



Wavelink Avalanche Site Edition
Java Console User Guide

Version 5.2

Revised 27/09/2011

Copyright © 2011 by Wavelink Corporation. All rights reserved.

Wavelink Corporation
10808 South River Front Parkway, Suite 200
South Jordan, Utah 84095
Telephone: (801) 316-9000
Fax: (801) 316-9099
Email: customerservice@wavelink.com
Web site: www.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 nonexclusive license to use each software or firmware program delivered hereunder (licensed program). Except as noted below, such license may not be assigned, sublicensed, or otherwise transferred by the user without prior written consent of Wavelink. No right to copy a licensed program in whole or in part is granted, except as permitted under copyright law. The user shall not modify, merge, or incorporate any form or portion of a licensed program with other program material, create a derivative work from a licensed program, or use a licensed program in a network without written permission from Wavelink. The user agrees to maintain Wavelink's copyright notice on the licensed programs delivered hereunder, and to include the same on any authorized copies it makes, in whole or in part. The user agrees not to decompile, disassemble, decode, or reverse engineer any licensed program delivered to the user or any portion thereof. Wavelink reserves the right to make changes to any software or product to improve reliability, function, or design. The information in this document is bound by the terms of the end user license agreement.



Table of Contents

| | |
|---|-----------|
| Chapter 1: Introduction | 1 |
| Components of Avalanche | 1 |
| Getting Started | 3 |
| About This Guide | 5 |
| Chapter 2: Licensing | 6 |
| Overview of Wavelink Licensing | 6 |
| Activating Licenses | 7 |
| Activating Automatically | 7 |
| Activating Manually | 8 |
| Activating Demo Mode | 9 |
| Importing a License | 9 |
| Releasing Licenses | 11 |
| Running the License Server | 11 |
| Importing the Enterprise License | 11 |
| Chapter 3: Avalanche Java Console | 13 |
| Launching the Avalanche Console | 13 |
| Understanding the Avalanche Console | 14 |
| Tool Bar | 15 |
| Navigation Window | 16 |
| Quick Start Tab | 16 |
| Profiles Tab | 17 |
| Managing Device Inventory Displays | 18 |
| Inventory Paging | 19 |
| Managing Device Filters | 19 |
| Modifying Columns for the Mobile Device Inventory | 20 |
| Adding Custom Columns for Mobile Device Lists | 20 |
| Reorganizing Columns for Mobile Device Lists | 21 |
| Displaying Custom Mobile Device Icons | 21 |
| Understanding Edit Mode | 22 |
| Changing Console Preferences | 23 |
| Customizing General Console Settings | 23 |
| Edit Lock Control | 24 |
| Specifying the Backup Location | 24 |
| Configuring Audit Logging | 25 |
| Viewing the Audit Log | 26 |
| Configuring E-mail Settings | 27 |
| Configuring HTTP Proxy Settings | 28 |
| Managing the Enterprise Server | 28 |
| Viewing the Enterprise Server Status | 29 |
| Purging Server Statistics | 30 |
| Performing a Dump Heap | 30 |



| | |
|---|-----------|
| Checking for Available Updates | 31 |
| Viewing the Inforail Status | 31 |
| Using the Support Generator | 32 |
| Using the Enabler Installation Tool | 34 |
| Chapter 4: Managing User Accounts | 36 |
| Creating User Accounts | 37 |
| Creating User Groups | 38 |
| Assigning User Permissions | 40 |
| Assigning Authorized Users | 41 |
| Assigning Authorized Users to Locations | 41 |
| Assigning Authorized Users to Profiles | 42 |
| Assigning Authorized Users to Mobile Device Groups | 42 |
| Configuring Integrated Logon | 43 |
| Changing Passwords | 44 |
| Removing User Accounts | 45 |
| Chapter 5: Location Management | 46 |
| Managing Device Servers | 46 |
| Starting and Stopping a Server | 47 |
| Viewing Server Properties | 47 |
| Monitoring Server Status | 47 |
| Managing Group Locations | 48 |
| Creating a Group Location | 48 |
| Viewing Mobile Devices in Group Locations | 49 |
| Additional Group Location Functions | 49 |
| Applying Profiles to Locations | 50 |
| Editing Exclusions | 51 |
| Chapter 6: Managing Network Profiles | 53 |
| Creating Network Profiles | 53 |
| Configuring General Settings for Network Profiles | 54 |
| Configuring Scheduled Settings | 55 |
| Configuring WLAN IP Settings | 55 |
| Configuring WLAN Settings | 57 |
| Configuring WWAN Settings | 60 |
| Exporting Profiles for Configuring Enablers | 62 |
| Chapter 7: Managing Scan to Configure Profiles | 63 |
| Creating a Scan to Config Profile | 63 |
| Configuring a Scan to Config Profile | 64 |
| Configuring Scan to Config Settings | 64 |
| Adding Custom Properties for Scan to Config Profiles | 65 |
| Adding a Registry Key to a Scan to Config Profile | 66 |
| Printing Barcodes | 66 |



| | |
|---|-----------|
| Scanning Barcodes..... | 67 |
| Chapter 8: Managing a Mobile Device Server..... | 69 |
| Configuring a Mobile Device Server Profile..... | 69 |
| Mobile Device Server Profile General Configuration..... | 70 |
| Configuring Blackouts..... | 74 |
| Restricting Simultaneous Device Updates..... | 75 |
| Scheduling Profile-Specific Device Updates..... | 75 |
| Viewing Mobile Device Server Licensing Messages..... | 77 |
| Reinitializing the Mobile Device Server..... | 77 |
| Retrieving Mobile Device Log Files..... | 78 |
| Chapter 9: Managing Software Profiles..... | 79 |
| Creating Software Profiles..... | 79 |
| Managing Software Packages..... | 80 |
| Adding a Software Package..... | 82 |
| Building New Software Packages..... | 84 |
| Creating CAB or MSI Packages..... | 85 |
| Copying Software Packages..... | 86 |
| Enabling Software Packages..... | 86 |
| Configuring Software Packages with a Utility..... | 86 |
| Configuring Software Packages for Delayed Installation..... | 87 |
| Peer-to-Peer Package Distribution..... | 88 |
| Chapter 10: Managing Mobile Devices..... | 91 |
| Mobile Device Inventory Tab..... | 91 |
| Viewing Mobile Device Details..... | 92 |
| Locating a Mobile Device..... | 94 |
| Locating a Device using Cell Tower Information..... | 94 |
| Viewing Location History..... | 95 |
| Configuring Mobile Device Properties..... | 95 |
| Creating Custom Properties..... | 96 |
| Creating Device-Side Properties..... | 97 |
| Editing Properties..... | 97 |
| Deleting Properties..... | 98 |
| Contacting the Mobile Device..... | 98 |
| Pinging Mobile Devices..... | 98 |
| Sending a Message to a Device User..... | 99 |
| Updating a Mobile Device..... | 100 |
| Chatting with a Device User..... | 101 |
| Wiping a Mobile Device..... | 101 |
| Using the Remote Control SMS Options..... | 102 |
| Using Remote Control..... | 102 |
| Launching the Session Monitor..... | 103 |
| Software Inventory..... | 104 |



| | |
|--|------------|
| Chapter 11: Managing Mobile Device Profiles | 106 |
| Creating a Mobile Device Profile | 106 |
| Configuring Device Wipe Folders | 107 |
| Editing Custom Properties for Mobile Device Profiles | 108 |
| Editing Registry Keys for a Mobile Device Profile | 109 |
| Adding a Registry Key to a Mobile Device Profile | 110 |
| Editing or Removing a Registry Key or Value | 111 |
| Configuring Mobile Device Profile Advanced Settings | 112 |
| Location Based Services | 112 |
| Geofence Areas | 113 |
| Regional Settings | 114 |
| Update Restrictions | 114 |
| Chapter 12: Managing Mobile Device Groups | 116 |
| Creating Mobile Device Groups | 116 |
| Viewing Devices in a Mobile Device Group | 118 |
| Pinging Mobile Devices within Mobile Device Groups | 118 |
| Sending Messages to Mobile Device Groups | 119 |
| Editing Properties for Mobile Device Groups | 119 |
| Additional Mobile Device Group Functions | 121 |
| Chapter 13: Managing Alert Profiles | 122 |
| Creating and Configuring Alert Profiles | 122 |
| Adding E-Mail Contacts | 124 |
| Adding SNMP Proxies | 126 |
| Alerts Tab | 126 |
| Using the Alert Browser | 126 |
| Using the Avalanche Map | 128 |
| Chapter 14: Using Selection Criteria | 130 |
| Building Selection Criteria | 131 |
| Selection Variables | 132 |
| Operators | 139 |
| Adding Properties to the Selection Variables | 142 |
| Chapter 15: Using the Task Scheduler | 143 |
| Applying and Deploying Profiles | 144 |
| Backing Up the System | 145 |
| Restoring the System | 146 |
| Removing Completed Tasks | 147 |



| | |
|---|-----|
| SSL Certificates for the Web Console..... | 148 |
| Avalanche Services..... | 157 |
| Port Information..... | 159 |
| Avalanche Copyrights and Licenses..... | 161 |
| Uninstalling Avalanche..... | 167 |
| Wavelink Contact Information..... | 168 |



Chapter 1: Introduction

Avalanche is a mobile device management system. From a central console, you can locate and manage devices, including monitoring and distributing software. Network security features allow you to manage wireless settings (including encryption and authentication), and apply those settings on demand throughout the network. Avalanche also provides tools for managing maps, alerts, and reports.

This guide is an introduction to the functions and components of Wavelink Avalanche. It presents:

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

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

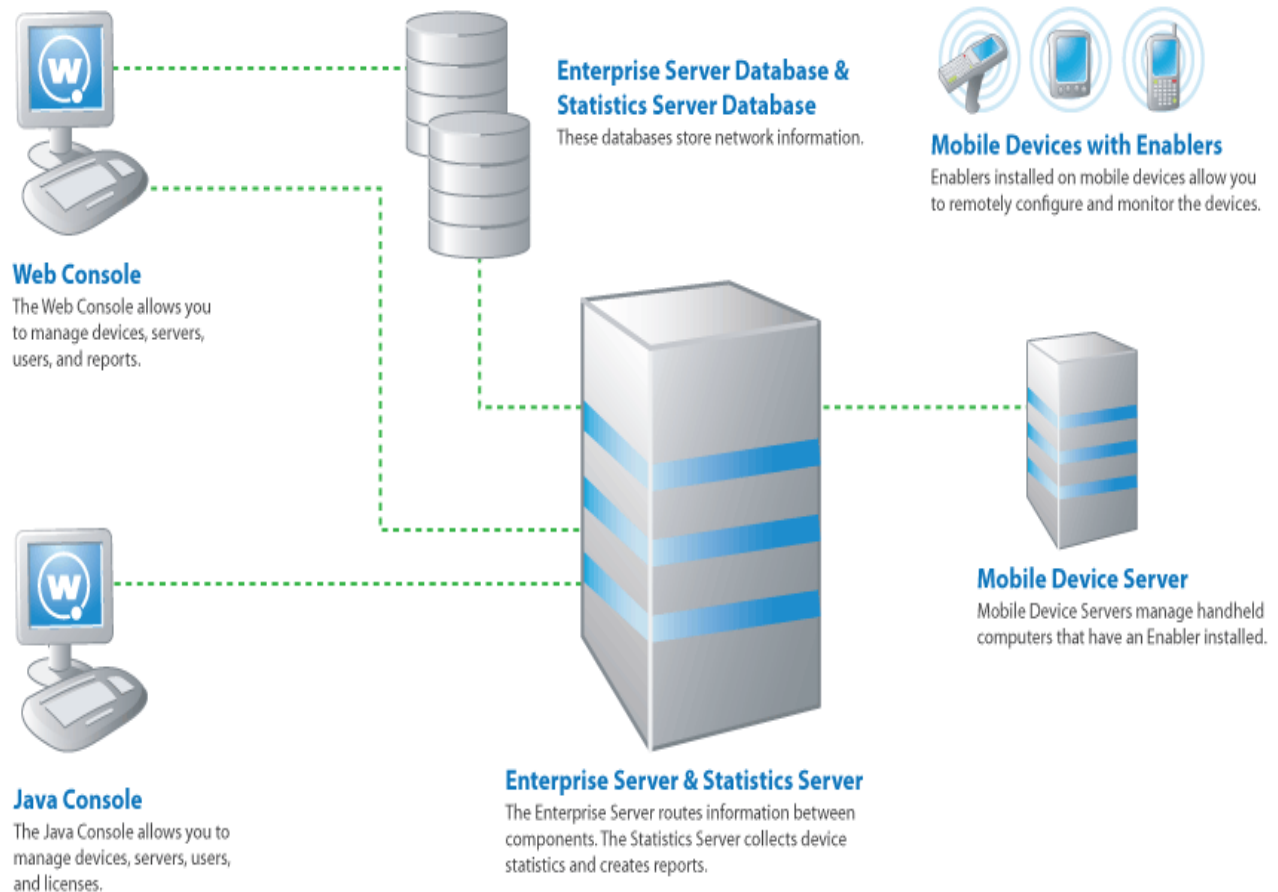
This section provides the following introductory information:

- [Components of Avalanche](#)
- [Getting Started](#)
- [About This Guide](#)

Components of Avalanche

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





The primary components of Avalanche include:

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

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

- **Enterprise Server.** The Enterprise Server facilitates all communication between the Console, the mobile device server, and the Enterprise Server database.



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

NOTE: Avalanche-supported databases use Windows-1252 character encoding. If you try to use double-byte characters or other characters that are not listed on this code page (for example, as the name of a location or profile), errors will occur and Avalanche will not save the information.

- **Mobile Device Server.** The mobile device server is responsible for communication between the Avalanche Console and mobile devices. It distributes licenses and profiles and reports device statistics.
- **Enablers.** Mobile devices must have an Avalanche Enabler installed in order to be managed by Avalanche. An Enabler relays information between the mobile device and the Mobile Device Server. With the Enabler installed, the mobile device can receive configuration instructions that you create in the Avalanche Console.

In Avalanche SE, the servers and databases are all installed on the same system. The Web Console and Java Console can be used local or remote from the enterprise server, but the Java Console must be installed at each location where it will be used.

Avalanche SE installs one mobile device server (at My Location). You can subdivide My Location into group locations, which are groups of mobile devices. When a configuration is applied at a location (either My Location or group locations), the devices included in that location will receive that profile.

Getting Started

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

- 1 **Install Avalanche.** For more information, see the *Installing Avalanche* paper on the Wavelink Web site.
- 2 **Activate Mobile Device licenses for Avalanche.** You should activate the number of licenses based on the number of devices you want to manage. For more information, see [Licensing](#).



- 3 **Create group locations.** Group locations are user-defined groups of devices that connect to the. For more information, see [Managing Group Locations](#).
- 4 **Configure profiles.** A profile allows you to manage configurations and settings centrally and then deploy those configurations to as many locations as necessary. In this way, you can update or modify multiple devices instead of manually changing settings for each one. Profiles must be enabled before being applied.

The following list provides information about each type of profile:

- | | |
|-------------------------------------|--|
| Mobile Device profile | A mobile device profile manages settings on your mobile devices, as well as adding, changing, and removing custom properties and registry keys. |
| Mobile Device Server profile | The Mobile Device Server profile configures how the mobile device server interacts with devices and the Enterprise Server. |
| Alert profile | An alert profile allows you to track events on your network and send notifications by e-mail or proxy server. |
| Network profile | A network profile provides gateway addresses, subnet masks, WWAN settings, and encryption and authentication information to devices on your network. |
| Software profile | A software profile allows you control over where and when software and files are distributed to mobile devices. |
| Scan to Config profile | Scan to Config profiles allow you to print network settings as barcodes, and then the settings are applied on the device when they are scanned. |

- 5 **Assign profiles to locations.** You can assign configured profiles to locations from the Console. When you assign a profile to a location and perform a universal deployment, the settings from the profiles are applied to the location and any associated devices. For more information, see [Applying Profiles to Locations](#).
- 6 **Configure Enablers.** Ensure that your mobile devices have Enablers installed, and configure the Enablers to connect to a mobile device server.
- 7 **Perform Updates.** To deploy settings to the selected locations, perform an update through the Task Scheduler. For more information see [Performing a Server Synchronization](#).

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



About This Guide

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

This help makes the following assumptions:

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

This help uses the following typographical conventions:

Courier New Any time you are instructed to type information, that information appears in the Courier New text style. This text style is also used for file names, file paths, or keyboard commands.

Examples:

The default location is `C:\Program Files\Wavelink\Avalanche.`

Press `CTRL+ALT+DELETE.`

Bold Any time this guide 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.

Example:

Click **File > Open.**

Italics Any time this guide refers to the titles of dialog boxes, that section appears in the *Italics* text style.

Example:

The *Infrastructure Profiles* dialog box appears.



Chapter 2: Licensing

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

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

- [Overview of Wavelink Licensing](#)
- [Activating Licenses](#)
- [Releasing Licenses](#)
- [Running the License Server](#)
- [Importing the Enterprise License](#)

Overview of Wavelink Licensing

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

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

NOTE: To obtain any Avalanche license, please contact Wavelink customer service or a sales representative.

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

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



Activating Licenses

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

This section provides information on the following processes:

- [Activating Automatically](#)
- [Activating Manually](#)
- [Importing a License](#)
- [Activating Demo Mode](#)

For other Wavelink products used in conjunction with Avalanche 5.2, use the same activation method (from the Avalanche Console) that you use for Avalanche 5.2. You can activate these product licenses automatically, or if you already have a `.lic` file associated with the license, import the `.lic` file.

NOTE: If you have a `wavelink.lic` file from an older installation, you must contact Wavelink Support to reissue the license before you can import it into Avalanche 5.x.

Activating Automatically

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

NOTE: If your Internet access is restricted through a proxy server, you will need to configure HTTP Proxy settings before you can activate licenses automatically. For information on configuring proxy settings, see [Configuring HTTP Proxy Settings](#).

To activate Avalanche:

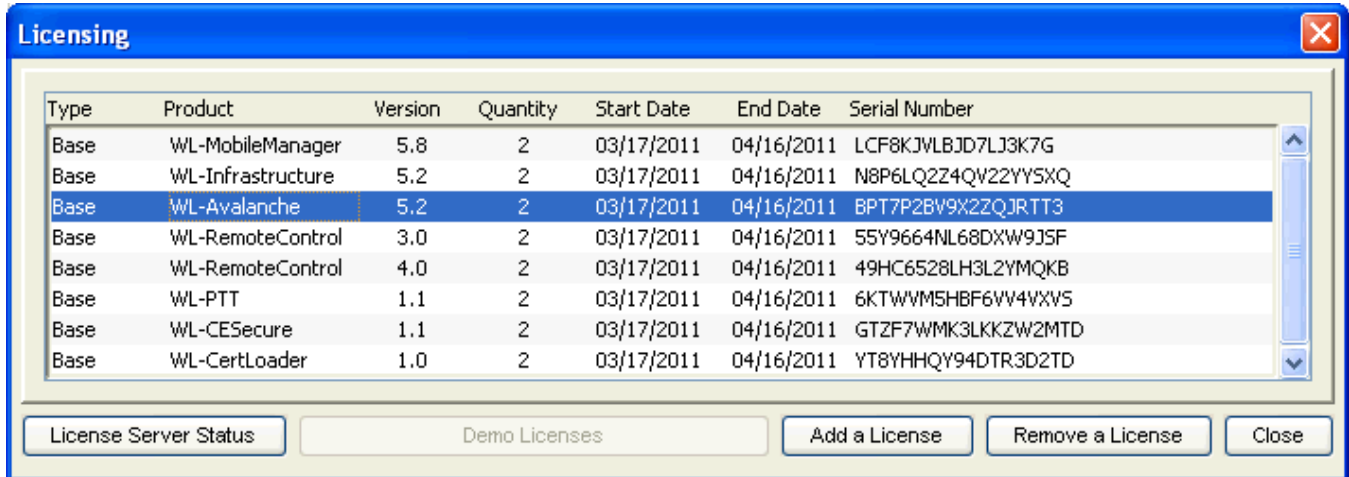
- 1 Obtain the Avalanche product licensing code from Wavelink.

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

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

The *Licensing* dialog box appears.





Licensing dialog box

3 Click Add a License.

The *Add a License* dialog box appears.

4 Click Activate a License.

The *Activate a License* dialog box appears.

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

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

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

The licenses appear in the *Licensing* dialog box.

Activating Manually

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

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

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

To manually activate a license:

- 1 Open a Web browser and navigate to <http://www.wavelink.com/activation>.



- 2 Enter the **Hardware Node Lock** and the **License Key** in the text boxes.
- 3 Click **Activate** button to activate license.

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

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

Activating Demo Mode

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

- Avalanche 5.2 (2 mobile device licenses and 2 infrastructure device licenses)
- Remote Control 4.0
- Remote Control 3.0
- Communicator 1.1
- CE Secure 1.1
- Certificate Manager 1.0

To activate demo mode:

- 1 Click **Tools > Manage Licensing**.

The *Licensing* dialog box appears.

- 2 Click **Demo Licenses**.

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

Importing a License

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

NOTE: If you have a `wavelink.lic` file from an older installation, you must contact Wavelink Support to reissue the license before you can import it into Avalanche 5.x.



To import a license:

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

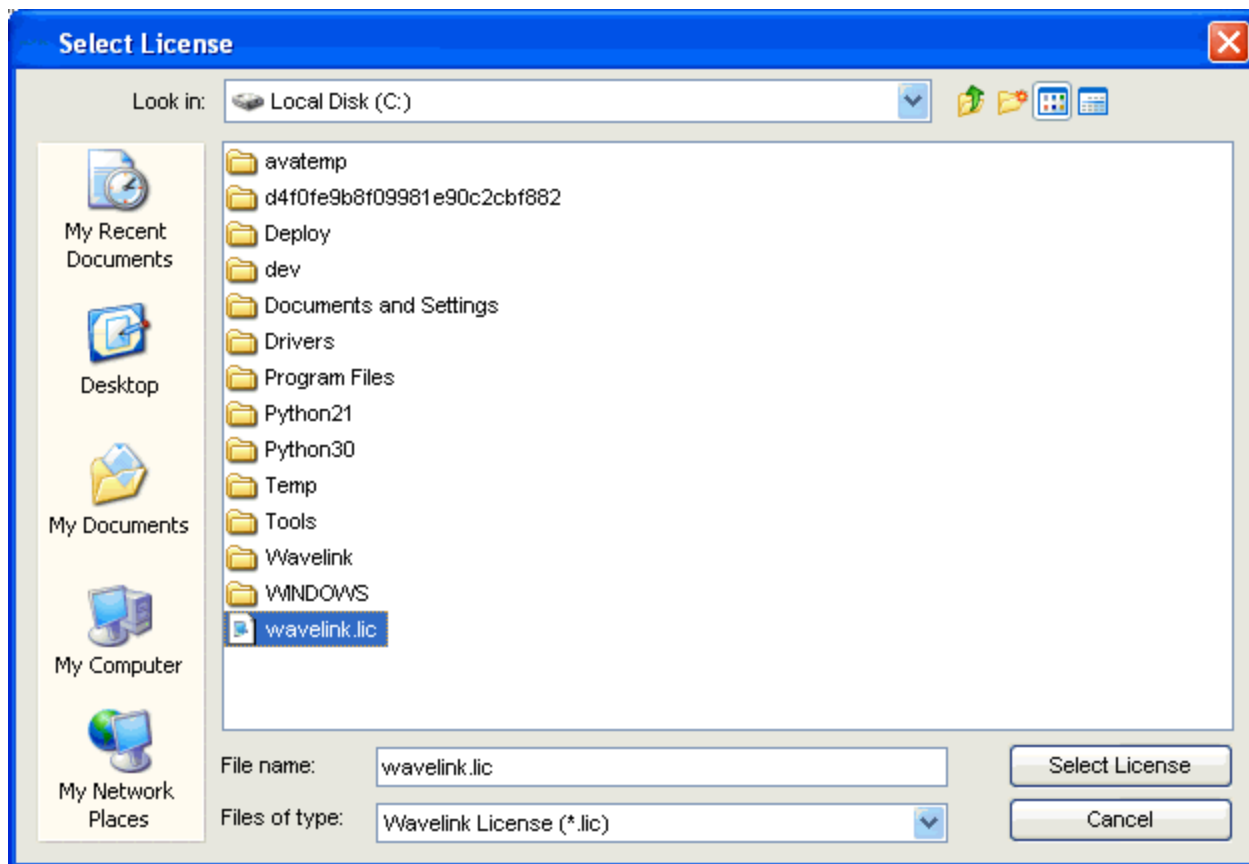
The *Licensing* dialog box appears.

