wavelink®

AVALANCHE™

Avalanche Manager

Version 3.6 User's Guide

W1-00004-01
Revised 10-12-05

Wavelink Corporation

6985 South Union Park Avenue
Suite 335
Midvale, Utah 84047
Telephone: (801) 316-9000
Fax: (801) 255-9699
WWW: http:\\www.wavelink.com

Email: info@wavelink.com

Table of Contents

Chapter 1: Introduction

Wavelink Avalanche is a client management system that automatically deploys software and configuration updates to mobile devices.

Mobile devices and their associated update systems are not inherently equipped with the capability to receive automatic updates. The goal of the Avalanche system is to address this fundamental issue by providing an effective, automated client management system that will greatly reduce your total cost of ownership.

About This Document

This section describes the assumptions behind this document and the typographical conventions used in this document.

Document Assumptions

The following assumptions are made about users of this document:

- The user is comfortable in a Windows application environment.
- The user is familiar with the wireless hardware in use, including the mobile device.
- The user knows the IP address of the mobile device, Avalanche Manager components (such as the Console and Agent), the router, as well as any other necessary network settings.

Document Conventions

This document uses the following typographical conventions:

Courier New

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

Examples:

Click `Next` to continue.

Press `CTRL+ALT+DELETE`.

Bold

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

Examples:

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

Click `Download` from the **HexFiles** menu.

Italics

Any time this document refers to another section within the manual, that section appears in the *Italic* text style.

Example:

See the *Troubleshooting* section for possible causes of this problem.

Keystroke conventions for the mobile device are as follows:

`Press A + B` Identifies a key sequence. Press and hold each key in turn.

`FUNC, CTRL, R` Identifies a key sequence. Press and release each key in turn.

`Hold A + B` Press and hold the indicated keys while performing or waiting for another function. Used in combination with another keystroke.

About the Wavelink Avalanche System

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

Avalanche Manager. This tool provides centralized agent-based client management within a network. The Avalanche Manager includes the Avalanche Manager Agent and the Avalanche Management Console. The Agent performs the actual management functions on the LAN or WAN, while the Management Console provides an administrative interface to one or more Agents.

Avalanche Enabler An agent that runs on each mobile device to allow management via the Avalanche Manager.

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

In the Avalanche system, a variety of network configurations can be used, such as a distributed Agent architecture or one in which the Avalanche Manager Agent and the Avalanche Management Console share the same host. The best configuration is dependent on the requirements of each particular site or enterprise and on the characteristics of their LAN or WAN. Several examples of configuring the Avalanche system are shown here.

In the configuration shown in Figure 1-1, multiple Agents are installed at individual sites across a WAN. In this configuration, you manage the mobile devices from a single location using a centralized installation of the Management Console.

The synchronization process that normally occurs between Agents and console involves file transfer, and for this reason the configuration is more effective if the speed and reliability of the WAN are very high.

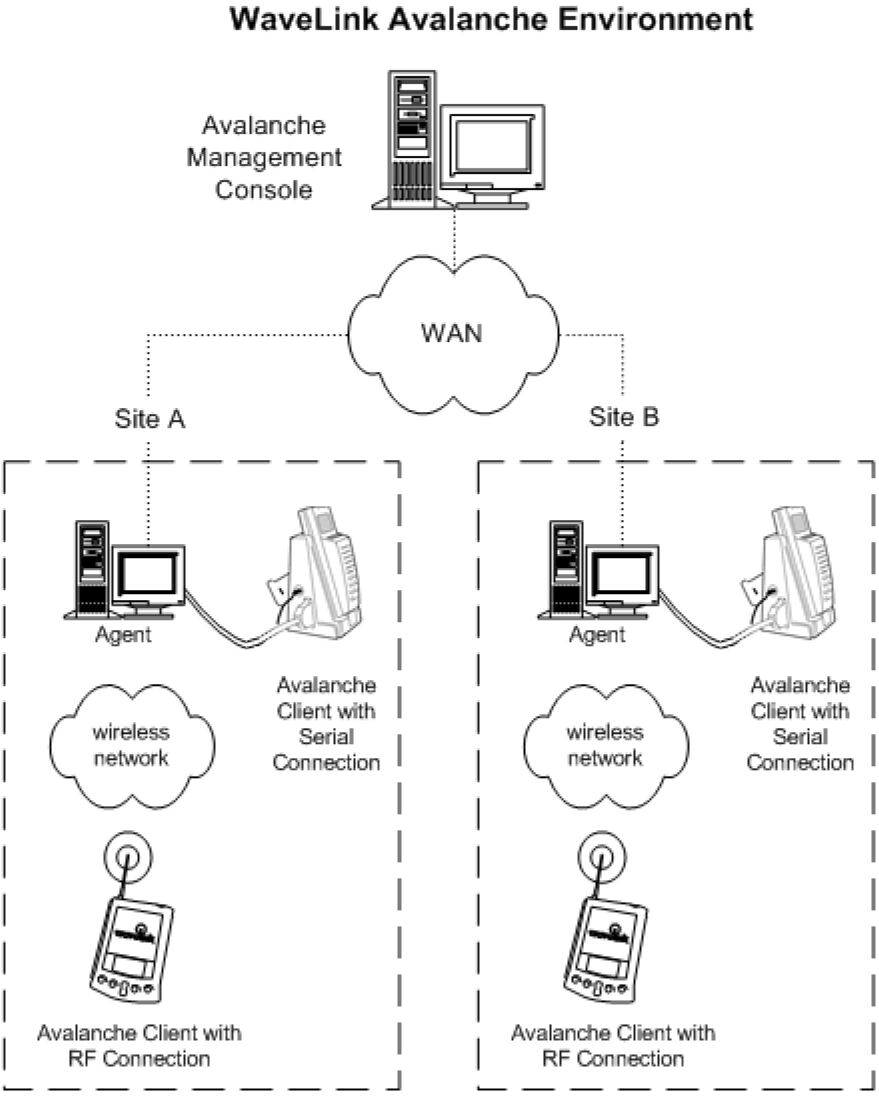

WaveLink Avalanche Environment
Avalanche Management Console
WAN
Site A
Site B
Agent
Avalanche Client with Serial Connection
wireless network
Avalanche Client with RF Connection
Agent
Avalanche Client with Serial Connection
wireless network
Avalanche Client with RF Connection

Figure 1-1. *Example of a Multiple Agent Network Configuration*

Figure 1-2 shows a configuration in which all clients connect to a single Agent. In this configuration, multiple installations of the Management Console provide distributed client management capabilities. You can use any Management Console or Avalanche Manager Agent for serial (or IrDA) downloads. This configuration is more effective if the speed and reliability of the WAN are very high.

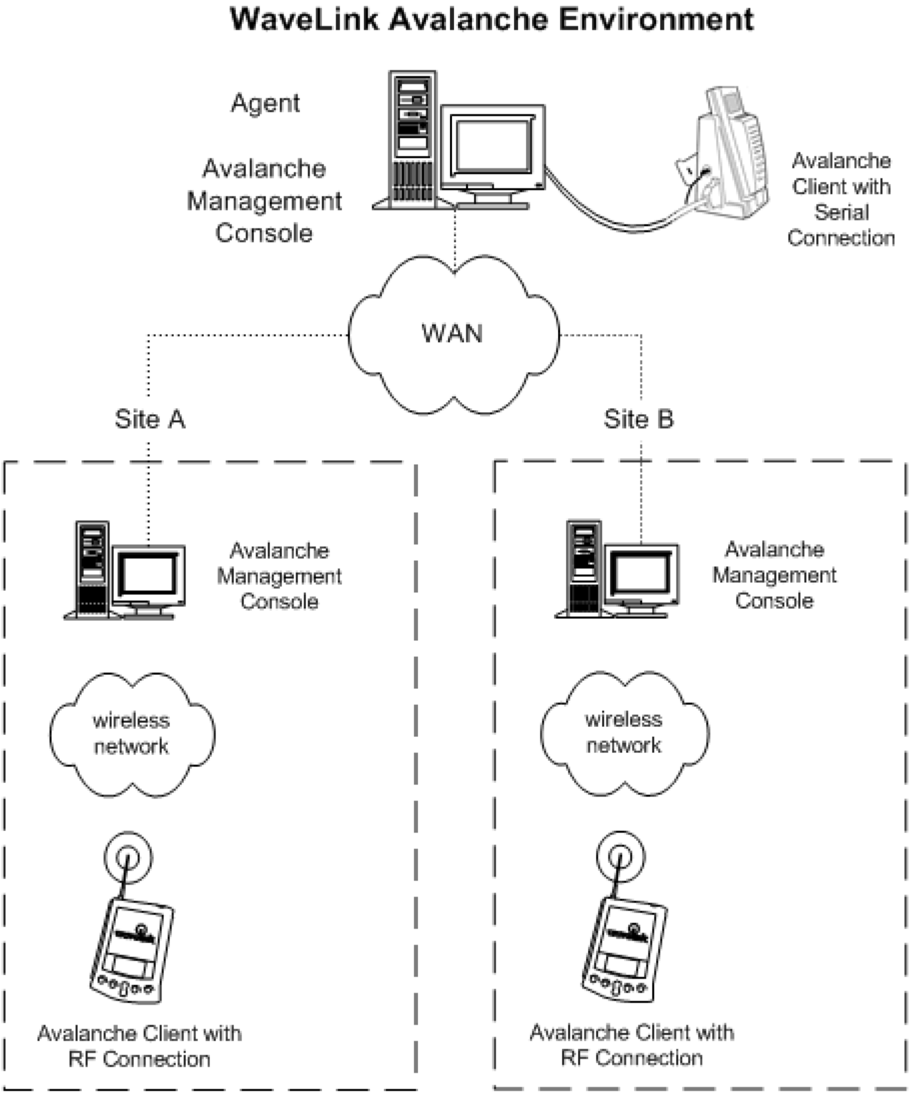

WaveLink Avalanche Environment
Agent
Avalanche Management Console
Avalanche Client with Serial Connection
WAN
Site A
Site B
Avalanche Management Console
Avalanche Management Console
wireless network
wireless network
Avalanche Client with RF Connection
Avalanche Client with RF Connection

Figure 1-2. *Example of a Multiple Console Network Configuration*

Figure 1-3 shows a configuration that relies on a single installation of the Avalanche Manager and the Agent. A configuration such as this, in which the

Agent and Management Console reside on the same host, is most effective when the speed and reliability of the WAN are low.

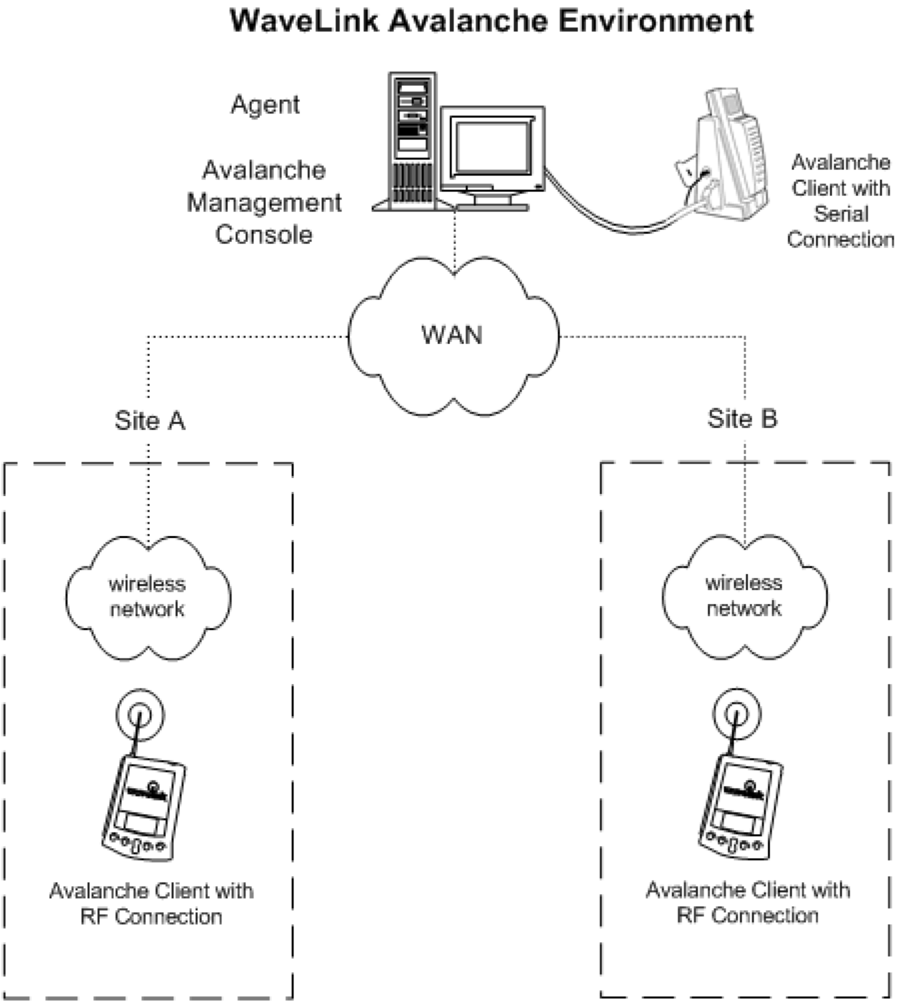

WaveLink Avalanche Environment
Agent
Avalanche Management Console
Avalanche Client with Serial Connection
WAN
Site A
Site B
wireless network
wireless network
Avalanche Client with RF Connection
Avalanche Client with RF Connection

Figure 1-3. *Example of a Single Agent and Console Network Configuration*

Features of Wavelink Avalanche

The Avalanche system provides the following benefits:

- More efficient site installations and software upgrades.
- Multiple applications on the same mobile device. Licensing is available to easily package virtually any application for use with Avalanche.
- Hands-free updates. No need to gather all mobile devices to perform a software update. You can even perform updates from off site.
- Automated RF firmware updates for devices. When RF firmware updates become available, the Enabler can receive them from the Agent, re-burn the firmware, and apply any associated RF driver updates, all without requiring end-user intervention.
- Centralized GUI tools for configuring client software. Configuration tools which are customized for each software package are included as plug-ins to the Avalanche Manager. For example, you can change a Telnet Client emulation parameter or a host profile in one location and automatically distribute the changes to each device.
- Central management of mobile device networking parameters (both IP and RF). In addition to providing support for BOOTP and DHCP, the Avalanche Manager provides the capability to automatically configure the Enabler with networking parameters.
- Unified management of diverse device architectures. Devices of completely different physical or operating system designs receive uniform treatment. This treatment eliminates the need to obtain a variety of tools and methods to manage each device type and assures that all software features possible are provided across platforms.
- Selective updates made easy. When any software or configuration is updated, the Avalanche Manager only transmits the altered components to the devices. This technique minimizes the bandwidth and time required, making high volume updates practical and simple.
- Multi-site management. The option to implement a distributed Agent architecture reduces bandwidth requirements for updates in the enterprise, allowing the mobile devices to connect directly to a local

Agent. In addition, multiple Agents can be managed from a single management console.

- Enterprise management. Backup and restore functions allow the rapid configuration of multi-site systems by re-deploying Agent configurations from one site to another in the enterprise.
- Automatic WEP. In addition to supporting static WEP keys, the Avalanche Manager supports the automatic generation and rotation of WEP keys at specified intervals to prevent hackers from breaking the WEP encryption code (patent pending). In conjunction with Wavelink Mobile Manager, which rotates WEP keys for access points, this feature of Avalanche Manager eliminates the known security risks of static WEP encryption.
- Log filtering. Avalanche Manager includes a log viewer that allows viewing of historical log data based on the MAC address of a specific mobile device.

About the Avalanche Manager

The Avalanche Manager consists of two primary components, the Avalanche Manager Agent and the Avalanche Management Console.

Avalanche Manager Agent

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

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

To determine appropriate software for each specific mobile device, the Avalanche Manager Agent relies on a hierarchical structure based on two logical components: software packages and software collections.

Software packages (See Figure 1-4) represent a collection of application files associated with a single product such as the Wavelink TN Clients or third party Avalanche-enabled software packages. All files in the package download automatically to the mobile device.

Software collections (See Figure 1-4) contain one or more software packages. You can configure each software collection so that the packages it contains apply only to certain mobile devices.

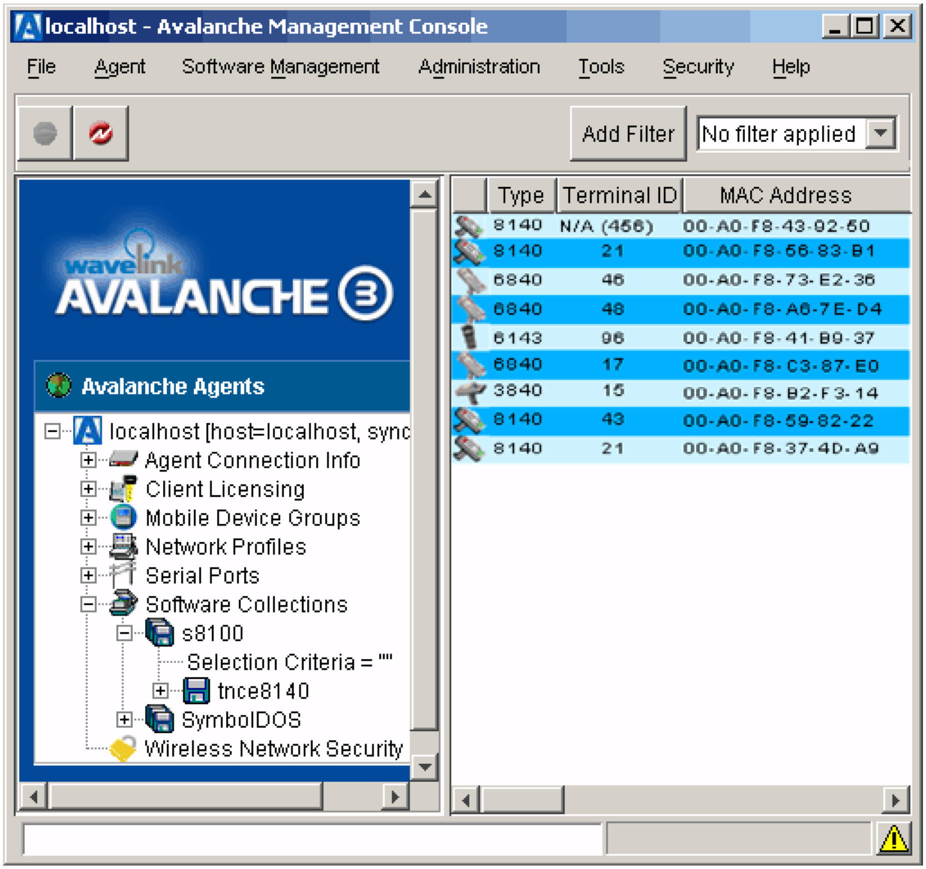
Avalanche Management Console

The Avalanche Management Console is the other primary component of the Avalanche Manager. The console provides the administrative interface that allows you to configure Agents. The Avalanche Management Console can connect to any Agent using any routable IP address, allowing the remote administration of different Agents across a LAN or WAN.

When the Management Console connects to a given Agent, it synchronizes with the Agent, downloading any updated information from the Agent to the local console.

NOTE Although it is not recommended, you can disable synchronization if desired.

The Management Console provides a visual representation of all software collections and software packages associated with that Agent. In addition, the console shows other configurable features associated with either the Agent, such as network interface information, or with the console itself. Figure 1-4 shows the Avalanche Management Console.



Type	Terminal ID	MAC Address
8140	N/A (456)	00-A0-F8-43-92-60
8140	21	00-A0-F8-56-83-B1
6840	46	00-A0-F8-73-E2-36
6840	48	00-A0-F8-A6-7E-D4
6143	96	00-A0-F8-41-B9-37
6840	17	00-A0-F8-C3-87-E0
3840	15	00-A0-F8-B2-F3-14
8140	43	00-A0-F8-59-82-22
8140	21	00-A0-F8-37-4D-A9

Figure 1-4. *Avalanche Management Console*

Software Packages

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

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

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

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

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

- **Plug-in configuration utilities**. These are configuration utilities which run on the Management Console. See *Running Plug-In Utilities with Avalanche* on page 121 for more information about these utilities.
- **Target Selection Criteria**. This feature limits distribution of the package to specific mobile devices. The selection criteria can encompass many device characteristics, including mobile device models, physical characteristics, IP and/or MAC addresses, etc. You can use the Management Console operators to apply your own restrictions in addition to these, but you will not be able to circumvent any restrictions placed in the package definition itself. For more information, see *Selection Criteria* on page 122.
- **Wireless download**. Packages download over the wireless network.

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

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

Software Collections

A software collection is a logical grouping of software packages that are maintained and managed by the Avalanche Manager. During package installation, the Avalanche Manager allows you to create a new software collection for the package or add it to an existing collection. You can create new collections or copy software from collection to collection as needed.

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

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

About the Avalanche Enabler

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

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

Licensing Third-Party Applications

Third party applications can be easily packaged to be managed using Avalanche. Contact Wavelink or see the Avalanche Web page http://www.wavelink.com/wavelink/avalanche for more details.

Chapter 2: Installation

This section contains the system requirements for Avalanche, information about required installation files to help you get started, and the complete installation process for the three main components in the Avalanche system: the Avalanche Manager, the Avalanche Enabler, and the Avalanche software packages.

The complete installation process is described in the following sections:

- Installing the Avalanche Manager
- Installing the Avalanche Enabler
- Installing an Avalanche Software Package

NOTE If you have already installed the Avalanche Manager, proceed to *Installing the Avalanche Enabler* on page 31.

Requirements

To successfully install and operate Avalanche, your environment must include the following elements:

- A network configured to use TCP/IP protocol
- Wireless access points (Ethernet or Token-Ring)
- Supported client software
- Supported mobile devices

In addition, the Avalanche Management Console and the Avalanche Manager Agent have specific hardware and software requirements.

Management Console Requirements

The Avalanche Management Console requires the following hardware and software components to operate effectively:

- JRE version required: 1.3.1_03

The Java™ 2 Runtime Environment is intended for use with Intel hardware.

- Windows 2000, Windows XP, or Windows 2003 Server
- A Pentium III 550 MHz or faster processor (Pentium IV 1.4 GHz or higher recommended)
- 256 MB of physical RAM (512 MB or more recommended)
- 200 MB or more of available hard disk space

NOTE The amount of hard disk space required will increase if the console synchronizes with more than one agent.

Agent Requirements

Most of the requirements for the Avalanche Manager Agent are based on the operating system to be used.

- RS232 serial port, RS232 digiboard port, or IrDA port.

  The ports are required for any Agent that will be performing serial-based (or IrDA-based) installations to mobile devices. Serial- based installations are required for the initial installation of the Avalanche Enabler on a mobile device.

NOTE The Agent does not require the JRE.

- Pentium III 550 MHz or faster processor (Pentium IV 1.4 GHz or higher recommended)
- 256 MB of physical RAM (512 MB or more recommended)
- 200 MB or more of available hard disk space
- Windows 2000, Windows XP, or Windows 2003 Server
- Microsoft ActiveSync 3.7.1 or later version (required for Local RAPI Gateways)

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.

For information on managing third-party applications with Avalanche, please see *Licensing Third-Party Applications* on page 13.

Supported Devices

Wavelink currently supports mobile devices from the following manufacturers:

- Denso
- Fujitsu
- HP
- HHP
- Intermec
- LXE
- PSC
- Symbol

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 Avalanche web site http://www.Wavelink.com/wavelink/avalanche for the most up to date list of supported devices.

Getting Started

Before you can install the Avalanche packages, you must acquire the correct installation files:

- If you have not installed the Avalanche Manager, obtain the `WLAvaMgr_vxxx.exe` executable (where xxx denotes the version number) from the Wavelink Web site, http://www.wavelink.com. The Avalanche Manager includes both the Avalanche Manager Agent and the Avalanche Management Console.

- Obtain the correct Avalanche Enabler file for your device. See *Installing the Avalanche Enabler* on page 31 for a list of the Enabler files.

- Obtain the desired client software package(s). This can be a Wavelink TN Client, a Wavelink Studio Client, or a third party Avalanche-enabled software package. All files in the package download automatically to the mobile device. For information on file names for Wavelink TN Clients and Wavelink Studio Clients, see *Software Package Naming Conventions* on page 41.

  You can obtain the installation key for the software by calling Wavelink at (425) 823-0111.

NOTE In some cases, you will need to obtain an RF firmware or driver update package. If you cannot resolve communication problems relating to your mobile device, contact your hardware representative to determine whether a firmware or driver update is required. Avalanche-enabled RF firmware and driver updates packages are available from Wavelink.

Contact Wavelink at sales@wavelink.com or (888) 697-WAVE for information about how to obtain licensed versions of the Avalanche Manager and client files.

Determining Agent and Console Placement

In the Avalanche system, a variety of network configurations can be used, such as a distributed Agent architecture or one in which the Avalanche Manager Agent and the Avalanche Management Console share the same host. The best configuration is dependent on the requirements of each particular site or enterprise and on the characteristics of its LAN or WAN.

In the configuration shown in Figure 2-1, multiple Agents are installed at individual sites across a WAN. In this configuration, you manage the mobile devices from a single location using a centralized installation of the Management Console.

The synchronization process that normally occurs between Agents and console involves file transfer, and for this reason this configuration is more effective if the speed and reliability of the WAN are very high.

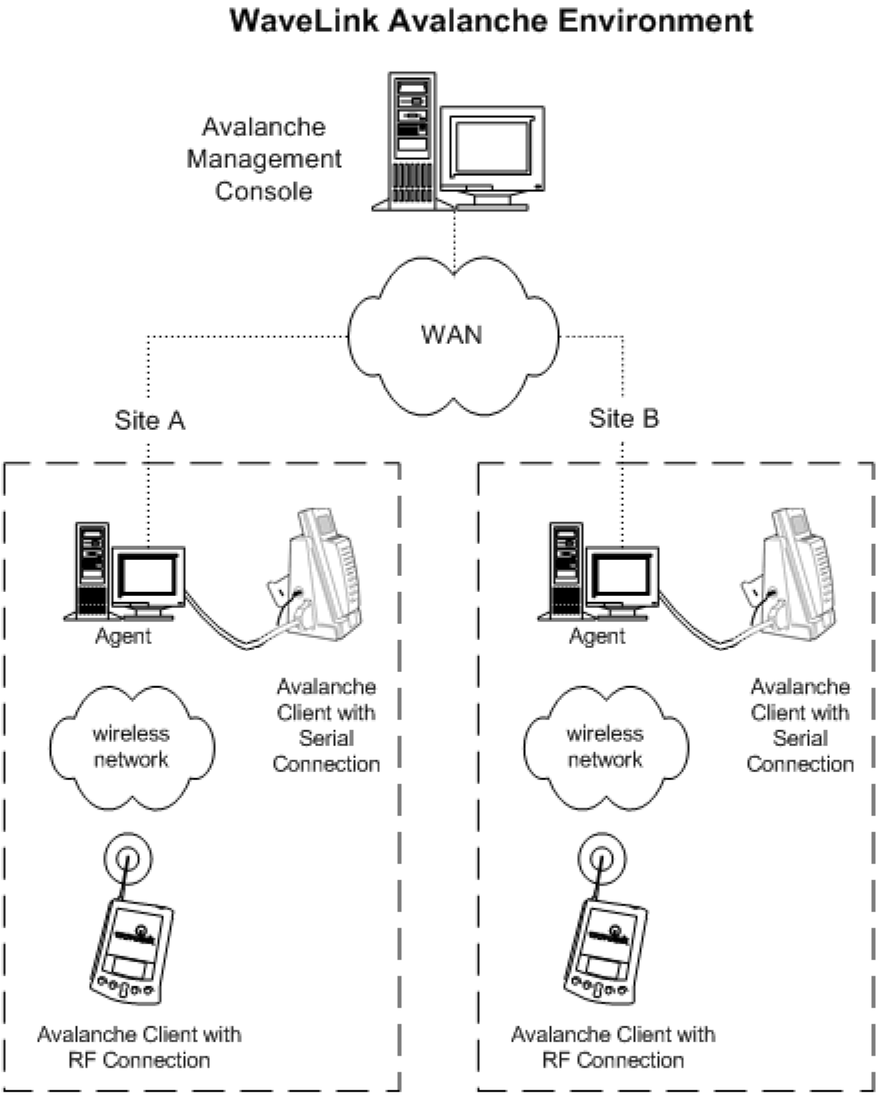

WaveLink Avalanche Environment
Avalanche Management Console
WAN
Site A
Site B
Agent
Avalanche Client with Serial Connection
wireless network
Avalanche Client with RF Connection
Agent
Avalanche Client with Serial Connection
wireless network
Avalanche Client with RF Connection

Figure 2-1. *Example of a Multiple Agent Network Configuration*

The preceding configuration (Figure 2-1) also supports serial and IrDA downloads at each site, if needed.

Figure 2-2 shows a configuration in which all clients connect to a single Agent. In this configuration, multiple installations of the Management

Console provide distributed client management capabilities. As with the centralized management configuration shown previously, this de-centralized management configuration is more effective if the speed and reliability of the WAN are very high.

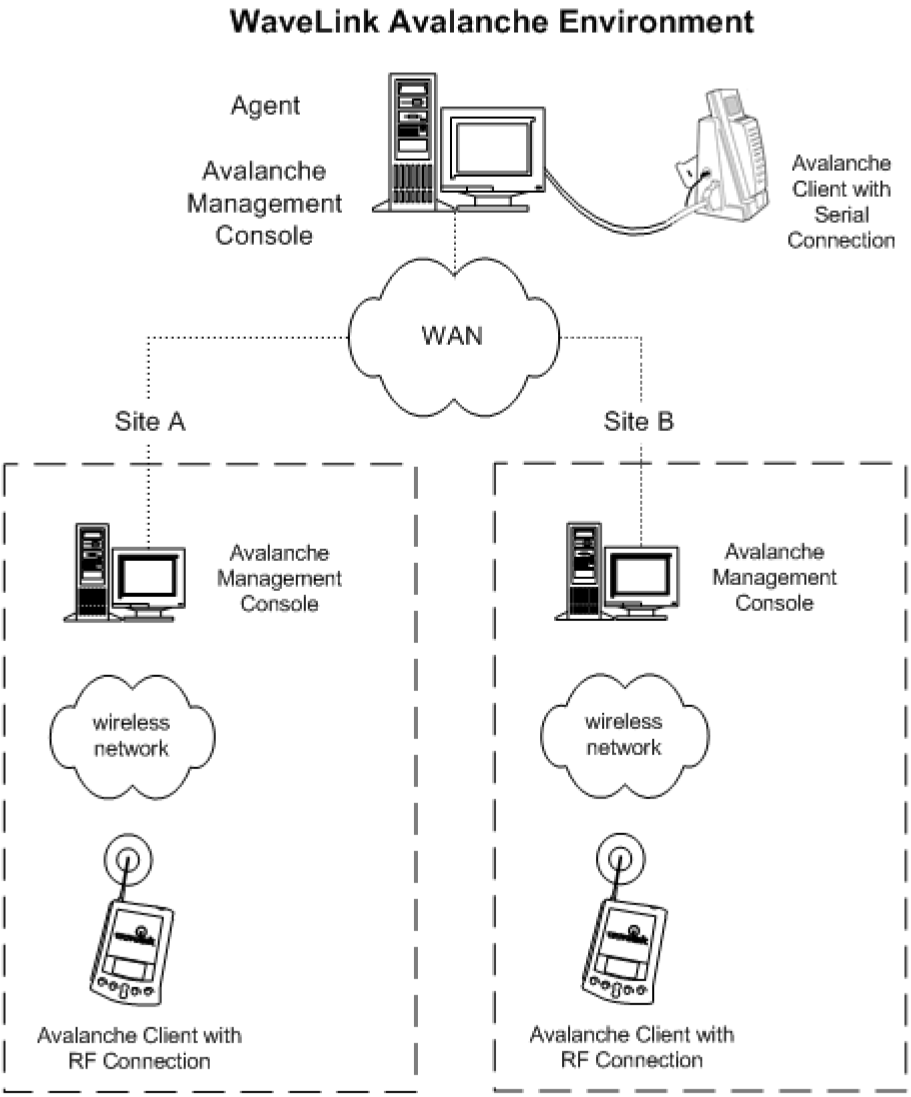

WaveLink Avalanche Environment
Agent
Avalanche Management Console
Avalanche Client with Serial Connection
WAN
Site A
Site B
Avalanche Management Console
wireless network
Avalanche Client with RF Connection
Avalanche Management Console
wireless network
Avalanche Client with RF Connection

Figure 2-2. *Example of a Multiple Console Network Configuration*

Figure 2-3 shows a configuration that relies on a single installation of the Avalanche Manager and the Agent. A configuration such as this, in which the Agent and Management Console reside on the same host, is most effective when the speed and reliability of the WAN are low.

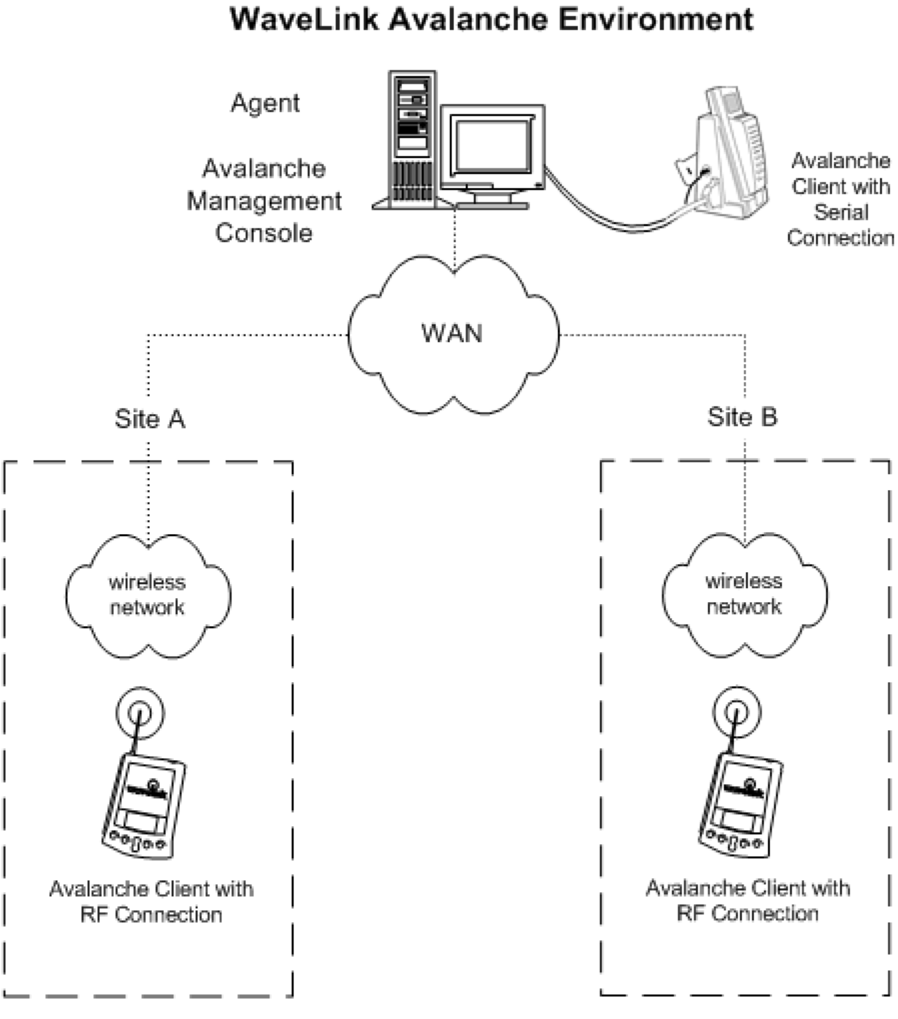

WaveLink Avalanche Environment
Agent
Avalanche Management Console
Avalanche Client with Serial Connection
WAN
Site A
Site B
wireless network
wireless network
Avalanche Client with RF Connection
Avalanche Client with RF Connection

Figure 2-3. *Example of a Single Agent and Console Network Configuration*

At the time you install the Avalanche Manager, you are provided with the option of installing the Management Console, the Agent, or both.

Installing the Avalanche Manager

This section describes in detail how to install the Avalanche Manager software.

NOTE The Avalanche Manager must be installed on the system that will be used to install the client software on the mobile device.

To install the Avalanche Manager:

1 Run the setup program.

Locate and run the Avalanche Manager installation file. You might have obtained this file by downloading it or from a CD. The name of the file is `WLAvaMgr_vxxx.exe`, where `xxx` represents the version number.

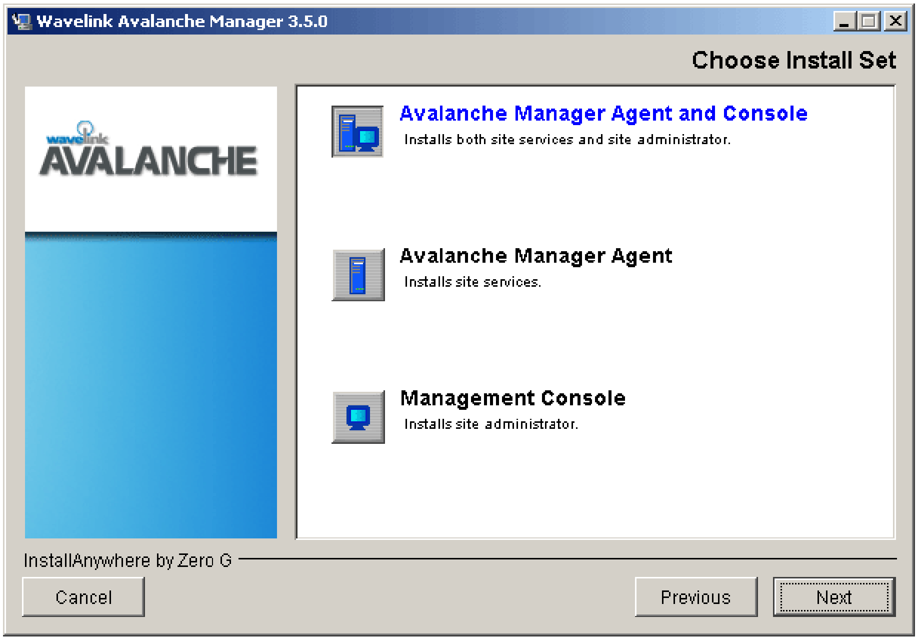
2 Follow the setup program's instructions.

In the *Introduction* dialog box, click Next.

In the *License Agreement* dialog box, read the license agreement, select I accept the terms of the License Agreement, and click Next.

In the *Choose Install Folder* dialog box, specify the target directory for installation (click `Choose` to change the default directory or click `Next` to accept the default directory).

After you choose a target directory for installation, the *Choose Install Set* dialog box appears (Figure 2-4).



Wavelink Avalanche Manager 3.5.0

Choose Install Set

Avalanche Manager Agent and Console

Installs both site services and site administrator.

Avalanche Manager Agent

Installs site services.

Management Console

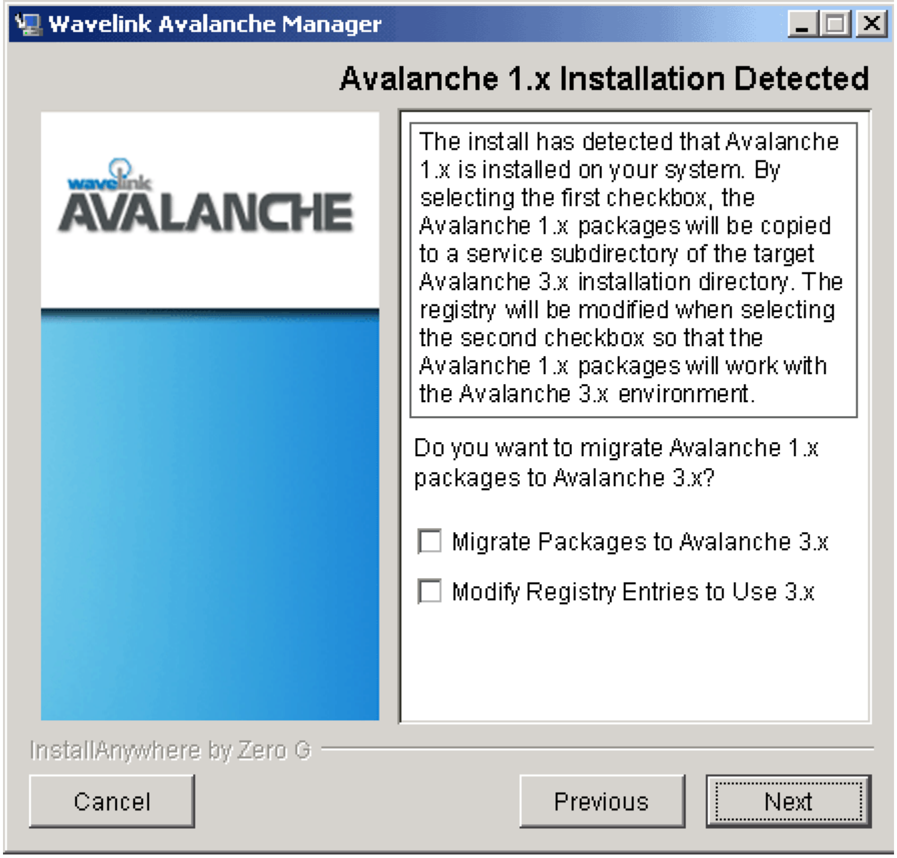
Installs site administrator.

Figure 2-4. *The Choose Install Set Dialog Box*

3 Select the desired installation option and click `Next`.

You can specify whether you want to install the Avalanche Management Console, the Avalanche Manager Agent, or both. For information about possible network configurations, see *About the Wavelink Avalanche System* on page 3 and *About the Avalanche Manager* on page 8.

The following dialog box appears.



Avalanche 1.x Installation Detected

The install has detected that Avalanche 1.x is installed on your system. By selecting the first checkbox, the Avalanche 1.x packages will be copied to a service subdirectory of the target Avalanche 3.x installation directory. The registry will be modified when selecting the second checkbox so that the Avalanche 1.x packages will work with the Avalanche 3.x environment.

Do you want to migrate Avalanche 1.x packages to Avalanche 3.x?

□ Migrate Packages to Avalanche 3.x

□ Modify Registry Entries to Use 3.x

Figure 2-5. *The Avalanche 1.x Installation Detected Dialog Box*

4 In the *Avalanche 1.x Installation Detected* dialog box, select whether to migrate packages, registry settings, or both from version 1.x of the Avalanche Manager, and click `Next`.

NOTE It is recommended that you migrate packages and registry entries.

5 In the *Avalanche 2.x Installation Detected* dialog box, select whether to migrate packages, registry entries, or both from version 2.x of the Avalanche Manager. The ability to select packages, registry settings, or both is unavailable if you have already migrated them.

NOTE It is recommended that you migrate registry settings. In the rare instance that you maintain installations of both Avalanche Manager 1.x and 2.x, and you want to migrate packages from both versions into Avalanche Manager 3.x, you must perform a second installation to accomplish this. For registry entries, only one installation is required.

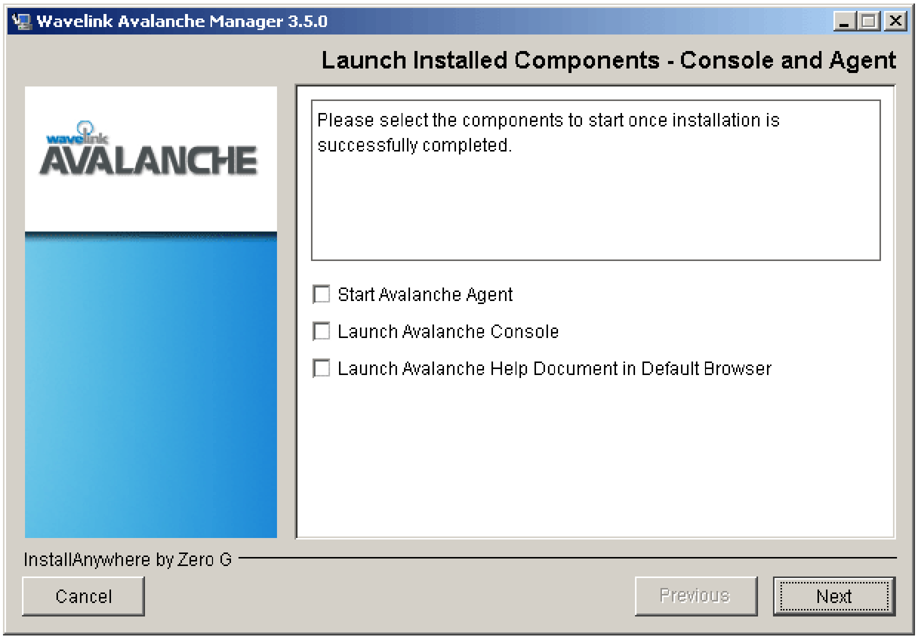
The *Pre-Installation Summary* dialog box appears.

6 In the *Pre-Installation Summary* dialog box, verify that the installation options are correct and select the desired option.

If you want to change previously-selected options, click `Previous`.

Click `Next` to begin the installation. The setup program installs the necessary files.

When the installation of files is complete, the *Launch Installed Components* dialog box appears.



Launch Installed Components - Console and Agent

Please select the components to start once installation is successfully completed.

□ Start Avalanche Agent

□ Launch Avalanche Console

□ Launch Avalanche Help Document in Default Browser

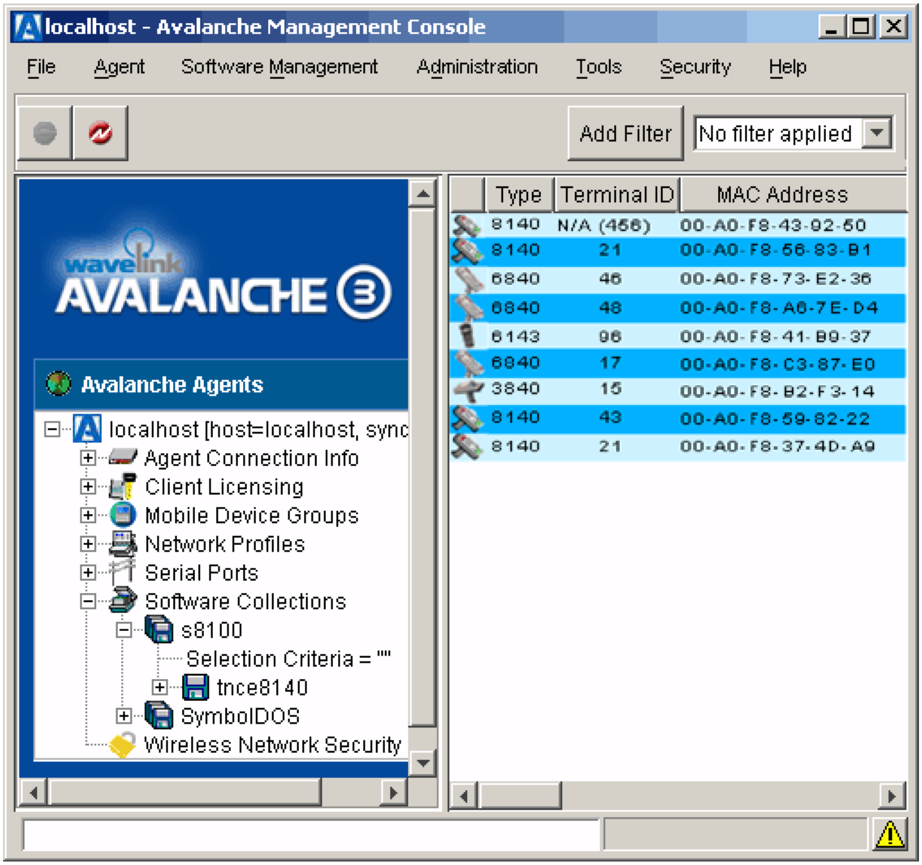
Figure 2-6. *The Launch Installed Components Dialog Box*

7 Enable the checkbox for the component you want to launch and click `Next`.

You can choose to launch any or all of the following components, depending on which components were installed: the Avalanche Manager Agent, the Management Console, and the online Help.

If you choose to launch the Agent, the Agent service automatically starts. If you do not start the Agent, you will need to start the Agent before you can use it to download any software using Wavelink Avalanche. See *Starting an Agent on Windows 2000/XP* on page 178 for information about starting the Agent service.

8 If you choose to launch the Avalanche Management console, the main screen of the console appears.



No filter applied

Type	Terminal ID	MAC Address
8140	N/A (456)	00-A0-F8-43-92-60
8140	21	00-A0-F8-56-83-B1
6840	46	00-A0-F8-73-E2-36
6840	48	00-A0-F8-A6-7E-D4
6143	96	00-A0-F8-41-B9-37
6840	17	00-A0-F8-C3-87-E0
3840	15	00-A0-F8-B2-F3-14
8140	43	00-A0-F8-59-82-22
8140	21	00-A0-F8-37-4D-A9

Figure 2-7. *Avalanche Management Console*

Authorizing the Avalanche Manager

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

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

You can activate your Avalanche Manager license using one of five methods: standard, manual, support, temporary, and demonstration. These options are accessed through the *Wavelink Activation* dialog box. This process is repeatable, allowing you to add new licenses to Avalanche Manager at any time.

The following steps describe how to activate your Avalanche Manager license using the standard method, which is the most common method used.

NOTE An enterprise licensing system is also available for high-volume customers. With the enterprise licensing system, there is no need to purchase additional client licenses when adding new devices. This licensing system also allows the inclusion of a customer logo that automatically displays during application startup. Contact your Wavelink customer service representative for more information.

To activate an Avalanche Manager License:

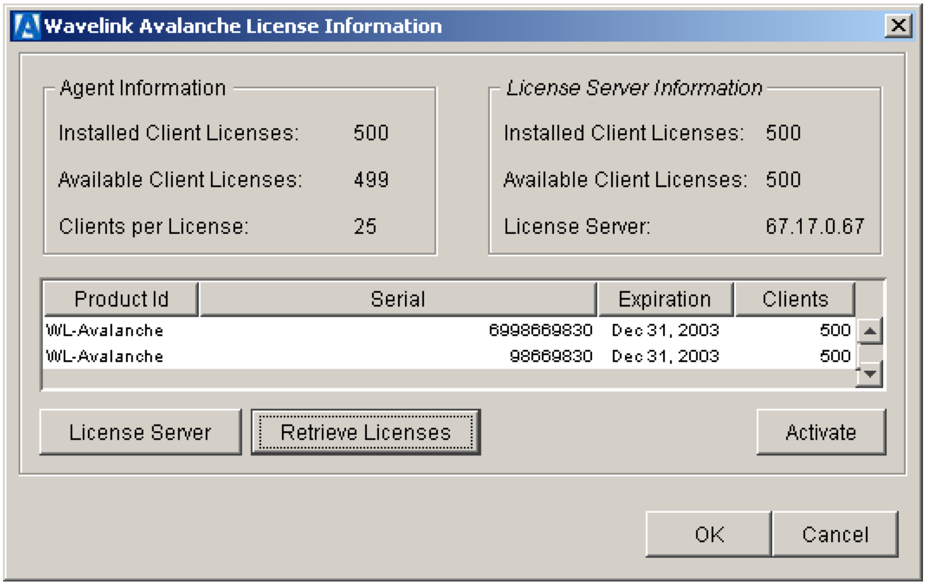
1. Locate your product license number.

   This number is sent to you in an e-mail when you first purchase Avalanche Manager.

2. From the Avalanche Management Console, connect to an Avalanche Manager Agent.

3. Select `Software Licensing` from the **Administration** menu.

   The *Wavelink Avalanche License Information* dialog box appears.



Agent Information

Installed Client Licenses: 500
Available Client Licenses: 499
Clients per License: 25

License Server Information

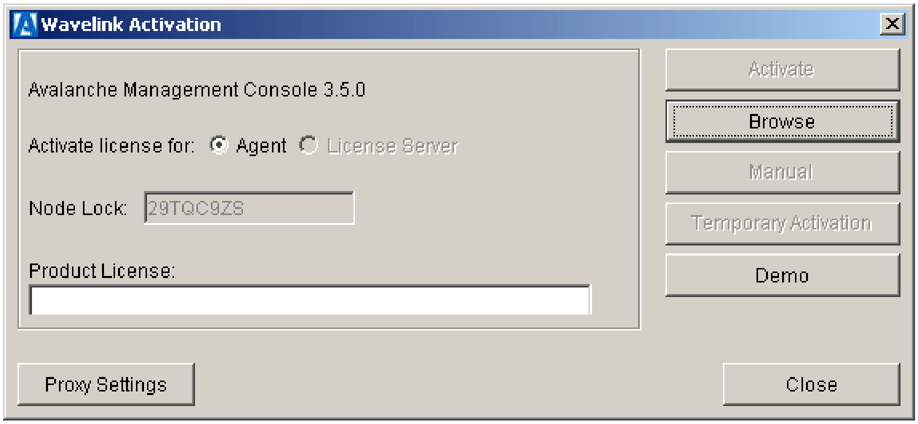
Installed Client Licenses: 500
Available Client Licenses: 500
License Server: 67.17.0.67

Product Id	Serial	Expiration	Clients
WL-Avalanche	6998669830	Dec 31, 2003	500
WL-Avalanche	98669830	Dec 31, 2003	500

Figure 2-8. *The Wavelink Avalanche License Information Dialog Box*

4 Click `Activate`.

The *Wavelink Activation* dialog box appears.



