Avalanche MC

Wavelink Avalanche Mobility Center

Version 4.6

amc-ug-46-20080516

Revised 7/24/08

Copyright © 2008 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.

Symbol, Spectrum One, and Spectrum24 are registered trademarks of Symbol Technologies, Inc.

Table of Contents

Chapter 7: Managing Network Profiles 143

Chapter 8: Managing Infrastructure Distributed Servers 167

Chapter 9: Managing Mobile Device Distributed Servers 183

Chapter 15: Managing Alerts 287

Chapter 16: Using Scan to Configure 301

Chapter 1: Introduction

This document is a complete guide to the functions and components of the Wavelink Avalanche Mobility Center (Avalanche MC). This document presents:

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

This introduction defines the assumptions and conventions of this document and provides an overview of Avalanche MC.

About This Document

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

Document Assumptions

This document makes the following assumptions:

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

Document Conventions

This document uses the following typographical conventions:

`Courier New`

Any time you interact with 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.

Example:

See *Components of Avalanche MC* on page 15 for more information.

The *Infrastructure Profiles* dialog box appears.

Managing Networks with Avalanche MC

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

- Components of Avalanche MC
- Location Management: dServer Locations and Regions
- Mobile Manager

Components of Avalanche MC

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

The primary components of Avalanche MC include:

- **Avalanche MC Console**. The Avalanche MC Console is your interface to wireless network components. With the Avalanche MC Console, you can manage and maintain everything from infrastructure device settings to mobile device software.

- **Avalanche MC Server**. The Avalanche MC Server facilitates all communication between the Console, the dServers, and the database.

- **Distributed Servers**. Distributed Servers (or dServers) consist of server-side software that is responsible for communicating information to and from the Avalanche MC Console and wireless components. Avalanche MC contains two types of dServers: an Infrastructure dServer and a Mobile Device dServer. These dServers must be installed at each location that you want to manage.

- **Enablers**. Mobile devices require an additional component, called an Enabler, to be managed by Avalanche MC. An Enabler is software installed on each mobile device that relays information between the mobile device and the Mobile Device dServer. With the Enabler installed, the mobile device can receive configuration instructions that you create in the Avalanche MC Console.

Location Management: dServer Locations and Regions

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

Avalanche MC divides locations into two categories: regions and dServer Locations. A dServer Location is the most basic component of the Avalanche MC Console. Each dServer Location contains at least one Server that communicates with specific wireless components. Because these dServer Locations are based on Servers, you can define a dServer Location in a way that best suits your network administration processes—for example, you can organize dServer Locations by location or by network role.

NOTE The number of wireless components managed at a dServer Location depends on the communication range of the Servers installed at that dServer 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 dServer Location level, using the Mobile Manager Administrator. See the *Mobile Manager User's Guide* for more information.

Avalanche MC further streamlines wireless network management by allowing you to create one or more collections of dServer Locations, called regions. Each dServer Location within a region contains a set of similar characteristics such as geographic location or role within your organization's structure. When you configure a region, the Avalanche MC Console applies the configurations to every dServer Location within that region.

Mobile Manager

Although you manage most aspects of your wireless network using the Avalanche MC Console, specific dServer Locations within the network might require additional configurations. These configurations can be made using the Mobile Manager Administrator. The Administrator is a tool designed to manage infrastructure devices at a specific dServer 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 MC installation and configuration and to ensure optimal performance, Wavelink recommends you perform the following steps in order:

1 **Install Avalanche MC**. For more information, refer to *Chapter 2: Installing Avalanche MC* on page 21.

2 **Activate Mobile Device dServer and Infrastructure dServer licenses for Avalanche MC.** 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 43.

3 **Create Regions.** A region is a collection of dServer 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 105.

4 **Create dServer Locations.** dServer Locations are the basic component of Avalanche MC and are where the Servers reside. For more information, refer to *Managing dServer Locations* on page 114.

5 **Install Servers.** Create a server package to deploy to the regions. This will install the Servers and apply all profile configuration to the devices at the dServer Location. For more information, refer to *Building Server Deployment Packages* on page 131.

6 **Configure profiles.** You can configure settings for network, software, alert, Server, and infrastructure profiles. Once you create these profiles, you assign the profiles to regions you have created. For more information, refer to *Chapter 15: Managing Alerts* on page 287, *Chapter 8: Managing Infrastructure Distributed Servers* on page 167, *Chapter 9: Managing Mobile Device Distributed Servers* on page 183, *Chapter 10: Managing Software Profiles* on page 209, *Chapter 7: Managing Network Profiles* on page 143, and *Chapter 11: Managing Infrastructure Profiles* on page 225.

7 **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 dServer Locations within the region. For more information, refer to *Assigning Profiles to Regions* on page 107.

8 **Perform Updates**. To ensure settings reach the selected regions and dServer Locations, perform a Universal Update through the Task Schedule. For more information refer to *Deploying Universal Updates* on page 334.

Avalanche MC employs profile-based configuration which allows you to create templates of configuration settings and then assign those templates to specific regions and dServer Locations. As a result, you can update or modify multiple dServers, instead of manually changing each one.

Once you assign and deploy a profile to a dServer, the dServer retains its configuration values until you the profile in Avalanche MC. Even if you alter configuration values without using Avalanche MC, when the dServer queries the mobile devices or infrastructure devices, 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 MC detects a device that is not associated with a profile, Avalanche MC assigns the default profile to that device.

How To Use This Guide

To assist you in setting up your Avalanche MC Enterprise, this user guide is organized in the following manner:

Chapter	Content
Chapter 1: Introduction	Introduces Avalanche MC and the components therein.
Chapter 2: Installation	Provides installation requirements and methods to install Avalanche MC.
Chapter 3: Licensing	Provides information about activating licenses for mobile and network infrastructure devices. This enables Avalanche MC to manage the devices.
Chapter 4: Avalanche MC Console	Introduces the tools of the Avalanche MC Console.
Chapter 5: User Accounts	Provides instructions to create user accounts and assign permissions to each account.
Chapter 6:Regions and dServer Locations	Provides location management information and instructions to create regions, dServer Locations and sites.
Chapter 7: Network Profile	Provides network configuration instructions.
Chapter 8: Infrastructure Distributed Server	Provides information about configuring Infrastructure dServer profiles and then applying the profiles to the Infrastructure dServer.

Chapter	Content
Chapter 9: Mobile Device dServer	Provides information about configuration options for the Mobile Device dServer including device administration and connections.
Chapter 10: Software Profiles	Provides software profiles configuration information and instructions for installing software packages.
Chapter 11: Infrastructure Profile	Provides information about creating and configuring Infrastructure Profiles.
Chapter 12: Update Profiles	Provides information how to configure and use update profiles to conserve bandwidth.
Chapter 13: Mobile Devices	Provides information about managing mobile devices through the Avalanche MC Console.
Chapter 14: Mobile Device Groups	Provides information about the function and use of Mobile Device Groups.
Chapter 15: Alert Profiles	Provides information about configuring alert profiles to notify the console when a certain event occurs at the dServers.
Chapter 16: Using Scan to Configure	Provides information about scan to configure barcode profiles and how to configure the profiles with network settings and apply those settings to a mobile device.
Chapter 17: Using Very Large Access Control Lists	Provides information about creating and using Very Large Access Control Lists.
Chapter 18: Using Selection Criteria	Defines selection criteria components.
Chapter 19: Using the Task Scheduler	Defines the tasks you can perform using the Task Scheduler.
Appendix A: Installing Enablers	Provides information about installing Enablers on mobile devices.
Appendix B: Manually Deploying Servers and Firmware	Provides the instructions for remotely deploy dServers and firmware.
Appendix C: Ports	Defines the ports used for Avalanche MC
Appendix D: Managing dServers on Linux OS	Provides information about managing Mobile Device dServers and Infrastructure dServers from a Linux console.
Appendix E: Avalanche MC Services	Defines the Avalanche MC services.
Appendix F: Wavelink Contact Information	Provides the contact information for Wavelink Customer Service.

Avalanche MC Terminology

For a complete list of Avalanche MC terms and components, refer to the Glossary.

Chapter 2: Installing Avalanche MC

Avalanche MC 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:

- Installation Requirements
- Which Version of Avalanche MC Should I Install?
- Installing Avalanche MC Enterprise
- Installing Avalanche MC Console Only
- Installing Avalanche MC Site
- Installing Avalanche MC with SQL Server
- Importing Avalanche Manager Backup Files
- Uninstalling Avalanche MC

Installation Requirements

Optimal requirements for the Enterprise Server, Console, Mobile Device dServer and Infrastructure dServer depend on a number of factors, such as the number of mobile devices you want to manage and your overall network setup.

The Avalanche MC software footprint is approximately 2 GB. The rest of the recommended space is reserved for software packages, firmware, alerts and logging. The actual amount of the space you will need depends on how you are running the system, how many devices and dServer locations you want, and the types of software packages you install.

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

The specifications quoted in this section are intended to serve as a guide only. For larger installations it is recommended that you contact Wavelink Customer Service for specific guidelines.

The following sets of requirements are necessary to install the components of Avalanche MC:

- **Avalanche MC Enterprise Server Requirements**. These requirements are necessary to install and run the Avalanche MC server.

- **Avalanche MC Console Requirements**. These requirements are necessary to install and run the Avalanche MC Console.

- **Mobile Device dServer Requirements**. These requirements are necessary to deploy Mobile Device dServers. For more information about Mobile Device dServers, refer to *Chapter 9: Managing Mobile Device Distributed Servers* on page 183.

- **Infrastructure dServer Requirements**. These requirements are necessary to deploy Infrastructure dServers. For more information about Infrastructure dServers, refer to *Chapter 8: Managing Infrastructure Distributed Servers* on page 167.

- **Microsoft Microsoft SQL Server Database Requirements**. These requirements are necessary if you are planning to use SQL Server for your database.

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

NOTE You cannot install Avalanche MC on a system where the PostgreSQL database is already installed.

Avalanche MC Enterprise Server Requirements

This section lists the hardware, software, and other requirements that the Avalanche MC Enterprise Server requires for best performance. These requirements are the same for Enterprise installations and Site installations.

The Avalanche MC software footprint is approximately 2 GB. The rest of the recommended space is reserved for software packages, firmware, alerts and logging. The actual amount of the space you will need depends on how you are running the system, how many devices and dServer locations you want, and the types of software packages you install.

Minimum Hardware Requirements

The Enterprise Server requires the following hardware components to operate effectively (when managing 1,000 devices or less):

- Intel Pentium 4 Processor at 2.8 GHz (or equivalent).
- 2 GB RAM
- Required free disk space: 50 GB

NOTE The Avalanche MC software uses 2 GB. The remaining disk space is reserved for software packages, firmware, alerts and logging.

Software Requirements

The Enterprise Server requires one of the following operating systems:

- Windows 2000 Server (SP 4)
- Windows 2000 Professional (SP 4)
- Windows 2003 Server (SP 2 or later)
- Windows XP (SP 2 or later)

NOTE These are the verified and recommend service pack versions. Previous service pack version may function, but have not been confirmed.

Other Requirements

The Enterprise Server requires these miscellaneous requirements:

- Administrator login rights. You must have administrator login rights to the machine on which you are installing Avalanche MC.
- Partition/Disk NTFS file system.

- J2SE Runtime Environment 5.0

NOTE J2SE Runtime Environment is automatically installed by the Avalanche MC installer if it is not already on your system.

Avalanche MC Console Requirements

This section lists the hardware, software, and other requirements that the Avalanche MC Console requires for best performance.

Minimum Hardware Requirements

The Avalanche MC Console requires the following hardware components to operate effectively:

- Intel Pentium 4 Processor at 2.0 GHz (or equivalent).
- 1.5 GB RAM
- Required free disk space: 5 GB
- Recommended free disk space: 10 GB

Software Requirements

The Avalanche MC Console requires one of the following operating systems:

- Windows 2000 Server (SP 4)
- Windows 2000 Professional (SP 4)
- Windows 2003 Server (SP 2)
- Windows XP (SP 2)

NOTE These are the verified and recommend service pack versions. Previous service pack version may function, but have not been confirmed.

Other Requirements

The Avalanche MC Console requires these miscellaneous requirements:

- Administrator login rights. You must have administrator login rights to the machine on which you are installing Avalanche MC.
- Partition/Disk NTFS file system.
- J2SE Runtime Environment 5.0

NOTE J2SE Runtime Environment will be automatically installed by the Avalanche MC installer if it is not already on your system.

Mobile Device dServer Requirements

This section lists the hardware, software, and other requirements, including RAPI requirements, that the Mobile Device dServer requires for best performance.

Minimum Hardware Requirements

The following are the minimum requirements for each dServer Location that contains a Mobile Device dServer:

- Intel Pentium 4 Processor at 2.8 GHz (or equivalent).
- 1.5 GB RAM
- 10 GB free disk space

NOTE Requirements for hard disk space are subject to change based on software package installation.

Software Requirements

The Mobile Device dServer for Avalanche MC requires one of the following operating systems:

- Windows 2000 Server (SP 4)
- Windows 2000 Professional (SP 4)
- Windows 2003 Server (SP 2)
- Windows XP (SP 2)

NOTE These are the verified and recommend service pack versions. Previous service pack version may function, but have not been confirmed.

RAPI Support Requirements

The following requirements apply to RAPI support and are only required if you want to use the RAPI interface feature:

- ActiveSync 3.7.1 or 3.8
- ActiveSync supported connection
- Serial port for serial connection

Other Requirements

- Shared file folder on the host system where the administrator has full control.
- Administrative rights on the system.

Infrastructure dServer Requirements

This section lists the hardware, software and other requirements that the Infrastructure dServer requires for best performance.

Minimum Hardware Requirements

The following are the minimum requirements for each dServer Location that contains an Infrastructure dServer:

- Intel Pentium 4 Processor at 2.8 GHz (or equivalent).
- 1.5 GB RAM
- 10 GB free disk space

The amount of space required is dependent on the following settings:

- Device statistics query interval. The default value is 30 minutes. If you decrease this interval, the hard disk requirements increase.

- Statistics settings (length of time to keep statistical records). The default value is seven months. If you increase this value, the hard disk requirements increase.
- Alert settings (length of time to keep alerts/maximum number of alerts). The default values are 30 days and 100,000 maximum alerts. If you increase these values, the hard disk requirements increase.

It is important to remember that these requirements are *minimum* requirements. If you plan to deploy multiple Infrastructure dServers, you will need to plan accordingly based on your network, system and set up.

Software Requirements

The Infrastructure dServer for Avalanche MC requires one of the following operating systems to run effectively:

- Windows 2000 Server (SP 4)
- Windows 2000 Professional (SP 4)
- Windows 2003 Server (SP 2)
- Windows XP (SP 2)

NOTE These are the verified and recommend service pack versions. Previous service pack version may function, but have not been confirmed.

Firmware Requirements

To support as many infrastructure devices as possible, Avalanche MC interacts with infrastructure devices in one of two modes: full support mode or compatibility mode. Avalanche MC selects which mode to use based on whether it can recognize the firmware version installed on an infrastructure device. In full support mode, the Server recognizes the firmware and is able to retrieve and set the majority of options for that infrastructure device. In compatibility mode, the Server cannot recognize the firmware and attempts to use existing infrastructure device property files to retrieve and set as many of the infrastructure device options as possible.

NOTE See your *Avalanche Mobility Center Release Notes* or contact Wavelink Customer Service to determine the firmware supported by your version of Avalanche MC.

Other Requirements

- Shared file folder on the host system where the administrator has full control.
- Administrative rights on the system.
- Partition/Disk NTFS file system

Microsoft SQL Server Database Requirements

The Installation script will be responsible to ask the user which DBMS should be used for the current installation. If MS SQL Server 2005 is selected, the user must supply the following pieces of information to the Installation script:

- Server name (DNS name or IP Address)
- Server Port
- SQL Server Account Name
- SQL Server Account Password

For SQL Server 2005 databases, the user is also responsible to have their DBA create a database on the indicated server with the name `amcxx` (where xx represents the release number of Avalanche MC). The owner of the database should be set to be the user account specified above.

Currently, no cross-platform (i.e. Postgres to SQL Server, or SQL Server to Postgres) migration is allowed.

Which Version of Avalanche MC Should I Install?

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

- If you plan to manage both mobile and network infrastructure devices in a distributed server environment, you should install Avalanche MC Enterprise.
- If you plan to manage both mobile device and network infrastructure appliances, but in a centralized dServer environment (only one dServer) you should install Avalanche MC Site.
- If you plan to manage mobile devices only install Avalanche MC Site.
- If you have already installed the Enterprise Server and other components of Avalanche MC on another system and just want to view the happenings at the console, you should install the Console only version of Avalanche MC.

Be sure you review the installation requirements for each version.

Installing Avalanche MC Enterprise

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

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

You can not install Avalanche MC on a system where Mobile Manager Enterprise is currently installed. You must remove Mobile Manager Enterprise before you attempt to install Avalanche MC. 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 at any time, 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 MC* on page 40.

To install Avalanche MC:

1 Download the self-extracting zip file from the Wavelink Web dServer Location.

2 Double-click the file to start the installation process.

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

The *Introduction* dialog box appears.

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

The *License Agreement* dialog box appears.

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

NOTE If you do not click **Yes**, you will not be able to complete the installation process.

The *Select Installation* dialog box appears.

5 Select **Enterprise** and click **Next**.

The *Choose Destination Location* dialog box appears.

6 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.

Avalanche MC is installed on your system. The Setup program configures several internal components to run on your system.

Once the installation is complete, you are immediately prompted to activate this installation of Avalanche MC for your network. For more information about activating Avalanche MC, refer to *Chapter 3: Licensing* on page 43.

7 If you do not want to activate at this time, click **Close**.

The *Finish* dialog box appears.

8 Click **Finish**.

Installing Avalanche MC 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 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.

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

The *Introduction* dialog box appears.

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

The **License Agreement** dialog box appears.

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

NOTE If you do not click **Yes**, you will not be able to complete the installation process.

The *Select Features* dialog box appears.

Because this is a console-only installation, **Console** is the only option and enabled by default.

5 Click **Next**.

The *Choose Destination Location* dialog box appears.

6 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 MC Console is installed on your system.

7 Click **Finish**.

Installing Avalanche MC Site

When you choose to install the Site version of Avalanche MC (as a replacement for Avalanche Manager Site) you automatically create one local dServer Location on the machine to which you are installing Avalanche MC. A Mobile Device dServer automatically installs to the local dServer Location.

Before you install Avalanche MC, remove any previous version of Avalanche MC from the system. This ensures Avalanche MC installs properly.

For information about removing Avalanche MC, refer to *Uninstalling Avalanche MC* on page 40.

To install Avalanche MC Site:

1 Download the self-extracting zip file from the Wavelink Web Site.

2 Double-click the file to start the installation process.

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

The *Introduction* dialog box appears.

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

The *License Agreement* dialog box appears.

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

NOTE If you do not click **Yes**, you will not be able to complete the installation process.

The *Setup Type* dialog box appears.

Because this is a console-only installation, **Console** is the only option and enabled by default.

5 Click **Next**.

The *Choose Destination Location* dialog box appears.

6 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.

Avalanche MC is installed on your system. The Setup program configures several internal components to run on your system.

Once the installation is complete, you are immediately prompted to activate this installation of Avalanche MC for your network. For more information about activating Avalanche MC, refer to *Activating Avalanche MC* on page 46.

7 If you do not want to activate at this time, click **Close**.

The *Finish* dialog box appears.

8 Click **Finish**.

Installing Avalanche MC with SQL Server

SQL server 2005 is supported in Avalanche MC. The server must already be installed. You will need the following database information to install Avalanche MC:

- Server name (DNS name or IP Address)
- Server Port
- SQL Server Account Name
- SQL Server Account Password

This information is necessary to connect to the database.

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

Before You Begin

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

- Create the database
- Create login
- Assign the login to the database and as the owner

Setting Login Properties

Before you can install Avalanche MC, a database administrator must set up a login on the SQL server.

To set the database login properties:

1 From SQL Server Management Studio, select **Object Explorer** and click **Security Folder > Logins**.

2 Right-click **Logins** and select **New Login**.

The *Login Properties* dialog box appears.

3 In the **Select a page** region, click **General**.

4 In the **Login Name** text box, enter the name for this login.

5 From the **Default database** drop-down list, select **amc46 .**

6 In the **Select a page** region, select **User Mapping**.

The *User Mapping* page appears.

7 From the **Database role membership for: amc 46** list box, enable **db_owner** and **db_public**.

8 Click **OK**.

Completing the Installation

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

To install Avalanche MC:

1 Download the self-extracting zip file from the Wavelink web site.

2 Double-click the file to start the installation process.

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

The *Introduction* dialog box 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**.

NOTE If you do not click **Yes**, you will not be able to complete the installation process.

The *Database Options* dialog box appears.

5 Select **SQL Server 2005** and click **Next**.

NOTE SQL Server must already be installed.

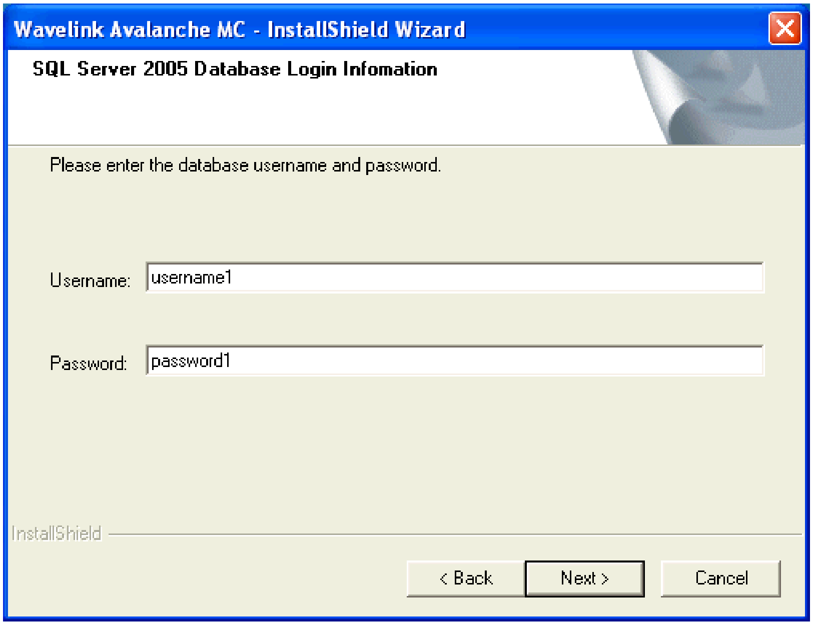
The *Database Location Information* dialog box appears.

6 Enter the Server Name (DNS name or IP address) and the port number where the database resides.

Avalanche MC uses this information to connect to the database.

7 Click **Next**.

The *Database Login* dialog box appears.



Wavelink Avalanche MC - InstallShield Wizard

SQL Server 2005 Database Login Infomation

Please enter the database username and password.

Username: username1

Password: password1

Figure 2-1. *Database Login Information*

8 Enter the user name and password for the database.

Avalanche MC uses this information to connect to the database.

9 Click **Next**.

The *Setup Type* dialog box appears.

10 Select which installation type you want to install.

- **Enterprise**. Installs support for Mobile Device dServers and Infrastructure dServers.
- **Site**. Installs one Mobile Device dServer on the local machine.

11 Click **Next**.

The *Choose Destination Location* dialog box appears.

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

13 Click **Finish**.

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

Importing Avalanche Manager Backup Files

Once you have installed Avalanche MC, you can import Avalanche Manager backup files (`.abk` files) using the Import Data tool. The import tool only works with Avalanche Manager 3.6 backup files. To import data from previous versions of Avalanche Manager, you must migrate to Avalanche Manager 3.6 and create the backup file from there.

The import tool imports Network Profiles, Software Collections, Mobile Device Groups and the client database from the backup file into Avalanche MC.

When you import a backup file, the information merges with any other information you have already configured in Avalanche MC. Once you complete the import, you need to perform a Universal Deployment to alert the Mobile Device and Infrastructure Server of the console changes.

For information about creating the Avalanche Manager backup file, refer to the *Wavelink Avalanche Manager User Guide*.

To import a backup file:

1 Launch the Avalanche MC Console.

For information about launching the Avalanche MC Console, refer to *Starting the Avalanche MC Console* on page 52.

2 From the **File Menu**, select **Import Data**.

An *Open* dialog box appears.

3 Navigate to the location of the `.abk` file and select **Open**.

The *Select a Region* dialog box appears.

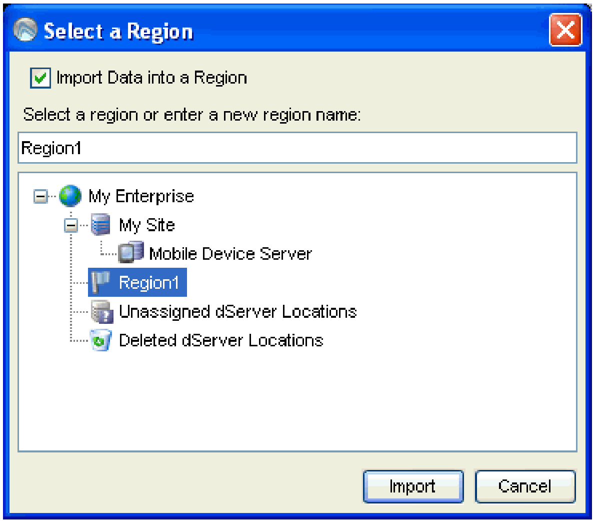

Select a Region
☑ Import Data into a Region
Select a region or enter a new region name:
Region1
My Enterprise
My Site
Mobile Device Server
Region1
Unassigned dServer Locations
Deleted dServer Locations
Import
Cancel

Figure 2-2. *Select a Region*

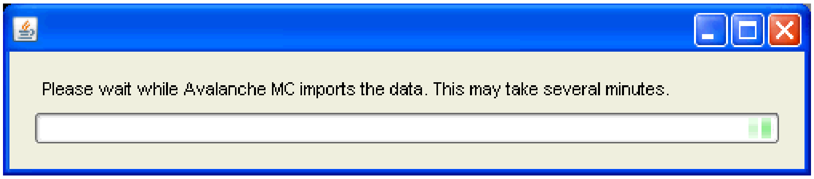
4 Enable the **Import Data into a Region** option if you want to select the region you to which the data is imported. Then type the name of or select the region and click **Import**.

-Or-

Disable the **Import Data into a Region** option and click **Import**. This imports the data to the My Enterprise level.

NOTE Selecting **Cancel** stops the importing process and closes the dialog box.

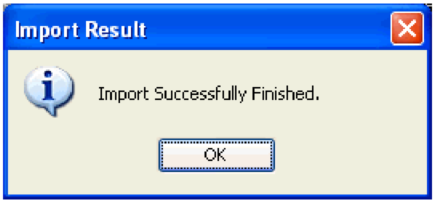
A status dialog box appears.



Please wait while Avalanche MC imports the data. This may take several minutes.

Figure 2-3. *Importing*

When the import is complete, the *Import Result* dialog box appears indicating whether the import was successful.



Import Successfully Finished.

Figure 2-4. *Import Result*

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

The data from the backup file has been imported to Avalanche MC and the database.

6 Perform a Universal Deployment to alert the Mobile Device and Infrastructure Server of the console changes.

For information about performing a Universal Deployment, refer to *Deploying Universal Updates* on page 334.

Migrated Components

The following table lists the Avalanche Manager data that is migrated to Avalanche MC.

Avalanche Manager Component	**Migrated to:**
Enterprise License	Enterprise License
License file (wavelink.lic)	License file (wavelink.lic) The License file in Avalanche Manager will only be applied to the local dServer and will not appear in the license server. Contact Wavelink Customer Service at 1-888-697-9283 for more information.
Network Profile	Network Profile Network Profiles will appear in the Network Profiles tab. Any profiles that were enabled in Avalanche Manager will be deployed and active immediately.

Table 2-1: *Components Migrated from Avalanche Manager to Avalanche MC*

Software Collections	Software Profiles Software Profiles will appear in the Software Profiles tab with the same names and settings as were configured in Avalanche Manager.
Mobile Device Groups	Mobile Device Groups Static Device Groups will not automatically contain mobile devices for the group. You will need to add matching devices to the group from the *Properties* dialog box for that mobile device group. The eServer will contact the Mobile Device Server and pull the devices that match the static group into the group. For information about adding matching devices to a mobile device group, refer to the *Avalanche Mobility Center User Guide*.
Mobile Device Inventory	Mobile Device Inventory

Table 2-1: *Components Migrated from Avalanche Manager to Avalanche MC*

Uninstalling Avalanche MC

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

When you uninstall Avalanche MC, you are given the option to uninstall the PostgreSQL database as well. If you select to uninstall Avalanche MC and the PostgreSQL database, all components of Avalanche MC and the database will be removed. If you select to uninstall Avalanche MC, 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 MC and/or the PostgreSQL database, it is recommended that you extract and backup database information and software collections. For more information, see *Appendix E: Backing Up and Restoring Avalanche MC* on page 339.

NOTE You may also want to save the `wavelink.lic` license file, as it will be removed when Avalanche MC is uninstalled. To save the license file, navigate to the folder where the license is stored (default location is `C:\Program Files\Wavelink\AvalancheMC`). Copy the license file and paste it to a different location on your hard drive.

To uninstall Avalanche MC:

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

-Or-

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

The *Uninstall Wizard* appears.

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

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

Chapter 3: Licensing

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

- Overview of Wavelink Licensing
- Running the License Server
- Activating Avalanche MC
- Releasing Licenses

Why Should I License My Devices?

Avalanche MC requires licenses for full functionality. You can access and use the Avalanche MC 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.

Overview of Wavelink Licensing

Avalanche MC licensing is based on a per mobile device or infrastructure device basis. This means that Avalanche MC can manage one mobile device or infrastructure device for each license.

This overview provides information about the following topics:

- Product Licenses
- Base and Maintenance Licenses
- Unlicensed Devices

Product Licenses

Avalanche MC uses four types of product licenses:

- Mobile device and infrastructure device licenses allow the Avalanche MC Console to manage mobile devices and infrastructure devices.

- Remote Control licenses enable the Avalanche MC Remote Control functionality.
- CE Secure licenses enable CE Secure functionality in Avalanche MC.

Mobile Device and Infrastructure Device Licenses

Avalanche MC requires one license for each mobile device or infrastructure device it manages. When a dServer detects a new wireless device, a license request is sent to the License Server. The License Server then sends a license to the dServer to be distributed. The license file is unique to the dServer and cannot be transferred to another dServer. Once the device receives the license, Avalanche MC can manage it. Mobile devices require an Avalanche license and infrastructure devices require a Mobile Manager license.

NOTE For License Server information, see *Running the License Server* on page 45

Remote Control Licenses

Avalanche MC requires one Remote Control license for each mobile device to which you want to connect remotely. For more information about Remote Control licenses, refer to the *Wavelink Avalanche Remote Control User's Guide*.

CE Secure Licenses

Avalanche MC requires one CE Secure license for each mobile device you want to manage. For more information about CE Secure licenses, refer to the *Wavelink Avalanche CE Secure User's Guide.*

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

Base and Maintenance Licenses

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*

License Acquisition

When a Mobile Device dServer detects a new mobile device, it analyzes all of the applicable factors and then requests the appropriate type of license from the License Server. If the license is available, the License Server sends down the appropriate license to the requesting Mobile Device dServer.

If a license expires or is released, the license returns to the pool of licenses in the License Server until it is sent to a Mobile Device dServer upon request.

Unlicensed Devices

When you run Avalanche MC 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 using the Avalanche MC Console. You cannot deploy software packages or network profiles to the mobile device.

- **For Infrastructure Devices**: The infrastructure devices appear in the Avalanche MC Console and in the Mobile Manager 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 application that runs on a host system as part of Avalanche MC. The License Server is responsible for supplying licenses to Avalanche MC mobile devices and infrastructure devices.

When a Mobile Device dServer or an Infrastructure dServer detects a new device, it sends a request to the License Server for that particular type of license. If the license is available, the License Server sends down the appropriate license to the requesting Server.

If a license expires or is released, the license returns to the pool of licenses in the License Server until it is sent to a Server upon request.

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

The License Server operates on TCP port 7221. For the License Server to function properly, this port must be open and not blocked by a firewall.

Activating Avalanche MC

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

- Nodelocking
- Activating Avalanche MC Licenses
- Activating Remote Control and CE Secure Licenses

Nodelocking

After you install Avalanche MC, you are asked to license it with a valid license code. This code uses a technique called nodelocking, in which Avalanche MC is licensed only for a specific computer, or node, on your network. A node is defined as several specific system attributes that, in combination, uniquely distinguish it from any other system in your organization.

Once a license for Avalanche MC is activated and associated with a specific node (nodelocked) you cannot move that license to another node. If you want to move the license, you need to contact Wavelink Customer Service.

Activating Avalanche MC Licenses

When you activate Avalanche MC licenses, a license file called `wavelink.lic` is installed on your system, which provides the information the product needs to operate.

There are four methods of activating Avalanche MC licenses:

- Activating Automatically
- Activating Manually
- Importing a License
- Activating Demo Mode

After you install Avalanche MC, the *Wavelink Activation* dialog box appears automatically. If you want to activate Avalanche MC immediately, you can perform one of the activation methods from this location. For each type of product license, you will need to enter a license code. If you do not want to activate Avalanche MC immediately, you can return to the *Wavelink Activation* dialog box at a later time by selecting **Start > Programs > Wavelink Avalanche MC > Activate**.

Activating Automatically

If Avalanche MC resides on a system that has Internet access, you can use the automatic license activation.

When you use the automatic activation method, Avalanche MC connects with a secure Wavelink Web dServer location to verify your license. A nodelock and a license file are sent to your host system. The license file called `wavelink.lic` is installed on your system, which provides the information the product needs to operate.

To activate Avalanche MC:

1 Obtain the Avalanche MC product licensing code from Wavelink**.**

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

2 Access the *Wavelink Activation* dialog box by clicking **Start > All Programs > Wavelink Avalanche MC > Activate**.

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

4 Click **Activate**.

Avalanche MC connects with a secure Wavelink Web site, your license and nodelock are verified, and a license file is sent to your host system. A new dialog box appears, displaying your licensing information and asking if you want to save the information for this installation.

5 Click **Yes** to accept the license file and activate your installation.

The Wavelink licensing process ties Avalanche MC to a specific computer on your network. If a situation requires you to re-install Avalanche MC on a different system, please contact Wavelink Customer Service to unlock your license from that system. Once the license is unlocked, you can re-install the product on a new system.

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. You can get this information from the Wavelink Activation dialog box.
- Product license code. This information comes from the e-mail you receive from Wavelink upon purchasing Avalanche MC.

To manually activate a license:

1 Obtain the information needed for the product license.

2 Open a Web browser and navigate to `http://www.wavelink.com/activation`.

3 Enter the **Hardware Node Lock** and the **License** code in the text boxes.

4 Click **Activate** button to activate license.

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

5 Click on the link and change **Save As** type to **All Files**.

6 Download the file to desired location.

7 Move `wavelink.lic` file to system with AMC installed.

8 Follow the steps to import a license into your AMC installation.

Importing a License

If you already have a license file for Avalanche MC or if you have received a `wavelink.lic` file using the manual activation method, you can activate the file by importing it. You have the option of importing multiple license files or consolidating several files.

To import a license:

1 Access the *Wavelink Activation* dialog box by clicking **Start > All Programs > Wavelink Avalanche MC > Activate**.

2 Click **Browse** and navigate to the location of the `wavelink.lic` file.

3 Select the `wavelink.lic` file and click **Yes**.

4 In the *Wavelink Activation* dialog box, click **Close**.

Activating Demo Mode

If you are installing Avalanche MC for demonstration purposes, you can run Avalanche MC in demo mode. Demo mode authorizes Avalanche MC to manage up to two infrastructure devices and two mobile devices for 30 days.

To activate demo mode:

1 Access the *Wavelink Activation* dialog box by clicking **Start > All Programs > Wavelink Avalanche MC > Activate**.

The *Wavelink Activation* dialog box appears.

2 Click **Demo**.

Avalanche MC will run in demo mode.

Activating Remote Control and CE Secure Licenses

You can use any of the four activation methods to activate both Remote Control and CE Secure licenses. However, you need to obtain the correct product license for the specific program you want to activate. To obtain both Remote Control and CE Secure product licenses, contact Wavelink Customer Service.

Refer to *Activating Automatically* on page 47, *Activating Manually* on page 48 and *Importing a License* on page 49 for steps to activate licenses.

Releasing Licenses

Licenses for mobile devices are frequently redistributed, providing flexibility in managing licenses. To encourage redistribution, you can configure the Mobile Device dServer 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 Mobile Device dServer to release licenses, refer to *Releasing Licenses* on page 189. For information about deleting devices from the Mobile Device Inventory, refer to *Deleting Mobile Devices* on page 272.

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 MC 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 console will retrieve the enterprise image.

Chapter 4: Avalanche MC Console

You interact with your wireless network primarily using the Avalanche MC Console.

What is the Avalanche MC Console?

The Avalanche MC Console is the GUI application that allows you to control global characteristics of your wireless network. These characteristics include creating infrastructure profiles, assigning IP addresses, and monitoring network performance. The console works with all the components of Avalanche MC and allows you to organize and define each component.

Overview of the Console

The Avalanche MC Console works with components of Avalanche MC called dServers. The dServers are responsible for sending instructions to and receiving data from wireless devices. Avalanche MC includes two types of dServers: Infrastructure dServers and Mobile Device dServers. From the Avalanche MC Console, you can deploy one or both of these dServers anywhere within your network.

To streamline wireless network management, the Avalanche MC Console allows you to categorize dServers into dServer Locations and regions. A dServer Location is defined as a location within your network that hosts at least one dServer. A region is defined as a collection of dServer Locations that share similar traits. Creating logical and organized dServer Locations and regions can greatly improve flexibility and allow you to manage your network with ease. Refer to *Chapter 6: Managing Regions and dServer Locations* on page 103 for more information about creating and organizing regions and dServer Locations.

This section contains the following topics:

- Starting the Avalanche MC Console
- Understanding Avalanche MC Console
- Changing Console Preferences
- Managing the Enterprise Server

- Avalanche MC Reporting Tool
- Using the Support Generator
- Using the Enabler Installation Tool

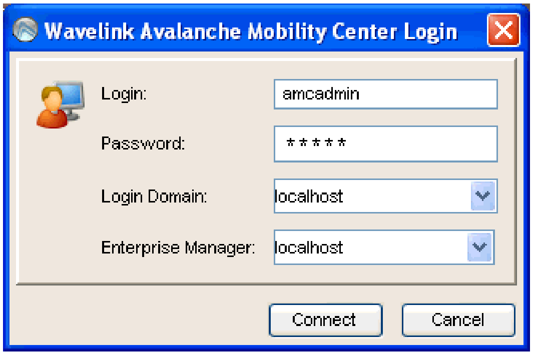
Starting the Avalanche MC Console

Using the Avalanche MC Console, you can configure and manage your wireless network on an enterprise-wide basis. You can start the Avalanche MC Console from the **Programs** menu or from a shortcut.

To start the Avalanche MC Console:

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

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



Wavelink Avalanche Mobility Center Login

Login: amcadmin

Password: *****

Login Domain: localhost

Enterprise Manager: localhost

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

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

Avalanche MC 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 85.

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

4 From the **Enterprise Manager** drop-down list, select your host (the enterprise server).

5 Click **Connect**.

The *EServer Login* dialog box appears. This dialog box indicates the progress of the Console as it attempts to contact the Enterprise Server. The Console will wait indefinitely for the Enterprise Server to respond. If your Console cannot contact the Enterprise Server, you may cancel the login.

If the login fails due to credential authorization issues, a dialog will appear indicating such.

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

Understanding Avalanche MC Console

The Avalanche MC Console consists of various tools to manage your wireless network. These tools are located in the Navigation Window, which also provides a tree view of the regions and dServer Locations within your wireless network. In addition, the Console contains tabs and tool bar options that provide you information regarding wireless network configuration and activity.

The Avalanche MC Console consists of the following areas:

- Tool Bar
- Quick Start Tab
- Health by Location Tab
- Navigation Window/Profile Selection
- Alert Legend

Tool Bar

The following table provides information about each Tool Bar button.

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

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

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 deploy any profile and configuration changes to dServers 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 Deployment Package wizard and build new deployment packages.

Click this icon to open the *Contact Manager* dialog box. This allows you to edit the e-mail addresses associated with alert profiles.

Click this icon to open the *Proxy Pool Manager* dialog box. This allows you to edit your proxies associated with alert profiles.

Click this icon to open the *Very Large Access Control List* dialog box. This allows you to edit the entries in the Very Large Access Control List.

Click this icon to open the *Scan to Config* dialog box. This allows you to create new barcode profiles, edit network settings associated with barcodes and to print barcodes.

Click this icon to launch the Avalanche MC Report Console.

Quick Start Tab

When you first launch the console, the **Quick Start** tab displays. This tab provides quick links to getting your first 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. For detailed information and steps about each tasks, refer to the online help.

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

- Set Up Enterprise
- Set Up Profiles
- Set Up Devices
- 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.

Set Up Enterprise

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

- Creating Regions. For details about this tasks, refer to *Managing Regions* on page 105.
- Creating dServer Locations. For details about this task, refer to *Managing dServer Locations* on page 114.

- Creating Distributed Server Packages. For details about this task, refer to *Building Server Deployment Packages* on page 131.
- Deploying Distributed Server Package. For details about this task, refer to *Deploying dServers* on page 331.

Set Up Profiles

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

- Creating Network Profiles. For details about this task, refer to *Chapter 7: Managing Network Profiles* on page 143.
- Creating Software Profiles. For details about this task, refer to *Chapter 10: Managing Software Profiles* on page 209.
- Creating Infrastructure Profiles. For details about this task, refer to *Chapter 11: Managing Infrastructure Profiles* on page 225.
- Applying Profiles to Regions and dServer Locations. For details about this task, refer to *Assigning Profiles to Regions* on page 107 and *Assigning Profiles to dServer Locations* on page 125.

Set Up Devices

This task allows you to install and Avalanche Enabler onto a mobile device. For details about the Avalanche Enabler, refer to the *Avalanche Enabler User Guide*.

Help and Support

This region provides links to the Avalanche MC Help, Wavelink Support, and launches the Support Generator. For details about using the Support Generator, refer to *Using the Support Generator* on page 77.

Health by Location Tab

The **Health by Location** tab provides a real-time view of the health of your wireless network. You can tell at a glance which dServer Locations are operating normally and which require attention.

The **Health by Location** tab consists of two areas: the Map and the Alert Browser. The Map pane provides a geographical overview of the health of your network.

Avalanche MC Map

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.
- Descries the map details using the small magnifying glass icon.
- Zoom in on 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 checkboxes located next to the navigation arrows. You can apply the following filters:

Combined dServers	Displays dServer Locations that contain both a Mobile Device dServer and an Infrastructure dServer.
Mobile Device dServers	Displays dServer Locations that contain only a Mobile Device dServer.
Infrastructure dServers	Displays dServer Locations that contain only an Infrastructure dServer.
View Map By Selected Region	Displays only those dServer Locations that belong to the region selected in the Navigation Window.

- 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 dServer Location with combined Servers (Mobile Device dServer and Infrastructure dServer).
Blue	Indicates a dServer Location with only a Mobile Device dServer.
Dark Green	Indicates a dServer Location with only an Infrastructure dServer.
Yellow	Indicates a dServer Location with one or more warning-level alerts (but no critical alerts).
Red	Indicates a dServer Location with one or more critical alerts.

When a dServer Location generates a warning or critical alert, the icon in the Map pane 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 dServer Location have been cleared from the Alert Browser.

- Save specific views of the Map. This feature allows you to immediately display a relevant section of your wireless network.

To save a view within the Map pane:

1. Position the Map pane 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 Avalanche MC.

To access a saved view:

- From the **Go to View** list, select which view you want to display.

- Move dServer Locations. Changing a dServer Location's location does not disrupt communications with that dServer Location.

To relocate a dServer Location:

1 Right-click the dServer Location you wish to relocate.

A drop-down menu appears.

2 Click **Relocate**.

3 Click and drag the dServer Location to the new location on the map.

The *Confirm dServer Location Relocation* dialog box appears.

4 Click **Yes**.

Alert Browser

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

Ack	Indicates whether you have acknowledged the alert.
Alert	Indicates the type of alert.
Date	Provides the time and date of the alert.
Description	Provides a detailed description of the alert.

Navigation Window/Profile Selection

The Navigation Window, located on the left side of the Avalanche MC Console, displays Profile Sets, dServer Locations and Regions in a tree view.

Profile Sets refers to the specific profile pages containing all the profiles and settings for that particular set. From the Navigation Window, you can access the following Profile Sets:

- **Infrastructure Profiles**. An Infrastructure Profile is a collection of infrastructure device settings that you can simultaneously apply to multiple infrastructure devices.

- **Infrastructure dServer Profiles**. Infrastructure dServer Profiles manage access privileges for your Infrastructure dServers.

- **Mobile Device dServer Profiles**. Mobile Device dServer profiles manage software and network settings for mobile devices.

- **Alert Profiles**. Alert profiles manage network alerts by allowing you to configure what type of network events are captured and where alerts are sent when those events occur.

- **Network Profiles**. Network profiles manage network settings for both infrastructure devices and mobile devices on an enterprise-wide level.

- **Software Profiles**. Software profiles contain the tools to build software packages and install the packages on the Mobile Device and Infrastructure dServers.

- **Update Profiles**. Update profiles manage specific times when mobile devices are not authorized to contact the Mobile Device dServer.

- **Mobile Device Groups**. Mobile device groups are collections of mobile devices that allow you to manage multiple devices simultaneously, using the same tools available for managing individual mobile devices.

- **dServer Locations and Regions**. Avalanche MC streamlines network management by allowing you to create dServer Locations and regions. A dServer Location contains at least one Server (Mobile Device dServer or Infrastructure dServer) that communicates with wireless devices (mobile or infrastructure devices). A Region is a collection of dServer Locations that share similar characteristics.

Profile Selection Functionality

When you select a Profile Set from the Navigation Window, the first profile in the Profile List for that set will be automatically selected. If you are returning to the Profile Set, the last profile that was viewed will automatically be selected in the Profile List.

