



Wavelink Avalanche Mobility Center
Java Console User Guide

Version 5.0

amcj-ug-50-20100520

Revised 20/5/2010

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	10
About This Document	10
Managing Networks with Avalanche	11
Components of Avalanche	12
Location Management: Server Locations and Regions	13
Mobile Manager	13
Getting Started	14
Chapter 2: Installing Avalanche	16
Which Version of Avalanche Should I Install?	16
Installing Avalanche Mobility Center	17
Installing Avalanche Console Only	18
Installing Avalanche with External Databases	19
Before You Begin (PostgreSQL)	20
Before You Begin (SQL Server)	20
Before You Begin (Oracle)	21
Completing an External Database Installation	21
Uninstalling Avalanche	23
Chapter 3: Licensing	25
Overview of Wavelink Licensing	25
Types of Licenses	26
Base and Maintenance Licenses	26
Infrastructure and Mobile Device Licenses	26
Unlicensed Devices	26
Running the License Server	27
Activating Licenses	27
Activating Avalanche Licenses	27
Activating Automatically	28
Activating Manually	29
Importing a License	30
Activating Demo Mode	31
Activating Licenses for Wavelink Products	32
Releasing Licenses	32
Importing the Enterprise License	33
Chapter 4: Avalanche Console	34
Launching the Avalanche Console	35
Understanding the Avalanche Console	36
Tool Bar	37
Navigation Window	37
Quick Start Tab	38
Server Configuration	38

Profiles Configuration	39
Tools	39
Help and Support	39
Profiles Tab	39
Understanding Edit Mode	41
Changing Console Preferences	42
Customizing General Console Settings	43
Configuring Deployment Settings	44
Edit Lock Control	46
Configuring Audit Logging	46
Viewing the Audit Log	48
Specifying the Backup Drive Location	49
Configuring E-mail Settings	49
Configuring HTTP Proxy Settings	50
Customizing Map Options	51
Managing the Enterprise Server	51
Configuring Server Blackout Periods	52
Using an Enterprise Server Blackout	52
Performing a Batch Release	53
Throttling Distributed Servers	54
Viewing the Enterprise Server Status	54
Controlling the Enterprise Server Message Backlogs	55
Limiting Distributed Server Connections	56
Purging Server Statistics	57
Performing a Dump Heap	58
Viewing the Inforail Status	59
Using the Support Generator	60
Using the Enabler Installation Tool	61
Chapter 5: Managing User Accounts	64
Defining Permission Types	64
Creating User Accounts	65
Creating User Groups	68
Assigning User Permissions	69
Regional Permissions	69
Profile Permissions	71
Assigning Authorized Users	73
Assigning Authorized Users to Regions	73
Assigning Authorized Users to Profiles	74
Configuring Integrated Logon	75
Changing Passwords	76
Removing User Accounts	77
Chapter 6: Managing Regions and Locations	78
General Overview	79
Managing Regions	80

Creating Regions	80
Creating Nested Regions	81
Viewing Region Properties	81
Assigning Profiles	81
Deleting Regions	83
Managing Server Locations	83
Determining Server Placement	84
Centralized Server Method	85
Distributed Server Method	86
Adding Server Locations	87
Understanding Unassigned Server Locations	89
Moving Server Locations to Regions	90
Modifying Server Location Properties	90
Assigning Profiles to Server Locations	91
Deleting Server Locations	91
Removing Server Locations	92
Restoring Server Locations	92
Managing Sites	93
Creating a Site	93
Viewing Mobile Devices Within Sites	94
Pinging Mobile Devices within Sites	94
Sending Messages to Sites	94
Editing Site Properties	95
Assigning Profiles to Sites	96
Additional Site Functions	96
Editing Exclusions	96
Managing Servers	98
Building Server Deployment Packages	98
Server Auto-Discovery	100
Stopping Servers	100
Starting Servers	100
Viewing Server Properties	100
Reinitializing the Mobile Device Server	101
Monitoring Server Status	101
Retrieving Mobile Device Log Files	102
Configuring Infrastructure Servers at Server Locations	103
Infrastructure Site Console and the Avalanche Console	103
Chapter 7: Managing Network Profiles	105
Creating Network Profiles	105
Configuring Network Profiles	106
Configuring Network Profile General Settings	106
Enabling Network Profiles	106
Managing IP Address Pools	107
Adding Authorized Users	108
Configuring Selection Criteria	109

Configuring Scheduled Settings	109
Configuring WLAN IP Settings	111
Configuring WLAN Settings	112
Configuring WWAN Settings	117
Applying Network Profiles	118
Viewing Where Network Profiles are Applied	119
Chapter 8: Managing Scan to Configure Profiles	120
Configuring Scan to Config Profiles	120
Adding Scan to Config Profiles	121
Configuring Settings	121
Adding Scan to Config Profile Authorized Users	122
Editing Custom Properties	124
Adding a Custom Property	124
Editing or Removing a Custom Property	125
Editing Registry Keys	125
Adding a Registry Key	126
Adding a Value to a Registry Key	126
Removing a Registry Key	127
Editing or Removing a Registry Key Value	128
Applying Scan to Config Profiles	129
Printing Barcodes	129
Scanning Barcodes	130
Chapter 9: Managing Infrastructure Distributed Servers	132
Creating Infrastructure Server Profiles	133
Configuring Infrastructure Server Settings	133
Enabling an Infrastructure Server Profile	133
Configuring Data Collection	134
Infrastructure Server Profile Authorized Users	135
Defining Device Access Privileges	136
Defining Access Privileges	138
Configuring SNMP V3 Settings	139
Cisco IOS Access Privileges	140
Replacing Insecure Protocols and Default Passwords	142
Configuring Infrastructure Server Blackouts	144
Viewing Where Infrastructure Server Profiles Are Applied	144
Applying Infrastructure Server Profiles to Regions	145
Removing an Infrastructure Server Profile	145
Viewing Infrastructure Server Licensing Messages	146
Chapter 10: Managing Infrastructure Profiles	147
Creating Infrastructure Profiles	148
Configuring Infrastructure Profiles	149
Infrastructure General Settings	149
Editing Advanced Properties	150

Assigning Infrastructure Profile Authorized Users	151
Configuring Infrastructure Selection Criteria	152
Configuring Infrastructure Scheduled Events	152
Configuring WLANs	154
Applying Infrastructure Profiles	156
Viewing Where Infrastructure Profiles Are Applied	156
Importing an Infrastructure Device Support File	157
Adding Custom Properties	158
Updating Infrastructure Device Firmware	159
Types of Firmware Support	159
Full Support Mode	160
Compatibility Mode	160
Supported Firmware	161
Importing Firmware	161
Manually Adding Firmware	164
Creating Firmware Packages	164
Deploying Firmware Packages	166
Setting a Default Profile for Specific Hardware	166

Chapter 11: Managing Infrastructure Devices **168**

Managing Device Filters	168
Creating Device Filters	168
Applying Device Filters	169
Filter View By Type	169
Displaying Devices	170
Tasks from the Device View	170
Querying the Device	172
Pinging the Device	172
Resetting Access Points	172
Changing Access Point Firmware	174
Connecting by Web Browser or Telnet	175
Deleting Devices	175
Viewing Composite Profiles	176
Viewing Advanced Properties	177
Viewing Related Devices	178

Chapter 12: Managing Very Large Access Control Lists **179**

Why Should I Create a Very Large Access Control List?	180
Adding Very Large Access Control List Entries	180
Modifying Very Large Access Control List Entries	181
Removing Very Large Access Control List Entries	181
Exporting and Importing a Very Large Access Control List	182
Exporting a VLACL	182
Importing a VLACL	182
Deploying the Very Large Access Control List	183

Chapter 13: Managing Mobile Device Distributed Servers	184
Creating Mobile Device Server Profiles	185
Configuring Mobile Device Server Profile Settings	185
Enabling Mobile Device Server Profiles	186
Mobile Device Server Security	186
Mobile Device Server Resources	188
Logging	188
Reserved Serial Ports	189
Terminal IDs	189
Configuring Mobile Device Server Resources	190
Mobile Device Server License Options	190
Mobile Device Server Profile Authorized Users	191
Mobile Device Settings on the Server Profile	192
Secondary Mobile Device Servers	193
Configuring Mobile Device Server Blackouts and Updates	195
Configuring Blackouts	195
Restricting Simultaneous Device Updates	196
Scheduling Profile-Specific Device Updates	197
Viewing Where Mobile Device Server Profiles Are Applied	199
Removing Mobile Device Server Profiles	199
Assigning Mobile Device Server Profiles to Regions	200
Viewing Mobile Device Server Licensing Messages	200
Reinitializing the Mobile Device Server	200
Chapter 14: Managing Software Profiles	201
Configuring Software Profiles	201
Adding Software Profiles	201
Adding Software Profiles from the Quick Start Tab	202
Editing Software Profiles	203
Enabling Software Profiles	203
Software Profile Authorized Users	204
Software Profile Selection Criteria	205
Applying Software Profiles	205
Viewing Where Software Profiles Are Applied	205
Managing Software Packages	206
Adding Software Packages	208
Building New Software Packages	210
Installing CAB or MSI Packages	212
Copying Software Packages	213
Enabling Software Packages	213
Configuring Software Packages with a Utility	214
Configuring Software Packages for Delayed Installation	214
Peer-to-Peer Package Distribution	216
Chapter 15: Managing Mobile Devices	219
Mobile Device Inventory Tab	219

Inventory Paging	220
Displaying Custom Mobile Device Icons	221
Deleting Mobile Devices	221
Modifying Columns	221
Adding Custom Columns	222
Reorganizing Columns	223
Managing Device Filters	223
Creating Device Filters	224
Applying Device Filters	225
Deleting Device Filters	225
Viewing Mobile Device Details	225
Configuring Mobile Device Properties	227
Viewing Properties	227
Creating Custom Properties	228
Creating Device-Side Properties	229
Editing Properties	229
Deleting Properties	230
Contacting the Mobile Device	230
Pinging Mobile Devices	231
Sending Messages	231
Updating a Mobile Device	232
Locating a Mobile Device	233
Viewing Location History	233
Using Remote Control	234
Launching the Session Monitor	235
Launching Wavelink Communicator	236
Software Inventory	237
Mobile Device Profiles	237
Creating a Mobile Device Profile	238
Configuring Mobile Device Profile General Settings	238
Mobile Device Profile Authorized Users	239
Editing Custom Properties for Mobile Device Profiles	240
Adding a Custom Property	241
Editing or Removing a Custom Property	242
Editing Registry Keys for Mobile Device Profiles	242
Adding a Registry Key	243
Adding a Value to a Registry Key	243
Removing a Registry Key	244
Editing or Removing a Registry Key Value	245
Configuring Mobile Device Profile Advanced Settings	246
Location Based Services	246
Geofence Areas	247
Regional Settings	248
Update Restrictions	248
Viewing Where Mobile Device Profiles are Applied	249

Chapter 16: Managing Mobile Device Groups	250
Creating Mobile Device Groups	250
Adding Devices to Static Mobile Device Groups	251
Removing Devices from Static Mobile Device Groups	252
Adding Mobile Device Group Authorized Users	252
Pinging Mobile Devices within Mobile Device Groups	253
Sending Messages to Mobile Device Groups	254
Editing Properties for Mobile Device Groups	254
Additional Mobile Device Group Functions	256
Chapter 17: Managing Alert Profiles	257
Managing Alert Profiles	257
Creating Alert Profiles	258
Configuring Alert Profiles	258
Alert Profile Authorized Users	260
Assigning Alert Profiles to a Region	261
Viewing Where Alert Profiles Are Applied	261
Removing Alert Profiles	262
Adding Profiled Contacts	262
Importing E-mail Addresses	264
Removing Contacts	265
Adding Profiled Proxies	265
Alerts Tab	266
Using the Alert Browser	266
Acknowledging Alerts	267
Clearing Alerts	267
Customizing Alert Browser Functionality	267
Using the Avalanche Map	268
Saving Map Views	269
Moving Server Locations	270
Chapter 18: Using Selection Criteria	271
Building Selection Criteria	272
Building Custom Properties	274
Selection Variables	274
Operators	283
Chapter 19: Using the Task Scheduler	286
Performing a Universal Deployment	289
Deploying Servers	290
Uninstalling Servers	291
Updating Infrastructure Firmware	292
Applying and Deploying Profiles	293
Backing Up the System	294
Restoring the System	295
Removing Completed Tasks	297

Appendix A: SSL Certificates	298
Appendix B: Avalanche Services	308
Appendix C: Port Information	311
Appendix D: Supported Firmware	314
Appendix E: Wavelink Contact Information	323
Glossary	324
Index	331

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 introduction provides the following introductory information:

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

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 12 for more information.

The *Infrastructure Profiles* dialog box appears.

Managing Networks with Avalanche

Wavelink Avalanche is a multiple-vendor solution for organizations seeking to deploy, configure, and maintain an enterprise-wide wireless network. This section describes several basic elements of Avalanche, including:

- Components of Avalanche

- Location Management: Server Locations and Regions
- Mobile Manager

Components of Avalanche

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

The primary components of Avalanche include:

- **Avalanche Java Console.** The Avalanche Java Console is your interface with wireless network components. With the Avalanche Console, you can manage and maintain everything from infrastructure 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.
- **Distributed Servers.** Distributed Servers (or Servers) are server-side software responsible for communication between the Avalanche Console and wireless components. Avalanche has two types of distributed servers: Infrastructure Servers and Mobile Device Servers.

- **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.

NOTE Some features of the Avalanche Console are only available with recent versions of the Enabler.

Location Management: Server Locations and Regions

One of the key aspects of Avalanche is location management. Avalanche divides locations into two categories: server locations and regions.

A server location is the most basic component of the Avalanche Console. Each server location contains at least one server that communicates with specific wireless components. Because these locations are based on servers, you can define a server location in a way that best suits your network administration processes—for example, you can organize server locations by location or by network role.

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

A collection of server locations is called a region. Typically, each server location within a region contains a set of similar characteristics such as geographic location or role within your organization's structure. When you apply configurations to a region, the Avalanche Console applies the configurations to every server location within that region.

Mobile Manager

Although you manage most aspects of your wireless network using the Avalanche Console, specific server locations within the network might require additional configurations. These configurations can be made using the

Infrastructure Site Console, formerly Mobile Manager Administrator. The Site Console is a tool designed to manage infrastructure devices at a specific server location.

For more information about Mobile Manager, refer to the *Mobile Manager User's Guide* or contact Wavelink Customer Service.

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 *Chapter 2: Installing Avalanche* on page 16.
- 2 Activate Mobile Device and Infrastructure 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 *Chapter 3: Licensing* on page 25.
- 3 Create regions.** A region allows you to group server locations that share a set of similar characteristics such as geographic location or role within your organization's structure. For more information, refer to *Managing Regions* on page 80.
- 4 Create server locations.** Server locations are the basic component of Avalanche and are where the Servers reside. For more information, refer to *Managing Server Locations* on page 83.
- 5 Configure profiles.** A profile allows you to manage configurations and settings centrally and then deploy those configurations to as many regions and locations as necessary. In this way, you can update or modify multiple servers instead of manually changing settings for each one. Avalanche provides network, scan to config, software, alert, Server, mobile device, and infrastructure profiles.
- 6 Assign profiles to regions.** You can assign configured profiles to regions within the Console. When you assign a profile to a region and install the Servers or perform a Universal Update, the settings from the profiles are applied to the server locations within the region. For more information, refer to *Assigning Profiles* on page 81.

- 7 Install servers.** Create a server package to deploy to the regions. This will install the Servers and apply profile configurations to the devices at the server location. For more information, refer to *Building Server Deployment Packages* on page 98.
- 8 Perform Updates.** To deploy settings to the selected regions and server locations, perform an update through the Task Scheduler. For more information refer to *Performing a Universal Deployment* on page 289.

Once you assign 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.

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:

- Which Version of Avalanche Should I Install?
- Installing Avalanche Mobility Center
- Installing Avalanche Console Only
- Installing Avalanche with External Databases
- Uninstalling Avalanche

If you are migrating to Avalanche 5.0 from an earlier version or if you have backup files (.abk) for Avalanche Manager that you want to migrate, see the Wavelink Web site for migration documentation.

Which Version of Avalanche Should I Install?

The type of Avalanche you install depends on your network management needs.

- If you plan to manage both mobile and network infrastructure devices in a centralized or distributed server environment, you should install Avalanche Mobility Center.
- If you plan to manage mobile devices only, you should install Avalanche Site Edition. For information on installing and using Avalanche Site Edition, see the separate user guide.
- If you have already installed the Enterprise Server and other components of Avalanche and want to be able to access and manage information from a different location, you should install the Console-only version of Avalanche.
- If you plan to maintain your databases on a separate system from the Enterprise Server, you should install Avalanche for an External Database.

Be sure you review the installation requirements for each version.

Installing Avalanche Mobility Center

This section provides instructions for the complete Enterprise installation process for Avalanche 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 23.

To install Avalanche:

- 1 Download the self-extracting zip file from the [Wavelink Web site](#).
- 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* dialog box appears.
- 4 If you agree with the terms in the License Agreement, click **Yes**.
The *Avalanche MC Setup* dialog box appears.
- 5 Enter the name of your company or organization in the text box and click **Next**.
The *AMC Installation Options* dialog box appears.

- 6 Select the type of installation desired.
 - **Custom.** Allows you to choose which components to install. If you choose **Custom** and click **Next**, you will be prompted to select the desired components. For more information on the components of Avalanche, see *Components of Avalanche* on page 12.
 - **Enterprise.** Installs full support for distributed mobile device and infrastructure servers, the enterprise server, the statistics server, and the databases.

Click **Next**.

The *Choose Destination Location* dialog box appears.

- 7 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* dialog box appears.

- 8 Click **Finish**.

Installing Avalanche Console Only

This section provides information about a Console-only installation of Avalanche MC. If you choose to install only the Avalanche MC Console, you must install the server and database components on a separate system for Avalanche MC to function.

To install Avalanche MC Console:

- 1 Download the self-extracting zip file from the [Wavelink Web site](#).
- 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* dialog box appears.

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

The *Choose Destination Location* dialog box 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** to continue the installation process.

The Avalanche Console is installed on your system.

- 6 Click **Finish**.

Installing Avalanche with External Databases

Avalanche MC uses two databases to store and manage information for your network. The standard Avalanche installation comes with a PostgreSQL database setup included. If you want your databases managed on a system other than the system running your Enterprise Server, or if you choose to use a different database management system (DBMS), you should use the External Database installation file.

While Wavelink recommends that you use the built-in Avalanche database platform (PostgreSQL) when possible, Avalanche MC also works with SQL Server 2005, SQL Server 2008, and Oracle 11g.

A basic assumption with the alternate database management system is that the customer takes responsibility for some of the database administration tasks that are otherwise handled in an automated manner with the built-in Avalanche databases.

NOTE When an alternate DBMS is used, you are responsible for properly licensing the DBMS.

Depending on the DBMS you are using, there are some tasks that must be accomplished before you install Avalanche with external databases. This section provides the following information:

- Before You Begin (PostgreSQL)
- Before You Begin (SQL Server)

- Before You Begin (Oracle)
- Completing an External Database Installation

Before You Begin (PostgreSQL)

You must complete the following tasks before you can install Avalanche to work with external PostgreSQL databases:

- Install PostgreSQL 8.4.
- Create the Avalanche databases. The databases must be named `avalanche50` and `avastats50`.
- Create the login role for the databases.
- If you are installing Avalanche in a different location than the database server, modify `pg_hba.conf` and `postgresql.conf` to support a remote connection.

Before You Begin (SQL Server)

You must complete the following tasks before you can install Avalanche with SQL Server:

- Install Microsoft SQL Server and obtain DBMS licenses.
- Create the Avalanche databases. The databases must be named `avalanche50` and `avastats50`.
- Create the login role for the databases.
- If you are installing Avalanche in a different location than the database server, you must configure the server to allow remote access.
- Install the Microsoft SQL Server Native Client and SQL Server Command Line Query Tool for your edition of SQL Server on the machine where you will be installing Avalanche.

NOTE You must use the Client and Query Tool specific to your edition. If you are using SQL Server 2005, these files will be `sqlncli.msi` and `SQLServer2005_SQLCMD.msi`. If you are using SQL Server 2008, these files will be `sqlncli.msi` and `SqlCmdLnUtils.msi`.

Before You Begin (Oracle)

You must complete the following tasks before you can install Avalanche with Oracle:

- Install Oracle 11g and obtain DBMS licenses.
- Perform an Administrator installation of the Oracle Client Utility (`win32_11gR1_client.zip`) at the location where you will be installing Avalanche.

NOTE If you do not use the Administrator installation type, Avalanche will not have all the tools necessary to communicate with the databases.

- Create the Avalanche databases. The databases must be named `avalanche50` and `avastats50`.
- Create the Avalanche SID (`ava50`) for the enterprise server.
- Create the username/password combination SID. If the statistics server is using the same SID as the enterprise server, create the username/password combination for it.
- Create and configure a `tsanames.ora` file in `[client install directory]\11.1.0\client_1\network\admin`

This file must define database addresses.
- If you are installing Avalanche in a different location than the database server, you must configure the server to allow remote access.

Completing an External Database Installation

Once you have created the database, created the login and assigned the login to the database, you can complete the Avalanche installation.

To install Avalanche:

- 1 Download the external database installation file from the [Wavelink web site](#).
- 2 Double-click the file to start the installation process.

NOTE At any time, you can cancel the installation process by clicking **Cancel**.

The *InstallShield Wizard* appears.

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

The *License Agreement* dialog box appears.

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

The *AMC Installation Options* dialog box appears.

- 5 Select the type of installation desired.
 - **Custom**. Allows you to choose which components to install. If you choose **Custom** and click **Next**, you will be prompted to select the desired components. For more information on the components of *Avalanche*, see *Components of Avalanche* on page 12.
 - **Enterprise**. Installs full support for distributed mobile and infrastructure servers.

- 6 Click **Next**.

The *Avalanche MC Setup* dialog box appears.

- 7 Type the name of your company or organization in the text box and click **Next**.

The *AMC Database Options* dialog box appears.

- 8 Select the desired database platform and click **Next**.

The *Database Location Information* dialog box appears.

9 Depending on the database platform you are using, different information is required on this page. Enter the required database information in the appropriate text boxes and click **Next**.

- If you are using a PostgreSQL or SQL Server database, enter the **Hostname** and **Port** for the enterprise database.
- If you are using an Oracle database, enter the **Hostname**, **Port**, and **SID** for the enterprise database.

The *Database Login Information* dialog box appears.

10 Enter the username and password for the enterprise database and click **Next**.

- If you are using an Oracle database, the installer will verify your credentials and then the *Stats Server Credentials* dialog box appears. Enter the username and password for the stats server database and click **Next**.

The *Install Destination Folder* dialog box appears.

11 Click **Next** to accept the default installation folder, or click **Change** to navigate to a folder of your choice. After you select an installation folder, click **Next** to continue the installation process.

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

12 Click **Finish**.

Once the installation is complete, you are prompted to activate Avalanche for your network.

Uninstalling Avalanche

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

When you uninstall Avalanche, you are given the option to uninstall the PostgreSQL database as well. If you select to uninstall Avalanche and the PostgreSQL database, all components of Avalanche and the database will be removed. If you select to uninstall Avalanche but opt to leave the database,

the `\db` folder located in the default installation directory will remain on your system. (Default location is `C:\Program Files\Wavelink\AvalancheMC\db`.)

NOTE If you plan on uninstalling Avalanche and/or the PostgreSQL database, it is recommended that you extract and backup database information and software collections. This can be done using the Task Scheduler. For more information, see *Chapter 19: Using the Task Scheduler* on page 286.

NOTE You may also want to save any `wavelink.lic` license files in a different location because they will be removed when Avalanche is uninstalled. To save a license file, navigate to the folder where the license is stored. Copy the license file and paste it to a different location.

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 or network infrastructure 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 or infrastructure 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.

This overview provides information about the following topics:

- Types of Licenses
- Unlicensed Devices

Types of Licenses

There are different licenses available for Avalanche MC depending on what version you are using and what devices you want to manage. This section provides information on the following licenses:

- Base and Maintenance Licenses
- Infrastructure and Mobile Device Licenses

Base and Maintenance Licenses

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

Table 3-1: *Licensing*

Infrastructure and Mobile Device Licenses

There are two types of licenses available for Avalanche MC: licenses for infrastructure devices and licenses for mobile devices. In order to manage your devices through Avalanche MC, you must have a license of the correct type for each device you want to manage.

Unlicensed Devices

When you run Avalanche without a valid license, it will behave as follows:

- **For mobile devices:** 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.
- **For infrastructure devices:** The infrastructure devices appear in the Avalanche Console, but you will not be able to manage the infrastructure device. You cannot deploy or apply profiles to the 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 and infrastructure devices. It operates 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 and Infrastructure Server will not be able to receive licenses.

Activating Licenses

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

- 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 50.

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.

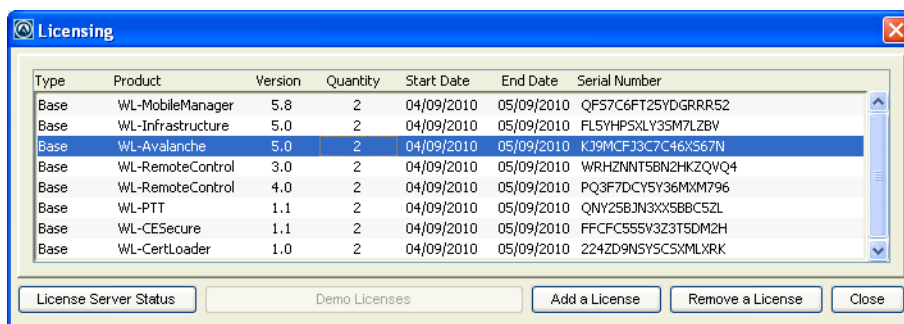


Figure 3-1. Licensing dialog box

- 3 Click **Add a License**.

The *Add a License* dialog box appears.

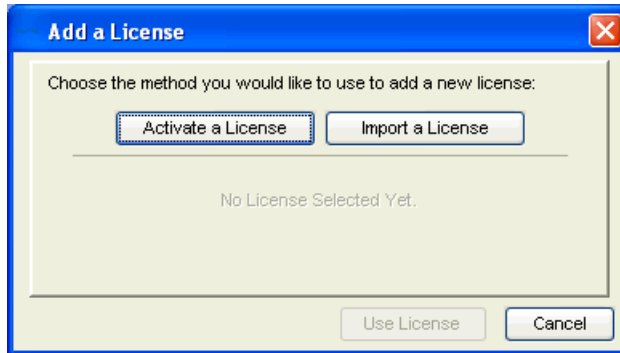


Figure 3-2. *Add a License dialog box*

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.