Avalanche Management Console 3.5.0

Activate license for: ● Agent ○ License Server

Node Lock: 29TQC9ZS

Product License:

Figure 2-9. *The Wavelink Activation Dialog Box*

5 Type your product license in the **Product License** text box

6 Click `Activate`.

The Avalanche Manager will connect to a secure Wavelink Web site to validate your product license and activate your installation. If you experience any difficulties with this process, you can use one of several alternate licensing processes. These process are described in *Appendix E: Avalanche Manager Licensing Process* on page 269.

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

Installing the Avalanche Enabler

The Avalanche Enabler is the 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 2-1: *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 D: Installing the Avalanche Enabler* on page 247:

- *Loading the Enabler on a Series 3000 Device* on page 247
- *Loading the Enabler on a Series 7000 Device* on page 251
- *Loading the Enabler on Palm OS Devices* on page 254
- *Loading the Enabler on WinCE/PocketPC Devices* on page 258
- *Loading the Enabler on Series 4000/5000 Devices* on page 264
- *Loading the Enabler on Windows* on page 265

After completing the installation of the Enabler, see *Installing an Avalanche Software Package* on page 41 to continue the installation process.

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 the Avalanche Enabler* on page 31 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 33 for more information.

The topics included in this section include:

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

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 D: Installing the Avalanche Enabler* on page 247 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 D: Installing the Avalanche Enabler* on page 247 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 *Chapter 7: Avalanche Manager Agent* on page 165 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`.

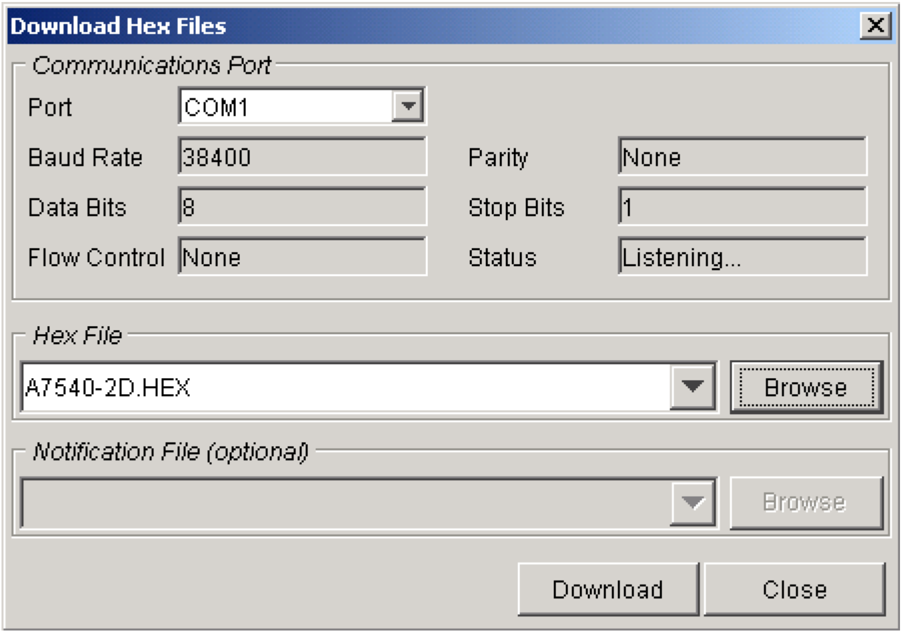
If the Avalanche Manager Agent did not automatically detect the COM ports during the installation, see *Chapter 8: Serial Ports* on page 185 before attempting a serial download.

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.



Download Hex Files

Communications Port

Port: COM1

Baud Rate: 38400

Parity: None

Data Bits: 8

Stop Bits: 1

Flow Control: None

Status: Listening...

Hex File

A7540-2D.HEX

Notification File (optional)

Figure 2-10. *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.

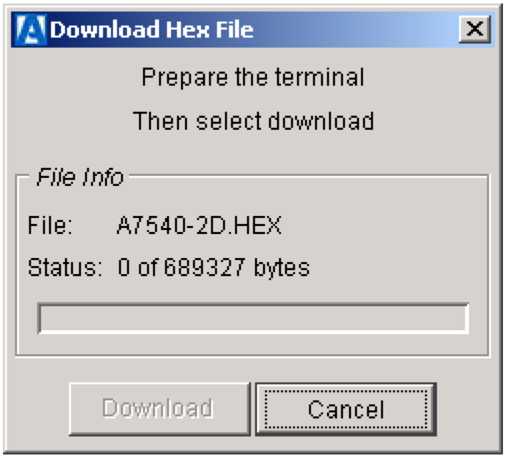
NOTE For Series 7000 DOS devices, you must download the partition file that matches the device's flash type before downloading the Enabler. See *Loading the Enabler on a Series 7000 Device* on page 251 to determine the name of the required partition file. Follow steps 5 and 6 to download the partition 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.



Download Hex File

Prepare the terminal

Then select download

File Info

File: A7540-2D.HEX

Status: 0 of 689327 bytes

Figure 2-11. *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 D: Installing the Avalanche Enabler* on page 247 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 2-2 below.

	Cold 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 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 2-2: *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 34 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 33 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 *Using Network Profiles* on page 89 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 *Chapter 7: Avalanche Manager Agent* on page 165 for more information.

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

Installing an Avalanche Software Package

An Avalanche software package is the collection of files that reside on the mobile device for a particular application, such as a Wavelink TN Client. This includes any support utilities used to configure or manage the application from the Avalanche Management Console.

You must first install software packages and configurations targeted for mobile devices on the Avalanche Manager. The Avalanche Manager Agent distributes software packages and configurations to the mobile devices. See *Using Software Packages* on page 113 for information regarding how to manage software packages once they have been installed.

NOTE If you use a Telnet Client software package, configure the host profiles and emulation parameters after installation. Refer to your client software documentation for more details.

Software Package Naming Conventions

This section includes information on naming conventions Wavelink TN Clients and Wavelink Studio Clients.

Wavelink TN Client Naming Conventions

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*][*Emulation*][*DbByte*][*Version*].[*Extension*]

Where

- *Component* is always `WLTNClient`
- *Platform* represents a device type and platform, such as S75
- *OS* represents the operating system, such as DOS
- *Emulation* represents the emulation type, such as 4in1
- *DbByte* indicates whether the package uses double byte fonts (DB)
- *Version* represents the package version number

- *Extension* represents the file extension for the package, such as `.ava` (or `.exe` for older packages)

An example of an Enabler file that uses this convention is `WLTNClient_S17_PL_4in1_DB_4_16_10.exe`, which represents the 1740 4in1 Emulation Client with double byte fonts.

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

S3K - Symbol 1K, 3K, 6K	DO -DOS	4in1 - 5250/3270/VT/HP	.ava - for packages
S40 - Symbol 4000	CE -CE 2.11	5232 - 5250/3270	.exe - older package
S72 - Symbol 7200	PPC - PPC 3.0	vthp - VT/HP	
S75 - Symbol 7500	PL - Palm		
S17 - Symbol 1700	W -Windows		
S27 - Symbol 2700			
S79 - Symbol 7900			
S81 - Symbol 8100			
S28 - Symbol 2800			
I50 - Intermec 5020			
WPC - Windows PC			

Table 2-3: *Software Package File Names*

NOTE Older packages might use a `.exe` extension.

NOTE Visit the Avalanche Web site at http://www.wavelink.com/wavelink/avalanche for help identifying the Wavelink software packages that might be required.

Wavelink Studio Client Naming Conventions

Installation files for Wavelink Studio Clients use the following naming convention:

```
WLC_[Device]_[OS]_[Radio]_[Version]_[Language]_[Font].[Extension]
```

Where

- *Device* is the hardware type
- *OS* is the operating system
- *Radio* is the radio type
- *Version* is the client version
- *Language* is the language type
- *Font* is the font size displayed
- *Extension* is the file extension (`.ava`)

For all Avalanche-enabled Wavelink Studio Clients, the Radio parameter is always `ava`.

For example, the Avalanche-enabled version of the Wavelink Studio Client for Symbol 3000 Series is `wlc_s3k_ds_ava_xxx.ava`.

Installing Software Packages to the Management Console

Before you can download a software package to a mobile device, you must install it to the Avalanche Management Console. The Install Software Package wizard provides this functionality.

This section provides instructions for installing both AVA and EXE software packages.

To install an AVA software package:

1 In the Management Console, verify that you are connected to the Avalanche Manager Agent.

You can connect to an Agent, by selecting `Connect to Agent` from the **Agent** menu. See *Chapter 7: Avalanche Manager Agent* on page 165 for more information.

2 Select `Install Software Package` from the **Software Management** menu.

The Install Software Package wizard launches. The first step in this wizard is to select the Avalanche package to install.

3 Type the path to the software package in the text box provided, or click [...] to navigate to the package.

This package must have an `.ava` extension. See *Software Package Naming Conventions* on page 41 for more information about package names.

4 Click `Next`.

The next step in the wizard is to select the software collection to which the package will belong.

5 Select a software collection and click `Next`.

Software collections are organized by the Avalanche Manager Agents to which you are connected. To locate a software package, expand the Avalanche Manager Agent node by clicking the plus icon next to it.

The Install Software Package wizard will install the package to the specified software collection.

6 Click `Finish`.

After the installation is complete, you can configure each package by right-clicking on the package in the Tree View of the Management Console and selecting the desired configuration utility, if any are included.

NOTE Software packages are disabled when you first install them to prevent packages from downloading before they are properly configured.

To install an EXE software package:

NOTE The mobile device must have been configured manually or via a network profile to continue with this section.

1 Launch Avalanche Management Console and connect to the Agent.

2 In the Tree View, right-click the Software Collections branch and select `New Software Collection`.

3 Type a name for the software collection, then click `OK`.

4 Use Windows Explorer to browse to the location of the emulation client EXE.

5 Double-click the EXE file.

6 Accept the license agreement and continue through the installation.

NOTE 3000-series clients prompt for an installation key. Type the installation key that was included with your order confirmation. If you are using a demonstration client, use the password `roidemo`.

7 Access the Avalanche Management Console and press `F5` to access the Install Software Package Wizard.

8 Click `Next` and accept the license agreement.

9 In the tree in the *Select Software Collection* dialog box, select the software collection, then click `Next`.

10 Once the installation is complete, click `Finish`.

11 In the Tree View, expand the software collection.

12 Right-click the software package and select `Enable` package.

13 Connect the mobile device to the Avalanche Manager using the wireless medium.

Warm boot a 3000-series client to connect to the Avalanche Manager. Use the `Connect C` option within the CE Avalanche Enabler to connect to the Avalanche Manager.

Downloading Software Packages to the Mobile Device

You can download software packages using either a wireless, serial, or IrDA.

NOTE Wireless downloads require a licensed version of the Avalanche Manager.

NOTE IrDA connections are treated like serial connections.

To download packages using a serial connection:

1 In the Management Console, verify that you are connected 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 *Chapter 7: Avalanche Manager Agent* on page 165 for more information.

2 Activate the software package in the Management Console by right-clicking on the package in the Tree View and clicking `Enable Package`.

3 To prepare for a serial download, verify that the mobile device is in the cradle or attached to its serial cable.

4 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, see *Chapter 8: Serial Ports* on page 185 before attempting a serial download.

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.

5 Activate the Enabler.

- On a DOS-based device, warm boot the device to activate the Enabler.
- On a Palm or CE device, double-click the **Avalanche** icon.

The software package automatically downloads to the mobile device.

See *Deploying Updates* on page 161 for more information about downloading software updates to mobile devices.

Before you can connect to your wireless network, you must verify that the network parameters on the mobile device are correct. See *Configuring the Enabler* on page 39 for more information.

To download packages using a wireless connection:

1 In the Management Console, verify that you are connected 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 *Chapter 7: Avalanche Manager Agent* on page 165 for more information.

2 Activate the software package in the Avalanche Manager by right-clicking on the package in the Tree View and selecting `Enable Package`.

3 Verify that the network parameters on the mobile device are correct. See *Configuring the Enabler* on page 39 for more information.

4 Take the mobile device out of the cradle or remove the serial connection to prepare for a wireless download.

5 Activate the Enabler.

- On a DOS-based device, warm boot the device to activate the Enabler.

- On a Palm or CE device, double-click the **Avalanche** icon.

The software package automatically downloads to the mobile device.

See *Deploying Updates* on page 161 for more information about downloading software updates to mobile devices.

Chapter 3: Avalanche Agent Configuration Settings

The first time you connect to an Avalanche Manager Agent, Avalanche Manager automatically launches the *Avalanche Agent Configuration Settings* dialog box. This dialog box allows you to configure the primary Avalanche Manager settings.

You can also access the Avalanche Agent Configuration Settings dialog box from the Avalanche Manager **Agent** menu.

This section provides the following information:

- Connecting to an Agent
- Accessing Avalanche Agent Configuration Settings
- Configuring Device Authentication
- Configuring Device Expiration
- Configuring Avalanche Logging
- Configuring Console Timeout
- Configuring Serial Ports
- Configuring Licensing
- Configuring Terminal IDs
- Configuring the FTP Server
- Configuring Transport Encryption

Connecting to an Agent

You can connect to an Agent using one of two methods:

- Select `Connect to Agent` from the **Agent** menu.
- Click the `Connect` button located on the Avalanche Management Console toolbar.

See *Connecting to an Agent* on page 170 for more information about connecting to an Agent.

The first time you connect to the Agent, the *Avalanche Agent Configuration Settings* dialog box appears.

Accessing Avalanche Agent Configuration Settings

Use the Avalanche Management Console **Agent** menu to access the *Avalanche Agent Configuration Settings* dialog box.

To access the Avalanche Agent Configuration Settings dialog box:

1. Connect to a new Avalanche Agent.
2. From the Avalanche Management Console **Agent** menu, select `Agent Configuration...`.

   The *Avalanche Agent Configuration Settings* dialog box appears.

Configuring Device Authentication

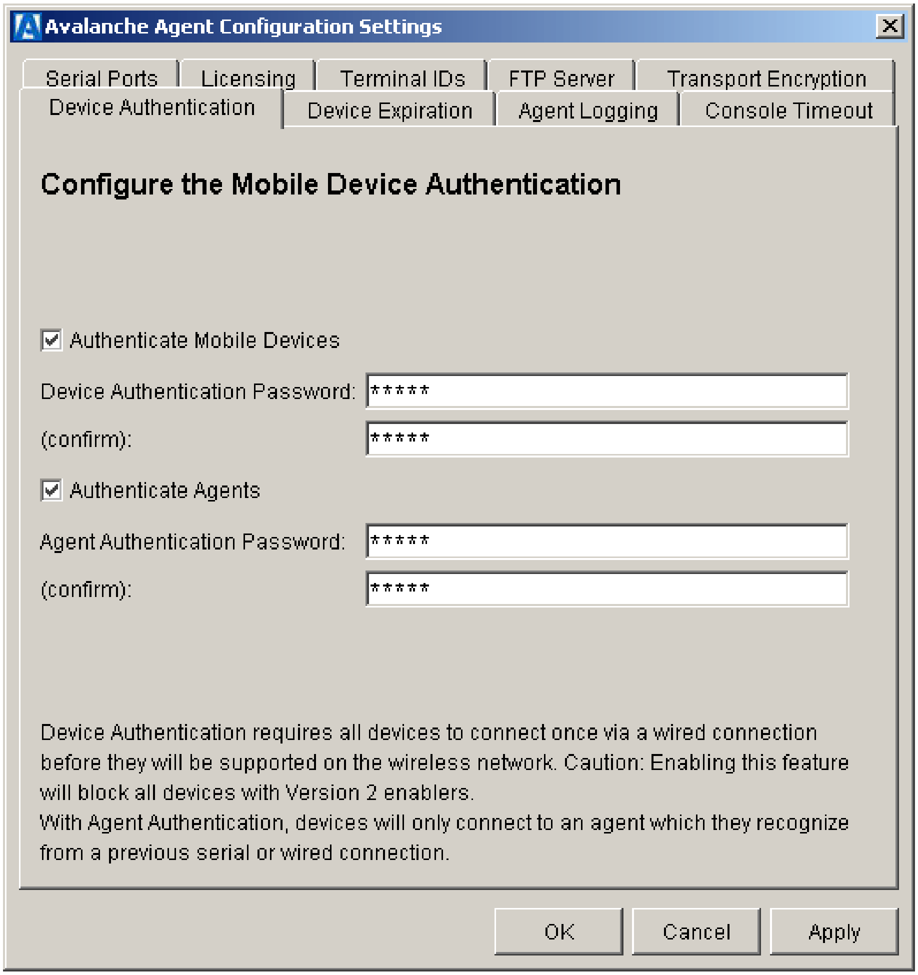
Use the *Avalanche Agent Configuration Settings* dialog box to configure Agent Authentication and Device Authentication.

- **Mobile Device Authentication.** When you enable Device Authentication, Avalanche Manager will only communicate over the network with mobile devices that possess the device authentication password. The device authentication password can only be delivered to the device over a serial connection between the Agent and the mobile device.

- **Agent Authentication.** When you enable Agent Authentication, mobile devices will only communicate with Avalanche Agents over the network with Avalanche Agents that can supply the correct password. The Agent will only supply mobile devices with a password over a serial connection between the Agent and the mobile device.

To configure device authentication:

1. Access the *Avalanche Agent Configuration Settings* dialog box.
2. Select the Device Authentication tab.



Avalanche Agent Configuration Settings

Configure the Mobile Device Authentication

☑ Authenticate Mobile Devices

Device Authentication Password: *****

(confirm): *****

☑ Authenticate Agents

Agent Authentication Password: *****

(confirm): *****

Device Authentication requires all devices to connect once via a wired connection before they will be supported on the wireless network. Caution: Enabling this feature will block all devices with Version 2 enablers.
With Agent Authentication, devices will only connect to an agent which they recognize from a previous serial or wired connection.

Figure 3-1. *Device Authentication Tab*

3 Select the authentication type(s) that you want to use.

4 Configure a password for each type of authentication.

5 Click `OK` or `Apply` to apply the new settings that you have configured.

The following list describes the options in the Device Authentication tab:

Authenticate Mobile Devices	Enables Device Authentication.
Device Authentication Password	Input the Device Authentication password.
(confirm)	Input the Device Authentication password for verification.
Authenticate Agents	Enables Agent Authentication.
Agent Authentication Password	Input the Agent Authentication password.
(confirm)	Input the Agent Authentication password for verification.

Configuring Device Expiration

Use the *Avalanche Agent Configuration Settings* dialog box to configure Device Expiration.

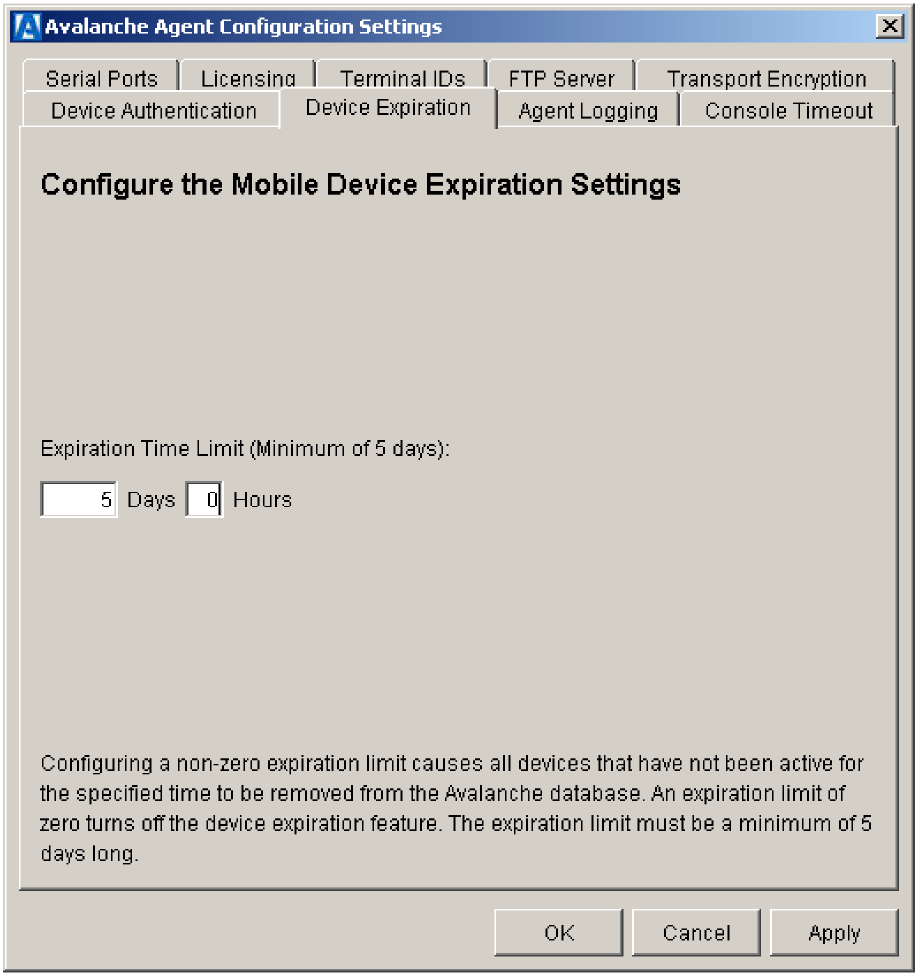
When Device Expiration is enabled, Avalanche Manager resets a timer each time it receives communication from a specific mobile device. If Avalanche Manager does not receive any kind of communication from a device before the timer reaches its expiration limit, Avalanche Manager deletes the mobile device from its database.

Use the Device Expiration tab to configure the expiration limit of the timer.

To configure Device Expiration:

1 Access the *Avalanche Agent Configuration Settings* dialog box.

2 Select the Device Expiration tab.



Configure the Mobile Device Expiration Settings

Expiration Time Limit (Minimum of 5 days):

5 Days 0 Hours

Configuring a non-zero expiration limit causes all devices that have not been active for the specified time to be removed from the Avalanche database. An expiration limit of zero turns off the device expiration feature. The expiration limit must be a minimum of 5 days long.

Figure 3-2. *Device Expiration Tab*

3 Use the `Expiration Time Limit` text boxes to configure the expiration limit.

NOTE If you set the timer to 0, Device Expiration is disabled.

4 Click `OK` or `Apply` to apply the settings that you have configured.

Configuring Avalanche Logging

Use the Avalanche Agent Configuration Settings dialog box to configure Avalanche logging.

Avalanche Manager supports the following logging levels:

- **Critical.** This level writes the least information to the log file, reporting only critical errors that have caused the Avalanche Agent service to crash.
- **Error.** This level writes Error messages and Critical messages to the log file.
- **Warning.** This level writes Critical messages, Error messages, and Warning messages to the log file.
- **Info.** This level is the default logging level and the Wavelink-recommended setting. This logging level writes enough information to the log file to diagnose most problems.
- **Debug.** This logging level writes large amounts of information to the log file that can be used to diagnose more serious problems.

NOTE Running Avalanche Manager in Debug mode is not recommended in a production environment unless there is a problem to diagnose. Running in Debug mode consumes considerable CPU resources.

The current Avalanche log file is saved as `Avalanche.log` to the `<Avalanche Installation Directory>\Service` directory.

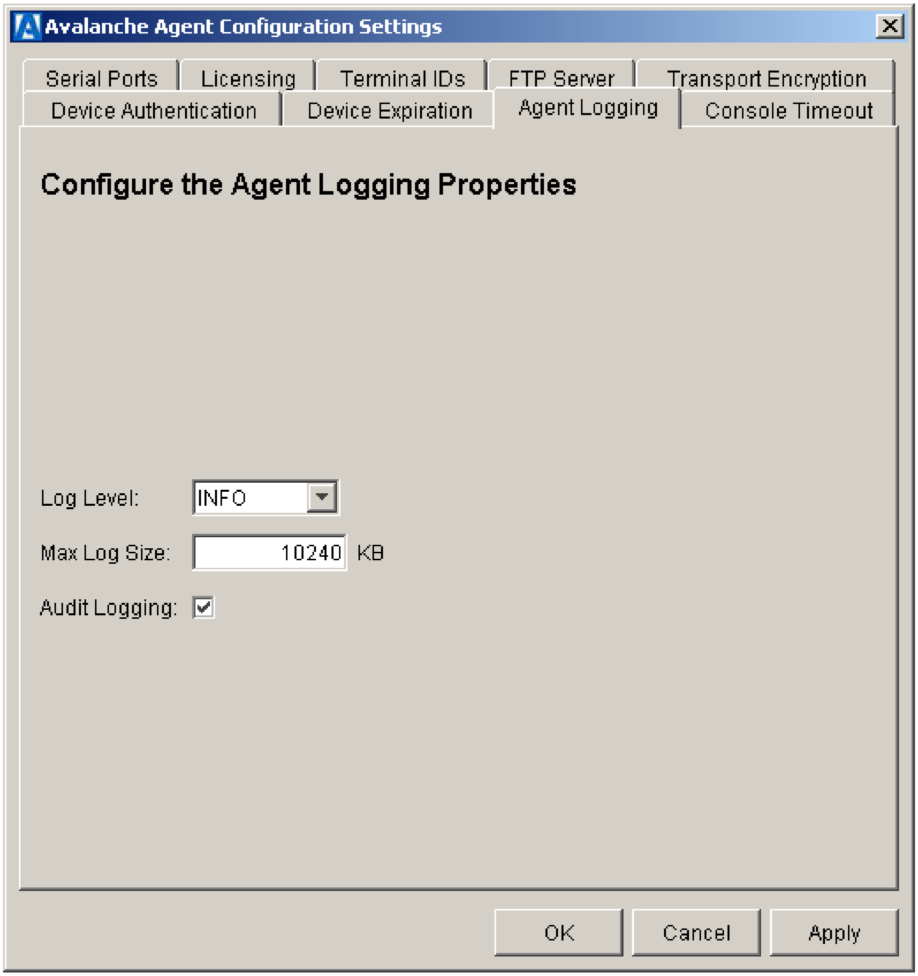
NOTE The default Avalanche installation path is `c:\Program Files\Wavelink\Avalanche`.

Avalanche Manager allows you to configure the maximum size of the log file. Once the current log file reaches the maximum size, it is saved as `Avalanche.log.<num>`, where `<num>` is a number between 001 and 999 (beginning with 001), and a new `Avalanche.log` file is created.

To configure Avalanche logging settings:

1 Access the *Avalanche Agent Configuration Settings* dialog box.

2 Select the Agent Logging tab.



Configure the Agent Logging Properties

Log Level: INFO

Max Log Size: 10240 KB

Audit Logging: ☑

Figure 3-3. *Agent Logging Tab*

3 Use the options in the Agent Logging tab to configure the Agent logging settings.

4 Click `OK` or `Apply` to apply the settings that you have configured.

Log Level Select the logging level that you want Avalanche Manager to use.

Max Log Size Specify the maximum size (in KB) of the log file before Avalanche Manager saves the old log file and begins a new one.

Audit Logging Enables Audit Logging. Audit logging reports information about user activities. (If you are not using user names, then the user shows as "unknown."

Configuring Console Timeout

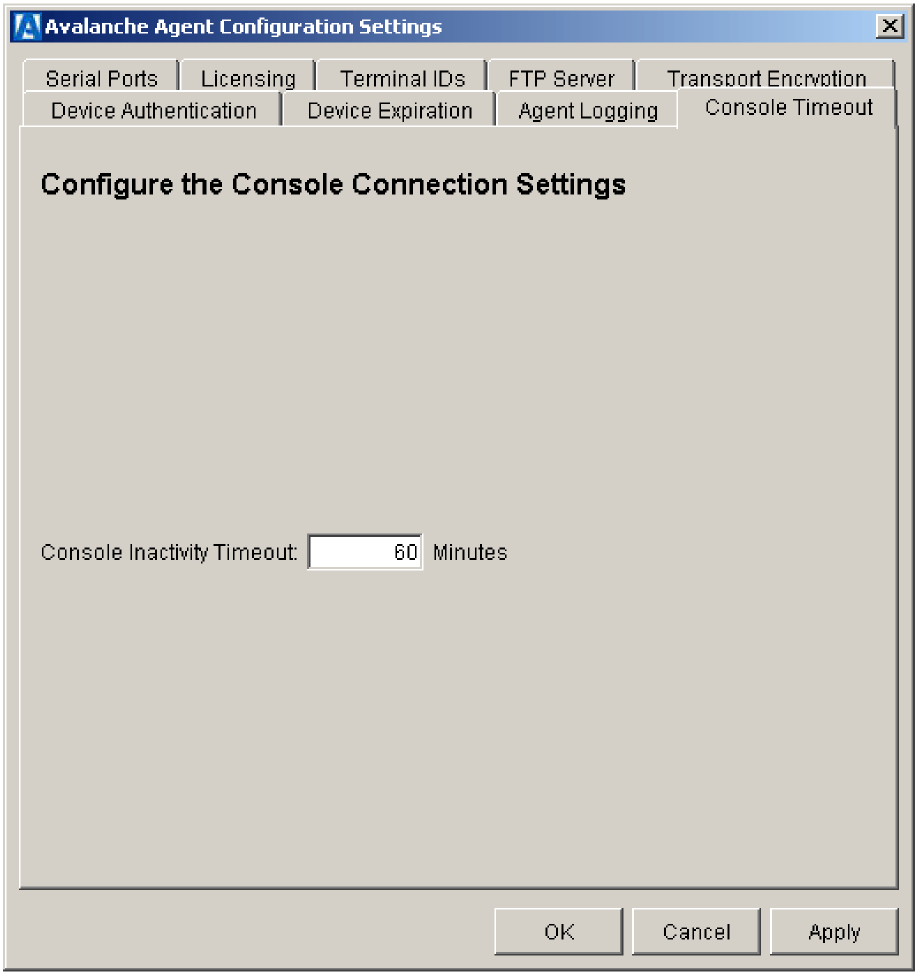
Use the *Avalanche Agent Configuration Settings* dialog box to configure the Console Timeout setting.

The console timeout setting determines how long Avalanche Manager allows an idle connection between the Management Console and the Agent to remain active before the Agent automatically terminates the connection.

To configure the console timeout setting:

1 Access the *Avalanche Agent Configuration Settings* dialog box.

2 Select the Console Timeout tab.



Console Inactivity Timeout: 60 Minutes

Figure 3-4. *Console Timeout Tab*

3 Input the console timeout (in minutes) in the **Console Inactivity Timeout** text box.

4 Click `OK` or `Apply` to apply the settings that you have configured.

NOTE Use a value of 0 to disable the Console Timeout feature.

Configuring Serial Ports

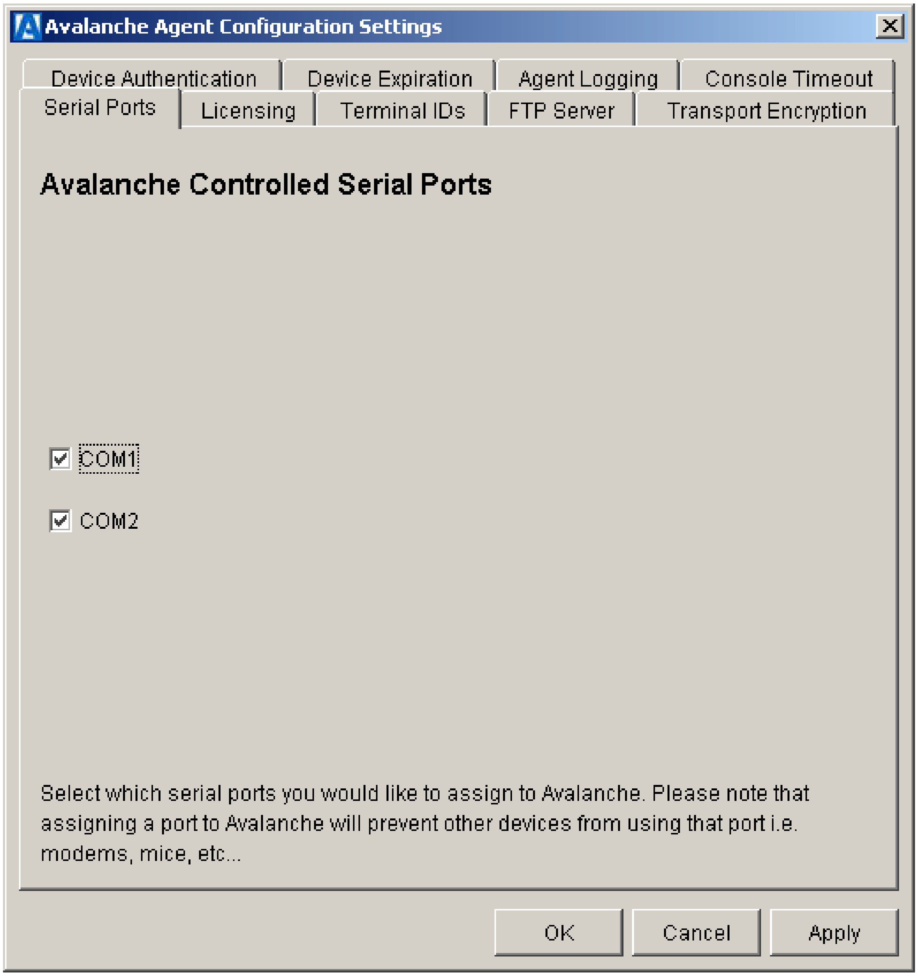
Use the *Avalanche Agent Configuration Settings* dialog box to specify which COM ports on the host system the Avalanche Agent will use.

You can deliver updates to Avalanche clients over a serial connection. However, only one application on a host system can maintain ownership of a COM port. If Avalanche Manager controls the COM ports on the host system, then no other application will be able to use them. Likewise, if another application on the host system (for example, Microsoft ActiveSync) has control of the COM ports, then Avalanche Manager will not be able to use them.

Serial connections are required to implement Mobile Device and Agent Authentication.

To configure the serial ports that Avalanche Manager will use:

1. Access the *Avalanche Agent Configuration Settings* dialog box.
2. Select the Serial Ports tab.



Avalanche Controlled Serial Ports

☑ COM1

☑ COM2

Select which serial ports you would like to assign to Avalanche. Please note that assigning a port to Avalanche will prevent other devices from using that port i.e. modems, mice, etc...

Figure 3-5. *Serial Port Tab*

3 In the Serial Ports tab, select the checkboxes of the Serial Ports that you want Avalanche Manager to use.

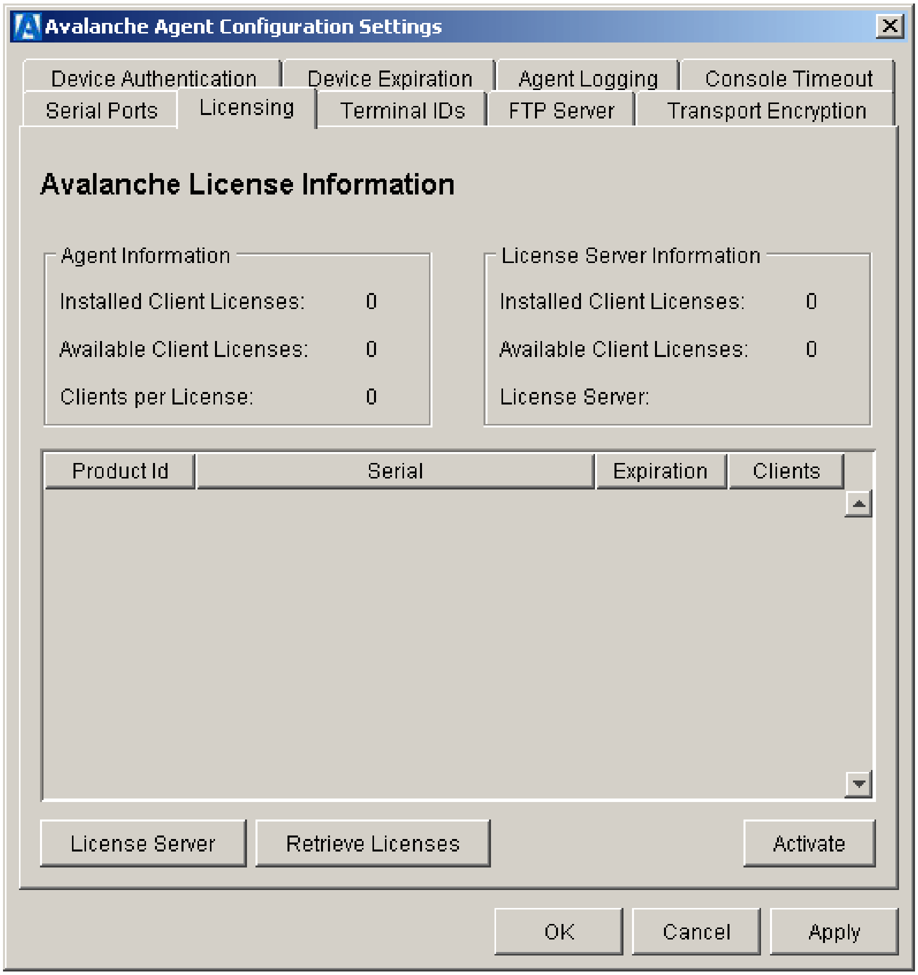
4 Click `OK` or `Apply` to apply the settings that you have configured.

Configuring Licensing

Use the Avalanche Agent Configuration Settings dialog box to input licensing information.

The Avalanche Agent and the Avalanche Management Console do not require a user license. However, you will need an Avalanche license for each device that you manage with Avalanche Manager.

Use the Licensing tab to configure those licenses.



Avalanche License Information

Agent Information

Installed Client Licenses: 0

Available Client Licenses: 0

Clients per License: 0

License Server Information

Installed Client Licenses: 0

Available Client Licenses: 0

License Server:

Product Id	Serial	Expiration	Clients

Figure 3-6. *Licensing Tab*

For more information about licensing, see XXX.

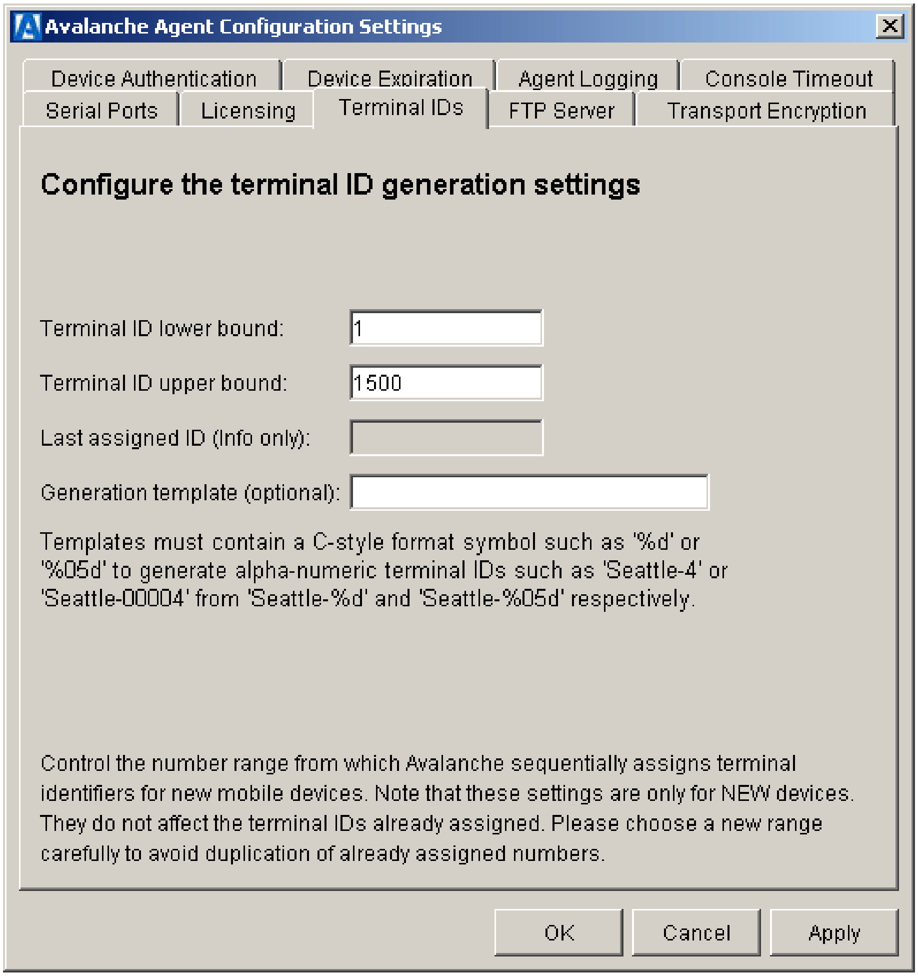
Configuring Terminal IDs

Use the *Avalanche Agent Configuration Settings* dialog box to configure the range of terminal IDs that Avalanche Manager assigns to mobile devices.

Avalanche Manager assigns each device a terminal ID the first time that the device communicates with Avalanche Manager. The number Avalanche Manager selects is the lowest number available in a range of configured numbers. Alternately, you can use C-style format to configure your own specific terminal ID.

To configure the Terminal ID settings:

1. Access the *Avalanche Agent Configuration Settings* dialog box.
2. Select the Terminal IDs tab.



Configure the terminal ID generation settings

Terminal ID lower bound: 1

Terminal ID upper bound: 1500

Last assigned ID (Info only):

Generation template (optional):

Templates must contain a C-style format symbol such as '%d' or '%05d' to generate alpha-numeric terminal IDs such as 'Seattle-4' or 'Seattle-00004' from 'Seattle-%d' and 'Seattle-%05d' respectively.

Control the number range from which Avalanche sequentially assigns terminal identifiers for new mobile devices. Note that these settings are only for NEW devices. They do not affect the terminal IDs already assigned. Please choose a new range carefully to avoid duplication of already assigned numbers.

Figure 3-7. *Terminal IDs Tab*

3 Configure the lower and upper limits for the range of Terminal IDs that Avalanche will assign to mobile devices.

Alternately, configure your own method using the **Generation Template** text box.

4 Click `OK` or `Apply` to apply the settings that you have configured.

Terminal ID lower bound Specify the lowest terminal ID that Avalanche Manager will assign a mobile device.

Terminal ID upper bound Specify the highest terminal ID that Avalanche Manager will assign a mobile device.

Last assigned ID (Info only) Indicates the last Terminal ID that Avalanche Manager assigned a mobile device.

Generational template (optional) Use a C-style format to allow Avalanche Manager to assign alphanumeric IDs.

Examples:

- `Seattle-%d` (generates IDs such as Seattle-4)
- `Seattle-%05d` (generates IDs such as Seattle-00004)

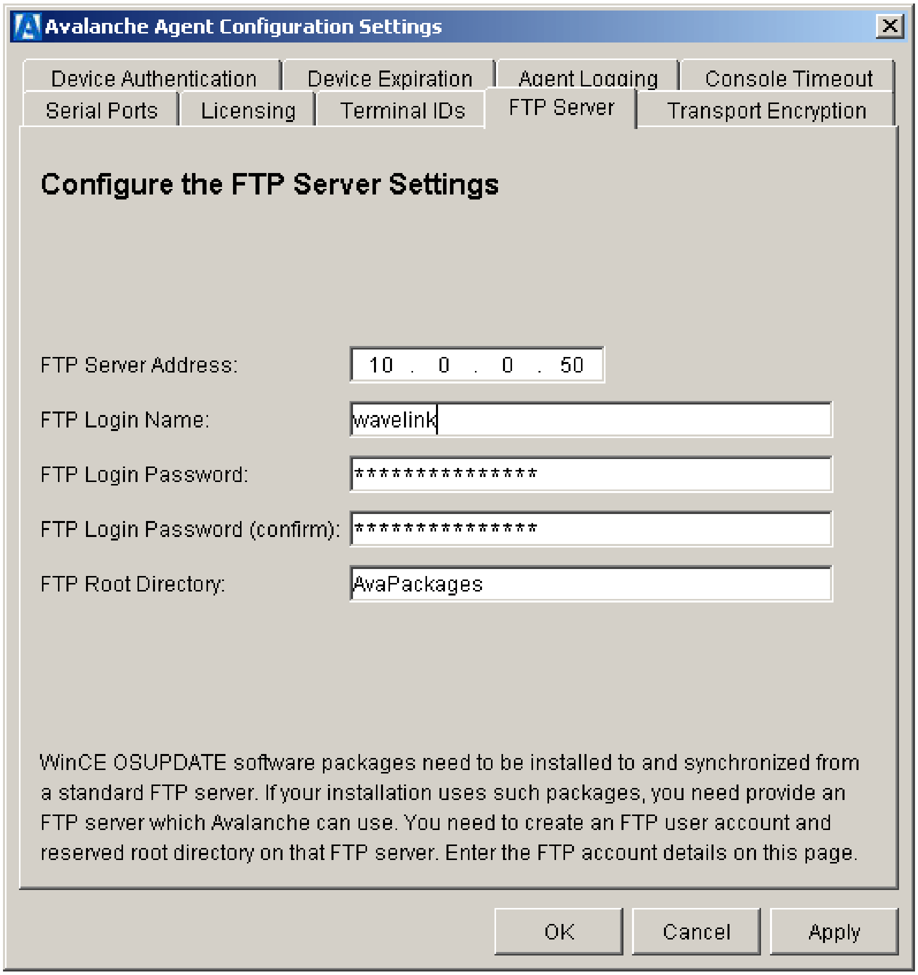
Configuring the FTP Server

If you are using WinCE OSUPDATE software packages, you will need to install and synchronize them from a standard FTP server. Use the *Avalanche Enabler Configuration Settings* dialog box to configure the IP address and login parameters of the FTP server.

To configure FTP server settings:

1 Access the Avalanche Enabler Configuration Settings dialog box.

2 Select the FTP Server tab.



Configure the FTP Server Settings

FTP Server Address: 10 . 0 . 0 . 50

FTP Login Name: wavelink

FTP Login Password: ***************

FTP Login Password (confirm): ***************

FTP Root Directory: AvaPackages

WinCE OSUPDATE software packages need to be installed to and synchronized from a standard FTP server. If your installation uses such packages, you need provide an FTP server which Avalanche can use. You need to create an FTP user account and reserved root directory on that FTP server. Enter the FTP account details on this page.

Figure 3-8. *FTP Server Tab*

3 Configure the settings in the FTP Server tab with the correct parameters for the FTP server that you will use to install and synchronize WinCE OSUPDATE software packages.

4 Click `OK` or `Apply` to apply the settings that you have configured.

FTP Server Address Indicates the IP address of the FTP server.

FTP Login Name Indicates the login name for the FTP server.

FTP Password Indicates the password for the login name.

FTP Login Password (Confirm)	Confirm the login password.
FTP Root Directory	Indicates the root FTP directory.

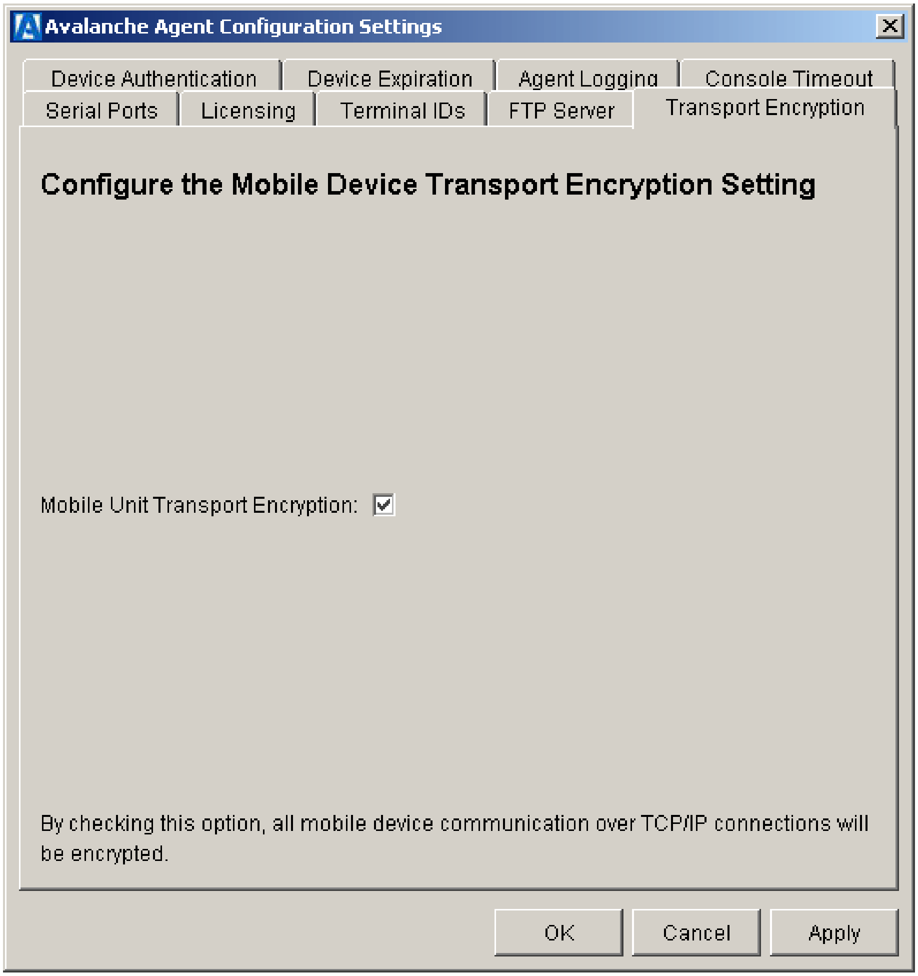
Configuring Transport Encryption

Use the *Avalanche Agent Configuration Settings* dialog box to enable/disable Avalanche transport encryption.

When you enable transport encryption, all TCP/IP communication between the Avalanche Agent and mobile devices will be encrypted.

To configure transport encryption:

1. Access the Avalanche Agent Configuration Settings dialog box.
2. Select the Transport Encryption tab.



Configure the Mobile Device Transport Encryption Setting

Mobile Unit Transport Encryption: ☑

By checking this option, all mobile device communication over TCP/IP connections will be encrypted.

Figure 3-9. *Transport Encryption Tab*

3 Select the Mobile Unit Transport Encryption option to enable transport encryption. (Alternately, de-select the option to turn off transport encryption.)

4 Click `OK` or `Apply` to apply the settings that you have configured.

Chapter 4: Avalanche Management Console

The user interface for the Avalanche Manager Agent is the Avalanche Management Console. You can have multiple Avalanche Management Consoles installed throughout your organization, allowing you to manage your wireless network from multiple locations.

When the Management Console connects to a given Agent, it synchronizes with the Agent, downloading any updated information from the Agent to the local console.

NOTE Although it is not recommended, you can also disable synchronization for an Agent, if desired. See *Adding an Agent* on page 166 for more information.

This section describes how to configure site profiles, software collections, packages, network profiles, and other Avalanche features using the Management Console.

The following list shows the topics covered in this section:

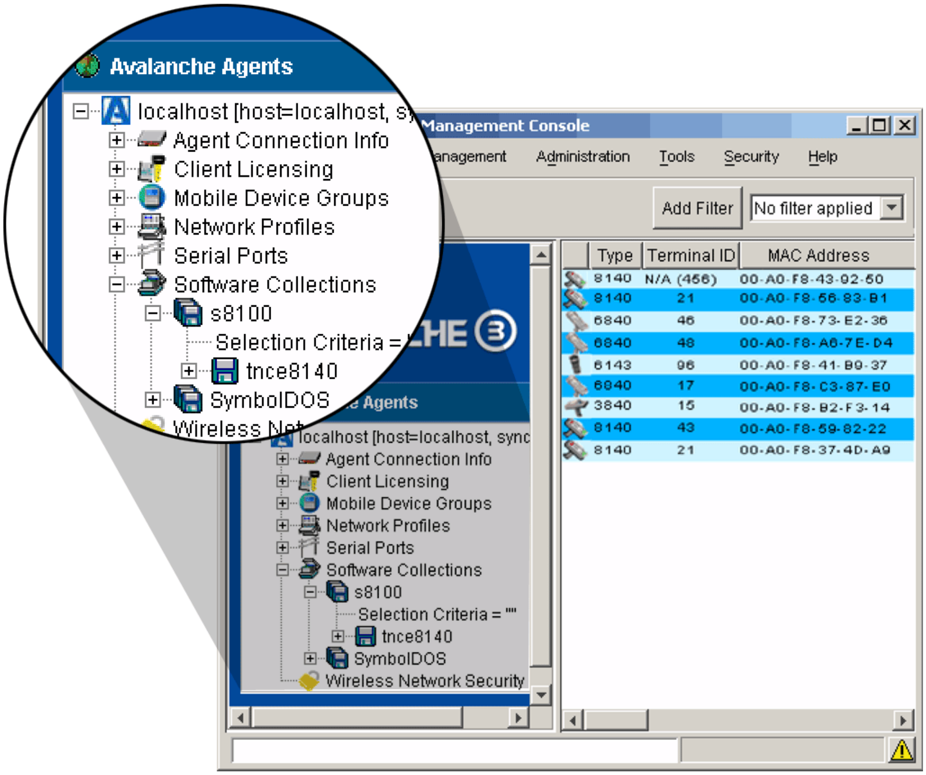
- Management Console Views
- Management Console Menus
- Management Console Status Bar
- Management Console TermProxy Configuration
- Configuring the Management Console

Management Console Views

The Avalanche Management Console display is a two-pane interface containing the Tree View and List View.