For example, if you select Alert Profiles from the Navigation Window and there are 10 profiles listed in the **Alert Profile List**, the first profile in that list will be selected. If you are returning to the Alert Profiles, the last profile that you modified or view will be automatically selected.

Navigating the Regions and dServer Locations List

You can move through the dServer Location and regions by either expanding each node or using the Search functionality.

To navigate to a desired region:

1. Expand **My Enterprise**.

2. Scroll and click through the tree.

To use the Search function:

1. Type in the name of the region or dServer Location in the text box just above the tree view.

2. Click **Search**.

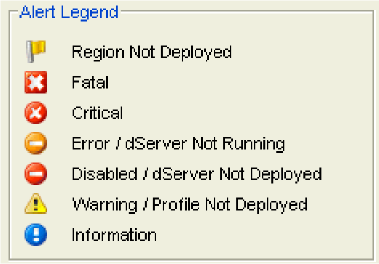
   The highlight will move to the first region or dServer Location whose name begins with the text you entered. The search is not case sensitive.

   If there are multiple matches, click **Search** until you reach the correct region or dServer Location.

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

Alert Legend

The Alert Legend provides descriptions of the icon alerts that may appear next to your regions, profiles and software packages.



Alert Legend

- ⚑ Region Not Deployed
- ☒ Fatal
- ⊗ Critical
- ⊖ Error / dServer Not Running
- ⛔ Disabled / dServer Not Deployed
- ⚠ Warning / Profile Not Deployed
- ❗ Information

Figure 4-2. *Alert Legend*

The following table provides a description of each alert based on where that alert appears in the console.

NOTE **Applied Profiles** or **Applied Software Profiles** refers to profiles that have been assigned to a region.

Region Not Deployed	Indicates that the region has changes that have not been deployed. Changes can be within applied profiles, applied profiles priority or any editing of any applied profile. These alerts are valid for profiles that have not been applied to a region. This alert will not appear for any changes to profiles that are not applied to a region.
Fatal	**For All** Indicates a fatal level alert. **Applied Profiles** Indicates that the profile requires certain settings that are not set. These settings must be configured for the profile to work. **Applied Software Profile** Indicates that the profile contains a software package that is invalid.
Critical	**For All** Indicates a critical level alert. **Applied Software Profile** Indicates that the profile contains a software package that has a broken seal.

Table 4-1: *Alerts*

Error/ dServer Not Running	**For All** Indicates an error level alert. **Region** Indicates that there is a dServer Location in the region hierarchy that has a Mobile Device dServer or Infrastructure dServer that currently is not running. **dServer Locations** Indicates that a Mobile Device dServer or Infrastructure dServer is currently not running. **Applied Software Profile** Indicates the profile has a software package that is currently disabled. **Mobile Device or Infrastructure dServers** Indicates that a Mobile Device dServer or Infrastructure dServer is currently not running.
Disabled/ dServer Not Deployed	**dServer Locations** Indicates that the dServer Location has no dServers deployed to it. **Regions** Indicates that there is a dServer Location in the region hierarchy that is missing a dServer. **Mobile Device or Infrastructure dServers** Indicates that the dServer has not been deployed. **Mobile Device Groups** Indicates that the mobile device group is disabled.
Warning	**For All** Indicates a warning level alert. **Applied Profiles** Indicates that the profile has changes that have not been deployed.
Information	**Applied Profiles** Indicates the type of profile typically has certain settings configured, but this profile does not have those settings configured. **Applied Software Profile** Indicates the profile has special software packages such as pre-licensed or sealed.

Table 4-1: *Alerts*

Changing Console Preferences

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

- Customizing Console Display
- Configuring Auto-Deployment Settings
- Enabling Audit Logging
- Viewing Console Activity
- Configuring HTTP Proxy Connections
- Customizing Map Options

Customizing Console Display

You can configure the appearance of the Avalanche MC Console, 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 console display:

1. From the **Tools** menu, select **Preferences**.

   The *Preferences* dialog box appears.

2. In the **Console Display Settings** region, configure the width, height, position and the frame positions for the Avalanche MC Console.

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

   You can choose the **Properties** tab, **Mobile Device Inventory** tab, **Infrastructure** tab or **Last Selected**. If you select **Last Selected,** when you navigate to a Region or dServer Location, the Console will select the previously selected page view (Mobile Device Inventory, Infrastructure Inventory or Region Properties), or the Region Properties if this is a new session and no previous context has been established. Basically it kind of assigns a default page view for the Region or dServer Location.

4 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 database on the Enterprise Server.

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

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

The Avalanche MC Console updates to reflect your changes.

Configuring Auto-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 perform automatic deployments, each time you make a change in the console, that change is deployed to the assigned regions/dServer Locations. This option is enabled by default for dServer Location installations. It is disabled for Enterprise installations. It is recommended that before enabling this option, you have most of your settings configured and deployed. If the option is enabled as you first configure and set up Avalanche MC, the Enterprise Server will become overloaded with the all the changes causing delays and potentially other errors.

You can also configure an option to automatically assign any profiles or profile changes to the **My Enterprise** region of the Navigation Window. When profiles are assigned in this manner, those profiles appear at the bottom of the assigned profiles list at the **My Enterprise** region. This option is enabled by default for both dServer Location and Enterprise installations.

The **Universal Deployment Refresh Delay** refers to the number of seconds the Avalanche MC 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 you configure the number of seconds too low, the console display will not have enough time to contact the Enterprise Server and refresh completely and you will not return to the same console location you were viewing before the deployment. The default page view will display. If the console display has enough time refresh completely, you will return to the same console location (region, profile and tab) you were viewing before the deployment.

To enable auto-options:

1 From the **Tools** menu, select **Preferences**.

   The *Preferences* dialog box appears.

2 Select **Enterprise Server** from the list box.

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 profile.

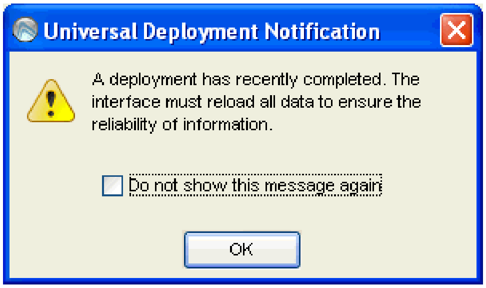
5 Enter the number of seconds the console will wait to refresh after settings are deployed in the **Universal Deployment Refresh Delay** text box.

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 MC performs a Universal Deployment, sending those changes to the appropriate regions and dServer Locations. During this deployment the *Universal Deployment Notification* dialog box appears. This dialog box informs you that because of the recent deployment, the Avalanche MC interface must reload and refresh to ensure the console displays accurate information.


Universal Deployment Notification

A deployment has recently completed. The interface must reload all data to ensure the reliability of information.

□ Do not show this message again

Figure 4-3. *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.

Enabling Audit Logging

The following events can be configured for logging:

- **Logon/Logoff**. If you select this option, the console will track users that log on to Avalanche MC and the times the user logs on and off.
- **Profile Applied**. If you select this option, the console will track every profile that is applied to a region or dServer Location.
- **Profile Modification**. If you select this option, the console tracks profiles that are modified and the modification that is made.

To enable audit logging:

1 From the **Tools** menu, select **Preferences**.

The *Preferences* dialog box appears.

2 Select **Enterprise Server** from the list box.

3 In the **Audit Log** region, activate the **Enable Audit Logging** check box.

4 Enable the events you want to record.

5 Click **Apply**.

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

Specifying the Backup Drive Location

You can specify where you want to store any backups of Avalanche MC. The location must be a qualified path for the eServer. 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 341.

To specify a location:

1. From the **Tools** menu, select **Preferences**.

   The *Preferences* dialog box appears.

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

Viewing Console Activity

If you enable audit logging for the console, you can view the activity from the Console Activity 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 user activity, and description of the changes that occurred.

To view the console activity:

- From the **Tools** menu, select **Console Activity Log**.

Configuring HTTP Proxy Connections

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 MC installation process.

To configure HTTP proxy settings:

1 From the **Tools** menu, select **Preferences**.

The *Preferences* dialog box appears.

2 Select **HTTP Proxy** from the list box.

3 Enable the **Use HTTP Proxy Server** checkbox.

4 In the **Host** text box, type either the IP address or host name of the proxy.

5 Optionally, enter a port number in the **Port** text box.

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

6 If you are using Basic Authentication for the HTTP proxy, type the **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 also modify the appearance of the map in the **Health by Location** tab.

To modify colors:

1 From the **Tools** menu, select **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 dServers and the eServer in the follow methods:

- Configuring Enterprise Server Blackout Periods
- Releasing Blackout Periods
- Performing Batch Releases
- Viewing the eServer Status
- Controlling the eServer Message Backlogs
- Purging dServer Statistics

Configuring Enterprise Server Blackout Periods

Blackout periods are defined as times when communication between the eServer and dServers is shut down. The dServers can not contact the eServer until the blackout period is released. Use the following options in the eServer Console dialog box to configure blackout periods between the eServer and the dServer.

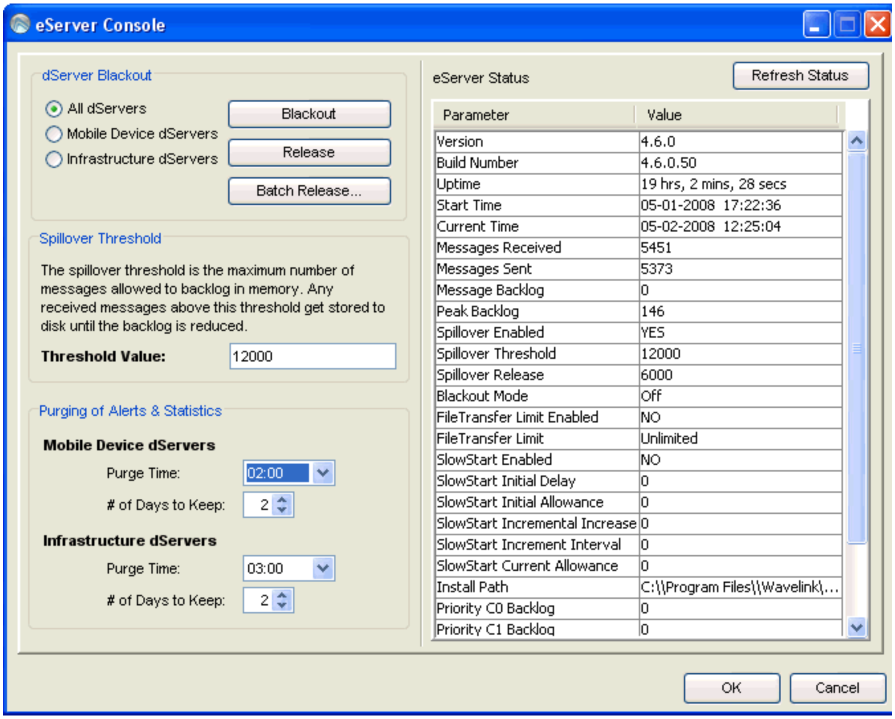
- **dServer Blackout**. You can select to shut down communication from **All dServers**, **Mobile Device dServer** or **Infrastructure dServers**.
- **Blackout**. Click this button to shut down all communication from the selected dServers to the eServer. Communication will not be restored until you click the **Release** button.
- **Release**. Click this button to release the eServers from the blackout state. This restores communication between the dServers and eServer.
- **Batch Release**. This option restores communication from the dServers to the eServer using a controlled method. From the dialog box that appears, you can select the number of dServers to release at a time and the interval (in seconds) at which to release the batches of dServers. This ensures only

a select number of dServers are released and able to communicate with the eServer at a time and also prevents a flood of communication to the eServer.

To configure eServer blackout periods:

1 From the **Tools** menu, select **Manage eServer**.

The *eServer Console* dialog box appears.



● All dServers
○ Mobile Device dServers
○ Infrastructure dServers

The spillover threshold is the maximum number of messages allowed to backlog in memory. Any received messages above this threshold get stored to disk until the backlog is reduced.

Threshold Value: 12000

Mobile Device dServers

Purge Time: 02:00

# of Days to Keep: 2

Infrastructure dServers

Purge Time: 03:00

# of Days to Keep: 2

Parameter	Value
Version	4.6.0
Build Number	4.6.0.50
Uptime	19 hrs, 2 mins, 28 secs
Start Time	05-01-2008 17:22:36
Current Time	05-02-2008 12:25:04
Messages Received	5451
Messages Sent	5373
Message Backlog	0
Peak Backlog	146
Spillover Enabled	YES
Spillover Threshold	12000
Spillover Release	6000
Blackout Mode	Off
FileTransfer Limit Enabled	NO
FileTransfer Limit	Unlimited
SlowStart Enabled	NO
SlowStart Initial Delay	0
SlowStart Initial Allowance	0
SlowStart Incremental Increase	0
SlowStart Increment Interval	0
SlowStart Current Allowance	0
Install Path	C:\\Program Files\\Wavelink\...
Priority C0 Backlog	0
Priority C1 Backlog	0

Figure 4-4. *eServer Console*

2 From the list of dServer options, select **All dServers**, **Mobile Device dServers** or **Infrastructure dSErvers**, 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 dServers you selected and the eServer until you release the blackout period.

Releasing Blackout Periods

Use the **Release** button in the *eServer Console* dialog box to restore communication between the dServers and the eServer.

To release blackout periods:

1 From the **Tools** menu, select **Manage eServer**.

The *eServer Console* dialog box appears.

2 Click **Release**.

3 Check that the **Blackout** parameter in the eServer Status region displays **OFF**.

Communication is restored between the dServers and eServer.

Performing Batch Releases

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

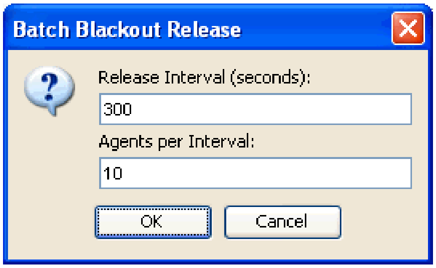
To perform a batch release:

1 From the **Tools** menu, select **Manage eServer**.

The *eServer Console* dialog box appears.

2 Click **Batch Release**.

The *Batch Blackout Release* dialog box appears.


Batch Blackout Release

Release Interval (seconds):

300

Agents per Interval:

10

Figure 4-5. *Batch Blackout Release*

3 In the **Release Interval**, specify the number of seconds you want to elapse between batch releases.

4 In the **dServers per Interva**l text box, specify the number of dServers you want released at each interval.

5 Click **OK**.

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

Viewing the eServer 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 the parameters and values displayed in the **eServer Status** region:

- **Version**. Indicates the version of the eServer.
- **Build Number**. Indicates the build number of the eServer.
- **Installation Path**. Displays the installation location of the eServer.
- **Start Time**. Displays the last time the eServer was started.
- **Current Time**. Displays the current time.
- **Uptime**. Indicates how long the eServer has been running since the last start time.

- **Messages Received**. Displays the total number of messages the eServer has received.
- **Messages Sent**. Indicates the total number of messages the eServer has sent.
- **Spillover Enabled**. Indicates whether the memory spillover function is enabled (YES or NO).
- **Spillover Threshold**. Indicates the memory level before spillover takes effect.
- **Spillover Release**. Indicates the number of seconds before the spillover is released.
- **Blackout Mode**. Indicates if blackout mode is enabled and which dServers are included in the black out.
  - **Off** indicates that blackout mode is not currently in use.
  - **All dServers** indicates that all dServers are in blackout mode and cannot communicate with the eServer.
  - **Mobile Device dServers** indicates the only the Mobile Device dServers are in blackout mode.
  - **Infrastructure dServers** indicates that only the Infrastructure dSErvers are in blackout mode.
- **Priority C0 - C2 Backlog** indicate the number of messages coming from consoles with C0 being the highest priority and C2 being the lowest priority.
- **Priority A0 - A2 Backlog** indicate the number of messages coming from the dServers with priority A0 being the highest priority and A2 being the lowest priority.

Controlling the eServer Message Backlogs

You can control the eServer message backlogs and preserve memory by setting the spillover threshold for eServer messages. The spillover threshold is the maximum number of eServer messages allowed to the backlog. Any received messages beyond this threshold are stored in a file to disk until the backlog is reduced. Once the backlog is reduced, messages are pulled from the stored file back into the log.

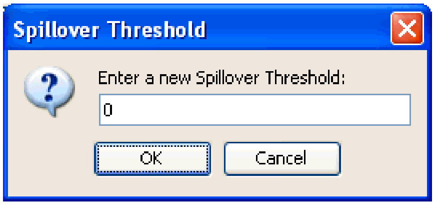
To configure the spillover threshold:

1 From the **Tools** menu, select **Manage eServer**.

The *eServer Console* dialog box appears.

2 Click **Set Spillover Threshold.**

The *Spillover Threshold* dialog box appears.



Spillover Threshold

Enter a new Spillover Threshold:

0

Figure 4-6. *Spillover Threshold*

3 Enter the threshold number and click **OK**.

Purging dServer Statistics

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

- **Purge Time**: Set the time of day you when you want to remove the statistics. This allows you to control the activity occurring on the Enterprise Server.
- **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 From the **Tools** menu, select **Manage eServer**.

The *eServer Console* dialog box appears.

2 In the **Purging Statistics** section, configure the days you want to keep the statistics and the time you want the statistics to be removed.

3 Click **OK** to save your settings.

Avalanche MC Reporting Tool

Avalanche MC features the Wavelink Avalanche MC Report Console, a reporting tool that allows you to build reports based on regions or device groups. Before you can connect to the Report Console, you must install the reporting utility. Contact Wavelink Customer Service to obtain the Wavelink Avalanche MC Report Console installation package. For more information about using the reporting tool, refer to the *Wavelink Avalanche MC Report Console User's Guide*.

To connect to the Avalanche MC Report Console:

1 Install the Report Console utility.

2 Click the reporting tool icon in the toolbar.

Your web browser will connect to the Report Console.

Changing Report Settings

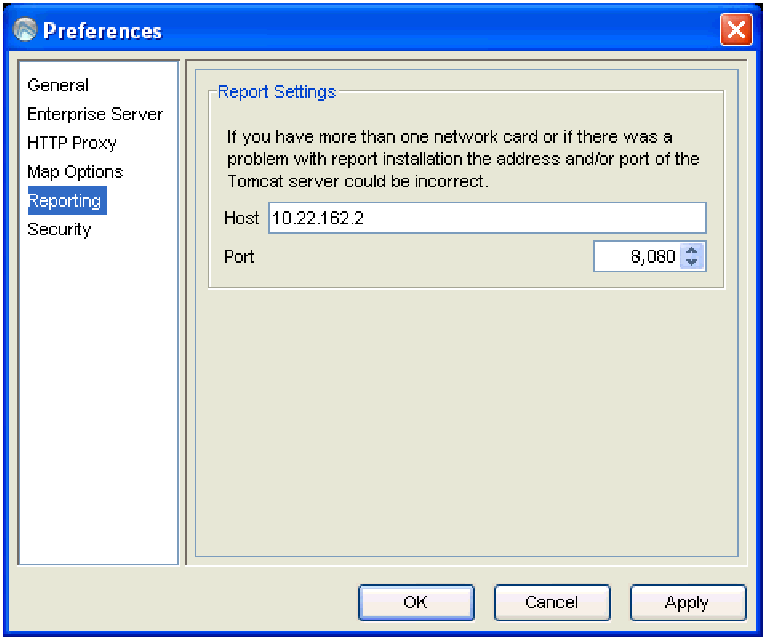
The Reporting Tool installation package contains the components to run the Reporting Tool and Apache Tomcat installation. Apache Tomcat provides an environment for the Java code to run in cooperation with a Web server. However, if you are already running a Tomcat server, you can redirect Avalanche MC to the host and port from which you are running it. You may need to do this if you have more than one network card of if there were problems installing the Reporting Tool.

To change report settings:

1 From the **Tools** menu, select **Preferences**.

The *Preferences* dialog box appears.

2 Select **Reporting** from the list box.



Report Settings

If you have more than one network card or if there was a problem with report installation the address and/or port of the Tomcat server could be incorrect.

Host 10.22.162.2

Port 8,080

Figure 4-7. *Reporting*

3 Enter the **Host** address of the Tomcat Server.

4 Enter the **Port number**.

5 Click **Apply**.

6 Click **OK** to close the dialog box.

Using the Support Generator

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

- EConsole.log
- EServer.log
- Inforail.log

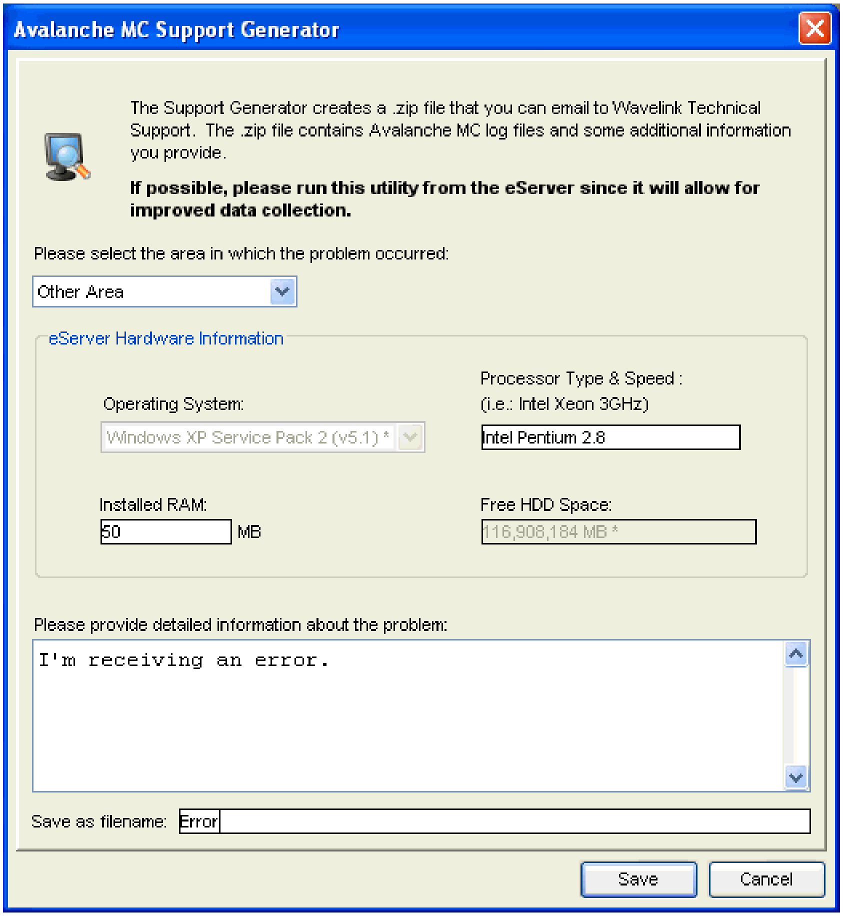
- LicenseServer.log

The Support Generator `.zip` files are saved to the installation location of Avalanche MC. The default location is `C:\Program Files\Wavelink\AvalancheMC\SUPPORT`. Once you create a `.zip` file, you can send the file to Wavelink Customer Service. Customer Service uses the `.zip` 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 MC Support Generator* dialog box appears.



Avalanche MC Support Generator

The Support Generator creates a .zip file that you can email to Wavelink Technical Support. The .zip file contains Avalanche MC log files and some additional information you provide.

If possible, please run this utility from the eServer since it will allow for improved data collection.

Please select the area in which the problem occurred: Other Area

eServer Hardware Information

Operating System: Windows XP Service Pack 2 (v5.1) *

Processor Type & Speed : (i.e.: Intel Xeon 3GHz) Intel Pentium 2.8

Installed RAM: 50 MB

Free HDD Space: 116,908,184 MB *

Please provide detailed information about the problem:

```
I'm receiving an error.
```

Save as filename: Error

Figure 4-8. *Avalanche MC Support Generator*

2 From the drop-down list, select the area of Avalanche MC 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 can not change the **Operating System** or **Free HDD Space** text boxes. These are populated by the support generator.

---

5 In the text box, provide detailed information about the problem. The more detailed and descriptive you are, the more thoroughly Customer Service will be able to understand the problem.

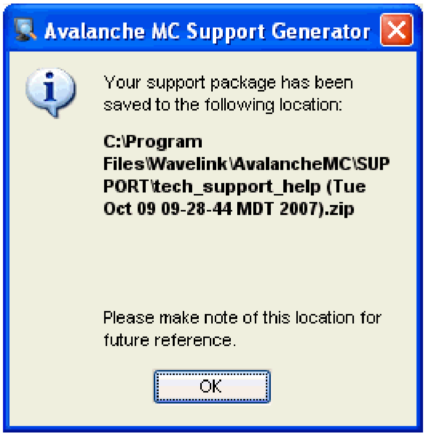
6 In the **Save as filename** text box, enter a name for this file.

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 complied into a `.zip` file and a dialog box appears displaying the location where the file is saved.



Avalanche MC Support Generator

Your support package has been saved to the following location:

C:\Program Files\Wavelink\AvalancheMC\SUPPORT\tech_support_help (Tue Oct 09 09-28-44 MDT 2007).zip

Please make note of this location for future reference.

Figure 4-9. *Avalanche MC 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 MC Console using Microsoft ActiveSync

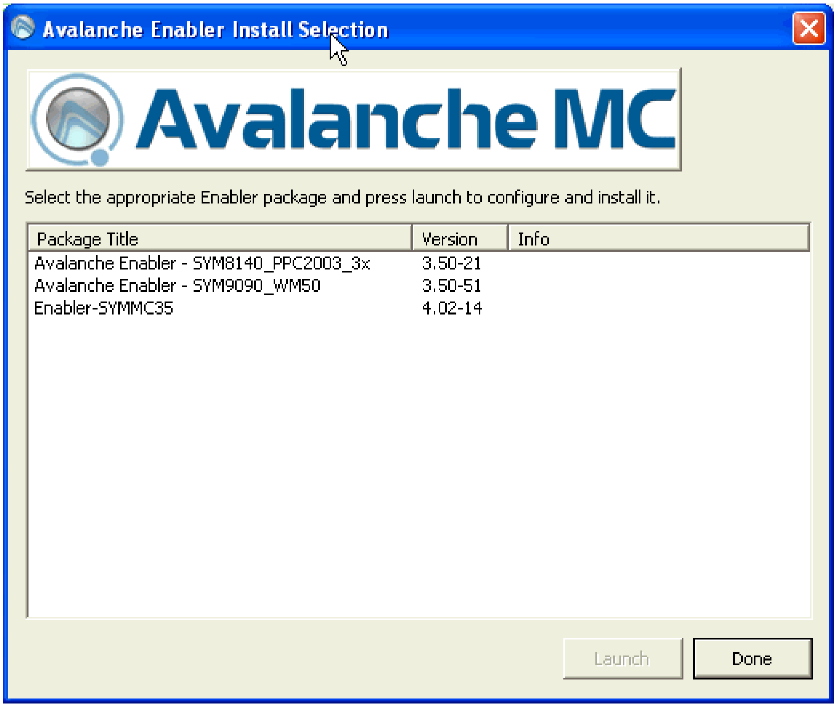
To use the Enabler Installation Tool, you must have the following:

- 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 Enabler option.

The Avalanche Enabler Install Selection dialog box appears.



Select the appropriate Enabler package and press launch to configure and install it.

Package Title	Version	Info
Avalanche Enabler - SYM8140_PPC2003_3x	3.50-21	
Avalanche Enabler - SYM9090_WM50	3.50-51	
Enabler-SYMMC35	4.02-14	

Figure 4-10. *Avalanche Enabler Install Selection*

2 From the dialog box, select which Enabler package you want to install on the mobile device.

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.

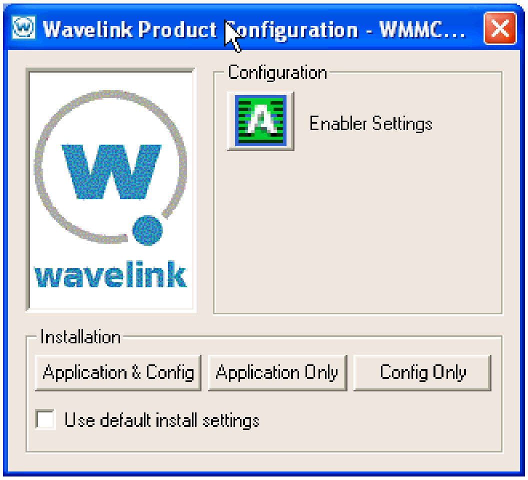


Figure 4-11. *Wavelink Product Configuration Utility*

3 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*.

Understanding Edit Mode

Edit mode is new to Avalanche MC. Before you can edit a profile, you must enter edit mode. To use edit mode, you employ the following icons located in the toolbar:

Click **Edit** to enable edit mode when working with any profiles. This button because available when you create a new profile or select a profile in from the list. It also becomes available when working with properties and assigning profiles to a region or location.

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 directives regarding the use of Edit Mode:

- Edit mode is required to edit any profile, dServer Location Properties, Site Properties and Region Properties.
- You must select a profile, create a profile or highlight a location under My Enterprise to enable the Edit button.
- When you enter Edit Mode, the Navigation Window will not be available until you exit Edit Mode.
- If you add a new profile, you will need to click Edit Mode before you can continue configuration.
- If you make a change in a profile that you are editing, you must **Save** or **Cancel** before you can leave the profile.
- If you exit a profile before you make any changes, Edit Mode automatically disables.
- You cannot remove a profile while you are in Edit Mode. You must either save or click **Cancel**. You can then select the profile and click Remove.
- You can not edit Unassigned dServer Locations or Deleted dServer Locations.

4 You do not need to enter Edit Mode to view where profiles are applied (**Applied To** 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 actual package not to the console. However, you must enter Edit Mode to configure any other software package options.

The following is a brief overview of the steps you must perform to edit any profile or property.

1. Create a profile
2. Select the profile
3. Click **Edit**.
4. Edit the tabs for the profile.
5. Click **Save** when you are finished.
6. To exit the edit mode without saving changes, click **Cancel**.

Chapter 5: Managing User Accounts

Avalanche MC allows you to create several different user accounts to designate users and assign specific privileges to those users. There are two types of accounts, Administrator and Normal. Upon installation of Avalanche MC, 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.

User accounts can be created for enterprise-wide components of Avalanche MC and are distributed to all the dServer locations on your wireless network. Consequently, a user that has Administrator permissions for the Avalanche MC Console also has Administrator permissions for any dServer Location on the network.

This chapter provides the following information about user accounts:

- Why Should I Create 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
- Viewing Account Status

Why Should I Create User Accounts?

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

Defining Permission Types

There are two types of user account permissions:

- **Regional Permissions**. These permissions are specific to various tasks and components of Avalanche MC. 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. Regional permission users must also be assigned as authorized users to specific regions in the Navigation Window. Users that are assigned as authorized users for specific regions must be assigned at least one regional permission.

- **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 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.

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.

Why Should I Assign User Permissions?

Until you assign a user some type of permission, that user will be able to log onto the Avalanche MC Console, but will have no other access. The user will not be able to perform any tasks or view any information in the console.

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 MC Console. You also assign permission levels to grant the user access to specific enterprise, Infrastructure dServer and/or Mobile Device dServer functionality.

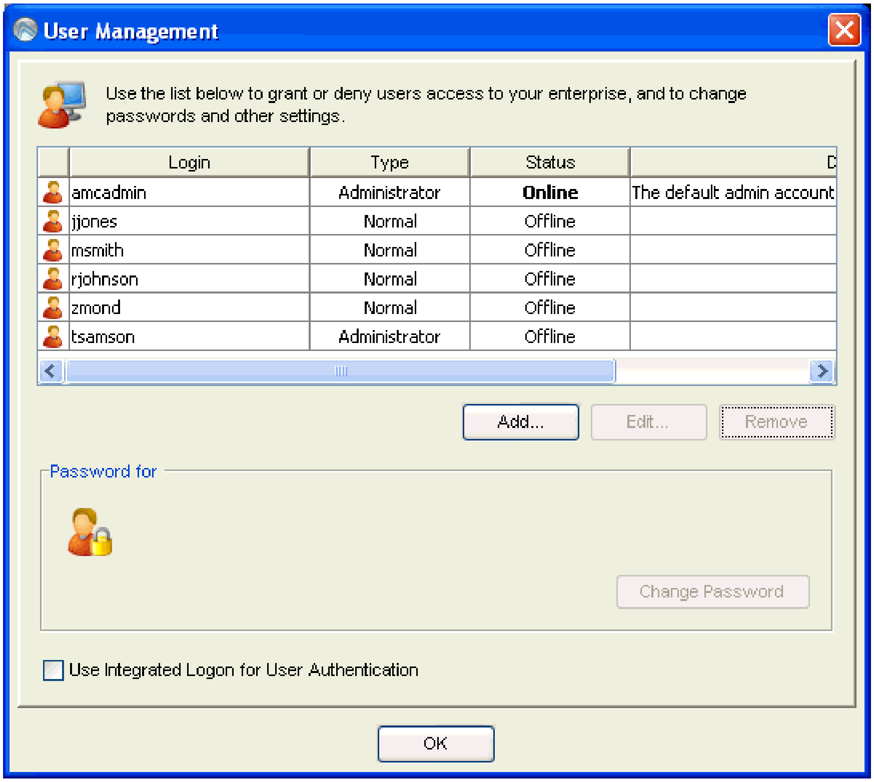
You can configure the following parameters when creating a user account:

- **Login**. This is the name the user will use to log in to the Avalanche MC Console.
- **Password**. This is the password that will grant access to the Avalanche MC Console. Passwords are case sensitive. The password has a 32 character limit.
- **Confirm Password**. You must confirm the password you assigned to the user.
- **First**. This is the first name of the user.
- **Last**. This is the last name of the user.
- **Type**. Select if the user is a Normal use 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 Console.
- **Description**. You can enter a description of the user or group.

To create a new account:

1 From the **Tools** menu, select `User Management`.

The *User Management* dialog box appears.



User Management

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

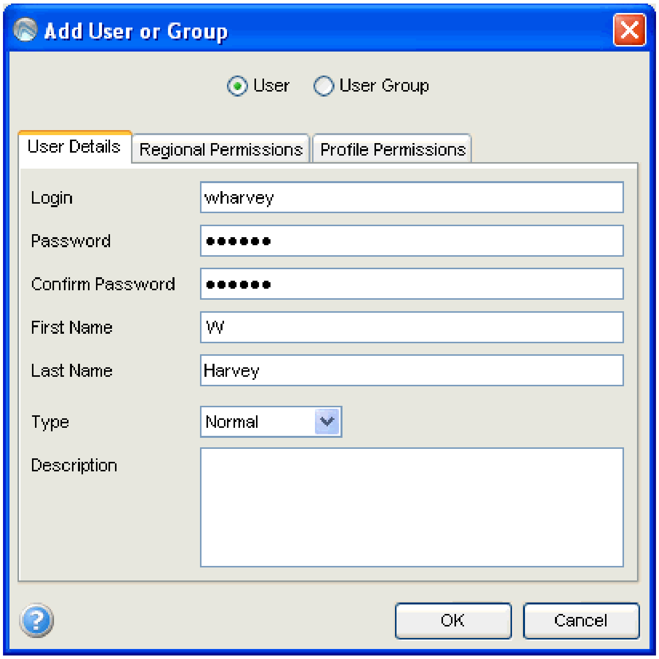
	Login	Type	Status	D
	amcadmin	Administrator	**Online**	The default admin account
	jjones	Normal	Offline	
	msmith	Normal	Offline	
	rjohnson	Normal	Offline	
	zmond	Normal	Offline	
	tsamson	Administrator	Offline	

□ Use Integrated Logon for User Authentication

Figure 5-1. *User Management*

2 Click `Add`.

The *Add User or Group* dialog box appears.



● User ○ User Group

Login: wharvey
Password: ••••••
Confirm Password: ••••••
First Name: W
Last Name: Harvey
Type: Normal
Description:

Figure 5-2. *Add User*

3 Enter the information in the available text boxes.

NOTE The password is case sensitive.

---

4 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 MC Console. The account is also distributed to any known dServer Locations on the network. 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 92.

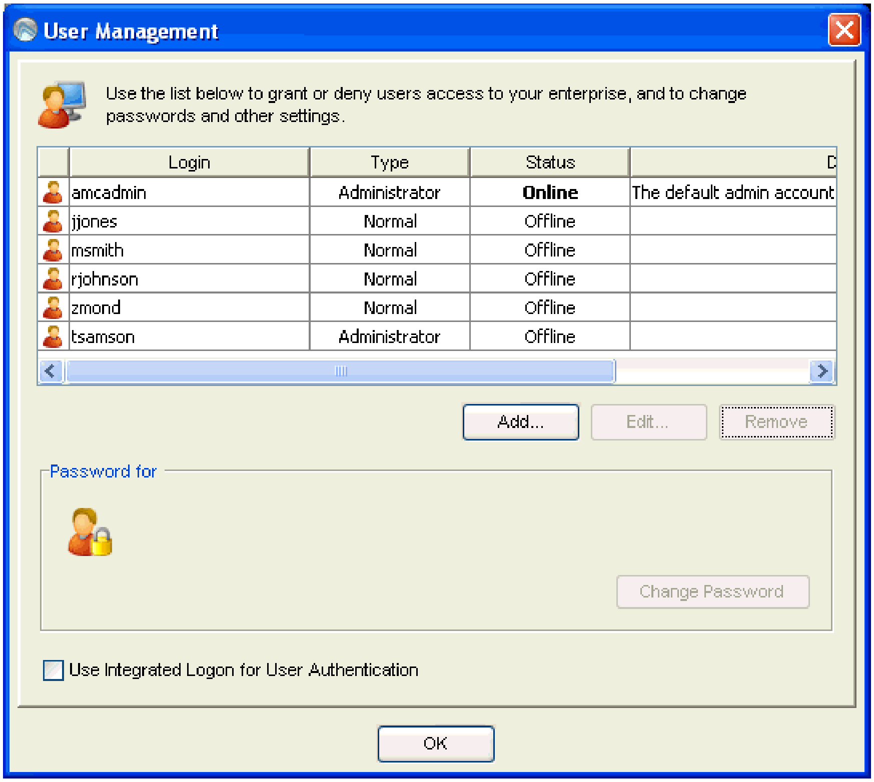
Creating User Groups

You can also create user groups. This allows you to grant permissions and access to the same components at the group level.

To create a user group:

1 From the **Tools** menu, select `User Management`.

The *User Management* dialog box appears.



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

	Login	Type	Status	D
	amcadmin	Administrator	**Online**	The default admin account
	jjones	Normal	Offline	
	msmith	Normal	Offline	
	rjohnson	Normal	Offline	
	zmond	Normal	Offline	
	tsamson	Administrator	Offline	

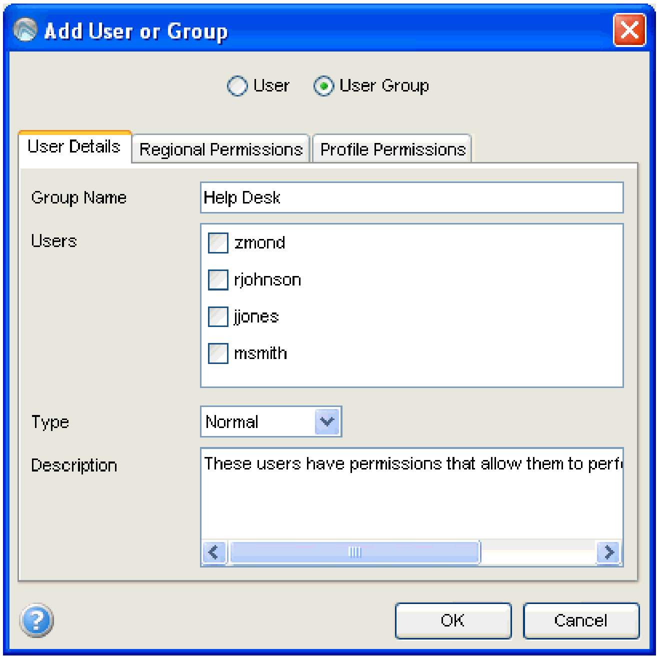
☐ Use Integrated Logon for User Authentication

Figure 5-3. *User Management*

2 Click **Add**.

The *Add User or Group* dialog box appears.

3 Select the **User Group** option.



○ User ● User Group

Group Name: Help Desk

Users:
□ zmond
□ rjohnson
□ jjones
□ msmith

Type: Normal

Description: These users have permissions that allow them to perf

Figure 5-4. *User Group*

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 single users, the list box will be empty. Refer to *Creating User Accounts* on page 87 for information about creating users.

---

6 From the **Type** drop-down list, select if the user group is Normal or Administrator.

7 In the description text box, enter a description of the group, for example what type of permissions are assigned to the group.

8 When you are finished, click **OK**.

Your user group is created. Now you should assign it some permissions. For more information about assigning permissions, refer to *Assigning User Permissions* on page 92.

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.

Assigning Regional Permissions

Regional Permissions are 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. Until you assign the user to a region, Regional Permissions assigned in the *User Management* dialog box do not take effect.

NOTE The permissions are dependent on being assigned at the region level. Each permission is only granted for the region to which the user is assigned. For information about assigning users to regions, refer to *Assigning Authorized Users to Regions* on page 98.

The following table describes the regional permissions:

Regional Permission	Read_Write	Read_Only
Alert Profile	Allows you to configure Alert profiles.	Allows you to view alerts that appear in the Alert Browser.
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.
Infrastructure	Allows you to manage the Infrastructure Inventory for assigned regions.	Allows you to view the Infrastructure Inventory for assigned regions.

Table 5-1: *Regional Permissions Explained*

Regional Permission	Read_Write	Read_Only
Infrastructure Profiles	Allows you to view, manage and apply infrastructure profiles.	Allows you to view which Infrastructure profiles are assigned to a region.
Mobile Device Groups	Allows you to edit mobile device groups.	Allows you to view mobile device groups.
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 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.
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.
Network Profiles	Allows you to apply and remove Network Profiles.	Allows you to view assigned Network Profiles.
Scan to Config	Grants access to the Scan to Config utility and allows you to create, manage and maintain barcode profiles and custom properties.	Allows you to view the scan to config utility and current barcode profiles
Server Profiles: Infrastructure	Allows you to apply and remove Infrastructure dServer profiles.	Allows you to view assigned Infrastructure dServer profiles.
Server Profiles: Mobile Device	Allows you to apply and remove Mobile Device dServer Profiles.	Allows you to view assigned Mobile Device dServer Profiles.

Table 5-1: *Regional Permissions Explained*

Regional Permission	Read_Write	Read_Only
Software Profile	Allows you to apply and remove Software Profiles.	Allows you to view assigned Software Profiles.
Update Profiles	Allows you to apply and remove Update Profiles to your regions.	Allows you to view assigned Update Profiles.

Table 5-1: *Regional Permissions Explained*

To assign regional permissions:

1 From the **Tools** menu, select **User Management**.

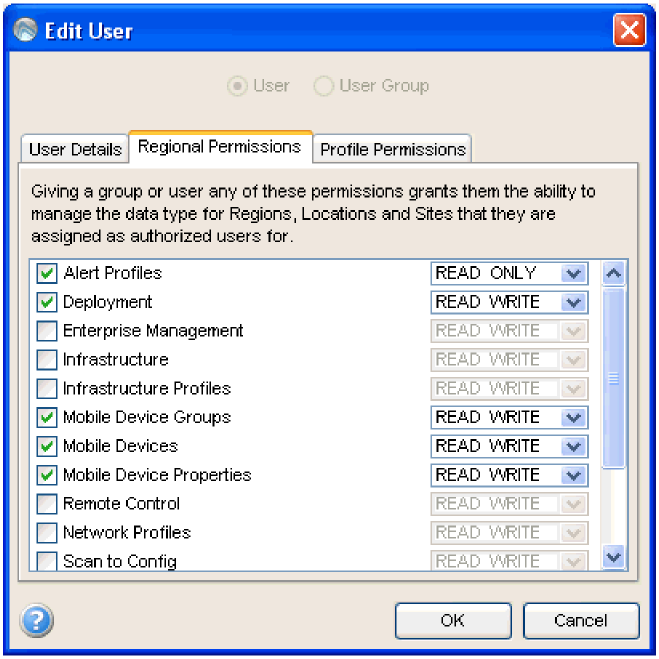
The *User Management* dialog box appears.

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.



Giving a group or user any of these permissions grants them the ability to manage the data type for Regions, Locations and Sites that they are assigned as authorized users for.

☑ Alert Profiles	READ ONLY
☑ Deployment	READ WRITE
□ Enterprise Management	READ WRITE
□ Infrastructure	READ WRITE
□ Infrastructure Profiles	READ WRITE
☑ Mobile Device Groups	READ WRITE
☑ Mobile Devices	READ WRITE
☑ Mobile Device Properties	READ WRITE
□ Remote Control	READ WRITE
□ Network Profiles	READ WRITE
□ Scan to Config	READ WRITE

Figure 5-5. *User Permissions*

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. The profile node or tab will be blank or inaccessible.

6 For each function that you enable, you Read_Write or Read_Only. The default is sent 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.

NOTE For each component in the Regional Permissions, you must assign the user to a region. Until the user is assigned to a specific region, the user will have no access to the component.

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

Assigning 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 delete all alert profiles.	Allows you to view alert profiles and the settings associated with the profile. However you can not modify the profiles in anyway.
Infrastructure Profiles	Allows you to create, configure, edit and delete all profiles.	Allows you to view existing infrastructure profiles and the settings associated with those profiles.
Mobile Device Groups	Allows you to create, configure, edit and delete mobile device groups.	Allows you to view mobile device groups and the settings associated with the groups.
Network Profiles	Allows you to create, configure edit and delete network profiles.	Allows you to view existing network profiles and the settings associated with those profiles.
Server Profiles (Infrastructure)	Allows you to create, configure, edit and delete infrastructure profiles.	Allows you to view existing infrastructure profiles and the associate settings.
Server Profiles (Mobile Devices)	Allows you to create, configure, edit and delete mobile device profiles.	Allows you to view existing mobile device profiles and the associated settings.
Software Profiles	Allows you to create, configure, edit, and delete software profiles.	Allows you to view existing software profiles and the associated settings.
Update Profiles	Allows you to create, configure, edit and delete software profiles.	Allows you to view existing update profiles and the associated settings.

