



Wavelink Avalanche Mobility Center  
Web 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](mailto:customerservice@wavelink.com)  
Web site: [www.wavelink.com](http://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

---

<b>Chapter 1: Introduction</b> .....	<b>1</b>
Components of Avalanche .....	1
Location Management .....	3
Getting Started .....	4
About This Guide .....	6
<b>Chapter 2: Avalanche Web Console</b> .....	<b>8</b>
Launching the Avalanche Web Console .....	8
Understanding the Web Console .....	9
Management Tabs .....	10
Location Navigation .....	13
Panels .....	14
Editing Columns .....	15
Using Device Filters .....	16
Understanding Edit Mode .....	17
Console Tools .....	18
Viewing System Information .....	18
Configuring Audit Logging .....	19
Viewing the Audit Log .....	20
Configuring General System Settings .....	21
Configuring E-mail Settings .....	23
Setting a System Message .....	23
Creating Links in the Tools Menu .....	24
Restricting Server-to-Server Communication .....	24
Checking for Available Updates .....	25
Installing Language Support .....	25
<b>Chapter 3: Managing User Accounts</b> .....	<b>27</b>
Creating User Accounts .....	28
Creating User Groups .....	29
Assigning User Permissions .....	30
Assigning Authorized Users .....	32
Assigning Authorized Users to Locations .....	32
Assigning Authorized Users to Profiles .....	32
Assigning Authorized Users to Mobile Device Groups .....	33
Configuring Integrated Logon .....	33
Removing User Accounts .....	34
<b>Chapter 4: Location Management</b> .....	<b>35</b>
Managing Regions .....	36
Creating Regions .....	36
Viewing Region Properties .....	37
Deleting Regions .....	37



Managing Server Locations .....	38
Determining Server Placement .....	38
Adding Server Locations .....	41
Moving Server Locations to Regions .....	42
Modifying Server Location Properties .....	43
Deleting Server Locations .....	43
Managing Group Locations .....	44
Creating a Group Location .....	44
Additional Group Location Functions .....	45
Applying Profiles to Locations .....	45
Editing Exclusions .....	46
<b>Chapter 5: Managing Network Profiles .....</b>	<b>48</b>
Creating Network Profiles .....	48
Configuring Scheduled Settings .....	50
Configuring WLAN IP Settings .....	50
Configuring WLAN Settings .....	52
Configuring WWAN Settings .....	55
<b>Chapter 6: Managing Scan to Configure Profiles .....</b>	<b>58</b>
Creating a Scan to Config Profile .....	58
Configuring a Scan to Config Profile .....	59
Adding Custom Properties for Scan to Config Profiles .....	60
Adding a Registry Key to a Scan to Config Profile .....	60
Printing Barcodes .....	61
Scanning Barcodes .....	61
<b>Chapter 7: Managing Infrastructure Devices .....</b>	<b>63</b>
Querying an Infrastructure Device .....	64
Pinging an Infrastructure Device .....	65
Resetting Access Points .....	65
Deleting Infrastructure Devices .....	66
Mapping Infrastructure Devices on a Floorplan .....	66
Importing a Floorplan .....	67
Plotting Infrastructure Devices .....	68
Adjusting the Floorplan Display .....	68
<b>Chapter 8: Managing a Mobile Device Server .....</b>	<b>70</b>
Creating and Configuring a Mobile Device Server Profile .....	70
Mobile Device Server Profile General Configuration .....	71
Configuring Blackouts .....	76
Scheduling Profile-Specific Device Updates .....	77
Viewing Mobile Device Server Licensing Messages .....	78
Viewing Server Details .....	78



<b>Chapter 9: Managing Software Profiles</b> .....	<b>80</b>
Creating Software Profiles .....	80
Managing Software Packages .....	81
Adding a Software Package .....	82
Building New Software Packages .....	83
Creating CAB or MSI Packages .....	85
Copying Software Packages .....	86
Enabling Software Packages .....	86
Configuring Software Packages with a Utility .....	87
Configuring Software Packages for Delayed Installation .....	88
Peer-to-Peer Package Distribution .....	89
<b>Chapter 10: Managing Mobile Devices</b> .....	<b>92</b>
Mobile Devices Panel .....	92
Viewing Mobile Device Details .....	93
Locating a Mobile Device .....	93
Locating a Device using Cell Tower Information .....	94
Viewing Location History .....	94
Configuring Mobile Device Properties .....	95
Creating Custom Properties .....	96
Creating Device-Side Properties .....	96
Editing Properties .....	97
Deleting Properties .....	97
Contacting the Mobile Device .....	98
Pinging Mobile Devices .....	98
Sending a Message to a Device User .....	98
Updating a Mobile Device .....	99
Chatting with a Device User .....	100
Wiping a Mobile Device .....	100
Using Remote Control .....	101
<b>Chapter 11: Managing Mobile Device Profiles</b> .....	<b>102</b>
Creating a Mobile Device Profile .....	102
Configuring Device Wipe Folders .....	103
Editing Custom Properties for Mobile Device Profiles .....	104
Editing Registry Keys for a Mobile Device Profile .....	105
Adding a Registry Key to a Mobile Device Profile .....	105
Editing or Removing a Registry Key or Value .....	106
Configuring Mobile Device Profile Advanced Settings .....	107
Location Based Services .....	107
Geofence Areas .....	108
Regional Settings .....	109
Update Restrictions .....	109



---

<b>Chapter 12: Managing Mobile Device Groups</b> .....	<b>110</b>
Creating Mobile Device Groups.....	110
Sending Messages to Mobile Device Groups.....	111
<b>Chapter 13: Managing Alert Profiles</b> .....	<b>112</b>
Creating and Configuring Alert Profiles.....	112
Adding E-Mail Contacts.....	113
Adding SNMP Proxies.....	115
Alerts Tab.....	115
Acknowledging and Clearing Alerts.....	116
Customizing Alerts Tab Functionality.....	117
<b>Chapter 14: Using Selection Criteria</b> .....	<b>118</b>
Building Selection Criteria.....	119
Selection Variables.....	120
Operators.....	126
Adding Properties to the Selection Variables.....	129
<b>Chapter 15: Avalanche Reports</b> .....	<b>130</b>
Configuring Reports.....	131
Generating and Scheduling Reports.....	132
Creating Custom Reports.....	132
<b>Chapter 16: Using the Task Scheduler</b> .....	<b>134</b>
Performing a Server Synchronization.....	136
Backing Up the System.....	136
Restoring the System.....	137
Removing Completed Tasks.....	138
<b>SSL Certificates for the Web Console</b> .....	<b>139</b>
<b>Avalanche Services</b> .....	<b>148</b>
<b>Port Information</b> .....	<b>150</b>
<b>Supported Firmware</b> .....	<b>153</b>
<b>Avalanche Copyrights and Licenses</b> .....	<b>172</b>
<b>Uninstalling Avalanche</b> .....	<b>178</b>
<b>Wavelink Contact Information</b> .....	<b>179</b>



## Chapter 1: Introduction

Avalanche is an infrastructure and mobile device management system. From a central console, you can locate and manage devices, including monitoring and distributing software and firmware. 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 Web 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 Web Console. For details about performing tasks from the Java Console, see the Java Console User Guide.

---

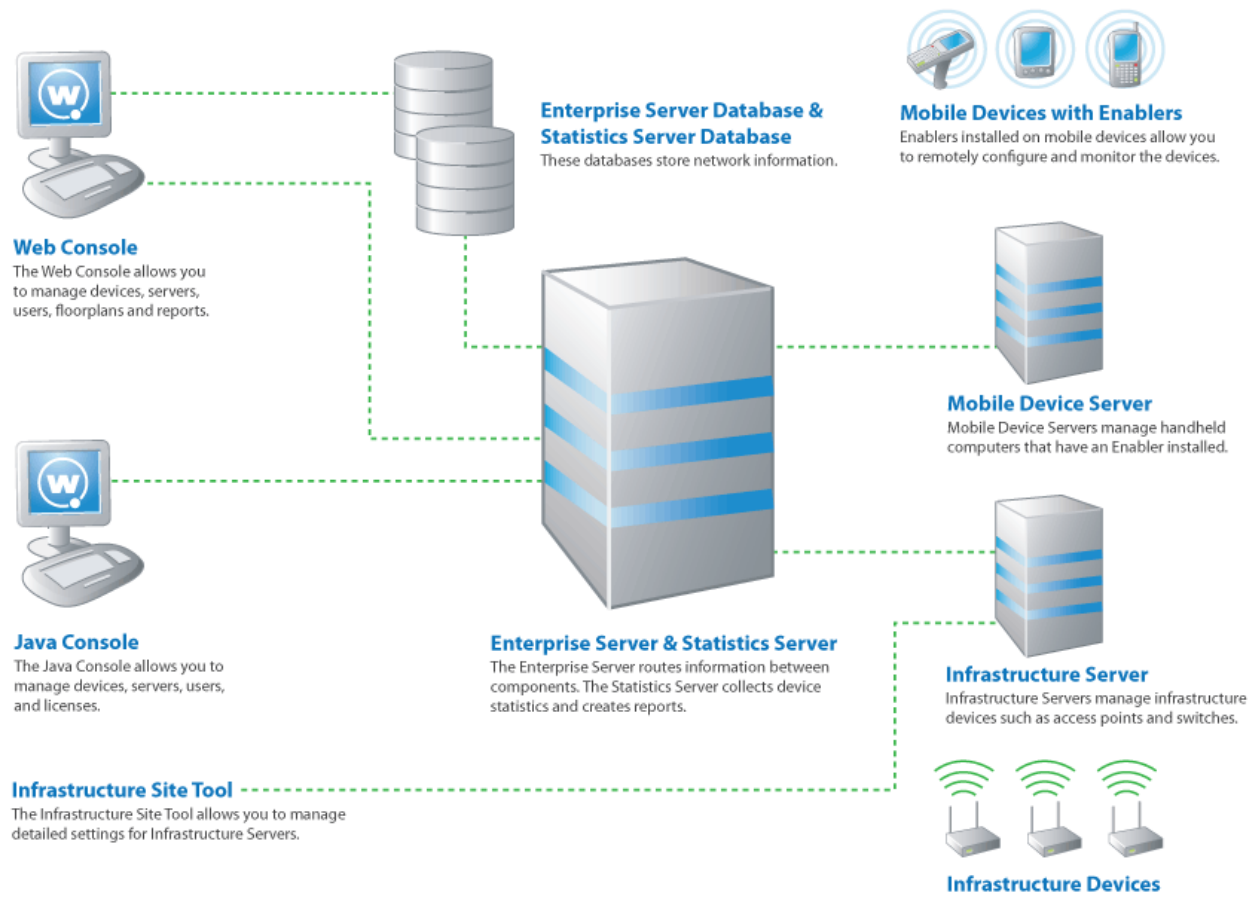
This section provides the following introductory information:

- [Components of Avalanche](#)
- [Location Management](#)
- [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 device servers, 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.

---

- **Device Servers.** Device servers are responsible for communication between the Avalanche Console and wireless devices. Avalanche has two types of device servers: Infrastructure Servers and Mobile Device Servers. Although there is only one Enterprise Server, you can have multiple device servers of either type.
- **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 MC, the Enterprise and Statistics Server, both databases, and the components for the Java and Web Consoles are all installed at one location. Once the Enterprise Server has been installed, you can use the Console to create device server packages. These server packages are deployed to the systems where you want the device servers installed. For information on where to install device servers, see [Determining Server Placement](#).

---

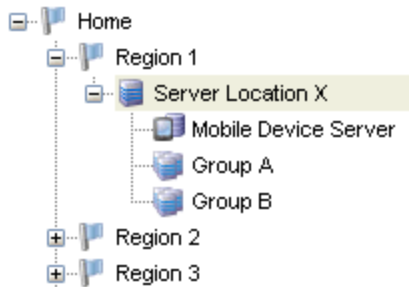
**NOTE:** Avalanche offers many options so that you can install components on different computers. For more information on installation options, see the *Installing Avalanche* paper on the Wavelink Web site.

---

## Location Management

One of the key aspects of Avalanche is location management. Avalanche organizes servers and devices in locations to make them easier to manage. Avalanche divides locations into three main categories: region locations, server locations and group locations. Locations are organized in the Navigation Window:





Navigation Window with sample locations

A server location is the basic component of the Avalanche system. Each server location contains at least one device server that communicates with specific wireless components.

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

For each server location with a Mobile Device Server, you also have the option of creating a group location. This is defined as a group of devices that connect to the same server. Devices are added to a group location when they meet selection criteria for that group. A device can belong to more than one group location concurrently. Group locations allow increased flexibility for assigning different profiles at the same server location.