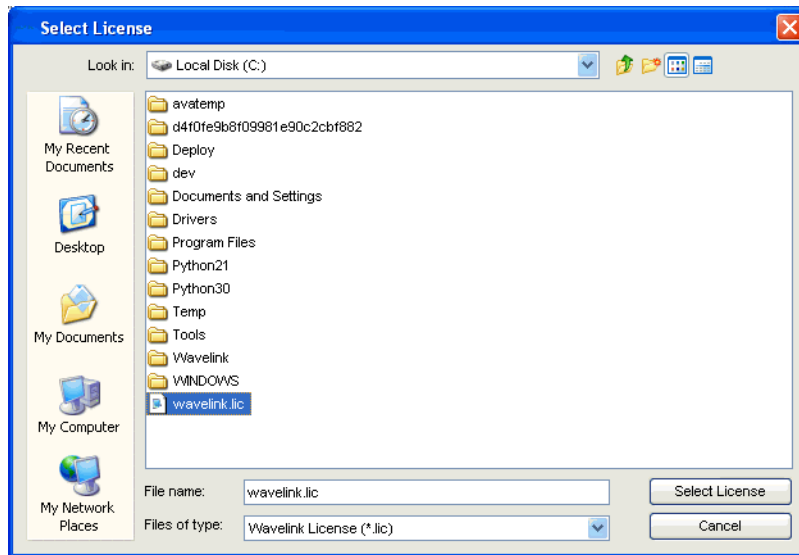


Figure 3-3. *Select License dialog box*

- 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 28, *Activating Manually* on page 29 or *Importing a License* on page 30 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 190. For

information about deleting devices from the Mobile Device Inventory, refer to *Deleting Mobile Devices* on page 221.

Importing the Enterprise License

Enterprise Licenses grant you unlimited licenses for your mobile devices and infrastructure 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 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.

To streamline wireless network management, the Avalanche Console allows you to organize distributed servers into server locations and regions. Creating logical and organized server locations and regions can greatly improve flexibility and allow you to manage your network with ease. Refer to *Chapter 6: Managing Regions and Locations* on page 78 for more information about regions and server locations.

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.

This section contains the following topics for the Java Console:

- Launching the Avalanche Console
- Understanding the Avalanche Console
- Changing Console Preferences
- 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 on an enterprise-wide basis. You can open the Avalanche Console from the **Programs** menu or from a shortcut.

To open the Avalanche Console:

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

The *Wavelink Avalanche Mobility Center Login* dialog box appears.

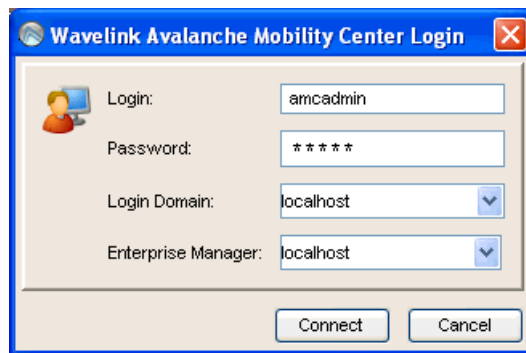


Figure 4-1. *Wavelink Avalanche Mobility Center Login*

- 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 log in. For information about changing passwords, refer to *Chapter 5: Managing User Accounts* on page 64.

- 3 From the **Login Domain** drop-down list, select your domain.
- 4 From the **Enterprise Manager** 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.

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 the regions and server locations within 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.

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 each Tool Bar button.



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 deploy any profile and configuration changes to Servers immediately. This allows you to immediately deploy changes without creating a deployment task in the Task Scheduler. You can still create and schedule deployments through the Task Scheduler.



Click this icon to open the Task Scheduler and create 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 Very Large Access Control List



Click this icon to open the Deployment Package wizard and build new deployment packages.



Click this icon to access the Avalanche Help.

Navigation Window

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

To use the Search function:

- 1 Type in the name of the region or server location in the text box just above the tree view.
- 2 Click **Search**.

The highlight will move to the first region or server location 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 region or server location.

The **Search** function finds server locations 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 quick links to 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:

- Server Configuration
- 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.

Server Configuration

The tasks in this region are required and must be done in the order presented. These tasks include:

- Creating a Region. For details, refer to *Managing Regions* on page 80.

- **Creating a Distributed Server Location.** For details, refer to *Managing Server Locations* on page 83.
- **Create a Distributed Server Package.** For details, refer to *Building Server Deployment Packages* on page 98.
- **Deploying Distributed Server Package to a Location.** For details, refer to *Deploying Servers* on page 290.

Profiles Configuration

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

- **Creating a Network Profile.** For details, refer to *Chapter 7: Managing Network Profiles* on page 105.
- **Add Device Software.** For details, refer to *Chapter 14: Managing Software Profiles* on page 201.
- **Creating an Infrastructure Profile.** For details, refer to *Chapter 10: Managing Infrastructure Profiles* on page 147.
- **Apply Profiles to Regions or Locations.** For details, refer to *Assigning Profiles* on page 81 and *Assigning Profiles to Server Locations* on page 91.

Tools

This section allows you to install an Avalanche Enabler onto a mobile device, access the Scan to Config utility 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 60.

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 *Chapter 17: Managing Alert Profiles* on page 257.

- **Infrastructure Server profile.** An Infrastructure Server profile allows you to define device access privileges for your Infrastructure Servers. For information on Infrastructure Server profiles, see *Chapter 9: Managing Infrastructure Distributed Servers* on page 132.
- **Infrastructure profile.** An infrastructure profile allows you to manage your infrastructure devices. For information on infrastructure profiles, see *Chapter 10: Managing Infrastructure Profiles* on page 147.
- **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 *Chapter 13: Managing Mobile Device Distributed Servers* on page 184.
- **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 *Mobile Device Profiles* on page 237.
- **Network profile.** A network profile allows you to configure network information (such as IP addresses) and encryption and authentication for you infrastructure and mobile devices. For information on network profiles, see *Chapter 7: Managing Network Profiles* on page 105.
- **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 *Chapter 8: Managing Scan to Configure Profiles* on page 120.
- **Software profile.** A software profile allows you to organize and configure software packages for deployment to multiple devices. For information on software profiles, see *Chapter 14: Managing Software Profiles* on page 201.

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 by type. When you activate a filter, only the profiles matching the filter will be displayed in the Profile List.

To filter the Profile List by type:

- 1 In the Profile List, right-click the header for the Profile Type column.
- 2 Click **Set Filter** in the context menu.

The *Set Column Filter* dialog box appears.

- 3 Enable the type(s) of profile you want to display in the Profile List and 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, region properties, 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 46.

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**, **Region Properties**, 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**, **Region Properties**, 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 cannot edit Unassigned dServer Locations or Deleted dServer Locations.
- 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
- Configuring Deployment 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 Map Options

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 From the **Default Enterprise Page Tab** drop-down list, select which tab of the Avalanche Console displays after an update or a deployment.

You can choose the **Properties** tab, **Mobile Device List**, **Infrastructure List** or **Last Selected**. If you choose **Last Selected**, any time you change region or server location, the Console will display the tab (Mobile Device Inventory, Infrastructure Inventory or Region Properties) most recently used. If no tab has been selected, this will default to the **Properties** tab.

- 6 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.

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

The Avalanche Console updates to reflect your changes.

Configuring Deployment Settings

From the *Preferences* dialog box you can configure Enterprise Server auto-deployments, profile auto-assignment, and the refresh delay for universal deployments.

- When you configure the Enterprise Server to **Auto Deploy Settings**, each change made at the Console is immediately deployed to the assigned regions/server locations. You can **Disable all Auto Deploy Notifications** if you don't want a notification each time an auto-deployment occurs.

NOTE It is recommended that before enabling auto-deployment, you have most of your settings configured and deployed. If the option is enabled as you first configure and set up Avalanche, the Enterprise Server may become overloaded, potentially causing delays and other errors.

- The **Universal Deployment Refresh Delay** refers to the number of seconds the Avalanche Console waits before trying to refresh the display after any type of deployment (through the Task Scheduler, **Deploy Now** button or an auto-deploy). The default is set to five seconds. This default works well for most systems.

When changing **Universal Deployment Refresh Delay**, consider the link speed between the Console and the Enterprise Server, the number of mobile devices you are managing, and the amount of data you are transferring (profiles and configurations). If the Console display has enough time to refresh completely, you will return to the same Console location (region, profile and tab) you were viewing before the deployment.

To configure deployment settings:

- 1 Click **Tools > Preferences**.

The *Preferences* dialog box appears.

- 2 Select the **Enterprise Server** tab.
- 3 Enable the **Auto Assign Profiles** option to automatically assign all profiles and profile changes to the **My Enterprise** region.
- 4 Enable the **Auto Deploy Settings** to automatically deploy all changes and configurations each time you save a configuration.
- 5 Enter the number of seconds the Console will wait to refresh after settings are deployed in the **Universal Deployment Refresh Delay** text box.
- 6 Click **Apply** to save the changes.
- 7 Click **OK** to close the *Preferences* dialog box.

NOTE If you enabled the **Auto Deploy Settings** option, profiles and configurations will not immediately deploy. Settings will deploy the next time you perform a save.

When **Auto Deploy Settings** is enabled, each time you make changes to the Console and save those changes, Avalanche performs a Universal Deployment, sending those changes to the appropriate regions and server locations. During this deployment the *Universal Deployment Notification* dialog box appears. This dialog box informs you that because of the recent deployment, the Avalanche interface must reload and refresh to ensure the Console displays accurate information.

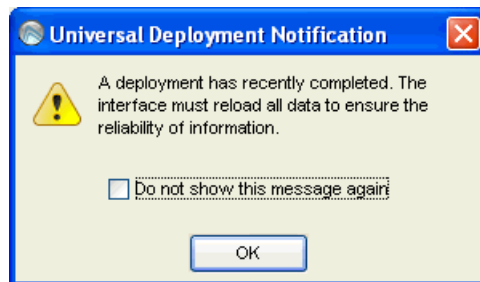


Figure 4-2. *Universal Deployment Notification*

- 8 To suppress this message so it does not appear during every deployment, enable the **Do not show this message again** check box and click **OK**.

The *Universal Deployment Notification* dialog box will no longer appear during an auto deployment.

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 48.

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 49.

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\AvalancheMC\backup`.

For information about backing up your system, refer to *Backing Up the System* on page 294.

To specify a location:

- 1 Click **Tools > Preferences**.

The *Preferences* dialog box appears.

- 2 Select the **Enterprise 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 location connections, you must configure HTTP proxy settings to enable the city search performed during the Avalanche installation process.

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.

The next time you create a server deployment package, the proxy server settings configured in this dialog box will be used.

- 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.

Customizing Map Options

You can modify the appearance of the map in the **Health by Location** tab.

To modify colors:

1 Click **Tools > Preferences**.

The *Preferences* dialog box appears.

2 Select **Map Options** from the list box.

3 Click the color blocks in the **Background Color**, **Foreground Color** and **Line Color** regions to customize the map colors.

4 Click **Apply** to save your changes.

5 Click **OK** to close the *Preferences* dialog box.

The map in the **Health by Location** tab reflects your changes.

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:

- Configuring Server Blackout Periods
- Viewing the Enterprise Server Status
- Controlling the Enterprise Server Message Backlogs
- Limiting Distributed Server Connections
- Purging Server Statistics
- Performing a Dump Heap

Configuring Server Blackout Periods

Blackout periods are defined as times when communication between the enterprise server and distributed servers is shut down. The distributed servers cannot contact the enterprise server until the blackout is released. Use the options in the *eServer Status* dialog box to configure blackout periods between the enterprise server and the distributed servers.

You can also throttle the distributed servers, reducing the number of messages sent to the enterprise server. When the distributed servers are throttled, device status updates are not sent to the enterprise server. Reducing network traffic in this manner may be useful in temporary situations where you plan on high bandwidth usage, such as a big universal deployment.

The following enterprise server blackout tasks can be performed:

- Using an Enterprise Server Blackout
- Performing a Batch Release
- Throttling Distributed Servers

Using an Enterprise Server Blackout

You can stop communication between the enterprise server and distributed servers by using a blackout period.

To configure enterprise server blackout periods:

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

The *eServer Status* dialog box appears.

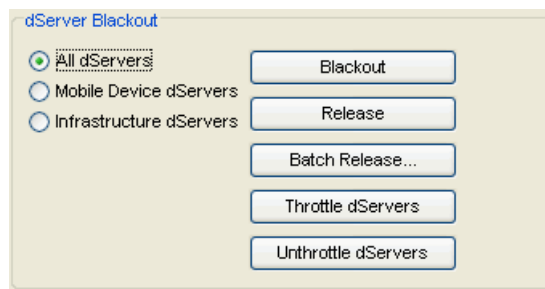


Figure 4-3. *dServer Blackout region*

- 2 From the list of Server options in the **dServer Blackout** section, select **All Servers**, **Mobile Device Servers** or **Infrastructure Servers**, based on the type of blackout you want.
- 3 Click **Blackout**.
- 4 Check that the **Blackout** parameter in the eServer Status region displays the appropriate type of blackout you configured.

There will be no communication between the Servers you selected and the eServer until you release the blackout period.

- 5 To release the distributed servers from blackout, click **Release** or perform a batch release. Check that the **Blackout** parameter in the eServer Status region displays **OFF**.

Performing a Batch Release

Batch releases restore communication from the distributed servers to the enterprise server in a controlled manner. Instead of releasing all the servers from the blackout at once, the servers are released in batches and at specified intervals. This prevents the servers from flooding the enterprise server with messages upon release.

To perform a batch release:

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

The *eServer Status* dialog box appears.

- 2 Click **Batch Release**.

The *Batch Blackout Release* dialog box appears.

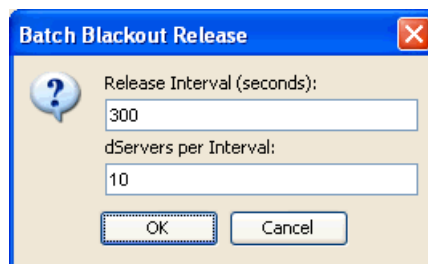


Figure 4-4. *Batch Blackout Release*

- 3 In the **Release Interval**, specify the number of seconds you want to elapse between batch releases.
- 4 In the **Servers per Interval** text box, specify the number of Servers you want released at each interval.
- 5 Click **OK**.

The Servers will be released according to the specifications you configured.

Throttling Distributed Servers

When the distributed servers are throttled, device status updates are not sent to the enterprise server. Reducing network traffic in this manner may be useful in temporary situations where you plan on high bandwidth usage, such as a big universal deployment.

To throttle the distributed servers:

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

The *eServer Status* dialog box appears.

- 2 In the dServer Blackout region, click **Throttle dServers**.

The distributed servers discard volatile device status information and hold all non-volatile data that would have been sent to the enterprise server. Pending updates are sent to the enterprise server once the servers are unthrottled.

- 3 To unthrottle the distributed servers, click **Unthrottle dServers**.

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.

Parameter	Value
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.
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.

Controlling the Enterprise Server Message Backlogs

You can control the enterprise server message backlog by setting the spillover threshold. The spillover threshold is the maximum number of messages from the distributed servers allowed in the backlog.

Once the threshold is reached, the distributed servers are throttled and further messages are stored in a file to disk until the backlog is reduced. When distributed servers are throttled, they will no longer send device statistics updates to the enterprise server. After the backlog has been reduced, messages are pulled from the store file back into the log and the distributed servers are no longer throttled.

To configure the spillover threshold:

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

The *eServer Status* dialog box appears.

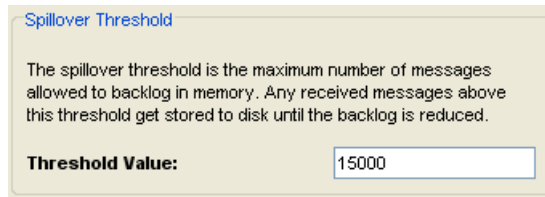


Figure 4-5. *Spillover Threshold in the eServer Status dialog box*

- 2 In the Spillover Threshold region, type the new **Threshold Value** in the box and click **OK**.

Limiting Distributed Server Connections

If you have a very large number of distributed servers, you may at times want to govern how many of them can simultaneously contact the enterprise server to prevent overloading the enterprise server. The dServer Governor allows you to set a maximum limit of how many distributed servers can contact the enterprise server at once.

If a distributed server tries to contact the enterprise server while the Governor is engaged and the limit has already been reached, the distributed server is queued. Servers in the queue are not permitted to send messages to the enterprise server. The Governor will rotate through the servers in the queue on a timed basis, allowing each to communicate with the enterprise server.

You can manually engage the dServer Governor, or you can enable the Governor and set it to automatically engage when the enterprise server has hit the spillover threshold a certain number of times. An alert profile can be configured to generate an alert when the Governor is engaged.

NOTE For more information on configuring the spillover threshold, see *Controlling the Enterprise Server Message Backlogs* on page 55.

The Governor must be manually disengaged. When you disengage the Governor, it is also disabled. You can view if the Governor is enabled or engaged in the *eServer Status* dialog box.

To limit the number of distributed servers in contact with the enterprise server:

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

The *eServer Status* dialog box appears.

- 2 In the dServer Governor region, type the **Maximum active dServers** in the provided text box.
- 3 If you want to engage the Governor immediately, ensure that the **Trigger Threshold** box says **0** and click **Start Governor**.

-Or-

If you want to enable the Governor to engage when the spillover threshold has been reached, enter the number of times the threshold must be reached before the Governor engages in the **Trigger threshold** box. Click **Start Governor**.

While the Governor is engaged, only the allowed number of dServers will be allowed to contact the enterprise server at a time. Once the limit is reached, the servers will be queued and take turns communicating with the enterprise server.

- 4 Click **Stop Governor** to resume regular network traffic and allow all distributed servers to contact the enterprise server.

Purging Server Statistics

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

- **Purge Time.** Set the time of day 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 4-6. 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 for each type of server.
- 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.

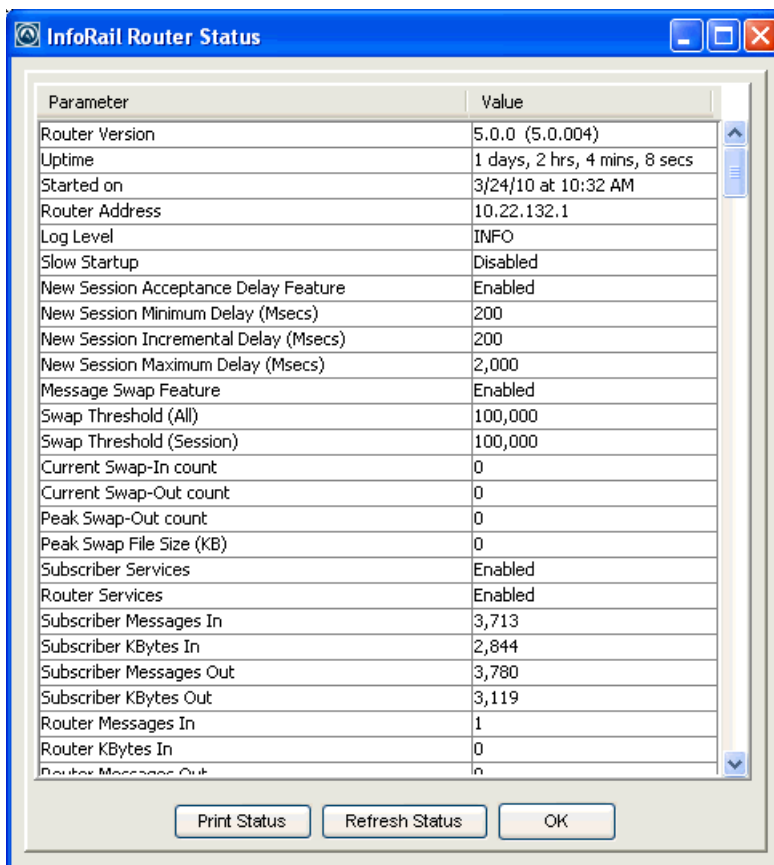


Figure 4-7. InfoRail Router Status

- 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`
- `EServer.log`
- `Inforail.log`

The Support Generator `.zip` files are saved to the installation location of Avalanche. 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.

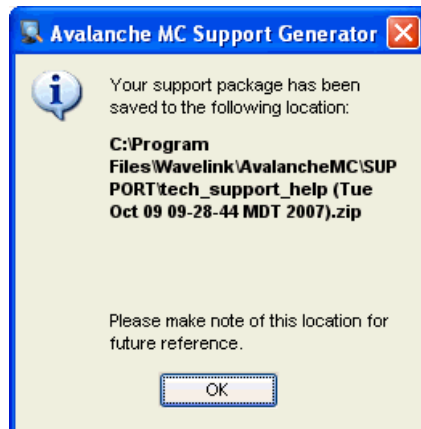


Figure 4-8. *Avalanche Support Generator Location*

- 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 Active Sync.

To install an Enabler:

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

The *Avalanche Device Enabler Installation* dialog box appears.

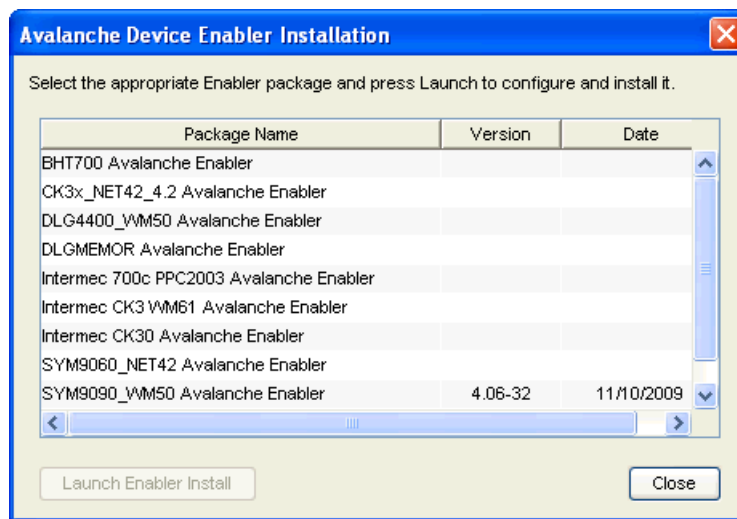


Figure 4-9. *Avalanche Device Enabler Installation*

- 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.

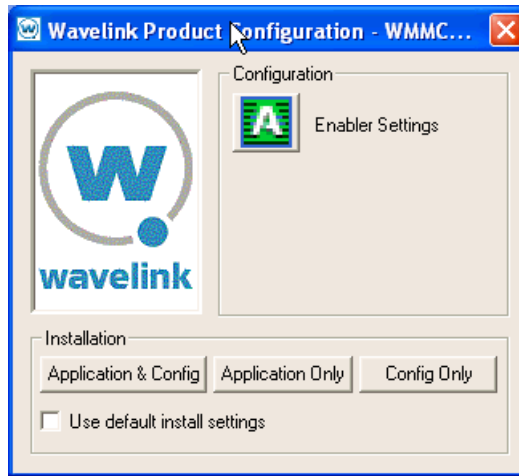


Figure 4-10. *Wavelink Product Configuration Utility*

- 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 and information about using ActiveSync, refer to the *Avalanche Enabler User Guide*.

Chapter 5: Managing User Accounts

A user account is required to log into 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 his home region. A Normal account is assigned to specific regions or profiles and is only authorized to view or make changes in his assigned areas.

Upon installation of Avalanche, an Administrator account is created automatically. This account allows you to create new Administrator or Normal user accounts and restrict or allow administration of your wireless network.

NOTE Wavelink recommends that you create a new administrative user.

This chapter provides the following information about user accounts:

- Defining Permission Types
- Creating User Accounts
- Creating User Groups
- Assigning User Permissions
- Assigning Authorized Users
- Configuring Integrated Logon
- Changing Passwords
- Removing User Accounts

Defining Permission Types

There are two types of user account permissions:

- **Regional Permissions.** These permissions are specific to various tasks and components of Avalanche. For each component you can grant read or read/write access. Read 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 within his home region.
- **Profile Permissions.** These permissions allow the user complete global access to the specified profile. Administrators can grant read or read/write access for each type of profile. Read/write allows the user to manage all aspects of the profile, from configuration to application. Read-only allows the user to view the profile, but does not allow any editing.

Within each of the permission types, you can assign the following levels of access:

- **None.** If you do not want a user to have access to any data, configurations or profiles, keep the access level at None. By default, all permissions are set to None.
- **Read/Write.** This level of access allows the user to access information and change configurations.
- **Read only.** This level of access allows the user to view the information, but does not allow the user to edit or configure any information.

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 sub-regions 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 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.

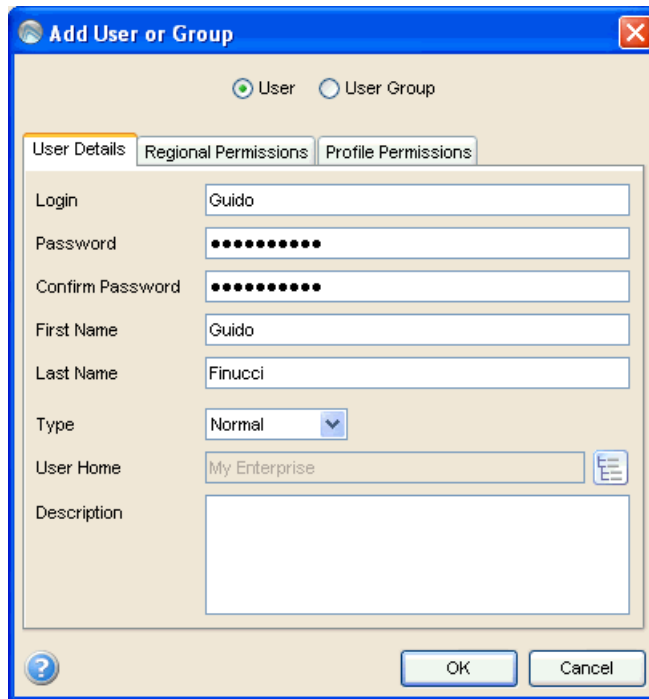
To create a new account:

- 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 Windows-style dialog box titled "Add User or Group". At the top, there are two radio buttons: "User" (selected) and "User Group". Below this are three tabs: "User Details" (selected), "Regional Permissions", and "Profile Permissions". The "User Details" tab contains several input fields: "Login" with the text "Guido", "Password" and "Confirm Password" both masked with dots, "First Name" with "Guido", "Last Name" with "Finucci", "Type" with a dropdown menu set to "Normal", "User Home" with "My Enterprise" and a tree icon to its right, and a large empty "Description" text area. At the bottom of the dialog are "OK" and "Cancel" buttons, and a help icon on the left.

Figure 5-1. Add User

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

NOTE The password is case sensitive.

