



Wavelink Avalanche Site Edition
Java Console User Guide

Version 5.0.1

asej-ug-501-20100824

Revised 24/8/2010

Copyright © 2010 by Wavelink Corporation All rights reserved.

Wavelink Corporation
6985 South Union Park Avenue, Suite 335
Midvale, Utah 84047
Telephone: (801) 316-9000
Fax: (801) 316-9099
Email: customerservice@wavelink.com
Website: <http://www.wavelink.com>

Email: sales@wavelink.com

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

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

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

The information in this document is bound by the terms of the end user license agreement.

Table of Contents

Chapter 1: Introduction	7
Managing Networks with Avalanche	7
Components of Avalanche	7
Location Management: My Location and Sites	9
Getting Started	9
About This Document	10
Chapter 2: Installing Avalanche	12
Installing Avalanche Site Edition	12
Uninstalling Avalanche	13
Chapter 3: Licensing	14
Overview of Wavelink Licensing	14
Running the License Server	15
Activating Licenses	15
Activating Avalanche Licenses	15
Activating Automatically	16
Activating Manually	17
Importing a License	18
Activating Demo Mode	19
Activating Licenses for Wavelink Products	20
Releasing Licenses	20
Importing the Enterprise License	21
Chapter 4: Avalanche Java Console	22
Launching the Avalanche Console	22
Understanding the Avalanche Console	24
Tool Bar	25
Navigation Window	25
Quick Start Tab	26
Profiles Configuration	26
Tools	26
Help and Support	26
Profiles Tab	27
Understanding Edit Mode	28
Changing Console Preferences	29
Customizing General Console Settings	30
Edit Lock Control	31
Configuring Audit Logging	31
Viewing the Audit Log	33
Specifying the Backup Drive Location	33
Configuring E-mail Settings	34
Configuring HTTP Proxy Settings	35

Managing Device Inventory Displays	35
Inventory Paging	36
Managing Device Filters	36
Creating Device Filters	36
Applying Device Filters	37
Deleting Device Filters	37
Modifying Columns for Mobile Device Lists	38
Adding Custom Columns for Mobile Device Lists	38
Reorganizing Columns for Mobile Device Lists	39
Displaying Custom Mobile Device Icons	40
Managing the Enterprise Server	40
Viewing the Enterprise Server Status	40
Purging Server Statistics	41
Performing a Dump Heap	42
Viewing the Inforail Status	42
Using the Support Generator	43
Using the Enabler Installation Tool	45
Chapter 5: Managing User Accounts	47
Creating User Accounts	48
Creating User Groups	50
Assigning User Permissions	51
Regional Permissions	51
Profile Permissions	53
Assigning Authorized Users to Profiles	55
Configuring Integrated Logon	55
Changing Passwords	56
Removing User Accounts	57
Chapter 6: Managing Sites and Locations	58
Managing Sites	58
Creating a Site	58
Assigning Profiles	59
Excluding Profiles	60
Viewing Mobile Devices within Sites	61
Pinging Mobile Devices within Sites	61
Sending Messages to Sites	61
Editing Site Properties	62
Additional Site Functions	63
Managing the Mobile Device Server	63
Modifying Server Location Properties	63
Stopping the Server	64
Starting Servers	64
Viewing Server Properties	65
Reinitializing the Mobile Device Server	65
Retrieving Mobile Device Log Files	65

Chapter 7: Managing Network Profiles	66
Creating Network Profiles	66
Configuring Network Profiles	67
Configuring Network Profile General Settings	67
Enabling Network Profiles	67
Managing IP Address Pools	68
Adding Authorized Users	68
Configuring Selection Criteria	69
Configuring Scheduled Settings	69
Configuring WLAN IP Settings	70
Configuring WLAN Settings	71
Configuring WWAN Settings	75
Viewing Where Network Profiles are Applied	77
Exporting Profiles for Configuring Enablers	77
Chapter 8: Managing Scan to Configure Profiles	79
Configuring Scan to Config Profiles	79
Adding Scan to Config Profiles	80
Configuring Settings	80
Adding Scan to Config Profile Authorized Users	81
Editing Custom Properties	81
Adding a Custom Property	82
Editing or Removing a Custom Property	82
Editing Registry Keys	83
Adding a Registry Key	83
Adding a Value to a Registry Key	84
Removing a Registry Key	84
Editing or Removing a Registry Key Value	85
Applying Scan to Config Profiles	86
Printing Barcodes	86
Scanning Barcodes	87
Chapter 9: Managing the Mobile Device Server	89
Configuring Mobile Device Server Profile Settings	89
Mobile Device Server Security	90
Mobile Device Server Resources	91
Mobile Device Server License Options	93
Mobile Device Server Profile Authorized Users	94
Mobile Device Settings on the Server Profile	94
Secondary Mobile Device Servers	96
Configuring Mobile Device Server Blackouts and Updates	97
Configuring Blackouts	97
Restricting Simultaneous Device Updates	98
Scheduling Profile-Specific Device Updates	99
Viewing Mobile Device Server Licensing Messages	100
Viewing Where Mobile Device Server Profiles Are Applied	101

Reinitializing the Mobile Device Server	101
Chapter 10: Managing Software Profiles	102
Configuring Software Profiles	102
Adding Software Profiles	102
Adding Software Profiles from the Quick Start Tab	103
Editing Software Profiles	104
Enabling Software Profiles	104
Software Profile Authorized Users	104
Software Profile Selection Criteria	105
Applying Software Profiles	105
Viewing Where Software Profiles Are Applied	105
Managing Software Packages	105
Adding Software Packages	107
Building New Software Packages	109
Installing CAB or MSI Packages	111
Copying Software Packages	112
Enabling Software Packages	112
Configuring Software Packages with a Utility	112
Configuring Software Packages for Delayed Installation	113
Peer-to-Peer Package Distribution	115
Chapter 11: Managing Mobile Devices	118
Mobile Device Inventory Tab	118
Viewing Mobile Device Details	119
Configuring Mobile Device Properties	120
Viewing Properties	121
Creating Custom Properties	121
Creating Device-Side Properties	122
Editing Properties	123
Deleting Properties	123
Contacting the Mobile Device	124
Pinging Mobile Devices	124
Sending Messages	125
Updating a Mobile Device	125
Locating a Mobile Device	126
Locating a Device using Cell Tower Information	127
Viewing Location History	127
Using Remote Control	128
Launching the Session Monitor	128
Launching Wavelink Communicator	130
Software Inventory	130
Chapter 12: Managing Mobile Device Profiles	131
Creating a Mobile Device Profile	131
Configuring Mobile Device Profile General Settings	132

Mobile Device Profile Authorized Users	132
Editing Custom Properties for Mobile Device Profiles	133
Adding a Custom Property	133
Editing or Removing a Custom Property	134
Editing Registry Keys for Mobile Device Profiles	135
Adding a Registry Key	135
Adding a Value to a Registry Key	136
Removing a Registry Key	136
Editing or Removing a Registry Key Value	137
Configuring Mobile Device Profile Advanced Settings	138
Location Based Services	138
Geofence Areas	139
Regional Settings	140
Update Restrictions	140
Viewing Where Mobile Device Profiles are Applied	141
Exporting Profiles for Configuring Enablers	142
Chapter 13: Managing Mobile Device Groups	143
Creating Mobile Device Groups	143
Adding Devices to Static Mobile Device Groups	144
Removing Devices from Static Mobile Device Groups	145
Viewing Devices in a Mobile Device Group	145
Adding Mobile Device Group Authorized Users	146
Pinging Mobile Devices within Mobile Device Groups	146
Sending Messages to Mobile Device Groups	147
Editing Properties for Mobile Device Groups	147
Additional Mobile Device Group Functions	149
Chapter 14: Managing Alert Profiles	150
Managing Alert Profiles	150
Creating Alert Profiles	151
Configuring Alert Profiles	151
Alert Profile Authorized Users	153
Viewing Where Alert Profiles Are Applied	153
Removing Alert Profiles	154
Adding Profiled Contacts	154
Importing E-mail Addresses	155
Removing Contacts	156
Adding Profiled Proxies	157
Deleting Proxies	157
Alerts Tab	158
Acknowledging Alerts	158
Clearing Alerts	158
Customizing Alert Browser Functionality	159
Chapter 15: Using Selection Criteria	160

Building Selection Criteria	161
Building Custom Properties	163
Selection Variables	163
Operators	171
Chapter 16: Using the Task Scheduler	175
Backing Up the System	175
Restoring the System	177
Appendix A: SSL Certificates	179
Appendix B: Avalanche Services	189
Appendix C: Port Information	191
Appendix D: Wavelink Contact Information	193
Glossary	194
Index	200

Chapter 1: Introduction

This document is a guide to the functions and components of Wavelink Avalanche. This document presents:

- An introduction to the Avalanche Java Console and conceptual information about Avalanche.
- Detailed information on the components of Avalanche.
- Tasks for creating an effective, secure wireless network.

NOTE The instructions contained in this guide pertain to the Avalanche Java Console. For details about performing tasks from the Web Console, see the Web Console User Guide.

This section provides the following introductory information:

- Managing Networks with Avalanche
- Getting Started
- About This Document

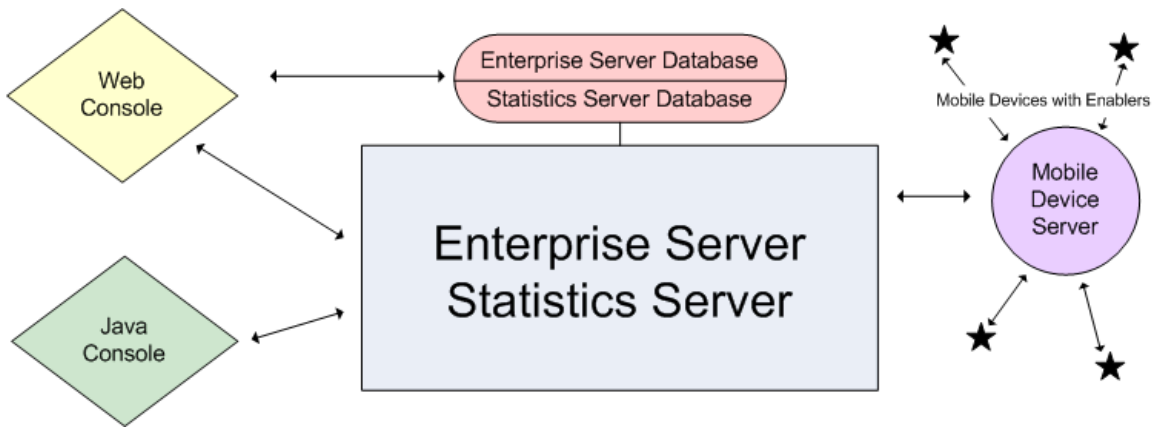
Managing Networks with Avalanche

Wavelink Avalanche provides solutions for organizations seeking to configure and maintain an enterprise-wide wireless network. This section describes several basic elements of Avalanche, including:

- Components of Avalanche
- Location Management: My Location and Sites

Components of Avalanche

Avalanche is an integrated system of several components, which together allow you to manage your wireless network quickly and efficiently. The following diagram provides a general overview of components and how they interact:



The primary components of Avalanche include:

- **Avalanche Java Console.** The Avalanche Java Console is your interface with wireless network components. With the Java Console, you can manage and maintain everything from device settings to mobile device software. The Java Console must be accessed from a computer where it has been installed.
- **Avalanche Web Console.** The Avalanche Web Console allows you to manage network components from any computer using an internet connection. It does not need to be installed.

NOTE To manage reports or use the floorplan setup, you must use the Web Console. These options are not available through the Java Console.

- **Enterprise Server.** The Enterprise Server facilitates all communication between the Console, the distributed servers, and the enterprise database.
- **Statistics Server.** The Statistics Server collects statistical information from your devices and distributed servers for reporting purposes and stores information in the stats database.
- **Databases.** Avalanche databases store information about your network and devices. There are two databases for Avalanche. The enterprise database handles information such as managing device configuration. The stats database manages statistical information regarding the state of devices on your network.

- **Mobile Device Server.** The Mobile Device Server is server-side software responsible for communication between the Avalanche Console, enterprise and statistics servers, and your mobile devices.
- **Enablers.** Mobile devices require additional software, called an Enabler, in order to be managed by Avalanche. An Enabler relays information between the mobile device and the Mobile Device Server. With the Enabler installed, the mobile device can receive configuration instructions that you create in the Avalanche Console.

In Avalanche Site Edition, the servers and databases are all installed on the same system. The Web Console and Java Console can be used locally or remotely, but the Java Console must be installed at each location where it will be used.

Location Management: My Location and Sites

One of the key aspects of Avalanche is location management. Avalanche SE provides you with one server location that you can subdivide into sites.

The Mobile Device Server relays information between the Avalanche Console, the enterprise server, the statistics server, and the mobile devices. Profiles can be applied at My Location and all mobile devices connecting to the Mobile Device Server that match the selection criteria will receive those profiles.

You can create sites at My Location. Each site uses selection criteria to determine which devices will be included. When a profile is applied at a site, all devices included in that site that match the profile selection criteria will receive that profile.

Getting Started

To better manage your Avalanche installation and configuration and to ensure optimal performance, Wavelink recommends you perform the following steps in order:

- 1 **Install Avalanche.** For more information, refer to *Installing Avalanche* on page 12.
- 2 **Activate Mobile Device licenses for Avalanche.** You should activate the number of licenses based on the number of devices you want to manage. For more information, refer to *Licensing* on page 14.
- 3 **Configure profiles.** A profile allows you to manage configurations and settings centrally and then deploy those configurations to as many sites as necessary. In this way, you can update or modify multiple sites instead of manually changing settings for each one. Avalanche provides network, scan to config, software, alert, Mobile Device Server, and mobile device profiles.

Once you create and deploy a profile, the Server and/or devices retain their configuration values until you change the profile or assign a new profile with a higher priority. Even if you alter device configuration values without using Avalanche, when the Server queries the device, it restores the configuration values from the assigned profile.

Default profiles reduce the time it takes to add new devices to a wireless network. If Avalanche detects a device that is not associated with a profile, Avalanche assigns the default profile for that location to that device.

About This Document

This user documentation provides assistance to anyone managing an enterprise-wide wireless network with Avalanche.

This document makes the following assumptions:

- You have a general understanding of the basic operational characteristics of your network operating systems.
- You have a general understanding of basic hardware configuration, such as how to install a network adapter.
- You have a working knowledge of your wireless networking hardware, such as infrastructure devices and mobile devices.
- You have administrative access to your network.

This document uses the following typographical conventions:

`Courier New`

Any time you interact with the physical keyboard or type information into a text box that information appears in the `Courier New` text style. This text style is also used for any file names or file paths listed in the text.

Examples:

The default location is `C:\Program Files\Adobe\FrameMaker7.1.`

Press `CTRL+ALT+DELETE.`

Bold

Any time this document refers to an option, such as descriptions of different options in a dialog box, that option appears in the **Bold** text style. This is also used for tab names and menu items.

Examples:

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

Italics

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

Examples:

See *Components of Avalanche* on page 7 for more information.

The *Infrastructure Profiles* dialog box appears.

Chapter 2: Installing Avalanche

Avalanche is designed to operate on a wide variety of network configurations. However, system requirements must be met to ensure optimal performance. Review requirements before installing. This chapter provides information about the following:

- Installing Avalanche Site Edition
- Uninstalling Avalanche

Installing Avalanche Site Edition

This section provides instructions for the installation process for Avalanche Site Edition (SE) with the included PostgreSQL database.

If you are currently running a version of Avalanche, refer to the migration documents or release notes located on the Wavelink Web site to ensure the latest version of Avalanche installs properly and no data is lost during the installation.

NOTE You cannot install Avalanche on a system where Mobile Manager Enterprise is currently installed. You must remove Mobile Manager Enterprise before you attempt to install Avalanche. For instructions about removing Mobile Manager Enterprise, refer to the *Mobile Manager Enterprise User's Guide* or contact Wavelink Customer Service.

NOTE If you stop the installation process, you must use the uninstall utility to remove any partially-installed components before you attempt to re-install. For information about uninstalling, refer to *Uninstalling Avalanche* on page 13.

To install Avalanche:

- 1 Obtain a copy of the installation file for Avalanche SE.
- 2 Double-click the file to start the installation process.
The *InstallShield Wizard* appears.
- 3 Click **Next** to continue the installation process.

The License Agreement screen appears.

- 4 If you agree with the terms in the License Agreement, click **Yes**.

The Choose Destination Location screen appears.

- 5 Click **Next** to accept the default installation folder, or click **Browse** to navigate to a folder of your choice. After you select an installation folder, click **Next**.

Avalanche is installed on your system.

The InstallShield Wizard Complete screen appears.

- 6 Click **Finish**.

Uninstalling Avalanche

You can run the Avalanche uninstall utility from the Windows Control Panel or from the **Programs** menu.

NOTE If you plan on uninstalling Avalanche and/or the PostgreSQL database, it is recommended that you backup database information and software collections. This can be done using the Task Scheduler. For more information, see *Using the Task Scheduler* on page 175.

To uninstall Avalanche:

- 1 From the **Start** menu, select **Settings > Control Panel > Add or Remove Programs > Wavelink Avalanche** and click **Change/Remove**.

-Or-

From the **Start** menu, select **Programs > Wavelink Avalanche > Uninstall Avalanche**.

The *Uninstall Wizard* appears.

- 2 Follow the wizard prompts, based on what you want to remove.

Upon completion, Avalanche and any selected components are removed from your system.

Chapter 3: Licensing

Avalanche requires licenses for full functionality. You can access and use the Avalanche Console without licenses, but you will be limited to the demo or unlicensed mode and will have limited functionality. You will not be able to manage mobile devices.

This chapter provides information about the licensing options for Avalanche, and includes the following topics:

- Overview of Wavelink Licensing
- Running the License Server
- Activating Licenses
- Releasing Licenses
- Importing the Enterprise License

Overview of Wavelink Licensing

Avalanche requires one license for each mobile device it manages. When a server detects a new wireless device, a license request is sent to the License Server. The License Server then sends a license to the server to be distributed. The license file is unique to the server and cannot be transferred to another server. Once the device receives the license, Avalanche can manage that device. If a license expires or is released, the license returns to the pool of licenses at the License Server until it is requested by another server.

For users' convenience, some licenses may come with a license start date. You can activate these licenses and they will appear in the *Licensing* dialog box, but the License Server will not be able to distribute them until the date specified.

NOTE To obtain any Avalanche license, please contact Wavelink Customer Service.

There are two sets of licenses available with Avalanche: base and maintenance. Base licenses are required to manage devices when using any variety of Avalanche version 5 (5.x). You will also need maintenance licenses if you have upgraded beyond version 5.1. For example, if you upgraded to 5.5, you would need a 5.x base license and a maintenance license for each device you want to manage.

The following table provides a summary of license types and functions.

This license type:	Will license:
Base/4.1 or earlier	Any mobile device with Enabler version 4.02
Older Maintenance (3.4 or earlier)	Any mobile device with an OS version earlier than 5.0 and any Enabler version
Current Maintenance (3.5 or later)	Any device with any Enabler version and any OS version

When you run Avalanche without a valid license, the mobile device appears in the Mobile Device Inventory list, but you will not be able to manage the mobile device. You cannot deploy software packages or network profiles to the mobile device.

Running the License Server

The License Server is a Wavelink service that runs on a host system as part of Avalanche. The License Server is responsible for supplying licenses to Avalanche mobile devices. It listens on TCP port 7221. For the License Server to function properly, this port must be open and not blocked by a firewall.

The License Server is a service that starts automatically. If for some reason the License Server is not running, the Mobile Device Server will not be able to receive licenses.

Activating Licenses

This section provides the following information about activating your Avalanche licenses:

- Activating Avalanche Licenses
- Activating Licenses for Wavelink Products

Activating Avalanche Licenses

When you activate Avalanche licenses, your licenses are verified and the License Server can then distribute them to the wireless devices on your network.

This section provides information on the following processes:

- Activating Automatically

- Activating Manually
- Importing a License
- Activating Demo Mode

Activating Automatically

If Avalanche resides on a system that has Internet access, you can use automatic license activation. Avalanche connects with a secure Wavelink Web Server to verify your license.

NOTE If your Internet access is restricted through a proxy server, you will need to configure HTTP Proxy settings before you can activate licenses automatically. For information on configuring proxy settings, see *Configuring HTTP Proxy Settings* on page 35.

To activate Avalanche:

- 1 Obtain the Avalanche product licensing code from Wavelink.

NOTE You receive this information in an e-mail from Wavelink upon purchasing Avalanche.

- 2 From the Avalanche Console, click **Tools > Manage Licensing**.

The *Licensing* dialog box appears.

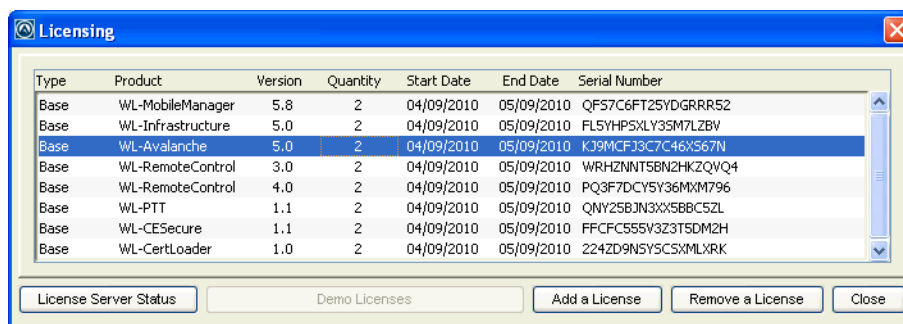


Figure 3-1. Licensing dialog box

3 Click **Add a License**.

The *Add a License* dialog box appears.



Figure 3-2. *Add a License* dialog box

4 Click **Activate a License**.

The *Activate a License* dialog box appears.

5 Type the Product License in the text box and click **Activate**.

Avalanche connects with a secure Wavelink Web site and your license is verified. The details of the new license appear in the *Add a License* dialog box.

6 Verify that the license information is correct and click **Use License**.

The licenses appear in the *Licensing* dialog box.

Activating Manually

If the server is not connected to the Internet or if you have problems with the automatic activation, you can activate your license manually.

To activate your license manually you will need the following information:

- Node lock for the system. To find the node lock, launch the Java Console and click **Help > About Avalanche**. The nodelock will be listed in the dialog box as **Wavelink Enterprise Service NodeLock**.
- Product license code. This information comes from the e-mail you receive from Wavelink upon purchasing Avalanche.

To manually activate a license:

- 1 Open a Web browser and navigate to `http://www.wavelink.com/activation`.
- 2 Enter the **Hardware Node Lock** and the **License Key** in the text boxes.
- 3 Click **Activate** button to activate license.

The Wavelink activation server verifies the information you entered and provides you a link to download a `wavelink.lic` file if your node lock and license key are valid.

- 4 Click on the link and change **Save As** type to **All Files**.
- 5 Download the file to desired location.
- 6 Move the `wavelink.lic` file to the system with Avalanche installed.
- 7 Follow the steps to import a license.

Importing a License

If you if you have received a `wavelink.lic` file using the manual activation method, you can activate the file by importing it.

NOTE If you have a `wavelink.lic` file from an older installation, you must contact Wavelink Support to reissue the license before you can import it into Avalanche 5.0.

To import a license:

- 1 From the Avalanche Console, click **Tools > Manage Licensing**.

The *Licensing* dialog box appears.

- 2 Click **Add a License**.

The *Add a License* dialog box appears.

- 3 Click **Import a License**.

The *Select License* dialog box appears.

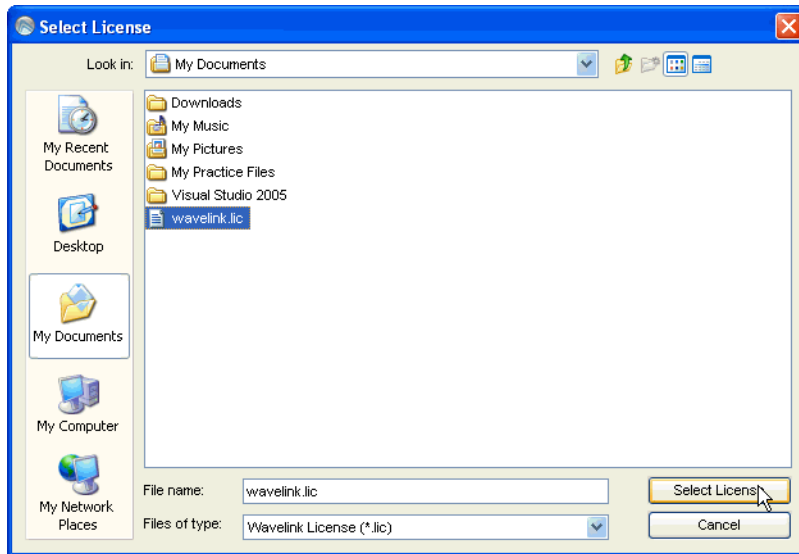


Figure 3-3. Select License dialog box

- 4 Navigate to the location of the `wavelink.lic` file, select it and click **Select License**.

The details of the new license appear in the *Add a License* dialog box.

- 5 Verify that the license information is correct and click **Use License**.

The licenses are imported and will appear in the list in the *Licensing* dialog box.

Activating Demo Mode

If you are installing Avalanche for demonstration purposes, you can run Avalanche in demo mode. Demo mode authorizes 2 base licenses for 30 days for the following products:

- Avalanche 5.0 (2 mobile device licenses and 2 infrastructure device licenses)
- Remote Control 4.0
- Remote Control 3.0
- Communicator 1.1
- CE Secure 1.1

- Certificate Manager 1.0

To activate demo mode:

- 1 Access the *Licensing* dialog box by clicking **Tools > Manage Licensing**.

The *Licensing* dialog box appears.

- 2 Click **Demo Licenses**.

Avalanche will run in demo mode. Once demo mode has been activated on one Console, no other Console connecting to the Enterprise Server will be able to activate demo mode.

Activating Licenses for Wavelink Products

For other Wavelink products used in conjunction with Avalanche 5.0, you must use the same activation method (from the Avalanche Console) that you used for Avalanche 5.0. You can activate these product licenses automatically, or if you already have a `.lic` file associated with the license, you can import the `.lic` file.

Refer to *Activating Automatically* on page 16, *Activating Manually* on page 17 or *Importing a License* on page 18 for steps to activate licenses.

NOTE If you have a `wavelink.lic` file from an older installation, you must contact Wavelink Support to reissue the license before you can import it into Avalanche 5.0.

Releasing Licenses

Licenses for mobile devices are frequently redistributed, providing flexibility in managing licenses. To encourage redistribution, you can configure the Mobile Device Server to release licenses from mobile devices that have not connected to the network within a specific number of days. You can also release licenses by deleting devices from the Mobile Device Inventory.

For information about configuring the Mobile Device Server to release licenses, refer to *Mobile Device Server License Options* on page 93. For information about deleting devices from the Mobile Device Inventory, refer to *Mobile Device Inventory Tab* on page 118.

Importing the Enterprise License

Enterprise Licenses grant you unlimited licenses for your mobile devices.

If you have an Enterprise License for your Avalanche system, you must import the license into the Console. This will apply the license to the Enterprise Server and brand the Console with an image of your choosing. Once you import the license, anytime the Console connects to the branded Enterprise Server, the image will appear in the upper-right corner of the Console.

For information about creating an image and obtaining an Enterprise License, contact Wavelink Customer Service.

There is no way to remove the enterprise image once it has been imported.

To import the Enterprise License:

- 1 From the **File** menu, select **Import > Enterprise License**.

A search dialog box appears.

- 2 Navigate to and select the Wavelink License File (.wlf extension).
- 3 Click **Open**.

The Enterprise license will be applied to the Enterprise Server and the Console will retrieve the enterprise image.

Chapter 4: Avalanche Java Console

You interact with your wireless network primarily using the Avalanche Console. The Avalanche Console allows you to control global characteristics of your wireless network. These characteristics include creating profiles, assigning IP addresses, and monitoring network performance.

The Avalanche Console is traditionally accessed from a computer where the Console has been installed. This installed Console is the Java Console. However, using a Web browser, you also can access a version of the Console from a computer where the Console has not been installed. This is called the Web Console. The Web Console allows you to create and view reports and floorplans, view inventory, and manage profiles and alerts for your enterprise.

NOTE This version of Avalanche help is specific to the Java Console. For more information on using the Avalanche Web Console, please see the *Avalanche SE Web Console User Guide* or launch the Web Console and click the **Help** button.

This section contains the following topics for the Java Console:

- Launching the Avalanche Console
- Understanding the Avalanche Console
- Changing Console Preferences
- Managing Device Inventory Displays
- Managing the Enterprise Server
- Viewing the Inforail Status
- Using the Support Generator
- Using the Enabler Installation Tool

Launching the Avalanche Console

Using the Avalanche Console, you can configure and manage your wireless network. You can open the Avalanche Console from the **Programs** menu or from a shortcut.

To launch the Avalanche Console:

- 1 From the **Start** menu, select **Programs > Wavelink Avalanche SE > Avalanche SE Console**.

The *Wavelink Avalanche Login* dialog box appears.