The number of wireless components managed at a server location depends on the communication range of the servers installed at that location. Traditionally, this range has been defined as a single subnet on your network; however, depending on your network architecture, you can configure an infrastructure server to communicate past a given subnet. This type of configuration takes place at the server location level, using the Infrastructure Site Tool. For information on using the Infrastructure Site Tool, see *Infrastructure Site Tool* and the *Avalanche Console*.

## 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 and Infrastructure licenses for Avalanche.** You should activate the number of licenses based on the number of devices you want to manage. For information on licensing, see the Java Console help.



- 3 **Create region locations.** A region allows you to group server locations that share a set of similar characteristics such as geographic location or role within your organization's structure. For more information, see [Managing Regions](#).
- 4 **Create server locations.** Server locations are the locations on your network where the device servers are installed. For more information, see [Managing Server Locations](#).
- 5 **Create group locations.** Group locations are user-defined groups of devices that connect to the same device server. For more information, see [Managing Group Locations](#).
- 6 **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 servers or 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:

<b>Infrastructure profile</b>	An infrastructure profile allows you to manage settings for infrastructure devices and schedule device events.
<b>Mobile Device profile</b>	A mobile device profile manages settings on your mobile devices, as well as adding, changing, and removing custom properties and registry keys.
<b>Server profiles</b>	You can assign one Mobile Device Server profile and one Infrastructure Server profile to each server location. These profiles configure how the device servers interact with devices and the Enterprise Server.
<b>Alert profile</b>	An alert profile allows you to track events on your network and send notifications by e-mail or proxy server.
<b>Network profile</b>	A network profile provides gateway addresses, subnet masks, WWAN settings, and encryption and authentication information to devices on your network.
<b>Software profile</b>	A software profile allows you control over where and when software and files are distributed to mobile devices.
<b>Scan to Config profile</b>	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.

- 7 **Assign profiles to locations.** You can assign configured profiles to locations from the Console. When you assign a profile to a location and install the Servers, or 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](#).



- 8 **Install servers.** Create a server package to deploy to the locations. This will install the servers and apply profile configurations to the servers and devices. For more information, see [Building Server Deployment Packages](#).
- 9 **Configure Enablers.** Ensure that your mobile devices have Enablers installed, and configure the Enablers to connect to a mobile device server.
- 10 **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** 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: Avalanche Web 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, including network and device configuration, and monitoring network performance.

The Avalanche Console is traditionally accessed from a computer where the Console has been installed. This installed Console is the Java Console. However, using an Internet connection, you also can access a version of the Console from a computer where the Console has not been installed. This is called the Web Console.

The Web Console allows you to create and view reports, view device inventories, manage profiles and alerts, and manage floorplans for your enterprise. However, there are some tasks available only with the Java Console, such as managing infrastructure server profiles.

---

**NOTE:** For information on tasks available from the Java Console, see the Java Console help.

---

This section contains the following topics about the Web Console:

- [Launching the Avalanche Web Console](#)
- [Understanding the Web Console](#)
- [Console Tools](#)

### Launching the Avalanche Web Console

To access the Web Console, you will need:

- An Internet browser, such as Internet Explorer or Firefox.
- An Internet connection between the Avalanche On Demand server and the computer where you will be using the Console.
- The web components installed at the same location as the enterprise server. If you performed a custom installation, you should have selected the **Web Components** option to be installed. If you performed an enterprise installation, the web components were installed automatically.
- Each user who will use the Console to configure software packages must have a JRE installed.
- Each user who will upload software packages, e-mail lists, or floorplan images must have the latest version of a Flash browser plug-in.



---

**NOTE:** If you choose to use a certificate to create a secure connection between the browser and the server, see [SSL Certificates for the Web Console](#) for information on launching the Web Console.

---

To access the Web Console from the Java Console:

- 1 Click **View > Launch Web Console**.

The Web Console appears in your default browser.

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

Avalanche is installed with a default user login of `amcadmin` and password of `admin`.

- 3 Click **Connect**.

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

To access the Web Console from a web browser:

- 1 In the address field of your browser, type:

```
http://[address]:8080/AvalancheWeb/
```

where `[address]` is the IP address or DNS name of the machine where the enterprise server is installed.

The User Login page appears.

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

Avalanche is installed with a default user login of `amcadmin` and password of `admin`.

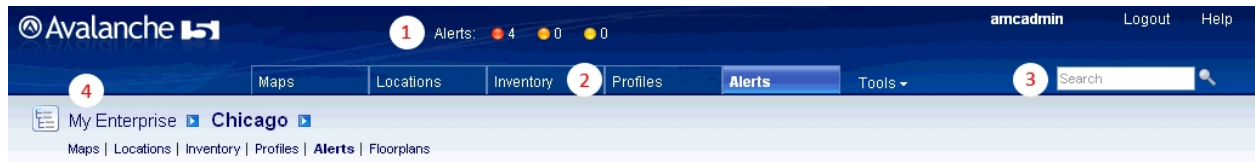
- 3 Click **Connect**.

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

## Understanding the Web Console

The top portion of the Web Console always contains the same elements: an alerts overview, management tabs, a search box, and location navigation. It also displays the current user and provides links for logout and help.





- 1 The alerts overview shows the number of critical, error, and warning alerts current in the user's home location. If there are any messages from the system administrator, they will also appear with the alerts overview.
- 2 The management tabs provide access to maps, inventories, alerts, and other properties of your enterprise. The **Tools** menu provides you with access to the Reports tool, user management, scheduled tasks, and system information and settings.
- 3 The search box allows you to search for content in the Console, such as a specific location.
- 4 The location navigation allows you to access information particular to a selected location. By selecting a location and then using the context links (underneath the name of the location), the information will be filtered to display only items pertinent to the selected location.

The rest of the page changes depending on which tab or context link you have selected, displaying panels with associated information. When you edit information from the Avalanche Console, it enters Edit Mode, locking the records for that item until the changes are saved or Edit Mode times out.

This section gives details about the following areas:

- [Management Tabs](#)
- [Location Navigation](#)
- [Panels](#)
- [Understanding Edit Mode](#)

## Management Tabs

The management tabs provide the user with available information relating to his home location. If the user's home location is Chicago, these tabs will display information for Chicago. If the user's home location is Region Two, the tabs will display information specific to Region Two.

---

**NOTE:** If you want to filter the information displayed by location, navigate to the location and then use the context links under the location name to navigate.

---

There are five management tabs and the **Tools** menu:

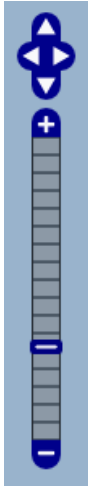




## Maps

The **Maps** tab provides a map displaying your locations. You can also view the location of alerts and device GPS position or history. From the Web Console map, you can view your locations, the highest alert level associated with each, and the GPS position and history of your mobile devices. Or, to filter the information displayed by location, navigate to the desired location and click the Maps context link.

The following options are available for configuring the map display:



The map navigation buttons allow you to zoom in and out and move the map view north, east, south and west. You can also move the map view by clicking and dragging the map.

**Show Locations** **Regions.** Displays all regions that have defined GPS locations on the map. You can view location-specific information in a callout box when you click on a location.

**Servers.** Displays all server locations that have defined GPS locations on the map.

**Group Locations.** Displays all group locations that have defined GPS locations will be displayed on the map.

**Show Alert Levels** **Critical Alerts.** When this option is enabled, the map will display any area in your network that has an unacknowledged critical alert.

**Error Alerts.** When this option is enabled, the map will display any area in your network that has an unacknowledged error alert.

**Warning Alerts.** When this option is enabled, the map will display any area in your network that has an unacknowledged warning alert.

**Informational Alerts.** When this option is enabled, the map will display any area in your network that has an unacknowledged informational alert.



**Show Device Positions** **Device GPS Position.** When this option is enabled, devices recently viewed will be displayed on the map at their reported location.

**Device GPS History.** When this option is enabled, the most recent device to have its location history plotted will have its location history displayed on the map.

**GEO Fences.** When this option is enabled, geofences that have been configured for all mobile device profiles applied to the context location will be displayed on the map.

---

**NOTE:** **Show Device Positions** options will only be available when you have plotted devices that have reported GPS coordinates.

---

## Locations

The **Locations** tab provides a panel with a summary of the location, a panel with details about any associated sub-locations, and a panel of associated authorized users. For information on managing locations with the Web Console, see [Location Management](#).

## Inventory

The **Inventory** tab provides panels listing mobile devices, infrastructure devices, device servers, and mobile device groups. You will only be able to see the devices, servers, and groups that are associated with your home location.

## Profiles

The **Profiles** tab provides panels listing applied and available profiles for the location. Profiles are collections of configurations that can be applied to devices or servers. A profile allows you to manage configurations and settings centrally and then deploy those configurations to as many locations as necessary. The Applied Profiles panel displays the profiles that are currently applied to the selected location and the type, status, and priority of those profiles. The Available Profiles panel displays all profiles that are available to be applied to the selected location.

---

**NOTE:** For information about specific profiles, see the Table of Contents. For information on applying a profile to a location, see [Applying Profiles to Locations](#).

---

Mobile Device Server and Infrastructure Server profiles are exclusive. With exclusive profiles, only the highest priority profile of that type will be applied at any given location. It is possible with inherited profiles that there may be two profiles with the same priority number applied at a location; in this situation, the profile that is applied at — or nearest to — the selected location will take priority.

You can change the priority of applied profiles at the location where they are assigned.



To change the priority of applied profiles:

- 1 In the Applied Profiles panel, click **Change Priority**.

The Change Priority page appears.

- 2 Reorder the profiles by dragging and dropping.
- 3 When you are done assigning priority, click **Save**.

## Alerts

The **Alerts** tab provides a panel listing current alerts associated with your location. For information on acknowledging and clearing alerts, see [Acknowledging and Clearing Alerts](#).

## Tools Menu

The **Tools** menu provides access to the Reports tool, user management, audit logs, scheduled tasks, system information and settings. For tasks related to the Tools menu, see [Console Tools](#).

## Location Navigation

When you use the management tabs, the Console displays information for your home location. When you navigate to a location and then use the context links, the Console will display only information pertinent to the selected location.

To navigate to a location to view:

- Click the arrow to the right of the home location. A dialog box will appear, listing the available locations within the home location. Click the name of the location you want to navigate to.

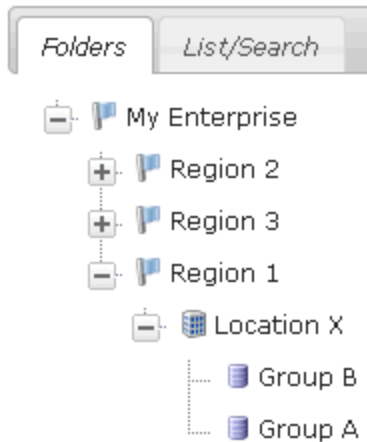
-Or-

- Click the Location View button to the left of the home location. The *Navigation* dialog box will appear, with tabs for a tree view or alphabetic list of the available locations. Using either the tree view or list, click the name of the location you want to navigate to.



*Location View button*





*Folders tab of the Location View*

## Panels

Each panel organizes and displays information about your enterprise. The columns and options of each panel differ based on what information is being displayed.



*Mobile Devices panel*

In the top left of the panel is the panel name.

The left of the panel displays filters for the information displayed in the panel. Use the automatic filters provided or click **Edit Filters** to create custom filters. When you use a filter, only the devices matching the filter's criteria show in the panel.

The top right of the panel contains options for displaying the information: how many items to display per page, and first/previous/next/last page options. There is also a **Help** button that opens a window to a related help page.

Some panels include large lists of information. By default, Avalanche generally displays the first ten items and then allows you to page through the rest of the list. You can change the number of items displayed per page, however, by clicking the preset number at the top of the panel. The options are **10**, **25**, **50**, **100**, or **All**. Or, if there are more than 2,000 items available for the list, the options will be **10**, **25**, **50**, **100**, or **2000**. To page through the list, you have the option of clicking **First**, **Previous**, **Next**, and **Last** arrows.

---

**NOTE:** **Previous** will take you to the page previous in the list, not the most recently viewed page.

---



To the left of the name of each item listed is a check box that allows you to select the item for a particular task. For example, if you wanted to delete multiple devices simultaneously, you could enable the check boxes for those devices and then click **Delete**.

Some of the columns in the panels give you the option of sorting the information in the list according to that column. Sort a list according to column by clicking the name of the column. The first click will sort the list in alphabetic order, and a second click will sort the list in reverse alphabetic order. To display different information in the panel, create or rearrange the columns. Create new columns to display custom information.

The following topics provide more information on configuring the information displayed in panels:

- [Editing Columns](#)
- [Using Device Filters](#)

### Editing Columns

Some of the columns in the panels give you the option of sorting the information in the list according to that column. Sort a list according to column by clicking the name of the column. The first click will sort the list in alphabetic order, and a second click will sort the list in reverse alphabetic order. To display different information in the panel, create or rearrange the columns. Create new columns to display custom information.