Table 5-2: *Profile Permissions*

To assign user permissions:

1 From the **Tools** menu, select **User Management**.

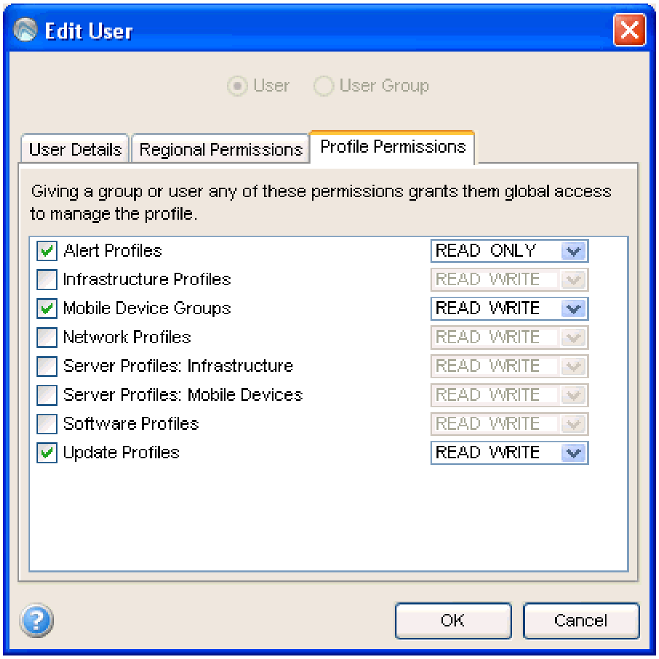
The *User Management* dialog box appears.

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.



Edit User

● User ○ User Group

User Details | Regional Permissions | Profile Permissions

Giving a group or user any of these permissions grants them global access to manage the profile.

☑ Alert Profiles	READ_ONLY
☐ Infrastructure Profiles	READ_WRITE
☑ Mobile Device Groups	READ_WRITE
☐ Network Profiles	READ_WRITE
☐ Server Profiles: Infrastructure	READ_WRITE
☐ Server Profiles: Mobile Devices	READ_WRITE
☐ Software Profiles	READ_WRITE
☑ Update Profiles	READ_WRITE

Figure 5-6. *User Permissions*

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 sent 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. If you do not configure the user to be an authorized user for a region, that user will not be able to manage any of the assigned Regional Permissions. Users that are Normal users but not configured to manage profiles can be assigned as authorized users for specific profiles.

Assigning Authorized Users to Regions

Once you assign a user a Regional Permission in the *User Management* dialog box, you must assign the user to a specific region. Until you assign a user to a region, the user does not have any permission to perform any Regional Permission tasks. When you assign a user to a region, that user has any Regional Permissions to all regions and dServer Locations beneath the assigned region.

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

To assign users to regions:

1 Select the region or dServer Location.

2 Select the **Region Properties** or **dServer Location Properties** tab.

3 Select the **Authorized Users** tab and click **Add User**.

The *Add Authorized User* dialog box appears. This dialog box lists all the Normal users assigned Regional Permissions. The dialog box does not list Administrator users, as these users already have permission to access all regions and dServer Locations.

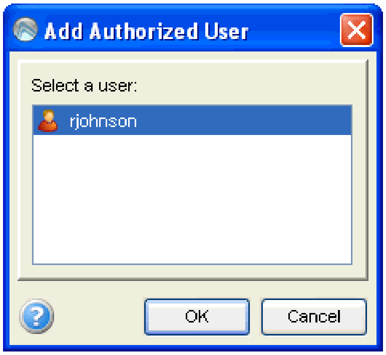


Figure 5-7. *Add Authorized User*

4 Select the user and click **Add**.

The user is added to the list of authorized users and has permission to manage any assigned Regional Permissions to the selected regions and any regions or dServer Locations beneath.

Assigning Authorized Users to Profiles

The **Authorized Users** tab allows you to assign administrative privileges for a specified profile to a user that has Normal user rights and is not assigned permissions to the profile through the Profile Permissions in the User Management dialog box. This means that any user assigned as an authorized user to a profile will have all administrative rights or read-only for that one profile.

To add an authorized user you must have at least one user configured with Normal permissions.

To add an authorized user:

1 Select the desired profile.

2 Select the **Authorized Users** tab and click **Add User**.

The *Select Profile Admin User* dialog box appears.

3 From the list, select the user.

4 From the drop-down list select **READ_WRITE** or **READ_ONLY** permission for the user.

5 Click **OK**.

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

Removing Authorized Users

If you do not want a user to have any privileges for a profile, you can remove that user from the Authorized User list. The user will be able to view the name of the profile, but will not have access to the data or be able to modify the profile.

To remove an authorized user:

1 From the **Authorized Users** tab, select the desired user.

2 Click **Remove User**.

The user is removed from the **Authorized Users** list for the profile.

Configuring Integrated Logon

Avalanche MC provides secure authentication by interfacing with services and utilizing security information. This allows console-users to log in to the Avalanche MC Console using the same information they use to log in to the network.

When you enable the integrated login, users with network logins can log on to the Avalanche MC 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.

NOTE If you are going to enable integrated logon, you must disable the guest account.

To enable integrated logon:

1 From the **Tools** menu, select `User Management.`

The *User Management* dialog box appears.

2 Enable the **Use Integrated Logon for User Authentication** option.

3 Click **OK**.

4 Log out of the Avalanche MC Console.

Avalanche MC 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 can not change passwords for any account.

To change a password:

1 From the **Tools** menu, select **User Management**.

The *User Management* dialog box appears.

2 Select the user account for which you want to change the password.

3 In the **Password For** region, 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 MC Console.

The new password information is now available for the Avalanche MC Console. The password also distributed to any known dServer Locations on the network.

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

Removing User Accounts

If you have an Administrator user account or belong to an administrator group, you can delete user accounts. Once you remove an account, that user will no longer have access to the Avalanche MC Console using that log in information.

To delete a user account:

1. From the **Tools** menu, select **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 is removed from the Avalanche MC Console. It is also removed from any known dServer Locations on the network.

Viewing Account Status

If you have an Administrator user account, you can view the status of other Avalanche MC users. This allows you to determine which user accounts are currently online. Normal user accounts can not view other users.

To view the status of a user:

- From the **Tools** menu, select **User Management**.

  The *User Management* dialog box appears.

  From the **Status** column in the user list, you can determine which user accounts are currently online. User groups do not show up as online.

Chapter 6: Managing Regions and dServer Locations

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

Avalanche MC divides locations into two categories: dServer Locations and regions. A dServer Location is the most basic component. Each dServer Location contains at least one Server that communicates with specific wireless components. Because dServer Locations are based on Servers, you can define a dServer Location in a way that best suits your network administration processes—for example, you can organize dServer Locations by location or by network role.

NOTE The number of wireless components managed at a dServer Location depends on the communication range of the Servers installed at that dServer 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 dServer Location level using the Mobile Manager dServer Location tool. See the *Mobile Manager User's Guide* for more information.

Avalanche MC streamlines wireless network management by allowing you to create one or more collections of dServer Locations, called regions. Each dServer Location within a region contains a set of similar characteristics such as geographic location or role within your organization's structure. When you configure a region, the Avalanche MC Console applies the configurations to every dServer Location within that region.

You control how many regions your organization uses and how many dServer Locations belong to each region. You can create as many or as few regions as your network management processes demand.

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

- Overview
- Managing Regions

- Managing dServer Locations
- Building Server Deployment Packages
- Server Auto-Discovery
- Managing dServers

Once you create the necessary dServer Locations and regions for your network, you can manage them by configuring Infrastructure and mobile device properties as needed. See *Managing Infrastructure dServer Profiles* on page 119 and *Managing Mobile Device dServer Profiles* on page 128 for more information.

Overview

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

1. **Install Avalanche MC.** For more information, refer to *Chapter 2: Installing Avalanche MC* on page 21.
2. **Activate Mobile Device dServer and Infrastructure dServer licenses for Avalanche MC.** 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 43.
3. **Create Regions.** A region is a collection of dServer 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 105.
4. **Create dServer Locations.** dServer Locations are the basic component of Avalanche MC and are where the Servers reside. For more information, refer to *Managing dServer Locations* on page 114.
5. **Configure profiles.** You can configure settings for network, software, alert, Server, and infrastructure profiles. Once you create these profiles, you assign the profiles to regions you have created. For more information, refer to *Chapter 15: Managing Alerts* on page 287, *Chapter 8: Managing Infrastructure Distributed Servers* on page 167, *Chapter 9: Managing Mobile Device Distributed Servers* on page 183, *Chapter 10: Managing Software*

Profiles on page 209, *Chapter 7: Managing Network Profiles* on page 143, and *Chapter 11: Managing Infrastructure Profiles* on page 225.

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 dServer Locations within the region. For more information, refer to *Assigning Profiles to Regions* on page 107.

7 **Install Servers.** Create a server package to deploy to the regions. This will install the Servers and apply all profile configuration to the devices at the dServer Location. For more information, refer to *Building Server Deployment Packages* on page 131.

Managing Regions

A region is a collection of dServer Locations that share a set of similar characteristics such as geographic location or role within your organization structure. To define the settings for Infrastructure and mobile devices (through profiles), you can apply the settings on a per-region basis.

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

This section provides information about the following:

- Why Should I Create a Region?
- Creating Regions
- Viewing Region Properties
- Creating Nested Regions
- Deleting Regions

NOTE To configure an individual dServer Location from the Avalanche MC Console, you create a region that contains only that dServer Location and apply settings to that region, or by accessing the Mobile Manager Administrator.

Why Should I Create a Region?

Regions are merely a way to organize your dServer locations. dServer Locations must be positioned in a region.

Creating Regions

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

To create a region:

1 From the **File** menu, select **New > Create Region**.

-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 collection of nested regions and the dServer Locations associated with those regions. Nested regions provide great flexibility when setting up your network and console structure. You can apply network, alert, and Mobile Device dServer and Infrastructure dServer profiles appropriately to each region.

Nested Regions and Network Profiles

When you create nested regions, network profiles can be applied to any region within your branch. Servers work their way up through the branch of nested regions examining the network profiles available in each region. When a Server finds a network profile that matches its selection criteria, the Server takes on that profile. If there is more than one network profile that matches the Server selection criteria, the Server takes on the first network profile listed in the **Network Profile** tab of the Avalanche MC Console. If the Server checks each region and does not find a matching network profile, the Server assumes the default network profile until a matching network profile is deployed to that region.

Nested Regions and Software Profiles

Software profiles assigned to a region in a branch of nested regions are deployed to all other regions within the assigned region. For example, if you have a five-step branch of regions and you assign a software profile to the third-step region in the branch, the third, fourth and fifth steps of the branch receive the software profile based on selection criteria. The first and second steps of the branch will not receive the software profile unless it is assigned specifically.

Nested Regions and Server Profiles

Server profiles are assigned specifically to each dServer Location in each region. There is no varying behavior for nested regions.

Nested Regions and Alert Profiles

When you assign an alert profile to a region, the alert profile is applied to the region to which it was assigned and all other nested regions in the branch. The default alert profile is deployed to all regions in the console.

Viewing Region Properties

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

To view region properties:

- In the Navigation Window, click the region.

  The main console window displays the properties for the selected region.

Assigning Profiles to Regions

Once you create a region you can assign any available profiles to that region. Profiles include:

- Why Should I Assign a Profile to a Region or dServer Location?
- Assigning Infrastructure Profiles to Regions

- Assigning Server Profiles to Regions
- Assigning Alert Profiles to Regions
- Assigning Network Profiles to Regions
- Assigning Software Profiles to Regions

This section provides information about how you can assign each type of profile to a region.

Why Should I Assign a Profile to a Region or dServer Location?

If you do not assign profiles to regions or dServer Locations, the settings in those profiles will not reach the dServers, resulting in the inability to manage network infrastructure and mobile devices.

Assigning Infrastructure Profiles to Regions

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 order in which the profiles are listed in the Avalanche MC console. If you have not already created an Infrastructure profile, you will need to create one. For information about creating Infrastructure profiles, refer to *Creating Infrastructure Profiles* on page 228. Once you assign an Infrastructure profile to a region, you must perform a Universal Deployment to update your Servers. For more information the Universal Deployment, refer to *Deploying Universal Updates* on page 334.

To assign an Infrastructure profile:

1 From the Navigation Window, select the region to which you want to assign an Infrastructure profile.

2 Click the **Region Properties** tab.

3 Click **Edit**.

4 In the **Infrastructure Profile** tab, click **Add**.

The *Add AP Profile Application* dialog box appears.

5 From the list of available Infrastructure profiles, select which profile you want to assign to this region.

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

6 If you want the hardware in the region to retain the default hardware profile, enable the **Default Hardware Profile** check box.

7 Click **OK**.

The profile is added to the **Infrastructure Profile** tab for the region.

8 Continue adding Infrastructure profiles to the region, if desired.

9 Use the **Move Up** and **Move Down** buttons to assign the order in which the Infrastructure profiles are applied to mobile devices.

10 Save your changes.

The assigned profile will be deployed to the Servers when you install the Servers or when you perform a Universal Deployment. For information about installing Servers, refer to *Deploying dServers* on page 331. For more information the Universal Deployment, refer to *Deploying Universal Updates* on page 334.

Assigning Server Profiles to Regions

You can assign one Mobile Device dServer profile and one Infrastructure dServer 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 MC console. If you have not already created a Server profile, you will need to create one. For information about creating Server profiles, refer to *Creating Infrastructure dServer Profiles* on page 168 or *Creating Mobile Device dServer Profiles* on page 184. Once you assign Server profile to a region, you must perform a Universal Deployment to update your Servers. For more information the Universal Deployment, refer to *Deploying Universal Updates* on page 334.

To assign a Server profile:

1 From the Navigation Window, select the region or dServer Location to which you want to assign a profile.

2 Select the **Distributed Servers Profile** tab.

3 Click **Edit**.

4 To assign an Infrastructure dServer profile, perform one of the following actions:

- Select the **Inherit Profile** option if you want to use the default Infrastructure profile.

-Or-

- Enable the **Assign Directly** option and select the profile you want to assign to this region from the drop-down list.

5 To assign a Mobile Device dServer profile, perform one of the following actions:

- Select the **Inherit Profile** option if you want to use the default Mobile Device dServer profile.

-Or-

- Enable the **Assign Directly** option and select the profile you want to assign to this region from the drop-down list.

6 Save your changes.

The assigned profile will be deployed to the dServers when you install the dServers or when you perform a Universal Deployment. For information about installing Servers, refer to *Deploying dServers* on page 331. For more information the Universal Deployment, refer to *Deploying Universal Updates* on page 334.

Assigning Alert Profiles to Regions

Alert profiles are assigned at a region level. Any alert profile assigned at the Enterprise level will be pushed down to all regions within the enterprise. Alerts assigned at the region level will be pushed to any other nested regions in that branch. Profiles assigned at the My Enterprise level will appear grayed out in the **Alerts** tab and can not be removed at the region level.

To assign an alert profile:

1 From the Navigation Window, select the region or dServer Location to which you want to assign a profile.

2 Select the **Alert Profile** tab and click **Edit**.

3 Click **Add**.

The *Add Alert Profile Application* dialog box appears.

4 From the list, select the alert profile you want to assign to the region.

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

---

5 Click **OK**.

The profile is added to the **Alerts** tab.

6 Continue adding Alert profiles to the region or dServer Location.

7 Save your changes.

The assigned profiles will deploy to the dServers when you install the Servers or when you perform a Universal Deployment. For information about installing Servers, refer to *Deploying dServers* on page 331. For information about performing a Universal Deployment, refer to *Deploying Universal Updates* on page 334.

Assigning Network Profiles to Regions

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 MC console. If you have not already created a network profile, you will need to create one. For information about creating network profiles, refer to *Creating Network Profiles* on page 144. Once you assign an network profile to a region, you must perform a Universal Deployment to update your Servers. For more information the Universal Deployment, refer to *Deploying Universal Updates* on page 334.

To assign a network profile:

1 From the Navigation Window, select the region or dServer Location to which you want to assign a network profile.

2 Select the **Network Profiles** tab and click **Edit**.

3 Click **Add**.

The *Add Network Profile Application* dialog box appears.

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

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

---

5 If you to configure selection criteria for the profile, click the selection criteria button and use the Selection Criteria Builder to build the selection criteria for this network profile.

For information about building selection criteria, refer to *Building Selection Criteria* on page 276.

6 Click **OK**.

The profile is added to the **Network Profiles** tab for the region.

7 Continue adding network profiles to the region or dServer Location.

8 Use the **Move Up** and **Move Down** buttons to assign the order in which the Network profiles are applied to mobile devices.

9 Save your changes.

The assigned profile will be deployed to the dServers when you install the Servers or when you perform a Universal Deployment. For information about installing Servers, refer to *Deploying dServers* on page 331. For more information the Universal Deployment, refer to *Deploying Universal Updates* on page 334.

Assigning Software Profiles to Regions

When you assign software profiles to a region, the profiles are deployed to all regions and dServer Locations nested within the assigned region based on selection criteria of the software packages. If you have not already created a software profile, you will need to create one. For information about creating software profiles, refer to *Creating Software Profiles* on page 209. Once you assign a software profile to a region, you must perform a Universal Deployment to update your Servers. For more information the Universal Deployment, refer to *Deploying Universal Updates* on page 334.

To assign software profiles

1 From the Navigation Window, select the region or dServer profile to which you want to assign a network profile.

2 Select the **Software Profiles** tab and click Edit,

3 Click **Add**.

The *Add Software Profile Application* dialog box appears.

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

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

5 If you want to configure selection criteria for the profile, click the selection criteria button and use the Selection Criteria Builder to build the selection criteria for this network profile.

NOTE For information about building selection criteria, refer to *Building Selection Criteria* on page 318.

6 Click **OK**.

The profile is added to the **Software Profiles** tab for the region.

7 Continue adding network profiles to the region or dServer Location.

8 Use the **Move Up** and **Move Down** buttons to assign the order in which the Network profiles are applied to mobile devices.

9 Save your changes.

The assigned profile will be deployed to the Servers when you install the Servers or when you perform a Universal Deployment. For information about installing Servers, refer to *Deploying dServers* on page 331. For more information the Universal Deployment, refer to *Deploying Universal Updates* on page 334.

Deleting Regions

You can delete unused regions from the Avalanche MC Console at any time. Any dServer Locations associated with a region automatically return to the **Deleted dServer 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 regions:

1 Right-click the region or dServer 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 dServer Locations in that region are moved to the **Deleted dServer Locations** folder.

NOTE You can restore dServer Locations that are in the deleted dServer Locations folder to the **Unassigned dServer Locations** folder where you can then reassign the dServer Locations to a new region. For more information about restoring deleted dServer Locations, refer to *Restoring dServer Locations* on page 126.

Managing dServer Locations

A dServer Location (formerly called sites) is any location that contains wireless components that are managed by an Infrastructure dServer, a Mobile Device dServer, or both. A dServer Location can be a unique physical entity, such as a warehouse, or a subsection of an entity, such as the third floor of an office building.

The number of wireless components managed at a dServer Location depends on the communication range of the dServers installed at that dServer 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.

There are two types of dServers that can deployed to a dServer Location, Infrastructure dServers and Mobile Device dServers. Each dServer Location can have up to one Mobile Device dServer and one Infrastructure dServer residing on it.

To ensure that all wireless devices are managed at a particular dServer 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 dServer Location-based tools included with Mobile Manager to configure the Server to manage multiple subnets.
- Segment the location into multiple dServer Locations by installing the appropriate Servers at each subnet.

In most cases, the location you want to manage with Avalanche MC does not contain a dServer. As a result, you must create a new dServer Location by deploying one or more dServers to that location.

This section provides information about the following topics:

- Why Should I Create dServer Locations?
- Determining dServer Placement
- Adding dServer Locations
- Understanding Unassigned dServer Locations
- Moving dServer Locations to Regions
- Modifying dServer Location Properties
- Deleting dServer Locations

Why Should I Create dServer Locations?

To manage your network infrastructure and mobile devices, you must deploy dServers to specified locations where the devices can communicate with the servers. These specified locations are referred to as dServer Locations.

Determining dServer Placement

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

Centralized Server Installation

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

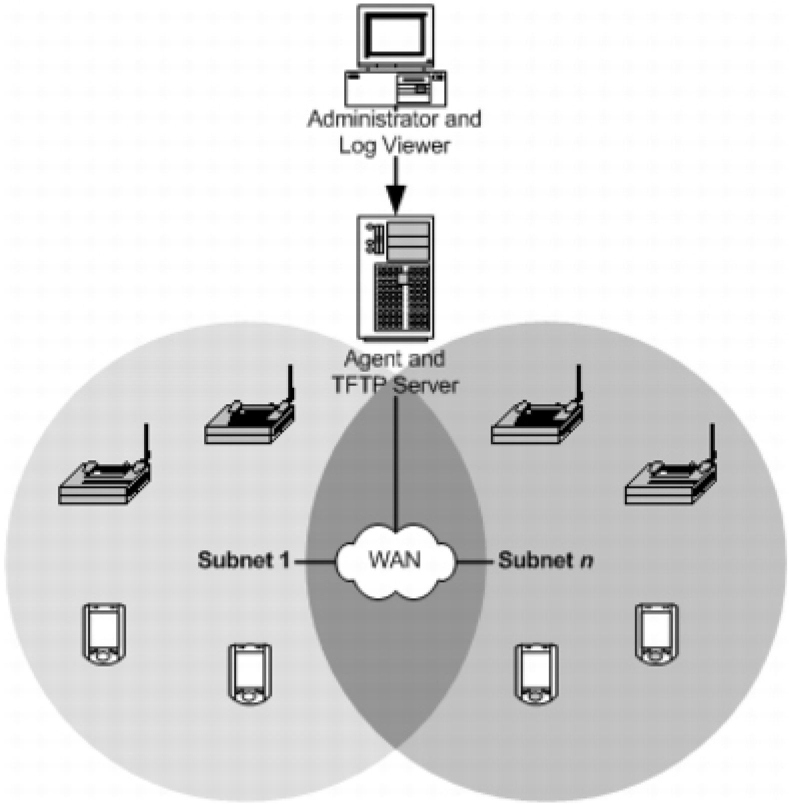


Figure 6-1. *A Centralized Installation of Avalanche MC (Simplified)*

If you determine that a centralized dServer 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 dServer knows where to listen for infrastructure broadcasts.

- You must know what switches and routers reside between the dServer 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 Installation

In distributed dServer installations, a dServer resides on each network subnet. These dServers are responsible for managing on a per-subnet basis. Often, distributed dServer installations of Avalanche MC are found in environments where wireless network uptime is critical to business operations. For example, if a company has multiple locations across the country, connectivity between each dServer 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 dServer on each subnet provides a more robust environment in which wireless network downtime is minimized.

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

- Because you are installing multiple dServers on multiple systems, it might take more time to completely install and optimize Avalanche MC for your network.

- You must ensure that when you upgrade Avalanche MC, you upgrade all dServers across the network.

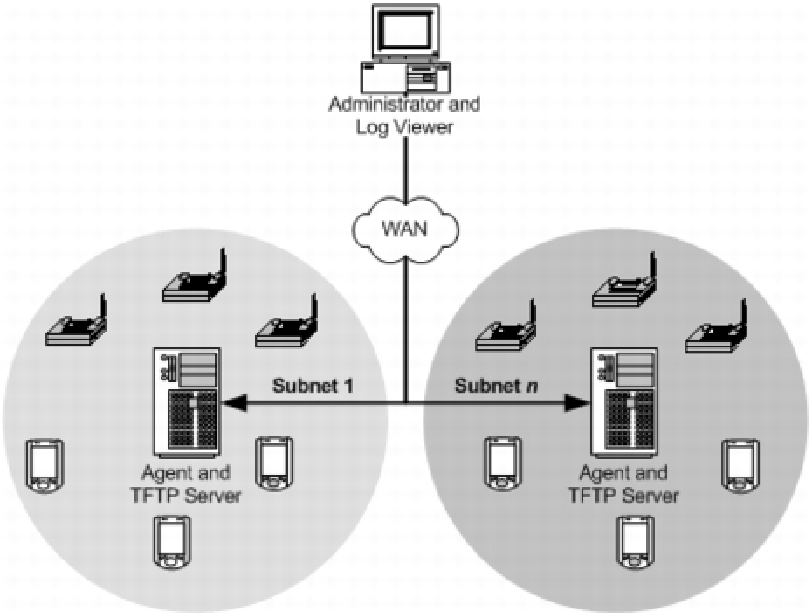


Figure 6-2. *A Distributed Installation of Avalanche MC (Simplified)*

For information about how to deploy infrastructure settings, refer to *Deploying dServers* on page 331.

If the location already contains one or more dServers, you do not need to create a new dServer Location. However, you must ensure that the Server installed at the dServer Location is compatible with the Avalanche MC Console. See *Installation Requirements* on page 21 for more information.

Adding dServer Locations

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

To add a dServer Location:

1 From the **File** menu, select **New** > **Create dServer Location**.

The *Enter dServer Location Name* dialog box appears.

2 Type the name of the dServer Location in the **dServer Location Name** text box and click **`Next`**.

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

3 Type the IP address of the system which contains (or will contain) a Server in the **dServer Location IP address** text box and click **Next**.

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

4 Type the name of the city where the dServer Location resides in the **dServer Location City Name** text box.

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

NOTE Avalanche MC connects to a database at the Wavelink Web site.

5 Click **Next**.

The *Choose dServer Location* dialog box appears.

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

The *Select Time Zone* dialog box appears.

7 Select the time zone for the city 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 dServer resides (or will reside) and click **Next.**

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

The *Select Shared Folder Location* dialog box appears.

9 Select the appropriate location for the shared folder.

NOTE If the *Enter Shared Folder Information* dialog box appears, type the name of the shared folder where Avalanche MC updates are installed in the **Share Name** text box.

Type the directory path where Avalanche MC 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 MC attempts to contact the dServer 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 dServer Location appears in the region in which you created it. You can assign the dServer Location to a different region, deploy Servers to the dServer Location or modify the dServer Location.

Understanding Unassigned dServer Locations

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

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

NOTE You can manage Infrastructure dServers listed in the **Unassigned dServer Locations** folder.

Moving dServer Locations to Regions

When you create regions, you assign dServer Locations to that region. One of the benefits of creating regions is that when you change region configuration settings, those changes can be applied to all dServer Locations assigned to that region. Before you can really manage anything at the dServer Location level, that dServer Location must belong to a region.

To move a dServer Location to a region:

- Right-click a region, select **Create dServer Location**.

NOTE When you use this method, you will be prompted to create a new dServer Location that will automatically be assigned to that selected dServer Location. For more information about creating dServer Locations, refer to *Adding dServer Locations* on page 119.

-Or-

- Right-click a dServer Location in the **Unassigned dServer Locations** folder, select **Move dServer Location To** from the menu that appears, and select the region.

  The dServer Location moves to the selected region and you can begin managing your mobile devices.

Modifying dServer Location Properties

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

You can modify the following dServer Location properties:

- Name

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

NOTE Wavelink does not recommend that you change a dServer Location IP address without performing the appropriate tasks. For information about changing a dServer Location IP address, refer to *Changing Mobile Device dServer Location IP Address* on page 123 and *Changing Infrastructure dServer Location IP Address* on page 124.

To modify dServer Location properties:

1 From the Navigation Window, click the dServer Location and then the **dServer Location Propertie**s tab.

2 Click **Edit**.

3 Edit the information as needed.

4 Save your changes.

Changing Mobile Device dServer Location IP Address

You can change the IP address of the system hosting a Mobile Device dServer. When you migrate the IP address of a Mobile Device dServer, you must modify the `Avalanche.properties` configuration file located in the folder where you installed the Mobile Device dServer.

To migrate the IP address:

1 Stop the Mobile Device dServer.

2 Navigate to the following location:

`[Mobile Device dServer deployment package location]\Wavelink\Avalanche\Service`.

3 Open the `Avalanche.properties` file in a text editor, such as Notepad.

4 Locate the `dServer LocationIdentifier` line and update this line with the new IP address.

5 Save the text file.

6 In the Avalanche MC Console, select the dServer Location that you are migrating to display the **dServer Location Properties** tab.

7 In the **IP Address** text box, change the IP address to reflect the changes in the `Avalanche.properties` file.

8 Save your changes.

9 Restart the Mobile Device dServer.

Your Mobile Device dServer is now located at the new IP address.

Changing Infrastructure dServer Location IP Address

You can change the IP address of the system hosting a Mobile Device dServer. When you migrate the Infrastructure dServer IP address you must modify the `dServer Locationir.cfg` file.

To migrate the IP address:

1 Stop the Infrastructure dServer.

2 Navigate to the following location:

`[Infrastructure dServer deployment package location]\Wavelink\MM\Program`.

3 Open the `dServer Locationir.cfg` file in a text editor, such as Notepad.

4 Locate the `dServer LocationIdentifier` line and update this line with the new IP address.

5 Save the text file.

6 In the Avalanche MC Console, select the dServer Location that you are migrating to display the **dServer Location Properties** tab.

7 In the **IP Address** text box, change the IP address to reflect the changes in the `dServer Locationir.cfg` file.

8 Save your changes.

9 Restart the Infrastructure dServer.

Your Infrastructure dServer is now located at the new IP address.

Assigning Profiles to dServer Locations

You can assign any configured profile to a dServer Location from the **dServer Location Properties** tab. You use the same method to assign profiles to dServer as you do to assign profiles to regions. For detailed steps about assigning profiles, refer to *Assigning Profiles to Regions* on page 107.

Deleting dServer Locations

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

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

- Removing dServer Locations
- Restoring dServer Locations

NOTE To completely remove a dServer Location, you must first remove the Servers associated with that dServer Location. For information about removing Servers, refer to *Uninstalling dServers* on page 339.

To move a dServer Location to the Deleted dServer Locations folder:

- Select the dServer Location from the Navigation Window and press the `Delete` key.

  -Or-

- Right-click the dServer Location and select **Delete** from the menu that appears.

Removing dServer Locations

You can completely remove dServer Locations located in the **Deleted dServer Locations** folder. When you remove dServer Locations from the **Deleted dServer Locations** folder, the dServer Location and historical data are completely deleted from the databases.

To completely remove a dServer Location, you must first remove the dServers associated with that dServer Location. For information about removing Servers, refer to *Uninstalling dServers* on page 339.

To completely delete a dServer Location:

- Select the dServer Location from the Navigation region and press the `Delete` key.

  -Or-

- Right-click the dServer Location and select **Delete** from the menu that appears.

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

Restoring dServer Locations

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

To restore a dServer Location:

1. In the Navigation region, expand the **Deleted Devices** folder.
2. Right-click the dServer Location you want to restore and select **Restore**.

   The dServer Location is restored to the **Unassigned dServer Locations** folder.

Creating Sites

Sites are groups of mobile devices that share a Mobile Device dServer. Sites are grouped together by unique selection criteria. This allows increased flexibility of assigning different profiles to individual sites at the same dServer Location.

To create a site:

1. Right-click the dServer Location where you want to place the site and click **Create Site**.

   The *Add 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 dServer Location.

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. 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, 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

1 Right-click the site from the Navigation Window.

2 Select **Ping Mobile Devices** from the menu that appears.

   The **Recent Activity** column 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 menu that 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 Site Properties

Site properties retrieve the common properties from all the devices in the site. You can then add, edit, and delete properties for 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 *Building Selection Criteria* on page 318 for related information.

User-defined properties created within a site apply to all devices within that within the site. If you view an individual mobile device in the **Mobile Device Inventory** tab, you will see properties created for the device within the site.

To add a property to a mobile device group:

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

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

2 Click **Add 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 name of the property in the **Property Name** text box.

5 Enter the value of the property in the **Property Value** text box.

6 Click **OK**.

The new property is added to the properties list.

7 When you are finished adding properties, click **OK** to return to the Avalanche MC Console.

To edit site properties:

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

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

2 Select the property that you want to edit and click **Edit Property**.

The *Edit Device Property* dialog box appears.

3 Type the new property value.

4 Click **OK**.

The edited property appears in the list.

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

To delete site properties:

1 Right-click site 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 MC Console.

The property will be deleted after the next update.

Assigning Profiles to Sites

You can assign any configured profile, except Mobile Device dServer Profiles and Infrastructure Profiles to a site from the **Site Properties** tab. You use the same method to assign profiles to a site as you do to assign profiles to regions. For detailed steps about assigning profiles, refer to *Assigning Profiles to Regions* on page 107.

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.

Building Server Deployment Packages

This section provides information about the following:

- Why Should I Create Server Deployment Packages?
- Deployment Packages for Infrastructure and Mobile Device dServers
- Deployment Packages for Infrastructure dServers
- Deployment Packages for Lightweight Infrastructure Updates
- Deployment Packages for Mobile Device dServers

Why Should I Create Server Deployment Packages?

Essentially, your dServers do not exist until you create and deploy server deployment packages. A deployment package is a collection of files that define dServer behavior, for both Infrastructure and Mobile Device dServers. You must create these packages so you can control your dServer Locations, thereby controlling your network infrastructure and mobile devices.

Deployment Packages for Infrastructure and Mobile Device dServers

When you create a combined deployment package for both infrastructure and mobile devices, Avalanche MC deploys a full-function Infrastructure dServer and a full-function Mobile Device dServer to a dServer Location that may or may not have dServers already.

To create a deployment package for all devices:

1 From the **Tools** menu, select **Deployment Packages**.

The *Deployment Package Manager* dialog box appears.

2 Click **Add**.

The *Select Package Type* dialog box appears.

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

The *Select Server Type* dialog box appears.

4 Select the **Combined Infrastructure and Mobile Unit dServers** option and click **Next**.

The *Enterprise dServer Location* dialog box appears.

5 Type the IP address of the Enterprise server and click **Next**.

The *Installation Path* dialog box appears.

6 Type the full path where the package is to be installed on the remote system in the *Installation Path* dialog box, for example: `C:\Program Files\Wavelink`.

If you want to include the RAPI gateway in this deployment package, enable the **Include RAPI Gateway** option. Click **Next**.

The *Select Infrastructure dServer Options* dialog box appears.

7 Determine how the Infrastructure dServer selects a network adapter and click **Next**.

- If you want the dServer to select the first available network adapter, select the **Use First Available** option.
- If you want the dServer to select an adapter based on a specific subnet, select the **Select by Subnet** option and then type the subnet address in the text box.

8 Determine the security options for the dServer and click **Next**.

- If you want the Server to operate without any security measures, select the **No Security** option.
- If you want the dServer to require a user name and password, select the **Security without Encryption** option.

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

The *Select Infrastructure Firmware Support* dialog box appears. This dialog box contains a collection of folders. Each folder represents a specific type of infrastructure.

9 If you only want to select from firmware bundled with Avalanche MC, enable the **Only show available firmware binaries included on server.**

NOTE When you enable the **Only show available firmware binaries included on server** option, you will be able to select firmware that is bundled with Avalanche MC and will deploy to the Infrastructure dServer.

If you do not enable this option, you will see a list of all firmware support including firmware options that are not bundled with Avalanche MC.

---

10 Select the firmware versions this dServer supports and then click **Next**.

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

The *Enter Package Name* dialog box appears.

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

Avalanche MC creates the deployment package. When it is finished, the *Package Complete* dialog box appears.

12 Click **Finish** to return to the *Deployment Package Manager* dialog box.

You can now create a new package, edit a package, or delete a package as needed.

13 Click **Close** to return to the Avalanche MC Console.

To deploy the Server package, you must use the Task Scheduler and perform a Deploy/Update Server task. For more information refer to *Deploying dServers* on page 331.

Deployment Packages for Infrastructure dServers

When you create a deployment package for Infrastructure dServers, Avalanche MC deploys a full-function Infrastructure dServer to a dServer Location that may or may not yet have an Infrastructure dServer. To create an Infrastructure dServer deployment package you must have at least one user configured with administrative privileges and a password.

To create a deployment package for Infrastructure dServers:

1. From the **Tools** menu, select **Deployment Packages**.

   The *Deployment Package Manager* dialog box appears.

2. Click **Add**.

   The *Select Package Type* dialog box appears.

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

   The *Select Server Type* dialog box appears.

4. Select the **Infrastructure dServer only** option and click **Next**.

5. Type the IP address of the license server on which you want the Infrastructure dServer to reside and click **Next**.

   The *Installation Path* dialog box appears.

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

   The *Select Infrastructure dServer Options* dialog box appears.

7. Determine how the Infrastructure dServer selects a network adapter and click **Next**.

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

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

8 Determine the security options for the dServer and console and click **Next**.

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

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

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

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

9 If you only want to select from firmware bundled with Avalanche MC, enable the **Only show available firmware binaries included on server.**

NOTE When you enable the **Only show available firmware binaries included on server** option, you will be able to select firmware that is bundled with Avalanche MC and will deploy to the Infrastructure dServer.

If you do not enable this option, you will see a list of all firmware support including firmware options that are not bundled with Avalanche MC.

10 Select the firmware versions this dServer will support and click **Next**.

To select firmware, open the appropriate folder within the dialog box. 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.

The *Enter Package Name* dialog box appears.

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

Avalanche MC creates the deployment package. When it is finished, the *Package Complete* dialog box appears.

12 Click **Finish** to return to the *Deployment Package Manager* dialog box.

You can now create a new package, edit a package, or delete a package as needed.

13 Click **Close** to return to the Avalanche MC Console.

To deploy the Server package, you must use the Task Scheduler and perform a Deploy/Update Server task. for more information refer to *Deploying dServers* on page 331.

Deployment Packages for Lightweight Infrastructure Updates

If you only want to update an existing Infrastructure dServer to the latest version of Avalanche MC, without changing any settings or deploying any firmware files, you can pick **Lightweight Infrastructure dServer Update.** The resulting deployment package will be much smaller in size because this package only replaces the core executables. This is particularly advantageous for low bandwidth networks.

To create a deployment package for Infrastructure updates:

1 From the **Tools** menu, select **Deployment Packages**.

The *Deployment Package Manager* dialog box appears.

2 Click **Add**.

The *Select dServer Type* dialog box appears.

3 Select the **Lightweight Infrastructure dServer Update** option and click **Next**.

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

Avalanche MC creates the deployment package. When it is finished, the *Package Complete* dialog box appears.

5 Click **Finish**.

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

Deployment Packages for Mobile Device dServers

This section describes how to create a deployment package that will manage mobile devices at a specific dServer Location.

To create a deployment package for mobile devices:

1 From the **Tools** menu, select **Deployment Packages**.

The *Deployment Package Manager* dialog box appears.

2 Click **Add**.

The *Select dServer Type* dialog box appears.

3 Select the **Mobile Unit Server Only** option and click **Next**.

The *Enterprise Server Location* dialog box appears.

4 Type the IP address of the Enterprise server on which you want the Mobile Device dServer to reside and click **Next**.

The *Installation Path* dialog box appears.

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

6 If you want to include the RAPI gateway in this deployment package, enable the **Include RAPI Gateway** option and click **Next**.

The *Enter Package Name* dialog box appears.

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

Avalanche MC creates the deployment package. When it is finished, the *Package Complete* dialog box appears.

8 Click **Finish** to return to the *Deployment Package Manager* dialog box.

You can now create a new package, edit a package, or delete a package as needed.

9 Click **Close** to return to the Avalanche MC Console.

To deploy the Server package, you must use the Task Scheduler and perform a Deploy/Update Server task. for more information refer to *Deploying dServers* on page 331.

Server Auto-Discovery

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

If you install Avalanche MC on a different system, dServers are not auto-discovered.You need to re-deploy Mobile Device dServers and Infrastructure dServers.

Managing dServers

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

Stopping dServers

You can stop a dServer from the Navigation Window of the Avalanche MC Console.

To stop dServers:

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

Starting dServers

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

To restart dServer:

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

Viewing dServer Properties

You can view dServer properties from the Navigation Window of the Avalanche MC Console. dServer 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 dServer properties:

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

Configuring Infrastructure dServers at dServer Locations

Although you manage much of your wireless network with the Avalanche MC Console, certain dServer Locations might require additional configuration or management. To accommodate this need, you can access the Mobile Manager Administrator. This tool allows you to fine-tune your wireless network by configuring your wireless network components and mobile device software at the dServer Location level.

Accessing Mobile Manager

You can access the Mobile Manager dServer Location tool in one of the following ways:

- Right-click a dServer Location in the Navigation Window and select **Launch dServer Console** from the menu that appears.

- Right-click a dServer Location in the map and select **Launch dServer Console** from the menu.

- Select a dServer Location; then select **Launch dServer Console** from the **Tools** menu.

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

Mobile Manager Management and the Avalanche MC Console

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

- IP addresses can be assigned either by the Avalanche MC Console or by Mobile Manager, but not both. Consequently, you must decide before you assign IP addresses if you want to manage them centrally or at the Mobile Manager level.

- WEP and WEP rotation settings assigned at the enterprise level will override any corresponding settings at the Mobile Manager level.

- The Avalanche MC Console is designed to apply configuration settings to groups of dServer Locations. To configure an individual dServer Location from the Avalanche MC Console, you can do so by creating a region that contains only that dServer Location and applying settings to that region.

Monitoring dServer Status

The **Distributed Server Status** tab provides information about a selected dServer. To view the status page, select a region, dServer Location or site in the Navigation Window and click 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 that the dServer is assigned to.

- **Location**. Lists the location (machine name) where the dServer resides.

- **Site Address**. Lists the IP address of the dServer Location.

- **Version**. Specifies the version of dServer deployed to the location.

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

🔴	Indicates the dServer is currently offline.
🟢	Indicates the dServer is currently online and running.

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

➡	Indicates changes have been made but are not yet deployed to the dServer.
✓	Indicates changes have been deployed but are not yet applied to the dServer.
☑	Indicates the dServer is up-to-date with the latest changes.

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

⬅	Indicates that the dServer is not currently in a blackout window.
➡	Indicates the dServer is currently in a blackout window and not available.

Chapter 7: Managing Network Profiles

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:

- Why Should I Create a Network Profile?
- Creating Network Profiles
- Editing Network Profiles
- Assigning Network Profiles
- Deleting Network Profiles
- Network Profile Configuration Descriptions

Why Should I Create a Network Profile?

A network profile is a configuration profile that you can apply to your wireless devices. Once the wireless devices is configured with the network values configured in the network profile, you can manage the devices through the Avalanche MC Console. If your wireless devices do not get the network values, you will not be able to manage them. Network profiles also allow you to configure multiple devices on your network at one time.

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 Navigation Window, select **Network Profiles**.
2. From the **Network Profiles** tab, click **Add Profile**.

   The *Input* dialog box appears.

3. Type the name of the new network profile in the text box and click **OK**.

   The new network profile appears in the **Network Profile List**. After creating a network profile, you must enable it in order to apply it to your devices.

Editing Network Profiles

Once you have created a network profile, you can edit the settings. This section presents specific tasks involved in configuring network profile settings. For a complete list of network profile settings, refer to *Network Profile Configuration Descriptions* on page 158. For information about assigning network profiles to a region, refer to *Assigning Network Profiles to Regions* on page 111.

This section provides information about editing the following:

- Configuring Network Profile General Settings
- Network Profile Selection Criteria
- Configuring Epoch Settings
- Wireless Settings

Configuring Network Profile General Settings

In the **General Settings** tab, you can edit the network profile name, status, IP address pools, and enable or disable the profile. For a list of general network profile settings, refer to *Network Profile General Settings* on page 158.

This section provides information about the following tasks:

- Enabling a Network Profile
- Managing IP Address Pools

Enabling a Network Profile

A network profile must be enabled, before you can assign that profile to regions. When the profile is deployed, the network settings are applied to mobile devices that match the selection criteria of that profile.

To enable a network profile:

1. From the **Network Profiles** tab, select the desired network profile from the **Network Profile List**.
2. Click **Add**.
3. In the **General Settings** tab, select the **Enabled** option to enable the profile.
4. Click **Save**.

   The network profile is enabled and can be assigned to any region in the console.

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.

The IP address pool can contain either static addresses or dynamic addresses with a Server address mask.

To add addresses to an IP address pool:

1. From the **Network Profiles** tab, select the desired network profile from the **Network Profile List**.
2. Click **Edit**.
3. In the **General Settings** tab, click **Edit IP Address Pools**.

   The *IP Address Pools* dialog box appears.

4 From the **Pool to Edit** drop-down list, select the IP address pool you wish to configure, either **Mobile Devices or Infrastructure**.

5 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)

6 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)

7 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

8 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 will display all entered addresses, including those already assigned.

9 Click **OK** to return to the **Network Profiles** tab.

10 Save your changes.

To delete addresses from an IP address pool:

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

2 Click **Save**.

3 In the **General Settings** tab, click **Edit IP Address Pools**.

The *IP Address Pools* dialog box appears.

4 From the **Pool to Edit** drop-down list, select the IP address pool you wish to edit.

5 Select the address(es) you wish to delete and click **Delete Selected**.

The *Confirm* dialog box appears, asking you to confirm the deletion.

6 Click **Yes** to delete the addresses.

The addresses are deleted from the list.

7 Click **OK** to return to the **Network Profiles** tab.

8 Save your changes.

Viewing Where Network Profiles Are Applied

The **Applied To** tab in the network profile page allows you to see exactly which regions, dServer 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 dServer Location Properties tabs and assign the profiles there. For information, refer to *Assigning Profiles to Regions* on page 107.

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, dServer Location or Site where the profile is applied.
- **Selection Criteria**. Any selection criteria that is applicable at the region, dServer Location or site where the profile is applied.

NOTE You do not need to enter Edit mode to view where profiles are applied.

To view:

1 In the Navigation Window, select **Network Profiles**.

2 From **Network Profile List**, select the network profile you want to see.

3 Click the **Applied To** tab.

The tab displays the information for the selected network profile.

Network 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 profiles. This means that any user assigned as an authorized user to a network profile will have all 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 85.

To add an authorized user:

1 In the **Network Profiles List**, select the desired profile.

2 Click **Edit**.

3 Select the **Authorized Users** tab and click **Add User**.

The *Add Authorized User* dialog box appears.