Tree View

The Tree View appears in the left portion of the Management Console, as shown in Figure 4-1. This view shows a hierarchical view of the entire system configuration.



Type	Terminal ID	MAC Address
8140	N/A (456)	00-A0-F8-43-02-50
8140	21	00-A0-F8-56-83-B1
6840	46	00-A0-F8-73-E2-36
6840	48	00-A0-F8-A6-7E-D4
6143	96	00-A0-F8-41-B9-37
6840	17	00-A0-F8-C3-87-E0
3840	15	00-A0-F8-B2-F3-14
8140	43	00-A0-F8-59-82-22
8140	21	00-A0-F8-37-4D-A9

Figure 4-1. *Main Branches*

The Tree View displays features and information associated with the currently connected Avalanche Manager Agent. This includes features and information associated with client licensing, network interface cards, and serial ports. A serial port can be either a standard serial port or a digiboard serial port.

Icons in the Tree View that appear with a superimposed X are disabled. By default, network profiles are disabled when initially created, and software packages are disabled when initially installed.

When you double-click an item in the Tree View, it displays detailed information about the selected item. If you select a software package, for example, the package type, version number, the number of files included in the package, the selection criteria, and the current status appear beneath the branch. The current status shows whether the package is On Hold (disabled) or Active (enabled).

When you click on software collections, software packages, and network profiles, the mobile devices associated with the selected item will appear in the List View. See *List View* on page 69 for more information.

List View

The List View, located in the right pane, shows a set or subset of mobile devices based on the currently selected item in the Tree View. For example, when you select a particular software package, all mobile devices that are associated with that software package appear in the List View.

NOTE For more details about the mobile devices that appear in the List View, including a list of all packages destined for the device and the update status of each, see *Viewing Mobile Device Information* on page 135.

The information that appears in the columns in the List View is as follows:

Type The model name of a given mobile device (i.e., 6840, 1040, etc.).

Terminal ID The unique ID automatically generated by the Avalanche Manager. You can use this ID when setting the workstation ID for 5250 emulation. See *Setting a Workstation ID* on page 138 for more information.

MAC Address The Media Access Control address of a mobile device. This address uniquely identifies this mobile device on a network from a physical standpoint.

IP Address The Internet Protocol address assigned to the mobile device.

U

The client update status of the mobile device. The check mark indicates that the mobile device is up to date, while an X indicates that an update is available but not yet loaded on the device.

U

The properties status of the mobile device. The check mark indicates that the properties of the mobile device are up to date, while an X indicates that properties have changed but have not yet been downloaded to the device.

L

The license update status of the mobile device. The certificate icon indicates that the mobile device is licensed, while an X indicates that a mobile device is unlicensed.

W

The status of the automatic WEP rotation. The padlock indicates that the automatic WEP configuration on the mobile device is up to date, while an X indicates that an automatic WEP configuration update is available but not yet loaded on the device.

Last Contact

The date and time of the last contact with the Avalanche Manager.

Activity

The current status of a mobile device with respect to the Avalanche Manager. For example, when the mobile device receives new software, the activity status is `Downloading`.

Details

The software update status, displayed in real time.

To view all mobile devices that are associated with an Agent, click on any item in the Tree View except a software collection, package, or a network profile. The mobile devices appear in the List View.

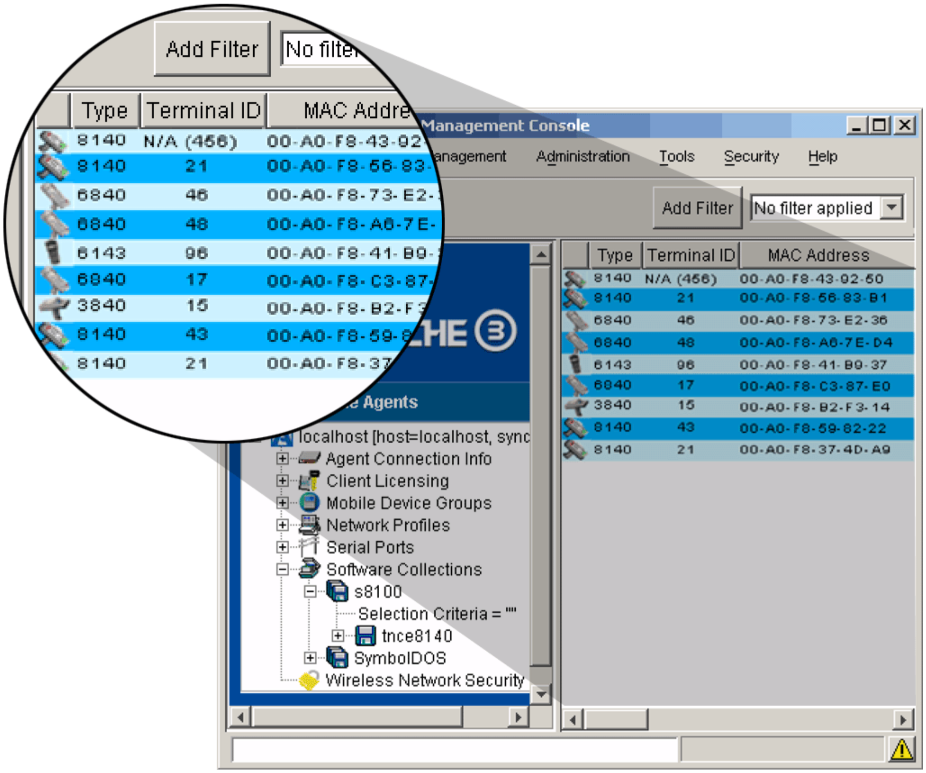
If the current selection in the Tree View is a software collection, software package, or a network profile, the specific item selected determines which subset of mobile devices appear in the List View. This applies to the following:

- When you select a software collection, all the mobile devices that match that collection’s selection criteria appear in the List View (Figure 4-2).

- When you select a software package, all the mobile devices that match both the selection criteria of that package and that of the software collection that contains the package (Figure 4-3 and 4-4) appear in the List View.

- When you select a network profile in the Tree View, all mobile devices associated with the IP addresses in that profile appear in the List View.

NOTE For more information about selection criteria, see *Selection Criteria* on page 122.

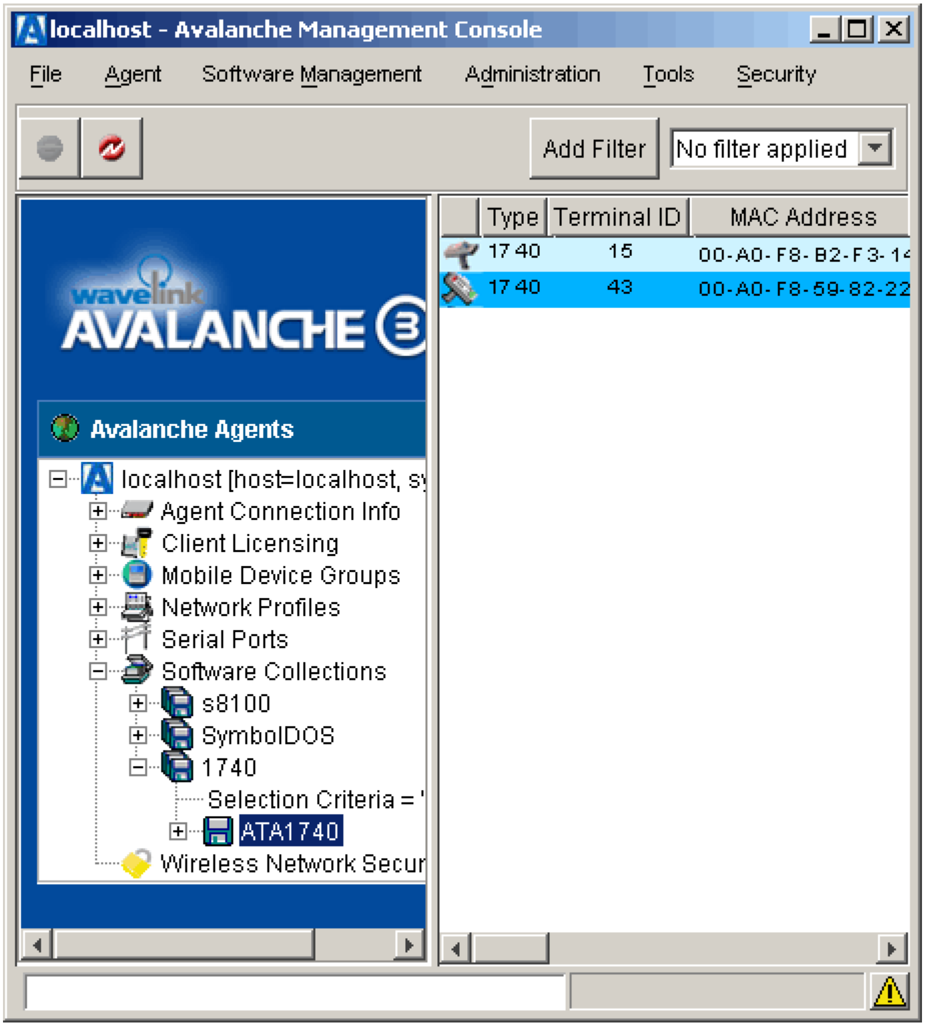


Type	Terminal ID	MAC Address
8140	N/A (456)	00-A0-F8-43-92-60
8140	21	00-A0-F8-56-83-B1
6840	46	00-A0-F8-73-E2-36
6840	48	00-A0-F8-A6-7E-D4
6143	96	00-A0-F8-41-B9-37
6840	17	00-A0-F8-C3-87-E0
3840	15	00-A0-F8-B2-F3-14
8140	43	00-A0-F8-59-82-22
8140	21	00-A0-F8-37-4D-A9

Figure 4-2. *List View*

The following screens provide several examples of this feature.

In Figure 4-3, the ATA1740 software package is selected. The List View shows the mobile devices that meet the selection criteria for the ATA1740 software package.

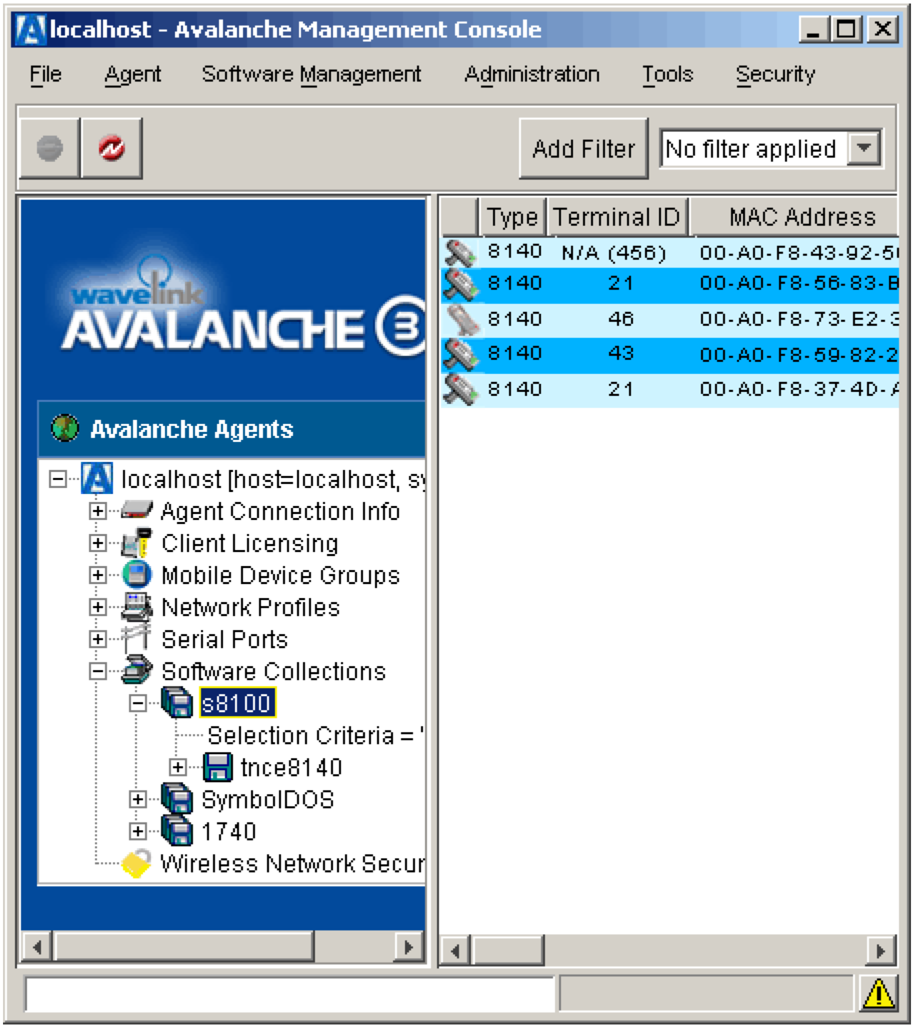


No filter applied

	Type	Terminal ID	MAC Address
	1740	15	00-A0-F8-B2-F3-1
	1740	43	00-A0-F8-59-82-22

Figure 4-3. *Example of Filtering a Software Package*

Figure 4-4 shows the mobile devices in the List View that meet the selection criteria for the `s8140` software collection, in contrast to the package. If the collection had the same selection criteria as the package, the same devices would appear in the List View. In this case, however, the collection has no selection criteria associated with it. Consequently, all mobile devices known to the current Avalanche Manager Agent appear in the List View.



Type	Terminal ID	MAC Address
8140	N/A (456)	00-A0-F8-43-92-5
8140	21	00-A0-F8-56-83-B
8140	46	00-A0-F8-73-E2-3
8140	43	00-A0-F8-59-82-2
8140	21	00-A0-F8-37-4D-

Figure 4-4. *Example of Filtering a Software Collection*

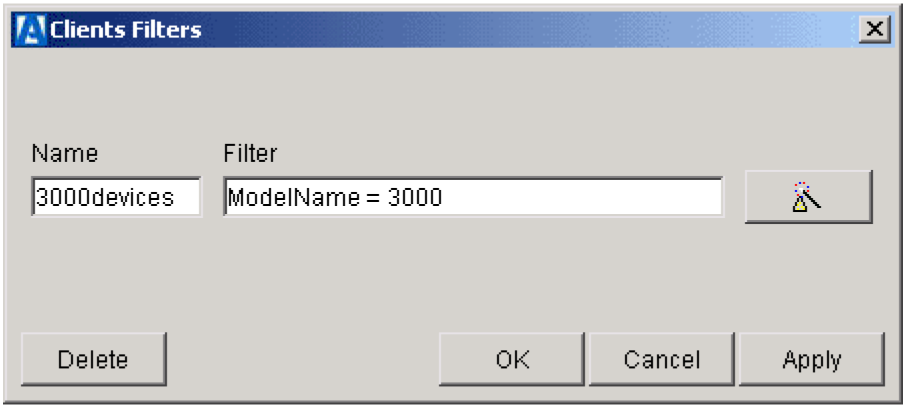
Filtering the List View

You can filter the List view of the Avalanche Management Console to display on specific mobile devices at any given time. These filters can be saved so you can access them as often as necessary.

To add a filter

1 From the Avalanche Management Console, click `Add Filter`.

The *Client Filters* dialog box appears.



Name: 3000devices

Filter: ModelName = 3000

Figure 4-5. *The Client Filters Dialog Box*

2 Enter a name for the filter in the **Name** text box.

3 Build an appropriate filter.

To build a filter, click the **Selection Criteria** button. The *Selection Criteria Builder* dialog box appears, allowing you to create a filter based on a variety of mobile device characteristics. See *Selection Criteria* on page 122 for more information.

4 When you are finished building a filter, click `OK` to return to the *Client Filters* dialog box. The filter will appear in the **Filter** text box.

5 Click `Apply`.

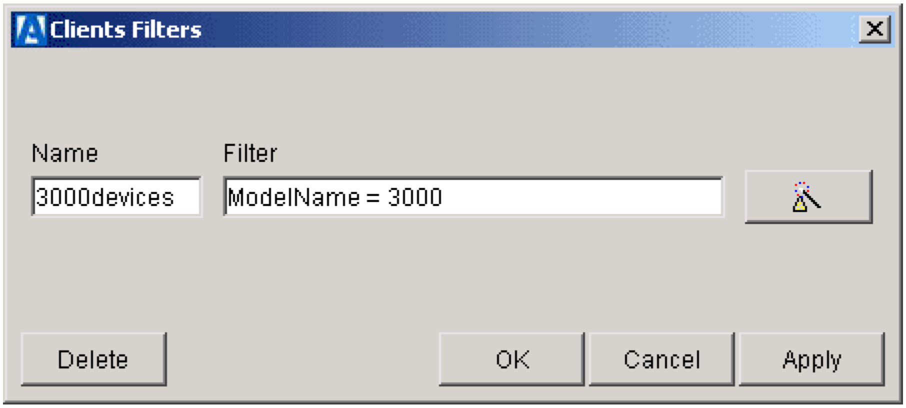
You can now select the filter from the **Filter** list located on the Avalanche Management Console toolbar. To use the filter, select it from the **Filter** list.

To delete a filter

1 Select a filter from the **Filter** list.

2 Click `Edit Filter`.

The *Client Filters* dialog box appears.



Clients Filters

Name: 3000devices

Filter: ModelName = 3000

Figure 4-6. *The Client Filters Dialog Box*

3 Click `Delete`.

Hiding and Showing Columns

The Management Console provides you with the ability to control which columns appear in the List View.

You can add columns based on any mobile device property.

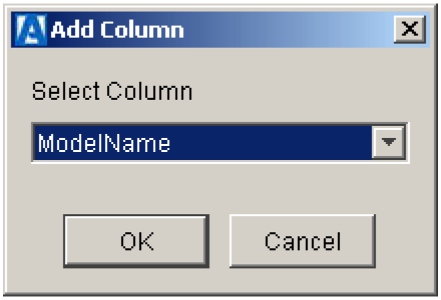
To hide a column:

Right-click on the column header for the column that you want to hide and select `Remove column`.

To show a column:

1 Right-click on any of the column headers and select `Add column`.

The *Add Column* dialog box appears.



Add Column

Select Column: ModelName

Figure 4-7. *The Add Column Dialog Box*

2 Select the column you want to add from the drop-down list.

3 Click `OK`.

To reset the default columns:

Right-click on any column header and select `Reset columns`.

Management Console Menus

The Management Console includes the following menus in the menubar:

- File Menu
- Agent Menu
- Software Management Menu
- Administration Menu
- Tools Menu
- Security Menu
- Help Menu

File Menu

Figure 4-8 shows the **File** menu for the Management Console.

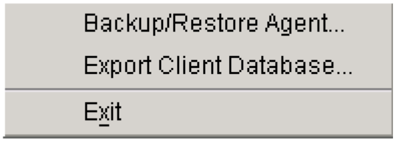


Figure 4-8. *File Menu*

The options available in the File menu include:

Backup/Restore Agent
Launches the Backup/Restore wizard that allows you to backup or restore all software collections associated with the current Agent and information associated with the local Avalanche setup. See *Backing Up an Agent* on page 181 and *Restoring an Agent* on page 182 for more information.

Export Client Database
Exports the client database associated with the current Agent to a CSV file (.csv file extension), allowing you to generate reports from another program. The CSV file is saved on the local console.

Exit
Exits the Management Console.

NOTE The Avalanche Manager Agent continues to run after you close the Management Console.

Agent Menu

The Agent menu provides functions that allow you to connect and disconnect from an Avalanche Manager Agent.

Figure 4-9 shows the **Agent** menu.

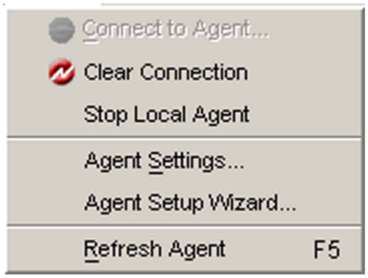


Figure 4-9. *Agent Menu*

The options on this menu include:

Connect to Agent Allows you to select and connect to an Avalanche Manager Agent.

Clear Connection Disconnects you from the current Avalanche Manager Agent to which you are connected.

Stop Local Agent Stops the Avalanche Agent, if it is currently running.

Agent Settings Allows you to modify the settings for the connected Avalanche Manager Agent.

Agent Setup Wizard Launches the Agent Setup Wizard.

Refresh Agent Refreshes the Avalanche Manager Agent.

Software Management Menu

The Software Management menu has a single option that allows you to install a software package.

Figure 4-10 shows the **Software Management** menu.

Figure 4-10. *Software Management Menu*

The option on this menu is:

Install Software Package Installs an Avalanche software package. See *Installing Software Packages to the Management Console* on page 43 for more information.

Administration Menu

The Administration menu provides functions that allow you to update your Avalanche product license and modify Avalanche Manager Console settings.

Figure 4-11 shows the **Administration** menu.

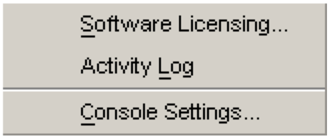


Figure 4-11. *Administration Menu*

The options on this menu include:

Software Licensing Allows you to update the license for your Avalanche installation. See *Authorizing the Avalanche Manager* on page 28 for more information.

Activity Log Allows you to open the activity log, which contains the record of activities since the Avalanche Management Console last started.

Console Settings Allows you to modify the settings for the Avalanche Management Console. See *Configuring the Management Console* on page 86 for more information.

Tools Menu

This menu contains the utilities required to schedule and monitor software package updates and to perform site management functions.

Figure 4-12 shows the **Tools** menu.

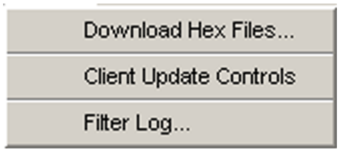


Figure 4-12. *Tools Menu*

The options in this menu include:

Download Hex Files Select Download Hex Files to transfer a HEX file to a DOS-based mobile device over a serial connection. Refer to *Using the Hex File Download Utility* on page 34 for details on downloading.

Client Update Controls Provides access to update management functions such as scheduling updates and controlling the use of network bandwidth. See *Configuring Updates* on page 157 for more information.

Filter Log Allows you to configure logging of Avalanche Manager data for a specific mobile device.

Security Menu

The Security menu provides functions for access to the Avalanche Management Console and wireless encryption.

Figure 4-13 shows the **Security** menu.

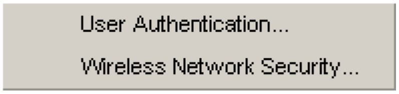


Figure 4-13. *Security Menu*

The options available in the Security menu include:

User Authentication Allows you to specify administrative rights for managing Agents on a per-user basis. See *User Authentication* on page 174 for more information.

Wireless Network Security Allows you to specify WEP key rotation for the mobile devices. See *Chapter 10: WEP Encryption* on page 195 for more information.

Help Menu

The Help menu allows you to access the online Help and version information about the Avalanche Manager.

Figure 4-14 shows the **Help** menu.

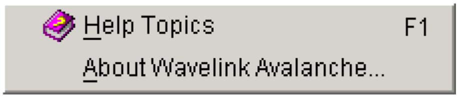


Figure 4-14. *Help Menu*

The options available in the Help menu include:

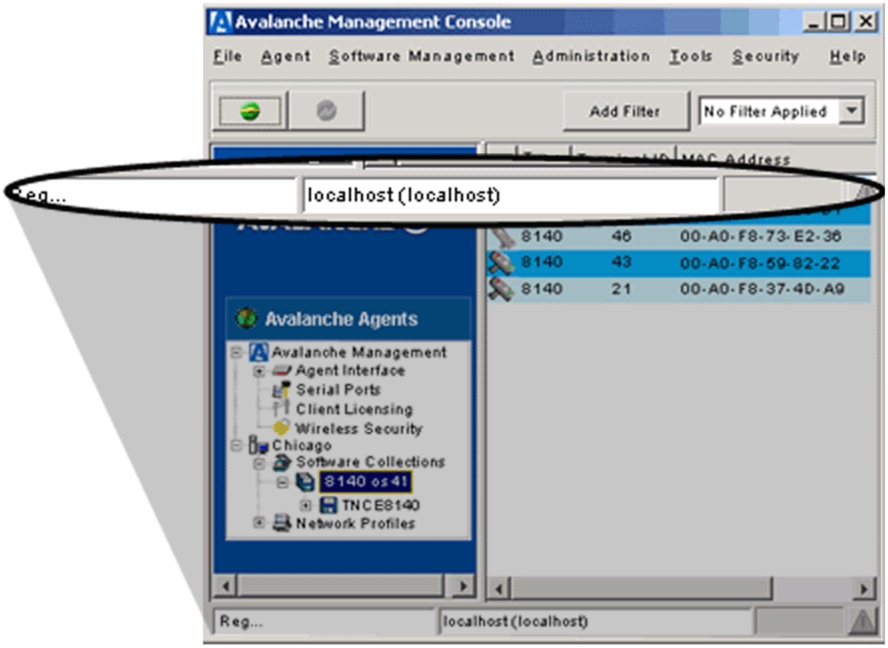
Help Topics Opens the online Help. If you are using the Help for the first time, this option allows you to initialize online Help by browsing for a path to the desired browser.

About Wavelink Avalanche Displays version information about the Avalanche Management Console.

Management Console Status Bar

The status bar of the Avalanche Management Console provides you with information relevant to Agent connections and activity. The information in the status bar includes the following information (in order from left to right):

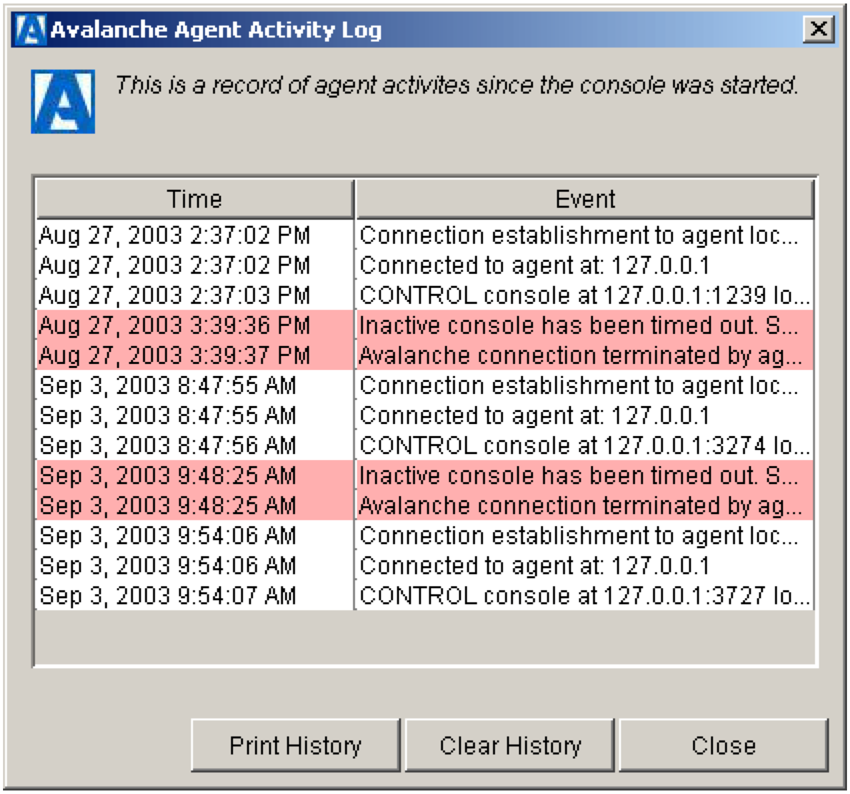
- Agent connection status
- Agent name or IP address
- Last occurring activity



		MAC Address
8140	46	00-A0-F8-73-E2-36
8140	43	00-A0-F8-59-82-22
8140	21	00-A0-F8-37-4D-A9

Figure 4-15. *The Status Bar*

In addition, the status bar contains an **Activity Log** button (represented by an exclamation point within a triangle). Clicking this button opens an *Agent Activity Log* dialog box, which displays a record of the Agent activities since the Avalanche Management Console last started.



Avalanche Agent Activity Log

This is a record of agent activites since the console was started.

Time	Event
Aug 27, 2003 2:37:02 PM	Connection establishment to agent loc...
Aug 27, 2003 2:37:02 PM	Connected to agent at: 127.0.0.1
Aug 27, 2003 2:37:03 PM	CONTROL console at 127.0.0.1:1239 lo...
Aug 27, 2003 3:39:36 PM	Inactive console has been timed out. S...
Aug 27, 2003 3:39:37 PM	Avalanche connection terminated by ag...
Sep 3, 2003 8:47:55 AM	Connection establishment to agent loc...
Sep 3, 2003 8:47:55 AM	Connected to agent at: 127.0.0.1
Sep 3, 2003 8:47:56 AM	CONTROL console at 127.0.0.1:3274 lo...
Sep 3, 2003 9:48:25 AM	Inactive console has been timed out. S...
Sep 3, 2003 9:48:25 AM	Avalanche connection terminated by ag...
Sep 3, 2003 9:54:06 AM	Connection establishment to agent loc...
Sep 3, 2003 9:54:06 AM	Connected to agent at: 127.0.0.1
Sep 3, 2003 9:54:07 AM	CONTROL console at 127.0.0.1:3727 lo...

Figure 4-16. *The Avalanche Agent Activity Log Dialog Box*

Management Console TermProxy Configuration

Wavelink TermProxy provides session persistence and other services to mobile devices using the Wavelink Telnet Client. Wavelink TermProxy provides a web-based configuration interface that supports secure HTTP (https) connections.

You can configure the web addresses (URLs) of multiple TermProxy servers through the Avalanche Management Console. Once you have configured the address of a TermProxy server, you can select to automatically connect to the TermProxy server's web interface. When you select to connect to TermProxy, the Avalanche Management Console will automatically launch your default web browser and direct it to the URL of the TermProxy server.

Configuring a TermProxy Server Connection

Before you can automatically connect to a TermProxy server, you must configure the URL for the TermProxy server.

To configure a TermProxy server URL:

1 Launch the Avalanche Management Console.

2 Click the TermProxy Configuration button.

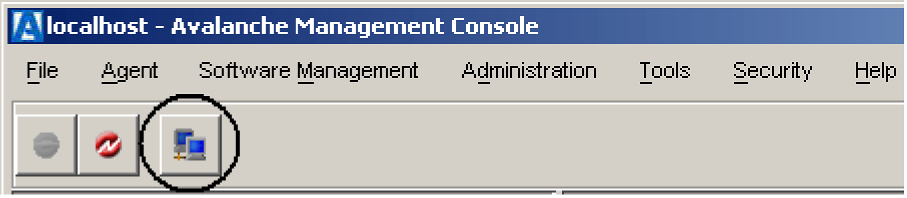


Figure 4-17. *TermProxy Configuration Button*

The *TermProxy Server Configurations* dialog box appears.

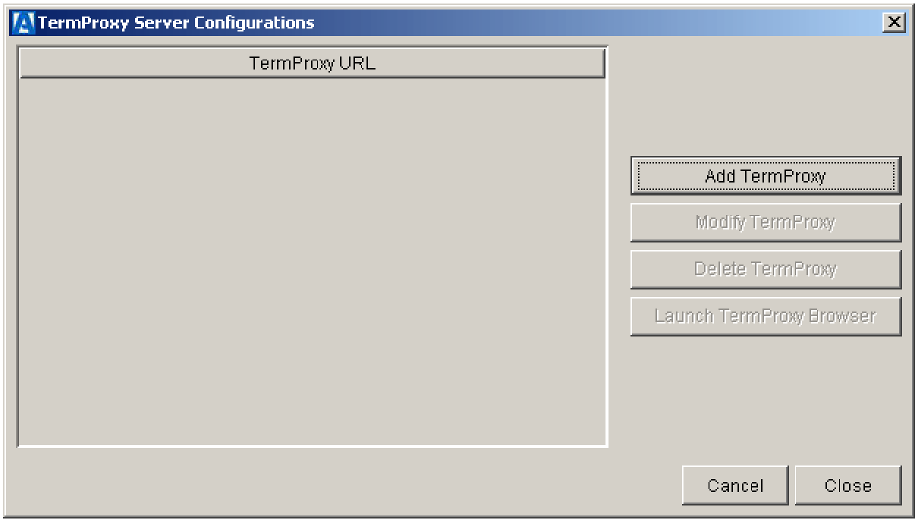
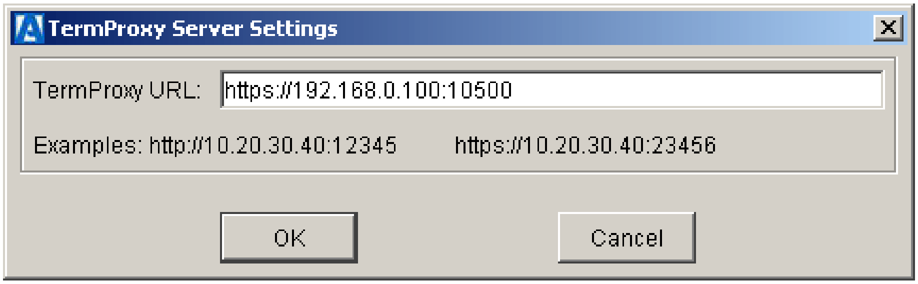


Figure 4-18. *TermProxy Server Configurations Dialog Box*

3 Click `Add TermProxy`.

The *TermProxy Server Settings* dialog box appears.

4 Type the URL of the TermProxy server in the `TermProxy URL` text box.



TermProxy Server Settings

TermProxy URL: https://192.168.0.100:10500

Examples: http://10.20.30.40:12345 https://10.20.30.40:23456

Figure 4-19. *Configuring the TermProxy URL*

5 Click `OK`.

The TermProxy URL now appears in the *TermProxy Server Configurations* dialog box.

Connecting to a TermProxy Server

You can use the *TermProxy Server Configurations* dialog box to connect to a TermProxy server.

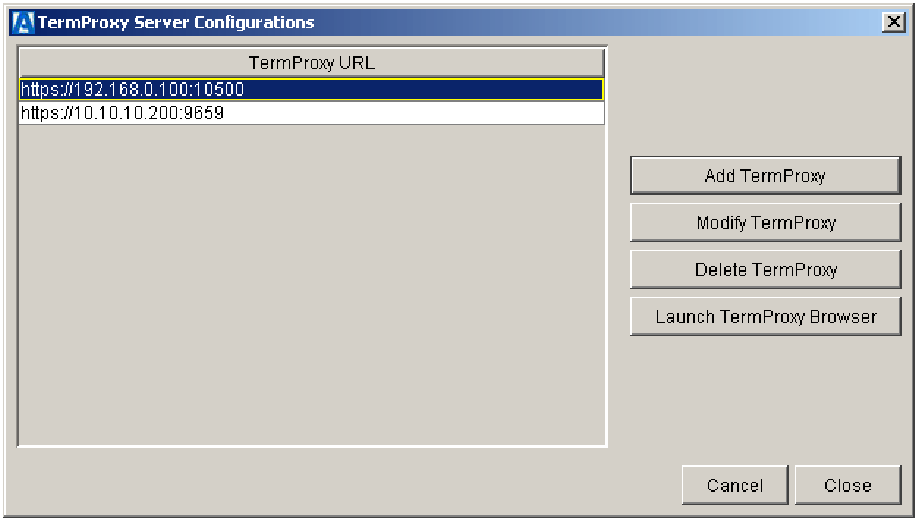
To connect to a TermProxy server:

1 Launch the Avalanche Management Console.

2 Click the TermProxy Configuration button.

The *TermProxy Server Configuration* dialog box appears.

3 From the list of configured TermProxy server URLs, select the TermProxy server to which you want to connect.



TermProxy URL
https://192.168.0.100:10500
https://10.10.10.200:9659

Figure 4-20. *Selecting the TermProxy Server*

4 Click `Launch TermProxy Browser`.

The default web browser on the host system launches and attempts to connect to the TermProxy server via the configured URL.

Configuring the Management Console

The Management Console allows you to configure options such as administrative access. This section contains information on the following topics:

- Logging Options
- Online Help

Logging Options

You can set the maximum log size and the log level for both the Management Console and the Agent log file.

The log for the Management Console is stored in the `\Wavelink\Avalanche\` subdirectory. The name of this log file is `AvalancheDefault.log`.

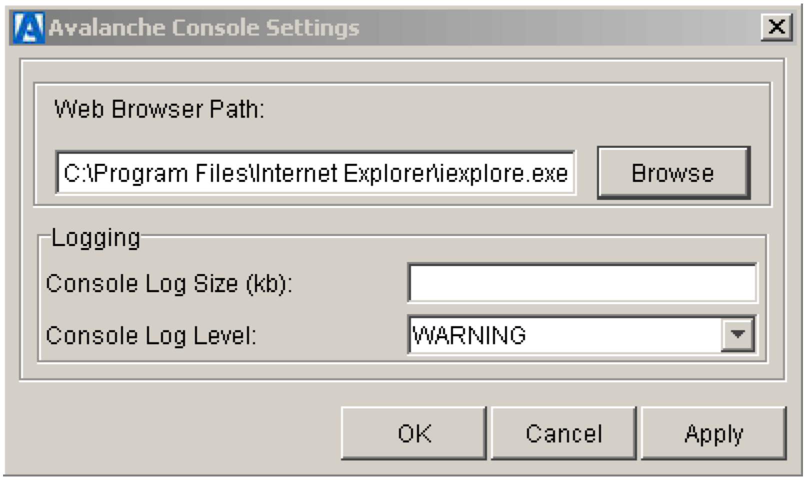
The log for the Agent is stored in the `\Wavelink\Avalanche\Service` subdirectory. The name of this log file is `Avalanche.log`.

NOTE See *Chapter 11: Log Filter* on page 203 for more information about viewing the Agent log with the log viewer.

To set options for the Management Console log:

1 Select `Console Settings` from the **Administration** menu.

2 In the *Avalanche Console Properties* dialog box (Figure 4-21), enter the maximum size of the Management Console's log file in the **Console Log Size** text box. The default size is 1024 KB.



Avalanche Console Settings

Web Browser Path: C:\Program Files\Internet Explorer\iexplore.exe

Logging

Console Log Size (kb):

Console Log Level: WARNING

Figure 4-21. *The Avalanche Console Settings Dialog Box*

3 Select the log level in the **Console Log Level** list. The available log levels are:

Critical	Logs unrecoverable errors.
Error	Logs all errors.
Warning	Logs warnings and errors. Warnings represent either insignificant errors or errors handled internally by the Avalanche Manager. This is the default setting for the console log.

Info Logs all errors, warnings, and informational messages.

Debug Logs additional debugging information typically used by technical support personnel.

To configure log options for the Avalanche Agent, see *Chapter 3: Avalanche Agent Setup Wizard* on page 49.

Online Help

You can set the default browser to be used with the online Help.

To configure the default browser:

1. Select `Avalanche Options` from the **Administration** menu.
2. In the *Avalanche Console Properties* dialog box (Figure 4-21), set the browser path.

   To enter the path manually, type the path in the **Web Browser Path** text box.

   To browse for the path, click `Browse` and navigate to the location of the desired browser executable. Select the browser and click `Select`.
3. Click `OK`.

Chapter 5: Managing Clients

The Management Console provides the ability to manage software and configuration information for download to specific clients or client groups. This section provides information and instructions for:

- Using Network Profiles
- Using Software Collections
- Using Software Packages
- Selection Criteria
- Viewing Mobile Device Information
- Sending Messages
- Pinging the Client
- Setting a Workstation ID
- Mobile Device Properties
- Mobile Device Groups

Using Network Profiles

Network profiles allow you to download network parameters such as IP addresses, the ESS ID, and WEP encryption keys to the mobile device over a serial or wireless connection.

NOTE By default, the Avalanche Manager Agent can initially download network profile settings by using a serial connection. See *Configuring a Network Profile* on page 91 for additional options. When you allow the Agent to overwrite manual settings on the device, additional restrictions will apply to the downloading of IP addresses.

NOTE To overwrite network profile settings on the mobile device over a wireless connection, the mobile device must be previously assigned a valid ESS ID and WEP key.

You can create selection criteria for a network profile that determines which mobile devices can receive the settings contained in the profile. See *Selection Criteria* on page 122 for more information about selection criteria.

When you double-click a network profile branch in the Tree View, the List View shows all the mobile devices eligible to receive settings contained in the profile, based upon the selection criteria of the profile.

You can create multiple network profiles, if desired. Each profile is disabled by default. If you enable multiple profiles, the Avalanche Manager Agent uses selection criteria to determine which network profile is used to download IP addresses, WEP keys, and network parameters. See *Selection Criteria* on page 122 for more information.

The topics in this section include:

- Adding a Network Profile
- Configuring a Network Profile
- Assigning IP Addresses
- Configuring Network Routing Parameters
- Using WEP Encryption
- Network Profile Epochs
- Applying Restrictions on the Download Medium
- Setting the Default Profile
- Enabling a Network Profile
- Deleting a Network Profile
- Renaming a Network Profile

Adding a Network Profile

You can create network profiles using the Tree View. Before you create a network profile, you must first be connected to an Agent.

To add a Network Profile:

1. Right-click the network profiles branch and select `New Network Profile`.

2. Type the name for the new network profile in the text box provided.

3. Click `OK`.

Configuring a Network Profile

The Avalanche Manager allows you to configure IP address assignment, WEP encryption keys, and other network parameters that will download to the mobile device.

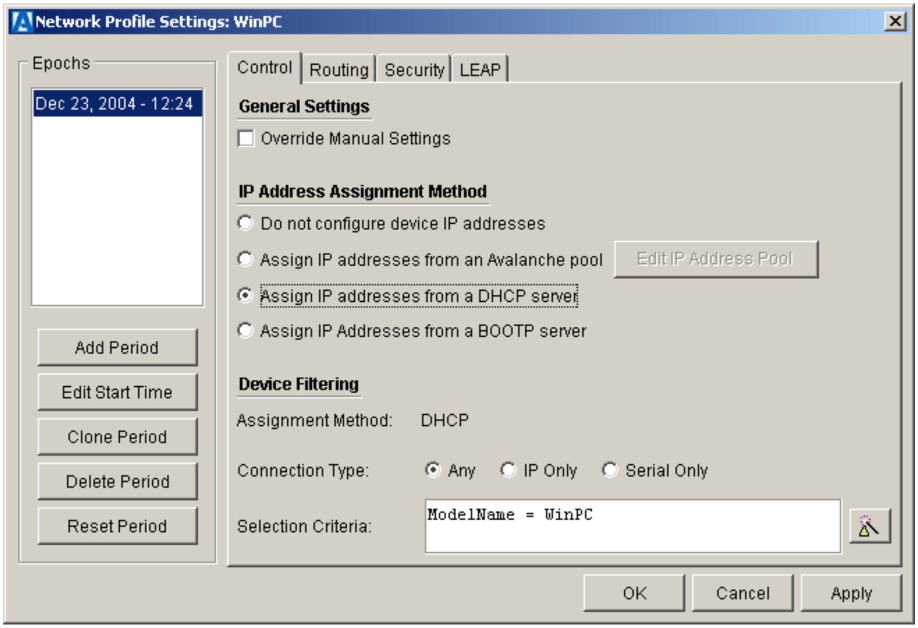
Before the settings configured in the network profile will download to the mobile devices, the profile must be activated. To activate the profile, right-click the profile and select `Enable Network Profile`.

The next time the Enabler activates, network profile settings download to the mobile device as part of the software update. The Avalanche Manager can download the ESS ID, its own IP address, the netmask, the router address, and DNS settings using either a serial or wireless connection. Before the Avalanche Manager can effect a wireless download, however, a mobile device must be configured with a valid ESS ID and WEP encryption key, if WEP is enabled on the wireless network.

To configure a network profile:

1. In the Tree View of the Management Console, right-click on the newly created network profile and choose `Settings`.

   The *Network Profile Settings* dialog box appears.



Dec 23, 2004 - 12:24

General Settings

□ Override Manual Settings

IP Address Assignment Method

○ Do not configure device IP addresses

○ Assign IP addresses from an Avalanche pool

● Assign IP addresses from a DHCP server

○ Assign IP Addresses from a BOOTP server

Device Filtering

Assignment Method: DHCP

Connection Type: ● Any ○ IP Only ○ Serial Only

Selection Criteria: `ModelName = WinPC`

Figure 5-1. *Network Profile Settings Dialog Box*

2 If you want the network profile settings, including the IP address, WEP keys, and other network parameters, to override manually set options on the mobile device, enable the **Override Manual Settings** checkbox. The settings for the appropriate network profile will download to the mobile device over serial or wireless connections.

NOTE This feature is most valuable if you need to manually configure devices for temporary use in another facility.

3 To configure IP address assignment, select an option in the **IP Address Assignment** section and see *Assigning IP Addresses* on page 93 for more information.

4 If your mobile devices move from one subnet to another, you can take advantage of MAC-level IP address assignment. With MAC-level IP address assignment, the mobile device will use a MAC-level broadcast to receive its IP address.

To implement MAC-level IP address assignment, one or both of the following conditions must be met:

- The IP address associating the mobile device to an Avalanche Manager Agent must be empty.
- The IP address manually set on the mobile device is none.

5 To configure miscellaneous network parameters including the ESS ID, select the **Routing** tab and see *Configuring Network Routing Parameters* on page 99 for more information.

6 To configure WEP encryption, select the **Security** tab and see *Using WEP Encryption* on page 103.

7 To determine the set of mobile devices for which the network profile is valid, select the Control tab and see *Selection Criteria* on page 122

8 To determine whether the settings in the profile can download over a wireless or serial connection, see *Applying Restrictions on the Download Medium* on page 107.

9 Once you have entered all desired options, click `OK` to accept the changes.

You can expand the network profiles branch in the Tree View to view the new network profile. Information about the profile appears beneath the branch.

Assigning IP Addresses

You can configure the network profile to use DHCP, BOOTP, or an IP address pool to manage IP address assignment on the mobile devices.

Although Avalanche fully supports BOOTP and DHCP, you obtain several advantages by using an IP address pool versus other methods:

- The presence of a special server, a potential “weak link,” is not required. If a BOOTP or DHCP server goes down, then all clients who use it become inoperable when the lease expires.
- IP address pools allow you to configure networking parameters using the Management Console. As a result, you can set up an entire site without manually modifying individual mobile devices.

- IP address pools simplify the management of IP addresses. Simplicity is critical if IP addresses are used for selection criteria. See *Selection Criteria* on page 122 for more information.

NOTE To overwrite network profile settings on the mobile device over a wireless connection, the mobile device must be previously configured with a valid ESS ID and, if WEP encryption is in use, a valid WEP key.

If you enable multiple profiles, the Avalanche Manager Agent applies the network profile settings based on which profile contains the IP settings that most closely match the current IP assignment on the connecting device. If no IP settings match, the Agent applies the settings in the default network profile. Only one profile can be assigned the default status. Once the Avalanche Manager Agent associates a network profile to a connecting device, all other settings such as WEP key encryption and ESS ID will download from this single profile.

For example, assume that there are three network profiles, A, B, and C. Network profile A is the default profile and uses an IP address pool. Network profile B also uses an IP address pool, but with a different IP address range. Network profile C uses DHCP.

In this case, when a mobile device connects to the Agent, it will download settings from a specific network profile based on the following criteria:

- If the mobile device is configured to use DHCP, it will download all settings from profile C only, because it is configured to use DHCP.

- If the mobile device has an IP address that matches an IP address in the configured IP address range for profile A, it will download all settings from profile A.

- If the mobile device has an IP address that matches an IP address in the configured IP address range for profile B, it will download all settings from profile B.

- If the mobile device has an IP address that does not match any IP addresses in the configured ranges for profile A or B, it will download all settings from profile A, including an IP address from the pool, because it is designated as the default profile.

For more information about IP assignment methods, see the following topics:

- Using an IP Address Pool
- Using DHCP
- Using BOOTP

Using an IP Address Pool

IP pooling uses configured IP ranges to assign an IP Address to a mobile device.

You can also use the IP address pool to pre-assign mobile devices to specific IP addresses based on the MAC address.

To add an IP address pool:

1 Right-click on a network profile in the Tree View and select `Settings`.

The *Network Profile Settings* dialog box appears (see Figure 5-1).

2 If you want the network profile settings, including the IP address, WEP keys, and other network parameters, to override manually set options on the mobile device, enable the **Override Manual Settings** checkbox. The settings for the appropriate network profile will download to the mobile device over serial or wireless connections. See *Using Network Profiles* on page 89 for more information.

NOTE This feature is most valuable if you need to manually configure devices for temporary use in another facility.

3 If your mobile devices move from one subnet to another, you can take advantage of MAC-level IP address assignment. With MAC-level IP address assignment, the mobile device will use a MAC-level broadcast to receive its IP address.

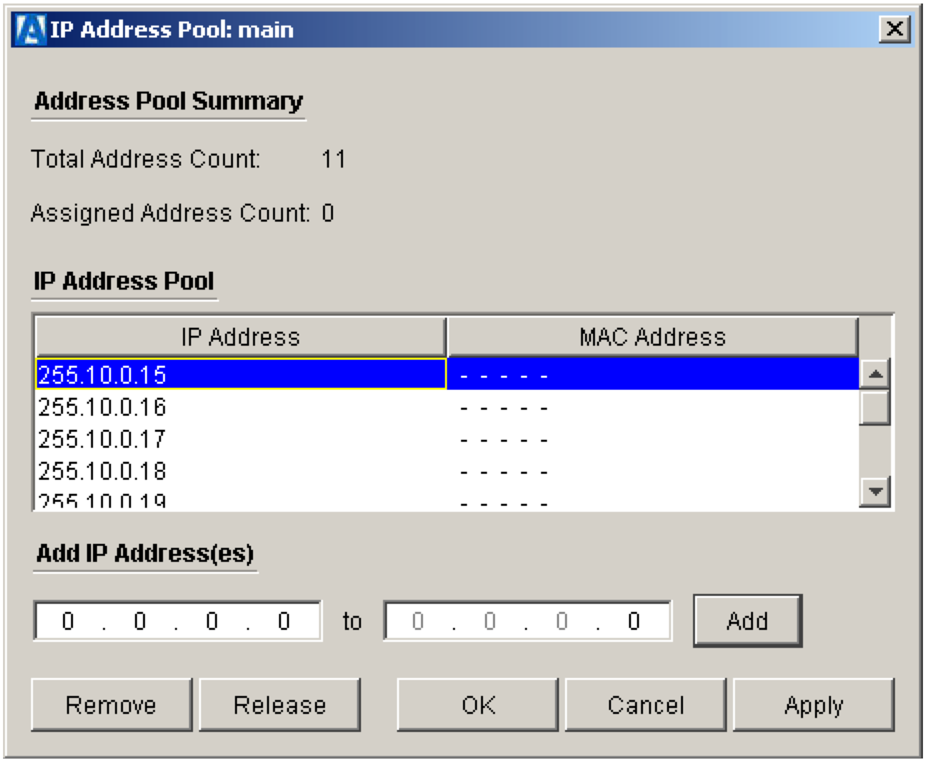
To implement MAC-level IP address assignment, one or more of the following conditions must be met:

- The IP address associating the mobile device to an Avalanche Manager Agent must be empty
- The IP address manually set on the mobile device is none
- The MAC address is pre-assigned to an IP address

4 In the Control tab of the *Network Profile Settings* dialog box, select the **Assign IP Addresses from an Avalanche Pool** option in the **Client IP Address Assignment** group box .

5 Click `Edit IP Address Pool`.

The *IP Address Pool* dialog box, shown in Figure 5-2, appears.



IP Address Pool: main

Address Pool Summary

Total Address Count: 11

Assigned Address Count: 0

IP Address Pool

IP Address	MAC Address
255.10.0.15	- - - - -
255.10.0.16	- - - - -
255.10.0.17	- - - - -
255.10.0.18	- - - - -
255.10.0.19	- - - - -

Add IP Address(es)

0 . 0 . 0 . 0 to 0 . 0 . 0 . 0

Figure 5-2. *IP Address Pool Dialog Box*

6 In the *IP Address Pool* dialog box, click `Add` to add a single IP address or a range. You can specify a range of IP addresses by providing the first address in the left field and the last address in the right field.