[To edit the columns displayed:](#)

- 1 In the Mobile Devices panel on the **Inventory** tab, click **Edit Columns**.

The *Modify Columns* dialog box appears. The Available Columns list shows column headers that do not currently display in the panel. The Selected Columns list shows column headers that currently display in the panel.

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

The column name moves to the Selected Columns list.

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

The column name returns to the Available Columns list.

- 4 Use **Move Up**, **Move Top**, **Move Down**, and **Move Bottom** to modify the order in which the columns appear in the Mobile Devices panel.

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

The columns are rearranged to reflect your modifications.



### To display custom columns:

- 1 In the Mobile Device panel on the **Inventory** tab, click **Edit Columns**.

The *Modify Columns* dialog box appears.

- 2 Click **Add Custom**.

The *Add Custom Property* dialog box appears.

- 3 Click **Select** to select the property you want to add as a column. This can be a custom property.

- 4 In the **Column Title** text box, type the name of the column as you want it to display in the Mobile Devices panel.

- 5 From the **Data Type** drop-down list, select the data type for this property. (This can be string, integer, or boolean data.)

- 6 In the **Tool tip** text box, type the name of the tool tip you want to display. This is the text displayed if you use the mouse to hover over the column title.

- 7 Click **Save** to return to the Modify Columns dialog box.

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

- 8 Select the column name and click **Add** to move the property to the Selected Columns list.

- 9 When you are finished, click **Save**.

The columns are arranged to reflect your modifications.

### Using Device Filters

The left of an inventory panel displays filters for the information displayed in the panel. When you enable the **Use Custom Filter** option and select a filter from the drop-down list, only the devices matching the filter's criteria show in the panel.

### To create a device filter:

- 1 In the panel, click **Edit Filters**.

The *Modify Filters* dialog box appears.

- 2 Click **New Filter**.

- 3 Enter a name for the filter in the **Filter Name** text box.

- 4 Click the **Launch wizard** button.



The *Selection Criteria Builder* dialog box appears, allowing you to create a filter based on a variety of device characteristics. For more information on using selection criteria, see [Using Selection Criteria](#).

- 5 When you have chosen the desired selection criteria, click **OK**.

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

- 6 Click **Add New Filter**.

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

- 7 Click **Save Changes**.

You can now select the filter from the Custom Filter drop-down list located to the left of the panel.

To apply a device filter:

- In the panel, enable the **Use Custom Filter** option and select the filter from the **Custom Filter** drop-down list.

The Inventory list will refresh to display the devices according to the filter settings.

## 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.

Consider the following when using Edit Mode:

- Navigating away from the page you are editing will erase any unsaved information and cancel the edit lock.
- You cannot edit unassigned or deleted server locations.
- You do not need to enter Edit Mode to view where profiles are applied.



## Console Tools

From the Web Console, you can view system information and perform tasks related to managing the enterprise server and Console. This includes allowing profile application at the root level, session timeout length, display language, alert settings, message backlog limit, and server-to-server restrictions. You can also customize the Tools menu of the Console to include custom links. This section includes information on the following tasks:

- [Viewing System Information](#)
- [Configuring Audit Logging](#)
- [Viewing the Audit Log](#)
- [Configuring General System Settings](#)
- [Configuring E-mail Settings](#)
- [Setting a System Message](#)
- [Creating Links in the Tools Menu](#)
- [Restricting Server-to-Server Communication](#)
- [Checking for Available Updates](#)
- [Installing Language Support](#)

### Viewing System Information

From the Web Console, you can view statistics about the enterprise server, Inforail, statistics server, infrastructure servers, and mobile device servers. You can also view the installed licenses.

To view system information:

- Click **Tools > Support**.

The System Information page appears. To view advanced details on specific components, click the related **Details** button.

At the bottom of the page you can view installed licenses for your Avalanche installation. From this location you cannot change any of this information; you must use the Java Console to manage licenses. See the Java Console help for details about licensing.





## 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. Configuring audit logging preferences, viewing, and clearing the log can only be performed by an Administrator.

---

**NOTE:** For information on viewing actions in 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 the Java Console User Guide.

The following events can be configured for logging:

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



---

<b>Scheduled Event, System Restore</b>	When a System Restore event has occurred.
<b>Scheduled Event, Uninstall Server</b>	When an Uninstall Server event has occurred.
<b>Scheduled Event, Universal Deployment</b>	When a scheduled Universal Deployment event has occurred.
<b>Scheduled Event, Update Firmware</b>	When an Update Firmware event has occurred.
<b>User Logon/Logoff</b>	When a user logs on or logs off the Avalanche Console.
<b>User modifications</b>	When a user account is modified.
<b>VLACL modifications</b>	When the VLACL is modified.
<b>Console to Device Server Events</b>	When servers are managed from the Console.

#### To enable audit logging:

- 1 Click **Tools > Settings**.

The System Settings page appears.

- 2 In the Audit Logging section, The Audit Logging Setting is displayed as either **Enabled** or **Disabled**. Click the setting to configure audit logging.
- 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 **Save**.

### 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 tracks 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. Only an administrator user can configure and view the audit log.

---

**NOTE:** For information about enabling and configuring the audit log, see [Configuring Audit Logging](#).

---



You must enable the audit log before you can view it. When viewing the audit log, select criteria you want the server to filter log-retrieval with, allowing Avalanche to retrieve the entire log or just the entries that pertain to the specified criteria.

To view the audit log:

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

The Audit Log page appears.

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

- 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 **Username** and select the username from the drop-down menu.

- 3 Click **Apply Filters** 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 General System Settings

From the Web Console, you can configure general settings for Avalanche, including allowing profile application, session timeout length, alert settings, message backlog limit, server-to-server restrictions, and localization settings.

---

**NOTE:** For information on configuring integrated logon for the Avalanche Console, see [Configuring Integrated Logon](#).

---

To configure general system settings:

- 1 Click **Tools > Settings**.

The System Settings page appears.

- 2 Modify the settings as desired:



- If you don't want profiles to be applied at the Home location, enable the **Disallow profile application at root level** option. This option will only be available to administrators.
- If you want to configure the length of time before an inactive Web Console user is logged off, or how often the page refreshes, type the number of minutes in the appropriate text box under **Web Settings**. The settings will only affect the Console for the user who configures them.
- If you want to configure how many days an alert is displayed, how many alerts are displayed, or how many alerts are stored in the database, type the appropriate numbers in the text boxes under **Alert Settings**. The alert display settings will only affect the Console for the user who configures them. The **Number of alerts to store** option will only be available to administrators.
- If you want to configure the maximum threshold for enterprise server messages allowed in the backlog, type the number of messages in the text box under **Message backlog**. If the spillover threshold is reached, the device servers are throttled and further messages are stored in a file to disk until the backlog is reduced. When device servers are throttled, they will no longer send device statistics updates to the enterprise server. After the backlog has been reduced, messages are pulled from the store file back into the log and the device servers are no longer throttled.
- If you want to enable or configure audit logging, click on the status and enable the desired options. For more information on audit logging, see [Configuring Audit Logging](#).
- If you want to change the **Language** used in the Avalanche Console, use the drop-down list to select the desired option. This setting will only affect the Console for the user who configures it. You must have the language package installed in order to select a language other than English.

The language package can be downloaded from the Wavelink Web site. Install the language package on the same computer as the enterprise server and the installed language option will appear in the **Language** drop-down list. For instructions on installing a language package, see [Installing Language Support](#).

- If you want to change the **Time Zone** used for the Console, use the drop-down list to select the desired option. This setting will only affect the Console for the user who configures it.

3 Click **Save** to save your changes.



## 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 System Settings page appears.

- 2 Click the **Email Settings** button.

The *Email Settings* dialog box appears.

- 3 Type the location of the e-mail server you want Avalanche to use in the **E-Mail server** text box.
- 4 Type the **Username** and **Password** in the text boxes.
- 5 Type the address a reply should be sent to if an alert e-mail is replied to in the **Reply-to email address** text box.
- 6 Type the address the e-mails will appear from in the **From email address** text box.
- 7 Select the port Avalanche should use when contacting the e-mail server.
- 8 Click **Save** to save your changes.

## Setting a System Message

The amcadmin user account has the option to set a system-wide message for all Web Console users. The message appears on the login screen and an icon appears at the top of the Console next to the alerts. When users click on the icon, a dialog box appears, displaying the system message.

To set a system-wide message for the Web Console:

- 1 Click **Tools > Settings**.

The System Settings page appears.

- 2 In the System Messages area, type the message in the text box.
- 3 Click **Save**.

The message will be displayed for all Web Console users.



## Creating Links in the Tools Menu

Add custom links in the Tools menu to provide easy access to other pages. When you create a link in the Tools menu, provide the text for the link and the URL to the desired page. This option is only available for administrator users.

To create a new link in the Tools menu:

- 1 Click **Tools > Support**.
- 2 In the Custom Tools Links panel, click **Add**.  
The *New Custom Tools Link* dialog box appears.
- 3 Type the name of the link that will appear in the Tools menu in the **Link Name** text box.
- 4 Type the full URL for the page in the **Link URL** text box. For example:  
`http://www.wavelink.com/`
- 5 Click **Add** to close the dialog box.
- 6 Click **Save**.

The link will appear in the custom links section of the **Tools** menu.

## Restricting Server-to-Server Communication

From the Web Console, you can suspend or throttle communication between the enterprise server and device servers. When communication is suspended, the device servers are not allowed to contact the enterprise server until the connection is resumed. When communication is throttled, the device servers will no longer send device statistics updates to the enterprise server. This reduces network traffic, but still allows for profiles and alerts to be sent and received.

You also have the option of releasing device servers from communication suspension in a gradual manner. With the **Gradual Resume** option, you can set the device servers to re-establish contact with the enterprise server on a staggered basis. Only a set number of servers will be allowed to reestablish contact each interval.

Communication suspension or throttling is available for all Mobile Device Servers, all Infrastructure Servers, or all device servers.

To configure server-to-server communication:

- 1 Click **Tools > Settings**.

The System Settings page appears.



- 2 In the Global Server-to-Server Communications panel, enable the checkbox next to the type of server you want to configure.
- 3 Select the action you want to perform:
  - If you want to suspend all communication between the selected device servers and the enterprise server, click **Suspend**.
  - If you want to release communications for the selected device servers, click **Resume**.
  - If you want to release communications for the selected servers in a gradual manner, click **Gradual Resume**. In the **Gradual Resume** dialog box that appears, enter the number of seconds in each interval and the number of servers allowed to re-establish contact during that interval.
  - If you want to throttle all communication between the selected device servers and the enterprise server, click **Limit**.
  - If you want to release the communication throttle, click **Release**.

## 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 **Tools > Check For Updates**.

The Check for Avalanche Updates page appears.

- 2 Click **Check for Updates**.

The *Check for Updates* dialog box appears.

- 3 Click **Accept** to allow Avalanche to send system and device information to Wavelink.
- 4 Updates for installed software appear in the Available Updates panel. Click the link to download the new version.

## Installing Language Support

The Web Console can be set to use languages other than English when you have installed a language support pack on the computer where Tomcat is running. See the Wavelink Web site for information on which languages are available.



To install an Avalanche language support pack:

- 1 Download the language support pack from the Wavelink web site.
- 2 Double-click the file to run the installer on the computer where Tomcat is running. (This is generally where the enterprise server is installed.)

The *InstallShield Wizard* appears.

- 3 Click **Next** to continue the installation process.
- 4 The language support pack is installed. Click **Finish** to close the installer.

Once you have installed the language support, you can configure the Web Console on a per-user basis to use the desired language. For information on configuring the Web Console to use an installed language, see [Configuring General System Settings](#).





## Chapter 3: 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](#)
- [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:

**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 page appears.



- 2 In the Users panel, click **New**.
- 3 The *Create User* dialog box appears. Click on the type of user you want to create.
- 4 The User Management page appears. Configure the settings for the user. **Login, Type, User Home, Password,** and **Confirm Password** are required fields.
- 5 Assign permissions now or an Administrator can modify permissions later.
- 6 Save your changes.

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 page appears.
- 2 In the Users panel, click **New**.
- 3 The *Create User* dialog box appears. Click **User Group**.  
The New User Group page appears.
- 4 Configure the settings and permissions for the group. **Group Name, Type,** and **User Home** are required fields.
- 5 In the Group User List panel, select the check boxes next to the names of the users who will be assigned to the user group.



- 6 Select the options in the Permissions panel to determine what users will have permissions for. Each user assigned to the group will have access for all group permissions as well as the permissions assigned for his user account. For more information about permissions, see [Assigning User Permissions](#).
- 7 Save your changes.

To view the users in a user group:

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

The User Management page appears.