- 4 To assign a user home, click the tree button to the left of the text box.
- 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 69.

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 65 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 69.

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 sub-regions or locations. There are two types of permissions:

- Regional Permissions
- Profile Permissions

Regional Permissions

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.
Deployment	Allows you to create and edit deployment packages as well as and schedule deployments to the regions you are assigned.	Allows you to view recent deployments.
Enterprise Management	Allows you to view, manage, and configure all regions to which you are assigned in the My Enterprise tree. You must have other regional permissions assigned.	Allows you to view all region configurations and settings.

Table 5-1: *Regional Permissions Explained*

Regional Permission	Read_Write	Read_Only
Infrastructure	Allows you to manage the Infrastructure Inventory for assigned regions.	Allows you to view the Infrastructure Inventory for assigned regions.
Infrastructure Profiles	Allows you to apply and remove infrastructure profiles.	Allows you to view which Infrastructure profiles are assigned to a region.
Infrastructure Site Tool	Allows you to access the Infrastructure Site Tool and use infrastructure tools.	Allows you to access the Infrastructure Site Tool and view information.
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 can not 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.

Table 5-1: Regional Permissions Explained

Regional Permission	Read_Write	Read_Only
Scan to Config Printing	Allows you to print Scan to Config profiles.	Allows you to print Scan to Config profiles.
Server Profiles: Infrastructure	Allows you to apply and remove Infrastructure Server profiles.	Allows you to view assigned Infrastructure Server profiles.
Server Profiles: Mobile Device	Allows you to apply and remove Mobile Device Server Profiles.	Allows you to view assigned Mobile Device Server Profiles.
Software Profile	Allows you to apply and remove Software Profiles.	Allows you to view assigned Software Profiles.

Table 5-1: *Regional Permissions Explained*

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 give you global access to each profile you are given permission for. This means that if you have permissions for Alert Profiles, you can add, configure, modify and delete as many Alert Profiles as you like. However this does not give you permission to apply the profiles to any

regions. You must be assigned at the region level to apply any profiles. This table describes each of the Profile Permissions:

Profile Permission	READ_WRITE	READ_ONLY
Alert Profiles	Allows you to create, edit and apply all alert profiles.	Allows you to view existing alert profiles.
Infrastructure Profiles	Allows you to create, edit and apply all infrastructure profiles.	Allows you to view existing infrastructure 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, edit, and apply Mobile Device Profiles.	Allows you to view existing Mobile Device Profiles.
Network Profiles	Allows you to create, edit and apply network profiles.	Allows you to view existing network profiles.
Server Profiles: Infrastructure	Allows you to create, edit and apply infrastructure profiles.	Allows you to view existing infrastructure profiles.
Server Profiles: Mobile Devices	Allows you to create, edit and apply mobile device 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, edit, and apply software profiles.	Allows you to view existing software profiles and the associated settings.

Table 5-2: *Profile Permissions*

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. The profile node or tab will be blank or inaccessible.
- 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 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 all the settings at that function, but the user can not modify any of the settings.
- 7 When you are finished, click **OK**.

Assigning Authorized Users

You must assign users configured with Regional Permissions to a region as an authorized user. Users that are Normal users but not configured to manage profiles can be assigned as authorized users for specific profiles.

This section contains the following information:

- Assigning Authorized Users to Regions
- Assigning Authorized Users to Profiles

Assigning Authorized Users to Regions

Each user must be assigned to a specific region. When you assign a user to a region, that user has any assigned Regional Permissions for all regions and Server Locations beneath the assigned region.

The **Authorized User** tab in the Region Properties and Server Location properties tabs lists all users that are allowed to access that region or Server Location. The tab also lists all regional permissions assigned to that user.

To assign users to regions:

- 1 Select the region or server location.
- 2 Select the **Region Properties** or **dServer Location Properties** tab.
- 3 Click **Edit**.

4 Click Authorized Users.

The *Profile Authorized Users* dialog box appears.

5 Click Add User.

The *Add Authorized User* dialog box appears.



Figure 5-2. *Add Authorized User*

6 Select the user and click OK.

The user is added to the list of authorized users.

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 permissions for each user.

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 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.

- 5 Retype the password to confirm it in the **Confirm New Password** text box.

- 6 Click **OK**.

- 7 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 Regions and Locations

One of the key aspects of Avalanche is location management. Avalanche divides locations into two categories: server locations and regions.

A server location is the basic component of the Avalanche Console. Each server location contains at least one server that communicates with specific wireless components. You can define a server location in a way that best suits your network administration processes—for example, you can organize server locations by location or by network role.

A collection of server locations is called a region. Typically, each server location within a region contains a set of similar characteristics such as geographic location or role within your organization's structure. When you apply configurations to a region, the Avalanche Console applies the configurations to every server location within that region.

For each server location with a Mobile Device Server, you also have the option of creating a site. Sites are groups of mobile devices that share a Mobile Device Server. Devices are added to a site when they meet selection criteria. A device can belong to more than one site concurrently. Sites allow increased flexibility for assigning different profiles at the same server location.

This section describes how to manage both server locations and regions and provides information about the following topics:

- General Overview
- Managing Regions
- Managing Server Locations
- Managing Sites
- Managing Servers
- Retrieving Mobile Device Log Files
- Configuring Infrastructure Servers at Server Locations

General Overview

Regions and locations allow you to structure Avalanche to match your network needs. To better manage your Avalanche configuration and to ensure optimal performance, Wavelink recommends you perform the following steps in order:

- 1 Install Avalanche.** For more information, refer to *Chapter 2: Installing Avalanche* on page 16.
- 2 Activate Mobile Device Server and Infrastructure Server 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 *Chapter 3: Licensing* on page 25.
- 3 Create regions.** A region is a collection of server locations that share a set of similar characteristics such as geographic location or role within your organization's structure. For more information, refer to *Managing Regions* on page 80.
- 4 Create server locations.** Server locations are the basic component of Avalanche and are where the Servers reside. For more information, refer to *Managing Server Locations* on page 83.
- 5 Configure profiles.** A profile allows you to manage configurations and settings centrally and then deploy those configurations to as many regions and locations as necessary. In this way, you can update or modify multiple servers instead of manually changing settings for each one. Avalanche provides network, scan to config, software, alert, Server, mobile device, and infrastructure profiles.
- 6 Assign profiles to regions.** You can assign configured profiles to regions with the Console. When you assign a profile to a region and install the Servers or perform a Universal Update, the settings from the profiles are applied to the server locations within the region. For more information, refer to *Assigning Profiles* on page 81.
- 7 Install servers.** Create a server package to deploy to the server locations. This will install the Servers and apply all profile configuration to the devices at the server location. For more information, refer to *Building Server Deployment Packages* on page 98.

Managing Regions

A region is a collection of server locations. Typically, each server location within a region contains a set of similar characteristics such as geographic location or role within your organization's structure. When you apply configurations to a region, the Avalanche Console applies the configurations to every server location within that region.

Avalanche allows you to create nested regions, enhancing your region and network control. You can add as many regions to the Avalanche Console as necessary to manage your wireless network effectively.

This section provides information about the following:

- Creating Regions
- Creating Nested Regions
- Viewing Region Properties
- Assigning Profiles
- Deleting Regions

NOTE To configure an individual server location from the Avalanche Console, create a region that contains only that server location and apply settings to that region.

Creating Regions

You can add any number of regions to the Avalanche Console to manage your wireless network effectively.

To create a region:

- 1 From the **File** menu, select **New > Create Region**. This method creates a region in the currently selected item in the Navigation Window.

-Or-

Right-click **My Enterprise** and select **Create Region**.

-Or-

If you are created nested regions, right-click the region you want to place the new region below and select **Create Region**.

- 2 In the *New Region* dialog box, type the name of the new region and click **OK**.

The new region appears as a node in the Navigation Window.

Creating Nested Regions

A nested region is a region that is placed within another region and appears a step below that region in the Navigation Window of the Console. A branch in the Navigation Window is a region, the nested sub-regions, and any server locations and sites associated with those regions.

When a profile is applied to a region, it is also applied to, or “inherited” by, all the associated sub-regions and server locations. A user with read/write permissions for a region has the option of excluding an inherited profile for his region, but he cannot change the priority of an inherited profile.

Viewing Region Properties

Once you create a region, you can view the properties of that region. Region properties include the region name, the Avalanche Console path (where that region is located under My Enterprise), profiles, and authorized users.

To view region properties:

- In the Navigation Window, click the region.

The **Region Properties** tab displays the properties for the selected region.

Assigning Profiles

Once you create a region you can assign any available profiles to that region. If you do not assign profiles to regions or server locations, the settings in those profiles will not be deployed to the Servers, resulting in the inability to manage network infrastructure and mobile devices. The following is information about applying the different types of profiles.

- **Infrastructure Profiles.** You can assign as many Infrastructure profiles to a region as you desire. The profiles are applied to the mobile devices based on selection criteria for the profile and the priority in which the profiles are listed in the Avalanche Console.

- **Server Profile.** You can assign one Mobile Device Server profile and one Infrastructure Server profile to region. 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 Avalanche Console.
- **Alert Profiles.** Alert profiles can be assigned at the enterprise or region level and will be deployed to all regions and server locations nested within the assigned region. You can apply multiple alert profiles to one region at a time.
- **Network Profiles.** You can assign as many network profiles to a region as you desire. 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 Avalanche Console.
- **Software Profiles.** When you assign software profiles to a region, the profiles are deployed to all regions and server locations nested within the assigned region based on selection criteria of the software packages.
- **Scan to Config Profiles.** When you assign Scan to Config profiles to a region, the profiles are made available for Normal users with permissions in that region to access and print them.

To assign a profile to a region:

- 1 Select the region or location where you want to assign the profile from the Navigation Window.
- 2 Select the **Region Properties** tab.
- 3 Click **Add** on the **Applied Profiles** tab.
- 4 From the list that appears, select the profile you want to apply and click **OK**.
- 5 Continue adding profiles until complete.
- 6 Save your changes.

The assigned profile will be deployed with the server when you install the Servers or when you perform a Universal Deployment after the server is installed. For information about installing Servers, refer to *Deploying Servers* on page 290. For more information about Universal Deployment, refer to *Performing a Universal Deployment* on page 289.

Deleting Regions

You can delete unused regions from the Avalanche Console at any time. Any server locations associated with a region automatically return to the **Deleted Server Locations** folder when you delete that region.

NOTE Deleting a region is permanent. There is no way to retrieve deleted regions. You must recreate the region.

To delete a region:

- 1 Right-click the region or server location from the Navigation Window and select **Delete**.

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

- 2 Click **Yes** to delete the region.

The region is removed from the Navigation Window and any server locations in that region are moved to the **Deleted Server Locations** folder.

NOTE You can restore server locations that are in the deleted Server Locations folder to the **Unassigned Server Locations** folder where you can then reassign the server locations to a new region. For more information about restoring deleted server locations, refer to *Restoring Server Locations* on page 92.

Managing Server Locations

A server location is any location with an Infrastructure Server, a Mobile Device Server, or both. A server location can manage wireless devices for a unique physical entity such as a warehouse, or a subsection of an entity such as the third floor of an office building.

NOTE The number of wireless components managed at a server location depends on the communication range of the Servers installed at that location. Traditionally, this range has been defined as a single subnet on your network; however, depending on your network architecture, you can configure a Server

to communicate past a given subnet. This type of configuration takes place at the server location level, using the Mobile Manager Administrator. See the *Mobile Manager User's Guide* for more information.

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

- Configure your network hardware to allow infrastructure and mobile device broadcasts to reach the Servers.
- Use the server location-based tools included with Mobile Manager to configure the Server to manage multiple subnets.
- Segment the location into multiple server locations by installing the appropriate Servers at each subnet.

This section provides information about the following tasks for managing server locations:

- Determining Server Placement
- Adding Server Locations
- Understanding Unassigned Server Locations
- Moving Server Locations to Regions
- Modifying Server Location Properties
- Assigning Profiles to Server Locations
- Deleting Server Locations

Determining Server Placement

Spacing your Infrastructure Servers correctly is an important task. The ability to manage your wireless network depends on Servers being able to locate and communicate with your infrastructure devices. Currently, there are two primary methods of installing Servers: centralized and distributed.

- Centralized Server Method
- Distributed Server Method

Centralized Server Method

In centralized Server installations, a single Server is responsible for managing all of the infrastructure devices on the network. Centralized Server installations are typically found in environments where specific locations within a network might be unable to support their own Servers. An example of this environment is a collection of retail stores. While the headquarters for these stores can support an Infrastructure Server, it might not be feasible for each individual store to have its own Server. In this case, installing the Server centrally is an ideal solution.

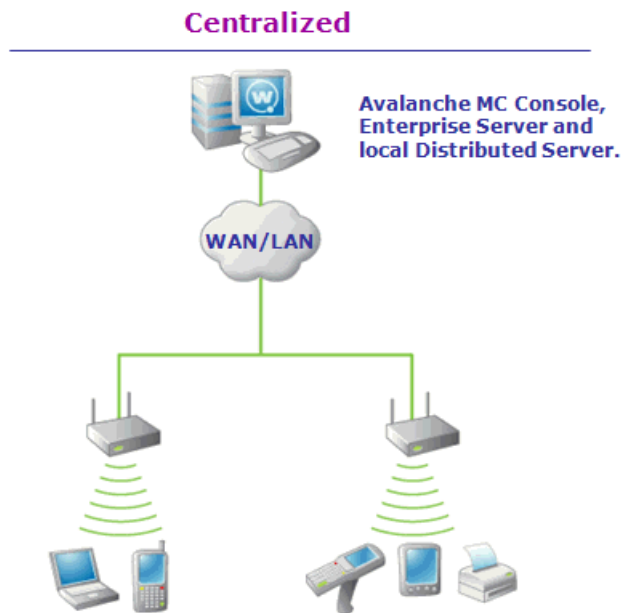


Figure 6-1. A Centralized Installation of Avalanche (Simplified)

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

- You must know the network subnets to ensure the Server knows where to listen for infrastructure broadcasts.

- You must know what switches and routers reside between the Server and infrastructure devices. (This is particularly helpful should any troubleshooting be necessary.)
- You must have a general understanding of the overall performance of the wireless network, to ensure that specific time-based features (such as WEP key rotation) are configured correctly.

Distributed Server Method

In distributed Server installations, a Server resides on each network subnet. These Servers are responsible for managing on a per-subnet basis. Often, distributed Server installations of Avalanche are found in environments where wireless connectivity is critical to business operations. For example, if a company has multiple locations across the country, connectivity between each server location might depend on factors outside the company's control—such as weather, the performance of third-party services, and so on. In these situations, installing a Server on each subnet provides a more robust environment in which wireless network downtime is minimized.

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

- Because you are installing multiple Servers on multiple systems, it might take more time to completely install and optimize Avalanche for your network.
- You must ensure that when you upgrade Avalanche, you upgrade all Servers across the network.

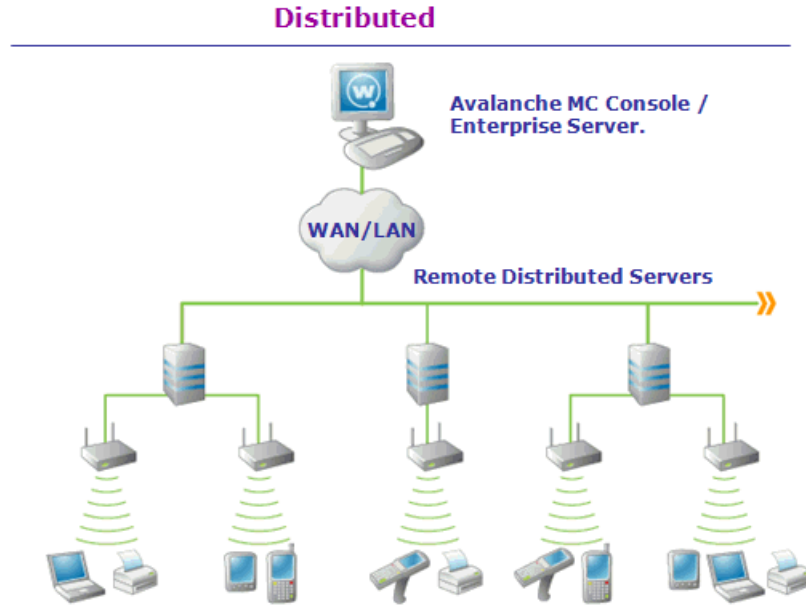


Figure 6-2. *A Distributed Installation of Avalanche (Simplified)*

For information about how to deploy Infrastructure Servers, refer to *Deploying Servers* on page 290.

If the location already contains one or more Servers, you do not need to create a new server location. However, you must ensure that the Server installed at the server location is compatible with the Avalanche Console.

Adding Server Locations

Before you deploy a Server (mobile device or infrastructure) to a server location, you must add that server location and information about the server location to the Avalanche Console. When you create a new server location, you give the server location a name and identify the IP address and location.

To add a server location:

- 1** Select **File > New > Create dServer Location**.

The *New dServer Wizard* appears.

- 2 Type the name of the server location in the **Location Name** text box and click **Next**.

The *Enter dServer Location Site Address* dialog box appears.

- 3 Type the IP address of the system which contains (or will contain) a Server in the **Location Site Address** text box and select the appropriate OS platform from the drop-down list. Click **Next**.

The *Enter dServer Location City Name* dialog box appears.

- 4 Type the name of the city where the server location resides in the **Server Location City Name** text box.

Avalanche will search its database to find all cities that have the name you specified. If you do not want Avalanche to search its database, enable the **Bypass this search** checkbox.

NOTE Avalanche connects to a database at the Wavelink Web site to perform this search.

- 5 Click **Next**.

The *Choose Server Location* dialog box appears.

- 6 Select the appropriate city from the **Search Results** list and click **Next**.

The *Select dServer Location Time Zone* dialog box appears.

- 7 Select the time zone for the destination and click **Next**.

The *Enter dServer Location Login Information* dialog box appears.

- 8 Type the **User Name**, **Password**, and **Domain** for the system on which the Server resides (or will reside) and click **Next**.

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

The *Enter Shared Folder Information* dialog box appears.

- 9 Type the name of the shared folder where Avalanche updates are installed in the **Share Name** text box.

Type the directory path where Avalanche updates are installed on this remote system in the **Share Path** text box. This path is not the network path (such as `\\system1\deploy\`), but is the local path to the shared folder (such as `c:\deploy\`).

- 10 Click **Next**.

Avalanche attempts to contact the server location to verify that all the information is correct. After a few moments, the *Connection Results* dialog box appears and displays if a connection was established to the Servers.

- 11 Click **Next**.

The *dServer Location Created* dialog box appears.

- 12 Click **Finish**.

The server location appears in the region where you created it. You can assign the server location to a different region, deploy Servers to the server location or modify the server location. For information on deploying servers, see *Deploying Servers* on page 290.

Understanding Unassigned Server Locations

The **Unassigned Server Locations** folder, located in the Navigation Window, is a temporary location for server locations that have not been assigned to a region. Server locations are placed in the **Unassigned Server Locations** folder when they are first created (if you have not specified a region). Once a server location is placed in the **Unassigned Server Locations** folder, you can assign that server location to a region.

Unassigned server locations will download the default profiles (network, software, etc.) but do not get any configured profile settings and do not receive updates such as Server settings, software packages, or Infrastructure profiles. Mobile devices will not connect to unassigned server locations. Server locations restored from the Deleted dServer Locations folder to the **Unassigned Server Locations** folder retain their last configuration.

Moving Server Locations to Regions

You may need to move an existing server location if the location was never assigned to a region, if a region was deleted, or if you want to restructure your network hierarchy. A server location must belong to a region before you can manage its settings.

To move a server location to a region:

- 1 Right-click a server location in the **Unassigned Server Locations** folder, and select **Move Location To Region** from the context menu.

The *Select a Region* dialog box appears.

- 2 Select the destination region and click **Select**.

The server location moves to the selected region and you can begin managing your mobile devices.

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.
- 4 Save your changes.

Assigning Profiles to Server Locations

You can assign any configured profile to a server location from the **Server Location Properties** tab. You use the same method to assign profiles to a server as you do to assign profiles to regions. For detailed steps of assigning a profile, refer to *Assigning Profiles* on page 81.

Deleting Server Locations

If a server location becomes unnecessary, you can delete it from the Avalanche Console. To retain historical data, Avalanche does not immediately remove server locations that you have decided to delete. Instead, these server locations move to the **Deleted Server Locations** folder, and cease to receive any new configuration values from the Avalanche Console. You can then access historical data about the server location at a later date.

From the **Deleted Server Locations** folder you can perform the following tasks:

- Removing Server Locations
- Restoring Server Locations

NOTE To completely remove a server location, you must first remove the Servers associated with that server location.

To move a server location to the Deleted Server Locations folder:

- Select the server location from the Navigation Window and press the **Delete** key.

-Or-

- Right-click the server location and select **Delete** from the context menu.

Removing Server Locations

You can completely remove server locations located in the **Deleted Server Locations** folder. When you remove server locations from the **Deleted Server Locations** folder, the server location and historical data are completely deleted from the databases.

To completely remove a server location, you must first remove the Servers associated with that server location. For information about removing Servers, refer to *Backing Up the System* on page 294.

To completely delete a server location:

- Select the server location from the Navigation Window and press the Delete key.

-Or-

- Right-click the server location and select **Delete** from the context menu.

NOTE You can stop the Server service and then delete the server location to remove it completely. However, if you start the Server service, Avalanche will automatically detect any deleted server locations and place them in the **Unassigned Server Locations** folder. Wavelink recommends removing Servers completely before deleting server locations.

Restoring Server Locations

If you restore a server location, the server location returns to the **Unassigned Server Locations** folder. From this region you can assign the restored server location back to the appropriate region.

To restore a server location:

- 1 In the Navigation Window, select **Deleted Devices**.
- 2 Right-click the server location you want to restore and select **Restore** from the context menu.

The server location is restored to the **Unassigned Server Locations** folder.

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

Creating a Site

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

To create a site:

- 1 Right-click the server location where you want to place the site 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.

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.

The properties consist of user-defined properties. Properties can be used as selection variables in selection criteria to control which devices receive particular updates.

NOTE Refer to *Chapter 18: Using Selection Criteria* on page 271 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.

Assigning Profiles to Sites

You can assign any configured profile — except Mobile Device Server Profiles and Infrastructure Profiles — to a site from the **Site Properties** tab. You use the same method to assign profiles to sites as you do to assign profiles to regions. For detailed steps about assigning profiles, refer to *Assigning Profiles* on page 81.

Additional Site Functions

Sites include several other functions, allowing 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:

Copy	Allows you to copy the site.
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.

Editing Exclusions

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

The profile will also be excluded from any associated sub-regions or locations. For example:

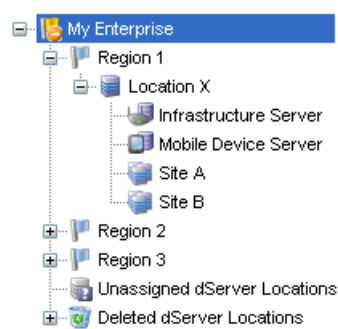


Figure 6-3. *Navigation Window for Editing Exclusions*

When a profile is applied at My Enterprise, it is also applied to all regions. However, if it is excluded at Region 1, the profile will also be excluded from Location X and Sites A and B.

When a profile has been excluded from a parent region, you can allow a sub-region or location to apply it. Using the above example, you could reapply a profile to Site A that has been excluded at Region 1. (It would still be excluded at Site B.)

To exclude an inherited profile:

- 1 From the Navigation Window, select the region, location or 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, but will still appear in the **Applied Profiles** tab for all sub-regions or locations.

To re-apply an inherited profile:

- 1 From the Navigation Window, select the region, location or site at which you want to re-apply an inherited profile.
- 2 Select the **Properties** tab.

- 3 On the **Applied Profiles** tab, click **Edit Exclusions**.
- 4 Disable the **Excluded** check box for the inherited profile you want to reapply.
- 5 Click **Save**.

The profile will be applied for the selected area. It will also be inherited as an applied profile, rather than as an excluded profile.

Managing Servers

This section provides the following information about managing your servers:

- Building Server Deployment Packages
- Server Auto-Discovery
- Stopping Servers
- Starting Servers
- Viewing Server Properties
- Reinitializing the Mobile Device Server
- Monitoring Server Status

Building Server Deployment Packages

After you create a server location in the Avalanche Console, you need to deploy the server software to the system you want it to run on. A deployment package is a collection of files that define Server behavior for both Infrastructure and Mobile Device Servers. You must create these packages and then deploy them in order to control your server locations.

You can build deployment packages for the following:

- **Combined Infrastructure and Mobile Device Servers.** When you create a combined deployment package for both infrastructure and mobile devices, Avalanche deploys an Infrastructure Server and a Mobile Device Server to a server location that may or may not have Servers already.

- **Infrastructure Server.** When you create a deployment package for Infrastructure Servers, Avalanche deploys a full-function Infrastructure Server to a server location that may or may not yet have an Infrastructure Server.

NOTE When you create an infrastructure server package, you are given the option to use **No Security**, **Security without encryption**, or **Security with encryption**. When security is enabled, the Infrastructure Server will use secure methods to communicate with the Infrastructure Site Console.

- **Lightweight Infrastructure Server Update.** An update package updates an existing Infrastructure Server to the latest version of Avalanche without changing any settings or deploying any firmware files. The resulting deployment package will be much smaller in size because this package only replaces the core executables.
- **Mobile Device Server.** Creates a deployment package that will manage mobile devices at a specific server location.
- **Linux Agent RPMs.** This deployment package allows you to select Linux RPMs to deploy to your locations.

NOTE When you are creating Combined Server, Infrastructure Server or Lightweight updates, you will have the options of configuring network adapters, security options and firmware binaries. These options are not available for Mobile Device Server or Linux RPMs.

To create a deployment package:

- 1 Click **Tools > Deployment Packages**.

The *Deployment Package Manager* appears.

- 2 Click **Add** to open the *New Package Wizard*.

- 3 Follow the prompts to build the package you need.

- 4 When your package is built, click **Finish** to return to the *Deployment Package Manager*.

- 5 Continue building packages or click **Close**.

The packages you build will now appear in the Task Scheduler and are ready to be deployed to your locations.

Server Auto-Discovery

If you have installed Avalanche on a system and deployed a Mobile Device Server, an Infrastructure Server, or both, the servers are continually attempting to contact Avalanche. When you uninstall Avalanche from a system but do not remove the distributed servers, the servers still attempt to contact that enterprise server. If you reinstall Avalanche on that same system, those servers are automatically discovered and appear in the **Unassigned Server Locations** folder in the following format: `Server Location:x.x.x.x`.

If you install the enterprise server on a different system, Servers are not auto-discovered. You need to redeploy Mobile Device Servers and Infrastructure Servers.

