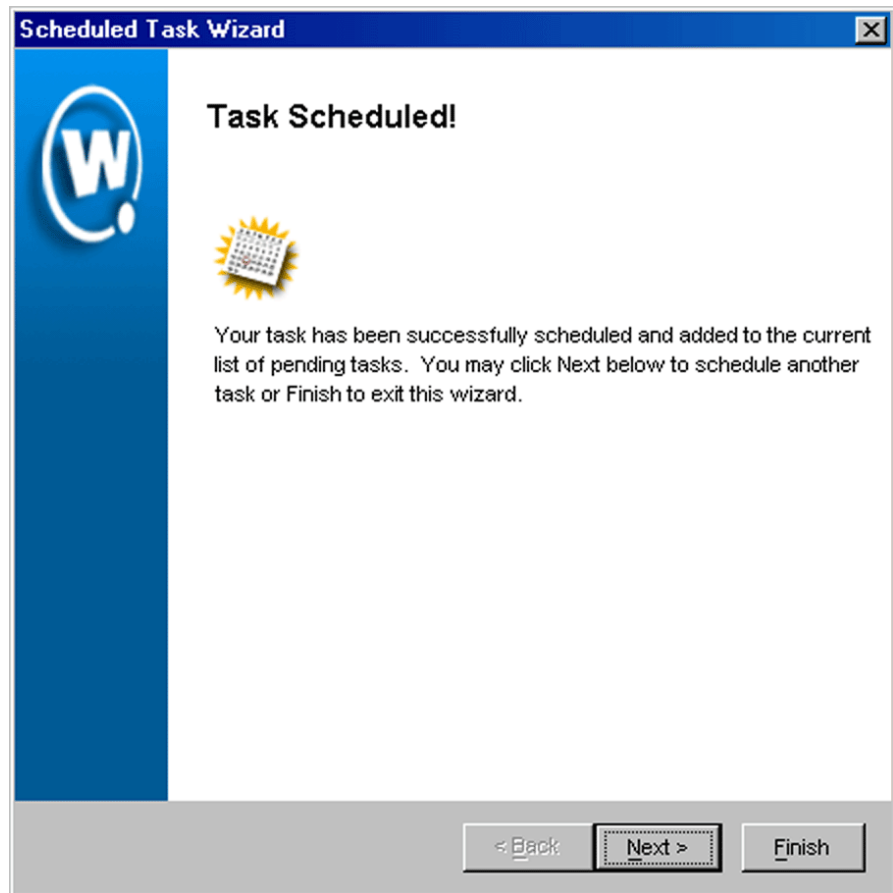




**Figure 9-15.** *The Review Your Task Dialog Box*

**11** Review your the task to ensure that it is correct and click Next.

The *Task Scheduled* dialog box appears.



**Figure 9-16.** *The Task Scheduled Dialog Box*

- 12 Click **Next** to schedule a new event, or click **Finish** to return to the Task Schedule dialog box.

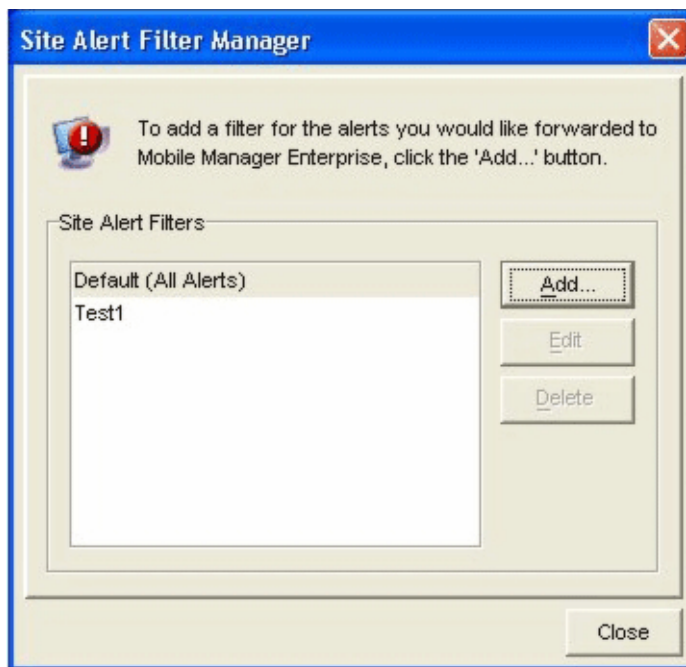
## Site Alert Filter Manager

Administrators can now centrally define what Alerts get sent to the Enterprise Console from the different access point servers (agents). This provides additional control to filter what alerts get propagated, which is especially

important for customers that have a large number of Mobile Manager agents deployed and have slow-link WAN connections to those agents.

The Alarm Browser in the Monitor Activity view shows you all alarms that have come in from any of your sites. Depending on the number of sites and their activity level, the volume of alarms may be difficult to keep up with for the user. The Site Alert Filter mechanism lets you limit the type of alarm messages sent from the sites to the console, which also reduces the amount of network traffic between the sites and the Enterprise Management Console.

To create Site Alert Filters, click on the Site Alert Filter Manager icon from the **Tools** menu:

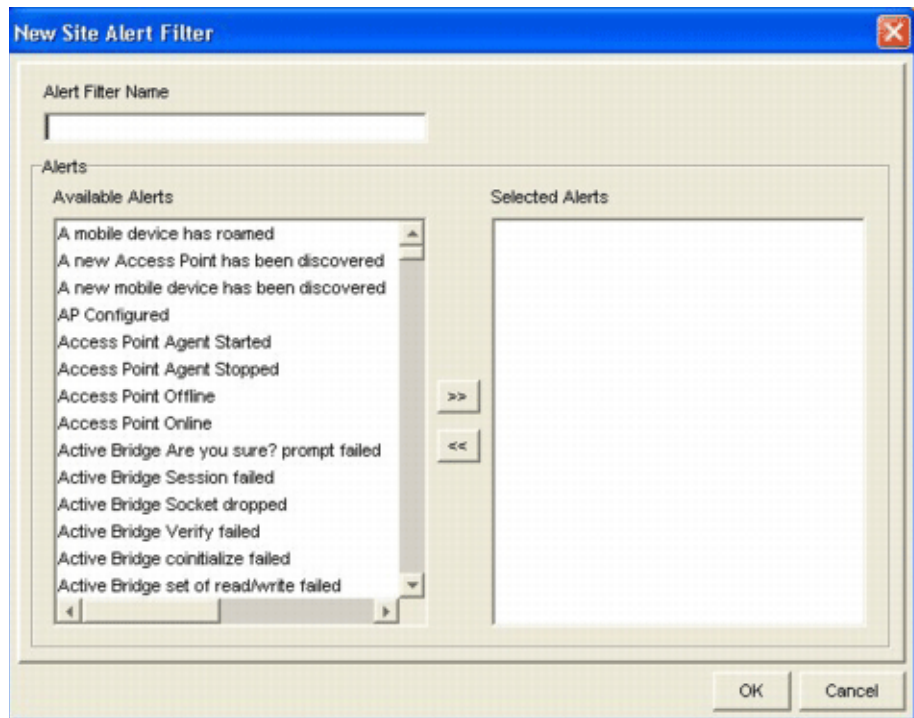


**Figure 9-17.** *Site Alert Filter Manager*

**To create a Site Alert Filter:**

- 1 Click Add...

The *New Site Alert Filter* dialog box appears



**Figure 9-18.** *New Site Alert Filter Dialog Box*

- 2 Type a name for this new filter
- 3 Highlight the alerts you want to continue to see in the list of Available Alerts. You can select multiple alerts with the Ctrl or Shift keys held down as you click.
- 4 Move the highlighted alerts over into the list of Selected Alerts with the >> button.
- 5 If you make a mistake, you can highlight in the list of Selected Alerts and remove those alerts with the << button.
- 6 Once your filter has all the Selected Alerts you want, click OK.

Mobile Manager returns you to the *Site Alert Filter Manager*. Click **C**lose when all your filters are just as you want them.

**To edit an existing Site Alert Filter:**

- 1 Highlight an entry in the list of Site Alert Filters
- 2 Click `Edit`. Note that the filter named 'Default' cannot be edited.
- 3 Manipulate the Filter just as described under 'To create a Site Alert Filter' above.
- 4 Once your filter has all the Selected Alerts you want, click `OK`.

Mobile Manager returns you to the Site Alert Filter Manager. Click `Close` when all your filters are just as you want them.

**To delete an existing Site Alert Filter:**

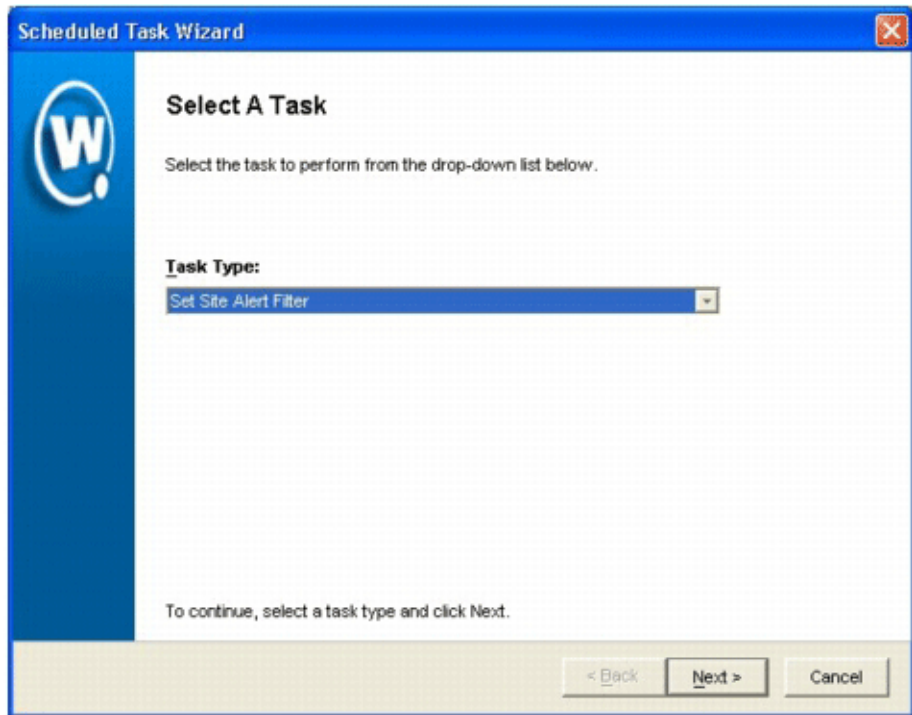
- 1 Highlight an entry in the list of Site Alert Filters
- 2 Click `Delete`. Note that the filter named 'Default' cannot be deleted.
- 3 Confirm the *Delete Selected Filters?* dialog

Mobile Manager returns you to the *Site Alert Filter Manager*. Click `Close` when all your filters are just as you want them.

**To apply an existing Site Alert Filter, you need to schedule a task of type Set Site Alert Filter:**

- 1 Pick `Task Schedule` from the **Tools** menu.

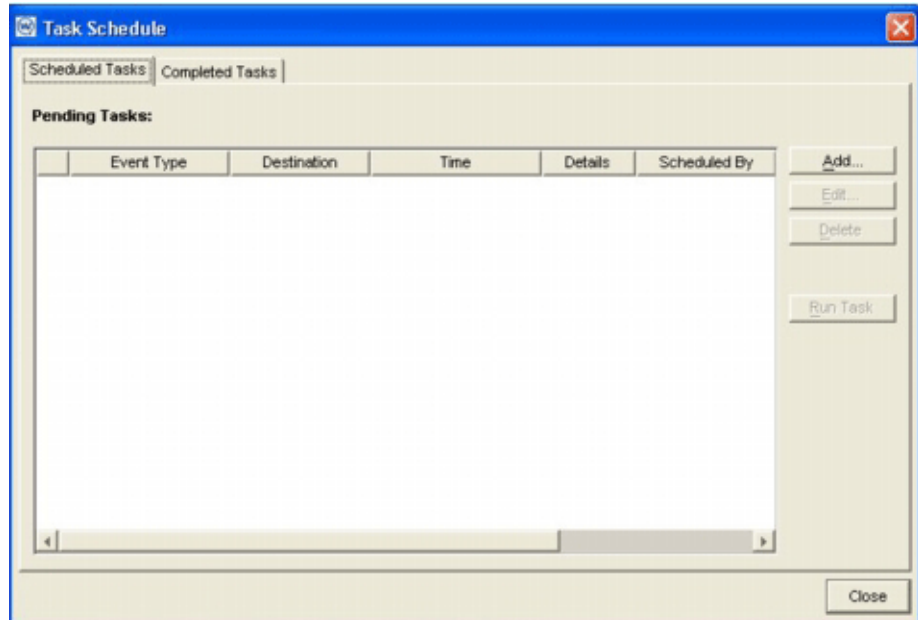
The *Task Schedule* dialog box appears.



**Figure 9-19.** *Task Schedule Dialog Box*

**2** Click Add.

The *Scheduled Task Wizard* appears.



**Figure 9-20.** *Schedule Task Wizard*

- 3** Select **Set Site Alert Filter** in the **Task Type** drop-down box. Click **Next**.
- 4** Check all the sites you want to apply this Alert Filter to. Click **Next**.
- 5** Pick the filter you desire. You can even create and/or edit filters from this wizard panel by clicking the **Open Site Alert Filter Manager** hyperlink. Click **Next**.
- 6** Pick when you want to execute your task. Click **Next** as needed.
- 7** Review your task. Click **Next** to begin execution.

---

**NOTE** That only one alert filter can be in effect at any given site, so any previous filter you might have had is replaced. If you want to receive all alerts again, apply the default filter to the site.