4 From the user list, select the user.

5 From the drop-down list, select the permission level for the user.

6 Click **OK**.

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

Network Profile Selection Criteria

Selection criteria allow you to specify which devices the network profile manages. There are three types of selection criteria: mobile device, infrastructure, and dynamic. Mobile device criteria define which mobile devices are managed by the profile, and infrastructure criteria define which infrastructure devices are managed. Dynamic selection criteria are defined by Avalanche MC and apply to a device’s encryption and authentication support.

For detailed information about creating selection criteria, refer to *Chapter 18: Selection Criteria* on page 317.

Configuring Epoch Settings

Epochs allow you to change the settings for a network profile and apply those changes at a specific time. An Epoch is created for each new network profile, and there is a maximum of 50 Epochs per network profile. Most network profile settings can be managed by Epochs.

The **Epochs** region has two tabs: the **Network Settings** tab and the **Wireless Settings** tab. The **Network Settings** tab allows you to set the IP addresses of the devices managed and provides other IP addresses that the devices might need. The **Wireless Settings** tab allows you to establish the SSID, encryption, and authentication settings for managed devices.

For a list of all available settings for an Epoch, refer to *Epochs Configuration Settings* on page 159.

This section provides information about the following tasks:

- Creating Epochs
- Editing Epoch
- Deleting Epochs
- Deploying Epochs

Creating Epochs

Epochs allow you to change a network profile and apply those changes to the mobile devices configured with that network profile at a specific time. If you wish to schedule only minor changes to a network profile that already exists, Avalanche MC provides the ability to clone an Epoch and then make modifications.

To create Epochs:

1 Select the network profile and click **Edit**.

1 Ensure you have enabled the **Manage Network Settings** checkbox in the **General Settings** tab.

2 In the **Epochs** region, click **Add Epoch.**

-Or-

From the **Network Profiles** tab, select the Epoch you want to clone and click **Clone Epoch**.

The *Select a date and time* dialog box appears.

3 Select the day and time you want the new settings to take effect.

4 Click **OK**.

The new Epoch date and time will appear in the drop-down list in the **Epochs** region.

5 Edit the network settings as desired.

6 Save your changes

The Epoch is saved and the network settings will be applied to the mobile devices at the specified date and time.

Editing Epoch

If you decide to change an Epoch's settings or apply the settings at a different time, you can edit the Epoch.

To edit Epochs:

1 Ensure you are in **Edit Mode**.

2 Select the Epoch from the drop-down list in the **Epochs** region.

3 Click **Edit Epoch**.

The *Select a date and time* dialog box appears.

4 Select the day and time you want the new settings to take effect.

5 Click **OK**.

6 Make any other desired changes to the network profile settings.

7 Save your changes.

The Epoch is saved and the network settings will be applied at the specified date and time.

Deleting Epochs

If an Epoch is no longer useful, you can delete it.

To delete Epochs:

1. Ensure you are in Edit Mode.
2. From the **Epochs** region in the **Network Profiles** tab, select the Epoch to be deleted from the drop-down list.
3. Click **Remove Epoch**.

   The Epoch is deleted.

Deploying Epochs

Any time the settings in the **Epoch** region are changed, those changes must be deployed to your mobile devices. For information about how to deploy a network profile, refer to *Deploying Universal Updates* on page 334.

Wireless Settings

Avalanche MC provides four encryption methods: WEP keys, automatic WEP key rotation, WPA (TKIP), and WPA2 (CCMP) to keep your network secure. In addition, there are authentication types available depending on which encryption method you select.

For a list of available settings in the **Wireless Settings** tab, refer to *Wireless Settings Tab* on page 162.

This section provides information about the following:

- Encryption Methods
- Authentication Methods
- Configuring WEP Keys
- Configuring WEP Key Rotation

Encryption Methods

There are four types of encryption available in Avalanche MC. To use any of the encryption methods, you must have an Enabler that supports that type of encryption. Contact Wavelink Customer obtain an enabler that supports encryption.

WEP. WEP, or Wired Equivalent Privacy, is a protocol for encrypting wireless network communications. You secure your wireless network by creating either a 40- or 128-bit WEP 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.

WEP key rotation. WEP key rotation employs four keys which are automatically rotated at specified intervals. These keys are known by both infrastructure and mobile devices. 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 is different from 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 Infrastructure dServer becomes unavailable (for example, due to a hardware crash), you must re-connect serially to each mobile device to ensure that WEP key settings are correctly synchronized.

WPA. 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. 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 CBC-MAC Protocol) instead of TKIP. WPA2 availability is dependent on some hardware types.

Authentication Methods

Avalanche MC supports Extensible Authentication Protocol (EAP) to ensure network security. There are five types of EAP and a pre-shared key option to configure. The availability of EAP authentication is dependent on hardware types. You also must have an Enabler on the mobile device that supports authentication. Contact Wavelink Customer Service to obtain an Enabler that supports authentication.

LEAP. (Lightweight Extensible Authentication Protocol) LEAP is available when you do not already have an encryption method selected. LEAP requires both client and server to authenticate and then creates a dynamic WEP key.

PEAP/MS-CHAPv2. (Protected Extensible Authentication Protocol combined with Microsoft Challenge Authentication Handshake 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. (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling) EAP-Fast is available when you are using encryption. EAP-Fast uses protected access credentials and optional certificates to establish a Transport Layer Security tunnel.

TTLS. (Tunneled Transport Layer Security) TTLS is available when you are using encryption. 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.

Configuring WEP Keys

WEP keys are set manually and then distributed to the devices managed by the network profile.

NOTE Avalanche MC only tracks the WEP keys that were assigned to devices through the Avalanche MC 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 MC.

To configure WEP keys:

1 Select the network profile and click **Edit**.

1 Ensure you have enabled the **Manage Wireless Settings** check box in the **General Settings tab**.

2 In the **Wireless Settings** tab, select **WEP** from the **Encryption** drop-down list.

3 If you want to display the encryption passwords, click **Show Password**. If you do not click **Show Password**, the passwords will remain hidden.

NOTE Once you navigate out of network profiles, save changes or cancel changes, the passwords will be hidden.

---

4 Select either the **40 bit** or **128 bit** option in the **Encryption Settings** region.

5 Select one of the four default keys and enter a key.

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.

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

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

---

6 Save your changes.

Configuring WEP Key Rotation

You can configure WEP key rotation for a network profile. When the profile is deployed the mobile devices receive those settings.

To configure WEP key rotation:

1 Select the network profile and click **Edit**.

1 Ensure you have enabled the **Manage Wireless Settings** check box in the **General Settings tab**.

2 In the **Wireless Settings** tab, select **WEP Key Rotation** from the **Encryption** drop-down list.

3 If you want to display the encryption passwords, click **Show Password**. If you do not click **Show Password**, the passwords will remain hidden.

NOTE Once you navigate out of network profiles, save changes or cancel changes, the passwords will be hidden.

---

4 Click on the **Settings** button that appears.

The *Automatic WEP Settings* dialog box appears.

5 Select the encryption algorithm type from the **Encryption Algorithm** drop-down list.

6 Use one of the following methods to select the date you want WEP key rotation to begin.

- Type the date in MM/DD/YYYY format in the **Start Date/Time** text box.

-Or-

- Click the **Calendar** button and select the starting date from the calendar.

7 Select the time you want WEP key rotation to begin from the **Start Date/Time** drop-down list.

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

The value in this text box determines how often Avalanche MC rotates and replaces WEP keys. For example, if you type `15` in this text box and select **Minutes** from the drop-down list, WEP keys are rotated for each infrastructure every 15 minutes and an existing WEP key is replaced by a newly-generated one.

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

---

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

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

10 Click **OK**.

The WEP key rotation settings appears in the **Encryption Settings** region.

11 Save your changes.

Your security settings are saved to the network profile and will be applied to mobile devices the next time you deploy the network profile.

Assigning 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 MC console. If you have not already created a network profile, you will need to create one. For information about creating network profiles, refer to *Creating Network Profiles* on page 144. Once you assign an network profile to a region, you must perform a Universal Deployment to update your Servers. For more information the Universal Deployment, refer to *Deploying Universal Updates* on page 334.

To assign a network profile:

1 From the Navigation Window, select the region or dServer location to which you want to assign a network profile.

2 Click the **Region Properties** tab or the **dServer Location** tab, based on the you selection in the Navigation Window.

3 Select the **Network Profiles** tab and click **Edit**.

4 Click **Add**.

The *Add Network Profile Application* dialog box appears.

5 From the list of available network profiles, select which profile you want to assign to this region.

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

6 If you to configure selection criteria for the profile, click the selection criteria button and use the Selection Criteria Builder to build the selection criteria for this network profile.

NOTE For information about building selection criteria, refer to *Building Selection Criteria* on page 318.

7 Click **OK**.

The profile is added to the **Network Profiles** tab for the region.

8 Continue adding network profiles to the region or dServer Location.

9 Use the **Move Up** and **Move Down** buttons to assign the order in which the Network profiles are applied to mobile devices.

10 Save your changes.

The assigned profile will be deployed to the dServers when you install the Servers or when you perform a Universal Deployment. For information about installing Servers, refer to *Deploying dServers* on page 331. For information about performing a Universal Deployment, refer to *Deploying Universal Updates* on page 334.

Deleting Network Profiles

If a network profile is no longer needed, you can delete it from the Avalanche MC Console. The devices to which the profile was applied will retain the assigned properties until another profile is applied.

To delete a network profile:

1 From the **Network Profiles** tab, select the network profile to be deleted from the **Network Profile List**.

2 Click **Remove Profile**.

The *Confirm Delete Network Profile* dialog box appears.

3 Click **Yes** to delete the profile.

The profile is deleted.

Network Profile Configuration Descriptions

This section provides information about the network profile settings available in each region of the **Network Profiles** tab. This information includes descriptions of each option in the following regions:

- Network Profile General Settings
- Selection Criteria Settings
- Epochs Configuration Settings

Network Profile General Settings

The following table provides information about the network 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.
IP Address Pools	Enables configuration of the IP address pools.
Manage Network Settings	Enables network settings management.
Manage Wireless Settings	Enables wireless settings management.
Override Manual Settings on Mobile Devices	Enables the profile to override the manual settings on mobile devices.

Table 7-1: *General Settings*

For more information about IP address pools, refer to *Managing IP Address Pools* on page 145.

Selection Criteria Settings

The following table provides information about the network profile settings in the **Selection Criteria** tabs.

Field	Description
Mobile Device Selection Criteria	Defines which mobile devices the profile will manage.
Dynamic Selection Criteria	Defines the type of encryption a device must support in order to be managed by the network profile. These criteria cannot be configured by the user.

Table 7-2: *Selection Criteria*

For information about creating selection criteria, refer to *Building Selection Criteria* on page 318.

Epochs Configuration Settings

There are two tabs in the **Epochs** region: the **Network Settings** tab and the **Wireless Settings** tab. To edit the options in these tabs, the corresponding checkbox in the **General Settings** tab must be enabled.

This section provides information about the settings in the following tabs:

- Network Settings Tab

- Wireless Settings Tab

For information about creating, editing, and deleting Epochs, refer to *Configuring Epoch Settings* on page 149.

Network Settings Tab

The following table provides information about the settings available in the **Network Settings** tab in the **Epochs** region.

Field	Description
IP Address Assignment Region	

Table 7-3: *Network Settings Tab*

Infrastructure	Sets the method by which IP addresses are assigned to infrastructure devices. **Manual Assignment.** The IP address is manually configured from the device. **IP Address Pool.** An infrastructure is assigned an IP address from an IP address pool. For information on creating an IP address pool, refer to *Managing IP Address Pools* on page 145. **DHCP Server.** An infrastructure is assigned an IP address by a DHCP server.
Mobile Devices	Sets the method by which IP addresses are assigned to mobile devices. **Manual Assignment.** The IP address is manually configured from the device. **IP Address Pool.** A mobile device is assigned an IP address from an IP address pool. For information on creating an IP address pool, refer to *Managing IP Address Pools* on page 145. **DHCP Server.** A mobile device is assigned an IP address by a DHCP server.
Infrastructure Settings Region	
Gateway Address	Provides wireless devices with the gateway address. The gateway address is the address for the node that handles traffic with devices outside the subnet.
Subnet Mask	Provides wireless devices with the subnet mask. The subnet mask determines whether a packet's destination is on the subnet.
Mobile Device Settings Region	
Server Address	Provides mobile devices with the server address. You can either provide the address or use the dServer Location value.
Use dServer Location Value	Sets the mobile device to use the mask/address value of the dServer Location to which the mobile devices connects
Gateway Address	Provides mobile devices with the gateway address.You can either provide the address or use the dServer Location value. The gateway address is the address for the node that handles traffic with devices outside the subnet.

Table 7-3: *Network Settings Tab*

Subnet Mask	Provides mobile devices with the subnet mask. You can either provide the address or use the dServer Location value. The subnet mask determines whether a packet's destination is on the subnet.
Domain Name System (DNS)	Enables a mobile device to access a DNS. A Domain Name System translates hostnames/domain names to IP addresses.
Domain Name	Provides mobile devices with the name of the domain where they reside.
Primary DNS	Provides mobile devices with the IP address for a primary DNS.
Secondary DNS	Provides mobile devices with the IP address for a secondary DNS (used if the primary DNS is unavailable).
Tertiary DNS	Provides mobile devices with the IP address for a tertiary DNS (used if the primary and secondary DNS are unavailable).

Table 7-3: *Network Settings Tab*

Wireless Settings Tab

The following table provides information about the settings available in the **Network Settings** tab in the **Epochs** region.

Field	Description
SSID	Provides wireless devices with the SSID. The SSID is a service set identifier that only allows communication with devices sharing the same SSID.
Encryption	Sets the type of encryption used. The following options are available from the encryption drop-down list: **Use Profile/None.** Devices do not encrypt information. **WEP.** Wired Equivalent Privacy uses either a 40- or 128-bit WEP key which is distributed to your devices. **WEP Key Rotation.** WEP key rotation employs four keys which are automatically rotated at specified intervals. **WPA (TKIP).** Wi-Fi Protected Access uses Temporal Key Integrity Protocol (TKIP) to encrypt information and change the encryption keys as the system is used. **WPA2 (CCMP).** WPA2 meets higher standards for encryption by using CCMP (Counter mode CBC-MAC Protocol) instead of TKIP. For more information about the types of encryption available with Avalanche MC, refer to *Encryption Methods* on page 151.
Encryption Settings Region	The options in this region are based on the encryption type you selected from the Encryption drop-down list.

Table 7-4: *Wireless Settings Tab*

Field	Description
Authentication	Sets the type of authentication used. The options in this drop-down are based on the encryption type you selected in the Encryption drop-down list. Not all options will appear for each selection. **None.** No authentication type is used. **LEAP.** Lightweight Extensible Authentication Protocol is available when you do not already have an encryption method selected. **EAP.** Extensible Authentication Protocol is available when you have selected an encryption method. **Pre-Shared Key (PSK).** PSK is available when you have selected an encryption method. For more information about the types of authentication available with Avalanche MC, refer to *Authentication Methods* on page 152.

Table 7-4: *Wireless Settings Tab*

Field	Description
EAP Authentication The EAP options are only available when you select WEP, WPA (TKIP) or WPA (CCMP) from the **Encryption** drop-down list.	
EAP Type	Sets the type of EAP authentication used. **PEAP/MS-CHAPv2.** Protected Extensible Authentication Protocol combined with Microsoft Challenge Authentication Handshake Protocol uses a public key certificate to establish a Transport Layer Security tunnel. **PEAP/GTC.** Protected Extensible Authentication Protocol with Generic Token Card is similar to PEAP/MS-CHAPv2, but uses an inner authentication protocol instead of MS-CHAP. **EAP-FAST.** Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling uses protected access credentials and optional certificates to establish a Transport Layer Security tunnel. **TTLS.** Tunneled Transport Layer Security uses public key infrastructure certificates (only on the server) to establish a Transport Layer Security tunnel. For more information about the types of authentication available with Avalanche MC, refer to *Authentication Methods* on page 152.
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.
Username	Sets the username for EAP credential authentication
Password	Sets the password for EAP credential authentication
Confirm	Confirms the password set for EAP credential authentication
Domain	Sets the domain name for EAP credential authentication
Include Windows logon domain with username	Includes the Windows logon domain with a username when using EAP credential authentication. This prevents authentication if the Windows logon has changed, even if the username is correct.

Table 7-4: *Wireless Settings Tab*

Field	Description
Pre-Shared Key (PSK) Authentication The PSK options are only available when you select WPA (TKIP) or WPA (CCMP) from the **Encryption** drop-down list.	
Use a 8-63 character pass phrase	Sets the PSK type as a pass phrase
Use a 64 character (256 Bit) hex key	Sets the PSK type as a hex key
(pre-shared key text box)	Sets the pre-shared key
Broadcast Key Rotation Interval	Sets the time interval at which the key is broadcast
LEAP Authentication The LEAP options are only available when you select WEP, WPA (TKIP) or WPA (CCMP) from the **Encryption** drop-down list.	
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.
Username	Sets the username for EAP credential authentication
Password	Sets the password for EAP credential authentication
Confirm	Confirms the password set for EAP credential authentication
Domain	Sets the domain name for EAP credential authentication
Include Windows logon domain with username	Includes the Windows logon domain with a username when using EAP credential authentication. This prevents authentication if the Windows logon has changed, even if the username is correct.

Table 7-4: *Wireless Settings Tab*

For information about configuring WEP, refer to *Configuring WEP Keys* on page 153. For information about configuring WEP key rotation, refer to *Configuring WEP Key Rotation* on page 154.

Chapter 8: Managing Infrastructure Distributed Servers

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

NOTE In early versions of Avalanche MC, Distributed Servers (or dServers) were referred to as Agents in both the user interface of the Avalanche MC 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 MC 4.1 release, Agents are referred to as dServers both in the user interface and the documentation. The Mobile Device Agent, is the Mobile Device dServer. The Access Point Agent is the Infrastructure dServer.

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

This section provides information about the following tasks:

- Creating Infrastructure dServer Profiles
- Configuring Infrastructure dServer General Settings
- Defining Device Access Privileges
- Configuring Enterprise Server Connections for Infrastructure dServer Profiles
- Applying Infrastructure dServer Profiles to Regions
- Viewing Infrastructure dServer Licensing Messages

Creating Infrastructure dServer Profiles

You can create as many Infrastructure dServer profiles as are necessary to manage your system.

To create Infrastructure dServer profiles:

1 From the Navigation Window, select **Infrastructure dServer Profile**.

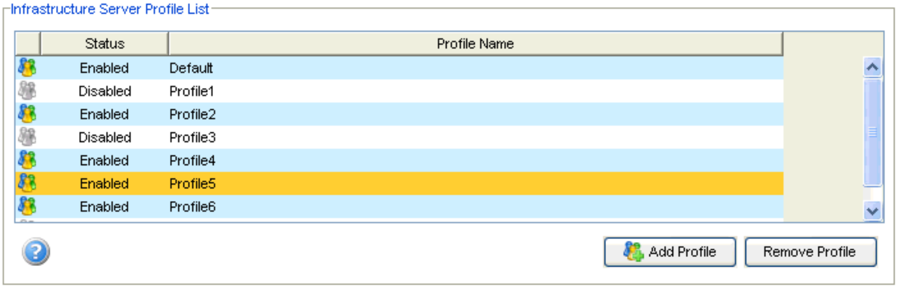
The **Infrastructure dServer Profiles** tab appears.

2 In the **Infrastructure dServer Profile List** region, click **Add Profile**.

The *Input* dialog box appears.

3 Enter the name of the profile and click **OK**.

The new profile appears in the **Infrastructure Profile List**.



Status	Profile Name
Enabled	Default
Disabled	Profile1
Enabled	Profile2
Disabled	Profile3
Enabled	Profile4
Enabled	Profile5
Enabled	Profile6

Figure 8-1. *Infrastructure Profile List*

Configuring Infrastructure dServer General Settings

You can set the Infrastructure dServer Profile status to enabled or disabled. Before you can assign the profile to a region, you must enable it.

You can also select to suppress radio statistics from the Infrastructure dServer. This will prevent any data from being written to the radio statistics table in the database. This helps control the amount of information that the Enterprise Server stores. Consider how much data is being collected, how often the Enterprise Server removes the statistics, and the impact across your bandwidth. This will ensure an educated decision on which options to enable.

To enable Infrastructure dServer profiles:

1 From the **Infrastructure dServer Profile List**, select the profile you want to enable.

2 Click **Edit**.

3 In the **General Settings** tab, enable the **Enabled** option.

4 If you want to restrain radio statistic collection, enable **Suppress Radio Statistic Data Collection**.

5 Save your changes.

You can now assign the profile to any region in the console.

Viewing Where Infrastructure dServer Profiles Are Applied

The **Applied To** tab in the network profile page allows you to see exactly which regions, dServer 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 dServer Location Properties tabs and assign the profiles there. For information, refer to *Assigning Profiles to Regions* on page 107.

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, dServer Location or Site where the profile is applied.

- **Selection Criteria**. Any selection criteria that is applicable at the region, dServer Location or site where the profile is applied.

To view:

1 In the Navigation Window, select **Infrastructure Profiles**.

2 From **Infrastructure Profile List**, select the network profile you want to see.

3 Click the **Applied To** tab.

The tab displays the information for the selected network profile.

Infrastructure dServer 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 an Infrastructure Profile will have all 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 85.

To add an authorized user:

1 In the **Infrastructure Profiles List**, select the desired profile.

2 Click **Edit**.

3 Select the **Authorized Users** tab and click **Add User**.

The *Select Software Profile Admin User* dialog box appears.

4 From the list, select the user.

5 Click **OK**.

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

Removing Infrastructure dServer Profile Authorized Users

If you do not want a user to have administrative privileges for a software profile, you can remove that user from the authorized user list. The user will continue to have Normal permissions, but will not longer be able to access or modify the software profile.

To remove an authorized user:

1 From the **Authorized Users** tab, select the desired user.

2 Click **Remove User**.

The user is removed from the **Authorized Users** list for the profile.

Defining Device Access Privileges

To manage wireless network components—including access points, switches, and routers—a dServer 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 dServer uses to configure the component. The types of authorizations are as follows:

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

The authorization required varies depending on the type of hardware being queried by the infrastructure. Frequently, a component requires more than one authorization type—for example, a dServer might need both an HTTP user name and an SNMP Read/Write name to correctly configure an infrastructure. 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 Telnet password HTTP user name and password
Symbol Access Point	SNMP Read/Write Community Name SNMP Read-Only Community Name HTTP user name and password
Symbol Wireless Switches	SNMP Read/Write Community Name SNMP Read-Only Community Name Telnet password

Table 8-1: *Authorization Required for Component Queries*

Hardware	Authorization
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 8-1: *Authorization Required for Component Queries*

NOTE If you find that a dServer 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 dServer 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, it moves through the list of SNMP Read/Write community names until it finds one the infrastructure will accept. If all attempts to communicate with an infrastructure fail, the dServer will generate an alert.

NOTE To apply new device access privileges to a region, you must send the information to the Servers within that region. See *Deploying Universal Updates* on page 292 for more information.

To define device access privileges:

1 In the **Infrastructure dServer Profile List**, select the profile for which you are defining privileges.

If there are no Infrastructure dServer profiles available, you will have to create one. Refer to *Creating Infrastructure dServer Profiles* on page 168 for more details.

2 Click **Edit**.

3 In the **Device Access Privileges** tab, 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 account, 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 MC 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.

4 If you want to display the names and passwords, click **Show Password**. If you do not click **Show Password**, the passwords will remain hidden.

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

5 Save your changes.

Cisco IOS Access Privileges

To manage Cisco IOS Access Points with the Avalanche MC 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.

For Cisco Access Points that use IOS, the following information is also required to authorize the Infrastructure dServer to manage the infrastructure:

- Telnet community name and password

- Telnet Enable password

By default, the Telnet user name, password, and Enable password for Cisco IOS Access Points is “Cisco”. If you enabled security for managing infrastructure devices with Avalanche MC, this default Telnet information is removed to prevent unauthorized use of the infrastructure.

Avalanche MC 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 Avalanche MC with security disabled, Avalanche MC will add a public SNMP Read/Write user. If you installed Avalanche MC with security enabled, Avalanche MC will add a SNMP Read/Write user with the same value as the Telnet user name. Avalanche MC 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 MC 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 MC 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 MC 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 **Infrastructure dServer Profile List**, select the profile for which you are defining privileges.

If there are no Infrastructure dServer Profiles available, you will have to create one. Refer to *Creating Infrastructure dServer Profiles* on page 168 for more details.

2 Click **Edit**.

3 In the **Device Access Privileges** region, configure the privileges for the profile.

- If you modified the Cisco IOS infrastructure so that its Telnet Enable password is not "Cisco," select the **Telnet** tab. Enter the Telnet Enable password that Avalanche MC 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.

Configuring Enterprise Server Connections for Infrastructure dServer Profiles

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

The **Enterprise Server Connection** tab allows you to create blackout windows and provides a weekly and daily view so you can see all the blackout windows scheduled to occur. The weekly view displays when each blackout occurs for that week. The daily view shows you exactly what time the blackout will occur.

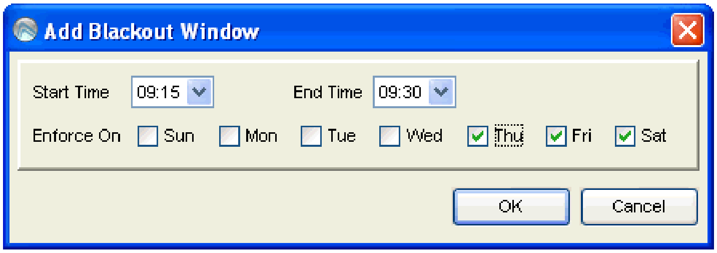
To configure Enterprise Server Connections:

1 In the **Infrastructure dServer Profile List**, select the profile for which you are defining privileges.

2 Click **Edit**.

3 In the **Enterprise Server Connection** tab, click **Add Blackout** window.

The *Add Blackout Window* dialog box appears.



Add Blackout Window

Start Time 09:15

End Time 09:30

Enforce On □ Sun □ Mon □ Tue □ Wed ☑ Thu ☑ Fri ☑ Sat

Figure 8-2. *Add Blackout Window*

4 Using the **Start Time** and **End Time** drop-down lists, 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 **Daily View** and **Weekly View** regions are updated with your new configurations.

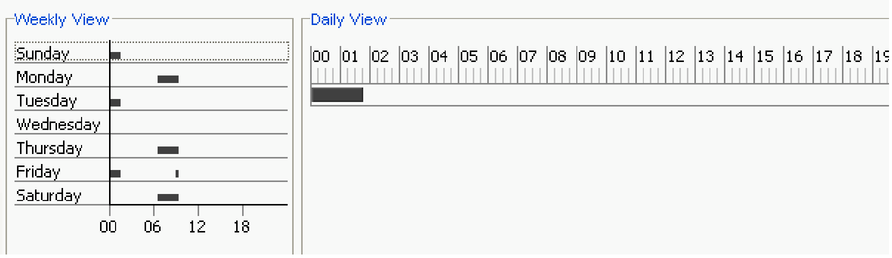


Figure 9. *Weekly and Daily Blackout Windows*

7 You can modify the blackout window by selecting the day of the week from the Weekly View. Click and drag the Daily View marker to indicate the desired time of the blackout.

8 Save the profile.

Applying Infrastructure dServer Profiles to Regions

Once you have created an Infrastructure dServer Profile, you can assign it to any region in your enterprise. You can then install the server at dServer locations within that region and deploy settings to that server. For more information about applying an Infrastructure dServer Profile to a region, refer to *Assigning Infrastructure Profiles to Regions* on page 108. For more information about installing servers and deploying server settings, refer to *Deploying dServers* on page 331.

Removing Infrastructure dServer Profiles

If you no longer are using an Infrastructure dServer profile, you can remove it from the console. When you remove an Infrastructure dServer 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 Infrastructure dServer profiles:

1 In the **Infrastructure dServer Profile List**, select the profile you want to delete 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 dServer Licensing Messages

The Avalanche MC Console receives messaging licenses from the deployed Infrastructure dServers. You can view these messages from the *dServer Licensing Messages* dialog box. This dialog box provides information about the dServer Location where the Server resides and the licensing message.

To view licensing messages:

1 From the **Tools** menu, select **dServer License Messages**.

The *dServer Licensing Messages* dialog box appears.

2 Click the **dServer Location** column to list the messages by dServer Location.

3 Click the **dServer** column to list the messages by dServer.

Chapter 9: Managing Mobile Device Distributed Servers

The Mobile Device dServer is server software that lets you remotely manage and configure mobile devices. Although you can use multiple dServers at different dServer Locations or on different network segments, you can manage all of your dServers from one Management Console—regardless of where the console resides on the network.

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

Avalanche MC allows you to manage the following software and network settings of the mobile devices operating on the network:

- **Administration Settings**. These settings include licensing, user files and terminal ID generation settings. Licenses for mobile devices are frequently redistributed, providing a great deal of flexibility in managing licenses. Within the Avalanche MC Console, these settings focus on when mobile device licenses are released from an inactive mobile device, allowing that license to move to a new device.

- **Connections**. Because mobile devices are frequently connected to cradles when they are not in use, Mobile Device dServers use COM ports to automatically detect and manage cradled mobile devices. These settings allow you to decide which COM ports Mobile Device dServers are allowed to use.

- **Security**. Avalanche MC includes several different authentication methods to prevent unauthorized mobile devices from accessing your network.

- **Scheduling Settings**. These settings include assigning times when the mobile devices should update and setting restrictions as to when the mobile devices should not update.

This section provides information about the following tasks:

- Creating Mobile Device dServer Profiles
- Enabling Mobile Device dServer Profiles
- Configuring Mobile Device dServer Log Files
- Managing Administration Tasks
- Configuring Device Connections
- Enabling Secondary Server Support
- Configuring Server Updates
- Removing Mobile Device dServer Profiles
- Assigning Mobile Device dServers to Regions
- Viewing Mobile Device dServer Licensing Messages

Creating Mobile Device dServer Profiles

Create Mobile Device dServer Profiles to manage your Mobile Device dServers. Profiles allow you to configure logging, device connections, secondary server support, updates and other settings for the dServer.

To add a Mobile Device dServer profile:

1. From the Navigation Window, select **Mobile Device dServer Profiles**.

   The **Mobile Device dServer Profiles** tab appears.

2. In the **Mobile Device dServer Profile List** region, click **Add Profile**.

   The *Input* dialog box appears.

3. Type the name of the Mobile Device dServer Profile and click **OK**.

   The profile is added to the **Mobile Device dServer Profile List**.

4. Save your changes.

Configuring Mobile Device dServer General Settings

Perform the following tasks from the General Settings tab:

- Enabling Mobile Device dServer Profiles
- Configuring Mobile Device dServer Log Files
- Suppressing Mobile Device dServer Statistics
- Configuring User Files

Enabling Mobile Device dServer Profiles

Before you can apply a Mobile Device dServer profile to any region, you must enable that profile.

To enable a Mobile Device dServer profile:

1. From the **Mobile Device dServer Profiles List**, select the profile you want to enable.
2. Click **Edit**.
3. In the **General Settings** tab, select the **Enabled** option.
4. Save your changes.

   The Mobile Device dServer profile is now enabled and you can assign it to any region in the Avalanche MC Console.

Configuring Mobile Device dServer Log Files

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

The log for the Mobile Device dServer is stored as a text file in the `Wavelink\AvalancheMC\` subdirectory. (The default Avalanche installation path is `c:\Program Files\Wavelink\AvalancheMC`.)

You can set the log level to the following states:

- **Critical**. This level writes the least information to the log file, reporting only critical errors that have caused the Mobile Device dServer service 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 default logging level and the Wavelink-recommended setting. 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 more serious 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.

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

To configure logging settings:

1. From the **Mobile Device dServer Profiles List**, select the profile you want to configure.
2. Click **Edit**.
3. From the **Logging Sensitivity** drop-down list, select the logging level you want Avalanche MC 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. Save your changes.

Suppressing Mobile Device dServer Statistics

You can select to suppress both radio statistics and software profile data collection for the Mobile Device dServer. This will prevent any data from being written to the software profile data table and radio statistics table in the database. This helps control the amount of information that the Enterprise Server stores. You do not have to suppress both sets of statistics. Consider how much data is being collected, how often the Enterprise Server removes the statistics, and the impact of the data across your bandwidth. This will ensure an educated decision on which options to enable.

To suppress statistics:

1 From the **Mobile Device dServer Profiles List**, select the profile you want to configure.

2 Click **Edit**.

3 In the **General Settings** tab, enable **Suppress Radio Statistic Data Collection** and enable **Suppress Software Profile Data Collection**.

4 Click **Save**.

Configuring User Files

The User Files setting establishes the directory path that Mobile Device Server uses to store retrievable user files. The path will be relative to the server installation location unless an absolute path is specified, beginning with a slash (/).

To configure the user files path:

1 From the **Mobile Device Server Profiles List**, select the profile you want to configure.

2 Click **Edit**.

3 Click the **Administration** tab.

4 In the **User Files** region, enter the file path name where you want to store retrievable files.

5 Save your changes.

Servers are updated during the next deployment.

Viewing Where Mobile Device dServer Profiles Are Applied

The **Applied To** tab in the network profile page allows you to see exactly which regions, dServer 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 dServer Location Properties tabs and assign the profiles there. For information, refer to *Assigning Profiles to Regions* on page 107.

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, dServer Location or Site where the profile is applied.
- **Selection Criteria**. Any selection criteria that is applicable at the region, dServer Location or site where the profile is applied.

To view:

1. In the Navigation Window, select **Mobile Device Server Profiles**.
2. From **Mobile Device Server Profile List**, select the network profile you want to see.
3. Click the **Applied To** tab.

   The tab displays the information for the selected network profile.

Mobile Device dServer 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 profiles. This means that any user assigned as an authorized user to a profile will have all 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 85.

To add an authorized user:

1. In the **Mobile Device dServer Profiles List**, select the desired profile.
2. Click **Edit**.
3. Select the **Authorized Users** tab and click **Add User**.

   The *Add Authorized User* dialog box appears.
4. From the user list, select the user.
5. From the drop-down list, select the permission level for the user.
6. Click **OK**.

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

Managing Administration Tasks

You can managing the following Mobile Device dServer Profile administration tasks from the **Administration** tab of the **Mobile Device dServer Profile** tab:

- Releasing Licenses
- Setting the Terminal ID

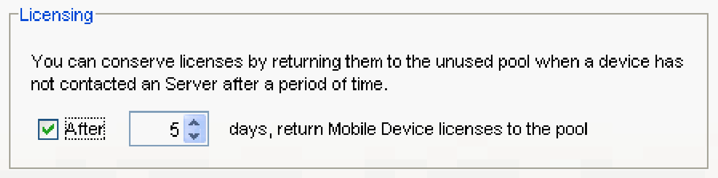
Releasing Licenses

You can conserve licenses by returning them to the unused pool when a device has not contacted a server after a period of time. You can configure the period of time which must elapse before the license is released. The minimum number of days is five.

To configure license release:

1. From the **Mobile Device dServer Profiles List**, select the profile you want to configure.
2. Click **Edit**.
3. Click the **Device Administration** tab.

4 In the **Licensing** region, enable the **After** option and enter the number of days after which the license should be returned.



Licensing

You can conserve licenses by returning them to the unused pool when a device has not contacted an Server after a period of time.

☑ After 5 days, return Mobile Device licenses to the pool

Figure 9-1. *Licensing*

5 Save your changes.

dServers are updated during the next deployment.

Setting the Terminal ID

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

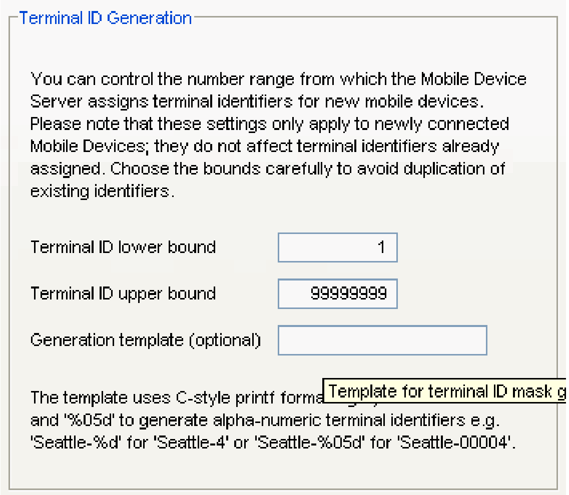
To configure the terminal ID settings:

1 From the **Mobile Device dServer Profiles List**, select the profile you want to configure.

2 Click **Edit**.

3 Click the **Device Administration** tab.

4 In the **Terminal ID Generation** region, configure the lower and upper limits for the range of terminal IDs that the Mobile Device dServer will assign to mobile devices.



Terminal ID Generation

You can control the number range from which the Mobile Device Server assigns terminal identifiers for new mobile devices. Please note that these settings only apply to newly connected Mobile Devices; they do not affect terminal identifiers already assigned. Choose the bounds carefully to avoid duplication of existing identifiers.

Terminal ID lower bound: 1

Terminal ID upper bound: 99999999

Generation template (optional):

The template uses C-style printf forma Template for terminal ID mask g
and '%05d' to generate alpha-numeric terminal identifiers e.g. 'Seattle-%d' for 'Seattle-4' or 'Seattle-%05d' for 'Seattle-00004'.

Figure 9-2. *Terminal ID Generation*

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

Terminal ID lower bound: Specify the lowest terminal ID that the Mobile Device dServer will assign a mobile device.

Terminal ID upper bound: Specify the highest terminal ID that the Mobile Device dServer will assign a mobile device.

Generation template (optional): Use a C-style format to allow the Mobile Device dServer to assign alphanumeric IDs.

Examples:

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

5 Save your changes.

dServers are updated during the next deployment.

Configuring Device Connections

This section provides information about configure the mobile devices including:

- Setting COM Ports
- Enabling the RAPI Gateway
- Configuring Connection Settings
- Enabling Device Caching
- Enabling Encryption
- Enabling Authentication

Setting COM Ports

Mobile devices that are new to the network cannot be configured via wireless connection; instead, they must be initially configured when they are physically connected to the network through a cradle. You can configure Mobile Device dServers to automatically listen for mobile devices using the COM ports on the remote system.

Only one application on a host system can maintain ownership of a COM port. If the Mobile Device dServer controls the COM ports on the host system, then no other application will be able to use them. Likewise, if another application on the host system (for example, Microsoft ActiveSync) has control of the COM ports, then the Mobile Device dServer will not be able to use them.

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

NOTE Settings for COM ports are configured on a per-region basis.

To establish COM port settings:

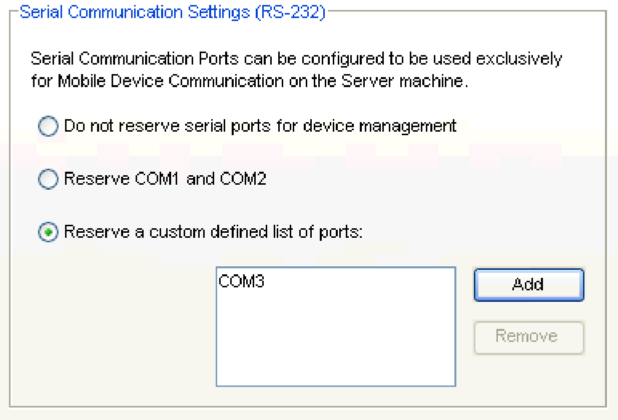
1 From the **Mobile Device dServer Profiles List**, select the profile you want to configure.

2 Click **Edit**.

3 Click the **Device Connections** tab.

4 In the **Serial Communication Settings (RS232)** region, configure the serial port options.

- Select the **Do not reserve serial ports for device management** if you do not need serial ports to manage your mobile devices.
- Select **Reserve COM1 and COM2** to reserve those two ports for Mobile Device communication on the Servers.
- Select **Reserve a custom defined list of ports** and click **Add** to specify which ports you want to use to manage your mobile devices.



Serial Communication Settings (RS-232)

Serial Communication Ports can be configured to be used exclusively for Mobile Device Communication on the Server machine.

○ Do not reserve serial ports for device management

○ Reserve COM1 and COM2

● Reserve a custom defined list of ports:

COM3

Figure 9-3. *COM Ports*

5 Save your changes.

dServers are updated during the next deployment.

Enabling the RAPI Gateway

Avalanche MC allows you to use Microsoft ActiveSync connections that exist on the system that hosts the Mobile Device dServer. Avalanche MC can automatically detect these connections and create a gateway that allows you to use the connection to facilitate Avalanche communication between the Mobile Device dServer and a mobile device. The communication medium over which the ActiveSync session has been established does not matter; the communication medium can be serial, USB, IrDA, or RF.

To enable the RAPI gateway:

1. From the **Mobile Device dServer Profiles List**, select the profile you want to configure.

2. Click **Edit**.

3. In the **Device Connections** tab, enable the **Enable the RAPI Gateway** checkbox.

4. Save your changes.

   dServers are updated during the next deployment.

Configuring Connection Settings

If you have your mobile device profile configured to use a secondary server if the primary server is unavailable, you can configure the manner in which your mobile devices attempt to connect to the secondary server. You can configure the following connection settings:

- **Override Connection Settings**. When you enable this option, the mobile device 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 its currently configured 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 every 10 seconds for 60 seconds (six times).

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

If the mobile device can not connect to the secondary server after the set amount of time it will attempt to connect to the next secondary server in the list. For information about configuring and ordering secondary servers, refer to *Enabling Secondary Server Support* on page 200.

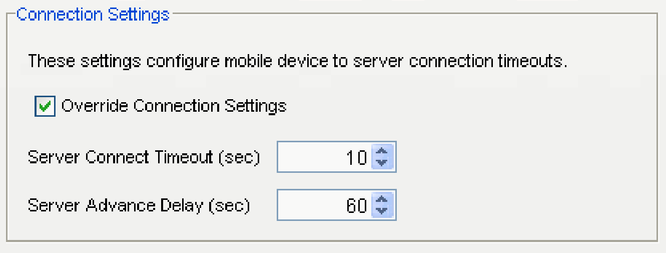
To configure time out settings:

1 From the **Mobile Device dServer Profiles List**, select the profile you want to configure.

2 Click **Edit**.

3 Click the **Device Connections** tab.

4 In the **Connections** setting region, enable the **Override Connection Settings** option.



Connection Settings

These settings configure mobile device to server connection timeouts.

☑ Override Connection Settings

Server Connect Timeout (sec) 10

Server Advance Delay (sec) 60

Figure 9-4. *Connection Settings*

5 Enter the number of seconds you want the mobile device to wait between connection attempts in the **Server Connect Timeout** text box.

6 Enter the number seconds you want the mobile device to attempt to connect to the secondary server in the **Server Advance Delay**.

7 Save your changes.

Enabling Device Caching

Device caching enables mobile devices to download software package files from other mobile devices instead of from the Mobile Device dServer. Device caching reduces the network bandwidth requirements for the network path from the Mobile Device dServer and the mobile device during software package synchronization.

A device that is enabled for Device Caching / Device Proxy will download the package and store it in a cache location.

Other proxy-enabled devices on the same subnet (i.e., within the same broadcast domain) can download the package form that device (or any other device that has cached that package).

A device that downloads the package from a peer will cache the package, and thus it will be able to act as a proxy for other devices.

You can configure the following parameters for device caching/device proxy in the device Registry:

- Enable Caching/Device Proxy
- Cache location
- Minimum size of cache location

Device Caching / Device Proxy are available in Avalanche 4.2 Enablers.

To enable device caching:

1. From the **Mobile Device dServer Profiles List**, select the profile you want to configure.
2. In the **Device Connections** tab, enable the **Enable Device Caching** option.
3. Save your changes.

Enabling Encryption

When you enable mobile device transport encryption, all TCP/IP communication between the Mobile Device dServer and mobile devices will be encrypted.

To enable mobile device transport encryption:

1. From the **Mobile Device dServer Profiles List**, select the profile you want to configure.
2. Click **Edit**.
3. In the **Security Settings** region, enable the **Enable Mobile Device Transport Encryption** option.
4. Save your changes.

Enabling Authentication

In conjunction with Access Control Lists and WEP security measures, Avalanche MC provides additional authentication methods for mobile devices. These options require that a mobile device first connect to the network through a serial connection before being able to roam the network wirelessly.

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

Mobile device authentication employs two options:

- **Enable Mobile Device Authentication**. This option forces mobile devices to connect to the network through a wired connection (such as a cradle) and receive an authentication key. When you enable this option, the Mobile Device dServer 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 dServer will not allow a TCP/IP connection.

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

NOTE Both of these options require mobile devices to connect to the network through a wired connection to receive authentication information. Proper planning is essential to ensure that all devices can connect to the wired network when these options are enabled—otherwise, these devices might be unable to connect to the network wirelessly.

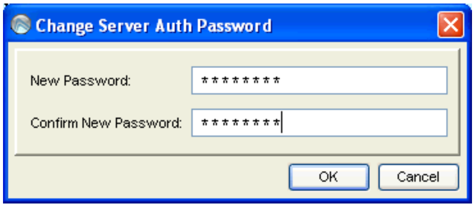
To authenticate mobile devices:

1 From the **Mobile Device dServer Profiles List**, select the profile you want to configure.

2 Click **Edit**.

3 If you want to restrict mobile devices to communicate only with a single, known Server, set the following options in the **Device Communications** tab:

- Enable the **Enable Server Authentication** checkbox.
- Set the administrative password for the Infrastructure dServer in the *Change Server Auth Password* dialog box that appears.



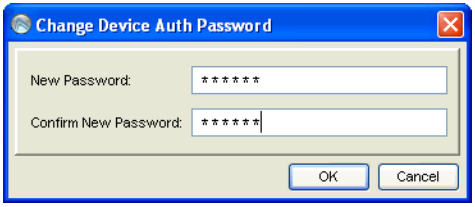
New Password: ********

Confirm New Password: ********

Figure 9-5. *Change Server Auth Password*

4 If you want to force mobile devices to connect to the wired network and receive an authentication key before being allowed to roam the network wirelessly, set the following options in the **Device Communications** tab:

- Enable the **Enable Mobile Device Authentication** checkbox.
- Set the administrative password for the mobile device in the *Change Device Auth Password* dialog box that appears.