Stopping Servers

If you have installed Avalanche on a system and deployed a Mobile Device Server, an Infrastructure Server, or both, you have the ability to start and stop the Server from the Avalanche Console.

To stop a server:

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

Starting Servers

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

To restart a server:

- From the Navigation Window, right-click the server you want to restart 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 Server you want view properties for and select **Mobile Device Server Properties or Infrastructure Server Properties** (depending on which type of server you selected).

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 you want reinitialize and select **Reinitialize Mobile Device Server**.

The server contacts the Enterprise Server and downloads any updates.

Monitoring Server Status

When you select a server location in the Navigation Window, you can view server information on the **Distributed Server Status** tab. You can not modify any information in this tab.

The following information displays in the columns:

- **Region.** Lists the region to which the Server is assigned.
- **Location.** Lists the location (machine name) where the Server resides.
- **Site Address.** Lists the IP address of the server location.
- **Version.** Specifies the version of Server deployed to the location.

- **Status.** Indicates the current status of the Server.



Indicates the Server is currently offline.



Indicates the Server is currently online and running.

- **Deployed.** Displays the status of the Server deployment.



Indicates changes have been made but are not yet deployed to the Server.



Indicates changes have been deployed but are not yet applied to the Server.



Indicates the Server is up-to-date with the latest changes.

- **Blackout.** Displays the Server blackout window status.



Indicates that the Server is not currently in a blackout window.



Indicates the Server is currently in a blackout window and not available.

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.

Configuring Infrastructure Servers at Server Locations

Although you manage much of your wireless network with the Avalanche Console, certain server locations might require additional infrastructure configuration or management. To accommodate this need, you can access the Infrastructure Site Console. This tool allows you to fine-tune your wireless network by configuring your wireless network components and mobile device software at the server location level.

To access the Infrastructure Site Console tool:

- Right-click a server location in the Navigation Window and select **Launch Infrastructure Site Console** from the menu that appears.
- Or -
- Select a server location; then select **Launch Infrastructure Site Console** from the **Tools** menu.

You will be required to login to the Infrastructure Site Console. Your specific Avalanche user login and password must have been deployed to the Infrastructure Server before you will be able to log in.

The Infrastructure Site Console appears in a separate window on your desktop. See *Mobile Manager User's Guide* for more information on the features of the application.

Infrastructure Site Console and the Avalanche Console

To ensure that your wireless network is managed correctly, it is important to understand the relationship between the configurations established using the Avalanche Console, and those established using the Infrastructure Site Console. Because the Avalanche Console is designed to distribute wireless

device settings across your entire network, it can conflict with settings applied to a specific server location. These conflicts can be easily avoided, however, by using the following guidelines when applying device configurations at the server location level:

- IP addresses can be assigned either by the Avalanche Console or by the Infrastructure Site Console, but not both. Consequently, you must decide before you assign IP addresses if you want to manage them centrally or at the Infrastructure Server level.
- WEP and WEP key rotation settings assigned at the enterprise level will override any corresponding settings at the Infrastructure Site level.
- The Avalanche Console is designed to apply configuration settings to groups of server locations. To configure an individual server location from the Avalanche Console, you can do so by creating a region that contains only that server location and applying settings to that region.

Chapter 7: Managing Network Profiles

A network profile is a group of configurations that you can apply to your wireless devices. Once the wireless devices are configured with the network values configured in the network profile, you can manage the devices through the Avalanche Console. If your wireless devices do not have the appropriate network values, you will not be able to manage them. Creating network profiles allows you to configure multiple devices on your network at once.

Network profiles allow you to configure the following parameters for your wireless devices:

- **Network information.** You can set network information such as gateway addresses and subnet masks for both infrastructure and mobile devices.
- **IP addresses.** You can select the method by which infrastructure and mobile devices receive their IP address assignments.
- **Security encryption and authentication.** You can select the types of encryption and authentication you want your wireless devices to use.
- **Epochs.** You can assign a specific time for a network profile change to take effect by creating a network Epoch.

This section contains the following topics:

- Creating Network Profiles
- Configuring Network Profiles
- Applying Network Profiles
- Viewing Where Network Profiles are Applied

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 region or 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 and/or infrastructure 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

The **Authorized Users** button allows you to assign administrative privileges for a specified 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.

For information about creating users and assigning permissions, refer to *Chapter 5: Managing User Accounts* on page 64.

To add an authorized user:

- 1 From the **Profiles** tab, select the network profile you want to configure.
- 2 Click **Edit**.
- 3 From the **Network Profile** tab, click **Authorized Users**.

The *Profile Authorized Users* dialog box appears.

NOTE If you are not in Edit Mode, you will be able to click **Authorized Users** and view current authorized users but will not be able to make any changes.

- 4 Click **Add User**.

The *Add Authorized User* dialog box appears.

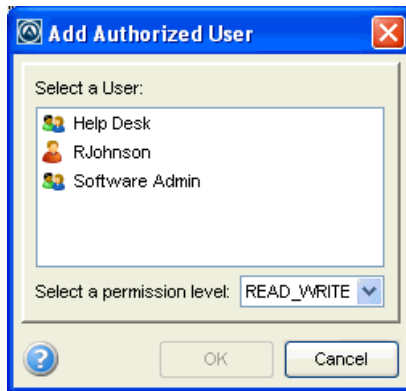


Figure 7-1. *Add Authorized User* dialog box

- 5 From the list, select the user.
- 6 From the drop-down list, select the level of permission.
- 7 Click OK.
- 8 The user is added to the list of authorized users.

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 *Chapter 18: Using Selection Criteria* on page 271.

Configuring Scheduled Settings

From a network profile, you can configure WLAN IP settings, WLAN SSID, encryption and authentication settings, and WWAN settings. These configurations are based on epochs, so they are considered scheduled settings.

Epochs allow you to change the settings for a network profile and apply those changes at a specific time. When you configure WLAN IP, WLAN, and WWAN settings, you select which epoch those settings are effective for.

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

NOTE There is a maximum of 50 epochs per network profile.

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).
(Infrastructure Device IP Settings) Manage IP Assignment	This option allows you to manage the IP addresses assigned to your infrastructure devices with a DHCP server.

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 which epoch you want the settings effective for from the drop-down list. If you would like to add an epoch to the drop-down list, click **Add** and select the date and time you want the epoch to begin.
- 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 reconnect 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 which epoch you want the settings effective for from the drop-down list. If you would like to add an epoch to the drop-down list, click **Add** and select the date and time you want the epoch to begin.
- 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 provide a path to the certificate.
- If you are using EAP_FAST, you can provide a path to a PAC (Protected Access Credential).
- 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 which epoch you want the settings effective for from the drop-down list. If you would like to add an epoch to the drop-down list, click **Add** and select the date and time you want the epoch to begin.
- 5 Select the **WWAN Settings** tab.
- 6 Configure the WWAN settings as desired.
- 7 Save your changes.

Applying Network Profiles

Once you have created a network profile, you can assign that profile to a region. The profile will be deployed to all the Server locations in that region when you perform a Universal Update. There is no limit on how many network profiles can be applied to a region. The profiles are applied to the mobile devices based on selection criteria for the profile and the priority in which the profiles are listed in the Avalanche Console.

For information about applying software profiles to regions, refer to *Assigning Profiles* on page 81. For information about deploying Universal Updates, refer to *Performing a Universal Deployment* on page 289.

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, you will need to access the Region or Server Location Properties tabs and assign the profiles there. For information, refer to *Assigning Profiles* on page 81.

The **Applied Locations** 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 network profile you want to view.
- 2 Click the **Applied Locations** tab.

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 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

The **Authorized Users** button allows you to assign administrative privileges for a specified 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.

For information about creating users and assigning permissions, refer to *Chapter 5: Managing User Accounts* on page 64.

To add an authorized user:

- 1 From the **Profiles** tab, select the Scan to Config Profile you want to configure.
- 2 Click **Edit**.
- 3 From the **Scan-to-Config Profile** tab, click **Authorized Users**.

The *Profile Authorized Users* dialog box appears.

NOTE If you are not in Edit Mode, you will be able to click **Authorized Users** and view current authorized users but will not be able to make any changes.

- 4 Click **Add User**.

The *Add Authorized User* dialog box appears.

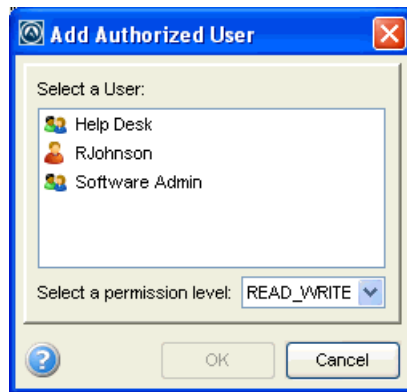


Figure 8-1. *Add Authorized User* dialog box

- 5 From the list, select the user.
- 6 From the drop-down list, select the level of permission.
- 7 Click **OK**.

The user is added to the list of authorized users.

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

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 **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.

NOTE Most properties will be device properties.

- 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 126.

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 to any region in the Console. When you apply a profile to a region, the users who have permissions for that region can make changes as necessary. For more information about assigning Scan to Config Profiles to a region, refer to *Assigning Profiles* on page 81.

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.

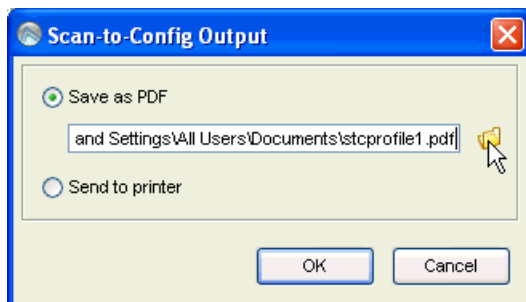


Figure 8-2. *Scan-to-Config Output* dialog box

- 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 network settings are applied and the *Scan Configuration* dialog box closes.

Chapter 9: Managing Infrastructure Distributed Servers

The Infrastructure Server is server software that allows you to remotely manage and configure infrastructure devices such as access points and routers. Although you can use multiple Servers at different Server Locations or on different network segments, you can manage all of your Servers from one Avalanche Console, regardless of where the Console resides on the network.

NOTE In early versions of Avalanche, Distributed Servers (or Servers) were referred to as Agents in both the user interface of the Avalanche Console and the documentation. The Mobile Device Agent managed mobile devices and the Access Point Agent managed access points and other network devices. Starting with Avalanche 4.1 release, Agents are referred to as Servers both in the user interface and the documentation. The Mobile Device Agent is the Mobile Device Server. The Access Point Agent is the Infrastructure Server.

Infrastructure Server Profiles allow you to define device access privileges for your Infrastructure Servers. Once you have configured an Infrastructure Server Profile, you can apply that profile to any region and deploy those settings to all Infrastructure Servers in that region.

This section provides information about the following tasks:

- Creating Infrastructure Server Profiles
- Configuring Infrastructure Server Settings
- Configuring Infrastructure Server Blackouts
- Viewing Where Infrastructure Server Profiles Are Applied
- Applying Infrastructure Server Profiles to Regions
- Removing an Infrastructure Server Profile
- Viewing Infrastructure Server Licensing Messages

Creating Infrastructure Server Profiles

Infrastructure Server Profiles are used to manage your Infrastructure Servers. Profiles allow you to configure data collection, access privileges, and other settings for the Server.

To create an Infrastructure Server profile:

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

The *Create Profile* dialog box appears.

- 2 From the **Profile Type** drop-down list, select **Infrastructure Server Profile**.
- 3 Type a name for the profile in the text box and click **OK**.

The profile is added to the **Profile List**.

Configuring Infrastructure Server Settings

You can configure the following options from the **Infrastructure Server Profile** tab:

- Enabling an Infrastructure Server Profile
- Configuring Data Collection
- Infrastructure Server Profile Authorized Users
- Defining Device Access Privileges

Enabling an Infrastructure Server Profile

You can set the status of an Infrastructure Server Profile to enabled or disabled. The profile can only be applied when it is enabled. If the profile is disabled after it has been applied, Avalanche will replace the settings with a default profile.

To enable an Infrastructure Server profile:

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

3 In the **Infrastructure Server Profile** tab, enable the **Enabled** option.

4 Save your changes.

You can now assign the profile to any region.

Configuring Data Collection

You can configure the types of data collected by the Infrastructure Server with the Infrastructure Server Profile. By suppressing data collection, you may increase the efficiency of the Server. When the data is not collected by the Infrastructure Server, no statistics are sent to the Stats Server either.

The options available for Infrastructure Server data collection include:

Suppress Infra Statistics Data Collection When this option is enabled, no infrastructure statistics are collected by the Infrastructure Server. This option overrides all the other data collection options.

Suppress Performance Statistics Data Collection When this option is enabled, no statistics such as utilization, capacity, bytes received/sent, or packets received/sent are collected by the server.

Suppress Current Statistics Data Collection When this option is enabled, no statistics representing the current state of infrastructure devices are collected by the server.

NOTE If you plan on generating any infrastructure device reports, current statistics should not be suppressed.

Suppress Running Statistics Data Collection When this option is enabled, no statistics regarding device status changes are collected by the server.

Suppress Associated MD Data Collection When this option is enabled, no statistics regarding associated mobile devices (such as RSSI measurements) are collected by the server.

Limit Running Statistics Data Quantity When this option is enabled, certain running statistics (such as device state changes) are not collected by the server.

To configure data collection for an Infrastructure Server Profile:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Infrastructure Server Profile** tab, enable the desired options in the **Data Collection** region.

NOTE If you enable **Suppress Infra Statistics Data Collection**, all data collection will be suppressed.

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

Infrastructure Server Profile Authorized Users

The **Authorized Users** tab allows you to assign administrative privileges to a specified profile to a user that has Normal user rights and is not assigned permissions to that profile. This means that any user assigned as an authorized user to an Infrastructure Profile will have administrative rights for that one profile.

To add an authorized user you must have at least one user configured with Normal permissions. For more information about creating users and assigning permissions, refer to *Chapter 5: Managing User Accounts* on page 64.

To add an authorized user:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Infrastructure Server Profile** tab, click the **Authorized Users** button.

The *Profile Authorized Users* dialog box appears.

- 4 Click **Add User**.

The *Add Authorized User* dialog box appears.

- 5 From the user list, select the user and the choose **READ_WRITE** or **READ_ONLY** for the permission level. Click **OK**.

The user is added to the **Authorized Users** list for the profile.

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

Defining Device Access Privileges

To manage wireless network components—including access points, switches, and routers—a Server must have the correct authorization. These authorizations are called device access privileges, where a privilege is an identified right that a particular user has to a particular infrastructure network device. The type of authorization required varies, depending on which protocol the Server uses to configure the component. The types of authorizations are as follows:

- SNMP Read-Only community name
- SNMP Read/Write community name
- Telnet password
- HTTP user name and password
- SNMP v3 user name

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

Hardware	Authorization
Switches	SNMP Read-Only community name
Cisco-Aironet 350/1200 Series Access Point	SNMP Read/Write community name HTTP user name and password
Cisco-Aironet (IOS)	SNMP Read/Write community name HTTP user name and password Telnet community name and password Telnet Enable password

Table 9-1: Authorization Required for Component Queries

Hardware	Authorization
Symbol Access Point	SNMP Read/Write community name SNMP Read-Only community name HTTP user name and password
Symbol Wireless Switch	SNMP Read/Write community name SNMP Read-Only community name Telnet password
Proxim Access Point	SNMP Read-Only community name SNMP Read/Write community name
Dell Access Point	SNMP Read-Only community name SNMP Read/Write community name

Table 9-1: *Authorization Required for Component Queries*

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

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

NOTE To give servers new device access privileges, you must deploy the information to the Servers. See *Performing a Universal Deployment* on page 289 for more information.

This section contains the following information:

- Defining Access Privileges
- Configuring SNMP V3 Settings
- Cisco IOS Access Privileges

- Replacing Insecure Protocols and Default Passwords

Defining Access Privileges

For Avalanche to manage your infrastructure devices, the Infrastructure Servers must have device access privileges.

To define device access privileges:

- 1** From the **Profiles** tab, select the profile for which you are defining privileges.
- 2** Click **Edit**.
- 3** If you want to display the names and passwords, click **Show Password**. If you do not click **Show Password**, the passwords will remain masked.
- 4** In the **Infrastructure Server Profile** tab, find the **Device Access Privileges** region. Configure the privileges for the profile.
 - To add an SNMP Read-Only user name, select the **SNMP R/O** tab, enter the community name in the text box at the bottom of the region and click **Add**.
 - To add an SNMP Read/Write user name, select the **SNMP R/W** tab, enter the community name and click **Add**.
 - To add a Telnet password, select the **TELNET** tab, enter the password and click **Add**.
 - To add an HTTP user name, select the **HTTP** tab and click **Add**. A dialog box appears, allowing you to enter a user name and password for the account. Each account must be assigned to a specific hardware manufacturer, such as Cisco or Symbol.

NOTE To manage Cisco-Aironet Access Points with the Avalanche Console, you must have both an HTTP account that has administrative privileges and an authorized SNMP Read/Write user name. HTTP access must be enabled on the infrastructure device.

- To add an SNMP V3 user, select the **SNMP V3** tab and click **Add**. A dialog box appears, allowing you to enter a user name, passwords, and

protocols for the account. For more information on SNMP V3 options, see Configuring SNMP V3 Settings.

NOTE Once you navigate away from the profile, save changes or cancel changes, the passwords will be hidden.

5 Save your changes.

Configuring SNMP V3 Settings

The SNMP V3 settings you configure in Avalanche are based on the type of access point you are configuring and the configurations of that device. Ensure you have the proper information about the device before you configure in Avalanche.

There are three levels of permissions that you can configure using SNMP V3:

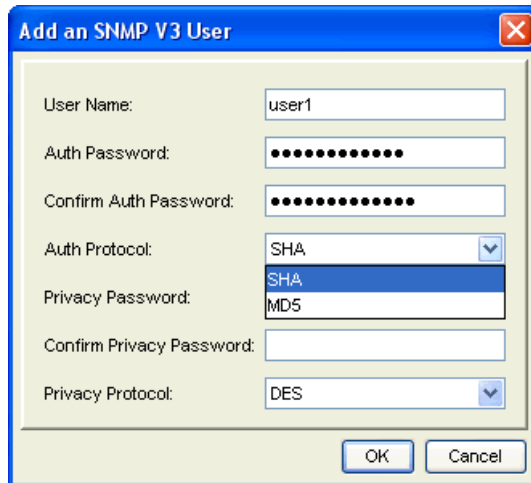
- User Name only (there is no authentication or privacy)
- User Name and Authentication (SHA or MD5).
- User Name, Authentication (SHA or MD5) and Privacy Protocol (DES or AES).

The level of permissions must be based on the settings your device supports and is configured with.

To add SNMP V3:

- 1 From the **Profiles** tab, select the profile for which you are defining privileges.
- 2 Click **Edit**.
- 3 In the **Infrastructure Server Profile** tab, find the **Device Access Privileges** region.
- 4 Click the **SNMP V3** tab.
- 5 Click **Add**.

The *Add an SNMP V3 User* dialog box appears.



The screenshot shows a dialog box titled "Add an SNMP V3 User". It contains the following fields and controls:

- User Name: user1
- Auth Password: [masked]
- Confirm Auth Password: [masked]
- Auth Protocol: SHA (dropdown menu)
- Privacy Password: [empty]
- Confirm Privacy Password: [empty]
- Privacy Protocol: DES (dropdown menu)
- Buttons: OK, Cancel

Figure 9-1. Add User

- 6 Enter a **User Name**.
- 7 Enter an **Auth Password**. Passwords must be at least eight characters long.
- 8 Continue configuring the user authentication and privacy based on your device settings.
- 9 Click **OK** when you are finished.

The user name will appear in the **SNMP V3** tab.

Cisco IOS Access Privileges

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

By default, the Telnet user name, password, and Enable password for Cisco IOS access points is "Cisco". If you enabled security for managing infrastructure devices when you installed the infrastructure server package, this default Telnet information is removed to prevent unauthorized use of the infrastructure device.

Avalanche will enable SNMP on the access point provided it can enter Enable mode. By default, SNMP is disabled and no SNMP Read/Write user exists.

If you installed the infrastructure server package with security disabled, Avalanche will add a public SNMP Read/Write user. If you installed Avalanche with security enabled, Avalanche will add a SNMP Read/Write user with the same value as the Telnet user name. Avalanche will remove the public SNMP Read/Write user any time you enable its security features.

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

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

To define Cisco IOS access privileges:

- 1 In the **Profiles** tab, select the profile for which you are defining privileges.
- 2 Click **Edit**.
- 3 In the **Device Access Privileges** region, configure the privileges for the profile.
 - If you modified the Cisco IOS infrastructure device so that its Telnet Enable password is not "Cisco," select the **TELNET** tab. Enter the Telnet Enable password that Avalanche requires and click **Add**.
- 4 Select the **HTTP** tab and click **Add**.
- 5 In the dialog box that appears, enter an HTTP user name and password. For Cisco IOS access points, this information is used as follows:

- HTTP user name is used as the Telnet user name.
 - HTTP password is used as the Telnet and Telnet Enable passwords.
- 6** Enable the **Make This User a Cisco AP Administrator** checkbox to make the new account a Cisco AP administrator.

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

7 Save your changes.

Replacing Insecure Protocols and Default Passwords

From the **Device Access Privileges** region on the Infrastructure Server profile, you can configure the devices currently using Telnet to switch to SSH, and devices using SNMP v2 to use SNMP v3.

You can also specify replacement passwords for devices that are currently using the manufacturer default passwords for SNMP v2, Telnet, and SNMP v3.

The following table lists which devices support the options in the **Security** tab:

Devices	Replace Telnet with SSH	Replace SNMP v2 with SNMP v3	Replace Defaults for SNMP v2	Replace Defaults for Telnet	Replace Defaults for SNMP v3
Symbol WS 5100 V3.0+, RFS 6000, RFS 7000	yes	yes	yes	yes	yes
Symbol WS 2000	yes	no	yes	no	no
Symbol AP 7131, 51x1	yes	no	yes	no	no
Symbol AP 4131	yes (firmware 3.95-04 and later)	no	yes	password only	no
Symbol AP 4121	no	no	yes	password only (firmware 02.70-12 and later)	no
Cisco IOS	yes	no	yes	yes	no
Cisco VxWorks	no	no	yes	no	no

Table 9-2: Devices Supporting Security Tab Options

Devices	Replace Telnet with SSH	Replace SNMP v2 with SNMP v3	Replace Defaults for SNMP v2	Replace Defaults for Telnet	Replace Defaults for SNMP v3
Proxim	yes	no	yes	password only	no
Avaya/SYSTIMAX	no	no	no	no	no

Table 9-2: *Devices Supporting Security Tab Options*

To change Telnet or SNMP settings:

- 1 In the **Profiles** tab, select the profile for which you are defining privileges.
- 2 Click **Edit**.
- 3 In the **Device Access Privileges** region, select the **Security** tab.
 - If you want to change all Telnet communication to SSH, enable the **Enable secure protocols and disable insecure protocols** option. This will also change SNMP v2 to SNMP v3 on devices that support this feature.

NOTE Disabling this check box after the settings have been applied will not enable Telnet or SNMP v2. If you want to revert to using Telnet or SNMP v2, you will need to change the device properties using the Infrastructure Site Console.

- If you want to change manufacturer default SNMP or Telnet credentials, enable the **Replace default SNMP and Telnet credentials** option, then type the new names/passwords in the appropriate text boxes.

NOTE If you change the credentials on the **Security** tab, ensure you also change the credentials on the corresponding **Device Access Privileges** tab.

- 4 Save your changes.

The settings are applied the next time a device is queried after the settings have been deployed to the server.

Configuring Infrastructure Server Blackouts

To eliminate heavy bandwidth usage and control the flow of connections to the Enterprise Server, you can configure blackout windows. Blackout windows prevent the Infrastructure Servers from contacting the Enterprise Server. Configure blackout windows based on when and how often you want the Servers connecting to the Enterprise Server.

The **Server Synchronization Blackout Windows** region allows you to create blackout windows and displays all the blackout windows scheduled to occur.

To configure Infrastructure Server blackout windows:

- 1 In the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Infrastructure Server Profile** tab, find the **Server Synchronization Blackout Windows** region and click **Add**.

The *Add Blackout Window* dialog box appears.

- 4 Using the **Start Time** and **End Time** boxes, select the time of day when you want the blackout to occur.
- 5 Enable the days of the week on which you want the blackout to occur.
- 6 Click **OK**.

The blackout window appears in the list.

- 7 Save your changes.

Viewing Where Infrastructure Server Profiles Are Applied

The **Applied To** 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 can not 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 To** tab, you will need to access the Region or Server Location Properties tabs and assign the profiles there. For information, refer to *Assigning Profiles* on page 81.

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 network profile.

Applying Infrastructure Server Profiles to Regions

Once you have created an Infrastructure Server Profile, you can assign it to any region in your enterprise. For more information about applying an Infrastructure Server Profile to a region, refer to *Assigning Profiles* on page 81. For more information about installing servers and deploying server settings, refer to *Deploying Servers* on page 290.

Removing an Infrastructure Server Profile

If you no longer are using an Infrastructure Server Profile, you can remove it from the Console. When you remove an Infrastructure Server Profile from the Console, any servers assigned to that profile will retain those profile settings until a new profile is deployed to that server.

To remove an Infrastructure Server Profile:

- 1 In the **Profiles** tab, select the profile from the Profile List and click **Remove Profile**.

The *Confirm Delete* dialog box appears.

- 2 If you want to remove the profile, click **Yes**.

The profile is removed from the list.

Viewing Infrastructure Server Licensing Messages

The Avalanche Console receives licensing messages from the deployed Infrastructure Servers. You can view these messages from the *dServer Licensing Messages* dialog box.

To view licensing messages:

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

The *dServer Licensing Messages* dialog box appears.

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

NOTE You can also view messages specific to a server by right-clicking the name of the server in the Navigation Window and selecting **Infrastructure Server Properties**.

Chapter 10: Managing Infrastructure Profiles

An infrastructure profile is a collection of settings that you can simultaneously apply to multiple infrastructure devices, allowing you to manage your network setup. Avalanche not only applies these settings to devices—it also enforces these settings, preventing unauthorized modifications.

When the Infrastructure Server receives an infrastructure profile, each infrastructure device that reports to that Server compares the hardware type configured for the profile. If the hardware and firmware listed in the profile match the device, the device assumes the profile.

NOTE For information on the infrastructure devices and firmware supported by Avalanche, see *Appendix D:Supported Firmware* on page 314.