---

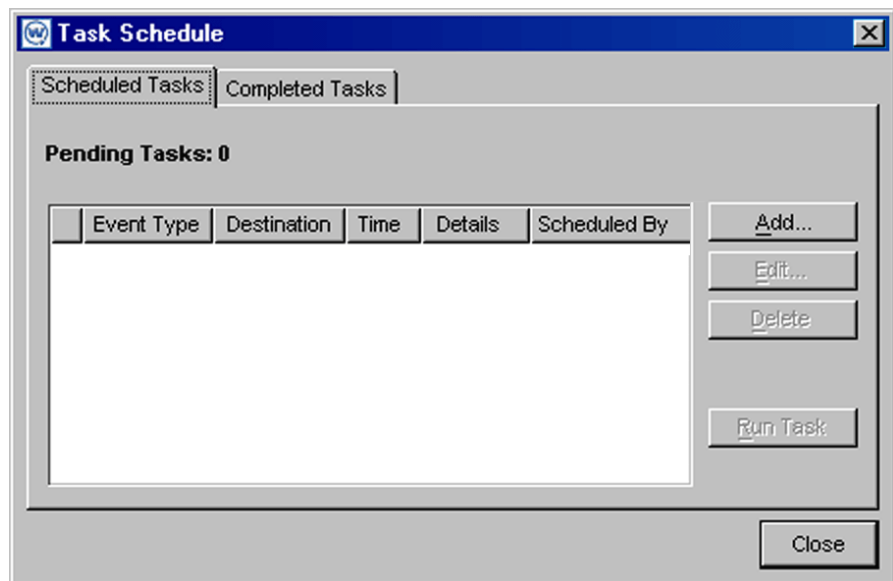
## Performing Database Maintenance

Mobile Manager uses a database to track a variety of information about wireless network activity. If you want to manage the size of this database, you can schedule an event that will remove out-of-date database entries.

### To perform database maintenance:

- 1 Select **Task Schedule** from the **Tools** menu.

The *Task Schedule* dialog box appears.

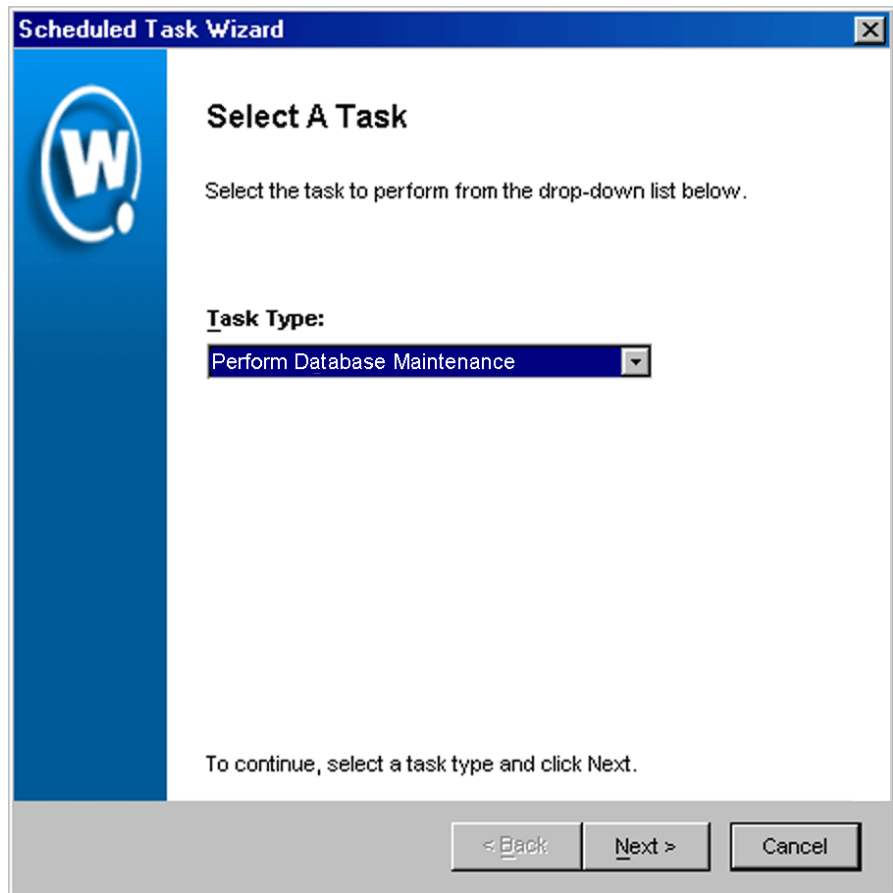


**Figure 9-21.** *The Task Schedule Dialog Box*

- 2 Click **Add**.

The *Select A Task* dialog box appears.

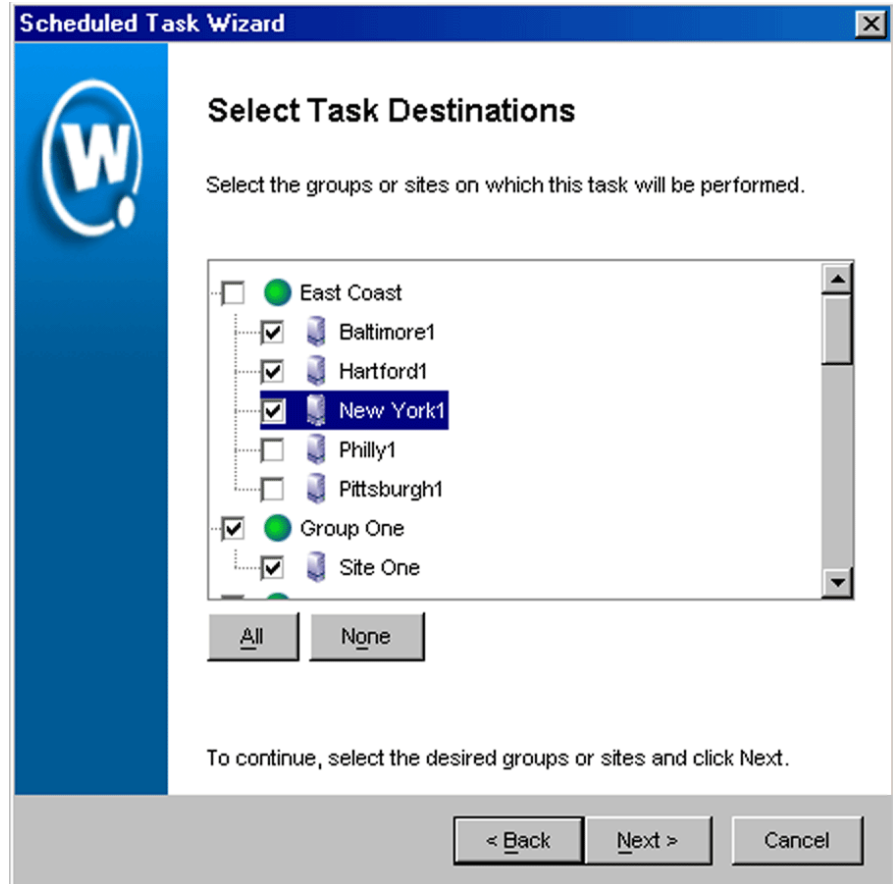




**Figure 9-22.** *The Select a Task Dialog Box*

- 3 Select Perform Database Maintenance from the **Task Type** list and click Next.

The *Database Maintenance Options* dialog box appears.



**Figure 9-23.** *The Select Task Destination Dialog Box*

- 4 If you want to remove alert entries from the database, enable the **Alert Data** checkbox.

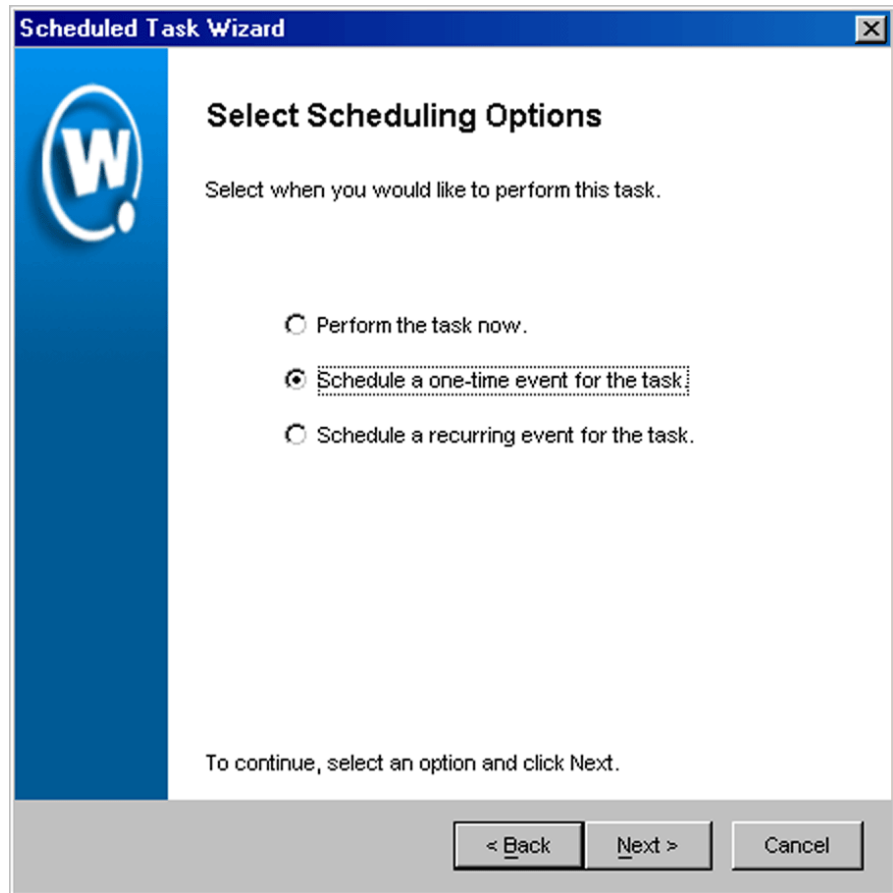
You can then configure the appropriate option to either remove entries older than a specific date or retain entries from a set number of day.

- 5 If you want to remove statistical information from the database, enable the **Statistical Information** checkbox.

You can then configure the appropriate option to either remove entries older than a specific date or retain entries from a set number of day.

6 Click **Next**.

The *Select Scheduling Options* dialog box appears.



**Figure 9-24.** *The Select Scheduling Options Dialog Box*

7 Determine when the event will occur.

If you want the event to occur immediately, select the **Perform the task now** option.

If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

If you want the event to occur on a regular basis, select the **Schedule a recurring event** for this task option.

- 8 Click **Next**.
- 9 If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.

**Scheduled Task Wizard**

### Schedule the Time Window

Select the start time and end time during which you would like to perform this task.

Start Time: 08 /19 / 2003 11:45

Run until complete

End by: 08 /19 / 2003 12:00

Use Site's Local Time

To continue, click Next.

< Back Next > Cancel

**Figure 9-25.** *The Schedule the Time Window Dialog Box*

Within this dialog box, you can set the following parameters for the event:

- Select the start date and time for the event.

- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.
  - If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.
- 10** If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

**Scheduled Task Wizard**

## Configure Task Recurrence

Use the controls below to configure the recurrence settings

**Task time**

Start Time: 00:00  Run until complete  Use Site's Local Time  
 End by: 00:00

**Recurrence pattern**

Daily  Weekly  Monthly

Recur every 1 week(s) on:

Sunday  Monday  Tuesday  Wednesday  
 Thursday  Friday  Saturday

**Range of recurrence**

Start: 08 / 19 / 2003  No end date  End by: / /

To continue, click Next.

< Back    Next >    Cancel

**Figure 9-26.** *The Configure Task Recurrence Dialog Box*

Within this dialog box, you can set the following parameters for this event:

- Select the start time for the event.
- Determine when you want the event to stop. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

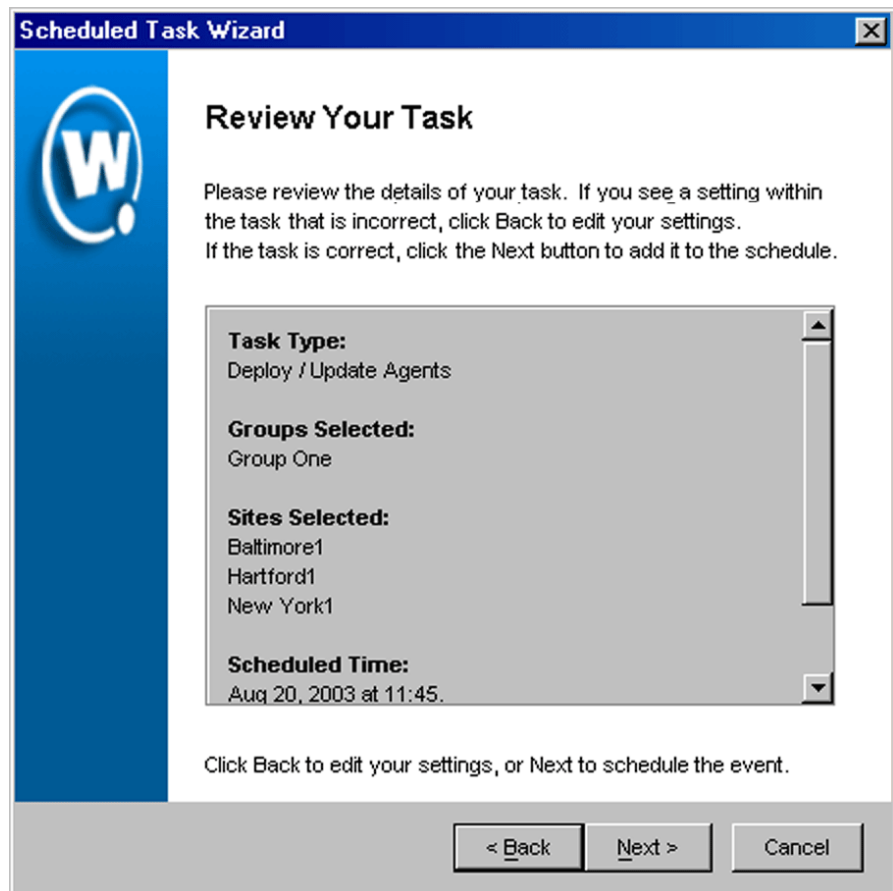
---

**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

**11** Click *Next*.

The *Review Your Task* dialog box appears.