- 2 In the Users panel, click the name of the user group you want to view.

The users assigned to the group are listed in the Group User List panel.

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

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

The User Management page appears.

- 2 In the Users panel, click the name of the user you want to view.

The user groups the user is assigned to are listed just above the Permissions panel.

## 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 page. 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		
<b>View</b> allows the user to view the settings for a profile.	<b>Edit</b> allows the user to edit the settings of a profile.	<b>Print</b> allows the user to print the barcodes for a Scan to Config profile.	<b>View</b> allows the user to view where profiles are applied.	<b>Edit</b> 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				
Infrastructure	<b>View</b> allows the user to view the infrastructure inventory for assigned locations.	<b>Manage</b> allows the user to manage the infrastructure inventory for assigned locations.	<b>Reset</b> allows the user to reset infrastructure devices.	<b>Site</b> allows the user to launch and use the Infrastructure Site Tool.
Mobile Devices	<b>View</b> allows the user to view the mobile devices for assigned locations.	<b>Manage</b> allows the user to manage the mobile devices for assigned locations or mobile device groups.		
Mobile Device Groups	<b>View</b> allows the user to view the mobile device groups and the devices they contain.	<b>Edit</b> allows the user to edit group properties for mobile device groups. A user must also have Mobile Devices permissions in order to view/edit the devices in a group.		
Mobile Device Properties	<b>View</b> allows the user to view mobile device properties.	<b>Edit</b> allows the user to edit properties for mobile devices.		
Remote Control	<b>View</b> allows the user to connect to a mobile device using Remote Control.	<b>Edit</b> 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	<b>View</b> allows the user to view location configurations and <b>Edit</b> allows the user to view, manage, and configure locations.



Other		
	settings.	
Synchronization	<b>View</b> allows the user to view recent and scheduled deployments.	<b>Edit</b> 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 Navigate to the location and click the Locations context link.
- 2 In the Authorized Users panel, click **Assign**.

The *Authorized Users* dialog box appears.

- 3 Select the user/group from the drop-down list.
- 4 Click **Save**.

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 The Profile Details page appears.
- 3 Add or remove users in the Authorized Users panel.
  - To remove an authorized user, select the check box next to the username and click **Remove**.
  - To add a user click **Assign**. In the *New Authorized User* dialog box, select the user and permission level from the drop-down lists and click **Save**. Only users who have permission for the current location will appear in the list.

## 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 **Inventory** tab, click on the name of the group you want to assign an authorized user to.

The Mobile Device Group Details page appears.

- 2 In the Authorized Users panel, click **Assign**.

The *New Authorized User* dialog box appears.

- 3 From the drop-down list, select the user and click **Save**. Only users who have permission for the current location will appear in the list.

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 > Settings.
- 2 In the Authentication Options panel, select from the following options:
  - Enable the **Active Directory through Wavelink CES** option.
  - Enable the **LDAP** option and then type the address of the LDAP server in the text box.
- 3 Click **Save**.
- 4 Log out of the Console.

Avalanche is now configured to recognize authenticated system users.

## 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 page appears.
- 2 Enable the check box next to the name of the user from the Users panel and click **Delete**.
- 3 Confirm you want to remove the user account.

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



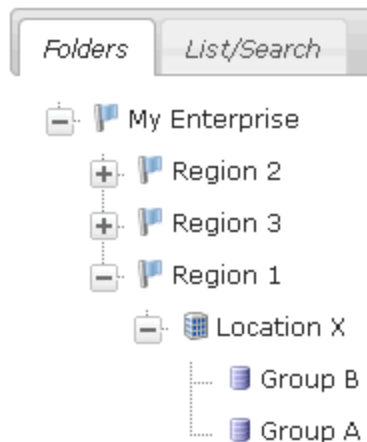


## Chapter 4: Location Management

Avalanche uses locations in order to organize devices, users, and settings. Avalanche divides locations into three main categories: region locations, server locations, and group locations. Locations are organized in the Location View, which can be accessed by clicking the Location View button:



*Location View button*



*Folders tab of the Location View*

A server location is the basic component of the Avalanche system. Each server location contains at least one mobile device or infrastructure server. You can define a server location in a way that best suits your network administration processes—for example, you can create server locations by geographic location or by network role.

A collection of one or more server locations is called a region. When you apply configurations to a region, the configurations are applied to every server location within that region. Regions allow you to manage settings for multiple server locations simultaneously.

For each server location, you also have the option of creating group locations. A group location is a group of devices that connect to the same server. Devices can be added to a group location using selection criteria. 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. For example, if Group A has the selection criterion: `ModelName = ITCK30`, any Intermec CK30 devices automatically appear in the Group A 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 Regions](#)
- [Managing Server Locations](#)
- [Managing Distributed Servers](#)
- [Managing Group Locations](#)
- [Applying Profiles to Locations](#)
- [Editing Exclusions](#)

## Managing Regions

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

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

This section provides information about the following:

- [Creating Regions](#)
- [Viewing Region Properties](#)
- [Deleting Regions](#)

## Creating Regions

Regions group together server locations that share similar characteristics. Regions can be nested inside of other regions.

When a profile is applied to a region, it is also applied to, or inherited by, all the associated sub-locations. A user with read/write permissions for a location has the option of excluding an



inherited profile for his location so it is not used, but he cannot change the priority of an inherited profile.

To create a region:

- 1 From the **Locations** tab, click **New** in the Sub-locations panel.

-Or-

Use the Location Tree to navigate to the region where you want to create the new region and click the **Locations** context link. In the Sub-locations panel, click **New**.

- 2 In the *New Subordinate Location* dialog box, click **Region**.

The New Region page appears.

- 3 Type a name for the new region in the text box, and configure the latitude, longitude, and notes if desired. If you prefer to click the location on a map rather than provide the latitude and longitude, click the **Use map to plot** button.
- 4 Save your changes.

## Viewing Region Properties

Once you create a region, you can view the properties of that region. Region properties include latitude and longitude, inventory information, applied and inherited profiles, alerts, floorplans, sub-locations and authorized users.

To view region properties:

- Navigate to the region and select the **Locations** context link.

The Location Summary panel displays the properties for the selected region.

## Deleting Regions

You can delete unused regions from the Avalanche Console at any time. Any server locations within a region are automatically moved to the **Deleted Server Locations** region when you delete that region.

---

**NOTE:** Deleting a region is permanent. There is no way to retrieve deleted regions.

---

To delete a region:

- 1 Navigate to the region directly above the region that you want to delete and click the **Locations** context link.
- 2 In the Sub-locations panel, select the check box next to the region you want to delete and click **Delete**.



- 3 The region is deleted and any server locations in that region are moved to the **Deleted Server Locations** folder.

---

**NOTE:** You can restore server locations that are in the deleted Server Locations region to the Unassigned Server Locations region. For more information about restoring deleted server locations, see [Deleting Server Locations](#).

---

## Managing Server Locations

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

---

**NOTE:** The number of wireless components managed at a server location depends on the communication range of the servers installed at that location. Traditionally, this range has been defined as a single subnet on your network; however, depending on your network architecture, you can configure a server to communicate past a given subnet. This type of configuration uses the Infrastructure Site Tool. See [Configuring Infrastructure Servers at the Server Location](#) for more information on using the Infrastructure Site Tool.

---

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

- [Determining Server Placement](#)
- [Adding Server Locations](#)
- [Moving Server Locations to Regions](#)
- [Modifying Server Location Properties](#)
- [Deleting Server Locations](#)

To view the properties of an existing server location, click the **Locations** tab and navigate to the location.

### Determining Server Placement

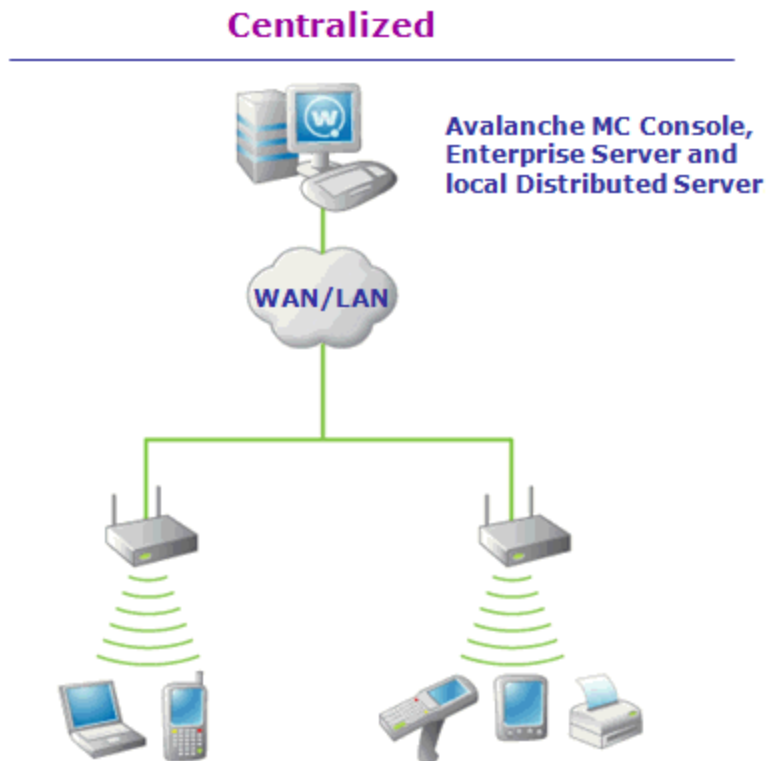
Spacing your device servers correctly is an important task. The ability to manage your wireless network depends on servers being able to locate and communicate with your devices. There are two primary methods of installing servers: centralized and distributed.

#### Centralized Server Method

In centralized server installations, a single server location is responsible for managing all of the devices on the network. Centralized server installations are typically found in environments where specific locations within a network might be unable to support their own servers. An



example of this environment is a collection of retail stores. While the headquarters for these stores can support an infrastructure server, it might not be possible for each individual store to have its own server. In this case, installing the server centrally is an ideal solution.



*A Centralized Installation of Avalanche (Simplified)*

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

- You must know the network subnets to ensure the server knows where to listen for infrastructure broadcasts.
- You must know what switches and routers reside between the server and devices. This is particularly helpful if troubleshooting becomes necessary.
- You must have a general understanding of the overall performance of the wireless network, to ensure that specific time-based features (such as WEP key rotation) are configured correctly.
- Should organizational needs change, a centralized installation of Avalanche can be modified to a distributed model without needing to uninstall or reinstall Avalanche.

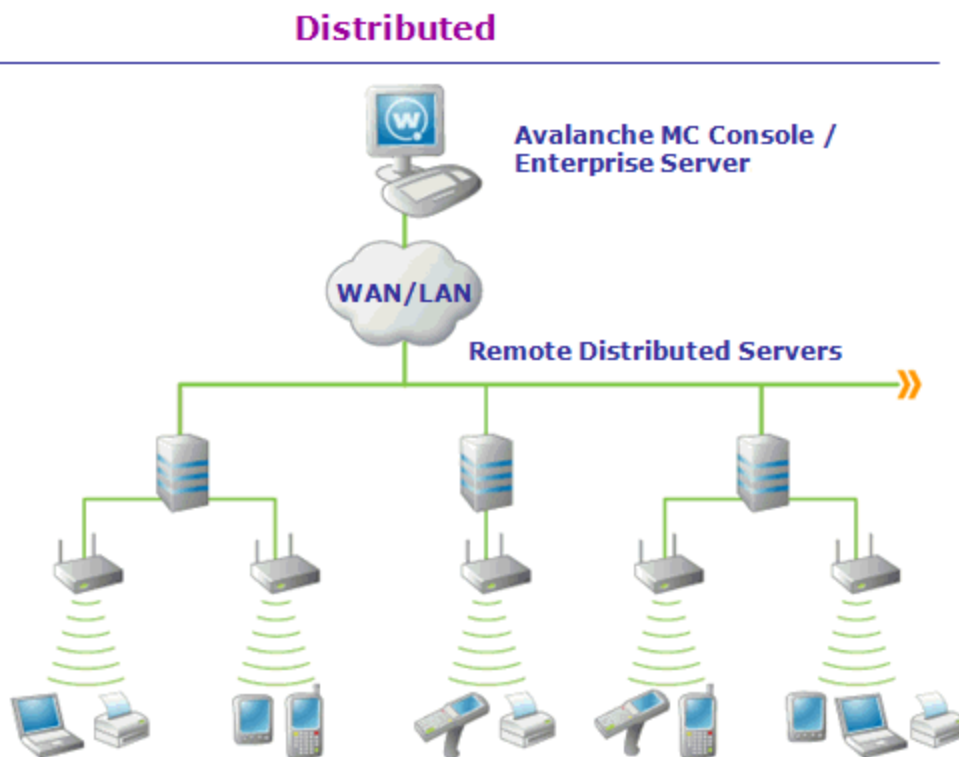


## Distributed Server Method

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

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

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



*A Distributed Installation of Avalanche (Simplified)*

For information about how to deploy servers, see the Java Console help.