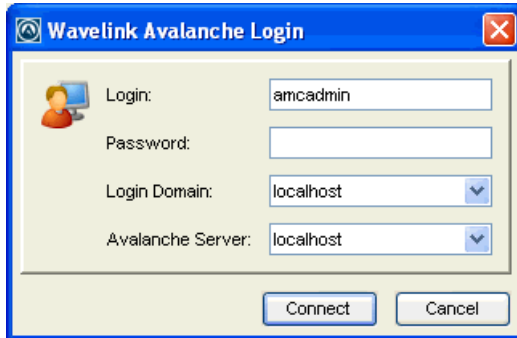


Figure 4-1. *Wavelink Avalanche Login*

- 2 Enter your **Login** and **Password**.

Avalanche is installed with a default user login of *amcadmin* and password of *admin*. Wavelink recommends you create a new password for this admin account once you have logged in. For information about changing passwords, refer to *Managing User Accounts* on page 47.

- 3 From the **Login Domain** drop-down list, select your domain.
- 4 From the **Avalanche Server** drop-down list, select your host (the location of the enterprise server).
- 5 Click **Connect**.

The *Avalanche Server Login* dialog box appears. This dialog box indicates the progress of the Console as it attempts to contact the Enterprise Server.

If your Console can contact the Enterprise Server and your credentials are valid, the Avalanche Console appears.

If there are updates available, a dialog box will appear asking if you want to download automatically. You can download the updates or save the updates for the next time you launch the Console.

NOTE To launch the Web Console after you have launched the Java Console, click **View > Launch Web Console**. For further information regarding the Web Console, click the Web Console **Help** button.

Understanding the Avalanche Console

The Avalanche Console consists of a Tool Bar, Navigation Window, and Management Tabs that allow you to manage your wireless network and provide information regarding wireless network configuration and activity.

- The buttons on the Tool Bar provide quick access to commonly used tools.
- The Navigation Window provides a tree view of your wireless network.
- The Management Tabs provide access to inventories, alerts, and other properties of your enterprise. The tabs available depend on what is selected in the Navigation Window.

Many of the options on the Management Tabs require you to enter Edit Mode before you can change them. This prevents any accidental changes and permits only one user to edit an item at a time.

This section gives details about the following areas:

- Tool Bar
- Navigation Window
- Quick Start Tab
- Profiles Tab
- Understanding Edit Mode

Tool Bar

The following table provides information about the Tool Bar buttons.



Click this button to log out of the Avalanche Console and log in as a different user.



Click this button to log out of the Avalanche Console. You will not be prompted to log in as another user.



Click this icon to open the Task Scheduler and schedule deployment tasks.



Click this icon to open the *User Management* dialog box. You can edit your list of users and permissions in this dialog box.



Click this icon to access the Avalanche Help.

The other three buttons on the Tool Bar are for using Edit Mode. For more information about Edit Mode, see *Understanding Edit Mode* on page 28.

Navigation Window

The Navigation Window, located on the left side of the Java Console, displays your enterprise in a tree view. You can move through the server location and sites by either expanding nodes or using the Search functionality.

To use the Search function:

- 1 Type in the name of the site in the text box just above the tree view.
- 2 Click **Search**.

The highlight will move to the first site whose name begins with the text you entered. The search is not case sensitive.

If there are multiple matches, click **Search** until you reach the correct site.

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

Quick Start Tab

When you first launch the Console, the **Quick Start** tab displays. This tab provides links for quickly getting your enterprise configured and includes required and optional tasks. Each task is accompanied by a brief description which you can view by clicking the plus [+] button.

The **Quick Start** is divided into the following sections:

- Profiles Configuration
- Tools
- Help and Support

If you do not want to display the **Quick Start** you can disable the tab by selecting **View > Quick Start**. You can also disable the **Show Quick Start on Startup** check box located on the **Quick Start** tab. This ensures the **Quick Start** does not appear each time you launch the Console.

Profiles Configuration

The tasks in this region are optional and can be done in any order. These tasks include:

- Create a Network Profile. For details, refer to *Managing Network Profiles* on page 66.
- Add Device Software. For details, refer to *Managing Software Profiles* on page 102.
- Create a Scan to Config Profile. For details, refer to *Managing Scan to Configure Profiles* on page 79.

Tools

This section allows you to install an Avalanche Enabler onto a mobile device or check for Avalanche updates.

Help and Support

This region provides links to the Avalanche Help, Wavelink Support, and launches the Support Generator. For details about using the Support Generator, refer to *Using the Support Generator* on page 43.

Profiles Tab

From the **Profiles** tab you can manage your profiles. A profile allows you to apply the same set of configurations to multiple servers or devices. There are eight types of profiles in Avalanche MC:

- **Alert profile.** An alert profile allows you to configure what events generate an alert and who is notified when an alert is generated. For information on alert profiles, see *Managing Alert Profiles* on page 150.
- **Mobile Device Server profile.** A Mobile Device Server profile allows you to configure administrative, security, and connection settings for your Mobile Device Servers. For information on Mobile Device Server profiles, see *Managing the Mobile Device Server* on page 89.
- **Mobile device profile.** A mobile device profile allows you to change settings on your mobile devices, as well as add, change, and remove custom properties and registry keys. For information on mobile device profiles, see *Managing Mobile Device Profiles* on page 131.
- **Network profile.** A network profile allows you to configure network information (such as IP addresses) and encryption and authentication for your mobile devices. For information on network profiles, see *Managing Network Profiles* on page 66.
- **Scan to Config profile.** A Scan to Config profile allows you to print network configuration information in a barcode. When the barcode is scanned with a device, the information is applied on the device. For information on Scan to Config profiles, see *Managing Scan to Configure Profiles* on page 79.
- **Software profile.** A software profile allows you to organize and configure software packages for deployment to multiple devices. For information on software profiles, see *Managing Software Profiles* on page 102.

On the **Profiles** tab, the Profile List displays all the profiles that have been created, along with their type, name, status, details, and any associated selection criteria. The columns in this list can be sorted in alphabetical order or reverse alphabetical order by clicking the column header.

You also have the option of filtering the profiles displayed. When you activate a filter, only the profiles matching the filter will be displayed in the Profile List. You can apply filters on multiple columns at the same time.

To filter the Profile List:

- 1 In the Profile List, right-click the header for the column you want to filter by.
- 2 Click **Set Filter** in the context menu.

The *Set Column Filter* dialog box appears.

- 3 If you are sorting by **Profile Type**, **Default?**, or **Status**, you see a list of available categories. Enable the checkboxes next to the categories you want to include in the filter and click **OK**.

-Or-

If you are sorting by **Name** or **Selection Criteria**, you are prompted to type a term you want to sort by. The filter includes all profiles with the term in the field you are sorting by. Click **OK**.

The filter is applied to the Profile List. To remove a filter after it has been applied, right-click the column header and select **Clear Filter**.

Understanding Edit Mode

The Tool Bar also contains three Edit Mode buttons. Before you can edit a profile, device group, or server location properties, you must enter Edit Mode.

While you are using Edit Mode, the item you are editing will be locked. While Edit Lock is engaged, no other user will be able to attempt to edit the configuration. Edit Lock has an automatic timeout, at which point you will be prompted in order to continue editing. If you do not respond to the prompt within the time configured, then your Edit Lock will be cancelled and you will not be able to save your changes.

The timeout for Edit Lock has a default setting of 15 minutes, and the prompt timeout has a default setting of 1 minute. For instructions on configuring these timeouts, see *Edit Lock Control* on page 31.

To use Edit Mode, you employ the following icons located in the toolbar:



Click **Edit** to enable Edit Mode so you can make configuration changes. This button is active when you are on the **Device Groups**, **Profiles**, or **dServer Location Properties** tabs.



Click **Cancel** to erase any changes you made in edit mode. When you click Cancel, you will exit edit mode.



Click **Save** to save configuration changes.

Consider the following when using Edit Mode:

- When you enter Edit Mode, you will not be able to navigate away from the current tab (i.e., **Device Groups, Profiles, or dServer Location Properties**) until you exit Edit Mode. The Navigation Window will not be available while you are in Edit Mode.
- If you add a new profile, you will need to click Edit Mode before you can continue configuration.
- You cannot remove a profile while you are in Edit Mode. You must either save or cancel. You can then select the profile and click **Remove Profile**.
- You do not need to enter Edit Mode to view where profiles are applied (**Applied Location** tabs).
- When working in software profiles, you do not need to be in Edit Mode to install or configure software packages. Software package configuration changes are saved to the package rather than to the Console. However, you must enter Edit Mode to configure any other software package options.

Changing Console Preferences

You can customize features of the Avalanche Console from the *Preferences* dialog box. This section provides information about the following Console preferences tasks:

- Customizing General Console Settings
- Edit Lock Control
- Configuring Audit Logging
- Viewing the Audit Log
- Specifying the Backup Drive Location

- Configuring E-mail Settings
- Configuring HTTP Proxy Settings

Customizing General Console Settings

Wavelink gives you the option to automatically check online each time you launch the Console to see if there are any software updates for Avalanche. You also can configure Avalanche to send usage data to Wavelink to improve service and usability. The Avalanche Console can be modified in appearance, including display size, position and default page view from the *Preferences* dialog box. You can also configure the manner in which the Alert Browser manages alerts.

To customize the general Console settings:

- 1 Click **Tools > Preferences**.

The *Preferences* dialog box appears.

- 2 Select the **General** tab.
- 3 In the Auto Update Settings region, configure whether Avalanche should check for updates or upload usage information to Wavelink.
- 4 In the Console Display Settings region, configure the width, height, and the frame positions for the Avalanche Console.
- 5 In the Alert Browser Settings region, use the text boxes to configure how many days an alert remains in the Alert Browser, the maximum number of alerts that can appear in the Alert Browser, and the maximum number of alerts to store.

NOTE Alerts are stored in the enterprise database.

- 6 Click **Apply** to save your changes.
- 7 Click **OK** to close the *Preferences* dialog box.

The Avalanche Console updates to reflect your changes.

Edit Lock Control

You can configure two options for Edit Lock: how long before the Edit Lock times out and prompts the user, and how quickly after the prompt appears the Edit Lock will terminate.

To configure Edit Lock control:

- 1 Click **Tools > Preferences**.

The *Preferences* dialog box appears.

- 2 Select the **Enterprise Server** tab.
- 3 In the Edit Lock Control region, select **Enable Edit Lock Control** and set the **Edit Lock Timeout** and **Timeout Warning Tolerance**.
- 4 Click **Apply** to save the changes.
- 5 Click **OK** to close the *Preferences* dialog box.

Configuring Audit Logging

The audit log in Avalanche collects information about actions performed from the Avalanche Console. As part of the data collection, the audit log includes the IP address of each Console that generated a logged event. Audit logging stores information in the enterprise database and can be enabled by any user. However, configuring audit logging preferences, viewing, and clearing the log can only be performed by an Administrator.

NOTE For information on viewing and clearing the audit log, see *Viewing the Audit Log* on page 33.

The audit log will store up to 200,000 actions in the database. When the 200,000 limit has been reached, Avalanche will store the oldest records in a `.csv` file in the backup directory and delete them from the database.

You can also archive the audit log at a specific time every day. When the information is archived, it is copied to a `.csv` file. The `.csv` file is stored in the same directory where a backup file would be stored. For information on configuring the backup file location, see *Specifying the Backup Drive Location* on page 33.

The following events can be configured for logging:

Deployment Package modifications	When a deployment package is modified.
Device Group modifications	When a device group is modified.
Node, Location modifications	When a region or location is modified.
Profile Application modifications	When a profile is applied, excluded, or removed from a location.
Profile modifications	When a profile is modified.
Scheduled Event, Apply/Deploy Profiles	When an Apply/Deploy Profiles event has occurred.
Scheduled Event, Deploy/Update Servers	When a Deploy/Update Servers event has occurred.
Scheduled Event, System Backup	When a System Backup event has occurred.
Scheduled Event, System Restore	When a System Restore event has occurred.
Scheduled Event, Uninstall Server	When an Uninstall Server event has occurred.
Scheduled Event, Universal Deployment	When a scheduled Universal Deployment event has occurred.
Scheduled Event, Update Firmware	When an Update Firmware event has occurred.
User Logon/Logoff	When a user logs on or logs off the Avalanche Console.
User modifications	When a user account is modified.
VLACL modifications	When the VLACL is modified.

To enable audit logging:

- 1 Click **Tools > Preferences**.

The *Preferences* dialog box appears.

- 2 Select the **Audit Logging** tab.
- 3 Enable the **Enable Audit Logging** check box.
- 4 If you want the audit log archived, enable **Enable Audit Log Archiving** and select the time of day (using a 24-hour clock) you want the log to be archived.
- 5 From the list, enable the events you want to record.
- 6 Click **Apply**.
- 7 Click **OK** to close the *Preferences* dialog box.

Viewing the Audit Log

If you enable audit logging for the Console, you can view the activity from the Audit Log. The log provides information based on the logging preferences you set for audit logging. You can view the date and time of the Console activity, the IP address and username of the person who performed the action, and a description of the changes that occurred.

A user can select criteria he wishes the server to filter log-retrieval with, allowing the user to retrieve the entire log or just the entries that meet the specified criteria.

To view the audit log:

- 1 Click **View > Audit Log**.

The *Audit Log* dialog box appears.

- 2 Use the filters at the bottom of the dialog box to filter which log entries you want displayed.
- 3 If you want to delete all entries in the audit log, click **Clear Log**. This will remove all entries from the database and archive the information in a `.csv` file in the backup directory.

Specifying the Backup Drive Location

You can specify where you want to store any backups of Avalanche. The location must be a qualified path for the Enterprise Server. If you do not want to specify a path, the backups will be stored to the default location, `C:\Program Files\Wavelink\AvalancheSE\backup`.

For information about backing up your system, refer to *Backing Up the System* on page 175.

To specify a location:

- 1 Click **Tools > Preferences**.

The *Preferences* dialog box appears.

- 2 Select the **Server** tab.
- 3 In the Backup/Restore region, enter the path where you want to save system backups.
- 4 Click **Apply**.
- 5 Click **OK** to close the *Preferences* dialog box.

Configuring E-mail Settings

When you create an alert profile, you have the option to e-mail alerts generated to that profile to an e-mail account. If you choose to e-mail alerts, you must configure Avalanche to contact an e-mail server.

To configure e-mail settings:

- 1 Click **Tools > Preferences**.

The *Preferences* dialog box appears.

- 2 Select the **E-Mail & HTTP** tab.
- 3 Type the location of the e-mail server you want Avalanche to use in the **E-Mail Server** text box.
- 4 Select the port Avalanche should use when contacting the e-mail server.
- 5 Type the **Username** and **Password** in the text boxes.
- 6 Type the address the e-mails will appear from in the **From Email** text box.
- 7 Type the address a reply should be forwarded to if an alert e-mail is replied to in the **Reply-to Email** text box.
- 8 Click **Apply**.
- 9 Click **OK** to return to the Avalanche Console.

Configuring HTTP Proxy Settings

If you are using an HTTP proxy for external Web site connections, you can configure HTTP proxy settings to ensure Avalanche can connect.

To configure HTTP proxy settings:

- 1 Click **Tools > Preferences**.

The *Preferences* dialog box appears.

- 2 Select the **E-Mail & HTTP** tab.
- 3 Enable the **Use HTTP Proxy Server** checkbox.
- 4 In the **Host** text box, type either the IP address or name of the proxy.
- 5 Type a port number in the **Port** text box.

If no port is entered, the port will default to port 80.

- 6 If you are using Basic Authentication for the HTTP proxy, type the **User Name** and **Password** in the appropriate text boxes. Otherwise, leave these options blank.
- 7 Click **OK** to save your changes.
- 8 To disable the use of a proxy, disable the **Use a Proxy Server** checkbox in the *Preferences* dialog box.

When you disable the proxy server and save the change, all proxy settings are removed from the database.

Managing Device Inventory Displays

Device lists are available on the **Mobile Device Inventory** and **Mobile Device Group** tabs. These lists display the devices associated with the currently selected region, server location, or mobile device group.

Device lists can be customized to display specific information. You can sort the lists, filter the lists using custom filters, or modify the columns displayed. This section contains the following information on customizing inventory displays:

- Inventory Paging
- Managing Device Filters

- Modifying Columns for Mobile Device Lists
- Adding Custom Columns for Mobile Device Lists
- Reorganizing Columns for Mobile Device Lists
- Displaying Custom Mobile Device Icons

Inventory Paging

Device lists allows you to select how many devices you want to appear in the inventory list at a time. The list displays the devices in the order Avalanche pulls the information from the database. You may need to page through the list to view more devices.

To configure inventory paging:

- 1 From the **Number of Devices Per Page** drop-down list, select the number of devices you want to display.
- 2 Use the arrow keys to move forward and backward through the pages.
- 3 Use the refresh button to refresh the list of mobile devices.

Managing Device Filters

You can filter which devices are displayed in a device list by creating and applying device filters. When a filter is applied, only the devices meeting the criteria associated with that filter will be displayed. Filtering is available for the lists in the Mobile Device Inventory and mobile device groups. This section contains the following information:

- Creating Device Filters
- Applying Device Filters
- Deleting Device Filters

Creating Device Filters

To display only devices that meet certain criteria in the device list, you must create a device filter.

To create a filter:

- 1 Click **Edit Filters**.

The *Modify Device Filters* dialog box appears.

- 2 Enter a name for the new filter in the **Filter Name** text box.
- 3 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 *Building Selection Criteria* on page 161 for more information on building selection criteria.

- 4 When you are finished building selection criteria for the filter, click **OK** to return to the *Modify Device Filters* dialog box.

The selection criteria appear in the **Filter Expression** text box.

- 5 Click **Add Filter**.

The filter is added to the **Existing Filters** list and is available to use.

- 6 Click **OK**.

You can now select the filter from the **Current Mobile/Infra Device Filter** drop-down list located at the top of the device list.

Applying Device Filters

After you create device filters, they can be applied to the device list. When the filter is applied, only the devices matching the selection criteria of the filter will appear in the device list.

To apply a filter:

- 1 Select the filter from the **Current Mobile/Infra Device Filter** drop-down list.
- 2 Click **Apply Filter**.

Deleting Device Filters

If you decide that a device filter is no longer necessary, you can delete that filter from the Avalanche Console.

To delete a filter:

- 1 Click **Edit Filters**.

The *Modifying Device Filters* dialog box appears.

- 2 In the Existing Filters list, select the filter you want to delete.

- 3 Click **Delete**.

Modifying Columns for Mobile Device Lists

The Avalanche Console allows you to control which columns appear in the mobile device list, and the manner in which they display.

To modify a column:

- 1 Right-click on the column header and select **Modify Columns**.

The *Modify Mobile Device Columns* dialog box appears. Column headers listed in the **Available Columns** list are headers that do not currently display in the tab. Column headers listed in the **Selected Columns** list are those that currently display in the tab.

- 2 From the **Available Columns** list, select which column you want to display and click **Add Column(s)**.

The column name moves to the **Selected Columns** list.

- 3 To remove columns from the **Selected Columns** list, select the column you want to remove and click **Remove Column(s)**.

The column name returns to the **Available Columns** list.

- 4 Use the **Move Up** and **Move Down** to modify the order in which the columns appear in the **Mobile Device Inventory** tab.

- 5 When you are finished, click **OK**.

The columns are rearranged to reflect your modifications.

Adding Custom Columns for Mobile Device Lists

If you have created custom properties for your mobile devices, you can display them in a column in a mobile device list.

For details about creating custom properties, refer to *Creating Custom Properties* on page 121.

To display columns for custom properties:

- 1 Right-click the column header and select **Modify Columns**.

The *Modify Mobile Device Columns* dialog box appears.

- 2 Click **Add Custom**.

The *Custom Property Column* dialog box appears.

- 3 From the **Property Key** drop-down list, select the custom property you want to add as a column.
- 4 In the **Column Title** text box, type the name of the column as you want it to display in the **Mobile Device Inventory** tab.
- 5 From the **Data Type** drop-down list, select what type of data this column displays.
- 6 Configure the remaining options according to preference.
- 7 Click **OK** to return to the *Modify Mobile Device Columns* dialog box.

The column name for the property is now listed in the **Available Columns** list.

- 8 Select the column name and click **Add Column** to move the property to the **Selected Columns** list.
- 9 Click **OK** to return to the Console.

The column now displays in the tab and can be sorted just as any other column.

Reorganizing Columns for Mobile Device Lists

You can remove, reset, and align columns for a mobile device list, as well as sorting the devices listed by column.

To reorganize columns:

- To remove columns, right-click the column and select **Remove Column**.
The column is removed from the list view. You can restore this column using the *Modify Mobile Device Columns* dialog box.
- To reset the columns, right-click the column header and select **Reset Columns**.
- To sort by column, right-click the column and select **Sort Ascending** or **Sort Descending**.
- To align columns, right-click the column and select **Align Column - Left**, **Align Column - Right**, or **Align Column - Center** according to the way you want the information to appear.

Displaying Custom Mobile Device Icons

The Console supports custom mobile device icons that are sent from the mobile device. There two device images are displayed: a small icon appears in the Mobile Device Inventory tab next to the name of the mobile device and a larger icon appears in the *Mobile Device Details* window.

For more information about custom device icons, refer to *Using Custom Device Icons in Avalanche*, located on the Wavelink web site.

Managing the Enterprise Server

From the **Tools** menu, you can manage the communication between the distributed servers and the enterprise server. This section contains the following tasks:

- Viewing the Enterprise Server Status
- Purging Server Statistics
- Performing a Dump Heap

Viewing the Enterprise Server Status

You can view the status of the eServer in the *eServer Console* dialog box. The eServer Status region lists the status (parameters and values) of the eServer. Click **Refresh Status** to receive the latest information from the eServer.

The following list describes some of the parameters and values displayed in the eServer Status region:

Parameter	Value
Version	The version of the enterprise server.
Build Number	The build number of the enterprise server.
Uptime	The length of time the enterprise server has been running.
Start Time	The last time the enterprise server was started.
Current Time	The current time.
Messages Received	The total number of messages the server has received.
Messages Sent	The total number of messages the server has sent.
Spillover Enabled	Whether the memory spillover function is enabled (YES or NO).
Spillover Threshold	The memory level before spillover takes effect.

Parameter	Value
Spillover Release	The number of seconds before the spillover is released.
Blackout Mode	<p>If blackout mode is enabled and which servers are included in the blackout.</p> <p>Off indicates that blackout mode is not currently in use.</p> <p>All Servers indicates that all servers are in blackout mode.</p> <p>Mobile Device Servers indicates that only the Mobile Device Servers are in blackout mode.</p> <p>Infrastructure Servers indicates that only the Infrastructure Servers are in blackout mode.</p>
Priority C0 - C2 Backlog	The number of messages coming from Consoles, with C0 being the highest priority and C2 being the lowest priority.
Priority A0 - A2 Backlog	The number of messages coming from the distributed servers, with A0 being the highest priority and A2 being the lowest priority.

Purging Server Statistics

To prevent database inflation, you can configure Avalanche to purge logged statistics. You can configure the following for Mobile Device Servers alerts and statistics:

- **Purge Time.** Set the time of day you when you want to remove the statistics.
- **Number of Days to Keep.** Set the number of days you want to keep the statistics before removing them. Wavelink recommends setting the days to keep statistics fairly low as the statistics accumulate quickly and the purging process could take a very long time if there are too many statistics. The maximum number of days you can set is 30.

To configure purge settings:

- 1 Click **View > Enterprise Server Status**.

The *eServer Status* dialog box appears.

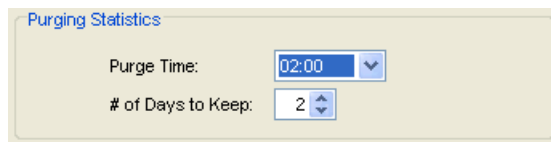


Figure 4-2. Purging Statistics in the *eServer Status* dialog box

- 2 In the **Purging Statistics** section, configure the days you want to keep the statistics and the time you want the statistics to be removed.
- 3 Click **OK** to save your settings.

Performing a Dump Heap

If the memory level starts to affect the performance of your Enterprise Server, you can perform a dump heap. This will dump all the live objects and classes into a file located in the default installation location.

Before you perform the dump, you can also verify the thread information which can help you decide if the dump is necessary.

To perform a dump heap:

- 1 Click **View > Enterprise Server Status**.

The *eServer Status* dialog box appears.

- 2 In the eServer Diagnostics region, click **Thread Information**.

A dialog box appears containing the thread information. You can print this information or close the dialog box.

- 3 Once you have determined you want to perform the dump heap, click **Dump Heap**.

A message appears indicating the name and the size of the dump file.

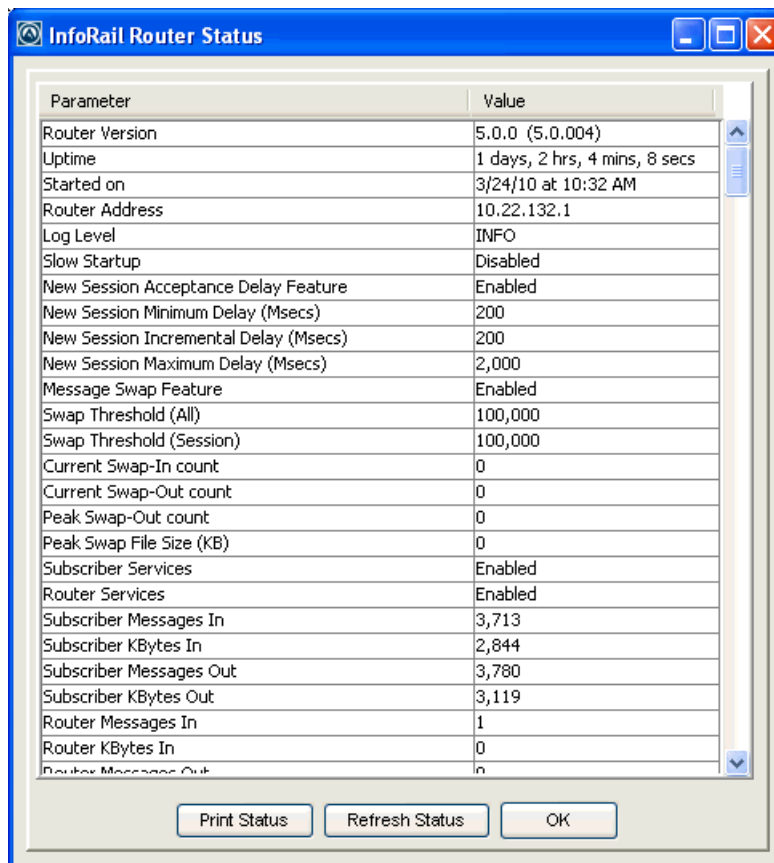
Viewing the Inforail Status

The InfoRail Router coordinates communication between Avalanche processes. The InfoRail Router Status dialog box provides information such as the version of the router, how long it has been running, the IP address, etc. From this dialog box you can print or refresh the status. You cannot change any of the parameters listed.

To view the InfoRail status:

- 1 Click **View > InfoRail Router Status**.

The dialog box appears.



Parameter	Value
Router Version	5.0.0 (5.0.004)
Uptime	1 days, 2 hrs, 4 mins, 8 secs
Started on	3/24/10 at 10:32 AM
Router Address	10.22.132.1
Log Level	INFO
Slow Startup	Disabled
New Session Acceptance Delay Feature	Enabled
New Session Minimum Delay (Msecs)	200
New Session Incremental Delay (Msecs)	200
New Session Maximum Delay (Msecs)	2,000
Message Swap Feature	Enabled
Swap Threshold (All)	100,000
Swap Threshold (Session)	100,000
Current Swap-In count	0
Current Swap-Out count	0
Peak Swap-Out count	0
Peak Swap File Size (KB)	0
Subscriber Services	Enabled
Router Services	Enabled
Subscriber Messages In	3,713
Subscriber KBytes In	2,844
Subscriber Messages Out	3,780
Subscriber KBytes Out	3,119
Router Messages In	1
Router KBytes In	0
Router Messages Out	0

Figure 4-3. InfoRail Router Status

- 2 To print the status page, click **Print Status**.
- 3 To refresh the statistics, click **Refresh Status**.
- 4 Click **OK** to close the dialog box.

Using the Support Generator

The Support Generator creates a `.zip` file that contains Avalanche log files and additional information you provide when you run the Support Generator. The log files compiled in the `.zip` file include:

- EConsole.log
- AvalancheServer.log
- InfoRail.log
- eConsoleNetstat.log

Once you create a .zip file, you can send the file to Wavelink Customer Service. Customer Service uses the file to quickly diagnose the problem and provide a solution.

To use the Support Generator:

- 1 From the **Quick Start** tab, click **Support Generator**.

The *Avalanche Support Generator* dialog box appears.

- 2 From the drop-down list, select the area of Avalanche where the problem is occurring.
- 3 In the **Processor** text box, enter your processor type.
- 4 In the **Installed RAM** text box, enter the amount of RAM you have installed.

NOTE You cannot change the **Operating System** or **Free HDD Space** text boxes. These are populated automatically by the Support Generator.

- 5 In the text box provided, enter detailed information about the problem. The more detailed your description, the more thoroughly Customer Service will be able to understand the problem.
- 6 In the **Save as filename** text box, enter a name for this file.

NOTE This is the name of the .zip file that you will e-mail to Wavelink Customer Service. It is not path where the file will be saved.

- 7 Click **Save**.

The log files are compiled into a .zip file and a dialog box appears displaying the location where the file is saved.

- 8 Make a note of the location and click **OK**.
- 9 Attach the `.zip` file to an e-mail and send the e-mail to `customerservice@wavelink.com`.