**Figure 9-27.** *The Review Your Task Dialog Box*

**12** Review your the task to ensure that it is correct and click **Next**.

The *Task Scheduled* dialog box appears.





**Figure 9-28.** *The Task Scheduled Dialog Box*

- 13 Click `Next` to schedule a new event, or click `Finish` to return to the Task Schedule dialog box.



## Chapter 10: 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 Management Console 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 Management Console, 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.

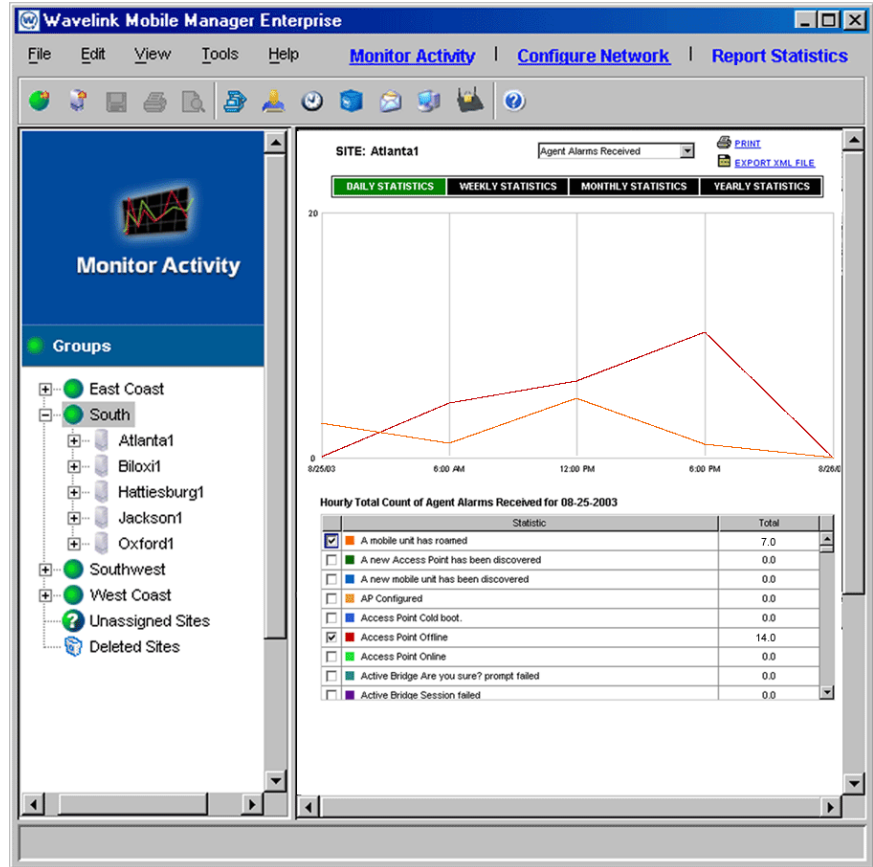


Figure 10-1. The Report Statistics View

This section contains the following topics:

- Gathering Statistics
- Generating Reports

## Gathering Statistics

If you want to view the [statistical](#) data of a group within your wireless network, you must first instruct Mobile Manager Enterprise to gather statistics from your Agents.

Gathering statistics requires scheduling a Gather Statistics event. An event is a period of time in which Mobile Manager Enterprise sends information to or retrieves information from the Agents residing within a specified group of sites. A Gather Statistics event is a type of deployment event in which you determine how much time you want Mobile Manager Enterprise to spend on acquiring statistical data from your access points. For example, you could create a Gather Statistics event that occurs from 7:00am to 7:00pm on Sunday for a group of sites called West Coast Operations. During that time, Mobile Manager Enterprise acquires statistical data from each access point within that group until 7:00pm, or when all statistics have been gathered.

---

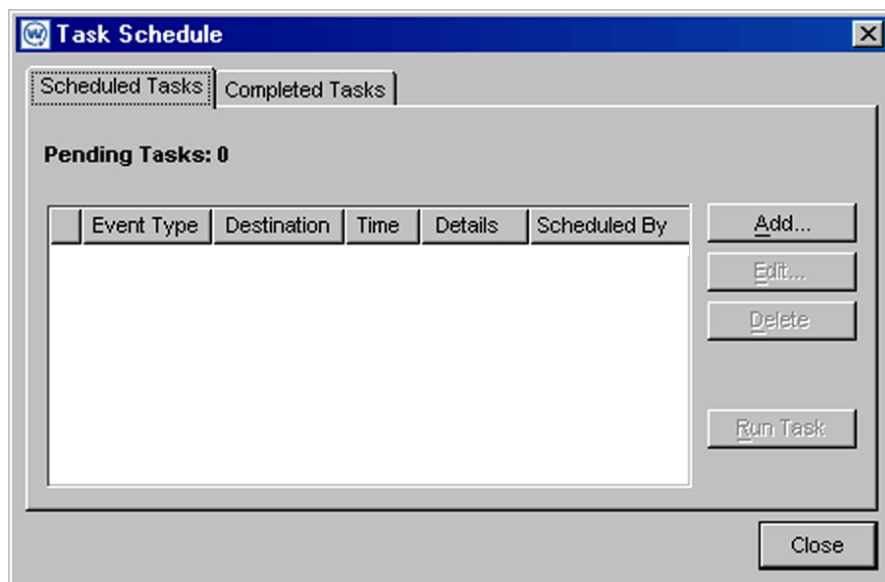
**NOTE** A Gather Statistics event does not allow you to select specific statistics. Mobile Manager Enterprise gathers all statistics stored for each access point.

---

**To gather statistics:**

- 1 Select **Task Schedule** from the **Tools** menu.

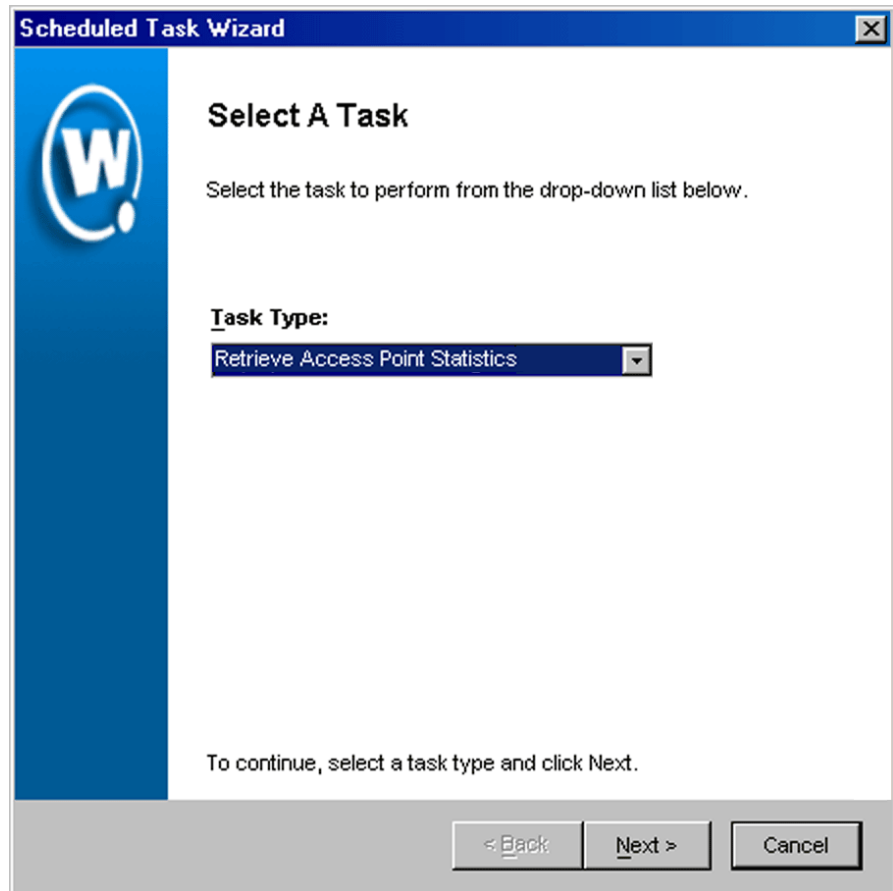
The *Task Schedule* dialog box appears.



**Figure 10-2.** The *Task Schedule* Dialog Box

- 2 Click Add.

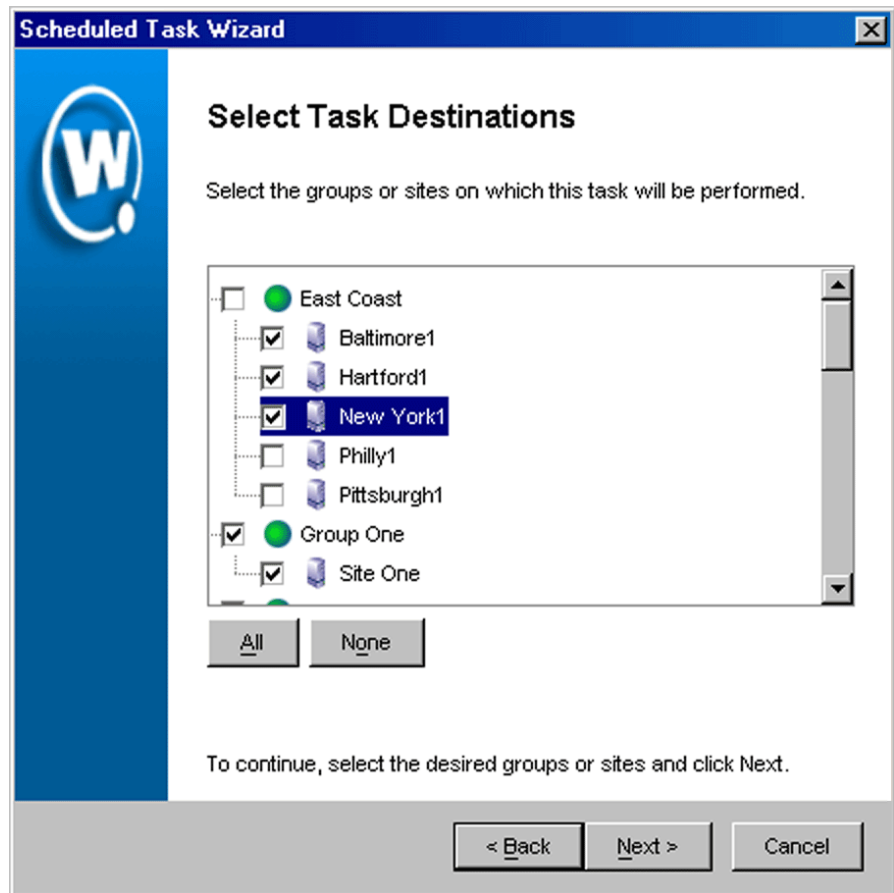
The *Select A Task* dialog box appears.



**Figure 10-3.** *The Select a Task Dialog Box*

- 3 Select Retrieve Access Point Statistics from the **Task Type** list and click Next.

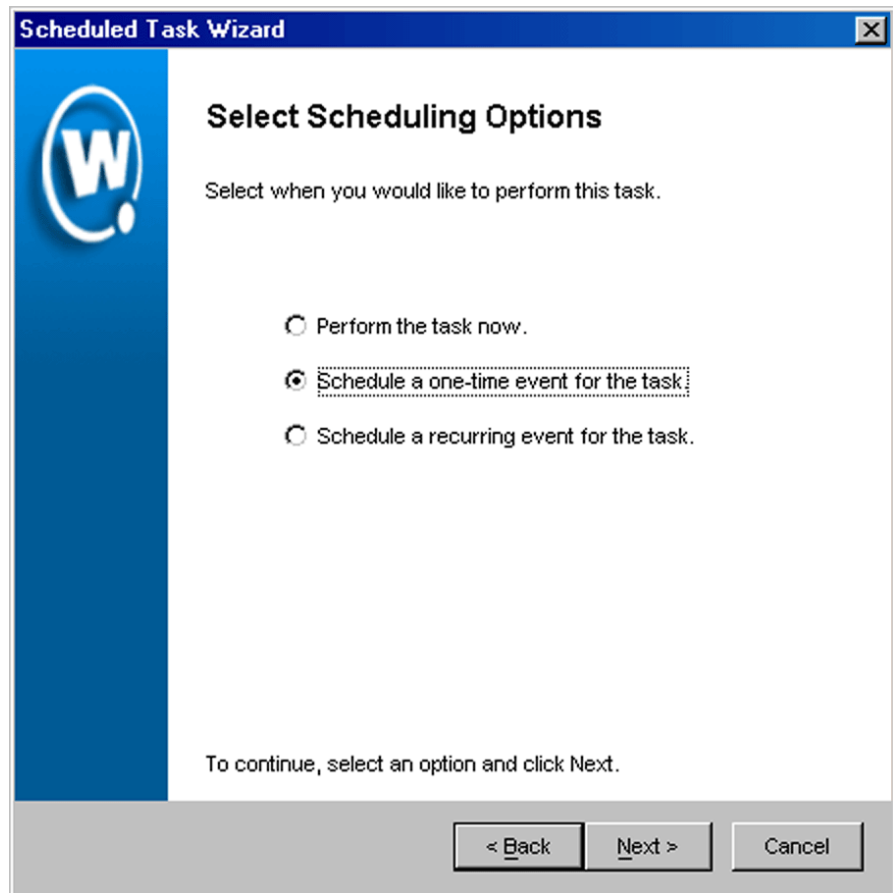
The *Select Task Destination* dialog box appears.