7 Repeat the preceding steps for any additional IP addresses or ranges that you want to add.

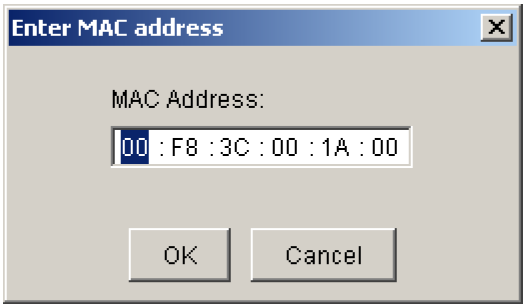
8 Click `OK`.

9 In the *Network Profile Settings* dialog box, click `OK`.

To associate an IP address to a MAC address:

1 In the *IP Address Pool* dialog box, double click the MAC address field in the row for the desired IP address.

The *Enter MAC Address* dialog box appears.



Enter MAC address

MAC Address:

00 : F8 : 3C : 00 : 1A : 00

Figure 5-3. *The Enter MAC Address Dialog Box*

2 Type the MAC address that you want to associate with the IP address.

3 Click `OK`.

When a mobile device with the specified MAC address associates with the Avalanche Manager, it will receive the corresponding IP address.

To remove an IP address from the IP address pool:

1 In the *IP Address Pool* dialog box, select one or more IP addresses from the list.

To select multiple IP addresses before you remove them:

- Press and hold the `Ctrl` key and click on specific non-contiguous IP address entries.
- Press on the first entry and then hold the `Shift` key and click on the last entry of a contiguous block of IP addresses.

2 Click `Remove`.

3 To save the changes, click `OK` or `Apply`.

To release an IP address from a mobile device:

1 In the *IP Address Pool* dialog box, select one or more IP addresses from the list.

To select multiple IP addresses before you release them:

- Press and hold the `Ctrl` key and click on specific non-contiguous IP address entries.
- Press on the first entry and then hold the `Shift` key and click on the last entry of a contiguous block of IP addresses.

2 Click `Release`.

The MAC addresses associated with any IP addresses you released return to a default value, `00-00-00-00-00-00`. The MAC addresses appear in the **MAC Address** column.

3 To save the changes, click `OK` or `Apply`.

If the network profile is active, all mobile devices with IP addresses slated for release will be re-assigned new IP addresses from the pool the next time the Enabler on the device activates.

Using DHCP

You can set the network profile to use DHCP for IP address assignment.

To use DHCP for IP address assignment:

1 Right-click on a network profile in the Tree View and select `Settings`.

The *Network Profile Settings* dialog box appears (see Figure 5-1).

2 In Control tab of the *Network Profile Settings* dialog box, select the **Assign IP addresses from a DHCP Server** option in the **Client IP Assignment** group box.

3 Click `OK`.

Using BOOTP

You can set the network profile to use BOOTP for IP address assignment.

To use BOOTP for IP address assignment:

1 Right-click on a network profile in the Tree View and select `Settings`.

The *Network Profile Settings* dialog box appears (see Figure 5-1).

2 In Control tab of the *Network Profile Settings* dialog box, select the **Assign IP Addresses from a BOOTP Server** option in the **Client IP Assignment** list.

3 Click `OK`.

Configuring Network Routing Parameters

The Avalanche Manager allows you to configure the ESS ID and IP routing parameters as needed.

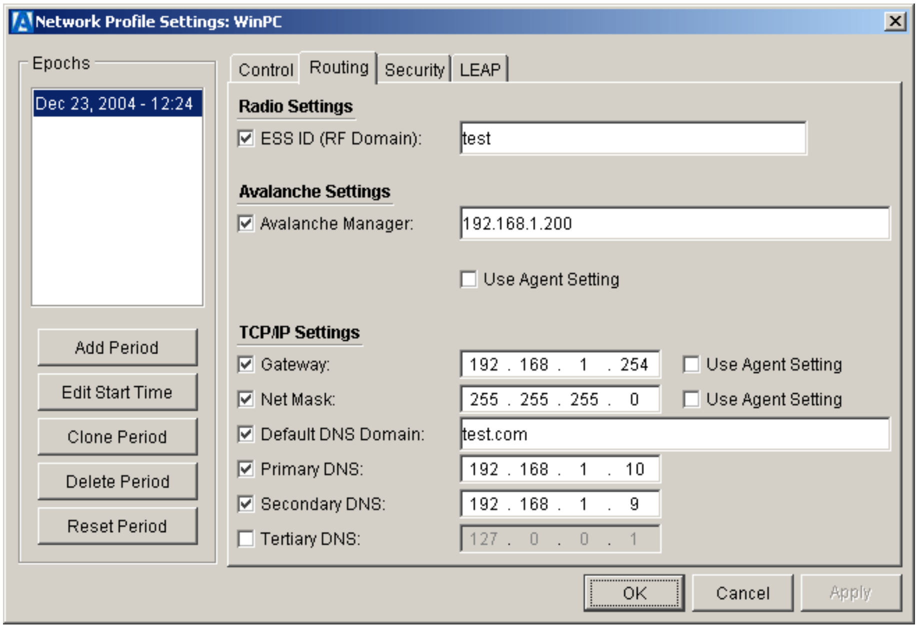
To configure the ESS ID and IP routing parameters:

1 In the Tree View of the Management Console, right-click on the newly created network profile and choose `Settings`.

The *Network Profile Settings* dialog box appears.

2 Select the **Routing** tab.

The following dialog box appears.


Network Profile Settings: WinPC

Epochs
Dec 23, 2004 - 12:24

Radio Settings
☑ ESS ID (RF Domain): test

Avalanche Settings
☑ Avalanche Manager: 192.168.1.200
□ Use Agent Setting

TCP/IP Settings
☑ Gateway: 192 . 168 . 1 . 254 □ Use Agent Setting
☑ Net Mask: 255 . 255 . 255 . 0 □ Use Agent Setting
☑ Default DNS Domain: test.com
☑ Primary DNS: 192 . 168 . 1 . 10
☑ Secondary DNS: 192 . 168 . 1 . 9
□ Tertiary DNS: 127 . 0 . 0 . 1

Figure 5-4. *The Routing Tab of the Network Profile Settings Dialog Box*

3 Configure miscellaneous network parameters, as needed.

To modify any or all of these parameters, activate the desired option by enabling the check box to its left.

NOTE You can set a blank value for any desired parameter. At the next update, this erases the corresponding value for the parameter on the mobile device.

---

4 Once you have entered all desired options, click `OK` to accept the changes.

5 To return settings to the default values, click `Default`.

The options you can configure in this dialog box include:

ESS ID

The wireless network identifier. The ESS ID must match the ESS ID of any access points with which the mobile devices need to connect.

Avalanche Manager

The IP address where the Avalanche Manager Agent resides.

This option associates the mobile device to a specific Agent. When the Enabler activates on a mobile device, the device automatically connects to the Avalanche Manager Agent with which it is associated. If the device is not associated with any Agent (i.e., the parameter is blank on the device), the device sends a network broadcast and connects to the first Agent that responds to its broadcast.

By setting a blank value for this parameter, you can erase the corresponding value for this parameter on the mobile device (at the next update), thereby forcing the device to perform a network broadcast to find an Agent.

To use the IP address of the current Agent, enable the **Use Agent Setting** checkbox beneath the option.

Gateway

The router address.

To use the router address of the current Agent, enable the **Use Agent Setting** checkbox to the right of the option.+

Netmask

The subnet mask.

To use the subnet mask of the current Agent, enable the **Use Agent Setting** checkbox to the right of the option.

Default DNS Domain

The default DNS domain, for example, `wavelink.com`.

Primary DNS

The IP address of the primary DNS server.

Secondary DNS

The IP address of the secondary DNS server.

Tertiary DNS

The IP address of the tertiary DNS server.

Using LEAP

Cisco-Aironet radio card adapter support an additional protocol, called the Lightweight Extensible Authentication Protocol, or LEAP. This protocol, derived from EAP for use in 802.1x wireless networks, 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.

NOTE See your Cisco-Aironet access point documentation for detailed information on these options.

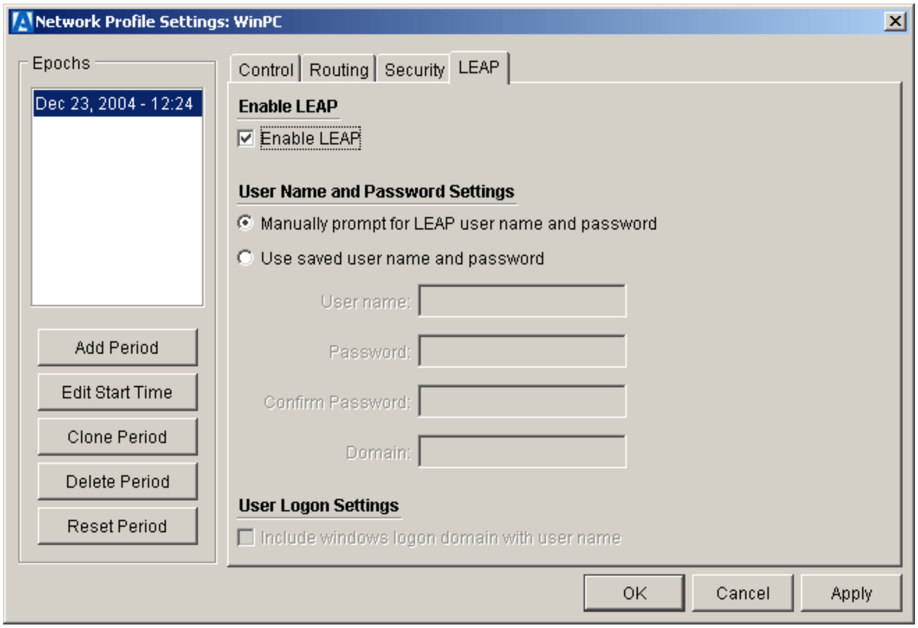
To configure LEAP settings:

1 In the Tree View of the Management Console, right-click on the newly created network profile and choose `Settings`.

The *Network Profile Settings* dialog box appears.

2 Select the **LEAP** tab.

The dialog box shown in Figure 5-5 appears.



Network Profile Settings: WinPC

Epochs

Dec 23, 2004 - 12:24

Enable LEAP

☑ Enable LEAP

User Name and Password Settings

● Manually prompt for LEAP user name and password

○ Use saved user name and password

User name:

Password:

Confirm Password:

Domain:

User Logon Settings

☐ Include windows logon domain with user name

Figure 5-5. *The LEAP Tab of the Network Profile Settings Dialog Box*

3 To activate LEAP for the network profile, enable the **Enable LEAP** checkbox.

4 If you want the mobile device user to manually enter a user name and password for authentication with the Radius server, verify that the **Manually prompt for LEAP user name and password** option is enabled.

NOTE For Windows CE devices, LEAP can be enabled, but—due to a hardware limitation—the user name and password cannot be downloaded to the mobile device.

---

5 If you want the client to automatically send a user name and password for authentication with the Radius server, enable the **Use saved user name and password** option, and type in authentication information in the following text boxes:

- **User name**. A valid user name on the Radius server.
- **Password**. The password associated with the user name.

- **Confirm Password**. The password associated with the user name.
- **Domain**. The Windows domain name.

If the Radius server requires that the domain name be included with the user name, enable the **Include Windows logon domain with user name** checkbox.

6 Once you have entered all desired options, click `OK` to accept the changes.

7 To return settings to the default values, click `Reset All`.

Using WEP Encryption

WEP, or Wired Equivalent Privacy, is a protocol for securing wireless network communications. You secure your wireless network by assigning a WEP key to mobile devices on the network. A WEP key encrypts transmissions on the wireless network. The Avalanche Manager supports both 40-bit and 128-bit encryption.

For more information about using WEP Encryption, see *Chapter 10: WEP Encryption* on page 195.

Network Profile Epochs

You can configure network profiles to contain multiple, independent groups of profile settings that will become active on the mobile device at a specified point in time and for a specified duration. These time-limited profile settings are called epochs.

By default, each network profile is configured with one epoch that begins at the current date and time. When you add additional epochs, you effectively create a multiplicity of network profile settings within a single profile, and you can manually change the network profile settings for each epoch. Only one of these epochs—the one that is valid for the current date and time—will be active on the mobile device at any time. Expired epochs and their associated settings are automatically deleted.

If the mobile device is running the Avalanche Enabler, version 3.0 or higher, all epochs for the network profile download to the mobile device during an update. The Enabler automatically changes the epoch settings at the appropriate time.

If the mobile device is running a version of the Avalanche Enabler prior to version 3.0, then only settings for the active epoch download to the mobile device during the next update. In this situation, the Agent periodically checks the network profile (every 15 minutes) to determine whether the settings have changed (that is, a new epoch has been activated with different settings). If the settings have changed, then the Agent flags the mobile device as in need of an update. Settings based on the new active epoch download to the mobile device at the next update.

A network profile can support up to ten epochs.

NOTE Before settings in a network profile download to the mobile device, the profile must be enabled. See *Enabling a Network Profile* on page 107 for information on enabling the network profile.

To add a network epoch:

1 In the Tree View of the Management Console, right-click on a network profile and choose `Settings`.

The *Network Profile Settings* dialog box appears. The default network epoch and any additional network epochs that you have configured appear on the left side of the dialog box.

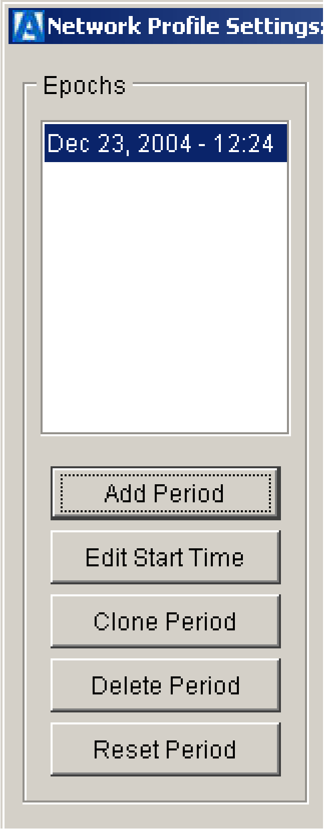
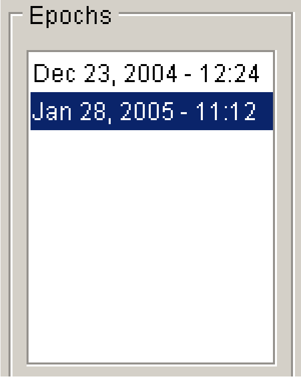


Figure 5-6. *Network Profile Settings Dialog Box*

2 Click `Add Period` or `Clone Period`.

When you click `Add Period`, a new epoch with default network profile settings is created. When you click `Clone Period`, a new epoch with network profile settings based on the current epoch is created.

The new network epoch appears in the Epochs text box of the dialog box, as shown in Figure 5-7.



Epochs

Dec 23, 2004 - 12:24

Jan 28, 2005 - 11:12

Figure 5-7. *Network Epochs*

3 Click the tab for the new network epoch.

4 In the Control tab, click the pop-up calendar button next to the **Period Start** text box.

5 In the pop-up calendar that appears, configure a start date and time.

6 Click `OK`.

7 Click `Apply`.

The network epoch tab is updated to show the new start date and time.

8 To configure network profile settings for the new epoch, select the different tabs in the profile and configure desired settings.

9 Click `OK`.

To remove a network epoch:

1 In the *Network Profiles* dialog box, select the tab for the epoch that you want to delete.

2 Click `Delete Period`.

To reset a network epoch to its default network profile settings:

1 In the *Network Profiles* dialog box, select the tab for the epoch that you want to reset.

2 Click `Reset Period`.

Applying Restrictions on the Download Medium

You can configure network profiles to allow wireless downloads, serial downloads, or both. By default, the profile will allow the use of either synchronization medium.

NOTE A licensed authorization is required to perform wireless downloads.

To set the download medium for the network profile:

1 Right-click on the network profile and select `Settings`.

2 In the *Network Profile Settings* dialog box, select the Control tab.

3 Set the desired synchronization option in the **Device Filtering** section.

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

NOTE IrDA connections are treated as serial connections.

4 Click `OK`.

Setting the Default Profile

Only one network profile can be designated as the default profile. See *Assigning IP Addresses* on page 93 for more information about default network profiles.

You can designate a network profile as the default profile by right-clicking on the profile in the Tree View and selecting `Set as Default Profile`.

Enabling a Network Profile

Configuration settings contained in a network profile will not download to mobile devices unless the profile has been enabled.

To enable a network profile, right-click on the profile in the Tree View and select `Enable Network Profile`.

Deleting a Network Profile

To delete a network profile from the Avalanche Manager, right-click on the profile in the Tree View and select `Delete Network Profile`.

Renaming a Network Profile

To rename a network profile, right-click on the profile in the Tree View and select `Rename Network Profile`. Enter the new name of the profile in the dialog box that appears and click `OK`.

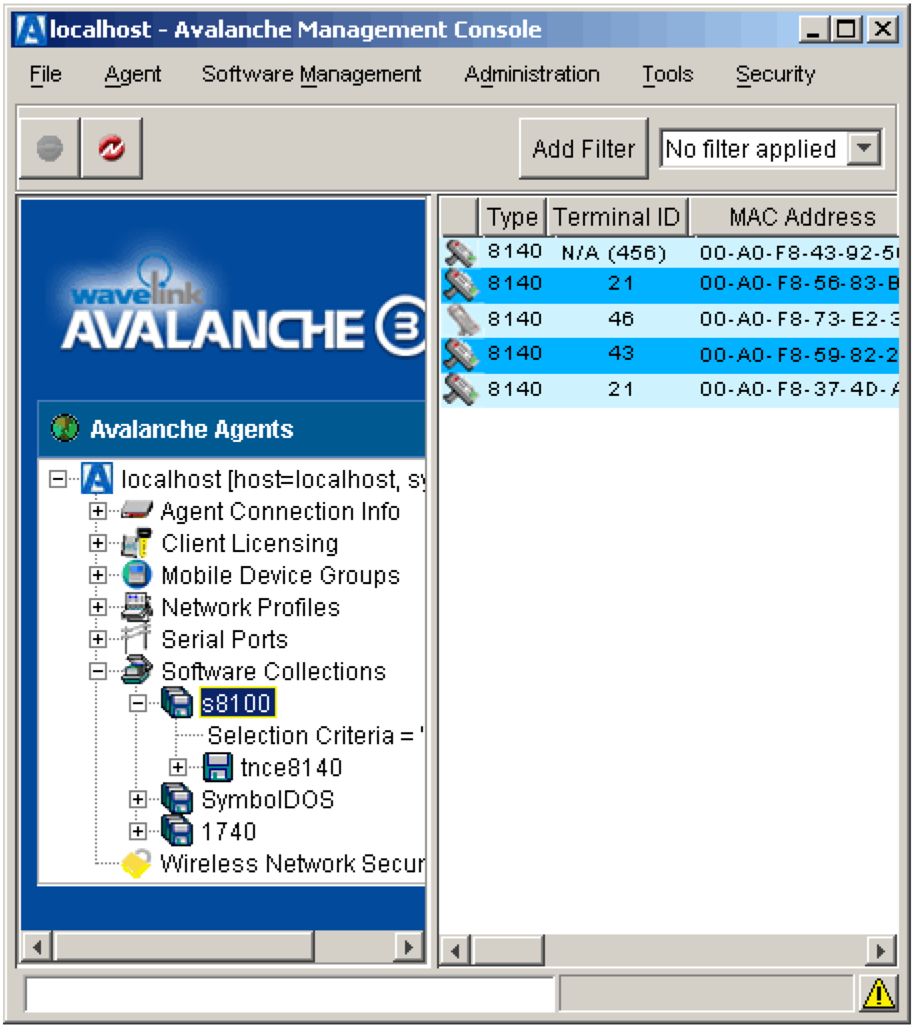
Using Software Collections

A software collection contains one or more software packages. You can configure software collections to restrict the use of the packages they contain to certain mobile devices. These restrictions, called selection criteria, can be based upon device types, IP addresses, or MAC addresses.

The selection criteria specifies the conditions that need to be met for the software package in the software collection to download to a mobile device. By default, software collections do not have any selection criteria configured. In this case, any mobile device can receive those packages. However, the packages themselves typically provide built-in selection criteria.

See *Selection Criteria* on page 122 for more information about selection criteria.

When you double-click a software collection branch in the Tree View, all the software packages associated with that collection appear beneath the branch. In addition, when you click on a software collection, the List View shows all the mobile devices eligible to receive software packages from the collection, based upon the selection criteria of the software collection only.



Type	Terminal ID	MAC Address
8140	N/A (456)	00-A0-F8-43-92-5
8140	21	00-A0-F8-56-83-B
8140	46	00-A0-F8-73-E2-3
8140	43	00-A0-F8-59-82-2
8140	21	00-A0-F8-37-4D-A

Figure 5-8. *Software Collection*

For mobile devices to receive software from a software collection, the software collection must be enabled. Once enabled, you can later disable a software collection to suspend distribution of its packages.

Right-clicking on the software collection displays the software collection context menu (see Figure 5-9). This context menu allows the user to configure, enable or disable, rename, delete, or copy the collection.

NOTE You can control access to software collections by assigning authorization groups to the collection. See *Assigning an Authorization Group to a Collection* on page 177 for more information.

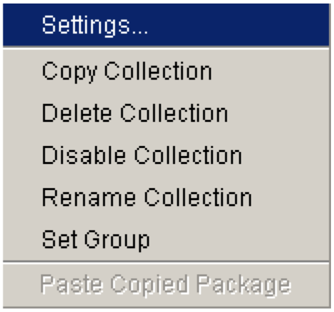


Figure 5-9. *Software Collection Context Menu*

The topics in this section include:

- Adding a Software Collection
- Configuring a Software Collection
- Activating a Software Collection
- Deleting a Software Collection
- Renaming a Software Collection

Adding a Software Collection

You can create software collections as needed.

To create a software collection:

1 In the Tree View, right-click on the **Software Collections** branch and click `New Software Collection`.

2 In the dialog box that appears, type in the desired name for the collection.

3 Click `OK`.

To configure the new collection, see *Configuring a Software Collection*.

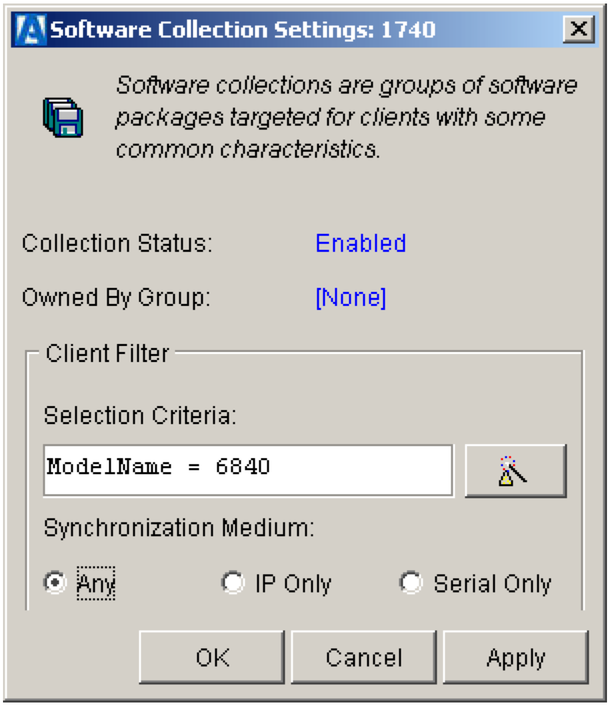
Configuring a Software Collection

You can configure a software collection with selection criteria to limit the distribution of the software packages contained in the collection. In addition, you can configure a collection to allow only serial downloads, wireless downloads, or both.

To configure a software collection:

1 Right-click on the software collection to be configured and select `Settings`.

The dialog box shown in Figure 5-10 appears.



Software Collection Settings: 1740

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

Collection Status: Enabled

Owned By Group: [None]

Client Filter

Selection Criteria:

ModelName = 6840

Synchronization Medium:

● Any ○ IP Only ○ Serial Only

Figure 5-10. *Software Collection Settings Dialog Box*

2 If you want to add selection criteria to the collection, click the **Selection Criteria Builder** button icon or type the appropriate selection criteria for the software collection.

See *Selection Criteria* on page 122 to build the selection criteria string using the selection criteria builder.

3 Select an option in the Synchronization Medium group box to set restrictions on the download medium.

See *Applying Restrictions on the Download Medium* on page 112 for more information.

4 When you are finished configuring the collection, click `OK`.

Applying Restrictions on the Download Medium

You can configure software collections to allow wireless downloads, serial downloads, or both. By default, the software collection will allow the use of either synchronization medium.

NOTE A licensed authorization is required to perform wireless downloads.

To set the download medium for the collection:

1 Right-click on the software collection and select `Settings`.

The dialog box shown in Figure 5-10 appears.

2 Set the desired synchronization medium option.

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

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

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

NOTE IrDA connections are treated as serial connections.

3 Click `OK`.

Activating a Software Collection

To activate a software collection, right-click on the desired collection in the Tree View and select `Enable Collection`.

Deleting a Software Collection

To delete a software collection from the Avalanche Manager, right-click on the profile in the Tree View and select `Delete Collection`.

NOTE Before a software collection can be deleted, all of the packages within that collection must be deleted.

Renaming a Software Collection

To rename a software collection, right-click on the profile in the Tree View and select `Rename Collection`. Enter the new name of the collection in the dialog box that appears and click `OK`.

Using Software Packages

Software packages represent Wavelink application clients (for example, Telnet Clients) or third party Avalanche-enabled packages that run in the mobile devices. Most packages restrict themselves to the appropriate mobile device type, based upon the selection criteria used at the time the package was created.

A software package consists of an application and its required support files. Software packages can be one of the following three package types:

Application packages These package types are added to the **Application** menu in the mobile device.

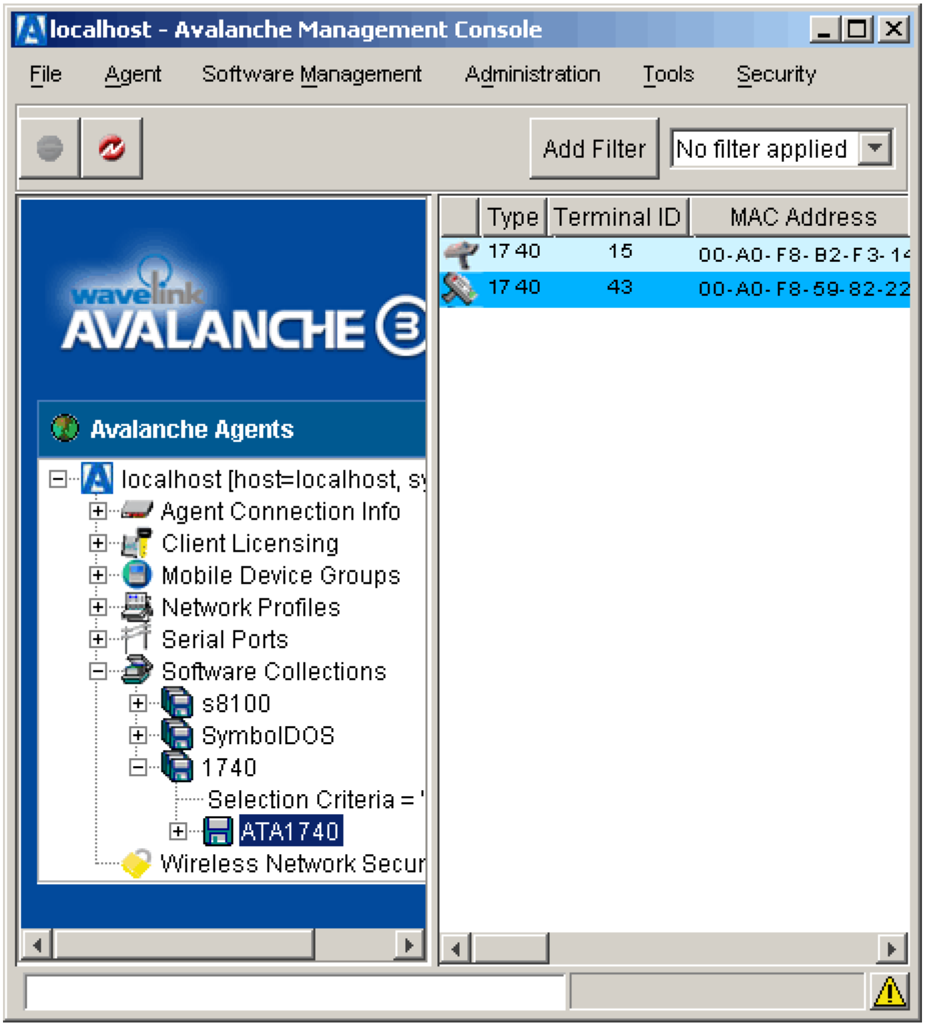
Support packages These package types contain updates to existing software packages or to the Avalanche Enabler. Support packages do not appear as new items under the **Application** menu of the mobile device. The Ava3 DHCP update software package, which was previously needed for Symbol 3000 mobile devices, is an example of a support package.

Auto packages

These package types automatically execute following a successful download. Like the support packages, auto packages do not modify the **Application** menu. RF firmware upgrade packages are examples of auto packages.

When you double-click on a software package in the Tree View, information associated with the package appears beneath the package. The name of the package, vendor name, selection criteria, package type, version, file count, and status of the software package appears beneath the package (see Figure 5-11). The selection criteria determines the mobile device type or types that the software package will service. For example, a PDT 8140 software package will automatically prevent itself from downloading to a 7200 Series device.

All mobile devices that meet the selection criteria of the software collection and the software package appear in the List View when you click on the package in the Tree View.



	Type	Terminal ID	MAC Address
	1740	15	00-A0-F8-B2-F3-14
	1740	43	00-A0-F8-59-82-22

Figure 5-11. *Software Package - TNCE8140*

In order for a software package to download to mobile devices, it must be enabled. In addition, the software collection that contains the package must also be enabled.

Right-click on the software package and its context menu appears (Figure 5-12). This menu provides the ability to configure, enable/disable, delete, and copy software packages. Advanced access is required to perform each of these functions. The **Configure Package** menu option is enabled when configuration utilities are available for the software package.

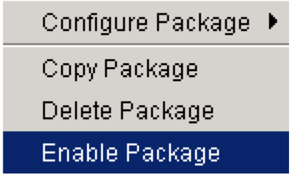


Figure 5-12. *Software Package Context Menu*

The topics in this section include:

- Activating a Software Package
- Copying a Software Package
- Deleting a Software Package
- Running Plug-In Utilities with Avalanche

Activating a Software Package

Before a software package can download to mobile devices, if must first be enabled.

To enable a software package, right-click on the desired package in the Tree View and select `Enable Package`.

Copying a Software Package

You can copy software packages into other software collections. This provides you with the ability to configure packages differently and download the packages to different sets of mobile devices. In this case, the selection criteria for each software collection will determine which devices receive the software package.

To copy a software package into another software collection:

1. Right-click on the package you want to copy and select `Copy Package`.
2. Right-click on the software collection into which you want to copy the package and select `Paste Copied Package`.

A message box showing the progress of the file transfer appears while the software package is copied into the software collection.

Deleting a Software Package

You can delete software packages from the Management Console, or you can delete unwanted or unneeded packages from the mobile device.

Deleting Software Packages from the Management Console

To delete a software package from the Management Console, right-click the software package in the Tree View of the Management Console and click `Delete Package`.

The deleted package will no longer appear in the Tree View of the console. If you delete a software package and the package resides on any mobile devices, that package receives an orphaned status. See *Deleting Software Packages from Mobile Devices* for more information.

Deleting Software Packages from Mobile Devices

To provide effective maintenance of software packages, the Management Console includes clean-up methods that delete unwanted packages from mobile devices.

The Avalanche Manager will only delete packages that are designated as orphaned packages. Orphaned packages are packages that are installed on a mobile device but not active in the Avalanche Manager Agent. Packages will receive an orphaned status in the following cases:

- If you disable or delete the package after it downloads to a mobile device.
- If you connect a mobile device containing older packages that were previously associated with a different Avalanche Manager. The older packages will display an orphaned status.

The Management Console includes the following clean-up options:

- Deleting specific orphaned packages from a specific mobile device.
- Globally deleting *all* orphaned packages from mobile devices. This applies to all mobile devices associated with the current Avalanche Manager Agent.

To delete an orphaned software package from a specific mobile device:

1 Locate the software package you want to delete in the Tree View of the Management Console.

2 Right-click on the software package icon and select `Disable Package`.

3 If you want to verify the new status, double-click the software package.

   Information about the software package appears beneath the package in the Tree View. The status of the package is now `On Hold`.

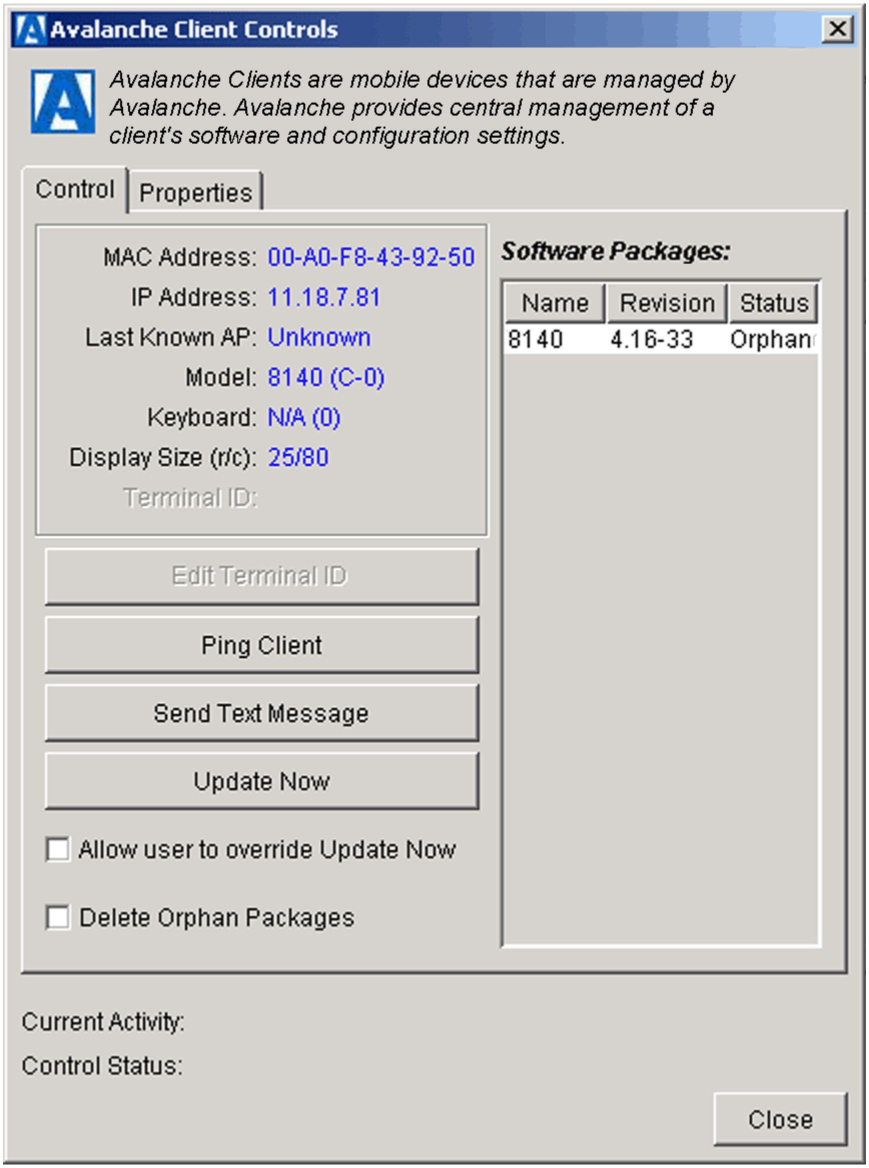
4 Right-click on the mobile device within the List View and select `Client Settings`. The *Avalanche Client Controls* dialog box appears as shown in Figure 5-13.

   The status of the software package that you disabled will appear in the **Software Packages** list as `Orphaned`.

5 Enable the **Delete Orphaned Packages** checkbox and click `Close`.

6 Initiate the removal of the orphaned software packages by activating the Enabler on the mobile device.

   For DOS devices, the Enabler activates whenever a device reboots (warm or cold boot).



Avalanche Clients are mobile devices that are managed by Avalanche. Avalanche provides central management of a client's software and configuration settings.

MAC Address: 00-A0-F8-43-92-50

IP Address: 11.18.7.81

Last Known AP: Unknown

Model: 8140 (C-0)

Keyboard: N/A (0)

Display Size (r/c): 25/80

Terminal ID:

□ Allow user to override Update Now

□ Delete Orphan Packages

Software Packages:

Name	Revision	Status
8140	4.16-33	Orphan

Current Activity:

Control Status:

Figure 5-13. *Avalanche Client Controls Dialog Box*

To delete ALL orphaned software packages from the mobile device:

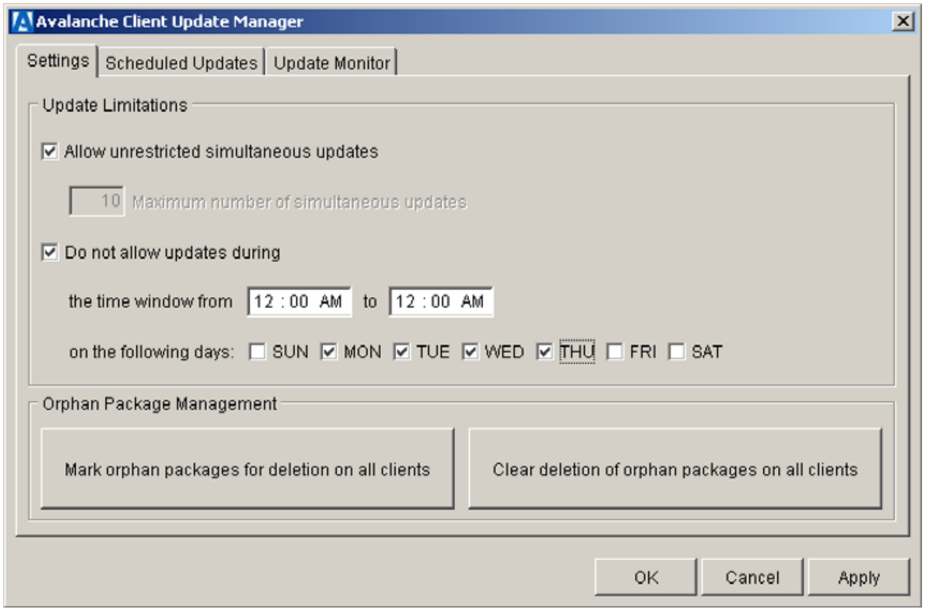
NOTE This function deletes all disabled software packages within all mobile devices associated with the current Avalanche Manager.

---

1 Verify that the configuration on the Management Console matches what you expect for each client.

To verify the configuration, double-click each mobile device in the List View and check the list of current packages in the *Avalanche Client Controls* dialog box. Those packages that the mobile device has which are not active in the Avalanche Manager Agent are marked as `Orphaned`.

2 Select `Client Update Controls` from the **Tools** menu. The dialog box shown in Figure 5-14 appears.



Avalanche Client Update Manager

Update Limitations

☑ Allow unrestricted simultaneous updates

10 Maximum number of simultaneous updates

☑ Do not allow updates during

the time window from 12 : 00 AM to 12 : 00 AM

on the following days: □ SUN ☑ MON ☑ TUE ☑ WED ☑ THU □ FRI □ SAT

Orphan Package Management

Settings
Scheduled Updates
Update Monitor
Mark orphan packages for deletion on all clients
Clear deletion of orphan packages on all clients
OK
Cancel
Apply

Figure 5-14. *Client Update Controls Dialog Box*

3 Click `Mark orphan packages for deletion on all clients.`

NOTE You can cancel the planned deletion of orphaned packages any time before the packages are actually deleted. To cancel a planned deletion, click `Clear deletion of orphaned packages on all clients`.

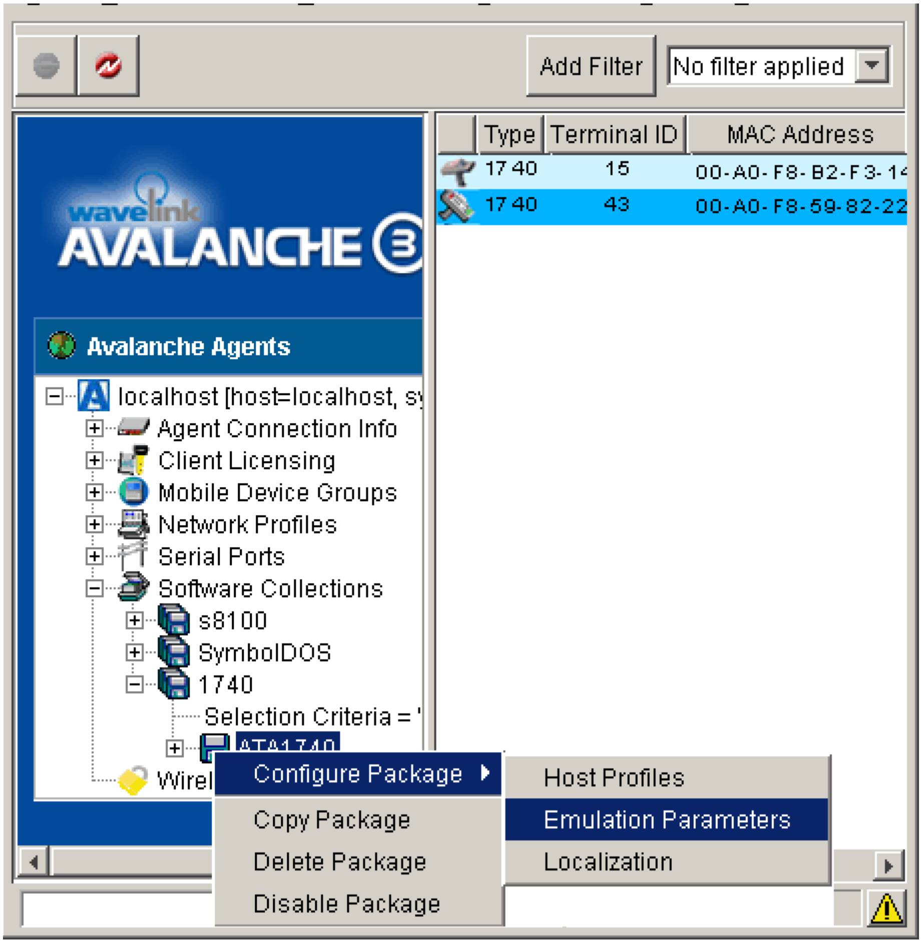
4 Click `Close`.

5 Initiate the removal of the orphaned software packages from all the mobile devices by activating their Enablers.

For DOS devices, the Enabler activates whenever a device reboots.

Running Plug-In Utilities with Avalanche

Avalanche has the capability to incorporate application plug-ins. These plug-ins are typically utilities used to configure the application. To access a plug-in utility in the Management Console, right-click on the software package that contains the desired application and choose `Configure Package`. The utilities (or plug-ins) included with the package are available in the context menu that appears. For example, a plug-in utility included with the Wavelink Avalanche TN Clients is the Emulation Parameters Configuration utility. Figure 5-15 shows how to access this utility in the Management Console.



Type	Terminal ID	MAC Address
1740	15	00-A0-F8-B2-F3-14
1740	43	00-A0-F8-59-82-22

Figure 5-15. *Accessing a Software Package Plug-In*

Selection Criteria

A set of rules called selection criteria, which you can apply to individual software collections and individual network profiles, define which mobile devices will receive designated updates. For a software collection, the selection criteria determines which mobile devices can receive the software packages contained in the collection. For a network profile, the selection criteria determines which mobile devices can receive the settings contained in the profile.

Additional selection criteria is typically associated with the software packages themselves, further restricting the distribution of the package, but package criteria is built-in to the package at the time of its creation.

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

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

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

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

To open the Selection Criteria Builder for a software collection:

1. In the Tree View, right-click on the software collection to be configured and select `Settings`.

   The dialog box shown in Figure 5-10 appears.

2. Click the **Selection Criteria Builder** icon.

   The dialog box shown in Figure 5-16 appears.

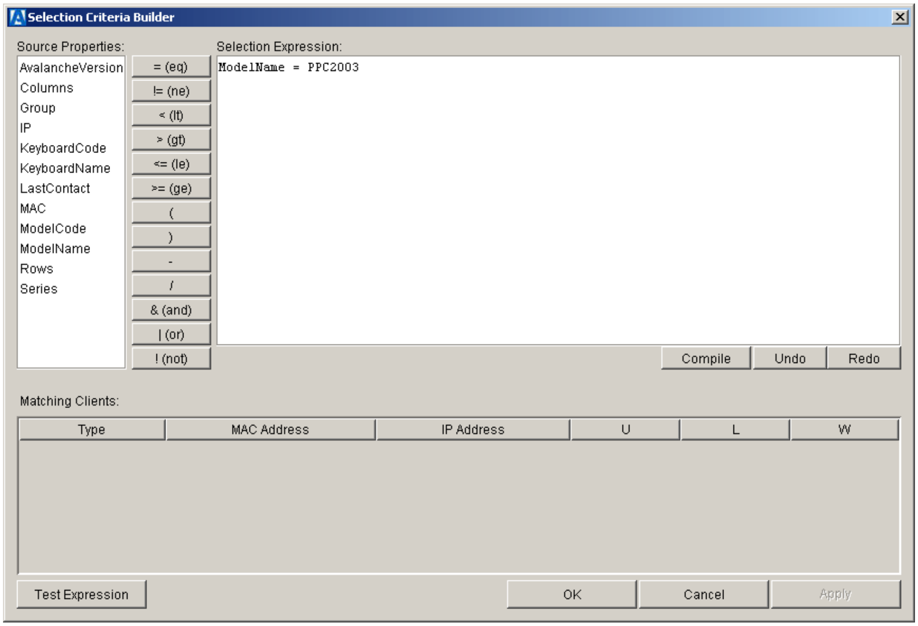
To open the Selection Criteria Builder for a network profile:

1. In the Tree View, right-click on the network profile to be configured and select `Settings`.

2. In the *Network Profile Settings* dialog box, select the **Control** tab.

3. Click the **Selection Criteria Builder** icon.

The dialog box shown in Figure 5-16 appears.



Selection Expression:

```
ModelName = PPC2003
```

Figure 5-16. *Selection Criteria Builder*

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. You may use any property that you have assigned a device as a selection criteria variable.

- 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 recommended 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 6840 to a `ModelName` variable by building the string, `ModelName = 6840`, then you will restrict packages or profiles to model 6840 mobile devices.

To build the selection criteria string:

1 Select and double-click a source property from the list of **Source Properites**.

When you double-click the source property, it will be added to the **Selection Expression** area.

NOTE For information about source properties, see *Selection Variables* on page 127.

---

2 Select one of the operator buttons.

When you select an operator, it will be added to the **Selection Expression** area and will be placed next to the last source property entered.

NOTE For information about operators, see *Operators* on page 132.

---

3 In the **Selection Expression** area, type a value for the source property that you selected.

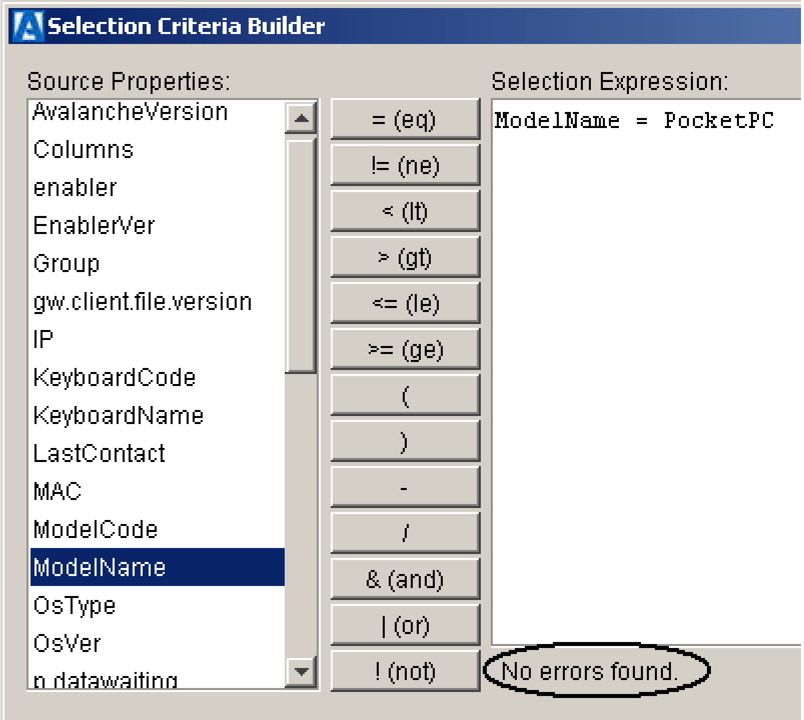
4 For each additional element you want to add to the selection criteria string, repeat the preceding steps.

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 `Compile`.

The Selection Criteria Builder will indicate whether the selection criteria expression contains any errors.



Selection Criteria Builder

Source Properties:

- AvalancheVersion
- Columns
- enabler
- EnablerVer
- Group
- gw.client.file.version
- IP
- KeyboardCode
- KeyboardName
- LastContact
- MAC
- ModelCode
- ModelName
- OsType
- OsVer
- p.datawaiting

Selection Expression:

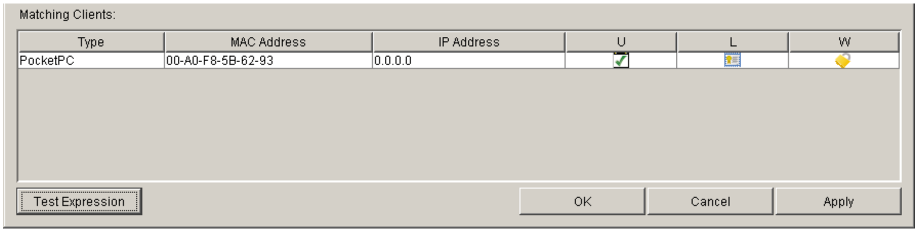
```
ModelName = PocketPC
```

No errors found.

Figure 5-17. *Selection Criteria Validation*

6 Click `Test Expression`.

Any clients that match the selection criteria will appear in the **Matching Clients** section of the *Selection Criteria Builder* dialog box.



Matching Clients:

Type	MAC Address	IP Address	U	L	W
PocketPC	00-A0-F8-5B-62-93	0.0.0.0	✓	▨	◆

Figure 5-18. *Selection Criteria Matching Clients*

7 Click `OK`.

For a software collection, the selection criteria string now appears in the *Software Collection Settings* dialog box (Fig. 5-10).

For a network profile, the selection criteria string now appears in the Filter tab of the *Network Profile Settings* dialog box.

Selection Variables

The selection criteria is based on the use of selection variables. In some cases, selection variables are mobile device properties, such as the Terminal ID.

You can place numbers and strings directly in the selection criteria string, with or without quotes.

NOTE Selection criteria strings are case sensitive.

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

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

The following Palm emulation selection criteria strings are valid:

```
Series = S
```

while the following is not:

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

Long strings are also supported as selection criteria. For example, the following string is valid:

```
Series = 3 | (MAC = 00-A0-F8-27-B5-7F | MAC = 00-A0-F8-80-3D-
4B | MAC = 00-A0-F8-76-B3-D8 | MAC = 00-A0-F8-38-11-83 | MAC
= 00-A0-F8-10-24-FF | MAC = 00-A0-F8-10-10-10)
```

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 example:

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

`ModelName`

The standard model name for a mobile 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 might appear in one of the views when the mobile device is selected

A few of the supported values include:

```
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, 7000CE, HHP7400, MX1, MX2, MX3,
VX1, iPAQ, iPAD, Falcon, ITCCK30,
ITC700
```

Example:

```
ModelName = 6840
```

`KeyboardName`

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

Supported values include:

```
35KEY
46KEY
101KEY
TnKeys
```

Example:

```
KeyboardName = 35KEY
```

`Series`

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

Supported values include:

`3` = DOS 3000 Series
`P` = DOS 4000 and 5000 Series
`7` = DOS 7000 Series
`T` = Telxon devices
`C` = CE devices
`S` = Palm devices
`W` = Windows machines
D = PSC and LXE DOS devices

Example:

```
Series = 3
```

`ModelCode`

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

Supported values include:

`1`= LRT 38xx/LDT
`2` = VRC39xx/69xx
`3` = PDT 31xx/35xx
`4` = WSS1000
`5` = PDT 6800
`6` = PDT 6100

Example:

```
ModelCode <= 2
```

This matches all 38xx, 39xx, and 69xx devices.

`KeyboardCode`

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

Supported values include:

`0` = 35-Key
`1` = More than 35 keys and WSS1000
`2` = Other devices with less than 35 keys

Example:

```
KeyboardCode = 0
```

`Rows`

The number of display rows the mobile device supports. The possible value range is 1 to 25.