- 2 Click **Add a License**.

The *Add a License* dialog box appears.

- 3 Click **Import a License**.

The *Select License* dialog box appears.



Select License dialog box

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

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

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

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



Releasing Licenses

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

For information about configuring the Mobile Device Server to release licenses, see [Mobile Device Server Profile General Configuration](#). For information about deleting devices from the Mobile Device Inventory, see [Mobile Device Inventory Tab](#).

Running the License Server

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

The License Server is a service that starts automatically. If for some reason the License Server is not running, the Mobile Device and Infrastructure Servers will not be able to receive licenses. For the name and default installation location of the License Server, see [Avalanche Services](#).

Importing the Enterprise License

Enterprise Licenses grant unlimited licenses for your devices.

Importing an Enterprise License will apply the license to the Enterprise Server and brand the Console with an image of your choosing. Once you import the license, any time the Console connects to the branded Enterprise Server, the image will appear in the bottom left corner of the Java Console.

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

To import the Enterprise License:

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

A search dialog box appears.

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



The Enterprise license will be applied to the Enterprise Server and the Console will retrieve the enterprise image. There is no way to remove the enterprise image once it has been imported.



Chapter 3: Avalanche Java Console

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

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

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

This section contains the following topics for the Java Console:

- [Launching the Avalanche Console](#)
- [Understanding the Avalanche Console](#)
- [Changing Console Preferences](#)
- [Managing the Enterprise Server](#)
- [Checking for Available Updates](#)
- [Viewing the Inforail Status](#)
- [Using the Support Generator](#)
- [Using the Enabler Installation Tool](#)

Launching the Avalanche Console

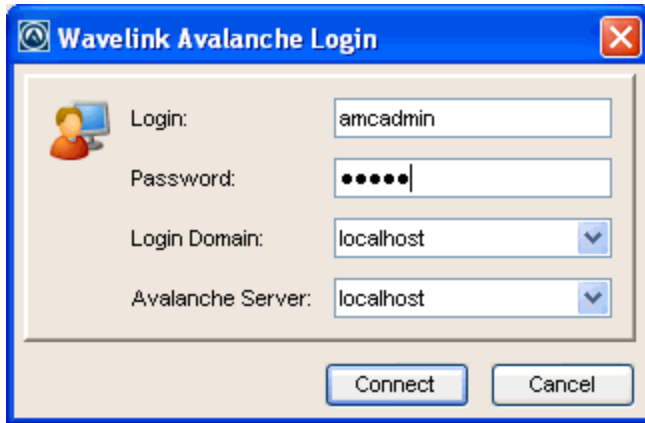
Configure and manage your wireless network on an enterprise-wide basis from the Avalanche Console. You can open the Avalanche Console from the **Programs** menu or from a shortcut.

To launch the Avalanche Console:

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

The *Wavelink Avalanche Login* dialog box appears.





Wavelink Avalanche Login

2 Enter your Login and Password.

Avalanche is installed with a default user login of *amcadmin* and password of *admin*. Wavelink recommends you create a new password for this account once you log in. For information about changing passwords, see [Managing User Accounts](#).

- 3 From the Login Domain drop-down list, select the login domain if you have configured Avalanche to use LDAP or Active Directory.**
- 4 From the Avalanche Server drop-down list, select your host (the IP address or DNS name of the enterprise server).**
- 5 Click Connect.**

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

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

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

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

Understanding the Avalanche Console

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



network configuration and activity.

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

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

This section gives details about the following areas:

- [Tool Bar](#)
- [Navigation Window](#)
- [Quick Start Tab](#)
- [Profiles Tab](#)
- [Managing Device Inventory Displays](#)
- [Understanding Edit Mode](#)

For information on the Alerts tab, Device Server Status tab, or Device Groups tab, go to the following sections:

- [Managing Alert Profiles](#)
- [Managing a Mobile Device Server](#)
- [Managing Mobile Device Groups](#)

Tool Bar

The following table provides information about the Tool Bar buttons.



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



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





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



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



Click this icon to access Console preferences such as audit logging and backup location settings.



Click this icon to access the Avalanche Help.

The other three buttons on the Tool Bar are for using Edit Mode. For more information about Edit Mode, see [Understanding Edit Mode](#).

Navigation Window

The Navigation Window, located on the left side of the Java Console, displays your enterprise in a tree view. Move through the locations by either expanding nodes or using the Search function. The **Search** function finds locations regardless of whether the tree is expanded or collapsed.

To use the Search function:

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

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

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

Quick Start Tab

When you first launch the Console, the **Quick Start** tab displays. This tab provides links for quickly getting your enterprise configured and includes required and optional tasks. Each task has a brief description which you can view by clicking the plus [+] button. The sections in the **Quick Start** tab vary depending on the location selected in the Navigation Tree.

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.

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

Profiles Configuration

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



- Creating a Network Profile. For details, see [Managing Network Profiles](#).
- Add Device Software. For details, see [Managing Software Profiles](#).
- Create a Scan to Config Profile. For details, see [Managing Scan to Configure Profiles](#).

Tools

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

Help and Support

This section provides links to the Avalanche Help, Wavelink Support, and launches the Support Generator. For details about using the Support Generator, see [Using the Support Generator](#).

Profiles Tab

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

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



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

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

To filter the Profile List:

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

The *Set Column Filter* dialog box appears.

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

-Or-

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

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

Managing Device Inventory Displays

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

Device lists can be customized to display specific information. You can sort the lists, filter the lists using custom filters, or modify the columns displayed. You can sort each column by right-clicking the column header and selecting **Sort Ascending** or **Sort Descending**. This section contains the following information on customizing inventory displays:

- [Inventory Paging](#)
- [Managing Device Filters](#)
- [Modifying Columns for the Mobile Device Inventory](#)
- [Adding Custom Columns for Mobile Device Lists](#)
- [Reorganizing Columns for Mobile Device Lists](#)
- [Displaying Custom Mobile Device Icons](#)



Inventory Paging

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

To configure inventory paging:

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

Managing Device Filters

You can filter which devices are displayed in a device list by creating and applying device filters. When a filter is applied, only the devices meeting the criteria associated with that filter are displayed. Filters are available for the lists in the Mobile Device Inventory and mobile device groups.

To create a filter for a device inventory:

- 1 Click **Edit Filters**.

The *Modify Device Filters* dialog box appears.

- 2 Enter a name for the new filter in the **Filter Name** text box.
- 3 Click the **Selection Criteria** button (in the upper right of the box).

The *Selection Criteria Builder* dialog box appears, allowing you to create a filter based on device characteristics. See [Building Selection Criteria](#) for more information on creating selection criteria.

- 4 After you choose selection criteria for the filter, click **OK** to return to the *Modify Device Filters* dialog box.

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

- 5 Click **Add Filter**.

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

- 6 Click **OK**.

To apply a filter to a device inventory:

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



To delete a filter from a device inventory:

- 1 Click **Edit Filters**.

The *Modifying Device Filters* dialog box appears.

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

Modifying Columns for the Mobile Device Inventory

The Avalanche Console allows you to control which columns appear in the Mobile Device Inventory 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 a column from the **Selected Columns** list, select the column you want to remove and click **Remove Column(s)**.

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

- 4 Use the **Move Up** and **Move Down** to modify the order in which the columns appear in the **Mobile Device Inventory** tab.
- 5 When you are finished, click **OK**.

The columns are rearranged to reflect your modifications.

Adding Custom Columns for Mobile Device Lists

If you have created custom properties for your mobile devices, you can display them in a column in a mobile device list. For details about creating custom properties, see [Creating Custom Properties](#).

To display columns for custom properties:

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

The *Modify Mobile Device Columns* dialog box appears.

- 2 Click **Add Custom**.



The *Custom Property Column* dialog box appears.

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

The column name for the property appears in the **Available Columns** list.

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

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

Reorganizing Columns for Mobile Device Lists

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

To reorganize columns:

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

Displaying Custom Mobile Device Icons

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



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

Understanding Edit Mode

In order to edit a profile, device group, or location properties, you must enter Edit Mode. While you are using Edit Mode, the item you are editing is locked. While an item is locked, no other user will be able to attempt to edit the configuration. Edit Lock has an automatic timeout, at which point you will be prompted in order to continue editing. If you do not respond to the prompt within the time configured, then your edit will be canceled and you will not be able to save your changes.

From the Java Console, you can configure the timeout and the length of time after the prompt appears before the user's lock is terminated. The timeout for Edit Lock has a default setting of 15 minutes, and the prompt timeout has a default setting of 1 minute. For instructions on configuring these timeouts, see [Edit Lock Control](#).

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



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



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



Click **Save** to save configuration changes.

Consider the following when using Edit Mode:

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



Changing Console Preferences

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

- [Customizing General Console Settings](#)
- [Edit Lock Control](#)
- [Specifying the Backup Location](#)
- [Configuring Audit Logging](#)
- [Viewing the Audit Log](#)
- [Configuring E-mail Settings](#)
- [Configuring HTTP Proxy Settings](#)

Customizing General Console Settings

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

To customize the general Console settings:

- 1 Click **Tools > Settings**.

The *Settings* dialog box appears.

- 2 Select the **General** tab.
- 3 In the Auto Update Settings area, configure whether Avalanche should check for updates or upload usage information to Wavelink.
- 4 In the Console Display Settings area, configure the width, height, and the frame positions for the Avalanche Console.
- 5 In the Alert Browser Settings area, 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: Avalanche stores alerts in the enterprise database.

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



- 7 Click **OK** to close the *Settings* dialog box.

The Avalanche Console updates to reflect your changes.

Edit Lock Control

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

If a user is editing an item such as a profile, he has a limited amount of time to make and save his changes before the Edit Lock times out. When the Edit Lock times out, a prompt will appear asking if he wants to extend the Edit Lock. If he does not respond to the prompt, the Edit Lock will be canceled, changes will not be saved, and other users will be able to edit the item.

To configure Edit Lock control:

- 1 Click **Tools > Settings**.

The *Settings* dialog box appears.

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

Specifying the Backup Location

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

For information about backing up Avalanche, see [Backing Up the System](#).

To specify a location:

- 1 Click **Tools > Settings**.

The *Settings* dialog box appears.

- 2 Select the **Enterprise Server** tab.
- 3 In the **Backup File Location** text box, type the path where you want to save system backups.
- 4 Click **Apply**.
- 5 Click **OK** to close the *Settings* dialog box.



Configuring Audit Logging

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

NOTE: For information on viewing and clearing the audit log, see [Viewing the Audit Log](#).

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

You can also archive the audit log at a specific time every day. When the information is archived, it is copied to a `.csv` file. The `.csv` file is stored in the same directory where backup files are stored. For information on configuring the backup file location, see [Specifying the Backup Location](#).

The following events can be configured for logging:

| | |
|---|--|
| Deployment Package modifications | When a deployment package is modified. |
| Device Commands | When one of the tools in the Device Details Tools panel is used. |
| Device Group modifications | When a device group is modified. |
| Group Location modifications | When a group location is modified. |
| Region Location modifications | When a region is modified. |
| Server Location modifications | When a server location is modified. |
| Profile Application modifications | When a profile is applied, excluded, or removed from a location. |
| Profile modifications | When a profile is modified. |
| Scheduled Event, Apply/Deploy Profiles | When an Apply/Deploy Profiles event has occurred. |
| Scheduled Event, Deploy/Update Servers | When a Deploy/Update Servers event has occurred. |



| | |
|--|---|
| Scheduled Event, System Backup | When a System Backup event has occurred. |
| Scheduled Event, System Restore | When a System Restore event has occurred. |
| Scheduled Event, Uninstall Server | When an Uninstall Server event has occurred. |
| Scheduled Event, Universal Deployment | When a scheduled Universal Deployment event has occurred. |
| Scheduled Event, Update Firmware | When an Update Firmware event has occurred. |
| User Logon/Logoff | When a user logs on or logs off the Avalanche Console. |
| User modifications | When a user account is modified. |
| VLACL modifications | When the VLACL is modified. |

To enable audit logging:

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

Viewing the Audit Log

The audit log collects information about actions performed from the Avalanche Console. As part of the data collection, the audit log includes the username and IP address for each logged event, the date and time of the Console activity, and a description of the changes that occurred. Audit logging generates entries in the enterprise database.

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

For information on configuring the events displayed in the audit log, see [Configuring Audit Logging](#).



To view the audit log:

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

The *Audit Log* dialog box appears.

- 2 Select the filter or filters you want to use:

- To show the most recent events, enable **Most Recent** and select the number of entries to show.
- To filter events by date, enable **Date Range** and use the calendar buttons to select the beginning and end dates.
- To filter events by IP address, enable **IP Range** and enter the range of addresses you want to view.
- To filter events by type, enable **Activity Type** and select the check boxes for the activities you want to view.
- To filter events by username, enable **User Name** and type the name of the user in the text box. You may only filter by one username at a time.

- 3 Click **Refresh Screen** to update the list according to your filter.

All events matching the filters appear in the list.

- 4 If you wish to delete all entries in the audit log, click **Clear Log**. This will remove all entries from the database and archive the information in a `.csv` file in the backup directory.

Configuring E-mail Settings

If you plan to use an SMTP server to forward alerts to an e-mail address, you must configure the name or IP address of the server, a username and password, and a reply-to e-mail address.

To configure e-mail settings:

- 1 Click **Tools > Settings**.

The *Settings* dialog box appears.

- 2 Select the **E-Mail & HTTP** tab.
- 3 Type the location of the e-mail server you want Avalanche to use in the **E-Mail Server** text box.
- 4 Select the port Avalanche should use when contacting the e-mail server.
- 5 Type the **Username** and **Password** in the text boxes.
- 6 Type the address the e-mails will appear from in the **From Email** text box.



- 7 Type the address a reply should be sent to if an alert e-mail is replied to in the **Reply-to Email** text box.
- 8 Click **Apply**.
- 9 Click **OK** to return to the Avalanche Console.

Configuring HTTP Proxy Settings

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

To configure HTTP proxy settings:

- 1 Click **Tools > Settings**.

The *Settings* dialog box appears.

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

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

- 8 To disable the use of a proxy, disable the **Use a Proxy Server** checkbox in the *Settings* dialog box.

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

Managing the Enterprise Server

The Enterprise Server and Enterprise Server database handle scheduling, deployments, profiles, users, and locations. You may review and optimize Enterprise Server performance using the following tasks:

- [Viewing the Enterprise Server Status](#)
- [Purging Server Statistics](#)



- [Performing a Dump Heap](#)

Viewing the Enterprise Server Status

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

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

| Parameter | Value |
|---------------------------------|--|
| Version | The version of the enterprise server. |
| Build Number | The build number of the enterprise server. |
| Uptime | The length of time the enterprise server has been running. |
| Start Time | The last time the enterprise server was started. |
| Current Time | The current time. |
| Messages Received | The total number of messages the server has received. |
| Messages Sent | The total number of messages the server has sent. |
| Spillover Enabled | Whether the memory spillover function is enabled (YES or NO). |
| Spillover Threshold | The memory level before spillover takes effect. |
| Spillover Release | The number of seconds before the spillover is released. |
| Blackout Mode | If blackout mode is enabled and which servers are included in the blackout. Off indicates that blackout mode is not currently in use. All Servers indicates that all servers are in blackout mode. Mobile Device Servers indicates that only the Mobile Device Servers are in blackout mode. Infrastructure Servers indicates that only the Infrastructure Servers are in blackout mode. |
| Priority C0 - C2 Backlog | The number of messages coming from Consoles, with C0 being the highest priority and C2 being the lowest priority. |
| Priority A0 - A2 Backlog | The number of messages coming from the device servers, with A0 being the highest priority and A2 being the lowest priority. |



Purging Server Statistics

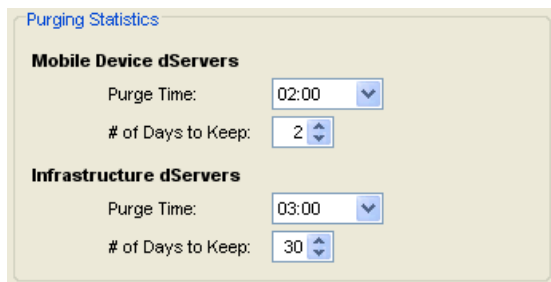
To prevent database inflation, you can configure Avalanche to purge logged statistics. You can configure the following for both Mobile Device Servers alerts and statistics:

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

To configure purge settings:

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

The *eServer Status* dialog box appears.



Purging Statistics in the eServer Status dialog box

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

Performing a Dump Heap

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

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

To perform a dump heap:

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

The *eServer Status* dialog box appears.

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



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

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

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

Checking for Available Updates

Avalanche tracks the Wavelink software you have installed on your devices and displays when there are updates for the software available. For example, it tracks the versions of the Enablers you have installed and provides a link when Wavelink releases a newer Enabler.

In order for Avalanche to check for new updates, it sends basic system and device information to Wavelink.

To check for available software updates:

- 1 Click **Help > Check For Updates**.

The *Avalanche Update* dialog box appears if you have not already agreed to submit update information to Avalanche.

- 2 Enable the **Accept** option and click **OK** to allow Avalanche to send system and device information to Wavelink.
- 3 If there are new updates available, the message **Updates Available** will appear in the lower right corner of the Console. Click on the message to view the available updates.
- 4 The *Available Updates* dialog box appears. Click on a link to download an update.

Viewing the InfoRail Status

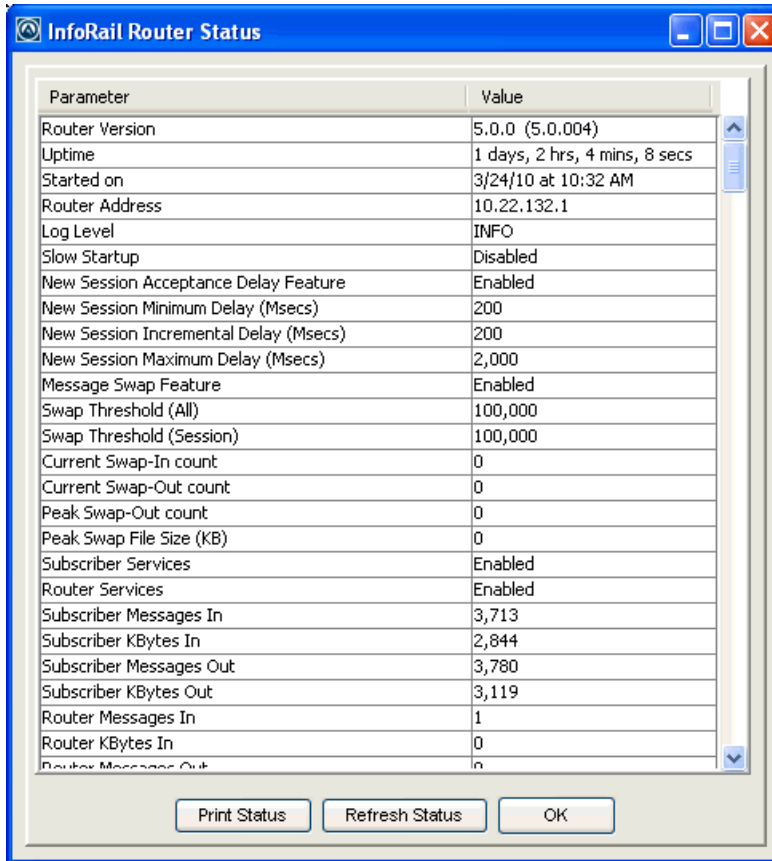
The InfoRail Router coordinates communication between Avalanche processes. The InfoRail Router Status dialog box provides information such as the version of the router, how long it has been running, and the IP address. From this dialog box you can print or refresh the status. You cannot change any of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

To view the InfoRail status:

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

The dialog box appears.





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

InfoRail Router Status

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

Using the Support Generator

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

```
AvalancheServer.log
EConsole.log
Inforail.log
eConsoleNetstat.log
```

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



To use the Support Generator:

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

The *Avalanche Support Generator* dialog box appears.

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

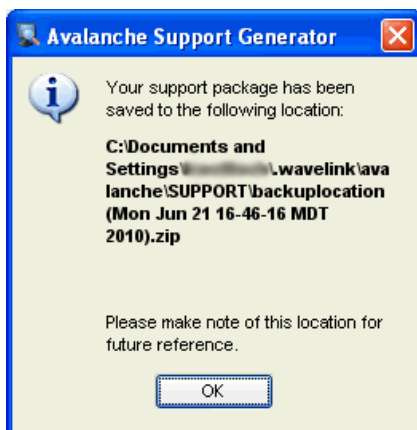
NOTE: You cannot change the **Operating System** or **Free HDD Space** text boxes. These are populated automatically by the Support Generator.

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

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

- 7 Click **Save**.

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



Avalanche Support Generator Location

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



Using the Enabler Installation Tool

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

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

- Enabler installation files 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 **Install Avalanche Enabler**.

The *Avalanche Device Enabler Installation* dialog box appears.



Avalanche Device Enabler Installation

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

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

The Enabler Configuration Tool appears.





Wavelink Product Configuration Utility

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

For details about all the configuration options of the Enabler and information about using ActiveSync, see the *Avalanche Enabler User Guide*.



Chapter 4: Managing User Accounts

A user account is required to log in to the Avalanche Console. User accounts allow you to define who can access components and perform tasks. Each user is assigned to a home location, which defines the locations the user has authority to manage.