**Figure 10-4.** *The Select Task Destination Dialog Box*

- 4 Select the groups or sites by enabling the checkbox next to the group or site name. You can also select all groups by clicking All.
- 5 Click Next.

The *Select Scheduling Options* dialog box appears.



**Figure 10-5.** *The Select Scheduling Options Dialog Box*

**6** Determine when the event will occur.

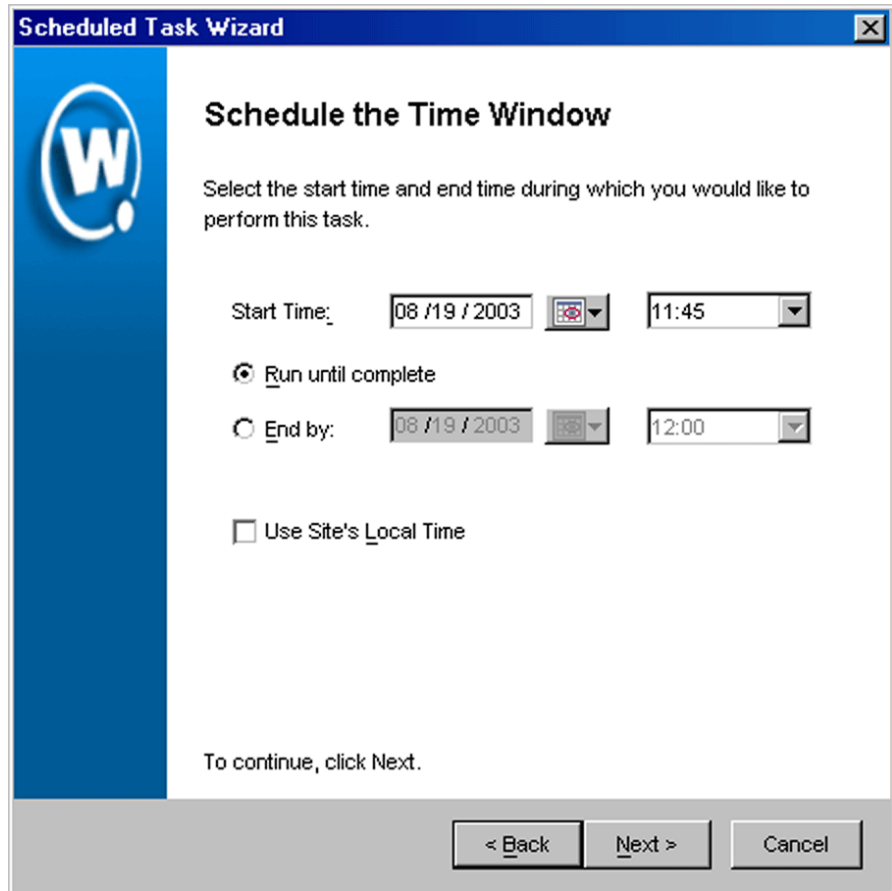
If you want the event to occur immediately select the **Perform the task now** option.

If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

If you want the event to occur on a regular basis, select the **Schedule a recurring event** for this task option.



- 7 Click Next.
- 8 If you selected the **Schedule a one-time event for this task** option, the *Schedule the Time Window* dialog box appears.



**Figure 10-6.** *The Schedule the Time Window Dialog Box*

Within this dialog box, you can set the following parameters for the event:

- Select the start date and time for the event.
- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete**

option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.
- 9** If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

**Scheduled Task Wizard**

## Configure Task Recurrence

Use the controls below to configure the recurrence settings

**Task time**

Start Time: 00:00  Run until complete  Use Site's Local Time  
 End by: 00:00

**Recurrence pattern**

Daily  Weekly  Monthly

Recur every 1 week(s) on:

Sunday  Monday  Tuesday  Wednesday  
 Thursday  Friday  Saturday

**Range of recurrence**

Start: 08 / 19 / 2003  No end date  End by: / /

To continue, click Next.

< Back Next > Cancel

**Figure 10-7.** The Configure Task Recurrence Dialog Box

Within this dialog box, you can set the following parameters for this event:

- Select the start time for the event.
- Determine when you want the event to stop. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Mobile Manager will generate an alert.

- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for the site, enable the **Use Site's Local Time** option. Otherwise, the start and end times are based on the local time for the Enterprise Management Console.

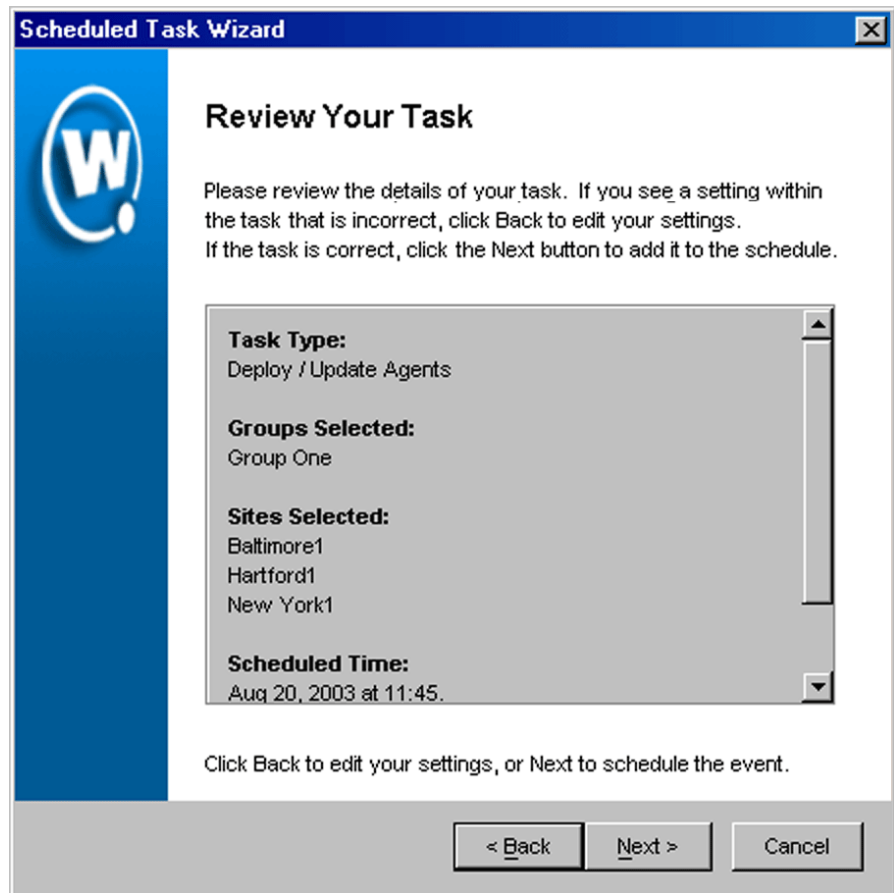
---

**NOTE** Once Mobile Manager begins to send data to a site, it does not stop until all data is sent. This prevents a site from receiving only part of the information it needs. When an event's end time is reached, Mobile Manager completes any deployments that are in-progress, but does not start sending data to any of the remaining sites.

---

**10** Click *Next*.

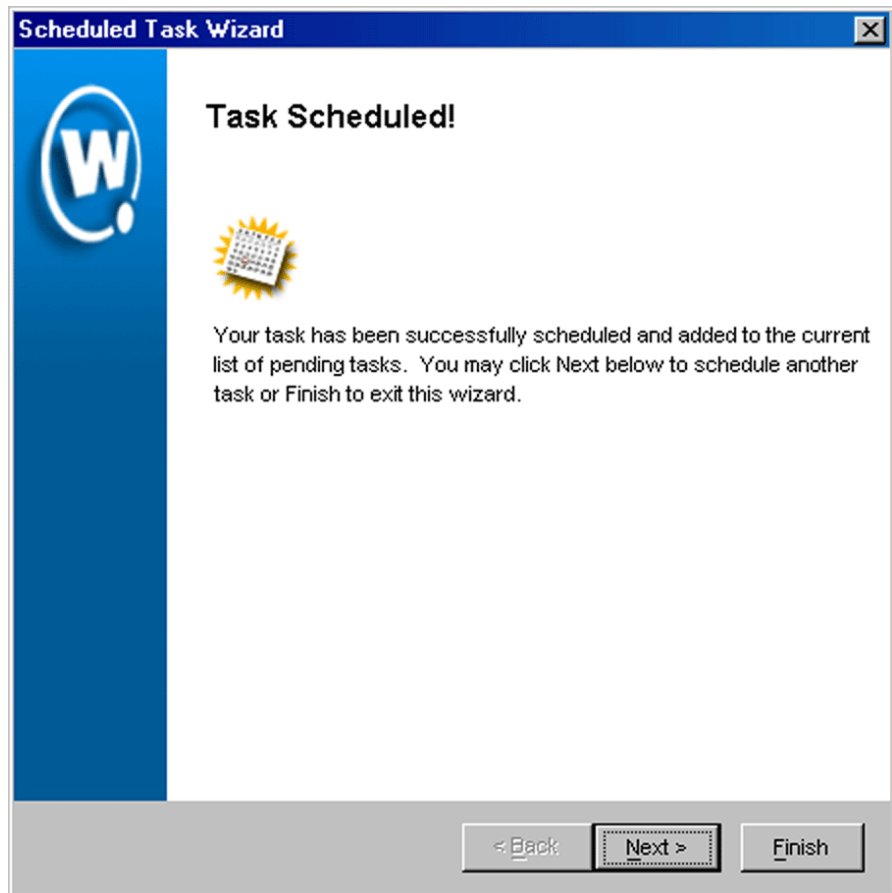
The *Review Your Task* dialog box appears.



**Figure 10-8.** *The Review Your Task Dialog Box*

**11** Review your the task to ensure that it is correct and click Next.

The *Task Scheduled* dialog box appears.



**Figure 10-9.** *The Task Scheduled Dialog Box*

- 12 Click **Next** to schedule a new event, or click **Finish** to return to the Task Schedule dialog box.

## Generating Reports

After the Enterprise Management Console 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.

---

**NOTE** Before you can generate a report, you must first gather statistics from your Agents. See *Gathering Statistics* on page 404 for more information on this process.

---

**To generate a report:**

- 1 Click `Report Statistics` from the Enterprise Management Console 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.





## Appendix A: Installing Mobile Device Enablers

This section describes how to download a copy of the Enabler to the mobile device. After the initial installation of the Enabler, future Enabler upgrades can occur over a wireless connection through the Avalanche Manager.

See *Installing Mobile Device Enablers* on page 25 to obtain the correct file name for the Avalanche Enabler.

This section contains instructions for loading the Avalanche Enabler on the following devices:

- [3000 Series](#)
- [7000 Series](#)
- [Palm OS](#)
- [Windows CE/Pocket PC](#)
- [VRC 4040/5050](#)

In addition, this section provides information on how to install the Enabler on a computer using a [Windows](#) operating system.

### Loading the Enabler on a Series 3000 Device

A 3000 series mobile device is any Symbol mobile device which relies on a hex image for its initial software download. The actual model numbers are

1xxx, 3xxx, and 6xxx, where each x denotes a digit in the model number. Some example model numbers are 1040, 3840, and 6940.

**To install the Enabler on a Series 3000 device:**

- 1 Boot the mobile device into Command Mode, according to the directions in table 1.

	Command Mode Boot Sequence
46-key LRT 3840 46-key PDT 3140 47-key PDT 3540 46-key PDT 6840 46-key PDT 6140	Power off the mobile device. Hold F+l. Press and release PWR. Release F+l.
54-key VRC 3940 54-key VRC 6940	Power off the mobile device. Hold A+D. Press and release ON/OFF. Release A+D.
35-key PDT 6140 35-key PDT 3140	Power off the mobile device. Hold BKSP+SHIFT. Press and release ON/OFF. Release BKSP+SHIFT.
27-key WSS 1040	Power off the mobile device. Hold FUNC+ENTER. Press and release PWR. Release FUNC+ENTER.

**Table 1:** *Command Mode Boot Sequences*

- 2 Use the up arrow and down arrow keys to select the Program loader function.
- 3 Place the mobile device in the cradle.
- 4 Press ENTER. The Program Loader screen appears.

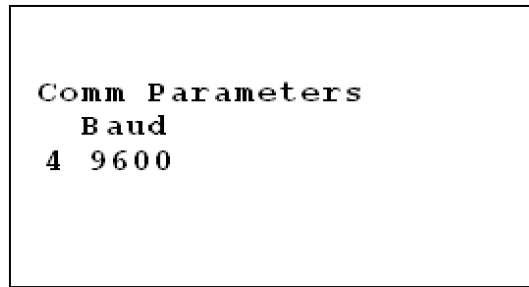
```

Program Loader
WARNING: EEPROM
WILL BE ERASED
CONTINUE? <ENT>

```

**Figure A-1.** *Program Loader EEPROM Erase*

- 5 Press ENTER to erase the non-volatile memory. The Comm Parameters screen appears.



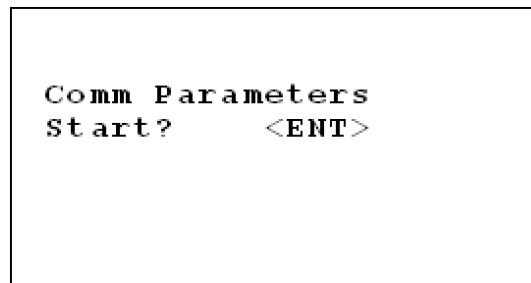
**Figure A-2.** Program Loader Baud Parameter

- 6 Use the Up Arrow/Down Arrow to select the communication parameters. Press ENTER at the end of the selection to accept the parameters.