Infrastructure Considerations

- Not all infrastructure devices support every feature of network profiles.
- From the **Infrastructure Inventory** tab, you can view what type of profile a particular infrastructure device is using. You can right-click any device to view the details about the profile as well as access the Advanced Properties.
- Avalanche has several security features that help prevent unauthorized access to your wireless network:
 - You can use a Very Large Access Control List to restrict mobile devices by MAC address. For more information, see *Chapter 12:Managing Very Large Access Control Lists* on page 179.
 - You can use encryption and authentication to secure your network. See *Chapter 7:Managing Network Profiles* on page 105 for more information on security protocols.

NOTE Do not disable the Web interface to Cisco-Aironet access points. Doing so prevents the Server from managing them.

This section provides information about the following topics:

- Creating Infrastructure Profiles
- Configuring Infrastructure Profiles
- Viewing Where Infrastructure Profiles Are Applied
- Configuring Infrastructure Scheduled Events
- Configuring WLANs
- Applying Infrastructure Profiles
- Importing an Infrastructure Device Support File
- Importing an Infrastructure Device Support File
- Adding Custom Properties
- Updating Infrastructure Device Firmware

Creating Infrastructure Profiles

Once you have organized your server locations into regions, you can create and assign infrastructure profiles. During a Universal Deployment, the Avalanche Console takes the configuration values for each profile assigned to a region and distributes them to the Infrastructure Servers associated with that region. The servers apply the profiles to infrastructure devices with the appropriate firmware.

Infrastructure profiles can be created for any hardware type that Avalanche supports. You can create profiles to be as basic or as detailed as your wireless network demands.

To create an infrastructure profile:

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

The *Create Profile* dialog box appears.

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

The infrastructure profile is created and can be enabled, configured, and assigned to a region or location.

After creating an infrastructure profile, you must enable it in order to apply it to your devices.

Configuring Infrastructure Profiles

You can configure infrastructure profiles as your network demands. This section provides information about the following:

- Infrastructure General Settings
- Editing Advanced Properties
- Assigning Infrastructure Profile Authorized Users
- Configuring Infrastructure Selection Criteria

Infrastructure General Settings

In the **Infrastructure Profile** tab, you can edit the infrastructure profile name, status, and default WLAN ID based on the needs of your infrastructure.

The following table provides information about the infrastructure profile settings in the **General Settings** tab.

Field	Description
Name	Sets the name of the profile.
Status	Sets the status of the profile as either enabled or disabled.
Hardware Model	Displays the hardware type of the infrastructure device.
Firmware Version	Displays the firmware version for the infrastructure device.
Default WLAN ID	Sets the number of the default WLAN ID.
Authorized Users	Sets the users authorized to view, apply and edit the profile.
Use Legacy Management	Determines whether infrastructure settings are defined using the Infrastructure Profiles tab or the <i>Advanced Properties</i> dialog box. This option is not user configurable.
Use 802.1Q Tagging	Determines whether to use 802.1Q tagging, the specification that establishes a standard method for tagging Ethernet frames with WLAN membership information.

Table 10-1: *General Settings*

Field	Description
Manage Infrastructure Using Secure Method	Determines whether the infrastructure device is managed using a secure method (such as SSH).
Edit Advanced Properties	This button allows you to configure advanced options for your infrastructure devices.

Table 10-1: *General Settings*

The **Manage Infrastructure Using Secure Method** option is only supported by the following infrastructure devices: Cisco IOS, Symbol 5131, and Symbol WS 2000.

To configure general settings for an infrastructure profile:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 Ensure you are on the **Infrastructure Profile** tab.
- 4 To enable the profile, select **Enabled**.
- 5 Click **Authorized Users** to assign a Normal user permissions for the profile.
- 6 If you have created multiple WLANs, you can select the default WLAN ID for this profile.
- 7 Save your changes.

The infrastructure profile is enabled and can be assigned to any region in the Console.

Editing Advanced Properties

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

If you are creating composite profiles, network settings will not appear in the advance properties dialog box. Network settings for composite profiles are configured in the network profile. For information about creating network

profiles refer to *Creating Network Profiles* on page 105. For more information about composite profiles, see *Configuring WLANs* on page 154.

To edit advanced properties:

- 1 From the **Profiles** tab, select the profile you want to configure from the list.
- 2 Click **Edit**.
- 3 In the **Advanced Settings** tab, click **Edit Advanced Properties**.

The *Advanced Properties* dialog box appears.

- 4 Configure the available options as desired. Some options may only be available with certain types of hardware or firmware.
- 5 When you are finished making changes, click **OK** to return to the Avalanche Console.
- 6 Save your changes.

Assigning Infrastructure Profile Authorized Users

The **Authorized Users** tab allows you to assign administrative privileges to for a specified profile to a user that has Normal user rights and is not assigned permissions to that profile. This means that any user assigned as an authorized user to a Infrastructure Profile will have all administrative rights for that one software profile.

To add an authorized user you must have at least one user configured with Normal permissions. For more information about creating users and assigning permissions, refer to *Chapter 5:Managing User Accounts* on page 64.

To add an authorized user:

- 1 From the **Profiles** tab, select the profile you want to configure.
- 2 Click **Edit**.
- 3 From the **Infrastructure Profile** tab, click **Authorized Users**.

The *Profile Authorized Users* dialog box appears.

NOTE If you are not in Edit Mode, you will be able to click **Authorized Users** and view current authorized users but will not be able to make any changes.

4 Click **Add User**.

The *Add Authorized User* dialog box appears.

5 From the list, select the user.

6 From the drop-down list, select the level of permission.

7 Click **OK**.

The user is added to the list of authorized users.

Configuring Infrastructure Selection Criteria

Selection criteria for an infrastructure profile determine which infrastructure devices will receive the profile.

To configure selection criteria:

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

2 Click **Edit**.

3 Click the **Selection Criteria** button to launch the Selection Criteria Builder.

4 Using the Selection Criteria Builder, create the selection criteria you want to assign to the profile.

For detailed information about creating selection criteria, refer to *Building Selection Criteria* on page 272.

5 When you are finished building your selection criteria, close the Selection Criteria Builder and save your changes.

Configuring Infrastructure Scheduled Events

You can schedule the following events for your infrastructure devices through an infrastructure profile:

- Reboot

- Disable All Radios
- Enable All Radios
- Disable 802.11a Radio
- Disable 802.11b Radio
- Disable 802.11g Radio
- Enable 802.11a Radio
- Enable 802.11b Radio
- Enable 802.11g Radio

NOTE Cisco (non-IOS) only supports the reboot event.

To schedule an event through an infrastructure profile:

- 1 From the **Profiles** tab, select the profile you want to configure.
- 2 Click **Edit**.
- 3 In the **Scheduled Events** tab, click **New Event**.

The *Scheduled Event* dialog box appears.

- 4 From the **Event Type** drop-down, select the type of event you want to schedule.
- 5 In the **Event Recurrence** region, select:
 - **One-Time Event** if you want the event to happen once.
 - **Recurring Event** if you want the event to happen on a daily or weekly basis.
- 6 If you select **Recurring Event**, configure the recurrence and the day of the week when you want the event to occur.
- 7 Click the calendar icon to select the date and time you want the event to occur.

8 Click **OK** to return to the *Scheduled Event* dialog box.

9 Click **OK** to close the *Scheduled Event* dialog box.

The event displays in the Scheduled Events list.

10 If you need to edit an event, select the event and click **Edit**.

11 Save your changes.

Configuring WLANs

When an infrastructure profile and a network profile are combined for an infrastructure device, the result is a composite profile. This ties together the hardware/firmware settings and the network/wireless settings. The following steps are an overview of creating a composite infrastructure profile:

- 1 Create an infrastructure profile. (See *Creating Infrastructure Profiles* on page 148.)
- 2 Create a network profile containing all the network and wireless settings that you want to apply to the infrastructure devices. (See *Creating Network Profiles* on page 105.)
- 3 Create a WLAN that binds the network profile and infrastructure profile. (See *Configuring WLANs* on page 154.)
- 4 Assign the profile to a server location or region. (See *Applying Infrastructure Profiles* on page 156.)
- 5 Assign the network profile to the same server location or region. (See *Assigning Profiles* on page 81.)
- 6 Deploy the configurations by performing a Universal Update. (See *Performing a Universal Deployment* on page 289.)

You can configure the following WLAN settings:

- **Network Profile.** You can select a specific network profile that binds to the infrastructure profile. The network profile determines all network and wireless settings. A network profile is used only once per infrastructure profile.

- **WLAN ID/Tag.** Enter the identification of the WLAN used by the standard 802.1Q.
- **Radio Type.** Select from A, B or G type radios. If your device does not specify which type of radio it uses, select G.
- **Broadcast SSID.** Select whether to broadcast the SSID associated with the network profile. This allows the SSID to be visible to devices that are scanning the network.
- **Disallow Device to Device Communication.** Enable this option to prevent mobile devices from communicating with each other.

NOTE You must create a network profile before you can create a WLAN. For information about network profiles, refer to *Chapter 7: Managing Network Profiles* on page 105.

To add a WLAN:

- 1 From the **Profiles** tab, select the profile you want to configure.
- 2 Click **Edit**.
- 3 In the **Infrastructure Profile** tab, click **Add WLAN**.

The *Add WLAN* dialog box appears.

- 4 From the **Network Profile** drop-down menu, select the profile to which you want to add the WLAN.
- 5 Enter the number of the **WLAN ID/Tag**.
- 6 From the **Radio Type** drop-down menu, select the radio type.
- 7 If you want the device to broadcast its SSID, enable the **Broadcast SSID** checkbox.
- 8 If you want to prevent the device from communicating with other devices, enable the **Disallow Device to Device Communication** checkbox.
- 9 Click **OK**.

The new WLAN appears in the **WLAN Configuration** region.

10 Save your changes.

Applying Infrastructure Profiles

You can assign as many Infrastructure profiles to a region or server location as you desire. The profiles are applied to the infrastructure devices based on selection criteria for the profile and the order in which the profiles are listed in the Avalanche Console. Once you assign an Infrastructure profile to a region, you must perform a Universal Deployment to update your Servers or you can deploy the settings immediately. For information about applying infrastructure profiles to regions, refer to *Assigning Profiles* on page 81. For information about deploying Universal Updates, refer to *Performing a Universal Deployment* on page 289.

Viewing Where Infrastructure Profiles Are Applied

The **Applied Locations** tab allows you to see exactly the 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, you will need to access the Region or Server Location Properties tabs and assign the profiles there. For information, refer to *Assigning Profiles* on page 81.

The **Applied Locations** 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 you want to view.
- 2 Click the **Applied Locations** tab.

The tab displays the information for the selected profile.

Importing an Infrastructure Device Support File

Device support files allow you to enable Avalanche to support a new infrastructure device. You must create a device support file for the new hardware/firmware, then import the file into Avalanche. Avalanche will use the support file to update the infrastructure device information.

NOTE For information about creating device support files, refer to the *Extended Device Support Reference Guide*, located on the Wavelink web site.

To import:

- 1 Ensure you have created a device support file and saved it in a zip file with the device icons. You should know the file location on your system.
- 2 From the Avalanche Console, select **File > Import > Extended Device Support**.

The *Extended Device Support* dialog box appears.

- 3 Click the **Import New Device** button.

The *Select Support File* dialog box appears.

- 4 Navigate to and select the `.zip` support file, then click **Select File**.

The *Select Support File* dialog box closes and a new dialog box appears, indicating whether the support file import was successful.

NOTE If the import was unsuccessful, the dialog box will indicate the reason the import failed. You can use this information to revise the support file as necessary.

- 5 Click **OK**.

If the file import was successful, the device information appears in the Supported Extended Devices list.

NOTE The support file does not include any device firmware. The firmware file must be imported separately. You can click on the **Remember to install the appropriate firmware** link, or import the firmware manually. See *Importing Firmware* on page 161 for more information.

- 6 If you want to remove a support file, select the appropriate file from the Supported Extended Devices list, and click **Remove**.
- 7 Click **Close** to exit the *Extended Device Support* dialog box and return to the Avalanche Console.

Once the support file and firmware have been imported, Avalanche will be able to support your device.

Adding Custom Properties

To add custom infrastructure device properties to new or existing devices, you must create a custom settings file. For information about creating these files, refer to the *Extended Device Support Reference Guide*, located on the Wavelink web site. After you create a custom settings file, import the file into Avalanche. Avalanche will use the file to update the infrastructure device information.

To add properties:

- 1 Ensure you have created a custom settings support file and know its location on your system.
- 2 From the Avalanche Console, select **File > Import > Custom Advanced Settings**.

The *Custom Advanced Settings* dialog box appears.

- 3 Click **Import New Setting**.

The *Select Custom Advanced Settings File* dialog box appears.

- 4 Navigate to and select the custom settings file and click **Select File**.

The *Select Custom Advanced Settings File* dialog box closes and the advanced settings information appears in the Installed Custom Advanced Settings list.

- 5 If you want to remove a custom settings file, select the appropriate file from the Installed Custom Advanced Settings list and click **Remove**.
- 6 Click **Close** to exit the *Custom Advanced Settings* dialog box and return to the Avalanche Console.

Once you have finished importing your support and firmware files, you need to build a firmware package with the new files. The firmware package should then be deployed to your Servers. For information on building a firmware package, see *Updating Infrastructure Firmware* on page 292.

Updating Infrastructure Device Firmware

Firmware is the software installed on infrastructure devices that determines what sort of properties and features that an infrastructure device supports. Avalanche supports a wide range of firmware for many different types of infrastructure devices.

When you first deploy an Infrastructure Server to a server location, you specify a selection of firmware that the Server supports. If you want to expand this selection, you can do so at any time by updating the infrastructure device firmware at the server location.

This section covers the following topics:

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

Types of Firmware Support

To support as many firmware versions as possible, Avalanche interacts with infrastructure devices in one of two ways: either in full support mode or in compatibility mode. Avalanche selects which mode to use based on whether it can recognize the firmware version installed on an infrastructure device. If neither mode is available for the firmware, the Avalanche does not manage the infrastructure device until the firmware version is changed.

Using the full support and compatibility modes provides you with a great deal of flexibility when determining what firmware versions you want to install on your infrastructure devices. These modes also reduce the risk of

infrastructure devices going unengaged because their firmware type was not recognized.

This section contains information on the following:

- Full Support Mode
- Compatibility Mode
- Supported Firmware
- Importing Firmware
- Manually Adding Firmware

Full Support Mode

If the firmware version installed on an infrastructure device matches a firmware version known to the Avalanche Server, the Server can communicate with that infrastructure device in full support mode. In full support mode, the Server is able to retrieve and set a vast majority of properties for that infrastructure device. This mode is the standard mode the Server uses to manage infrastructure devices.

Compatibility Mode

If the Server is unable to recognize the firmware installed on the infrastructure device, it attempts to communicate with it in compatibility mode. In compatibility mode, the Server relies on existing firmware property files to retrieve and set as many of the device's properties as possible.

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

NOTE The Server uses alternative firmware versions only as a basis to manage infrastructure devices with unrecognized firmware; the Server does not update the actual firmware of the infrastructure device unless you specifically instruct it to do so.

See the *Avalanche Release Notes* for the specific firmware ranges the Server uses to manage infrastructure devices with unrecognized firmware.

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

Hardware	Fully-supported Firmware	Compatible Firmware Range
Cisco-Aironet 350	12.01T1	12.01T1 - 12.99
Symbol T3	03.50-18	03.50-00 - 03.50-99

Table 10-2: *Firmware Version Matches for Compatibility Mode Support (Samples)*

The following example uses the information in Table 10-2 to demonstrate how the Server manages infrastructure devices with unrecognized firmware. A Cisco-Aironet access point is installed on a network that used firmware version 12.02T1. The Server discovers this access point, and identifies that it cannot recognize the firmware version. The Server then checks to see if firmware 12.02T1 falls within a firmware range. It finds that if a firmware version falls between 12.01T1 and 12.99, it should use firmware version 12.01T1 to manage the access point. Consequently, the Server begins to manage the new access point based on the 12.01T1 firmware.

Supported Firmware

When you create firmware packages, you have the option to view and then select from all the versions of firmware that Avalanche supports. The Infrastructure Server will be able to manage infrastructure devices with any of the firmware types listed. For a list of supported firmware, see *Appendix D: Supported Firmware* on page 314.

Importing Firmware

Avalanche no longer ships with firmware files; however, you can import the firmware through the **Manage Firmware** utility. You must have downloaded the firmware files from either the manufacturer or from Wavelink.

You can also re-install firmware that has already been installed. When you attempt to do this, the Console will remind that you that you are overwriting the existing installed firmware.

To import firmware:

- 1 Ensure you have downloaded the firmware files from Wavelink or the manufacturer and know the location of the files.
- 2 From the **File** menu, select **Import > Firmware Files**.

The *Manage Infrastructure Firmware* dialog box appears. This dialog box displays the manufacturer, model, version and whether the firmware has been installed.

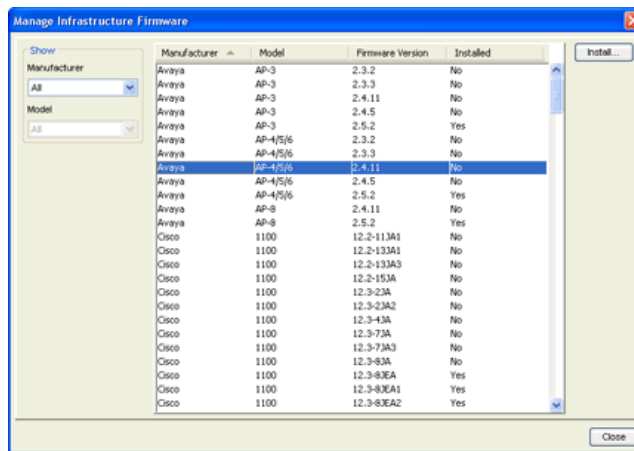


Figure 10-1. *Manage Infrastructure Firmware*

- 3 In the **Show** area, sort the firmware list by **Manufacturer** and **Model** (if necessary).
- 4 Select the firmware you want to install and click **Install**.

A *Select Source Folder* dialog box appears and displays the firmware file name in the **File of type** text box.

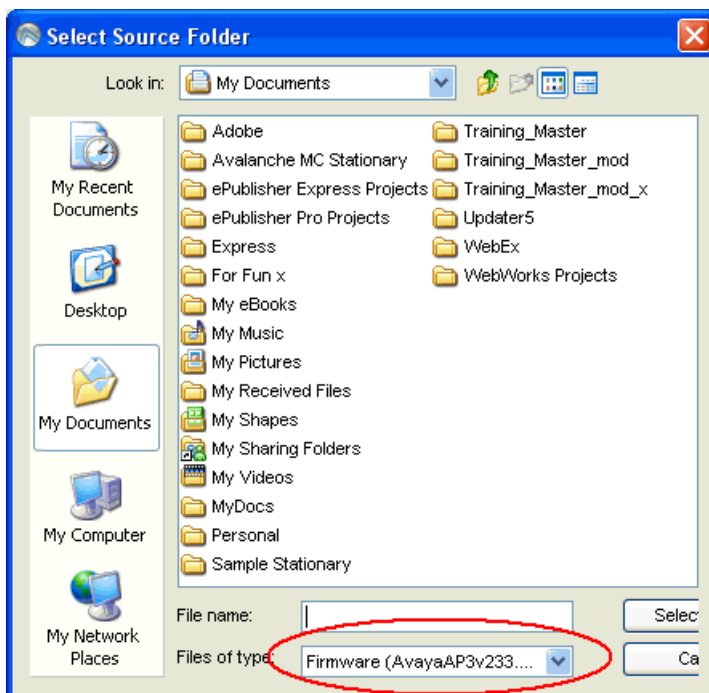


Figure 10-2. *Select Source Folder*

- 5 Navigate to the folder that contains the firmware file and click **Select**.

If the folder does not contain the firmware or the support file if one was specified by the Wavelink index, the Console displays an error message.

If the folder contains all the necessary firmware files then the files will be moved to the Enterprise Server `deploy\firmware` folder.

NOTE If you are attempting to reinstall a firmware version that is already installed, you will see a warning that tells you the firmware already exists and asks if you are sure you want to overwrite the existing firmware. Click **Yes** to continue the installation.

A success message appears when the import completes. The firmware will appear in the applicable dialog box when you add an infrastructure profile. The new firmware is also available to deploy to Infrastructure

Servers. When you create a firmware package, you will be able to select and bundle the added firmware to the firmware package.

NOTE There is currently no supported method of un-importing firmware.

Manually Adding Firmware

In addition to importing firmware files, you have the option of manually dropping firmware binary files into the “firmware” directory.

If the firmware files are pre-coded in the existing available firmware list, Avalanche will recognize the files within 10 minutes and update the firmware package wizard. An alert is generated when the system detects these firmware files. Avalanche will not recognize any firmware file names that do not already exist in the list of supported firmware.

To manually add firmware to Avalanche:

- 1** Obtain the firmware binary files from the device manufacturer, or contact Wavelink Customer Service.
- 2** Place these folders in the Avalanche firmware folder located in the installation directory. The default location is:
`C:\Program Files\Wavelink\AvalancheMC\deploy\firmware`
- 3** Wait approximately 10 minutes for Avalanche to update with the new firmware information. An alert will appear and display information about the newly added firmware.

-Or-

Stop and restart the Wavelink Avalanche Enterprise Server to force Avalanche to update immediately.

The new firmware will now be available to deploy to Infrastructure Servers. When you create a firmware package, you will be able to select and bundle the added firmware to the firmware package.

Creating Firmware Packages

An Avalanche firmware package is a collection of files that allow Servers to support the software installed on infrastructure devices. You can create a firmware package to contain as many firmware versions as you need;

however, it is important to remember that the larger the firmware package, the longer it takes to send to a given server location.

To create a firmware package:

1 Click **Tools > Deployment Packages**.

The *Deployment Package Manager* dialog box appears.

2 Click **Add**.

The *New Package Wizard* dialog box appears.

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

The *Select Package Type* dialog box appears.

4 Enable **Create a Firmware Update Package** and click **Next**.

The *Select Infrastructure Firmware Support* dialog box appears. This dialog box contains a collection of folders, with each folder representing a specific type of infrastructure device.

5 If you only want to select from firmware available to the enterprise server, enable the **Only show available firmware binaries included on server**.

NOTE If this option is not enabled, you will see a list of all supported firmware.

6 To select firmware, open the appropriate folder. A list of available firmware versions appears. Enable the checkbox next to the firmware name. You can select any number of firmware versions from each folder.

7 If you have not imported any firmware, click the **Import New Firmware** button. This directs you to the **Firmware Import** tool. Refer to *Importing Firmware* on page 161 for further instructions.

8 Once you enable your selections in the *Select Infrastructure Firmware Support* dialog box, click **Next**.

The *Enter Package Name* dialog box appears.

9 Type the name of the package in the **Package Name** text box and click **Next**.

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

10 Click **Finish**.

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

Deploying Firmware Packages

Once you create a firmware package, you must deploy it to your servers. For information about deploying firmware packages, refer to *Updating Infrastructure Firmware* on page 292.

Setting a Default Profile for Specific Hardware

When you have multiple infrastructure devices that are the same model but are using different firmware, Avalanche allows you to standardize the firmware type. You can create a default profile for that hardware, and all devices matching the hardware type will use the firmware specified in the default profile.

NOTE The firmware must be made available at the Infrastructure Server in order to apply a default profile for specific hardware.

This option is not supported by all APs.

To set a default profile for specific hardware:

- 1 Create an infrastructure profile for the hardware, specifying the type of firmware you want all the devices of that type to use. For information on creating an infrastructure profile, see *Creating Infrastructure Profiles* on page 148.
- 2 Select the region where you want to apply the default profile from the Navigation Window.
- 3 From the **Region Properties** tab, click **Add** on the **Applied Profiles** tab.

The *Applied Profiles* dialog box appears.
- 4 Select the infrastructure profile from the list and click **OK**.

- 5 The *Infrastructure Profile Application* dialog box appears.
- 6 Enable **Default Profile for Hardware** and click **OK**.

The profile becomes the default infrastructure profile for that type of hardware.

Chapter 11: Managing Infrastructure Devices

Infrastructure devices can be managed through the **Infrastructure Inventory** tab. This tab displays a list of all your infrastructure devices and details about them. This chapter provides information about the following Infrastructure Inventory topics:

- Managing Device Filters
- Tasks from the Device View

Managing Device Filters

Filters allow you to order and sort the manner in which you want to view your infrastructure devices. This section contains the following information:

- Creating Device Filters
- Applying Device Filters
- Filter View By Type
- Displaying Devices

Creating Device Filters

To display devices with a specific characteristic in the **Infrastructure Inventory** tab, you must first create a new filter.

To create a filter:

- 1 From the **Infrastructure Inventory** tab, click **Edit Filters**.

The *Modify Infra Device Filters* dialog box appears.

- 2 Enter a name for the 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 device characteristics. See *Building Selection*

Criteria on page 272 for more information on using the Selection Criteria Builder.

- 4 When you have created the desired selection criteria, click **OK** to return to the *Modify Infra Device Filters* dialog box.

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

- 5 Click **Add Filter**.

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

- 6 Click **OK**.

You can now select the filter from the **Current Infra Device Filter** drop-down list located at the top of the **Infrastructure Inventory** tab.

Applying Device Filters

After you create device filters, you must apply them to the Infrastructure Inventory list. After the filter is applied, only the devices matching the selection criteria of the filter will appear in the Device View.

To apply filters:

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

The Device View will reorder to display the devices according to the filter settings.

Filter View By Type

You can also use the options next to **Filter View by Type** to display your devices according to your preferences. The **Filter View by Type** allows you to filter by the following:

- APs
- Wireless Switches
- Wired Switches
- Foreign APs

- Rogue APs
- Access Ports

Enabling any one or more of these options will cause the Device View to reflect those selections.

Displaying Devices

The **Infrastructure Inventory** tab allows you to select how many devices you want to appear in the inventory list at a time.

To configure device list paging:

- From the **Number of Devices Per Page** drop-down list, select the number of devices you want to display.

NOTE This option is located at the bottom of the screen.

Tasks from the Device View

The Device View in the **Infrastructure Inventory** tab shows a set or subset of infrastructure devices based on the currently selected item in the Navigation Window. For example, when you select a particular group or region, the devices that are associated with that group or region appear in the list. The following default information is provided for each type of device:

Name	The official name of the device.
Manufacturer	The manufacturer of the device.
Model	The model of the device.
Version	The version of firmware currently running on the device.
IP Address	The IP address of the device.
Mac Address	The MAC address of the device.
Last Contact	The last time the device was in contact with the infrastructure Server.

Status	Indicates the current status of the device.
Up	A green circle with a check indicates that the device is up and running. A red X indicates the device is down or there may be an issue with the device..
Profile	Indicates whether the profile assigned to the device is composite.
Extra Information	Lists information such as profiles applied, associated mobile devices, or other details of the device.

You can sort each column by right-clicking the column header and selecting **Sort Ascending** or **Sort Descending**.