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

NOTE: Avalanche is installed with a default Administrator account named `amcadmin` with the password `admin`. Wavelink recommends you create a new password for this account once you log in.

When a Normal account is created, you can assign permissions to that account. These permissions can apply to all profiles of a type (for example, all alert profiles), to specific tools (for example, Remote Control), or location management and synchronization. If you want to assign permissions on a profile-by-profile basis, you also have the option to authorize the user for individual profiles.

As an alternative to assigning permissions to each Normal account, you can assign permissions to a user group. Each Normal account that is part of the user group will have the permissions which are assigned to the group. If a user is removed from the group, he will no longer have the associated permissions. A Normal account can belong to more than one user group at a time.

If your network uses Active Directory or LDAP for user access, you can set up integrated logon for Avalanche. Avalanche will accept the usernames and passwords accepted on your network. Guest accounts must be disabled on the computer where Avalanche is installed.

This section provides the following information about user accounts:

- [Creating User Accounts](#)
- [Creating User Groups](#)
- [Assigning User Permissions](#)
- [Assigning Authorized Users](#)
- [Configuring Integrated Logon](#)
- [Changing Passwords](#)
- [Removing User Accounts](#)



Creating User Accounts

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

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

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

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

User Type Select if the user is a Normal user or an Administrator. If the user is a Normal user, you will need to assign Regional or Profile permissions. If the user is an Administrator, he will have access to the entire company.

User Home This is the portion of your network that the user will be assigned to. The user will only be able to access profiles and information pertinent to his assigned location.

Description You can enter a description of the user or group.

Login This is the name the user will use to log in to the Avalanche Console. The login is case sensitive. The following special characters are not allowed:
~ ! ^ * () + = | ? / < > , [] : ; { } \ " & space

Password This is the password that will grant access to the Avalanche Console. Passwords are case sensitive. The password has a 32-character limit.

Confirm Password You must confirm the password you assign to the user.

First Name This is the first name of the user.

Last Name This is the last name of the user.

To create a new account:

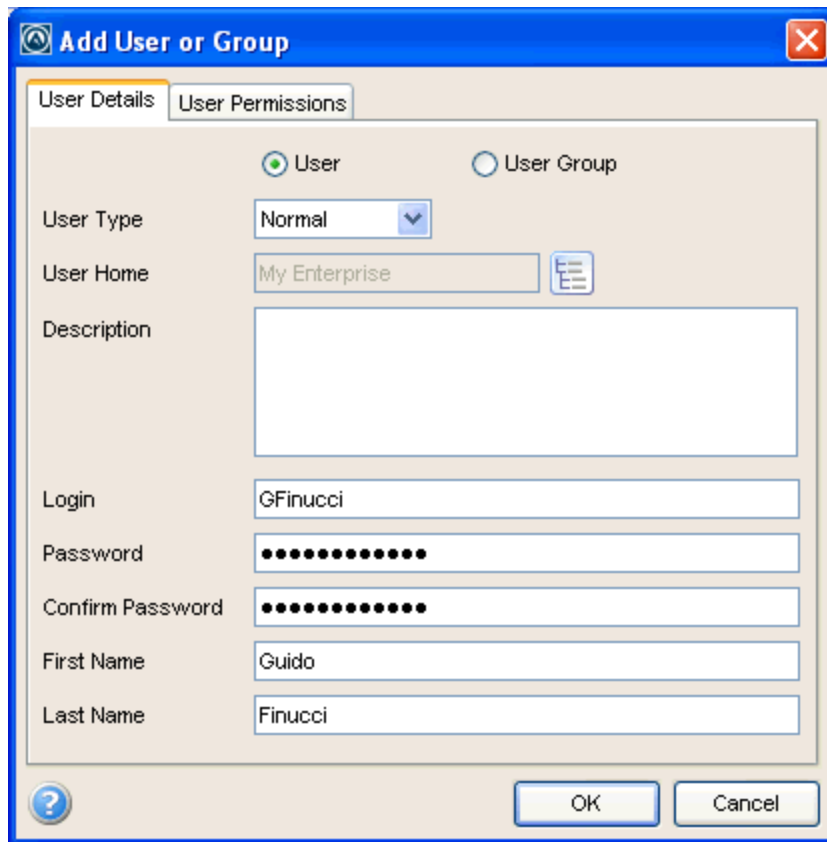
- 1 Click **Tools > User Management**.

The *User Management* dialog box appears.



- 2 Click **Add**.

The *Add User or Group* dialog box appears.



- 3 Enter the information in the available text boxes. **User Type**, **User Home**, **Login**, **Password**, and **Confirm Password** are required fields.
- 4 To assign a user home, click the tree button to the left of the text box.
- 5 Assign permissions by clicking on the tabs now or an Administrator can modify permissions later.
- 6 When you are finished, click **OK**.

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

The new account is available. However, if a new user is set as a Normal user, that user will not have access to any areas of the Console until permissions are assigned to that user. For more information, see [Assigning User Permissions](#).

Creating User Groups

In addition to individual user accounts, you can create user groups. Users assigned to a user group will have permissions for all areas associated with that user group in addition to the



permissions granted for their individual accounts.

For convenience, there are default user groups created, including:

- Software Admin
- Help Desk
- Network Admin

These user groups are set with a series of default permissions. You can edit the permissions for the groups to suit your needs or create a new user group.

To create a new user group:

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

The *User Management* dialog box appears.

- 2 Click **Add**.

The *Add User or Group* dialog box appears.

- 3 Select the **User Group** option.

- 4 In the **Group Name** text box, enter the name of the group.

- 5 In the **Users** list, check all users that you want to add to the group.

NOTE: If you have not added any Normal users, the list box will be empty. See [Creating User Accounts](#) for information about creating users.

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

- 7 You can assign regional and profile permissions by clicking on the tabs now, or an Administrator can modify permissions later.

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

To view the users in a user group:

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

The *User Management* dialog box appears.

- 2 Select the user group you want to view details for and click **Edit**.

- 3 The *Edit User Group* dialog box appears. The users assigned to the group are in the **Users** list. If desired, edit the information and click **OK**.

To view the user groups that a specific user is assigned to:

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



The *User Management* dialog box appears.

- 2 Select the user you want to view details for and click **Edit**.
- 3 The *Edit User* dialog box appears. The groups the user is assigned to are in the **User Groups** list. If desired, edit the information and click **OK**.

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 permissions to a functionality, that user has permissions for that specific functionality in his home location and any associated sub-locations. A user must have permissions for a location in order to view or edit the profiles, devices, or groups associated with the location.

Permissions can be assigned when a user is created, or from a specific location, profile, or mobile device group. This section describes the permissions available from the *User Management* dialog box. For information on giving permissions to a user for a specific location, profile, or mobile device group, see [Assigning Authorized Users](#).

The following table describes permissions that are available for profiles:

| Management | | | Applications | |
|---|--|--|---|---|
| View allows the user to view the settings for a profile. | Edit allows the user to edit the settings of a profile. | Print allows the user to print the barcodes for a Scan to Config profile. | View allows the user to view where profiles are applied. | Edit allows the user to edit where profiles are applied. |

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

The following table describes permissions that are available for inventory:

| Inventory | | |
|----------------------|--|---|
| Mobile Devices | View allows the user to view the mobile devices for assigned locations. | Manage allows the user to manage the mobile devices for assigned locations or mobile device groups. |
| Mobile Device Groups | View allows the user to view the mobile device groups and the | Edit allows the user to edit group properties for mobile device groups. A user must also have Mobile Devices permissions in order to |



| Inventory | | |
|--------------------------|---|--|
| | devices they contain. | view/edit the devices in a group. |
| Mobile Device Properties | View allows the user to view mobile device properties. | Edit allows the user to edit properties for mobile devices. |
| Remote Control | View allows the user to connect to a mobile device using Remote Control. | Edit allows the user to connect to a device using Remote Control or configure Remote Control connection profiles. |

The following table describes the other permissions that are available:

| Other | | |
|---------------------|---|---|
| Location Management | View allows the user to view location configurations and settings. | Edit allows the user to view, manage, and configure locations. |
| Synchronization | View allows the user to view recent and scheduled deployments. | Edit allows the user to create and deploy infrastructure or server packages, and initiate server synchronization. This includes universal deployments. |

Assigning Authorized Users

Users that are Normal users but not configured to manage profiles can be assigned as authorized users for specific locations, profiles, or device groups.

This section contains the following information:

- [Assigning Authorized Users to Locations](#)
- [Assigning Authorized Users to Profiles](#)
- [Assigning Authorized Users to Mobile Device Groups](#)

Assigning Authorized Users to Locations

Each user is assigned a home location. When you assign a user to a location, that user can access all locations beneath the assigned location. You must be an Administrator in order to assign users to locations.



To assign a user to a location:

- 1 Select the location.
- 2 Select the **Location Properties** tab.
- 3 Click **Edit**.
- 4 Select the **Authorized Users** tab.
- 5 Click **Add User**.

The *Add Authorized User* dialog box appears.

- 6 Select the user and click **OK**.

The user is added to the list of authorized users for that location.

Assigning Authorized Users to Profiles

You can assign administrative privileges to a Normal user for a specific profile. If you want to give a Normal user permissions for all profiles of a specific type, see [Assigning User Permissions](#).

To add or remove an authorized user:

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

The *Profile Authorized Users* dialog box appears.

- 4 Add or remove authorized users as desired.
 - To add an authorized user, click **Add**. Click on the name of the user from the list and the permission level from the drop-down list and click **OK**.
 - To remove an authorized user, select the name of the user and click **Remove**.

Assigning Authorized Users to Mobile Device Groups

You can assign administrative privileges for a specified mobile device group to a Normal user. Any user assigned as an authorized user to a group will have all administrative rights for that one group.

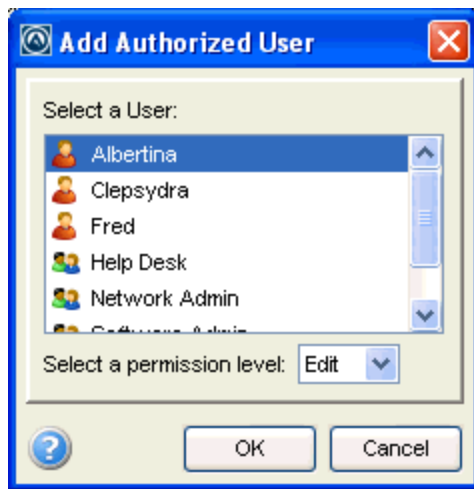
NOTE: A user must have mobile device permissions in order to view or edit devices in a mobile device group.



To add an authorized user:

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

The *Add Authorized User* dialog box appears.



Add Authorized User dialog box

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

The user is added to the list of authorized users.

Configuring Integrated Logon

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

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



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

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

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

To enable integrated logon:

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

The *User Management* dialog box appears.

- 2 Select from the following options:

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

- 3 Click **OK**.

- 4 Log out of the Console.

Avalanche is now configured to recognize authenticated system users.

Changing Passwords

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

To change a password:

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

The *User Management* dialog box appears.

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

- 3 Click **Change Password**.

The *Change User Password* dialog box appears.

- 4 Type the new password in the **New Password** text box.



- 5 Retype the password to confirm it in the **Confirm New Password** text box.
- 6 Click **OK**.
- 7 Click **OK** again to return to the Avalanche Console.

The new password information is applied immediately.

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

Removing User Accounts

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

To delete a user account:

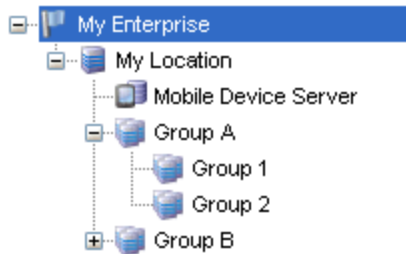
- 1 Click **Tools > User Management**.
- The *User Management* dialog box appears.
- 2 Select a user from the list.
 - 3 Click **Remove**.
 - 4 Confirm you want to remove the user account.

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



Chapter 5: Location Management

Avalanche uses locations in order to organize devices, users, and settings. Avalanche lets you organize devices in group locations to make them easier to manage. Locations are organized in the Navigation Window:



Locations in the Navigation Window

Avalanche installs a mobile device server during the installation process. The server is automatically placed at My Location. In order to organize devices, users, and settings, you can create sub-locations under My Location. These sub-locations are called group locations.

Avalanche uses selection criteria to determine which devices belong to each group location. For example, if Group 1 has the selection criterion: `ModelName = ITCCK30`, any Intermec CK30 devices automatically appear in the Group 1 inventory as well as the server location inventory. A device can belong to more than one group location concurrently.

Each user and profile has a home location. A user will be able to access items associated with his home location and any sub-locations. A profile will be available at its home location and inherited by any sub-locations. Profiles can be excluded from sub-locations so that they are not applied, however. When a profile is created, the home location is set by default to the location you currently have selected.

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

- [Managing Device Servers](#)
- [Managing Group Locations](#)
- [Applying Profiles to Locations](#)
- [Editing Exclusions](#)

Managing Device Servers

This section provides general information about managing distributed mobile device servers. For more information, see [Managing a Mobile Device Server](#).

- [Starting and Stopping a Server](#)



- [Viewing Server Properties](#)
- [Monitoring Server Status](#)

Starting and Stopping a Server

You can start and stop a device server from the Navigation Window of the Avalanche Console.

To restart a server:

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

To stop a server:

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

Viewing Server Properties

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

To view Server properties:

- From the Navigation Window, right-click the server you want view properties for and select the **Mobile Device Server Properties** option.

Monitoring Server Status

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

The following information displays in the columns:

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



Indicates the Server is currently offline.



Indicates the Server is currently online and running.

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





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



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



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

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



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



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

Managing Group Locations

Group locations are groups of mobile devices that connect to the same server. Group locations allow increased flexibility for assigning different profiles at the same server location. Avalanche uses selection criteria to determine which devices belong to each group location.

NOTE: An exception is a group location that has sub-locations. It does not use selection criteria. Instead, these "parent" groups display all of the devices that are included in the sub-locations.

A device can belong to more than one group location concurrently. If a device is included in more than one group location, it will use the profiles from the highest priority location. Locations are assigned priority as they are created, so the first location you create has the highest priority.

This section contains the following tasks for managing group locations:

- [Creating a Group Location](#)
- [Viewing Mobile Devices in Group Locations](#)
- [Additional Group Location Functions](#)

Creating a Group Location

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



To create a group location:

- 1 Right-click the server location where you want to place the group location and select **Create Group Location**.

The *New Group Location* dialog box appears.

- 2 Type a name for the group location.
- 3 If you do not want inherited profiles and device groups to be visible, enable the **Hide inherited profiles and device groups** option.
- 4 Use the Selection Criteria Builder to configure unique selection criteria for the group location.
- 5 When you are finished, click **OK**.

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

Viewing Mobile Devices in Group Locations

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

To view the mobile devices:

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

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

Additional Group Location Functions

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

The additional options for group locations are as follows:

Copy Allows you to copy the group location.

Delete Allows you to delete the group location.



Applying Profiles to Locations

Once you have established your locations and created profiles, you can assign profiles to your network. A profile applies settings for your devices or server. If you do not assign the profiles you create to locations, the settings in those profiles will not be deployed.

When you assign a profile to a location, it is also applied to any sub-locations and their devices. The profiles are applied to the devices based on the selection criteria for the profile and the priority in which the profiles are listed in the Avalanche Console. For information on excluding profiles that have been inherited, see [Editing Exclusions](#).

Each profile can have selection criteria that define which devices can use the profile. A profile can be assigned additional selection criteria when it is applied to a location. This may be useful when a single location requires specialized or additional criteria. For information on selection criteria, see [Using Selection Criteria](#).

For a general description of the types of profiles available, see [Getting Started](#).

[To apply a profile to a location:](#)

- 1 Select the location where you want to apply the profile from the Navigation Window.
- 2 Select the **Properties** tab.
- 3 Click **Add** on the **Applied Profiles** tab.
- 4 From the list that appears, select the profile you want to apply and click **OK**.
- 5 The Application Selection Criteria dialog box appears.
- 6 Use the Selection Criteria Builder or type the selection criteria in the dialog box, if desired, and click **OK**.

The profile is added to the location.

- 7 Save your changes.

The assigned profile will be deployed.

[To view where a profile has been applied:](#)

- 1 From the **Profiles** tab, select the profile you want to view.
- 2 Click the **Applied Locations** tab. You cannot change the information from this tab. This tab displays the following information:
 - **Parent Path**. Displays any parent locations.
 - **Group**. The name of the location where the profile is applied.



- **Selection Criteria.** Any selection criteria that are applicable at the location where the profile is applied.

Editing Exclusions

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

For example:



Navigation Window

When a profile is applied at My Enterprise, it is also applied to all sub-locations. However, if it is excluded at Group A, the profile will also be excluded from Group 1 and Group 2.

When a profile has been excluded from a parent location, you can allow a sub-location to apply it. Using the above example, you could reapply a profile to Group 1 that has been excluded at Group A. (It would still be excluded at Group 2.)

To exclude an inherited profile:

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

The profile will be excluded, but will still appear in the **Applied Profiles** tab for all sub-locations.



To reapply an inherited profile:

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

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



Chapter 6: Managing Network Profiles

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

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

The **Authorized Users** button for a network profile allows you to assign administrative privileges for a profile to a user that has Normal user rights and is not assigned permissions to profiles. This allows you to give a user permission for one specific profile. Users that have permission for the profile will not appear in the list of available users. For information about creating users and assigning permissions, see [Managing User Accounts](#).

This section contains the following topics:

- [Creating Network Profiles](#)
- [Configuring General Settings for Network Profiles](#)
- [Configuring Scheduled Settings](#)
- [Exporting Profiles for Configuring Enablers](#)

Creating Network Profiles

A network profile allows you to control network settings for mobile devices. The profile must be enabled and applied to a location and then it will be used by all devices meeting the profile's selection criteria. The home location for the profile is the location you have selected when you create the profile.

To create a network profile:

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

The Add Profile Wizard appears.

- 2 Select the **Network Profile** option and click **Next**.
- 3 Type a **Name** for the profile and set the status to either **Enabled** or **Disabled**. Click **Next**.
- 4 Use the Selection Criteria Builder to create selection criteria for the profile. Click **Next**.
- 5 Confirm that the information is correct and click **Finish**.



The profile is created and can be configured.

Configuring General Settings for Network Profiles

Once you have created a network profile, you can configure the IP address pools, status, and whether the profile overrides the settings on the mobile device.

Network profiles allow you to assign IP addresses to your wireless devices from a list of IP addresses called an IP address pool. You can create IP address pools for mobile devices and/or infrastructure devices.

Selection criteria define which mobile devices are managed by the profile. Dynamic selection criteria are defined by Avalanche and apply to a device's encryption and authentication support. For detailed information about using selection criteria, see [Using Selection Criteria](#).

To add addresses to an IP address pool:

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

The *IP Address Pools* dialog box appears.

- 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)

- 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)

- 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

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

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

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



- 4 Save your changes.

To enable a network profile:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Network Profile** tab, select **Enabled**.
- 4 If you want the settings on the network profile to override any manual IP settings on the device, enable the **Override Settings on Mobile Devices** option. If the profile is configured to override, it overrides each time the device connects. This option is only available when the **Manage WLAN IP** option is enabled.
- 5 Save your changes.

The network profile is now enabled.

Configuring Scheduled Settings

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

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

NOTE: Old Enablers don't store scheduled settings. They will receive the new network settings the first time they connect with the server after the scheduled start time.

This section contains information on the following configuration options:

- [Configuring WLAN IP Settings](#)
- [Configuring WLAN Settings](#)
- [Configuring WWAN Settings](#)

Configuring WLAN IP Settings

With a network profile, you can configure WLAN IP settings for your devices and schedule when those settings will be applied. The options include:



| | |
|---|---|
| Manage IP Assignment | Allows you to manage the IP addresses assigned to your mobile devices. You can choose to use either a DHCP server or IP pool assignment. |
| Server Address | <p>Provides mobile devices with the server address. You can provide the address, DNS name, or use the server location value. If you choose to use the server location value, the mobile devices use the mask/address of the server to which the device connects.</p> <p>If using a DNS name, click Validate to ensure the address can be resolved. If the mobile device profile has provided a server address, that address will override whatever is provided by the network profile.</p> |
| Gateway Address | Provides mobile devices with the address for the node that handles traffic with devices outside the subnet. You can provide the address, DNS name, or use the server location value. |
| Subnet Mask | Provides mobile devices with the subnet mask. You can provide the address, DNS name, or use the server location value. |
| Domain Name System (DNS) | Provides the domain name to the devices. |
| Primary DNS | Provides mobile devices with the IP address for a primary DNS. |
| Secondary | Provides mobile devices with the IP address for a secondary DNS (used if the primary DNS is unavailable). |
| Tertiary | Provides mobile devices with the IP address for a tertiary DNS (used if the primary and secondary DNS are unavailable). |
| (Infrastructure Device IP Settings) Manage IP Assignment | Allows you to manage the IP addresses assigned to your infrastructure devices with a DHCP server. |

To configure WLAN IP settings for a network profile:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Network Profile** tab, enable the **Manage WLAN IP** option.
- 4 In the Scheduled Settings area, select the date and time you want the settings to take effect from the drop-down list.



- If you would like to add another start time for different settings to the list, click **Add** and select the date and time you want it to begin.
 - If you want to add another start time using the settings currently configured, click **Clone**.
 - If you want to change the currently selected start time, click **Edit**.
- 5 Select the **WLAN IP Settings** tab.
 - 6 Configure the WLAN IP settings as desired.
 - 7 Save your changes.

Configuring WLAN Settings

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

SSID This option provides wireless devices with the SSID. The SSID is a service set identifier that only allows communication between devices sharing the same SSID.

Encryption This option allows you to enable encryption between your devices and the server. You have the following options for encryption:

Use Profile/None. Devices do not encrypt information.

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

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



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

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

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

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

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

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

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

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



PEAP/MS-CHAPv2. (Protected Extensible Authentication Protocol combined with Microsoft Challenge Handshake Authentication Protocol)

PEAP/MS-CHAPv2 is available when you are using encryption. It uses a public key certificate to establish a Transport Layer Security tunnel between the client and the authentication server.

PEAP/GTC. (Protected Extensible Authentication Protocol with Generic Token Card) PEAP/GTC is available when you are using encryption. It is similar to PEAP/MS-CHAPv2, but uses an inner authentication protocol instead of MS-CHAP.

EAP_FAST/MS-CHAPv2. (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling combined with MS-CHAPv2) EAP-FAST uses protected access credentials and optional certificates to establish a Transport Layer Security tunnel.

EAP_FAST/GTC. (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling with Generic Token Card) EAP-FAST uses protected access credentials and optional certificates to establish a Transport Layer Security tunnel.

TTLS/MS-CHAPv2. (Tunneled Transport Layer Security with MS-CHAPv2) TTLS uses public key infrastructure certificates (only on the server) to establish a Transport Layer Security tunnel.