New Password: ******

Confirm New Password: ******

Figure 9-6. *Change Device Auth Password*

NOTE If a dServer Location environment involves mobile devices roaming from one Server to another, it is highly recommended that you do **NOT** activate this option.

5 Save your changes.

dServers are updated during the next deployment.

Configuring Enterprise Server Connections for Mobile Device dServers

You can configure blackout windows where the Mobile Device dServers are not allow to contact the Enterprise Server. This eliminates heavy bandwidth and allows you to control the flow of you device connections to the Enterprise Server.

The **Enterprise Server Connection** tab allows you to create blackout windows and then provides you with a weekly and daily view so you know exactly when your dServers will not be able to contact the Enterprise Server. The weekly view displays when each black out occurs for that week. The daily view shows you exactly what time the blackout will occur.

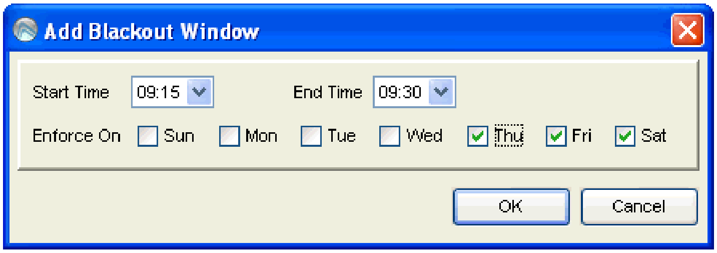
To configure Enterprise Server Connections:

1 In the **Mobile Device dServer Profile List**, select the profile for which you are defining privileges.

2 Click **Edit**.

3 In the **eServer Connection** tab, click **Add Blackout** window.

The *Add Blackout Window* dialog box appears.



Start Time 09:15 End Time 09:30

Enforce On ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☑ Thu ☑ Fri ☑ Sat

Figure 9-7. *Add Blackout Window*

4 Using the **Start Time** and **End Time** drop-down lists, 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 **Daily View** and **Weekly View** regions are updated with your new configurations.

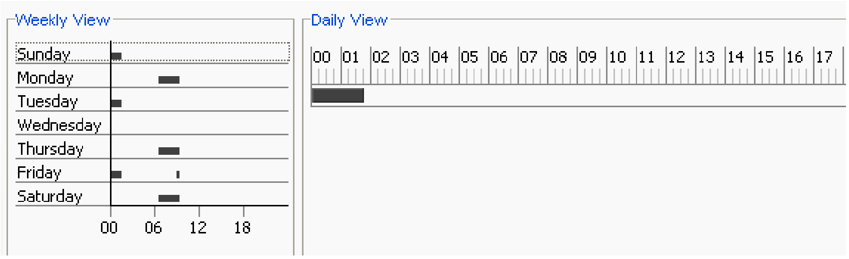


Figure 10. *Weekly and Daily Blackout Windows*

7 You can modify the blackout window by selecting the day of the week from the Weekly View. Click and drag the Daily View marker to indicate the desired time of the blackout.

8 Save the profile.

Enabling Secondary Server Support

Avalanche MC allows you to configure Mobile Device dServer profiles with secondary server support. This allows mobile devices to attempt to connect to a secondary Mobile Device dServer if the primary server is not available. Mobile devices attempt to connect to the first server listed in the **Secondary Server** tab. If the device can not connect to that server, it will move down the server 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.

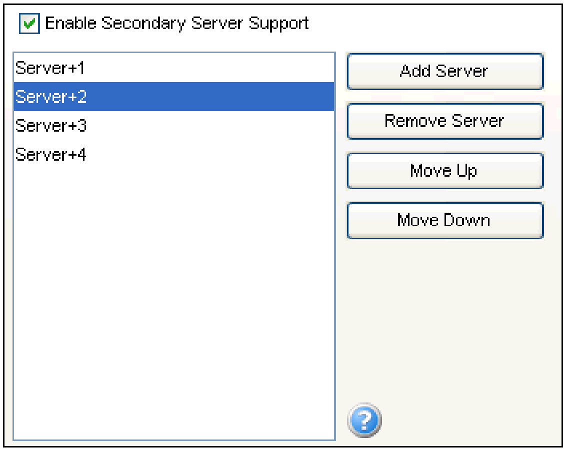
NOTE Unexpected mobile device behavior may occur if the secondary server is configured differently than the primary server. The mobile device may take on the network profile of the secondary server.

To add secondary servers:

1 From the **Mobile Device dServer Profiles List**, select the profile to which you want to add secondary servers.

2 Click **Edit**.

3 Click the **Secondary Servers** tab.



☑ Enable Secondary Server Support

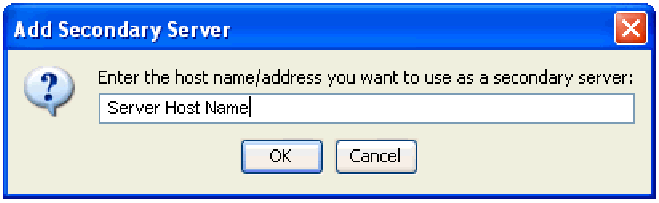
Server+1
Server+2
Server+3
Server+4

Figure 10-8. *Secondary Server Support*

4 Enable the **Enable Secondary Server Support** checkbox.

5 Click **Add**.

The *Add Secondary Server* dialog box appears.



Add Secondary Server

Enter the host name/address you want to use as a secondary server:

Server Host Name

Figure 10-9. *Add Secondary Server*

6 Enter the host name or address of the secondary server.

7 Click **OK**.

The server is added to the list box.

8 Add as many secondary servers as you desire.

9 If you want to remove a server, select the server and click **Remove Server**.

10 Use the **Move UP** and **Move Down** buttons to set the order of the secondary servers.

NOTE Mobile devices connect to secondary servers in the order the servers are listed in the list box.

11 When you are finished adding secondary servers, save your changes.

Your Mobile Device dServer Profile is now configured for secondary server support.

Configuring Server Updates

When you configure a Mobile Device dServer update, you have the following options:

- **Scheduling Server Updates**. This option allows you to schedule when you want to update the Mobile Device dServer software.
- **Configuring Update Restrictions**. This option allows you to assign dates and times when you do not want the server update to take place. You can also configure how many software updates can take place at the server at one time.
- **Deleting Orphaned Packages**. The option allows you to remove packages from the server that have been removed from the Avalanche MC console.

Scheduling Server Updates

The Avalanche MC Console allows you to update your Mobile Device dServer software in a timely and efficient manner.

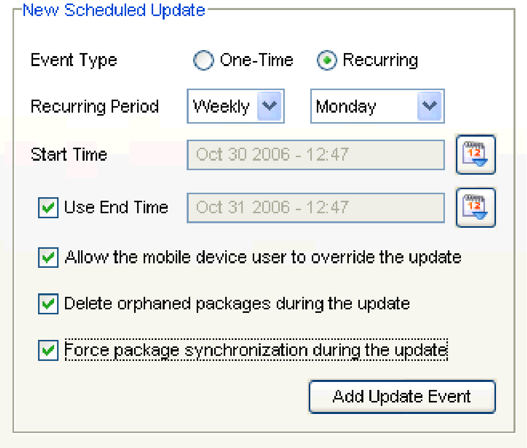
To schedule updates:

1 From the **Mobile Device dServer Profiles List**, select the profile you want to configure.

2 Click **Edit**.

3 Click the **Update Schedule** tab.

4 In the **New Scheduled Update** region, select whether the event is a **One-Time** event or a **Recurring** event option.



New Scheduled Update

Event Type ○ One-Time ● Recurring

Recurring Period Weekly Monday

Start Time Oct 30 2006 - 12:47

☑ Use End Time Oct 31 2006 - 12:47

☑ Allow the mobile device user to override the update

☑ Delete orphaned packages during the update

☑ Force package synchronization during the update

Figure 10-10. *New Update Schedule*

5 If you select **Recurring Event** option, 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.

6 Configure the update start time by clicking the calendar button next to the **Start Time** text box. This button opens a calendar allowing you select the day and time on which the update begins.

7 If you want to establish an end time for this update, enable the **Use End Time** checkbox and select the date and time you want the update to end.

NOTE Selecting an end time is not required. This allows you to create events that recur indefinitely.

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

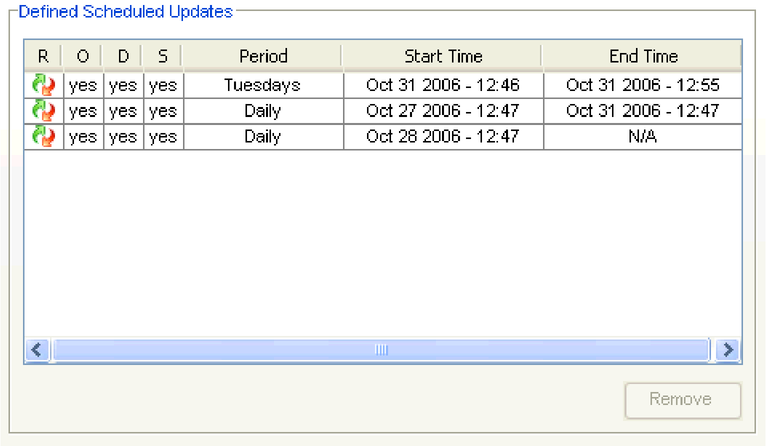
8 If you want the mobile device user to be able to override this update, enable the **Allow mobile device user to override the update** option.

9 If you want to remove any orphaned packages from the mobile device, enable the **Delete orphaned packages during the update** option.

For more information about orphaned packages, refer to *Deleting Orphaned Packages* on page 206.

10 If you want to synchronize the software packages, enable the **Force package synchronization during the update** option.

11 Click **Add Update Event** to add the new event to **Defined Schedule Update** region.


Defined Scheduled Updates

R	O	D	S	Period	Start Time	End Time
🔄	yes	yes	yes	Tuesdays	Oct 31 2006 - 12:46	Oct 31 2006 - 12:55
🔄	yes	yes	yes	Daily	Oct 27 2006 - 12:47	Oct 31 2006 - 12:47
🔄	yes	yes	yes	Daily	Oct 28 2006 - 12:47	N/A

Figure 10-11. *Defined Scheduled Updates*

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 MC. 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.

Configuring Update Restrictions

When you schedule updates for Mobile Device dServers, you might want to exclude specific dates and times. For example, you might want to prevent Avalanche MC from trying to update software during hours when your mobile devices are in use.

NOTE The dates and times you exclude from scheduling events apply to all events for that Mobile Device dServer profile —you cannot set specific exclusion dates and times for each update.

To exclude dates and times from a scheduling event:

1 From the **Mobile Device dServer Profiles List**, select the profile you want to configure.

2 Click **Edit**.

3 Click the **Update Restrictions** tab.

4 From the **Update Exclusion Window** region, enable the **Use a mobile device update exclusion window** option.

5 Using the **Prohibit updates between** lists, select the start and end times between which software updates should not occur.

6 Select the days during which these start and end times apply by enabling the check box next to the day.

For example, if you want to prevent software updates from occurring from 7:00 am to 7:00 pm from Monday through Friday, you would select 07:00 from the start time list, select 19:00 from the end time list, and enable the checkboxes for Monday, Tuesday, Wednesday, Thursday, and Friday.

7 If you want to allow any number of simultaneous updates, enable the **Allow unlimited simultaneous mobile device updates** option in the **Synchronization Exclusion Window** region.

-Or-

If you want to set the maximum number of simultaneous updates, disable the **Allow unlimited simultaneous mobile device updates** option and type the maximum number of simultaneous updates in the active text box.

Software updates require sending application package files to each mobile device. The amount of time needed to send these files depends on how large the application package files are. If you do not need to conserve bandwidth, you can allow unlimited simultaneous updates. If you want to conserve network bandwidth, you can set a maximum number of simultaneous updates that can occur.

NOTE The maximum number of simultaneous updates that you allow applies to all events for a region.

Deleting Orphaned Packages

As you update and modify the software installed on mobile devices, devices begin to acquire orphaned packages. Orphaned packages are parts of application files that no longer apply to applications on a mobile device. Packages will receive an orphaned status in the following cases:

- If a package has been deleted from the Avalanche MC Console.
- If a package is part of a software collection that has been disabled.
- If the package is disabled.

You can instruct the Mobile Device dServers in a region to delete any orphaned packages on mobile devices they manage.

To configure the deletion of orphaned packages:

1 From the **Mobile Device dServer Profiles List**, select the profile you want to configure.

2 Click **Edit**.

3 Click the **Update Schedule** tab.

4 If you want to delete all orphan packages, enable the **Delete orphaned packages during the update** option.

5 Schedule a mobile device update to send the configuration to the mobile devices. For details, refer to *Scheduling Server Updates* on page 202.

NOTE Marking packages for deletion are specific to each update task. For each update you add, you will need to configure the behavior for orphaned packages.

Removing Mobile Device dServer Profiles

If you no longer are using a Mobile Device dServer profile, you can remove it from the console. When you remove a Mobile Device dServer 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 dServer profile:

1 From the **Mobile Device dServer Profiles List**, select the profile you want to remove.

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 dServers to Regions

Once you have configured your Mobile Device dServer profile, you can apply that profile to any region in the console. When you apply a Mobile Device dServer profile to a region, that profile will be deployed to all Mobile Device dServers in that region matching the profile criteria. For more information about assigning Mobile Device dServer Profiles to a region and then applying those profiles to servers, refer to *Assigning Server Profiles to Regions* on page 109.

Viewing Mobile Device dServer Licensing Messages

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

To view licensing messages:

1 From the **Tools** menu, select **dServer License Messages**.

The *dServer Licensing Messages* dialog box appears.

2 Click the **dServer Location** column to list the messages by dServer Location.

3 Click the **dServer** column to list the messages by dServer.

Chapter 10: 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.

This section contains the following topics:

- Why Should I Create a Software Profile?
- Creating Software Profiles
- Software Packages
- Software Profile Settings and Tables

Why Should I Create a Software Profile?

Software profiles allow you to control the organization of and configure software packages for deployment to multiple devices. Software profiles are useful for configuring software packages for multiple devices on your network at one time.

Creating Software Profiles

There are two types of software profiles: normal and Enabler. When you create an Enabler software profile, you should install *only* Enabler Install Kit packages to that profile. For all other types of software packages, you should use a normal software profile. For information on the types of software packages, refer to *Software Packages* on page 214.

- **Normal software profiles.** When a mobile device matching the selection criteria is connected to Avalanche MC, Avalanche MC will download the software package(s) to the device. If no activation time is set, the package(s) will be installed immediately. If an activation time is set, the package(s) will be installed at the specified time.
- **Enabler software profiles.** When a mobile device matching the selection criteria is connected to Avalanche MC, Avalanche MC will check the mobile device for compatibility with each of the Enabler Install Kit

packages within the Enabler software profile. If Avalanche MC finds a matching Enabler for the device, it will download and install the Enabler.

NOTE Enabler Install Kits are deployed using the RAPI gateway only.

This section contains the following information:

- Adding Software Profiles
- Editing Software Profiles
- Applying Software Profiles
- Removing Software Profiles
- Software Profile Authorized Users
- Removing Software Profile Authorized Users

Adding Software Profiles

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

To add a software profile:

1 From the Navigation Window, select **Software Profiles**.

The **Software Profiles** tab appears.

2 Click **Add Profile**.

The *Input* dialog box appears.

3 Type the name of the new software profile and click **OK**.

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

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

4 In the **General Settings** tab, use the **Profile Type** drop-down list to select whether this profile is a **Normal** software profile or an **Enabler** software profile.

5 From the **File** menu, select **Save**.

Editing Software Profiles

Once a software profile has been created, you can edit the name, status, type, and selection criteria. For a complete list of software profile settings, see *Software Profile General Settings* on page 221.

This section contains information about the following:

- Enabling Software Profiles
- 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 mobile devices.

To enable a software profile:

1 In the **Software Profiles** tab, select the desired profile from the **Software Profile List**.

2 Click **Edit**.

3 In the **General Settings tab**, select the **Enabled** option to enable the profile.

4 Save your changes.

The profile status displays in the **Software Profile List**.

Software Profile Selection Criteria

Selection criteria determine which mobile devices receive the software profile. For information about creating selection criteria for software profiles, refer to *Building Selection Criteria* on page 318.

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 dServer locations in that region when you perform a Universal Update. For information about applying software profiles to regions, refer to *Assigning Software Profiles to Regions* on page 112. For information about deploying Universal Updates, refer to *Deploying Universal Updates* on page 334.

Removing Software Profiles

When a software profile is no longer useful, you can delete it from the Avalanche MC Console.

To remove a software profile:

1 In the **Software Profiles** tab, select the profile you want to remove from the **Software Profile List**.

2 Click **Remove Profile**.

The *Confirm Deletion* dialog box appears.

3 Click **Yes** to delete the software profile.

The software profile is deleted from the Avalanche MC Console.

Viewing Where Software Profiles Are Applied

The **Applied To** tab in the network profile page allows you to see exactly which regions, dServer 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 dServer Location Properties tabs and assign the profiles there. For information, refer to *Applying Software Profiles* on page 211.

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, dServer Location or Site where the profile is applied.
- **Selection Criteria**. Any selection criteria that is applicable at the region, dServer Location or site where the profile is applied.

To view:

1 In the Navigation Window, select **Software Profiles**.

2 From **Software Profile List**, select the network profile you want to see.

3 Click the **Applied To** tab.

The tab displays the information for the selected network profile.

Software Profile Authorized Users

The **Authorized Users** tab allows you to assign administrative privileges to for a specified software profile to a user that has Normal user rights and is not assigned permissions to software profiles. This means that any user assigned as an authorized user to a software 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 63.

To add an authorized user:

1 In the **Software Profiles List**, select the desired profile.

2 Click **Edit**.

3 Select the **Authorized Users** tab and click **Add User**.

The *Select Software Profile Admin User* dialog box appears.

4 From the drop-down list, select the user.

5 Click **OK**.

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

6 Save your changes.

Removing Software Profile Authorized Users

If you do not want a user to have administrative privileges for a software profile, you can remove that user from the authorized user list. The user will continue to have Normal permissions, but will not longer be able to access or modify the software profile.

To remove an authorized user:

1. From the **Authorized Users** tab, select the desired user.
2. Click **Remove User**.

   The user is removed from the **Authorized Users** list for the profile.

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 MC Console. Each software package is usually pre-assigned with default selection criteria.

Software packages can be one of the following package types:

- **Application packages**. These packages are added to the **Application** menu in the mobile device.
- **Support packages**. These packages contain updates to existing software packages or to the Avalanche Enabler. Support packages do not appear as new items under the **Application** menu of the mobile device. The Ava3 DHCP update software package, which was previously needed for Symbol 3000 mobile devices, is an example of a support package.
- **Auto Run packages**. These packages automatically execute following a successful download. Like the support packages, auto run packages do not modify the **Application** menu. RF firmware upgrade packages are examples of auto packages.
- **Enabler Install Kits**. These packages allow you to install an Enabler on a device automatically. They have built-in selection criteria so that each device receives the correct Enabler. These packages are only used with an Enabler software profile.
- **Enabler Update Kits**. These packages allow for automatic updates to the Enablers installed on your devices. These packages are only used with an normal software profile, *not* with an Enabler software profile.

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 not to the console. However, you must enter Edit Mode to configure any other software profile options.

This section includes the following information:

- Installing Software Packages
- Configuring Software Packages Settings
- Configuring Software Packages for Delayed Installation
- Removing Software Packages

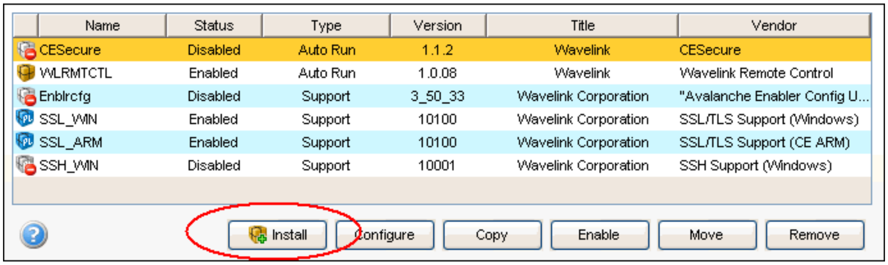
Installing Software Packages

Once you create a software profile, you must install 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 install or configure software packages. Software package configuration changes are saved to the actual package not to the console. However, you must enter Edit Mode to configure any other software package options.

To install software packages:

1. Select the desired profile from the **Software Profiles List**.
2. From the **Installed Software Packages** region of the **Software Profiles** tab, click **Install**.



Name	Status	Type	Version	Title	Vendor
CESecure	Disabled	Auto Run	1.1.2	Wavelink	CESecure
WLRMTCTL	Enabled	Auto Run	1.0.08	Wavelink	Wavelink Remote Control
Enblrcfg	Disabled	Support	3_50_33	Wavelink Corporation	"Avalanche Enabler Config U...
SSL_WIN	Enabled	Support	10100	Wavelink Corporation	SSL/TLS Support (Windows)
SSL_ARM	Enabled	Support	10100	Wavelink Corporation	SSL/TLS Support (CE ARM)
SSH_WIN	Disabled	Support	10001	Wavelink Corporation	SSH Support (Windows)

Figure 10-1. *Install Software Package*

The *Install Software Package Wizard* appears.

3 Type the path to the package location, or click **[...]** to browse to the package location.

4 After you have entered the package location, click **Next**.

The *License Agreement* appears.

5 Enable the **YES, I agree** option and click **Next**.

NOTE If you do not enable the **YES, I agree** option, you will not be able to complete the installation process.

The software package is installed.

6 Click **Finish** to close the *Install Software Package Wizard*.

You can now configure the package and copy or move it to another profile.

Configuring Software Packages Settings

Once a software package has been installed, you can perform several tasks, including:

- Configuring Software Packages
- Copying Software Packages
- Enabling Software Packages
- Moving Software Packages

Configuring Software Packages

Some software packages come with options that should be configured before the packages are installed on a mobile device. These options are configured from the Avalanche MC Console. Configuration options will differ based on the software package you are configuring.

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 Select the desired profile from the **Software Profiles List**.

2 From the **Installed Software Packages** region of the **Software Profiles** tab, select the package you want to configure.

3 Click **Configure**.

The *Configure Software Package* dialog box appears.

4 From the available list, edit the configuration options for the package.

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

---

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

The software package is configured and ready to be deployed.

Copying Software Packages

You can copy a software package and its configuration 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 Select the desired profile from the **Software Profiles List**.

2 Click **Edit**.

3 From the **Installed Software Packages** region of the **Software Profiles** tab, select the package you want to copy.

4 Click **Copy**.

The *Copy Software Package* dialog box appears.

5 From the drop-down list, select the profile you want to contain the software package and click **OK**.

The package is copied to the destination 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 **Installed Software Packages** region of the **Software Profiles** tab, select the package you want to enable.
2. Click **Edit**.
3. Click **Enable**.
4. From the **File** menu, select **Save**.

   The profile's new status shows in the **Installed Software Packages** region.

Moving Software Packages

A software package and its configuration can be moved from one software profile to another.

To move a software package:

1. From the **Installed Software Packages** region of the **Software Profiles** tab, select the package you want to move.
2. Click **Edit**.
3. Click **Move**.

   The *Move Software Package* dialog box appears.

4. Select the profile the package will be moved to from the drop-down list and click **OK**.

   The package is moved to the destination profile.

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 you want the mobile device to install 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.

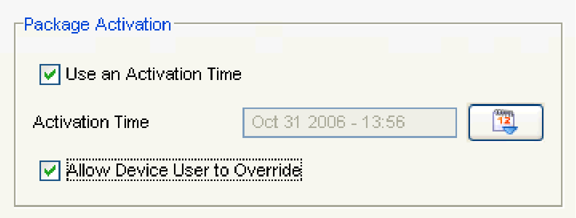
Package activation is supported in Enabler version 4.1 and later.

To configure a software package for delayed installation:

1 From the **Installed Software Packages** region of the **Software Profiles** tab, select the package you want to configure.

2 Click **Edit**.

3 In the **Package Activation** section, enable the **Use an Activation Time** checkbox.



Package Activation

☑ Use an Activation Time

Activation Time: Oct 31 2006 - 13:56

☑ Allow Device User to Override

Figure 10-2. *Package Activation*

4 Click the **Calendar** button to select a date and time for the package to be installed on the device.

The *Select a date and time* dialog box appears.

5 Select a date and time for the package installation on the device and click **OK**.

6 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, they will be prompted to choose another time to install.

7 Save your changes.

Removing Software Packages

When a software package is no longer useful, it can be removed from the Avalanche MC Console. If you remove a software package, the package becomes an orphaned package on the mobile device. For more information, refer to *Deleting Orphaned Packages* on page 206.

To remove a software package:

1 From the **Installed Software Packages** region of the **Software Profiles** tab, select the package to be removed.

2 Click **Remove**.

The *Confirm Deletion* dialog box appears.

3 Click **Yes** to remove the package from the Avalanche MC Console.

The package is removed.

Software Profile Settings and Tables

This section provides information about the settings and tables in the **Software Profiles** tab, including:

- Software Profile List
- Software Profile General Settings
- Installed Software Packages

Software Profile List

The **Software Profile List** displays information about your software profiles.

Field	Description
Name	Displays the name of the software profile.
Type	Displays the type of the software profile.

Table 10-1: *Software Profile List*

Field	Description
Status	Displays the enabled/disabled status of the software profile.
Selection Criteria	Displays the selection criteria used to apply the software profile.

Table 10-1: *Software Profile List*

Software Profile General Settings

The following table provides information about the software 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.
Profile Type	Sets the type of the profile as either Normal or Enabler.

Table 10-2: *General Settings*

Installed Software Packages

The following table provide information about the **Installed Software Packages** region in the **Software Profiles** tab.

Field	Description
Name	Displays the name of the software package.
Status	Displays the enabled/disabled status of the software package.
Type	Displays the type of the software package.
Version	Displays the version of the software package.
Vendor	Displays the vendor associated with the software package.
Title	Displays the title of the software package.

Table 10-3: *Software Packages*

The **Installed Software Packages** region also includes the following regions:

- Package Activation
- Package Tracking
- Package Selection Criteria
- Package Distribution

Package Activation

The following table displays the software package options in the **Package Activation** region.

Field	Description
Use an Activation Time	Enables an activation time for the software package installation on the mobile device.
Activation Time	Sets the activation time for the software package installation on the mobile device.
Allow Device User to Override	Enables the device user to override the package installation at the time of activation.

Table 10-4: *Package Activation*

Package Tracking

The following table displays the information included in the **Package Tracking** region.

Field	Description
Installation	Displays the date/time of package installation and the user who installed the package.
Last Configured	Displays the date/time of the last configuration and the user who performed the configuration.

Table 10-5: *Package Tracking*

Package Selection Criteria

Package selection criteria are determined by Avalanche MC. You cannot change the package selection criteria.

Package Distribution

The following table provides descriptions of the configuration options in the **Package Distribution** tab.

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

The following tables provides information about the results that will occur with the different configurations in the Package Distribution tab. The table assumes that the first option (Enable Cached Peer to Peer Distribution) is enabled. Emphasis is placed on the configurations which allow the mobile devices to receive the updates.T

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

Table 10-6: *Configuration Results for Package Distribution*

Chapter 11: 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 infrastructure. Avalanche MC not only applies these settings to devices—it also enforces these settings, preventing unauthorized modifications.

Infrastructure profiles are made up of configurations that manage your infrastructure devices and a specified network profile.

When the Infrastructure dServer receives an infrastructure profile, each infrastructure device that reports to that dServer compares the hardware type configured for the profile. If the hardware in the profile matches the hardware of the infrastructure device, the dServer examines the firmware. If the firmware is compatible with the infrastructure device, the device assumes the profile.

Avalanche MC supports the following infrastructure devices:

- Symbol WS 2000
- Symbol 5100 v. 3.0 +
- Symbol AP 5131
- Cisco 1100
- Cisco 1200 IOS
- Cisco 1310 BR
- Symbol WS 5000 v. 1.2+
- Symbol AP 4131
- Cisco 350 IOS
- Cisco 1130
- Cisco 1242
- Symbol AP 4121

The following steps are an overview of creating a composite Infrastructure profile:

1 Create an Infrastructure Profile. (*Creating Infrastructure Profiles* on page 228.)

2 Create a network profile containing all the network and wireless settings that you want to apply to the infrastructure devices. (*Creating Network Profiles* on page 144.)

3 Create a VLAN that binds the network profile and infrastructure profile.(*Configuring VLANs* on page 237.)

4 Assign the profile to a dServer Location or region. (*Assigning Infrastructure Profiles* on page 240.)

5. Assign the network profile to the same dServer Location or region. (*Assigning Network Profiles to Regions* on page 111).

6. Deploy the configurations using the Deploy Now icon or performing a Universal Update. (*Deploying Universal Updates* on page 334.)

Infrastructure Considerations

- Not all infrastructure devices support every feature of the network profiles.

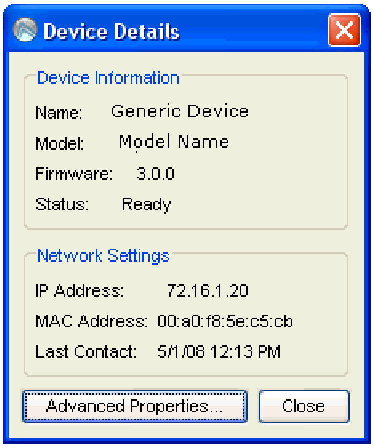
- You can view the type of profile you are using at a particular infrastructure device using Mobile Manager. For more information, refer to the *Mobile Manager User's Guide*.

- 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 device as well as access the Advanced Properties.

- If an infrastructure device is assigned a profile manually (using Mobile Manager) a profile from Avalanche MC will not override that profile. You must remove the assigned profile (using Mobile Manager) and then deploy the Avalanche MC infrastructure profile.

- You access infrastructure device details by right-clicking an infrastructure device and selecting View Device Details. The dialog box provides the following device information:

  - Name of the device
  - Model
  - Firmware Version
  - Status
  - IP Address
  - MAC Address
  - Last Contact (This refers to the last time the Infrastructure dServer was able to contact the device.)



Device Information

Name: Generic Device

Model: Model Name

Firmware: 3.0.0

Status: Ready

Network Settings

IP Address: 72.16.1.20

MAC Address: 00:a0:f8:5e:c5:cb

Last Contact: 5/1/08 12:13 PM

Figure 11-1. *Infrastructure Device Details*

You can modify advanced properties for the infrastructure device by clicking **Advanced Properties**.

See the *Mobile Manager User's Guide* for more information on creating, modifying or applying infrastructure profiles using Mobile Manager.

This section provides information about the following topics:

- Creating Infrastructure Profiles
- Configuring Infrastructure Profiles
- Viewing Where Infrastructure Profiles Are Applied
- Configuring VLANs
- Assigning Infrastructure Profiles
- Deleting Infrastructure Profiles
- Updating Infrastructure Device Firmware
- Infrastructure Profile Settings and Descriptions

Creating Infrastructure Profiles

Once you organize your network dServer Locations into regions, you can create and assign infrastructure profiles to each region. The Avalanche MC Console takes the configuration values for each profile assigned to a region and applies them to the Infrastructure dServers associated with that region. As a result, you can configure multiple dServer Locations on your network at one time.

Profiles apply only to one specific region; however, you can copy a profile from one region to another. Profiles can be created for any hardware type that Avalanche MC supports. You can create profiles to be as basic or as detailed as your wireless network demands.

NOTE To apply profiles to a region, you must send the information to the Servers within that region. See *Deploying Universal Updates* on page 292 for more information.

To create a profile:

1 Select **Infrastructure Profiles** from the Navigation Window.

The **Infrastructure Profiles** tab appears.

2 In the **Infrastructure Profile List** region, click **Add Profile**.

The *Add Infrastructure Profile* dialog box appears.

3 Type a name for the profile in the **Name** text box.

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

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

6 Click **OK**.

The new profile appears in the **Infrastructure Profile List** region.

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

Cloning Infrastructure Profiles

If you have previously configured an infrastructure profile and want to make minor modifications to create a new profile, you can clone profiles.

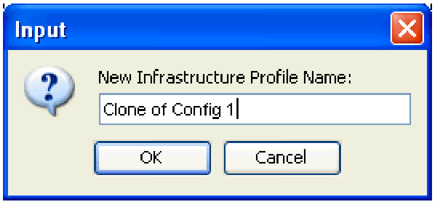
To clone infrastructure profiles:

1 Select **Infrastructure Profiles** from the Navigation Window.

The **Infrastructure Profiles** tab appears.

2 Select the profile you want to clone from the **Infrastructure Profile List** region.

An *Input* dialog box appears.



Input

New Infrastructure Profile Name:

Clone of Config 1

Figure 11-2. *Infrastructure Profile Clone*

3 Enter the name of the new infrastructure profile and click **OK**.

The profile appears in the **Infrastructure Profile List** region and contains all the settings and configurations of the original profile.

Configuring Infrastructure Profiles

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

- General Settings
- Enabling Infrastructure Profiles
- Editing Advanced Properties
- Editing Authentication Servers

- Assigning Infrastructure Profile Authorized Users
- Removing Infrastructure Profile Authorized Users
- Configuring Infrastructure Selection Criteria

General Settings

In the **General Settings** tab, you can edit the infrastructure profile name, status, firmware version, and default VLAN ID based on the needs of your infrastructure. For detailed information about the configuration options in the **General Settings** tab, refer to *Infrastructure Profiles General Settings* on page 250.

Enabling Infrastructure Profiles

You must enable an infrastructure profile before you assign it to regions or dServer Locations.

To enable an infrastructure profile:

1. From the **Infrastructure Profiles** tab, select the desired profile from the **Infrastructure Profile List**.
2. Click **Edit**.
3. In the **General Settings** tab, select the **Enabled** option to enable the profile.
4. Save the profile.

   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 MC 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 144.

To edit advanced properties:

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

2 Click **Edit**.

3 In the **Advanced Settings** tab, click **Edit Advanced Properties**.

The *Advanced Properties* dialog box appears.

NOTE You can view supported properties and property descriptions for different infrastructure devices in the Avalanche MC Console in the *Advanced Properties* dialog box for a profile.

Review the following tasks to ensure a well-designed infrastructure profile:

- Controlling How Infrastructure Devices Are Configured
- Activating Infrastructure Device Security Features

Controlling How Infrastructure Devices Are Configured

Depending on the manufacturer, infrastructure devices are configurable using one of several methods. These methods are:

- Serial connection
- Telnet session
- Web browser
- Avalanche MC
- Mobile Manager Site Console

You can activate or deactivate an infrastructure profile using Avalanche MC or Mobile Manager depending on the type of infrastructure profile.

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

Activating Infrastructure Device Security Features

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

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

1. Build and maintain a Very Large Access Control List.

   You can add and remove MAC addresses from the Very Large Access Control List to restrict access to authorized mobile devices. For more information, see *Chapter 17: Managing Very Large Access Control Lists* on page 269.

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

   WEP, or Wired Equivalent Privacy, is a protocol for securing wireless network communications. You secure your wireless network by assigning a WEP key to an infrastructure device. This key encrypts transmissions between a mobile device and an infrastructure device. See *Chapter 7: Managing Distributed Servers* on page 119 for more information on WEP and other security protocols.

It is highly recommended that you implement all of these security features to maintain the integrity of your wireless network. Refer to *Chapter 9: Managing Mobile Device Distributed Servers* on page 183 and *Chapter 8: Managing Infrastructure Distributed Servers* on page 167 for more information on wireless network security.

Editing Authentication Servers

You can edit authentication servers for your infrastructure profiles. This allows you to secure wireless communications on your network.

To edit authentication servers:

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

2 Click **Edit**.

3 In the **Advanced Settings** tab, click **Edit Authentication Servers**.

The *Authentication Servers* dialog box appears.

4 In the **Host Name/IP Address** text box, enter the DNS name or IP address of the authentication server.

NOTE You can enter up to four different authentication servers.

---

5 In the **Port** text box, enter the TCP port you are using for authentication.

6 If your authentication server is configured for accounting, enter the port the server is using in the **Acct Port** text box.

7 Type the shared secret your authentication server uses in the **Shared Secret** text box.

8 Select the authentication type by enabling the appropriate checkbox. You can choose from the following authentication types:

- **EAP.** When selected, the infrastructure device will use EAP to authenticate mobile devices.

- **MAC.** When selected, the infrastructure device will authenticate mobile devices using the devices’ MAC address.

- **Accounting.** When selected, the infrastructure device will send accounting messages to the server address entered.

- **Admin.** When selected, Admin logins will be authenticated using the server address entered.

9 In the **Retry Settings** region, configure the following:

- **Reauth Tries.** Sets the number of times the infrastructure device can attempt to contact an authentication server.

- **Reauth Period (sec).** Sets the number of seconds the infrastructure device can wait before authentication fails.

10 Click **OK**.

The changes are applied to the profile.

11 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 85.

To add an authorized user:

1 In the **Infrastructure Profiles List**, select the desired profile.

2 Click **Edit**.

3 Select the **Authorized Users** tab and click **Add User**.

The *Select Software Profile Admin User* dialog box appears.

4 From the list, select the user.

5 From the drop-down, select the level of permission for the user.

6 Click **OK**.

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

Removing Infrastructure Profile Authorized Users

If you do not want a user to have administrative privileges for a software profile, you can remove that user from the authorized user list. The user will continue to have Normal permissions, but will not longer be able to access or modify the software profile.

To remove an authorized user:

1 From the **Authorized Users** tab, select the desired user.

2 Click **Remove User**.

Configuring Infrastructure Selection Criteria

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

To configure selection criteria:

1 Select the profile for which you want to configure selection criteria.

2 Click the **Edit** mode button.

3 Click the **Selection Criteria** tab.

4 Click the **Wizard** icon to open the **Selection Criteria Wizard**.

5 Using the commands in the wizard, build the selection criteria you want to assign to the profile.

For detailed information about creating selection criteria, refer to *Building Selection Criteria* on page 318.

6 When you are finished building your selection criteria, close the **Selection Criteria Wizard** and save your changes.

Viewing Where Infrastructure Profiles Are Applied

The **Applied To** tab in the network profile page allows you to see exactly which regions, dServer 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 dServer Location Properties tabs and assign the profiles there. For information, refer to *Assigning Profiles to Regions* on page 107.

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, dServer Location or Site where the profile is applied.
- **Selection Criteria**. Any selection criteria that is applicable at the region, dServer Location or site where the profile is applied.

To view:

1. In the Navigation Window, select **Infrastructure Profiles**.
2. From **Infrastructure Profile List**, select the network profile you want to see.
3. Click the **Applied To** tab.

   The tab displays the information for the selected network profile.

Configuring Infrastructure Scheduled Events

You can schedule the following infrastructure events:

- Reboot
- Disable all radios
- Enable all radios
- Disable radio A
- Disable radio B
- Disable radio G
- Enable A
- Enable B
- Enable G

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

To schedule an event:

1 Select the infrastructure profile that you want to schedule an event for.

2 Click the **Edit** mode button.

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, if you want the event to happen once.
- Recurring event, if you want the event to persist.

6 If you select **Recurring Event**, configure the day or the day of the week you want the event to occur on.

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 tab list.

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

11 Click the **Save** icon to save your changes.

Configuring VLANs

VLAN configuration allows you to create Virtual Local Area Networks to control the flow of data over your network.You can use VLAN configuration to bind an infrastructure profile to a network profile. For details about configuring network profiles, refer to *Chapter 7: Managing Network Profiles* on page 143. You must have at least one network profile created to configure a VLAN. This section includes the following:

- Creating VLANs

- Editing a VLAN
- Removing a VLAN

Creating VLANs

Create VLANs to bind a network profile to an infrastructure profile. You can configure the following VLAN 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.
- **VLAN ID/Tag.** Enter the identification of the VLAN 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. If you are using a Cisco device, select the type of radio the device uses.
- **Broadcast SSID**. Select whether to broadcast the SSID associated with the infrastructure 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 VLAN. For information about network profiles, refer to *Chapter 7: Managing Network Profiles* on page 143.

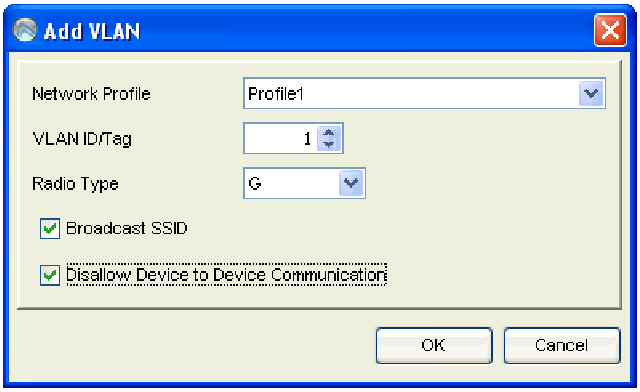
To add a VLAN:

1 From the **Infrastructure Profile List**, select the desired profile.

2 Click **Edit**.

3 In the **VLAN Configuration** region, click **Add VLAN**.

The *Add VLAN* dialog box appears.



Add VLAN

Network Profile: Profile1

VLAN ID/Tag: 1

Radio Type: G

☑ Broadcast SSID

☑ Disallow Device to Device Communication

Figure 11-3. *Add VLAN*

4 From the **Network Profile** drop-down menu, select the profile to which you want to add the VLAN.

5 Enter the number of the **VLAN 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 VLAN appears in the **VLAN Configuration** region.

10 Save your changes.

Editing a VLAN

Once a VLAN has been created, you can edit it any time changes are necessary.

To edit a VLAN:

1 Ensure you are in Edit Mode.

2 From the **VLAN Configuration** region, select the desired VLAN.

3 Click **Edit VLAN**.

The *Edit VLAN* dialog box appears.

4 Make any necessary changes and click **OK**.

The changes are applied to the VLAN.

Removing a VLAN

If you decide a VLAN is no longer necessary, you can remove it from the Avalanche MC Console.

To remove a VLAN:

1 From the **VLAN Configuration** region, select the desired VLAN.

2 Click **Remove VLAN**.

The *Confirm Delete* dialog box appears.

3 Click **Yes**.

The VLAN is removed from the Avalanche MC Console.

Assigning Infrastructure Profiles

You can assign as many Infrastructure profiles to a region or dServer 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 MC console. Once you assign an Infrastructure profile to a region, you must perform a Universal Deployment to update your dServers or you can deploy the settings immediately. For more information the Universal Deployment, refer to *Deploying Universal Updates* on page 334.

To assign infrastructure profiles:

1 From the Navigation Window, select the region or dServer Location to which you want to assign an infrastructure profile.

2 Click **Edit**.

3 In the **Infrastructure Profile** tab, click **Add**.

The *Add AP Profile Application* dialog box appears.

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

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

5 If you want the hardware in the region to retain the default hardware profile, enable the **Default Hardware Profile** check box.

NOTE If you enable this check box, the dServer will only match hardware types. If the hardware type matches, the dServer will change the firmware so it matches the infrastructure profile.

6 Click **OK**.

The profile is added to the **Infrastructure Profile** tab for the region.

7 Continue adding infrastructure profiles to the region.

8 Use the **Move Up** and **Move Down** buttons to assign the order in which the infrastructure profiles are applied to devices.

9 Save your changes.

10 Click the **Deploy Now** icon.

The assigned profile will deploy to the dServers. You can also perform a Universal Deployment. For information about performing a Universal Deployment, refer to *Deploying Universal Updates* on page 334.

Deleting Infrastructure Profiles

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

To delete a profile from a region:

1 Select a region or dServer from the Navigation Window.

2 Select the **Region Properties** or **dServer Location Properties** tab (based on the location of the profile).

3 Click **Edit**.

4 Select the **Infrastructure Profiles** tab.

5 Select the desired profile and click **Remove**.

You can also delete a profile from the **Infrastructure Profile List**. Deleting a profile from the **Infrastructure Profile List** is permanent and cannot be undone. If you decide after deleting a profile that you still want that profile, you must recreate it.

NOTE Deleted profiles remain at each dServer Location until the dServer Location is synchronized with the Avalanche MC Console.

To delete a profile from the Infrastructure Profile List:

1 Select **Infrastructure Profiles** from the Navigation Window.

The Infrastructure Profiles tab appears.

2 Select the desired profile and click **Remove Profile**.

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 MC supports a wide range of firmware for many different types of infrastructure devices.

When you first deploy an Infrastructure dServer to a dServer 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 dServer 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 MC interacts with infrastructure devices in one of two ways: either in full support mode or in compatibility mode. Avalanche MC 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 MC 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.

Full Support Mode

If the firmware version installed on an infrastructure device matches a firmware version known to the Avalanche MC 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 Mobility Center 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 11-1: *Firmware Version Matches for Compatibility Mode Support (Samples)*

The following example uses the information in Table 10-1 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 MC supports. The Infrastructure dServer will be able to manage infrastructure devices with any of the firmware types listed.

Importing Firmware

Avalanche MC 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.

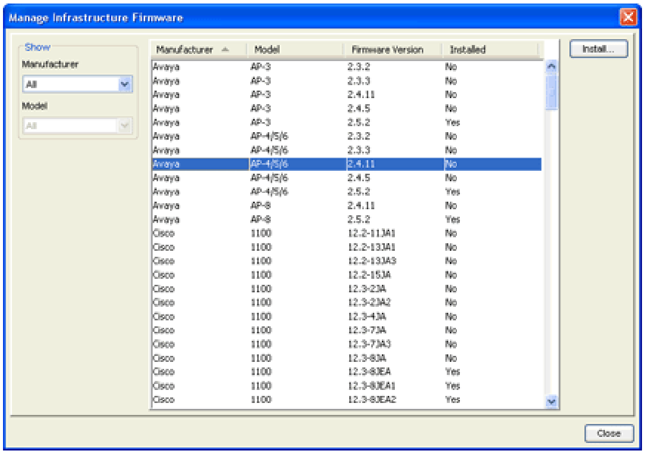
You can also re-install firmware that has already been installed. When you attempt to do this, the Console will remind that you that you are overwriting the existing installed firmware.

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.