You can perform the following tasks on the devices listed in the Device View:

- Querying the Device
- Pinging the Device
- Resetting Access Points
- Changing Access Point Firmware
- Connecting by Web Browser or Telnet
- Deleting Devices
- Viewing Composite Profiles
- Viewing Advanced Properties
- Viewing Related Devices

NOTE All tasks, aside from Viewing Related Devices, are available for both switches and access points.

You cannot perform any of these tasks except Viewing Related Devices and Deleting Devices on an access port.

Querying the Device

When a query occurs, an Infrastructure Server updates the statistical data and configuration settings of an infrastructure device. These queries occur at specific intervals—either an interval that you established for the Server, or the default interval of once every 10 minutes.

Occasionally you might want to force a Server to query a device—for example, if you want a specific configuration change to become effective immediately.

To force a query:

- 1 Right-click the desired device from the **Infrastructure Inventory** tab.
- 2 Select **Query** from the context menu.

The Server updates the device statistical data and configuration settings with the latest information. You can view this information in the Device Information section located at the bottom of the screen.

Pinging the Device

You can ping infrastructure devices from the Avalanche Console. This feature indicates whether the device is active or not.

NOTE Since the ping is sent from the Infrastructure Server, there does not need to be a valid network path from the Console to the device.

To ping the device:

- 1 Right-click the desired device from the **Infrastructure Inventory** tab.
- 2 Select **Ping** from the context menu.

The **Status** column in the display window will indicate whether the device could be reached.

Resetting Access Points

If you decide to reset an access point's properties for any reason, you can do so at any time. You have two options for resetting access points: a normal reset and a reset to factory settings. When you reset to factory settings, you are resetting the device to all the original factory settings.

If the "Retain IP Address" factory reset mode is available, Avalanche will attempt to use it so that communication is not disrupted after the factory reset. However, some devices reset their IP addresses. This is mainly an issue for devices assigned a static IP address. Factory reset should only be used if you are certain the device will return with a valid IP address or if you have physical access to the device and can reconfigure it using factory-specific methods.

If you are using a DHCP server during a factory reset, some devices may adopt a different DHCP IP address and a network search may be required to find them.

NOTE You cannot reset Symbol access points to factory defaults if a router, or any network equipment that blocks layer 2 protocols, exists between the Server and the access points.

To reset an access point:

- 1 Right-click the name of the access point from the **Infrastructure Inventory** tab.
- 2 Select **Reset** from the context menu.

A dialog box appears, asking you to confirm that you want to reset the access point.

- 3 Click **Yes**.

The Server resets the access point. While the device resets, its status appears as **Resetting**.

To reset an access point to its factory defaults:

- 1 Right-click the device point from the **Infrastructure Inventory** tab and select **Reset Factory** from the context menu.

A dialog box appears, asking you to confirm that you want to reset the device.

- 2 Click **Yes**.

The Server resets the device to the factory default settings of its current firmware. While the device resets, its status appears as **Reset Factory**.

Changing Access Point Firmware

You can remotely update the firmware of an infrastructure device as long as the firmware is available at the Infrastructure Server.

NOTE Firmware can also be upgraded across multiple access points simultaneously using the "Default Profile for Hardware" feature of Infrastructure Profiles (for those access points that support this capability).

To update the firmware:

- 1 Right-click the device from the **Infrastructure Inventory** tab and select **Update Firmware**.

The *Update Firmware* dialog box appears.

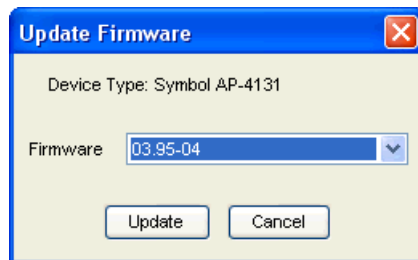


Figure 11-1. *The Update Firmware Dialog Box*

- 2 Select the firmware you want to install on your access points from the **Firmware** list.

NOTE If there is no firmware available at the Server, the drop-down list will be empty.

- 3 Click **Update** to update the firmware of your device.

During firmware upgrade the status appears as **Updating Firmware**. Alerts will be generated indicating the start and end of the firmware upgrade and whether the upgrade succeeded or failed.

Connecting by Web Browser or Telnet

Most device manufacturers provide the ability to configure their access points through a Web browser. You can access the Web interface for any access point that appears in the **Infrastructure Inventory** tab.

You can select to connect through HTTP or HTTPS based on what you have enabled on your device.

To connect to an access point through a Web browser:

- 1 Right-click the device from the **Infrastructure Inventory** tab and select **Connect to device using**.
- 2 From the menu that appears select **HTTP**, **HTTPS** or **Telnet** based on the method you want to use to connect.
 - If you are using HTTP or HTTPS, Avalanche automatically launches the default Web browser for your host system to display the Web interface for the device.
 - If you are using Telnet, a Telnet connection opens to that device.

NOTE You can only connect to an access point by Web browser if that device IP is reachable from the system hosting Avalanche Console.

Deleting Devices

You can delete devices from the Infrastructure Inventory. This removes the device from the **Infrastructure Inventory** tab and releases the license that device was using.

To delete devices:

- 1 In the **Infrastructure Inventory** tab, right-click the device you want to delete and select **Delete**.

A dialog box appears asking if you are sure you want to remove the device.

- 2 Select **Yes**.

The device is removed, but will not immediately disappear from the Device View. The next time the Server checks in, the device will disappear.

NOTE There are some devices, when connected to the network, that may be immediately rediscovered.

Viewing Composite Profiles

The composite profile view is the instantaneous view of properties as they currently are on that device (a combination of applied infrastructure and network profile) as computed by the infrastructure server. You can view the composite profile for devices that are assigned such profiles from the Infrastructure Inventory, but any changes you want to make must be made in the infrastructure profile.

To view composite profile information:

- In the **Infrastructure Inventory** tab, right-click the device you want to view and select **View Composite Profile**.

An *Advanced Properties* dialog box will appear, allowing you to view the information about the composite profile.

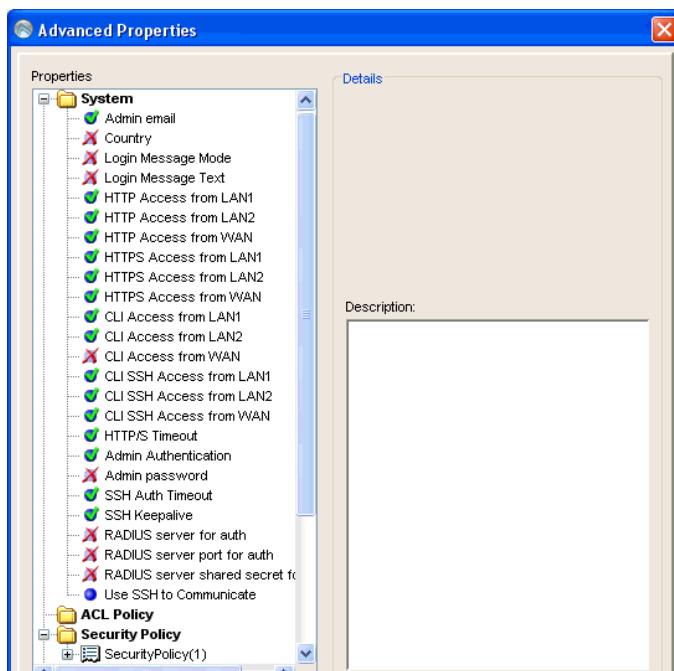


Figure 11-2. Composite Profile Information

Viewing Advanced Properties

The advanced properties view shows the current properties that exist on the selected device. You can view the advanced properties for infrastructure devices from the Infrastructure Inventory, but any changes you want to make must be made in the infrastructure profile.

To view advanced properties:

- In the **Infrastructure Inventory** tab, right-click the device you want to view and select **View Advanced Properties**.

An *Advanced Properties* dialog box will appear allowing you to view the information.

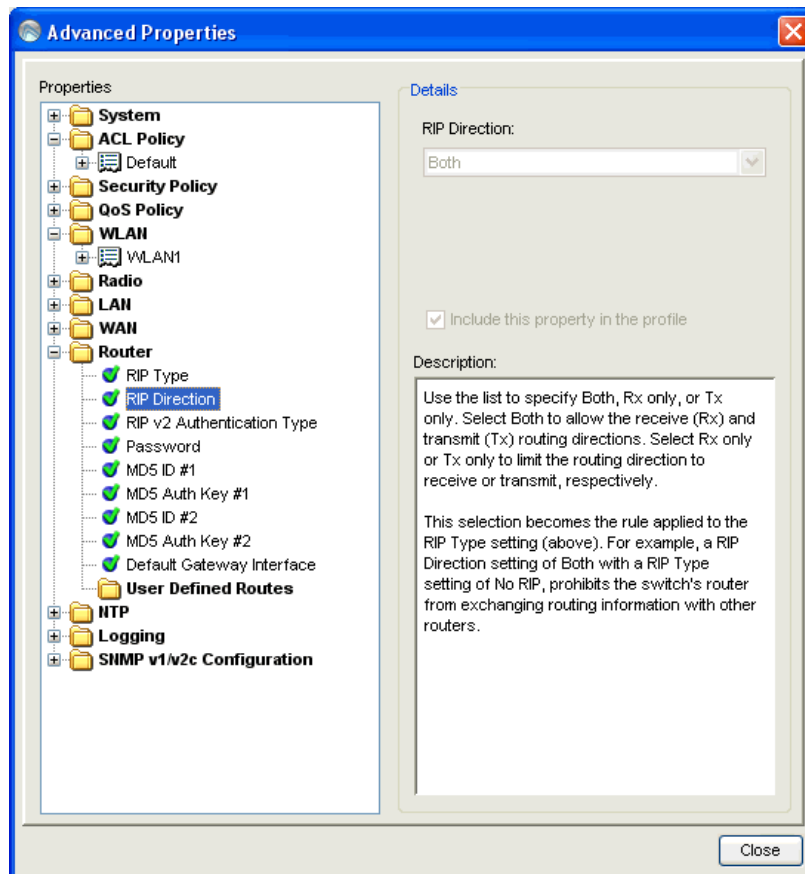


Figure 11-3. *Advanced Properties*

Viewing Related Devices

When working with a switch or access port, you can view the devices associated with it.

To find the related devices:

- In the **Infrastructure Inventory** tab, right-click an access port or switch and select **Find related**.

The Infrastructure Inventory displays those switches and access ports related to the one you selected.

Chapter 12: Managing Very Large Access Control Lists

Infrastructure devices support a feature called the Access Control List. This list contains the MAC addresses of devices that are allowed to access your wireless network. Only those mobile devices that are on an Access Control List can communicate with your network through an infrastructure device. However, Access Control Lists are limited in the number of MAC addresses they can contain. This can be restrictive in an enterprise consisting of thousands of mobile devices.

To address this issue, Avalanche supports the Very Large Access Control List (VLACL), which can contain an unlimited number of MAC addresses. This list is similar to the Access Control List, but it is supported by the Infrastructure Server as opposed to an individual access point. With the Very Large Access Control List enabled, the infrastructure devices refer to the Infrastructure Server to know which mobile devices are allowed access to the network.

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

By default, the Very Large Access Control List is disabled, allowing any mobile device to connect to Servers.

NOTE For more information about configuring the Infrastructure-supported Access Control Lists, see the *Mobile Manager User's Guide*.

This section contains information about the following topics:

- Why Should I Create a Very Large Access Control List?
- Adding Very Large Access Control List Entries
- Modifying Very Large Access Control List Entries
- Removing Very Large Access Control List Entries

- Exporting and Importing a Very Large Access Control List
- Deploying the Very Large Access Control List

Why Should I Create a Very Large Access Control List?

If security is a high priority, it is recommended that you configure the Very Large Access Control List for your wireless network. When the Very Large Access Control List is applied, the infrastructure devices check the MAC address of each mobile device against the MAC addresses listed in the Server's Very Large Access Control List. If there is a match, it allows the mobile device to connect to the network. If the infrastructure device does not find a match, it refuses to communicate with the mobile device.

Adding Very Large Access Control List Entries

The Avalanche Console allows you to add as many mobile device MAC addresses to the Very Large Access Control List as your network demands.

To add a MAC address:

- 1 From the **Tools** menu, select **Access Control**.

The *Very Large Access Control List* dialog box appears.

- 2 Enable the **Enable Very Large Access Control List** option.
- 3 Click **Add**.

The *VLACL Entry* dialog box appears.

- 4 Type the MAC address for the mobile device in the **MAC Address** text box.
- 5 Type the name of the mobile device in the **Name** text box.
- 6 Click **OK**.

The MAC address appears in the **Very Large Access Control List**.

- 7 Click **Add** to enter an additional MAC address, or click **OK** to return to the Avalanche Console.

Modifying Very Large Access Control List Entries

After you build a Very Large Access Control List, you can modify entries by changing the device names. You can not change the MAC address. To make MAC address changes, you need to remove the entry from the list and then recreate an entry with the updated information.

To modify the name of an Access Control List entry:

- 1 From the **Tools** menu, select **Access Control**.

The *Very Large Access Control List* dialog box appears.

- 2 Select an entry from the **Very Large Access Control List**.
- 3 Right-click the appropriate entry and select **Rename** from the menu that appears.

A cursor appears within the name column for the entry.

- 4 Type the new name.
- 5 Press **Enter**.

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

- 6 Click **OK**.

Removing Very Large Access Control List Entries

You can remove a MAC address from the Very Large Access Control List at any time. This prevents the device from connecting to infrastructure devices within your network.

To remove a Very Large Access Control List entry:

- 1 From the **Tools** menu, select **Access Control**.

The *Very Large Access Control List* dialog box appears.

- 2 Select the entry you want to remove.
- 3 Click **Delete**.

The Avalanche Console deletes the entry from the **Very Large Access Control List**.

- 4 Click **OK** to return to the Avalanche Console.

Exporting and Importing a Very Large Access Control List

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

Exporting a VLACL

When you export a Very Large Access Control List file, the file must be either a `.csv` or `.txt` file.

To export a Very Large Access Control List file:

- 1 From the **Tools** menu, select **Access Control**.

The *Very Large Access Control List* dialog box appears.

- 2 Click **Export**.

A standard *Save* dialog box appears.

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

- 4 Click **Save**.

Importing a VLACL

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

- [MAC Address], [Device Name]

NOTE The preceding format is required for both `.txt` and `.csv` files. The MAC addresses must have a colon separating the octets. You can add as many MAC addresses as necessary to the comma-delimited file as long as each entry complies with this format.

To import a Very Large Access Control List file:

- 1 From the **Tools** menu, select **Access Control**.

The *Very Large Access Control List* dialog box appears.

- 2 Click **Import**.

A standard *Open* dialog box appears.

- 3 Locate and select the text file.

- 4 Click **Open**.

The *Very Large Access Control List* dialog box updates to display the added entries.

- 5 Click **OK** to return to the Avalanche Console.

Deploying the Very Large Access Control List

After you create a Very Large Access Control List, you can deploy it. To deploy the VLACL, you perform a universal deployment. For information about universal deployments, refer to *Performing a Universal Deployment* on page 289.

Chapter 13: Managing Mobile Device Distributed Servers

The Mobile Device Server is distributed server software that lets you remotely manage and configure mobile devices. Although you can use multiple Servers at different Server Locations or on different network segments, you can manage all of your Servers from the Avalanche Console, regardless of where you access the Console.

NOTE In previous versions of Avalanche, Distributed Servers were referred to as Agents in both the user interface of the Avalanche Console and the documentation. The Mobile Device Agent (also referred to as the Avalanche Agent) managed mobile devices. Starting with Avalanche 4.1 release, Agents are referred to as Distributed Servers (Servers) both in the user interface and the documentation. The Mobile Device Agent is the Mobile Device Server.

Through a Mobile Device Server profile, Avalanche allows you to manage the following settings for your Mobile Device Servers 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 Servers 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 Mobile Device Servers through Mobile Device Server Profiles. It contains the following tasks:

- Creating Mobile Device Server Profiles
- Configuring Mobile Device Server Profile Settings
- Configuring Mobile Device Server Blackouts and Updates
- Viewing Where Mobile Device Server Profiles Are Applied
- Removing Mobile Device Server Profiles

- Assigning Mobile Device Server Profiles to Regions
- Viewing Mobile Device Server Licensing Messages
- Reinitializing the Mobile Device Server

For information on deploying a Mobile Device Distributed Server, see *Building Server Deployment Packages* on page 98.

Creating Mobile Device Server Profiles

Mobile Device Server Profiles are used to manage your Mobile Device Servers. Profiles allow you to configure logging, device connections, secondary server support, updates and other settings for the Server.

To create a Mobile Device Server profile:

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

The *Create Profile* dialog box appears.

- 2 From the **Profile Type** drop-down list, select **Mobile Server Profile**.

- 3 Type the name of the Mobile Device Server Profile in the text box and click **OK**.

The profile is added to the **Profile List**.

Configuring Mobile Device Server Profile Settings

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

- Enabling Mobile Device Server Profiles
- 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

Enabling Mobile Device Server Profiles

Mobile Device Server Profiles are disabled by default when you create them. You must enable the profile before its settings will be applied.

To enable a 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, select the **Enabled** option.
- 4 Save your changes.

The Mobile Device Server Profile is now enabled.

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 a Server Location environment involves mobile devices roaming from one Server to another, it is highly 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 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 provides you with the options to set logging levels for the Mobile Device Server, reserve serial ports for the use of the Server, and set the range of terminal IDs the Server can assign to mobile devices. The following sections provide information on configuring these options:

- Logging
- Reserved Serial Ports
- Terminal IDs
- Configuring Mobile Device Server Resources

Logging

The log file records actions that have occurred on the Mobile Device Server. You can set the maximum log size and the log level for the file.

You can set the log function to the following levels:

- **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.

The current Avalanche log file is saved as `Avalanche.log` to the `<Avalanche Installation Directory>\Service` directory. Avalanche allows you to configure the maximum size of the log file. Once the current log file reaches the maximum size, it is saved as `Avalanche.log.<num>`, where `<num>` is a number between 000 and 999 (beginning with 001), and a new `Avalanche.log` file is created.

To configure logging options, see *Configuring Mobile Device Server Resources* on page 190.

Reserved 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.

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

To configure serial port reservation, see *Configuring Mobile Device Server Resources* on page 190.

Terminal IDs

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 configured numbers.

You can also configure your own alphanumeric 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`.

To configure the range of terminal IDs that the Server assigns, see *Configuring Mobile Device Server Resources* on page 190.

Configuring Mobile Device Server Resources

A Mobile Device Server Profile provides you with the options to set logging levels for the Mobile Device Server, reserve serial ports for the use of the server, and set the range of terminal IDs the Server can assign to mobile devices.

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

The **Authorized Users** button allows you to assign administrative privileges for a specified profile to a user that has Normal user rights and is not assigned permissions to profiles. This means that any user assigned as an authorized user to a profile will have administrative rights for that one profile.

To add an authorized user you must have at least one user configured with Normal permissions. For more information about creating users and assigning permissions, refer to *Chapter 5: Managing User Accounts* on page 64.

To add an authorized user:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Mobile Device Server Profile** tab, click the **Authorized Users** button.

The *Profile Authorized Users* dialog box appears.

- 4 Click **Add User**.

The *Add Authorized User* dialog box appears.

- 5 From the user list, select the user and then choose `READ_WRITE` or `READ_ONLY` for the permission level. Click **OK**.

The user is added to the **Authorized Users** list for the profile.

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

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 following 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 Mobile Device Server profiles 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 the network profile and if you do not have one configured, the mobile device will never receive those network settings.

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 the 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 after the end time, the blackout 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, the blackout window 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 a 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, if desired, 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, if the software collection it belongs to has been disabled, or if the package 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 would normally provide information on those files.

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 If you chose a post-synchronization event, the start and 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. This allows you to create events that 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 Where Mobile Device Server Profiles Are Applied

The **Applied To** tab in the **Profiles** tab allows you to see exactly which regions, 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 81.

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.

Removing Mobile Device Server Profiles

If you no longer are using a Mobile Device Server profile, you can remove it from the Console. When you remove a Mobile Device Server profile from the Console, any servers assigned to that profile will retain those profile settings until a new profile is deployed to that server.

To remove a Mobile Device Server profile:

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

The *Confirm Delete* dialog box appears.

- 3 Click **Yes** to confirm.

The profile is removed from the list and no longer available.

Assigning Mobile Device Server Profiles to Regions

Once you have configured your Mobile Device Server profile, you can apply that profile to any region in the Console. When you apply a Mobile Device Server profile to a region, that profile will be deployed to all Mobile Device Servers in that region matching the profile criteria. For more information about assigning Mobile Device Server Profiles to a region and then applying those profiles to servers, refer to *Assigning Profiles* on page 81.

Viewing Mobile Device Server Licensing Messages

The Avalanche Console receives licensing messages from the deployed Mobile Device Servers. 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.

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 14: Managing Software Profiles

A software profile is a configuration profile that can be assigned to multiple regions. The software packages associated with the profile are installed on all devices meeting the selection criteria in those regions. 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 region 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 **Apply the Software Profile** dialog, you can choose to apply the profile and designate where you want it to be applied. Click **Next** to continue.
- 6 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 208.
- 7 Click **Next**.

The End User License Agreement appears.

- 8 Enable **Yes I agree** to agree to the license agreement and click **Next**.
- 9 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**.
- 10 The *Configure the Software Package* dialog box appears.
- 11 If desired, enable the software package and configure it using the available utilities.
- 12 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 206.

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

The **Authorized Users** button allows you to assign administrative privileges for a specified 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.

For information about creating users and assigning permissions, refer to *Chapter 5: Managing User Accounts* on page 64.

To add an authorized user:

- 1** From the **Profiles** tab, select the software profile you want to configure.
- 2** Click **Edit**.
- 3** From the **Software Profile** tab, click **Authorized Users**.

The *Profile Authorized Users* dialog box appears.

NOTE If you are not in Edit Mode, you will be able to click **Authorized Users** and view current authorized users but will not be able to make any changes.

- 4** Click **Add User**.

The *Add Authorized User* dialog box appears.

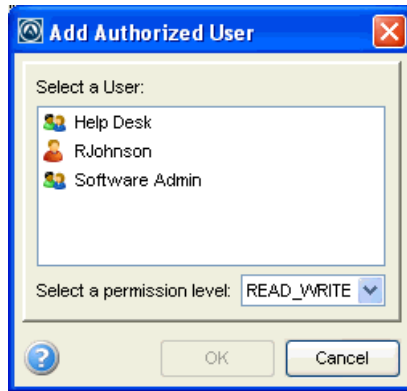


Figure 14-1. *Add Authorized User dialog box*

- 5 From the list, select the user.
- 6 From the drop-down list, select the level of permission.
- 7 Click **OK**.
- 8 The user is added to the list of authorized users.

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 272.

Applying Software Profiles

Once you have created a software profile and added software packages to the profile, you can assign that profile to a region. The profile will then be deployed to all the Server locations in that region when you perform a Universal Update. For information about applying software profiles to regions, refer to *Assigning Profiles* on page 81. For information about deploying Universal Updates, refer to *Performing a Universal Deployment* on page 289.

Viewing Where Software Profiles Are Applied

The **Applied Locations** tab in the software 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, you will need to access the Region or Server Location Properties tabs and assign the profiles there. For information, refer to *Applying Software Profiles* on page 205.

The **Applied Locations** 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 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.
Installed	Displays the date, time, and user for the package installation.
Configured	Displays the date, time, and user for the most recent package configuration.

Table 14-1: *Software Packages*

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 210.

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.

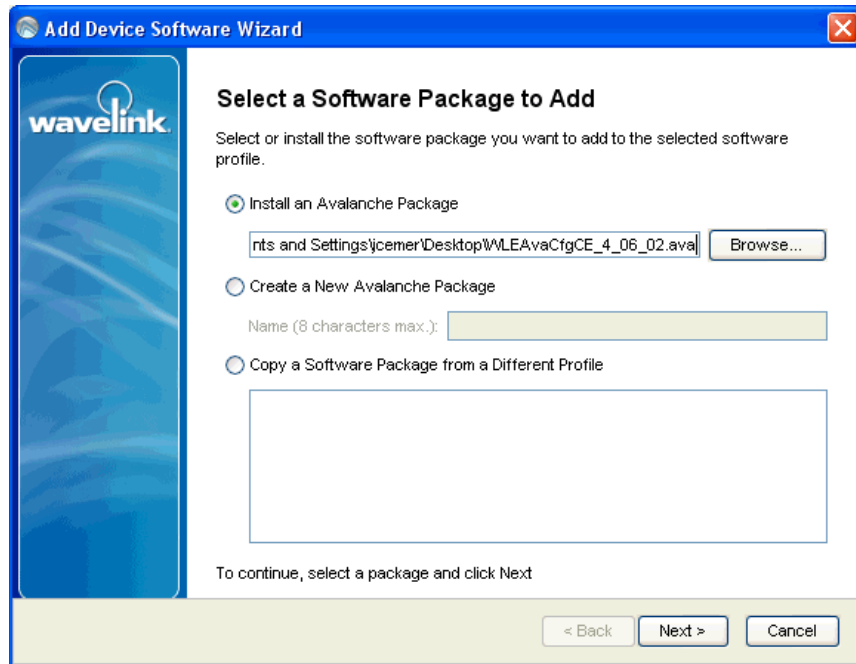


Figure 14-2. *Select Package*

- 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(s) 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.

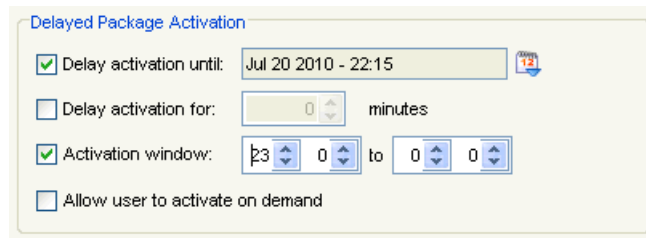
Delayed package installation provides flexible control over when the mobile device installs software packages.

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 14-3. *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 mobile 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>	<p><i>Can</i> contact the Server for updates at any time.</p>	<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>	<p><i>Can</i> contact the Server for updates at any time.</p>	<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>	<p><i>Can</i> contact the Server for updates at any time.</p>	<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>	<p><i>Can</i> contact the Server for updates at any time.</p>	<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>
<p>No options are enabled</p>	<p><i>Can</i> contact the Server for updates at any time.</p>	<p><i>Can</i> contact package store devices or Server for updates at any time.</p>

Table 14-2: Configuration Results for Package Distribution

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 15: Managing Mobile Devices

This section provides information about the following mobile device topics:

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

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 region, all mobile devices that are associated with that region 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 also customize the columns in the **Mobile Device Inventory** tab to display according to your preference.