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

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

To configure WLAN settings:

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



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

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

- 7 Save your changes.

Configuring WWAN Settings

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

Connection Name A name for the connection.



| | |
|---|---|
| Connection Type | There are two connection types available for your WWAN-enabled devices: APN (GPRS / EDGE / 3G). Provide a domain (Access Point Name) if you are using this type of connection. An example of an APN would be: wap.cingular Dial-Up. The number to be dialed by the modem. This does not correspond to the number of the device. |
| Credentials | Sets the Username, Password, and Domain credentials for the connection when they are necessary. |
| Custom Properties | This option allows you to add custom properties to the devices that receive this network profile. By clicking Edit/View , you can add, edit, and delete properties and their values. |
| Enable TCP/IP header compression | Improves the performance of low-speed connections. |
| Enable software compression | Improves the performance of low-speed connections. |
| Activate phone as needed | Allows the Enabler to activate the device's phone if a WWAN connection is necessary. |
| Dial broadband connection as needed | Allows the Enabler to attempt a WWAN connection if a LAN connection cannot be established. |
| Public IP address for Avalanche Server | Provides the IP address of the enterprise server that is accessible from a WWAN. This is necessary if the device tries to contact the server when connecting from outside of the server's local network. |

To configure WWAN settings:

- 1 From the **Profiles** tab, select the network profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Network Profile** tab, enable the **Manage WWAN** option.
- 4 In the Scheduled Settings region, select the date and time you want the settings to take effect from the drop-down list.



- If you would like to add another start time for different settings to the list, click **Add** and select the date and time you want it to begin.
 - If you want to add another start time using the settings currently configured, click **Clone**.
 - If you want to change the currently selected start time, click **Edit**.
- 5 Select the **WWAN Settings** tab.
 - 6 Configure the WWAN settings as desired.
 - 7 Save your changes.

Exporting Profiles for Configuring Enablers

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

To export profiles for Enabler configuration:

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



Chapter 7: Managing Scan to Configure Profiles

Avalanche allows you to create Scan to Configure profiles (barcode profiles) that are configured with network settings. You can then print the profiles as barcodes and a mobile device with an Enabler 3.5 (or later versions) can scan these barcodes. The information from the scanned barcodes is used to configure the network settings on the device, such as the IP address, subnet mask, and gateway. The length of the barcode is configurable.

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, the Enabler does not support the scan to configure feature.

This section contains instructions for the following tasks:

- [Creating a Scan to Config Profile](#)
- [Configuring a Scan to Config Profile](#)
- [Printing Barcodes](#)
- [Scanning Barcodes](#)

Once you have configured your Scan to Config profile, you can apply that profile to any location in the Console. When you apply a profile to a location, the users who have permissions for that location can make changes as necessary. For more information about assigning Scan to Config profiles to a location, see [Applying Profiles to Locations](#).

Creating a Scan to Config Profile

A Scan to Config profile is used to configure network settings, device properties, and registry keys on a mobile device. Once you have configured the profile from the Avalanche Console, you can print the barcodes and then use a device to scan the barcodes. The home location for the profile is the location you have selected when you create the profile.

NOTE: WEP key rotation is not supported for Scan to Config profiles.

To create a Scan to Config profile:

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

The Add Profile Wizard appears.

- 2 Select the **Scan To Config Profile** option and click **Next**.
- 3 Type a **Name** for the profile and set the status to either **Enabled** or **Disabled**. Click **Next**.
- 4 Confirm that the information is correct and click **Finish**.



The profile is created and can be configured.

For more information on configuring device properties and registry keys, see [Configuring a Scan to Config Profile](#).

Configuring a Scan to Config Profile

Configuring Scan to Configure profiles allows you to select the network information you want the mobile devices to use. Use information from a network profile or add separate details such as custom properties or registry keys.

The **Authorized Users** button allows you to assign administrative privileges for a profile to a user that has Normal user rights and is not assigned permissions to profiles. This allows you to give a user permission for one specific profile. Users that have permission for the profile will not appear in the list of available users. For information about creating users and assigning permissions, see [Managing User Accounts](#).

- [Configuring Scan to Config Settings](#)
- [Adding Custom Properties for Scan to Config Profiles](#)
- [Adding a Registry Key to a Scan to Config Profile](#)

Configuring Scan to Config Settings

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

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

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

To configure the settings:

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

Click **Edit**.

- 2 To encrypt the barcodes, type a passcode in the **Encryption Passcode** text box and confirm it in the **Confirm Passcode** text box.



- 3 Set the maximum length of the barcode. This defines how many characters are encoded in each barcode.
- 4 If you have already configured a network profile and want to use the settings from that profile, enable **Use settings from network profile**. Choose which epoch to use by enabling either **Use currently active Epoch** or **Use selected Epoch** and selecting an epoch from the drop-down list.
- 5 If you want to set a static IP address for the device, enable **Assign static IP address** and type the **IP Address**, **Subnet Mask** and **Gateway** in the appropriate boxes.

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

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

The profile is updated with the configured network settings.

Adding Custom Properties for Scan to Config Profiles

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

To add a custom property:

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

The *Edit Property* dialog box appears.
- 4 Type the **Name** and **Value** in the text boxes.
- 5 Select whether the property is a Device or Network property.

NOTE: Most properties will be device properties.

- 6 Click **OK**.

The task is added to the list in the Properties area. The property will be added when the profile is applied on the mobile device.

- 7 Save your changes.



Adding a Registry Key to a Scan to Config Profile

You can add registry keys and values to a profile. These keys will be added to the device registry when the profile is applied.

To add a registry key:

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

The *Add Registry Key* dialog box appears.

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

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

To add a value to a registry key:

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

The *Add Registry Value* dialog box appears.

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

The task is added to the list in the Registry Settings area. The value will be added when the profile is applied on the mobile device.

Printing Barcodes

Once you have created and configured a Scan to Config profile, you can print that profile. The profile prints as a set of barcodes in random order. You can then scan the barcodes with a

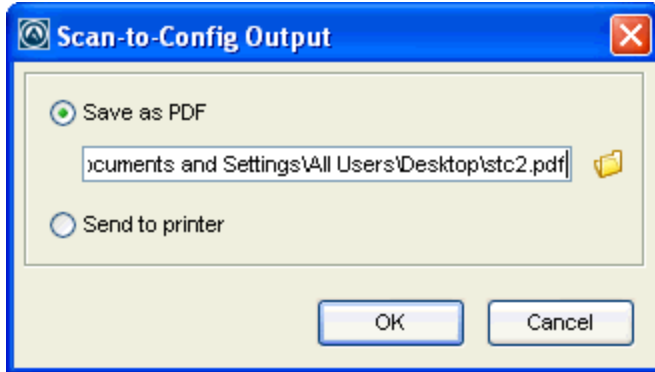


mobile device to change the network settings on that device. You have the option to print the barcodes to a printer or to a .pdf file.

To print a Scan to Config profile as a barcode:

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

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



Scan-to-Config Output dialog box

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

- Or -

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

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

Scanning Barcodes

To scan and apply a Scan to Config profile, you must open the *Scan Configuration* dialog box from the Enabler on the mobile device. Use the mobile device to scan the barcodes in any order. When all the barcodes are scanned, the Enabler applies the configurations on the device.

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



To scan the configuration:

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

The *Scan Configuration* dialog box appears.

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

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

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



Chapter 8: Managing a Mobile Device Server

A Mobile Device Server is server software that lets you remotely manage and configure mobile devices.

Through a Mobile Device Server profile, Avalanche allows you to manage the following settings for your mobile device servers and mobile devices:

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

This section provides information about managing mobile device servers. It contains the following tasks:

- [Configuring a Mobile Device Server Profile](#)
- [Viewing Mobile Device Server Licensing Messages](#)
- [Reinitializing the Mobile Device Server](#)
- [Retrieving Mobile Device Log Files](#)

For information on starting or stopping a server, or viewing server properties and status, see [Managing Device Servers](#).

Configuring a Mobile Device Server Profile

A Mobile Device Server profile allows you to configure logging, device connections, secondary server support, updates and other settings for the mobile device server.

Configure the following settings for a mobile device server:

- [Mobile Device Server Profile General Configuration](#)
- [Configuring Blackouts](#)
- [Restricting Simultaneous Device Updates](#)
- [Scheduling Profile-Specific Device Updates](#)



The **Authorized Users** button allows you to assign administrative privileges for a profile to a user that has Normal user rights and is not assigned permissions to profiles. This allows you to give a user permission for one specific profile. Users that have permission for the profile will not appear in the list of available users. For information about creating users and assigning permissions, see [Managing User Accounts](#).

Mobile Device Server Profile General Configuration

The general settings for a mobile device Server profile include security, terminal IDs, logging, licenses, secondary servers, and settings for how the server handles mobile device information.

Server Security

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

Avalanche offers two options for encryption:

Transport Matches the level of encryption with the capacity of the mobile device.

Encryption Communication between the Mobile Device Server and mobile devices will be encrypted to the degree possible.

Strict Transport Encryption Uses AES encryption for information. Only devices that support AES encryption (Enabler 5.0 or newer) will be able to connect to the server when strict transport encryption is enabled.

Avalanche offers two options for authentication:

Mobile Device Authentication Requires mobile devices to initially connect to the server through a serial connection (RS232) and receive an authentication key. When you enable this option, the Mobile Device Server will challenge any device attempting to connect to the server for a password. If the mobile device does not have the correct password, the Mobile Device Server will not allow a TCP/IP connection.

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



Server Authentication Forces mobile devices to communicate with a single known server. Mobile devices must first connect to the network through a serial connection (RS232) to receive information about the server with which they are allowed to communicate. When you enable this option, the mobile device will challenge any Mobile Device Server attempting contact for a password. If the Mobile Device Server does not have the correct password, the mobile device will not allow a TCP/IP connection.

Both authentication options require mobile devices to connect to the network through a serial connection to receive authentication information before they will be allowed to connect wirelessly. Authentication passwords are set through a dialog box. This dialog box appears when the options are first enabled, or you can click **Set Password** next to the desired authentication option.

Server Resources

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

Reserved Serial Ports Configures a Mobile Device Server to automatically listen for mobile devices using the serial ports on a remote system. Only one application on a host system can maintain ownership of a serial port. If the Mobile Device Server controls the serial ports on the host system, then no other application will be able to use them. Likewise, if another application on the host system (for example, Microsoft ActiveSync) has control of the serial ports, then the Mobile Device Server will not be able to use them. If you list more than one port, separate them with semicolons. For example: COM1 ; COM2

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

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

You also have the option to use a C-style format to create a template for the terminal ID range. For example, `Seattle-%d` would generate IDs such as `Seattle-4`, and `Seattle-%05d` would generate IDs such as `Seattle-00004`.

To change a terminal ID that has already been assigned to a device, click **Edit Terminal ID** on the **Properties** tab of the *Mobile Device Details* dialog box.



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

The following logging options are available on a Mobile Device Server:

Critical. Writes the least information to the log file, reporting only critical errors that have caused the Mobile Device Server to crash.

Error. Writes errors that are caused by configuration and/or communication problems as well as and Critical messages to the log file.

Warning. Writes Critical messages, Error messages, and indicates possible operational problems in the log file.

Info. The recommended logging level. This logging level documents the flow of operation and writes enough information to the log file to diagnose most problems.

Debug. Writes large amounts of information to the log file that can be used to diagnose problems.

Max Log Size. Specifies the maximum size (in kB) of the log file before beginning a new file.

Avalanche Licensing

A Mobile Device Server profile has the following licensing options:

Release Device licenses after _ days of inactivity Sets how long the Mobile Device Server will wait before it returns a license for an inactive device to the pool of unused licenses.

Enable Fast-Expiration Allows the server to terminate the license lease after the specified time period without contacting the device. If this option is disabled, the server will attempt to contact any devices that have not communicated with the server in the configured time period. If the device does not respond, the license lease will be terminated.

Secondary Servers

You can configure the following connection settings:



| | |
|---|---|
| Enable Secondary Server Support | Authorizes the mobile device to attempt to connect a secondary Mobile Device Server if the primary server is not available. You can click on the Secondary Servers button to configure the list of secondary servers and their addresses/hostnames. |
| Override Connection Timeout Settings | The Mobile Device Server profile settings will override any connection settings configured on the mobile device. |
| Server Connect Timeout | Configures the number of seconds the mobile device will wait between attempts to connect to the current mobile device server. |
| Server Advance Delay | Configures the number of seconds before the device advances to the next server. Ensure the Server Advance Delay setting is a multiple of the Server Connect Timeout setting. For example, if you have your Server Connect Timeout set to 10 seconds and the Server Advance Delay set to 60 seconds, the mobile device will attempt to contact the server six times (every 10 seconds for 60 seconds). |

Device Settings

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

| | |
|-------------------------------------|---|
| Device Chat Timeout | Sets the amount of time in minutes that both the device and the server will wait before dropping a chat session. |
| Device Comeback Delay | Sets the amount of time in minutes that the mobile device will wait before trying to reconnect to the Mobile Device Server after a connect rejection (i.e., if the device tried to connect during an exclusion window). |
| Enable Device Caching | Enables mobile devices to download software package files from other mobile devices on the same subnet instead of from the Mobile Device Server. Device caching reduces the demands on the Mobile Device Server during software package synchronization. For information about implementing device caching, call Wavelink Customer Support. |
| Enable Persistent Connection | Causes each device to create a persistent TCP connection with the Mobile Device Server. This ensures communication in an environment where UDP packets cannot reliably be transmitted between the server and the device. |



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

Configuring Blackouts

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

To create a blackout window:

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



- 3 From the **Blackouts and Updates** tab:
 - if you want to create a server-to-server blackout window, click the **Add** button in the Server-to-Server Communication Restrictions region.
 - if you want to create a device-to-server restriction window, click the **Add** button in the Device-to-Server Communication Restrictions region.

The *Add Blackout Window* dialog box appears.

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

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

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

Restricting Simultaneous Device Updates

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

To restrict simultaneous device updates:

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

Scheduling Profile-Specific Device Updates

From the Mobile Device Server profile, you can schedule profile-specific updates for your mobile devices.

When you configure a Mobile Device Server update, you have the following options:



| | |
|--|--|
| Event type | Select a one-time event, a recurring event, or a post-synchronization event. A post-synchronization event will take place after each synchronization between the Enterprise Server and the Mobile Device Server. This ensures that each time the Server is updated, the devices are as well. |
| Time Constraints | Set the start time and, if desired, the end time for the event. |
| Allow the mobile device user to override the update | Creates a prompt when the update is scheduled to occur that allows the mobile device user to override the update. |
| Delete orphaned packages during the update | Causes packages that have been orphaned to be removed from the device. A package is considered orphaned if it has been deleted from the Avalanche Console, if the software profile it belongs to has been disabled, or if the package has been disabled. |
| Force package synchronization during the update | Causes the Mobile Device Server to verify the existence and state of each file of each package individually rather than consulting the meta-file which would normally provide information on those files. |

To schedule a profile-specific device update:

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

The *Add Scheduled Update* dialog box appears.

- 4 Select the event type. If you select **Recurring Event**, the **Recurring Period** lists become active. The first list allows you to determine whether the update occurs on either a daily or weekly basis. If you select **Weekly** from this list, the second list becomes active, allowing you to select the day on which the update occurs.
- 5 Set the start time by clicking the calendar icon to open the *Select a date and time* dialog box. Choose the start time and click **OK**.

NOTE: If you chose a post-synchronization event, the start and stop time options are disabled.



- 6 If desired, enable the **Stop if not completed by** option. Set the stop time by clicking the calendar icon to open the *Select a date and time* dialog box. Choose the stop time and click **OK**. Selecting an end time is not required. This allows you to create events that recur indefinitely.
- 7 Enable the other update options as desired.
- 8 Click **OK**.

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

NOTE: Many mobile devices incorporate a sleep function to preserve battery life. If a device is asleep, you must “wake” it before it can receive a server-initiated update from Avalanche. Wake-up capability is dependent on the type of wireless infrastructure you are using and the mobile device type. Contact your hardware and/or wireless provider for details.

Viewing Mobile Device Server Licensing Messages

The Avalanche Console receives messages about license usage from the mobile device server. You can view these messages from the *Device Server Licensing Messages* dialog box. This dialog box provides information about the location where the server resides and the licensing message.

To view licensing messages:

- Click **View > Distributed Server License Messages**.

The *Device Server Licensing Messages* dialog box appears.

Reinitializing the Mobile Device Server

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

To reinitialize the Mobile Device Server:

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

The server contacts the Enterprise Server and downloads any updates.



Retrieving Mobile Device Log Files

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

To retrieve mobile device log files:

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

The file is saved. Unzip the file to view the mobile device log files.



Chapter 9: Managing Software Profiles

Software profiles allow you to organize and configure software for deployment to mobile devices. Add software packages to the profile, configure them, and schedule how and when they are installed. When the profile is enabled and applied to a location, the software packages associated with the profile are installed on devices meeting the selection criteria for the profile and packages.

This section contains the following topics:

- [Creating Software Profiles](#)
- [Managing Software Packages](#)

Creating Software Profiles

Create software profiles to manage how and when software is distributed or updated on mobile devices. The home location for the profile is the location you have selected when you create the profile. Once a software profile has been created, you can edit the name, status, and selection criteria. You can also add software packages to the profile. For information on adding and configuring software packages, see [Managing Software Packages](#).

The **Authorized Users** button allows you to assign administrative privileges for a profile to a user that has Normal user rights and is not assigned permissions to profiles. This allows you to give a user permission for one specific profile. Users that have permission for the profile will not appear in the list of available users. For information about creating users and assigning permissions, see [Managing User Accounts](#).

Selection criteria determine which mobile devices receive the software profile. Only devices that meet the selection criteria for the software profile will receive the software associated with the profile. For information about creating selection criteria, see [Building Selection Criteria](#).

You can create software profiles from the **Profiles** tab or from the **Quick Start** tab.

To create a software profile from the **Profiles** tab:

- 1 From the **Profiles** tab, click **Add Profile**.
The *Add Profile Wizard* appears.
- 2 Select the **Software Profile** option and click **Next**.
- 3 Type a **Name** for the profile and set the status to either **Enabled** or **Disabled**. Click **Next**.
- 4 Use the Selection Criteria Builder to create selection criteria for the profile. Click **Next**.
- 5 Confirm that the information is correct and click **Finish**.

The profile is created and can be configured.



To add a software profile from the **Quick Start** tab:

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

The *Add Device Software Wizard* launches.

- 2 In the **Create a New Software Profile** text box, enter a name for the profile and then click **Next**.
- 3 If desired, enable the profile and choose selection criteria for it. Click **Next**.
- 4 In the Apply the Software Profile screen, you can choose to apply the profile and designate where you want it to be applied. Click **Next** to continue.
- 5 In the Select a Software Package to Add screen, you can add, create or copy a package to the profile. For information about all these options see [Adding a Software Package](#).
- 6 Click **Next**.

The End User License Agreement appears.

- 7 Enable **Yes I agree** to agree to the license agreement and click **Next**.
- 8 The Installing the Software Package screen appears and the software is added to the profile. When the package has been installed successfully, click **Next**.
- 9 The Configure the Software Package screen appears. If desired, enable the software package and configure it using the available utilities.
- 10 Click **Finish**.

The software profile is created and can be enabled and configured.

Managing Software Packages

A software package is a collection of application files that reside on a mobile device. This includes any support utilities used to configure or manage the application from the Avalanche Console. Each software package usually has default selection criteria that cannot be changed.

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

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



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

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

This section includes the following information:

- [Adding a Software Package](#)
- [Building New Software Packages](#)
- [Creating CAB or MSI Packages](#)
- [Copying Software Packages](#)
- [Enabling Software Packages](#)
- [Configuring Software Packages with a Utility](#)
- [Configuring Software Packages for Delayed Installation](#)
- [Peer-to-Peer Package Distribution](#)



Adding a Software Package

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

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

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

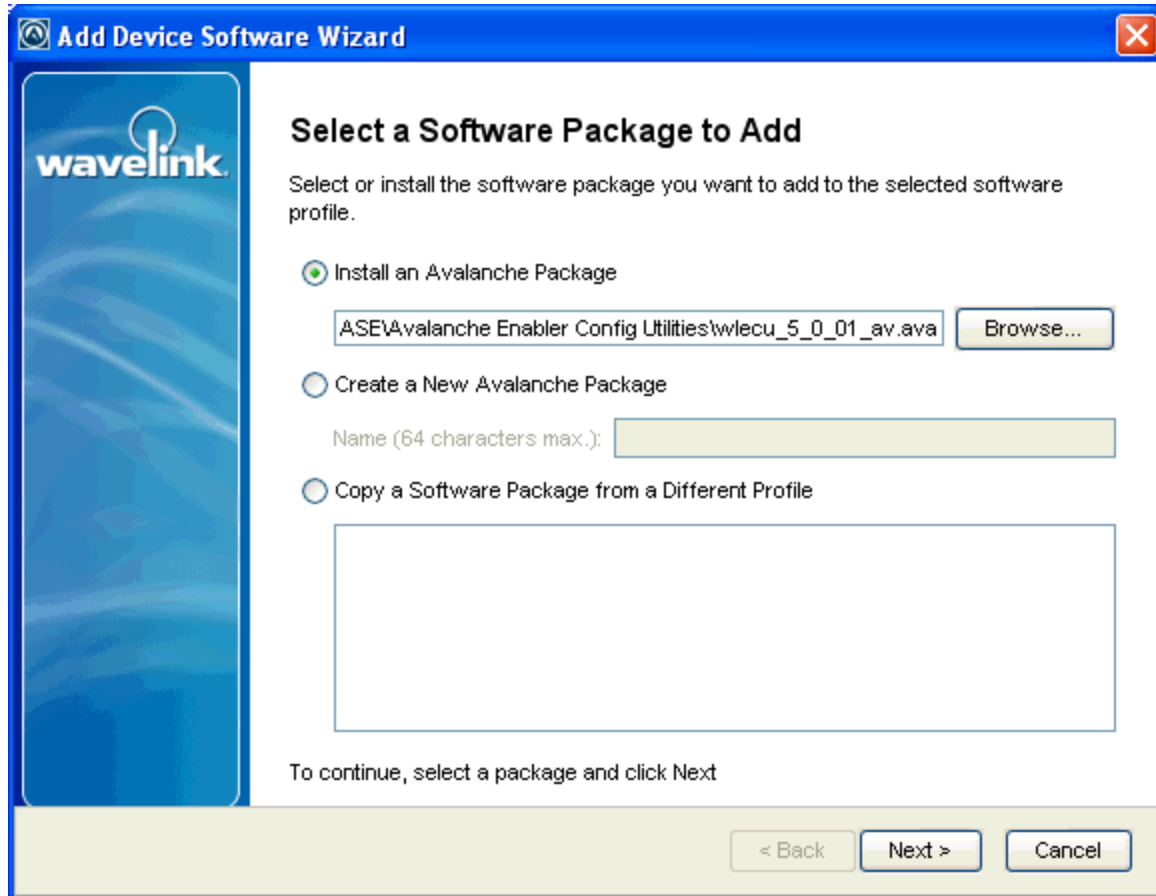
The following instructions provide information about adding an Avalanche package to a software profile. For information about building a new package, see [Building New Software Packages](#).