Using the Enabler Installation Tool

The Enabler Installation Tool allows you to configure and deploy Enablers to mobile devices directly from the Avalanche Console using Microsoft ActiveSync.

To use the Enabler Installation Tool, you must have the following:

- Enabler installation packages on the machine where you are running the console.
- Mobile devices connected to the machine through ActiveSync.

To install an Enabler:

- 1 From the **Quick Start** tab, select the **Install Avalanche Enabler**.

The *Avalanche Device Enabler Installation* dialog box appears.

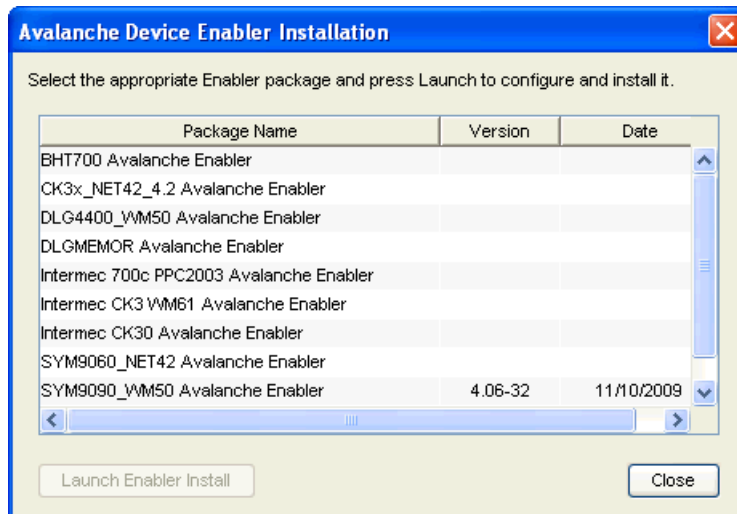


Figure 4-4. *Avalanche Device Enabler Installation*

- 2 From the dialog box, select which Enabler package you want to install on the mobile device and click **Launch Enabler Install**.

NOTE You must have at least one Enabler installation package on your machine or this dialog box will be blank.

The Enabler Configuration Tool appears.

- 3 Configure the Enabler as desired.
- 4 Once you configure the Enabler settings, use ActiveSync to send the Enabler to your connected mobile device.

For details about all the configuration options of the Enabler, refer to the *Avalanche Enabler User Guide*.

Chapter 5: Managing User Accounts

A user account is required to log in to the Avalanche Console. User accounts allow you to define who can access components and perform tasks. Users will not be able to access the Console without an account.

There are two types of accounts: Administrator and Normal. An Administrator account can access and modify all the configurations in Avalanche associated with its home region. A Normal account is assigned to specific regions or profiles and can only view or make changes in its assigned areas.

NOTE Avalanche is installed with a default user login of `amcadmin` and password of `admin`. Wavelink recommends you create a new password for this account once you log in.

When a Normal account is created, you can assign permissions to that account from the *User Management* dialog box. These permissions can apply to all profiles of a type (i.e., all alert profiles), or to specific tools (i.e., Infrastructure Site Tool). If you want to assign permissions on a profile-by-profile basis, you also have the option to make the account an authorized user for individual profiles.

As an alternative to assigning permissions to each Normal account, you can assign permissions to a user group. Each Normal account that is part of the user group will have the permissions assigned to the group. Each Normal account will have those permissions only as long as it belongs to the user group. A Normal account can belong to more than one user group at a time.

This chapter provides the following information about user accounts:

- Creating User Accounts
- Creating User Groups
- Assigning User Permissions
- Assigning Authorized Users to Profiles
- Configuring Integrated Logon
- Changing Passwords
- Removing User Accounts

NOTE For assigning authorized users to a specific mobile device group, see *Adding Mobile Device Group Authorized Users* on page 146.

Creating User Accounts

Administrator accounts allow you to create new user accounts. When creating a new account, you assign a user name and password to the account allowing the user to log on to the Avalanche Console. You also assign permission levels to grant the user access to specific functionality.

When a user account is created, it must be assigned a “home.” The user (either Normal or Administrator) will only be allowed to access information for their home region and any associated sites or locations.

NOTE A user assigned to a region who has read/write permissions for profiles can exclude an inherited profile, but will not be able to modify it.

You can configure the following parameters when creating a user account:

- **Login.** This is the name the user will use to log in to the Avalanche Console. The login is case sensitive. The following special characters are not allowed:
~ ` ! ^ * () + = | ? / < > , [] : ; { } \ " & space
- **Password.** This is the password that will grant access to the Avalanche Console. Passwords are case sensitive. The password has a 32 character limit.
- **Confirm Password.** You must confirm the password you assign to the user.
- **First Name.** This is the first name of the user.
- **Last Name.** This is the last name of the user.
- **Type.** Select if the user is a Normal user or an Administrator. If the user is a Normal user, you will need to assign Regional or Profile permissions. If the user is an Administrator, the user will have access to the entire enterprise.

- **User Home.** This is the portion of your network that the user will be assigned to. The user will only be able to access profiles and information pertinent to his assigned region.
- **Description.** You can enter a description of the user or group.

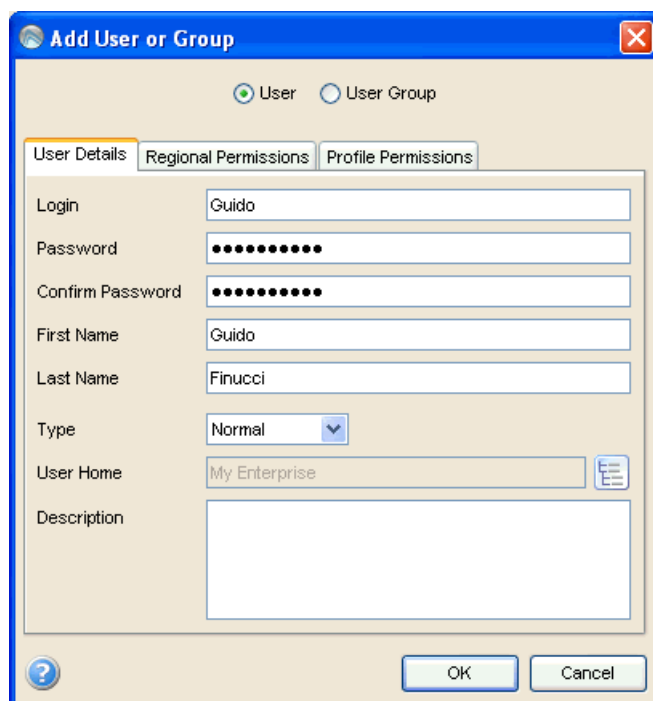
To create a new account:

- 1 Click **Tools > User Management**.

The *User Management* dialog box appears.

- 2 Click **Add**.

The *Add User or Group* dialog box appears.



The screenshot shows a dialog box titled "Add User or Group" with a blue header and a close button (X) in the top right corner. Below the title bar, there are two radio buttons: "User" (selected) and "User Group". The main area of the dialog is divided into three tabs: "User Details", "Regional Permissions", and "Profile Permissions". The "User Details" tab is active and contains the following fields:

- Login: Guido
- Password: Masked with 10 dots
- Confirm Password: Masked with 10 dots
- First Name: Guido
- Last Name: Finucci
- Type: Normal (dropdown menu)
- User Home: My Enterprise (with a list icon to the right)
- Description: Empty text area

At the bottom of the dialog, there is a help icon (question mark) on the left and "OK" and "Cancel" buttons on the right.

Figure 5-1. Add User

- 3 Enter the information in the available text boxes. **Login**, **Password**, **Confirm Password**, and **Type** are required fields.

NOTE The login and password are case sensitive.

- 4 The **User Home** will be assigned as My Enterprise.
- 5 You can assign regional and profile permissions by clicking on the tabs now, or an Administrator can modify permissions later.
- 6 When you are finished, click **OK**.

The new user is added to the list in the *User Management* dialog box.

The new account is now available and the user can log on to the Avalanche Console. However, if the user is set as a Normal user, that user will not have access to any areas of the Console until you assign permissions and permission levels to that user. For more information, refer to *Assigning User Permissions* on page 51.

Creating User Groups

In addition to individual user accounts, you can create user groups. Users assigned to a user group will have permissions for all areas associated with that user group in addition to the permissions granted for their individual accounts. For convenience, there are default user groups created, including:

- Software Admin
- Help Desk
- Network Admin

These user groups are set with a series of default permissions. You can modify the groups to suit your needs.

To create a user group:

- 1 Click **Tools > User Management**.

The *User Management* dialog box appears.

- 2 Click **Add**.

The *Add User or Group* dialog box appears.

- 3 Select the **User Group** option.
- 4 In the **Group Name** text box, enter the name of the group.
- 5 In the **Users** list, check all users that you want to add to the group.

NOTE If you have not added any Normal users, the list box will be empty. Refer to *Creating User Accounts* on page 48 for information about creating users.

- 6 From the **Type** drop-down list, select if the user group is Normal or Administrator.
- 7 You can assign regional and profile permissions by clicking on the tabs now, or an Administrator can modify permissions later.
- 8 When you are finished, click **OK**.

Your user group is created. For information about assigning permissions, refer to *Assigning User Permissions* on page 51.

Assigning User Permissions

If you have an Administrator account, you have unlimited permissions, and can assign and change permissions for Normal user accounts. When a Normal user account is assigned Read/Write permissions to a functionality, that user has administrative rights to that specific functionality in his home region and any associated sites or locations. For a Normal user account, there are two types of permissions:

- Regional Permissions
- Profile Permissions

Regional Permissions

Regional permissions are specific to various tasks and components of Avalanche. For each component you can grant read or read/write access. Read-only allows the user to view the configurations and settings for the component. Read/write allows the user to configure parameters and settings for the specified component.

Regional permissions are specific to the user's home region. This includes any associated sub-regions or locations. The following table describes the regional permissions:

Regional Permission	Read_Write	Read_Only
Alert Profiles	Allows you to apply and remove alert profiles.	Allows you to view assigned alert profiles.
Enterprise Management	Allows you to view, manage, and configure all locations to which you are assigned in the My Enterprise tree.	Allows you to view all location configurations and settings.
Mobile Devices	Allows you to manage the Mobile Device Inventory tab and gives you rights to all the mobile device functions in the Mobile Device Details such as ping and text.	Allows you to view the Mobile Device Inventory and mobile device properties.
Mobile Device Profiles	Allows you to apply and remove mobile device profiles.	Allows you to view assigned mobile device profiles.
Mobile Device Properties	Grants you access to the Mobile Device Details dialog box allowing you to create, edit, or delete properties on the mobile device.	Allows you to view the Mobile Device Details.
Network Profiles	Allows you to apply and remove network profiles.	Allows you to view assigned network profiles.
Remote Control	Allows you to use Remote Control. When you enable Read_Write functionality for Remote Control, Read_Only for Mobile Devices and Mobile Device Properties is automatically enabled. This grants you full access to use Remote Control. Also allows you to configure Remote Control connection profiles for particular devices.	Allows you to connect to Remote Control and view mobile devices. You cannot configure Remote Control connection profiles.
Scan to Config	Allows you to apply and remove Scan to Config profiles.	Allows you to view assigned Scan to Config profiles.
Scan to Config Printing	Allows you to print Scan to Config profiles.	Allows you to print Scan to Config profiles.

Regional Permission	Read_Write	Read_Only
Server Profiles: Mobile Devices	Allows you to apply and remove Mobile Device Server profiles.	Allows you to view assigned Mobile Device Server profiles.
Software Profiles	Allows you to apply and remove software profiles.	Allows you to view assigned software profiles.

To assign regional permissions:

- 1 Click **Tools > User Management**.

The *User Management* dialog box appears.

- 2 Select the user account to which you are assigning permissions.

- 3 Click **Edit**.

The *Edit User* dialog box appears.

- 4 Click the **Regional Permissions** tab.

- 5 Enable the checkbox next to each permission you want to grant the user. The user will not be able to access any functions that you leave unchecked. They will not be able to see the data or modify any conditions.

- 6 For each function that you enable, select **READ_WRITE** or **READ_ONLY**. The default is set to **READ_WRITE**, which allows the user to view and modify any settings in the area where they have permission. **READ_ONLY** allows the user to view settings, but the user can not modify them.

- 7 When you are finished, click **OK**.

Profile Permissions

Profile permissions allow the user complete global access to the specified profile. For each profile you can grant read or read/write access. Read/write allows the user to manage configuration of the profile. Read-only allows the user to view the profile, but does not allow any editing.

However, this does not give you permission to apply the profiles to any regions. You must be assigned regional permissions to apply any profiles. This table describes each of the Profile Permissions:

Profile Permission	READ_WRITE	READ_ONLY
Alert Profiles	Allows you to create and edit all alert profiles.	Allows you to view existing alert profiles.
Mobile Device Groups	Allows you to create, edit and delete mobile device groups.	Allows you to view mobile device groups and the settings associated with the groups.
Mobile Device Profiles	Allows you to create and edit mobile device profiles.	Allows you to view existing mobile device profiles.
Network Profiles	Allows you to create and edit network profiles.	Allows you to view existing network profiles.
Server Profiles: Mobile Devices	Allows you to create and edit mobile device server profiles.	Allows you to view existing mobile device profiles.
Scan to Config	Allows you to create, configure, and print Scan to Config profiles.	Allows you to view existing Scan to Config profiles.
Software Profiles	Allows you to create and edit software profiles.	Allows you to view existing software profiles and the associated settings.

To assign user permissions:

- 1 Click **Tools > User Management**.

The *User Management* dialog box appears.

- 2 Select the user account to which you are assigning permissions.

- 3 Click **Edit**.

The *Edit User* dialog box appears.

- 4 Click the **Profile Permissions** tab.

- 5 Enable the checkbox next to each function that you want this user to have permission to. The user will not be able to access any functions that you leave unchecked. They will not be able to see the data or modify any conditions.

- 6 For each function that you do enable, you have the option to select whether the permission type is READ_WRITE or READ_ONLY. The default is READ_WRITE,

which allows the user to view and modify any settings in the area where they have permission. `READ_ONLY` allows the user to view settings but not modify them.

- 7 When you are finished, click **OK**.

Assigning Authorized Users to Profiles

You can assign administrative privileges for a specific profile to a user that has Normal user rights and is not assigned permissions to profiles.

To add an authorized user you must have at least one user configured with Normal permissions. Users that have permission for the profile will not appear in the list of available users.

To add or remove an authorized user:

- 1 From the **Profiles** tab, click on the name of the profile you want to configure.
- 2 Click **Edit**.
- 3 Click **Authorized Users**.

The *Profile Authorized Users* dialog box appears.

- 4 Click **Add User**.

The *Add Authorized User* dialog box appears.

- 5 Add or remove authorized users as desired.
 - To add an authorized user, click **Add** in the Authorized Users region. Select the user and permission level from the drop-down lists and click **Save**.
 - To remove an authorized user, select the checkbox next to the user and click **Remove** at the top of the Authorized Users region.

The authorized users list is applied immediately.

Configuring Integrated Logon

Avalanche allows Console users to log in to the Avalanche Console using the same information they use to log in to the network.

Integrated logon is disabled by default; however, you can enable authentication through the CE Secure authentication service that is installed on the Enterprise Server or through Windows Active Directory LDAP authentication. When you select to use Windows Active Directory LDAP service, users are authenticated using standard Java LDAP APIs. You will need to specify the IP address of the LDAP server.

When you select either integrated login option, users with network logins can log on to the Avalanche Console as Normal users. These accounts will not have any permissions assigned to them until an administrator configures each account.

If you have configured user accounts in the *User Management* dialog box and then enable the integrated logon feature, those users configured in the Console will not be allowed to access the Console. The only users allowed to access the Console will be those that can log in to the network.

NOTE The default `amcadmin` account should be able to login with or without integrated logon enabled.

To enable integrated logon:

1 Click **Tools > User Management**.

The *User Management* dialog box appears.

2 Select from the following options:

- Enable the **Windows Active Directory Authentication through Wavelink CES Server** option.
- Enable the **Authentication through LDAP Server** option and then enter the address of the LDAP Server.

3 Click **OK**.

4 Log out of the Avalanche Console.

Avalanche is now configured to recognized authenticated system users.

Changing Passwords

If you have an Administrator account, you can change any user account password. Users with Normal accounts cannot change passwords for any account.

To change a password:

- 1 Click **Tools > User Management**.

The *User Management* dialog box appears.

- 2 From the list, select the user account for which you want to change the password.
- 3 Click **Change Password**.

The *Change User Password* dialog box appears.

- 4 Type the new password in the **New Password** text box and confirm it in the **Confirm New Password** text box.
- 5 Click **OK**.
- 6 Click **OK** again to return to the Avalanche Console.

The new password information is applied immediately.

NOTE You can also change passwords by editing the user account.

Removing User Accounts

If you have an Administrator user account, you can delete user accounts. Once you remove an account, that user will no longer have access to the Avalanche Console using that login information.

To delete a user account:

- 1 Click **Tools > User Management**.

The *User Management* dialog box appears.

- 2 Select a user from the list.
- 3 Click **Remove**.
- 4 Confirm you want to remove the user account.

The deleted account will no longer be able to access the Avalanche Console.

Chapter 6: Managing Sites and Locations

One of the primary tasks you accomplish with Avalanche SE is location management. Location management is performed in Avalanche SE using My Enterprise, My Location and sites.

You cannot create additional My Enterprise or My Location components. However, you can create sites based on how you want to group and manage your mobile devices.

- Managing Sites
- Managing the Mobile Device Server

Managing Sites

Sites are groups of mobile devices that share a Mobile Device Server. Sites are defined by unique selection criteria. Sites allow increased flexibility for assigning different profiles at the same server location.

This section contains the following tasks for managing sites:

- Creating a Site
- Assigning Profiles
- Viewing Mobile Devices within Sites
- Pinging Mobile Devices within Sites
- Sending Messages to Sites
- Editing Site Properties
- Additional Site Functions

Creating a Site

Creating sites allows flexibility in assigning profiles. A site must be created where there is a Mobile Device Server.

To create a site:

- 1 Right-click My Location and select **Create Site**.

The *New Site* dialog box appears.

- 2 Enter a name for the site.
- 3 Use the Selection Criteria Builder to configure unique selection criteria for the site group.
- 4 When you are finished, click **OK**.

A site appears under the server location. The mobile devices meeting the specified selection criteria will be assigned to the site.

Assigning Profiles

Profiles are automatically assigned and applied at the My Enterprise level. If you want to apply profiles manually, you can disable the auto-assign option and then apply your profiles to My Enterprise or specific sites. The profiles are applied to the mobile devices based on selection criteria for the profile and the order in which the profiles are listed in the Console.

To disable auto assign:

- 1 From the **Tools** menu, select **Preferences**.
- 2 From the *Preferences* dialog box that appears, select the **Server** tab.
- 3 In the Deployment Settings section, disable the **Auto Assign Profiles** option.
- 4 Click **OK** to save your changes and return to the Console.

You can now manually assign profiles.

To assign a profile:

- 1 Select the site you where you want to apply the profile and click the **Site Properties** tab.

NOTE If you are applying the profile to My Enterprise, select My Enterprise and click **Properties**.

- 2 Click **Edit**.
- 3 Select the applicable profile tab and click **Add**.

The *Add Profile Application* dialog box appears.

- 4 From the list of available profiles, select which profile you want to assign to this location.

NOTE To add more than one profile at a time, hold the `Shift` or `Ctrl` key as you select.

- 5 Configure the other options based on the type of profile you are assigning.
- 6 Click **OK**.

The profile is added.

- 7 Continue adding profiles, if desired.
- 8 Use the **Move Up** and **Move Down** buttons to assign the priority in which the profiles are applied to mobile devices.
- 9 Save your changes.

The profiles are assigned to the selected location.

Excluding Profiles

When you apply profiles to My Enterprise or My Location, the Avalanche Console applies the configurations to all sites within that region. That profile is considered an inherited profile. However, you can exclude an inherited profile from a site. The profile will still appear in the **Applied Profiles** tab, but will not be applied to any related devices.

To exclude an inherited profile:

- 1 From the Navigation Window, select the site at which you want to exclude an inherited profile.
- 2 Select the **Properties** tab.
- 3 On the **Applied Profiles** tab, click **Edit Exclusions**.
- 4 Enable the **Excluded** check box for the inherited profile you want to exclude.
- 5 Click **Save**.

The profile will be excluded for the site.

Viewing Mobile Devices within Sites

You can view the mobile devices that belong to an individual site from the **Mobile Device Inventory** tab.

To view the mobile devices:

- 1 From the Navigation Window, select the site you want to view.
- 2 Select the **Mobile Device Inventory** tab.

Only the mobile devices that belong to the site will appear in the list.

Pinging Mobile Devices within Sites

You can ping the mobile devices in a site simultaneously if the devices are in range and running the Avalanche Enabler.

NOTE 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 mobile devices

- 1 Right-click the site from the Navigation Window.
- 2 Select **Ping Mobile Devices** from the context menu.

The **Recent Activity** column in the Mobile Device Inventory reports the status of the ping for each device in the group.

Sending Messages to Sites

You can send the same message to all devices in a site simultaneously.

To send messages:

- 1 Right-click the site from the Navigation Window.
- 2 Select **Send Text Message** from the context menu.
- 3 Type a message in the **Text Message Field**.

- 4 Enable the **Provide Audible Notification** text box if you want a sound to play when the mobile device receives the message.
- 5 Click **OK**.

The **Recent Activity** column reports the status of the message for each device in the group.

Editing Site Properties

You can modify mobile device properties at the site level. When you edit device properties for a site, the Console retrieves the common properties from all the devices in the site. You can then add, edit, and delete properties for the site. All property changes made at this level will be applied on the mobile devices in the site. Properties can be used as selection variables in selection criteria to control which devices receive particular updates.

NOTE Refer to *Building Selection Criteria* on page 161 for related information.

To add or edit a property for mobile devices in a site:

- 1 Right-click a site and select **Edit Device Properties**.

The *Edit Group Mobile Device Properties* dialog box appears.

- 2 Click **Add Property** or **Edit Property**.

The *Add Device Property* dialog box appears.

- 3 From the **Category** drop-down list, select **General** or **Custom** based on the property you are creating.
- 4 Enter the **Property Name** and **Property Value** in the provided text boxes.
- 5 Click **OK**.

The new property is added to the properties list.

- 6 When you are finished editing properties, click **OK** to return to the Avalanche Console.

Additional Site Functions

Sites allow you to more efficiently manage your mobile devices. These options are available by right-clicking the site and selecting the appropriate option.

The additional options for sites are as follows:

Delete	Allows you to delete the site.
Mark Orphan Packages for Deletion	Marks orphaned packages on the devices within the site for deletion.
Unmark Orphan Packages for Deletion	Unmarks orphan packages for deletion.
Update Now	Allows you to update all mobile devices within that site immediately.

Managing the Mobile Device Server

You can manage the Mobile Device Server from the Avalanche Console with the following tasks.

- Modifying Server Location Properties
- Stopping the Server
- Starting Servers
- Viewing Server Properties
- Reinitializing the Mobile Device Server
- Retrieving Mobile Device Log Files

Modifying Server Location Properties

Once you have created a server location, you can modify the server location properties. The properties that appear in the **dServer Location Properties** tab were configured at the time you created the server location. You can also view the Server Location Statistics including Server versions and the number of licensed devices for each Server.

You can modify the following server location properties:

- Name
- Path
- Notes
- Site Address (You can enter either the IP address or a DNS name)
- City
- State or Region
- Country
- Time Zone

To modify server location properties:

- 1 From the Navigation Window, click the server location and then the **dServer Location Properties** tab.
- 2 Click **Edit**.
- 3 Edit the information as needed.

Save your changes.

Stopping the Server

You can start and stop the Mobile Device Server from the Avalanche Console.

To stop the server:

- From the Navigation Window, right-click the server and select **Stop Distributed Server**.

Starting Servers

You can restart the Server from the Navigation Window of the Console.

To restart a server:

- From the Navigation Window, right-click the Mobile Device Server and select **Start Distributed Server**.

Viewing Server Properties

You can view Server properties from the Navigation Window of the Avalanche Console. Server properties include the version of the server, the date the server was started and the status of the server (Running or Stopped) and licensing information.

To view Server properties:

- From the Navigation Window, right-click the Mobile Device Server and select **Mobile Device Server Properties**.

Reinitializing the Mobile Device Server

Reinitializing the Mobile Device Server allows you to restart the server without stopping and starting the service. The server will sync with the Enterprise Server and load any changes it detects, but the service keeps running so you will not lose contact with any devices that are updating.

To reinitialize the Mobile Device Server:

- From the Navigation Window, right-click the Mobile Device Server and select **Reinitialize Mobile Device Server**.

The server contacts the Enterprise Server and downloads any updates.

Retrieving Mobile Device Log Files

You can retrieve mobile device log files stored on the Mobile Device Server. When you retrieve the mobile device log files, a zip file is created and saved in a location you specify. The logging level and size of the log are configured in the Mobile Device Server profile.

To retrieve mobile device log files:

- 1 Right-click the Mobile Device Server in the Navigation Window and select **Retrieve log files** from the context menu.
- 2 In the dialog box that appears, select the location where you want to save the zip file and click **Save**.

The file is saved.

Chapter 7: Managing Network Profiles

A network profile is used to configure devices for your network. The profile contains information such as gateway addresses, subnet masks, WWAN settings, and encryption and authentication information. You can also use a network profile to assign IP addresses to your devices. Once the wireless devices are configured with the values from the network profile, you can manage the devices through the Avalanche Console.

You can schedule a specific time for a network profile change to take effect. By default, network settings take effect when the profile is enabled. However, you can configure the date and time for the settings to take effect.

This section contains the following topics:

- Creating Network Profiles
- Configuring Network Profiles
- Viewing Where Network Profiles are Applied
- Exporting Profiles for Configuring Enablers

Creating Network Profiles

A network profile allows you to control network settings for all devices meeting its selection criteria.

To create a network profile:

- 1 From the **Profiles** tab, click **Add Profile**.

The *Create Profile* dialog box appears.

- 2 Select **Network Profile** from the drop-down list and type the name of the profile in the **Profile Name** text box.
- 3 Click **OK**.

The network profile is created and can be enabled, configured, and assigned to a location.

Configuring Network Profiles

Once a Network Profile has been created, you can configure the network settings for distribution to your devices.

This section contains information about the following configuration tasks:

- Configuring Network Profile General Settings
- Configuring Selection Criteria
- Configuring Scheduled Settings

Configuring Network Profile General Settings

Once you have created a Network Profile, you can configure the status, authorized users, IP pools, and whether the profile overrides the settings on the mobile device.

This section contains information on the following tasks:

- Enabling Network Profiles
- Managing IP Address Pools
- Adding Authorized Users

Enabling Network Profiles

A network profile can have its status set to enabled or disabled. The profile must be enabled before you can apply it. You also have the option to force the settings in the network profile to override any settings already on the device.

To enable a network profile:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Network Profile** tab, select **Enabled**.
- 4 If you want the settings on the network profile to override any manual settings on the device, enable the **Override Settings on Mobile Devices** option.
- 5 Save your changes.

The network profile is now enabled.

Managing IP Address Pools

Network profiles allow you to assign IP addresses to your wireless devices from an IP address pool. You can create IP address pools for mobile devices.

To add addresses to an IP address pool:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Network Profile** tab, click **Manage IP Address Pools**.

The *IP Address Pools* dialog box appears.

- 4 In the **Start** text box, type the lowest number you wish to include in your pool.

For example:

192.168.1.1 (for static addresses)

0.0.0.1 (for addresses with a Server address mask)

- 5 In the **End** text box, type the highest number you wish to include in your pool.

For example:

192.168.1.50 (for static addresses)

0.0.0.50 (for addresses with a Server address mask)

- 6 If you desire the addresses in the range to be masked with the Server address, enable the **Mask With Server Address** checkbox and enter the mask.

For example:

0.0.0.255

- 7 Click **Add** to add the IP addresses to the IP address pool.

The available addresses and the mask will appear in the table to the right. This list will display all entered addresses, including those already assigned.

- 8 Click **OK** to return to the **Network Profiles** tab.
- 9 Save your changes.

Adding Authorized Users

You can add authorized users for all network profiles or enable a user for a specific network profile. For information on adding an authorized user, see *Managing User Accounts* on page 47.

Configuring Selection Criteria

Selection criteria allow you to specify which devices the network profile manages. Mobile device criteria define which mobile devices are managed by the profile. Dynamic selection criteria are defined by Avalanche and apply to a device's encryption and authentication support.

For detailed information about creating selection criteria, refer to *Using Selection Criteria* on page 160.

Configuring Scheduled Settings

From a network profile, you can configure WLAN IP settings, WLAN SSID, encryption and authentication settings, and WWAN settings. These configurations can be scheduled to start at a specific time, so they are considered scheduled settings.

When you configure WLAN IP, WLAN, and WWAN settings, you select the start time for those settings to take effect. Once the settings take effect, if there is more than one network profile enabled and applied at a location, the network profile with the highest priority will be the profile that is applied on your devices.

NOTE If you have an older Enabler, it will receive the new network settings the first time it connects with the server after the scheduled start time.

This section contains information on the following configuration options:

- Configuring WLAN IP Settings
- Configuring WLAN Settings
- Configuring WWAN Settings

Configuring WLAN IP Settings

From a network profile, you can configure WLAN IP settings for your devices. These settings will be deployed with the profile and applied on the device. The options include:

Manage IP Assignment This option allows you to manage the IP addresses assigned to your mobile devices. You can choose to use either a DHCP server or IP pool assignment.