## Adding Server Locations

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

<b>Location Name</b>	Name of the new server location.
<b>Hide inherited profiles and device groups</b>	Any inherited profiles or device groups are not displayed for the location.
<b>IP Address or hostname</b>	IP address of the server location.
<b>OS Platform</b>	The operating system of the computer where the server will be installed.
<b>Name</b>	The city where the server will reside. This allows Avalanche to plot the server location on its map. When you provide a city name, Avalanche will attempt to connect to a database on the Wavelink web site to find cities with that name.
<b>State</b>	The state where the server will reside.
<b>Country</b>	The country where the server will reside.
<b>Latitude and Longitude</b>	The coordinates of the server location.
<b>Time Zone</b>	The time zone for the area where the server resides. If servers are in different time zones, this can affect deployment schedules.
<b>Admin user</b>	The username for an account that has administrative access to the computer where the server will be installed. The user must have full control for the shared folder.
<b>Admin Password</b>	The password for the user account.
<b>Domain</b>	The domain for the user account.



- Share Name** The name of a shared folder on the computer where the server will be installed. The user must have full control for this folder. This folder must be created and shared access allowed before you attempt to deploy a server to the server location or the deployment will fail.
- Share Path** The path for the shared folder. This path is NOT the network path (such as `\\system1\deploy\`), but is the local path to the shared folder (such as `c:\deploy\`).

#### To add a server location:

- 1 Navigate to the region where you will put the server location and click the **Locations** context link.
- 2 In the Sub-locations panel, click **New**.
- 3 In the *New Subordinate Location* dialog box, click **Server**.

The New Server Location page appears.

- 4 Configure the options as desired. If you prefer to plot the location on a map rather than provide the latitude and longitude, click the **Use map to plot** button. When you are finished, click **Save**.

The server location appears in the region where you created it. You can assign the server location to a different region, deploy servers to the server location or modify the server location. For information on deploying servers, see the Java Console help.

## Moving Server Locations to Regions

You may need to move an existing server location if you want to restructure your network hierarchy. A server location must belong to a region before you can manage its settings.

---

**NOTE:** If you want to move a server location from the Deleted Locations or the Unassigned Locations regions, you must use the Java Console.

---

#### To move a server location to a region:

- 1 Navigate to the server location you want to move and click the Locations context link.
- 2 In the location details area, click **Move**.

The Choose Location dialog box appears.

- 3 Select the region you want to move the location to.

The server location is moved to the new region.





## Modifying Server Location Properties

Once you have created a server location, you can modify the server location properties.

To modify server location properties:

- 1 Navigate to the server location you want to edit and click on the **Locations** context link.
- 2 Click **Edit**.
- 3 Edit the information as needed.
- 4 Save your changes.

## Deleting Server Locations

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

From the Deleted Server Locations region you can remove the server location completely or restore the server location so that you can manage it. When you remove server locations from the Deleted Server Locations region, the server location and historical data are completely deleted from the databases. When a server is restored, it is moved to the Unassigned Server Locations region until you move it to the desired region.

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

- 1 Navigate to the region directly above the location that you want to delete and click the **Locations** context link.
- 2 In the Sub-locations panel, select the check box next to the location you want to delete and click **Delete**.

---

**NOTE:** To restore or completely delete a server location, you must use the Java Console.

---

You can stop the device server and then delete the server location. However, if you start the server again, Avalanche will automatically detect the deleted server location and place it in the Unassigned Server Locations region. Wavelink recommends uninstalling servers completely before deleting server locations. See the Java Console help for information on uninstalling servers.

Unassigned server locations will download the default profiles but do not get any other profile settings and do not receive updates such as server settings, software packages, or infrastructure profiles. Mobile devices will not connect to unassigned server locations. Server



locations restored from the Deleted Server Locations region to the Unassigned Server Locations region retain their last configuration.

## 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](#)
- [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 Navigate to the server location where you want to place the group location and click the **Locations** context link.
- 2 In the Sub-locations panel, click **New**.
- 3 The *New Subordinate Location* dialog box appears. Click **Group**.

The New Group Location page appears.

- 4 Configure the options as desired. If you prefer to plot the location on a map rather than provide the latitude and longitude, click the **Use map to plot** button. When you are finished, click **Save**.
- 5 If you do not want inherited profiles and device groups to be visible, enable the **Hide inherited profiles and device groups** option.
- 6 Click **Save**.



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

## 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 servers. 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 (region, server, or group), it is also applied to any sub-locations and their servers and 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 Navigate to the location where you want to apply the profile and click the **Profiles** context link. In the Available Profiles panel, select the check box next to the name of the profile you want to apply and click **Apply**.

The Applied Profile page appears. Any **Profile Selection Criteria** are displayed in the list. (These are the selection criteria used for the profile.)

- 2 If you want to use additional selection criteria for the profile at this specific location, type them in the **Application Selection Criteria** text box or click **Launch wizard** to use the Selection Criteria Builder.



- 3 Click **Apply** to apply the profile without deploying it. If you want to schedule a server synchronization for the location, click **Schedule Synchronization** and select the desired synchronization options.

---

**NOTE:** You can also apply a profile to a location from the Profile Details page. From the **Profiles** tab, click the name of the profile you want to apply. In the Applied Locations panel, click **New** and select the location you want to apply the profile to. When you use this method, you do not have the option to use additional selection criteria.

---

To view where a profile has been applied:

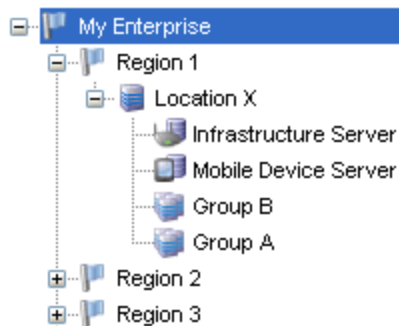
- From the **Profiles** tab, click the name of the profile you want to view.

The home location for the profile appears in the profile details. You can also view the locations where the profile has been applied in the Applied Locations panel.

## 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 Region 1, the profile will also be excluded from Location X and Groups A and B.

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 A that has been excluded at Region 1. (It would still be excluded at Group B.)



To exclude an inherited profile:

- 1 Navigate to the location where you want to exclude a profile and click the **Profiles** context link.
- 2 In the Applied Profiles panel, locate the profile you want to exclude and click **Included** in the Excluded column for that profile.

The status of the profile will change from **Included** to **Excluded** and the profile information will be grayed out.

- 3 To reapply an excluded profile, click **Excluded** in the Applied Profiles panel.



## Chapter 5: 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** panel 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 Scheduled Settings](#)

### 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 **New Profile**.

The *New Profile* dialog box appears.

- 2 Select **Network Profile**.

The New Profile Details page appears.

- 3 Type a name for the profile in the **Name** text box.

- 4 If desired, enable the profile or set the profile to override any manual settings on the mobile device. If the profile is configured to override, it overrides each time the device connects.



- 5 Click **Launch wizard** to use the Selection Criteria Builder to determine which devices the network profile manages. For details about using selection criteria, see [Using Selection Criteria](#).
- 6 To add a mobile device IP address pool, click **Edit**.

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 left. This list will display all entered addresses.

- Click **Save** to return to the New Profile Details page.

- 7 If desired, type any **Notes** in the text box.
- 8 If you want the profile to manage WLAN IP, WLAN, or WWAN settings, enable the appropriate check box. When the boxes are enabled, the related panels appear below. For information on the options in these panels, see [Configuring Scheduled Settings](#).
- 9 Click **Save**.

The network profile is created and can be configured further or assigned to a location.



## 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:

**Server Address** 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.

If using a DNS name, click **Validate** to ensure the address can be resolved. If the mobile device profile has provided a server address, that address will override whatever is provided by the network profile.

**Gateway** 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.

**Manage DNS** Allows the profile to manage DNS options for the devices.





<b>Domain Name</b>	Provides the domain name to the devices.
<b>Primary</b>	Provides mobile devices with the IP address for a primary DNS.
<b>Secondary</b>	Provides mobile devices with the IP address for a secondary DNS (used if the primary DNS is unavailable).
<b>Tertiary</b>	Provides mobile devices with the IP address for a tertiary DNS (used if the primary and secondary DNS are unavailable).
<b>Manage IP Assignment</b>	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.
<b>Manage IP Assignment (Infrastructure Device Settings)</b>	Allows you to manage the IP addresses assigned to your infrastructure devices with a DHCP server.

[To configure current WLAN IP settings:](#)

- 1 From the Available Profiles panel on the **Profiles** tab, click on the network profile you want to edit.

The Network Profile Details page appears.

- 2 Click **Edit**.

The Edit Network Profile page appears.

- 3 Enable the **Manage WLAN IP** checkbox.

The WLAN IP Settings panel appears.

- 4 Configure the WLAN IP settings as desired.

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

[To configure scheduled changes for WLAN IP settings:](#)

- 1 From the Available Profiles panel on the **Profiles** tab, click on the network profile you want to edit.

The Network Profile Details page appears.

- 2 In the Scheduled Profile Changes panel, click **New**.

- 3 Select the **Start Date** and **Time** that you want the settings to take effect and configure the scheduled settings as desired.

- 4 Click **Save**.



The changes are applied at the scheduled time.

## 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:

**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.

**WPA(TKIP) + WPA2(AES).** 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 **defined**, 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.

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

To configure current WLAN settings:

- 1 From the Available Profiles panel on the **Profiles** tab, click on the network profile you want to edit.

The Network Profile Details page appears.

- 2 Click **Edit**.

The Edit Network Profile page appears.

- 3 Enable the **Manage WLAN** checkbox.

The WLAN Settings panel appears.

- 4 Configure the WLAN settings as desired. If you select 128-bit WEP, WPA, or WPA2 encryption, you can enable the **Use authentication** check box to select the type of authentication to use.
  - 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, choose the 40- or 128-bit key size, the starting date and time, rotation interval, and a passcode.
  - If you are using a pre-shared key with WPA or WPA2, type the passphrase or hex key in the **Key** text box. Use the **Broadcast key rotation interval** option to set how often the key is rotated.
  - If you select PEAP or TTLS authentication, enable the **Validate Server Certificate** check box to provide a path to the certificate.



- If you select EAP\_FAST, provide a path and password to a PAC (Protected Access Credential) file. This will provision devices with the PAC file.
- If you are an authentication method, 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 the encryption method you have selected.

---

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

To configure scheduled changes for WLAN settings:

1 From the Available Profiles panel on the **Profiles** tab, click on the network profile you want to edit.

The Network Profile Details page appears.

2 In the Scheduled Profile Changes panel, click **New**.

3 Select the **Start Date** and **Time** that you want the settings to take effect and configure the scheduled settings as desired.

4 Click **Save**.

The changes are applied at the scheduled time.

## 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.



<b>Custom Properties</b>	This option allows you to add custom properties to the devices that receive this network profile. By clicking <b>Edit/View</b> , you can add, edit, and delete properties and their values.
<b>Enable TCP/IP header compression</b>	Improves the performance of low-speed connections.
<b>Enable software compression</b>	Improves the performance of low-speed connections.
<b>Activate phone as needed</b>	Allows the Enabler to activate the device's phone if a WWAN connection is necessary.
<b>Dial broadband connection as needed</b>	Allows the Enabler to attempt a WWAN connection if a LAN connection cannot be established.
<b>Public address for Avalanche Server</b>	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 current WWAN settings:

- 1 From the Available Profiles panel on the **Profiles** tab, click on the network profile you want to edit.  
The Network Profile Details page appears.
- 2 Click **Edit**.  
The Edit Network Profile page appears.
- 3 Enable the **Manage WWAN** checkbox.  
The WWAN Settings panel appears.
- 4 Configure the WWAN settings as desired.
- 5 Click **Save** to save your changes.



To configure scheduled changes for WWAN settings:

- 1 From the Available Profiles panel on the **Profiles** tab, click on the network profile you want to edit.

The Network Profile Details page appears.

- 2 In the Scheduled Profile Changes panel, click **New**.
- 3 Select the **Start Date** and **Time** that you want the settings to take effect and configure the scheduled settings as desired.
- 4 Click **Save**.

The changes are applied at the scheduled time.



## Chapter 6: 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 **New Profile**.

The *New Profile* dialog box appears.

- 2 Select **Scan-to-Config Profile**.

The New Profile Details page appears.

- 3 Type a name for the profile in the **Name** text box.