	Value
Baud	38400
Data Bits	8
Parity	None
Flow Control	None

**Table 2:** Download Communication Parameters

The Comm Parameters screen appears.



**Figure A-3.** Program Loader - Comm Parameters

---

**NOTE** If the cradle supports multiple mobile devices, prepare each in the same manner.

---

- 7 Press ENTER on the mobile device.

The Program Loader–Receiving screen appears and the mobile device is now ready to download the Enabler.

- 8 Verify that a COM port is available for use.

To check the status on a COM port, double-click the COM port in the Tree View and read the information that appears in the Status branch. The status for an available COM port is Listening.

If the Avalanche Manager Agent did not automatically detect the COM ports during the installation, see the *Avalanche Manager's User Guide* before attempting a serial download.

---

**NOTE** COM ports used by other software programs or hardware peripherals should be removed from the list of available serial ports.

---

---

**NOTE** The Avalanche Manager Agent must reside on the system with the serial port connections. However, you can manage the Agent either from a local or remote Management Console. To manage the Agent from a remote console, you must connect to the Agent from the console using a routable IP address.

---

- 9 Download the Enabler using the HEX file download utility included with the Avalanche Manager. See *Downloading Hex Files* on page 27 for more instructions.

After the files have been downloaded, a 3000 Series device indicates a successful file transfer with status code 0000.

## Loading the Enabler on a Series 7000 Device

Downloading the Avalanche Enabler on a Series 7000 DOS device involves the following tasks:

- Configuring Serial Ports
- Running the Enabler Build Kit
- Preparing the Mobile Device
- Downloading the Enabler

**To configure serial ports:**

- Follow the steps in *Using the Hex File Download Utility* on page 28.

**To run the Avalanche Enabler build kit:**

- 1 If you downloaded the enabler kit, navigate to the file and double-click it.

A command prompt appears for several seconds, and several files, including HEX-KIT.EXE, and INSTALL.BAT, appear in the current directory.

---

**NOTE** The name of the Enabler build kit for Symbol 7000 Series devices is Ava7xxx.exe, where the xxx delineates the specific mobile device type). Installation of the build kit is required only for devices that do not ship with Wavelink Avalanche.

---

---

**NOTE** If you are installing the Avalanche Enabler from a CD-ROM, insert the CD-ROM into your CD-ROM drive, locate the build kit executable and double-click the file to open it. Navigate to the location of the INSTALL.BAT file.

---

- 2 Double-click the INSTALL.BAT file.

A command prompt appears. Verify the drive where the directory will be located.

- 3 Press any key to continue.

A second command prompt appears, describing the build kit. This prompt specifies the location for the standard hex file, download utility, and a custom kit for building specialized hex files.

- 4 Press any key to install the build kit.

The build kit installs the necessary files into a new directory on your hard drive (for example, C:\AVA7546). When the installation is complete, this screen closes.

The required hexfiles and partition files will be located in the new directory.

**To prepare a Series 7000 device to download files:**

- 1 Connect the mobile device to the system using the appropriate synchronization/charging cable.
- 2 To determine the partition size for your mobile device, command boot the device by holding down the POWER button and the SCAN button until the device beeps. This takes approximately 15 seconds.

Immediately after the beep, the mobile device screen briefly displays its flash type. The flash type determines what partition file to load. This table lists the flash types, the partition sizes available, and the corresponding name of the partition file.

	Partition Size	Partition file
0400	2 MB	PT-0400A.HEX
0800	4 MB	PT-0800A.HEX
0808A	8 MB	PT-0808A.HEX
0818A	16 MB	PT-0818A.HEX

**Table 3:** *Flash Type*

- 3 Note the name of the required partition file for downloading later.
- 4 If the Baud Rate screen is not the current screen, select Prev Menu from the mobile device's Command screen. On the Baud Rate screen, you set the download speed for the device.

---

**NOTE** The interface of the mobile device is a touch screen. Use a stylus to select options. The arrow keys, used for scrolling, are located on either side of the device screen.

---



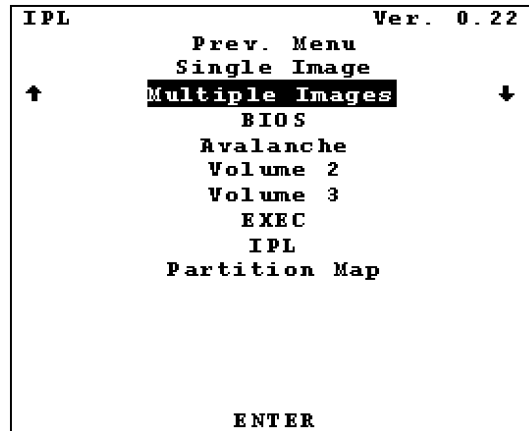
---

**NOTE** The default download speed using the built-in download utility, or through a cradle, is 38400. To use a higher speed you need Symbol's cable #25-37380-01, and it is recommended you use the WinHex utility to download.

---

- 5 Choose the appropriate download speed and select ENTER.

The Command screen appears. Figure 3-1 shows an example of the Command screen for the mobile device.



**Figure A-4.** The Command Screen for a Symbol 7000 Series Device

- 6 On the Command screen, choose Multiple Images and select ENTER. The Waiting for Data screen appears and the mobile device is now ready to download the Enabler.

**To download the Enabler:**

- 1 Verify that a COM port is available for use.

To check the status on a COM port, double-click the COM port in the Tree View and read the information that appears in the Status branch. The status for an available COM port is Listening.

If the Avalanche Manager Agent did not automatically detect the COM ports during the installation, see the *Avalanche Manager User's Guide* before attempting a serial download.

---

**NOTE** COM ports used by other software programs or hardware peripherals should be removed from the list of available serial ports.

---

---

**NOTE** The Avalanche Manager Agent must reside on the system with the serial port connections. However, you can manage the Agent either from a local or remote Management Console. To manage the Agent from a remote console, you must connect to the Agent from the console using a routable IP address.

---

- 2 Download the Enabler using the HEX file download utility included with the Avalanche Manager. See *Downloading Hex Files* on page 27 for more instructions.

You must download the correct partition file before you download the Enabler file.

## Loading the Enabler on Palm OS Devices

Wavelink Avalanche currently supports the SPT 1740 Palm OS device.

---

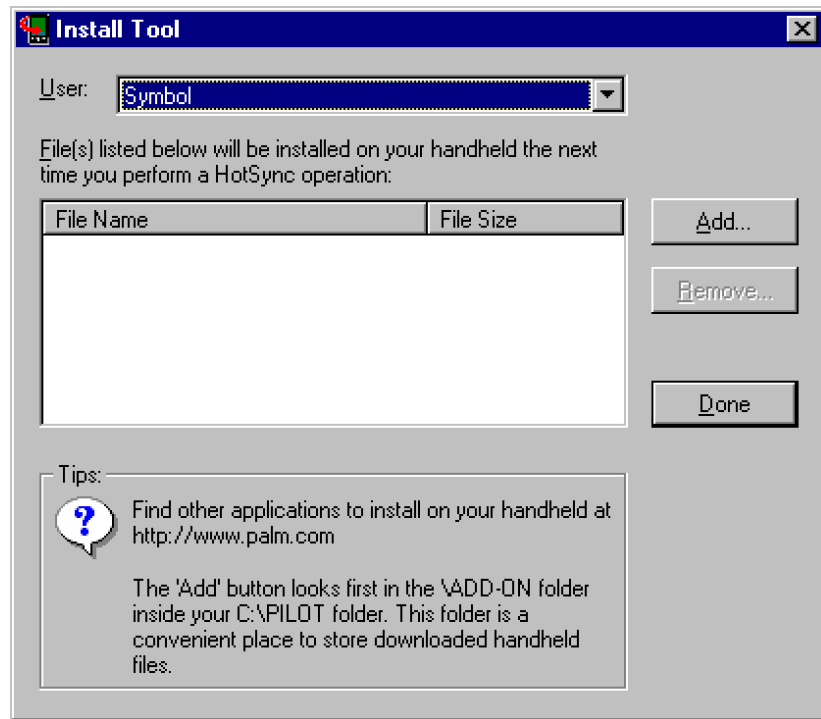
**NOTE** It is assumed that the Palm Desktop is already installed on the system. See the Palm Desktop documentation for more information.

---

### To install the Enabler on a Palm OS device:

- 1 Acquire the Avalanche enabler for the device and navigate to the location where you downloaded the Enabler file.
- 2 Launch the Palm Desktop application on the system.
- 3 Click the **Install** button on the left hand side of the screen. The Install Tool window opens.

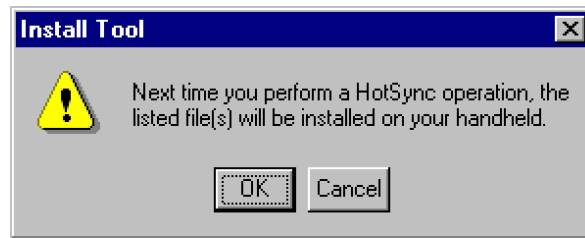




**Figure A-5.** *Install Tool*

- 4** In the Install Tool Window, click Add, then browse for and select the Enabler file.
- 5** Click Open.
- 6** Click Done.

The following message box appears.



**Figure A-6.** *Install Tool Message*

- 7 Exit the Palm Desktop.
- 8 Hotsync the mobile device.

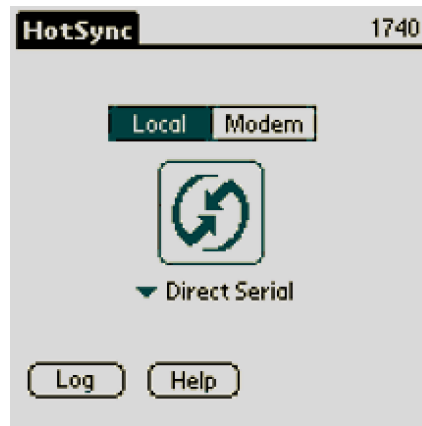
To Hotsync, connect the mobile device to the serial connection or setup the RF connection (see the Palm Desktop documentation for more information). If the device is set up for serial connection, it will automatically launch the HotSync utility. Otherwise, click the **HotSync** icon on the device.

The Hotsync screen is shown in Figure 7.

---

**NOTE** If you started the Avalanche Manager Agent, the Agent will be using any serial ports that it detected. These serial ports will appear in the Tree View of the Avalanche Manager when you are connected to the Agent. To force the Agent to release the ports, see the *Avalanche Manager User's Guide*.

---



**Figure A-7.** *The HotSync Screen*

- 9 Click the Hotsync icon to begin the download process.

Before you can connect to the wireless network, you must configure the network parameters in the Avalanche Enabler.

**To configure the Enabler on a Palm device:**

- 1 When the download process is complete, click the **Avalanche** icon on the Applications screen to launch the Avalanche Enabler.

When the Enabler launches, it will first try to associate to an ESSID. If it associates, it then queries the network for an Avalanche Manager. If it finds a Manager, the Enabler checks to see if the Manager contains a package enabled for it based on its device type, and it will start to transfer the package to the mobile device. If the device is connected to the system by a serial connection, the Enabler will also query to find an Avalanche Manager, and then transfer any enabled packages with which it is associated.

The Enabler opens the Select Application screen. This screen provides three options: the **Execute** button runs an installed application; the **Connect** button tries to connect to an Avalanche Manager; and the **Setup** button opens the Enabler configuration screen. If an application is already installed on the mobile device and appears in the Select Application screen, the Enabler will automatically launch the application after a designated time period, usually about five seconds.

- 2 In the Select Application Screen, click *Setup*.
- 3 In the Avalanche Settings screen, click *Modify*.
- 4 On the Network Preference screen, click *Details*.
- 5 Configure the ESS ID, IP address, and DNS settings. When you are finished, click *Done*.
- 6 In the Avalanche Setup screen, enter the IP address of the Avalanche Manager and click *OK*.

The Avalanche Enabler setup is complete. See *Installing Software Packages* on page 257 for information on downloading software packages.

## Loading the Enabler on WinCE/PocketPC Devices

Wavelink Avalanche currently supports numerous WinCE and PocketPC mobile devices, including Symbol 2740, 2800, 7900, 8100, and 8900 CE devices.

Contact Wavelink at (425) 823-0111 to obtain the most current list of CE devices supported by Wavelink Avalanche.

Before you can download the Enabler and the client files to the mobile device, you must establish a partnership using ActiveSync.

---

**NOTE** It is assumed that ActiveSync has been previously installed on the system. Pocket PC devices require ActiveSync version 3.1.

---

### To establish an ActiveSync partnership with the mobile device:

- 1 Launch ActiveSync.
- 2 Connect the custom serial cable for the TN client while ActiveSync searches for the mobile device.

---

**NOTE** For VRC7900 devices, connect the cable to Port 2.

---

---

**NOTE** For the SPT2740, ensure that you use the SPT2740 cable rather than the SPT1740 cable. Otherwise, you can experience problems in connecting to ActiveSync. The cable part number for the SPT2740 is 25-38383-01, Rev A.