Server Address This option provides mobile devices with the server address. You can provide the address, DNS name, or use the server location value. If you choose to use the server location value, the mobile devices use the mask/address of the server to which the device connects.

NOTE If using a DNS name, click **Validate** to ensure the address can be resolved.

If the mobile device profile has provided a server address, that address will override whatever is provided by the network profile.

Gateway Address This option provides mobile devices with the address for the node that handles traffic with devices outside the subnet. You can provide the address, DNS name, or use the server location value.

Subnet Mask This option provides mobile devices with the subnet mask. You can provide the address, DNS name, or use the server location value.

Domain Name System (DNS) This option provides the domain name to the devices.

Primary DNS Provides mobile devices with the IP address for a primary DNS.

Secondary	Provides mobile devices with the IP address for a secondary DNS (used if the primary DNS is unavailable).
Tertiary	Provides mobile devices with the IP address for a tertiary DNS (used if the primary and secondary DNS are unavailable).

To configure WLAN IP settings for a network profile:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Network Profile** tab, enable the **Manage WLAN IP** option.
- 4 In the Scheduled Settings region, select the date and time you want the settings to take effect from the drop-down list.
 - If you would like to add another start time for different settings to the list, click **Add** and select the date and time you want it to begin.
 - If you want to add another start time using the settings currently configured, click **Clone**.
 - If you want to change the currently selected start time, click **Edit**.
- 5 Select the **WLAN IP Settings** tab.
- 6 Configure the WLAN IP settings as desired.
- 7 Save your changes.

Configuring WLAN Settings

From a network profile, you can configure WLAN settings for your devices. These settings will be deployed with the profile and applied on the device. The options include:

SSID	This option provides wireless devices with the SSID. The SSID is a service set identifier that only allows communication between devices sharing the same SSID.
Encryption	This option allows you to enable encryption between your devices and the server. You have the following options for encryption:

Use Profile/None. Devices do not encrypt information.

WEP. Wired Equivalent Privacy is an encryption protocol using either a 40- or 128-bit key which is distributed to your devices. When WEP is enabled, a device can only communicate with other devices that share the same WEP key.

NOTE Avalanche only tracks the WEP keys that were assigned to devices through the Avalanche Console. Consequently, WEP keys displayed in the console might not match the keys for a wireless device if you modified them from outside of Avalanche.

WEP Key Rotation. WEP key rotation employs four keys which are automatically rotated at specified intervals. Each time the keys are rotated, one key is replaced by a new, randomly generated key. The keys are also staggered, meaning that the key sent by an infrastructure device is different than the one sent by a mobile device. Because both infrastructure and mobile devices know which keys are authorized, they can communicate securely without using a shared key.

NOTE WEP key rotation settings are not recoverable. If the system hosting the Server becomes unavailable (for example, due to a hardware crash), you must re-connect serially to each mobile device to ensure that WEP key settings are correctly synchronized.

WPA (TKIP). WPA, or Wi-Fi Protected Access, uses Temporal Key Integrity Protocol (TKIP) to encrypt information and change the encryption keys as the system is used. WPA uses a larger key and a message integrity check to make the encryption more secure than WEP. In addition, WPA is designed to shut down the network for 60 seconds when an attempt to break the encryption is detected. WPA availability is dependent on some hardware types.

WPA2 (AES). WPA2 is similar to WPA but meets even higher standards for encryption security. In WPA2, encryption, key management, and message integrity are handled by CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) instead of TKIP. WPA2 availability is dependent on some hardware types.

WPA2 Mixed Mode. WPA Mixed Mode allows you to use either AES or TKIP encryption, depending on what the device supports.

Custom Properties

This option allows you to add custom properties to the devices that receive this network profile. By clicking **Edit/View**, you can add, edit, and delete properties and their values.

Authentication Settings

The authentication type available depends on the encryption you are using and what is supported by your Enabler and hardware. Authentication options include:

EAP. Extensible Authentication Protocol. Avalanche supports five different EAP methods:

- **PEAP/MS-CHAPv2.** (Protected Extensible Authentication Protocol combined with Microsoft Challenge Handshake Authentication Protocol) PEAP/MS-CHAPv2 is available when you are using encryption. It uses a public key certificate to establish a Transport Layer Security tunnel between the client and the authentication server.
- **PEAP/GTC.** (Protected Extensible Authentication Protocol with Generic Token Card) PEAP/GTC is available when you are using encryption. It is similar to PEAP/MS-CHAPv2, but uses an inner authentication protocol instead of MS-CHAP.
- **EAP_FAST/MS-CHAPv2.** (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling combined with MS-CHAPv2) EAP-FAST uses protected access credentials and optional certificates to establish a Transport Layer Security tunnel.

- **EAP_FAST/GTC.** (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling with Generic Token Card) EAP-FAST uses protected access credentials and optional certificates to establish a Transport Layer Security tunnel.
- **TTLS/MS-CHAPv2.** (Tunneled Transport Layer Security with MS-CHAPv2) TTLS uses public key infrastructure certificates (only on the server) to establish a Transport Layer Security tunnel.

Pre-Shared Key (PSK). PSK does not require an authentication server. A preset authentication key (either a 8-63 character pass phrase or a 64 character hex key) is shared to the devices on your network and allows them to communicate with each other.

LEAP. (Lightweight Extensible Authentication Protocol) LEAP requires both client and server to authenticate and then creates a dynamic WEP key.

To configure WLAN settings:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Network Profile** tab, enable the **Manage WLAN** option.
- 4 In the Scheduled Settings region, select the date and time you want the settings to take effect from the drop-down list.
 - If you would like to add another start time for different settings to the list, click **Add** and select the date and time you want it to begin.
 - If you want to add another start time using the settings currently configured, click **Clone**.
 - If you want to change the currently selected start time, click **Edit**.
- 5 Select the **WLAN Settings** tab.
- 6 Configure the WLAN settings as desired.

- If you are using WEP keys, you must select either **40 Bit** or **128 Bit** key size, and create the keys. The keys you enter must be in hex format. A 40-bit key should have 10 characters and a 128-bit key should have 26 characters. To change the value for one of the hex digits in a key, type a new value (between 0-9 and A-F) in the appropriate text box. An example of a 40-bit key would be: 5D43AB290F.
- If you are using WEP key rotation, you must choose the encryption algorithm, starting date and time, rotation interval, and a pass code. After you enable WEP key rotation, click the **Settings** button to configure these options.
- If you are using PEAP, TTLS, or LEAP authentication, you can enable **Validate Server Certificate** and provide a path to the server certificate. This option will provision mobile devices with the server certificate.
- If you are using EAP_FAST, you can provide a path to a PAC (Protected Access Credential). This option will provision mobile devices with the PAC.
- If you are using an EAP method or LEAP, you can configure whether the **User Credentials** are **Prompt** (user is prompted when credentials are required) or **Fixed** (credentials are automatically sent when required).

NOTE The availability of authentication settings is dependent on what encryption method you have selected.

7 Save your changes.

Configuring WWAN Settings

From a network profile, you can configure WWAN settings for your devices with WWAN capabilities. These settings will be deployed with the profile and applied on the device. The options include:

Connection Name	A name for the connection.
Connection Type	There are two connection types available for your WWAN-enabled devices: APN (GPRS / EDGE / 3G). Provide an Access Point Name if you are using a 3G connection. An example of an APN would be: wap.cingular Dial-Up. The number to be dialed by the modem. This does not correspond to the number of the device.
Credentials	Sets the method for sending EAP credentials. Prompt. When the credentials are needed, the user is prompted with a dialog box to enter the information. Fixed. When the credentials are needed, the information is automatically sent without prompting the user.
Custom Properties	This option allows you to add custom properties to the devices that receive this network profile. By clicking Edit/View , you can add, edit, and delete properties and their values.
Enable TCP/IP header compression	Improves the performance of low-speed connections.
Enable software compression	Improves the performance of low-speed connections.
Activate phone as needed	Allows the Enabler to activate the device's phone if a WWAN connection is necessary.

Dial broadband connection as needed	Allows the Enabler to attempt a WWAN connection if a LAN connection cannot be established.
Public IP address for Avalanche Server	Provides the IP address of the enterprise server that is accessible from a WWAN. This is necessary if the device tries to contact the server when connected through a WWAN network outside of the server's local network.

To configure WWAN settings:

- 1 From the **Profiles** tab, select the network profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Network Profile** tab, enable the **Manage WWAN** option.
- 4 In the Scheduled Settings region, select the date and time you want the settings to take effect from the drop-down list.
 - If you would like to add another start time for different settings to the list, click **Add** and select the date and time you want it to begin.
 - If you want to add another start time using the settings currently configured, click **Clone**.
 - If you want to change the currently selected start time, click **Edit**.
- 5 Select the **WWAN Settings** tab.
- 6 Configure the WWAN settings as desired.
- 7 Save your changes.

Viewing Where Network Profiles are Applied

The **Applied Locations** tab in the network profile page allows you to see exactly which regions, Server Locations and sites to which a selected profile is directly applied. You cannot change of the information in this tab. If you need to apply a profile to a different location than what you see in the **Applied Locations** tab, refer to *Assigning Profiles* on page 59.

The **Applied Locations** tab displays the following information:

- **Parent Path.** The direct path back to the My Enterprise region.

- **Group.** The name of the Server Location or Site where the profile is applied.
- **Selection Criteria.** Any selection criteria that is applicable where the profile is applied.

To view:

- 1 From the **Profiles** tab, select the network profile you want to view.
- 2 Click the **Applied Locations** tab.

Exporting Profiles for Configuring Enablers

You can export profiles from Avalanche to use when you are installing Enablers on mobile devices. Avalanche allows you to export a network profile, a mobile device profile, or both. After you have configured the profile, export it and save it to the computer from which you are installing the Enabler(s). Using an exported profile to configure the Enabler allows you to quickly and easily connect the device to the Mobile Device Server.

To export profiles for Enabler configuration:

- 1 From the Console, click **File > Export > Profiles for Mobile Device Configuration**.
The *Export Profiles For Mobile Devices* dialog box appears.
- 2 From the lists, select the network profile and/or mobile device profile you want to export.
- 3 In the **Encryption Password** text box at the top of the dialog box, type a password that will be required in order to import the profile(s).
- 4 Click **OK**.
- 5 The *Save Export File* dialog box appears. Select the location where you want to save the file and click **Save**.
- 6 If you are using a different computer to install Enablers, move the export file to the computer you are using for Enabler installation.
- 7 Follow the instructions in the *Enabler User Guide* to import the profile settings and apply them to the Enabler.

Chapter 8: Managing Scan to Configure Profiles

Avalanche allows you to create Scan to Config profiles (barcode profiles) that are configured with network settings. You can then print the profiles as barcodes and a mobile device with an Enabler 3.5 (or later versions) can scan these barcodes. The information from the scanned barcodes is used to configure the network settings on the device.

NOTE To verify that the scan to configure functionality is available on your Enabler, check the **File** menu of the Enabler. If the **Scan Config** option appears in the **File** menu, the scan to config feature is available. If this option is not there, your Enabler does not support the scan to configure feature.

Contact Wavelink Customer Service for information about obtaining an Enabler that supports the scan to configure functionality.

This section contains instructions for the following tasks:

- Configuring Scan to Config Profiles
- Applying Scan to Config Profiles
- Printing Barcodes
- Scanning Barcodes

Configuring Scan to Config Profiles

When you create a Scan to Config profile, you can perform the following tasks:

- Adding Scan to Config Profiles
- Configuring Settings
- Adding Scan to Config Profile Authorized Users
- Editing Custom Properties
- Editing Registry Keys

Adding Scan to Config Profiles

A Scan to Config profile is used to configure network settings, device properties, and registry keys on a mobile device with an Enabler. Once you have configured the profile from the Avalanche Console, you can print the barcodes and then use a device to scan the barcodes.

To create a Scan to Config profile:

- 1 From the **Profiles** tab, click **Add Profile**.

The *Create Profile* dialog box appears.

- 2 Select **Scan To Config Profile** from the drop-down list and type the name of the profile in the **Profile Name** text box.
- 3 Click **OK**.

The profile is created and can be enabled and configured.

Configuring Settings

When you create a Scan to Config profile, you can configure the maximum barcode length and network settings such as the IP address, subnet mask, and gateway. You also have the option of using the network settings contained in a network profile.

You can also configure a passcode for the profile. The passcode is used to encrypt the barcode data. The mobile device user must enter the same passcode when they are using scan to configure so that the Enabler can decrypt the barcode data when it is scanned. If the user does not input the correct passcode at the device, then the barcode data is not decrypted and the scan registers as invalid.

When a mobile device scans the barcodes created from a Scan to Config profile, the mobile device receives the network settings configured within that barcode.

NOTE WEP key rotation is not supported.

To configure the settings:

- 1 From the **Profiles** tab, select the Scan to Config profile you want to configure.

Click **Edit**.

- 2 To encrypt the barcodes, type a passcode in the **Encryption Passcode** text box and confirm it in the **Confirm Passcode** text box.
- 3 Set the maximum length of the barcode.
- 4 If you have already configured a network profile and want to use the settings from that profile, enable **Use settings from network profile**. Choose which epoch (or set of scheduled settings) to use by enabling either **Use currently active Epoch** or **Use selected Epoch** and selecting an epoch from the drop-down list.
- 5 If you want to set a static IP address for the device, enable **Assign static IP address** and type the **IP Address**, **Subnet Mask** and **Gateway** in the appropriate boxes.

NOTE You cannot set a static IP address and use a network profile concurrently.

- 6 Click **Save** to save your changes.

The profile is updated with the configured network settings.

Adding Scan to Config Profile Authorized Users

You can add authorized users for all scan to config profiles or enable a user for a specific scan to config profile. For information on adding an authorized user, see *Managing User Accounts* on page 47.

Editing Custom Properties

Custom properties allow you to define specific properties that you want applied to the mobile device. An example of a custom property would be `location = Chicago`. Once a custom property has been applied to a device, you can use it as a selection criterion. You can apply custom properties to mobile devices through a Scan to Config profile.

You also have the option to edit or remove custom properties currently existing on the device through a Scan to Config profile. You must know the name of the property in order to edit or remove it.

This section contains information on the following tasks:

- Adding a Custom Property
- Editing or Removing a Custom Property

Adding a Custom Property

You can add a custom property to a mobile device through a Scan to Config profile. Add the property to the profile, print the profile as a set of barcodes, and scan the barcodes with the device.

To add a custom property:

- 1 From the **Profiles** tab, select the Scan to Config profile you want to configure.
- 2 Click **Edit**.
- 3 In the Device Properties region, click **Add**.

The *Edit Property* dialog box appears.

- 4 Type the **Name** and **Value** in the text boxes.
- 5 Select whether the property should be a device property or a network property.
- 6 Click **OK**.

The task is added to the list in the Device Properties region. The property will be added when the barcodes are scanned by the mobile device.

- 7 Click **Save** to save your changes.

Editing or Removing a Custom Property

You can edit or remove an existing custom property on a mobile device through a Scan to Config profile. Make changes to the property from the profile, print the profile as a set of barcodes, and scan the barcodes with the device. You must know the name of the property in order to edit or remove it.

To edit or remove a custom property:

- 1 From the **Profiles** tab, select the Scan to Config profile you want to configure.
- 2 Click **Edit**.
- 3 In the Device Properties region, click **Add**.

The *Add Property* dialog box appears.

- 4 Select the **Category** to which the property belongs.
- 5 Type the **Name** of the existing property in the text box.

- 6 If you want to edit the value of the property, type the new value in the **Value** text box.
- 7 If you are editing the value of the property, select **Add** from the **Action** drop-down list. If you want to remove the property from the device, select **Remove** from the **Action** drop-down list.
- 8 Click **OK**.

The task is added to the list in the Device Properties region. The property will be edited when the barcodes are scanned by the mobile device.

- 9 Click **Save** to save your changes.

Editing Registry Keys

You can add registry keys to a Scan to Config profile. Once you add a registry key to the profile, you can add values for the key. You also have the option to edit or remove existing registry keys or values on the device. You must know the name and location of the key or value in order to edit or remove it.

This section contains information on the following tasks:

- Adding a Registry Key
- Adding a Value to a Registry Key
- Removing a Registry Key
- Editing or Removing a Registry Key Value

Adding a Registry Key

You can add registry keys to a Scan to Config profile. These keys will be added to the device when the barcodes are scanned.

To add a registry key:

- 1 From the **Profiles** tab, select the Scan to Config profile you want to configure.
- 2 Click **Edit**.
- 3 In the Registry Settings region, select where you want to add the key and click **Add a new registry key**.

The *Add Registry Key* dialog box appears.

- 4 Select the **Parent Key** from the drop-down list.
- 5 Type the **Name** of the new key in the text box.
- 6 Select **Add** from the **Action** drop-down list.
- 7 Click **OK**.

The key is added to the profile and you can configure its value.

Adding a Value to a Registry Key

After you have created a registry key for a Scan to Config profile, you can add values to the key.

To add a value to an existing registry key:

- 1 From the **Profiles** tab, select the Scan to Config profile you want to configure.
- 2 Click **Edit**.
- 3 In the Registry Settings region, select the key to which you want to add a value and click **Add a new registry value**.

The *Add Registry Value* dialog box appears.

- 4 Type the **Name** of the new value in the text box.
- 5 Select the **Type** from the drop-down list.
- 6 Type the **Data** in the text box.
- 7 Select **Add** from the **Action** drop-down list.
- 8 Click **OK**.

The task is added to the list in the Registry Settings region. The value will be added when the barcodes are scanned by the mobile device.

- 9 Click **Save** to save your changes.

Removing a Registry Key

You can remove an existing registry key on a mobile device through a Scan to Config profile. Make changes to the key from the profile, print the profile as a set of barcodes, and scan the barcodes with the device. You must know the name of the key/value in order to remove it.

To remove a registry key:

- 1 From the **Profiles** tab, select the Scan to Config profile you want to configure.
- 2 Click **Edit**.
- 3 In the Registry Settings region, select the parent key of the key you want to delete and click **Add a new registry key**.

The *Add Registry Key* dialog box appears.

- 4 Ensure the **Parent Key** in the drop-down list is correct.
- 5 Type the **Name** of the key in the text box.
- 6 Select **Remove** from the **Action** drop-down list.
- 7 Click **OK**.

The task is added to the list in the Registry Settings region. The key will be removed when the barcodes are scanned by the mobile device.

- 8 Click **Save** to save your changes.

Editing or Removing a Registry Key Value

You can edit or remove an existing registry key value on a mobile device through a Scan to Config profile. Make changes to the key from the profile, print the profile as a set of barcodes, and scan the barcodes with the device. You must know the name of the key and value in order to edit or remove it.

NOTE In order to edit or remove a registry key value, you must add the registry key to the Scan to Config profile even if the key already exists on the device. For more information on adding a registry key, see *Adding a Registry Key* on page 83.

To edit or remove a registry key value:

- 1 From the **Profiles** tab, select the Scan to Config profile you want to configure.
- 2 Click **Edit**.
- 3 In the Registry Settings region, select the key for which you want to edit or remove a value and click **Add a new registry value**.

The *Add Registry Value* dialog box appears.

- 4 Type the **Name** of the existing value in the text box.
- 5 If you want to edit the **Type** or **Data** of the value, enter the appropriate information in the provided boxes.
- 6 If you are editing the value, select **Add** from the **Action** drop-down list. If you want to remove the value from the device, select **Remove** from the **Action** drop-down list.
- 7 Click **OK**.

The task is added to the list in the Registry Settings region. The value will be changed when the barcodes are scanned by the mobile device.

- 8 Click **Save** to save your changes.

Applying Scan to Config Profiles

Once you have configured your Scan to Config profile, you can apply that profile. When you apply a profile to a location or site, the users who have permissions for that location can make changes as necessary. For more information about assigning Scan to Config profiles, refer to *Assigning Profiles* on page 59.

Printing Barcodes

Once you have created and configured a Scan to Config profile, you can print that profile. The profile prints as a set of barcodes in random order. You can then scan the barcodes with a mobile device to change the network settings on that device. You have the option to print the barcodes on a printer or to a `.pdf` file.

To print a barcode:

- 1 From the **Profiles** tab, select the Scan to Config profile you want to print.
- 2 From the **Scan-to-Config Profile** tab, click **Print**.

The *Scan-to-Config Output* dialog box appears.

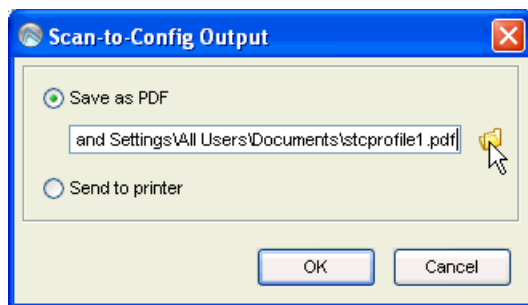


Figure 8-1. Scan-to-Config Output dialog box

- 3 If you want to print the barcodes to a .pdf file, select **Save as PDF**, type the name and location for the file in the text box and click **OK**.

NOTE You can also use the file icon to browse to the location where you want to store the file.

- Or -

If you want to print the barcodes on a printer, select **Send to printer** and click **OK**.

- 4 If you selected **Save as PDF**, the barcodes are saved in the specified location. If you selected **Send to printer**, the *Print* dialog box appears. Configure the printing options as desired and click **OK** to print the barcodes.

Scanning Barcodes

To scan and apply a Scan to Config profile, you must open the *Scan Configuration* dialog box from the Enabler on the mobile device. Use the mobile device to scan the barcodes in any order. This sends the configurations to the Enabler and updates the network profile.

You must have an Enabler 3.5 or later version to use the scan to configure functionality. Contact Wavelink Customer Service for information about obtaining an Enabler 3.5.

Network settings do not get processed on the mobile device until all of the barcodes are scanned. The barcodes contain data that tell the device how many barcodes are in the set and the sequence number of each one. This allows you to scan the barcodes out of sequence and the mobile device will reconstruct it properly.

To scan the configuration:

- 1 From the Enabler on the mobile device select **File > Scan Config**.

The *Scan Configuration* dialog box appears.

- 2 Enter the passcode (if configured) and begin scanning.

As you scan the barcodes you will be able to view the status, the number of remaining barcodes, and the number of scanned barcodes.

Once you have scanned all available barcodes, the settings are applied and the *Scan Configuration* dialog box closes.

Chapter 9: Managing the Mobile Device Server

The Mobile Device Server is distributed server software that lets you remotely manage and configure mobile devices. Through a Mobile Device Server profile, Avalanche allows you to manage the following settings for your Mobile Device Server and mobile devices:

- **Administrative Settings.** These settings include server resources, licensing, user files, data collection and terminal ID generation.
- **Connection Settings.** You can configure when the Server and devices are allowed connections and how connections should be established.
- **Security Settings.** Avalanche supports encryption and authentication methods to help keep your information secure and prevent unauthorized mobile devices from accessing your network.

This section provides information about managing the Mobile Device Server through a Mobile Device Server profile. It contains the following tasks:

- Configuring Mobile Device Server Profile Settings
- Configuring Mobile Device Server Blackouts and Updates
- Viewing Mobile Device Server Licensing Messages
- Viewing Where Mobile Device Server Profiles Are Applied
- Reinitializing the Mobile Device Server

Configuring Mobile Device Server Profile Settings

Configure the following settings from the **Mobile Device Server Profile** tab:

- Mobile Device Server Security
- Mobile Device Server Resources
- Mobile Device Server License Options
- Mobile Device Server Profile Authorized Users
- Mobile Device Settings on the Server Profile

- Secondary Mobile Device Servers

Mobile Device Server Security

Avalanche supports encryption and authentication methods to prevent unauthorized mobile devices from accessing your network.

Avalanche offers two options for encryption:

- **Transport Encryption.** When you enable transport encryption, Avalanche will match the level of encryption with the capacity of the mobile device. TCP/IP communication between the Mobile Device Server and mobile devices will be encrypted to the degree possible.
- **Strict Transport Encryption.** When you enable strict transport encryption, Avalanche will use AES encryption for information. Only devices that support AES encryption (Enabler 5.1 or newer) will be able to connect to the server when strict transport encryption is enabled.

Avalanche offers two options for authentication:

- **Mobile Device Authentication.** This option requires mobile devices to connect to the network through a wired connection (such as a cradle) and receive an authentication key. When you enable this option, the Mobile Device Server will challenge any device attempting to connect to the Server for a password. If the mobile device does not have the correct password, the Mobile Device Server will not allow a TCP/IP connection.

NOTE If the network setup involves mobile devices roaming from one server to another, it is strongly recommended that you do **NOT** activate mobile device authentication.

- **Server Authentication.** This option forces mobile devices to communicate with a single known Server. Mobile devices must first connect to the network through a wired connection to receive information about the Server with which they are allowed to communicate. When you enable this option, the mobile device will challenge any Mobile Device Server attempting contact for a password. If the Mobile Device Server does not have the correct password, the mobile device will not allow a TCP/IP connection.

Server Authentication is supported by DOS devices, but has limited CE device support. For more information about supported devices, contact Wavelink Customer Service.

NOTE Both authentication options require mobile devices to connect to the network through a wired connection to receive authentication information before they will be allowed to connect wirelessly.

To configure Mobile Device Server security:

- 1 From the **Profiles** tab, select the Mobile Device Server profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Mobile Device Server Profile** tab, enable the desired options in the Server Security region.
 - If you want to use encryption, select the type of encryption you want to use from the **Mobile Device Transport Encryption** drop-down menu.
 - If you enable **Enable Mobile Device Authentication**, the *Change Device Auth Password* dialog box appears. Enter a password and confirm it in the provided text boxes, then click **OK**.
 - If you enable **Enable Server Authentication**, the *Change Server Auth Password* dialog box appears. Enter a password and confirm it in the provided text boxes, then click **OK**.

NOTE If a password for authentication has already been set, the *Change Auth Password* dialog box will not appear automatically. You can access it by clicking **Set Password** next to the desired authentication option.

- 4 Save your changes.

Mobile Device Server Resources

A Mobile Device Server profile allows you to configure the following aspects of server resources:

- **Logging.** The current Avalanche log file is saved as `Avalanche.log` to the `<Avalanche Installation Directory>\Service` directory. Once the current log file reaches the maximum size, it is saved as `Avalanche.log.<num>` (where `<num>` is a number between 000 and 999), and a new `Avalanche.log` file is created.

- **Serial Ports.** You can configure Mobile Device Servers to automatically listen for mobile devices using the serial ports on a remote system. Only one application on a host system can maintain ownership of a serial port. If the Mobile Device Server controls the serial 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 serial ports, then the Mobile Device Server will not be able to use them.

NOTE Serial connections are required to implement Mobile Device and Server Authentication.

- **Terminal ID range.** The Mobile Device Server assigns each device a terminal ID the first time that the device communicates with Mobile Device Server. The number the Mobile Device Servers selects is the lowest number available in a range of numbers you can configure.

To configure the terminal ID range, use a C-style format to create a generation template. For example, `Seattle-%d` would generate IDs such as `Seattle-4`, and `Seattle-%05d` would generate IDs such as `Seattle-00004`.

The following table lists the logging options available on a Mobile Device Server:

Logging Level	The log file records actions that have occurred on the Mobile Device Server. Logging options include: <ul style="list-style-type: none">• Critical. This level writes the least information to the log file, reporting only critical errors that have caused the Mobile Device Server to crash.• Error. This level writes errors that are caused by configuration and/or communication problems as well as and Critical messages to the log file.• Warning. This level writes Critical messages, Error messages, and indicates possible operational problems in the log file.
---------------	--

- **Info.** This level is the recommended logging level. This logging level documents the flow of operation and 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 problems.

NOTE Debug mode is not recommended in a production environment unless there is a problem to diagnose. Running in Debug mode consumes considerable CPU resources. If you run in Debug mode, it is also recommended that you increase the log size.

To configure Mobile Device Server resources:

1 From the **Profiles** tab, select the profile from the Profile List.

2 Click **Edit**.

In the **Mobile Device Server Profile** tab, find the Server Resources region.

3 From the **Logging Level** drop-down list, select the logging level you want Avalanche to report.

4 In the **Max Log Size** text box, specify the maximum size (in KB) of the log file should write to before saving the file and beginning a new log.

5 In the **Reserved Serial Ports** text box, specify the serial ports you want to reserve for the Mobile Device Server to use. If you are listing more than one port, separate them with semicolons. For example: COM1 ; COM2

6 In the Terminal ID Generation region, configure the lower and upper limits for the range of terminal IDs that the Mobile Device Server will assign to mobile devices. Alternately, configure your own method using the **Generation template** text box.

7 Save your changes.

Mobile Device Server License Options

You can return licenses to the unused pool when a device has not contacted a server after a period of time. The period of time which must elapse before the license is released can be configured. The minimum number of days is five.

To configure license release:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.

In the **Mobile Device Server Profile** tab, find the Avalanche Licensing region.

- 3 Enable the **Release Device licenses after** option and enter the number of days after which the license should be returned.
- 4 If desired, enable **Enable Fast-Expiration** to allow the server to terminate the license lease after the specified time period without contacting the device.

NOTE If **Enable Fast-Expiration** is disabled, the server will attempt to contact any devices that have not communicated with the server in the configured time period. If the device does not respond, the license lease will be terminated.