This section provides information about the following tasks:

- Inventory Paging
- Displaying Custom Mobile Device Icons
- Deleting Mobile Devices
- Modifying Columns
- Adding Custom Columns
- Reorganizing Columns

Inventory Paging

The **Mobile Device Inventory** tab allows you to select how many devices you want to appear in the inventory list at a time.

The inventory displays the devices in the order Avalanche pulls the information from the database. You may need to page through the list to view other filtered 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.

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.

Because the image data is transferred from the mobile device to the Mobile Device Server, to the Enterprise Server and finally to the Console, there may be a temporary delay in the display of the device images. No device images will display until the icons are available at the Console. Once the icons become available, they will display the next time the inventory list is loaded or refreshed. The icons will display in the *Mobile Device Details* dialog box the next time it opens.

Enablers that support this must make two icons available to the Console. The large icon must be a `.png` image. It is recommended that the small icon be a `.png` image as well. For more information about custom device icons, refer to *Using Custom Device Icons in Avalanche*, located on the Wavelink web site.

Deleting Mobile Devices

You can 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.

Modifying Columns

The Avalanche Console allows you to control which columns appear in the **Mobile Device Inventory** tab, 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

If you have created custom properties for your mobile devices, you can display them in a column in the **Mobile Device Inventory** tab.

For details about creating custom properties, refer to *Creating Custom Properties* on page 228.

To display columns for custom properties:

- 1 From the **Mobile Device Inventory** tab, 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 **Mobile Device Inventory** tab.

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

Reorganizing Columns

You can remove, reset, and align columns from the **Mobile Device Inventory** tab, as well as sorting devices 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.

Managing Device Filters

You can filter which devices are displayed in the Mobile Device Inventory List by creating and applying mobile device filters. When a filter is applied,

only the devices meeting the criteria associated with that filter will be displayed. 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 Mobile Device Inventory List, you must create a mobile device filter.

To create a filter:

- 1 From the **Mobile Device Inventory** tab, click **Edit Filters**.

The *Modify Mobile 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 272 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 Mobile 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 Device Filter** drop-down list located at the top of the **Mobile Device Inventory** tab.

Applying Device Filters

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

To apply filters:

- 1 From the **Mobile Device Inventory** tab, select the filter from the **Current Mobile Device Filter** drop-down list.
- 2 Click **Apply Filter**.

Deleting Device Filters

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

To delete a filter:

- 1 From the **Mobile Device Inventory** tab, click **Edit Filters**.

The *Modifying Mobile Device Filters* dialog box appears.

- 2 In the Existing Filters list, select the filter you want to delete.
- 3 Click **Delete**.

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.

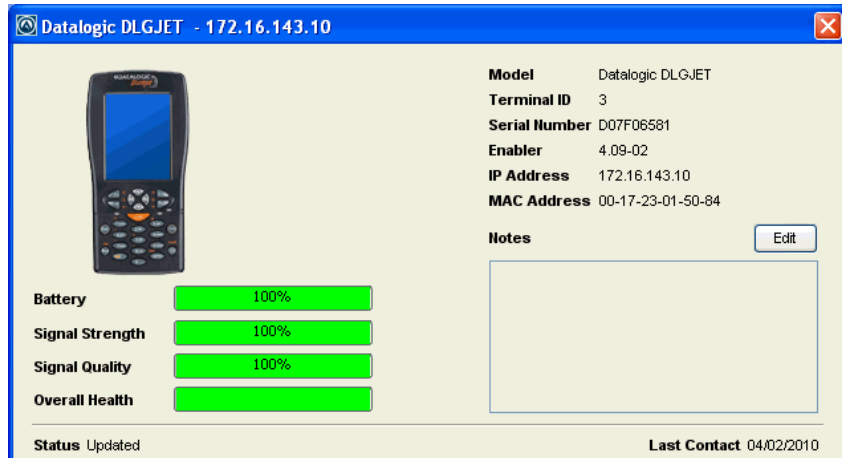


Figure 15-1. Device Details summary information

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 237.
 - **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 227.
 - **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 230.

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 272 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 254.

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 254.

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
- 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 272 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.

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.

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.

Before you can use Remote Control, you must perform the following tasks:

- 1 Obtain the Remote Control software package.
- 2 Install the Remote Control software package into Avalanche.
- 3 License the Remote Control program.
- 4 Deploy the Remote Control software package to your mobile device.

NOTE For detailed information about these tasks, refer to the *Wavelink Avalanche Remote Control User Guide*.

This section provides information about using Remote Control to connect to a mobile device. By default, you can connect to the mobile device wirelessly based on the IP address. There are several other connection configuration options. For more information, refer to the *Wavelink Avalanche Remote Control User Guide*.

To use Remote Control to connect to a mobile device:

- 1 Ensure you have installed the Remote Control package to the Avalanche Console and deployed it to the mobile device.
- 2 From the **Mobile Device Inventory** tab, double-click the mobile device to which you want to connect.

The *Mobile Device Details* dialog box opens

- 3 Click the **Device Control** tab.
- 4 Double-click the **Remote Control** icon.

Remote Control connects to the mobile device. Once you are connected to a mobile device, you can use access File Registry, File Explorer, and Process managing using the available icons.

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. The Session Monitor 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 208 for more information.
- 3 Configure the Telnet Client software package.
- 4 Deploy the Telnet Client to the mobile device. For more information about updates, refer to *Performing a Universal Deployment* on page 289.
- 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 or region 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 or region 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 or region 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.

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 custom 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 region or 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.
- 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 *Chapter 18: Using Selection Criteria* on page 271.
- 10 Click **Save** to save your changes.

Mobile Device Profile Authorized Users

The **Authorized Users** button allows you to assign administrative privileges for a specified 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.

For information about creating users and assigning permissions, refer to *Chapter 5: Managing User Accounts* on page 64.

To add an authorized user:

- 1 From the **Profiles** tab, select the Mobile Device Profile you want to configure.

- 2 Click **Edit**.
- 3 From the **Mobile Device Profile** tab, click **Authorized Users**.

The *Profile Authorized Users* dialog box appears.

NOTE If you are not in Edit Mode, you will be able to click **Authorized Users** and view current authorized users but will not be able to make any changes.

- 4 Click **Add User**.

The *Add Authorized User* dialog box appears.

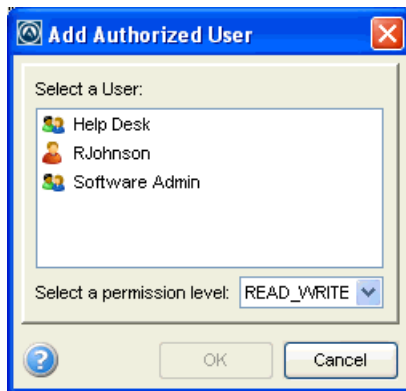


Figure 15-2. *Add Authorized User* dialog box

- 5 From the list, select the user.
- 6 From the drop-down list, select the level of permission.
- 7 Click **OK**.

The user is added to the list of authorized users.

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

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 243.

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 go outside when the device is trying to acquire GPS coordinates.

- **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** region 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 after the end time, the blackout 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, the blackout window 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 regions, 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 81.

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.

Chapter 16: 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 region or 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
- 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 the selection criteria for the devices you want to belong to the group. Avalanche retrieves those devices currently listed in the Mobile Device Inventory list that match the selection criteria. If a new device that matches the selection criteria for that mobile device group connects to the Avalanche Console, it is automatically placed in the mobile device group. Therefore, dynamic mobile device groups will continuously add and remove mobile devices based on the selection criteria, without continued management.

- **Static Mobile Device Groups.** A static mobile device group contains all the mobile devices in your inventory that match a set of configured selection criteria. You configure the selection criteria when the group is created, and then 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 in 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 To enable the group, select **Enabled** from the drop-down list.
- 5 Choose whether you want the group to be **Static** or **Dynamic**.
- 6 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** tab, 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.

Adding Mobile Device Group Authorized Users

The **Authorized Users** button allows you to assign administrative privileges for a specified mobile device group to a user that has Normal user rights. This means that any user assigned as an authorized user to a group will have all administrative rights for that one group. To add an authorized user you must have at least one user configured with Normal permissions.

For information about creating users and assigning permissions, refer to *Chapter 5: Managing User Accounts* on page 64.

To add an authorized user:

- 1 From the **Device Groups** tab, select the group you want to assign a new authorized user.
- 2 Click **Edit**.
- 3 Select the **Authorized Users** tab.
- 4 Click **Add User**.

The *Add Authorized User* dialog box appears.

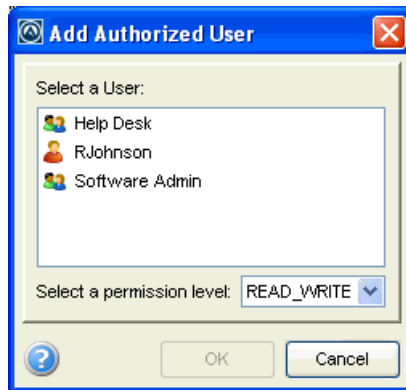


Figure 16-1. *Add Authorized User dialog box*

- 5 From the list, select the user.
- 6 From the drop-down list, select the level of permission.
- 7 Click **OK**.

The user is added to the list of authorized users.

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 272 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 17: 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
- 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
- Assigning Alert Profiles to a Region
- 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 region or 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 262 and *Adding Profiled Proxies* on page 265.

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.

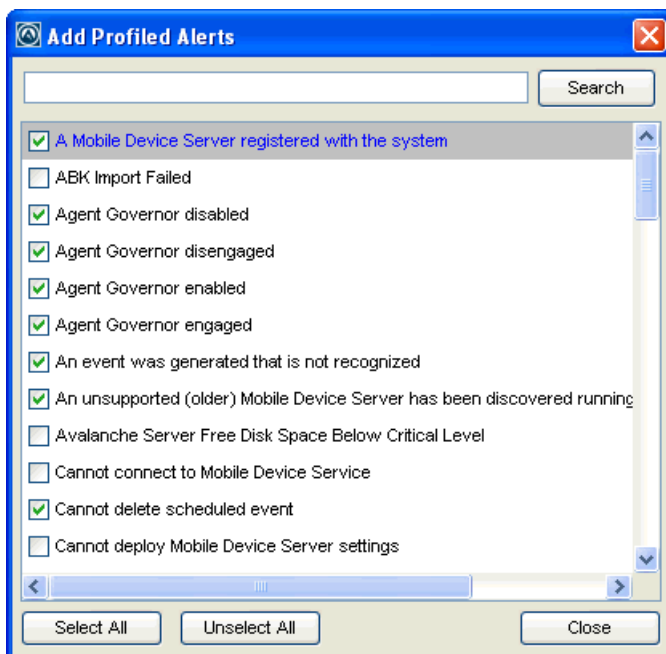


Figure 17-1. Add Profiled Alerts dialog box

- 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 49.

- 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

The **Authorized Users** button allows you to assign administrative privileges for a specified 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.

For information about creating users and assigning permissions, refer to *Chapter 5: Managing User Accounts* on page 64.

To add an authorized user:

- 1 From the **Profiles** tab, select the alert profile you want to configure.
- 2 Click **Edit**.
- 3 From the **Alert Profile** tab, click **Authorized Users**.

The *Profile Authorized Users* dialog box appears.

NOTE If you are not in Edit Mode, you will be able to click **Authorized Users** and view current authorized users but will not be able to make any changes.

4 Click **Add User**.

The *Add Authorized User* dialog box appears.

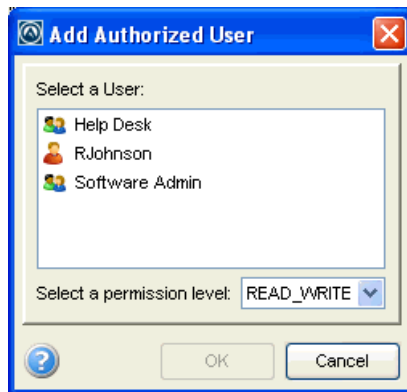


Figure 17-2. *Add Authorized User dialog box*

- 5 From the list, select the user.
- 6 From the drop-down list, select the level of permission.
- 7 Click **OK**.

The user is added to the list of authorized users.

Assigning Alert Profiles to a Region

Once you configure and enable an alert profile, you can assign the profile to a region or location and it is applied after the next deployment.

You can assign more than one alert profile to a region. Each profile will generate alerts based on the events assigned to that profile. If you have specified the same alert in two different profiles assigned to the same region, only one alert for a matching event will be generated.

For more information about assigning alert profiles to a region, refer to *Assigning Profiles* on page 81. For more information about performing a Universal Deployment to deploy alert profile changes, refer to *Performing a Universal Deployment* on page 289.

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 81.

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 are applicable at the region, Server Location or site 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 49.

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**.

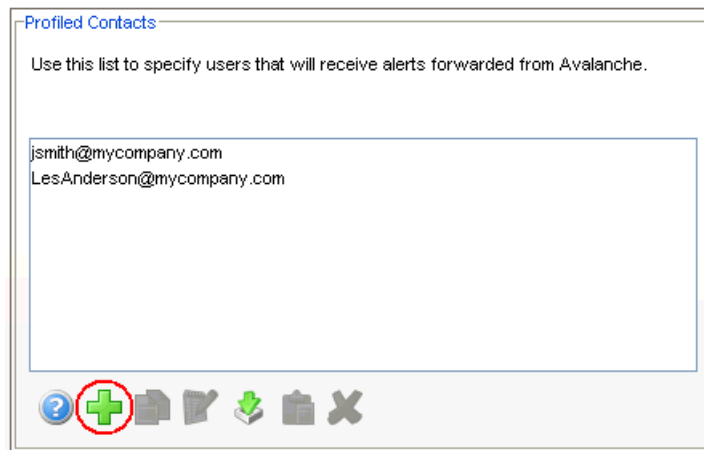


Figure 17-3. Add button in the Profiled Contacts region

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.

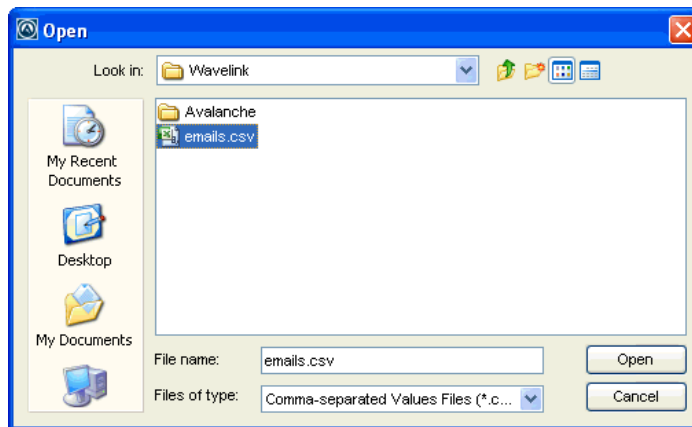


Figure 17-4. *Open dialog box*

- 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, enabling you to integrate Avalanche with your existing network management tools.

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 box.

- 5 Repeat Steps 3 and 4 until you are finished adding proxy addresses.
- 6 Save your changes.

Alerts Tab

The **Alerts** tab provides a real-time view of the health of your wireless network. You can tell at a glance which server locations are operating normally and which require attention.

The **Health by Location** tab consists of two areas: the Map and the Alert Browser. This section contains information on the following tasks:

- Using the Alert Browser
- Using the Avalanche Map

Using the Alert Browser

In the **Alerts** tab, the region at the bottom of the screen is called the Alert Browser. The 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, the Server Location at which the alert was generated begins flashing in the Map view. To stop this flashing, you must acknowledge the alert.

To acknowledge an alert:

- In the Alert Browser, enable the checkbox next to the alert you want to acknowledge.

-Or-

- To acknowledge all alerts in the list, click **Acknowledge All**.

The Server Locations in the Map view stop flashing.

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 checkbox 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 remains 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 From the **Tools** menu, select **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 Alarm Browser will update to reflect your changes.

Using the Avalanche Map

The map provides a geographical overview of the health of your network. Use the following methods to navigate the map:

- Use the navigation arrows to display different portions of the map.
- Center the map on its default location by using the center button of the navigation arrows.
- Enlarge and display greater detail of a portion of the map using the large magnifying glass icon.
- Describes the map details using the small magnifying glass icon.
- Zoom to specific areas by clicking within the map and dragging the pointer across the desired region. A square appears around the region. Release the mouse button and the map refreshes to display a closer view of the selected area.
- Apply filters so that only specific wireless components appear within the map. These filters are activated by the check boxes located next to the navigation arrows. You can apply the following filters:

Combined Servers Displays server locations that contain both a Mobile Device Server and an Infrastructure Server.

Mobile Device dServers Displays server locations that contain only a Mobile Device Server.

Infrastructure dServers Displays server locations that contain only an Infrastructure Server.

View Map By Region	Displays only those server locations that belong to the region selected in the Navigation Window.
Mobile Devices	Displays the mobile devices associated with the region selected.
Mobile Device GPS History	Displays mobile devices by the GPS history.

- Color-code map components. This helps identify components and provide notifications of network health. The color codes for the components that appear in the map are as follows:

Purple	Indicates a server location with combined Servers (Mobile Device Server and Infrastructure Server).
Blue	Indicates a server location with only a Mobile Device Server.
Dark Green	Indicates a server location with only an Infrastructure Server.
Yellow	Indicates a server location with one or more warning-level alerts (but no critical alerts).
Red	Indicates a server location with one or more critical alerts.

When a server location generates a warning or critical alert, the icon in the Map flashes yellow or red, based on the highest severity level in its alert list. The flashing stops when you acknowledge the alert in the Alert Browser. The icon returns to its base color when all warnings and critical alerts for the server location have been cleared from the Alert Browser.

You also can perform the following tasks on the Avalanche map:

- Saving Map Views
- Moving Server Locations

Saving Map Views

You can save specific views of the Avalanche map. This feature allows you to immediately display a relevant section of your wireless network.

To save a map view:

- 1 Position the map using the navigation arrows and zooming in on the relevant geographic area.
- 2 Click **Save View**.
- 3 Type the name of the view in the dialog box that appears.
- 4 Click **OK**.

The view is now saved on the system hosting the Console and can be accessed by selecting it from the **Go to View** drop-down list.

Moving Server Locations

Changing a server location's position on the map only changes where the location is displayed on the map. It does not actually move the server. Changing the display does not disrupt communications with that server location.

To relocate a server location:

- 1 Right-click the server location you wish to relocate.
- 2 Select **Relocate** from the context menu.
- 3 Click the map where you want to move the server location.

The *Confirm Server Location Relocation* dialog box appears.

- 4 Click **Yes**.

Chapter 18: 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 or infrastructure 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, infrastructure profiles, and mobile device groups. To access the Selection Criteria Builder, click the Selection Criteria button:



Figure 18-1. 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.

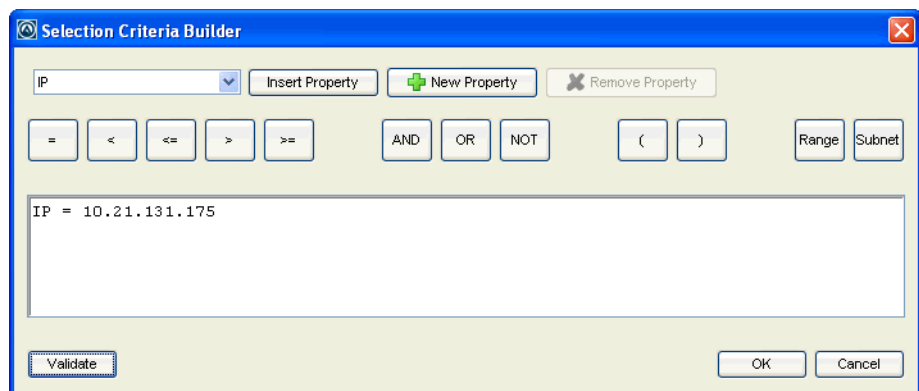


Figure 18-2. Selection Criteria Builder

- 2 From the drop-down list, select a property and click **Insert Property**.

NOTE For information about properties, see *Selection Variables* on page 274.

- 3 Select one of the operator buttons.

NOTE For more information about operators, see *Operators* on page 283.

- 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	<p>IP address of the mobile device(s).</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.
KeyboardCode	<p>A number set by the device manufacturer and used internally by the BIOS to identify the keyboard type.</p> <p>Supported values include:</p> <ul style="list-style-type: none">0 = 35-Key1 = More than 35 keys and WSS10002 = Other devices with less than 35 keys <p>Example:</p> <p>KeyboardCode = 0</p>

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

MAC address of the mobile device.

Enter any MAC addresses as a string of hexadecimal digits. Dashes or colons between octets are optional. For example:

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

ModelName

The standard model name for a mobile device. This name is often a number but it can be alphanumeric. 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.

A few of the supported values include:

1040, 1740, 1746, 1840, 1846, 2740,
2840, 3140, 3143, 3540, 3840, 3843,
3940, 4040, 5040, 6140, 6143, 6840,
6843, 6940, 7240, 7540, 7940, 8140,
8940, PTC960, TR1200, VT2400, WinPC,
WT2200, 7000CE, HHP7400, MX1, MX2, MX3,
VX1, iPAQ, iPAD, Falcon, ITCCK30,
ITC700

Example:

ModelName = 6840

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

Supported values include:

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

Example:

```
ModelCode <= 2
```

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

`OSVer` Predefined property designated by the Enabler. Values with decimals in them must be surrounded by double quote marks.

```
OSVer = "4.20"
```

`OS Type` Predefined property designated by the Enabler.

```
OSType = PocketPC
```

`Processor` Predefined property designated by the Enabler.

```
Processor = ARM
```

`ProcessorType` Predefined property designated by the Enabler.

```
ProcessorType = xScale
```

Assigned IP

IP address of the mobile device.

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.

Series

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

Supported values include:

3 = DOS 3000 Series

P = DOS 4000 and 5000 Series

7 = DOS 7000 Series

T = Telxon devices

C = CE devices

S = Palm devices

W = Windows machines

D = PSC and LXE DOS devices

Example:

Series = 3

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	<p>The unique ID for the mobile device that Avalanche generates. The initial terminal ID is 1, and the values increment as needed.</p> <p>Example:</p> <pre>Terminal ID = 5</pre>

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	<p>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.</p> <p>Example:</p> <pre>@exists ne some.property @exists ==Some.property & Some.property = "value"</pre>
---------	--

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 19: Using the Task Scheduler

The Task Scheduler enables you to schedule network management activities for your server locations and regions.

When you configure an aspect of your wireless network using the Avalanche Console, those configurations are not immediately sent to the rest of your network. Instead, you can schedule specific times during which the new configurations are sent. The Task Scheduler provides several advantages, including the ability to specify which server locations or regions receive the changes and the ability to implement changes during periods of low network activity.

Scheduling options for the Task Scheduler include:

Perform the task now Runs the task immediately.

Schedule a one-time event for the task Performs the task once at the scheduled time. This selection allows you to configure the following options:

Task Start Time. The date and time of day the event will begin.

Run until complete. When this option is selected, the task will run until it is complete.

Use End Time. The time of day when the task will end.

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

Use Location's Local Time. Uses the time local to the specified server(s) rather than the local time of the enterprise server.

Schedule a recurring event for the task

Performs the task repeatedly at the scheduled times. This selection allows you to configure the following options:

Task Start Time. The time of day the event will begin.

Use end time. The time of day the event will end.

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

Use Location's Local Time. Uses the time local to the specified server(s) rather than the local time of the enterprise server.

Daily. The task is performed daily. When Daily is selected, you can also configure the following options:

- **Every weekday.** Runs the scheduled task every day Monday - Friday.
- **Every weekend.** Runs the scheduled task every Saturday and Sunday.

Weekly. The task is performed on a weekly basis. When **Weekly** is selected, you can also configure the following options:

- **Run every __ week(s) on.** This option allows you to configure whether the task is run weekly or at a longer interval. For example, if you want the task to run every other Saturday, type 2 in the text box and enable the **SAT** checkbox.

- **[days of the week]**. These checkboxes allow you to specify which days of the week the task is performed.

Monthly. The task is performed on a monthly basis. When **Monthly** is selected, you can also configure the following option:

- **Run on the __ day, every __ month(s).** This option allows you to set the day of the month to run the task, and how many months apart the task should be run.

Start date. Specifies the date the task should begin running.

No end date. When this option is selected, the task will continue repeating indefinitely.

End by. When this option is selected, the task will no longer run after the specified date.

The Task Scheduler available from the Java Console allows you to perform the following tasks:

- Performing a Universal Deployment
- Deploying Servers
- Uninstalling Servers
- Updating Infrastructure Firmware
- Applying and Deploying Profiles
- Backing Up the System
- Restoring the System
- Removing Completed Tasks

Performing a Universal Deployment

Any time you make changes to profiles, settings or configurations in the Avalanche Console, you must perform a universal deployment before those changes are applied to your Servers and mobile devices.

To perform a universal deployment:

- 1 Click **Tools > Task Schedule**.

The *Task Schedule* dialog box appears.

- 2 Click **Add**.

The *Select A Task* dialog box appears.

- 3 Select **Universal Deployment** from the **Task Type** drop-down list and click **Next**.

The *Select Task Destinations* dialog box appears.

- 4 Select the regions or server locations by enabling the check box next to the region or server location name. You can also select all regions by clicking **Select All**.

- 5 Click **Next**.

The *Select Scheduling Options* dialog box appears.

- 6 Determine when the event will occur and click **Next**.

The *Review Your Task* dialog box appears.

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

The *Task Scheduled* dialog box appears.

- 8 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 Tasks** list. The task will run according to its schedule, and once it has completed, it will move to the **Completed Tasks** list.

Deploying Servers

After you have added a server location and created a deployment package, you can deploy an infrastructure or mobile device server using the Task Scheduler. When you deploy a server, the package is sent to the server location and the server is installed.

To deploy a server:

- 1 Ensure you have created a server deployment package and added a server location to your enterprise in the Avalanche Console.

- 2 Click **Tools > Task Schedule**.

The *Task Schedule* dialog box appears.

- 3 Click **Add**.

The *Select A Task* dialog box appears.

- 4 Select **Deploy/Update Distributed Servers** from the **Task Type** drop-down list and click **Next**.

The *Select Task Destinations* dialog box appears.

- 5 Select the server location by enabling the checkbox next to its name.

- 6 Click **Next**.

The *Select Server Package to Deploy* dialog box appears.

- 7 Select a server package and click **Next**.

NOTE If you have not created a deployment package, you can do so at this time by clicking the **Open Deployment Package Manager** link at the bottom of the dialog box. See *Building Server Deployment Packages* on page 98 for more information on creating deployment packages.

The *Select Scheduling Options* dialog box appears.

- 8 Determine when the event will occur and click **Next**.

The *Review Your Task* dialog box appears.

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

The *Task Scheduled* dialog box appears.