To add a software package:

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

The *Add Device Software Wizard* appears.





Select Package

- 3 Select **Install an Avalanche Package** and browse to the location of the software package.
- 4 Select the file and click **Next**.
A *License Agreement* dialog box appears.
- 5 Accept the license agreement and click **Next**.
- 6 The package files will begin extracting locally. When the extraction is complete, click **Next**.
- 7 The Configure the Software Package screen appears. If desired, enable the software package and configure it using the available utilities.
- 8 When you are finished configuring, click **Finish** to complete the installation.

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



Building New Software Packages

Avalanche allows you to compile files to create a new software package. Creating a package bundles files together so they can be installed together. Ensure you know the location of the files you want to include in the package.

In addition to the files, a new software package has the following options:

Title A title for the package.

Vendor The package vendor.

Version The version number of the package.

Install Drive The drive on the mobile device where the package will be installed.

Drive

Install Path The exact path where the package will be installed.

Path

Post Install Options Options for if the device will perform a warm boot or a cold boot after installation

Install Options has completed, or if a program runs once installation is completed. When you select

Options to run a program, the drop-down list will become active and you can select a program from your package to run.

NOTE: Post-install actions are optional unless you select to run a program. Then you are required to select which program you want to run.

To build a new package:

1 Select the profile to which the package will belong from the Profiles List.

2 From the **Software Profile** tab, click **Install Package**.

The *Add Device Software Wizard* appears.

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

4 Click **Next**.

A *Specify the Files in the Ad Hoc Package* screen appears.

5 Click **Add** and browse to the location of the files you want to add to the package.

6 Select the file and click **Open**.

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

7 Click **Next**.



The *Ad Hoc Package Options* screen appears.

- 8 Configure the package options and click **Next**.

The *Add Selection Criteria* screen appears.

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

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

- 10 Click **Next**.

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

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

- 12 Click **Finish** to complete the package.

Creating CAB or MSI Packages

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

To create `.CAB` or `.MSI` packages:

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

The *Add Device Software Wizard* appears.

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

The *CAB or MSI File Options* screen appears.

- 7 Enter the name of the package.



- 8 If you want the package to be uninstalled once the program information is retrieved by the mobile device, enable **Remove After Install**.
- 9 Click **Next**.
- 10 The package files will begin extracting locally. When the extraction is complete, click **Next**.
The *Configure the Software Package* screen appears. This dialog box allows you to enable the package immediately and displays any configuration tools available for the package.
- 11 Click **Finish** to complete the package creation.

Copying Software Packages

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

To copy a software package:

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

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

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

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

Enabling Software Packages

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

To enable a software package:

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

Configuring Software Packages with a Utility

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



Avalanche Console. Configuration options will differ based on the software package. For details about configuring software packages, see the specific user guide for that product.

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

To configure a software package:

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

The *Configure Software Package* dialog box appears.

- 4 From the available list, double-click the utility you want to use to configure the package.
- 5 When the options are configured, click **OK**.

The software package is configured for deployment.

Configuring Software Packages for Delayed Installation

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

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

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

Package activation is supported by Enabler version 4.1 and later.

To configure a software package for delayed installation:

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



Delayed Package Activation

Delay activation until: Jul 20 2010 - 22:15

Delay activation for: 0 minutes

Activation window: 23:00 to 00:00

Allow user to activate on demand

Delayed Package Activation

- 4 In the Delayed Package Activation area, enable the options as desired:
 - If you want to delay package activation until a specific date and time, enable the **Delay activation until** option and click on the calendar button to select a date and time.
 - To further delay the package installation after it has been activated, configure the **Delay activation for** __ minutes option.
 - If you want the package to be activated during a certain time window, enable the **Activation window** option and configure the hours during which the package will activate.
 - If you want the device user to have the option to override the software package installation at the activation time, enable the **Allow user to activate on demand** checkbox. When this option is selected, the user will be able to install the package as soon as it is downloaded.
- 5 Save your changes.

Peer-to-Peer Package Distribution

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

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

| Field | Description |
|--|---|
| Enabled Cached Peer-to-Peer Package Distribution | Enable this option to allow a package to be shared across multiple devices via peer-to-peer connections. When deployed to a mobile device, the package will then be available for other mobile devices to receive the profile from that package store device. |
| Do not | Enable this option to configure the time at which a non-package store device can contact a package store device to receive an update. A non-package store |



| Field | Description |
|---|---|
| allow non-Package Store Devices to begin updating until | device refers to a mobile device that is not being used to update other mobile devices. |
| Do not allow server to update non-Package Store Devices until | Enable this option to configure the time at which a non-package store mobile device can contact the Server to update and receive this package. Once the configured time is reached, the mobile devices will first attempt to contact a package store device to receive the update. If a package store device cannot be contacted or the connection times out, the device will then attempt to contact the Server. A non-package store device refers to a mobile device that is not being used to update other mobile devices. |

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

| If | Then Package Store Devices | And Non-Package Store Devices |
|---|--|---|
| 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) | <i>Can</i> contact the Server for updates at any time. | Cannot contact any package store devices. Will attempt to contact the Server to receive 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) | <i>Can</i> contact the Server for updates at any time. | <i>Can</i> contact package store devices to update and receive the profile. If the device can't contact a package store device, it will attempt to contact the Server. |
| 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 | <i>Can</i> contact the Server for updates | Cannot contact the Server for updates. Cannot contact any package store devices. |



| If | Then Package Store Devices | And Non-Package Store Devices |
|---|--|---|
| | at any time. | |
| 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 | <i>Can</i> contact the Server for updates at any time. | <i>Can</i> contact package store devices to receive updates. If the device can't contact a package store device or the connection times out, the device <i>can</i> contact the Server to receive updates. |
| No options are enabled | <i>Can</i> contact the Server for updates at any time. | <i>Can</i> contact package store devices or Server for updates at any time. |

NOTE: For more information on how to configure devices for peer-to-peer package distribution, contact Wavelink Customer Service.

To configure peer-to-peer package distribution:

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



Chapter 10: Managing Mobile Devices

This section provides information about the following mobile device topics:

- [Mobile Device Inventory Tab](#)
- [Viewing Mobile Device Details](#)
- [Configuring Mobile Device Properties](#)
- [Contacting the Mobile Device](#)
- [Software Inventory](#)

Mobile Device Inventory Tab

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

Model The model name of the mobile device.

Name

Terminal ID The unique ID automatically generated by Avalanche or assigned by a Console user.

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.

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

Last Contact The date and time of the last contact the mobile device had with Avalanche.

Recent Activity The status of a mobile device with respect to Avalanche. For example, when the mobile device receives new software, the activity status is *Downloading*.

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



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

To delete mobile devices:

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

The device is removed. It retains the ability to connect and re-associate itself with the server, however.

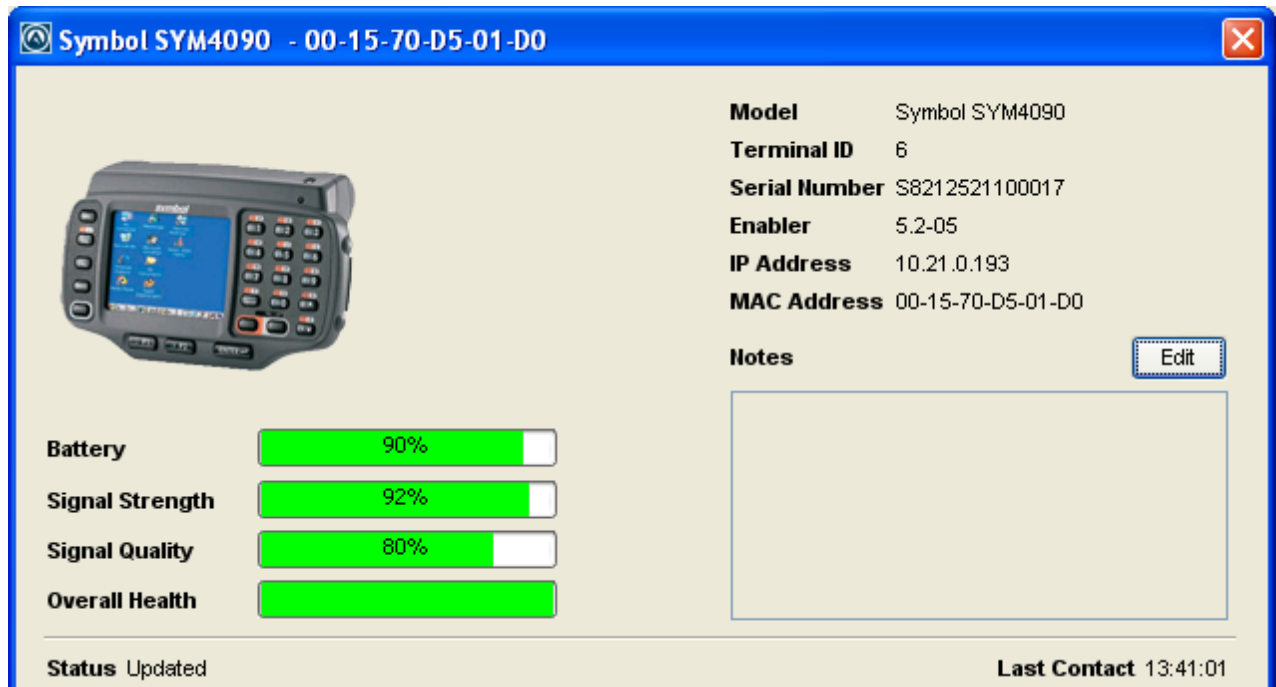
Viewing Mobile Device Details

The *Mobile Device Details* dialog box appears when you right-click the mobile device you want to view and select **Mobile Device Details**. It provides information about a specific mobile device and consists of the following areas:

- **Summary Information**. Provides a quick summary of device, health, signal strength and battery life information. The bars will display red, yellow, or green depending on the status of the battery, signal strength, overall health, and signal quality of the device.

The overall health of a device is determined by properties reported by the device. If any one of seven properties reports a warning level, the overall health is set to that warning level. The properties are: low flash memory, low RAM memory, low battery charge, critical battery charge, low signal strength, low signal quality, or a package install status as either "pending" or "error".





Symbol SYM4090 - 00-15-70-D5-01-D0

Model Symbol SYM4090
Terminal ID 6
Serial Number S8212521100017
Enabler 5.2-05
IP Address 10.21.0.193
MAC Address 00-15-70-D5-01-D0

Notes

Battery 90%
Signal Strength 92%
Signal Quality 80%
Overall Health

Status Updated **Last Contact** 13:41:01

Device Details summary information

- **Device Tabs.** Provides access to the following tabs:
 - **General.** Provides general network and wireless information about the device.
 - **Installed Software.** Provides information about the software applications installed on the device. For details, see [Software Inventory](#).
 - **Packages.** Lists all the packages currently available for the device and the status of each package.
 - **Properties.** Lists the properties of the device and their values. This tab also allows you to add properties and values. For details about the tasks you can perform in the **Properties** tab, see [Configuring Mobile Device Properties](#).
 - **Applied Profiles.** Lists the profiles that are applied.
 - **Device Control.** Provides options for updating the mobile device, sending text messages, pinging the device, using Remote Control, and connecting to the Session Monitor. For details, see the links below or [Contacting the Mobile Device](#).
 - **Priority of Matching Profiles.** Lists the profiles on the device by priority.
 - **History.** Provides a history of Avalanche actions for the mobile device. This may include actions such as changes to packages, edited properties, applying a profile, rebooting the device, or changes to the Enabler configuration by a device user. This information is only available for devices with 5.2 Enablers that are configured to report



the events. (This can be configured on the Reporting tab of the Enabler Configuration Utility.)

The following sections provide information on viewing a device's location or location history:

- [Locating a Mobile Device](#)
- [Locating a Device using Cell Tower Information](#)
- [Viewing Location History](#)

Locating a Mobile Device

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

To view the location of a mobile device:

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

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

Locating a Device using Cell Tower Information

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

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

To locate a device using cell tower information:

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

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



Viewing Location History

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

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

To view the location history of a mobile device:

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

The *Start and End Time* dialog box appears.

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

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

Configuring Mobile Device Properties

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

NOTE: See [Building Selection Criteria](#) for more information on using properties as selection variables.

You can view the properties for a specific mobile device by right-clicking the device from the **Mobile Device Inventory** and selecting **Mobile Device Details** from the context menu.

The columns that appear in the **Properties** tab are as follows:

Name The name of the property.

Value The value of the property.



Pending Value Indicates whether the property needs to be updated on the mobile device. If it needs to be updated, column will display the pending value in italics.

Icon Indicates whether the value of the property is static, snapshot, or configurable data. Static means the information does not change, snapshot means that the property is updated by the device, and configurable means that a user may change the value.

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

- [Creating Custom Properties](#)
- [Creating Device-Side Properties](#)
- [Editing Properties](#)
- [Deleting Properties](#)

Creating Custom Properties

From the Avalanche Console, you can create custom properties on the mobile devices. These properties can then be used to build selection criteria for software profiles or as device filters.

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

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

To create custom properties:

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



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

Creating Device-Side Properties

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

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

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

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

Editing Properties

Some of the pre-defined properties (and all of the custom properties) on mobile devices support editing of values. When you change the value of a property, the new value is downloaded to the mobile device at the next update.

Custom properties can be edited either for a specific mobile device, for a mobile device group, or using a mobile device profile or a Scan to Config profile. For information on editing properties for a group of devices, see [Editing Properties for Mobile Device Groups](#). For information on using a profile to edit properties, see the section for that profile type.

To edit a property for a mobile device:

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

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

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



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

Deleting Properties

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

To delete a property:

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

Contacting the Mobile Device

This section provides information about connecting to a mobile device and viewing device location. The following tasks are available from the **Device Control** tab in the *Mobile Device Details* dialog box.

- [Pinging Mobile Devices](#)
- [Sending a Message to a Device User](#)
- [Updating a Mobile Device](#)
- [Chatting with a Device User](#)
- [Using the Remote Control SMS Options](#)
- [Using Remote Control](#)
- [Launching the Session Monitor](#)

NOTE: The Registry Explorer, File Explorer, and Process Manager icons available in this dialog box are only available when the mobile device has a licensed Remote Control client.

Pinging Mobile Devices

You can ping devices that are currently in range and running the Avalanche Enabler. This is not an ICMP-level ping, but rather an application-level status check. This feature indicates whether the mobile device is active or not.



You can also ping all the mobile devices in a group location simultaneously if the devices are in range and running the Avalanche Enabler.

To ping a mobile device:

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

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

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

To ping mobile devices in a group location:

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

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

Sending a Message to a Device User

Send a text-based message to a device currently in range and running the Avalanche Enabler. You can also send the same message to all devices in a group location simultaneously.

To send a message to a 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 **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**.

To send a message to the devices in a group location:

- 1 Right-click the group location from the Navigation Window.
- 2 Select **Send Text Message** from the context menu.
- 3 Type a message in the **Text Message Field**.
- 4 Enable the **Provide Audible Notification** text box if you want a sound to play when the mobile device receives the message.
- 5 Click **OK**.

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

Updating a Mobile Device

You can perform individual updates for mobile devices that are currently in range and running the Avalanche Enabler or an Avalanche-enabled application.

When you update the device, you have the following options:

| | |
|--|--|
| Allow User to Override the Update | Gives the mobile device user the option to override the update. |
| Force Package Synchronization | Forces the package to update on the device. |
| Delete Orphan Packages | Removes orphan packages from the device. Edit the list of orphan packages to remove specific packages from the device. |

NOTE: The rules that govern which mobile devices can receive a particular update are determined by the selection criteria. See [Building Selection Criteria](#) for more information on building selection criteria.

To update a mobile device:

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

The *Update Now* dialog box appears.

- 4 Enable the options as desired and select which orphan packages you want to remove.



- 5 Click **OK**.

The **Status** field in the Activity region allows you to monitor the status of the update.

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

NOTE: Many mobile devices incorporate a sleep function to preserve battery life. If a device is asleep, you must “wake” it before it can receive a “pushed” update from Avalanche. Wake-up capability is dependent on the type of wireless infrastructure you are using and the mobile device type. Contact your hardware and/or wireless provider for details.

Chatting with a Device User

A user can initiate a two-way chat session that allows the device user and the Console user to communicate text back and forth. The device user can create an alert to request a chat session, but the session can only be initiated from the Console.

To initiate device chat:

- 1 In the **Mobile Device Inventory**, right-click the device you want to chat with and click **Device Chat**.

The *Two-way mobile device messaging* dialog box appears.

- 2 Type the message you want to send in the lower text box. When you press **Send** or **Enter**, the message is sent to the device and appears in the upper text box. The device user’s response will appear in the upper text box.
- 3 When you are finished you can save the message as a `.txt` file by clicking **Save**, or click **Close** to close the dialog box.

Wiping a Mobile Device

When you have applied a mobile device profile that has Device Wipe folders configured, you can perform a remote wipe of the device. A remote wipe will delete the contents of the folders and reboot the device. If files in the folders were unable to be deleted because they were in use, the Enabler will attempt to delete them after the reboot. If the server is unable to contact the device using a TCP/IP connection, it will attempt to send the wipe command using SMS.

If there is more than one mobile device profile applied on the device, all of the Device Wipe folders for all of the applied profiles will be deleted during a device wipe.

NOTE: Avalanche does not provide a method for restoring any of the information in the deleted folders.



To perform a remote device wipe:

- 1 From the **Mobile Device Inventory** tab, right-click the device you want to view.
- 2 From the context menu, select **Wipe Device**.
- 3 The *Confirm Device Wipe* dialog box appears. Click **Yes** if you are certain you want to wipe the folders specified in the mobile device profile.

The server will send the device a command to delete the folders specified in the mobile device profile.

Using the Remote Control SMS Options

The SMS options on the **Device Control** tab of the *Mobile Device Details* dialog box are specific to Avalanche Remote Control. If you have Remote Control installed and configured with the correct WWAN information, you can use these options to send SMS messages to the device. You can either send a text message to the device user, or you can send an SMS message that tells the Enabler to connect to the server to download any updates.

To use Remote Control SMS options:

- 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 **SMS Text Message** or **SMS Update Now** icon.

If you choose to send a text message, type the message and click **Send**.

Using Remote Control

Remote Control functionality is only available for devices that have a licensed Remote Control package installed.

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

- 1 Obtain the Remote Control software.
- 2 Install the Remote Control server.
- 3 Add the Remote Control software package to an Avalanche software profile.
- 4 License Remote Control.
- 5 Deploy the Remote Control software package to your mobile device.



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

This section provides basic information about using Remote Control to connect to a mobile device. For more information, see the *Wavelink Avalanche Remote Control User Guide*.

To use Remote Control to connect to a mobile device:

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

The *Mobile Device Details* dialog box opens

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

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

Launching the Session Monitor

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

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

- 1 Obtain a TE Client 5.x (or later version) software package.
- 2 Add the software package to a software profile. See [Adding a Software Package](#) for more information.
- 3 Configure the Client software package.
- 4 Deploy the Client to the mobile device. For more information about deployment, refer to [Performing a Server Synchronization](#).
- 5 Launch the Client on the mobile device.
- 6 Launch the Session Monitor.



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

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

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

- 1 Ensure you have installed a TE Client on the mobile device.
- 2 Select the location where the device is from the Navigation Window.
- 3 Click the **Mobile Device Inventory** tab.
- 4 Right-click the device for which you want to launch the Session Monitor and select **Session Monitor** from the menu.

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

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

- 1 Ensure you have installed a TE Client on the mobile device.
 - 2 Select the location where the device is from the Navigation Window.
 - 3 Click the **Mobile Device Inventory** tab.
 - 4 To open the *Mobile Device Details* dialog box:
 - Double-click the mobile device on which you want to launch session monitor.
- Or-
- Right-click the mobile device on which you want to launch session monitor and select **Mobile Device Details**.
 - 5 In the *Mobile Device Details* dialog box, click the **Device Control** tab.
 - 6 Double-click the **Session Monitor** icon.

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

Software Inventory

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



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

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



Chapter 11: Managing Mobile Device Profiles

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

- [Creating a Mobile Device Profile](#)
- [Configuring Device Wipe Folders](#)
- [Editing Custom Properties for Mobile Device Profiles](#)
- [Editing Registry Keys for a Mobile Device Profile](#)
- [Configuring Mobile Device Profile Advanced Settings](#)

NOTE: For information on exporting a profile to use for configuring an Enabler, see [Exporting Profiles for Configuring Enablers](#).

Creating a Mobile Device Profile

Use a mobile device profile to change settings on your mobile devices, as well as add, change, and remove custom properties and registry keys. Mobile device profiles allow you to configure the server that the devices should connect to, SMS notification, package sync, orphan package removal, and selection criteria. A mobile device profile has the following general options:

| | |
|--------------------------------------|---|
| Status | Enables or disables the profile. |
| Home | Sets the home location for the profile. |
| Notes | Any notes for the profile. |
| Server Address | Specifies the address of a specific mobile device server you want the devices to connect to. |
| Enable SMS Notification | Allows SMS messages to be sent to the device from the Avalanche Console. |
| Force Package Synchronization | Synchronizes each file of each package on the device without checking the meta-file, which provides information about the state of the files. When the option is not enabled, the server checks the meta-file, and then synchronizes only the files that have been altered or do not match. |



- Restrict simultaneous device updates** Limits the number of devices using the profile that are allowed to update simultaneously. This may be useful if there is a particular update that will take significant bandwidth or time. Restrict how many devices receive that update at a time so that other functions aren't affected.
- Orphan Package Removal** Removes packages that have been orphaned from the device. A package is considered orphaned if it has been deleted from the Avalanche Console, if the software profile it belongs to has been disabled, or if the package has been disabled. Orphaned packages must be listed by name. Orphaned packages must be listed by name. Orphan package removal will only happen once, when the profile is first applied.
- Selection Criteria** Determines which devices the profile is applied to. For information on selection criteria, see [Using Selection Criteria](#).
- Authorized Users** Allows you to assign administrative privileges for a profile to a user that has Normal user rights and is not assigned permissions to profiles. This allows you to give a user permission for one specific profile. Users that have permission for the profile will not appear in the list of available users. For information about creating users and assigning permissions, see [Managing User Accounts](#).

Other options on a mobile device profile such as custom properties, registry keys, device wipe folders, and advanced configurations are described in other sections. The home location for the profile is the location you have selected when you create the profile.

To create and configure a mobile device profile:

- 1 From the **Profiles** tab, click **Add Profile**.
The Add Profile Wizard appears.
- 2 Select the **Mobile Device Profile** option and click **Next**.
- 3 Type a **Name** for the profile and set the status to either **Enabled** or **Disabled**. Click **Next**.
- 4 Use the Selection Criteria Builder to create selection criteria for the profile. Click **Next**.
- 5 Confirm that the information is correct and click **Finish**.