- 5 Save your changes.

Mobile Device Server Profile Authorized Users

For information on adding an authorized user for the Mobile Device Server profile, see *Assigning Authorized Users to Profiles* on page 55.

Mobile Device Settings on the Server Profile

You can configure settings from the Mobile Device Server profile that affect how the mobile device interacts with the Mobile Device Server. These settings include:

- **Device Chat Timeout.** This option sets the amount of time in minutes that both the device and the enterprise server will wait before dropping a chat session.
- **Device Comeback Delay.** This option sets the amount of time in minutes that the mobile device will wait before trying to reconnect to the Mobile Device Server after a connect rejection (i.e., if the device tried to connect during an exclusion window).
- **Enable Device Caching.** This option enables mobile devices to download software package files from other mobile devices on the same subnet instead of from the Mobile Device Server. Device caching reduces the demands on the Mobile Device Server during software package synchronization. For information about implementing device caching, call Wavelink Customer Support.

- **Enable Persistent Connection.** This option causes each device to create a persistent TCP connection with the Mobile Device Server. This ensures communication in an environment where UDP packets cannot reliably be transmitted between the server and the device.
- **Enable SMS Notification.** This option allows the Mobile Device Server to use SMS notification if a device cannot be reached by UDP packets. This option is only available for devices with a phone, and must also be configured on the device and at the enterprise server. For more information on enabling SMS notification, call Wavelink Customer Service.
- **Suppress GPS Data Collection.** When this option is enabled, the Mobile Device Server will discard GPS data collected from the devices rather than transmitting it to the enterprise server.
- **Suppress Radio Statistics Data Collection.** When this option is enabled, the Mobile Device Server will discard radio statistics data collected from the devices rather than transmitting it to the enterprise server.
- **Suppress Realtime Properties Data Collection.** When this option is enabled, the Mobile Device Server will discard realtime properties data collected from the devices rather than transmitting it to the enterprise server.
- **Suppress Software Profile Data Collection.** When this option is enabled, the Mobile Device Server will discard software profile data collected from the devices rather than transmitting it to the enterprise server.
- **User Files Upload Path.** When a package's .PPF file specifies that files are to be uploaded to Home, this option provides the path to Home on the machine local to the Mobile Device Server. If no path is specified, Home is defined as the Mobile Device Server installation directory.
- **User Files Download Path.** When a package's .PPF file specifies files that are to be downloaded from Home, this option provides the path to Home on the machine local to the Mobile Device Server. If no path is specified, Home is defined as the Mobile Device Server installation directory.

To configure mobile device settings on the Mobile Device Server profile:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Mobile Device Server Profile** tab, find the Device Settings region.

- 4 Configure the settings as desired.
- 5 Click **Save**.

Secondary Mobile Device Servers

Avalanche allows you to configure the Mobile Device Server profile with secondary server support. This allows mobile devices to attempt to connect to a secondary Mobile Device Server if the primary server is not available. Mobile devices attempt to connect to the servers in the Secondary Server List. If the device cannot connect to the first server on the list, it will move to the next server on the list until it is able to connect to a server. If the mobile device can not connect to any servers, it remains offline and an alert appears in the Alert Browser.

NOTE A network profile is required for secondary server support. The secondary server properties are set using a network profile.

NOTE Unexpected mobile device behavior may occur if the secondary server is configured differently than the primary server. The mobile device may adopt the network profile of the secondary server.

You can configure the following connection settings:

- **Enable Secondary Server Support.** When you enable this option, the mobile device is authorized to attempt to connect a secondary Mobile Device Server if the primary server is not available. You can click on the **Secondary Servers** button to configure the list of secondary servers and their addresses/hostnames.
- **Override Connection Timeout Settings.** When you enable this option, the Mobile Device Server profile settings will override any connection settings configured on the mobile device.
- **Server Connect Timeout.** This option configures the number of seconds the mobile device will wait between attempts to connect to the current mobile device server.
- **Server Advance Delay.** This option configures the number of seconds prior to advancing to the next secondary server.

For example, if you have your **Server Connect Timeout** set to 10 seconds and the **Server Advance Delay** set to 60 seconds, the mobile device will attempt to contact the server six times (every 10 seconds for 60 seconds).

NOTE Ensure the **Server Advance Delay** setting is a multiple of the **Server Connect Timeout** setting.

To configure secondary server support:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Mobile Device Server Profile** tab, find the Secondary Servers region.
- 4 Configure the settings as desired.
- 5 Click **Save**.

Configuring Mobile Device Server Blackouts and Updates

From the Mobile Device Server profile, you can configure blackout windows when the Enterprise Server is not allowed to contact the Mobile Device Server. You also have the option to restrict when and how many mobile devices can update simultaneously from the server. These options allow you more control over bandwidth usage. You can also schedule profile-specific updates for mobile devices.

This section contains the following information:

- Configuring Blackouts
- Restricting Simultaneous Device Updates
- Scheduling Profile-Specific Device Updates

Configuring Blackouts

To allow you more control over bandwidth usage, Avalanche uses blackout windows and update restrictions in the Mobile Device Server profile. During a server-to-server blackout, the Mobile Device Server is not allowed to communicate with the Enterprise Server. During a device-to-server restriction, the mobile devices are not allowed to communicate with the server.

To create a blackout window:

- 1 From the **Profiles** tab, select the Mobile Device Server profile from the Profile List.
- 2 Click **Edit**.
- 3 From the **Blackouts and Updates** tab:
 - if you want to create a server-to-server blackout window, click the **Add** button in the Server-to-Server Communication Restrictions region.
 - if you want to create a device-to-server restriction window, click the **Add** button in the Device-to-Server Communication Restrictions region.

The *Add Blackout Window* dialog box appears.

- 4 Select the start and end time of the blackout window, and enable the boxes for the days you want the blackout to apply.

NOTE Blackout windows are scheduled using a 24-hour clock. If you create a window where the start time is later than the end time, the window will continue to the end time on the following day. For example, if you scheduled a window for 20:00 to 10:00 on Saturday, it would run from Saturday 20:00 until Sunday 10:00.

- 5 Click **OK**.
- 6 Save your changes.

Restricting Simultaneous Device Updates

You can restrict how many mobile devices can update simultaneously from each server using the Mobile Device Server profile.

To restrict simultaneous device updates:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Blackouts and Updates** tab, find the Device Update Settings region.
- 4 Enable the **Restrict simultaneous device updates to** option and set the maximum number of devices that can update simultaneously.

- 5 Click **Save**.

Scheduling Profile-Specific Device Updates

From the Mobile Device Server profile, you can schedule profile-specific updates for your mobile devices. When you configure a Mobile Device Server update, you have the following options:

- **Event Type.** You can select a one-time event, a recurring event, or a post-synchronization event. A post-synchronization event will take place after each synchronization between the Enterprise Server and the Mobile Device Server. This ensures that each time the Server is updated, the devices are as well.
- **Time Constraints.** You can set the start time and the end time for the event.
- **Allow the mobile device user to override the update.** When this option is enabled, the mobile device user is prompted when the update is scheduled to occur and has the option to override the update.
- **Delete orphaned packages during the update.** When this option is enabled, packages that have been orphaned are removed from the device. A package is considered orphaned if it has been deleted from the Avalanche Console or if the package or the software profile it belongs to has been disabled.
- **Force package synchronization during the update.** When this option is enabled, the Mobile Device Server verifies the existence and state of each file of each package individually rather than consulting the meta-file, which provides file state information.

To schedule a profile-specific device update:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 From the **Blackouts and Updates** tab, click **Add Event**.

The *Add Scheduled Update* dialog box appears.

- 4 Select the event type. If you select **Recurring Event**, the **Recurring Period** lists become active. The first list allows you to determine whether the update occurs on either a daily or weekly basis. If you select **Weekly** from this list, the second list becomes active, allowing you to select the day on which the update occurs.

- 5 Set the start time by clicking the calendar icon to open the *Select a date and time* dialog box. Choose the start time and click **OK**.

NOTE For a post-synchronization event, the start/stop time options are disabled.

- 6 If desired, enable the **Stop if not completed by** option. Set the stop time by clicking the calendar icon to open the *Select a date and time* dialog box. Choose the stop time and click **OK**.

NOTE Selecting an end time is not required. Events can recur indefinitely.

- 7 Enable the other update options as desired.
- 8 Click **OK**.

When an event is scheduled, it appears in the Device Update Settings List. Once the event has occurred, it will not automatically be deleted from the list. If you want to remove an event from the list, you must select it and click **Remove Event**.

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 Avalanche. 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.

Viewing Mobile Device Server Licensing Messages

The Avalanche Console receives licensing messages from the Mobile Device Server. You can view these messages from the *dServer Licensing Messages* dialog box. This dialog box provides information about the Server Location where the Server resides and the licensing message.

To view licensing messages:

- 1 From the **View** menu, select **Distributed Server License Messages**.

The *dServer Licensing Messages* dialog box appears.

- 2 Click the **Site** column to list the messages by Site.
- 3 Click the **dServer** column to list the messages by Server.

Viewing Where Mobile Device Server Profiles Are Applied

The **Applied To** tab in the **Profiles** tab allows you to see exactly which Server Locations and Sites to which a selected profile is directly applied. You cannot change this information from this tab. For information on how to assign your profiles to regions, refer to *Assigning Profiles* on page 59.

The **Applied To** tab displays the following information:

- **Parent Path.** The direct path back to the My Enterprise region.
- **Group.** The name of the Region, Server Location or Site where the profile is applied.
- **Selection Criteria.** Any selection criteria that is applicable at the region, Server Location or site where the profile is applied.

To view:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click the **Applied To** tab.

The tab displays the information for the selected profile.

Reinitializing the Mobile Device Server

Reinitializing the Mobile Device Server allows you to restart the server without stopping and starting the service. The server will sync with the Enterprise Server and load any changes it detects, but the service keeps running so you will not lose contact with any devices that are updating.

To reinitialize the Mobile Device Server:

- 1 From the Navigation Window, select the Mobile Device Server you want reinitialize.
- 2 Right-click and select **Reinitialize Mobile Device Server**.

The server contacts the Enterprise Server and downloads any updates.

Chapter 10: Managing Software Profiles

A software profile is a configuration profile containing software packages. The packages associated with the profile are installed on all devices meeting the selection criteria. Software profiles allow you to organize and configure software packages for deployment to multiple devices.

This section contains the following topics:

- Configuring Software Profiles
- Managing Software Packages

Configuring Software Profiles

This section contains the following information:

- Adding Software Profiles
- Adding Software Profiles from the Quick Start Tab
- Editing Software Profiles
- Applying Software Profiles
- Viewing Where Software Profiles Are Applied

Adding Software Profiles

Before you can install any software packages, you must create a software profile.

To add a software profile:

- 1 From the **Profiles** tab, click **Add Profile**.

The *Create Profile* dialog box appears.

- 2 Select **Software Profile** from the drop-down list and type the name of the profile in the **Profile Name** text box.

NOTE Software profile names are case-sensitive and must be unique.

- 3 Click **OK**.
- 4 The software profile is created and can be enabled, configured, and assigned to a site or location.

Adding Software Profiles from the Quick Start Tab

You can add software profiles from the **Profiles** tab or from the **Quick Start** tab. The following steps are instructions for using the Add Device Software Wizard from the **Quick Start** tab.

To add a software profile:

- 1 From the **Quick Start** tab, select **Add Device Software**.

The *Add Device Software Wizard* launches.

- 2 In the **Create a New Software Profile** text box, enter the name of the profile and then click **Next**.

Your software profile is created. The following steps in the wizard are optional. If you only want to create the profile and not configure any options, click **Finish**. Your profile appears in the software profiles tab. If you want to configure, continue with the wizard.

- 3 In the **Configure the Software Profile** dialog that appears, you can enable the profile and configure selection criteria.

- 4 Click **Next**.

- 5 In the **Select a Software Package to Add** dialog, you can add, create or copy a package to the profile. For information about all these options refer to *Adding Software Packages* on page 107.

- 6 Click **Next**.

The End User License Agreement appears.

- 7 Enable **Yes I agree** to agree to the license agreement and click **Next**.

- 8 The *Installing the Software Package* dialog box appears and the software is added to the profile. When the package has been installed successfully, click **Next**.

- 9 The *Configure the Software Package* dialog box appears.

10 If desired, enable the software package and configure it using the available utilities.

11 Click **Finish**.

Your configured profile with the installed packages will appear in the **Software Profiles** tab.

Editing Software Profiles

Once a software profile has been created, you can edit the name, status, and selection criteria. You can also add software packages to the profile. For information on adding and configuring software packages, see *Managing Software Packages* on page 105.

This section contains information about the following:

- Enabling Software Profiles
- Software Profile Authorized Users
- Software Profile Selection Criteria

Enabling Software Profiles

A software profile can have its status set to enabled or disabled. The profile must be enabled before you can apply it.

To enable a software profile:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Software Profile** tab, select **Enabled**.
- 4 Save your changes.

The software profile is now enabled.

Software Profile Authorized Users

You can add authorized users for all software profiles or enable a user for a specific software profile. For information on adding an authorized user, see *Managing User Accounts* on page 47.

Software Profile Selection Criteria

Selection criteria determine which mobile devices receive the software profile. Only devices that meet the selection criteria for the software profile will receive the software associated with the profile. For information about creating selection criteria, refer to *Building Selection Criteria* on page 161.

Applying Software Profiles

Once you have created a software profile and added software packages to the profile, you can enable the profile and it will be applied and deployed. For information about manually applying software profiles, refer to *Assigning Profiles* on page 59.

Viewing Where Software Profiles Are Applied

The **Applied Locations** tab in the software profile page allows you to see exactly which Server Locations and Sites to which a selected profile is directly applied. You cannot change of the information in this tab. If you need to apply a profile to a different location than what you see in the **Applied Locations** tab, you will need to access the **dServer Location Properties** tab and assign the profiles there. For information, refer to *Applying Software Profiles* on page 105.

The **Applied Locations** tab displays the following information:

- **Parent Path.** The direct path back to the My Enterprise region.
- **Group.** The name of the Server Location or Site where the profile is applied.
- **Selection Criteria.** Any selection criteria that is applicable where the profile is applied.

To view:

- 1 From the **Profiles** tab, select the software profile you want to view.
- 2 Click the **Applied Locations** tab.

The tab displays the information for the selected profile.

Managing Software Packages

A software package is a collection of application files that reside on a mobile device. This includes any support utilities used to configure or manage the application from

the Avalanche Console. Each software package usually has default selection criteria that cannot be changed.

The Software Packages region on the **Software Profile** tab allows you to install and configure the software packages associated with that software profile. You can enable the package, configure how the package is activated and distributed, and use the package utilities to configure it.

NOTE When working in software profiles, you do not need to be in Edit Mode to install or configure software packages. Software package configuration changes are saved to the actual package. However, you must enter Edit Mode to configure any other software profile options.

You can also view the packages currently associated with your software profile. The following details are displayed in the Software Packages List:

Field	Description
Name	Displays the name of the software package.
Status	Displays the enabled/disabled status of the software package.
Size	Displays the file size of the software package.
Type	<p>Displays the type of the software package. Software packages are divided into the following categories:</p> <ul style="list-style-type: none"> • Control. An internally used package specific to the Avalanche Console. A network profile is an example of a control package. • Application. These packages install an application which can be run from the Application Menu screen on the mobile device. An example of an application package is the Telnet Client. • Support. These packages deliver files and do not add new items to the Application Menu screen on the mobile device. An example of a support package is a package that updates an existing file. • Auto Run. These packages automatically run after download but do not appear in the mobile device's application list. An Enabler Update Kit is an example of an auto run package.
Version	Displays the version of the software package.
Title	Displays the title of the software package.
Vendor	Displays the vendor associated with the software package.

Field	Description
Installed	Displays the date, time, and user for the package installation.
Configured	Displays the date, time, and user for the most recent package configuration.

This section includes the following information:

- Adding Software Packages
- Building New Software Packages
- Installing CAB or MSI Packages
- Copying Software Packages
- Enabling Software Packages
- Configuring Software Packages with a Utility
- Configuring Software Packages for Delayed Installation
- Peer-to-Peer Package Distribution

Adding Software Packages

Once you create a software profile, you must add the software packages to that profile. Through the software profile you can configure the software package settings and then deploy the packages to specific mobile devices.

When working in software profiles, you do not need to be in Edit Mode to add or configure software packages. Software package configuration changes are saved to the actual package. However, you must enter Edit Mode to configure any other software package options.

You can add packages, copy packages that have already been added to a different profile, or create custom software packages from the Avalanche Console using the Add Device Software Wizard. Before you create a custom package, ensure you know the location of all the files you want to include and ensure that the files are valid.

Using the Add Device Software Wizard, you can also enable and configure the added, created, or copied software package. The following instructions provide information about adding an Avalanche package to a software profile. For information about building a new package refer to *Building New Software Packages* on page 109.

To add a software package:

- 1 Select the profile to which the package will belong from the Profiles List.
- 2 From the **Software Profile** tab, click **Add Package**.

The *Add Device Software Wizard* appears.

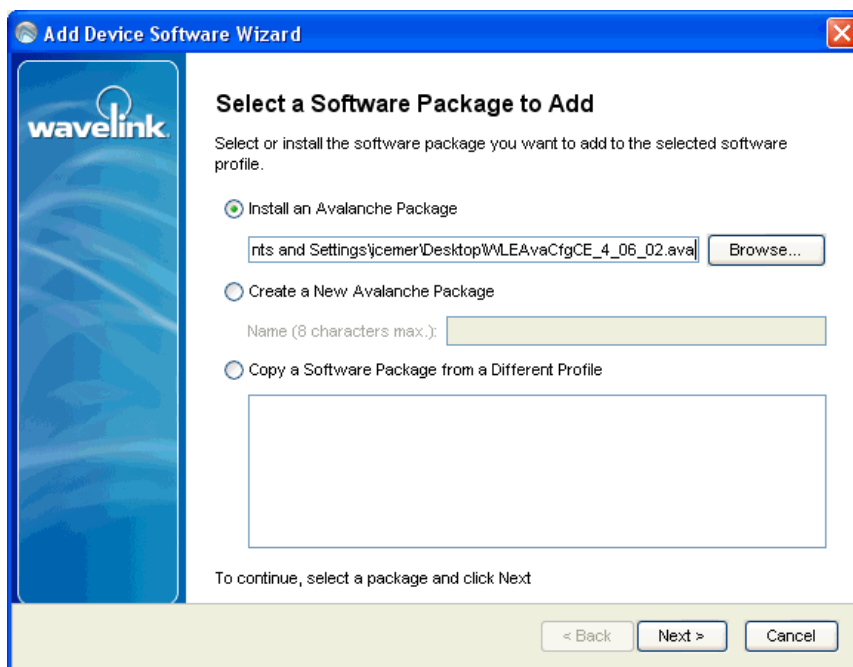


Figure 10-1. *Select Package*

- 3 Select **Install an Avalanche Package** and browse to the location of the software package.
- 4 Select the file and click **Next**.
A *License Agreement* dialog box appears.
- 5 Accept the license agreement and click **Next**.
- 6 The package files will begin extracting locally. When the extraction is complete, click **Next**.

The *Configure Software Package* dialog box appears. This dialog box allows you to enable the package immediately and displays the utilities available for the package.

- 7 If you want to configure your software package, double-click the configuration tool you want to launch.
- 8 When you are finished configuring, click **Finish** to complete the installation.

After software packages are configured and enabled, you can deploy the software profile and the packages will be distributed to all devices in the applied region that meet the selection criteria.

Building New Software Packages

The Add Device Software Wizard allows you to compile files to create a new software package. Ensure you know the location of the files you want to include the package.

To build a new package:

- 1 Select the profile to which the package will belong from the Profiles List.
- 2 From the **Software Profile** tab, click **Add Package**.

The *Add Device Software Wizard* appears.

- 3 Select **Create a New Avalanche Package** and type a name for the package in the text box.
- 4 Click **Next**.

A *Specify the Files in the Ad Hoc Package* dialog box appears.

- 5 Click **Add** and browse to the location of the files you want to add to the package.
- 6 Select the file and click **Open**.

The file path location appears in the text box. Continue adding files as desired.

- 7 Click **Next**.

The *Ad Hoc Package Options* dialog box appears.

- 8 Configure the following options:
 - **Title**. Enter a title for the package.

- **Vendor.** Enter the package vendor.
- **Version.** Enter the version number of the package.
- **Install Drive.** Specify the drive on the mobile device where you to install the package.
- **Install Path.** Specify the exact installation path for the package.
- **Post Install Options.** You can specify if you want the device to perform a warm boot or cold boot after installation has completed. You can also specify a program to run once installation is complete. When you select to run a program, the drop-down list will become active and you can select which program from your package you want to run.

NOTE Changing any of these settings is optional unless you select to run a program. Then you are required to select which program you want to run.

9 Click **Next**.

The *Add Selection Criteria* dialog box appears.

- 10 If you want to configure selection criteria for the package, enable **Add Selection Criteria** and enter the information in the text box. By creating selection criteria for your package, only the devices which meet the selection criteria will receive the package.

NOTE When you enable **Add Selection Criteria**, the Selection Criteria Builder button to the left of the list is enabled. You can click it and use the Selection Criteria Builder to help you create the criteria, if desired.

11 Click **Next**.

- 12 The package files will begin extracting locally. When the extraction is complete, click **Next**.

The *Configure the Software Package* dialog box appears. This dialog box allows you to enable the package immediately and displays any configuration tools available for the package.

13 Click **Finish** to complete the installation.

Installing CAB or MSI Packages

You can use Avalanche to push `.cab` or `.msi` files to your mobile devices. When you install a `.cab` file, the file automatically installs. It can also be configured to uninstall once the program information is retrieved by the mobile device.

To install `.cab` or `.msi` packages:

- 1 Select the profile to which the package will belong from the Profiles List.
- 2 From the **Software Profile** tab, click **Add Package**.

The *Add Device Software Wizard* appears.

- 3 Create a new profile or enable the **Select to existing software profile** option and select the profile to which you want to install.
- 4 Click **Next**.
- 5 Select **Add an Avalanche software package** and browse to the location of the `.cab` or `.msi` file.
- 6 Click **Next**.

The *CAB or MSI File Options* dialog box appears.

- 7 Enter the name of the package (limit eight characters).
- 8 If you want the package to be uninstalled once the program information is retrieved by the mobile device, enable **Remove After Install**.
- 9 Click **Next**.
- 10 The package files will begin extracting locally. When the extraction is complete, click **Next**.

The *Configure the Software Package* dialog box appears. This dialog box allows you to enable the package immediately and displays any configuration tools available for the package.

- 11 Click **Finish** to complete the installation.

Copying Software Packages

You can copy a software package and its configuration from one software profile to another. Copying software packages allows you to configure a software package just once and then copy it into all the profiles that require that package.

To copy a software package:

- 1 From the **Profiles** list, select the profile from which you want to copy the package.
- 2 In the Software Packages region, right-click the package you want to copy.
- 3 Click **Copy** from the context menu.

The *Please select the target profile* dialog box appears.

- 4 Select the profile to which you want to copy the package from the drop-down list.
- 5 Click **OK**.

The package and its configuration is copied to the target software profile.

Enabling Software Packages

A software package can have its status set to enabled or disabled. The package must be enabled to be installed on mobile devices. You do not need to enable a package to configure it.

To enable a software package:

- 1 From the **Profiles** tab, select the software profile with the package you want to enable.
- 2 Click **Edit**.
- 3 Select the package from the list in the Software Packages region.
- 4 Click **Enable**.
- 5 Save your changes.

Configuring Software Packages with a Utility

Some software packages come with configuration utilities that allow you to configure options before the packages are installed on a mobile device. These utilities can be

accessed from the Avalanche Console. Configuration options will differ based on the software package.

NOTE While the provided instructions use the buttons, you can also right-click a software package to configure it.

To configure a software package:

- 1 From the **Profiles** tab, select the software profile with the software package you want to configure.
- 2 From the Software Packages region of the **Software Profile** tab, select the package.
- 3 Click **Configure**.

The *Configure Software Package* dialog box appears.

- 4 From the available list, double-click the utility you want to use to configure the package.

NOTE Configuration details are specific to the type of software package. For details about configuring software packages, refer to the specific user guide for that product.

- 5 When the options are configured, click **OK**.

The software package is configured for deployment.

Configuring Software Packages for Delayed Installation

Software packages can be configured to install on a delayed basis. Delayed packages are downloaded to the mobile device just like any other package, but do not get installed on the device until the configured activation time. For applicable devices, the downloaded packages are stored in persistent storage and can survive a cold boot.

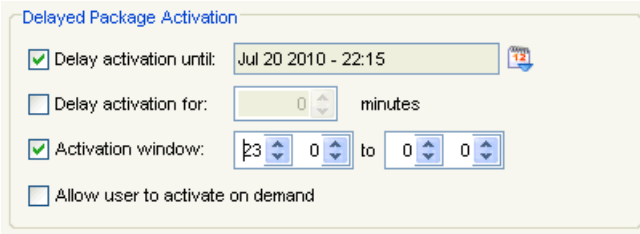
Delayed package installation provides flexible control over when the mobile device installs software packages.

NOTE If package activation is not supported by the Enabler version on the device, the package is treated as disabled and will not be downloaded to the device until the activation time expires.

Package activation is supported by Enabler version 4.1 and later.

To configure a software package for delayed installation:

- 1 From the **Profiles** tab, select the software profile with the package you want to delay.
- 2 Click **Edit**.
- 3 Select the package from the list in the Software Packages region.



The screenshot shows a configuration window titled "Delayed Package Activation". It contains four options:

- Delay activation until: Jul 20 2010 - 22:15 (with a calendar icon)
- Delay activation for: 0 minutes
- Activation window: 23 to 00
- Allow user to activate on demand

Figure 10-2. Delayed Package Activation

- 4 In the Delayed Package Activation region, enable the options as desired:
 - If you want to delay package activation until a specific date and time, enable the **Delay activation until** option and click on the calendar button to select a date and time.
 - To further delay the package installation after it has been activated, configure the **Delay activation for __ minutes** option.
 - If you want the package to be activated during a certain time window, enable the **Activation window** option and configure the hours during which the package will activate.
- 5 If you want the device user to have the option to override the software package installation at the activation time, enable the **Allow Device User to Override** checkbox.

If the user chooses to override the installation time, he will be able to install the package as soon as it is downloaded, instead of waiting until the activation time.

6 Save your changes.

Peer-to-Peer Package Distribution

Peer-to-peer package distribution allows you to control bandwidth usage on your network by allowing a “package store” device to receive an update from the Mobile Device Server and then distribute the update to other mobile devices.

The following table provides descriptions of the configuration options in package distribution.

Field	Description
Enabled Cached Peer-to-Peer Package Distribution	Enable this option to allow a package to be shared across multiple devices via peer-to-peer connections. When deployed to a mobile device, the package will then be available for other mobile devices to receive the profile from that package store device.
Do not allow non-Package Store Devices to begin updating until	Enable this option to configure the time at which a non-package store device can contact a package store device to receive an update. A non-package store device refers to a mobile device that is not being used to update other mobile devices.
Do not allow server to update non-Package Store Devices until	Enable this option to configure the time at which a non-package store device can contact the Server to update and receive this package. Once the configured time is reached, the mobile devices will first attempt to contact a package store device to receive the update. If a package store device cannot be contacted or the connection times out, the device will then attempt to contact the Server. A non-package store device refers to a mobile device that is not being used to update other mobile devices.

The following tables provides information about the results that will occur with the different configurations in package distribution.

If	Then Package Store Devices	And Non-Package Store Devices
<p>Do Not Allow Non-Package Store Devices To Begin Updating Until is enabled and the configured time has not been reached</p> <p>(Do Not Allow Server to Update Non-Package Store Devices Until is not enabled)</p>	<i>Can</i> contact the Server for updates at any time.	<p>Cannot contact any package store devices.</p> <p>Will attempt to contact the Server to receive updates.</p>
<p>Do Not Allow Non-Package Store Devices To Begin Updating Until is enabled and the configured time has been reached</p> <p>(Do Not Allow Server to Update Non-Package Store Devices Until is not enabled)</p>	<i>Can</i> contact the Server for updates at any time.	<p><i>Can</i> contact package store devices to update and receive the profile.</p> <p>If the device can not contact a package store device, it will attempt to contact the Server.</p>
<p>Do Not Allow Non-Package Store Devices To Begin Updating Until is enabled and Do Not Allow Server to Update Non-Package Store Devices Until is enabled and the configured time has not been reached</p>	<i>Can</i> contact the Server for updates at any time.	<p>Cannot contact the Server for updates.</p> <p>Cannot contact any package store devices.</p>
<p>Do Not Allow Non-Package Store Devices To Begin Updating Until is enabled and Do Not Allow Server to Update Non-Package Store Devices Until is enabled and the configured time has been reached</p>	<i>Can</i> contact the Server for updates at any time.	<p><i>Can</i> contact package store devices to receive updates.</p> <p>If the device can not contact a package store device or the connection times out, the device <i>can</i> contact the Server to receive updates.</p>
No options are enabled	<i>Can</i> contact the Server for updates at any time.	<i>Can</i> contact package store devices or Server for updates at any time.

To configure peer-to-peer package distribution:

- 1 From the **Profiles** tab, select the software profile with the package you want to distribute.
- 2 Click **Edit**.
- 3 In the Peer-to-Peer Package Distribution region, configure the desired options.
- 4 Save your changes.