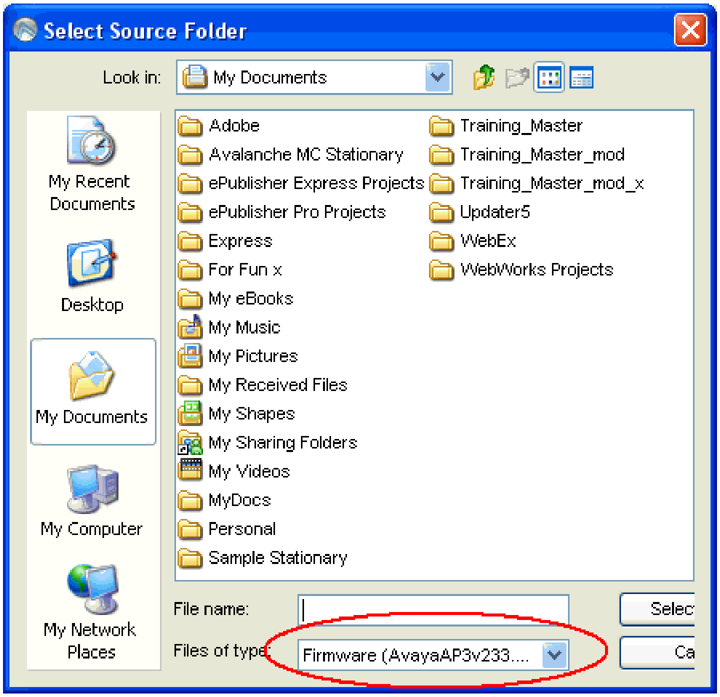
Manufacturer	Model	Firmware Version	Installed
Avaya	AP-3	2.3.2	No
Avaya	AP-3	2.3.3	No
Avaya	AP-3	2.4.11	No
Avaya	AP-3	2.4.5	No
Avaya	AP-3	2.5.2	Yes
Avaya	AP-4/5/6	2.3.2	No
Avaya	AP-4/5/6	2.3.3	No
Avaya	AP-4/5/6	2.4.11	No
Avaya	AP-4/5/6	2.4.5	No
Avaya	AP-4/5/6	2.5.2	Yes
Avaya	AP-8	2.4.11	No
Avaya	AP-8	2.5.2	Yes
Cisco	1100	12.2-11JA1	No
Cisco	1100	12.2-13JA1	No
Cisco	1100	12.2-13JA3	No
Cisco	1100	12.2-15JA	No
Cisco	1100	12.3-2JA	No
Cisco	1100	12.3-2JA2	No
Cisco	1100	12.3-4JA	No
Cisco	1100	12.3-7JA	No
Cisco	1100	12.3-7JA3	No
Cisco	1100	12.3-8JA	No
Cisco	1100	12.3-8JEA	Yes
Cisco	1100	12.3-8JEA1	Yes
Cisco	1100	12.3-8JEA2	Yes

Figure 11-4. *Manage Infrastructure Firmware*

3 In the **Show** area, you 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.



Look in: My Documents

File name:

Files of type: Firmware (AvayaAP3v233....

Figure 11-5. *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 transmitted 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. Click Cancel to cancel the process.

A success message appears when the transmit 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 dServers. 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

Avalanche MC contains a limited number of firmware versions that can deployed to the Infrastructure dServers. You have the ability to manually drop additional firmware binary files into the “firmware” directory.

When you place these binary files in the correct directory, Avalanche MC will recognize the files within 10 minutes and update the firmware package wizard. An alert is generated if the system detects manual firmware files.

The system will only recognize firmware files that are pre-coded in the existing available firmware list. Avalanche MC will not recognize any firmware file names that do not already exist in the list of supported firmware.

To manually add firmware to Avalanche MC:

1. Obtain the firmware binary files from the device manufacturer, or contact Wavelink Customer Service.

2. Place these folders in the Avalanche MC 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 MC 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 MC Enterprise Server to force Avalanche MC to update immediately.

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

Creating Firmware Packages

A firmware package is a collection of files that allow dServers 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 dServer Location.

To create a firmware package:

1 From the **Tools** menu, select **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 Infrastructure Firmware Support* dialog box appears. This dialog box contains a collection of folders, with each folder representing a specific type of infrastructure device.

4 If you only want to select from firmware bundled with Avalanche MC, enable the **Only show available firmware binaries included on server.**

NOTE When you enable the **Only show available firmware binaries included on server** option, the firmware that requires helper files to run in Avalanche MC will display. Helper files refer to files that are necessary to run these specific firmware versions. The helper files are included with Avalanche MC. This is not a list of firmware included with Avalanche MC, as there are no longer any firmware versions included.

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

5 To select firmware, open the appropriate folder within the dialog box. 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.

6 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 244 for further instructions.

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

The *Enter Package Name* dialog box appears.

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

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

9 Click **Finish**.

Avalanche MC 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 dServers. For information about deploying firmware packages, refer to *Deploying Infrastructure Firmware Packages* on page 336.

Infrastructure Profile Settings and Descriptions

This section provides descriptions of the settings and configurations in the **Infrastructure Profiles** tab, including:

- Infrastructure Profile List
- Infrastructure Profiles General Settings

Infrastructure Profile List

The **Infrastructure Profile List** displays information about your infrastructure profiles.

Field	Description
Name	Displays the name of the infrastructure profile.
Model	Displays the hardware type of the infrastructure device.
Firmware	Displays the firmware version of the infrastructure device.
Status	Displays the enabled/disabled status of the infrastructure profile.

Table 11-2: *Infrastructure Profile List*

Infrastructure Profiles General Settings

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	Sets the firmware version for the infrastructure device.
Use Legacy Management	Determines whether infrastructure settings are defined using the **Infrastructure Profiles** tab or the *Advanced Properties* dialog box. This option is not user configurable.
Default VLAN ID	Sets the number of the default VLAN ID.
Use 802.1Q Tagging	Determines whether to use 802.1Q tagging, the specification that establishes a standard method for tagging Ethernet frames with VLAN membership information.
Manage Infrastructure Using Secure Method	Determines whether the infrastructure device is managed using a secure method (such as SSH).

Table 11-3: *General Settings*

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

Chapter 12: Managing Update Profiles

Control mobile device updates at a more granular level by creating Update Profiles. Update Profiles are intended to decrease traffic by restricting specific mobile devices from contacting the Mobile Device dServer during assigned times. These assigned times are called Exclusion Windows. Exclusion Windows are scheduled periods of time when your mobile devices are not authorized to contact the Mobile Device dServer. Once applied to a region or dServer, the Update Profile regulates when and which mobile devices can contact the dServer for updates.

To conserve bandwidth and increase compliance for critical software updates, you can create separate Update Profiles that are applicable to different groups of mobile devices at different dServers. Use selection criteria to create Update Profiles that specify when certain mobile devices can contact the dServer.

You can improve the performance, responsiveness, and reliability of the update process by optimizing the schedule of the updates. The best way to schedule and apply Update Profiles varies depending on many factors including the number of mobile devices attempting to contact each Mobile Device dServer and your bandwidth capabilities.

You can set similar Exclusion Windows between mobile devices and Mobile Device dServers from the Mobile Device dServer Profile. However, Exclusion Windows from the Mobile Device dServer Profile do not include the selection criteria functionality and the option to schedule Exclusion Windows at different times on different days.

NOTE The dates and times you exclude from scheduling events apply to all events. You cannot set specific exclusion dates and times for each update. You can configure activation for specific software packages from a Software Profile. For more information, refer to *Chapter 10: Managing Software Profiles* on page 209.

This chapter includes the following topics:

- Adding Update Profiles
- Configuring Update Profile Settings
- Adding Update Profiles Authorized Users

- Scheduling Exclusion Windows
- Applying Selection Criteria
- Assigning Update Profiles to Regions

Adding Update Profiles

Create separate Update Profiles based on when you want your mobile devices to contact the Mobile Device dServer.

To add an update profile:

1. From the Navigation Window, select **Update Profiles**.
2. In the **Update Profile List** region, click **Add**.

   An *Input* dialog box appears.
3. Enter a name for the update profile.
4. Click **OK**.

Configuring Update Profile Settings

Before you can apply an Update Profile, you must enable it and configure it. You can set the number of simultaneous updates that can occur at the Mobile Device dServer. Consider how your bandwidth speed may be affected before configuring this setting.

To configure general settings:

1. Select the update profile you want to configure.
2. Click **Edit**.
3. In the **General Settings**, enable the profile.
4. Enable the profile.
5. If you want to allow any number of simultaneous updates, enable the **Allow unlimited simultaneous mobile device updates** option in the **Synchronization Exclusion Window** region.

-Or-

If you want to set the maximum number of simultaneous updates, disable the **Allow unlimited simultaneous mobile device updates** option and type the maximum number of simultaneous updates in the active text box.

6 Save your changes.

Viewing Where Update Profiles Are Applied

The **Applied To** tab in the network profile page allows you to see exactly which regions, dServer 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 dServer Location Properties tabs and assign the profiles there. For information, refer to *Assigning Update Profiles to Regions* on page 256.

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, dServer Location or Site where the profile is applied.
- **Selection Criteria**. Any selection criteria that is applicable at the region, dServer Location or site where the profile is applied.

To view:

1 In the Navigation Window, select **Alert Profiles**.

2 From **Alert Profile List**, select the network profile you want to see.

3 Click the **Applied To** tab.

The tab displays the information for the selected network profile.

Adding Update Profiles Authorized Users

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

To add an authorized user you must have at least one user assigned to Normal permissions, but not that does not have global permission for the profile. Users that have already have permission for the profile will not appear in the Authorized User list.

For information about creating users and assigning permissions, refer to *Chapter 5: Managing User Accounts* on page 85.

To add an authorized user:

1 In the **Update Profiles List**, select the desired profile.

2 Click **Edit**.

3 Select the **Authorized Users** tab and click **Add User**.

   The *Add Authorized User* dialog box appears.

4 From the list, select the user.

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

6 Click **OK**.

   The user is added to the list box and retains permissions for Update Profiles, based on the assigned level.

Scheduling Exclusion Windows

Exclusion windows allow you to schedule times when mobile devices are not allowed to contact the Mobile Device dServer.

To schedule exclusion windows:

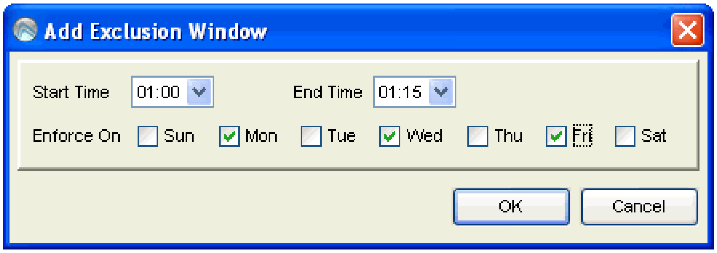
1 Select the update profile for which you are scheduling an exclusion window.

2 Click **Edit**.

3 Select the **Exclusion Window** tab.

4 Click **Add Exclusion Windows**.

The *Add Exclusion Window* dialog box appears.



Start Time 01:00 End Time 01:15

Enforce On ☐ Sun ☑ Mon ☐ Tue ☑ Wed ☐ Thu ☑ Fri ☐ Sat

Figure 12-1. *Add Exclusion Window*

5 Use the **Start Time** and **End Time** drop-down lists to schedule the time of the exclusion window.

6 Enable the days of the week that you schedule the exclusion window.

7 Click **OK**.

The exclusion window appears in the **Weekly View** and **Daily View** of the **Exclusion Window** tab.

8 Save your changes.

Editing Exclusion Windows

Once you have created an exclusion window, you can edit the configuration from the **Weekly View** and **Daily View** regions of the **Exclusion Window** tab.

To edit exclusion windows:

1 Ensure you are in Edit Mode.

1 In the **Weekly View**, select the day of the week you want to modify.

2 In the **Daily View**, click and hold the exclusion window marker.

3 Drag the marker to the time you want to schedule.

4 Save the profile.

Applying Selection Criteria

You can use selection criteria to selectively configure which mobile devices receive the Update Profile. For details about Selection Criteria and the operators to use, refer to *Chapter 18: Selection Criteria* on page 317.

Assigning Update Profiles to Regions

You can assign as many Update Profiles to a region or dServer as you desire. The profiles are applied based on selection criteria for the profile and the order in which the profiles are listed in the Avalanche MC console. Once you assign an update profile to a region, you must perform a Universal Deployment to update your dServers. For more information the Universal Deployment, refer to *Deploying Universal Updates* on page 334.

To assign an Infrastructure profile:

1 From the Navigation Window, select the region to which you want to assign an Infrastructure profile.

2 Click Edit.

3 In the **Update Profile** tab, click **Add**.

The *Add Update Profile* dialog box appears.

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

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

5 Click **OK**.

The profile is added to the **Update Profile** tab for the region.

6 Continue adding profiles to the region, if desired.

7 Use the **Move Up** and **Move Down** buttons to assign the order in which the Infrastructure profiles are applied to mobile devices.

8 Save your changes.

Chapter 13: 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
- Software Inventory
- Controlling the Mobile Device
- Device Statistics

Mobile Device Inventory Tab

The **Mobile Device Inventory** tab lets you view all the devices (and device status) currently associated with Avalanche MC.

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

Model Name The model number of the mobile device.

Terminal ID The unique ID automatically generated by Avalanche MC

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

Last Contact The date and time of the last contact the mobile device had with Avalanche MC.

Recent Activity The current status of a mobile device with respect to Avalanche MC. 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.

The Console supports custom mobile device icons that are sent from the mobile device. There will be two device images 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 dServer, 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 .png image as well. For more information about custom device icons, refer to *Using Custom Device Icons in Avalanche MC*, located on the Wavelink web site.

This section provides information about the following customizing tasks:

- Modifying Columns
- Removing Columns
- Resetting Columns
- Sorting Columns

- Aligning Columns
- Displaying Custom Properties

Modifying Columns

The Avalanche MC 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 column header changes to reflect your modifications.

Removing Columns

You can remove columns that you do not want to display.

To remove a column:

- Right-click the column that you want to remove 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.

Resetting Columns

You can reset the column header to display the original, default columns.

To reset the columns:

- Right-click the in the column header and select **Reset Columns**.

Sorting Columns

You can sort columns in ascending or descending order.

To sort columns:

- Right-click the column you want to sort and select **Sort Ascending** or **Sort Descending**.

Aligning Columns

You can align column information to the left, right or center.

To align columns:

- Right-click the column you want to align and select **Align Left**, **Align Right,** or **Align Center** according to the way you want the information to appear.

Displaying Custom Properties

If you have created custom properties for your mobile devices, you can modify the columns that display in the **Mobile Device Inventory** tab to display columns for these properties.

For details about creating custom properties, refer to *Creating User-Defined Properties* on page 267.

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 to the column list.

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.

Managing Device Filters

This section contains the following information:

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

Creating Device Filters

To display specific devices in the **Mobile Device Inventory** tab, you must first create a new 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 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 276 for more information.

4 When you are finished building a filter, click **OK** to return to the *Modify Mobile Device Filters* dialog box.

The filter 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 Mobile Device Filter** list located at the top of the **Mobile Device Inventory** tab.

Applying Device Filters

After you create device filters, you must apply them to the Mobile Device Inventory list. After 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 Select the filter from the **Current Mobile Device Filter** list.

2 Click **Apply Filter**.

Deleting Device Filters

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

To delete a filter:

1 Select a filter from the **Current Mobile Device Filter** list.

2 Click **Edit Filter**.

The *Modifying Mobile Device Filters* dialog box appears.

3 In the **Existing Filters** region, select the filter you want to delete.

4 Click **Delete**.

Displaying Devices

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

The paging functionality displays the number of devices you select to view per page in the order Avalanche MC pulls those devices from database. If you attempt to page through a selected number of devices and have a device filter applied, you may not see all of your devices that match the filter. This is because Avalanche MC displays the first 25 or 50 devices, and then applies the filter. If there are devices in the list that do not match the filter, those devices are removed from the list. The next number of matching devices is not automatically pulled into the view. You will need to page through the list to view other filtered devices.

To configure device list 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.

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**. This region provides a quick summary of device, health, and battery life information.

  The Health Data icon will display red, yellow or green depending on the health of the device. Health is based on several different things. The following table provides information about the different states of the device:

Green. If the device health icon reports a green status there are no issues with the device. Packages are installed. Battery level, signal strength, signal quality and disk space all meet the specified threshold.

Yellow. If the device health icon reports a yellow status, it could mean any of the following:

- The battery level has dropped below the minimum threshold (default 20% of battery life left). You can configure the threshold based on your requirements.
- The signal strength or signal quality has dropped below the minimum threshold. Default is set at two bars.
- There are software packages that are not completely installed (could be pending or currently installing).
- The disk space has reached the minimum threshold. The program memory and flash memory (a defined flash drive location) both have a default of 5% threshold.

Red. If the device health icon reports a red status, the device is in a critical state.

- The battery level has dropped below the minimum threshold (default 5% of battery life left).
- The signal strength and signal quality have dropped to only one bar.
- A software package has returned an error and cannot be installed.
- The device is in danger of running out of disk space or there is no disk space left.

- **Activity**. This region provides current status information and the time and date the mobile device was last contacted.
- **Device Tabs**. This region provides access to the following tabs:
  - **General**. The **General** tab provides general network and wireless information about the device.

- **Installed Software.** The **Installed Software** tab provides information about the software applications installed on the device. For details, refer to *Software Inventory* on page 269.
- **Packages**. The **Packages** tab lists all the packages currently available for the device and the status of each package. You can view software packages and the current state of each software package associated with the mobile device.
- **Properties**. The **Properties** tab 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 265.
- **Device Control**. The **Device Control** tab 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 *Controlling the Mobile Device* on page 270.

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 user-defined properties. 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 318 for related information.

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

Pre-defined properties are device-specific and dependent on the version of the Avalanche Enabler running on the mobile device. Properties can be used for selection criteria in addition to the selection variables. See *Building Selection Criteria* on page 276 for more information.

From the **Properties** tab, you can perform the following tasks:

- Viewing Properties
- Creating User-Defined Properties
- Creating Device-Side Properties
- Editing Properties
- Deleting Properties

Viewing Properties

You can view the properties associated with a specific mobile device.

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 property is static, snapshot, or configurable data.

Understanding Wireless Properties

Wireless properties are properties that the device reports and are then sent to the Enterprise Server. Any property with a `wles` prefix is considered a wireless property and will be saved to the database.

Understanding Real-Time Properties

Avalanche MC gathers real-time properties from the mobile devices it contacts. These statistics are reported to the console every five minutes. They are not saved to the Mobile Device dServer or the Enterprise Server.

Creating User-Defined Properties

Avalanche MC provides the ability to create user-defined properties on the mobile devices. These properties can then be used to build selection criteria for software updates.

You can add user-defined properties to individual mobile devices or to mobile device groups. When you add a property to a group, it is added to all mobile devices that are members of the group.

Once you create a custom property, you can then use that property in the **Mobile Device Inventory** tab. For more information, refer to *Displaying Custom Properties* on page 260.

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

To create user-defined 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.

Creating Device-Side Properties

You have the ability to create property files on the mobile device and then use those files to collect device-specific information and display this information in the **Properties** tab.

A properties file is a plain-text file with an arbitrary or generic name followed by the `.prf` extension. The plain-text file contains key-value pairs that represent properties. The Avalanche Enabler reads the keyvalue pairs and transfers them to Avalanche MC as properties for the mobile device. These properties are displayed in the **Properties** tab of the Mobile Device Details dialog box.

A properties file must:

- Have a unique name
- Have a `.prf` extension
- Contain a vendor entry
- Contain only one unique key-value pair per line
- Mark supplemental, inconsequential text with the appropriate comment delimiters

Avalanche MC uses the vendor name to organize user-defined properties. The **Properties** tab in the *Mobile Device Details* dialog box displays the device-side properties that it has collected from the mobile device. Each property that displays is prefaced with the vendor name that is specified in the properties file from which Avalanche MC obtained the property. A period (.) separates the vendor name and the property.

For more information about creating device-side properties, please contact Wavelink Customer Service.

Editing Properties

Some of the pre-defined properties (and all of the user-defined properties) support editing of values. When you change the value of a property, the new value is downloaded to the mobile device at the next update.

User-defined properties can be edited either for a specific mobile device or for a group of devices using the group property editor.

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 the Pending Value column for the property.

Deleting Properties

You can delete any configurable mobile device property from the selection criteria builder.

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**.

Software Inventory

This section provides information about the Installed Software tab. 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.

Controlling the Mobile Device

This section provides information about the following tasks that you can perform from the **Device Control** tab:

- Pinging Mobile Devices
- Sending Messages
- Updating the Mobile Device
- RAPI Gateways
- Using Remote Control
- Launching the Session Monitor

Pinging Mobile Devices

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

To ping the client:

1. 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 client 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 clients that are currently in range and running the Avalanche Enabler, an Avalanche-enabled application or, in some cases, a configuration utility.

To send a message:

1 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 the Mobile Device

You can perform individual updates to clients that are currently in range and running the Avalanche Enabler or an Avalanche-enabled application.

NOTE The rules that govern which mobile devices can receive a particular update are determined by the selection criteria. See *Building Selection Criteria* on page 276 for more information.

To update 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 **Update Now** icon.

The *Update Now* dialog box appears.

4 Enable the **Allow User to Override the Update** option if you want to give the mobile device user the option to override the update.

5 Enable the **Force Package Synchronization** option if you want to force the package to update the device.

6 Enable the **Delete Orphan Packages** option if you want to remove orphan packages from the mobile device.

7 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 MC. 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**.

Deleting Mobile Devices

You can delete mobile devices from the Mobile Device Inventory. This removes the device from the **Mobile Device Inventory** tab 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.

RAPI Gateways

Avalanche MC allows you to use Microsoft ActiveSync connections that exist on the system that hosts the Mobile Device dServer. Avalanche MC can automatically detect these connections and create a gateway that allows you to use the connection to facilitate communication between the Mobile Device dServer and a mobile device. The communication medium over which the ActiveSync session has been established does not matter; the communication medium can be serial, USB, IrDA, or RF.

Using Remote Control

Remote Control functionality is only available for devices that have a licensed Remote Control package installed in Avalanche MC.

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 MC.
3. License the Remote Control program.
4. Deploy the Remote Control software package to your mobile device.
5. Begin using Remote Control.

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

This section provides information about the Remote Control tasks you can perform from the **Device Control** tab:

- Connecting to a Mobile Device
- Accessing the File Registry

- Accessing the File Explorer
- Accessing the Process Manager

NOTE For detailed description and information about all the features and functionality of the Remote Control program, refer to the *Wavelink Avalanche Remote Control User's Guide*.

Connecting to a Mobile Device

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

To connect Remote Control to a mobile device:

1 Ensure you have installed the Remote Control package to the Avalanche MC Console and updated 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.

Accessing the File Registry

You can view and make changes to the file registry for a mobile device using Remote Control.

To access the file registry:

1 Ensure you have a Remote Control connection between Avalanche MC and the mobile device.

2 From the **Device Control** tab, double-click the **File Registry** icon.

The device File Registry appears.

Accessing the File Explorer

You can view and make changes in the File Explorer for a mobile device using Remote Control.

To access the file explorer:

1. Ensure you have a Remote Control connection between Avalanche MC and the mobile device.

2. From the **Device Control** tab, double-click the **File Explorer** icon.

   The device File Explorer appears.

Accessing the Process Manager

The Process Manager allows you to view and close programs that are currently running on the mobile device.

To access the Process Manager:

1. Ensure you have a Remote Control connection between Avalanche MC and the mobile device.

2. From the **Device Control** tab, double-click the **Process Manager** icon.

   The Process Manager appears.

Launching the Session Monitor

The Session Monitor utility allows you to view the Telnet Client on a mobile device from the Avalanche MC 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 MC, you will need perform the following tasks:

- Obtain a Telnet 5.x (or later version) software package.

NOTE To obtain software packages, please contact Wavelink Customer Service.

- Install the Telnet software package. Refer to *Installing Software Packages* on page 215 for more information.

- Configure the Telnet Client software package.
- Perform an update to deploy the Telnet Client to the mobile device. For more information about updates, refer to *Deploying Universal Updates* on page 334.
- Launch the Telnet Client on the mobile device.
- Launch the Session Monitor.

This section provides information about launching the Session Monitor from Avalanche MC. For detailed Telnet installation and configuration information, refer to the *Wavelink Telnet Client User's 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 and configured a Telnet package.
2. Select a dServer 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 and connects to the session. 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 and configured a Telnet Client software package.
2. Select a dServer Location or region from the Navigation Window.
3. Click the **Mobile Device Inventory** tab.
4. 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 Click the **Device Details** tab.

6 Double-click the **Session Monitor** icon.

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

Device Statistics

The Enabler will collect various device statistics and write them to a file for later upload to the Avalanche Agent. The Avalanche Agent will eventually send the file on to the dServer. The following _DEVPROP.PRF properties have been defined to help configure the frequency of gathering and reporting statistics to the Avalanche Agent:

Reporting.Stats.Enabled	0-Disable, 1-Enable	Default-1
Reporting.Stats.GatherInterval	0-n, Expressed in minutes	Default-10 min.
Reporting.Stats.ReportInterval	0-n, Expressed in hours	Default-24 hours
Reporting.Stats.ReportFileSize	0-n, Expressed in KB units	Default-512 KB
Reporting.MinimumLinkSpeed	Expressed in KB/sec.	Default-188 KB/s

- **GatherInterval** is how often to take a snapshot of the statistics.
- **ReportInterval** is how often to have the file uploaded to the Agent for reporting.
- If **GatherInterval** or **ReportFileSize** is set to 0, this has the effect of setting **Enabled** to 0.
- **MinimumLinkSpeed** is used to limit the upload to connections that meet the specified link speed only.
- **ReportFileSize** is used to limit the size of the statistics file on the device. Once this threshold is reached, the oldest records will be deleted to make room for new records to be added.

You can view the values for the preceding properties under **Reporting** in the Properties tab of the *Mobile Device Details* dialog box. See *Configuring Mobile Device Properties* on page 265 for related information.

The Enabler will also inventory all installed software packages and (for WindowsCE) all `.eve` files on the device. Since this can be a time consuming operation, the inventory collection is done in the background. Unlike device statistics, the frequency is not configurable. Every 24 hours a new software inventory file is created. The following _DEVPROP.PRF properties are used to configure inventory collection:

Reporting.Software.Enabled	0-Disable, 1-Enable	Default-1
Reporting.MinimumLinkSpeed	Expressed in KB/sec.	Default-188 KB/s

Chapter 14: Managing Mobile Device Groups

To better organize your wireless network, you can use the Avalanche MC 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 devices can be members of multiple mobile device groups.

The topics in this section 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.

If you disable a mobile device group, the group is removed from any Mobile Device dServers in that region.

This section provides information about creating static groups and dynamic groups.

Creating Static Mobile Device Groups

A static mobile device group is essentially a snapshot of all the mobile devices in your inventory that match a set of configured selection criteria.

When you create a static group, you configure the selection criteria for the devices you want to belong to the group. Avalanche MC retrieves those devices currently listed in the Mobile Device Inventory list that match the selection criteria.

If a new device matching the selection criteria for that mobile device group connects to the Avalanche MC Console, it will not automatically be placed in the mobile device group. You will need to manually add any new devices to the group. For information about manually assigning a mobile device to a group, refer to *Adding Devices to Static Mobile Device Groups* on page 280.

To create a static device group:

1 Right-click the **Mobile Device Groups** node in the Navigation Window and select **New Mobile Device Group.**

The *New Mobile Device Group* dialog box appears.

2 Type a name for the group.

3 To enable the group, select **Enabled** from the drop-down list.

4 Enable the **Static** option.

5 Click **OK**.

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

Adding Devices to Static Mobile Device Groups

Once you create a static mobile device group, you can configure the selection criteria for that group.

To add mobile devices to a static mobile device group:

1 From the Navigation Window, select the static group.

2 Right-click and select **Properties**.

The *Mobile Device Group Properties* dialog box appears.

3 Click the **Selection Criteria** button to open the Selection Criteria Builder and then create your selection criteria.

-Or-

Manually type selection criteria into the text box.

For information about building selection criteria, refer to *Building Selection Criteria* on page 318.

4 When you have finished creating the selection criteria, click **Add Matching Devices to Group**.

Avalanche MC locates the matching devices that currently exist in the Mobile Device Inventory list and adds them to the group.

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.

Creating 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 MC 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 MC Console, it is automatically placed in the mobile device group. Therefore, dynamic mobile device groups can be constantly adding and removing mobile devices based on the selection criteria assigned to that group.

To create a dynamic device group:

1 Right-click the **Mobile Device Groups** node in the Navigation Window and select **New Mobile Device Group.**

The *New Mobile Device Group* dialog box appears.

2 Type a name for the group.

3 To enable the group, select **Enabled** from the drop-down list.

4 Enable the **Dynamic** option.

5 Click the **Selection Criteria** button to open the Selection Criteria Builder.

-Or-

Manually type selection criteria into the text box.

For information about building selection criteria, refer to *Building Selection Criteria* on page 318.

6 Click **OK**.

Avalanche MC locates the matching devices that currently exist in the Mobile Device Inventory list and adds them to the group.

Adding Mobile Device Group Authorized Users

The **Authorized Users** tab allows you to assign administrative privileges to for a specified mobile device group to a user that has Normal user rights and is not assigned permissions to group. 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, but not that does not have global permission for the profile. Users that have permission for the mobile device groups will not appear in the Authorized User list.

For information about creating users and assigning permissions, refer to *Chapter 5: Managing User Accounts* on page 85.

To add a user:

1 Right-click a device group in the Navigation Window and select **Properties.**

The *Mobile Device Group* dialog box appears.

2 Select the **Authorized Users** tab and click **Add User**.

The *Add Authorized User* dialog box appears.

3 From the list, select the user.

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

5 Click **OK**.

The user is added to the list box and retains permissions for the mobile device group, based on the assigned level.

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 Right-click the group from the Navigation Window.

2 Select **Ping Mobile Devices** from the menu that appears.

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

Sending Messages to Mobile Device Groups

You can use mobile device groups to send messages to users. This allows you to send the same message to multiple devices simultaneously.

To send messages to device groups:

1 Right-click the group from the Navigation Window.

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

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

Mobile device group properties retrieve the common properties from all the devices in the group. You can then add, edit, and delete properties for mobile device groups.

Mobile device group 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 *Building Selection Criteria* on page 318 for related information.

User-defined properties created within a mobile device group will apply to all devices within that group. If you view an individual mobile device in the **Mobile Device Inventory** tab, you will see that property created for the device within the mobile device group.

To add a property to a mobile device group:

1 Right-click on a mobile device group and select **Edit Device Properties**.

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

2 Click **Add 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 name of the property in the **Property Name** text box.

5 Enter the value of the property in the **Property Value** text box.

6 Click **OK**.

   The new property is added to the properties list.

7 When you are finished adding properties, click **OK** to return to the Avalanche MC Console.

To edit 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 edit and click **Propert**y.

The *Edit Device Property* dialog box appears.

3 Type the new property value.

4 Click **OK**.

The edited property appears in the list.

5 Click **OK** to return to the Avalanche MC 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 Propert**y.

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 MC Console.

The property will be deleted after the next update.

Additional Mobile Device Group Functions

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

The additional options for mobile device groups are as follows:

Enable/Disable	Allows you to enable or disable the group.
Copy	Allows you to copy the group.
Delete	Allows you to delete the group.

Rename Allows you to rename the group.

Mark Orphan Packages for Deletion Marks orphaned packages on the devices within the group for deletion.

Unmark Orphan Packages for Deletion Unmarks orphan packages for deletion.

Update Now Allows you to update all mobile devices within that group immediately.

Chapter 15: Managing Alerts

You can manage network alerts in Avalanche MC using alert profiles. Alerts refer to activity that occurs on a wireless device and ways to respond to those alerts. Examples of when a network alert might be generated are if a Server goes offline or if a new Infrastructure device is discovered. Alert profiles allow you to specify what type of network events generate alerts and where alerts are sent when those events occur.

This chapter provides information about the following topics:

- Managing Alert Profiles
- Creating Contact Lists
- Creating Proxy Pools
- Using the Alert Browser

Managing Alert Profiles

There are three types of alert profiles:

- **Default Alert Profiles**. The default alert profile consists of preset alerts and is deployed as part of the Mobile Device dServer deployment package. These alerts provide information about the Mobile Device dServer only. You do not need to create a new dServer Location alert profile for the Mobile Device dServer. However if you want to receive notifications through e-mail or a proxy, you must create a Normal alert profile configured with events that match the default profile events. You can modify the default alert profile to your preference.
- **Site Alert Profiles**. ISite alert profiles are deployed to the dServer Location and contain a list of events that will generate alerts. When an event that matches the dServer Location alert profile is generated, an alert is sent to the Enterprise Server or configured proxy server. You can assign as many dServer Location alert profiles to a region as you desire. Each dServer Location alert profile deployed to a dServer Location adds to the existing alert profiles at the dServer Location. If you have duplicate alerts configured in profiles, the server will just receive one alert.

- **Normal Alert Profiles**. Normal alert profiles reside at the Avalanche MC enterprise level. These profiles determine when notification of an alert should be sent to the e-mail addresses or proxy. When an alert is generated at the dServer Location level by either the default alert profile or the dServer Location alert profile, that alert is sent to the Enterprise Server. If the alert matches the Normal alert profile, Avalanche MC sends an alert notification to the e-mail addresses assigned to that alert profile or forwards the alert to a proxy computer. If no alerts generated at the dServer Location match the Normal alert profile, no e-mail is sent. Each Normal alert profile deployed to a dServer Location adds to the existing alert profiles at the dServer Location. If you have duplicate alerts configured in the profile, you will receive two separate notifications at either the e-mail address or proxy.

This section provides the following alert-related task information:

- What Type of Alert Profile Should I Create?
- Creating Alert Profiles
- Enabling Alert Profiles
- Configuring Alert Profiles
- Assigning Alert Profiles to a Region
- Removing Alert Profiles

What Type of Alert Profile Should I Create?

The type of alert profile you create depends on what type events you want to be notified of and the manner in which you want to receive the alerts. The Default Alert profile is automatically sent to the Mobile Device dServer, however you can modify it to only alert you of certain events. If you want to receive a notification about the Mobile Device dServer, sent to an e-mail address or proxy server, you must create a Normal alert profile. If you want to receive alerts about individual dServer Locations, you should create a dServer Location Alert profile.

Creating Alert Profiles

When you create an alert profile, you specify the profile as a dServer Location alert profile or a Normal alert profile.

dServer Location alert profiles are configured with a list of events that will generate an alert. These profiles are then deployed to the dServer Location. When an event matching the alert profile occurs, an alert is generated and sent to the Avalanche MC Console. dServer Location alert profiles cannot be configured to send alert notifications to e-mail addresses. You must create a Normal alert profile to receive e-mail notification of alerts. However, you can view dServer Location alerts in the **Health by Location** tab in the Avalanche MC Console.

Normal alert profiles reside at the Enterprise Server level. These profiles exist to send notification of alerts to selected e-mail addresses. To receive e-mail notification of any alerts generated by the dServer Location alert profile, you must create a Normal alert profile that contains events matching those listed in the dServer Location alert profile. Your Normal alert profile must also contain events matching those listed in the default alert profile if you want to receive e-mail notification for any alerts generated by the default alert profile.

You do not need to deploy Normal alert profiles.

To create an alert profile:

1 From the Navigation Window, select the Alert Profiles node.

   The **Alert Profiles** tab appears.

2 In the **Alert Profiles** region, click **Add Profile**.

   The *Input* dialog box appears.

3 Type a name for the alert profile in the **New Alert Profile Name** text box.

4 Click **OK**.

   The new alert profile appears in the **Alert Profile List**.

5 In the **General Settings tab**, select whether this profile is a **Normal** alert profile or a **dServer Location** alert profile.

6 If you want to enable the profile, select the **Enabled** option.

7 From the **File** menu, select **Save.**

   The alert profile is created, enabled and can be assigned to a region and deployed.

Viewing Where Alert Profiles Are Applied

The **Applied To** tab in the network profile page allows you to see exactly which regions, dServer 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 dServer Location Properties tabs and assign the profiles there. For information, refer to *Assigning Profiles to Regions* on page 107.

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, dServer Location or Site where the profile is applied.
- **Selection Criteria**. Any selection criteria that is applicable at the region, dServer Location or site where the profile is applied.

To view:

1 In the Navigation Window, select **Infrastructure Profiles**.

2 From **Infrastructure Profile List**, select the network profile you want to see.

3 Click the **Applied To** tab.

The tab displays the information for the selected network profile.

Configuring Alert Profiles

Once you create an alert profile, you need to assign which alerts should be generated based on events taking place at the dServer Location or enterprise level. If you do not assign any specific alerts, you will continue to receive alerts based on the default profile that is packaged with the Server deployment package. If you configure an alert profile and then assign that profile to a region, the new alert profile overwrites the existing default alert profile at the dServer Locations in that region. Once the default alert profile is overwritten, you can assign more than one alert profile to a region. The alert profiles assigned to each region will not overwrite each over. Instead, each alert profile generate alerts based on the events assigned to that profile.

You can also specify which e-mail address should be notified when an event matching a selected alert occurs and assign proxies from the proxy pool to the alert profile. For information about creating a contact list or a proxy pool, refer to *Creating Contact Lists* on page 293 and *Creating Proxy Pools* on page 295.

To configure an alert profile:

1 In the **Alert Profile List**, select the profile to which you are assigning alerts.

2 Click **Edit**.

3 In the **Profiled Alerts** region, enable any alert that you want to include in this alert profile.

4 If you want to receive an e-mail when a specified event takes place, enable any e-mail addresses in the **Profiled Contacts** list.

NOTE The **Profiled Contacts** list is only available for Normal alerts. For information about creating the **Profiled Contacts** list, refer to *Creating Contact Lists* on page 293.

---

5 If you want to forward alerts that occur to a proxy address, enable the proxy addresses in the **Profiled Proxies** list.

NOTE The **Profiled Proxies** list is only available for Normal alerts. For information bout creating the **Profiled Proxies** list, refer to *Creating Proxy Pools* on page 295.

---

6 Save your changes.

Your alert profile is configured to notify the server when any of those selected alerts occur.

Alert 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 profiles. This means that any user assigned as an authorized user to a profile will have all administrative rights for that one profile.

To add an authorized user you must have at least one user configured with Normal permissions, but not that does not have global permission for the profile. Users that have permission for the profile, will not appear in the Authorized User list.

For information about creating users and assigning permissions, refer to *Chapter 5: Managing User Accounts* on page 85.

To add an authorized user:

1 In the **Update Profiles List**, select the desired profile.

2 Click **Edit**.

3 Select the **Authorized Users** tab and click **Add User**.

   The *Add Authorized User* dialog box appears.

4 From the list, select the user.

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

6 Click **OK**.

   The user is added to the list box and retains permissions for Alert Profiles, based on the assigned level.

Assigning Alert Profiles to a Region

Once you configure an alert profile (Site or Normal), you can assign the profile to a region. Then after the next deployment, the alert profile is applied to the dServer Locations within the region. If you assign a new alert profile to a region, that new alert profile is added to the list of profiles and does not overwrite other Site or Normal alert profiles in that region. 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 Alert Profiles to Regions* on page 110. For more information about performing a Universal Deployment to deploy alert profile changes, refer to *Deploying Universal Updates* on page 334.

Removing Alert Profiles

If you determine that an alert profile is unnecessary, you can delete it from the Avalanche MC 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 **Alert Profiles List**, select the profile you want to remove and click **Remove Profile.**

2. Confirm that you want to remove the profile.

   The profile is removed from the **Alert Profiles List**.

3. From the **File** menu, select **Save.**

Creating Contact Lists

Each Normal alert profile can use one or more e-mail addresses to inform you when a specified event occurs. If you want the Avalanche MC Console to notify you of an alert by e-mail, you must create a contact list. Contacts are available for Normal alert profiles only.

When you create your contact list, you add any e-mail addresses you want to receive alerts to the list. Your entire contact list is available for every Normal alert profile. When you configure Normal alert profiles, you can select which addresses you want to receive alerts from that alert profile.

To create a contact list:

1. From the **Alert Profile List**, select the profile you want to configure.

2. Click **Edit**.

3. In the **Profiled Contacts** tab, select **Edit Contacts**.

   The *Contact Manager* dialog box appears.

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

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

5. To verify the validity of the e-mail server, click **Test Server**.

Avalanche MC attempts to contact the e-mail server and displays a dialog box informing you if it was successful or not.

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

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

7 Add any e-mail addresses to which you want alert notification e-mails sent, such as `jsmith@widget.com`.

- To add an e-mail address, click **Add** and type the appropriate information in the *Contact Information* dialog box. Click **OK**.

The address appears in the **Available Contacts** list.

8 Repeat Step 5 until you are finished adding e-mail addresses.

9 Click **OK**.

The contacts display in the **Profiled Contacts** list box.

NOTE The contact list only applies to Normal alert profiles.

10 Save your changes.

Importing E-mail Addresses

You can add e-mail addresses to the **Profiled Contacts** list by importing a comma-delimited `.csv` file that was exported from Microsoft Outlook.

To import e-mail addresses:

1 From the **Alerts Profile List**, select the profile you want to configure.

2 Click **Edit.**

3 In the **Profiled Contacts** tab, select **Edit Contacts**.

The *Contact Manager* dialog box appears.

4 Click **Import**.

An *Open* dialog box appears.

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

6 Click **Open**.

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

7 Click **OK**.

The contacts display in the **Profiled Contacts** list box.

Removing Contacts

You can delete e-mail addresses from the **Profiled Contacts** list when you no longer need those addresses. When you delete an address from the contact list, that address no longer receives the alerts.

To remove a contact:

1 Ensure you are in Edit Mode.

2 In the **Profiled Contacts** tab, select **Edit Contacts**.

The *Contact Manager* dialog box appears.

3 In the **Available 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 Click **OK** to return to the **Profile Contacts** tab.

Creating Proxy Pools

The Avalanche MC Console allows you to set one or more proxies for an alert profile. When you set a proxy, the console automatically forwards the alert to the IP address of the proxy, enabling you to integrate Avalanche MC with your existing network management tools. To use proxies with alert profiles you must create a proxy pool. Proxies are available to Normal alert profiles only.

To add proxies to the proxy pool:

1 Select the profile you want to configure.

2 Click **Edit**.

3 In the **Profiled Proxies** tab, select **Edit Proxies**.

The *Proxy Pool Manager* dialog box appears.

4 Click **Add**.

The *Add Proxy Address* dialog box appears.

5 In the **Proxy Address** text box, enter the IP address and click **OK**.

The address appears in the **Available IP Addresses** list box.

6 Repeat Steps 2 and 3 until you are finished adding proxy addresses.

7 Click **OK** to return to the **Alert Profiles** tab.

Any proxy addresses you added appear in the **Profiled Proxies** list box.

Deleting Proxies

If a proxy is no longer necessary, you can delete that proxy from the pool.

To delete a proxy:

1 Ensure you are in Edit Mode.

2 In the **Profiled Proxies** tab, select **Edit Proxies**.

The *Proxy Pool Manager* dialog box appears.

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

4 Click **Delete**.

5 Confirm that you want to delete the proxy.

Avalanche MC deletes the proxy from the list.

6 Click **OK** to return to the **Alerts Profile** tab.

Using the Alert Browser

In the **Health by Location** 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 dServer Location that sent the alert stops flashing in the Map pane.

Alert Displays the type of alert.

Date The time and date when the alert occurred.

Description Provides a brief description of the alert.

Acknowledging Alerts

When a new alert appears in the Alert Browser, the dServer 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 dServer Locations in the Map view stop flashing.

Clearing Alerts

When the Alert Browser begins to fill with alerts, you may want to clear out 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 In the **Alert Browser Settings** region, use the text boxes to configure the alert specific 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.

Alert Profile Descriptions

The following tables provide a list of the settings and the description of those settings.

- Alert Profile List
- Alert Profile General Settings

Alert Profile List

The Alert Profile List displays information about your software profiles.

Field	Description
Name	Displays the name of the alert profile.
Status	Displays if the alert profile is enabled or disabled.
dServer Location	Indicates if the alert is a Site alert. If YES, the alert is a Site alert. If NO, the alert is a Normal alert.
Alerts	Displays the number of Profiled Alerts that are assigned to the profile.
Contacts	Displays the number of contacts in the contact list that are assigned to receive notifications from this alert profile.
Proxies	Displays the number of proxies that are assigned to receive nictitation from this alert profile.

Table 15-1: *Software Profile List*

Alert Profile General Settings

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

Field	Description
Name	Sets the name of the alert profile.

Table 15-2: *General Settings*

Field	Description
Status	Sets the status of the profile as either enabled or disabled.
Type	Sets the type of the profile as either Normal or dServer Location. dServer Location alert profiles are deployed to the dServer Location and contain a list of events that will generate alerts. When an event that matches the dServer Location alert profile is generated, an alert is sent to the Avalanche MC server or configured proxy server. You can assign as many dServer Location alert profiles to a region as you desire. Each dServer Location alert profile deployed to a dServer Location adds to the existing alert profiles at the dServer Location. If you have duplicate alerts configured in profiles, the server will just receive one alert. Normal alert profiles reside at the Avalanche MC enterprise level. These profiles determine when notification of an alert should be sent to the e-mail addresses or proxy. When an alert is generated at the dServer Location level by either the default alert profile or the dServer Location alert profile, that alert is sent to the Avalanche MC server. If the alert matches the Normal alert profile, Avalanche MC sends an alert notification to the e-mail addresses assigned to that alert profile or forwards the alert to a proxy computer. If no alerts generated at the dServer Location match the Normal alert profile, no e-mail is sent. Each Normal alert profile deployed to a dServer Location adds to the existing alert profiles at the dServer Location. If you have duplicate alerts configured in the profile, you will receive two separate notifications at either the e-mail address or proxy

Table 15-2: *General Settings*

Chapter 16: Using Scan to Configure

Avalanche MC allows you to create scan to config profiles (barcode profiles) that are configured with network profile 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 stored in the Avalanche profile on the Enabler. You can create as many barcode profiles as you need and save them in the *Scan to Config* dialog box in the Avalanche MC Console.