The profile is created. Use the **Edit** button to configure the options for the profile.

Configuring Device Wipe Folders

Device wipe folders in a mobile device profile allow you to specify folders or directories on the device that contain sensitive information. When a device is wiped, all the information in the



folders is deleted.

To configure device wipe folders:

- 1 From the **Profiles** tab, select the mobile device profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Mobile Device Profile** tab, click **Add** in the Device Wipe Folders area.

The *Add Folder* dialog box appears.

- 4 Type the path to the folder on the device and click **OK**.

If the server is unable to contact the device using a TCP/IP connection, it will attempt to send the wipe command using SMS. When the device's Enabler receives the command, it will delete all files in the specified folders and force the device to reboot. If any of the selected files were in use, the Enabler will try again to delete them after the reboot.

For information on performing a device wipe after the mobile device profile has been deployed, see [Wiping a Mobile Device](#).

Editing Custom Properties for Mobile Device Profiles

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

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

NOTE: Deleting a property from a profile will not remove the property from the device.

To add a custom property:

- 1 From the **Profiles** tab, select the profile you want to configure.
- 2 Click **Edit**.
- 3 In the Device Properties area, select the group (such as General or Custom) to which you want to add the property. Click **Add**.

The *Add Property* dialog box appears.

- 4 Type the **Property Name** and **Property Value** in the text boxes.
- 5 Select **add** from the **Action** drop-down list.



- 6 Click **OK**.

The task is added to the list in the Properties area. The property will be added when the profile is applied on the mobile device.

- 7 Save your changes.

To edit or remove a custom property from the device:

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

- 2 Click **Edit**.

- 3 In the Device Properties area, select the group (such as General or Custom) to which you want to add the property. Click **Add**.

The *Add Property* dialog box appears.

- 4 Select the **Category** to which the property belongs.

- 5 Type the **Property Name** of the existing property in the text box.

- 6 If you want to edit the value of the property, type the new value in the **Value** text box.

- 7 If you are editing the value of the property, select **Add** from the **Action** drop-down list. If you want to remove the property from the device, select **Remove** from the **Action** drop-down list.

- 8 Click **OK**.

The task is added to the list in the Properties area. The property will be edited when the profile is applied on the mobile device.

- 9 Save your changes.

Editing Registry Keys for a Mobile Device Profile

You can add registry keys to a mobile device profile which will be added to the device registry when the profile is applied. Once you add a registry key to the profile, you can add values for the key. You also have the option to edit or remove existing registry keys or values on the device. You must know the name and location of the key or value in order to edit or remove it.

This section contains information on the following tasks:

- [Adding a Registry Key to a Mobile Device Profile](#)
- [Editing or Removing a Registry Key or Value](#)



Adding a Registry Key to a Mobile Device Profile

You can add registry keys and values to a profile. These keys will be added to the device registry when the profile is applied.

NOTE: Removing a registry key from the profile does not remove it from the device. For information on removing it from the device, see [Editing or Removing a Registry Key or Value](#).

To add a registry key:

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

The *Add Registry Key* dialog box appears.

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

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

To add a value to a registry key:

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

The *Add Registry Value* dialog box appears.

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



The task is added to the list in the Registry Settings area. The value will be added when the profile is applied on the mobile device.

Editing or Removing a Registry Key or Value

You can remove an existing registry key on a mobile device through a mobile device profile. Make changes to the key from the profile and apply the profile. If it is a mobile device profile, deploy the profile; if it is a Scan to Config profile, print and scan the barcodes. You must know the name of the key/value in order to remove it.

NOTE: In order to edit or remove a registry key value, you must add the registry key to the profile even if the key already exists on the device. For more information on adding a registry key, see [Adding a Registry Key to a Mobile Device Profile](#).

To remove a registry key:

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

The *Add Registry Key* dialog box appears.

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

The task is added to the list in the Registry Settings area. The key will be removed when the profile is applied on the mobile device.

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

To edit or remove a registry key value:

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

The *Add Registry Value* dialog box appears.

- 4 Type the **Name** of the existing value in the text box.



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

The task is added to the list in the Registry Settings area. The value will be changed when the profile is applied on the mobile device.

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

Configuring Mobile Device Profile Advanced Settings

You can configure GPS reporting, geofence areas, time zone settings and update restrictions for your mobile devices from a mobile device profile. This section includes the following topics:

- [Location Based Services](#)
- [Geofence Areas](#)
- [Regional Settings](#)
- [Update Restrictions](#)

Location Based Services

Location-based services allow you to manage GPS statistics collection when your mobile devices have GPS capabilities and a phone. Configure the following options:

| | |
|--|---|
| Enable location-based services | Enables GPS reporting for devices using the selected mobile device profile. |
| Reporting interval | Determines how often the device reports its GPS statistics to the Mobile Device Server. |
| Report location using cell towers | Uses information from nearby cell towers to establish the location of the device. |
| Report location using GPS | Uses GPS coordinates to establish the location of the device. |
| GPS acquisition timeout | Determines how often the device checks its GPS coordinates. |



| | |
|---|---|
| Prompt user to initiate timeout | Prompts the mobile device user to ask if Avalanche should be allowed to collect and report location-based data. This prompt will appear when the Enabler is launched. |
| Notify user after _ consecutive GPS failures | Provides a notification to the mobile device user after the device has failed to acquire GPS coordinates the specified number of times. |

To configure location-based services:

- 1 From the **Profiles** tab, select the mobile device profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Advanced Settings** tab, enable the desired options in the Location Based Services area.
- 4 Save your changes.

Geofence Areas

A geofence is a virtual perimeter defined by GPS coordinates. You can configure a geofence area for your mobile devices. When you configure a geofence area and define it as the Home area, Avalanche can generate an alert when devices report a GPS position that is outside of the defined area.

To configure a geofence area:

- 1 From the **Profiles** tab, select the mobile device profile from the Profile List.
- 2 Click **Edit**.
- 3 In the **Advanced Settings** tab, ensure that **Enable location-based services** is enabled.
- 4 Click **Add** in the Geofence Areas region.

The *Add Geofence Area* dialog box appears.

- 5 Type a name for the area in the **Name** text box.
- 6 If you want the area to be a home area, enable the **Is a Home Area** check box.
- 7 Enter the start and end latitude and longitude for the geofence. The start point should be the southwest corner of your area, and the end point should be the northeast.
- 8 Click **Select**.

The area is added to the list.



Regional Settings

You can set the region and time zone for your mobile devices from a mobile device profile.

To change the regional settings of a mobile device profile:

- 1 From the **Profiles** tab, select the profile from the Profile List.
- 2 Click **Edit**.
- 3 From the **Advanced Settings** tab, use the drop-down lists in the Regional Settings area to select the region and time zone for your devices.
- 4 If you want to edit the time zone settings that load automatically when you select the time zone from the drop-down list, click **Edit Time Zone**.
- 5 If you want to revert to the time zone settings used on the local computer, click **Refresh Time Zone**.
- 6 Enable the **Automatically adjust clock for Daylight Savings Time** option if you want the devices to switch over automatically.
- 7 Save your changes.

Update Restrictions

For more control over bandwidth usage, restrict device-to-server updates by using blackout windows. During a device-to-server blackout, the mobile devices are not allowed to communicate with a Mobile Device Server.

To create a blackout window:

- 1 From the **Profiles** tab, select a mobile device profile from the Profile List.
- 2 Click **Edit**.
- 3 From the **Advanced Settings** tab, click **Add** in the Update Restrictions area.

The *Add Exclusion Window* dialog box appears.

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

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

- 5 Click **OK**.



- 6 Save your changes.



Chapter 12: Managing Mobile Device Groups

To better organize your wireless network, you can use the Avalanche Console to create collections of mobile devices, called mobile device groups. These groups allow you to manage multiple devices simultaneously, using the tools available for managing individual mobile devices. A mobile device group can include devices assigned to the group's home location or associated sub-locations. Each mobile device can be a member of multiple mobile device groups.

A mobile device group will be available at its home location and inherited by any sub-locations. When a mobile device group is created, the home location is set by default to the location you currently have selected.

You can add authorized users for all mobile device groups or enable a user for a specific mobile device group. For information on adding an authorized user, see [Assigning Authorized Users to Mobile Device Groups](#).

The topics in this section include:

- [Creating Mobile Device Groups](#)
- [Viewing Devices in a Mobile Device Group](#)
- [Pinging Mobile Devices within Mobile Device Groups](#)
- [Sending Messages to Mobile Device Groups](#)
- [Editing Properties for Mobile Device Groups](#)
- [Additional Mobile Device Group Functions](#)

Creating Mobile Device Groups

Mobile device groups allow you to group devices together based on selection criteria you configure. You can create dynamic or static groups. In both group types, new devices can be added to the group based on changes to the selection criteria. However, in a static group, devices cannot be deleted from the group unless they are deleted on an individual basis.

- **Dynamic Mobile Device Groups.** When you create a dynamic group, you configure selection criteria to define which devices you want to belong to the group. The devices currently in the Mobile Device Inventory that match the selection criteria are added to the group.

If a new device that matches the selection criteria for a dynamic mobile device group connects to the Avalanche Console, it is automatically placed in the mobile device group.



Therefore, dynamic mobile device groups will continually add and remove mobile devices based on the selection criteria, without further management.

- **Static Mobile Device Groups.** When you create a static group, you configure selection criteria to define which devices you want to belong to the group. The devices currently in the Mobile Device Inventory that match the selection criteria are added to the group. If you add mobile devices to your network, you can add those devices to a static mobile device group as long as they meet the group's selection criteria.

If a new device matching the selection criteria for a static mobile device group connects to the Avalanche Console, it will not automatically be placed in the mobile device group. You will need to manually add or delete devices if you want to modify the group. To modify 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.

The home location for the group is the location you have selected when you create the group.

To create a mobile device group:

- 1 Select the **Device Groups** tab.
- 2 Click **Add Group**.

The *Create Device Group* dialog box appears.

- 3 Type a **Name** for the group.
- 4 Select whether you want the group to be **Static** or **Dynamic**.
- 5 Select whether you want the group to be **Enabled** or **Disabled**.
- 6 Use the Selection Criteria Builder to create criteria to define the device group.
- 7 Click **OK**.

The group appears in the Device Groups List.

To add mobile devices to a static mobile device group:

- 1 Select the **Device Groups** tab.
- 2 Select the static mobile device group from the Device Groups List.
- 3 Click **Edit**.
- 4 In the Device Group Properties area, click **Add Matching Devices**.

Any devices in the current Mobile Device Inventory that match the selection criteria are added to the group.



- 5 Save your changes.

Viewing Devices in a Mobile Device Group

The **Device Group** tab shows a set of mobile devices in the currently selected mobile device group. The following default information is provided for each mobile device:

Model The model name of the mobile device.

Name

Terminal ID The unique ID automatically generated by Avalanche or assigned by a Console user.

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

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

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

Last Contact The date and time of the last contact the mobile device had with Avalanche.

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

You can also customize the columns in the device list or filter the devices displayed. For information on customizing the device list, see [Managing Device Inventory Displays](#).

Pinging Mobile Devices within Mobile Device Groups

You can use mobile device groups to ping a collection of mobile devices simultaneously. You can ping mobile devices that are currently in range and running the Avalanche Enabler, an Avalanche-enabled application, or in some cases a configuration utility.

NOTE: This is not an ICMP-level ping, but rather an application-level status check. This feature indicates whether the mobile device is active or not.

To ping mobile devices within device groups:

- 1 Select the **Device Groups** tab.



- 2 Right-click the mobile device group you want to ping and select **Ping Devices** from the context menu.

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

Sending Messages to Mobile Device Groups

You can send messages to the users of all mobile devices in a device group simultaneously.

To send messages to device groups:

- 1 Select the **Device Groups** tab.
- 2 Right-click the mobile device group you want to send a message to and select **Send Text Message** from the context menu.

The *Send Text Message: Group of Devices* dialog box appears.

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

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

Editing Properties for Mobile Device Groups

You can modify mobile device properties from a mobile device group. When you edit device properties for a group, the Console retrieves the common properties from all the devices in the group. You can then add, edit, and delete properties for the group. All property changes made at this level will be applied on the mobile devices in the group.

NOTE: See [Building Selection Criteria](#) for information on using properties in selection criteria.

To add a property to a mobile device group:

- 1 Select the **Device Groups** tab.
- 2 Right-click the mobile device group whose properties you want to edit and select **Edit Device Properties** from the context menu.

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

- 3 Click **Add Property**.



The *Add Device Property* dialog box appears.

- 4 From the **Category** drop-down list, select the category where you want the property to be saved.
- 5 Enter the name of the property in the **Property Name** text box.
- 6 Enter the value of the property in the **Property Value** text box.
- 7 Click **OK**.

The new property is added to the properties list.

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

To edit a mobile device group property:

- 1 Select the **Device Groups** tab.
- 2 Right-click the mobile device group whose properties you want to edit and select **Edit Device Properties** from the context menu.

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

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

The *Edit Device Property* dialog box appears.

- 4 Type the **New Property Value**.
- 5 Click **OK**.

The edited property appears in the list.

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

To delete a mobile device group property:

- 1 Right-click on a mobile device group and select **Edit Device Properties**.

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

- 2 Select the property that you want to delete and click **Delete Property**.
- 3 Confirm that you want to delete the property.

The Pending Value column for the property displays the status of the property.

- 4 Click **OK** to remove the property and return to the Avalanche Console.

The property will be deleted after the next update.



Additional Mobile Device Group Functions

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

The additional options for mobile device groups are as follows:

Enable/Disable Allows you to enable or disable the group. When the group is disabled, any selection criteria using the group as a selection variable will return a “false” value.

Update Now Allows you to update all mobile devices within that group immediately.

Clone Group Clones the group and its settings.

Remove Group Deletes the group from the Avalanche Console.



Chapter 13: Managing Alert Profiles

You can manage alerts in Avalanche using alert profiles. An alert profile gives you options for configuring what network events generate an alert and who is notified when an alert is generated. A server going offline or a new mobile device being discovered are examples of alert events.

This section provides information about the following topics:

- [Creating and Configuring Alert Profiles](#)
- [Alerts Tab](#)

Creating and Configuring Alert Profiles

Alert profiles are configured with a list of events that will generate an alert. These profiles are then deployed to the locations. When an event on the list occurs, an alert is generated and sent to the Avalanche Console. If the profile is configured for forwarding the alert to e-mail recipients or a proxy, the Console forwards the alert. The home location for the profile is the location you have selected when you create the profile.

The **Authorized Users** button allows you to assign administrative privileges for a profile to a user that has Normal user rights and is not assigned permissions to profiles. This allows you to give a user permission for one specific profile. Users that have permission for the profile will not appear in the list of available users. For information about creating users and assigning permissions, see [Managing User Accounts](#).

The settings that can be configured for an alert profile include:

Profiled Contacts Each alert profile can notify one or more e-mail addresses when specified events occur. If you want the Avalanche Console to send notification by e-mail, you must add the e-mail address to the Email Recipients list for that profile. The entire contact list will receive e-mails for all alerts generated by that profile.

Profiled Proxies The Avalanche Console allows you to set one or more proxy hosts for an alert profile. When you add a proxy to a profile, the Console automatically forwards all alerts for that profile to the IP address of the proxy, enabling you to integrate Avalanche with your existing network management tools.

Profiled Alerts Avalanche provides a list of events that will generate alerts. You can choose events from this list when you create an alert profile.

See the following sections for additional information on configuring e-mail addresses and SNMP proxies for alert profiles:

- [Adding E-Mail Contacts](#)



- [Adding SNMP Proxies](#)

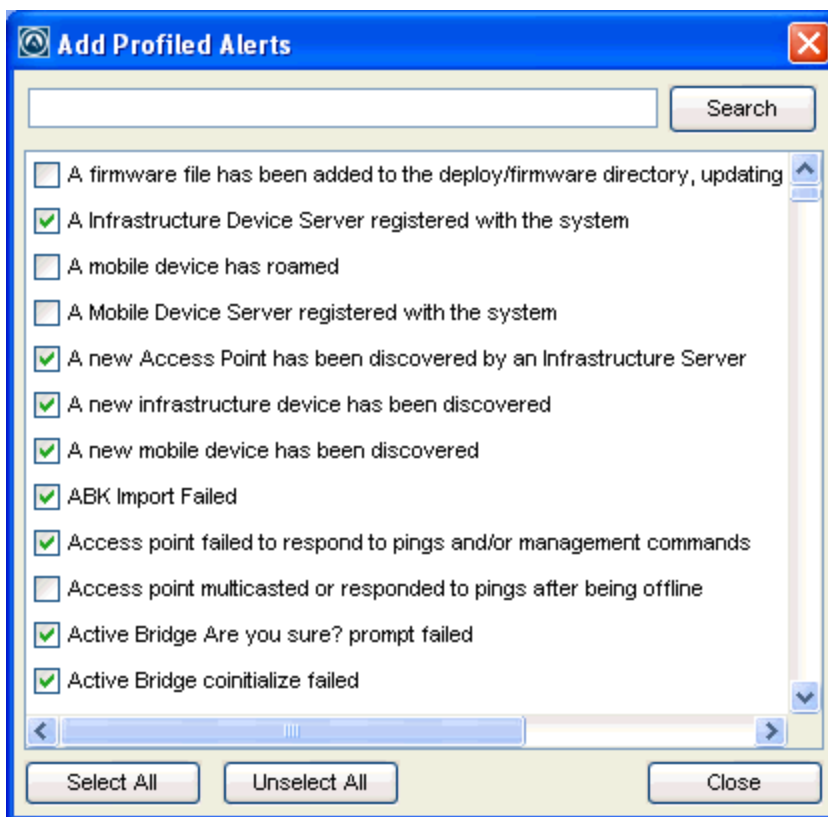
To create an alert profile:

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

The Add Profile Wizard appears.

- 2 Select the **Alert Profile** option and click **Next**.
- 3 Type a **Name** for the profile and set the status to either **Enabled** or **Disabled**. Click **Next**.
- 4 Click **Add** to specify the alerts the profile will monitor.

The *Add Profile Alerts* dialog box appears.



Add Profile Alerts dialog box

- 5 From the list, select the events for which you want an alert to be generated. When you are finished, click **Close**.
- 6 The selected alerts appear in the list. click **Next**.
- 7 Confirm that the information is correct and click **Finish**.

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



To configure an alert profile:

- 1 From the **Profiles** tab, select the alert profile you want to configure.
- 2 Click **Edit**.
- 3 Select **Enabled** to enable the profile, if desired.
- 4 In the **Alert Profile** tab, click **Add** in the Profiled Alerts area. From the list, select the events for which you want an alert to be generated. When you are finished, click **Close**.
- 5 If you want to forward alerts to an e-mail address or a proxy address:

- If you want to receive an e-mail when an alert is generated, click **Add** in the Profiled Contacts area.

The *Contact Information* dialog box appears.

Enter the contact information and click **OK**. The contact will appear in the Profiled Contacts list.

NOTE: You must configure the e-mail settings in the *Preferences* dialog box before Avalanche can e-mail you when alerts are generated. For information on configuring e-mail settings, see [Configuring E-mail Settings](#).

- If you want to forward alerts to a SNMP proxy, click **Add** in the Profiled Proxies area.

The *Proxy Address* dialog box appears.

Enter the proxy address and click **OK**. The address will appear in the Profiled Proxies list.

- 6 Save your changes.

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

Adding E-Mail Contacts

Each alert profile can notify one or more e-mail addresses when related events occur. If you want the Avalanche Console to notify you of an alert by e-mail, add the e-mail address to the Profiled Contacts list for that profile. The entire contact list will receive e-mails for all alerts generated by that profile.

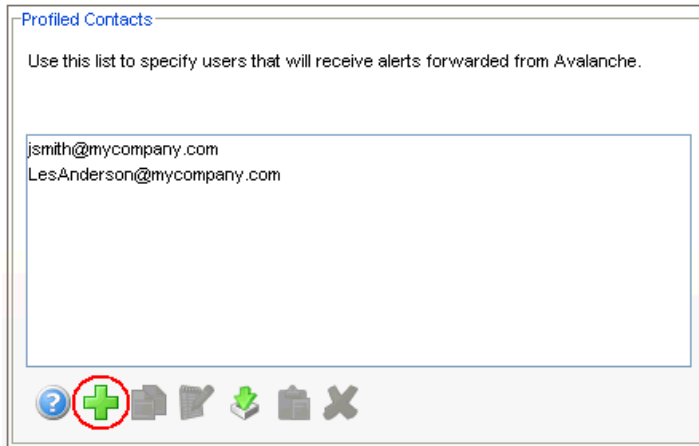
NOTE: You must configure the e-mail settings before Avalanche will send e-mails when alerts are generated. For information on configuring e-mail settings, see [Configuring E-mail Settings](#).



A list of e-mail addresses in a comma-delimited `.csv` file (for example, one exported from Microsoft Outlook) can be imported in order to add multiple e-mail addresses at a time.

To add e-mail contacts:

- 1 On the **Profiles** tab, select the profile you want to configure from the Profile List.
- 2 Click **Edit**.
- 3 In the **Profiled Contacts** tab, click **Add**.



Add button in the Profiled Contacts area

The *Contact Information* dialog box appears.

- 4 Type the desired information in the provided text boxes. An e-mail address is required. When you are done, click **OK**.

The contact is displayed in the **Profiled Contacts** list box.

- 5 Repeat Step 4 until you are finished adding e-mail addresses.
- 6 Save your changes.

To import e-mail addresses:

- 1 On the **Profiles** tab, select the profile you want to configure from the Profile List.
- 2 Click **Edit**.
- 3 In the Profiled Contacts region, click **Import Contacts**.

An *Open* dialog box appears.

- 4 Navigate to and select the `.csv` file that contains the e-mail addresses that you want to import.
- 5 Click **Open**.

The e-mail addresses contained in the text file appear in the **Available Contacts** list.



- 6 Click **OK**.

The contacts display in the **Profiled Contacts** list.

Adding SNMP Proxies

The Avalanche Console allows you to set one or more SNMP proxies for an alert profile. When you add a proxy to a profile, the Console automatically forwards all alerts for that profile to the IP address of the proxy, enabling you to integrate Avalanche with your existing network management tools.

To add an SNMP proxy:

- 1 On the **Profiles** tab, select the profile you want to configure from the Profile List.
- 2 Click **Edit**.
- 3 In the Profiled Proxies region, click **Add**.

The *Proxy Address* dialog box appears.

- 4 In the **Proxy Address** text box, enter the IP address and click **OK**.

The address appears in the **Profiled Proxies** list box.

- 5 Repeat Steps 3 and 4 until you are finished adding proxy addresses.
- 6 Save your changes.