Chapter 11: Managing Mobile Devices

This section provides information about the following mobile device topics:

- Mobile Device Inventory Tab
- Viewing Mobile Device Details
- Configuring Mobile Device Properties
- Contacting the Mobile Device
- Software Inventory

Mobile Device Inventory Tab

The **Mobile Device Inventory** tab shows a set of mobile devices based on the currently selected item in the Navigation Window. For example, when you select a particular location, all mobile devices that are associated with that location appear in the list. The following default information is provided for each mobile device:

Model Name	The model name of the mobile device.
Terminal ID	The unique ID automatically generated by Avalanche.
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.
Status	The client update status of the mobile device. A 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.
Last Contact	The date and time of the last contact the mobile device had with Avalanche.
Recent Activity	The status of a mobile device with respect to Avalanche. For example, when the mobile device receives new software, the activity status is Downloading .

You can customize the columns in the **Mobile Device Inventory** tab to display according to your preference or filter the devices shown. For information on customizing the Mobile Device Inventory, see *Managing Device Inventory Displays* on page 35.

You can also delete mobile devices from the Mobile Device Inventory. This removes the device from the Mobile Device Inventory list and releases the license that mobile device was using.

To delete mobile devices:

- In the **Mobile Device Inventory** tab, right-click the device you want to delete and select **Delete**.
- The device is removed. It retains the ability to connect and re-associate itself with the server, however.

Viewing Mobile Device Details

You can perform mobile device tasks from the *Mobile Device Details* dialog box. The *Mobile Device Details* dialog box provides device-specific information and consists of the following regions:

- **Summary Information.** This region provides a quick summary of device, health, signal strength and battery life information.

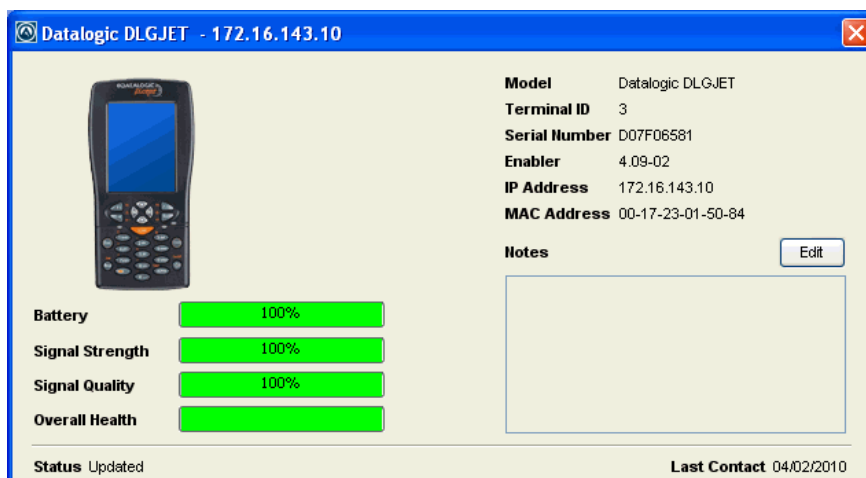


Figure 11-1. Device Details summary information

The Health Data bars will display red, yellow or green depending on the status of the battery, signal strength, signal quality, and overall health of the device.

- **Device Tabs.** This region provides access to the following tabs:
 - **General.** Provides general network and wireless information about the device.
 - **Installed Software.** Provides information about the software applications installed on the device. For details, refer to *Software Inventory* on page 130.
 - **Packages.** Lists all the packages currently available for the device and the status of each package.
 - **Properties.** Lists the properties of the device and their values. This tab also allows you to add properties and values. For details about the tasks you can perform in the **Properties** tab, refer to *Configuring Mobile Device Properties* on page 120.
 - **Applied Profiles.** Lists the profiles that are applied.
 - **Device Control.** Provides options for updating the mobile device, sending text messages, pinging the device, using Remote Control, and connecting to the Session Monitor. For details, refer to *Contacting the Mobile Device* on page 124.

To view mobile device details:

- Right-click the mobile device you want to view and select **Mobile Device Details**.

Configuring Mobile Device Properties

Mobile device properties consist of pre-defined and custom properties. Pre-defined properties are device-specific and dependent on the version of the Enabler running on the mobile device. Custom properties can be associated with individual mobile devices or with mobile device groups. Properties can be used as selection variables in selection criteria to control which devices receive particular updates.

NOTE Refer to *Building Selection Criteria* on page 161 for more information on using properties as selection variables.

From the **Properties** tab of the *Mobile Device Details* dialog box, you can perform the following tasks:

- Viewing Properties
- Creating Custom Properties
- Creating Device-Side Properties
- Editing Properties
- Deleting Properties

Viewing Properties

You can view the properties associated with a specific mobile device in the Mobile Device Inventory List.

To view the properties:

- 1 From the **Mobile Device Inventory** tab, right-click the device you want to view and click **Mobile Device Details**.
- 2 Click the **Properties** tab.

The columns that appear in this dialog box are as follows:

Name	The name of the property.
Value	The value of the property.
Pending Value	Indicates whether the property needs to be updated on the mobile device. If it needs to be updated, column will display the pending value in italics.
Icon	Indicates whether the value of the property is static, snapshot, or configurable data.

Creating Custom Properties

From the Avalanche Console, you can create custom properties on the mobile devices. These properties can then be used to build selection criteria for software updates or to filter on the **Mobile Device Inventory** tab.

NOTE Like the pre-defined properties, custom properties appear as selection variables in the Selection Criteria Builder.

You can add custom properties to individual mobile devices or to mobile device groups. When you add a property to a group, it is added to all mobile devices that are members of the group. For instructions on adding a property to a group, see *Editing Properties for Mobile Device Groups* on page 147.

To create custom properties:

- 1 From the **Mobile Device Inventory** tab, right-click the device you want to view and click **Mobile Device Details**.
- 2 Click the **Properties** tab.
- 3 Click **Add Property**.
- 4 From the drop-down list, select what type of property you want to add.
- 5 Type the name and the value of the property in the **Property Name** and **Property Value** text boxes.
- 6 Click **OK**.

The property is added to the list in the **Properties** tab under the chosen heading and the device will receive it upon the next update.

Creating Device-Side Properties

Avalanche provides the ability to turn third-party information that is generated at the mobile device into properties that can then be transferred to and displayed in the Avalanche Console. These properties are called device-side properties. You can use the device-side properties feature to obtain either static or dynamic information. For example, a device-side property could report a device's serial number or state changes within a specific application.

NOTE It is important to note that the Avalanche Enabler sends device-side properties to the Enterprise Server; it does not collect the information. Vendors must create their own applications and utilities to gather the required information and write it to a plain-text file on the device.

Device-side properties must be written in key-value pairs to a plain-text file with a `.prf` extension and one vendor entry. Avalanche uses the vendor name to organize and display user-defined properties in the **Properties** tab of the *Mobile Device Details* dialog box.

For more information about creating device-side properties, see the *Creating Device-Side Avalanche Properties* white paper on the Wavelink Web site.

Editing Properties

Some of the pre-defined properties (and all of the custom 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.

Custom properties can be edited either for a specific mobile device or for a group of devices. For information on editing properties for a group of devices, see *Editing Properties for Mobile Device Groups* on page 147.

To edit a property for a mobile device:

- 1 From the **Mobile Device Inventory** tab, right-click the device you want to view and click **Mobile Device Details**.
- 2 Click the **Properties** tab.
- 3 Select the property that you want to edit.

If the property is editable, the **Edit Property** button becomes active.

- 4 Click **Edit Property** and type the new value for the property.
- 5 Click **OK**.

The new value downloads to the mobile device at the next update. If the device has not yet received an updated property value, the pending value appears in italics in the Pending Value column for the property.

Deleting Properties

You can delete any configurable mobile device property from the Avalanche Console.

To delete a property:

- 1 From the **Mobile Device Inventory** tab, right-click the device you want to view and click **Mobile Device Details**.
- 2 Click the **Properties** tab.
- 3 Select the property that you want to delete and click **Delete Property**.
- 4 Click **OK**.

Contacting the Mobile Device

This section provides information about the following tasks that you can perform from the **Device Control** tab in the *Mobile Device Details* dialog box:

- Pinging Mobile Devices
- Sending Messages
- Updating a Mobile Device
- Locating a Mobile Device
- Locating a Device using Cell Tower Information
- Viewing Location History
- Using Remote Control
- Launching the Session Monitor
- Launching Wavelink Communicator

Pinging Mobile Devices

You can ping devices that are currently in range and running the Avalanche Enabler. 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 a mobile device:

- 1 From the **Mobile Device Inventory** tab, right-click the device you want to view and click **Mobile Device Details**.
- 2 Click the **Device Control** tab.
- 3 Double-click the **Ping Device** icon.

The **Status** field in the Activity region displays the status of the ping request.

NOTE You can also ping the device from the **Mobile Device Inventory** tab by right-clicking the mobile device and selecting **Ping Device**.

Sending Messages

You can send a text-based message to a device currently in range and running the Avalanche Enabler.

To send a message:

- 1 From the **Mobile Device Inventory** tab, right-click the device you want to view and click **Mobile Device Details**.
- 2 Click the **Device Control** tab.
- 3 Double-click the **Send Text Message** icon.

The *Send Text Message* dialog box appears.

- 4 Type a message in the **Text Message** field.
- 5 Enable the **Provide Audible Notification** option if you want a sound to play when the mobile device receives the message.
- 6 Click **OK**.

The **Status** field in the Activity region displays the status of the text message request.

NOTE You can also send a text message to the client from the **Mobile Device Inventory** tab by right-clicking the mobile device and selecting **Send Text Message**.

Updating a Mobile Device

You can perform individual updates for mobile devices 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 *Building Selection Criteria* on page 161 for more information on building selection criteria.

To update a mobile device:

- 1 From the **Mobile Device Inventory** tab, right-click the device you want to update and click **Mobile Device Details**.

- 2 Click the **Device Control** tab.
- 3 Double-click the **Update Now** icon.

The *Update Now* dialog box appears.

- Enable the **Allow User to Override the Update** option if you want to give the mobile device user the option to override the update.
 - Enable the **Force Package Synchronization** option if you want to force the package to update the device.
 - Enable the **Delete Orphan Packages** option if you want to remove orphan packages from the mobile device.
- 4 From the dialog box, select which orphan packages you want to remove.
 - 5 Click OK.

The **Status** field in the Activity region 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 Avalanche. 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.

NOTE You can also update the mobile device from the **Mobile Device Inventory** tab by right-clicking the mobile device and selecting **Update Now**.

Locating a Mobile Device

You can view the most recently reported location of a mobile device with GPS capabilities. The device is displayed as an icon on the map. In order to use this option, you must have a statistics server running, and statistics reporting must be enabled.

To view the location of a mobile device:

- 1 From the **Mobile Device Inventory** tab, right-click the device you want to view.

- 2 From the context menu, select **Locate**.

The Map View appears with the mobile device icon displaying the most recently reported location of the device.

Locating a Device using Cell Tower Information

When a device has GPRS capabilities, it can report the cell tower it is currently connected to. The Console can use this information to display an approximate location for the device on the map.

NOTE Avalanche uses `geoservices.wavelink.com` to retrieve information about the location of the cell towers. You must be able to access this Web site in order to use the Locate Cell Tower function.

To locate a device using cell tower information:

- 1 Navigate to a region, location or mobile device group containing the device you want to locate.
- 2 Right-click the name of the device and select **Locate via Cell Tower** from the context menu.

An icon appears on the map displaying the location of the cell tower the device is currently connected to.

Viewing Location History

You can view the recently reported locations of a mobile device with GPS capabilities. In order to use this option, you must have a statistics server running, and statistics reporting must be enabled.

NOTE You can only view the location history of one device at a time.

To view the location history of a mobile device:

- 1 From the Mobile Device Inventory, right-click the device you want to view.
- 2 From the context menu, select **Location History**.

The *Start and End Time* dialog box appears.

- 3 Use the calendar buttons and time text boxes to specify the window of time for which you want to view location information.
- 4 Click **OK**.

The device location history is displayed on the map as a series of icons representing the reported locations during the specified time.

Using Remote Control

Remote Control functionality is only available for devices that have a licensed Remote Control package installed in Avalanche SE. Remote Control is not functional, until you complete the following tasks:

- 1 Obtain and install the Remote Control software package.
- 2 License the Remote Control program.
- 3 Deploy the Remote Control software package to your mobile device.

Once deployed, you can use Remote Control. For detailed information about all tasks regarding Remote Control, including connecting to a mobile device and accessing various components of the device, refer to the *Wavelink Avalanche Remote Control User's Guide*.

Launching the Session Monitor

The Session Monitor utility allows you to view the Telnet Client on a mobile device from the Avalanche Console. The Session Monitor includes an override feature that allows you to take control of the Telnet Client on the mobile device. It also includes a logging feature that allows you to create a trace for Telnet sessions.

To use the Session Monitor with Avalanche, you will need perform the following tasks:

- 1 Obtain a Telnet 5.x (or later version) software package.
- 2 Install the Telnet software package. Refer to *Adding Software Packages* on page 107 for more information.
- 3 Configure the Telnet Client software package.
- 4 Deploy the Telnet Client to the mobile device.
- 5 Launch the Telnet Client on the mobile device.

6 Launch the Session Monitor.

This section provides information about launching the Session Monitor from Avalanche. For detailed Telnet installation and configuration information, refer to the *Wavelink Telnet Client User Guide*.

You can launch the Session Monitor from the **Mobile Device Inventory** tab or from the *Mobile Device Details* dialog box.

To launch the Session Monitor from the *Mobile Device Inventory* tab:

- 1 Ensure you have installed a Telnet package to the Avalanche Console and deployed it to the mobile device.
- 2 Select a Server Location from the Navigation Window.
- 3 Click the **Mobile Device Inventory** tab.
- 4 Right-click the device on which you want to launch the Session Monitor and select **Session Monitor** from the menu.

The Telnet Session Monitor window opens. The yellow-lined box represents what the mobile device user can see on the mobile device screen.

To launch the Session Monitor from the *Mobile Device Details* dialog box:

- 1 Ensure you have installed a Telnet package to the Avalanche Console and deployed it to the mobile device.
- 2 Select a Server Location from the Navigation Window.
- 3 Click the **Mobile Device Inventory** tab.
- 4 To open the *Mobile Device Details* dialog box:
 - Double-click the mobile device on which you want to launch session monitor.

-Or-

 - Right-click the mobile device on which you want to launch session monitor and select **Mobile Device Details**.
- 5 In the *Mobile Device Details* dialog box, click the **Device Details** tab.
- 6 Double-click the **Session Monitor** icon.

The Telnet Session Monitor window opens. The yellow-lined box represents what the mobile device user can see on the mobile device screen.

Launching Wavelink Communicator

Communicator is a push-to-talk application that enables users to communicate with one another in a one-to-one (device to device) or one-to-many (broadcast) mode of operation. You can launch it from the Avalanche Console and use it to talk to people who are using mobile devices with Communicator installed. For detailed information refer to the *Wavelink Communicator User Guide*.

To launch Communicator:

- 1 Ensure you have installed a Communicator package to the Avalanche Console and deployed it to the mobile device.
- 2 Select a Server Location from the Navigation Window.
- 3 Click the **Mobile Device Inventory** tab.
- 4 Right-click the device you want to communicate with and select **Launch Communicator**.
- 5 Alternately you can access the *Mobile Device Details* dialog box, click the **Device Details** tab and double-click the Communicator icon.

The Communicator will connect to the mobile device and you can begin transmissions.

Software Inventory

The Console gathers mobile device software inventory every 24 hours and displays the information in the **Installed Software** tab of the *Mobile Device Details* dialog box. The **Installed Software** tab consists of two parts:

- The **Registered Applications** tab displays the applications on the mobile device that have uninstallers registered with the system. These applications will also be displayed in the Windows settings *Installed Applications* dialog box on the mobile device.
- The **All Applications** tab lists the file name and file path of all executable that can be run on the mobile device.

This is informational data only and cannot be modified from this tab.

Chapter 12: Managing Mobile Device Profiles

You can use a mobile device profile to change settings on your mobile devices, as well as add, change, and remove custom properties and registry keys. This section contains the following topics:

- Creating a Mobile Device Profile
- Configuring Mobile Device Profile General Settings
- Mobile Device Profile Authorized Users
- Editing Custom Properties for Mobile Device Profiles
- Editing Registry Keys for Mobile Device Profiles
- Configuring Mobile Device Profile Advanced Settings
- Viewing Where Mobile Device Profiles are Applied

Creating a Mobile Device Profile

You can use a mobile device profile to change settings on your mobile devices, as well as add, change, and remove properties and registry keys.

To create a mobile device profile:

- 1 From the **Profiles** tab, click **Add Profile**.

The *Create Profile* dialog box appears.

- 2 Select **Mobile Device Profile** from the drop-down list and type the name of the profile in the **Profile Name** text box.
- 3 Click **OK**.

The mobile device profile is created and can be enabled, configured, and assigned to a location.

Configuring Mobile Device Profile General Settings

When you create a mobile device profile, you can configure the server that the devices should connect to, SMS notification, package sync, orphan package removal, and selection criteria.

To configure mobile device profile general settings:

- 1 From the **Profiles** tab, select the mobile device profile you want to configure.
- 2 Click **Edit**.
- 3 From the **Mobile Device Profile** tab, select **Enabled** if you want to enable the profile.
- 4 If you want the mobile devices to communicate with a specific server, type the address of the server in the **Server Address** text box.
- 5 If you want to enable SMS notifications, enable the **Enable SMS Notifications** check box.
- 6 If you want to **Force Package Synchronization** when the devices connect, enable the check box. This will ensure that the devices have all the packages available to them at the server.
- 7 If you want to **Restrict simultaneous device updates**, enable the check box and the set the maximum number of devices that can update simultaneously.
- 8 If there is a package you want removed when it becomes orphaned, type the name in the **Orphan Package Removal** text box. If you want to specify more than one, separate the names with commas.
- 9 If you want to restrict which mobile devices use the profile, use the Selection Criteria Builder to create selection criteria for the profile. For more information on using the Selection Criteria Builder, see *Using Selection Criteria* on page 160.
- 10 Click **Save** to save your changes.

Mobile Device Profile Authorized Users

You can add authorized users for all mobile device profiles or enable a user for a specific mobile device profile. For information on adding an authorized user, see *Managing User Accounts* on page 47.

Editing Custom Properties for Mobile Device Profiles

Custom properties allow you to define specific properties that you want applied to the mobile device. An example of a custom property would be `location = Chicago`. Once a custom property has been applied to a device, you can use it as a selection criterion. You can apply custom properties to mobile devices through a mobile device profile.

You also have the option to edit or remove custom properties currently existing on the device through a mobile device profile. You must know the name of the property in order to edit or remove it.

This section contains information on the following tasks:

- Adding a Custom Property
- Editing or Removing a Custom Property

Adding a Custom Property

You can add a custom property to a mobile device through a mobile device profile. Add the property to the profile, then deploy the profile to the device.

To add a custom property:

- 1 From the **Profiles** tab, select the mobile device profile you want to configure.
- 2 Click **Edit**.
- 3 Click the **Mobile Device Profile** tab.
- 4 In the Device Properties region, click **Add**.

The *Add Property* dialog box appears.

- 5 Select the category to which you want to add the property.
- 6 Type the **Property Name** and **Property Value** in the text boxes.
- 7 Select **Add** from the **Action** drop-down list. This indicates that the property should be added to the device.
- 8 Click **OK**.

The task is added to the list in the Device Properties region. The property will be added to the device when the profile is deployed.

- 9 Click **Save** to save your changes.

Editing or Removing a Custom Property

You can edit or remove an existing custom property on a mobile device through a Mobile Device profile. Make changes to the property from the profile, then deploy the profile to the mobile device. You must know the name of the property in order to edit or remove it.

To edit or remove a custom property:

- 1 From the **Profiles** tab, select the Mobile Device profile you want to configure.
- 2 Click **Edit**.
- 3 Click the **Mobile Device Profile** tab.
- 4 In the Device Properties region, click **Add**.

The *Add Property* dialog box appears.

- 5 Select the **Category** to which the property belongs.
- 6 Type the **Name** of the existing property in the text box.
- 7 If you want to edit the value of the property, type the new value in the **Value** text box.
- 8 If you are editing the value of the property, select **Add** from the **Action** drop-down list. If you want to remove the property from the device, select **Remove** from the **Action** drop-down list.
- 9 Click **OK**.

The task is added to the list in the Device Properties region. The property will be edited when the profile is deployed to the mobile devices.

- 10 Click **Save** to save your changes.

Editing Registry Keys for Mobile Device Profiles

You can add registry keys to a Mobile Device profile. Once you add a registry key to the profile, you can add values for the key. You also have the option to edit or remove existing registry keys or values on the device. You must know the name and location of the key or value in order to edit or remove it.

This section contains information on the following tasks:

- Adding a Registry Key
- Adding a Value to a Registry Key
- Removing a Registry Key
- Editing or Removing a Registry Key Value

Adding a Registry Key

You can add registry keys to a Mobile Device profile. These keys will be added to the device when the profile is deployed to the mobile devices.

To add a registry key:

- 1 From the **Profiles** tab, select the Mobile Device profile you want to configure.
- 2 Click **Edit**.
- 3 Click the **Mobile Device Profile** tab.
- 4 In the Registry Settings region, select **Computer** and click **Add a new registry key**.

The *Add Registry Key* dialog box appears.

- 5 Select the **Parent Key** from the drop-down list.
- 6 Type the **Name** of the new key in the text box.
- 7 Select **Add** from the **Action** drop-down list.
- 8 Click **OK**.

The key is added to the profile and you can configure its value.

Adding a Value to a Registry Key

After you have created a registry key for a Mobile Device profile, you can add values to the key.

To add a value to an existing registry key:

- 1 From the **Profiles** tab, select the Mobile Device profile you want to configure.
- 2 Click **Edit**.
- 3 Click the **Mobile Device Profile** tab.
- 4 In the Registry Settings region, select the key to which you want to add a value and click **Add a new registry value**.

The *Add Registry Value* dialog box appears.

- 5 Type the **Name** of the new value in the text box.
- 6 Select the **Type** from the drop-down list.
- 7 Type the **Data** in the text box.
- 8 Select **Add** from the **Action** drop-down list.
- 9 Click **OK**.

The task is added to the list in the Registry Settings region. The value will be added when the profile is deployed to the mobile devices.

- 10 Click **Save** to save your changes.

Removing a Registry Key

You can remove an existing registry key on a mobile device through a Mobile Device profile. Make changes to the key from the profile, then deploy the profile to the mobile device. You must know the name of the key/value in order to remove it.

To remove a registry key:

- 1 From the **Profiles** tab, select the Mobile Device profile you want to configure.
- 2 Click **Edit**.
- 3 Click the **Mobile Device Profile** tab.

- 4 In the Registry Settings region, select **My Computer** and click **Add a new registry key**.

The *Add Registry Key* dialog box appears.

- 5 Select the **Parent Key** from the drop-down list.
- 6 Type the **Name** of the key in the text box.
- 7 Select **Remove** from the **Action** drop-down list.
- 8 Click **OK**.

The task is added to the list in the Registry Settings region. The key will be removed when the profile is deployed to the mobile devices.

- 9 Click **Save** to save your changes.

Editing or Removing a Registry Key Value

You can edit or remove an existing registry key value on a mobile device through a Mobile Device profile. Make changes to the key from the profile, then deploy the profile to the device. You must know the name of the key and value in order to edit or remove it.

NOTE In order to edit or remove a registry key value, you must add the registry key to the Mobile Device profile even if the key already exists on the device. For more information on adding a registry key, see *Adding a Registry Key* on page 135.

To edit or remove a registry key value:

- 1 From the **Profiles** tab, select the mobile device profile you want to configure.
- 2 Click **Edit**.
- 3 Click the **Mobile Device Profile** tab.
- 4 In the Registry Settings region, select the key for which you want to edit or remove a value and click **Add a new registry value**.

The *Add Registry Value* dialog box appears.

- 5 Type the **Name** of the existing value in the text box.

- 6 If you want to edit the **Type** or **Data** of the value, enter the appropriate information in the provided boxes.
- 7 If you are editing the value, select **Add** from the **Action** drop-down list. If you want to remove the value from the device, select **Remove** from the **Action** drop-down list.
- 8 Click **OK**.

The task is added to the list in the Registry Settings region. The value will be edited when the profile is deployed to the mobile devices.

- 9 Click **Save** to save your changes.

Configuring Mobile Device Profile Advanced Settings

You can configure GPS reporting, geofence areas, time zone settings and update restrictions for your mobile devices from a mobile device profile. This section includes the following topics:

- Location Based Services
- Geofence Areas
- Regional Settings
- Update Restrictions

Location Based Services

Location-based services allow you to manage GPS statistics collection when your mobile devices have GPS capabilities and a phone. You can configure the following options:

- **Enable location-based services.** Enables GPS reporting for devices using the selected mobile device profile.
- **Reporting interval.** Determines how often the device reports its GPS statistics to the Mobile Device Server.
- **Report location using cell towers.** Uses information from nearby cell towers to establish the location of the device.

- **Report location using GPS.** Uses GPS coordinates to establish the location of the device.
- **GPS acquisition timeout.** Determines how often the device checks its GPS coordinates.
- **Prompt user to initiate GPS acquisition.** Prompts the mobile device user to ask if Avalanche should be allowed to collect and report location-based data. This prompt will appear when the Enabler is launched.
- **Notify user after __ consecutive GPS failures.** Provides a notification to the mobile device user after the device has failed to acquire GPS coordinates the specified number of times.

To configure location-based services:

- 1 From the **Profiles** tab, select the mobile device profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Advanced Settings** tab, enable the desired options in the Location Based Services region.
- 4 Save your changes.

Geofence Areas

A geofence is a virtual perimeter defined by GPS coordinates. You can configure a geofence area for your mobile devices. When you configure a geofence area and define it as the Home area, Avalanche can generate an alert when devices report a GPS position that is outside of the defined area.

To configure a geofence area:

- 1 From the **Profiles** tab, select the mobile device profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Advanced Settings** tab, ensure that **Enable location-based services** is enabled.
- 4 Click **Add** in the Geofence Areas region.

The *Add Geofence Area* dialog box appears.

- 5 Type a name for the area in the **Name** text box.

- 6 If you want the area to be a home area, enable the **Is a Home Area** check box.
- 7 Enter the start and end latitude and longitude for the geofence. The start point should be the southwest corner of your area, and the end point should be the northeast.
- 8 Click **Select**.

The area is added to the list.

Regional Settings

You can set the region and time zone for your mobile devices from a mobile device profile.

To change the regional settings of a mobile device profile:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 From the **Advanced Settings** tab, use the drop-down lists in the Regional Settings area to select the region and time zone for your devices.
- 4 If you want to edit the time zone settings that load automatically when you select the time zone from the drop-down list, click **Edit Time Zone**.
- 5 If you want to revert to the time zone settings used on the local computer, click **Refresh Time Zone**.
- 6 Save your changes.

Update Restrictions

To allow you more control over bandwidth usage, Avalanche uses blackout windows. During a device-to-server blackout, the mobile devices are not allowed to communicate with a Mobile Device Server.

To create a blackout window:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 From the **Advanced Settings** tab, click **Add** in the Update Restrictions region.

The *Add Exclusion Window* dialog box appears.

- 4 Select the start and end time of the blackout window, and enable the boxes for the days you want the blackout to apply.

NOTE Blackout windows are scheduled using a 24-hour clock. If you create a window where the start time is later than the end time, the window will continue to the end time on the following day. For example, if you scheduled a window for 20:00 to 10:00 on Saturday, it would run from Saturday 20:00 until Sunday 10:00.

- 5 Click **OK**.
- 6 Save your changes.

Viewing Where Mobile Device Profiles are Applied

The **Applied To** tab in the **Profiles** tab allows you to see exactly which Server Locations and Sites to which a selected profile is directly applied. You cannot change this information from this tab. For information on how to assign your profiles to locations, refer to *Assigning Profiles* on page 59.

The **Applied To** tab displays the following information:

- **Parent Path.** The direct path back to the My Enterprise region.
- **Group.** The name of the Server Location or site where it is applied.
- **Selection Criteria.** Any selection criteria that is applicable where the profile is applied.

To view:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click the **Applied To** tab.

The tab displays the information for the selected profile.

Exporting Profiles for Configuring Enablers

You can export profiles from Avalanche to use when you are installing Enablers on mobile devices. Avalanche allows you to export a network profile, a mobile device profile, or both. After you have configured the profile, export it and save it to the computer from which you are installing the Enabler(s). Using an exported profile to configure the Enabler allows you to quickly and easily connect the device to the Mobile Device Server. For instructions on exporting profiles, see *Exporting Profiles for Configuring Enablers* on page 77.

Chapter 13: Managing Mobile Device Groups

To better organize your wireless network, you can use the Avalanche 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. Mobile device groups can include devices from the entire network, regardless of the location of the device. Each mobile device can be a member of multiple mobile device groups.

The topics in this chapter include:

- Creating Mobile Device Groups
- Viewing Devices in a Mobile Device Group
- Adding Mobile Device Group Authorized Users
- Pinging Mobile Devices within Mobile Device Groups
- Sending Messages to Mobile Device Groups
- Editing Properties for Mobile Device Groups
- Additional Mobile Device Group Functions

Creating Mobile Device Groups

Mobile device groups allow you to group devices together based on selection criteria you configure. You can create dynamic or static groups. In both group types, new devices 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.