---

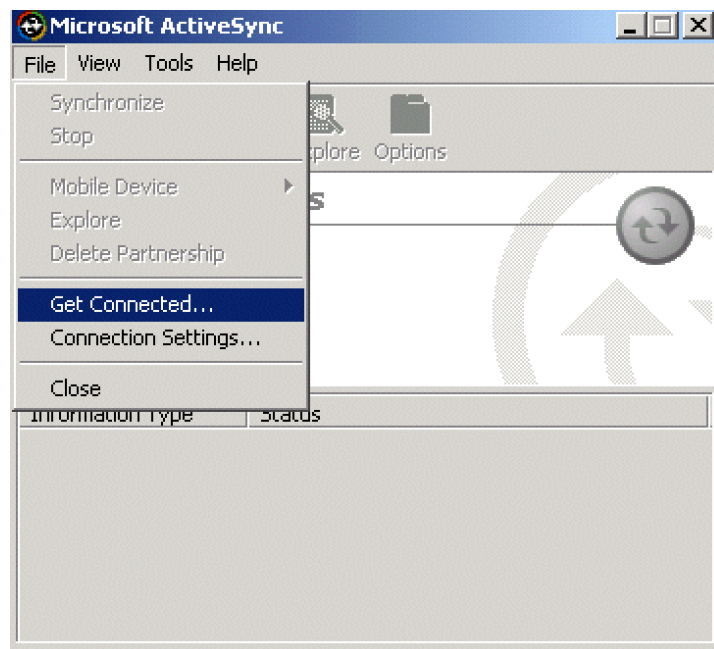
- 3 ActiveSync scans the serial ports to find the one that is connected to the mobile device.

---

**NOTE** If you started the Avalanche Manager Agent, the Agent will be using any serial ports that it detected. These serial ports will appear in the Tree View of the Avalanche Manager when you are connected to the Agent. To force the Agent to release the ports, see the *Avalanche Manager User's Guide*.

---

- 4 In ActiveSync, select Get Connected from the **File** menu.



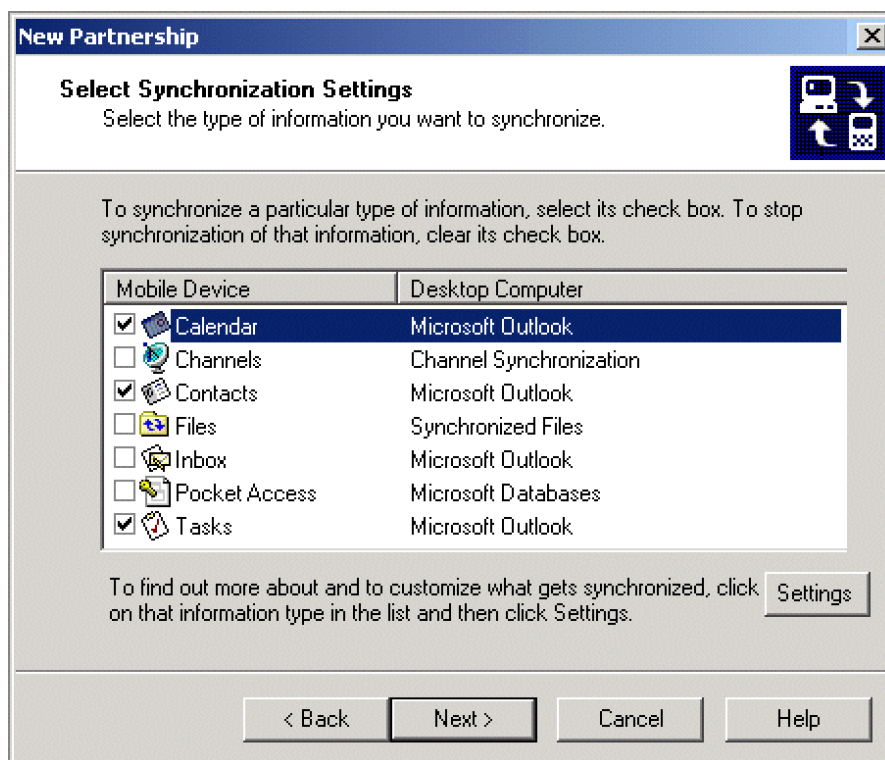
**Figure A-8.** ActiveSync Get Connected Menu Option

An ActiveSync Partnership is required to download the Enabler to the mobile device. The dialog box shown in Figure A-9 appears.



**Figure A-9.** *New Partnership*

- 5 Follow the on-screen prompts. Synchronize with your system only when prompted.
- 6 Determine which applications will be used on the mobile device and set the Synchronization Settings accordingly. See Figure A-10.



**Figure A-10.** *Synchronization Settings*

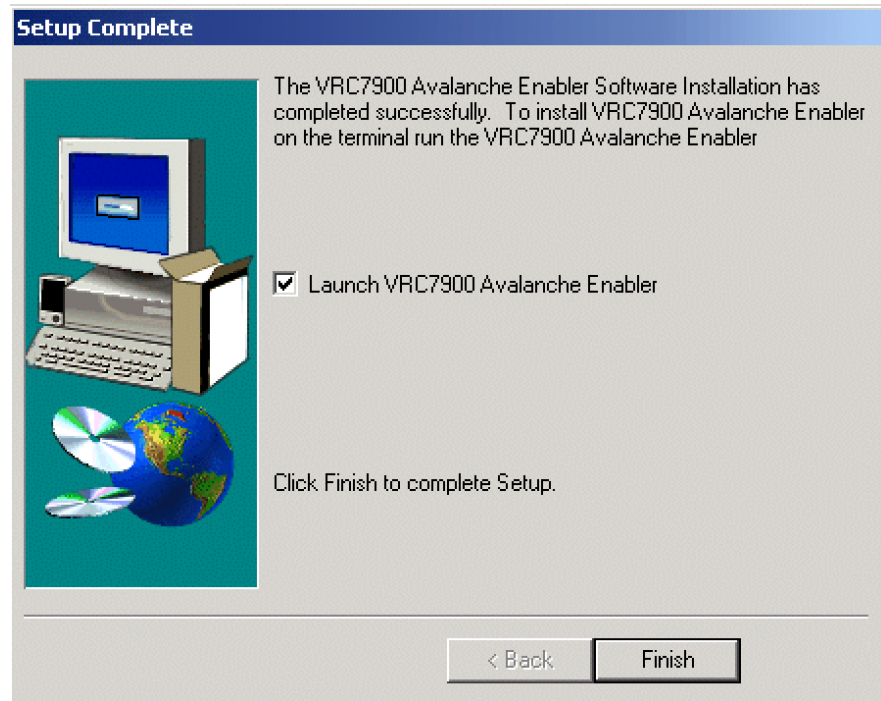
**To install the Avalanche Enabler:**

- 1 Verify that ActiveSync is still running. Navigate to the Enabler file and double-click the file to start the Enabler installation.
- 2 In the Welcome dialog box, click **Next**.
- 3 Choose the desired installation destination.

It is recommended that the default destination folder be used. The default folder is `C:\Program Files\Wavelink\Avalanche\Client\[device type]`. The Enabler must be installed on the system before it is installed on the CE device.

- 4 Add the program icons to the default program folder of Wavelink Avalanche.

- 5 Add a shortcut on the system when prompted.
- 6 In the Setup Complete dialog box, verify that the **Launch Avalanche Enabler** option is enabled and click **Finish**.

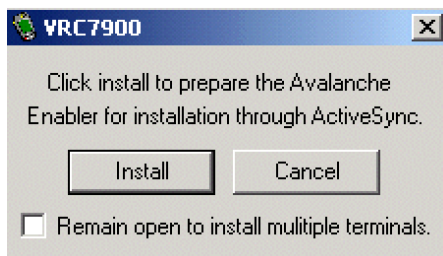


**Figure A-11.** Setup Complete Dialog Box

The Install Enabler through ActiveSync dialog box automatically appears.

- 7 If multiple mobile devices are to receive the installation files, enable the check box in the lower left.
- 8 Click **Install**.





**Figure A-12.** *Install Enabler through ActiveSync*

- 9 Follow the on-screen installation prompts to complete the installation of the Enabler on the CE device. It is recommended that the default folder be used.

---

**NOTE** If this is a reinstall, the prompts on the system and the mobile device will indicate this. Respond to these prompts as needed.

---

Before you can connect to the wireless network, you must configure the network parameters in the Avalanche Enabler.

**To configure the Enabler on a Windows CE/Pocket PC device:**

- 1 On the mobile device, click the **Avalanche** icon to launch the Avalanche Enabler.

When the Enabler launches, it will first try to associate to an ESSID. If it associates, it then queries the network for an Avalanche Manager. If it finds one, it checks to see if there is a package enabled for it based on its device type, and it will start to transfer the client to the mobile device. If the device is connected to the system by a serial connection, the mobile device will also query to find an Avalanche Manager, and then transfer any enabled packages with which it is associated.

The Enabler will open the Select Application dialog box. This dialog box provides three options; the **Execute** button runs an installed application; the **Connect** button tries to connect to an Avalanche Manager, and the **Setup** button opens the Avalanche Configuration dialog box. If an application is already installed on the mobile device and appears in the Select Application dialog box, the Enabler will automatically launch the application after a designated time period, usually about five seconds.

- 2 In the Select Application dialog box, click *Setup*.

The Avalanche/IP Configuration dialog box appears. The first tab has boxes to enter in the Avalanche Manager IP address and another box to enter in the ESSID.

- 3 Click the **IP** tab to configure IP settings. Here you can set the mobile device to use DHCP or manually input an IP address, subnet mask, and Gateway.
- 4 Click the **DNS** tab and, if necessary, and enter the required DNS settings.
- 5 Click **OK**.

A dialog box appears with the following message: "The next time the adapter is used the new settings will take place."

- 6 Click **OK**.

The Avalanche Enabler setup is complete. See *Installing Software Packages* on page 257 for information on downloading software packages.

## Loading the Enabler on Series 4000/5000 Devices

Follow these steps to download and install the Avalanche Enabler onto a 4000 or 5000 Series mobile device.

### To install the Avalanche Enabler to Series 4000 or 5000 devices:

- 1 Insert the floppy disk containing the Enabler file into the device's external floppy disk drive, typically the A: drive.
- 2 At the command line, type the appropriate command to install the Enabler from the A:\ drive.

```
AVA4040 -d *.* c:\
```

-or-

```
AVA5040 -d *.* c:\
```

- 3 Reboot the VRC4040 or the VRC5040.

The Avalanche Enabler is now loaded on the VRC mobile device.

---

**NOTE** If 802.11 is needed, the RF update software package (RF4\_vxx.exe, where xx represents the version number) must also be installed from the Avalanche Manager using a serial connection. See *Installing Software Packages* on page 257 for more information.

---

## Loading the Enabler on Windows

Follow these steps to download and install the Avalanche Enabler onto a computer using a Windows operating system.

**1** Download the Enabler from the Wavelink Web site, [www.wavelink.com](http://www.wavelink.com).

**2** Open the downloaded file.

A *Welcome* dialog box appears.

**3** Click **Continue** to start the installation process.

An introductory dialog box appears, providing information on the installation process.

**4** Click **Next**.

The License Agreement Dialog box appears.

**5** If you agree to the terms of the license agreement, click **Yes** to continue.

The *Choose Destination Folder* dialog box appears.

**6** Select the destination folder for the Enabler and click **Next**.

The *Select Program Folder* dialog box appears.

**7** Select the program folder for the Enabler and click **Next**.

The Enabler is installed. After the installation is complete, a dialog box appears, asking if you want to create a shortcut icon to the Enabler on your desktop. Click either **Yes** or **No**.

The Setup Complete dialog box appears.

- 8 To start the Enabler immediately, enable the **Yes, I want to launch the Enabler now** check box and then click Finish. Otherwise, click Finish to complete the installation.

## Future Releases

Support for Symbol, Palm, and Windows CE/PocketPC devices continues to expand. Future releases will include support for loading Windows PCs and loading EPOC.

Contact your software supplier for information on availability of Avalanche Enablers for mobile devices not otherwise listed.

## Appendix B: Country Codes for Importing Sites

When you import sites into Mobile Manager, you must create your list of files using specific country codes. These codes are necessary for Mobile Manager to locate the country within its database.

---

**NOTE** Additional information on importing sites is available in *Importing Sites* on page 130.

---

The following table lists the codes that Mobile Manager recognizes.