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 Barcode Profiles
- Printing Barcodes
- Scanning Barcodes

Configuring Barcode Profiles

When you create a barcode profile, you can perform the following tasks:

- Adding Barcode Profiles
- Configuring Network Settings
- Creating Custom Properties
- Editing Barcode Profiles
- Deleting Barcode Profiles

Adding Barcode Profiles

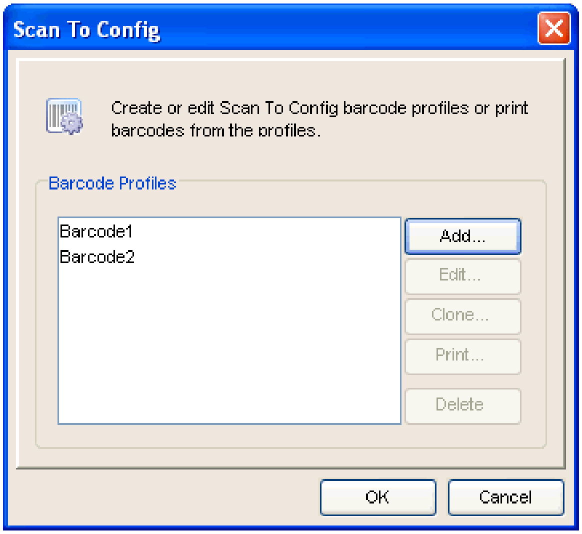
You can create as many different barcode profiles as you need. The profiles appear in the **Barcode Profiles** list box in the *Scan To Config Profile* dialog box. Once you have configured your the network settings for the profile, you can print the barcodes and then use a wireless device to scan the barcode and set the network settings for that device.

When you create a barcode profile, you can also configure a passcode for that 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.

To create a barcode profile:

1 From the **Tools** menu, select **Scan To Config**.

The *Scan To Config* dialog box appears.



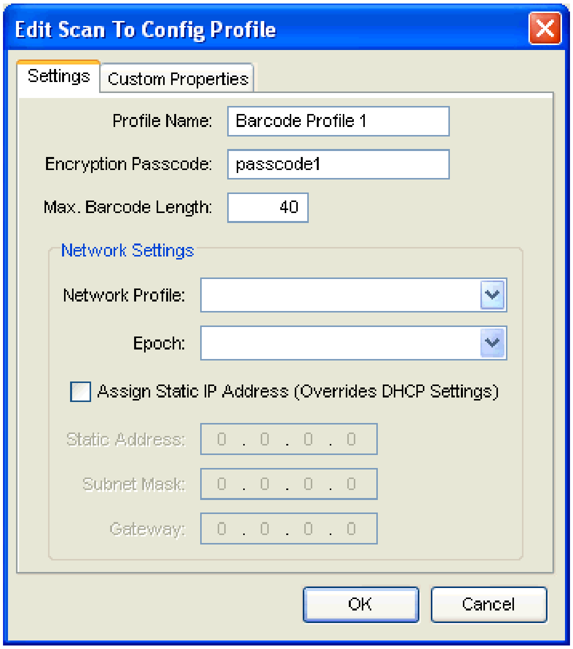
Create or edit Scan To Config barcode profiles or print barcodes from the profiles.

Barcode1
Barcode2

Figure 16-1. *Scan To Config*

2 Click **Add**.

The *Edit Scan To Config Profile* dialog box appears.



Profile Name: Barcode Profile 1

Encryption Passcode: passcode1

Max. Barcode Length: 40

Network Profile:

Epoch:

□ Assign Static IP Address (Overrides DHCP Settings)

Static Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Gateway: 0 . 0 . 0 . 0

Figure 16-2. *Edit Scan To Config Profile*

3 In the **Profile Name** text box, type the name of the profile.

4 In the **Passcode** text box, type the name of the encryption passcode you are going to use (optional).

5 In the **Max. Barcode Length**, type number of characters you want the barcodes to be (1 - 40 characters).

6 Click **OK**.

The barcode profile is added to the **Barcode Profiles** list.

Configuring Network Settings

You can configure the settings of a barcode profile from the *Edit Scan To Config Profile* dialog box.

You need to have created at least one network profile that you can apply to this barcode profile. If you have not created any network profiles, refer to *Creating Network Profiles* on page 144 for information about creating them.

When a mobile device scans the barcode, 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 **Tools** menu, select **Scan To Config**.

The *Scan To Config* dialog box appears.

2 Select the profile you want to configure settings for and click **Edit**.

The *Edit Scan To Config Profile* dialog box appears.

3 From the **Network Profile** drop-down list, select the network profile you want to use for this barcode profile.

For information about creating network profiles, refer to *Creating Network Profiles* on page 144.

NOTE IP pools are not supported. You must specify enable DHCP in the network profile or enable DHCP.

---

4 If the network profile you selected contains epochs, you can select which epoch you want to use.

5 If you want to manually assign a static IP address, subnet mask, and gateway, enable the **Assign Static IP Address** option.

Assigning this information overrides any DHCP settings.

6 Configure the settings.

7 Click **OK**.

The profile is updated with the configured network settings.

Creating Custom Properties

Custom properties allow you to define specific properties that you want applied to the mobile device. These properties are configured into the barcode profile, and then printed out in the barcodes. When the mobile device scans the barcode, the properties are placed on the mobile device. Custom properties are one way of refining selection criteria for mobile devices.

You can perform the following tasks associated with custom properties:

- Adding Custom Properties
- Editing Custom Properties
- Deleting Custom Properties

Adding Custom Properties

When you add a custom property, that property is included in the information created in the barcode. When you scan the barcode with a mobile device, the custom property is placed on the mobile device along with the network profile. Custom properties must be created individually for each barcode profile.

You can create either device specific properties or network specific properties. A device property adds properties in the device properties section on the mobile device and can be used with selection criteria related to that device.

A network property allows custom properties to be configured for the network adapter on the device. This allows flexibility for network management features that may be supported on a particular device.

To add a custom property:

1. From the **Tools** menu, select **Scan To Config**.

   The *Scan To Config* dialog box appears.

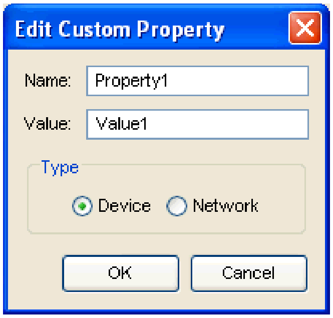
2. Select the profile to which you want to add a custom property and click **Edit**.

   - If you have not created a barcode profile, click **Add**.

   The *Edit Scan To Config Profile* dialog box appears.

3. Select the **Custom Properties** tab and click **Add**.

   The *Edit Custom Property* dialog box appears.



Name: Property1

Value: Value1

Type

● Device ○ Network

Figure 16-3. *Edit Custom Property*

4 In the **Name** text box, enter the name of the custom property.

5 In the **Value** text box, enter the value for the property.

6 Select whether this property is a device specific property or a network specific property.

7 Click **OK**.

The new property is added to the list box for that specific barcode.

8 Click **OK** again to return to the *Scan to Config* dialog box.

Editing Custom Properties

You can edit any custom property in the list box.

To edit a custom property:

1 From the **Tools** menu, select **Scan To Config**.

The *Scan To Config* dialog box appears.

2 Select the profile for which you want to edit a property and click **Edit**.

3 From the **Custom Properties** tab, select the property you want to modify.

4 Click **Edit**.

The *Edit Custom Properties* dialog box appears.

5 Make the desired changes.

6 Click **OK**.

The updated property appears in the list box.

Deleting Custom Properties

You can remove any custom properties that are no longer applicable to the barcode profile.

To remove a custom property:

1 From the **Tools** menu, select **Scan To Config**.

The *Scan To Config* dialog box appears.

2 Select the profile for which you want to remove a property and click **Edit**.

3 From the **Custom Properties** tab, select the property you want to remove.

4 Click **Remove**.

The property is removed from the list box and will not be configured into the barcode profile.

Editing Barcode Profiles

You can edit any of the barcode profiles you create.

To edit a barcode profile:

1 From the **Tools** menu, select **Scan to Config**.

The *Scan To Config* dialog box appears.

2 From the **Barcode Profiles** list box, select the barcode profile you want to modify.

3 Click **Edit**.

4 Make the desired changes.

5 Click **OK**.

You can print the modified barcode profile and update your mobile devices.

Deleting Barcode Profiles

If you no longer need a barcode profile, you can remove it from the barcode profile list.

To delete a barcode profile:

1 From the **Tools** menu, select **Scan to Config**.

The *Scan To Config* dialog box appears.

2 From the **Barcode Profiles** list box, select the barcode profile you want to remove.

3 Click **Delete**.

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

Printing Barcodes

Once you have created and configured a barcode profile, you can print that profile. The profile prints as a set of barcodes in random order. You can then scan the barcodes with the mobile device to set the mobile device network settings.

To print a barcode:

1 From the **Tools** menu, select **Scan to Config**.

The *Scan To Config* dialog box appears.

2 From the **Barcode Profiles** list box, select the barcode profile you want to print.

3 Click **Print**.

The barcode profile is printed as a set of barcodes.

Scanning Barcodes

To deploy the network configurations to the mobile device, you must open the *Scan Configuration* dialog box from the Enabler on the mobile device. Use the mobile device to scan each barcode in any order. This sends the configurations to the Enabler and update the Avalanche 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 also 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 to the Avalanche profile and the *Scan Config* dialog box closes.

Chapter 17: 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 MC 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 is supported by the Infrastructure dServer as opposed to an individual access point. With the Very Large Access Control List enabled for a region, the infrastructure devices refer to the Infrastructure dServer to know which mobile devices are allowed access to the network.

NOTE Mobile devices connecting to a Cisco-Aironet Infrastructure can connect regardless of whether their MAC addresses are listed in the Infrastructure's Access Control List. However, the Infrastructure 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 for a region, allowing any mobile device to connect to dServers within that region.

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
- Importing and Exporting 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 you deploy the Very Large Access Control List to a region, the infrastructure devices within the region check the MAC address of each mobile device against the MAC addresses listed in the dServer's Very Large Access Control List. If the dServer finds a match, it allows the mobile device to connect to the network. If the Infrastructure does not find a match, it refuses to communicate with the mobile device.

Adding Very Large Access Control List Entries

The Avalanche MC 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 additional MAC addresses, or click **OK** to return to the Avalanche MC 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 MC Console deletes the entry from the **Very Large Access Control List**.

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

Importing and Exporting 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 apply the same Very Large Access Control List to multiple regions or save records of entries for backup purposes.

Exporting

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

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. 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 Select **Access Control** from the **Tools** menu.

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 MC Console.

Deploying the Very Large Access Control List

After you create a Very Large Access Control List, you can deploy it to selected dServer Locations and regions. To deploy the VLACL, you perform a Universal Deployment. For information Universal Deployment, refer to *Deploying Universal Updates* on page 334.

Chapter 18: Selection Criteria

Selection criteria are a set 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 determines which mobile devices can receive the software packages contained in the collection. For a network profile, the selection criteria determines which mobile devices can receive the settings contained in the profile.

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

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

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

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

You can use the selection criteria builder to build a valid selection criteria string. You can also use the selection criteria builder to test the selection criteria string on specific mobile devices that appear in the **Mobile Device Inventory** tab.

This section provides information on the following tasks:

- Building Selection Criteria
- Selection Variables
- Operators

Building Selection Criteria

You can access the Selection Criteria Builder from several different places in the Avalanche MC Console, including: Network Profiles, Software Profiles, Infrastructure Profiles, and Mobile Device Groups.

NOTE Selection criteria also applies to software packages, however, you cannot edit software package selection criteria in Avalanche MC.

In the Selection Criteria Builder, you can build the selection criteria string by selection or typing string elements one element at a time. The string elements include:

- Selection variables such as **ModelName** or **KeyboardName**. These variables determine the type of restriction placed on the package or profile. For example, by using a **ModelName** variable, you can restrict the package or profile to a specific class of mobile devices, based on their model numbers. You may use any property that you have assigned a device as a selection criteria variable.

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

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

- Actual values that are assigned to a selection variable. For example, if you assign a value of 6840 to a **ModelName** variable by building the string `ModelName = 6840`, then you will restrict packages or profiles to model 6840 mobile devices.

To build selection criteria:

1. Access the Selection Criteria Builder.

2. From the drop-down list, select a source property and click **Insert Property**.

NOTE For information about source properties, see *Selection Variables* on page 320.

3 Select one of the operator buttons.

NOTE For more information about operators, see *Operators* on page 327.

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

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

NOTE Selection criteria strings are case sensitive.

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

```
ModelName=6840
ModelName = 6840
ModelName=”6840”
```

The following Palm emulation selection criteria string is valid:

```
Series = S
```

While the following is not:

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

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

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

Selection variables for the selection criteria string are as follows:

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

Example:

```
Columns > 20
```

`EnablerVer`

Predefined property designated by the Enabler.

Values with decimals must be surrounded by double quote marks.

EnablerVer = “3.10-13”

`IP`

IP address of the mobile device.

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

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

`KeyboardCode`

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

Supported values include:

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

Example:

```
KeyboardCode = 0
```

`KeyboardName`

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

Supported values include:

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

Example:

```
KeyboardName = 35KEY
```

`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 must be quoted.

- mm/dd/yyyy

  `LastConact = “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”`

- Plus 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)

- Plus 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 as well. Examples include 6840, 3940, 4040. If the model number is unknown, it might appear in one of the views when the mobile device is selected.

A few of the supported values include:

```
1040, 1740, 1746, 1840, 1846, 2740,
2840, 3140, 3143, 3540, 3840, 3843,
3940, 4040, 5040, 6140, 6143, 6840,
6843, 6940, 7240, 7540, 7940, 8140,
8940, PTC960, TR1200, VT2400, WinPC,
WT2200, 7000CE, HHP7400, MX1, MX2, MX3,
VX1, iPAQ, iPAD, Falcon, ITCCK30,
ITC700
```

Example:

```
ModelName = 6840
```

`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 compared in three ways:

- Direct comparison with a single IP address. For example, IP = 10.1.1.1.
- Comparison with an arbitrary address range. For example, IP = 10.1.1.5 – 10.1.1.15 (This can also be written as IP = 10.1.1.5 – 15.)
- Comparison with a subnet number. This is done by supplying the network number along with the 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`

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

Example:

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

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

`Syncmedium`

The type of synchronization medium for the mobile device to use.

Supported values include:

SyncMedium=any
SyncMedium=ip
SyncMedium=serial

`Terminal ID`

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

Example:

```
Terminal ID = 5
```

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

Operators

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

For example:

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

NOTE Spaces around operators are optional.

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

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

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

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

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

All mobile devices with 20 rows receive the software packages within the collection except for those with 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)
```

Both 6840 and 3840 mobile devices can receive the software packages.

`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

The selection criteria targets all non-6840 mobile devices.

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

Example:

```
Rows > 20
```

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

Example:

```
Rows < 21
```

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

Example:

```
Rows >= 21
```

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

Example:

```
Rows <= 20
```

Operators use the following precedence:

1. Parenthesis
2. OR operator
3. AND operator
4. NOT operator

5 All other operators

Chapter 19: Using the Task Scheduler

The Task Scheduler enables you to schedule network management activities for your dServer Locations and regions.

When you configure an aspect of your wireless network using the Avalanche MC Console, those configurations are not immediately sent to the rest of your network. Instead, you schedule specific times during which the new configurations are sent. The Task Scheduler provides several advantages, including the ability to specify which dServer Locations or regions receive the changes and the ability to implement changes during periods of low network activity.

The Task Scheduler allows you to perform the following tasks:

- Deploying dServers
- Deploying Universal Updates
- Deploying Infrastructure Firmware Packages
- Uninstalling dServers
- Backing Up the System
- Restoring the System

Deploying dServers

After you create one or more deployment packages and add one or more dServer Locations to the Avalanche MC Console, you can deploy a dServer using the Task Scheduler. Deploying a dServer is defined as sending a deployment package to a specific location within your network.

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

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

To deploy a dServer Location:

1. If you have not already done so, create a deployment package as described in *Creating Server Deployment Packages* on page 108.

2. From the **Tools** menu, select **Task Scheduler.**

   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** list and click **Next**.

   The *Select Task Destination* dialog box appears.

5. Select the region or dServer Locations by enabling the checkbox next to the region or dServer Location name. You can also select all regions by clicking **All**.

6. Click **Next**.

   The *Select Server Package to Deploy* dialog box appears.

7. Select a dServer package and click **Next**.

NOTE If you have not created a deployment package, you can do so at this time by clicking the **Open Deployment Package Manager** link at the bottom of the dialog box. See *Creating Server Deployment Packages* on page 108 for more information on creating deployment packages.

The *Select Scheduling Options* dialog box appears.

8. Determine when the event will occur and click **Next**.

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

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

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

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

9 Select the start date and time for the event.

10 Determine when you want the event to end.

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

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

11 If you want the start and end time for this event to be based on the local time for the dServer Location, enable the **Use dServer Location's Local Time** option. Otherwise, the start and end times are based on the local time for the Avalanche MC Console.

12 Click **Next**.

The *Review Your Task* dialog box appears.

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

The *Task Scheduled* dialog box appears.

14 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 **Successfully Completed Tasks** list.

NOTE If you want to run the task manually, select the task and click **Run Task**.

Deploying Universal Updates

Anytime you make changes to profiles, settings or configurations in the Avalanche MC Console, you must perform a Universal Update before those changes are applied to your dServers and mobile devices.

To perform a universal deploy:

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

The *Task Schedule* dialog box appears.

2 Click `Add`.

The *Select A Task* dialog box appears.

3 Select `Universal Deployment` from the **Task Type** list and click `Next`.

The *Select Task Destinations* dialog box appears.

4 Select the regions or dServer Locations by enabling the checkbox next to the region or dServer Location name. You can also select all regions by clicking `All`.

5 Click `Next`.

The *Select Scheduling Options* dialog box appears.

6 Determine when the event will occur.

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

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

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

7 Click `Next`.

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

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

- Select the start date and time for the event.
- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the Run until complete option. If you want the event to end after a specified amount of time, select the **End** by option and then select the end date and time for the event. If the event is not finished by this date and time, Avalanche MC will generate an alert.
- If you want the start and end time for this event to be based on the local time for the dServer Location, enable the **Use dServer Location's Local Time** option. Otherwise, the start and end times are based on the local time for the Avalanche MC Console.

9 If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

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

- Select the start time for the event.
- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End** by option and then select the end date and time for the event. If the event is not finished by this date and time, Avalanche MC will generate an alert.
- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.

- If you want the start and end time for this event to be based on the local time for the dServer Location, enable the **Use dServer Location's Local Time** option. Otherwise, the start and end times are based on the local time for the Avalanche MC Console.

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

---

10 Click **Next**.

The *Review Your Task* dialog box appears.

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

The *Task Scheduled* dialog box appears.

12 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 **Successfully Completed Tasks** list.

Deploying Infrastructure Firmware Packages

Once you create a firmware package, you must deploy to the Infrastructure dServers in your dServer Locations and regions.

For information about creating firmware packages, refer to *Creating Firmware Packages* on page 248.

To deploy firmware packages:

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

The *Task Schedule* dialog box appears.

2 Click `Add`.

The *Select A Task* dialog box appears.

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

The *Select Task Destination* dialog box appears.

4 Select the regions or dServer Locations by enabling the checkbox next to the group or dServer 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.

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

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

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

9 Click `Next`.

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

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

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

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

- If you want the start and end time for this event to be based on the local time for the dServer Location, enable the **Use dServer Location's Local Time** option. Otherwise, the start and end times are based on the local time for the Avalanche MC Console.

11 If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

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

- Select the start time for the event.
- Determine when you want the event to stop. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **End by** option and then select the end date and time for the event. If the event is not finished by this date and time, Avalanche MC will generate an alert.
- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for the dServer Location, enable the **Use dServer Location's Local Time** option. Otherwise, the start and end times are based on the local time for the Avalanche MC Console.

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

12 Click **Next**.

The *Review Your Task* dialog box appears.

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

The *Task Scheduled* dialog box appears.

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

Uninstalling dServers

You can remove a dServer from a dServer Location at any time. When you remove a dServer from a dServer Location you will not longer be able to manage mobile devices associated with that dServer. You can either install a new dServer or delete the dServer Location.

To remove a dServer:

1 From the **Tools** menu, select **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** list and click **Next**.

The *Select Task Destinations* dialog box appears.

4 Select the regions or dServer Locations from which you want to remove Servers by enabling the checkbox next to the region or dServer Location name. Click **All** to select all regions.

The *Select Distributed Servers to Uninstall* dialog box appears.

5 Select if you want to uninstall the Infrastructure dServer, the Mobile Device dServer, or both Servers.

The *Select Scheduling Options* dialog box appears.

6 Determine when the event will occur.

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

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

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

---

7 Click **Next**.

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

8 Select the start date and time for the event.

9 Determine when you want the event to end.

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

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

10 If you want the start and end time for this event to be based on the local time for the dServer Location, enable the **Use dServer Location's Local Time** option. Otherwise, the start and end times are based on the local time for the Avalanche MC Console.

11 Click **Next**.

The *Review Your Task* dialog box appears.

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

The *Task Scheduled* dialog box appears.

13 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 the Servers are removed, the task will move to the **Successfully Completed Tasks** list.

Backing Up the System

When you back up Avalanche MC, the database information and software collections are both saved in a zip file. This section provides information about using the Task Scheduler to backup the Avalanche MC system. Avalanche MC Scheduled Task Wizard provides the capability to backup and restore your entire system. You should back up the system regularly, and also when uninstalling Avalanche MC. If for any reason Avalanche MC files are deleted or corrupted, you will be able to restore them from the backup files.

NOTE If PostgreSQL is not installed in the Wavelink directory, backup and restore functionality will fail.

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

The *Task Schedule* dialog box appears.

2 Click **Add**.

The *Select A Task* dialog box appears.

3 Select **System Backup** from the **Task Type** 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.

- If you want the event to occur immediately, select the **Perform the task now** option.
- If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.
- If you want the event to occur on a regular basis, select the **Schedule a recurring event for the task** option.

6 Click **Next**.

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

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

- Select the start date and time for the event.
- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **Use end time** option and then select the date and time for the event. If the event is not finished by this date and time, Avalanche MC will generate an alert.
- If you want the start and end time for this event to be based on the local time for the dServer Location, enable the **Use Location's Local Time** option. Otherwise, the start and end times are based on the local time for the Avalanche MC Console.

8 If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

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

- Select the start time for the event.
- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **Use end time** option and then select the end date and time for the event. If the event is not finished by this date and time, Avalanche MC will generate an alert.
- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for the dServer Location, enable the **Use Location's Local Time** option. Otherwise, start and end times are based on the local time for the Avalanche MC Console.

9 Click **Next**.

The *Review Your Task* dialog box appears.

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

The *Task Scheduled* dialog box appears.

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

The task is added to the **Scheduled and Recurring Tasks** list. The task will run according to its schedule, and once it has completed, it will move to the **Successfully Completed Tasks** list.

Restoring the System

Once the system information has been saved, you can use the Task Scheduler to restore the information to Avalanche MC.

You cannot restore a system backup from a previous version of Avalanche MC. The backup version must match the Avalanche MC version. If you attempt to restore a system backup from a previous version of Avalanche MC, 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.

NOTE If PostgreSQL is not installed in the Wavelink directory, backup and restore functionality will fail.

To restore the system:

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

The *Task Schedule* dialog box appears.

2 Click **Add**.

The *Select A Task* dialog box appears.

3 Select **Restore System** from the **Task Type** 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 MC to the latest backup file.

- Select **Restore by path** to specify the file name and path of the desired system backup.

NOTE The default file path is `C:\Program Files\Wavelink\AvalancheMC\backup`

- Select **Restore selected** to choose the desired system backup according to the tag name.

The *Select Scheduling Options* dialog box appears.

5 Determine when the event will occur and click **Next**.

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

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

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

6 Click **Next**.

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

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

- Select the start date and time for the event.

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

- If you want the start and end time for this event to be based on the local time for the dServer Location, enable the **Use Location's Local Time** option. Otherwise, the start and end times are based on the local time for the Avalanche MC Console.

8 If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

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

- Select the start time for the event.

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

- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.

- Set the start and end dates for the event.

- If you want the start and end time for this event to be based on the local time for the dServer Location, enable the **Use Location's Local Time** option. Otherwise, start and end times are based on the local time for the Avalanche MC Console.

9 Click **Next**.

The *Review Your Task* dialog box appears.

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

The *Task Scheduled* dialog box appears.

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

The task is added to the **Scheduled and Recurring Tasks** list. The task will run according to its schedule, and once it has completed, it will move to the **Successfully Completed Tasks** list.

Appendix A: Manually Deploying Avalanche MC

Avalanche Mobility Center (MC) provides the ability to build packages that allow you to remotely deploy dServers and firmware. The packages that are created in this process rely on a deployment mechanism that is built into Avalanche MC. This enhancement provides an alternative means to deploy packages to remote sites. An alternative means of deployment might be desirable if customers prefer to use custom software for deployment, which might be necessitated, for example, by low bandwidth connections.

Overview

The general tasks required to use local deployment are:

1. Use the Software Package Wizard in the Avalanche MC Console to create an dServer or firmware deployment package (.zip file).
2. Configure the local deployment batch file with the correct parameters.
3. Deploy the package and the local deployment files to the target machine. You can choose your own mechanism to transfer these files to the remote site.
4. Run the batch file locally on a single target machine.
5. Test the deployment on the target machine.
6. Distribute and run the package on other target machines.

The topics in this document include:

- Important Notes About the Package Wizard
- Editing the Local Deployment Batch File
- Deploying dServers

Important Notes About the Package Wizard

When the Package Wizard builds a package, it stores the package file in a subdirectory of `<install directory>\Wavelink\Avalanche MC\Deploy`. The specific subdirectories of interest are:

`\AgentPackage`	Contains the package (.zip) file for an access point dServer and/or a mobile device dServer.
`\FirmwarePackage`	Contains the package (.zip) file for firmware support.

In addition, local deployment files are stored in the following directory:

```
<install directory>\Wavelink\Avalanche
MC\Deploy\LocalDeploy
```

You must place the package file and all files contained in the `\LocalDeploy` subdirectory into a single directory on the target machine.

Editing the Local Deployment Batch File

You can edit the local deployment batch file before or after you transfer the package files and the local deployment files. This file is named `LocalDeploy.bat`. Use a text editor (such as Notepad) to edit the file.

The file contains an example of how to invoke the deploy command. Edit the example according to your site requirements. Depending on whether you are deploying an Infrastructure dServer, a Mobile Device dServer, or firmware support, different switches are required, as shown the following table.

Deployment Type	Deploy Command Syntax
Mobile Device dServer only	deploy -h “-w*Path*” “-i*FileName*” -o*1*
Infrastructure dServer only	deploy -h “-a*Adapters*” “-w*Path*” “-i*FileName*” -o*0*
Both dSErvers	deploy -h “-a*Adapters*” “-w*Path*” “-i*FileName*” -o*2*
Firmware Support	deploy -h “-i*FileName*” -o*3*
Uninstall	deploy -h -o*4*

Table 2-1. *Deployment Commands*

Some of the properties you configure in the Package Wizard are used in Avalanche MC deployment mechanism and are not included in the package file. These properties will need to be manually included in the batch file as described in this section. The following is a complete list of arguments that are needed for deploy.exe:

NOTE If the -h option is used, which indicates this is a local deployment, then -s, -l and -p can be ignored.

Command Line Descriptions

Description for the command line options are as follows:

-h	Required switch that specifies local deployment.
-aAdapters	Specifies the network card(s) that the Infrastructure dServer will use. The Adapters attribute consists of two comma- separated elements, the first of which specifies the network card used to manage devices, and the second value specifies the network card used for access by remote administrators. Each of these elements can be one of the following two values: -f = The first network adapter -s Subnet = The adapter on the specified subnet.(For example, if your adapter is on 172.16.1.16 and your subnet mask is 255.0.0.0, then you would use 172.0.0.0. If your subnet mask was 255.255.0.0, the Subnet attribute would be 172.16.0.0. With a subnet mask of 255.255.255.0, the Subnet attribute would be 172.16.1.0.) Examples: “-a-f, -f” should be used with a single network card or if you want to use the first network card both to manage devices and for remote administration. “-a-f, -s 172.0.0.0” specifies that the first network card will be used to manage devices and the network card residing on the 172.0.0.0 subnet will be used for remote administration. “-a-s 172.16.0.0, -s 10.10.0.0” specifies a subnet for each card when a subnet mask of 255.255.0.0 is in use for both network cards.
-wPath	Specifies the path for installation for one or both dServers. Example: `-wC:\Program Files\Wavelink` If this is a new installation of the dServer(s), this value must exactly match the value configured in the Package Wizard. If you are overwriting an existing installation, the deployment program will automatically install the dServer(s) to the current installation directory.

Table 2-2. *Command Line Descriptions*

-iFileName	The name of the package (.zip) file to install. Example: `-iMMOnly.zip`
-oOption	The installation option. The possible values for the Option attribute are: 0 = Install the Infrastructure dServer 1 = Install the Mobile Device dServer 2 = Install both dServers 3 = Install additional firmware 4 = Uninstall Avalanche MC Example: -o2 The option you choose here must match the option configured in the Package Wizard.
-s	The share directory. Example: `c:\temp folder` and name the share directory <`temp`>
-d	The destination directory on the remote machine. From the previous example this would be `c:\temp`.
-l	The user account to used to map a remote drive. This can be in the format of Domain\User.
-p	The password of the user account specified in the -l option.
-i	The fully qualified path to the zip file.
-x	The fully qualified path to deploy.exe and iserv.exe.
-w	The application install directory. Example: `c:\program files\wavelink`
-q	The Infrastructure dServer path, which is appended to the -w option.
-r	The Mobile Device dServer path, which is also appended to the -w option.
-u	The location of the unzip32.dll. Normally this would simply be "-uunzip32.dll"
-c	The IP address of the site.

Table 2-2. *Command Line Descriptions*

Examples of the Deploy Command

The following example deploys firmware:

- `deploy -h -iC1200-15.zip -o3`

The following example uninstalls Avalanche MC:

- `deploy -h -04`

The following example deploys an Infrastructure dServer:

-
  ```
  deploy -h "-a-f, -s 172.0.0.0" "-wC:\Program 
  Files\Wavelink" -iMMOnly.zip -o0
  ```

NOTE The quotation marks are required when spaces are included in the attribute value.

Deploying dServers

The following steps provide an *example* of how deploy dServers manually.

1. Create a directory called `c:\temp\deployment`.
2. Place an example deployment package called `both-dServers.zip` in the `c:\temp\deployment` directory.
3. Place the following files in the same directory:
   - `deploy.exe`
   - `iserv.exe`
   - `unzip32.dll`

   These files are located in the Avalanche MC deploy directory.
4. Edit the `LocalDeploy.bat` file.

Use the following example switches to deploy both dServers to a site that has the IP address of 10.10.10.10. The `c:\temp directory` is the destination directory.

-
  ```
  deploy -h -o2 -dc:\temp "-ic:\temp\deployment\both-
  dServers.zip" "-a-f, -f"  "-wc:\program 
  files\wavelink" -qmm -ravalanche -uunzip32.dll -
  c10.10.10.10
  ```

5 Open a command line on the target machine.

6 Switch to the directory containing the batch file and all deployment files.

7 Type the command `LocalDeploy.bat` and press the `Enter` key.

NOTE You can use this use this method to deploy dServers to all the sites you use. The only thing that changes is the IP address of the site.

You could also create batch file that takes one argument; the IP address of the site. Using the example above, the batch file would look like this:

```
deploy -h -o2 -xc:\temp\deployment -dc:\temp "-
ic:\temp\deployment\both-dServers.zip" "-a-f, -f"  "-
wc:\programfiles\wavelink" -qmm -ravalanche -
uunzip32.dll -c%1
```

- %1 being the IP address of the site.

NOTE It is highly recommended that you test your batch file and deployment on a single machine before proceeding with a large deployment.

Appendix B: Avalanche MC Services

This appendix lists all of the Avalanche MC services.

Services List

Under each service title, you'll find the file path where the service is located and which type of server (Enterprise Server, Infrastructure dServer or Mobile Device dServer) uses the service.

Wavelink Authentication Service

C:\Program Files\Wavelink\AvalancheMC\CESecureServer.exe

Enterprise Server

Apache Tomcat

C:\Program Files\Apache Software Foundation\Tomcat 5.5\bin\tomcat5.exe

Enterprise Server

Wavelink Agent

C:\Program Files/Wavelink\MM/Program\\AgentSvc.exe

Enterprise Server and Infrastructure dServer

Wavelink Alerts

C:\Program Files/Wavelink\MM/Program\\AlertSvc.exe

Infrastructure dServer

Wavelink Avalanche MC Service Manager (1 of 2)

C:\Program Files/Wavelink\MM/Program\\WLAmcServiceManager.exe

Mobile Device dServer and Infrastructure dServer

NOTE The last Wavelink Avalanche MC Service Manager to be installed determines the path to the service.

Wavelink Avalanche MC Service Manager (2 of 2)

C:\Program Files\Wavelink\Avalanche\Service\WLAmcServiceManager.exe

Infrastructure dServer and Mobile Device dServer

NOTE The last Wavelink Avalanche MC Service Manager to be installed determines the path to the service.

Wavelink Avalanche Agent

C:\Program Files/Wavelink\Avalanche/Service\WLAvalancheService.exe

Mobile Device dServer

Wavelink Avalanche Enterprise Service

C:\Program Files\Wavelink\AvalancheMC\wrapper.exe

Enterprise Server

Wavelink Deployment

C://Program Files//Wavelink//AvalancheMC\IServ.exe

Infrastructure dServer and Mobile Device dServer

Wavelink Information Router

C:\Program Files\Wavelink\AvalancheMC\wlinforailservice.exe

Enterprise Server

Wavelink License Server

C:\Program Files\Wavelink\AvalancheMC\LicenseServer.exe

Enterprise Server

Wavelink Service Manager

C:\Program Files/Wavelink\MM/Program\\svcmgr.exe

Infrastructure dServer

Wavelink Statistics

C:\Program Files/Wavelink\MM/Program\\StatSvc.exe

Infrastructure dServer

Wavelink System Server

C:\Program Files\Wavelink\MM\Program\wrapper.exe

Infrastructure dServer

Wavelink TFTP Server

C:\Program Files/Wavelink\MM/Program\\TftpSvc.exe

Infrastruture dServer

Wavelink-Tomcat

C:\Program Files\Wavelink\MM\Tomcat\bin\tomcat.exe

Infrastructure dServer

Appendix C: Port Information

The tables in this appendix provide information about the ports used in Avalanche MC. The tables include:

- Enterprise Server Ports
- Mobile Device dServer Ports
- Infrastructure dServer Ports

NOTE All ports are inbound ports that must be opened in the firewall.

Enterprise Server Ports

The following table provides a list of ports that the Enterprise Server uses.

Port	Description	Port Type
5432	Avalanche MC JDBC (Internal Use, facilitates communication between the Enterprise Server and PostgreSQL database.	TCP
7221	Avalanche MC License Server	TCP
7226	InfoRail Service IR to IR router port	TCP
7225	InfoRail Service	TCP
5002	AMC Wavelink Authentication Service	TCP
1899	Remote Control Communication	TCP
5001	CE Secure Authentication Service	TCP

Table 4-1. *Ports Used*

Mobile Device dServer Ports

The following table provides a list of the ports that the Mobile Device dServer uses.

Port	Description	Port Type
1777	Mobile Device dServer MU Protocol Service	TCP/UDP

Infrastructure dServer Ports

The following table provides a list of the ports that the Infrastructure dServer uses.

Port	Description	Port Type
7200	Infrastructure dServer RPC	TCP
7208	Infrastructure RMI	TCP
7210	Infrastructure dServer Alert Service RPC	TCP
7211	Infrastructure dServer Service Manager	TCP
7212	Infrastructure dServer SNMP Server	UDP
7213	Infrastructure dServer SNMP Alert Service	UDP
7214	Infrastructure dServer SNMP Statistics Service	UDP
7215	Infrastructure dServer SNMP Server Security	UDP
7216	Infrastructure dServer System Interface	TCP
7217	Infrastructure dServer Web Server (Tomcat)	TCP
7218	Infrastructure dServer Web Server (Apache)	TCP
7219	Infrastructure dServer UDP Proxy (Internal use)	UDP
161	SNMP	TCP/UDP
80	HTTP	TCP
69	Trivial File Transfer Protocol	UDP
23	Telnet	TCP/UDP

Appendix D: Supported Firmware

Avalanche MC is not packaged with any firmware files. You must obtain supported firmware from the manufacturer and then import the files into Avalanche MC.

The following table lists the vender, hardware and firmware versions supported in Avalanche MC.

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	12.3-8JEC 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 12.2-13JA1 12.2-11JA1

Vendor	Hardware	Supported Versions
	1300	12.4.10b-JA 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	12.3-8JEC 12.3-8JEB1 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
	1240 IOS	12.4.10b-JA 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	12.4.10b-JA 10.4-3g-JA 12.3-8JEA3 12.3-8JEA2 12.3-11JA4 12.3-11JA1 12.3-8JEB 12.3-8JEA1 1.3-8JEA
	Cisco 340 AP	12.05 12.04 12.03T 12.02T1 12.01T1 1123T 11.10T1
	Cisco 350 AP	12.05 12.04 12.03T 12.02T1 12.01T1 11.23T 11.10T1
	Cisco 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
Motorola/Symbol	AP-3020	04.02-19
	AP-4121	02.70-12 02.10-06 02.52-13 02.21-23
	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	2.0.0.0-045R 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
	AP-5181	2.0.0.0-045R 1.1.2.0-005R 1.1.1.0-020R
	RSF 7000	1.1.1.0-003R 1.1.0.0-038R 1.0.1.0-012R

Vendor	Hardware	Supported Versions
	WS2000	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 1.5.0.0-216r 1.0.10.08
	WS5000	1.2.0.39o 1.2.0.39f 1.1.4.30f 1.1.430SP1
	WS5000 v1.2+	2.1.4.0-001R 2.1.3.0-010R 2.1.2.0-010R 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 1.4.1.0-014R 1.2.5.0-02R 1.2.0-39o 1.2.0.39f 1.1.4.30f
	WS5100 v1.4+	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 1.4.3.0-012R 1.4.1.0-014R 1.4.4.0-014R
	WS5100 v3.0+	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 2.1.1.0-006R

Vendor	Hardware	Supported Versions
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	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	3.6.3 3.4.0 3.2.1 3.1.0
	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	3.6.6 3.4.0 3.2.1 3.1.0 2.6.0 2.5.2
Systimax	AirSPEED AP 541	2.6.0 2.5.2
	AirSPEED AP 542	2.6.0 2.5.2 2.4.11

Transitional Firmware

The following is a list of transitional firmware. Transitional firmware refers to firmware needed to move to the actual firmware version that is supported in this version for Avalanche MC.

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

- 3.0.0.0-267R v1.4+

Appendix E: Installing Mobile Device Enablers

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

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

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

Where

- *Component* is always `wle`
- *Platform* represents a device type and platform, such as s90
- *OS* represents the operating system, such as DOS
- *Radio* represents the network type, such as 802.11B
- *Version* represents the Enabler version number, such as 1.31
- *Extension* represents the file extension, such as `.hex` for DOS Enablers

An example of an enabler file that uses this convention is wle_s90_ppc2003_8b_350003.exe, which represents the Symbol 9000 Pocket PC 2003 Enabler, version 3.5003, for 802.11B networks.

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

Platform	OS	Radio	Extension
HHP955- - HHP 9500	DO -DOS	SP - Pre 802.11	.hex - for DOS
ick31 - Intermec CK31	ce -CE 2.11	80 - 802.11	.exe - for Win CE
PSC44 - PSC 4400	PP - PPC 3.0	8B - 802.11B	.prc - for Palm

Table A-1. *Enabler File Names*

Platform	OS	Radio	Extension
S3K - Symbol 1K, 3K, 6K	PL - Palm	All - All radios	
s79 - Symbol 7900	W -Windows		
s81 - Symbol 8100			
s90 - Symbol 9000	wm -Windows Mobile		
winpc - Windows PC			

Table A-1. *Enabler File Names*

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

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

To obtain Enablers, contact Wavelink Customer Service.

Downloading Hex Files

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

You can download the Winhex utility at the Wavelink Web site. Contact Wavelink Customer Service for more information.

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

To download the Enabler:

1. Launch the Avalanche MC Console.

2. Verify that a COM port is available for use.

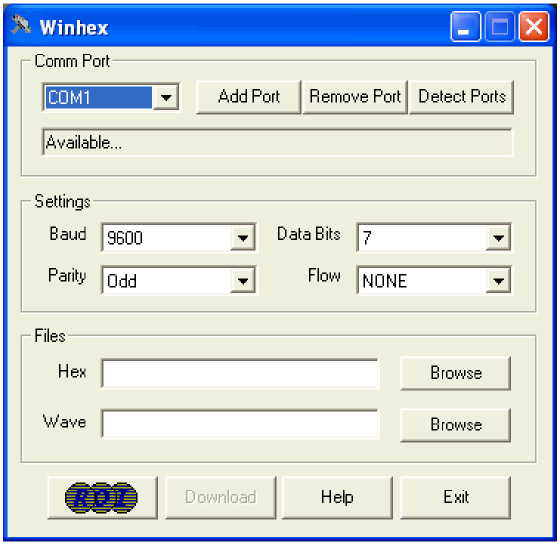
   To check the status on a COM port, click the **Device Settings** tab and read the information that appears in the Serial Communication Settings region. Enable **Reserve Serial Ports 1 and 2**.

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

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

---

3. Launch the Winhex utility.



COM1

Available...

Baud 9600

Data Bits 7

Parity Odd

Flow NONE

Hex

Wave

Figure A-1. *Winhex*

4 From the drop-down list, select the desired COM port.

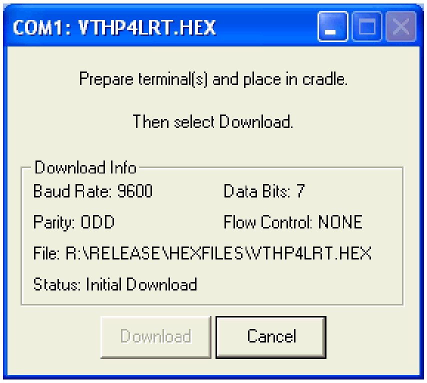
5 Verify that the port status is **Available...**

6 In the **Settings** region, configure the **Baud**, **Data Bits**, **Parity** and **Flow** settings.

7 In the **Files** region, click **Browse** to browse for the location of the hex file.

8 Click **Download**.

The following dialog box appears.



Prepare terminal(s) and place in cradle.

Then select Download.

Download Info

Baud Rate: 9600 Data Bits: 7

Parity: ODD Flow Control: NONE

File: R:\RELEASE\HEXFILES\VTHP4LRT.HEX

Status: Initial Download

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

9 Click `Download`.

NOTE If the **Download** button is disabled, verify that the mobile device is prepared to receive data. See *Downloading the Enabler* on page 371 for more information.

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

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

Downloading the Enabler

The installation of the Avalanche Enabler is OS- or device-specific. For information on loading the Enabler for a specific OS or device type, see the following sections:

- Loading the Enabler on a 3000 Series Device
- Loading the Enabler on Palm OS Devices
- Loading the Enabler on WinCE/PocketPC Devices

- Loading the Enabler on Windows

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

Configuring the Enabler

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

- To configure the mobile device through the Avalanche MC Console, create a network profile. Changes made to configuration through a network profile download to the device the next time the Enabler activates (typically on reboot). See the *Chapter 7: Managing Network Profiles* on page 119 for information about creating a profile.

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

Loading the Enabler on a 3000 Series Device

A 3000 Series mobile device is any Symbol mobile device which relies on a hex image for its initial software download. The actual model numbers are 1xxx, 3xxx, and 6xxx, where each x denotes a digit in the model number. Some example model numbers are 1040, 3840, and 6940.

To install the Enabler on a Series 3000 device:

1 Boot the mobile device into Command Mode, according to the directions in following table:

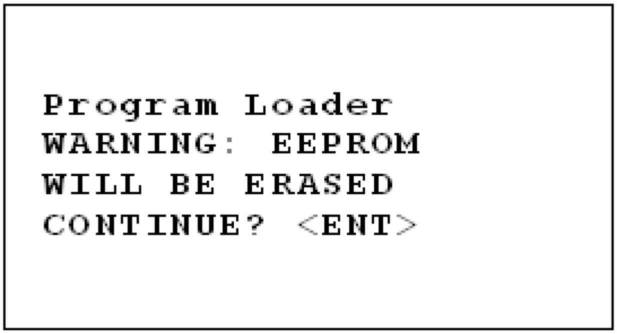
Device Type	Command Mode Boot Sequence
46-key LRT 3840 46-key PDT 3140 47-key PDT 3540 46-key PDT 6840 46-key PDT 6140	Power off the mobile device. Hold F+I. Press and release PWR. Release F+I.
54-key VRC 3940 54-key VRC 6940	Power off the mobile device. Hold A+D. Press and release ON/OFF. Release A+D.
35-key PDT 6140 35-key PDT 3140	Power off the mobile device. Hold BKSP+SHIFT. Press and release ON/OFF. Release BKSP+SHIFT.
27-key WSS 1040	Power off the mobile device. Hold FUNC+ENTER. Press and release PWR. Release FUNC+ENTER.

Table 1: *Command Mode Boot Sequences*

2 Use the up arrow and down arrow keys to select the Program loader function.

3 Place the mobile device in the cradle.

4 Press ENTER. The Program Loader screen appears.

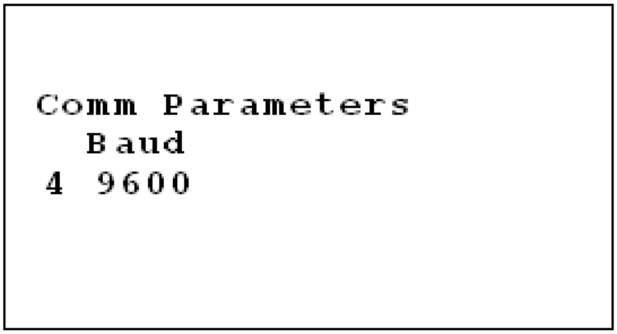


```
Program Loader
WARNING: EEPROM
WILL BE ERASED
CONTINUE? <ENT>
```

Figure A-3. *Program Loader EEPROM Erase*

5 Press `ENTER` to erase the non-volatile memory.

The Baud Parameters screen appears.