- **Dynamic Mobile Device Groups.** When you create a dynamic group, you configure selection criteria to define which devices you want to belong to the group. Avalanche retrieves the devices currently listed in the Mobile Device Inventory list that match the selection criteria.

If a new device that matches the selection criteria for a dynamic mobile device group connects to the Avalanche Console, it is automatically placed in the mobile device group. Therefore, dynamic mobile device groups will continually add and remove mobile devices based on the selection criteria, without further management.

- **Static Mobile Device Groups.** When you create a static group, you configure selection criteria to define which devices you want to belong to the group. The devices currently in the Mobile Device Inventory that match the selection criteria are added to the group.

If a new device matching the selection criteria for a static mobile device group connects to the Avalanche Console, it will not automatically be placed in the mobile device group. You will need to manually add or delete devices if you want to modify the group. Refer to the following sections for managing static mobile device groups:

- Adding Devices to Static Mobile Device Groups
- Removing Devices from Static Mobile Device Groups

To create a mobile device group:

- 1 Select the **Device Groups** tab.
- 2 Click **Add Group**.

The *Create Device Group* dialog box appears.

- 3 Type a name for the group.
- 4 Select whether you want the group to be **Enabled** or **Disabled**.
- 5 Select whether you want the group to be **Static** or **Dynamic**.
- 6 Use the Selection Criteria Builder to create criteria to define the device group.
- 7 Click **OK**.

The group appears in the Device Groups List.

Adding Devices to Static Mobile Device Groups

If you have added mobile devices to your network, you can add those devices to a static mobile device group as long as they meet the group's selection criteria.

To add mobile devices to a static mobile device group:

- 1 Select the **Device Groups** tab.
- 2 Select the static mobile device group from the Device Groups List.

- 3 Click **Edit**.
- 4 In the Device Group Properties region, click **Add Matching Devices**.

Any devices in the current Mobile Device Inventory that match the selection criteria are added to the group.

- 5 Save your changes.

Removing Devices from Static Mobile Device Groups

If you want to make changes to a static mobile device group, you must first remove all current devices from the group. Next, modify the selection criteria as desired, and add the appropriate mobile devices back into the group. You cannot remove individual mobile devices from a static group.

Viewing Devices in a Mobile Device Group

The **Mobile Device Group** tab shows a set of mobile devices in the currently selected mobile device group. The following default information is provided for each mobile device:

Model Name	The model name of the mobile device.
Terminal ID	The unique ID automatically generated by Avalanche.
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.
Status	The client update status of the mobile device. A 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.
Last Contact	The date and time of the last contact the mobile device had with Avalanche.
Recent Activity	The status of a mobile device with respect to Avalanche. For example, when the mobile device receives new software, the activity status is Downloading .

You can also customize the columns in the device list to display according to your preference. For information on customizing the device list, see *Managing Device Inventory Displays* on page 35.

Adding Mobile Device Group Authorized Users

You can add authorized users for all mobile device groups or enable a user for a specific mobile device group.

To add an authorized user for a mobile device group:

- 1 From the **Device Groups** tab, click on the name of the device group you want to configure.
- 2 Click **Edit**.
- 3 Click **Authorized Users**.

The *Profile Authorized Users* dialog box appears.

- 4 Click **Add User**.

The *Add Authorized User* dialog box appears.

- 5 Add or remove authorized users as desired.
 - To add an authorized user, click **Add** in the Authorized Users region. Select the user and permission level from the drop-down lists and click **Save**.
 - To remove an authorized user, select the checkbox next to the user and click **Remove** at the top of the Authorized Users region.

The authorized users list is applied immediately.

Pinging Mobile Devices within Mobile Device Groups

You can use mobile device groups to ping a collection of mobile devices simultaneously. You can ping mobile devices that are currently in range and running the Avalanche Enabler, an Avalanche-enabled application, or in some cases a configuration utility.

NOTE 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 mobile devices within device groups:

- 1 Select the **Device Groups** tab.
- 2 Right-click the mobile device group you want to ping and select **Ping Devices** from the context menu.

The Recent Activity column in the Mobile Device List reports the status of the ping for each device in the group.

Sending Messages to Mobile Device Groups

You can send messages to the users of all mobile devices in a device group simultaneously.

To send messages to device groups:

- 1 Select the **Device Groups** tab.
- 2 Right-click the mobile device group you want to send a message to and select **Send Text Message** from the context menu.

The *Send Text Message: Group of Devices* dialog box appears.

- 3 Type a message in the **Text Message Field**.
- 4 Enable the **Provide Audible Notification** text box if you want a sound to play when the mobile device receives the message.
- 5 Click **OK**.

The Recent Activity column reports the status of the message for each device in the group.

Editing Properties for Mobile Device Groups

You can modify mobile device properties from a mobile device group. When you edit device properties for a group, the Console retrieves the common properties from all the devices in the group. You can then add, edit, and delete properties for the group.

All property changes made at this level will be applied on the mobile devices in the group.

NOTE Refer to *Building Selection Criteria* on page 161 for information on using properties in selection criteria.

To add a property to a mobile device group:

- 1 Select the **Device Groups** tab.
- 2 Right-click the mobile device group whose properties you want to edit and select **Edit Device Properties** from the context menu.

The *Edit Mobile Device Group Properties* dialog box appears.

- 3 Click **Add Property**.

The *Add Device Property* dialog box appears.

- 4 From the **Category** drop-down list, select **General** or **Custom** based on the property you are creating.
- 5 Enter the name of the property in the **Property Name** text box.
- 6 Enter the value of the property in the **Property Value** text box.
- 7 Click **OK**.

The new property is added to the properties list.

- 8 When you are finished adding properties, click **OK** to return to the Avalanche Console.

To edit a mobile device group property:

- 1 Select the **Device Groups** tab.
- 2 Right-click the mobile device group whose properties you want to edit and select **Edit Device Properties** from the context menu.

The *Edit Mobile Device Group Properties* dialog box appears.

- 3 Select the property that you want to edit and click **Edit Property**.

The *Edit Device Property* dialog box appears.

4 Type the new property value.

5 Click **OK**.

The edited property appears in the list.

6 Click **OK** to return to the Avalanche Console.

To delete a mobile device group property:

1 Right-click on a mobile device group and select **Edit Device Properties**.

The *Edit Mobile Device Group Properties* dialog box appears.

2 Select the property that you want to delete and click **Delete Property**.

3 Confirm that you want to delete the property.

The Pending Value column for the property displays the status of the property.

4 Click **OK** to remove the property and return to the Avalanche Console.

The property will be deleted after the next update.

Additional Mobile Device Group Functions

Mobile device groups include 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:

Enable/Disable	Allows you to enable or disable the group. When the group is disabled, any selection criteria using the group as a selection variable will return a “false” value.
Update Now	Allows you to update all mobile devices within that group immediately.
Clone Group	Clones the group and its settings.
Remove Group	Deletes the group from the Avalanche Console.

Chapter 14: Managing Alert Profiles

You can manage alerts in Avalanche using alert profiles. An alert profile gives you options for configuring what events generate an alert and who is notified when an alert is generated. Examples of what might generate an alert might be if a server goes offline or if a new mobile device is discovered.

This chapter provides information about the following topics:

- Managing Alert Profiles
- Adding Profiled Contacts
- Adding Profiled Proxies
- Deleting Proxies
- Alerts Tab

Managing Alert Profiles

Alert profiles can be configured according to what events you want to generate an alert and if alerts should be forwarded to a proxy or e-mail account. Multiple alert profiles can be assigned to the same portion of your network. A default alert profile is created when Avalanche is installed and is automatically applied to a Mobile Device Server. The default profile can be modified according to your preferences.

This section provides the following alert-related task information:

- Creating Alert Profiles
- Configuring Alert Profiles
- Alert Profile Authorized Users
- Viewing Where Alert Profiles Are Applied
- Removing Alert Profiles

Creating Alert Profiles

Alert profiles are configured with a list of events that will generate an alert. These profiles are then deployed to the Server Locations. When an event on the list occurs, an alert is generated and sent to the Avalanche Console.

To create an alert profile:

- 1 From the **Profiles** tab, click **Add Profile**.

The *Create Profile* dialog box appears.

- 2 Select **Alert Profile** from the drop-down list and type the name of the profile in the **Profile Name** text box.
- 3 Click **OK**.

The alert profile is created and can be enabled, configured, and assigned to a location.

Configuring Alert Profiles

Once you create an alert profile, you need to assign which events should generate an alert. You can also specify e-mail addresses or proxies to be notified when selected alerts are generated. For information about creating a contact list or a proxy pool, refer to *Adding Profiled Contacts* on page 154 and *Adding Profiled Proxies* on page 157.

To configure an alert profile:

- 1 From the **Profiles** tab, select the alert profile you want to configure.
- 2 Click **Edit**.
- 3 Select **Enabled** to enable the profile, if desired.
- 4 In the **Alert Profile** tab, click **Add** in the Profiled Alerts region.

The *Add Profiled Alerts* dialog box appears.

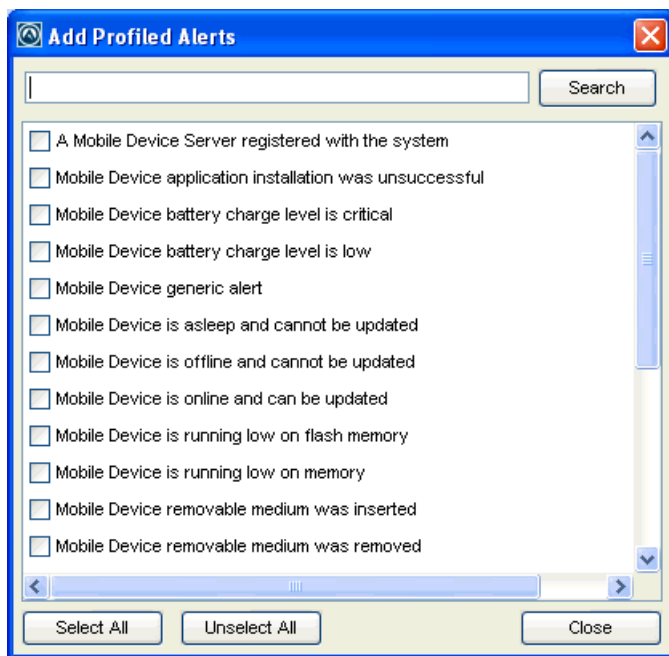


Figure 14-1. Add Profiled Alerts dialog box

- 5 From the list, select the events for which you want an alert to be generated. When you are finished, click **Close**.
- 6 If you want to forward alerts to an e-mail address or a proxy address:
 - If you want to receive an e-mail when an alert is generated, click **Add** in the Profiled Contacts region.

The *Contact Information* dialog box appears.

Enter the contact information and click **OK**. The contact will appear in the Profiled Contacts list.

NOTE You must configure the e-mail settings in the *Preferences* dialog box before Avalanche can e-mail you when alerts are generated. For information on configuring e-mail settings, see *Configuring E-mail Settings* on page 34.

- If you want to forward alerts to a proxy address, click **Add** in the Profiled Proxies region.

The *Proxy Address* dialog box appears.

Enter the proxy address and click **OK**. The address will appear in the Profiled Proxies list.

7 Save your changes.

Your alert profile will notify the server and any proxies or e-mail addresses when any of the selected events occur.

Alert Profile Authorized Users

You can add authorized users for all alert profiles or enable a user for a specific alert profile. For information on adding an authorized user, see *Managing User Accounts* on page 47.

Viewing Where Alert Profiles Are Applied

When you have selected an alert profile, the **Applied To** tab allows you to see exactly where the profile is applied. You cannot change of the information in this tab. For information on applying a profile, refer to *Assigning Profiles* on page 59.

The **Applied To** tab displays the following information:

- **Parent Path.** The direct path back to the My Enterprise region.
- **Group.** The name of the Server Location or site where the profile is applied.
- **Selection Criteria.** Any selection criteria that are applicable where the profile is applied.

To view where an alert profile is applied:

- 1 From the **Profiles** tab, select the alert profile you want to view.
- 2 Click the **Applied To** tab.

The tab displays the information for the selected profile.

Removing Alert Profiles

If you determine that an alert profile is unnecessary, you can delete it from the Avalanche Console. When you remove a profile from the Console, devices that are assigned to that profile retain those settings until you assign a new alert profile to the device.

To remove an alert profile:

- 1 From the **Profiles** tab, select the profile you want to remove and click **Remove Profile**.
- 2 Click **Yes** to confirm that you want to remove the profile.

The profile is removed from the Profiles List.

Adding Profiled Contacts

Each alert profile can notify one or more e-mail addresses when specified events occur. If you want the Avalanche Console to notify you of an alert by e-mail, you must add the e-mail address to the Profiled Contacts list for that profile. The entire contact list will receive e-mails for all alerts generated by that profile.

NOTE You must configure the e-mail settings in the *Preferences* dialog box before Avalanche can e-mail you when alerts are generated. For information on configuring e-mail settings, see *Configuring E-mail Settings* on page 34.

To add e-mail contacts to an alert profile:

- 1 On the **Profiles** tab, select the profile you want to configure from the Profile List.
- 2 Click **Edit**.
- 3 In the **Profiled Contacts** tab, click **Add**.

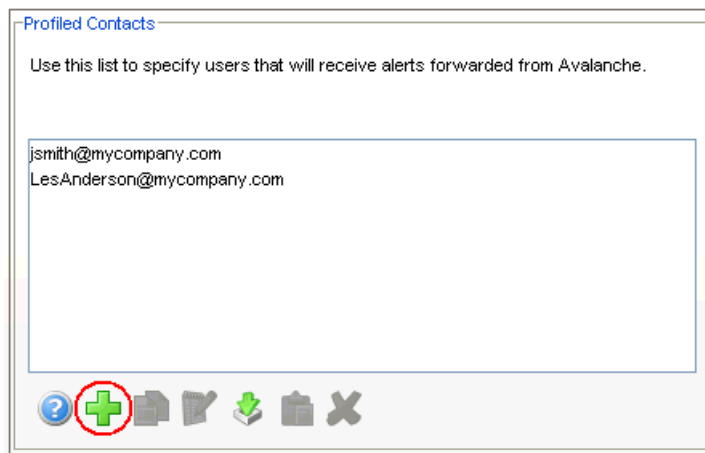


Figure 14-2. Add button in the Profiled Contacts region

The *Contact Information* dialog box appears.

- 4 Type the desired information in the provided text boxes. An e-mail address is required. When you are done, click **OK**.

The contact is displayed in the **Profiled Contacts** list box.

- 5 Repeat Step 4 until you are finished adding e-mail addresses.
- 6 Save your changes.

Importing E-mail Addresses

You can add e-mail addresses to the **Profiled Contacts** list of an alert profile by importing a comma-delimited `.csv` file (for example, one exported from Microsoft Outlook).

To import e-mail addresses:

- 1 On the **Profiles** tab, select the profile you want to configure from the Profile List.
- 2 Click **Edit**.
- 3 In the Profiled Contacts region, click **Import Contacts**.

An *Open* dialog box appears.

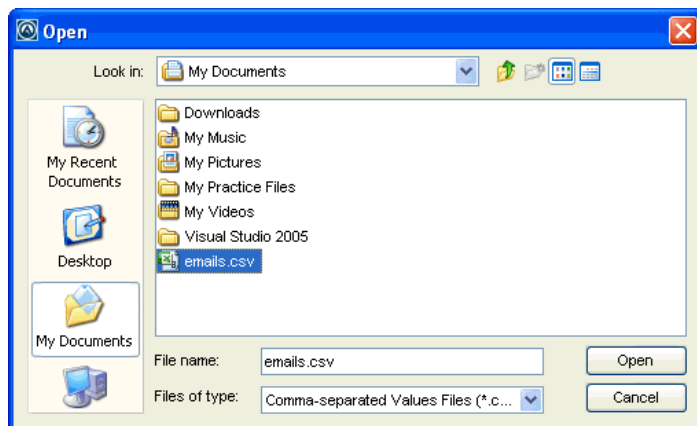


Figure 14-3. Open dialog box

- 4 Navigate to and select the `.csv` file that contains the e-mail addresses that you want to import.
- 5 Click **Open**.

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

- 6 Click **OK**.

The contacts display in the Profiled Contacts list.

Removing Contacts

You can delete e-mail addresses from the Profiled Contacts list when you no longer want to send alerts to those addresses.

To remove a contact from an alert profile:

- 1 On the **Profiles** tab, select the profile you want to configure from the Profile List.
- 2 Click **Edit**.
- 3 In the Profiled Contacts region, select the e-mail address you want to remove from the list.
- 4 Click **Remove**.
- 5 Confirm that you want to delete the e-mail address.

The e-mail address is removed from the list.

- 6 Save your changes.

Adding Profiled Proxies

The Avalanche Console allows you to set one or more proxies for an alert profile. When you add a proxy to a profile, the Console automatically forwards all alerts for that profile to the IP address of the proxy.

To add proxies to an alert profile:

- 1 On the **Profiles** tab, select the profile you want to configure from the Profile List.
- 2 Click **Edit**.
- 3 In the Profiled Proxies region, click **Add**.

The *Proxy Address* dialog box appears.

- 4 In the **Proxy Address** text box, enter the IP address and click **OK**.

The address appears in the **Profiled Proxies** list.

- 5 Repeat Steps 3 and 4 until you are finished adding proxy addresses.
- 6 Save your changes.

Deleting Proxies

If a proxy is no longer necessary, you can delete that proxy from the list.

To delete a proxy from an alert profile:

- 1 On the **Profiles** tab, select the profile you want to configure from the Profile List.
- 2 Click **Edit**.
- 3 In the Profiled Proxies region, select the IP address of the proxy from the list.
- 4 Click **Delete**.
- 5 Confirm that you want to delete the proxy.
- 6 Save your changes.

Alerts Tab

The **Alerts** tab provides a real-time view of the health of your wireless network. The Alert Browser is a table overview of the alerts that occur on your wireless network. It provides the following information about each alert:

Ack	Allows you to acknowledge that you have seen the alert. When you acknowledge an alert, the Server Location that sent the alert stops flashing in the Map pane.
Alert	Displays the type of alert.
Date	The time and date when the event occurred.
IP	Displays the IP address where the event occurred.
Description	Provides a brief description of the event.

This section provides information about the following tasks:

- Acknowledging Alerts
- Clearing Alerts
- Customizing Alert Browser Functionality

Acknowledging Alerts

When a new alert appears in the Alert Browser, you must acknowledge the alert before you can clear it from the list.

To acknowledge an alert:

- In the Alert Browser, enable the check box next to the alert you want to acknowledge.
- Or-
- To acknowledge all alerts in the list, click **Acknowledge All**.

Clearing Alerts

When the Alert Browser begins to fill with alerts, you may want to remove acknowledged alerts that are no longer relevant.

To clear alerts:

- 1 Acknowledge any alerts you want to clear by marking the check box next to the alert.
- 2 Click **Clear All**.

All acknowledged alerts will be removed from the list. Alerts that were not marked as acknowledged will remain in the Alert Browser.

Customizing Alert Browser Functionality

In the *Preferences* dialog box, you can configure the way the Alert Browser manages and displays alerts. You can configure the following settings:

- Number of days an alert is displayed in the Alert Browser.
- Maximum number of alerts that are listed in the Alert Browser.
- Maximum number of alerts to store. Alerts are stored in the database on the Enterprise Server.

To customize the Alert Browser functions:

- 1 Click **Tools > Preferences**.

The *Preferences* dialog box appears.

- 2 On the **General** tab in the Alert Browser Settings region, use the boxes to configure the alert settings.
- 3 Click **Apply** to save your changes.
- 4 Click **OK** to close the *Preferences* dialog box.

The Alert Browser will update to reflect your changes.

Chapter 15: Using Selection Criteria

Selection criteria are sets of rules which you can apply to individual software collections and individual network profiles. These criteria define which mobile devices will receive designated updates. For a software collection, the selection criteria determine which mobile devices can receive the software packages contained in the collection. For a network profile, the selection criteria determine which mobile devices can receive the settings contained in the profile.

Additional selection criteria are typically built into the software packages themselves, further restricting the distribution of the package. The built-in selection criteria associated with a particular software package are set by Wavelink or the third-party application developer and, once created, they 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 for flexible combination of multiple variables.

Additionally, if you want to set criteria but only want to match part of the expression you can use an asterisk [*] as a wildcard to represent single or multiple characters.

NOTE Asterisks are not allowed in property names or values because the symbol denotes a wildcard.

Selection criteria are compiled into internal formats that can be efficiently interpreted by the distributed servers. Most of the profile-related criteria also need to be translated into database SQL/HQL queries in order to build device inventories. The database interfaces used by Avalanche put a length limit on the generated SQL expressions which can be exceeded when selection criteria get too complex. Selection criteria containing more than 150 expressions have a good chance of exceeding database imposed limits.

To reduce the size and complexity of selection criteria, the user should make use of the range and wildcard capabilities built into the selection criteria language.

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 **Mobile Device Inventory** tab.

This section provides the following information:

- Building Selection Criteria
- Building Custom Properties
- Selection Variables
- Operators

Building Selection Criteria

You can access the Selection Criteria Builder from several different places in the Avalanche Console, including network profiles, software profiles, and mobile device groups. To access the Selection Criteria Builder, click the Selection Criteria button:



Figure 15-1. Selection Criteria button

NOTE Selection criteria also apply to software packages; however, you cannot edit software package selection criteria in Avalanche.

In the Selection Criteria Builder, 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 criterion variable.
- Operators such as 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 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 selection criteria:

- 1 Access the Selection Criteria Builder.

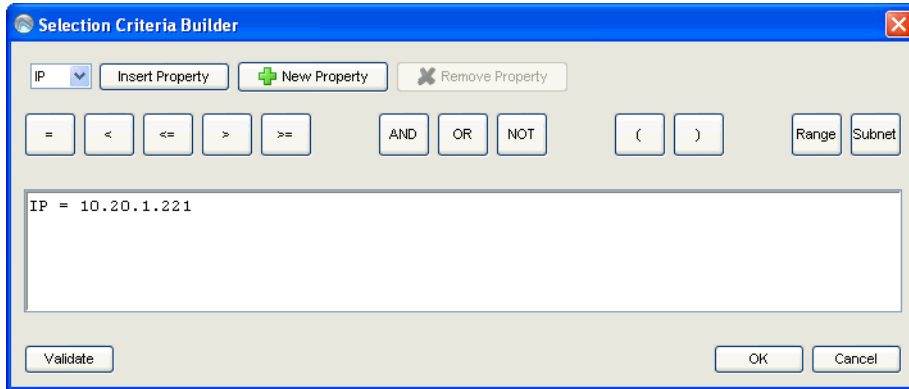


Figure 15-2. Selection Criteria Builder

- 2 From the drop-down list, select a property and click **Insert Property**.

NOTE For information about properties, see *Selection Variables* on page 163.

- 3 Select one of the operator buttons.

NOTE For more information about operators, see *Operators* on page 171.

- 4 Type a value for the source property that you selected.
- 5 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.

- 6 Click **Validate**.

The Selection Criteria Builder will indicate whether the selection criteria expression is valid.

- 7 Click **OK** to return to the Selection Criteria Builder.

- 8 Click **OK** to close the *Selection Criteria Builder* dialog box.

Building Custom Properties

You can build custom properties to use in your selection criteria.

To build custom properties:

- 1 From the Selection Criteria Builder, select **New Property**.

The *Add Custom Property* dialog box appears.

- 2 Enter the name for the custom property and click **OK**.

The new property is added to the drop-down list.

Selection Variables

Selection criteria are 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 string is valid:

```
Series = S
```

While the following are 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:

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

Example:

```
Columns > 20
```

EnablerVer Predefined Enabler version number.

Values with decimals must be surrounded by double quote marks.

```
EnablerVer = "3.10-13"
```

IP

IP address of the mobile device(s).

Enter all IP addresses using dot notation. IP addresses can be written 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. This is done by supplying the network number along with the subnet mask 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

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

KeyboardName

A value indicating 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

Last Contact

The parser for the LastContact property is unique because it not only allows specifying absolute time stamps, but also relative ones, forcing their constant reevaluation as the time-base changes.

Examples of time-stamp formats:

- mm/dd/yyyy

LastContact = "12/22/2005" (All day)

- HH:MM mm/dd/yyyy

LastContact = "23:15 12/22/2005" (All minute long, 24 hour notation)

- hh:mm AP mm/dd/yyyy

LastContact = "11:15 PM 12/22/2005"

- Also range-forms of the above

The relative format uses an offset from the current time.

- <offset>M

LastContact = 60M (60 minutes in the past)

- <offset>H

Last Contact = 1H (one hour in the past, the whole hour)

- <offset>D

Last Contact = 1D (one day in the past, the whole day)

- Also range-forms of the above

Special syntax allows inverted ranges from the range form to reduce the amount of confusion.

LastContact=7D-1M

MAC	<p>MAC address of the mobile device.</p> <p>Enter any MAC addresses as a string of hexadecimal digits. Dashes or colons between octets are optional. For example:</p> <pre>MAC = 00:A0:F8:85:E8:E3</pre>
ModelName	<p>The standard model name for a mobile device. This name is often a number but it can be alphanumeric. Examples include 6840, 3940, and 4040. If the model number is unknown, it might appear in one of the views when the mobile device is selected.</p> <p>A few of the supported values include:</p> <pre>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, ITCK30, ITC700</pre> <p>Example:</p> <pre>ModelName = 6840</pre>
ModelCode	<p>A number set by the device manufacturer and used internally by the BIOS to identify the hardware.</p> <p>Supported values include:</p> <pre>1 = LRT 38xx/LDT 2 = VRC39xx/69xx 3 = PDT 31xx/35xx 4 = WSS1000 5 = PDT 6800 6 = PDT 6100</pre> <p>Example:</p> <pre>ModelCode <= 2</pre> <p>This matches all 38xx, 39xx, and 69xx devices.</p>

OSVer	<p>Predefined property designated by the Enabler. Values with decimals in them must be surrounded by double quote marks.</p> <p>OSVer = "4.20"</p>
OS Type	<p>Predefined property designated by the Enabler.</p> <p>OSType = PocketPC</p>
Processor	<p>Predefined property designated by the Enabler.</p> <p>Processor = ARM</p>
ProcessorType	<p>Predefined property designated by the Enabler.</p> <p>ProcessorType = xScale</p>
Assigned IP	<p>IP address of the mobile device.</p> <p>Enter all IP addresses using dot notation. IP addresses can be written in three ways:</p> <ul style="list-style-type: none">• 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. This is done by supplying the network number along with the subnet mask 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

Series	<p>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.</p>
	<p>Supported values include:</p>
	<p>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</p>
	<p>Example:</p>
	<pre>Series = 3</pre>
Rows	<p>The number of display rows the mobile device supports. The possible value range is 1 to 25.</p>
	<p>Example:</p>
	<pre>(KeyboardName=35Key) & (Rows=20)</pre>
	<p>This example matches all mobile devices with 20 rows and 35-key keyboards.</p>
Syncmedium	<p>The type of synchronization medium for the mobile device to use.</p>
	<p>Supported values include:</p>
	<pre>any ip serial</pre>

Terminal ID The unique ID for the mobile device that Avalanche 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.

@exists Enables the user to check for the existence of a property. The @exists function name is case-sensitive and can only be used with an EQ or NE operator.

Example:

```
@exists ne some.property
```

```
@exists ==Some.property & Some.property =  
"value"
```

Operators

All selection criteria strings are evaluated from left to right, and precedence of operations is used when calculating the selection criteria. 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))
```

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 criterion, or you may use the letter abbreviation (NOT, AND, OR, etc.). If you use the letter abbreviation for the operator, then you must use uppercase letters. Spaces around

operators are optional, and you can use the wildcard [*] for left wildcard constants and right wildcard constants.

Operators use the following precedence:

- 1 Parentheses
- 2 OR operator
- 3 AND operator
- 4 NOT operator
- 5 All other operators

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

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

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

All mobile devices receive the software package except for those with both 20 rows and 35Key keyboards.

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.

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

6840 and 3840 mobile devices can receive the software package.

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
```

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 results in TRUE if the expression on the left is less than or equal to the expression on the right.

Example:

```
Rows <= 20
```

(*) Wildcard operator.

Wildcard expressions should be quoted and must be used with either an EQ or NE operator.

Keyboardname = "35*" - Tail is the wildcard

Keyboardname = "*35" - Head is the wildcard

Keyboardname = "*" - Entire constant is the wildcard

You can also use wildcards for IP addresses.

IP = 10.20.*.*

This would be equivalent to 10.20.0.0-10.20.255.255. A wildcard address must contain all four octets and can only be used with either the EQ or the NE operator.

Chapter 16: Using the Task Scheduler

The Task Scheduler enables you to schedule system backups, and allows you to restore a backup copy when necessary. This section provides information on the following tasks:

- Backing Up the System
- Restoring the System

Backing Up the System

This section provides information about using the Task Scheduler to backup the Avalanche system. When you are using a PostgreSQL database, Avalanche provides the capability to backup and restore all your Avalanche information. You should back up the system regularly. If for any reason Avalanche files are deleted or corrupted, you will be able to restore them from the backup files. When you back up Avalanche, the database information and software collections are both saved in a zip file.

NOTE If you are attempting to back up your system on a Linux operating system, Wavelink recommends you perform the back up manually.