Code	Name
AA	Aruba
AC	Antigua and Barbuda
AE	United Arab Emirates
AF	Afghanistan
AG	Algeria
AJ	Azerbaijan
AL	Albania
AM	Armenia
AN	Andorra
AO	Angola
AQ	American Samoa
AR	Argentina
AS	Australia
AT	Ashmore and Cartier Islands
AU	Austria
AV	Anguilla
AY	Antarctica
BA	Bahrain
BB	Barbados
BC	Botswana
BD	Bermuda
BE	Belgium

**Table B-1.** Country Codes for Importing Sites

Code	Name
BF	Bahamas
BG	Bangladesh
BH	Belize
BK	Bosnia and Herzegovina
BL	Bolivia
BM	Burma
BN	Benin
BO	Belarus
BP	Solomon Islands
BQ	Navassa Island
BR	Brazil
BS	Bassas Da India
BT	Bhutan
BU	Bulgaria
BV	Bouvet Island
BX	Negara Brunei Darussalam
BY	Burundi
CA	Canada
CB	Cambodia
CD	Chad
CE	Sri Lanka
CF	Republic of the Congo
CG	Democratic Republic of the Congo
CH	China
CI	Chile
CJ	Cayman Islands
CK	Cocos Islands
CM	Cameroon
CN	Comoros
CO	Colombia
CQ	Northern Mariana Islands
CR	Coral Sea Islands
CS	Costa Rica
CT	Central African Republic

**Table B-1.** Country Codes for Importing Sites

Code	Name
CU	Cuba
CV	Cape Verde
CW	Cook Islands
CY	Cyprus
DA	Denmark
DJ	Djibouti
DO	Dominica
DQ	Jarvis Island
DR	Dominican Republic
EC	Ecuador
EG	Egypt
EI	Ireland
EK	Equatorial Guinea
EN	Estonia
ER	Eritrea
ES	El Salvador
ET	Ethiopia
EU	Europa Island
EZ	Czech Republic
FG	Guiana
FI	Finland
FJ	Fiji
FK	Falkland Islands
FM	Micronesia
FO	Faroe Islands
FP	French Polynesia
FQ	Baker Island
FR	France
FS	French Southern and Antarctic Lands
GA	Gambia
GB	Gabonese Republic
GG	Georgia
GH	Ghana
GI	Gibraltar

**Table B-1.** Country Codes for Importing Sites

Code	Name
GJ	Grenada
GK	Bailiwick of Guernsey
GL	Greenland
GM	Germany
GO	Glorioso Islands
GP	Guadeloupe
GQ	Guam
GR	Greece
GT	Guatemala
GV	Guinea
GY	Guyana
GZ	Gaza Strip
HA	Haiti
HK	Hong Kong
HM	Heard Island and Mcdonald Islands
HO	Honduras
HQ	Howland Island
HR	Croatia
HU	Hungary
IC	Iceland
ID	Indonesia
IM	Isle of Man
IN	India
IO	British Indian Ocean Territory
IP	Clipperton Island
IR	Iran
IS	Israel
IT	Italy
IV	Ivory Coast
IZ	Iraq
JA	Japan
JE	Bailiwick of Jersey
JM	Jamaica
JN	Jan Mayen

**Table B-1.** Country Codes for Importing Sites



Code	Name
JO	Jordan
JQ	Johnston Atoll
JU	Juan De Nova Island
KE	Kenya
KG	Kyrgyz
KN	North Korea
KQ	Kingman Reef
KR	Kiribati
KS	South Korea
KT	Christmas Island
KU	Kuwait
KZ	Kazakhstan
LA	Laos
LE	Lebanon
LG	Latvia
LH	Lithuania
LI	Liberia
LO	Slovakia
LQ	Palmyra Atoll
LS	Liechtenstein
LT	Lesotho
LU	Luxembourg
LY	Libya
MA	Madagascar
MB	Martinique
MC	Macau
MD	Moldova
MF	Mayotte
MG	Mongolia
MH	Montserrat
MI	Malawi
MK	Macedonia
ML	Mali
MN	Monaco

**Table B-1.** Country Codes for Importing Sites

Code	Name
MO	Morocco
MP	Mauritius
MQ	Midway Islands
MR	Mauritania
MT	Malta
MU	Oman
MV	Maldives
MW	Montenegro
MX	Mexico
MY	Malaysia
MZ	Mozambique
n/a	Aksai Chin
n/a	Demilitarized Zone
n/a	United Nations Disengagement Observation Force
n/a	United Kingdom Sovereign Base Area
n/a	Us Naval Base Guantanamo Bay
NC	Territory of New Caledonia and Dependencies
NE	Niue
NF	Norfolk Island
NG	Niger
NH	Vanuatu
NI	Nigeria
NL	Netherlands
NM	No Man's Land and Mount Scopus Area
NO	Norway
NP	Nepal
NR	Nauru
NS	Suriname
NT	Netherlands Antilles
NU	Nicaragua
NZ	New Zealand
OS	Oceans (general)
PA	Paraguay
PC	Pitcairn, Henderson, Ducie and Oeno Islands

**Table B-1.** Country Codes for Importing Sites

Code	Name
PE	Peru
PF	Paracel Islands
PG	Spratly Islands
PK	Pakistan
PL	Poland
PM	Panama
PO	Portugal
PP	Papua New Guinea
PS	Palau
PU	Guinea-Bissau
QA	Qatar
RE	Department of Reunion
RM	Marshall Islands
RO	Rumania
RP	Philippines
RQ	Puerto Rico
RS	Russia
RW	Rwanda
SA	Saudi Arabia
SB	Saint Pierre and Miquelon
SC	Saint Kitts and Nevis
SE	Seychelles
SF	South Africa
SG	Senegal
SH	Saint Helena
SI	Slovenia
SL	Sierra Leone
SM	San Marino
SN	Singapore
SO	Somalia
SP	Spain
SR	Serbia
ST	Saint Lucia
SU	Sudan

**Table B-1.** Country Codes for Importing Sites

Code	Name
SV	Svalbard
SW	Sweden
SX	South Georgia and the South Sandwich Islands
SY	Golan Heights
SY	Syria
SZ	Switzerland
TD	Trinidad and Tobago
TE	U.S. Virgin Islands
TH	Thailand
TI	Tajikistan
TK	Turks and Caicos Islands
TL	Tokelau
TN	Tonga
TO	Togo
TP	Sao Tome and Principe
TS	Tunisia
TT	East Timor
TU	Turkey
TV	Tuvalu
TW	Taiwan
TX	Turkmenistan
TZ	Tanzania
UF	(NULL)
UG	Uganda
UK	UK
UM	U.S. Minor Outlying Islands
UP	Ukraine
US	USA
UV	Burkina Faso
UY	Uruguay
UZ	Uzbekistan
VC	Saint Vincent and the Grenadines
VE	Venezuela
VI	British Virgin Islands

**Table B-1.** Country Codes for Importing Sites

<b>Code</b>	<b>Name</b>
VM	Vietnam
VQ	U.S. Virgin Islands
VT	Vatican City
WA	Namibia
WE	West Bank
WF	Wallis and Futuna Islands
WI	Western Sahara
WQ	Wake Atoll
WS	Samoa
WZ	Swaziland
YI	Yugoslavia
YM	Yemen
ZA	Zambia
ZI	Zimbabwe

**Table B-1.** *Country Codes for Importing Sites*



## Appendix C: Local Deployment Enhancement

Mobile Manager Enterprise provides the ability to build packages that allow you to remotely deploy Agents and firmware. The packages that are created in this process rely on a deployment mechanism that is built into Mobile Manager Enterprise. This enhancement provides an alternative means to deploy packages to remote sites. An alternative means of deployment might be desirable if customers prefer to use custom software for deployment, which might be necessitated, for example, by low bandwidth connections.

The general tasks required to use local deployment are:

- 1 Use the Package Wizard in the Enterprise Management Console to create an Agent or firmware deployment package (.zip file).
- 2 Configure the local deployment batch file with the correct parameters.
- 3 Deploy the package and the local deployment files to the target machine. You can choose your own mechanism to transfer these files to the remote site.
- 4 Run the batch file locally on a single target machine.
- 5 Test the deployment on the target machine.
- 6 Distribute and run the package on other target machines.

The topics in this section include:

- Important Notes about the Package Wizard
- Editing the Local Deployment Batch File

### Important Notes about the Package Wizard

For information on using the Package Wizard:

- See *Creating Sites* on page 82 to deploy a package containing one or more Agents.

- See *Creating Firmware Packages* on page 187 to deploy a firmware support package.

When the Package Wizard builds a package, it will store the package file in a subdirectory of `<install directory>\EM\Enterprise\EnterpriseManager\Deploy`. The specific subdirectories of interest are:

<code>\AgentPackage</code>	Contains the package (.zip) file for an access point Agent and/or a mobile device Agent.
<code>\FirmwarePackage</code>	Contains the package (.zip) file for firmware support.

In addition, local deployment files are stored in the following directory:

```
<install
directory>\EM\Enterprise\EnterpriseManager\Deploy\LocalDe
ploy
```

You must place the package file and all files contained in the `\LocalDeploy` subdirectory into a single directory on the target machine.

## Editing the Local Deployment Batch File

You can edit the local deployment batch file before or after you transfer the package files and the local deployment files. This file is named `LocalDeploy.bat`. Use a text editor (such as Notepad) to edit the file.

The file contains instructions for invoking the `deploy` command. You must manually add the `deploy` command to the file. Depending on whether you are deploying an access point Agent, a mobile device Agent, or firmware support, different switches are required, as shown in Table C-1.

Mobile Device Agent only	<code>deploy -h "-wPath" "-iFileName" -o1</code>
Access Point Agent only	<code>deploy -h "-aAdapters" "-wPath" "-iFileName" -o0</code>
Both Agents	<code>deploy -h "-aAdapters" "-wPath" "-iFileName" -o2</code>
Firmware Support	<code>deploy -h "-iFileName" -o3</code>
Uninstall	<code>deploy -h -o4</code>

**Table C-1.** *Deployment Type and Command Syntax*



---

**NOTE** Some of the properties you configure in the Package Wizard are used in Mobile Manager Enterprise deployment mechanism and are not included in the package file. These properties will need to be manually included in the batch file as described in this section.

---

Descriptions for the command line switches are as follows:

`-h` Required switch that specifies local deployment.  
`-aAdapters` Specifies the network card(s) that the access point Agent will use.

The *Adapters* attribute consists of two comma-separated elements, the first of which specifies the network card used to manage devices, and the second value specifies the network card used for access by remote administrators. Each of these elements can be one of the following two values:

`-f` = The first network adapter

`-s Subnet` = The adapter on the specified subnet. (For example, if your adapter is on 172.16.1.16 and your subnet mask is 255.0.0.0, then you would use 172.0.0.0. If your subnet mask was 255.255.0.0, the *Subnet* attribute would be 172.16.0.0. With a subnet mask of 255.255.255.0, the *Subnet* attribute would be 172.16.1.0.)

Examples:

“`-a-f, -f`” should be used with a single network card or if you want to use the first network card both to manage devices and for remote administration.

“`-a-f, -s 172.0.0.0`” specifies that the first network card will be used to manage devices and the network card residing on the 172.0.0.0 subnet will be used for remote administration.

“`-a-s 172.16.0.0, -s 10.10.0.0`” specifies a subnet for each card when a subnet mask of 255.255.0.0 is in use for both network cards.

*-wPath* Specifies the path for installation for one or both Agents.

Example:

“-wC:\Program Files\Wavelink”

---

**NOTE** If this is a new installation of the Agent(s), this value must exactly match the value configured in the Package Wizard.

---

If you are overwriting an existing installation, the deployment program will automatically install the Agent(s) to the current installation directory.

*-iFileName* The name of the package (.zip) file to install.

Example:

“-iMMOnly.zip”

*-oOption* The installation option. The possible values for the *Option* attribute are:

0 = Install the access point Agent

1 = Install the mobile device Agent

2 = Install both Agents

3 = Install additional firmware

4 = Uninstall Mobile Manager Enterprise

Example:

-o2

The option you choose here must match the option configured in the Package Wizard.

Here are a few examples of the deploy command.

The following example deploys an access point Agent:

```
deploy -h "-a-f, -s 172.0.0.0" "-wC:\Program  
Files\Wavelink" -iMMOnly.zip -o0
```

---

**NOTE** The quotation marks are required when spaces are included in the attribute value.

---

The following example deploys firmware:

```
deploy -h -iC1200-15.zip -o3
```

This example uninstalls Mobile Manager Enterprise:

```
deploy -h -o4
```

**To run the batch file:**

- 1 Open a command line on the target machine.
- 2 Switch to the directory containing the batch file and all deployment files.
- 3 Type the command LocalDeploy.bat and press the Enter key.

---

**NOTE** It is highly recommended that you test your batch file and deployment on a single machine before proceeding with a large deployment.

---



## Appendix D: Functions Available

Listed here are the functions that are available in the Enterprise Management Console based on a user's Agent Type and Permissions. For brevity, this appendix uses 'non-read-only' to indicate Read/Write or Administrative permission.

### General

#### Top-Level Menu

Enterprise User:

- File > New, Move Site To, Rename, Page Setup, Print Preview, Print Current Report, Import/Export Site Data, Options, Properties, Exit

Access Point Agent, Mobile Device Agent, and Read Only users:

- File > Save, Page Setup, Print Preview, Print Current Report, Options, Properties, Exit

All other menus are available the same for all users.

#### Toolbar

Enterprise User:

- New Group, New Site, Save, Print, Print Preview, Software Collections Manager, User Manager, Task Schedule, Deployment Package Manager, Email Option Manager, Proxy Pool Manager, Very Large Access Control List, Site Alert Filter Manager, Help

Access Point Agent, Mobile Device Agent, and Read Only users:

- Save, Print, Print Preview, Software Collections Manager, User Manager, Task Schedule, Deployment Package Manager, Email Option Manager, Proxy Pool Manager, Very Large Access Control List, Site Alert Filter Manager, Help

### Dialog Boxes

#### Options Dialog

Control is only enabled for Enterprise Users, non-read-only.

### **Group and Site Properties Dialog**

Control is only enabled for Enterprise Users, non-read-only.

### **Software Collections Manager Dialog**

Control is enabled for Enterprise Users and Mobile Device Agent Users, non-read-only.

Enterprise and Mobile Device Agent users, non-read-only have the following menu configuration:

- File > New Collection, Install Package, Delete, Rename, Restore from Repository, Refresh, Close
- Edit > Configure, Enable, Disable, Copy, Move, Select All
- Help > Software Collections Help

Access Point Agent and Read Only users have the following menu configuration:

- File > Refresh, Close
- Edit > Select All
- Help > Software Collections Help

Additionally, popup menus and keyboard shortcuts (except ctrl-a for select all) are disabled for Access Point Agent and Read Only users.

### **User Manager Dialog**

Users with Administrator permissions are able to create, edit, and delete users as follows:

Enterprise users:

- Create all types of users
- Edit all user types

- Can change agent type for Access Point Agent and Mobile Device Agent users only
- Can change permission level for all users, except Enterprise users with Administrator permissions
- Can delete all users except oneself

Access Point Agent users:

- Create Access Point Agent users only
- Edit Access Point Agent users
  - Can change permission levels for all Access Point Agent users
- Can delete all Access Point Agent users except oneself

Mobile Device Agent users:

- Create Mobile Device Agent users only
- Edit Mobile Device Agent users
  - Can change permission levels for all Mobile Device Agent users
- Can delete all Mobile Device Agent users except oneself

### **Deployment Package Manager Dialog**

Non-read-only users are able to create, edit, and delete packages as follows:

Enterprise users:

- All packages

Access Point Agent users:

- Access Point Agent Packages
- Lightweight Access Point Agent Updates
- Firmware Update Packages

Mobile Device Agent users:

- Mobile Device Agent Packages

When attempting to edit or delete an existing package without the proper permissions, a message box will alert the user that access to the selected package is denied.