- 4 To encrypt the barcodes, type a passcode in the **Encryption Passcode** text box and confirm it in the **Confirm Passcode** text box. 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.
- 5 Set the maximum barcode length. This defines how many characters are encoded in each barcode.
- 6 If you have already configured a network profile and want to use the settings from that profile, enable **Use settings from network profile** and select the network profile from the drop-down list. Enable **Use current profile setting** to use the current settings or, if the network profile has multiple scheduled settings, enable **Use scheduled profile change effective** and select an epoch from the drop-down list.
- 7 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.
- 8 If desired, type any notes in the **Notes** text box.
- 9 Click **Save**.

The profile is created and appears in the Profiles tab. To edit the configuration, click on the name of the profile and click **Edit** on the Profile Details page.

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** panel 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](#).

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



## 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, click on the name of the profile you want to configure.
- 2 Click **Edit**.
- 3 In the Properties panel, click **New**.

The *New 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 **Add**.
- 7 Click **Save**.

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

## 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, click on the name of the profile you want to configure.

The Profile Details page appears.

- 2 Click **Edit**.
- 3 The Edit Profile page appears.
- 4 In the Registry Keys panel, click **New**.

The *New Registry Entry* dialog box appears.

- 5 Select the **Root** from the drop-down list.



- 6 Type the name of the key in the **Key** text box.
- 7 Type the value entry of the key in the **Name** text box.
- 8 Enter the data for the value entry in the **Data** text box.
- 9 Select the **Type** of the value from the drop-down list.
- 10 Select **Create key** as the **Action**.
- 11 Click **Add** to add the registry key and value to the list.
- 12 When you are done, click **Save**.

The key and value are saved to the profile.

## 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. The Avalanche Web Console prints the barcodes to a .pdf file which you can save or send to a printer.

To print a Scan to Config profile as a barcode:

- 1 From the **Profiles** tab, click on the name of the Scan to Config profile you want to configure.

The Scan to Config Profile Details page appears.

- 2 Click **Print Barcodes**.

The `scanToConfig.pdf` appears. You can print or save this file.

## 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 7: Managing Infrastructure Devices

Infrastructure devices can be managed through the Infrastructure Inventory. This panel displays a list of infrastructure devices and details about them. You can page through or filter the devices displayed in the list. For information on paging through or filtering the list, see [Panels](#).

The device list in the Infrastructure Inventory shows a set or subset of infrastructure devices based on the currently selected location. When you select a particular location, the devices that are associated with that location appear in the list. The following information is provided for each device:

<b>Name</b>	The official name of the device.
<b>Model</b>	The model of the device.
<b>Type</b>	The type of infrastructure device.
<b>Group</b>	The group location the device is associated with. If the device is not associated with a group location, this column will default to the server location.
<b>Version</b>	The version of firmware currently running on the device.
<b>IP Address</b>	The IP address of the device.
<b>Last Contact</b>	The last time the device was in contact with the infrastructure Server.
<b>Status</b>	Indicates the current status of the device.
<b>Up</b>	A green circle with a check indicates that the device is up and running. A red X indicates there is an issue with the device.
<b>Mobile Devices</b>	Indicates whether the profile assigned to the device is composite.
<b>Notes</b>	Lists any notes users have saved for the device.

View the details of an infrastructure device by clicking its name. The Device Details page lists the properties of a device, the profiles applied, and any related switches or access points.

---

**NOTE:** Infrastructure devices are added using the Infrastructure Site Tool. In addition to devices using [Supported Firmware](#), Avalanche can manage devices that conform to the MIB-

---



---

II standard as generic devices. Generic devices will have limited support or information available.

---

You can perform the following tasks to manage infrastructure devices:

- [Querying an Infrastructure Device](#)
- [Pinging an Infrastructure Device](#)
- [Resetting Access Points](#)
- [Deleting Infrastructure Devices](#)
- [Mapping Infrastructure Devices on a Floorplan](#)

---

**NOTE:** All tasks except viewing related devices are available for both switches and access points.

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

---

**NOTE:** To update firmware, manage Infrastructure Server profiles or infrastructure profiles, you must use the Java Console.

---

## Querying an Infrastructure Device

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

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

**To query a device:**

- 1 Enable the check box to the left of the desired device in the Infrastructure Devices panel.
- 2 Click **Query**.

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



## Pinging an Infrastructure Device

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

---

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

---

To ping a device:

- 1 Enable the check box to the left of the device in the Infrastructure Devices panel.
- 2 Click **Ping**.

The Status column will indicate whether the device could be reached.

## Resetting Access Points

There are two options for resetting access points: a normal reset that reboots the device and a reset to factory settings.

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

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

---

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

---

To reboot an access point:

- 1 Enable the check box to the left of the desired device in the Infrastructure Devices panel.
- 2 Click **Reboot**.

The **Status** column will indicate the state of the device.

To reset an access point to its factory defaults:

- 1 In the Infrastructure Devices panel, click the name of the device you want to reset.  
The Device page appears.
- 2 In the Tools panel, click **Reset Factory**.



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

- 3 Click **Yes**.

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

## Deleting Infrastructure Devices

You can delete devices from the Infrastructure Inventory. This removes the device from the Infrastructure Devices panel and releases the license that device was using. After a device is deleted and the infrastructure server updated, the device will disappear from the inventory. However, if the device is still connected to the network, then it may be immediately rediscovered.

From the Java Console, you also have the option to exclude an infrastructure device. When a device is excluded, it will be permanently removed from the Infrastructure Inventory. An excluded device will not be rediscovered. For more information, see the Java Console User Guide.

To delete a device:

- 1 In the Infrastructure Devices panel, enable the check box to the left of the device you want to delete.
- 2 Click **Delete**.

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

- 3 Select **Yes**.

The device will disappear from the inventory the next time the infrastructure server is updated.

## Mapping Infrastructure Devices on a Floorplan

With the Web Console, you can import floorplans, plot where your infrastructure devices are located, and view radio coverage and associated mobile devices on the map. You can have multiple floorplans and associate an infrastructure device with more than one floorplan.

---

**NOTE:** You must have a statistics server running and your devices must be reporting statistics in order for Avalanche floorplans to function effectively.

---

This section contains information on the following tasks:

- [Importing a Floorplan](#)
- [Plotting Infrastructure Devices](#)





- [Adjusting the Floorplan Display](#)

## Importing a Floorplan

In order to view your infrastructure devices on a floorplan, you must first import the image of your floorplan. The floorplan will be associated with a specific location. This floorplan will be saved in the enterprise database and be available to anyone using the Web Console.

The floorplan image you import must be in one of the following file formats: .jpg, .png, or .gif.

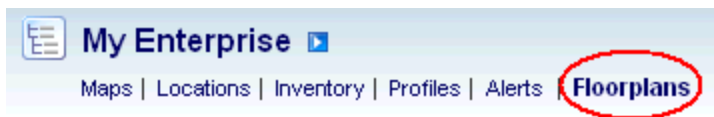
---

**NOTE:** You must have a Flash plug-in for your browser in order to import a floorplan.

---

To import a floorplan image:

- 1 Navigate to the location with which you want the floorplan associated and click the Floorplans context link.



*Floorplans Context Link*

- 2 In the Selected Floor Plan panel, click **New**.  
The New Floorplan Wizard appears.
- 3 Type a name for the floorplan in the **Floorplan Name** text box.
- 4 Click **Select** to navigate to the location of the floorplan image file. When you have selected the image file, click **Next**.

---

**NOTE:** You can use the same image file to create multiple floorplans with different device mapping.

---

The Set Floorplan Scale page appears.

- 5 Click on the image to set a start point and an end point for a known distance on the floorplan.
- 6 After the start and end points have been set, the **Enter actual distance** options appear. Use the text box and drop-down list to indicate how far apart the start and end points are. This will set the scale for the floorplan.
- 7 Click **Finish** to save the floorplan and its scale.

The floorplan appears in the Selected Floor Plan panel. Select the name of the floorplan from the drop-down list to view it.



## Plotting Infrastructure Devices

Once you have imported a floorplan, you can plot your infrastructure devices on the floorplan. This can give you a visual representation of where your devices are and what areas they cover. Avalanche automatically displays a list of infrastructure devices being managed that you can place on your floorplan.

To plot an infrastructure device on a floorplan:

- 1 From the Floorplans page, select the floorplan you want to edit from the drop-down list in the Selected Floor Plan panel.
- 2 In the Available Managed Infrastructure panel, click the Plot icon for the device you want to place on the floorplan.
- 3 The *Plot* dialog box appears. Place the device on the floorplan by clicking the appropriate location.

A device icon appears on the map.

## Adjusting the Floorplan Display

A floorplan can display the location of your infrastructure devices, their estimated radio range, and the associated mobile devices. The predicted radio range is an estimation that does not take physical obstructions into account. It is based on the radio type and power level reported by the device.

When associated mobile devices are displayed, they appear near the infrastructure device with which they are associated. The placement of the mobile device icon is not intended to be an accurate location of the mobile device; rather, the distance between the infrastructure icon and the mobile device icon demonstrate the possible range of the mobile device based on known signal strength and signal power statistics received from the devices.

The options for adjusting the floorplan display include:

**Infrastructure Devices** Displays plotted infrastructure devices on the floorplan.



<b>Predicted Coverage</b>	Displays the predicted coverage of infrastructure devices as a heatmap. You can select the type of radio range to be displayed. <ul style="list-style-type: none"><li>• 802.11a</li><li>• 802.11b</li><li>• 802.11g</li><li>• 802.11n</li><li>• 4.9 GHz</li><li>• Frequency Hopping</li></ul>
<b>Mobile Devices — Show managed</b>	Displays mobile devices being managed by Avalanche.
<b>Mobile Devices — Show unmanaged</b>	Displays mobile devices not being managed by Avalanche.
<b>Limit to Plotted Infrastructure Devices selected below</b>	Displays only those devices that have the check box next to their name in the Plotted Infrastructure panel enabled.

---

**NOTE:** If the current power level for a device is reported as 0, you will not be able to view predicted coverage for that device. The reported power level may be 0 if the device is disabled.

The following models do not reliably report the current power level: Proxim 2000, 4000, 4900, 600, 700, Dell TrueMobile 1170, HP ProCurve 520wl, Avaya AP-3, AP-4, AP-5, AP-6 and AP-8, SYSTIMAX AirSPEED AP 541 and AP 542.

If the **desired channel** on a Symbol/Motorola WS 2000 is set to 0, the power level will be reported as 0. The desired channel can be changed from the Infrastructure Site Console.

---

To adjust the floorplan display:

- 1 From the Floorplans page, select the floorplan you want to edit from the drop-down list in the Selected Floor Plan panel.
- 2 Enable the options to the left in the Selected Floor Plan panel.

The floorplan will display as configured.



## 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:

- [Creating and Configuring a Mobile Device Server Profile](#)
- [Viewing Mobile Device Server Licensing Messages](#)
- [Viewing Server Details](#)

Before you can manage a Mobile Device Server, you must create a server deployment package and deploy the server to the desired location. For information on creating a package and deploying it, as well as other server management tasks, see the Java Console User Guide.

### Creating and 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. A mobile device server profile can have its status set to enabled or disabled. The profile should be enabled before you can apply it. The home location for the profile is the location you have selected when you create the profile.

To create a mobile device server profile:

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

The *New Profile* dialog box appears.

- 2 Click **Mobile Device Server Profile**.

Type the name of the profile in the Name text box and configure the profile settings.



Configure the following settings for a mobile device server:

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

The **Authorized Users** panel 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.

## Server Resources

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

**Serial Ports reserved for management** 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.

**Restrict number of concurrent devices** Allows only the specified number of devices to update simultaneously.



## Terminal ID

A Mobile Device Server profile allows you to configure how terminal IDs are determined:

**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.

## Server Logging

A Mobile Device Server profile has the following logging settings:

**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.



## License Return

A Mobile Device Server profile has the following licensing options:

**Release 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 Server

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 Connection 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 Statistics

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:





<b>Device Chat Timeout</b>	Sets the amount of time in minutes that both the device and the server will wait before dropping a chat session.
<b>Device Comeback Delay</b>	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).
<b>Enable Device Caching</b>	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.
<b>Enable Persistent Connection</b>	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.
<b>Enable SMS Notification</b>	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.
<b>Suppress GPS Data Collection</b>	Causes the Mobile Device Server to discard GPS data collected from the devices rather than transmitting it to the enterprise server.
<b>Suppress Radio Statistics Collection</b>	Causes the Mobile Device Server to discard radio statistics data collected from the devices rather than transmitting it to the enterprise server.
<b>Suppress Realtime Properties Data Collection</b>	Causes the Mobile Device Server to discard realtime properties data collected from the devices rather than transmitting it to the enterprise server.
<b>Suppress Software Inventory Collection</b>	Causes the Mobile Device Server to discard software profile data collected from the devices rather than transmitting it to the enterprise server.