To back up the system:

- 1 Click **Tools > Task Schedule**.

The *Task Schedule* dialog box appears.

- 2 Click **Add**.

The *Select A Task* dialog box appears.

- 3 Select **System Backup** from the **Task Type** drop-down list and click **Next**.

The *Create A System Backup* dialog box appears.

- 4 In the **Tag Name** text box, enter an identifier for the system backup and click **Next**. This tag is used to select the correct file when restoring the system. It is not the same as the name of the zip file.

The *Select Scheduling Options* dialog box appears.

- 5 Determine when the event will occur.
 - If you want the event to occur immediately, select the **Perform the task now** option.
 - If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.
 - If you want the event to occur on a regular basis, select the **Schedule a recurring event for the task** option.

6 Click **Next**.

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

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

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

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

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

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

9 Click **Next**.

The *Review Your Task* dialog box appears.

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

The *Task Scheduled* dialog box appears.

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

The task is added to the **Scheduled and Recurring Tasks** list. The task will run according to its schedule, and once it has completed, it will move to the **Completed Tasks** list.

Restoring the System

If you have created a system backup using the Task Scheduler, you can use the Task Scheduler to restore the information to Avalanche.

You cannot restore a system backup from a previous version of Avalanche. The backup version must match the Avalanche version. If you attempt to restore a system backup from a previous version of Avalanche, the restoration will fail.

NOTE If you are attempting to restore the system on a Linux operating system, Wavelink recommends you perform the restoration manually.

To restore the system:

1 Click **Tools > Task Schedule**.

The *Task Schedule* dialog box appears.

2 Click **Add**.

The *Select A Task* dialog box appears.

3 Select **Restore System** from the **Task Type** drop-down list and click **Next**.

The *Restore A System Backup* dialog box appears.

4 Select the system backup you wish to restore and click **Next**.

- Select **Restore the most recent system backup** to restore Avalanche to the latest backup file.
- Select **Restore by path** to specify the file name and path of the desired system backup.

NOTE The default file path is:

C:\Program Files\Wavelink\AvalancheSE\backup

- Select **Restore selected** to choose the desired system backup according to the tag name.

The *Review Your Task* dialog box appears.

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

The *Task Scheduled* dialog box appears.

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

The task is added to the **Scheduled and Recurring Tasks** list. The task will run according to its schedule, and once it has completed, it will move to the **Completed Tasks** list.

Appendix A: SSL Certificates

The Avalanche Web Console uses Hypertext Transfer Protocol (http) by default, which is not encrypted. If you want your information to be encrypted, you can configure Avalanche to use https with an SSL certificate instead.

If you intend to use Avalanche with an SSL certificate for a secure connection, you have the options of purchasing a certificate through a third-party Certificate Authority (such as Verisign), or creating a self-signed certificate.

NOTE If you create a self-signed certificate, web browsers will not initially recognize the certificate and will display warning messages that the site is not trusted. They may require you to make an exception in order to connect to the enterprise server. The connection will be encrypted, however.

This section contains instructions for the following tasks:

- Implementing a Certificate from a Certificate Authority
- Implementing a Self-Signed Certificate

Implementing a Certificate from a Certificate Authority

You can choose to use Avalanche with a certificate from a Certificate Authority. Note that the following instructions are based upon acquiring a certificate through the certificate authority, Verisign. The steps may vary somewhat when using another certificate authority vendor.

Wavelink strongly recommends that you backup the keystore file, the actual certificate file, the intermediate certificate, the certificate request, and the server.xml document after you have implemented your certificate. This would include the following files:

- amckeystore.keystore
- [your certificate].cer
- intermediateCA.cer
- certreq.csr
- server.xml

This section contains the following tasks for obtaining an SSL certificate from a certificate authority:

- Creating a Keystore
- Generating the Certificate Signing Request
- Importing an Intermediate Certificate
- Importing a Certificate
- Activating SSL for Tomcat
- Accessing the Web Console over a Secure Connection
- Troubleshooting

Creating a Keystore

To create a keystore for the certificate, use the `keytool.exe` utility. You will need to provide a Common Name (domain name), organizational unit, organization, city, state, and country code. You will also need to provide a keystore name and passwords for the keystore and alias. These are arbitrary, but should be noted for future reference.

To generate a keystore for the certificate:

- 1 From a command line, navigate to:
`[Avalanche installation directory]\JRE\Bin`
- 2 Use the command:
`keytool -genkey -alias amccert -keyalg RSA -keystore amckeystore.keystore`
- 3 At the prompt **Enter keystore password**, type the keystore password. When prompted, re-enter the password.
- 4 At the prompt **What is your first and last name**, type the Common Name.

NOTE The Common Name (domain name) you enter should be one that your company owns. Add a DNS entry if needed to resolve this computer to the Common Name.

- 5 At the prompts, enter your organizational unit, organization, city, state, and the country code.
- 6 When you are prompted to review your information, type `yes` to confirm that it is correct. If you type `no`, you will be guided through the prompts again.
- 7 At the prompt **Enter key password for <amccert>**, type a password to use for the alias. If you want to use the same password for the alias as you used for the keystore, press `Return`.

An example of generating a keystore:

```
Enter keystore password: avalanche
```

```
Re-enter new password: avalanche
```

```
What is your first and last name?
```

```
[Unknown]: avaself.wavelink.com
```

```
What is the name of your organizational unit?
```

```
[Unknown]: Engineering
```

```
What is the name of your organization?
```

```
[Unknown]: Wavelink Corporation
```

```
What is the name of your City or Locality?
```

```
[Unknown]: Midvale
```

```
What is the name of your State or Province?
```

```
[Unknown]: Utah
```

```
What is the two-letter country code for this unit?
```

```
[Unknown]: US
```

```
Is CN=avaself.wavelink.com, OU=Engineering, O=Wavelink Corporation,  
L=Midvale, ST=Utah, C=US correct?
```

```
[no]: yes
```

```
Enter key password for <amccert>
```

```
(RETURN if same as keystore password):
```

Generating the Certificate Signing Request

Once you have created the keystore, you can use the `keytool.exe` utility to generate a certificate signing request (`certreq.csr`) file to send to a certificate authority.

To generate a certificate signing request:

- 1 From a command line, navigate to:
`[Avalanche installation directory]\JRE\Bin`
- 2 Use the command:
`keytool -certreq -keyalg RSA -alias amccert -file certreq.csr
-keystore "C:\Program Files\Wavelink\AvalancheMC\JRE\bin\
amckeystore.keystore"`
- 3 Enter your keystore password.

When you apply to a certificate authority for an SSL web server certificate, you will need to submit the `certreq.csr` file. This file should be created in the `C:\Program Files\Wavelink\AvalancheMC\JRE\bin` folder.

Importing an Intermediate Certificate

When you acquire an intermediate certificate from your certificate authority, import it into the keystore. You may need to copy the contents of the intermediate certificate to a text editor and save the file as `intermediateCA.cer`. This file must be saved in the `[Avalanche installation directory]\JRE\bin` directory before you can import it.

To import an intermediate certificate:

- 1 From a command line, navigate to:
`[Avalanche installation directory]\JRE\bin`
- 2 Use the command:
`keytool -import -alias intermediateCA -keystore "[Avalanche
installation directory]\JRE\bin\amckeystore.keystore"
-trustcacerts -file intermediateCA.cer`

NOTE In this command, the filename `intermediateCA.cer` is used. If your intermediate certificate has a different name, use it instead.

- 3 Enter your keystore password.

The intermediate certificate is added to the keystore.

Importing a Certificate

Once you have received your certificate, you need to import it into the keystore. Your certificate will probably come as a file with the extension `.cer` or in the body of an e-mail. If it comes in the body of an e-mail, copy the contents to a text editor and save the file with a `.cer` extension. This file must be saved in the `[Avalanche installation directory]\JRE\bin` directory before you can import it.

To import a certificate:

- 1 From a command line, navigate to:
`[Avalanche installation directory]\JRE\bin`
- 2 Use the command:

```
-import -alias amccert -keystore "C:\Program  
Files\Wavelink\AvalancheMC\JRE\bin\amckeystore.keystore"  
-trustcacerts -file ava-wavelink-com.cer
```

NOTE As an example, `ava-wavelink-com.cer` is used as the filename. Replace this filename with the name of your certificate.

- 3 Enter your keystore password.

The certificate is added to the keystore.

Activating SSL for Tomcat

Once you have generated a certificate, you must activate SSL for Tomcat. You must modify the `server.xml` file and then restart the Tomcat server.

To activate SSL for Tomcat:

- 1 Navigate to
`[Avalanche Install location]\WebUtilities\tomcat\conf`
and open the `server.xml` file with a text editor such as Notepad.
- 2 Find

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"  
    maxThreads="150" scheme="https" secure="true"  
    clientAuth="false" sslProtocol="TLS" />
```
- 3 Remove the comment markers so that the section is not commented out.

4 Modify the section to contain the following information:

```
<Connector port="8443"
  protocol="org.apache.coyote.http11.Http11NioProtocol" SSLEnabled="true"
  maxThreads="150" scheme="https" secure="true" clientAuth="false"
  sslProtocol="TLS" keystoreFile="C:\Program Files\Wavelink\AvalancheMC\
  JRE\bin\amckeystore.keystore" keystorePass="[keypass]"/>
```

Where [keypass] is the keystore password you entered when creating the certificate. For the above example, this would be `avalanche`.

```
keystorePass="avalanche"
```

NOTE If you are not using port 443 for any other applications, you can change the connector port to 443. Changing the port to 443 will allow you to access the Web Console without entering the port within the URL.

5 Save your changes to the file.

6 Restart the Apache Tomcat for Wavelink service.

Accessing the Web Console over a Secure Connection

Once you have generated a certificate, activated SSL for Tomcat, and restarted the Tomcat server, you can access the Web Console over a https connection.

To access the Web Console over a secure connection:

- In the address field of your browser, type:

```
https://<Your Domain Name>:8443/AvalancheWeb
```

-Or-

- If you changed the connector port to 443, type:

```
https://<Your Domain Name>/AvalancheWeb
```

Troubleshooting

To troubleshoot issues connecting to the Apache Tomcat server using SSL after changes are made, go to

```
C:\Program Files\Wavelink\AvalancheMC\WebUtilities\Tomcat\logs
```

to find Catalina Tomcat logs.

NOTE You need to stop the Tomcat service to get all the log messages.

Example log file: `catalina.2010-02-24.log`

Implementing a Self-Signed Certificate

These instructions explain how to generate a self-signed certificate in the Apache Tomcat environment. If you choose not to use a Certificate Authority, you can still use a https connection to connect to the Web Console by creating your own certificate.

NOTE Internet browsers will not recognize a self-signed certificate as legitimate and will display warnings before allowing you access.

NOTE Wavelink strongly recommends backing up `server.xml` and `selfsignkeystore.keystore` when you have implemented a self-signed certificate.

This section contains the following tasks for implementing a self-signed certificate:

- Generating a Certificate
- Activating SSL for Tomcat
- Accessing the Web Console over a Secure Connection
- Troubleshooting

Generating a Certificate

To create a self-signed certificate, use the `keytool.exe` utility. You will need to provide a Common Name (domain name), organizational unit, organization, city, state, and country code when creating your certificate. You will also need to provide a keystore name and passwords for the keystore and alias. These are arbitrary, but should be noted for future reference.

To generate a self-signed certificate:

- 1 From a command line, navigate to:
`[Avalanche installation directory]\JRE\Bin`
- 2 Use the command:
`keytool -genkey -alias amcselfcert -keyalg RSA -keystore selfsignkeystore.keystore`
- 3 At the prompt **Enter keystore password**, type the keystore password. When prompted, re-enter the password.
- 4 At the prompt **What is your first and last name**, type the Common Name.

NOTE The Common Name (domain name) you enter should be one that your company owns. Use a DNS entry if needed to resolve this computer to the Common Name.

- 5 At the prompts, enter your organizational unit, organization, city, state, and the country code.
- 6 When you are prompted to review your information, type `yes` to confirm that it is correct. If you type `no`, you will be guided through the prompts again.
- 7 At the prompt **Enter key password for <amcselfcert>**, type a password to use for the alias. If you want to use the same password for the alias as you used for the keystore, press `Return`.

An example of generating a self-signed certificate:

```
Enter keystore password: avalanche
```

```
Re-enter new password: avalanche
```

```
What is your first and last name?  
[Unknown]: avaself.wavelink.com
```

```
What is the name of your organizational unit?  
[Unknown]: Engineering
```

```
What is the name of your organization?  
[Unknown]: Wavelink Corporation
```

```
What is the name of your City or Locality?  
[Unknown]: Midvale
```

What is the name of your State or Province?

[Unknown]: Utah

What is the two-letter country code for this unit?

[Unknown]: US

Is CN=avaself.wavelink.com, OU=Engineering, O=Wavelink Corporation, L=Midvale, ST=Utah, C=US correct?

[no]: yes

Enter key password for <amcselfcert>

(RETURN if same as keystore password):

Activating SSL for Tomcat

Once you have generated a certificate, you must activate SSL for Tomcat. You must modify the `server.xml` file and then restart the Tomcat server.

To activate SSL for Tomcat:

1 Navigate to

[Avalanche Install location]\WebUtilities\tomcat\conf
and open the `server.xml` file with a text editor such as Notepad.

2 Find

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
  maxThreads="150" scheme="https" secure="true"
  clientAuth="false" sslProtocol="TLS" />
```

3 Remove the comment markers so that the section is not commented out.

4 Modify the section to contain the following information:

```
<Connector port="8443"
  protocol="org.apache.coyote.http11.Http11NioProtocol"
  SSLEnabled="true" maxThreads="150" scheme="https"
  secure="true" clientAuth="false" sslProtocol="TLS"
  keystoreFile="C:\Program Files\Wavelink\AvalancheMC\
  JRE\bin\selfsignkeystore.keystore"
  keystorePass="[keypass]"/>
```

Where `[keypass]` is the keystore password you entered when creating the certificate. For the above example, this would be `avalanche`.

```
keystorePass="avalanche"
```

NOTE If you are not using port 443 for any other applications, you can change the connector port to 443. Changing the port to 443 will allow you to access the Web Console without entering the port within the URL.

- 5 Save your changes to the file.
- 6 Restart the Apache Tomcat for Wavelink service.

Accessing the Web Console over a Secure Connection

Once you have generated a certificate, activated SSL for Tomcat, and restarted the Tomcat server, you can access the Web Console over a https connection.

To access the Web Console over a secure connection:

- In the address field of your browser, type:

```
https://<Your Domain Name>:8443/AvalancheWeb
```

-Or-

- If you changed the connector port to 443, type:

```
https://<Your Domain Name>/AvalancheWeb
```

Troubleshooting

To troubleshoot issues connecting to the Apache Tomcat server using SSL after changes are made, go to

```
C:\Program Files\Wavelink\AvalancheMC\WebUtilities\Tomcat\logs
```

to find Catalina Tomcat logs.

NOTE You need to stop the Tomcat service to get all the log messages.

Example log file: `catalina.2010-02-24.log`

Appendix B: Avalanche Services

This appendix lists all of the Avalanche services. Under each service title, you'll find the file path where the service is located and which type of server (Enterprise Server, Statistics Server or Mobile Device Server) uses the service.

Wavelink Authentication Service

C:\Program Files\Wavelink\AvalancheMC\CESecureServer.exe

Enterprise Server

Apache Tomcat

C:\Program Files\Wavelink\AvalancheMC\WebUtilities\Tomcat\bin\tomcat6.exe

Enterprise Server

Wavelink Alerts

C:\Program Files\Wavelink\MM\Program\AlertSvc.exe

Mobile Device Server

Wavelink Avalanche Service Manager

C:\Program Files\Wavelink\Avalanche\Service\WLAmcServiceManager.exe

Mobile Device Server

Wavelink Avalanche Agent

C:\Program Files\Wavelink\Avalanche\Service\WLAvalancheService.exe

Mobile Device Server

Wavelink Avalanche Enterprise Server

C:\Program Files\Wavelink\AvalancheMC\eserver.exe

Enterprise Server

Wavelink Information Router

C:\Program Files\Wavelink\AvalancheMC\WLInfoRailService.exe

Enterprise Server

Wavelink License Server

C:\Program Files\Wavelink\AvalancheMC\WLLicenseService.exe

Enterprise Server

Wavelink Stat Server Enterprise

C:\Program Files\Wavelink\AvalancheMC\StatServer.exe

Stats Server

Wavelink Deployment

C:\Program Files\Wavelink\AvalancheMC\iserv.exe

Enterprise Server

Appendix C: Port Information

This appendix provides information about the ports used in Avalanche SE. The information provided includes:

- Database Ports
- Enterprise Server Ports
- Mobile Device Server Ports
- Wavelink Products Used with Avalanche

NOTE Except where noted, the ports listed are all inbound ports.

Database Ports

When Avalanche is installed with the default database (PostgreSQL), the default port for database communication is 5432.

Enterprise Server Ports

The following table provides a list of ports that the Enterprise Server uses.

Port	Description	Port Type
5002	Wavelink Authentication Service	TCP
7221	Avalanche License Server	TCP
7225	InfoRail Service	TCP
7226	InfoRail Service IR-to-IR router port	TCP
8009	Tomcat AJP for integrating with Apache httpd	TCP
8080	Tomcat HTTP	TCP

NOTE The Enterprise Server also listens on 8443 for a Tomcat connection with an SSL certificate. You can change this to 443 in the `server.xml` file if no other program is using 443.

Mobile Device Server Ports

The following table provides a list of the ports that the Mobile Device Server uses.

Port	Description	Port Type
1777	Protocol Service	TCP/UDP
1778	Services persistent connections to mobile devices	TCP

Wavelink Products Used with Avalanche

The following table provides a list of the ports that are used by Wavelink products often used in conjunction with Avalanche.

Port	Product	Port Type
1899	Remote Control	TCP
1900	Remote Control	TCP
5001	CE Secure	TCP

Appendix D: Wavelink Contact Information

If you have comments or questions regarding this product, please contact Wavelink Customer Service.

E-mail Wavelink Customer Support at: CustomerService@wavelink.com

For customers within North America and Canada, call the Wavelink Technical Support line at 801-316-9000 (option 2) or 888-699-9283.

For international customers, call the international Wavelink Technical Support line at +800 9283 5465.

For Europe, Middle East, and Africa, hours are 9 AM - 5 PM GMT.

For all other customers, hours are 7 AM - 7 PM MST.

Glossary

ActiveSync	A synchronization program developed by Microsoft. It allows a mobile device synchronize with the machine running Avalanche.
Administrator User Accounts	Users assigned as Administrator Accounts have unlimited permissions, and can assign and change permissions for Normal user accounts.
Alert Profile	A collection of traits that define a response to a specific network or statistical alert. Typically, an alert profile consists of the alerts being monitored and either an e-mail address or proxy computer to which the alert is forwarded.
Authorized Users	Authorized users are users that have permission to access assigned areas of the Console and the ability to perform certain tasks. Administrator users have access to all areas and tasks in their Home region; Normal users must be assigned to specific areas or tasks in order to view or perform them.
Avalanche Console	The Avalanche Console is the graphical user interface (GUI) where you manage your Servers, profiles and devices. The Java Console must be installed on a computer, but the Web Console can be accessed from any Web browser that can connect to your enterprise server.
Blackout Window	A period of time when the Mobile Device Servers are not allow to contact the Enterprise Server, eliminating heavy bandwidth and allowing control the flow of device connections to the Enterprise Server.

CE Secure	A Wavelink plug-in that provides advanced user authentication and security on Windows CE mobile devices.
Client	A mobile device with an installed Avalanche Enabler. The Enabler allows the client to communicate with a Server and to be configured and managed through Avalanche.
Default Profile	A profile that the Servers automatically assign to mobile devices. The Servers apply these default profiles to any devices discovered that are not assigned to a profile.
Device Filters	Device filters allow you to display specific mobile devices in the Mobile Device Inventory based on selection criteria.
DHCP	Dynamic Host Configuration Protocol. An IP service that allows DHCP clients to automatically obtain IP parameters from a DHCP server.
DNS	Domain Name System. A service that provides hostname-to-IP address mapping.
Enabler	The software installed on a mobile device that allows Avalanche to manage it.
Enterprise Server	The Enterprise Server is the service that manages communication and collaboration between the components of Avalanche.
Epochs	An epoch consists of a collection of network settings and configured times in which the settings for a network profile changes. Epochs can be created for each configured network profile. Most network profile settings can be managed by Epochs.

ESSID	Extended Service Set ID. The identifier of an extended service set for devices that are participating in an infrastructure mode wireless LAN.
Exclusion Windows	Exclusion Windows are scheduled periods of time when your mobile devices are not authorized to contact the Mobile Device Server to conserve bandwidth and increase compliance for critical software updates. Exclusion Windows are configured through Mobile Device Server profiles.
Filters	Device filters allow you to display specific devices in the Inventory based on selection criteria.
Geofence	A virtual perimeter defined by GPS coordinates. When a mobile device that is assigned a geofence area leaves that area, Avalanche will display an alert.
Home Region	Each user must be assigned a home region. He will only be allowed to access information for his home region and any associated sub-regions or locations.
Java Console	The Console is the graphical user interface (GUI) where you manage your Servers, profiles and devices. The Java Console must be installed on a computer. See also Web Console.
Mobile Device	A hand-held or vehicle-mounted device, such as a scan gun or PDA, that travels with a user as he conducts daily operations.
Mobile Device Server	The Mobile Device Server consists of server side software packages that facilitate communication between the mobile devices and the Enterprise Server.
Mobile Device Server Profile	Mobile Device Server profiles allow you to define device configuration settings for the mobile device Server.

Mobile Device Groups	A mobile device group consists of mobile devices with similar characteristics. These groups are defined by selection criteria.
Network Profile	A collection of settings that allow you to download network parameters such as IP addresses, the ESSID, and encryption and authentication settings to devices over a serial or wireless connection.
Normal User Accounts	Users assigned as Normal users do not have access to any component of Avalanche until assigned permissions.
Orphan Packages	A software package that has been deployed to a client through Avalanche, but has been disabled or is not recognized by the Server. You must orphan a software package before you can use Avalanche to delete it from the client.
Ping	An IP service that is used to test IP connectivity. Part of the ICMP service.
Profile	A collection of configuration settings that can be applied to multiple regions/ locations simultaneously.
Ports	Typically used to map data to a particular process running on a computer.
PostgreSQL	A powerful, open source relational database system packaged with Avalanche.
Profile Permissions	Provide global access to each profile you are given permission for. Does not allow permission to apply the profiles to any regions until you are assigned Regional Permissions for a region.

Regional Permissions	Provide access to specific to regions. To have full permissions at a region, a user must be assigned the Regional Permission in the User Management dialog box and then be assigned as an Authorized User to the specific region. See Authorized User.
Remote Control	A Wavelink plug-in that allows you to remotely view and perform tasks on mobile devices.
Scan to Configure	The ability to configure barcode profiles that contain network profile settings. You can then print the profiles as barcodes and scan the barcodes with a mobile device with an Enabler version 3.5 or later. The Enabler configures the network settings on the mobile device.
Secondary Servers	If configured and assigned, secondary servers allow mobile devices to attempt to connect to a secondary Mobile Device Server if the primary server is not available.
Selection Criteria	Parameters that can be used for filters, profile or package management, or device group definition.
Selection Variables	The basis for selection criteria. In some cases, selection variables are mobile device properties.
Software Packages	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 Console.
Software Profiles	A logical grouping of software packages maintained and managed by the Avalanche.

SSID	Service Set Identifier. A unique name, up to 32 characters long, that is used to identify a wireless LAN. The SSID is attached to wireless packets and acts as a password to connect to a specific LAN.
Task Scheduler	The Task Scheduler provides the means to deploy Servers, send updates, and perform system backups.
Telnet	A TCP/IP utility used for terminal emulation, which allows a client to connect and interact with a remote host system.
Terminal ID	The identification number of a specific (physical) terminal or workstation on the network.
User Account	A login name and password used by an individual to access the Console. A user can have Administrator or Normal permissions.
Web Console	The Avalanche Console is the graphical user interface (GUI) where you manage your Servers, profiles and devices. The Web Console can be accessed from any Web browser that can connect to your enterprise server and allows you to manage and view reports and floorplans.
WEP	Wired Equivalent Privacy. An encryption standard for wireless networks that provides the equivalent security of a wired connection for wireless transmissions.

Index

A

- activating Avalanche
 - automatically 16
 - demo mode 19
- alerts
 - acknowledging 158
 - clearing 158
 - configuring profiles 151
 - contact list 154
 - managing 150
 - proxy pools 157
- assigning profiles 59
- authorized users 55
- Avalanche
 - components 7
 - Console settings 30
 - installing 12
 - overview 9
 - restoring 177
 - services 189
- Avalanche Console
 - customizing 29
 - starting 22

B

- backing up Avalanche 175
- backlogs 40
- backup drive location 33
- backups, performing 175
- barcode profiles
 - adding 80
 - configuring 79
 - custom properties 81
 - editing 86
 - network settings 80
- barcodes
 - printing 86
 - scanning 87

- blackout periods, Enterprise Server 40
- building selection criteria 161

C

- chat timeout 94
- Communicator 130
- components of Avalanche 7
- contact information 193
- contact list
 - creating 154
 - importing addresses 155
 - removing addresses 156
- creating
 - custom properties 121
 - mobile device groups 143
 - user accounts 48
- custom properties, selection criteria 163

D

- default login 23
- delayed software package installation 113
- demo mode 19
- dump heap 42

E

- Enabler Installation Tool 45
- encryption 71
- Enterprise Server
 - backlogs 40
 - blackout periods 40
 - configurations 40
 - dump heap 42
 - purging server statistics 41
 - status 40
- export profiles 77

G

- GPS reporting 94

H

HTTP proxy connection 35

I

InfoRail status 42

installing

 Avalanche 12

 software packages 107

IP address pools 68

L

LDAP 56

License Server 15

licenses 14

 overview 14

 releasing 20

 running the License Server 15

location management 9

login, default 23

M

Mobile Device Details dialog box 119

mobile device groups 143

 adding properties 147

 additional functions 149

 creating 143

 pinging 146

 sending messages to 147

Mobile Device Inventory tab

 custom properties 36

 device filters 36

 modifying columns 38

 removing columns 39

mobile device profiles 131

mobile device server

 license options 93

 licensing messages 100

 reinitializing 101

mobile device server profiles

 authentication 91

mobile devices

 caching 94

 contacting 124

 creating custom properties 121

 deleting properties 123

 details 119

 device filters 36

 device-side properties 122

 editing properties 123

 GPS reporting 94

 installed software tab 130

 locating 126

 location history 127

 pinging 124

 properties 120

 Remote Control 128

 sending messages 125

 server profile settings 94

 session monitor 128

 updating 99, 125

 viewing properties 121

Mobile Manager Enterprise, removing 12

modifying

 mobile device columns 38

 Server Location properties 63

N

navigation window 25

network profile

 scheduled settings 69

 WLAN IP settings 70

 WLAN settings 71

 WWAN settings 75

network profiles 66

 configuring 67

 creating 66

 enabling 67

 IP address pools 68

O

overview 9

P

password

 default 23

 user accounts 56

peer-to-peer package distribution 115

permissions

 profile 53

 regional 51

 user accounts 51

pinging mobile devices 124, 146

pinging sites 61

ports 191

 database 191

 enterprise server 191

 Mobile Device Server 192

profile permissions 53

properties

 custom 121

 deleting 123

 editing 123

 mobile device groups 147

 mobile devices 120

proxies 157

purging server statistics 41

R

regional permissions 51

regions 9

reinitializing the Mobile Device Server 65

releasing licenses 20

Remote Control 128

removing

 columns 39

 user accounts 57

restoring Avalanche 177

S

scan to configure 79

 barcode profiles 79

 creating custom properties 81

 printing barcodes 86

 scanning barcodes 87

scheduled settings 69

selection criteria

 building 161

 custom properties 163

selection variables

 Assigned IP 169

 Columns 164

 EnablerVer 164

 IP 165

 KeyboardCode 165

 KeyboardName 166

 LastContact 167

 MAC 168

 ModelCode 168

 ModelName 168

 OSType 169

 OSVer 167, 169

 Processor 169

 ProcessorType 169

 Rows 170

 Series 170

 Terminal ID 171

sending messages 147

Server

 properties 65

 starting 63

 stopping 63

Server Locations 9

services, Avalanche 189

session monitor 128

sites 58

 editing properties 62

 pinging clients 61

- sending messages to 61
- software inventory 130
- software packages
 - configuring 112
 - copying 112
 - delayed installation 113
 - enabling 112
 - installing 107
 - peer-to-peer distribution 115
- software profiles
 - adding 102
 - applying 105
 - editing 104
 - enabling 104
 - managing 102
- SSID 71
- starting the Avalanche Console 22
- static mobile device groups
 - adding devices 144
 - removing devices 145
- Support Generator 43
- syntactical symbols
 - And (&) 172
 - Eq (=,=) 173
 - Not (!) 172, 174
 - Or (|) 172

T

- task scheduler 175

U

- uninstalling servers 175
- user accounts 47
 - authorized users 55
 - creating 48
 - creating groups 50
 - enabling domain validation 55
- LDAP 56
 - password 56
 - permissions 51

- removing 57
- user groups 50

W

- Wavelink contact information 193
- WLAN IP settings 70
- WLAN settings 71
- WWAN settings 75