For deleting a multiple selection, packages will be deleted until one is encountered to which the user is denied access. At that point, a message box will inform the user of the situation and deleting will stop.

### **Task Scheduler**

Non-read-only users are able to schedule, run, and reschedule tasks as follows:

Enterprise users:

- All tasks

Access Point Agent users:

- Deploy Access Point Settings
- Update Very Large Access Control List
- Update Access Point Firmware
- Retrieve Access Point Statistics

Access Point Agent users that have Administrator permission can additionally:

- Update User Accounts – only Access Point Agent users will be deployed

Mobile Device Agent users:

- Deploy Mobile Device Settings

Mobile Device Agent users that have Administrator permission can additionally:

- Update User Accounts – only Mobile Device Agent users will be deployed

When attempting to edit, delete, or run an existing task without the proper permissions, a message box will alert the user that access to the selected tasks is denied.



For deleting a multiple selection, tasks will be deleted until one is encountered to which the user is denied access. At that point, a message box will inform the user of the situation and deleting will stop.

### **Email Manager Dialog**

Control is enabled for Enterprise and Access Point Agent users, non-read- only.

### **Proxy Manager Dialog**

Control is enabled for Enterprise and Access Point Agent users, non-read- only.

### **Very Large Access Control List Dialog**

Control is enabled for Enterprise and Access Point Agent users, non-read- only.

### **Site Alert Filter Manager Dialog**

Control is enabled for Enterprise users, non-read-only.

## **Views**

### **Monitor Activity**

#### **Popup Menu for Site on Map**

Enterprise users:

- Site Name, Re-center Map, Cancel, Connect To Site, Relocate, Clear Alarms, Properties

Access Point Agent, Mobile Device Agent, and Read Only users:

- Relocate menu item is removed

### **Configure Network**

#### **Network Settings**

EssId:

- Enabled for Enterprise users, non-read-only

IP Address Management:

- IP Address Option for Access Points: enabled only for Enterprise and Access Point Agent users, non-read-only
- IP Address Option for Mobile Devices: enabled only for Enterprise and Mobile Device Agent users, non-read-only
- Add button: Visible and enabled for non-read-only users
- Add dialog: Enterprise users can select which agent the addresses shall be used for, otherwise, these options are not visible.
- Delete button: Visible and enabled for non-read-only users
- Advanced dialog:
  - General tab: controls enabled only for Enterprise users, non-read-only
  - Mobile Device Settings tab: controls enabled Enterprise and Mobile Device Agent users, non-read-only

#### WEP Settings:

- Controls enabled for Enterprise users, non-read-only

#### Device Access Privileges:

- Visible and enabled only for Enterprise and Access Point Agent users, non-read-only

### **Access Point Profiles**

Enabled for Enterprise and Access Point Agent users, non-read-only

- Popup menu for selection contains the following: New Access Point Profile, Refresh Profile List, Cut, Copy, (Paste), Delete, Properties
- Popup menu for non-selection contains the following: New Access Point Profile, Refresh Profile List, (Paste), Select All

Mobile Device Agent and Read Only users can view all profile properties, but cannot create new, copy, move, or otherwise edit.

- Popup menu for selection contains the following: Refresh Profile List, Properties

- Popup menu for non-selection contains the following: Refresh Profile List, Select All

### **Mobile Device Settings**

Enabled for Enterprise and Mobile Device Agent users, non-read-only

Alert Profiles:

Enabled for Enterprise and Access Point Agent users, non-read-only

- Popup menu for selection contains the following: New Alert Profile, Refresh Profile List, Cut, Copy (Paste), Delete, Properties
- Popup menu for non-selection contains the following: New Alert Profile, Refresh Profile List, (Paste), Select All

Mobile Device Agent and Read Only users can view all profile properties, but cannot create new, copy, move, or otherwise edit.

- Popup menu for selection contains the following: Refresh Profile List, Properties
- Popup menu for non-selection contains the following: Refresh Profile List, Select All



# Index

## A

- access control lists
  - building 311
  - deploying 322
  - exporting files 318
  - importing files 318
  - modifying entries 314
  - removing 316
- access points 12
  - activating security 167
  - applying settings 174
  - configuration 167
  - creating profiles 160
  - deploying settings 227
  - deployment packages 83
  - managing 153
  - properties 166
  - scheduling profiles 171
  - security 167
  - security settings 361
  - settings 174
  - updating firmware 186
- access privileges 154
- activating Mobile Manager 22
- adding
  - MAC addresses 312
  - sites 119
  - sites to the Enterprise Management Console 110
  - synchronization events 283
  - tasks 71
- advanced
  - radio properties 350
  - security options 348
- Agent
  - assigning to mobile devices 215
  - centralized installation 17
  - deleting 138

- distributed installation 19
  - placement 17
- alarm browser 50, 399
- alerts
  - configuring statistical alerts 394
  - creating profiles 390
  - deleting profiles 393
  - deleting statistical alerts 398
  - editing statistical alerts 398
  - managing 385
  - modifying profiles 393
  - profiles 385
  - setting the destination IP address for 399
  - site alert filter manager 408
  - statistical 394
- assigning
  - Agent to mobile device 215
  - ESS IDs 205
  - IP addresses 208
- authenticating mobile devices 295
- automatic synchronization 294
- available functions 475

## B

- building
  - access control lists 311
  - selection criteria 269

## C

- capturing network events 168
- changing account passwords 58
- Cisco IOS
  - access privileges 157
  - VLANS 340
- client software 16
- collections
  - creating 253
  - deleting 280

- disabling 278
- enabling 277
- renaming 255
- COM ports 295
- compatibility mode 186
- components of Mobile Manager 9
- configuring
  - access points 167
  - automatic WEP rotation 333
  - Enabler 33
  - packages 265
  - profiles 162
  - site components 151
  - WEP Keys 331
- controlling site communication 51
- copying packages 263
- country codes 459
- creating
  - access point profiles 160
  - alert profiles 390
  - deployment packages 83
  - e-mail address list 386
  - firmware packages 187
  - profiles 162
  - proxy pool 388
  - sites 82
  - software collections 253
  - user accounts 55
- D**
- database maintenance 414
- defining selection criteria 265
- deleting
  - Agent 138
  - alert profiles 393
  - collections 280
  - completed tasks 78
  - e-mail addresses 388
  - orphaned packages 293
  - packages 280
  - profiles 165
  - proxies 390
  - sites 146
  - tasks 74
  - user accounts 57
- deploying
  - access control lists 322
  - access point settings 227
  - firmware packages 192
  - mobile device settings 238
  - network settings 217
  - security settings for all devices 351
  - security settings to access points 361
  - security settings to mobile devices 372
  - security settings 351
  - settings for all devices 217
  - settings to mobile devices 297
  - sites 121
  - user accounts 59
- deployment packages
  - access points 83
  - all devices 100
  - creating 83
  - mobile devices 93
- device access privileges 154
- devices
  - Palm OS 446
  - Series 3000 439
  - Series 4000/5000 456
  - Series 7000 442
  - supported 17
  - WinCE/PocketPC 450
- disabling
  - collections 278
  - packages 278
- document
  - assumptions 7
  - conventions 8
- downloading
  - Enabler 27

Hex files 27

## **E**

EAP 344  
EAP accounting 347  
editing  
    local deployment batch file 470  
    tasks 73  
    user accounts 57  
e-mail address  
    creating list 386  
    deleting 388  
    importing 387  
Enabler  
    configuring 33  
    downloading 27  
    installing 25  
enabling  
    collections 277  
    EAP accounting 347  
    packages 277  
Enterprise Management Console  
    Configure Network view 42  
    Groups window 46  
    modifying colors 40  
    Monitor Activity view 37  
    preferences 48  
    Report Statistics view 45  
    Saving views 40  
    Search 47  
    starting 35  
    views 37  
ESS IDs 205  
excluding  
    dates 292  
    times 292  
existing site data 133  
exporting  
    access control list files 318  
    site data 134

Extensible Authentication Protocol 344

## **F**

firmware  
    creating packages 187  
    deploying packages 192  
    support 186  
    updating 186  
full support mode 186  
functions 475  
future releases 458

## **G**

gateway IP addresses 212  
gathering statistics 426  
generating reports 436  
groups  
    adding sites 150  
    deleting 152  
    location management 9

## **H**

Hex files  
    download utility 28  
    downloading 27  
    simultaneous download 32

## **I**

importing  
    access control list files 318  
    e-mail addresses 387  
    existing site data 133  
    sites 459  
    sites 130  
installing  
    centralized Agent 17  
    distributed Agent 19  
    Enablers 25  
    mobile device enablers 439  
    Mobile Manager 11, 20  
    software packages 257

- internet connectivity 12
- IP addresses
  - assigning 208
  - for Network Alerts 399
  - removing 212
  - managing 207

## **L**

- licenses 13, 294
- loading the Enabler
  - Palm OS devices 446
  - Series 3000 device 439
  - Series 4000/5000 devices 456
  - Series 7000 device 442
  - WinCE/PocketPC devices 450
  - Windows 457
- local deployment batch file 470
- local deployment enhancement 469
- locating
  - access points 12
  - sites 136
- location management 81

## **M**

- MAC addresses 312
- managing
  - access points 153
  - alerts 385
  - IP addresses 207
  - locations 81
  - mobile devices 251
  - network settings 205
  - networks 8
  - security settings 309
  - software 252
- maximum simultaneous updates 292
- mobile devices
  - authenticating 295
  - deploying settings 297
  - deployment packages 93

- installing enablers 439
- managing 251
- settings 238
- synchronizing software 282
- security settings 372

- Mobile Manager
  - activating 22
  - components of 9
  - installation 11
  - installing 20
  - managing networks 8
  - requirements 14
- modifying
  - access control list entries 314
  - alert profiles 393
  - gateway IP addresses 212
  - profiles 165
  - sites 136
- modifying colors 40
- modifying subnet masks 212
- moving packages 261

## **N**

- network
  - events 168
  - layout 11
  - segmentation 12
  - services 49
- network settings
  - deploying 217
  - managing 205

## **O**

- operators 275
- orphaned packages 293

## **P**

- Package Wizard 469
- packages
  - configuring 265



- copying 263
- deleting 280
- disabling 278
- enabling 277
- installing 257
- moving 261
- Palm OS 446
- performing database maintenance 414
- profiles
  - configuring 162
  - creating alert 390
  - creating 162
  - deleting alert 393
  - deleting 165
  - modifying alert 393
  - modifying 165
  - refreshing 166
- proxies
  - creating proxy pool 388
  - deleting 390
- Proxim VLANs 342

**R**

- radio properties 350
- refreshing
  - profiles 166
  - Software Collections Manager 281
- releases 458
- removing
  - access control list entries 316
  - IP addresses 212
- renaming collections 255
- reporting 425, 436
  - gathering statistics 426
  - network data 425
- requirements
  - firmware 16
  - hardware 14
  - Mobile Manager 14
  - software 16

- rescheduling tasks 77
- running tasks 75

## **S**

- scheduling access point profiles 171
- security
  - advanced options 348
  - deploying all device settings 351
  - deploying settings 351
  - deploying settings to access points 361
  - deploying settings to mobile devices 372
- segmentation 12
- selecting location of network services 49
- selection criteria
  - building 269
  - defining 265
- selection variables 271
- Series 3000 device 439
- Series 4000/5000 devices 456
- Series 7000 device 442
- setting
  - COM ports 295
  - destination IP address for Network Alerts 399
  - simultaneous updates 292
- simultaneous downloads 32
- simultaneous updates 292
- site communication 51
- Site Import/Update Utility 119
- site management 151
- site tools 151
- site-level tools 10
- sites
  - accessing site tools 151
  - adding 110, 119
  - alert filter manager 408
  - configuring components 151
  - creating 82
  - deleting 146
  - deploying 121

- importing 130
- locating 136
- location management 9
- modifying 136
- tools 151
- software
  - configuring packages 265
  - copying packages 263
  - creating collections 253
  - installing packages 257
  - managing 252
  - moving packages 261
- Software Collections Manager 281
- starting the Enterprise Management Console 35
- statistical alerts
  - configuring 394
  - deleting 398
  - editing 398
- statistics 426
- stopping automatic WEP rotation 337
- subnet masks 212
- support
  - firmware 186
  - full 186
- supported
  - client software 16
  - devices 17
- synchronization events 283
- synchronizing mobile device software 282

## T

- Task Scheduler
  - adding tasks 71
  - deleting tasks 74
  - editing tasks 73
  - rescheduling tasks 77
  - running tasks immediately 75
  - using 70
  - viewing task progress 76

- tasks
  - adding 71
  - deleting completed 78
  - deleting 74
  - editing 73
  - rescheduling 77
  - running 75
  - viewing progress 76

## U

- updating firmware 186
- user accounts
  - changing passwords 58
  - creating 55
  - deleting 57
  - deploying 59
  - editing 57
  - viewing account status 58
- using the Task Scheduler 70

## V

- viewing
  - account status 58
  - task progress 76

## W

- WEP 330
  - automatic rotation 340
  - automatic rotation and Proxim VLANs 342
  - automatic rotation 332
  - Cisco IOS VLANs 340
  - configuring 331
  - configuring automatic rotation 333
  - stopping automatic rotation 337
  - types of deployments 331
- WinCE/PocketPC devices 450
- Windows 457
- Wire Equivalent Privacy 330