Example:

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

This example matches all mobile devices with 20 rows, except those with 35-key keyboards.

`Columns`

The number of display columns the mobile device supports. The possible value range is 1 to 80.

Example:

```
Columns > 20
```

`Terminal ID`

The unique ID for the mobile device that the Avalanche Manager generates. The initial terminal ID is 1, and the values increment as needed.

Example:

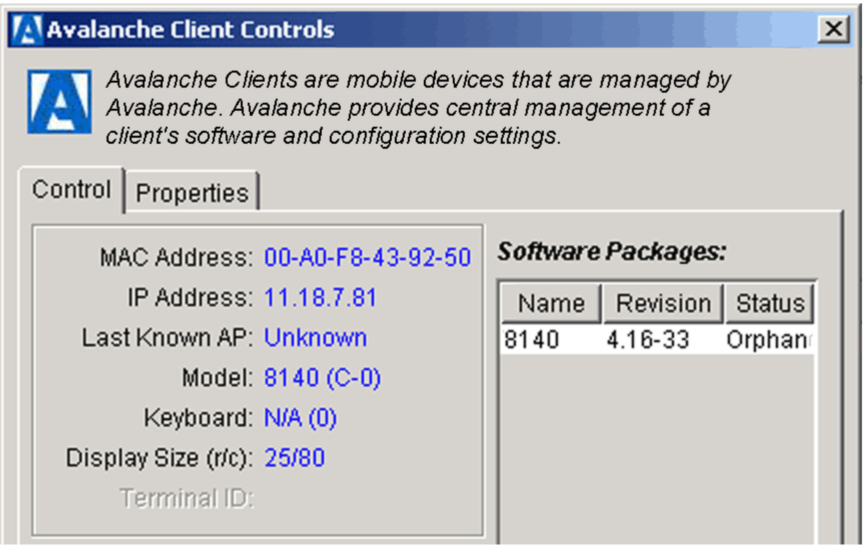
```
Terminal ID = 5
```

NOTE You can redefine terminal IDs for mobile devices as needed. If you are using terminal IDs in a workstation ID, the value must not exceed the character limit for the host. Typically, hosts support 10 characters.

Viewing Current Values for Selection Variables

You can view values for some selection variables for specific mobile devices in the *Avalanche Client Controls* dialog box. To view these values, double-click the device in the List View.

Fig 5-19 shows the MAC address, IP address, series, model, and keyboard values for a 8140 device. These correspond to the following selection variables: `MAC`, `IP`, `ModelName`, `Series`, `ModelCode`, and `KeyBoardCode`, respectively. These values are shown in the left portion of the dialog box.



Avalanche Client Controls

Avalanche Clients are mobile devices that are managed by Avalanche. Avalanche provides central management of a client's software and configuration settings.

MAC Address: 00-A0-F8-43-92-50
IP Address: 11.18.7.81
Last Known AP: Unknown
Model: 8140 (C-0)
Keyboard: N/A (0)
Display Size (r/c): 25/80
Terminal ID:

Software Packages:

Name	Revision	Status
8140	4.16-33	Orphan

Figure 5-19. *Example of Viewing Selection Variables*

You can view additional values for properties that function as selection variables by clicking the Properties tab. The properties that appear on this tab also appear in the Selection Criteria Builder wizard. See *Viewing Properties* on page 150 for more information.

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.

You may use the symbol of the operator (!, &,. |, etc.) in a selection criteria, or you may use the letter abbreviation (NOT, AND, OR, etc.). If you use the letter abbreviation for the operator, then you must format the letter abbreviation in all upper-case letters.

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

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

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

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

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

Example:

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

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

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

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

`EQ (=)` Binary operator that results in TRUE if the two expressions on either side of it are equivalent.

Example:

```
ModelName = 6840
```

`NE (!=)` Not equal to.

Example:

ModelName != 6840

In this example, the selection criteria targets all non-6840 mobile devices.

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

Example:

```
Rows > 20
```

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

Example:

```
Rows < 21
```

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

Example:

```
Rows >= 21
```

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

Example:

```
Rows <= 20
```

Operators use the following precedence:

1 Parenthesis

2 OR operator

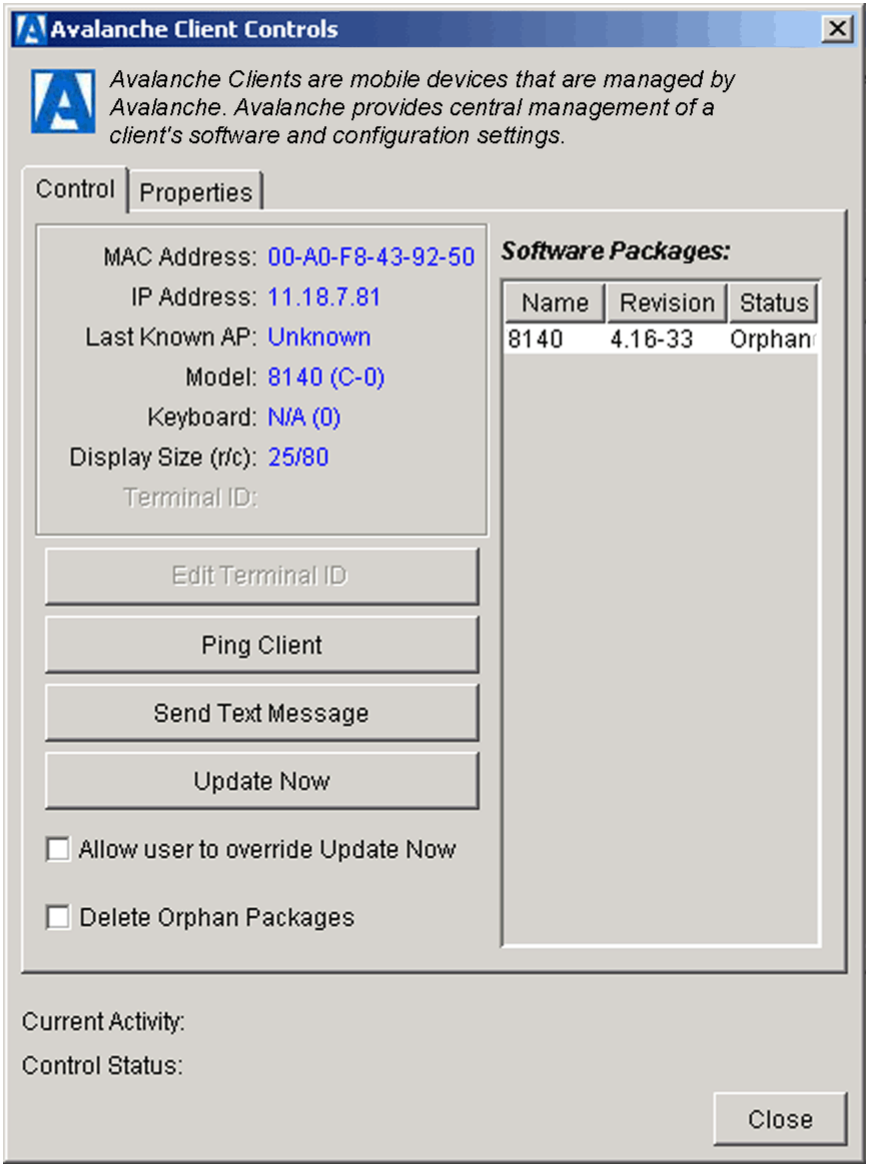
3 AND operator

4 NOT operator

5 All other operators

Viewing Mobile Device Information

To view information about a specific mobile device, double-click on the mobile device in the List View of the Management Console. The *Avalanche Client Controls* dialog box appears.



Avalanche Client Controls

Avalanche Clients are mobile devices that are managed by Avalanche. Avalanche provides central management of a client's software and configuration settings.

MAC Address: 00-A0-F8-43-92-50
IP Address: 11.18.7.81
Last Known AP: Unknown
Model: 8140 (C-0)
Keyboard: N/A (0)
Display Size (r/c): 25/80
Terminal ID:

Software Packages:

Name	Revision	Status
8140	4.16-33	Orphan

□ Allow user to override Update Now

□ Delete Orphan Packages

Current Activity:

Control Status:

Figure 5-20. *The Avalanche Client Controls Dialog Box*

The following information about the device is available in this dialog box:

- Detailed information about the mobile device, including the MAC address, IP address, the last access point associated with the mobile device, the device model name, the keyboard type, display size, and terminal ID.

- A list of the current packages installed on the mobile device with revision information and current status.

  The possible status for a package is `Install Pending`, `Update Pending`, `Delete Pending`, `Active`, or `Orphaned`. Orphaned packages are packages that are installed on a mobile device but not active in the Avalanche Manager Agent.

- Information showing the current activity or status of the mobile device. This is the same information provided under the **Activity** and **Detail** columns under the List View of the Management Console.

Sending Messages

You can use the Management Console to send a text-based message to clients that are currently in range and running the Avalanche Enabler, an Avalanche-enabled application or, in some cases, a configuration utility.

To send a message:

1 Double-click on a mobile device in the List View of the Management Console.

The *Avalanche Client Controls* dialog box, shown in Figure 5-20, appears.

2 Click `Send Text Message`.

The following dialog box appears.

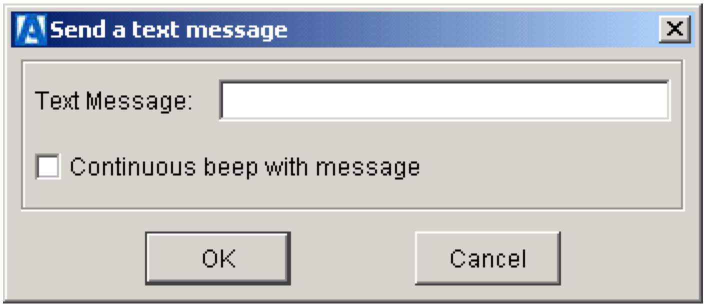


Figure 5-21. *The Send a Text Message Dialog Box*

3 Type a message in the **Text Message** text box.

4 If you want to send a continuous beep, enable the **Continuous Beep with Message** checkbox.

This option continues to send a beep until you tap or select `CLEAR` on the mobile device.

5 Click `OK` to send the message.

NOTE The **Control Status** field on the bottom of the window allows you to monitor the status of the control feature currently in use.

Pinging the Client

You can use the Management Console to ping clients that are currently in range and running the Avalanche Enabler, an Avalanche-enabled application, or in some cases a configuration utility. This is not an "ICMP"-level ping, but rather an application-level status check. This feature indicates whether the mobile device is active or not.

To ping the client:

1 Double-click on a mobile device in the List View of the Management Console.

The *Avalanche Client Controls* dialog box, shown in Figure 5-20, appears.

2 Click `Ping Client`.

The **Control Status** field on the bottom of the window allows you to monitor the status of the ping request.

Setting a Workstation ID

This feature allows the user to define a unique identifier that Avalanche Manager associates with a mobile device. Workstation IDs are supported only in TN5250 environments.

You can configure the workstation ID in two different ways:

- Manual entry of the workstation ID into a mobile device.

  If you want to manually assign a workstation ID, see the appropriate Wavelink Avalanche TN Client documentation.

NOTE To implement workstation IDs, see the Wavelink Avalanche TN Client documentation for configuring host profiles.

- Automated configuration through the Avalanche Management Console. Using automated configuration, you can download workstation IDs to the mobile device through wireless or serial connections.

  One method of automated configuration relies on a feature in the Avalanche Manager called terminal ID. In combination with the workstation ID, this feature creates a unique ID for each session.

  A second method of automated configuration relies on features incorporated into the client software package. These features can create a unique workstation ID based on IP address, MAC address and/or session number.

NOTE See *Basing Workstation IDs on Terminal IDs* on page 139 and *Basing Workstation IDs on IP, MAC or Session Information* on page 141 for restrictions on the use of automatic configuration of workstation IDs.

Basing Workstation IDs on Terminal IDs

The proper implementation of the workstation ID based on terminal IDs has the following requirements:

- Wavelink Avalanche TN clients, version 4.16-05 or better.

- Enabler update kits version 1.54-00 or better.

To implement the workstation ID feature using the terminal ID:

1. Install required software packages that are valid for use with the terminal ID.

2. Ensure that each mobile device has a unique terminal ID in the List View of the Avalanche Manager.

The Manager assigns each mobile device with an ID when you enable the terminal ID feature. See *Using the Avalanche Agent Setup Wizard* on page 49 for more information about terminal IDs.

- This ID can be modified by double-clicking on the device listed in the Manager's List View. The Avalanche Client Controls window will then open. See Figure 5-20.
- Click `Edit Terminal ID`. Edit the values as needed and click `OK`.

Modifications to the terminal ID will be shown in parentheses in the List View. The current terminal ID will precede the modified ID. As soon as the device is updated, the new (modified) terminal ID will show as the current ID.

Typically, a host will only allow a 10 character workstation ID. Keep the terminal ID short. Workstations IDs longer that exceed the maximum length will be truncated.

3 Open the host profile utility associated with the software package.

NOTE For Wavelink Avalanche TN Clients, you can access this dialog box by right-clicking on the client software package and clicking `Configure Package > Host Profiles` from the context menu. For the workstation ID to apply, select the emulation type `IBM 5251-11`.

---

4 In the host profile, enter the workstation ID name based upon the following criteria:

- The length must be 1 to 10 characters.
- The first character must be a letter, #, $, or @.
- The remaining characters can be letters, numbers, #, $, @ or underscore.
- To ensure that the workstation ID is unique, enter a %t in the field to be used as part of the workstation ID. The %t will be replaced by the terminal ID of the mobile device. It is valid to have characters before and/or after the %t variable. For example, `ES%tA` is a valid workstation ID.

NOTE Hosts allow a maximum of 10 characters for the workstation ID. To avoid the truncation of the workstation ID, use a short terminal ID.

5 Click `OK` to save all changes.

Basing Workstation IDs on IP, MAC or Session Information

The proper implementation of the workstation ID based on IP, MAC, or session information requires that you use a Wavelink Avalanche TN Client, version 4.16-11 or better.

To implement the workstation ID using IP, MAC, or session information:

1 Install the required client software package.

2 Open the host profile utility associated with the software package.

NOTE For Wavelink Avalanche TN Clients, you can access this dialog box by right-clicking on the client software package and clicking `Configure Package > Host Profiles` from the context menu. For the workstation ID to apply, select the emulation type `IBM 5251-11`.

3 In the host profile, enter the workstation ID name based upon the following criteria:

- The length must be 1 to 10 characters.
- The first character must be a letter, #, $, or @.
- The remaining characters can be letters, numbers, #, $, @ or underscore.
- To ensure that the workstation ID is unique, use one or more of the following variables shown in Table 5-1. If needed, numbers can be zero-padded by placing a number in front of the letter; however, truncation is not supported. For example, if the variable %2b is used and the octet is 8, the workstation ID will be the zero-padded value 08. If the variable

%2b is used and the octet is 127, 127 will be used to create the workstation ID, because the value 127 cannot be truncated.

Variable	Description
%a, %b, %c, %d	Uses 1st, 2nd, 3rd, 4th octet of device's IP address, respectively.
%m, %n, %o, %p, %q, %r	Uses 1st, 2nd, 3rd, 4th, 5th, 6th octet of device's MAC address, respectively.
%s	Uses Session number (Telnet clients can be configured up to four sessions).

Table 5-1: *Workstation ID Variables*

NOTE Hosts allow a maximum of 10 characters for the workstation ID. To avoid the truncation of the workstation ID, use a short terminal ID.

4 Click `OK` to save all changes.

Mobile Device Groups

To better organize your wireless network, you can use the Avalanche Management Console to create collections of mobile devices, called mobile device groups. These groups allow you to manage multiple devices simultaneously, using the same tools available for managing individual mobile devices.

The topics in this section include:

- Creating Mobile Device Groups
- Assigning Mobile Devices to Groups
- Pinging Clients within Mobile Device Groups
- Sending Messages to Mobile Device Groups
- Additional Mobile Device Group Functions

Creating Mobile Device Groups

You can create a mobile device group at any time.

To create a device group:

1. Right-click the **Mobile Device Groups** icon in the Tree View.

2. Select `New Mobile Device Group` from the menu that appears.

   A dialog box appears, asking you to type a name for the new group.

3. Type a name for the group and click `OK`.

The group appears below the **Mobile Device Groups** icon.

Assigning Mobile Devices to Groups

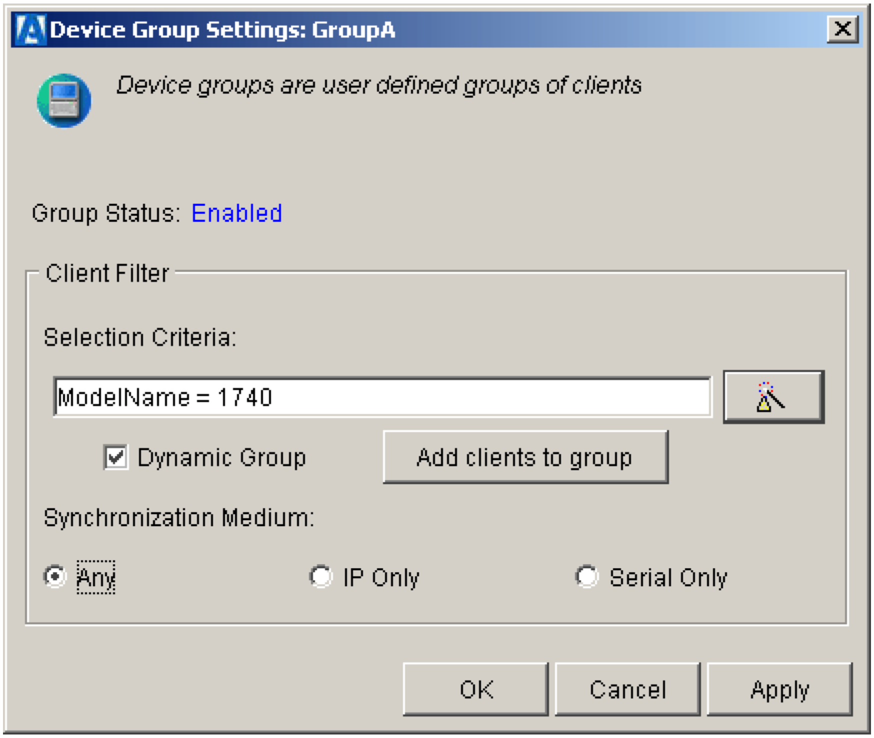
Once you create a group, you define selection criteria to define which mobile devices are added to the group. You can create dynamic or static groups. In both group types, new members can be added to the group based on changes to the selection criteria. However, in a static group, devices cannot be deleted from the group unless they are deleted on an individual basis.

To assign mobile devices to a group based on selection criteria:

1. Right-click the group from the Tree View.

2. Select `Settings` from the menu that appears.

   The *Device Group Settings* dialog box appears (Figure 5-22), allowing you to define the selection criteria that the Avalanche Manager will use to assign new mobile devices to the group.



Device Group Settings: GroupA

Device groups are user defined groups of clients

Group Status: Enabled

Client Filter

Selection Criteria:

ModelName = 1740

☑ Dynamic Group

Synchronization Medium:

● Any ○ IP Only ○ Serial Only

Figure 5-22. *The Device Group Settings Dialog Box*

3 Enable the **Dynamic Group** option.

4 Click the **Selection Criteria Builder** button icon and then create the selection criteria for the group.

See *Selection Criteria* on page 122 for more information on selection criteria.

NOTE The Avalanche Manager limits the number of device subsets you can create in groups. For example, Group A, B, and C might contain selection criteria that allows overlap among devices, with the result that some devices reside in multiple groups. If mobile devices exceed these internal limits, an error message appears and the Management Console prevents the invalid configuration.

To manually assign mobile devices to a group:

1 Right-click the group from the Tree View.

2 Select `Settings` from the menu that appears.

The *Device Group Settings* dialog box appears (Figure 5-22).

3 Disable the **Dynamic Group** option.

By disabling this option, you define the group as a static group. When you want to remove a mobile device from a static group, you must manually delete it.

4 Manually type a selection criteria string in the **Selection Criteria** text box.

5 Click `Add clients to group`.

The mobile devices that match the selection criteria are automatically added to the group.

NOTE You can also drag a device from the Device View of Avalanche Manager to a group in the Tree View to add the mobile device to that group.

Removing Mobile Devices from a Mobile Device Group

You can manually remove mobile devices from static groups.

To remove a client:

1 In the Tree View of the Management Console, select the group containing the mobile device you want to remove.

2 In the List View, right-click on the mobile device and select `Remove Client from Group: Group` *`X`*

where *X* is the name of the group.

Pinging Clients within Mobile Device Groups

You can use mobile device groups to ping a collection of mobile devices simultaneously.

To ping clients within device groups:

1 Right-click the group from the Tree View.

2 Select `Ping Client(s)` from the menu that appears.

See *Pinging the Client* on page 138 for more information on pinging clients.

Sending Messages to Mobile Device Groups

You send messages to users using mobile device groups, allowing you to send the same message to multiple devices simultaneously.

To send messages to device groups:

1 Right-click the group from the Tree View.

2 Select `Send Text Message` from the menu that appears.

See *Sending Messages* on page 137 for more information on sending messages to clients.

Applying Restrictions on the Download Medium

You can configure mobile device groups to allow wireless downloads, serial downloads, or both. By default, the mobile device group will allow the use of either synchronization medium.

NOTE A licensed authorization is required to perform wireless downloads.

To set the download medium for the collection:

1 In the Tree View of the Management Console, right-click on the mobile device group and select `Settings`.

The dialog box shown in Figure 5-22 appears.

2 Set the desired synchronization medium option.

If you want to restrict the software updates associated with the current mobile device group to wireless only, enable the **IP Only** option.

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

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

NOTE IrDA connections are treated as serial connections.

3 Click `OK`.

Additional Mobile Device Group Functions

Mobile device groups also include several other functions, allowing you to more efficiently manage your mobile devices. These options are available by right-clicking the mobile device group and selecting the appropriate option.

The additional options for mobile device groups are as follows:

Copy Group	Allows you to copy the group.
Delete Group	Allows you to delete the group.
Enable/Disable Group	Allows you to enable or disable the group.
Rename Group	Allows you to rename the group.
Update Now	Allows you to update all mobile devices within that group immediately.
Mark Orphan Packages for Deletion	Marks orphaned packages on the devices within the group for deletion.
Clear Deletion of Orphaned Packages	Clears orphaned packages on the devices within the group.

Mobile Device Properties

Mobile device properties consist of pre-defined and user-defined properties. The pre-defined properties are specific to the version of the Avalanche Enabler running on the mobile device. Properties can be used as selection variables in selection criteria to control which devices receive particular updates.

NOTE See *Selection Criteria* on page 122 for related information.

User-defined properties can be associated with individual mobile devices or with mobile device groups.

Pre-defined properties are specific to the version of the Avalanche Enabler running on the mobile device. Properties can be used for selection criteria in addition to the selection variables. See *Selection Criteria* on page 122 for more information.

Pre-defined properties supported on the Avalanche Enabler, version 3 or higher, include:

AgentAddress The IP address or name of the Agent associated with the mobile device.

AppliedProfile The name of the network profile associated with the mobile device.

AutoRun Specifies whether the Avalanche package installed on the mobile device automatically runs at startup. This only takes effect if the Avalanche package is the only package that appears in the **Application** menu on the device. The possible values for this property are:

0 - disabled
1 - enabled

Columns The number of columns on the mobile device display.

EnablerVer The version of the Enabler running on the mobile device.

KeyboardName The mobile device keyboard type, for example, 46KEY.

ModelName The model name of the mobile device, for example, 6840.

OsType The operating system type, for example, DOS.

OsVer The version of the operating system of the mobile device.

OverrideManual

If you want the network profile settings, including the IP address, WEP keys, and other network parameters, to override manually set options on the mobile device, enable this property. The settings for the appropriate network profile will download to the mobile device over wired or wireless connections. See *Using Network Profiles* on page 89 for more information.

NOTE This feature is most valuable if you need to manually configure devices for temporary use in another facility.

The possible values for this property are:

0 - disabled
1 - enabled

Processor

The processor type of the mobile device, for example, x86.

RadioSpeed

The network throughput supported by the radio card, for example, 1Mb, 2Mb, or 11Mb.

RadioType

The radio type, typically the name of the radio card manufactuer, for example, Symbol or Cisco.

Rows

The number of rows on the mobile device display.

ScannerType

The scanner type, typically 1D or 2D.

Series

The mobile device series type. For example, a 3 indicates Symbol 3000 Series.

TerminalID

This feature allows the user to define a unique identifier that Avalanche Manager associates with a mobile device. Workstation IDs are supported only in TN5250 environments. See *Setting a Workstation ID* on page 138 for more information.

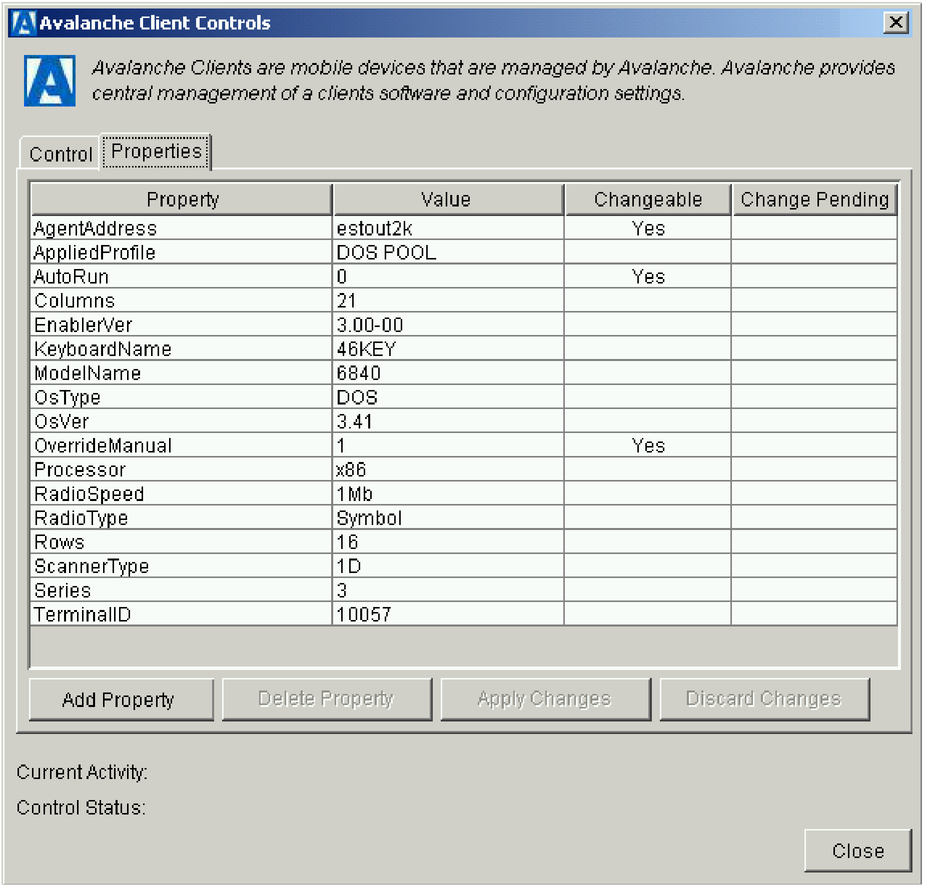
Viewing Properties

You can view properties associated with a specific mobile device using either the property editor for individual properties or the group property editor.

To view the properties using the individual property editor:

1 Double-click the mobile device in the List View of the Management Console.

2 In the *Avalanche Client Controls* dialog box, click the Properties tab. The following dialog box appears.



Avalanche Client Controls

Avalanche Clients are mobile devices that are managed by Avalanche. Avalanche provides central management of a clients software and configuration settings.

Property	Value	Changeable	Change Pending
AgentAddress	estout2k	Yes	
AppliedProfile	DOS POOL		
AutoRun	0	Yes	
Columns	21		
EnablerVer	3.00-00		
KeyboardName	46KEY		
ModelName	6840		
OsType	DOS		
OsVer	3.41		
OverrideManual	1	Yes	
Processor	x86		
RadioSpeed	1Mb		
RadioType	Symbol		
Rows	16		
ScannerType	1D		
Series	3		
TerminalID	10057		

Current Activity:

Control Status:

Figure 5-23. *The Properties Tab of the Avalanche Client Controls Dialog Box (v. 3.x Enabler)*

The columns that appear in this dialog box are as follows:

Property The name of the property.

Value The value of the property.

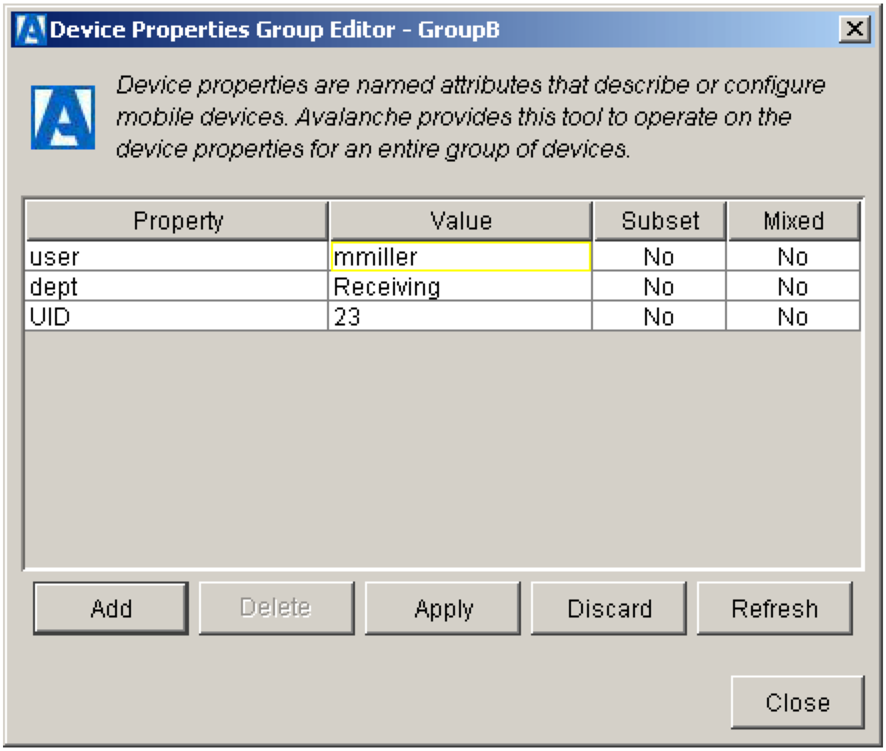
Changeable Indicates whether the property can be edited (`Yes`) or not (`No`).

Change Pending Indicates whether the property needs to be updated on the mobile device. If it needs to be updated, the value is `Yes`.

To view properties using the group property editor:

1. In the Tree View of the Management Console, right-click the desired group and select `Edit Device Properties`.

The *Device Properties Group Editor* dialog box appears.



Device properties are named attributes that describe or configure mobile devices. Avalanche provides this tool to operate on the device properties for an entire group of devices.

Property	Value	Subset	Mixed
user	mmiller	No	No
dept	Receiving	No	No
UID	23	No	No

Figure 5-24. *The Device Properties Group Editor Dialog Box*

Only user-defined properties associated with mobile devices in the group appear in the group property editor. The columns that appear in this dialog box are as follows:

Property	The name of the property.
Value	The value of the property
Subset	Indicates whether the property applies to a subset of mobile devices in the group (Yes) or all mobile devices in the group (No).
Mixed	Indicates whether the value of the property is different for some of the mobile devices in the group (Yes) or the same (No).

Adding User-Defined Properties

Avalanche Manager provides the ability to create user-defined properties on the mobile devices. These properties can then be used to build selection criteria for software updates.

You can add user-defined properties to individual mobile devices or to mobile device groups. When you add a property to a group, it is created for all mobile devices that are members of the group.

NOTE Like the pre-defined properties, user-defined properties appear as selection variables in the Selection Criteria Builder wizard.

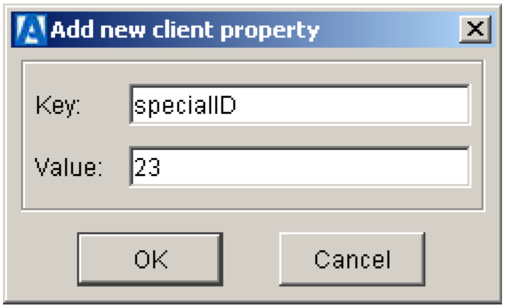
To add a user-defined property to a mobile device:

1. Double-click a mobile device in the List View of the Management Console.

2. In the *Avalanche Client Controls* dialog box (see Figure 5-23), select the Properties tab.

3. Click `Add Property`.

   The following dialog box appears.



Add new client property

Key: specialID

Value: 23

Figure 5-25. *The Add New Client Property Dialog Box*

4. Type the name of the property in the **Key** text box.

5. Type the value of the property in the **Value** text box.

6. Click `OK`.

The new property appears in the Properties tab of the *Avalanche Client Controls* dialog box.

The new value downloads to the mobile device at the next update. If the device has not yet received an updated property value, a `Yes` appears in the **Change Pending** column for the property.

To add a user-defined property to a group:

1 Right-click on the group in the Tree View of the Management Console and select Edit Device Properties.

The *Device Properties Group Editor* dialog box appears (Figure 5-24).

2 Click `Add Property`.

The Add New Client Property dialog box appears (Figure 5-25).

3 Type the name of the property in the **Key** text box.

4 Type the value of the property in the **Value** text box.

5 Click `OK`.

The new property appears in the *Device Properties Group Editor* dialog box and will apply to all mobile devices in the group.

At the next update, the new property downloads to all the mobile device in the group.

NOTE If a mobile device has not yet received an updated property value, a `Yes` appears in the **Change Pending** column for the property in the Properties tab of the *Detailed Client Controls* dialog box.

Editing Properties

Some of the pre-defined properties (and all of the user-defined properties) support editing of values. When you change the value of a property, the new value is downloaded to the mobile device at the next update.

User-defined properties can be edited either for a specific mobile device or for a group of devices using the group property editor.

NOTE Property editing is supported only on the Avalanche Enabler, version 3 or higher.

To edit a property for a mobile device:

1. Double-click a mobile device in the List View of the Management Console.

2. In the *Avalanche Client Controls* dialog box (see Figure 5-23), select the Properties tab.

3. Click in the **Value** column for an editable property.

   If property is editable, a `Yes` displays as its value under the **Changeable** column.

4. Type the new value for the property.

5. Click `Apply Changes`.

   The new value downloads to the mobile device at the next update. If the device has not yet received an updated property value, a `Yes` appears in the **Change Pending** column for the property.

To edit a property for a group:

1. In the Tree View of the Management Console, right-click the group containing the property you want to edit and select `Edit Device Properties`.

2. In the *Device Properties Group Editor* dialog box, click in the **Value** column for an editable property.

   Only user-defined properties appear in this dialog box. All of these properties can be edited.

3. Type the new value for the property.

4. Click `Apply Changes`.

The new property value takes effect for all the mobile devices in the group.

At the next update, the new value downloads to all the mobile device in the group that contain the specified property. The **Subset** column displays a `Yes` value if all mobile devices in the group contain the property.

NOTE If a mobile device has not yet received an updated property value, a `Yes` appears in the **Change Pending** column for the property in the Properties tab of the *Detailed Client Controls* dialog box.

Chapter 6: Managing Updates

In addition to automating client software and configuration updates, the Avalanche system also provides you with the ability to configure and monitor the update process. This section includes information on the following topics:

- Configuring Updates
- Deploying Updates
- Monitoring Updates

Configuring Updates

Wavelink Avalanche allows you to schedule server-initiated updates and control the use of network bandwidth during both server-initiated and client-initiated updates.

To configure updates, select `Client Update Controls` from the **Tools** menu. In the *Client Update Controls* dialog box, you can schedule updates for software packages and configure the use of network bandwidth during updates.

Managing Network Bandwidth

Wavelink Avalanche allows you to restrict the maximum amount of network bandwidth used at any one time for client updates. These restrictions apply to both client- and server-initiated updates. In the absence of critical bandwidth shortage, unrestricted updates can be safely allowed.

To configure the use of network bandwidth for updates:

1 Select `Client Update Controls` from the **Tools** menu.

The *Avalanche Client Update Manager* dialog box, shown in Figure 6-1, appears.

2 If you want to allow unrestricted updates, enable the **Allow Unrestricted Simultaneous Updates** checkbox.

If you want to restrict network bandwidth during updates, disable the **Allow Unrestricted Simultaneous Updates** checkbox and type in the maximum number of simultaneous updates.

3. If you want to create a blackout period, during which client updates are not allowed, enable the **Do Not Allow Updates During the Time Window** checkbox. You can then type the start and end times during which updates are not allowed, as well as select the days of the week when this blackout period is in effect.

4. Click `OK`.

In addition, you can use other methods to help minimize network impact:

- Rely on client-initiated updates.

  After changing client software and configurations at the Management Console, allow each client to receive the changes when they next synchronize (typically following reboot). You can check the update status for clients at any time by selecting an item in the Tree View. When you click on the item, all mobile devices associated with the Avalanche Manager will appear in the List View. The client's update status appears in the **Status** column.

NOTE When you select a software collection, software package, or network profile, only the relevant subset of mobile devices will appear in the List View.

- Schedule a server-initiated global update for off-peak hours.

  Using the options described in *Scheduling Updates*, the Avalanche Manager can update all the mobile devices during the night or at any convenient time when the network and the clients are not in use.

Scheduling Updates

This option allows you to schedule a server-initiated global update.

You can perform global or individual updates to clients that are currently in range and running the Avalanche Enabler, an Avalanche-enabled application, or in some cases a configuration utility.

To schedule updates:

1. Select `Client Update Controls` from the **Tools** menu.

The *Avalanche Client Update Manager* dialog box, shown in Figure 6-1, appears.

2 Click the Scheduled Updates tab, as shown in Figure 6-1.

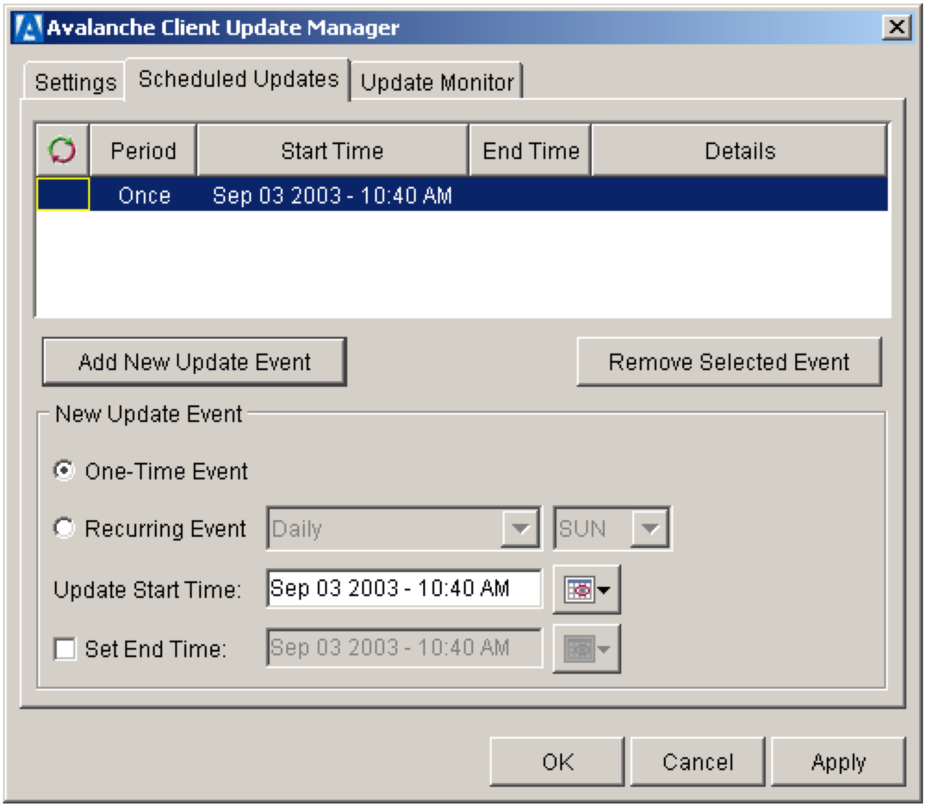
3 If the update is going to occur only once, select the **One-Time Event** option.

4 If the update is going to occur on a regular basis, select the **Recurring Event** option.

If you select this option, a list become active. This list allows you to determine whether the update occurs on either a daily or weekly basis. If you select `Weekly` from this list, a second list becomes active, allowing you to select the day on which the update occurs.

5 Type the start time for the update in the **Update Start Time** text box.

6 Select the date on which this update starts by clicking the date button next to the **Update Start Time** text box. This button opens a calendar, allowing you to select the day on which the update begins.



	Period	Start Time	End Time	Details
	Once	Sep 03 2003 - 10:40 AM		

● One-Time Event

○ Recurring Event Daily SUN

Update Start Time: Sep 03 2003 - 10:40 AM

□ Set End Time: Sep 03 2003 - 10:40 AM

Figure 6-1. *The Scheduled Updates Tab of the Avalanche Client Update Manager Dialog Box*

7 If you want to establish an end time for this update, enable the **Use End Time** checkbox.

NOTE Selecting an end time is not required, allowing you to create events that recur indefinitely.

8 When you enable the **Use End Time** checkbox, a text box becomes active, allowing you to type the end time for the update. You can also select the date on which this update ends by clicking the date button next to this text box. This button opens a calendar, allowing you to select the day on which the update ends.

9 Click `Add Update Event` to add the new event to the Management Console.

10 Click `OK`.

NOTE Many mobile devices incorporate a sleep function to preserve battery life. If a device is asleep, you must “wake” it before it can receive a server-initiated (pushed) update from the Avalanche Manager. Wake-up capability is dependent on the type of wireless infrastructure you are using and the mobile device type. Contact your hardware and/or wireless provider for details.

To monitor the status of a current update or to see the results of one that previously completed, select `Global Update Monitor` from the **Tools** menu. See *Monitoring Updates* on page 162 for more details.

Deploying Updates

Wavelink Avalanche uses "push/pull" technology to deploy software and configuration updates to the mobile device.

NOTE You must enable a package before you can download it to the mobile device. To enable a package, right-click on the package in the Tree View and select `Enable Package`.

- Mobile devices automatically “pull” updates from the Avalanche Manager Agent whenever the Enabler activates.

  For DOS/Embedded devices, the Enabler activates whenever a device reboots. Consequently, when a DOS/Embedded device reboots, it automatically connects to the Avalanche Manager Agent with which it is associated. If the device is not associated with any Agent, the device sends a network broadcast and connects to the first Agent that responds to it.

  You can associate the mobile device with a specific Agent using a network profile or by manually configuring the Avalanche Enabler on the mobile device. See *Using Network Profiles* on page 89 for more information about network profiles.

For a Palm or Windows CE/Pocket PC device, the Enabler activates when you click the **Enabler** icon on the device. These devices then connect to the Agent in the same manner as a DOS/Embedded device.

- You can also “push” global updates or individual updates to mobile devices from the Avalanche Manager Agent. See *Scheduling Updates* on page 158 for more information about scheduling global updates.

  You can perform global or individual updates to clients that are currently in range and running the Avalanche Enabler or an Avalanche-enabled application.

NOTE The rules that govern which mobile devices can receive a particular update are determined by the selection criteria. See *Selection Criteria* on page 122 for more information.

To push an update to an individual mobile device:

1 Double-click on the mobile device in the List View of the Management Console.

  The *Avalanche Client Controls* dialog box, shown in Figure 5-20, appears.

2 Click `Update Now`.

The **Control Status** field on the bottom of the *Avalanche Client Controls* dialog box allows you to monitor the status of the update.

NOTE Many mobile devices incorporate a sleep function to preserve battery life. If a device is asleep, you must “wake” it before it can receive a “pushed” update from the Avalanche Manager. Wake-up capability is dependent on the type of wireless infrastructure you are using and the mobile device type. Contact your hardware and/or wireless provider for details.

Monitoring Updates

The Avalanche Manager allows you to monitor the current status of an ongoing global update or check the results of the last completed global update.

To open the global update monitor, select `Client Update Controls` from the **Tools** menu and click the Update Monitor tab. The dialog box shown in figure 6-2 appears.

The fields in this dialog box include:

Start Time The start time of the update.

End Time The end time of the update

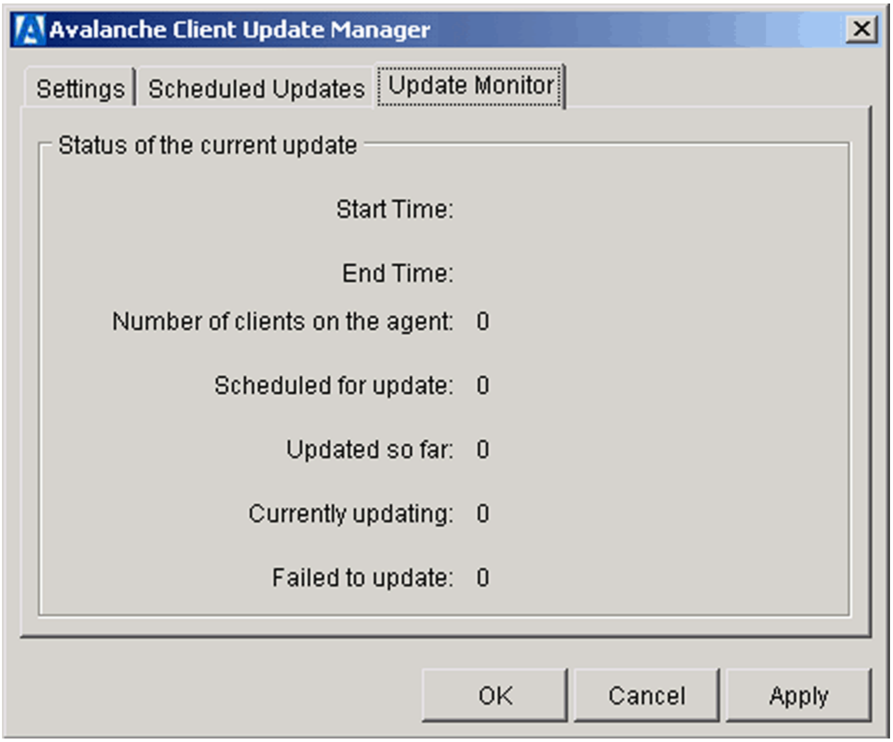
Number of Clients on the Agent The total number of clients registered with the Avalanche Manager at the start of the update.

Scheduled for Update The number of clients in need of an update.

Updated So Far The number of clients that have completed their update (only applies while an update is active).

Currently Updating The number of clients currently in the process of being updated (only applies while an update is active).

Failed Update Count The current number of clients failing to respond to the update command. These may be out of range or completely powered down devices. The Management Console's List View shows which clients still need updating. You can handle these clients independently or by scheduling another global update.



Status of the current update

Start Time:

End Time:

Number of clients on the agent: 0

Scheduled for update: 0

Updated so far: 0

Currently updating: 0

Failed to update: 0

Figure 6-2. *Global Client Update Monitor*

Chapter 7: Avalanche Manager Agent

One of the primary components of the Avalanche Manager is the Agent. The Agent performs software and configuration updates and is configured through the Management Console.

This section provides a summary of the Agent's functions and instructions on how to interact with it directly using the native operating system and the Management Console.

Select a link below to learn more about Wavelink Avalanche Agents:

- Understanding Agents
- Adding an Agent
- Viewing Agent Information
- Connecting to an Agent
- Disconnecting from an Agent
- Removing an Agent Profile
- Starting an Agent on Windows 2000/XP
- Stopping an Agent from Windows 2000/XP
- Uninstalling an Agent on Windows 2000/XP
- Managing an Agent from the Command Prompt
- Configuring the Agent Port
- Backing Up an Agent
- Restoring an Agent
- Removing Mobile Devices

Understanding Agents

The Agent is server software that lets you remotely manage and configure mobile devices. Although you can use multiple Agents at different sites or on different network segments, you can manage all of your Agents from one Management Console—regardless of where the console resides on the network.

Agents and Windows 2000/XP

On Windows 2000/XP and the Windows 2003 Server, the Agent functions as a system service. As a system service, the Agent runs in the system background. It neither appears on the system desktop nor on the taskbar. Once you start the Agent, it continues to function regardless whether anyone is logged on to the system.

Adding an Agent

Before you can connect to an Agent, you must add an Agent profile using the Management Console.

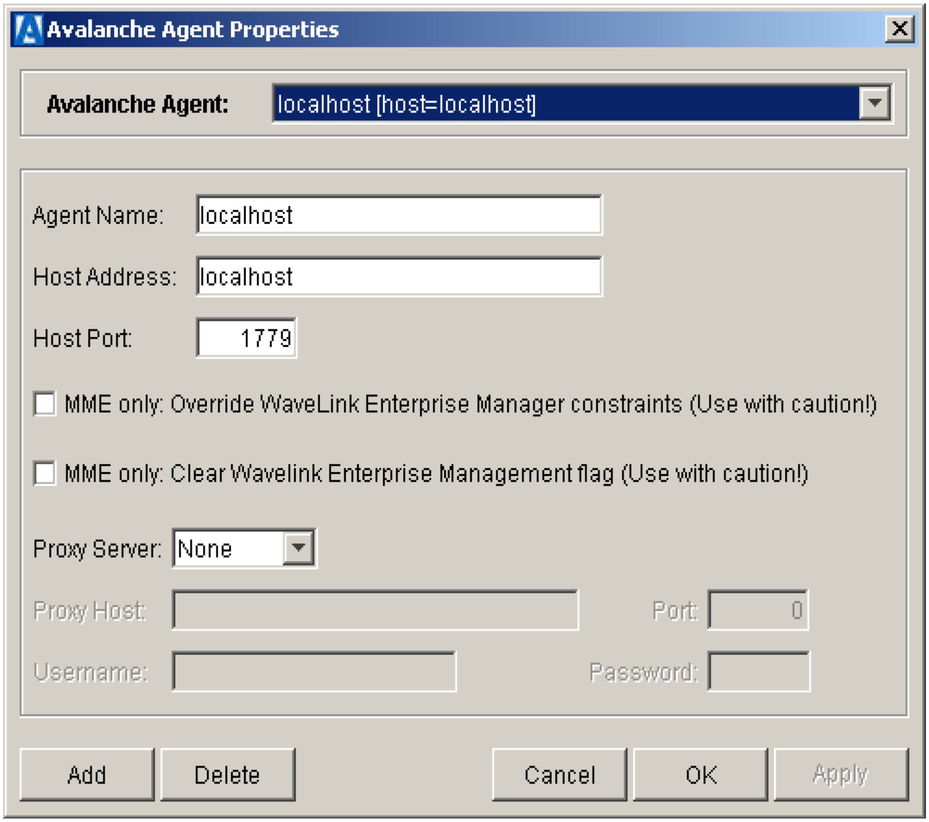
The Management Console automatically creates an Agent profile for localhost, if the Agent has been installed on the local system.

You can add, modify, and delete local or remote Agent profiles as needed.

To add an Agent:

1 Select `Agent Settings` from the Agent menu.

The *Avalanche Agent Properties* dialog box appears.



Avalanche Agent: localhost [host=localhost]

Agent Name: localhost

Host Address: localhost

Host Port: 1779

□ MME only: Override WaveLink Enterprise Manager constraints (Use with caution!)

□ MME only: Clear Wavelink Enterprise Management flag (Use with caution!)

Proxy Server: None

Proxy Host: Port: 0

Username: Password:

Figure 7-1. *The Avalanche Agent Properties Dialog Box*

The Agent profile, localhost, is selected by default.

2. Enter the name of the new Agent in the **Agent Name** text box.

3. Enter the IP address of the Agent in the **Agent IP Address** text box. A valid IP address is any routable IP address hosting an Agent.

4. Enter the port used by the new Agent in the **Host Port** text box.

5. If you want the Management Console to override any settings established by the Mobile Manager Enterprise Edition, enable the **Override Wavelink Enterprise Manager Constraints** checkbox.

6. If the Agent resides past a firewall, you can connect to it through a proxy using the SOCKS protocol.

To configure the connection through a proxy, select `SOCKS 4` from the **Proxy Server** list. Then, type the IP address of the proxy server in the **Proxy Host** text box, and the port number for the proxy in the **Port** text box.

7 Click `Add`.

NOTE You can manually synchronize the console to the Agent by selecting `Synchronize Packages with Agent` from the **Administration** menu.

The Agent profile appears in the **Avalanche Agent Settings** list. See *Viewing Agent Information* for more information.