Alerts Tab

The **Alerts** tab provides a real-time view of the health of your wireless network. You can tell at a glance which locations are operating normally and which require attention. The tab consists of two areas: the Map and the Alert Browser. This section contains information on the following tasks:

- [Using the Alert Browser](#)
- [Using the Avalanche Map](#)

Using the Alert Browser

In the **Alerts** tab, the area at the bottom of the screen is called the Alert Browser. The browser is a table overview of the alerts that occur on your wireless network. It provides the following information about each alert:



| | |
|--------------------|--|
| Ack | Allows you to acknowledge that you have seen the alert. When you acknowledge an alert, the Server Location that sent the alert stops flashing in the Map pane. |
| Alert | Displays the type of alert. |
| Date | The time and date when the event occurred. |
| IP | Displays the IP address where the event occurred. |
| Description | Provides a brief description of the event. |

When a new alert appears in the Alert Browser, the server location at which the alert was generated begins flashing in the map. To stop the flashing, acknowledge the alert. When the Alert Browser begins to fill with alerts, you may want to remove acknowledged alerts that are no longer relevant.

In the *Settings* 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 acknowledge an alert:

- In the Alert Browser, enable the checkbox next to the alert you want to acknowledge. To immediately show the result, click **Refresh**.

-Or-

- To acknowledge all alerts in the list, click **Acknowledge All**.

The locations in the Map view stop flashing.

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.

To customize the Alert Browser functions:

- 1 Click **Tools > Settings**.



The *Settings* dialog box appears.

- 2 On the **General** tab in the Alert Browser Settings area, use the boxes to configure the alert settings.
- 3 Click **Apply** to save your changes.
- 4 Click **OK** to close the dialog box.

The Alert Browser will update to reflect your changes.

Using the Avalanche Map

The map provides a geographical overview of the health of your network. Use the following methods to navigate the map:

- Use the navigation arrows to display different portions of the map.
- Center the map on its default location by using the center button of the navigation arrows.
- Zoom in on a portion of the map using the [+] magnifying glass icon.
- Zoom out on a portion of the map using the [-] magnifying glass icon.
- Apply filters so that only specific wireless components appear within the map. These filters are activated by the check boxes located next to the navigation arrows. You can apply the following filters:

Combined Servers Displays server locations that contain both a Mobile Device Server and an Infrastructure Server.

Mobile Device Servers Displays server locations that contain only a Mobile Device Server.

Infrastructure Servers Displays server locations that contain only an Infrastructure Server.

View Map By Region Displays only those server locations that belong to the area selected in the Navigation Window.

Mobile Devices Displays the mobile devices associated with the region selected.

Mobile Device GPS History Displays mobile devices by the GPS history.

- Color-code map components. This helps identify components and provide notifications of network health. The color codes for the components that appear in the map are as follows:



| | |
|-------------------|---|
| Purple | Indicates a server location with both a Mobile Device Server and an Infrastructure Server. |
| Blue | Indicates a server location with only a Mobile Device Server. |
| Dark Green | Indicates a server location with only an Infrastructure Server. |
| Yellow | Indicates a server location with one or more warning-level alerts (but no critical alerts). |
| Red | Indicates a server location with one or more critical alerts. |

When a server location generates a warning or critical alert, the icon in the Map flashes yellow or red, based on the highest severity level in its alert list. The flashing stops when you acknowledge the alert in the Alert Browser. The icon returns to its base color when all warnings and critical alerts for the server location have been cleared from the Alert Browser.

You can also save specific map views to simplify navigation.

To save a map view:

- 1 Position the map using the navigation arrows and zooming in on the relevant geographic area.
- 2 Click **Save View**.
- 3 Type the name of the view in the dialog box that appears.
- 4 Click **OK**.

The view can be accessed by selecting it from the **Go to View** drop-down list. The view will only be available to users on the local machine.



Chapter 14: Using Selection Criteria

Selection criteria are sets of rules which you can apply to profiles or devices. These criteria define which mobile devices receive the profile or are added to a group.

Additional selection criteria are typically built into software packages to restrict the distribution of the package to devices that can use it. The built-in selection criteria associated with a particular software package are set by Wavelink or the third-party application developer and, once created, cannot be modified.

A selection criterion 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. For example, set a profile so that it is only applied to Hand Held 7400 devices by using the criterion:

```
ModelName = HHP7400
```

After the profile is enabled and applied to a location, it is distributed to devices in the location that meet the selection criterion.

If you want to set criteria but only want to match part of the expression, use an asterisk (*) as a wildcard to represent single or multiple characters. You can also use parentheses and boolean operators for flexible combination of multiple variables.

NOTE: The database interfaces used by Avalanche put a length limit on SQL expressions which can be exceeded when selection criteria get too complex. Selection criteria containing more than 150 expressions have a good chance of exceeding database-imposed limits. 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.

To reduce the size and complexity of selection criteria, the user should make use of the range and wildcard capabilities.

The selection criteria builder provides a list of operators and preset selection variables, and also allows you to add custom properties as selection variables. Use the selection criteria builder to build valid selection criteria.

This section provides the following information:

- [Building Selection Criteria](#)
- [Selection Variables](#)
- [Operators](#)
- [Adding Properties to the Selection Variables](#)



Building Selection Criteria

You can access the Selection Criteria Builder from several different places in the Avalanche Console, including network profiles, software profiles, and mobile device groups. To access the Selection Criteria Builder, click the Selection Criteria button:



Selection Criteria button

NOTE: Selection criteria are also used for software packages; however, you cannot edit software package selection criteria in Avalanche.

In the Selection Criteria Builder, you can build the selection criteria string by selecting or typing string elements one element at a time. The string elements include:

- Selection variables such as **ModelName** or **KeyboardName**. These variables determine the type of restriction placed on the package or profile. For example, by using a **ModelName** variable, you can restrict the package or profile to a specific class of mobile devices, based on their model numbers. You may use any property that you have assigned a device as a selection criterion variable.
- Operators such as AND (&), and OR (|) that are used to assign a value to a selection variable or to combine multiple variables.

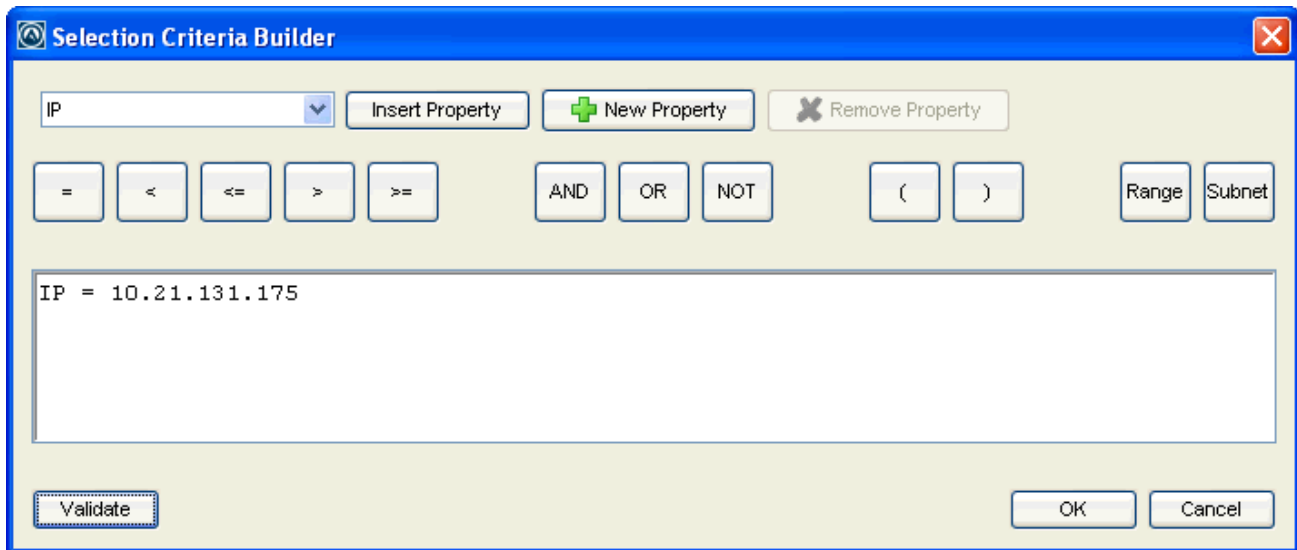
NOTE: Parentheses are recommended when multiple operators are involved. Nesting of parentheses is allowed.

- Actual values that are assigned to a selection variable. For example, if you assign a value of 6840 to a **ModelName** variable by building the string `ModelName = 6840`, then you will restrict packages or profiles to model 6840 mobile devices.

To build selection criteria:

- 1 Access the Selection Criteria Builder.





Selection Criteria Builder

- 2 From the drop-down list, select a property and click **Insert Property**. For information about properties, see [Selection Variables](#).
- 3 Select one of the operator buttons. For more information about operators, see [Operators](#).
- 4 Type a value for the 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.

Selection Variables

Selection criteria are based on the use of selection variables. Some selection variables are preset, or you can create your own

You can place numbers and strings directly in the selection criteria string with or without quotes. Selection criteria strings are case sensitive.

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



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

The following string is valid:

```
Series = S
```

While these are not:

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

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

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

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.

The Selection Criteria Builder in Avalanche has some selection variables already created. You can also add custom device properties as selection variables. The following table lists the preset selection variables:

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

Example:

```
Columns > 20
```

EnablerVer Predefined Enabler version number.

Values with decimals must be surrounded by double quote marks.

```
EnablerVer = "3.10-13"
```



IP IP address of the mobile device(s).

Enter all IP addresses using dot notation. IP addresses can be written in three ways:

- Direct comparison with a single IP address. For example, `IP = 10.1.1.1`.
- Comparison with an arbitrary address range. For example, `IP = 10.1.1.5 - 10.1.1.15` (This can also be written as `IP = 10.1.1.5 - 15`.)
- Comparison with a subnet. This is done by supplying the network number along with the subnet mask or CIDR value. For example, `IP = 10.1.1.0/255.255.255.0`. Using CIDR notation, this can also be written as `IP = 10.1.1.0/24`.

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

Supported values include:

0 = 35-Key

1 = More than 35 keys and WSS1000

2 = Other devices with less than 35 keys

Example:

`KeyboardCode = 0`



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

Supported values include:

35KEY

46KEY

101KEY

TnKeys

Example:

KeyboardName = 35KEY



Last Contact The parser for the LastContact property is unique because it not only allows specifying absolute time stamps, but also relative ones, forcing their constant reevaluation as the time-base changes.

Examples of time-stamp formats:

- mm/dd/yyyy

LastContact = "12/22/2005" (All day)

- HH:MM mm/dd/yyyy

LastContact = "23:15 12/22/2005" (All minute long, 24 hour notation)

- hh:mm AP mm/dd/yyyy

LastContact = "11:15 PM 12/22/2005"

- Also range-forms of the above

The relative format uses an offset from the current time.

- <offset>M

LastContact = 60M (60 minutes in the past)

- <offset>H

Last Contact = 1H (one hour in the past, the whole hour)

- <offset>D

Last Contact = 1D (one day in the past, the whole day)

- Also range-forms of the above

Special syntax allows inverted ranges from the range form to reduce the amount of confusion.

LastContact=7D-1M

MAC MAC address of the mobile device.

Enter any MAC addresses as a string of hexadecimal digits. Dashes or colons between octets are optional. For example:

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



ModelName The standard model name for a mobile device. This name is often a number but it can be alphanumeric. Examples include 6840, 3940, and 4040. If the model number is unknown, it might appear in one of the views when the mobile device is selected.

A few of the supported values include:

```
1040, 1740, 1746, 1840, 1846, 2740, 2840, 3140, 3143,  
3540, 3840, 3843, 3940, 4040, 5040, 6140, 6143, 6840,  
6843, 6940, 7240, 7540, 7940, 8140, 8940, PTC960,  
TR1200, VT2400, WinPC, WT2200, 7000CE, HHP7400, MX1,  
MX2, MX3, VX1, iPAQ, iPAD, Falcon, ITCK30, ITC700
```

Example:

```
ModelName = 6840
```

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

Supported values include:

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

Example:

```
ModelCode <= 2
```

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

OSVer Predefined property designated by the Enabler. Values with decimals in them must be surrounded by double quote marks.

```
OSVer = "4.20"
```

OS Type Predefined property designated by the Enabler.

```
OSType = PocketPC
```

Processor Predefined property designated by the Enabler.

```
Processor = ARM
```



ProcessorType Predefined property designated by the Enabler.

```
ProcessorType = xScale
```

Assigned IP IP address of the mobile device.

Enter all IP addresses using dot notation. IP addresses can be written in three ways:

- Direct comparison with a single IP address. For example, `IP = 10.1.1.1`.
- Comparison with an arbitrary address range. For example, `IP = 10.1.1.5 - 10.1.1.15` (This can also be written as `IP = 10.1.1.5 - 15`.)
- Comparison with a subnet. This is done by supplying the network number along with the subnet mask or CIDR value. For example, `IP = 10.1.1.0/255.255.255.0`
Using CIDR notation, this can also be written as `IP = 10.1.1.0/24`

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

Supported values include:

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

Example:

```
Series = 3
```



- Rows** 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 and 35-key keyboards.
- Syncmedium** The type of synchronization medium for the mobile device to use.
- Supported values include:
- ```
anyipserial
```
- Terminal ID** The unique ID for the mobile device generated by Avalanche or assigned by a user. The initial terminal ID is 1, and the values increment as needed. 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.
- Example:
- ```
Terminal ID = 5
```
- @exists** Enables the user to check for the existence of a property. The `@exists` function name is case-sensitive and can only be used with an EQ or NE operator.
- Example:
- ```
@exists ne some.property
```
- ```
@exists ==Some.property & Some.property = "value"
```

## Operators

All selection criteria strings are evaluated from left to right, and precedence of operations is used when calculating the selection criteria. When more than one operator is involved, you must include parentheses in order for the selection criteria string to be evaluated properly.

For example:

```
(ModelName=3840) or ((ModelName=6840) and (KeyboardName= 46Key))
```



The preceding selection criteria string states that both 3840 mobile devices (regardless of keyboard type) and 6840 mobile devices with a 46-key keyboard will receive the software profile.

You may use the symbol of the operator (!, &, |, etc.) in a selection criterion, or you may use the letter abbreviation (NOT, AND, OR, etc.). If you use the letter abbreviation for the operator, then you must use uppercase letters. Spaces around operators are optional, and you can use the wildcard character [\*] for left wildcard constants and right wildcard constants.

Operators use the following precedence:

- 1 Parentheses
- 2 OR operator
- 3 AND operator
- 4 NOT operator
- 5 All other operators

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

**NOT** Binary operator that negates the boolean value that follows it.

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

All mobile devices receive the software package except for those with both 20 rows and 35Key keyboards.

**AND** Binary operator that results in TRUE if and only if the expressions before and after it are also both TRUE.

(&)

Example:

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

**OR** Binary operator that results in TRUE if either of the expressions before and after it are also TRUE.

(|)

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

6840 and 3840 mobile devices can receive the software package.



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

Example:

```
ModelName = 6840
```

**NE** Not equal to.

(!=)

Example:

```
ModelName != 6840
```

Targets all non-6840 mobile devices.

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

Example:

```
Rows > 20
```

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

Example:

```
Rows < 21
```

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

Example:

```
Rows >= 21
```

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

Example:

```
Rows <= 20
```



(\*) Wildcard operator.

Wildcard expressions should be quoted and must be used with either an EQ or NE operator.

Keyboardname = "35\*" - Tail is the wildcard

Keyboardname = "\*35" - Head is the wildcard

Keyboardname = "\*" - Entire constant is the wildcard

You can also use wildcards for IP addresses.

IP = 10.20.\*.\*

This would be equivalent to 10.20.0.0-10.20.255.255. A wildcard address must contain all four octets and can only be used with either the EQ or the NE operator.

## Adding Properties to the Selection Variables

Using profiles, you can add custom properties to your devices. These custom properties or properties already existing on the device can be used for selection criteria. In order to use a property as a selection variable, add the property to the Selection Criteria Builder.

---

**NOTE:** Asterisks are not allowed in property names or values because the symbol denotes a wildcard.

---

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.



## Chapter 15: Using the Task Scheduler

The Task Scheduler enables you to schedule network management activities for your locations.

When you configure an aspect of your wireless network using the Avalanche Console, those configurations are not immediately sent to the rest of your network. Instead, you can schedule specific times for the new configurations to be sent. The Task Scheduler provides several advantages, including the ability to specify which locations receive the changes and the ability to implement changes during periods of low network activity.

Scheduling options for the Task Scheduler include:

**Perform the task now** Runs the task immediately.

**Schedule a one-time event for the task** Performs the task once at the scheduled time. This selection allows you to configure the following options:

**Task Start Time.** The date and time of day the event will begin.

**Run until complete.** When this option is selected, the task will run until it is complete.

**Use End Time.** The time of day when the task will end.

**Use Location's Local Time.** Uses the time local to the specified server(s) rather than the local time of the enterprise server.

**Schedule a recurring event for the task** Performs the task repeatedly at the scheduled times. This selection allows you to configure the following options:

**Task Start Time.** The time of day the event will begin.

**Use end time.** The time of day the event will end.

**Use Location's Local Time.** Uses the time local to the specified server(s) rather than the local time of the enterprise server.

**Daily.** The task is performed daily. When Daily is selected, you can also configure the following options:



**Every weekday.** Runs the scheduled task every day Monday - Friday.

**Every weekend.** Runs the scheduled task every Saturday and Sunday.

**Weekly.** The task is performed on a weekly basis. When **Weekly** is selected, you can also configure the following options:

**Run every \_\_ week(s) on.** This option allows you to configure whether the task is run weekly or at a longer interval. For example, if you want the task to run every other Saturday, type 2 in the text box and enable the **SAT** checkbox.

**[days of the week].** These check boxes allow you to specify which days of the week the task is performed.

**Monthly.** The task is performed on a monthly basis. When **Monthly** is selected, you can also configure the following option:

**Run on the \_\_ day, every \_\_ month(s).** This option allows you to set the day of the month to run the task, and how many months apart the task should be run.

**Start date.** Specifies the date the task should begin running.

**No end date.** When this option is selected, the task will continue repeating indefinitely.

**End by.** When this option is selected, the task will no longer run after the specified date.

The Task Scheduler allows you to perform the following tasks:

- [Applying and Deploying Profiles](#)
- [Backing Up the System](#)
- [Restoring the System](#)
- [Removing Completed Tasks](#)

## Applying and Deploying Profiles

A profile must be applied and deployed in order for the settings to take effect. When you use the Task Scheduler to apply and deploy profiles, select a time for the profile to be deployed.

To deploy a profile:

- 1 Click **Tools > Task Schedule**.

The *Task Schedule* dialog box appears.



- 2 Click **Add**.

The *Scheduled Task Wizard* dialog box appears.

- 3 Select **Apply / Deploy Profiles** from the **Task Type** drop-down list and click **Next**.

The *Select the Targets* screen appears.

- 4 Select the locations to which the profile will be applied by enabling the check box next to the location name. You can also select the locations where the profile will be deployed at the time the task is performed. Click **Next**.

---

**NOTE:** If the scheduled task applies the profile but does not deploy it, the profile will be deployed during the next universal deployment.

---

The *Schedule the Time Window* dialog box appears.

- 5 Determine when the event will occur and click **Next**.

The *Review Your Task* dialog box appears.

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

The *Task Scheduled* dialog box appears.

- 7 Click **Next** to schedule a new event, or click **Finish**.

## Backing Up the System

This section provides information about using the Task Scheduler to back up the Avalanche system. Backup and restore functionality is available when you are using PostgreSQL databases installed at the same location as the Enterprise Server. When you back up Avalanche, the enterprise database information and software packages are saved in a zip file.

You should back up the system regularly. If for any reason Avalanche files are deleted or corrupted, you will be able to restore them from the backup files. For information on the default backup directory or changing where backups are stored, see [Specifying the Backup Location](#).

---

**NOTE:** If you are attempting to back up your system on a Linux operating system, Wavelink recommends you perform the back up manually.

---

To back up the system:

- 1 Click **Tools > Task Schedule**.

The *Task Schedule* dialog box appears.

- 2 Click **Add**.





The *Scheduled Task Wizard* appears.

- 3 Select **System Backup** from the **Task Type** drop-down list and click **Next**.

The Create A System Backup screen 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 screen appears.

- 5 Determine when the event will occur and click **Next**.

The Review Your Task screen appears.

- 6 Review your task to ensure that it is correct and click **Next**.

The Task Scheduled screen appears.

- 7 Click **Next** to schedule a new event, or click **Finish**.

The task is added to the **Scheduled and Recurring Tasks** list.

## Restoring the System

If you have created a system backup using the Task Scheduler, you can use the Task Scheduler to restore the information to Avalanche.

You cannot restore a system backup from a previous version of Avalanche. The backup version must match the Avalanche version. If you attempt to restore a system backup from a previous version of Avalanche, the restoration will fail.

---

**NOTE:** If you are attempting to restore the system on a Linux operating system, Wavelink recommends you perform the restoration manually.

---

To restore the system:

- 1 Click **Tools > Task Schedule**.

The *Task Schedule* dialog box appears.

- 2 Click **Add**.

The *Scheduled Task Wizard* appears.

- 3 Select **Restore System** from the **Task Type** drop-down list and click **Next**.

The Restore A System Backup screen appears.



- 4 Select the system backup you wish to restore and click **Next**.
  - Select **Restore the most recent system backup** to restore Avalanche to the latest backup file.
  - Select **Restore by path** to specify the file name and path of the desired system backup.
  - Select **Restore selected** to choose the desired system backup from the list according to the tag name.

The Review Your Task screen appears.

- 5 Review your task to ensure that it is correct and click **Next**.

The Task Scheduled screen appears.

- 6 Click **Next** to schedule a new event, or click **Finish**.

The task is added to the **Scheduled and Recurring Tasks** list.

- 7 Restart the enterprise server, statistics server, and Tomcat service after the files are restored. If Avalanche is installed on a Windows OS, this is done from the Windows Services list. For the specific names of the services, see [Avalanche Services](#).

## Removing Completed Tasks

When the Task Scheduler has completed an event, that event appears in the **Completed Tasks** list. By default the Task Scheduler is set to retain all completed tasks in the list. You can configure Avalanche to remove tasks periodically.

[To schedule task removal:](#)

- 1 Click **Tools > Task Schedule**.

The *Task Schedule* dialog box appears.

- 2 Enable the **Remove Completed Events After** option and then select the number of days you want to pass before the completed tasks are removed.
- 3 Click **Refresh** to update the scheduler.

The completed tasks will be removed according to your settings.



## SSL Certificates for the Web Console

When you use the Avalanche Web Console, by default it connects to the server using Hypertext Transfer Protocol (http), which is not encrypted. If you want your information to be encrypted, you can configure Avalanche to use https with an SSL certificate instead.

If you intend to use Avalanche with an SSL certificate for a secure connection, you have the options of purchasing a certificate through a third-party Certificate Authority (such as Verisign) or creating a self-signed certificate.

---

**NOTE:** If you create a self-signed certificate, web browsers will not initially recognize the certificate and will display warning messages that the site is not trusted. They may require you to make an exception in order to connect. The connection will be encrypted, however.