```
Comm Parameters
   Baud
 4  9600
```

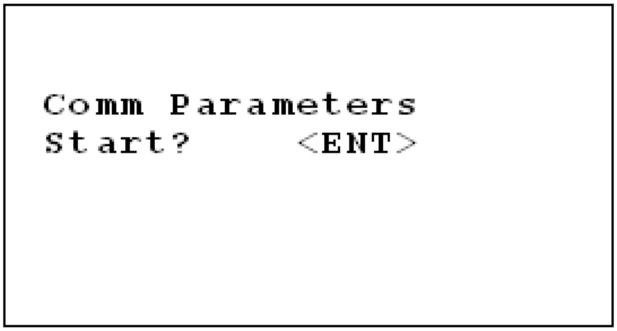
Figure A-4. *Program Loader Comm Parameter*

6 Use the up arrow and down arrow keys to select the communication parameters. Press `ENTER` at the end of the selection to accept the parameters.

Parameter	Value
Baud	38400
Data Bits	8
Parity	None
Flow Control	None

Table A-2. *Download Communication Parameters*

The Comm Parameters screen appears.



```
Comm Parameters
Start?     <ENT>
```

Figure A-5. *Program Loader - Comm Parameters*

NOTE If the cradle supports multiple mobile devices, prepare each in the same manner.

7 Press `ENTER` on the mobile device.

The Program Loader–Receiving screen appears and the mobile device is now ready to download the Enabler.

8 Verify that a COM port is available for use.

To check the status on a COM port, click the **Device Settings** tab and read the information that appears in the Serial Communication Settings region. Enable **Reserve Serial Ports 1 and 2**.

Refer to *Enabling Encryption* on page 196 for more information about COM ports.

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

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

9. Download the Enabler using the Winhex. See *Downloading Hex Files* on page 368 for more instructions.

   After the files have been downloaded, a 3000 Series device indicates a successful file transfer with status code 0000.

Loading the Enabler on Palm OS Devices

Wavelink Avalanche currently supports the SPT 1740 Palm OS device.

NOTE It is assumed that the Palm Desktop is already installed on the system. See the Palm Desktop documentation for more information.

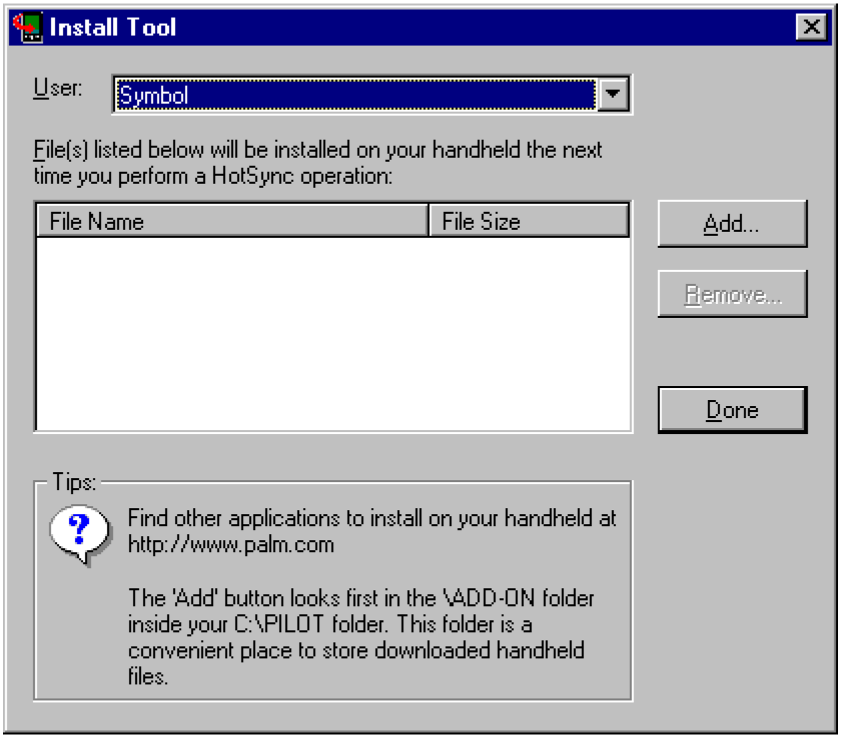
To install the Enabler on a Palm OS device:

1. Acquire the Avalanche Enabler for the device and navigate to the location where you downloaded the Enabler file.

2. Launch the Palm Desktop application on the system.

3. Click the **Install** button on the left hand side of the screen.

   The Install Tool utility appears.



File(s) listed below will be installed on your handheld the next time you perform a HotSync operation:

Find other applications to install on your handheld at http://www.palm.com

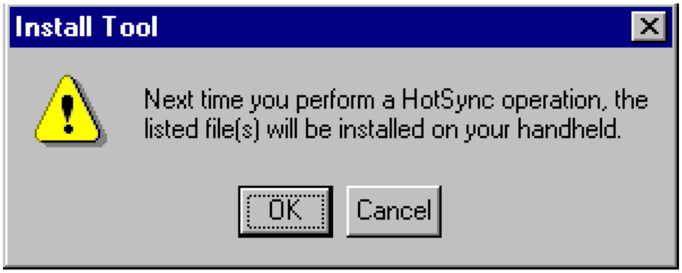
The 'Add' button looks first in the \ADD-ON folder inside your C:\PILOT folder. This folder is a convenient place to store downloaded handheld files.

Figure A-6. *Install Tool*

4 In the Install Tool Window, click `Add`, then browse for and select the Enabler file.

5 Click `Open` and then click `Done`.

The following message box appears.



Next time you perform a HotSync operation, the listed file(s) will be installed on your handheld.

Figure A-7. *Install Tool Message*

6 Exit the Palm Desktop.

7 Hotsync the mobile device.

To Hotsync, connect the mobile device to the serial connection or setup the RF connection (see the Palm Desktop documentation for more information). If the device is set up for serial connection, it will automatically launch the HotSync utility. Otherwise, click the **HotSync** icon on the device.

NOTE When you start the Mobile Device dServer, the dServer will be using any serial ports that it detected. For more information about serial ports, refer to *Enabling Encryption* on page 196. COM ports used by other software programs or hardware peripherals should be removed from the list of available serial ports.

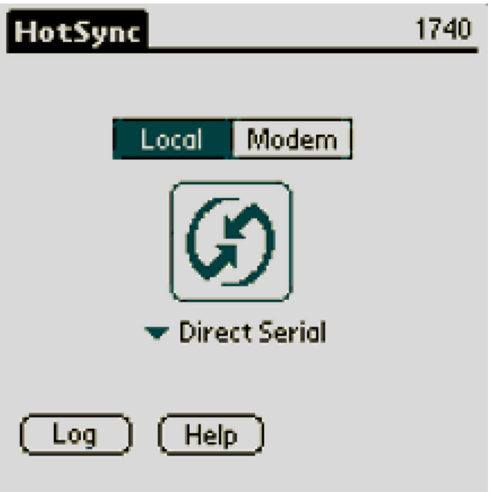


Figure A-8. *The HotSync Screen*

8 Click the Hotsync icon to begin the download process.

Before you can connect to the wireless network, you must configure the network parameters in the Avalanche Enabler.

To configure the Enabler on a Palm device:

1 When the download process is complete, click the **Avalanche** icon on the Applications screen to launch the Avalanche Enabler.

When the Enabler launches, it will first try to associate to an ESSID. If it associates, it then queries the network for Avalanche MC. If it finds Avalanche MC, the Enabler checks to see if Avalanche MC contains a package enabled for it based on its device type, and starts to transfer the package to the mobile device.

The Enabler opens the Select Application screen. This screen provides three options: the **Execute** button runs an installed application; the **Connect** button tries to connect to Avalanche MC; and the **Setup** button opens the Enabler configuration screen. If an application is already installed on the mobile device and appears in the Select Application screen, the Enabler will automatically launch the application after a designated time period, usually about five seconds.

2. In the Select Application screen, click **Setup**.

3. In the Avalanche Settings screen, click **Modify**.

4. On the Network Preference screen, click **Details**.

5. Configure the ESSID, IP address, and DNS settings. When you are finished, click **Done**.

6. In the Avalanche Setup screen, enter the IP address of Avalanche MC and click **OK**.

   The Avalanche Enabler setup is complete. See *Installing Software Packages* on page 184 for information on downloading software packages.

Loading the Enabler on WinCE/PocketPC Devices

Wavelink Avalanche MC currently supports numerous WinCE and PocketPC mobile devices, including Symbol 9000, 8800, and MC3000 CE devices, HHP 9500 Dolphin devices, PSC 4200 and 4400 devices and Intermec CK31 devices.

Contact Wavelink at (425) 823-0111 to obtain the most current list of CE devices supported by Wavelink Avalanche MC.

Before you can download the Enabler and the client files to the mobile device, you must establish a partnership using ActiveSync.

NOTE It is assumed that ActiveSync has been previously installed on the system. Pocket PC devices require ActiveSync version 3.1.

To establish an ActiveSync partnership with the mobile device:

1. Launch ActiveSync.
2. Connect the custom serial cable for the TN client while ActiveSync searches for the mobile device.

NOTE For VRC7900 devices, connect the cable to Port 2.

3. ActiveSync scans the serial ports to find the one that is connected to the mobile device.

NOTE When you start the Mobile Device dServer, the dServer will be using any serial ports that it detected. For more information about serial ports, refer to *Enabling Encryption* on page 196. COM ports used by other software programs or hardware peripherals should be removed from the list of available serial ports.

4. In ActiveSync, select **Get Connected** from the **File** menu.

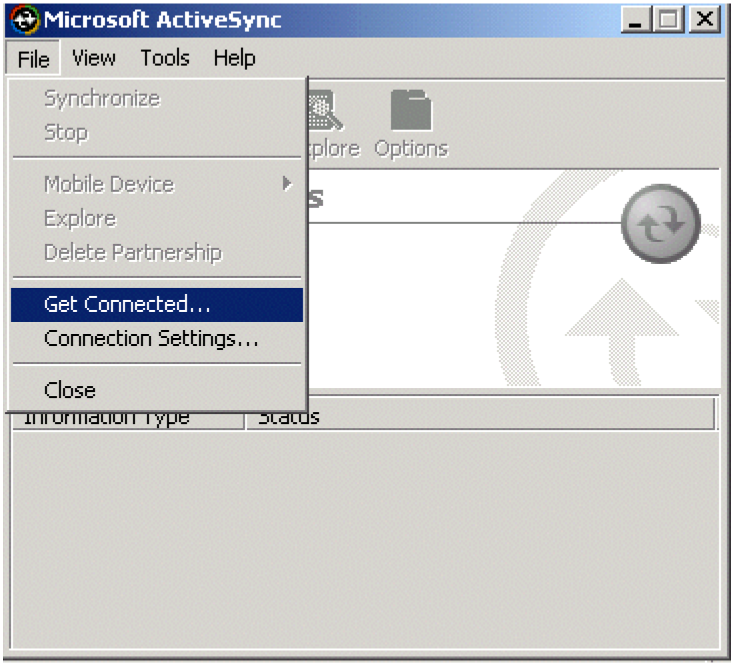
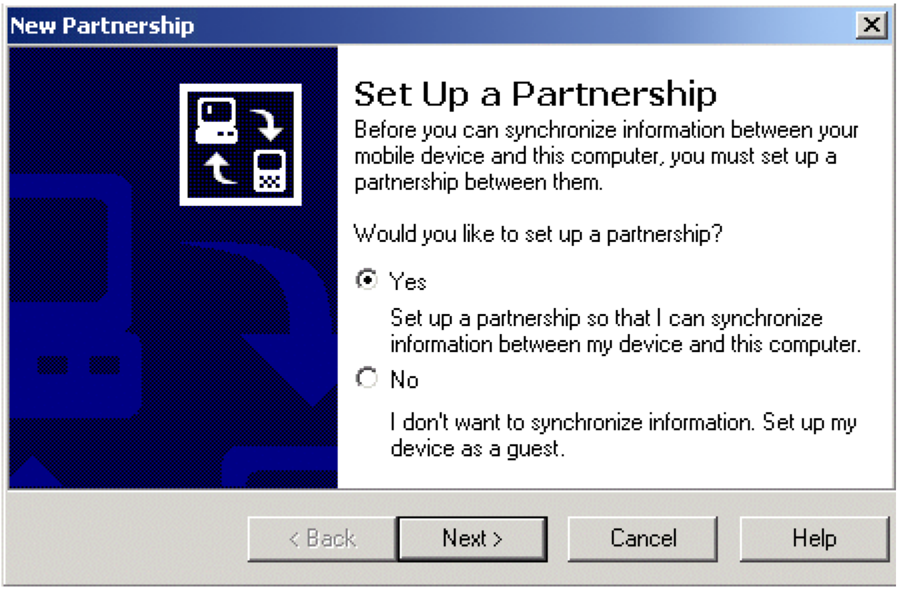


Figure A-9. *ActiveSync Get Connected Menu Option*

An ActiveSync Partnership is required to download the Enabler to the mobile device. The following dialog box appears:



New Partnership

Set Up a Partnership

Before you can synchronize information between your mobile device and this computer, you must set up a partnership between them.

Would you like to set up a partnership?

● Yes

Set up a partnership so that I can synchronize information between my device and this computer.

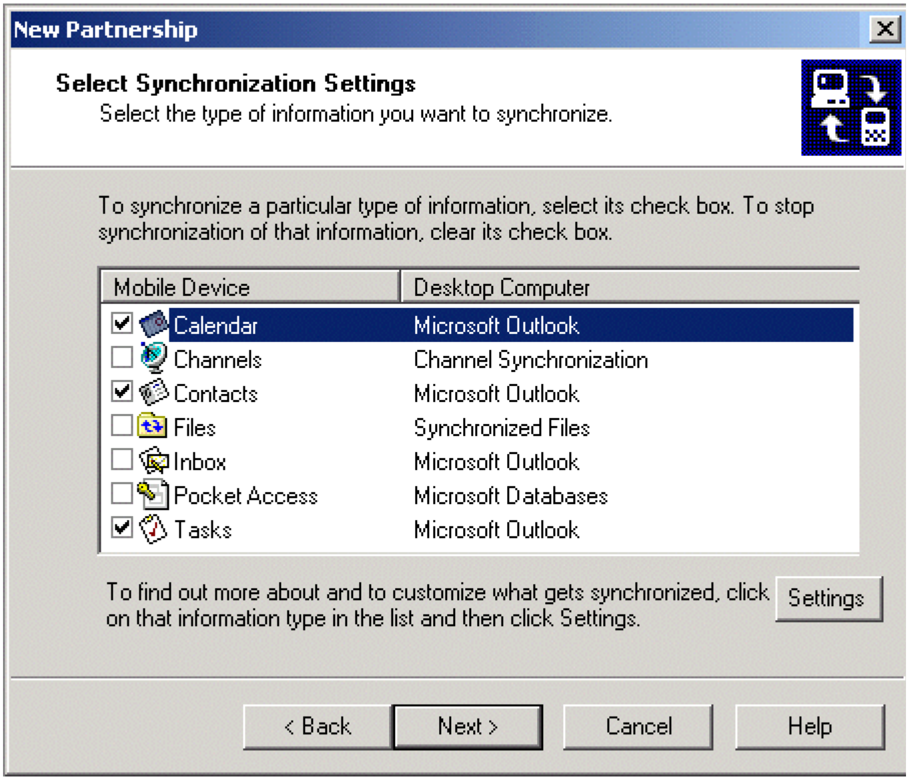
○ No

I don't want to synchronize information. Set up my device as a guest.

Figure A-10. *New Partnership*

5 Follow the on-screen prompts. Synchronize with your system only when prompted.

6 Determine which applications will be used on the mobile device and set the Synchronization Settings accordingly.



New Partnership

Select Synchronization Settings

Select the type of information you want to synchronize.

To synchronize a particular type of information, select its check box. To stop synchronization of that information, clear its check box.

Mobile Device	Desktop Computer
☑ Calendar	Microsoft Outlook
□ Channels	Channel Synchronization
☑ Contacts	Microsoft Outlook
□ Files	Synchronized Files
□ Inbox	Microsoft Outlook
□ Pocket Access	Microsoft Databases
☑ Tasks	Microsoft Outlook

To find out more about and to customize what gets synchronized, click on that information type in the list and then click Settings.

Figure A-11. *Synchronization Settings*

To install the Avalanche Enabler:

1 Verify that ActiveSync is still running. Navigate to the Enabler file and double-click the file to start the Enabler installation.

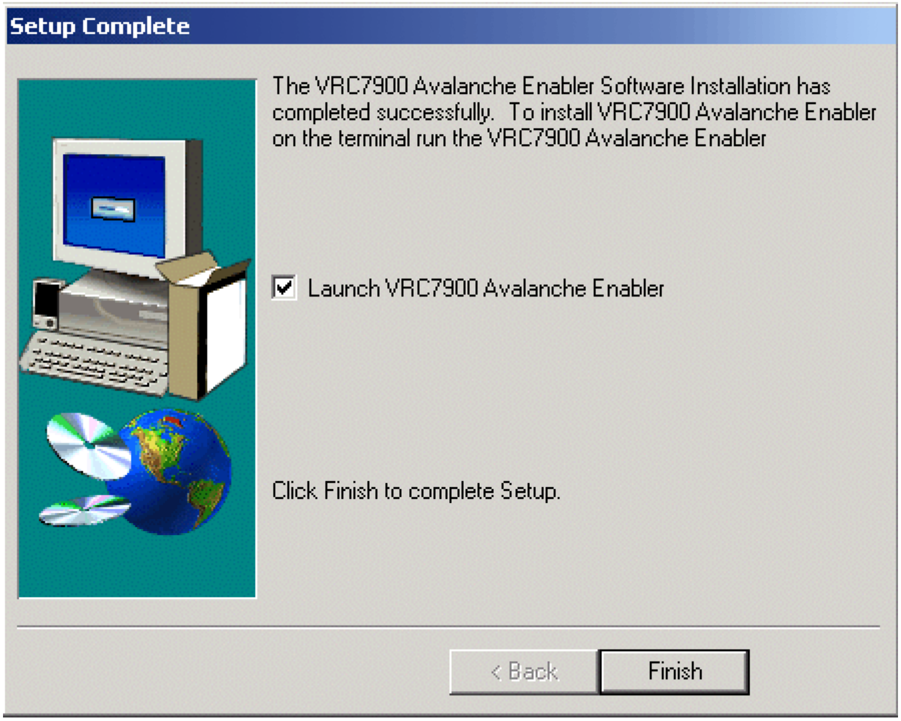
2 In the *Welcome* dialog box, click **Next**.

3 Choose the desired installation destination.

4 Add the program icons to the default program folder of Wavelink Avalanche MC.

5 Add a shortcut on the system when prompted.

6 In the *Setup Complete* dialog box, verify that the **Launch Avalanche Enabler** option is enabled and click `Finish`.



Setup Complete

The VRC7900 Avalanche Enabler Software Installation has completed successfully. To install VRC7900 Avalanche Enabler on the terminal run the VRC7900 Avalanche Enabler

☑ Launch VRC7900 Avalanche Enabler

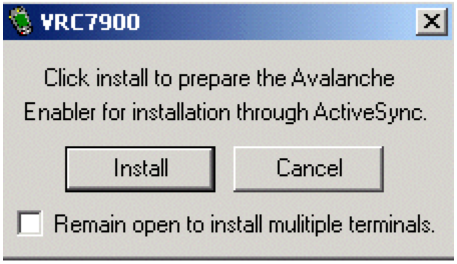
Click Finish to complete Setup.

Figure A-12. *Setup Complete Dialog Box*

The *Install Enabler through ActiveSync* dialog box automatically appears.

7 If multiple mobile devices are to receive the installation files, enable the checkbox in the lower left.

8 Click `Install`.



VRC7900

Click install to prepare the Avalanche Enabler for installation through ActiveSync.

□ Remain open to install mulitiple terminals.

Figure A-13. *Install Enabler through ActiveSync*

9 Follow the on-screen installation prompts to complete the installation of the Enabler on the CE device. It is recommended that the default folder be used.

NOTE If this is a reinstall, the prompts on the system and the mobile device will indicate this. Respond to these prompts as needed.

Before you can connect to the wireless network, you must configure the network parameters in the Avalanche Enabler.

To configure the Enabler on a Windows CE/Pocket PC device:

1 On the mobile device, click the **Avalanche** icon to launch the Avalanche Enabler.

When the Enabler launches, it will first try to associate to an ESSID. If it associates, it then queries the network for Avalanche MC. If it finds one, it checks to see if there is a package enabled for it based on its device type, and it will start to transfer the client to the mobile device. If the device is connected to the system by a serial connection, the mobile device will also query to find Avalanche MC, and then transfer any enabled packages with which it is associated.

The Enabler will open the *Select Application* dialog box. This dialog box provides three options; the **Execute** button runs an installed application; the **Connect** button tries to connect to Avalanche MC, and the **Setup** button opens the *Avalanche Configuration* dialog box. If an application is already installed on the mobile device and appears in the *Select Application* dialog box, the Enabler will automatically launch the application after a designated time period, usually about five seconds.

2 In the *Select Application* dialog box, click **Setup**.

The *Avalanche/IP Configuration* dialog box appears. The first tab has boxes to enter in the Avalanche MC IP address and another box to enter in the ESSID.

3 Click the **IP** tab to configure IP settings. Here you can set the mobile device to use DHCP or manually input an IP address, subnet mask, and gateway.

4 Click the **DNS** tab and, if necessary, and enter the required DNS settings.

5 Click **OK**.

A dialog box appears with the following message: “The next time the adapter is used the new settings will take place.”

6 Click `OK`.

The Avalanche Enabler setup is complete. See *Installing Software Packages* on page 184 for information on downloading software packages.

Loading the Enabler on Windows

Follow these steps to download and install the Avalanche Enabler onto a computer using a Windows operating system.

1 Download the Enabler from the Wavelink Web site.

2 Open the downloaded file.

A *Welcome* dialog box appears.

3 Click **Continue** to start the installation process.

An introductory dialog box appears, providing information on the installation process.

4 Click **Next**.

The *License Agreement* dialog box appears.

5 If you agree to the terms of the license agreement, click **Yes** to continue.

The *Choose Destination Folder* dialog box appears.

6 Select the destination folder for the Enabler and click **Next**.

The *Select Program Folder* dialog box appears.

7 Select the program folder for the Enabler and click **Next**.

The Enabler is installed. After the installation is complete, a dialog box appears, asking if you want to create a shortcut icon to the Enabler on your desktop. Click either **Yes** or **No**.

The *Setup Complete* dialog box appears.

8 To start the Enabler immediately, enable the **Yes, I want to launch the Enabler now** checkbox and then click `Finish`. Otherwise, click `Finish` to complete the installation.

Future Releases

Support for mobile devices continues to expand. Contact your Wavelink Customer Service for information on availability of Avalanche Enablers for mobile devices not otherwise listed. For contact information, refer to *Appendix G: Wavelink Contact Information* on page 405.

Appendix F: Managing Avalanche MC on Linux OS

Avalanche MC allows you to install and manage the Avalanche MC Enterprise Server, the Mobile Device dServer, the License Server and the InfoRail service on a Linux operating system.

NOTE You will need to install the Avalanche MC Console on a Windows operating system to manage your infrastructure and mobile devices.

This document provides detailed instructions about the following information:

- Overview of Installation Steps
- Mobile Device dServer Installation Requirements
- Creating Server Directories
- Setting User Permissions
- Initializing the Database
- Installing the Enterprise Server
- Installing the Mobile Device dServer
- Installing the InfoRail Service
- Installing the License Server
- Starting the Servers
- Managing the Mobile Device dServer
- Using the Package Converter
- Increasing the Open Files Limit
- Generating Licenses

Overview of Installation Steps

Perform the following steps, in order, to ensure the servers are correctly installed on a Linux operating system:

1. Obtain the Enterprise Server, Mobile Device dServer, License Server and InfoRail service tar files.

NOTE To obtain these files, contact Wavelink Customer Service at customerservice@wavelink.com.

2. Verify installation requirements.
3. Create directories for the Enterprise Server, Mobile Device dServer, License Server and InfoRail service tar files.
4. Extract the server files to the proper directories.
5. Set user permissions to allow the Linux user to execute commands for each server.
6. Initialize the database for Avalanche MC.
7. Run the servers.

Enterprise Installation Requirements

- 2.6 kernel
- Java Run-Time Environment (JRE) 1.6
- PostgreSQL 8.6.2
- Sufficient rights to install programs and create and maintain the Avalanche MC Server working directory
- Firewall openings for Server services
- Intel Pentium 4 Processor at 2.8 GHz (or equivalent).
- 1 GB RAM

- 2 GHz and above
- Required free disk space: 20 GB
- Recommended free disk space: 100 GB

Mobile Device dServer Installation Requirements

The following specifications are required to install the Mobile Device dServer on a Linux OS:

- 2.4 or 2.6 kernel
- 256 MB of physical RAM (512 MB or more is recommended)
- 200 MB or more of available hard disk space (plus additional space for software packages)
- Sufficient rights to install programs and create and maintain the Avalanche MC Server working directory
- Sufficient rights to access USB and serial ports
- Firewall openings for Server services
- The Linux user account that is running the Mobile Device dServer must be a member of the **tty** and **uucp** groups for USB and serial support
- Sufficient number of open files. Refer to *Increasing the Open Files Limit* on page 402 for information about allowing more files to be open.

Creating Server Directories

You must create directories before you can install the servers.

To create wavelink directories:

1. Log in as root.
2. Create the following directories:
   - `/opt/wavelink`

- `/var/opt/wavelink`

  You will install the Enterprise Server, Mobile Device dServer, License Server and InfoRail tar files to these directories.

3 Change the owner of both directories to a non-root user.

4 Log out.

5 Login again as the non-root user.

  You can now install the Enterprise Server, Mobile Device dServer. License Server and InfoRail files.

Setting User Permissions

Before you can execute any scripts to start the Enterprise Server, Mobile Device dServer or InfoRail service, you need to set permissions that allow the user to execute scripts.

To set permissions:

1 Open a terminal and navigate to `/var/opt/wavelink/eserver.`

2 Set the permissions to allow the user to execute scripts by typing

```
chmod +rwx *
```

  You can now execute the scripts needed to run Avalanche MC.

Initializing the Database

Initializing the database creates a database for Avalanche MC within the PostgreSQL engine. To initialize the database, you run a script that connects to PostgreSQL and executes a series of sequel scripts. This creates a database for Avalanche MC within the PostgreSQL database engine. You can view the sequel scripts in the /var/opt/wavelink/eserver/db directory. The script also seeds the database with the information that the system needs to operate Avalanche MC.

To initialize the database:

1 Navigate to System Settings > Server Settings > Services.

2 Select PostgreSQL and enable the checkbox.

3 Click Start.

4 Open a terminal and navigate to /var/opt/wavelink/eserver.

5 Type `./db_setup.sh`.

The PostgreSQL database engine creates a database for Avalanche MC. You can now install and start the Enterprise Server.

Installing the Enterprise Server

The Enterprise Server manages mobile devices and infrastructure devices. You must manage the Enterprise Server through the Avalanche MC Console which must be installed on a machine with a Windows operating system.

To install the Enterprise Server

1 Ensure you have created the appropriate directories and are logged in as a non-root user.

2 Extract the file `eserver.450.tgz` to the `/var/opt/wavelink` directory.

Once you extract the Enterprise Server tar file, you must set user permissions and initialize the database before you start the Enterprise Server. For more information refer to *Setting User Permissions* on page 392 and *Initializing the Database* on page 392.

Installing the Mobile Device dServer

Installing the Linux Mobile Device dServer involves extracting the tar file that comes bundled with Avalanche MC. Once Avalanche MC is installed, the tar files `gen26_WLAvalanche_450.tgz (for the 2.6 kernel) and RH8_WLAvalanche_450.tgz (for the 2.4 kernel)` will be located in `<Avalanche MC install directory>/deploy`.

To extract the tar file on a Linux OS:

1 Save the appropriate file for your system in an installation directory of your choice.

The recommended installation directory is `/opt/Wavelink/avalanche`. The Avalanche MC dServer is designed to use `/var/opt/Wavelink/avalanche` as its working directory.

2 Open a shell and navigate to the installation directory.

3 Type `tar -xzf ./Avalanche_450.tgz` and press `Enter`.

The tar file will create the binaries `WLAvalanche`.

Installing the InfoRail Service

When you install the InfoRail service on Linux, you extract the tar file gen26_WLInfoRail_450.tgz to the appropriate directories.

To install the InfoRail:

1 Create the following InfoRail directories in both `/opt/wavelink` and `/var/opt/wavelink`.

- `/opt/wavelink/inforail`
- `/var/opt/wavelink/inforail`

2 Extract the tar file `gen26_WLInfoRail_50.tgz` to the `/opt/wavelink/inforail` directory.

Once you extract the tar file, you must set user permissions before you start the InfoRail service. For more information refer to *Setting User Permissions* on page 392.

Installing the License Server

Extract the License Server files to the appropriate directories.

To install the License Server:

1 Create the following License Server directories in both `/opt/wavelink` and `/var/opt/wavelink`.

- `/opt/wavelink/licenseserver`
- `/var/opt/wavelink/licenseserver`

2 Extract the tar file `gen26_WLLicenseServer_450.tgz` to the `/opt/wavelink/inforail` directory.

Starting the Servers

Once you extract the server files, set user permissions and set up the database, you can start the Enterprise Server, Mobile Device dServer, License Server and InfoRail service.

To start the Enterprise Server:

1 Open a shell and navigate to `/var/opt/wavelink/eserver`

2 Type `./eserver.sh` and press `Enter.`

The Enterprise Server is running on the system.

To start the InfoRail service:

1 Open a shell and navigate to `/opt/wavelink/inforail`.

2 Type:

- `./WLInfoRail for linux kernel 2.4`

NOTE To run as a daemon, append –d to the end of the execute command. Append -t to stop the daemon

3 Press `Enter`.

The InfoRail service is running on the system.

To start the Mobile Device dServer:

1 Open a shell and navigate to `/opt/wavelink/avalanche`.

2 Type:

- `./WLAvalanche`

NOTE To run as a daemon, append –d to the end of the execute command. Append -t to stop the daemon.

3 Press `Enter`.

The Mobile Device dServer is running on the system.

To start the License Server:

1 Open a shell and navigate to `/opt/wavelink/licenseserver`.

2 Type:

- `./WLLicenseservice`

NOTE To run as a daemon, append –d to the end of the execute command. Append -t to stop the daemon.

---

3 Press `Enter`.

Managing the Mobile Device dServer

Once you install and start the mobile Mobile Device dServer, you can manage the dServer from the Linux system on which it is installed.

NOTE To manage the dServer from the Avalanche MC Console, you must configure the dServer to connect with an Enterprise Server (Windows or Linux platform). The Avalanche MC Console must be running on a Windows platform (Windows 2000, XP Professional, or Windows 2003 Server).

The following information is included in this section:

- Configuring Linux Mobile Device dServer Communication
- Manually Installing License Files
- Configuring Serial and USB Support
- Managing the Linux Mobile Device dServer from the Console

Configuring Linux Mobile Device dServer Communication

Before the dServer will function properly, you must complete the following steps:

- Configure Avalanche.properties
- Configure the Firewall

Configure Avalanche.properties

To configure the dServer to connect to the Avalanche MC Enterprise Server and License Server, create and configure an `Avalanche.properties` file.

To configure the dServer properties:

1. Create a file named `Avalanche.properties` in the working directory and use a text editor to add the following properties to the file:

   ```
   InfoRail.Server=<IP address of the Enterprise Server>
   Licenseserver=<IP address of the License Server>
   SiteIndentifier=<IP address of the dServer>
   ```

   For example:

   ```
   InfoRail.Server=62.4.56.3
   Licenseserver=62.4.56.3
   SiteIndentifier=62.4.56.3
   ```

NOTE If you plan to manually install a license file (`.lic or .abr`), you do not need to include the `Licenseserver` property.

2. Save and close `Avalanche.properties`.

   The dServer will now be able to connect to the Enterprise Server and the License Server.

Configure the Firewall

Open TCP and UDP ports 1777 in your firewall to allow the Linux Mobile Device dServer to communicate with mobile devices. The dServer must be permitted to create unrestricted outbound TCP/IP connections.

For more information about ports necessary to run Avalanche MC, refer to Appendix C in the *Avalanche MC User Guide*.

Manually Installing License Files

Normally the dServer will automatically retrieve a license from the License Server. However, if you are not using a License Server, you can manually license the Linux Mobile Device dServer. License files can either be `wavelink.lic` files or brand license files (`.abr`).

To manually license the Mobile Device dServer license file:

1. Open a shell and navigate to the working directory.
2. Type `./WLAvalanche -n` and press `Enter`.

   The nodelock number of the Linux system displays. You will need to provide this number to Wavelink Customer Service to obtain a license.
3. Save the license file in the `<working dir>/MAIN.PRF` directory on the machine running the Mobile Device dServer.
4. Restart the Mobile Device dServer.

   The Mobile Device dServer is now licensed and can be managed from the Avalanche MC Console.

Managing the Linux Mobile Device dServer from the Console

Once the Mobile Device dServer is installed, configured, and has contacted the Enterprise Server, it appears in the **Unassigned dServer locations** folder of the Avalanche MC Console. The dServer Location can be identified by the IP address of the Linux host. You can then move the dServer Location to a region and rename, configure, and manage it. The Mobile Device dServer will not accept connections from mobile devices until it is assigned to a region.

NOTE If the Mobile Device dServer does not appear on the Avalanche MC Console, check to make sure the information in the `Avalanche.properties` file is correct.

NOTE Some older software packages may not install properly on a Linux host because of file path case sensitivity. If a package installs correctly in Avalanche MC but is not distributed to a Mobile Device dServer (possibly resulting in a software installation failure alert), retrieve the

`Avalanche.log` file from the Linux host and inspect it for package installation errors. Wavelink Customer Support can help with the proper formatting of older or custom-built packages that may fail due to case-sensitive paths.

Configuring Serial and USB Support

Mobile devices can communicate with the Mobile Device dServer via a serial or a USB connection. The Linux user account that is running the Mobile Device dServer must be a member of the **tty** and **uucp** groups in order for USB and serial support to work.

This section provides the following information:

- Enabling Serial Support
- Enabling USB Support

Enabling Serial Support

The mobile device and the Mobile Device dServer must both be configured to enable serial communication. To enable serial communication on your mobile device, refer to the specific user manual for that device. You can configure the Mobile Device dServer for serial connections through the Avalanche MC Console.

To configure serial connections:

1. From the Avalanche MC Console, select the **Mobile Device dServer Profile** node.

   The **Mobile Device dServer** tab appears.

2. Select the Mobile Device dServer profile that you want to configure.
3. Click the **Device Connections** tab.
4. In the **Serial Communication Settings (RS232)** region, enable the **Reserve Serial Ports 1 and 2** checkbox to reserve those two ports for mobile device communication on the dServers.
5. Save your changes.
6. Assign the updated Mobile Device dServer Profile to the correct region or deploy the updated settings to the correct region.

Serial communication is now enabled for all the Mobile Device dServers in that region.

Enabling USB Support

USB connections are only available if you have a Linux kernel 2.6.9 or newer. The manufacturers and device codes supported through the USB serial interface can be found in the source code for the ipac driver (usually `/usr/src/linux/drivers/usb/serial/ipac.c`).

USB connections are only supported on devices with a 3.50-29 (or later) version of the Wavelink Avalanche Enabler. To establish a USB connection between the mobile device and the Mobile Device dServer, you must configure the Enabler for USB connections.

To configure the Enabler to communicate over a USB connection:

1. Access the **Connection** tab for the Enabler configuration.
2. Enable the following checkboxes:
   - **Check serial connection**
   - **Disable ActiveSync**

   The mobile device will now be able to connect via USB.

To connect to the Linux Mobile Device dServer over a USB connection:

1. Ensure that the Enabler is configured correctly.
2. Connect the device to the Mobile Device dServer system with the proper USB cable.
3. From the mobile device, force a connection to the Mobile Device dServer by selecting **Connect** from the Avalanche Enabler **File** menu.

   The mobile device will indicate that it has established a serial connection with the Mobile Device dServer, and will download any required updates over this connection.

NOTE You cannot use the console to force an update to the client over the USB connection (i.e. via the **Update Now** Avalanche MC Console command).

Using the Package Converter

The Avalanche Package Converter allows you to take older `.ava` files and convert them into a format that is suitable for Linux.

Requirements

The Avalanche Package Converter requires Java JRE or JDK version 1.3.1_03 or above to run. The Java executable should be in the search path.

The Package Converter also needs some temporary disk space for its operation.The program uses the system temporary directory defined with the TMP environment variable for that purpose. If necessary, you can set the TMP variable before running the program.

The Avalanche Package Converter must be run on Windows platform.

Converting Packages

The Package Converter is a `.zip` file. To obtain the converter, contact customer service. The `.zip` file contains the following files:

- **runit.bat**. This is a Windows batch file that runs the converter.
- **readme.txt**. This is the text file that provides information about the Package Converter.
- **PackageConverter.jar**. This is the Package Converter code.

This section provides instructions about converting packages. For the purpose of this document, the input package file refers to the original package that you are converting. The output package file refers to the converted package.

To convert a package:

1. Locate the `PackageConvert.zip` file in the Avalanche MC installation directory.
2. Unzip the file into a directory of your choice.
3. Place all `.ava` packages that you are going to convert in this same directory.
4. Open a command prompt

5 Navigate to the location of the Package Converter.

6 Use the following format to convert packages:

```
runit <options> <Input Package> <Output Package>
```

7 Press `Enter`.

The package is converted and placed in the same directory.

The following is a list of options you can use to manipulate the Package Converter:

-k	This command builds a synthetic CTT file from the PPF.
-h	This command displays the help page.
-m	An optional version 3 main executable
-n	This command forces the Package Converter to run strictly as a version 2 package to version 3 package converter.
-r “<new package name>”	This command allows you to rename the output package.
-s “<vendor name>”	This command changes the vendor name from Wavelink Corporation to a specified name.
-v	This command runs the Package Converter in verbose mode.

Increasing the Open Files Limit

If the InfoRail server is run under a user account whose per-process limit on open files is too low, the log file returns entries with errors. New subscribers will not be able to connect to the router. To raise the number of open connections or files, the per-process limit needs to be increased. The limit can be increased temporarily using the `ulimit` command before executing the router or permanently by increasing the limit for the account or the whole system.

To temporarily increase:

1 Insert this command into the script that starts the router:

```
ulimit -n <new limit>
```

2 Log out of the system and then log back in for the changes to take effect.

To permanently increase:

1 Add the following lines to the `etc/security/limits.conf` file:

```
<account> soft nofile <softlimit>

<account> hard nofile <hardlimit>
```

The account field can be in various forms such as group names and wild cards.

2 Log out of the system and then log back in for the changes to take effect.

Changing the Overall Open Files Limit

You may also receive error messages if the overall number of open files for the entire system has been exceeded. You can check the configured limit for open files and then increase the overall number of open files for the system.

To check the configured limit:

- Enter the following command

```
cat /proc/sys/fs/file-max
```

This command reports three values. The first value is the total allocated file openings. The second value is the total free allocated file openings. The third value is the maximum open files allowed.

To increase the file-max value

1 Navigate to `/etc/sysctl.conf` and add the following line:

```
fs.file-max = <new limit>
```

2 Reboot the system.

Generating Licenses

The Wavelink Product Activation page generates a wavelink.lic file for the license server. To generate the file, it requires a license key obtained through Wavelink Customer Support and the nodelock of the Linux host on which the license server is running. You can obtain the nodelock for the license server two ways:

- The license server displays the nodelock when the server is started from a shell.

- The license server log file (licenserver.log) contains the nodelock near the top of the file.

There is not an automated way to add a license to an existing wavelink.lic file. If you get a new wavelink.lic from the activation site and want to add it to the existing wavelink.lic, concatenate the two files to form a new file

```
mv wavelink.lic old.wavelink.lic

cat old.wavelink.lic added.wavelink.lic > wavelink.lic
```

To generate a license:

1 Ensure that the TCP/IP port 7221 is open.

2 Obtain the nodelock and license key.

3 Open `http://www.wavelink.com/activation/index.asp.`

4 Enter the **Hardware Node Lock** and **License Key**.

5 Click **Activate**.

   The activation page generates a `wavelink.lic` file.

6 Store the license file in the home directory. The default location is `/var/opt/wavelink/licenseserver`.

   The License Server will detect the file the next time a license allocation is requested by the dServer.

Revision History

- Document created. 02/12/2008.

Appendix G: Wavelink Contact Information

If you have comments or questions regarding this product, please contact Wavelink Customer Service via e-mail or telephone.

Email: customerservice@wavelink.com

Phone: 425-823-0111

Glossary

ActiveSync

A synchronization program developed by Microsoft. It allows a mobile device synchronize with either the machine running Avalanche MC.

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 alert 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. Authorized users

Avalanche MC Console

The Avalanche MC Console is the graphical user interface (GUI) where you manage your dServers, profiles and devices.

Blackout Window

A period of time when the Mobile Device dServers and Infrastructure dServers are not allow to contact the Enterprise Server, eliminating heavy bandwidth and allowing control the flow of device connections to the Enterprise Server. Also referred to as Enterprise Server Connection.

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, which allows the client to communicate with an dServer and to be configured and managed through Avalanche MC.

Default Profile

A profile that the dServers automatically assign to network infrastructure or mobile devices. The dServers 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 dServer Location.

Device Access Privileges

Defined authorization for the Infrastructure dServer to manage wireless network components including access points, switches, and routers.

Device Filters

Allow you to display specific mobile devices in the Mobile Device Inventory based on selection criteria.

DHCP

Dynamic Host Configuration Protocol. An IP service that allows DHCP clients to automatically obtain IP parameters from a DHCP server.

Distributed Servers

Also known as dServers. dServers are server side software packages that facilitate communication between infrastructure and mobile devices and the Enterprise Server. There are Infrastructure dServers and Mobile Device dServers. Infrastructure dServers manage network infrastructure devices such as routers and access points. Mobile Device dServers manage hand-held mobile devices.

Distributed Server Locations
Also known as dServer Locations. These are locations within your network where you want to manage mobile and infrastructure devices. You must deploy either a Infrastructure dServer or a Mobile Device dServer to a dServer Location.

DNS
Domain Name System. A service that provides host name-to-IP address mapping.

Enabler
The software installed on a mobile device that allows Avalanche MC to manage it.

Enterprise Server
The Enterprise Server is the platform that manages communication and collaboration between the components of Avalanche MC.

Enterprise Server Connections
See Blackout Window.

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 dServer to conserve bandwidth and increase compliance for critical software updates. Exclusion Windows are configured through Update Profiles.

Firmware
Firmware is the software installed on access points that determines what sort of properties and features that an access point supports.

Infrastructure Device

Infrastructure devices include access points, routers and switches.

Infrastructure dServer Profile

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

Infrastructure Profile

An infrastructure profile is a collection of settings that you can simultaneously apply to multiple infrastructure devices allowing you to manage your network infrastructure through Avalanche MC.

Mobile Device

A hand-held or vehicle-mounted device, such as a scan gun or PDA, that travels with a user as they conduct daily operations.

Mobile Device dServer Profile

Mobile Device dServer Profiles allow you to define device configuration settings for the mobile device dServer. Once you have configured Mobile Device dServer Profile you can apply that profile to your regions and deploy those settings to all Mobile Device dServers in that region

Mobile Device Groups

Groupings of mobile devices with similar characteristics defined by selection criteria.

Mobile Manager

A Wavelink solution that allows you to add, manage, and secure infrastructure devices on a wireless network.

Network Profile

A collection of settings that allow you to download network parameters such as IP addresses, the ESS ID, and WEP encryption keys to the mobile device over a serial or wireless connection.

Nodelock

The process in which a Wavelink license is bound to a specific computer on a network. The Wavelink licensing process uses an algorithm to combine a product serial number and a computer system's node to generate a unique license number for product authorization.

Normal User Accounts

Users assigned as Normal users do not have access to any component of Avalanche MC until assigned permissions.

Orphan Packages

A software package that has been deployed to a client through Avalanche MC, but has been disabled or is not recognized by the dServer. You must orphan a software package before you can use Avalanche MC 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 access points simultaneously.

Ports

Ports are typically used to map data to a particular process running on a computer.

PostgreSQL

A powerful, open source relational database system packaged with Avalanche MC

Profile Permissions

Provide global access to each profile you are given permission for. Does not allow permission to apply the profiles to any regions until you are assigned Regional Permissions for a region.

RAPI

A connection to the RAPI (Microsoft ActiveSync) interface on a host system. Avalanche uses the Local Gateway to perform updates and to install Avalanche Enablers to mobile devices. RAPI support is only available for ActiveSync versions pervious to version 4.0.

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 manage 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 3.5 (or later versions). The information configures the network profile of the mobile device.

Secondary Servers

If configured and assigned, secondary servers allow mobile devices to attempt to connect to a secondary Mobile Device dServer if the primary server is not available.

Selection Criteria

A collection of parameters that define which mobile devices receive specific software updates.

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 MC Console.

Software Profiles

A logical grouping of software packages maintained and managed by the Avalanche MC.

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 BSS or ESS.

Task Scheduler

The Task Scheduler provides the means to deploy dServers, send updates, and perform system back ups.

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 a specific access point. Unlike an Access Control List, which is managed by the access point, a VLACL is managed by an Agent, allowing it to support thousands of MAC addresses.

Update Profiles

Update Profiles decrease traffic by restricting specific mobile devices from contacting the Mobile Device dServer during assigned times using Exclusion Windows. See also, Exclusion Windows.

User Account A login name and password used by an individual to access the Administrator. User accounts are assigned permission level.

WEP Wired Equivalent Privacy. An encryption standard for wireless networks that provides the equivalent security of a wired connection for wireless transmissions.

Index