Viewing Agent Information

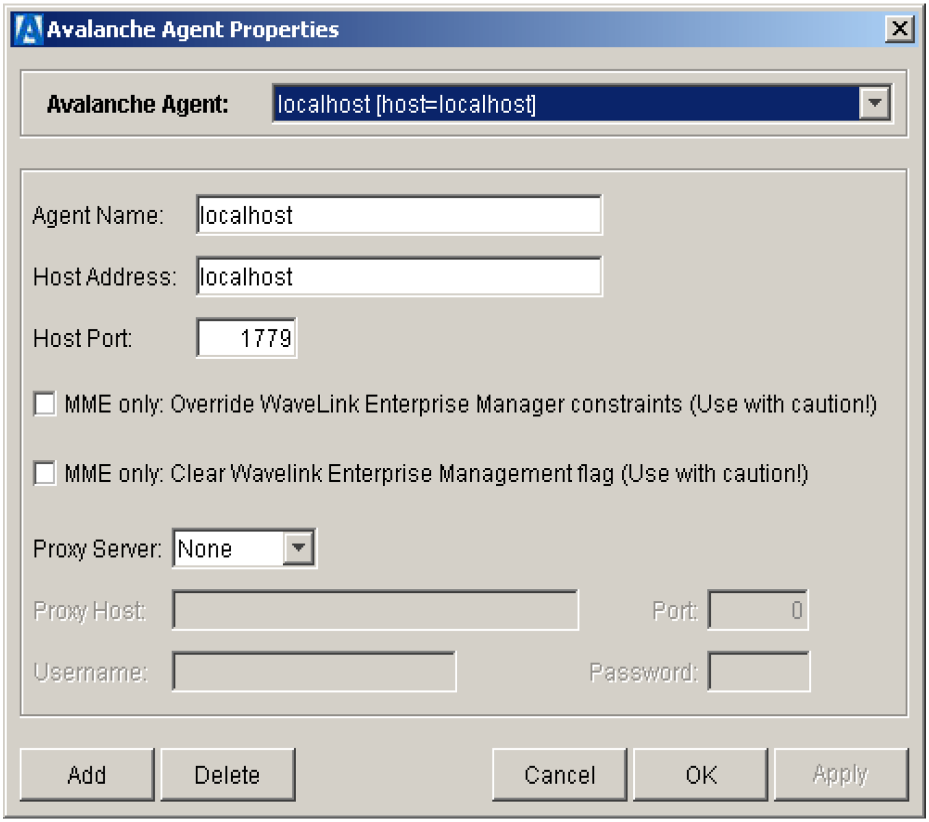
You can view information about the Avalanche Manager Agent's network interface by double-clicking on the **Agent Network Interface** branch in the Tree View. The IP address and MAC address of the current Agent's network interface card appear in the Tree View.

In addition, you can view more detailed information about an Agent profile.

To view an Agent's profile:

1 Select `Agent Settings` from the **Agent** menu.

The *Avalanche Agent Properties* dialog box appears.



Avalanche Agent: localhost [host=localhost]

Agent Name: localhost

Host Address: localhost

Host Port: 1779

□ MME only: Override WaveLink Enterprise Manager constraints (Use with caution!)

□ MME only: Clear Wavelink Enterprise Management flag (Use with caution!)

Proxy Server: None

Proxy Host:

Port: 0

Username:

Password:

Figure 7-2. *The Avalanche Agent Properties Dialog Box*

2 Select an Agent from the **Avalanche Agent** list.

Information about the Agent appears in the columns under the **Agents** group box.

Agent Name	Name of the Agent.
Host Address	IP address of the system hosting the Agent.
Host Port	Port number for the Agent.

MME only: Ignore Wavelink Enterprise Manager Constraints

This option is unavailable unless Mobile Manager Enterprise Edition is installed on your network. This option makes the Avalanche Agent function independently from instructions sent by the Mobile Manager Enterprise Edition.

MME only: Clear Wavelink Enterprise Manager flag

This option is unavailable unless Mobile Mobile Enterprise Edition is installed on your network. See the documentation for *Mobile Manager Enterprise* for more information.

Proxy Server

Allows you to select a proxy server to connect to the Agent. If the Agent resides on the other side of a firewall, you can connect to it using the SOCKS protocol. To use this protocol, select the SOCKS 4 proxy server.

Proxy Host

The IP address of the proxy server.

Port

The port number used to connect to the proxy server.

Username

Not implemented.

Password

Not implemented.

You can edit the Agent information by selecting an Agent and modifying any of these options and clicking `Apply`.

You can also delete an Agent by selecting an Agent and clicking `Delete`.

Connecting to an Agent

Before you can connect to an Agent, a valid profile for that Agent must exist. By default, an Agent profile for localhost is created when you install the Management Console and the Agent on a single system. To add additional profiles, see *Adding an Agent* on page 166.

If you already have created an Agent connection, you can connect to it directly. If you want to connect to a new Agent connection, you can use the Agent Connection wizard to create the new connection.

To connect to an existing Agent connection

1 Select `Connect to Agent` from the **Agent** menu.

The Agent Connection wizard appears. The first step in this wizard is to either connect to an existing Agent connection or create a new one.

2 Select the **Use an existing Agent** connection option.

3 Select the Agent connection from the list.

4 Click `Next`.

If the Agent you are trying the connect to is not running, the wizard displays an dialog box that allows you to start the Agent before proceeding. Once the Agent has started, click `Next`.

The dialog box shown in Figure 7-3 appears.

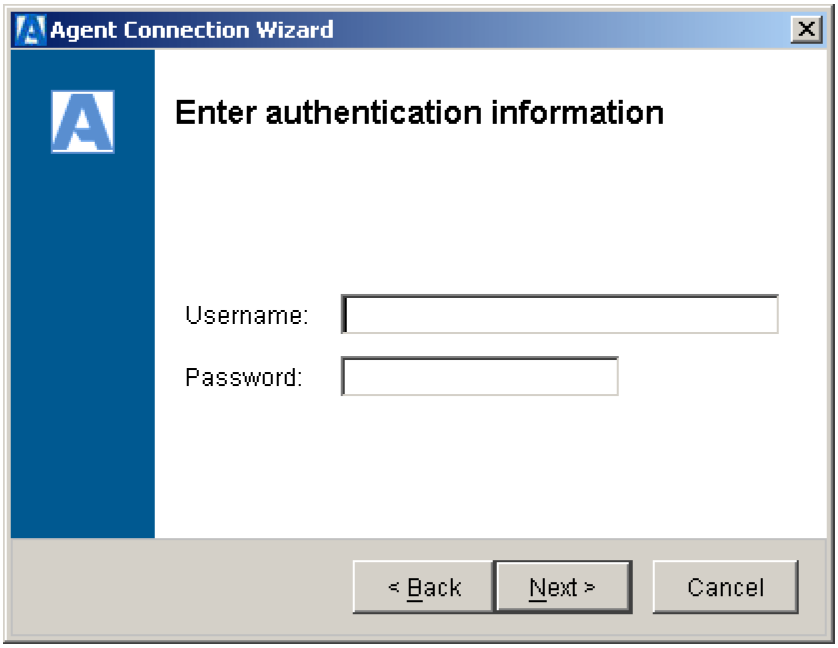


Figure 7-3. *The Enter Authentication Information Dialog Box*

5 Configure authorization settings.

If you want to connect to the Agent as an authorized user, enter a valid user name and password.

If you want to connect to the Agent with read-write guest authorization, leave the **Username** and **Password** text boxes blank. However, if authorization is required for the Agent, access to the Agent will be denied.

6 Click `Next`.

The Agent Connection wizard connects to the Agent.

If the Agent is not able to not connect, the message box will indicate that a connection could not be established. In this case, verify that you are using the correct IP address for the Agent and that the address is accessible on the LAN or WAN. See *Viewing Agent Information* on page 168 for more information. In addition, you must also verify that the Agent service to which you want to connect has been started. See *Starting an Agent on Windows 2000/XP* on page 178 for more information.

7 Click `Finish`.

See *Using the Avalanche Agent Setup Wizard* on page 49 to configure the new Agent.

To connect to a new Agent connection:

1 Select `Connect to Agent` from the **Agent** menu.

The Agent Connection wizard appears. The first step in this wizard is to either connect to an existing Agent connection or create a new one.

2 Select the **Create a new Agent connection** option.

3 Click `Next`.

The next step in the wizard is to establish the parameters for the new connection.

4 Enter the name of the new Agent in the **Agent Name** text box.

5 Enter the IP address of the Agent in the **Host Address** text box. A valid IP address is any routable IP address hosting an Agent.

6 Enter the port used by the new Agent in the **Host Port** text box.

7 If you want the Management Console to override any settings established by the Mobile Manager Enterprise Edition, enable the **Ignore Wavelink Enterprise Manager Constraints** checkbox.

8 If the Agent resides past a firewall, you can connect to it through a proxy using the SOCKS protocol.

To configure the connection through a proxy, select `SOCKS 4` from the **Proxy Server** list. Then, type the IP address of the proxy server in the **Proxy Host** text box, and the port number for the proxy in the **Port** text box.

9 Click `Next`.

The *Enter Authorization Information* dialog box, shown in Figure 7-3, appears.

10 Configure authorization settings.

If you want to connect to the Agent as an authorized user, enter a valid user name and password.

If you want to connect to the Agent with read-write guest authorization, leave the **Username** and **Password** text boxes blank. However, if authorization is required for the Agent, access to the Agent will be denied.

11 Click `Next`.

The Agent Connection wizard connects to the Agent.

If the Agent is not able to connect, the message box will indicate that a connection could not be established. In this case, verify that you are using the correct IP address for the Agent and that the address is accessible on the LAN or WAN. See *Viewing Agent Information* on page 168 for more information. In addition, you must also verify that the Agent service to which you want to connect has been started. See *Starting an Agent on Windows 2000/XP* on page 178 for more information.

12 Click `Finish`.

See *Using the Avalanche Agent Setup Wizard* on page 49 to configure the new Agent. This wizard automatically appears when you connect to a new Agent

Disconnecting from an Agent

You can disconnect from an Agent at any time. However, once you disconnect from an Agent, you cannot access the software collections and packages associated with that Agent.

To disconnect from an Agent, select `Clear Connection` from the **Agent** menu.

NOTE An Agent continues to run on the host even after you have disconnected it from the Management Console. To stop the Agent completely, see *Stopping an Agent from Windows 2000/XP* on page 179.

Removing an Agent Profile

You can delete local or remote Agent profiles as needed. An Agent continues to run on the host even after you have removed its profile in the Management Console. To stop the Agent completely, see *Stopping an Agent from Windows 2000/XP* on page 179.

To remove an Agent:

1. Select `Agent Settings` from the **Agent** menu.

   The *Avalanche Agent Settings* dialog box appears.

2. In the *Avalanche Agent Settings* dialog box, select the Agent you want to remove and click `Delete Agent`.

   A message box appears asking you to confirm whether you want to delete the Agent.

3. Click `Yes`.

User Authentication

Avalanche Manager provides the ability to control administrative access to Agents from the Management Console. Administrative access can be controlled on a per-user basis, with different permission levels assigned to users. Permission levels include none (no access), read, write, and administrator.

Only users with administrator permissions can modify user authentication settings.

You can also place users into groups, and restrict access to specific software collections based on group membership.

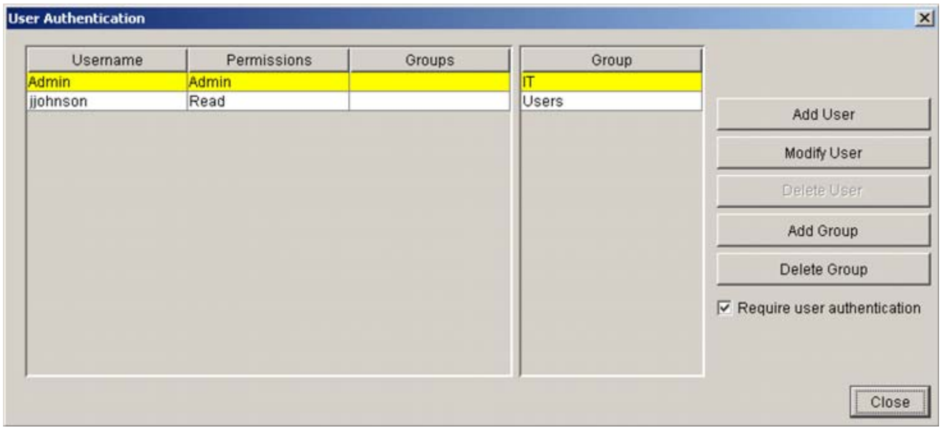
Adding a User

You must be logged onto an Agent with administrative permissions to add a user.

To add a user:

1 In the main console window, select `User Authentication` from the **Security** menu.

The *User Authentication* dialog box appears.



User Authentication

Username	Permissions	Groups
Admin	Admin	
jjohnson	Read	

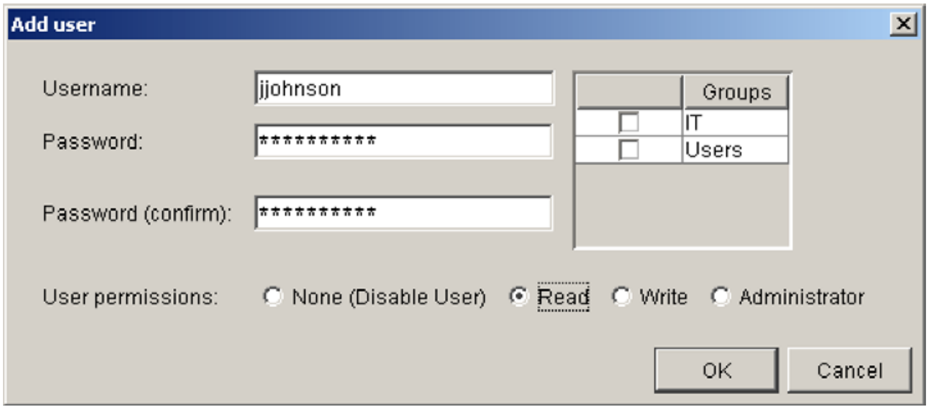
Group
IT
Users

☑ Require user authentication

Figure 7-4. *The User Authentication Dialog Box*

2 Click `Add User`.

The *Add User* dialog box appears.



Add user

Username: jjohnson

Password: **********

Password (confirm): **********

	Groups
□	IT
□	Users

User permissions: ○ None (Disable User) ● Read ○ Write ○ Administrator

Figure 7-5. *The Add User Dialog Box*

3 Type a name for the user in the **Username** text box.

4 Type a password for the user in the **Password** text box.

5 Type the password a second time in the **Password (confirm)** text box.

6 Select the user permission level. The following levels of user permissions are supported:

None Users with no permissions will be prevented from connecting to an Agent.

Read Users with read permission can view packages and collections, but will not be able to modify them.

Write Users with write permission can view and modify packages and collections, and modify their own password.

Administrator Users with administrative permissions can view and modify packages and collections, and modify all user authentication settings.

7 If you want the user to become a member of one or more existing groups, enable the checkbox next to any groups that appear under the **groups** column.

8 Click `OK`.

The new user appears in the *User Authentication* dialog box.

Removing a User

When you remove a user, the user loses access to Agents in the Management Console.

To remove a user:

1 In the main console window, select `User Authentication` from the **Security** menu.

The *User Authentication* dialog box, shown in Figure 7-4, appears.

2 Select the user you want to remove.

3 Click `Delete User`.

Adding an Authorization Group

User authorization groups allow you to limit access to software collections based on a user's group affiliation.

To add an authorization group:

1 In the main console window, select `User Authentication` from the **Security** menu.

The *User Authentication* dialog box, shown in Figure 7-4, appears.

2 Click `Add Group`.

3 In the dialog box that appears, type the name for the new group and click `OK`.

The group appears in the *User Authorization* dialog box.

Assigning an Authorization Group to a Collection

Once you have created one or more authorization groups, you can assign them to specific software collections. Once you assign a group to a collection, only users with membership in the specified group and write privileges can modify the collection.

To assign an authorization group to a collection:

1. In the Tree View of the Management Console, right-click on the software collection and select `Set User Group`.
2. In the dialog box that appears, select the group that will be allowed access to the collection.
3. Click `OK`.

Removing an Authorization Group

You can remove an authorization group at any time.

To remove an authorization group:

1. In the main console window, select `User Authentication` from the **Security** menu.

   The *User Authentication* dialog box, shown in Figure 7-4, appears.

2. Select the group you want to remove.
3. Click `Delete Group`.

The group is removed from the *User Authorization* dialog box.

Starting an Agent on Windows 2000/XP

You can start an Agent on Windows 2000/XP and the Windows 2003 Server by using the Windows Services control panel.

To start an Agent using the Services control panel:

1. Open the Services control panel.

   The *Services* dialog box appears.

2. Right-click the Wavelink Avalanche Manager from the **Services** list.
3. Select `Start`.

   Notice that, in the **Startup** column, the Agent is listed as `Automatic`, indicating that the Agent automatically starts after a system reboot.

To disable this feature, double-click the entry to open its *Properties* dialog box. Within this dialog box, select `Manual` from the **Startup Type** list.

Stopping an Agent from Windows 2000/XP

You can stop an Agent on Windows 2000/XP and the Windows 2003 Server by using the Windows Services control panel.

To stop an Agent using the Services control panel:

1 Open the Services control panel.

The *Services* dialog box appears.

2 Right-click `Wavelink Avalanche Manager` from the **Services** list.

3 Select `Stop`.

Uninstalling an Agent on Windows 2000/XP

You can uninstall the Avalanche Manager Agent and the Management Console by using the standard uninstall included with Windows 2000/XP and the Windows 20003 Server.

To uninstall the Agent manually:

1 Open a command prompt and navigate to the <*Wavelink Avalanche Install Path*>`\Services` subdirectory.

2 In the command prompt, use the command `WLAvalancheService -u` to uninstall the Agent service.

To uninstall the Agent using Add/Remove Programs:

1 In the Control Panel, double-click the **Add/Remove Programs** icon.

The *Add/Remove Programs* dialog box appears.

2 Select the Wavelink Avalanche Manager program and click `Change/Remove`.

This uninstalls both the Agent service and the Management Console. If you want only the Agent removed, you must uninstall both and re-install the console only.

Managing an Agent from the Command Prompt

The Avalanche Manager Agent provides management functions through the command prompt. You can use these options to manage a local Agent.

To manage the Agent from the command prompt:

1. If the Agent is running, stop the Agent.
2. Open a command prompt and navigate to the `\Service` subdirectory where the Avalanche Manager was installed.
3. Run the following command:

```
WLAvalancheService <option>
```

The following options are currently supported:

`-v`	Displays version information
`-i`	Installs the service (the Agent)
`-u`	Uninstalls the service
-s	Starts the service
-q	Stops the service
-h	Launches the online help

Configuring the Agent Port

For communication between the Agent and the Management Console, Avalanche Manager uses port 1779 by default. You can change this port (for example, if another application on your network requires it) by modifying the `Avalanche.properties` file.

To change the Agent port:

1. Navigate to the Avalanche Manager installation directory (by default, `C:\Program Files\Wavelink\Avalanche`).
2. Use a text editor such as Notepad to open the file named `Avalanche.properties`.

3 Type an entry on a new line in the file, using the BindInfoForConsoleService property. Use a syntax based on one of the following examples:

```
BindInfoForConsoleService=10.22.117.2
```

The preceding example instructs the console to use the default port, 1779, when communicating with the Agent at the specified IP address.

```
BindInfoForConsoleService=10.22.117.2:1818
```

The preceding example instructs the console to use the port 1818 when communicating with the Agent at the specified IP address.

```
BindInfoForConsoleService=1818
```

The preceding example instructs the console to use port 1818 when communicating with any Agent.

4 Save and close the `Avalanche.properties` file.

Backing Up an Agent

When you back up an Agent, you back up all configuration information associated with the Agent.

You can use this feature to quickly duplicate the system configuration on any local or remote Agent.

The system configuration is backed up to the current Agent, then to a file on the local machine with a `.ABK` extension.

To back up an entire system configuration for an Agent:

1 Connect to the Agent containing the system configuration you want to back up. See *Connecting to an Agent* on page 170 for more information.

2 Select `Backup/Restore Agent` from the **File** menu.

The Avalanche Agent Backup/Restore wizard appears. The first step in this wizard is to determine if you want to backup your system or restore it.

3 Select the **Make an Agent backup** option and click `Next`.

The next step in this wizard is to determine what files you want to back up.

4 Select the files that you want to back up by enabling the checkbox next to each entry. When you are finished, click `Next`.

The next step in this wizard is to determine where the backup file will be stored.

5 Enter the full path where the backup file will be stored, or click `[...]` to browse to a location. When you are finished, click `Next`.

A backup of the Avalanche Agent will be created in the specified directory.

6 Click `Finish`.

Restoring an Agent

You can restore an Agent configuration to any local or remote Agent. The Agent will overwrite all older information when you restore the system configuration, except licensing information, which is resident on the local system.

To restore an entire system configuration for an Agent:

1 Connect to the Agent where you want to restore the system configuration. See *Connecting to an Agent* on page 170 for more information.

2 Select `Backup/Restore System` from the **File** menu.

The Avalanche Agent Backup/Restore wizard appears. The first step in this wizard is to determine if you want to backup your system or restore it.

3 Select the **Restore from an Agent backup** option and click `Next`.

The next step in the wizard is to determine which backup file from which you want to restore.

4 Enter the full path where the backup file is stored, or click `[...]` to browse to a location. When you are finished, click `Next`.

The next step in this wizard is to determine what files you want to restore.

5 Select the files that you want to restore by enabling the checkbox next to each entry. When you are finished, click `Next`.

The Agent settings will be restored from the backup file.

6 Click `Finish`.

Removing Mobile Devices

Under normal operation, the Avalanche Manager Agent maintains a record of each mobile device in its database to help track current software levels, etc.

If removing a record from the database is desired, the following method is provided.

To remove a mobile device from the database:

1 Right-click on the mobile device targeted for removal within the List View and select `Remove Client` from the context menu.

2 At the confirmation prompt, click `Yes` to confirm removal of the mobile device record from the Agent database.

Chapter 8: Serial Ports

When you connect to an Avalanche Manager Agent, the Agent attempts to automatically detect available serial ports. You must verify that a COM port is available to the Avalanche Manager Agent before you can download packages over a serial connection or download hex files with the hex file download utility.

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.

NOTE The presence of the Avalanche Management Console on the local system is not required. To manage the Agent from a remote console, you must connect to the Agent from the console using a routable IP address.

The topics in this sections include:

- Verifying the Status of a Port
- Adding a Port
- Configuring a Port
- Removing a Port

Verifying the Status of a Port

To check the status of 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`.

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

Adding a Port

If the available communication ports were not detected when you connected to the Agent, you can still instruct the Agent to detect ports automatically. In addition, you can manually add serial ports.

To detect available COM ports automatically:

1. Right-click the **Serial Ports** icon from the Tree View and select `Auto-detect Available Ports`.

2. If the *Enter Password* dialog box appears, type the password, `access`, and click `OK`.

A message box displaying the results of the port detection appears.

To manually add an available port:

1. Right-click the **Serial Ports** icon from the Tree View and select `Manually Add a Port`.

   The *Add Serial Port* dialog box appears.

2. Select the port device name from the drop-down list and click `OK`.

   The Avalanche Manager will validate the port name before adding the new port.

3. In the Tree View, double-click the new port name.

   The port information appears in beneath the new COM port in the Tree View.

4. Verify that the port is available. The status of an available port is `Listening`.

Configuring a Port

For any typical operation, port settings should *not* be modified from the default settings. The default port communication settings are:

- 38,400 bps connection speed

- 8 data bits

- 1 stop bit
- No parity
- No flow control
- Default download acceleration (70%)

In the event that port settings must be modified, the means to modify these settings is provided.

To modify port settings:

NOTE Changing the port settings from the default values will prevent mobile devices from connecting to the Avalanche Manager Agent if the new settings do not match. It is recommended that you do not change any port settings from the default values. However, if you are experiencing numerous retries when attempting serial downloads, you can reduce the download acceleration without modifying any other port settings.

1. Right-click on the desired COM port in the Tree View and click `Settings`.

   The *Serial Port Settings* dialog box appears.

2. Click `Modify`.

   A warning message box appears informing you that the COM port must be disconnected before you can modify its settings. The warning also describes the possible loss of connectivity with mobile devices.

3. If you want to continue, click `Yes`.
4. Modify settings as desired.
5. Click `Save`.
6. Click `OK`.

Removing a Port

If a port is already in use by another peripheral, it is recommended that you remove that port from the available ports of the Avalanche Management Console.

To remove a port:

1 In the Tree View, right-click the port targeted for removal and select `Delete Port`.

A message box appears asking you to confirm that you want to delete the selected port.

2 Verify that the correct port will be removed and click `Yes`.

Chapter 9: Avalanche Gateways

Avalanche Manager allows you to use Microsoft ActiveSync connections that exist on the system that hosts the Avalanche Manager Agent. Avalanche Manager can automatically detect these connections and create a gateway that allows you to use the connection to facilitate Avalanche communication between the Avalanche Manager Agent and a mobile device. The communication medium over which the ActiveSync session has been established does not matter; the communication medium can be serial, USB, IrDA, or RF.

You can use an Avalanche Gateway to perform the following types of tasks:

- Update an Avalanche client
- Install a network profile to an Avalanche client
- Install a Windows CE Avalanche Enabler on a mobile device

This section provides the following information:

- System Requirements
- Opening a Local Gateway
- Disconnecting a Local Gateway

System Requirements

To use the Local Gateway feature of Avalanche Manager, ensure that the host system meets the following requirements:

- Microsoft ActiveSync 3.7.1 or later version

NOTE Uninstalling Microsoft ActiveSync removes registry values that Avalanche Manager uses to create the Local Gateway.

NOTE If you reinstall Microsoft ActiveSync, you will need to reinstall Avalanche Manager 3.5.

Opening a Local Gateway

Before you can use a Gateway, you must allow Avalanche Manager to open the Gateway to the ActiveSync connection. You can open a Gateway from the Tree View of Avalanche Manager.

To open a Local Gateway:

1 In the Tree View, locate and right-click **Avalanche Gateways**.

A single-item menu list appears.

2 Select `Auto Connect Local Gateways`.

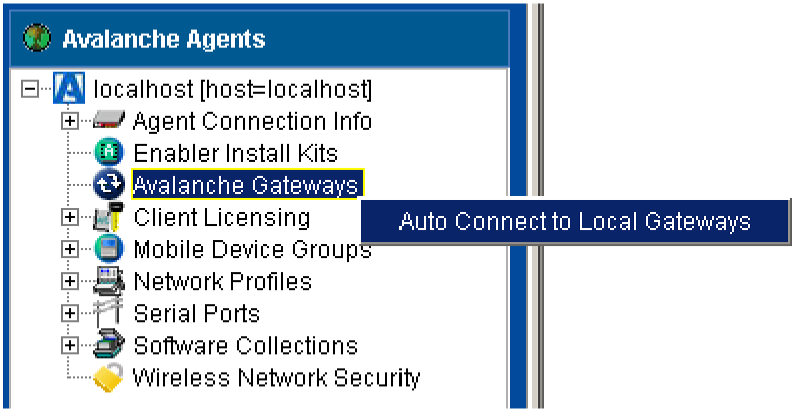


Figure 9-1. *Connecting to a Local Gateway*

Any Local Gateways on the host system are detected.

After a Local Gateway is detected, it appears beneath **Avalanche Gateways** in the Tree View.

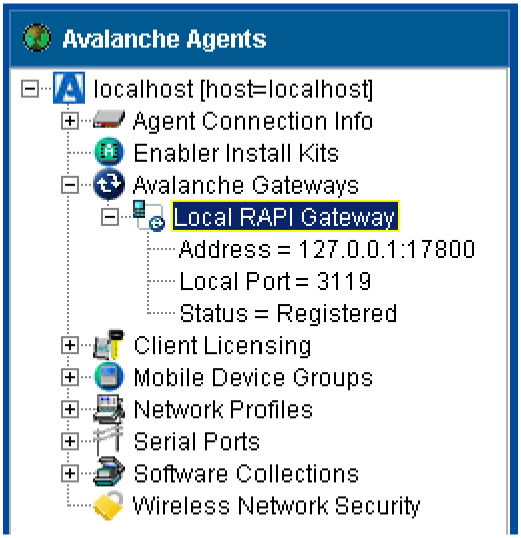


Figure 9-2. *Local Gateway*

3 Establish a Microsoft ActiveSync connection between the host system and the mobile device.

NOTE The Avalanche Manager Agent must reside on the host system.

NOTE You may use either a Guest or a Standard Microsoft ActiveSync partnership.

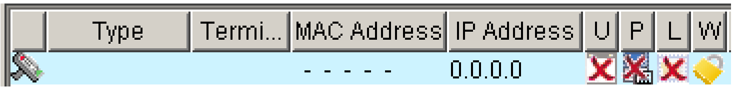
When the Microsoft ActiveSync connection is complete, Avalanche Manager will detect the connection and use the Local Gateway to perform any necessary Avalanche updates. If Avalanche Manager does not initially detect the connection, physically disconnect and then reconnect the mobile device to the host system.

If the mobile device already has an Enabler, it will register with the Avalanche Manager and perform any necessary updates.

If the mobile device does not have an Enabler, then Avalanche Manager will attempt to detect the device type, operating system, and other parameters. If the parameters match the selection criteria for any of the

Enabler Install Kits that are installed, Avalanche Manager will download and install on the mobile device the Enabler with the best match.

If Avalanche Manager is not able to locate an Enabler for a mobile device, then it will not attempt to download and install an Enabler. Mobile devices without an Enabler will appear in the Device View of Avalanche Manager until they are erased.



	Type	Termi...	MAC Address	IP Address	U	P	L	W
			- - - - -	0.0.0.0	✗	✗	✗	

Figure 9-3. *Orphan Mobile Device*

It is important to note that Avalanche updates over the Local Gateway occur only when Avalanche Manager detects a new ActiveSync connection. You cannot use the Avalanche Manager `Update Now` menu option to push updates over the Local Gateway connection. Likewise, you cannot use the cannot use the `Connect` feature of the Avalanche Enabler to perform an update over the Local Gateway.

Disconnecting a Local Gateway

Even when the Microsoft ActiveSync connection is terminated, Avalanche Manager still maintains the Local Gateway connection. If you no longer need to use a Gateway, you can manually disconnect or otherwise delete the Gateway from Avalanche Manager.

To disconnect a Local Gateway:

1 Connect to the Avalanche Manager Agent.

2 In the Tree View, locate and right-click the Local Gateway that you want to disconnect.

A single-item menu list appears.

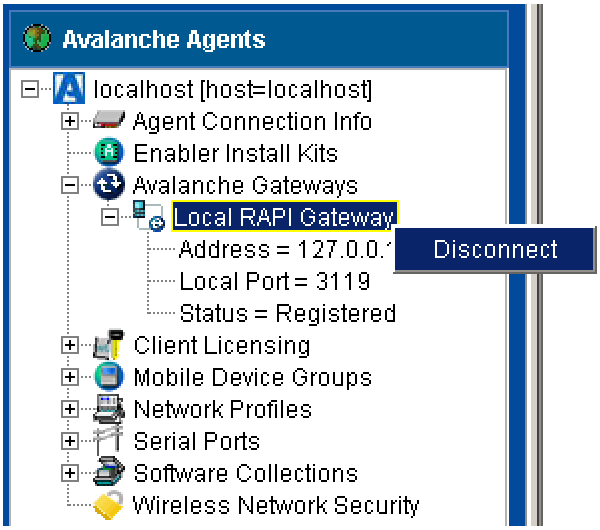


Figure 9-4. *Disconnecting a Local Gateway*

3 Select `Disconnect`.

The Local Gateway is removed from the Tree View.

Chapter 10: WEP Encryption

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 mobile devices and access points, allowing them to securely communicate with each other.

NOTE The Avalanche Manager only tracks the WEP keys that were assigned to mobile devices through the Management Console. Consequently, WEP keys displayed manually might not match the keys in the Avalanche Manager.

Types of WEP Key Deployments

The Avalanche Manager offers you two methods of deploying WEP keys to your mobile devices. First, you can deploy static WEP keys. However, this type of deployment has been shown through numerous studies to be vulnerable to decryption.

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

NOTE Automatic WEP is supported on DOS devices using version 1.61-00 or better of the Avalanche Enabler. In addition, the DOS TN Client version must be 4.16-40 or better. For information about CE devices that support automatic WEP, contact Wavelink at (801) 316-9000.

Static WEP

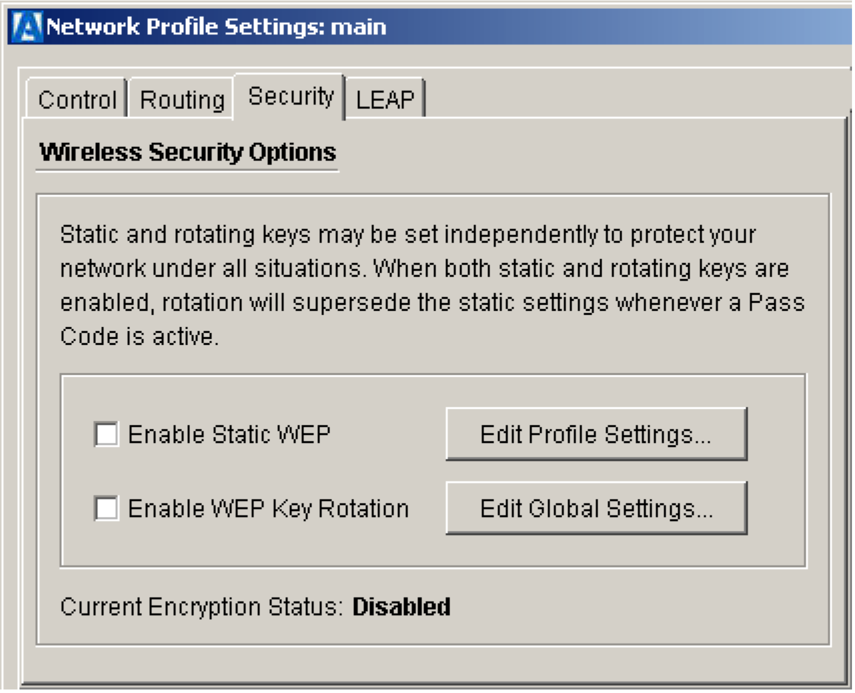
You secure your wireless network by assigning static WEP keys to mobile devices on the network. The Avalanche Manager supports both 40-bit and 128-bit encryption.

To set WEP Keys for mobile devices:

1 In the Tree View of the Avalanche Manager, double-click the desired network profile. The *Network Profile Settings* dialog box appears (see Figure 5-1).

2 Select the **Security** tab.

The following dialog box appears.



Wireless Security Options

Static and rotating keys may be set independently to protect your network under all situations. When both static and rotating keys are enabled, rotation will supersede the static settings whenever a Pass Code is active.

☐ Enable Static WEP

☐ Enable WEP Key Rotation

Current Encryption Status: **Disabled**

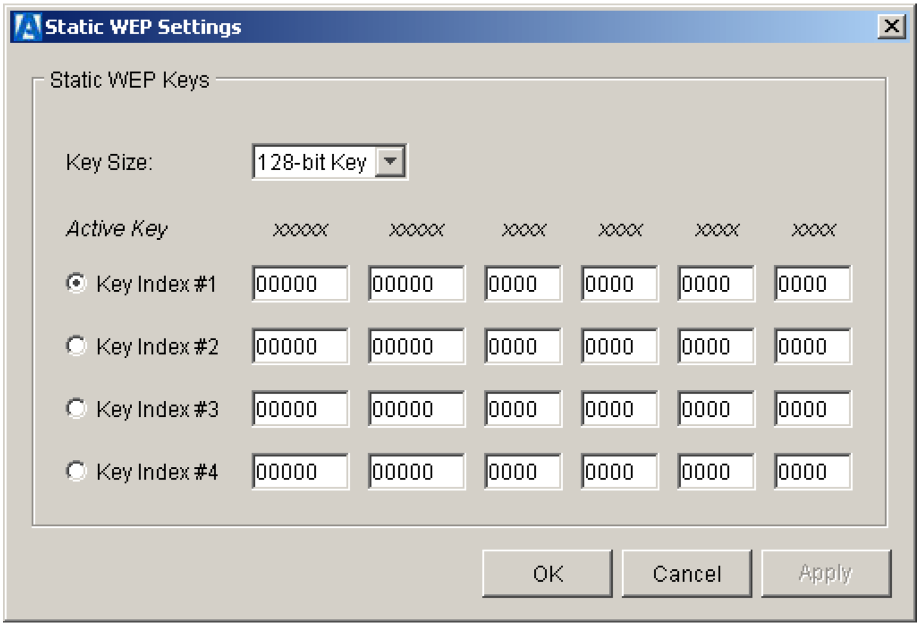
Figure 10-1. *The Network Profile Security Dialog Box*

3 For static WEP implementations, enable the **Use Static WEP Keys** checkbox.

NOTE If you want to use the automatic WEP implementation, enable the **Enable WEP Key Rotation** checkbox. See *Automatic WEP Rotation* for more information.

4 Click `Edit Profile Setting`.

The *Static WEP Settings* dialog box appears.



Static WEP Settings

Static WEP Keys

Key Size: 128-bit Key

Active Key	xxxxx	xxxxx	xxxx	xxxx	xxxx	xxxx
● Key Index #1	00000	00000	0000	0000	0000	0000
○ Key Index #2	00000	00000	0000	0000	0000	0000
○ Key Index #3	00000	00000	0000	0000	0000	0000
○ Key Index #4	00000	00000	0000	0000	0000	0000

Figure 10-2. *The Static WEP Settings Dialog Box*

5 Select either 40-bit or 128-bit encryption from the **Key Size** drop-down list.

6 Enter desired WEP keys in the **Static WEP Keys** group box.

For 40-bit encryption, enter 10 hex digits (between 0-9 and A-F).

For 128-bit encryption, enter 26 hex digits (between 0-9 and A-F).

7 Select the **Key Index** # option for the WEP key you want to activate.

The activated WEP key will download to each mobile device the next time its Enabler activates.

8 Click `OK`.

9 Verify that the network profile is enabled by right-clicking the profile in the Tree View and selecting `Enable Profile`.

NOTE You must ensure that any access points to which the mobile devices will connect share the same WEP key as the mobile devices. If the keys do not match, the mobile device cannot communicate with the access points.

Automatic WEP Rotation

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

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

Automatic WEP rotation fortifies WEP implementation on several levels. First, the keys used by access points and mobile devices in automatic WEP rotation 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.

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 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, 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 apply to all network profiles configured to use the automatic WEP feature—you cannot set multiple automatic WEP parameters for different profiles.

Avalanche and Mobile Manager

For any type of WEP encryption to be successful, both mobile devices and access points must know the WEP key used to decrypt and encode transmissions. Because automatic WEP rotation constantly creates and rotates WEP keys, the intervals and parameters used to change the WEP keys for your mobile devices must be synchronized with your access points.

To synchronize automatic WEP rotation settings on both mobile devices and access points, you must use the Wavelink Avalanche Manager and Mobile Manager products simultaneously, matching the settings for WEP rotation on each product. The Avalanche Manager handles the automatic WEP rotation configurations for your mobile devices, while Mobile Manager handles those same settings for your access points.

NOTE You cannot implement automatic WEP unless you use both the Avalanche Manager and Mobile Manager products.

Information on Mobile Manager and how it can improve your wireless network management can be found on the Wavelink Web site, www.wavelink.com.

Configuring Automatic WEP

You can configure only one set of automatic WEP rotation parameters for each Avalanche Manager Agent. These parameters can only be applied to mobile devices through a network profile.

Automatic WEP rotation also requires a starting time, which instructs the Agent when to initiate your settings. This starting time facilitates the synchronization between the Avalanche Manager and Mobile Manager products. When you first implement automatic WEP rotation, you can set the start time to be any time that you want. Any time you make changes to your automatic WEP configuration, you must set the start time to be 48 hours or more from the current time and date. This safety measure ensures correct synchronization between Wavelink products.

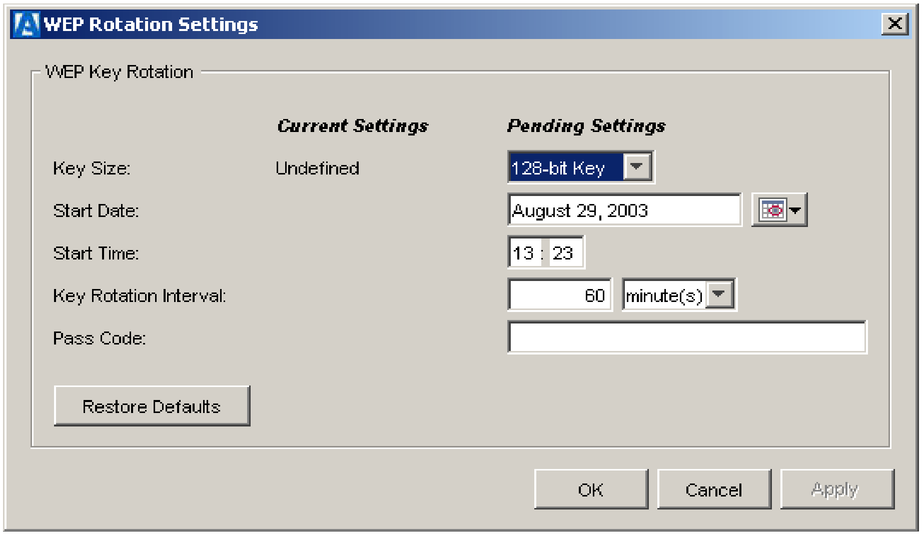
NOTE Automatic WEP rotation is supported on DOS devices using version 1.61-00 or better of the Avalanche Enabler. In addition, the DOS TN Client version must be 4.16-40 or better. For information about CE devices that support automatic WEP rotation, contact Wavelink at (801) 316-9000.

To configure automatic WEP:

1 Connect to the Avalanche Manager Agent.

2 Select `Wireless Network Security` from the **Security** menu.

The *WEP Rotation Settings* dialog box appears.



WEP Rotation Settings

WEP Key Rotation

	Current Settings	Pending Settings
Key Size:	Undefined	128-bit Key
Start Date:		August 29, 2003
Start Time:		13 : 23
Key Rotation Interval:		60 minute(s)
Pass Code:		

Figure 10-3. *The WEP Rotation Settings Dialog Box*

3 Determine the size of the WEP keys you want to use by selecting either `40 Bit Key` or `128 Bit Key` from the **Key Size** list.

The default option is `Undefined`, which prevents the implementation of WEP key rotation.

To stop active WEP rotation, select `Stop Rotation` from the **Key Size** list. When you stop rotation, the WEP key rotation interval passes and disables WEP key rotation. If static WEP keys were previously configured, Avalanche Manager implements static WEP. Otherwise, network communication reverts to open (no encryption).

4 Select the start date when you want to initiate automatic WEP rotation in the **Start Date** text box.

The button showing the current date allows you to select the start date from a pop-up calendar.

5 Type the start time when you want to initiate automatic WEP rotation in the **Start Time** text box by entering the appropriate values for hours and minutes.

Hours are in 24 hour military time. For example, 14 in the hours portion of the **Start Time** text box is equivalent to 2:00 pm.

NOTE The start time you select depends on whether you are implementing WEP for the first time or modifying existing settings. If you are implementing automatic WEP for the first time, the start time can be any time you require. If you are modifying settings, the start time must be more than 48 hours later than the current time and date.

6 Type the frequency of WEP key rotation in the **Key Rotation Interval** text box.

The default value is `60`. To define this value, select either `hours` or `minutes` from the drop-down list to the right.

The value in the **Key Rotation Interval** text box determines when the Avalanche Manager rotates and replaces WEP keys. For example, if you type `120` in this text box, WEP keys are rotated for each mobile device every two hours and an existing WEP key is replaced by a newly-generated one.

NOTE The bit key, start date, start time, rotation interval, and passcode must exactly match the same WEP key rotation settings in Mobile Manager. If you have the current versions of Mobile Manager and Avalanche, WEP key rotation settings that you configure for one Agent automatically are configured for the other if both Agents reside on the same host system.

7 Type the passcode in 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 generate unique WEP keys for your mobile devices without having to modify them manually.

8 Click `OK`.

You can now use this automatic WEP rotation setup for your network profiles.

To implement automatic WEP rotation:

1 Right-click a network profile from the Tree View and select `Settings`.

2 Click the Security tab.

3 Enable the **Enable WEP Key Rotation** checkbox.

4 Repeat this procedure for any other network profiles in use.

Chapter 11: Log Filter

The Avalanche Manager Agent automatically generates logs based on specific events that occur. These logs are stored in the `\Wavelink\Avalanche\Service` subdirectory. The name of the log file is `Avalanche.log`.

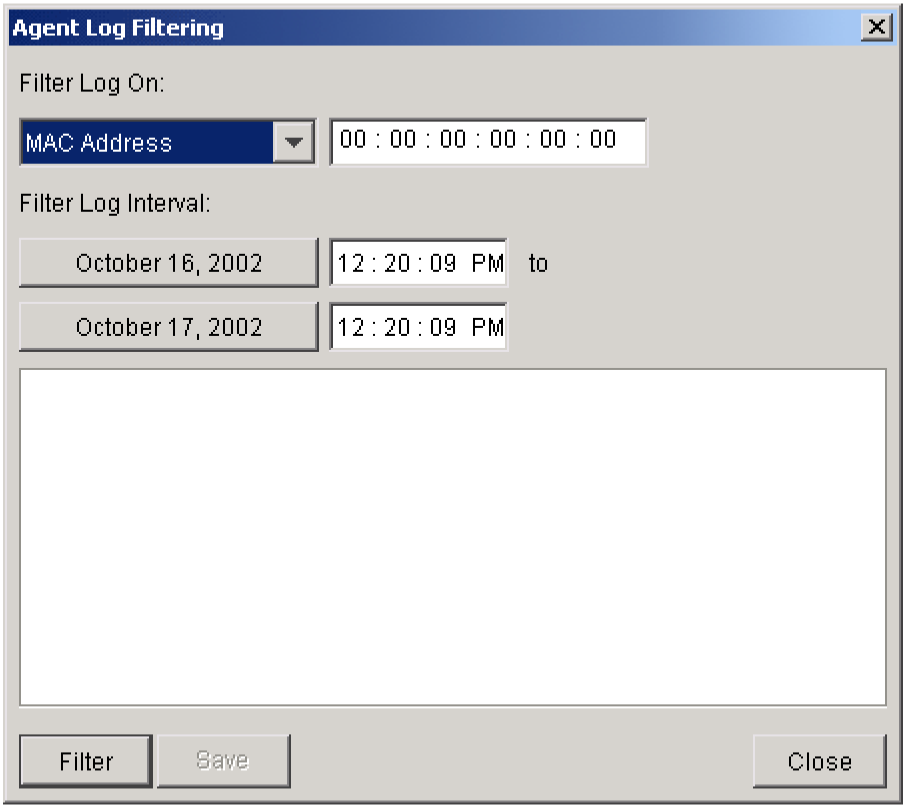
You can filter log files based on the MAC address of a specific mobile device. When the log files are set for a specific MAC address, only data generated for that device will be included in the log file.

NOTE See *Logging Options* on page 86 for information about setting logging options in the Management Console.

To filter the log:

1 Select `Filter Log` from the **Tools** menu.

The following dialog box appears.


Agent Log Filtering

Filter Log On:

MAC Address

00 : 00 : 00 : 00 : 00 : 00

Filter Log Interval:

October 16, 2002 12 : 20 : 09 PM to

October 17, 2002 12 : 20 : 09 PM

Figure 11-1. *Log View Controls Dialog Box*

2 In the **MAC Address** text box, type the MAC address of the mobile device for which you want to view the pertinent log data. The full string of the MAC address is required. This field is case sensitive.

3 In the **Date/Time Range** text boxes, enter a start date for logging information in the left text box and an end date for logging information in the right text box.

4 Click `Filter`.

If a previous version of the log exists, a message prompt will appear asking if you want to create a new log. If you want to overwrite the old log, click `Yes`.

The log filtered for the specific MAC address appears.

When you click `View Log`, the Agent creates a copy of `Avalanche.log`, names it `AgentAvalanche.log`, and places it in the root directory of the Management Console, `\Wavelink\Avalanche`. This log file is used by the log viewer.

The following information appears in the log:

Type The first column displays the log message type. These correspond to the log levels described in *Logging Options* on page 86:

CR - Critical error
ER - Error message
IN - Informational
WA - Warning
DB - Debugging information

Date The second column shows the date the message occurred.

Time The third column shows the time the message occurred.

Description The fourth column provides a description of the logged message.

Appendix A: Troubleshooting

This section is designed to assist system administrators with the most common problems encountered when using the Avalanche product. The first section of this appendix contains a summary of problems and causes. The remaining sections of this appendix provide detailed information to resolve problems based on the following issues:

- Mobile device is not communicating (cannot ping device)
- Mobile device is not communicating (can ping device)
- Mobile device IP address assignment problems
- Mobile device cannot connect to host
- Software package download problems
- Mobile device flash drive is full

Summary

The troubleshooting summary logically groups problems based on their type:

- Problems downloading a hex file (DOS devices only)
- Problems synchronizing with the Avalanche Manager Agent
- Enabler configuration problems
- Host communication problems

Problems Downloading a Hex File

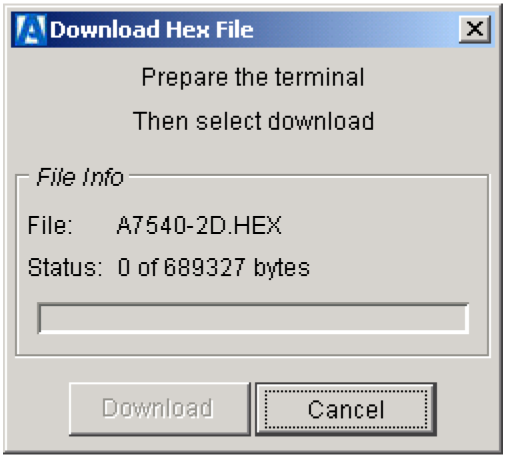
NOTE The errors in this section are specific to DOS-based devices that use the download utility included with the Management Console.

Download button is gray or not enabled in the Download Hexfiles dialog box.

- Incorrect port selected
- No hex file selected

Download button is gray or not enabled in the communications port dialog box (See Figure 12).

- Null modem cable is not found, not connected properly, defective or damaged.
- Cradle is not powered or powered with the wrong power supply.
- The mobile device is not seated properly within the cradle.



Prepare the terminal

Then select download

File: A7540-2D.HEX

Status: 0 of 689327 bytes

Figure 12. *Communications Port Dialog Box with Configuration Problem*

Download button is gray or not enabled on the communications port dialog box on the Management Console (See Figure 12). Awaiting DSR appears momentarily on the mobile device and then Status 0020 is displayed.

- A straight through cable is employed rather than a null modem cable.

Communications port dialog box on the Management Console displays a status of "Download Aborted - Lost DSR" and the mobile device shows a status of 0004.

- The parity setting on the mobile device does not match that of the Avalanche Manager.

One of the status codes in Table 1 appears on the mobile device.

- Refer to Table 1 for status code meanings.

- Status code 0200 during download indicates poor communications between the Avalanche Manager Agent and the cradle. This might be due to the integrity or length of the cable.

	Meaning
0000	Download was successful
0002	Receive overrun error
0004	Receive parity error
0008	Receive framing error
0010	Programming voltage not present
0020	DSR or CD not detected on open
0080	ABORT key hit during comm
0100	CD lost during session
0200	Illegal Intel hexadecimal record
0400	Unsupported Intel record
0600	NVM EEPROM failed to erase
0800	Receive time-out error
1000	Control start character time-out
2000	Clear To Send inactive time-out error
4000	Receive buffer full

Table 1: *Download HEX file Communication Status Codes*

Communications port dialog box on the Management Console displays a status of "Download Aborted - Lost DSR" and the mobile device shows a status of 0040 after a download has begun.

- The mobile device was removed from the cradle during the middle of the file transfer.
- The cradle lost power during the file transfer.

Problems Synchronizing with the Avalanche Manager Agent

Mobile Device does not attach to the Avalanche Manager Agent using RF.

- Network setup is configured incorrectly in the Management Console.
- Mobile device network setup is incorrect.
- Either the Agent's or the mobile device's IP address is already in use.

- The Avalanche Manager setting within the mobile device is incorrect.

Refer to *Using a Wireless Connection* section under *Mobile Device Does Not Attach to the Agent* on page 231 to determine what the problem is.

Mobile device does not attach to the Avalanche Manager Agent using a serial connection.

- A full null modem cable is not being used.
- Cable is defective.

Refer to *Using a Serial Connection* section under *Mobile Device Does Not Attach to the Agent* on page 231 to determine what the problem is.

Mobile device attaches but the Avalanche Manager Agent doesn't try to download anything.

- The software package is not enabled.
- The software collection is not enabled.
- The software package already resides on the mobile device.
- The selection criteria of the software collection or software package may exclude the mobile device from receiving the software package.

Refer to *Mobile Device Attaches but No Download Attempt Follows* on page 233 for details.