---

This section contains instructions for the following tasks:

- [Implementing a Certificate from a Certificate Authority](#)
- [Implementing a Self-Signed Certificate](#)

### Implementing a Certificate from a Certificate Authority

You can choose to use Avalanche with a certificate from a Certificate Authority. Note that the following instructions are based upon acquiring a certificate through the certificate authority Verisign. The steps may vary somewhat when using another certificate authority vendor.

Wavelink strongly recommends that you backup the keystore file, the actual certificate file, the intermediate certificate, the certificate request, and the server.xml document after you have implemented your certificate. This would include the following files:

- amckeystore.keystore
- [your certificate].cer
- intermediateCA.cer
- certreq.csr
- server.xml

This section contains the following tasks for obtaining an SSL certificate from a certificate authority:

- [Creating a Keystore](#)
- [Generating the Certificate Signing Request](#)
- [Importing an Intermediate Certificate](#)



- [Importing a Certificate](#)
- [Activating SSL for Tomcat](#)
- [Accessing the Web Console over a Secure Connection](#)
- [Troubleshooting](#)

## Creating a Keystore

To create a keystore for the certificate, use the `keytool.exe` utility. You will need to provide a Common Name (domain name), organizational unit, organization, city, state, and country code. You will also need to provide a keystore name and passwords for the keystore and alias. These are arbitrary, but should be noted for future reference.

To generate a keystore for the certificate:

- 1 From a command line, navigate to:  
`[Avalanche installation directory]\JRE\Bin`
- 2 Use the command:  
`keytool -genkey -alias amccert -keyalg RSA -keystore amckeystore.keystore`
- 3 At the prompt **Enter keystore password**, type the keystore password. When prompted, re-enter the password.
- 4 At the prompt **What is your first and last name**, type the Common Name.

---

**NOTE:** The Common Name (domain name) you enter should be one that your company owns. Add a DNS entry if needed to resolve this computer to the Common Name.

---

- 5 At the prompts, enter your organizational unit, organization, city, state, and the country code.
- 6 When you are prompted to review your information, type `yes` to confirm that it is correct. If you type `no`, you will be guided through the prompts again.
- 7 At the prompt **Enter key password for <amccert>**, type a password to use for the alias. If you want to use the same password for the alias as you used for the keystore, press Return.

An example of generating a keystore:

```
Enter keystore password: avalanche
```

```
Re-enter new password: avalanche
```

```
What is your first and last name?[Unknown]: avaself.wavelink.com
```

```
What is the name of your organizational unit?[Unknown]: Engineering
```



```
What is the name of your organization?[Unknown]: Wavelink Corporation
What is the name of your City or Locality?[Unknown]: Midvale
What is the name of your State or Province?[Unknown]: Utah
What is the two-letter country code for this unit?[Unknown]: US
Is CN=avaself.wavelink.com, OU=Engineering, O=Wavelink Corporation,
L=Midvale, ST=Utah, C=US correct?[no]: yes
Enter key password for <amccert>(RETURN if same as keystore
password):
```

## Generating the Certificate Signing Request

Once you have created the keystore, you can use the `keytool.exe` utility to generate a certificate signing request (`certreq.csr`) file to send to a certificate authority.

To generate a certificate signing request:

- 1 From a command line, navigate to:  
`[Avalanche installation directory]\JRE\Bin`
- 2 Use the command:  
`keytool -certreq -keyalg RSA -alias amccert -file certreq.csr  
-keystore "[Avalanche installation  
directory]\JRE\bin\amckeystore.keystore"`
- 3 Enter your keystore password.

When you apply to a certificate authority for an SSL web server certificate, you will need to submit the `certreq.csr` file. This file should be created in the `[Avalanche installation directory]\JRE\bin` folder.

## Importing an Intermediate Certificate

When you acquire an intermediate certificate from your certificate authority, import it into the keystore. You may need to copy the contents of the intermediate certificate to a text editor and save the file as `intermediateCA.cer`. This file must be saved in the `[Avalanche installation directory]\JRE\bin` directory before you can import it.

To import an intermediate certificate:

- 1 From a command line, navigate to:  
`[Avalanche installation directory]\JRE\bin`
- 2 Use the command:  
`keytool -import -alias intermediateCA -keystore "[Avalanche  
installation directory]\JRE\bin\amckeystore.keystore"  
-trustcacerts -file intermediateCA.cer`



---

**NOTE:** In this command, the filename `intermediateCA.cer` is used. If your intermediate certificate has a different name, use it instead.

---

- 3 Enter your keystore password.

The intermediate certificate is added to the keystore.

## Importing a Certificate

Once you have received your certificate, you need to import it into the keystore. Your certificate will probably come as a file with the extension `.cer` or in the body of an e-mail. If it comes in the body of an e-mail, copy the contents to a text editor and save the file with a `.cer` extension. This file must be saved in the `[Avalanche installation directory]\JRE\bin` directory before you can import it.

To import a certificate:

- 1 From a command line, navigate to:  
`[Avalanche installation directory]\JRE\bin`
- 2 Use the command:  
`keytool -import -alias amccert -keystore "[Avalanche installation directory]\JRE\bin\amckeystore.keystore" -trustcacerts -file ava-wavelink-com.cer`

---

**NOTE:** As an example, `ava-wavelink-com.cer` is used as the filename. Replace this filename with the name of your certificate.

---

- 3 Enter your keystore password.

The certificate is added to the keystore.

## Activating SSL for Tomcat

Once you have generated a certificate, you must activate SSL for Tomcat. You must modify the `server.xml` file and then restart the Tomcat server.

To activate SSL for Tomcat:

- 1 Navigate to  
`[Avalanche Install location]\WebUtilities\tomcat\conf`  
and open the `server.xml` file with a text editor such as Notepad.
- 2 Find  
`<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" />`



3 Remove the comment markers so that the section is not commented out.

4 Modify the section to contain the following information:

```
<Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
SSLEnabled="true" maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" keystoreFile="C:\Program
Files\Wavelink\AvalancheMC\ JRE\bin\amckeystore.keystore"
keystorePass="[keypass]"/>
```

Where [keypass] is the keystore password you entered when creating the certificate. For the above example, this would be avalanche.

```
keystorePass="avalanche"
```

---

**NOTE:** If you are not using port 443 for any other applications, you can change the connector port to 443. Changing the port to 443 will allow you to access the Web Console without entering the port within the URL.

---

5 Save your changes to the file.

6 Restart the Apache Tomcat for Wavelink service.

## Accessing the Web Console over a Secure Connection

Once you have generated a certificate, activated SSL for Tomcat, and restarted the Tomcat server, you can access the Web Console over a https connection.

To access the Web Console over a secure connection:

- In the address field of your browser, type:

```
https://[Your Domain Name]:8443/AvalancheWeb
```

-Or-

- If you changed the connector port to 443, type:

```
https://[Your Domain Name]/AvalancheWeb
```

## Troubleshooting

To troubleshoot issues connecting to the Apache Tomcat server using SSL after changes are made, go to

```
[Avalanche installation directory]\WebUtilities\Tomcat\logs
```

to find Catalina Tomcat logs.



---

**NOTE:** You need to stop the Tomcat service to get all the log messages.

---

Example log file: `catalina.2010-02-24.log`

## Implementing a Self-Signed Certificate

These instructions explain how to generate a self-signed certificate in the Apache Tomcat environment. If you choose not to use a Certificate Authority, you can still use a https connection to connect to the Web Console by creating your own certificate.

---

**NOTE:** Internet browsers will not recognize a self-signed certificate as legitimate and will display warnings before allowing you access.

---

---

**NOTE:** Wavelink strongly recommends backing up `server.xml` and `selfsignkeystore.keystore` when you have implemented a self-signed certificate.

---

This section contains the following tasks for implementing a self-signed certificate:

- [Generating a Certificate](#)
- [Activating SSL for Tomcat](#)
- [Accessing the Web Console over a Secure Connection](#)
- [Troubleshooting](#)

### Generating a Certificate

To create a self-signed certificate, use the `keytool.exe` utility. You will need to provide a Common Name (domain name), organizational unit, organization, city, state, and country code when creating your certificate. You will also need to provide a keystore name and passwords for the keystore and alias. These are arbitrary, but should be noted for future reference.

To generate a self-signed certificate:

- 1 From a command line, navigate to:  
`[Avalanche installation directory]\JRE\Bin`
- 2 Use the command:  
`keytool -genkey -alias amcselfcert -keyalg RSA -keystore selfsignkeystore.keystore`
- 3 At the prompt **Enter keystore password**, type the keystore password. When prompted, re-enter the password.
- 4 At the prompt **What is your first and last name**, type the Common Name.





---

**NOTE:** The Common Name (domain name) you enter should be one that your company owns. Use a DNS entry if needed to resolve this computer to the Common Name.

---

- 5 At the prompts, enter your organizational unit, organization, city, state, and the country code.
- 6 When you are prompted to review your information, type `yes` to confirm that it is correct. If you type `no`, you will be guided through the prompts again.
- 7 At the prompt **Enter key password for <amcselfcert>**, type a password to use for the alias. If you want to use the same password for the alias as you used for the keystore, press Return.

**An example of generating a self-signed certificate:**

```
Enter keystore password: avalanche
```

```
Re-enter new password: avalanche
```

```
What is your first and last name?[Unknown]: avaself.wavelink.com
```

```
What is the name of your organizational unit?[Unknown]: Engineering
```

```
What is the name of your organization?[Unknown]: Wavelink Corporation
```

```
What is the name of your City or Locality?[Unknown]: Midvale
```

```
What is the name of your State or Province?[Unknown]: Utah
```

```
What is the two-letter country code for this unit?[Unknown]: US
```

```
Is CN=avaself.wavelink.com, OU=Engineering, O=Wavelink Corporation,
L=Midvale, ST=Utah, C=US correct?[no]: yes
```

```
Enter key password for <amcselfcert>(RETURN if same as keystore
password):
```

## Activating SSL for Tomcat

Once you have generated a certificate, you must activate SSL for Tomcat. You must modify the `server.xml` file and then restart the Tomcat server.

**To activate SSL for Tomcat:**

- 1 Navigate to  
[Avalanche Install location]\WebUtilities\tomcat\conf  
and open the `server.xml` file with a text editor such as Notepad.
- 2 Find  
`<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"`



```
maxThreads="150" scheme="https" secure="true" clientAuth="false"
sslProtocol="TLS" />
```

3 Remove the comment markers so that the section is not commented out.

4 Modify the section to contain the following information:

```
<Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
SSLEnabled="true" maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" keystoreFile="C:\Program
Files\Wavelink\AvalancheMC\JRE\bin\selfsignkeystore.keystore"
keystorePass="[keypass]" />
```

Where [keypass] is the keystore password you entered when creating the certificate. For the above example, this would be avalanche.

```
keystorePass="avalanche"
```

---

**NOTE:** If you are not using port 443 for any other applications, you can change the connector port to 443. Changing the port to 443 will allow you to access the Web Console without typing the port as part of the URL.

---

5 Save your changes to the file.

6 Restart the Apache Tomcat for Wavelink service.

## Accessing the Web Console over a Secure Connection

Once you have generated a certificate, activated SSL for Tomcat, and restarted the Tomcat server, you can access the Web Console over a https connection.

To access the Web Console over a secure connection:

- In the address field of your browser, type:

```
https://<Domain Name>:8443/AvalancheWeb
```

-Or-

- If you changed the connector port to 443, type:

```
https://<Domain Name>/AvalancheWeb
```

## Troubleshooting

To troubleshoot issues connecting to the Apache Tomcat server using SSL after changes are made, go to

```
[Avalanche installation directory]\WebUtilities\Tomcat\logs
```



to find Catalina Tomcat logs.

---

**NOTE:** You need to stop the Tomcat service to get all the log messages.

---

Example log file: `catalina.2010-02-24.log`



## Avalanche Services

This is a list all of the Avalanche services. Under each service title, you'll find the file path where the service is located for a default installation and which server the service is associated with.

### Apache Tomcat for Wavelink

C:\Program Files\Wavelink\Avalanche\WebUtilities\Tomcat\bin\tomcat7.exe

The Tomcat server is responsible for making the Web Console available. It is normally installed with the Enterprise Server.

### Wavelink Authentication Service AMC

C:\Program Files\Wavelink\AvalancheSE\CESecureServer.exe

The authentication server authenticates users when your system is configured to use SecurePlus or integrated logon. It is installed with the Enterprise Server.

### Wavelink Avalanche Service Manager

C:\Program Files\Wavelink\Avalanche\Service\WLAmcServiceManager.exe

The service manager starts and stops the mobile device server. It is installed with a device server.

### Wavelink Avalanche Enterprise Server

C:\Program Files\Wavelink\AvalancheSE\eserver.exe

This is the enterprise server.

### Wavelink Information Router

C:\Program Files\Wavelink\AvalancheSE\WLInfoRailService.exe

The inforail service handles messages between servers and databases. It is normally installed with the enterprise server.

### Wavelink License Server

C:\Program Files\Wavelink\AvalancheSE\WLLicenseService.exe

The license server manages licensing. It is normally installed with the enterprise server.

### Wavelink Stat Server Enterprise

C:\Program Files\Wavelink\AvalancheSE\StatServer.exe



The statistics server handles reports and device statistics. It is generally installed with the enterprise server.

## Wavelink Avalanche Agent

C:\Program Files\Wavelink\Avalanche\Service\WLAvalancheService.exe

This is the mobile device server.



## Port Information

This page provides information about the ports used in Avalanche MC.

### Database Inbound Ports

The databases listen on different ports depending on the database management system you are using (PostgreSQL, Oracle, or Microsoft SQL Server) and whether the database administrator has changed the port number. The following table lists the default port for each database management system. Be sure to configure Avalanche and your network with the correct port number.

The standard Avalanche installation uses a PostgreSQL database management system.

| Database Management System | Default Port | UDP/TCP | Source                                            |
|----------------------------|--------------|---------|---------------------------------------------------|
| PostgreSQL                 | 5432         | TCP     | Enterprise Server, Statistics Server, Web Console |
| Oracle                     | 1521         | TCP     | Enterprise Server, Statistics Server, Web Console |
| MS SQL Server              | 1433         | TCP     | Enterprise Server, Statistics Server, Web Console |

### Enterprise/Statistics Server Ports

The following table provides a list of ports that the Enterprise and Statistics Server use to communicate. The Tomcat server is usually installed local to the Enterprise Server.

| Traffic Description                                                        | Port | UDP/TCP | Source                                                                   | Destination                                        |
|----------------------------------------------------------------------------|------|---------|--------------------------------------------------------------------------|----------------------------------------------------|
| LDAP user verification.                                                    | 389  | TCP     | Enterprise Server                                                        | LDAP server                                        |
| Active Directory user verification.                                        | 5002 | TCP     | Enterprise Server                                                        | Active Directory server                            |
| Mobile device server requesting licenses from the License Server.          | 7221 | TCP     | Mobile Device Server                                                     | Enterprise Server                                  |
| InfoRail transmission of information between servers, consoles, databases. | 7225 | TCP     | Mobile Device Server, Enterprise Server, Web and Java Console, databases | Mobile Device Server, Statistics Server, databases |
| InfoRail talking to itself.                                                | 7226 | TCP     | Local traffic                                                            | Local traffic                                      |
| Web Console requesting information.                                        | 8080 | TCP     | Web Console                                                              | Tomcat server                                      |



**NOTE:** If you use an SSL certificate, the Tomcat server listens on 8443 for a connection. You can change this to 443 in the `server.xml` file if no other program is using 443. For more information on changing the port for a Web Console connection, see [SSL Certificates for the Web Console](#).

## Mobile Device Server Ports

The following table provides a list of the ports that the Mobile Device Server uses to communicate with the Enabler installed on a mobile device.

| Traffic Description                                           | Port | UDP/TCP |
|---------------------------------------------------------------|------|---------|
| Protocol Service. Traffic between the server and the Enabler. | 1777 | UDP/TCP |
| MUV3. Services persistent connections to mobile devices.      | 1778 | TCP     |

## Wavelink Products Used with Avalanche

The following table provides a list of the ports that are used by Wavelink products often used in conjunction with Avalanche.

| Port | Product              | Port Type |
|------|----------------------|-----------|
| 1899 | Remote Control       | TCP/UDP   |
| 1900 | Remote Control       | TCP       |
| 5001 | CE Secure/SecurePlus | TCP       |



## Avalanche Copyrights and Licenses

This document lists the copyrights and licenses for third-party tools and libraries used in the Avalanche product.

### Use of Apache Software Foundation Components

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). The software is made available under the Apache License 2.0. A copy of the license may be obtained from <http://www.apache.org/LICENSE-2.0>.

### Use of MD5 Message Digest Algorithm

This product includes components derived from the RSA Data Security, Inc. MD5 Message digest algorithm.

### Use of Trilead Java SSH Client

This product includes a copy of Trilead Java SSH client library. It is made available under the following license:

Copyright (c) 2007 Trilead AG (<http://www.trilead.com>)

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- a.) Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- b.) Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- c.) Neither the name of Trilead nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Trilead SSH-2 for Java includes code that was written by Dr. Christian Plattner during his PhD at ETH Zurich. The license states the following:

Copyright (c) 2005 - 2006 Swiss Federal Institute of Technology (ETH Zurich),





Department of Computer Science (<http://www.inf.ethz.ch>),  
Christian Plattner. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- a.) Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- b.) Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- c.) Neither the name of ETH Zurich nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Java implementations of the AES, Blowfish and 3DES ciphers have been taken (and slightly modified) from the cryptography package released by "The Legion Of The Bouncy Castle".

Their license states the following:

Copyright (c) 2000 - 2004 The Legion Of The Bouncy Castle  
(<http://www.bouncycastle.org>)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.



## Use of zlib

zlib.h -- interface of the 'zlib' general purpose compression library version 1.2.5, April 19th, 2010

Copyright (C) 1995-2010 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly

Mark Adler

To download zlib or for more information visit <http://www.zlib.net/>.

## Use of JoeSNMP

This product includes a copy of JoeSNMP Java SNMP library. The software is made available under the GNU LGPL license as follows:

joeSNMP is Copyright (C) 2002-2003 Blast Internet Services, Inc.

All rights reserved. joeSNMP is a derivative work, containing both original code, included code and modified code that was published under the GNU Lesser General Public License.

Copyright (C) 1999-2001 Oculan Corp. All rights reserved.

Copyrights for modified and included code are included in the individual source files.

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.



You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

See: <http://www.fsf.org/copyleft/lesser.html>

For more information contact:

joeSNMP Licensing

## Use of Expat

This product includes a copy of the Expat XML parser. The software is made available through the following copyright notice:

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper

Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Expat maintainers.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## Use of 7-Zip

This product includes a copy of the 7-Zip archive utility. The software is made available through this license:

7-Zip

License for use and distribution

~~~~~

7-Zip Copyright (C) 1999-2011 Igor Pavlov.

Licenses for files are:

- 1) 7z.dll: GNU LGPL + unRAR restriction
- 2) All other files: GNU LGPL

The GNU LGPL + unRAR restriction means that you must follow both GNU LGPL rules and unRAR restriction rules.



Note: You can use 7-Zip on any computer, including a computer in a commercial organization. You don't need to register or pay for 7-Zip.

GNU LGPL information

-----

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version. This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You can receive a copy of the GNU Lesser General Public License from

<http://www.gnu.org/>

unRAR restriction

-----

The decompression engine for RAR archives was developed using source code of unRAR program.

All copyrights to original unRAR code are owned by Alexander Roshal.

The license for original unRAR code has the following restriction:

The unRAR sources cannot be used to re-create the RAR compression algorithm, which is proprietary. Distribution of modified unRAR sources in separate form or as a part of other software is permitted, provided that it is clearly stated in the documentation and source comments that the code may not be used to develop a RAR (WinRAR) compatible archiver.

--

Igor Pavlov

## Use of OpenMap Software

This product includes OpenMap components by BBN software (<http://openmap.bbn.com/>).

The software is made available under the BBN license, a copy of which may be obtained from <http://openmap.bbn.com/license.html>.

## Use of the Java iText PDF library

This product includes a copy of the Java iText PDF library, version 2.1.7.

The software is made available under the GNU LGPL license. The library was written by Bruno Lowagie, Paulo Soares, and others.

## Use of the Java dom4j XML library

This product includes a copy of the Java dom4j XML library.

The software is made available by MetaStuff under the following license:



Copyright 2001-2005 (C) MetaStuff, Ltd. All Rights Reserved.

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "DOM4J" must not be used to endorse or promote products derived from this Software without prior written permission of MetaStuff, Ltd. For written permission, please contact [dom4j-info@metastuff.com](mailto:dom4j-info@metastuff.com).
4. Products derived from this Software may not be called "DOM4J" nor may "DOM4J" appear in their names without prior written permission of MetaStuff, Ltd. DOM4J is a registered trademark of MetaStuff, Ltd.
5. Due credit should be given to the DOM4J Project - <http://www.dom4j.org>

THIS SOFTWARE IS PROVIDED BY METASTUFF, LTD. AND CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL METASTUFF, LTD. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Use of Quartz Scheduler

Quartz Scheduler source code and documentation are available under the following license:

Quartz Scheduler is licensed under the Apache License, Version 2.0 (the "License"); you may not use Quartz binaries or source in whole or in part except in compliance with the License. You may obtain a copy of the License at:

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

© 2001-2011 Terracotta, Inc., <http://www.terracotta.org>



## Uninstalling Avalanche

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

When you uninstall Avalanche, you are given the option to uninstall the PostgreSQL database as well. If you select to uninstall Avalanche and the PostgreSQL database, all components of Avalanche and the database will be removed. If you select to uninstall Avalanche but opt to leave the database, the `\db` folder located in the default installation directory will remain on your system. (The default location is `C:\Program Files\Wavelink\AvalancheMC\db`.)

The uninstall utility will not uninstall any infrastructure or mobile device servers that have been deployed. If you want to uninstall device servers, use the Task Scheduler to uninstall them *before* using the uninstall utility. For more information see [Uninstalling Servers](#).

If you uninstall and reinstall the enterprise server (on the same system) without uninstalling the device servers, the device servers are automatically discovered and appear in the **Unassigned Server Locations** region. If you install the enterprise server on a different system, device servers are not auto-discovered. They will need to be redeployed.

---

**NOTE:** If you plan on uninstalling Avalanche and/or the PostgreSQL database, it is recommended that you extract and backup database information and software profiles with the Task Scheduler. For more information, see [Using the Task Scheduler](#).

---

### To uninstall Avalanche:

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

-Or-

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

The *Uninstall Wizard* appears.

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

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



## Wavelink Contact Information

If you have comments or questions regarding this product, please contact Wavelink Customer Service.

E-mail Wavelink Customer Support at: [CustomerService@wavelink.com](mailto:CustomerService@wavelink.com)

For customers within North America and Canada, call the Wavelink Technical Support line at 801-316-9000 (option 2) or 888-699-9283.

For international customers, call the international Wavelink Technical Support line at +800 9283 5465.

For Europe, Middle East, and Africa, hours are 9 AM - 5 PM GMT.

For all other customers, hours are 7 AM - 7 PM MST.