- 10 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 Tasks** list. The task will run according to its schedule, and once it has completed, it will move to the **Completed Tasks** list.

Uninstalling Servers

You can remove a server from a server location at any time. When you remove a server from a server location, you will not longer be able to manage devices associated with that server. You can either install a new server or delete the server location.

To remove a server:

- 1 Click **Tools > Task Schedule**.

The *Task Schedule* dialog box appears.

- 2 Click **Add**.

The *Select A Task* dialog box appears.

- 3 Select **Uninstall Distributed Servers** from the **Task Type** drop-down list and click **Next**.

The *Select Task Destinations* dialog box appears.

- 4 Select the server location from which you want to remove a server by enabling the checkbox next to its name.

The *Select Distributed Servers to Uninstall* dialog box appears.

- 5 Select if you want to uninstall the Infrastructure Server, the Mobile Device Server, or both Servers. Click **Next**.

The *Select Scheduling Options* dialog box appears.

- 6 Determine when the event will occur and click **Next**.

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

The *Review Your Task* dialog box appears.

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

The *Task Scheduled* dialog box appears.

- 8 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 Tasks** list. The task will run according to its schedule, and once the servers are removed, the task will move to the **Completed Tasks** list.

Updating Infrastructure Firmware

Once you create a firmware package, you must deploy to the infrastructure servers in your network.

For information about creating firmware packages, refer to *Creating Firmware Packages* on page 164.

To deploy firmware packages:

- 1 Click **Tools > Task Schedule**.

The *Task Schedule* dialog box appears.

- 2 Click **Add**.

The *Select A Task* dialog box appears.

- 3 Select **Update Infrastructure Firmware** from the **Task Type** drop-down list and click **Next**.

The *Select Task Destinations* dialog box appears.

- 4 Select the regions or server locations by enabling the checkbox next to the group or server location name. You can also select all groups by clicking **All**.

5 Click **Next**.

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

6 Select the firmware packages you want to deploy by enabling the checkbox next to the name of the firmware package.

7 Click **Next**.

The *Select Scheduling Options* dialog box appears.

8 Determine when the event will occur and click **Next**.

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

The *Review Your Task* dialog box appears.

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

The *Task Scheduled* dialog box appears.

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

Applying and Deploying Profiles

A profile must be applied and deployed in order for the settings to take effect. When you use the Task Scheduler to apply and deploy profiles, you can select

To deploy a profile:

1 Click **Tools > Task Schedule**.

The *Task Schedule* dialog box appears.

2 Click **Add**.

The *Scheduled Task Wizard* dialog box appears.

3 Select **Apply / Deploy Profiles** from the **Task Type** drop-down list and click **Next**.

The *Select the Targets* screen appears.

- 4 Select the regions or server locations to which the profile will be applied by enabling the checkbox in the Apply column. You can also select the locations where the profile will be deployed at the time the task is performed. Click **Next**.

NOTE If the profile is applied to a location but not deployed at the time the task is performed, the profile will be deployed the next time there is a universal deployment.

The *Schedule the Time Window* dialog box appears.

- 5 Determine when the event will occur and click **Next**.

The *Review Your Task* dialog box appears.

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

The *Task Scheduled* dialog box appears.

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

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 a name for the system backup and click **Next**.

NOTE The tag is an identifier that can be used to select the correct file when restoring the system. The tag 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 and click **Next**.

The *Review Your Task* dialog box appears.

- 6 Review your task to ensure that it is correct and click **Next**.

The *Task Scheduled* dialog box appears.

- 7 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.

NOTE If there is any information in the system that was not backed up, it will be replaced when the system is restored.

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.
- 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.

Removing Completed Tasks

When the Task Scheduler has completed an event, that event appears in the **Completed Tasks** list. By default the Task Scheduler is set to retain all completed tasks in this list. However, you can configure the scheduler to remove task periodically.

To schedule task removal:

- 1 Click **Tools > Task Schedule**.

The *Task Schedule* dialog box appears.

- 2 Enable the **Remove Completed Events After** option and then select the number of days you want to pass before the completed tasks are removed.
- 3 Click **Refresh** to update the scheduler.

NOTE If you want to remove all completed tasks immediately, enable the option, leave the number of days at zero and click **Refresh**.

The completed tasks will be removed according to your settings.

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, Infrastructure 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 Agent

C:\Program Files\Wavelink\MM\Program\AgentSvc.exe

Enterprise Server and Infrastructure Server

Wavelink Avalanche Service Manager (1 of 2)

C:\Program Files\Wavelink\MM\Program\WLAmcServiceManager.exe

Mobile Device Server and Infrastructure Server

Wavelink Avalanche Service Manager (2 of 2)

C:\Program Files\Wavelink\Avalanche\Service\WLAmcServiceManager.exe

Mobile Device Server and Infrastructure Server

NOTE The last Wavelink Avalanche Service Manager to be installed determines the path to the service.

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 Service Manager

C:\Program Files\Wavelink\MM\Program\svcmgr.exe

Infrastructure Server

Wavelink Stat Server Enterprise

C:\Program Files\Wavelink\AvalancheMC\StatServer.exe

Stats Server

Wavelink TFTP Server

C:\Program Files\Wavelink\MM\Program\TftpSvc.exe

Infrastruture Server

Wavelink Deployment

C:\Program Files\Wavelink\AvalancheMC\iserv.exe

Enterprise Server

Wavelink Alerts

C:\Program Files\Wavelink\MM\Program\AlertSvc.exe

Infrastructure Server

Wavelink Avalanche Agent

C:\Program Files\Wavelink\Avalanche\Service\WLAvalancheService.exe

Mobile Device Server

Appendix C: Port Information

This appendix provides information about the ports used in Avalanche MC. The information provided includes:

- Database Ports
- Enterprise Server Ports
- Infrastructure 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.

When Avalanche connects to an external database, it uses the hostname and port provided by the user at the time of installation. The port is typically 5432 for a PostgreSQL database, 1433 for an MS SQL Server database, or 1521 for an Oracle database.

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.

Infrastructure Server Ports

The following table provides a list of the ports that the Infrastructure Server uses.

Port	Description	Port Type
22	SSH ¹	TCP/UDP
23	Telnet ¹	TCP/UDP
25	SMTP ²	TCP
69	TFTP	UDP
80	HTTP ¹	TCP
161	SNMP ¹	TCP/UDP
162	SNMP Traps	UDP
2313	Discovery of Proxim APs through IAPP	UDP
7200	Infrastructure Site Console initiates authentication with Infrastructure Server	TCP
7205	Alert Service passes alerts to Infrastructure Server	TCP
7210	Alert Service initiates authentication with Infrastructure Site Console	TCP
7211	Infrastructure Site Console starts/stops Infrastructure Server	TCP
7212	Communication between Infrastructure Site Console and Infrastructure Server	UDP
7213	Alert Service communicates with Infrastructure Site Console	UDP
7215	Infrastructure Server authentication with Infrastructure Site Console	UDP

¹ These ports are used outbound to connect to infrastructure devices.

² This port is used outbound to connect to the SMTP server.

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: Supported Firmware

Avalanche is not packaged with any firmware files. You must obtain supported firmware from the manufacturer and then import the files into Avalanche.

The following table lists the vendor, hardware and firmware versions supported in Avalanche.

Vendor	Hardware	Supported Versions
Avaya	AP-3	2.5.2 2.4.11 2.4.5 2.3.3 2.3.2
	AP-4/5/6	2.5.2 2.4.11 2.4.5 2.3.3 2.3.2
	AP-8	2.5.2 2.4.11
Cisco	1100 IOS	12.3-8JED 12.3-8JEC3 12.3-8JEC 12.3-8JEB1 12.3-8JEB 12.3-8JEA3 12.3-8JEA2 12.3-8JEA1 12.3-8JEA 12.3-8JA 12.3-7JA3 12.3-7JA 12.3-4JA 12.3-2JA 12.3-2JA2 12.2-15JA 12.2-13JA3 12.2-13JA1 12.2-11JA1

Vendor	Hardware	Supported Versions
Cisco	1130	12.4.21a-JA1 12.4.10b-JDA3 12.4.10b-JA 12.4-3gJA1 12.4-3gJA 12.3-8JEA3 12.3-8JEA2 12.3-11JA4 12.3-11JA1 12.3-8JEB 12.3-8JEA1 12.3-8JEA 12.3-8JA 12.3-7JA3 12.3-7JA 12.3-4JA 12.3-2JA 12.3-2JA2
	1200	12.05 12.04 12.03T 12.02T1 12.01T1 11.56 11.42T
	1200 IOS	12.3-8JED 12.3-8JEC3 12.3-8JEC 12.3-8JEB1 12.3-8JEA3 12.3-8JEA2 12.3-8JEB 12.3-8JEA1 12.3-8JEA 12.3-8JA 12.3-7JA3 12.3-7JA 12.3-4JA 12.3-2JA 12.3-2JA2 12.2-15JA 12.2-13JA3 12.2-13JA4 12.2-13JA1 12.2-11JA1

Vendor	Hardware	Supported Versions
Cisco	1240 IOS	12.4.21a-JA1 12.4.10b-JDA3 12.4.10b-JA 12.4-3gJA1 12.4-3gJA 12.3-8JEA3 12.3-8JEA2 12.3-11JA4 12.3-11JA1 12.3-8JEB 12.3-8JEA1 12.3-8JEA
	1310BR	12.4.21a-JA1 12.4.10b-JDA3 12.4.10b-JDA2 12.4.10b-JA 12.4.3g-JA1 12.3-8JEA3 12.3-8JEA2 12.3-11JA4 12.3-11JA1 12.3-8JEB 12.3-8JEA1 12.3-8JEA 12.2(15)JA 10.4-3g-JA
	340 AP	12.05 12.04 12.03T 12.02T1 12.01T1 11.23T 11.10T1
	350 AP	12.05 12.04 12.03T 12.02T1 12.01T1 11.23T 11.10T1
	350 Bridge	12.05 12.04 12.03T 12.02T1 12.01T1 11.23T 11.10T1

Vendor	Hardware	Supported Versions
Cisco	350 IOS	12.3-8JEA3 12.3-8JEA2 12.3-8JEA1 12.3-8JEA 12.3-8JA 12.3-7JA3 12.3-7JA 12.3-4JA 12.3-2JA 12.3-2JA2 12.2-15JA 12.2-13JA2 12.2-13JA1
Dell	TrueMobile 1170	2.2.2
HP	ProCurve 520wl	2.4.5 2.1.2
Meru	MC1000	3.6-111(via Extended Device Support)
Motorola/Symbol	AP-3020	04.02-19
	AP-4121	02.70-12 02.70-06 02.52-13 02.51-23
	AP-4131	03.95-04 03.94-15a 03.93-00 03.92-21 03.70-77 03.70-46a 03.50-26 03.50-18
	AP-5131	2.3.1.0-004R 2.3.0.0-019R 2.2.2.0-001R 2.2.1.0-007R 2.2.0.0-023R 2.1.1.0-001R 2.1.0.1-003R 2.1.0.0-030R 2.0.0.0-045R 1.1.2.0-005R 1.0.1.0-004R 1.1.0.0-045R 1.0.0.0-188R 1.1.1.0-020R

Vendor	Hardware	Supported Versions
Motorola/Symbol	AP 5181	2.3.1.0-004R 2.3.0.0-019R 2.2.2.0-001R 2.2.1.0-007R 2.2.0.0-023R 2.1.1.0-001R 2.1.0.1-003R 2.1.0.0-030R 2.0.0.0-045R 1.1.2.0-005R 1.1.1.0-020R
	AP 7131	4.0.3.0-010R 4.0.2.0-003R 4.0.1.0-019R 4.0.0.0-057R 3.2.2.0-005R 3.2.1.0-012R 3.2.0.0-067R 3.0.2.0-028R 3.0.0.0-039R
	RFS 7000	4.2.0.0-024R 4.1.0.0-042R 4.0.2.0-001R 4.0.1.0-005R 4.0.0.0-067R 1.3.2.0-010R 1.3.1.0-003R 1.3.0.0-029R 1.2.0.0-040R 1.1.1.0-003R 1.1.0.0-038R 1.0.1.0-012R
	RFS 6000	4.2.0.0-024R 4.1.0.0-042R 4.0.2.0-001R 4.0.1.0-005R 4.0.0.0-067R 3.3.2.0-010R 3.3.0.0-029R 3.2.0.0-040R 3.1.0.0-024R

Vendor	Hardware	Supported Versions
Motorola/Symbol	WS 2000	2.4.3.0-020R 2.4.1.0-005R 2.4.0.0-023R 2.3.2.0-003R 2.3.1.0-012R 2.3.0.0-035R 2.3.0.0-034R 2.2.3.0-020R 2.2.2.0-003R 2.2.1.0-018R 2.2.0.0-021R 2.1.1.0-009R 2.1.0.0-035R 2.0.0.0-036R 1.5.0.0-216r 1.0.10.08
	WS 5000	1.2.0.39o 1.2.0.39f 1.1.4.30f 1.1.4.30SP1
	WS 5000 v1.2+	2.1.5.0-003R 2.1.4.0-001R 2.1.3.0-010R 2.1.2.0-010R 2.1.1.0-006R 2.1.0.0-029R 2.0.0.0-034R 1.4.3.0-012R 1.4.2.0-005R 1.4.1.0-014R 1.2.5.0-022R 1.1.4.30f
	WS 5100 v1.4+	2.1.5.0-003R 2.1.4.0-001R 2.1.3.0-010R 2.1.2.0-010R 2.1.1.0-006R 2.1.0.0-029R 2.0.0.0-034R 1.4.3.0-012R 1.4.2.0-005R 1.4.1.0-014R

Vendor	Hardware	Supported Versions
Motorola/Symbol	WS 5100 v3.0+	3.3.3.0-006R 3.3.2.0-010R 3.3.1.0-003R 3.3.0.0-029R 3.2.0.0-040R 3.1.0.0-045R 3.0.4.0-004R 3.0.3.0-003R 3.0.2.0-008R 3.0.1.0-145R 3.0.0.0-267R
Proxim	2000	2.5.5 2.5.3 2.5.2 2.4.11 2.4.5 2.4.4 2.3.3 2.3.1 2.2.2
	4000	4.0.3 4.0.2 4.0.0 3.7.0 3.6.3 3.4.0 3.2.1 3.1.0 2.6.0 2.5.2 2.4.11 2.4.10
	4900	4.0.9 4.0.3 4.0.2 4.0.0 3.7.0 3.6.3 3.4.0 3.2.1 3.1.0

Vendor	Hardware	Supported Versions
Proxim	600	2.5.5
		2.5.3
		2.5.2
		2.4.11
		2.4.5
		2.4.4
		2.3.3
		2.3.1
	2.2.2	
	700	4.0.3
		4.0.2
		4.0.1
		4.0.0
		3.7.0
3.6.6		
SYSTEMAX	AirSPEED AP 541	2.6.0
		2.5.2
	AirSPEED AP 542	2.6.0
		2.5.2
		2.4.11

Transitional Firmware

Transitional firmware refers to the rare cases when a particular firmware version is required when updating to a newer revision of firmware.

For example, when updating the WS5100 v1.4+ to a WS5100 v3.0+, you must first be on the 2.1.1.0-006R firmware, and then update to 3.0.0.0-267R. Once the update to 3.0.0.0-267R is completed, you may then update to any 3.x.x firmware.

Transitional firmware versions are fully supported in Avalanche.

The following is a list of transitional firmware.

Cisco 350 AP

- 12.2-13JA1

Cisco 1200

- 12.2-11JA1

Motorola/Symbol WS2000

- 2.0.0.0-036R

Motorola/Symbol WS5000

- 1.1.4.30SP1

Motorola/Symbol WS5100

- 2.1.1.0-006R
- 3.0.0.0-267R

Appendix E: 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 and Infrastructure 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 network infrastructure or mobile devices. The Servers apply these default profiles to any devices discovered that are not assigned to a profile.
Deployment Package	Deployment packages are software packages that can either install Distributed Server software or firmware. Deployment packages are built in the Deployment Package Manager and then must be deployed to a specified Server Location.
Device Access Privileges	Defined authorization for the Infrastructure Server to manage wireless network components, including access points, switches, and routers. An example would be SNMP community names.
DHCP	Dynamic Host Configuration Protocol. An IP service that allows DHCP clients to automatically obtain IP parameters from a DHCP server.
Distributed Servers	Also known as Servers or dServers. Servers are software packages run as services that facilitate communication between infrastructure and mobile devices and the Enterprise Server. There are Infrastructure Servers and Mobile Device Servers. Infrastructure Servers manage network infrastructure devices such as routers and access points. Mobile Device Servers manage hand-held mobile devices.

Distributed Server Locations	Also known as Server Locations. These are locations within your network where you want to manage mobile and infrastructure devices. You must deploy either a Infrastructure Server or a Mobile Device Server to a Server Location.
DNS	Domain Name System. A service that provides hostname-to-IP address mapping.
dServer	See Distributed Servers.
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.

Firmware	Firmware is the software installed on access points that determines what sort of properties and features that an access point supports.
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 sites or locations.
Infrastructure Device	Infrastructure devices include access points, routers and switches.
Infrastructure Profile	An infrastructure profile is a collection of settings that you can simultaneously apply to multiple infrastructure devices.
Infrastructure Server Profile	Infrastructure server profiles allow you to define device access privileges and data collection for your Infrastructure Servers.
Infrastructure Site Console	A tool that helps you manage infrastructure devices.
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 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.

Mobile Manager	A Wavelink solution that allows you to add, manage, and secure infrastructure devices on a wireless network. Also referred to as the Infrastructure Site Console.
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 sites/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 sites 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.
Very Large Access Control List	A Very Large Access Control List (or VLACL) is a list of MAC addresses that are allowed to communicate through access points. Unlike an Access Control List, which is managed by the access point, a VLACL is managed by an Infrastructure Server, allowing it to support thousands of MAC addresses.
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

- access control lists
 - adding entries 180
 - deploying 183
 - exporting files 182
 - importing files 182
 - managing 179
 - modifying 181
 - removing 181
- access ports 178
- activating Avalanche
 - automatically 28
 - demo mode 31
- activating Avalanche licenses 27
- alert profiles
 - assigning 261
 - removing 262
- alerts
 - acknowledging 267
 - assigning profiles 261
 - clearing 267
 - configuring profiles 258
 - contact list 262
 - managing 257
 - proxy pools 265
- assigning profiles 81
- authorized users 73, 151
 - profiles 74
 - regions 73
- auto deployment 44
- Avalanche
 - activating licenses 27
 - components 12
 - Console settings 43
 - installing 17
 - overview 14
 - restoring 295

- services 308

- Avalanche Console
 - customizing 42
 - saving views 270
 - starting 35

B

- backing up Avalanche 294
- backlogs 54
- backup drive location 49
- backups, performing 294
- barcode profiles
 - adding 121
 - configuring 120
 - custom properties 124
 - editing 129
 - network settings 121
- barcodes
 - printing 129
 - scanning 130
- base licenses 26
- batch releases 53
- blackout periods, Enterprise Server 51
- building selection criteria 272

C

- chat timeout 192
- Cisco IOS privileges 140
- Communicator 236
- compatibility mode 160
- components of Avalanche 12
- composite profile 154
- composite profiles, viewing 176
- console 51
 - auto deployment settings 44
 - customizing 43
 - preferences 42
- contact information 323

- contact list
 - creating 262
 - importing addresses 264
 - removing addresses 265
 - creating
 - custom properties 228
 - deployment packages 98
 - firmware packages 164
 - mobile device groups 250
 - network profiles 105
 - Server Locations 87
 - user accounts 65
 - custom properties, selection criteria 274
 - customizing the map 51
- ## D
- default
 - login 35
 - password 35
 - delayed software package installation 214
 - demo mode 31
 - deploying
 - access control lists 183
 - firmware 166
 - infrastructure firmware packages 292
 - servers 290
 - deployment notification 45
 - deployment packages 98
 - device access privileges
 - Cisco IOS 140
 - defining 136
 - dServer Governor 56
 - dServer governor 56
 - dump heap 58
- ## E
- Enabler Installation Tool 61
 - encryption 112
 - Enterprise Server
 - backlogs 54
 - batch releases 53
 - blackout periods 51
 - configurations 51
 - dump heap 58
 - purging server statistics 57
 - status 54
 - enterprise server connections 144
 - eServer, see Enterprise Server 51
 - exporting, access control list files 182
- ## F
- firmware
 - changing 174
 - compatibility 160
 - creating packages 164
 - full support 160
 - infrastructure 159
 - support 159
 - supported 161
 - firmware, supported 314
 - full support mode 160
- ## G
- GPS reporting 192
- ## H
- HTTP proxy connection 50
- ## I
- importing
 - access control list files 182
 - support file 157
 - InfoRail status 59
 - infrastructure
 - managing 147
 - updating firmware 159
 - infrastructure devices 168
 - advanced properties 177
 - changing firmware 174
 - connecting by web browser 175

- device filters 168
- displaying devices 170
- pinging 172
- querying 172
- resettings 172
- viewing composite profiles 176
- infrastructure firmware packages 292
- infrastructure profiles
 - deleting 157
 - properties 159
 - refreshing 159
- Infrastructure Server profiles
 - applying to a region 144
 - device access privileges 136, 140
 - removing 145
- installing
 - Avalanche 17
 - centralized server 85
 - distributed server 86
 - software packages 208
- IP address pools 107
- L**
- LDAP 75
- License Server 27
- licenses 25
 - base 26
 - maintenance 26
 - overview 25
 - releasing 32
 - running the License Server 27
 - unlicensed devices 26
- location management 13
- log file 188
- login, default 35
- M**
- maintenance licenses 26
- managing
 - access control lists 179
 - infrastructure 147
 - mobile devices 219
- map 268
- map options 51
- map pane
 - relocating a site 270
 - saving views 270
- Mobile Device Details dialog box 225
- mobile device groups 250
 - adding properties 254
 - additional functions 256
 - creating 250
 - pinging 253
 - sending messages to 254
- Mobile Device Inventory tab
 - custom properties 223
 - device filters 223
 - modifying columns 221
 - removing columns 223
- mobile device profiles 237
- mobile device server
 - license options 190
 - licensing messages 200
 - reinitializing 200
 - reserving serial ports 189
- mobile device server profiles
 - adding 185
 - assigning to a region 200
 - authentication 187
 - enabling 186
 - log file 188
 - removing 199
- mobile devices
 - caching 192
 - contacting 230
 - creating custom properties 228
 - deleting properties 230
 - details 225
 - device filters 223
 - device-side properties 229

- editing properties 229
- GPS reporting 192
- installed software tab 237
- locating 233
- location history 233
- log file 188
- managing 219
- pinging 231
- properties 227
- Remote Control 234
- sending messages 231
- server profile settings 192
- session monitor 235
- updating 197, 232
- viewing properties 227

Mobile Manager 13

Mobile Manager Enterprise, removing 17

modifying

- mobile device columns 221
- Server Location properties 90

moving a site (Server Location) 270

moving Server Locations to regions 90

N

navigation window 37

nested regions 81

- creating 81
- profile behavior 81

network events 151

network profile

- scheduled settings 109
- WLAN IP settings 111
- WLAN settings 112
- WWAN settings 117

network profiles 105

- configuring 106
- creating 105
- enabling 106
- IP address pools 107

O

overview 14

P

password

- default 35
- user accounts 76

peer-to-peer package distribution 216

permission types 64

permissions 64

- profile 71
- regional 69
- software profiles 151
- user accounts 69

pinging infrastructure devices 172

pinging mobile devices 231, 253

pinging sites 94

ports 311

- database 311
- enterprise server 311
- Infrastructure Server 312
- Mobile Device Server 313

profile permission

- assigning 71
- definition 64

profiles

- composite 154
- software 201

properties

- custom 228
- deleting 230
- editing 229
- infrastructure profile 159
- mobile device groups 254
- mobile devices 227
- region 81

proxies

- adding 265

purging server statistics 57

Q

- querying infrastructure devices 172
- quick start
 - disabling 38
 - overview 38

R

- regional permission
 - assigning 69
 - definition 64
- regions 13, 80
 - adding 80
 - assigning network profiles 118
 - assigning profiles 81
 - deleting 83
 - nested regions 81
 - properties 81
- reinitializing the Mobile Device Server 101
- releasing licenses 32
- Remote Control 234
- Removing 199
- removing
 - columns 223
 - Server Locations 92
 - user accounts 77
- removing completed tasks 297
- resetting access points 172
- restoring
 - Avalanche 295
 - Server Locations 92

S

- scan to configure 120
 - barcode profiles 120
 - creating custom properties 124
 - printing barcodes 129
 - scanning barcodes 130
- scheduled settings 109
- selection criteria
 - building 272

- custom properties 274
- selection variables
 - Assigned IP 281
 - Columns 275
 - EnablerVer 275
 - IP 276
 - KeyboardCode 276
 - KeyboardName 277
 - LastContact 278
 - MAC 279
 - ModelCode 280
 - ModelName 279
 - OSType 280
 - OSVer 278, 280
 - Processor 280
 - ProcessorType 280
 - Rows 282
 - Series 281
 - Terminal ID 282
- sending messages 254
- Server
 - auto-discovery 100
 - properties 100
 - starting 98
 - stopping 98
- server
 - centralized installation 85
 - distributed installation 86
- Server Locations 13, 83
 - creating 87
 - moving 90
 - properties 90
 - removing 92
 - restoring 92
 - unassigned Server Locations 89
- server,deployment 290
- services, Avalanche 308
- session monitor 235
- site-level tools 13
- sites 93

- editing properties 95
- pinging clients 94
- sending messages to 94
- software inventory 237
- software packages
 - configuring 214
 - copying 213
 - delayed installation 214
 - enabling 213
 - installing 208
 - peer-to-peer distribution 216
- software profiles
 - adding 201
 - applying 205
 - authorized users 151
 - editing 203
 - enabling 203
 - managing 201
- special characters for login 66
- SSID 112
- starting the Avalanche Console 35
- static mobile device groups
 - adding devices 251
 - removing devices 252
- support file, importing 157
- Support Generator 60
- supported firmware 314
- syntactical symbols
 - And (&) 284
 - Eq (=,=) 284
 - Not (!) 283, 285
 - Or (|) 284

T

- task scheduler 286
- terminal IDs 189
- types of firmware support 159

U

- unassigned Server Locations 89

- uninstalling servers 294
- universal deployments 289
- unlicensed devices 26
- updates 232
- user accounts 64
 - authorized users 73
 - creating 65
 - creating groups 68
 - enabling domain validation 75
 - LDAP 75
 - password 76
 - permissions 69
 - removing 77
 - special characters 66
- user groups 68

W

- Wavelink contact information 323
- WLAN IP settings 111
- WLAN settings 112
- WLAN settings for infrastructure 154
- WWAN settings 117