Mobile device attaches and a download begins but fails when using serial or RF connection.

- Poor network conditions exist.
- Cradle or null modem might not meet the necessary specifications.

See *Mobile Device Attaches and a Download Begins but Fails* on page 235 for details.

Mobile device will not receive a software package that the Avalanche Manager Agent is trying to send.

- Mobile device flash disk is full.

See *Mobile Device Flash Drive is Full* on page 235 to resolve this issue.

Enabler Configuration Problems

I cannot ping the mobile device. The mobile device is not communicating at all.

- The firmware and the RF driver are mismatched.
- TCP/IP stack is configured improperly.
- TCP/IP address assignment method (i.e., IP pooling, BOOTP, DHCP) is not set up correctly.
- The network ID (i.e., ESS ID) does not match that of the RF network.
- Antennas for the access points might not be connected.
- The mobile device MAC address may not be present in an enabled Access Control List on an access point.

See *Mobile Device Is Not Communicating (cannot ping)* on page 212 and *Mobile Device IP Address Assignment Problem* on page 222 to assist with the solution.

I can ping the mobile device but the mobile device is not communicating.

- No host profile is configured for the Telnet client software application selected.
- The IP Address is in use by another node on the network.

See *Mobile Device is Not Communicating (Can Ping)* on page 221 to assist with the solution.

Host Communication Problems

Mobile Device cannot connect to the host.

- No Telnet software packages are found on the mobile device.
- A host profile is not configured for the Telnet software package in use.
- An error message occurred after an attempt to connect to the host was made.

Refer to *Mobile Device Cannot Connect to the Host* on page 226 for help to resolve the problem.

Mobile Device Is Not Communicating (cannot ping)

You Cannot Ping the Mobile Device

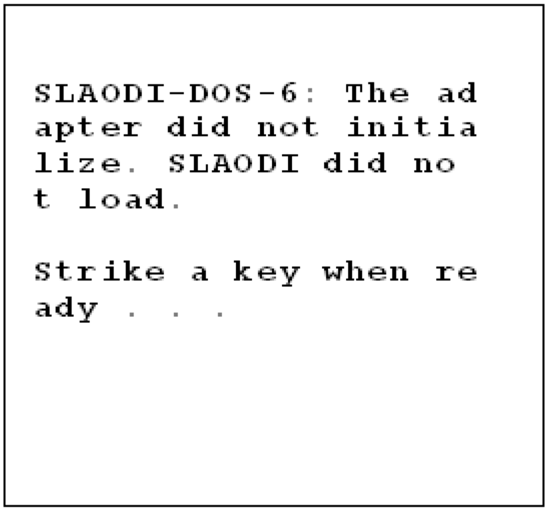
To resolve communication problems that occur in which you cannot ping the mobile device, you must consider the following additional factors:

- SLAODI (i.e., Radio Driver) is Not Loading
- SLAODI (i.e., Radio Driver) Loads
- TCP/IP Stack Fails to Load
- SLAODI (i.e., Radio Driver) Loads (cannot perform MAC level ping)

NOTE Although the types of errors in this section might be generic, recommended solutions may be specific to DOS-based or Symbol devices. The example screenshots and keypad commands included here are based on Symbol devices.

SLAODI (i.e., Radio Driver) is Not Loading

This is most likely due to a firmware mismatch. Refer to *Appendix B: RF Firmware and Radio Updates* on page 241. Figure 13 shows an example of a unsuccessful radio driver load when the mobile device boots. Watch a mobile device carefully after a boot is performed to view the data indicating an unsuccessful radio driver load.

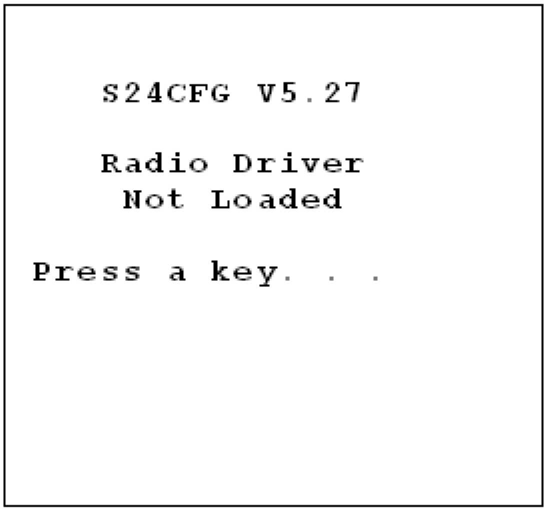


```
SLAODI-DOS-6: The ad
apter did not initia
lize. SLAODI did no
t load.

Strike a key when re
ady . . .
```

Figure 13. *Unsuccessful Radio Driver Load (Symbol)*

When accessing the Radio Configuration function in this state, the Terminal Info item within the Radio Parameters sub-menu displays a screen similar to that shown in Figure 14.



```
    S24CFG V5.27

    Radio Driver
     Not Loaded

Press a key. . .
```

Figure 14. *Terminal Info Also Displays Unsuccessful Radio Driver (Symbol)*

SLAODI (i.e., Radio Driver) Loads

The mobile device still doesn't communicate with the network

The SLAODI (i.e., radio driver) driver loaded, but you cannot ping the mobile device. Perform the steps described here to determine whether the problem is an RF problem or a TCP/IP configuration issue.

1 Telnet to the access point from a TCP/IP network node that has a VT100 Telnet Client.

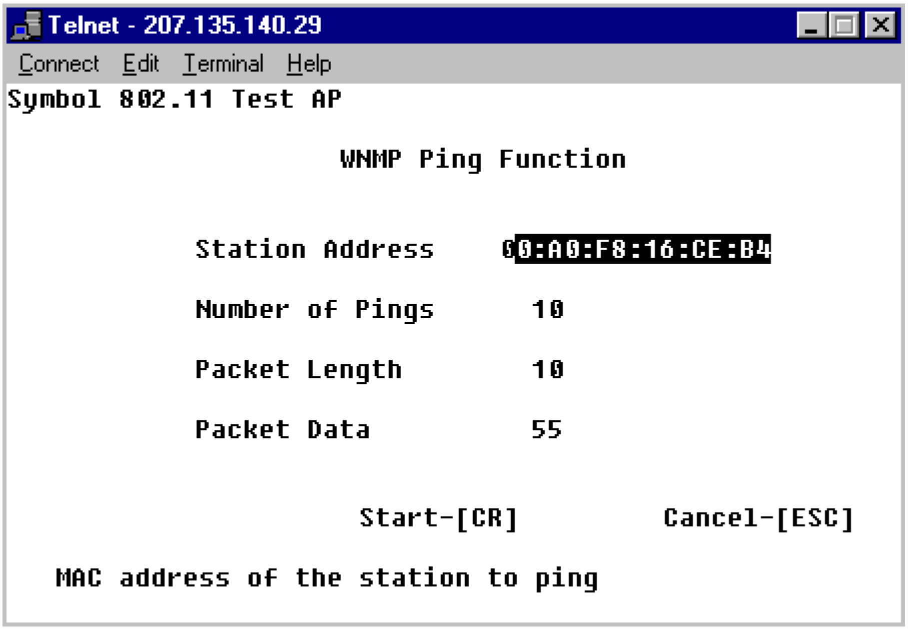
NOTE The keyboard commands here are specific to Symbol access points.

---

2 After logging into the access point, select `Show Mobile Units` from the Main Menu. If the MAC Address does not reside in the Mobile Units table, proceed to *You cannot Perform a MAC Level Ping to the Mobile Device* on page 216. If the MAC Address does appear in the Mobile Units table, highlight the MAC address in the Mobile Units table and select the access point ping option to perform a MAC Address ping to the mobile device. Once the ping starts, a screen similar to the one in Figure 15 appears.

3 Follow the instructions on the screen to perform the ping. Note the number of pings transmitted and received. If no pings are received from the mobile device, proceed to *You cannot Perform a MAC Level Ping to the Mobile Device* on page 216.

4 If the MAC level ping is successful, confirm the IP Address, the Subnet Mask, and IP Router Address with the network administrator.



```
Symbol 802.11 Test AP

                    WNMP Ping Function


           Station Address      00:A0:F8:16:CE:B4

           Number of Pings        10

           Packet Length          10

           Packet Data            55


                     Start-[CR]          Cancel-[ESC]

   MAC address of the station to ping
```

Figure 15. *Access Point Ping Function Screen*

TCP/IP Stack Fails to Load

Review the following possible causes in the order presented when the TCP/IP stack fails to load:

- CAUSE 1: No IP address for the mobile device is specified.
- CAUSE 2: BOOTP/DHCP setting does not acquire the IP address.
- CAUSE 3: The IP address assigned to the mobile device is already assigned to another mobile device.

CAUSE 1: No IP address for the mobile device is specified.

Specify an IP address for the mobile device in the Avalanche Enabler Configuration screen.

CAUSE 2: BOOTP/DHCP setting does not acquire the IP address.

Refer to *Mobile Device IP Address Assignment Problem* on page 222 to solve this problem.

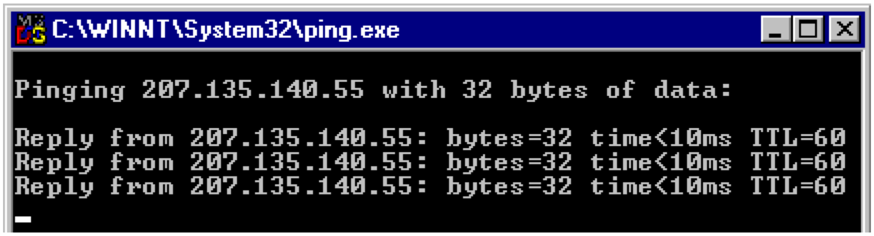
CAUSE 3: The IP address assigned to the mobile device is already assigned to another mobile device.

Perform the following steps to confirm:

1 Power off the mobile device.

2 Ping the mobile device from another TCP/IP node on the network. The example shown in Figure 16 demonstrates a ping performed from the Run window on a system using Windows NT 4.0.

3 If a response is achieved, this signifies that another network node is using this IP address. Contact the network administrator to attain a new IP assignment for the mobile device.



```
Pinging 207.135.140.55 with 32 bytes of data:

Reply from 207.135.140.55: bytes=32 time<10ms TTL=60
Reply from 207.135.140.55: bytes=32 time<10ms TTL=60
Reply from 207.135.140.55: bytes=32 time<10ms TTL=60
_
```

Figure 16. *Successful Ping from Windows NT 4.0 Machine*

SLAODI (i.e., Radio Driver) Loads

You cannot Perform a MAC Level Ping to the Mobile Device

Check the following possible causes in the order described:

- CAUSE 1: Possible protocol mismatch between the RF driver and firmware.
- CAUSE 2: Possible mismatch between the access points and the mobile devices.
- CAUSE 3: The antenna(s) for the access point(s) might be incorrect or missing.
- CAUSE 4: The network ID (i.e., ESS ID) might be configured incorrectly.
- CAUSE 5: The MAC address of the device might not be allowed by the access point.

CAUSE 1: Possible protocol mismatch between the RF driver and firmware.

For example, the mobile device could be using 802.11 firmware and the radio drivers could be Pre-802.11. Perform the steps displayed here to determine whether the mobile device is using 802.11 or Pre-802.11 (i.e., Spring) firmware.

1 Access the Avalanche Enabler Configuration screen (or the Config Menu screen) by pressing `FUNC,CTRL,R`. Type the password, `system`. Press the `Y` key to confirm terminating an active session.

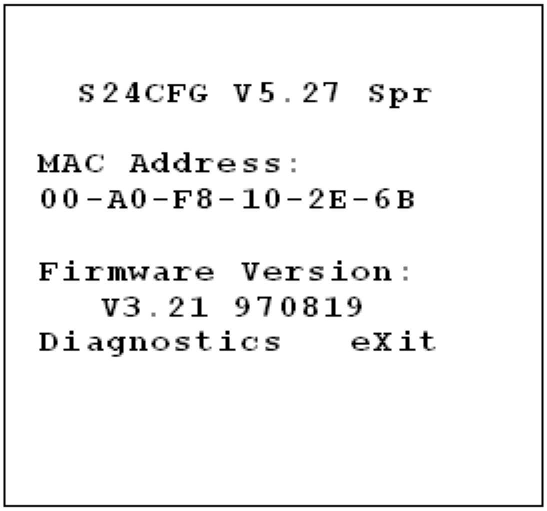
NOTE The keyboard commands in this example are specific to Symbol 3000 Series mobile devices.

---

2 From the Config screen, choose `Radio Parameters`.

3 At the Radio screen, select `Terminal Info`.

4 Verify the firmware version displayed on this screen. A version beginning with a 3 indicates the mobile device is utilizing Pre-802.11 (i.e., Spring protocol) whereas a firmware version beginning with a 4 specifies 802.11 protocol usage. See Figure 17.



```
  S24CFG V5.27 Spr

MAC Address:
00-A0-F8-10-2E-6B

Firmware Version:
   V3.21 970819
Diagnostics   eXit
```

Figure 17. *Terminal Info Screen (Symbol)*

5 Press the `X` key to exit this screen..

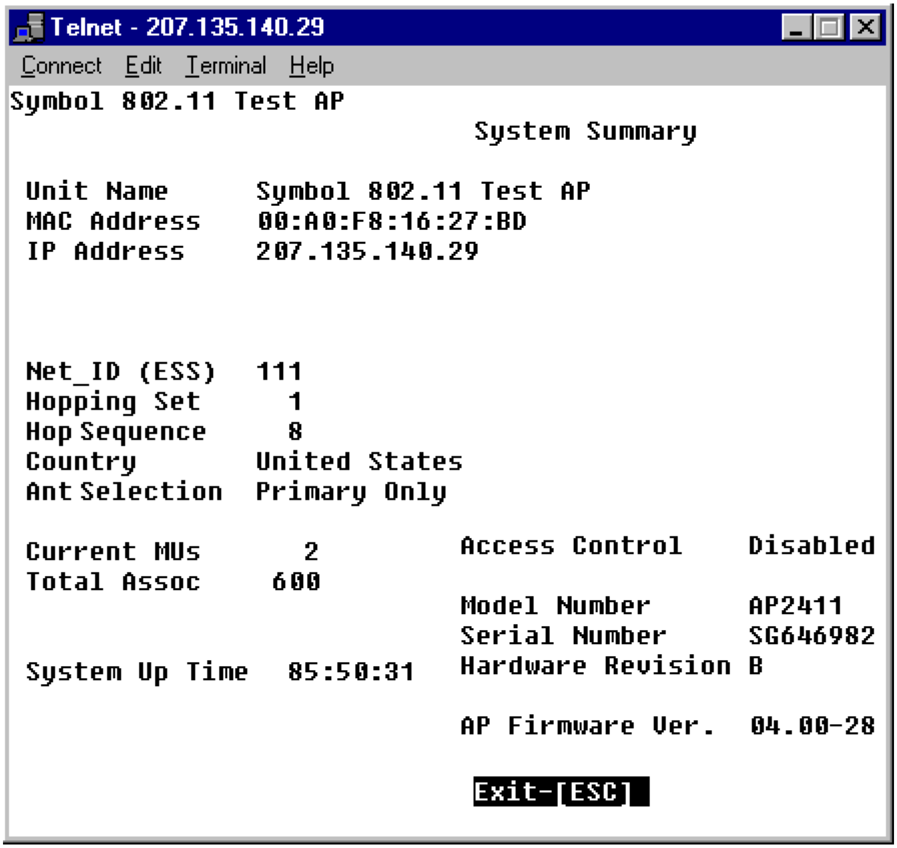
CAUSE 2: Possible mismatch between the access points and the mobile devices.

In this case, the access point might employ 802.11 radio protocol and the mobile device might employ the Pre-802.11 protocol or vice versa. Take the following steps to verify the type of access point:

1. Telnet to the access point from a TCP/IP network node that has a VT100 Telnet Client.

NOTE The keyboard commands here are specific to Symbol access points.

2. Type the password, `Symbol`, at the prompt to log into the access point.
3. Press `ESC` to bring up the Main Menu of the access point.
4. Select `Show System Summary` from the Main Menu. Note the access point firmware version. A version beginning with 3 indicates the access point is utilizing Pre-802.11 (i.e., Spring protocol), whereas an access point firmware version beginning with a 4 specifies an access point using the 802.11 protocol. See Figure 18.
5. Press `CTRL+D` to terminate the Telnet Session.



```
Symbol 802.11 Test AP
                             System Summary

 Unit Name      Symbol 802.11 Test AP
 MAC Address    00:A0:F8:16:27:BD
 IP Address     207.135.140.29



 Net_ID (ESS)   111
 Hopping Set      1
 Hop Sequence     8
 Country        United States
 Ant Selection  Primary Only

 Current MUs       2          Access Control    Disabled
 Total Assoc     600
                              Model Number      AP2411
                              Serial Number     SG646982
 System Up Time   85:50:31    Hardware Revision B

                              AP Firmware Ver.  04.00-28

                               Exit-[ESC]
```

Figure 18. *System Summary of 802.11 Access Point*

CAUSE 3: The antenna(s) for the access point(s) might be incorrect or missing.

Attach the correct antenna to the mobile device.

CAUSE 4: The network ID (i.e., ESS ID) might be configured incorrectly.

Check the network ID on the mobile device.

1 Access the Avalanche Enabler Configuration screen (or the Config Menu screen) by pressing `FUNC`, `CTRL`, `R`. Enter the password, `system`. Press the `Y` key to confirm terminating an active session.

2 From the Enabler Configuration screen, select `Radio Parameters`.

3 At the Radio screen, select `Radio Parameters`.

4 Note the active RF network ID (ESS ID). This must match the network ID being used in the access point.

NOTE Within the Enabler Configuration screen, `FUNC, 1` provides help to navigate the appropriate sub-screens.

Check the Network ID within the access point.

1 Telnet to the access point from a TCP/IP network node that has a VT100 Telnet Client.

2 Type the password, `Symbol`, at the prompt to log into the access point. Press `ESC` to bring up the Main Menu of the access point.

3 Select `Show System Summary` from the Main Menu. Note the access point Net ID. It should match the network ID configured on the mobile device. See Figure 18.

4 Press `CTRL+D` to terminate the Telnet Session.

CAUSE 5: The MAC address of the device might not be allowed by the access point.

Verify that the Access Control List Feature is being used in the access point. If it is, confirm that the MAC address of the mobile device is in the Allowed Mobile Devices list. Use these steps to confirm:

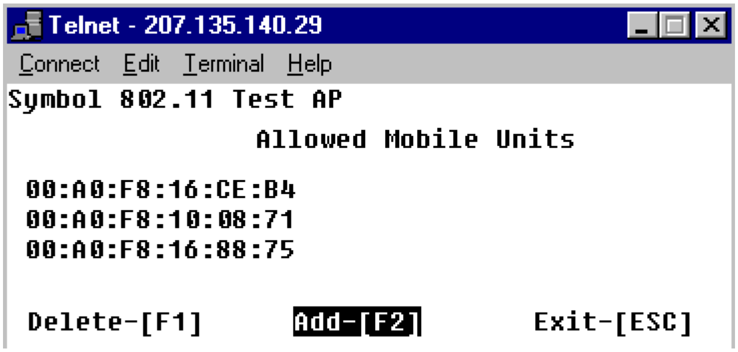
1 Telnet to the access point from a TCP/IP network node that has a VT100 Telnet Client.

2 Type the password, `Symbol`, at the prompt to log into the access point. Press the `ESC` key to bring up the Main Menu of the access point.

3 Select `Show System Summary` from the Main Menu. Note whether Access Control is enabled or not.

4 Choose `Select Access Control List` to view the allowed mobile devices for the access point. If the mobile device in use is not in the list, it will not be able to communicate with the network. See Figure 19.

5 Press `CTRL+D` to terminate the Telnet Session.



```
Symbol 802.11 Test AP
                    Allowed Mobile Units

 00:A0:F8:16:CE:B4
 00:A0:F8:10:08:71
 00:A0:F8:16:88:75

 Delete-[F1]          Add-[F2]          Exit-[ESC]
```

Figure 19. *Access Point Access Control List*

Mobile Device is Not Communicating (Can Ping)

You Can Ping the Mobile Device

NOTE Although the types of errors in this section are generic, recommended solutions may be specific to DOS-based or Symbol devices. The example screenshots and keypad commands included here are based on Symbol devices.

Check the following items in the order mentioned.

- CAUSE 1: No host profile is configured for the Telnet client software package.
- CAUSE 2: The IP address of the mobile device is assigned to another mobile device.

CAUSE 1: No host profile is configured for the Telnet client software package.

See *Mobile Device Cannot Connect to the Host* on page 226.

CAUSE 2: The IP address of the mobile device is assigned to another mobile device.

Use these steps to determine if this is the problem:

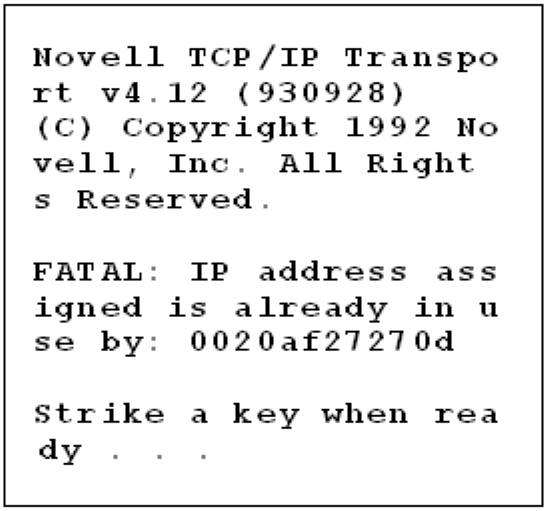
If the mobile device boots, do the following:

1 Power off the mobile device.

2 Ping the mobile device. See Figure 16 for sample ping.

3 If you can ping the mobile device while the mobile device is powered off, another mobile device or network node shares this IP Address. Contact your network administrator.

If the mobile device does not boot, and the mobile device displays a message similar to that seen in Figure 20 at boot time, the mobile device is sharing an IP Address with another node on the network. Contact your network administrator to resolve the problem.



```
Novell TCP/IP Transpo
rt v4.12 (930928)
(C) Copyright 1992 No
vell, Inc. All Right
s Reserved.

FATAL: IP address ass
igned is already in u
se by: 0020af27270d

Strike a key when rea
dy . . .
```

Figure 20. *Duplicate IP Address Message (Symbol)*

Mobile Device IP Address Assignment Problem

Resolution of problems pertaining to the assignment of IP addresses depends upon the following factors:

- IP address is not allocated using Manager IP pools
- IP address is not acquired using BOOTP
- IP address is not acquired using DHCP

NOTE Although the types of errors in this section are generic, recommended solutions might be specific to DOS-based or Symbol devices. The example screenshots and keypad commands included here are based on Symbol devices.

IP Address is Not Allocated Using IP Address Pools

The possible causes for this problem are as follows:

- CAUSE 1: No IP address pool exists.
- CAUSE 2: Incorrect activation or configuration of the IP address pool.
- CAUSE 3: The mobile device is not in a cradle.
- CAUSE 4: The mobile device fails to attach to the Avalanche Manager Agent.

CAUSE 1: No IP address pool exists.

Check to see if an IP address pool exists on the Management Console:

1 Right-click a network profile in the Tree View and select `Settings`.

2 Confirm whether the profile is set to use an IP address pool, based on the option selected in the **Client IP Assignment** list.

3 Repeat the preceding steps for each additional network profile.

CAUSE 2: Incorrect activation or configuration of the IP address pool.

Confirm the following items:

- The IP address pool is activated.
- IP addresses are available for mobile device (i.e., MAC Address) assignment.

Use the procedures shown here to verify the above items.

1 Open each network profile in the Tree View of the Management Console to determine which profile displays a status of `Active` beneath the branch.

If none of the network profiles are active, enable the one containing the desired IP address pool.

2. Right-click the active network profile and click `Settings`.

3. In the network profile dialog box, click `Edit IP Pool`.

   Note whether IP Addresses are available for assignment to mobile devices. See *Using an IP Address Pool* on page 95 for more information.

CAUSE 3: The mobile device is not in a cradle.

The Avalanche Manager Agent must assign the IP address via the serial connection when using an IP address pool, unless the network profile is configured to override settings on the mobile device. See *Assigning IP Addresses* on page 93 for more information.

CAUSE 4: The mobile device fails to attach to the Avalanche Manager Agent.

See *Mobile Device Does Not Attach to the Agent* on page 231 and refer to the *Using a Serial Connection* section.

IP Address is Not Acquired Using BOOTP

The possible causes for this problem are:

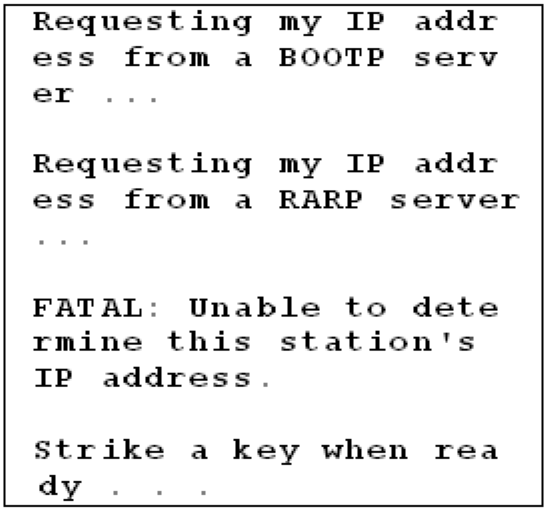
- CAUSE 1: BOOTP might not be selected on the mobile device.
- CAUSE 2: BOOTP server/relay agent might be down or absent, or IP addresses might not be available on the BOOTP server.

CAUSE 1: BOOTP might not be selected on the mobile device.

Review the Avalanche Enabler Configuration setup on the mobile device to ensure that BOOTP is selected as the IP address of the mobile device. See the appropriate Avalanche TN Client user guide for details.

CAUSE 2: BOOTP server/relay agent might be down or absent, or IP addresses might not be available on the BOOTP server.

When a message similar to the one shown in Figure 21 appears, contact the network administrator to verify that either a BOOTP server or BOOTP relay agent resides on the local network segment. In addition, determine whether IP Addresses are available on the BOOTP server.



```
Requesting my IP addr
ess from a BOOTP serv
er ...

Requesting my IP addr
ess from a RARP server
...

FATAL: Unable to dete
rmine this station's
IP address.

Strike a key when rea
dy . . .
```

Figure 21. *BOOTP Failure Message (Symbol)*

IP Address is Not Acquired Using DHCP

The possible causes are:

- CAUSE 1: The AVA3 update kit is not installed

NOTE If using Enabler version 1.59-00 or newer, the update kit is no longer required.

- CAUSE 2: DHCP is not selected on the mobile device
- CAUSE 3: DHCP server not present on the network segment, and/or the DHCP server has no IP addresses available.

CAUSE 1: The AVA3 update kit is not installed

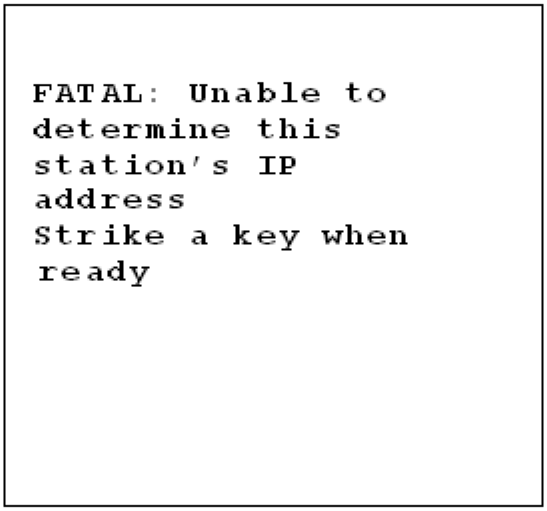
Refer to the appropriate Avalanche TN Client documentation for details on performing this task.

CAUSE 2: DHCP is not selected on the mobile device

Review the Enabler Configuration setup within the mobile device to ensure that DHCP is selected as the IP address of the mobile device. Refer to the appropriate Avalanche TN Client user guide for details.

CAUSE 3: DHCP server not present on the network segment, and/or the DHCP server has no IP addresses available.

When a message similar to the one shown in Figure 22 appears, contact the network administrator to verify that a DHCP server resides on the local network segment. In addition, ensure that IP addresses are available on the DHCP server.



```
FATAL: Unable to
determine this
station's IP
address
Strike a key when
ready
```

Figure 22. *IP Address not Assigned via DHCP (Symbol)*

Mobile Device Cannot Connect to the Host

NOTE Although the types of errors in this section are generic, recommended solutions may be specific to DOS-based or Symbol devices. The example screenshots and keypad commands included here are based on Symbol devices.

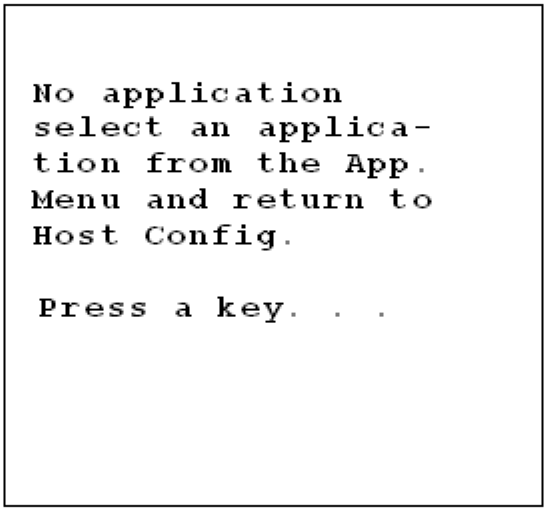
Review this section to determine what may be inhibiting the mobile device from communicating with the host. The possible causes are:

- CAUSE 1: No application selected (or present) on the mobile device.
- CAUSE 2: No host profile configured for the application.

- CAUSE 3: Cause related to a connection progress or connection error message that appeared.
- CAUSE 4: Cause related to a connection progress message that appeared.

CAUSE 1: No application selected (or present) on the mobile device.

When accessing the Host Profiles submenu from the Enabler Configuration function, the screen shown in Figure 23 appears.



```
No application
select an applica-
tion from the App.
Menu and return to
Host Config.

 Press a key. . .
```

Figure 23. *No Application Selected Screen (Symbol)*

This message means that no software applications have been selected. For example, the Avalanche Enabler has been loaded and configured, but no Telnet Client software packages reside on the mobile device. Download a Telnet Client software package to the mobile device and add a host profile to resolve this issue. Review the appropriate Avalanche TN Client user guide for more information.

CAUSE 2: No host profile configured for the application.

In this case, a message appears after an application is selected indicating that the mobile device cannot communicate with the host. This means there is no host profile configured with this application (see Figure 24). To resolve this problem, take the following steps:

1 Access the Avalanche Enabler Configuration screen (or the Config screen) by pressing `FUNC,CTRL,R`. Enter the password, `system`. Press the `Y` key to confirm terminating an active session.

NOTE The keyboard commands in this example are specific to Symbol 3000 Series mobile devices.

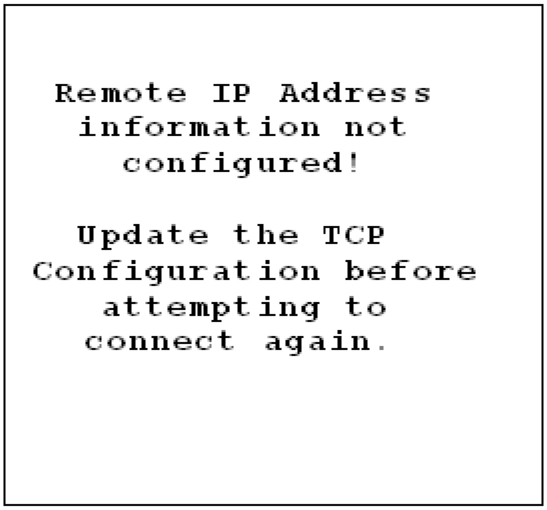
---

2 At the Config screen, select `Host Profiles` and press `ENTER`.

3 Press the `ENTER` key or use `CTRL+A` to add a new host profile.

4 Save the new host profile and exit the Enabler Configuration screens.

NOTE Within the Enabler Configuration screen, Function 1 provides help to maneuver on appropriate screens.



```
Remote IP Address
 information not
   configured!

  Update the TCP
Configuration before
   attempting to
  connect again.
```

Figure 24. *No Host Profile Created Message (Symbol)*

CAUSE 3: Cause related to a connection progress or connection error message that appeared.

The mobile device uses the following standard Telnet messages to inform the user of their connection progress and any error conditions that can occur. This section is intended to help diagnose any problems associated with error messages that appear when the mobile device is attempting to communicate with the host.

```
No host connection
```

- This is the standard "not connected" message. No errors are indicated.

```
Connection to xxxx Refused
```

- A connection to the host was made, but the host refused the connection—typically because it is out of resources, the telnet server software is down or it is not running on the selected port.

```
Connection to xxxx has Timed Out
```

- The host could not be located. Common reasons include:
    - The host is down.
    - The configured host address is incorrect.
    - The Enabler’s netmask and/or router address are incorrect.
    - The physical network is down.

  - The Spectrum 24 network is down (The access point is down or the Spectrum 24 Network ID is incorrectly configured).

  - Some hosts may cause a time out during connection if they are very busy, even though there are no configuration or hardware errors.

```
Negotiated emulation (xxxx) is not supported
```

- An emulation type has been negotiated with the host, but it is not a type that this client can support. Either the emulation type has been incorrectly configured, or the host does not support the type which was selected and has therefore negotiated down to another type.

```
Connection to xxxx has been terminated
```

Or:

```
Connection closed by foreign host
```

- The host closed the session, either by the user’s request or for its own reasons (inactivity time-out, host is going down, etc.) This message may also occur if communications fail while the session is up; failure may occur in either the physical or the wireless network.

```
Invalid server address: xxxx
```

Or:

```
Invalid remote IP address
```

In this case, there are two possibilities:

1. If the host profile contains the "name" of the host, then this error occurred because the "name" did not resolve into the IP address. Either the name is wrong, or the name server(s) are down.

NOTE If there is a long delay before getting this message, then the name server is most likely down. If the message comes back within a few seconds, then the name itself is probably wrong.

2. If the host profile contains the IP address of the host, then the address string contained an invalid character.

CAUSE 4: Cause related to a connection progress message that appeared.

This section is intended to help diagnose any problems associated with mobile device messages that are displayed when the session is establishing a connection.

```
Looking up host xxxx
```

- The client is checking DNS to resolve a host name.

```
Trying to connect to xxxx
```

- The client is currently attempting to connect to the host. This message will remain until a socket-level connection is made.

```
Connected to xxxx
```

- A socket-level connection has been made but the client is still waiting for the host to complete the telnet negotiations and send out the first screen.

The screen might arrive quickly or, if the host is slow, it can take a moment. If the screen does not arrive at all, then the host is having problems internally.

Software Package Download Problems

Resolution of problems that pertain to downloading software packages depend upon the following additional factors:

- Mobile device does not attach to the Agent
- Mobile device attaches but no download attempt follows
- Mobile device attaches and a download begins but fails

NOTE Although the types of errors in this section may be generic, recommended solutions may be specific to DOS-based or Symbol devices. The example screenshots and keypad commands included here are based on Symbol devices.

Review these items in the order they are presented.

Mobile Device Does Not Attach to the Agent

Resolution of this problem depends on whether you are using a wireless or serial connection:

Using a Wireless Connection

When using a wireless connection, the possible causes are:

- CAUSE 1: Incorrect network setup on the Avalanche Manager
- CAUSE 2: Incorrect network parameters on the mobile device or incorrect network configuration on the Management Console
- CAUSE 3: The IP address of the mobile device or the Avalanche Manager Agent may be in use on another network node.
- CAUSE 4: Incorrect IP configuration

CAUSE 1: Incorrect network setup on the Avalanche Manager

Verify the network setup on the Management Console. Make sure the adapter is functioning properly and the IP configuration is correct. Consult your Windows documentation for more information.

CAUSE 2: Incorrect network parameters on the mobile device or incorrect network configuration on the Management Console

Ping the mobile device from the Management Console. If the ping is unsuccessful, proceed with the steps shown here.

1. Ensure that the following mobile device network parameters are configured properly. These are:
   - IP Address
   - Subnet Mask
   - IP Router Address
   - Network ID (i.e., ESS ID)
2. Check the network configuration of the Management Console.

CAUSE 3: The IP address of the mobile device or the Avalanche Manager Agent may be in use on another network node.

When the ping from the Avalanche Manager to the mobile device is successful, check for duplicate IP addresses on the mobile device and the Avalanche Manager Agent.

If the mobile device boots, take the following steps:

1. Power off the mobile device or the system hosting the Avalanche Manager Agent depending on which IP address you are verifying.
2. Ping the mobile device or Avalanche Manager Agent from another network node. See Figure 16 for sample ping. If you can ping the mobile device or the Avalanche Manager Agent while either one is in the off position, another mobile device or network node shares this IP address. Contact your network administrator to fix this problem.

If the mobile device does NOT boot and displays a message similar to that seen in Figure 20 at boot time:

- The mobile device is sharing an IP Address with another node on the network. In this case, the TCP/IP stack did not load. Contact your network administrator.

CAUSE 4: Incorrect IP configuration

Verify the Avalanche configuration:

- Open the Avalanche menu item within the Avalanche Enabler Configuration screen to check the IP configuration for the Avalanche Manager Agent.

  If IP address for the Agent is empty, the mobile device performs a broadcast to find the Agent that responds first. However, if the Agent resides in one segment and the mobile device resides in another, you must enter the IP address of the Agent in the Version Control configuration form, and you must use the appropriate Router IP Address. Refer to the appropriate Avalanche TN Client user guide for more information.

Using a Serial Connection

When using a serial connection, the possible causes are:

- CAUSE 1: The null modem cable is not a full null modem
- CAUSE 2: Bad or incorrect cable

CAUSE 1: The null modem cable is not a full null modem

The serial connection is usable when downloading a HEX file, but the mobile device cannot communicate with the Avalanche Manager Agent. In this case, the null modem cable being used is not a full null modem (i.e., if fails to meet the specifications the cradle or the requirements of the mobile device). The null modem cable used must not block or loop back DSR because the Enabler uses it to detect the presence of the Avalanche Manager Agent.

CAUSE 2: Bad or incorrect cable

The serial connection does not allow HEX file downloads. The cable might be bad or incorrect for this type of communication. Refer to *Problems Downloading a Hex File* on page 207 for more information.

Mobile Device Attaches but No Download Attempt Follows

The possible causes are:

- CAUSE 1: The software package might be disabled.
- CAUSE 2: Software package may not be present on the mobile device.
- CAUSE 3: Selection criteria mismatch

CAUSE 1: The software package might be disabled.

To verify that the software package is enabled:

- Open the software package branch in the Tree View, and check the status of the package when information about the package appears beneath the branch.

  For a software package to download to the mobile device, the status must display `Active`. See *Using Software Packages* on page 113 for more information.

CAUSE 2: Software package may not be present on the mobile device.

To verify that the software package has been downloaded to the mobile device. Take the following steps:

1. Double-click on the mobile device in the List View.
2. Review the Avalanche Client Controls dialog box to find the status of software packages assigned to the mobile device. Refer to *Viewing Mobile Device Information* on page 135 for more information.

CAUSE 3: Selection criteria mismatch

The selection criteria of the software collection or the software package can be set to exclude this mobile device from the receiving the software package. To view the selection criteria:

- To view the selection criteria for the software collection, right-click on the software collection and select `Settings`.
- To view the selection criteria for the package, open the software package brnach in the Tree View.

See *Selection Criteria* on page 122 for information regarding selection criteria.

Mobile Device Attaches and a Download Begins but Fails

Fails using RF Connection

Poor network conditions may be causing the symptom to occur. See your network administrator. To confirm this condition, isolate the mobile device, an access point, and the Avalanche Manager Agent from the rest of the network and restart the wireless download.

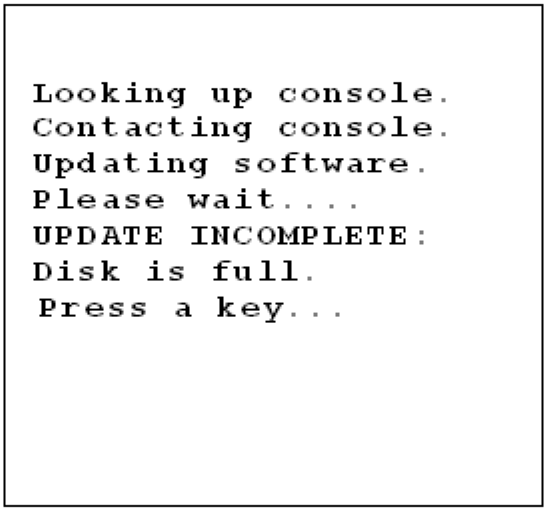
Fails using Serial Connection

Some older cradles tend to have difficulty with downloads. Make sure the cradle and null modem cable meet the specifications of the mobile device. See *Using a Serial Connection* under *Mobile Device Does Not Attach to the Agent* on page 231 for more details.

Mobile Device Flash Drive is Full

NOTE Although the types of errors in this section are generic, recommended solutions might be specific to DOS-based or Symbol devices. The example screenshots and keypad commands included here are based on Symbol devices.

The Avalanche Enabler displays a message when the flash drive is full (see Figure 25). Follow these steps to recover from this situation.

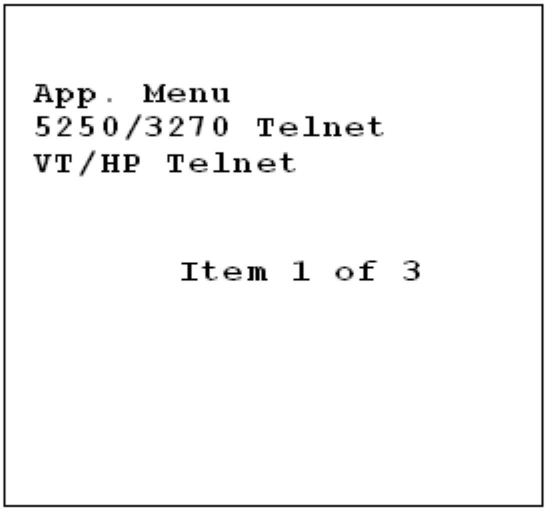


```
Looking up console.
Contacting console.
Updating software.
Please wait....
UPDATE INCOMPLETE:
Disk is full.
 Press a key...
```

Figure 25. *Flash Drive Full Message (Symbol)*

Take the following steps to clear the flash drive on a Series 3000 mobile device:

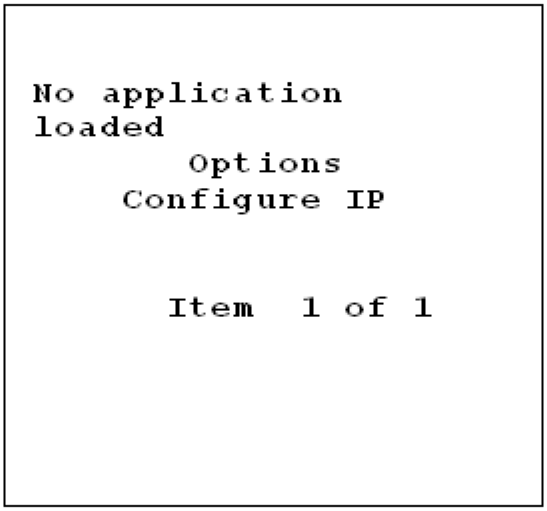
1 Cold boot the mobile device so that the App Menu screen shown in Figure 26 appears. If no application software packages are loaded on the mobile device, Figure 27 will appear. However, if the screen shown in Figure 28 appears, skip the next step.



```
App. Menu
5250/3270 Telnet
VT/HP Telnet


      Item 1 of 3
```

Figure 26. *App. Menu (Symbol)*

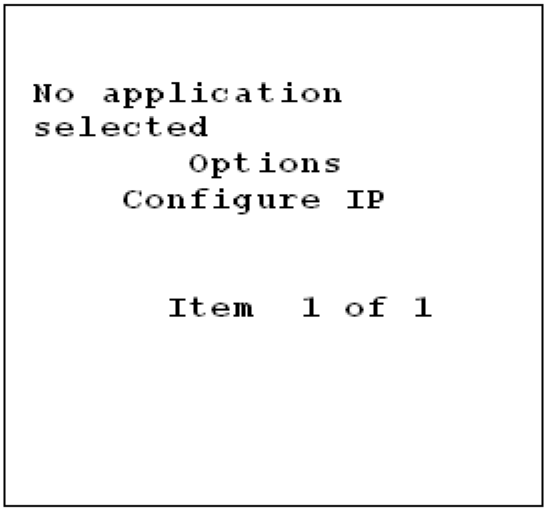


```
No application
loaded
      Options
   Configure IP


     Item  1 of 1
```

Figure 27. *No Application Loaded (Symbol)*

2 Press the `ESC` key (i.e., `CLEAR` on most mobile devices) from the screen shown in Figure 26. The following screen appears.



```
No application
selected
       Options
    Configure IP


      Item  1 of 1
```

Figure 28. *No Application Selected (Symbol)*

3 Press `FUNC,CTRL,F` to clear the flash drive. Type `flash` at the password prompt to confirm the operation.

Take the following steps to resolve this problem on a Series 4040 and 5040 mobile device:

1 Boot the mobile device.

2 Press `ESC` at the Access screen to use other applications installed on the mobile device. See Figure 29.

3 If no application software packages are loaded on the mobile device, Figure 27 appears. If Figure 27 appears, skip the next step.

4 Press the `ESC` key from the screen shown in Figure 27 and Figure 28.

5 Press `ALT,F` to delete the apps directory and the temp directory on the 4040 and 5040 mobile devices.

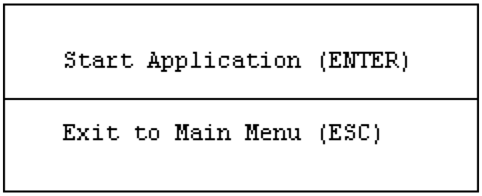


Figure 29. *VRC 4040/5040 App Access Menu*

Contact Us

For questions or problems with Avalanche, contact Wavelink Corporation at support@Wavelink.com or call 801-316-9000. In addition, see our Web site at http://www.wavelink.com/wavelink/avalanche.

Appendix B: RF Firmware and Radio Updates

Incompatibilities between firmware and radio drivers sometimes occur when hardware manufacturers implement new firmware into mobile devices. As this occurs, Wavelink creates new packages to update the software to match the radio drivers with the firmware.

RF Firmware and Driver Packages (1 or 2 Mb)

RF Firmware packages are currently available for Series 3000, Series 4000, and Series 7000 mobile devices. These packages provide the means to update a mobile device's radio firmware and driver to a current and known operational version. They can also be used to flash pre-802.11 protocol radios to 802.11 or vice-versa. The names of the firmware packages are:

- `RF3_vXXX.exe` for Series 3000 mobile devices
- `RF4_vXXX.exe` for Series 4000 mobile devices
- `RF7_vXXX.exe` for Series 7000 mobile devices.

To change the firmware within the mobile device:

NOTE If the firmware update procedures are not followed carefully, mobile devices may become inoperable. Do not power off mobile devices during firmware upgrades.

1. Install the packages to the appropriate software collection and site profile on the Management Console. Open the firmware package branch in the Tree View of the Management Console to determine whether the software package type is `Auto-Run`. Auto-run packages run immediately after a successful download to the mobile device. For more information regarding software packages, see *Using Software Packages* on page 113.
2. Right-click the package and select either a Pre-802.11 firmware update or an 802.11 firmware update.
3. If necessary, modify the selection criteria of the software collection to further restrict which mobile devices receive this firmware update package.

The selection criteria of the firmware update package is set to differentiate between the different series types. It does not, however, differentiate between 1 MB, 2 MB, and 11 MB mobile device types. The selection criteria cannot be modified to ensure that these packages do not download to the incorrect mobile devices. In this case, you must modify the selection criteria of the software collection to ensure that the correct devices receive the firmware update.

4 Right-click the firmware package to enable it.

NOTE Ensure that other mobile devices residing in the same software collection are not booted while you update the devices that need the firmware upgrades.

---

5 If the mobile device is currently operating at a given site, you can download the firmware upgrade package over a wireless connection. The access points will require firmware updates for the mobile devices to communicate. If the mobile device is not currently operating and doesn't match the firmware at the site, employ the cradle to download the firmware upgrade.

6 Perform a cold boot or warm boot on the mobile device to download the firmware package from the Avalanche Manager. Once the firmware update package downloads successfully to the device, it automatically executes.

7 After you perform the firmware update, access the Avalanche Enabler Configuration Screen (i.e., Config Screen).

8 Modify the network ID to correspond to the appropriate access point network. In the 802.11 environment, the network ID is called the ESS ID. The network ID in the pre-802.11 environment supports three characters whereas the ESS ID (or network ID) allows 32 characters in the 802.11 environment. When the mobile device is setup for 802.11, the network ID field scrolls so that you can enter Network IDs with more than 3 characters.

RF Firmware and Driver Packages (11 MB)

Some mobile devices use the 802.11B protocol. This protocol supports 11MB transfer rates.

As hardware improves, new firmware is implemented into mobile devices, occasionally causing incompatibilities between the firmware and radio drivers. As this occurs, Wavelink creates new packages to update the software to match the radio drivers with the firmware.

For example, the PDT7546 mobile device contained radio driver 1.15-02 and firmware version 1.00-03. The radio driver 1.15-02 is compatible with the firmware version 1.00-03. However, when Symbol Technologies installed the newer firmware version 2.20-01 into the 11Mb 7540 series mobile devices, an incompatibility issue emerged. Wavelink Corporation created the `RF7-11_v20` software package, which upgrades the radio driver to version 2.23-00 and is compatible with the newer firmware.

To assess which firmware and radio driver is loaded on the mobile device, access the Avalanche Enabler Configuration screen (i.e., Config screen), `FUNC, CTRL, R`. Type in the password, `system`. Type `Y` to confirm the termination of an active session. Select `Radio Parameters`, and then select `Terminal Info`.

NOTE If the mobile device is flash formatted after you implement the new firmware, this package might need to be reapplied to ensure that compatible radio drivers and firmware are loaded.

Steps for loading the RF update packages for the 11 MB mobile device are as follows:

NOTE If the firmware update procedures are not followed carefully, mobile device may become inoperable. Do not power off mobile devices during firmware upgrades.

1. Install the packages to the appropriate software collection and site profile on the Avalanche Manager. Open the firmware package in the Tree View and check the information beneath the branch to determine whether the software package is of type Auto-Run. Auto-Run packages run immediately after a successful download to the mobile device. For more information regarding software packages, see *Using Software Packages* on page 113.

2. Modify the selection criteria of the software collection to further restrict which mobile devices receive this firmware update package.

The selection criteria of the firmware update package is set to differentiate between the different series types. It does not, however, differentiate between 1 MB, 2 MB, and 11 MB mobile device types. The selection criteria cannot be modified to ensure that these packages do not download to the incorrect mobile devices. In this case, you must modify the selection criteria of the software collection to ensure that ensure that the correct devices will receive the firmware update.

3 Right-click the firmware package to enable it.

NOTE Ensure that other mobile devices residing in the same software collection are not booted while you update the devices that need the firmware upgrades.

---

4 If the mobile device is currently operating at a given site, you can download the firmware upgrade package over a wireless connection. The access points will require firmware updates for the mobile devices to communicate. If the mobile device is not currently operating and doesn't match the firmware at the site, employ the cradle to download the firmware upgrade.

5 Perform a cold boot or warm boot on the mobile device to download the firmware package from the Avalanche Manager. Once the firmware update package downloaded successfully, it automatically executes.

Contact Wavelink at 801-316-9000 for the latest information on which packages are available. Currently, the following packages are available.

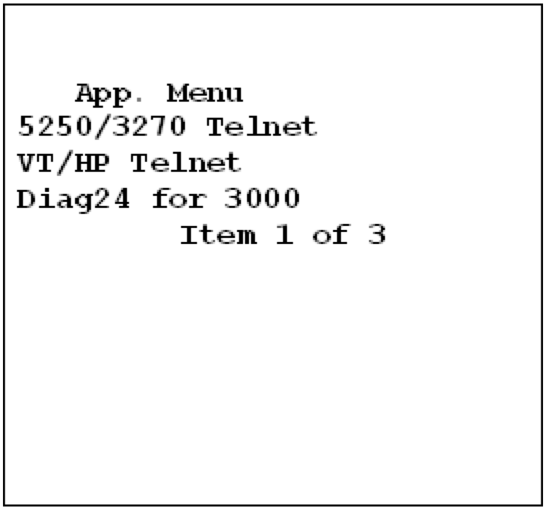
`RF3-11_vXX.exe`	for 3000 Series mobile devices
`RF7-11_vXX.exe`	for 7000 Series mobile devices

Appendix C: RF Diagnostics

Wavelink provides Avalanche-enabled software packages for the Symbol RF diagnostic tools.