## Device Specific File Transfers

**Directory for files uploaded from device** 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.

**Directory for files downloaded to device** 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/exclusion window:

- 1 From the **Profiles** tab, click on the Mobile Device Server profile from the **Available Profile** panel.

The Mobile Device Server Profile Details page appears.

- 2 Click **Edit**.
- 3 If you want to create a server-to-server blackout window, click the **New** button in the Server-to-Server Communications Restrictions panel.

- Or -

If you want to create a device-to-server exclusion window, click the **New** button in the Device-to-Server Communication Restrictions panel.

The *New Blackout/Exclusion Window* dialog box appears.

- 4 Type the start and end time of the blackout window. Enable the boxes for the days you want the blackout to apply and click **Save**.

---

**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.

---



## 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:

<b>Event type</b>	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.
<b>Time Constraints</b>	Set the start time and, if desired, the end time for the event.
<b>Allow the mobile device user to override the update</b>	Creates a prompt when the update is scheduled to occur that allows the mobile device user to override the update.
<b>Delete orphaned packages during the update</b>	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.
<b>Force package synchronization during the update</b>	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, click on the Mobile Device Server profile from the **Available Profile** panel.

The Mobile Device Server Profile Details page appears.

- 2 Click **Edit**.
- 3 In the **Device Update Schedule** panel, click **New**.

The *New Device Server Update* dialog box appears.



- 4 Select the event type. If you select **Recurring Event**, determine whether the update occurs on either a daily or weekly basis. If you select **Weekly** from this list, you must also select the day on which the update occurs.
- 5 Set the start date and time.

---

**NOTE:** If you chose a post-synchronization event, the start and stop time options do not apply.

---

- 6 If desired, enable the **Stop if not completed by** option. Set the stop date and time. Selecting an end time is not required.
- 7 Enable the other update options as desired.
- 8 Click **Save**.

The update appears in the Device Update Schedule panel.

---

**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 deployed mobile device servers. You can view these messages from the System Support page. A user must be an administrator to access this page.

To view licensing messages:

- 1 Click **Tools > Support**.

The System Support page appears.

- 2 Next to **Mobile Device Server(s)**, click the **Details** button.

- 3 The *Mobile Device Servers* dialog box appears. Click the name of the server you want to view messages for.

The Mobile Device Server Details page appears.

## Viewing Server Details

This section provides information about viewing details for mobile device and infrastructure servers. For information on managing servers, see the Java Console Help.



To view server properties:

1 Click **Tools > Support**.

2 Next to the name of the server type, click **Details**.

The *Device Servers* dialog box appears.

3 Click the name of the device server you want to view properties for.

The Device Server Details page appears.



## 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** panel 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](#).

To create a software profile:

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

The *New Profile* dialog box appears.

- 2 Select **Software Profile**.

The New Profile Details page appears.

- 3 Type a name for the profile in the **Name** text box.

---

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

---

- 4 If desired, enable the profile now.



- 5 Click **Launch wizard** to use the Selection Criteria Builder to determine which devices the software profile will be applied to. For details about creating and using selection criteria, see [Using Selection Criteria](#).
- 6 Click **Save**.

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 panel on the Software Profile Details page 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.

---

In order to use package utilities to configure a package from the Web Console, you must have a current JRE installed on the computer where you are using the Web Console. Avalanche will download the utility to the local computer to allow you to configure the package, and then save your changes to the package in the Enterprise Server database.

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

Field	Description
Package Name	Displays the name of the software package.
Configure	Displays the date, time, and user for the most recent package configuration.
Status	Displays the enabled/disabled status of the software package.
Type	Displays the type of the software package. Software packages are divided into the following categories: <ul style="list-style-type: none"> <li>• <b>Control.</b> An internally used package specific to the Avalanche Console. A network profile is an example of a control package.</li> <li>• <b>Application.</b> These packages install an application which can be run from</li> </ul>



Field	Description
	<p>the Application Menu screen on the mobile device. An example of an application package is the Telnet Client.</p> <ul style="list-style-type: none"> <li>• <b>Support.</b> 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.</li> <li>• <b>Auto Run.</b> 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.</li> </ul>
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.

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.





---

**NOTE:** You must have a Flash plug-in for your browser in order to upload a software package. In order to use package utilities to configure a package from the Web Console, you must have a current JRE installed on the computer where you are using the Web Console.

---

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 From the **Available Profiles** panel on the **Profiles** tab, click on the software profile you want to edit.

The Software Profile Details page appears.

- 2 In the **Software Packages** panel, click **New**.

The Software Package Wizard appears.

- 3 Select **Install an Avalanche package**.

- 4 Click **Select Package** to browse to the location of the software package. When you have selected the file, click **Open**.

- 5 In the Software Package Wizard, click **Next**.

A License Agreement appears.

- 6 Accept the license agreement and click **Next**.

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

- 8 The Configure Software Package page appears. If desired, you can enable the package immediately.

- 9 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.



---

**NOTE:** You must have a Flash plug-in for your browser in order to upload files and create software packages.

---

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.

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

**Post Install Options** Options for if the device will perform a warm boot or a cold boot after installation has completed, or if a program runs once installation is completed. When you select 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 From the Available Profiles panel on the **Profiles** tab, click on the software profile you want to edit.

The Software Profile Details page appears.

- 2 In the Software Packages panel, click **New**.

The Software Package Wizard appears.

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

- 4 Click **Next**.

The Specify the Files in the Ad Hoc Package page appears.

- 5 Use the **Add File** button to navigate to and select the file you want to add to the package and click **Add**.

The file is added to the list.

- 6 Continue adding files as desired. When you have added all the files, click **Next**.



The Ad Hoc Package Options page appears.

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

The Add Selection Criteria to the Ad Hoc Package page appears.

- 8 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 **Launch Wizard** button is enabled. You can click it and use the Selection Criteria Builder to help you create the criteria, if desired.

---

- 9 Click **Next**.

- 10 The files will be prepared for installation on a device. When the package is complete, click **Next**.

The Configure Software Package page appears. This page allows you to enable the package immediately.

- 11 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 install .CAB or .MSI packages:

- 1 From the Available Profiles panel on the **Profiles** tab, click on the software profile you want to add the package to.

The Software Profile Details page appears.

- 2 In the Software Packages panel, click **New**.

The Software Package Wizard appears.

- 3 Select **Install an Avalanche Package** and browse to the location of the .CAB or .MSI file.

- 4 Click **Next**.

The CAB or MSI File Options page appears.

- 5 Type the name of the package.



- 6 If you want the package to be uninstalled once the program information is retrieved by the mobile device, enable **Remove after install**.
- 7 Click **Next**.
- 8 The files will be prepared for installation on a device. When the package is complete, click **Next**.

The Configure Software Package page appears. This dialog box allows you to enable the package immediately.

- 9 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 Available Profiles panel on the **Profiles** tab, click on the software profile you want to add the package to.

The Software Profile Details page appears.

- 2 In the Software Packages panel, click **New**.

The Add Device Software page appears.

- 3 Select **Copy a software package from a different profile** and choose the package you want to copy from the drop-down list. Click **Next**.

- 4 Choose whether the package is **Enabled** or **Disabled** and click **Finish**.

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, click the name of the software profile with the package you want to enable.

The Software Profile Details page appears.

- 2 In the Software Packages panel, click Disabled in the Status column for the package you want to enable.



The package is enabled.

## 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:** You must have a current JRE installed locally in order to use package configuration utilities.

---

To configure a software package using the included utility:

- 1 From the **Profiles** tab, click the name of the software profile with the package you want to configure.

The Software Profile Details page appears.

- 2 In the Software Packages panel, click **Configure** for the software package you want to configure.

---

**NOTE:** If you do not have Java installed locally, click **Install Java** in the Configure column. After installing Java, the **Configure** option will be available.

---

- 3 Depending on your browser and security settings, you may be prompted to trust the Wavelink certificate. If you are prompted to select the program to use for opening the file, choose **Java Web Start Launcher** from the list and click **OK**.
- 4 The *Configure Software Package* dialog box appears and the package utility is downloaded. Click **Next**.
- 5 Select the utility you want to use and click **Launch Config**.
- 6 The utility is launched. Configure the package options as desired.

---

**NOTE:** If there is an error saying that Java was unable to launch the application, check the Java settings for your computer. From the Java Control Panel (accessible from the Windows Control Panel), go to the **General** tab. Click **Settings** in the Temporary Internet Files area. Ensure that the **Keep temporary files on my computer** option is disabled and apply the change.

---

- 7 When you are done configuring the package, click **Next** in the *Configure Software Package* dialog box.
- 8 The configuration is sent to the Enterprise Server. Click **Finish** to close the dialog box. The configurations will be applied when the package is deployed.



## 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, click the name of the software profile with the package you want to configure.

The Software Profile Details page appears.

- 2 In the Software Packages panel, click the name of the package you want to configure.

The Software Package Details page appears.

- 3 Click **Edit**.

- 4 Configure the installation options as desired:

- If you want to delay package activation until a specific date and time, enable the **Install date** option, click on the calendar button to select a date, and type the time in the provided text box.
- To further delay the package installation after it has been activated, enable and configure the **Install delay** option. This will delay the installation of the package after it has been downloaded.
- If you want the package to be activated during a certain time window, enable the **Install 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 delay, enable the **Allow device user to install on demand** checkbox. When this option is selected, the user will be able to install the package as soon as it is downloaded.



- If you want to use the device for proxy package distribution, use the Use mobile device for proxy distribution of this package option. For more information on this option, see [Peer-to-Peer Package Distribution](#).

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

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



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

**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, click the name of the software profile with the package you want to configure.

The Software Profile Details page appears.

- 2 In the Software Packages panel, click the name of the package you want to configure.

The Software Package Details page appears.

- 3 Click **Edit**.

- 4 Configure the proxy distribution options as desired.

- 5 Save your changes.



## Chapter 10: Managing Mobile Devices

This section provides information about the following mobile device topics:

- [Mobile Devices Panel](#)
- [Viewing Mobile Device Details](#)
- [Configuring Mobile Device Properties](#)
- [Contacting the Mobile Device](#)

### Mobile Devices Panel

The Mobile Devices panel on the Inventory page shows a set of mobile devices based on the currently selected location. The following default information is provided for each mobile device:

**Model Name** The model name of the mobile device.

**Terminal ID** The unique ID automatically generated by Avalanche 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`.

In addition to the device tasks in the Mobile Device panel, there are two buttons above the Mobile Device panel: **Update Now** and **Send Message**. These buttons are location-specific. They allow you to update or send a message to all mobile devices at your current location and any nested locations.

For more information about options available for the Mobile Device Panel, see [Panels](#).



## Viewing Mobile Device Details

The Mobile Device Details page appears when you click on the name of a mobile device. 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, and signal quality of the device. For advanced details, you can click the **Advanced** button. For information about the profiles applied for the device and their priority, click the **Profile Info** button.
- **Tools panel.** Provides tools for contacting and managing your device. For information on using the tools in this panel, see [Contacting the Mobile Device](#).
- **Properties panel.** Displays the properties last reported from the mobile device. These will include custom properties. For information on configuring properties for a mobile device, see [Configuring Mobile Device Properties](#).
- **Packages panel.** Displays the packages installed on the device, their revision numbers, and reported status (whether the package has been installed, is pending, or the installation failed).
- **Device History panel.** Displays a history of Avalanche actions for the mobile device. This may include actions such as changing packages, editing properties, applying a profile, rebooting the device, or changing 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.)
- **Applied Profiles panel.** Displays the profiles that are applied to this device. You can filter the applied profiles by using the check boxes at the left of the panel.
- **Installed Software panel.** Displays the software installed on the mobile device.

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 Click the **Inventory** tab.
- 2 In the Mobile Devices panel, select the check box next to the device you want to locate and click **Locate**.

---

**NOTE:** You can also locate devices using the Mobile Devices panel on a Mobile Device Group page.

---

The map appears with the mobile device icon displaying the most recently reported location of the device. The device's GPS details are in a callout box. If your current location has mobile device profiles with geofence areas configured, the geofence areas will be displayed on the map.

## 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 or mobile device group containing the device you want to locate.
- 2 Click the Inventory context link.
- 3 In the Mobile Devices panel, select the checkbox next to the names of the device(s) you want to locate and click **Locate Cell Tower**.

---

**NOTE:** You can also locate devices using the Mobile Devices panel on a Mobile Device Group page.

---

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 Click the **Inventory** tab.
- 2 In the Mobile Devices panel, click the name of the device you want to view a history for.  
The Device Details page appears.
- 3 In the Tools panel, click **Location History**.

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 clicking on the name of the device from the **Inventory** tab.

The columns that appear in the Properties panel are as follows:

**Property Group** The group the property belongs to.

**Data Type** Indicates if the value is configurable or snapshot. Configurable means that a user may change the value, and snapshot means that the property is updated by the device.