Symbol RF Diagnostic Programs

For the Series 3000 mobile devices, the Diag24 software package is called `Diag24_3.exe`, and for the Symbol radio system card, it is called `Diag24pc.exe`. Install these software packages on the Avalanche Manager in the same way you install a Telnet Client software package. Once you enable a particular package, it will download to the mobile device after a device reboot. Contact your Symbol representative if you have questions regarding Diag24 usage. Coldboot on a Series 3000 device to access the Diag24 package. On Series 4000 and Series 5000 mobile devices, use the Diag24pc.exe software package and use VRC 4040/5040 App Access Menu to access Diag24 at boot time.



```
   App. Menu
5250/3270 Telnet
VT/HP Telnet
Diag24 for 3000
        Item 1 of 3
```

Figure 30. *App. Menu with Diag24*

Appendix D: Installing the Avalanche Enabler

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 the Avalanche Enabler* on page 31 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

This section also provides the following information:

- Loading the Enabler on Windows
- Loading the Enabler through a Local Gateway

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 2.

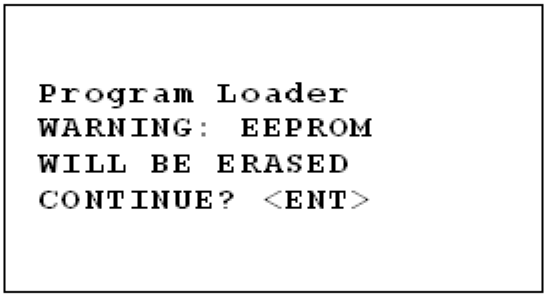
	Command Mode Boot Sequence
46-key LRT 3840 46-key PDT 3140 47-key PDT 3540 46-key PDT 6840 46-key PDT 6140	Power off the mobile device. Hold F+I. Press and release PWR. Release F+I.
54-key VRC 3940 54-key VRC 6940	Power off the mobile device. Hold A+D. Press and release ON/OFF. Release A+D.
35-key PDT 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 2: *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.

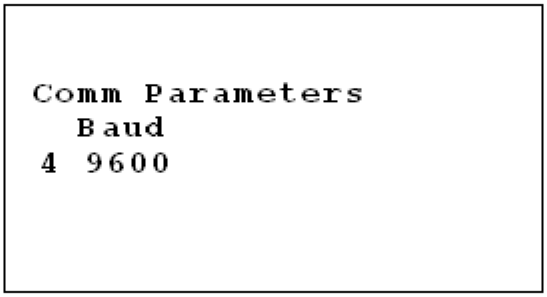
4 Press `ENTER`. The Program Loader screen appears.



```
Program Loader
WARNING: EEPROM
WILL BE ERASED
CONTINUE? <ENT>
```

Figure 31. *Program Loader EEPROM Erase*

5 Press ENTER to erase the non-volatile memory. The Comm Parameters screen appears.



```
Comm Parameters
  Baud
4 9600
```

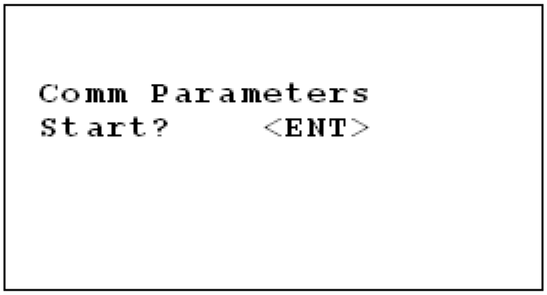
Figure 32. *Program Loader Baud Parameter*

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 3: *Download Communication Parameters*

The Comm Parameters screen appears.



```
Comm Parameters
Start?      <ENT>
```

Figure 33. *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 *Chapter 8: Serial Ports* on page 185 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 34 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 34.

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.

Flash Type	Partition Size	Partition file
0400	2 MB	PT-0400A.HEX
0800	4 MB	PT-0800A.HEX

Table 4: *Flash Type*

Flash Type	Partition Size	Partition file
0808A	8 MB	PT-0808A.HEX
0818A	16 MB	PT-0818A.HEX

Table 4: *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.

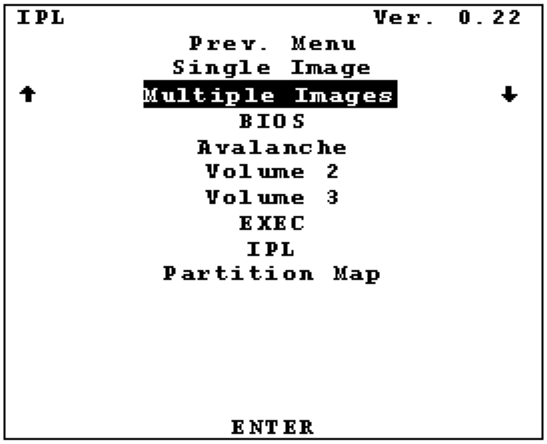


Figure 34. *The Command Screen for a Symbol 7000 Series Device*

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 *Chapter 8: Serial Ports* on page 185 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 34 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.

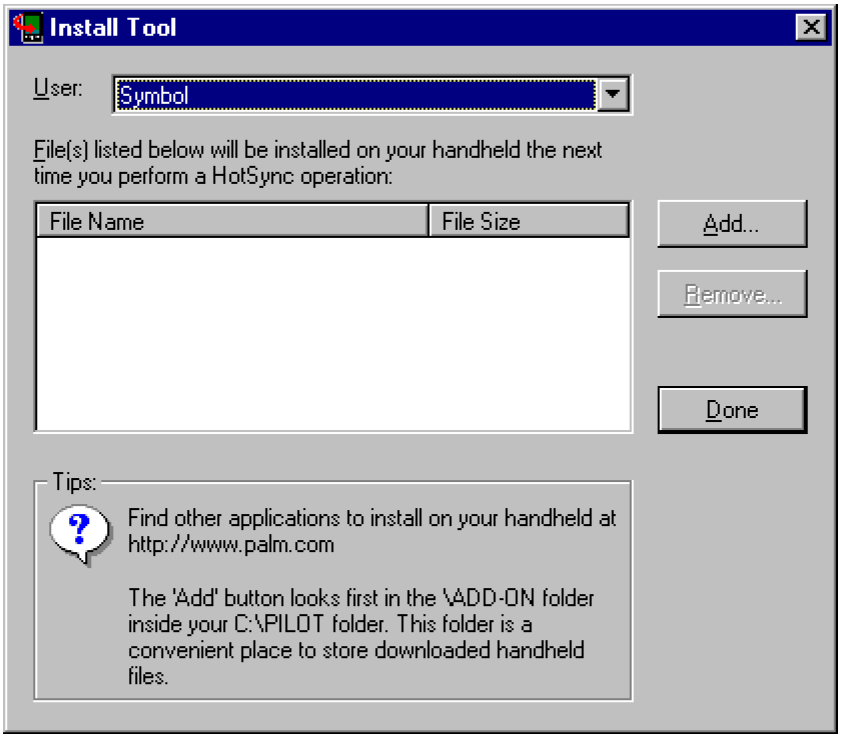
NOTE It is assumed that the Palm Desktop is already installed on the system. See the Palm Desktop documentation for more information.

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.



User: Symbol

File(s) listed below will be installed on your handheld the next time you perform a HotSync operation:

File Name	File Size

Find other applications to install on your handheld at http://www.palm.com

The 'Add' button looks first in the \ADD-ON folder inside your C:\PILOT folder. This folder is a convenient place to store downloaded handheld files.

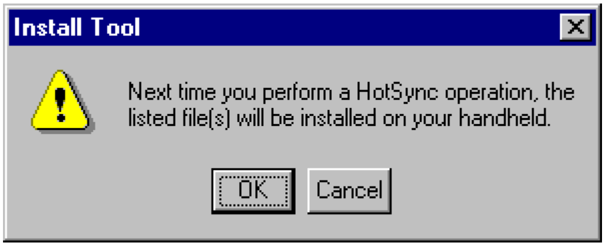
Figure 35. *Install Tool*

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.



Next time you perform a HotSync operation, the listed file(s) will be installed on your handheld.

Figure 36. *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 37.

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 *Stopping an Agent from Windows 2000/ XP* on page 179.

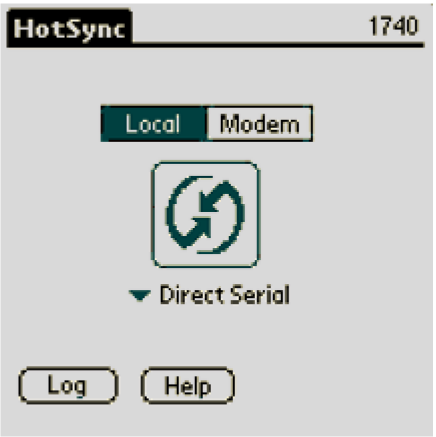


Figure 37. *The HotSync Screen*

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 an Avalanche Software Package* on page 41 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 *Stopping an Agent from Windows 2000/ XP* on page 179.

4 In ActiveSync, select `Get Connected` from the **File** menu.

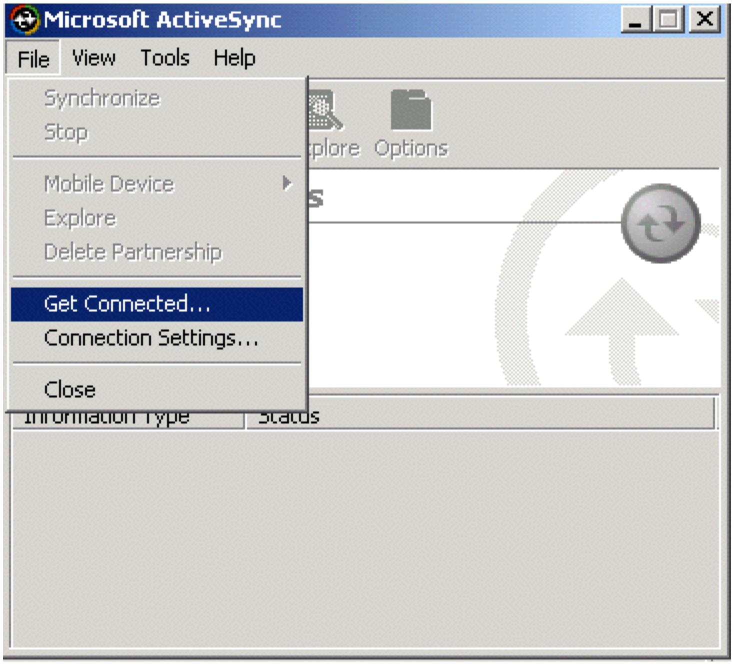
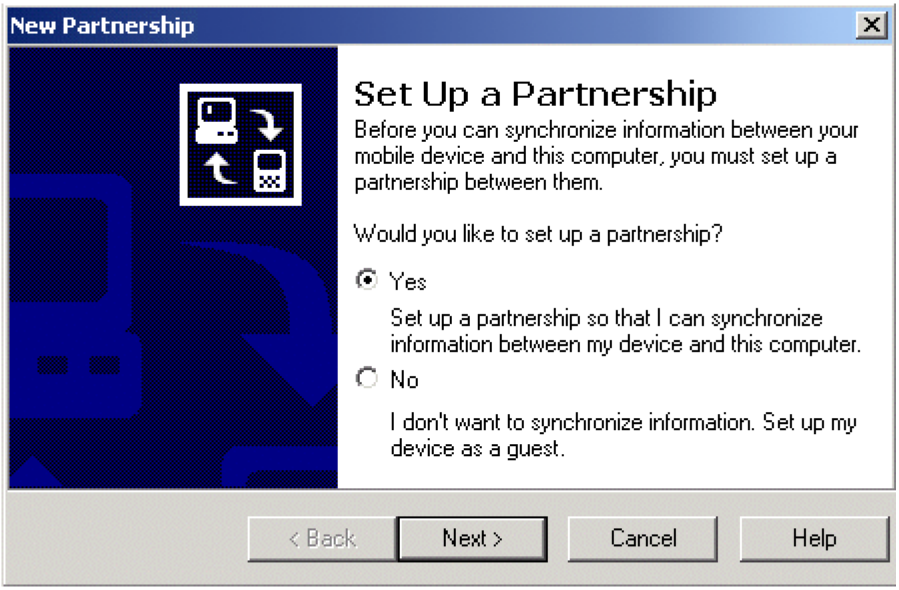


Figure 37-2 *ActiveSync Get Connected Menu Option*

An ActiveSync Partnership is required to download the Enabler to the mobile device. The dialog box shown in Figure 37-3 appears.



Set Up a Partnership

Before you can synchronize information between your mobile device and this computer, you must set up a partnership between them.

Would you like to set up a partnership?

● Yes

Set up a partnership so that I can synchronize information between my device and this computer.

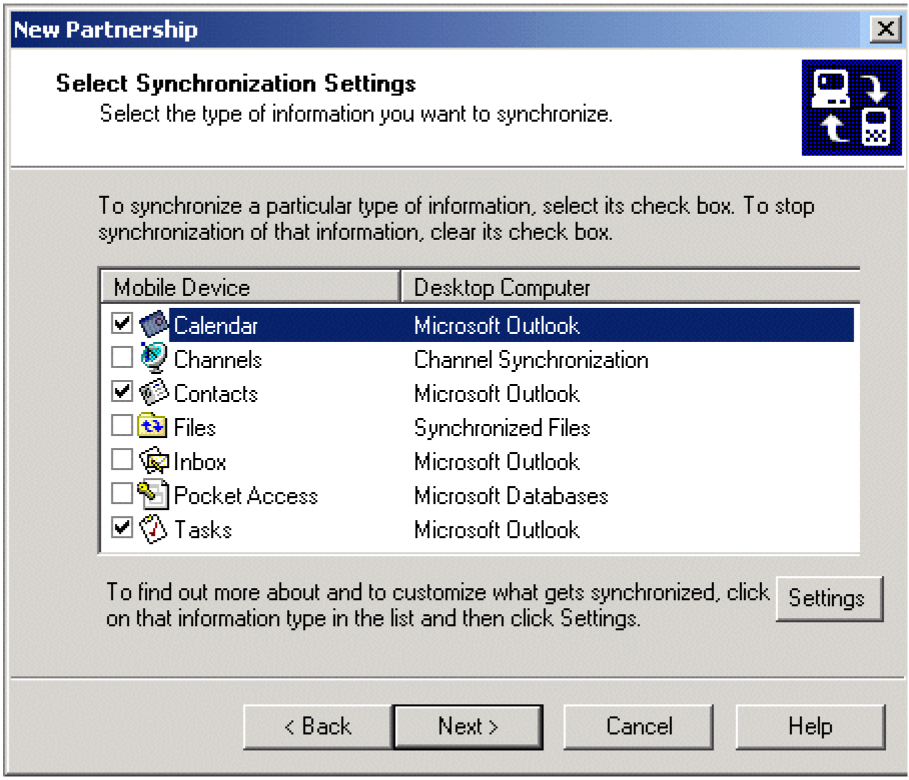
○ No

I don't want to synchronize information. Set up my device as a guest.

Figure 37-3 *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 37-4.



New Partnership

Select Synchronization Settings

Select the type of information you want to synchronize.

To synchronize a particular type of information, select its check box. To stop synchronization of that information, clear its check box.

Mobile Device	Desktop Computer
☑ Calendar	Microsoft Outlook
□ Channels	Channel Synchronization
☑ Contacts	Microsoft Outlook
□ Files	Synchronized Files
□ Inbox	Microsoft Outlook
□ Pocket Access	Microsoft Databases
☑ Tasks	Microsoft Outlook

To find out more about and to customize what gets synchronized, click on that information type in the list and then click Settings.

Figure 37-4 *Synchronization Settings*

To install the Avalanche Enabler:

1 Verify that ActiveSync is still running. Navigate to the Enabler file and and double-click the file to start the Enabler installation.

2 In the Welcome dialog box, click **Next**.

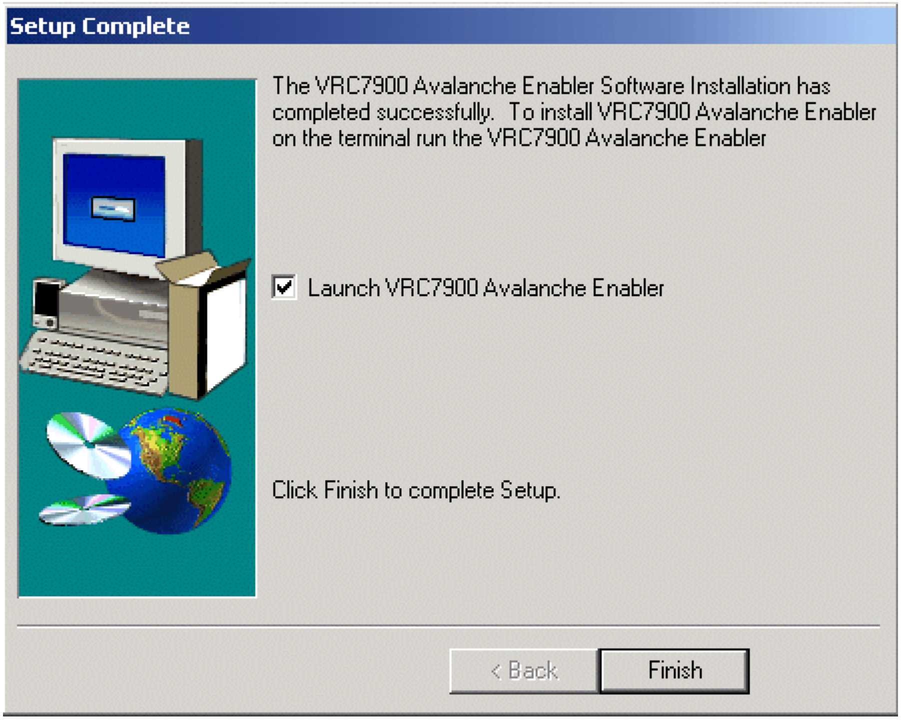
3 Choose the desired installation destination.

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`.



Setup Complete

The VRC7900 Avalanche Enabler Software Installation has completed successfully. To install VRC7900 Avalanche Enabler on the terminal run the VRC7900 Avalanche Enabler

☑ Launch VRC7900 Avalanche Enabler

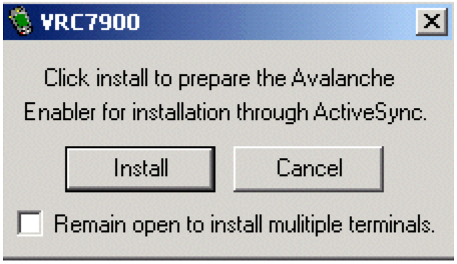
Click Finish to complete Setup.

Figure 37-5 *Setup Complete Dialog Box*

The Install Enabler through ActiveSync dialog box automatically appears (Figure 37-6).

7 If multiple mobile devices are to receive the installation files, enable the check box in the lower left.

8 Click `Install`.



VRC7900

Click install to prepare the Avalanche Enabler for installation through ActiveSync.

□ Remain open to install mulitiple terminals.

Figure 37-6 *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 an Avalanche Software Package* on page 41 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 an Avalanche Software Package* on page 41 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.

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.

Loading the Enabler through a Local Gateway

You can use a Local Gateway to install the Enabler on a Windows CE device.

The process of using a Local Gateway to install the Enabler on a device involves the following tasks:

1. Install the Enabler Install Kit for the mobile device in Avalanche Manager.
2. Enable the Enabler Install Kit for the mobile device.
3. Create a Microsoft ActiveSync connection between the host system and the device and then configure Avalanche to use the connection as a Local Gateway.
4. Connect the device to install the Enabler.

Contact your Wavelink representative for information about the availability of Enabler Install Kits for mobile devices.

To install an Enabler using an Enabler Install Kit:

1. Obtain the Enabler Install Kit and place it in a local or network location that the Avalanche Manager Agent can access.
2. Connect to the Avalanche Manager Agent.
3. In the Avalanche Manager Tree View, right-click **Enabler Install Kits**.

   A single-item menu list appears.
4. Select `Install Enabler Kit`.

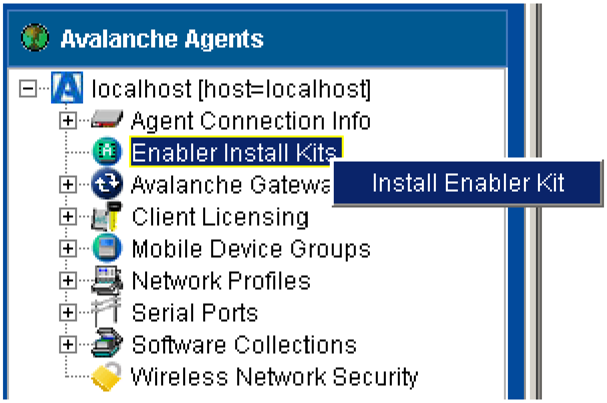


Figure 38. *Selecting to Install an Enabler Kit*

A dialog box appears.

Type the path (including the file name) to the Enabler Install Kit or use the browse feature of the dialog box to locate and select the Enabler Install Kit file.

5 Click `OK`.

The Enabler Install Kit is installed.

After the Enabler Install Kit is installed in Avalanche Manager, it appears in the Tree View beneath **Enabler Install Kits**.

By default, the Avalanche Enabler Kit is disabled. You must enable the Enabler install kit before Avalanche Manager will deploy it to mobile devices over the Local Gateway.

6 Right-click the Enabler Install Kit that you want to enable.

A menu list appears.

7 Select `Enable Enabler Install Kit`.

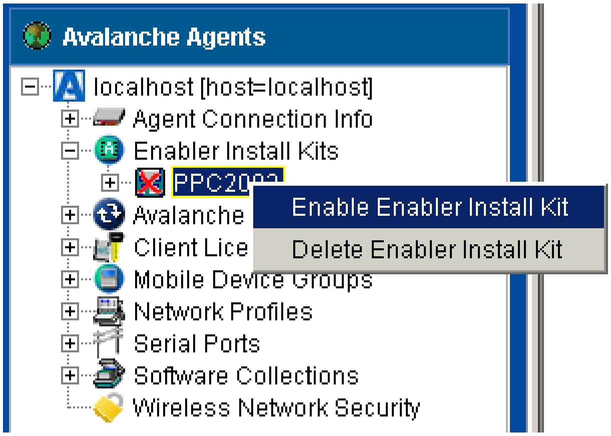


Figure 39. *Enabling the Enabler Install Kit*

The Enabler Install Kit is now enabled and ready to be deployed to mobile devices through a Local Gateway.

8 Open a Local Gateway on the host system.

NOTE For more information about opening a Local Gateway, see XXX.

When a mobile device is connected to the Avalanche Manager, the Manager will check the mobile device for compatibility with each of the enabled Enabler Update Kits.

When Avalanche Manager finds a matching Enabler for the device, it will download and install the Enabler.

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 E: Avalanche Manager Licensing Process

Avalanche Manager incorporates a licensing process that reduces the risk of user error during product activation and protects against unauthorized installations. This system uses a technology called nodelocking to uniquely identify the system to which an Avalanche Manager Agent is installed.

This section provides an overview of the nodelocking technology and describes the different ways you can activate your Avalanche Manager license.

NOTE An enterprise licensing system is also available for high-volume customers. With the enterprise licensing system, there is no need to purchase additional Avalanche Manager licenses when adding new devices. This licensing system also allows the inclusion of a customer logo that automatically displays during application startup. Contact your Wavelink customer service representative for more information.

Nodelocking Defined

Nodelocking is a technique in which a software product 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. Nodelocking is an advantage because it provides a reliable method of identifying a valid Avalanche Manager Agent install. This advantage, in turn, gives Wavelink the ability to simultaneously verify valid licenses and reduce efforts in license management.

NOTE Identifying a node is completely automated by the Wavelink licensing process—it does not require that you have a detailed understanding of each system on your network.

Activating Your Avalanche Manager License

Each Avalanche Manager license contains a set of Avalanche client licenses. The number of client licenses determines the number of clients that can connect to and receive updates from Avalanche Manager.

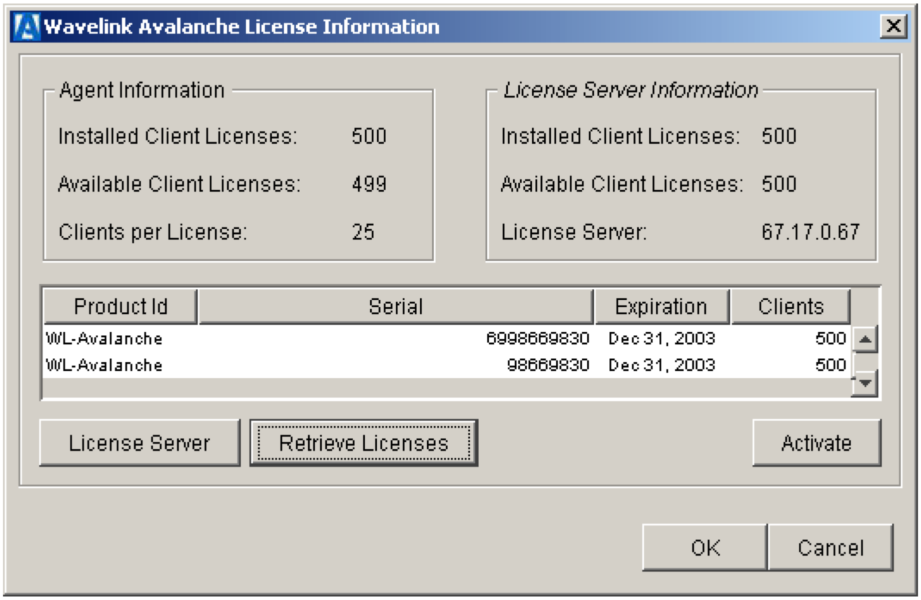
You can activate your Avalanche Manager license using one of five methods: standard, manual, support, temporary, and demonstration. These options are accessed through the *Wavelink Activation* dialog box. This process is repeatable, allowing you to add new licenses to Avalanche Manager at any time.

To access the Wavelink Activation dialog box:

1 From the Avalanche Management Console, connect to an Avalanche Manager Agent.

2 Select `Software Licensing` from the **Administration** menu or double-click the Client Licensing icon from the Tree View.

The *Wavelink Avalanche License Information* dialog box appears.



Agent Information

Installed Client Licenses: 500

Available Client Licenses: 499

Clients per License: 25

License Server Information

Installed Client Licenses: 500

Available Client Licenses: 500

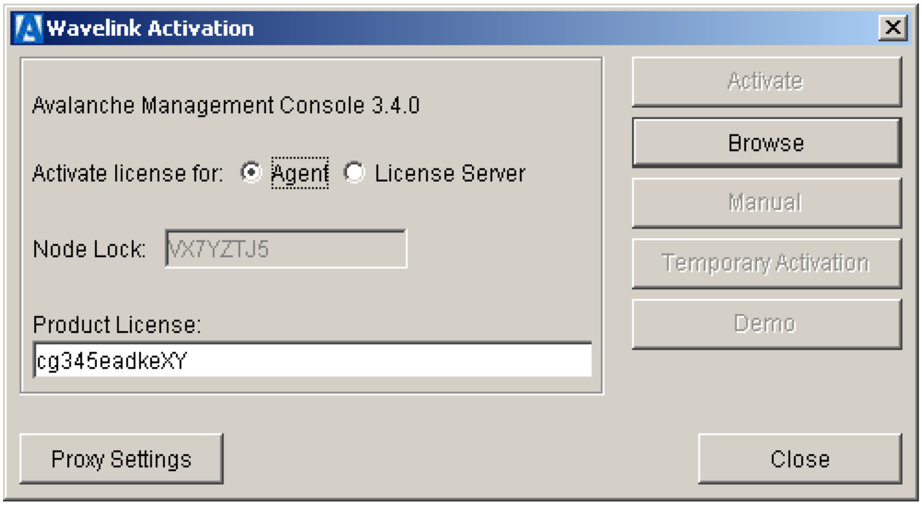
License Server: 67.17.0.67

Product Id	Serial	Expiration	Clients
WL-Avalanche	6998669830	Dec 31, 2003	500
WL-Avalanche	98669830	Dec 31, 2003	500

Figure E-1. *The Wavelink Avalanche License Information Dialog Box*

3 Click `Activate`.

The *Wavelink Activation* dialog box appears.



Avalanche Management Console 3.4.0

Activate license for: ● Agent ○ License Server

Node Lock: VX7YZTJ5

Product License: cg345eadkeXY

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

From this dialog box, you can type your product license in the **Product License** text box and select an appropriate activation method. Your product license number is included with the e-mail you received when you purchased Wavelink Avalanche Manager.

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

There are several methods of activating a license:

- standard
- manual
- support
- temporary

- demonstration

Standard License Activation

The most common method to activate your Avalanche Manager license is by using the **Activate** button. This button instructs the Avalanche Manager to send your licensing information to a secure Wavelink database, which contains all the relevant information about your product purchase. Once the information is verified, a unique activation code is sent back to Avalanche Manager.

To license Avalanche Manager:

1 From the Avalanche Management Console, connect to an Avalanche Manager Agent.

2 Select `Software Licensing` from the **Administration** menu or double-click the Client Licensing icon from the Tree View.

The *Wavelink Avalanche License Information* dialog box appears, as shown in Figure E-1.

3 Click `Activate`.

The *Wavelink Activation* dialog box appears, as shown in Figure E-2.

4 If you want to associate the new license with the current Agent, verify that the **Agent** option is selected to the right of the **Activate License for** field.

If you want to distribute the licenses from a license server, select the **License Server** option.

NOTE The **License Server** option is only available if a license server is running. See *Using a License Server* on page 277 for more information.

5 Type your product license number included with the e-mail you received after you purchased the product into the **Product License** text box.

6 Click `Activate`.

Browsing to a Wavelink.lic File

Typically, the new licensing process requires that the system hosting the Avalanche Manager Agent has access to the Internet; however, if this is not the case, an alternate method is available. This method lets you use a different, Internet-capable computer to retrieve your activation code.

To browse to a Wavelink.lic file:

1 Note the nodelock number that appears during the installation process.

2 Access the Wavelink Activation Web site at www.wavelink.com/activation.

This Web site allows you to type in your license and nodelock information. You can then activate the license, which results in a license file being generated. By following the directions on the Web site, you can save this license file to a location on your system.

3 From the Avalanche Management Console, connect to an Avalanche Manager Agent.

4 Select `Software Licensing` from the **Administration** menu or double-click the Client Licensing icon from the Tree View.

The *Wavelink Avalanche License Information* dialog box appears, as shown in Figure E-1.

5 Click `Activate`.

The *Wavelink Activation* dialog box appears, as shown in Figure E-2.

6 If you want to associate the new license with the current Agent, verify that the **Agent** option is selected to the right of the **Activate License for** field.

If you want to distribute the licenses from a license server, select the **License Server** option.

NOTE The **License Server** option is only available if a license server is running. See *Using a License Server* on page 277 for more information.

7 Type your product license number included with the e-mail you receive after you purchase the product into the **Product License** text box.

8 Click `Browse` to locate and select the `Wavelink.lic` file.

9 Click `Close`.

An example of when you would use this process is if you need to install an Agent at a remote location, such as a retail outlet, that does not have access to the Internet.

Support License Activation

In the event that both the automatic and manual methods of activating a license are unavailable, you can contact a Wavelink customer service representative by calling (888) 697-WAVE and pressing 9. This representative will be able to use the nodelock number that appears in your *Wavelink Activation* dialog box, along with your license information, to either generate a license file and send that file to you, or supply you with the information you need to activate your licenses.

Once you have this information, you can follow these steps to activate your license:

To manually activate your license:

1 From the Avalanche Management Console, connect to an Avalanche Manager Agent.

2 Select `Software Licensing` from the **Administration** menu or double-click the Client Licensing icon from the Tree View.

The *Wavelink Avalanche License Information* dialog box appears, as shown in Figure E-1.

3 Click `Activate`.

The *Wavelink Activation* dialog box appears, as shown in Figure E-2.

4 If you want to associate the new license with the current Agent, verify that the **Agent** option is selected to the right of the **Activate License for** field.

If you want to distribute the licenses from a license server, select the **License Server** option.

NOTE The **License Server** option is only available if a license server is running. See *Using a License Server* on page 277 for more information.

5 Type your product license number included with the e-mail you receive after you purchase the product into the **Product License** text box.

6 Click `Manual`.

A dialog box appears, allowing you to supply the information given to you by the Wavelink customer support representative.

7 Click `Close`.

Temporary Activation

If you find yourself in a situation in which you have difficulties activating your Avalanche Manager license—for example, because you cannot activate the Wavelink activation Web site—and Wavelink customer support is unavailable, you can activate your licenses temporarily. This option allows you to activate 500 licenses for 7 days, which should provide you with enough time to resolve any issues with Wavelink customer support without impacting your implementation of Avalanche Manager on the network.

To temporarily activate Avalanche Manager:

1 From the Avalanche Management Console, connect to an Avalanche Manager Agent.

2 Select `Software Licensing` from the **Administration** menu or double-click the Client Licensing icon from the Tree View.

The *Wavelink Avalanche License Information* dialog box appears, as shown in Figure E-1.

3 Click `Activate`.

The *Wavelink Activation* dialog box appears, as shown in Figure E-2.

4 If you want to associate the new license with the current Agent, verify that the **Agent** option is selected to the right of the **Activate License for** field.

If you want to distribute the licenses from a license server, select the **License Server** option.

NOTE The **License Server** option is only available if a license server is running. See *Using a License Server* on page 277 for more information.

5 Type your product license number included with the e-mail you receive after you purchase the product into the **Product License** text box.

6 Click `Temporary Activation`.

Avalanche Manager temporarily activates your licenses for a seven-day period.

NOTE If you use the temporary activation option, it is highly recommended that you contact Wavelink support as soon as possible, to ensure that your licenses are activated permanently.

Demonstration Activation

If you are installing a Wavelink product for demonstration or evaluation purposes, you can click the **Demo** button within the *Wavelink Activation* dialog box once you type a valid license number into the **Product License** text box. Once you click this button, the Activation dialog box creates a specialized license file. This file allows you to use a limited installation of Avalanche Manager for 30 days. This limited installation provides you with license for two mobile devices. After 30 days, you must either activate the installation permanently by using the **Activate** button, or uninstall the product.

NOTE This option is only available once.

To activate a demonstration license:

1 From the Avalanche Management Console, connect to an Avalanche Manager Agent.

2 Select `Software Licensing` from the **Administration** menu or double-click the Client Licensing icon from the Tree View.

The *Wavelink Avalanche License Information* dialog box appears, as shown in Figure E-1.

3 Click `Activate`.

The *Wavelink Activation* dialog box appears, as shown in Figure E-2.

4 Type your product license number included with the e-mail you receive after you purchase the product into the **Product License** text box.

5 Click `Demo`.

Using a License Server

Under most circumstances, Avalanche Manager licenses are installed, created, and assigned to each Agent on a network. These licenses are available to that specific Agent only, minimizing the need for license management. Larger installations, however, also have the option of implementing a license server—a specialized server component that manages and distributes licenses from a central location. The license server runs as a system service.

Activating a License Server

An inactive license server is included with each Agent install.

To start the license server

1 Verify that you have a license file that contains all of your purchased licenses installed on the system on which the license server will operate.

2 Open a command prompt and navigate to the `\ls` subdirectory where the Avalanche Manager was installed.

3 If you have not yet installed the license server, run the following command:

```
LicenseServer -i
```

This command installs the license server.

4 Run the following command to start the license server service:

```
LicenseServer -s
```

Configuring a License Server

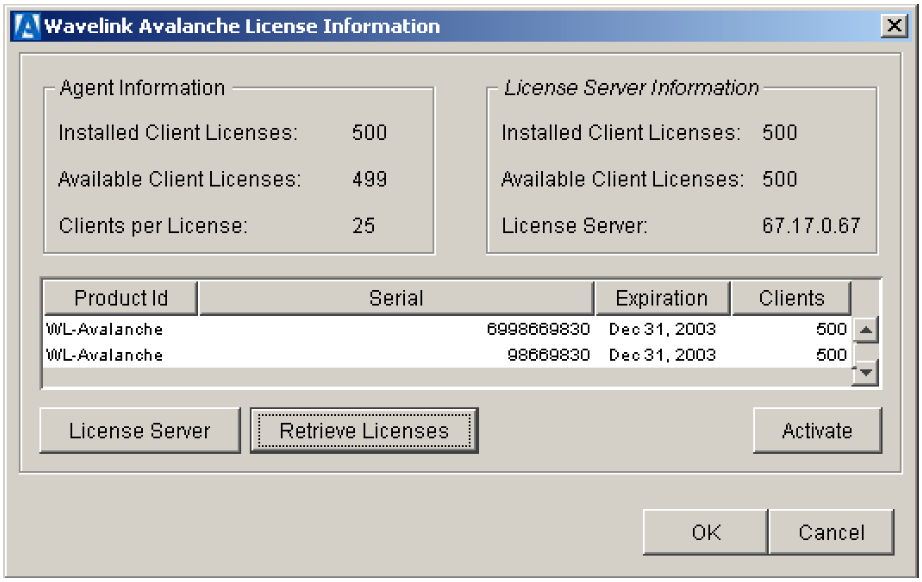
Once you start a license server, you can use the Avalanche Management Console to configure how the license server distributes licenses.

To configure a license server:

1. From the Avalanche Management Console, connect to the Avalanche Manager Agent that resides on the same system as the license server.

2. Select `Software Licensing` from the **Administration** menu or double-click the **Client Licensing** icon from the Tree View.

   The *Wavelink Avalanche License Information* dialog box appears.



Agent Information

Installed Client Licenses: 500

Available Client Licenses: 499

Clients per License: 25

License Server Information

Installed Client Licenses: 500

Available Client Licenses: 500

License Server: 67.17.0.67

Product Id	Serial	Expiration	Clients
WL-Avalanche	6998669830	Dec 31, 2003	500
WL-Avalanche	98669830	Dec 31, 2003	500

Figure E-3. *The Wavelink Avalanche License Information Dialog Box*

At the top of this dialog box is a summary of your license information. This summary includes the following information:

- **Installed Client Licenses**. This field displays the number of client licenses you currently have available for the Agent to which you are connected.

- **Available Client Licenses**. This field displays the number of client licenses are currently unassigned to mobile devices for the Agent to which you are connected.
- **Clients Per License**. This field displays how many client licenses the license server will distribute to an Agent when that Agent requests more licenses.
- **Installed Client Licenses**. This field displays the total number of client licenses associated with the license server.
- **Available Client Licenses**. This field displays the number of client licenses available to other Agents.
- **License Server.** This field displays the IP address of the license server.

3 Designate the address of the license server by clicking `License Server`.

In the *License Server Settings* dialog box, type the IP address of the license server in the **License Server** text box.

4 In the **Clients per License** text box, type the number of client licenses (the license block size) to distribute to the Agent when the Agent runs out of licenses.

The license block size also determines the number of unused client licenses that return to the license server when their lease time expires.

NOTE It is recommended that you use a small value for the license block size. Client licenses returned to the license server are returned only in full block sizes. For example, if you configure a block size of 25, and 24 are unused when their lease expires, no licenses are returned to the license server. However, if 26 licenses are unused, then 25 licenses (the full block size) are returned to the license server.

5 If you want to send additional client licenses to an Agent, click `Retrieve Licenses`.

A dialog box appears, allowing you to specify how many client licenses you want to send to the Agent.

6 Click `Apply` to save your changes.

Client licenses assigned by a license server are leased for anywhere between three to nine days. When these licenses expire, they are re-acquired without affecting network operations. After that time, they are returned to the license server as unassigned licenses.

You can also configure the license server to use a proxy server. This might be necessary if a firewall resides between the license server and the Management Console.

To configure proxy settings for a license server:

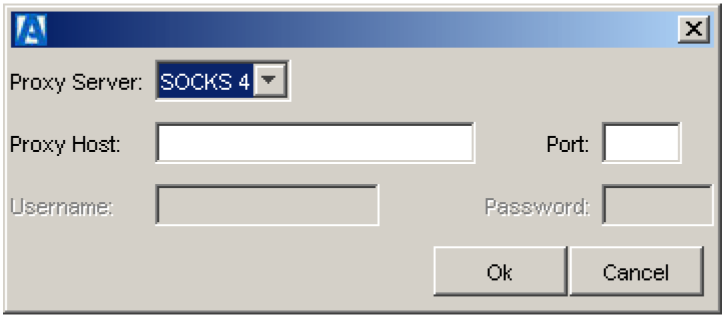
1 From the Avalanche Management Console, connect to the Avalanche Manager Agent that resides on the same system as the license server.

2 Select `Software Licensing` from the **Administration** menu or double-click the **Client Licensing** icon from the Tree View.

3 In the *Wavelink Avalanche License Information* dialog box (Figure E-3), click `Activate`.

4 In the *Wavelink Activation* dialog box (Figure E-2), click `Proxy Settings`.

The following dialog box appears.



Proxy Server: SOCKS 4

Proxy Host:

Port:

Username:

Password:

Figure E-4. *The Proxy Server Settings Dialog Box*

5 Select the proxy server type.

If the license server resides past a firewall, you can connect to it through a proxy using the SOCKS protocol. To configure the connection through a proxy, select `SOCKS 4` from the **Proxy Server** list. Then, type the IP address of the proxy server in the **Proxy Host** text box, and the port number for the proxy in the **Port** text box.

If the license server resides past a Windows HTTP firewall, you can connect to it through a proxy using the HTTP protocol. To configure the connection through a proxy, select `HTTP` from the **Proxy Server** list. Then, type the IP address of the proxy server in the **Proxy Host** text box, and the port number for the proxy in the **Port** text box. If the server authenticates users from a user database, type a valid username in the **Username** text box, and a valid Password in the **Password** text box.

6 Click `OK`.

Managing a License Server from the Command Prompt

The license server provides access to management functions through the command prompt. You can use these options to manage a local license server.

NOTE The license server runs as a system service.

To manage a license server from the command prompt:

1 Open a command prompt and navigate to the `\ls` subdirectory where the Avalanche Manager was installed.

2 Run the following command:

```
LicenseServer <option>
```

The following options are currently supported:

`-c`	Enables console mode at the command prompt. In console mode, the console window displays debugging information between the Agent and the license server. The information that appears is based on the license server's debug level. This option is not yet implemented.
`-h`	Not implemented.
`-i`	Installs the service
`-u`	Uninstalls the service
`-s`	Starts the service

`-q` Stops the service

`-v` Displays license server version information

`-l` *`LOGLEVEL`* Sets the logging level for the license server log. Logged messages are stored in the log file (`.log` file extension) in the `\ls` subdirectory.

The possible values for *LOGLEVEL* include:

CRITICAL - Critical error
ERR - Error message
NOTICE - Informational
WARN - Warning
DEBUG - Debugging information

Glossary

802.11 An IEEE wireless standard that provides specifications for wireless communications.

.ABK The file extension used to contain the backup data of the Avalanche Manager Agent.

.AVA The file extension used to identify avalanche packages.

.HEX The file extension used to identify a hex file or image.

3270 client An emulation client designed to imitate an 3270 terminal.

5250 client An emulation client designed to imitate an 5250 terminal.

access control A process in which use of Avalanche Manager components is restricted to specific user accounts. Access control typically involves a user name and password.

access point A hardware device that sends and receives radio broadcasts from mobile devices. Access points are connected by Ethernet to the rest of the network, and serve as a bridge between mobile devices and wired network components, such as servers.

activity log A file that contains a record of Agent activities since the Avalanche Management Console last started.

Agent The primary software component responsible for managing mobile devices.

Agent profile A set of information that defines the Agent to which the Avalanche Management Console is connecting. Agent profiles contain information such as its name, IP address, and port number.

application environment An environment in which an application is designed to operate. Application environments consist of mobile device type, operating system, and other factors.

application package A collection of software files that comprise an application installed on a mobile device.

auto package A collection of software files that execute immediately after they are downloaded. Firmware updates are examples of auto packages.

automatic WEP A Wavelink security solution in which WEP keys are rotated automatically on both access points and mobile devices.

Avalanche Management Console The primary interface through which you manage and maintain mobile devices.

Avalanche Manager A Wavelink solution that enables remote, over-the-air software synchronization for mobile devices.

Backup/Restore Wizard A wizard that allows you to backup and restore information Avalanche Manager contains.

binary A digital encoding/decoding system in which there are exactly two possible states. Boolean values are an example of a binary system, because it can have two values: true or false.

boolean operators Operators used to invoke a specific action on a variable or set of variables. Examples of operators include equals (=), and (&), and or (|).

BOOTP A protocol that lets a network user be automatically configured without user involvement.

client A software application that resides on a mobile device. The client is designed to allow the mobile device to communicate effectively with the rest of the network.

client group A logical groupings of clients.

client management system A software application, such as Avalanche Manager, that is responsible for managing and maintaining the clients deployed on a network.

configuration utility A tool that allows you to change the settings of a mobile device application.

cradle A hardware connector that allows a mobile device to connect to a desktop system.

device See mobile device.

DHCP Server A server application designed to automatically assign IP addresses to network components.

digiboard port A generic term for a serial port card that allows a system to expand the number of serial ports that can connect to it.

distributed Agent architecture An installation of Avalanche Manager in which multiple Agents are installed across several network segments, or subnets.

DNS server A server designed to manage the domain names and IP addresses used within a network.

driver update package A collection of files designed to update the radio driver of a mobile device.

Embedded OS A propertiary operating system installed on a mobile device.

emulation The process in which one computer or mobile device imitates another. For example, a VT100 emulation sets a mobile device to operate like a VT100 terminal.

emulation parameter A configuration setting that controls how emulation operates on a mobile device.

Enabler The software installed on a mobile device that allows Avalanche Manager to manage it.

ESS ID ESS ID, short for Extended Service Set Identity, is an identifier used to segment a wireless network. All components on a wireless network must share a common ESS ID to communicate with each other. The ESS ID is very similar to the Microsoft Workgroup name youcreate in IP properties to configure desktop computers to belong to the same subnet. Also known as Net ID.

Ethernet A standardized local area network system that is the dominant standard for connecting multiple computers and other devices together.

expression In Avalanche Manager, an equation used to verify that a mobile device should receive a software update. Expressions are used when creating selection criteria: for example, `modelname = 6840`.

Local Gateway A connection to the RAPI (Microsoft ActiveSync) interface on a host system. Avalanche uses the Local Gateway to perform updates and to install Avalanche Enablers to mobile devices.

firmware Software routines stored in read-only memory (ROM) of a device. Firmware is the code that determines how an access point performs and what types of features it supports.

flash disk See flash drive.

flash drive A section of mobile device memory used to store specific application or operating system data.

hex file download utility A software program designed to facilitate the installation of .HEX files to a mobile device.

hex image A common file format used in wireless applications.

host profile A collection of settings that defines how an emulation client connects to a server.

host profile utility A software application designed to facilitate the management of host profiles.

host system The computer on which one or more Avalanche Manager components are installed.

Hotsync A software application used to connect a desktop system to a Windows CE or Pocket PC mobile device.

HP client An emulation client designed to imitate an HP terminal.

ICMP Short for Internet Control Message Protocol that is used between a host system and a gateway to the Internet.

IP address The Internet protocol address assigned to the mobile device.

IP address pool A collection of IP addresses that the Agent draws from and assigns to mobile devices.

Java 2 Runtime Environment A runtime environment that is required for running Java applications.

JRE See Java 2 Runtime Environment.

LAN Short for Local Area Networ, the LAN is the collectinon of inter-connected hardware devices.

license code A Wavelink-generated code used to authorize an installation of Mobile Manager.

List View The view within the Avalanche Management Console that displays devices that belong to a software collection or package selected from the Tree View.

log A file that contains records of network activity.

LWP An installation process that is typically used with Symbol mobile devices.

MAC address The Media Access Control address of a mobile device. This address is a physical identification of the mobile device.

MAC-level broadcast The layer 2 broadcasts that are periodically sent by mobile devices and access points across a network.

MAC-level IP address assignment The process in which mobile devices receive IP address assignments based on the sending and receiving of MAC-level broadcasts.

mobile device A hand-held or vehicle-mounted device, such as a scan gun or PDA, that travels with a user as they conduct daily operations.

Mobile Manager A Wavelink-designed solution that allows you to add, manage, and secure a wireless network.

netmask Another term for subnet mask, the netmask is a set of numbers that tells a network device what other devices to communicate with based on IP address. Netmasks reduce the number of packets a particular device has to look at to determine if a response is required.

network ID An identifier used to distinguish one network component from another.

network interface card A hardware component that allows a device, such as a server, to connect to a LAN.

network profile A collection of settings that allow you to download network parameters such as IP addresses, the ESS ID, and WEP encryption keys to the mobile device over a serial or wireless connection.

node A set of several specific system attributes that, in combination, uniquely distinguish a computer from any other computer. The Wavelink license process uses nodes to create a nodelock, preventing unauthorized installations of the product.

nodelock The process in which a Wavelink license is bound to a specific computer on a network. The Wavelink licensing process uses an algorithm to combine a product serial number and a computer system’s node to generate a unique license number for product authorization.

null modem cable A specific cable designed to connect mobile devices to desktop systems.

orphaned package A package that has been installed on a mobile device but is not active in the Avalanche Manager Agent.

package See software package.

parity A method of checking whether any data has been lost or written over when it is moved. Parity is used to help download new software to mobile devices through serial connections.

partition file A file stored on a specfic section, or partition of a mobile device's hard drive.

pass code A collection of letters and numbers that is incorporated into the algorithm used to generate WEP keys for automatic WEP rotation.

ping The method of determining whether you can connect with a computer or device. Ping is also a utility program common to most operating systems that attempts to contact a device using its IP address.

plug-in A utility that are typically installed in addition to Avalanche Manager to configure a specific application.

port settings The specific values that define the characteristics of a given port. Examples of port settings includes port number or baud rate.

Program Loader A built-in application, included with most Symbol mobile devices, that handles the loading of new software to the mobile device.

property In Avalanche Manager, a property is a characteristic of a mobile device, such as its Terminal ID or model name.

pull Term used to describe the process in which a mobile device initiates the retreival of a software update.

push
Term used to describe the process in which a server component (like the Avalanche Manager Agent) initiates the installation of a software update to a mobile device.

radio driver
A set of software routines that control the behavior of a mobile device's radio.

RF
Short for radio frequency, RF is frequently used interchangeably with the term "wireless."

RF driver
See radio driver.

rotation interval
The period of time in which WEP keys are rotated both on access points and mobile devices.

selection criteria
A collection of parameters that define which mobile devices receive specific software updates.

Selection Criteria Wizard
A wizard that allows you to create one or more selection criteria, which allow you to control which mobile devices receive specific software updates.

serial connection
A connection in which a mobile device is connected to a desktop system through its serial port.

serial download
The process of downloading software to a mobile device through a serial connection.

software collection
A logical grouping of software packages maintained and managed by the avalanche Manager.

software package
The collection of files that reside on the mobile device for a particular application. These files include any support utilities used to configure or manage the application from the Avalanche Management Console.

static WEP
The standard WEP implementation, in which WEP keys remain constant unless changed by an administrator.

studio client
A client designed to operate with Wavelink Studio servers.

support package A collection of software files that update or enhance a given application, but are not applications themselves.

synchronization medium The method used to send software updates to a mobile device. There are two types of mediums available to Avalanche Manager: wireless (RF), and serial.

system service A set of software routines that run in the background of a desktop system or mobile device.

TCP/IP The basic communication protocol used to transmit data over the Internet.

TCP/IP stack The layers through which data passes on both clients and servers using TCP/IP.

Telnet client An emulation client designed to imitate an Telnet connection.

Terminal ID A unique identifier that is automatically generated by Avalanche Manager. This ID helps to distinquish one mobile device from another.

Token-ring A local-area network in which all systems are connecting in a ring or star topology. This protocol is the second-most widely used protocol for LANs after Ethernet.

Tree View The view within the Avalanche Management Console that displays information about the software collections and packages available to mobile devices.

truncate The process in which data is stopped abruptly at a specific point. Truncating is typically used to limit the size of a data stream.

unary Consisting of one and only one state. The Not operator (!) is an example of an operator that has a unary state.

unlicensed mode A mode in which Avalanche Manager can temporarily operate without requiring license authorization.

VT client An emulation client designed to imitate an VT terminal.

VT100 A mainframe system, often used in terminal emulation.

WAN Short for Wide-Area Network, a WAN refers to a large collection of hardware devices that are connected over vast distances. Typically, a WAN consists of multiple LANS that have been connected together.

WEP Short for Wired Equivlent Privacy, WEP is a security protocol designed to encrypt wireless transmissions. WEP uses four sequences of numbers, called keys, which are used to encrypt and decrypt data sent between access points and mobile devices.

WEP key A sequence of numbers that is used to encrypt or decrypt a wireless transmission.

wireless connection A connection through which data transmissions occur through radio transmissions.

workstation ID A unique identifier that distinguishes one mobile device from another.

Index