**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.

From the Properties panel on the Mobile Device Details page, 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 **Inventory** tab, click the name of the mobile device you want to configure.

The Mobile Device Details page appears.

- 2 In the Properties panel, click **New**.

The *New Mobile Device Property* dialog box appears.

- 3 Type the category to which you want to add the property in the **Property Group** text box.

- 4 Type the **Name** and **Value** of the property in the text boxes.

- 5 Click **Save**.

The property is added to the list in the Properties panel.

## 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, or using a mobile device profile or a Scan to Config profile. 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 **Inventory** tab, click the name of the mobile device you want to configure.

The Mobile Device Details page appears.

- 2 In the Properties panel, select the check box next to the name of the property you want to edit and click **Edit**.

The *Edit Property* dialog box appears.

- 3 Type the **New Value** for the property and click **Save**.

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

## Deleting Properties

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

To delete a property:

- 1 From the **Inventory** tab, click the device you want to update in the Mobile Devices panel.

The Mobile Device Details page appears.

- 2 In the Properties panel, enable the check box to the left of the property.

- 3 Click **Delete**.



The property will be deleted from the mobile device.

## 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 Mobile Device Details page.

- [Pinging Mobile Devices](#)
- [Sending a Message to a Device User](#)
- [Updating a Mobile Device](#)
- [Using Remote Control](#)

---

**NOTE:** The Registry Explorer, File Explorer, and Process Manager icons available on this page 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.

To ping a mobile device:

- 1 From the **Inventory** tab, click the name of the device you want to ping in the Mobile Devices panel.

The Mobile Device Details page appears.

- 2 In the Tools panel, click **Ping Device**.

The Status field displays the status of the ping request.

---

**NOTE:** You can also ping the device from the Mobile Devices panel by selecting the check box to the left of the mobile device and clicking **Ping**.

---

### Sending a Message to a Device User

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

To send a message to a mobile device:

- 1 From the **Inventory** tab, click the device you want to send a message to in the Mobile Devices panel.

The Mobile Device Details page appears.

- 2 In the Tools panel, click **Send Message**.





The *Send Message* dialog box appears.

- 3 Type a message in the text box.
- 4 Click **Send**.

The Status field for the device displays the status of the text message request.

---

**NOTE:** You can also send a message to the device from the Mobile Devices panel by selecting the check box to the left of the mobile device and clicking **Message**.

---

## Updating a Mobile Device

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

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

<b>Allow User to Override the Update</b>	Gives the mobile device user the option to override the update.
<b>Force Package Synchronization</b>	Forces the package to update on the device.
<b>Delete Orphan Packages</b>	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 **Inventory** tab, click the device you want to update in the Mobile Devices panel.  
The Mobile Device Details page appears.
- 2 In the Tools panel, click **Update Now**.  
The *Update Now* dialog box appears.
- 3 Enable the options as desired and select which orphan packages you want to remove.
- 4 Click **Update Device(s)**.

The Status field displays the status of the update.



---

**NOTE:** You can also update the device from the Mobile Devices panel by selecting the check box to the left of the mobile device and clicking **Update**.

---

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

---

## 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 From the Inventory tab, click the name of the device you want to chat with.  
The Mobile Device Details page appears.
- 2 Click **Device Chat** in the Tools panel.  
The *Mobile Device Chat* dialog box appears.
- 3 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.
- 4 When you are finished, 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 Click the **Inventory** tab.



- 2 In the Mobile Devices panel, select the check box next to the device you want to wipe and click **Wipe Device**.
- 3 The *Confirm* dialog box appears. Click **Confirm** if you are certain you want to wipe the folders specified in the mobile device profile.

The server sends a wipe command to the device.

## 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 From the **Inventory** tab, click the device you want to connect to from the Mobile Devices panel.

The Mobile Device Details page appears.

- 2 In the Tools panel, click **Remote Control**.

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.



## 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](#)

### 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:

<b>Enabled</b>	Enables or disables the profile.
<b>Home location</b>	Sets the home location for the profile.
<b>Mobile device selection criteria</b>	Determines which devices the profile is applied to. For information on selection criteria, see <a href="#">Using Selection Criteria</a> .
<b>Orphan Package Removal</b>	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.
<b>Notes</b>	Any notes for the profile.
<b>Server Address</b>	Specifies the address of a specific mobile device server you want the devices to connect to.
<b>Enable SMS Notification</b>	Allows SMS messages to be sent to the device from the Avalanche Console.



<b>Force Package Synchronization</b>	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.
<b>Restrict simultaneous device updates</b>	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.
<b>Authorized Users</b>	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 <a href="#">Managing User Accounts</a> .

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 from the Profiles tab:

- 1 If you are creating a new mobile device profile, click **New Profile** in the Available Profiles panel and click Mobile Device Profile in the dialog box that appears. When the Mobile Device Profile page appears, type a name for the new profile.

-Or-

If you are configuring a profile that has already been created, click on the mobile device profile from the Profiles tab. When the Mobile Device Profile page appears, click **Edit**.

- 2 Configure the profile settings.
- 3 Click **Save** to save your changes.

## 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, click the name of the mobile device profile you want to configure.

The Mobile Device Profile Details page appears.



- 2 Click **Edit**.
- 3 In the Device Folders panel, click **New**.

The *Device Folder* dialog box appears.

- 4 Type the full **Device Path** to the folder in the text box and click **Save**.

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, click on the name of the profile you want to configure.
- 2 Click **Edit**.
- 3 In the Properties panel, click **New**.  
The *New Property* dialog box appears.
- 4 Type the **Group (optional)**, **Name**, and **Value** in the text boxes.
- 5 Select the **Create Property** option.
- 6 Click **Add**.
- 7 Click **Save**.

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



To edit or remove a custom property from the device:

- 1 From the **Profiles** tab, click on the name of the profile you want to configure.
- 2 Click **Edit**.
- 3 In the Properties panel, click **New**.  
The *New Property* dialog box appears.
- 4 Type the **Group (optional)**, **Name**, and **Value** in the text boxes. If you are editing the property, this is the new value for the property.
- 5 If you are editing the value of the property, select **Create property**. If you want to remove the property from the device, select **Delete property**.
- 6 Click **Add**.
- 7 Click **Save**.

The task is added to the list. The property will be edited or deleted when the profile is applied on the mobile device.

## 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, click on the name of the profile you want to configure.

The Profile Details page appears.



- 2 Click **Edit**.
- 3 The Edit Profile page appears.
- 4 In the Registry Entries panel, click **New**.  
The *New Registry Entry* dialog box appears.
- 5 Select the **Root** from the drop-down list.
- 6 Type the name of the key in the **Key** text box.
- 7 Type the value entry of the key in the **Name** text box.
- 8 Enter the data for the value entry in the **Data** text box.
- 9 Select the **Type** of the value from the drop-down list.
- 10 Select **Create key** as the **Action**.
- 11 Click **Add** to add the registry key and value to the list.
- 12 When you are done, click **Save**.

The key and value are saved to the profile.

## 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 edit or remove a registry key or value:

- 1 From the **Profiles** tab, click on the name of the profile you want to configure.  
The Profile Details page appears.
- 2 Click **Edit**.  
The Edit Profile page appears.
- 3 In the **Registry Entries** panel, click **New**.  
The *New Registry Entry* dialog box appears.
- 4 Select the **Root** from the drop-down list.





- 5 Type the name of the key in the **Key** text box.
- 6 Type the value entry of the key in the **Name** text box.
- 7 Enter the data for the value entry in the **Data** text box.
- 8 Select the **Type** of the value from the drop-down list.
- 9 If you are editing the key or key value, select **Create key** as the **Action**. If you are deleting the key or key value, select **Delete key**.
- 10 Click **Save**.

The task is added to the list in the Registry keys panel. The value will be edited when the profile is applied on the mobile device.

## 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.



<b>GPS acquisition timeout</b>	Determines how often the device checks its GPS coordinates.
<b>Prompt user to initiate timeout</b>	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.
<b>Notify user _ consecutive GPS failures</b>	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, click the name of the mobile device profile you want to configure.  
The Mobile Device Profile Details page appears.
- 2 In the Other Settings panel, configure the options as desired.
- 3 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. Geofence areas are displayed when you use the Locate function to locate your devices on the map. 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, click the name of the mobile device profile you want to configure.  
The Mobile Device Profile Details page appears.
- 2 Click **Edit**.
- 3 In the Geofence Areas panel, click **New**.  
The *Add Geofence* dialog box appears.
- 4 Type a name for the area in the **Name** text box.
- 5 If you want the area to be a home area, enable the **Home** check box.
- 6 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.
- 7 Click **Save**.  
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, click the name of the mobile device profile you want to configure.  
The Mobile Device Profile Details page appears.
- 2 Enable the **Manage regional settings** check box and select the region from the drop-down list.
- 3 Enable the **Manage time zone** check box and select the time zone from the drop-down list.
- 4 Enable the **Automatically adjust clock for Daylight Savings Time** option if you want the devices to switch over automatically.
- 5 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 an update restriction:

- 1 From the **Profiles** tab, click the name of the mobile device profile you want to configure.  
The Mobile Device Profile Details page appears.
- 2 In the Update Restrictions panel, click **Add**.  
The *New Update Restrictions Window* dialog box appears.
- 3 Select the start time and duration (in minutes) of the restriction window, and enable the boxes for the days you want the restriction 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.

---

- 4 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](#)
- [Sending Messages to Mobile Device Groups](#)

### 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 Click the **Inventory** tab.
- 2 In the Mobile Device Groups panel, click **New**.  
The *New Mobile Device Group* dialog box appears.
- 3 Type a **Name** for the group.
- 4 Select whether you want the group to be **Dynamic** or **Static**.
- 5 Click **Launch wizard** to launch the Selection Criteria Builder. Use selection criteria to define which devices will be included in the group.
- 6 When you are finished configuring the group, click **Save** to save your changes.

The group is created and the mobile devices matching the selection criteria are added.

## 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 Click the **Inventory** tab or context link.
- 2 In the Mobile Device Groups panel, enable the check box to the left of the name of the group you want to send a message to.
- 3 Click **Send Message**.

The *Send Message* dialog box appears.

- 4 Type the message in the text box and click **Send**.

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



## 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** panel 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:

- Email Recipients** 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.
- SNMP Forwarding** 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.
- Available 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 **New Profile**.

The *New Profile* dialog box appears.

- 2 Select **Alert Profile**.

The New Profile Details page appears.

- 3 Type a name for the profile in the **Name** text box.
- 4 If desired, enable the profile or type any notes in the **Notes** text box.
- 5 Configure the **Email Recipients**, **SNMP Forwarding**, and **Available Alerts**.

---

**NOTE:** You must have the SMTP server settings configured if you want to send alert e-mails. For information on configuring the SMTP server settings, see [Configuring E-mail Settings](#).

---

- To add a custom message to any e-mails sent for this profile, enable the **Add custom text to emails** option and type the message in the text box that appears.
  - To add an e-mail recipient, click **New** in the Email Recipients panel.
  - To add an SNMP address, click **New** in the SNMP Forwarding panel.
  - To add events to the alert profile, select the checkbox next to the event in the Available Alerts panel. Use the arrows to page through the events, or use the filters to restrict which events appear.
- 6 Click **Save**.

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. You must have a Flash plug-in for your browser in order to import a `.csv` file. You can also export the e-mail addresses associated with an alert profile to a `.csv` file.

**To add an e-mail contact:**

- 1 From the Available Profiles panel on the **Profiles** tab, click on the alert profile you want to edit.

The Alert Profile Details page appears.

- 2 Click **Edit**.

The Edit Alert Profile page appears.

- 3 Click **New** in the Email Recipients panel.

The *Add Email Recipient* dialog box appears.

- 4 Type the **First Name**, **Last Name**, and **Email Address** in the provided text boxes and click **Save**.

The contact appears in the Email Recipient panel.

**To import e-mail addresses:**

- 1 From the Available Profiles panel on the **Profiles** tab, click on the alert profile you want to edit.

The Alert Profile Details page appears.

- 2 Click **Edit**.

- 3 In the Email Recipients panel, click **Import**.

The *Import Email Recipients* dialog box appears.

- 4 Click **Browse** to navigate to and select the `.csv` file that contains the e-mail addresses that you want to import.

- 5 Click **Open**.

- 6 Click **Save**.

The contacts appear in the Email Recipients panel.

Click **Save**.





#### To export e-mail addresses:

- 1 From the Available Profiles panel on the **Profiles** tab, click on the alert profile you want to edit.

The Alert Profile Details page appears.

- 2 In the Email Recipients panel, select the check boxes next to the e-mail addresses you want to export and click **Export**.

- Or -

In the Email Recipients panel, click **Export All**.

The *Opening EmailExport.csv* dialog box appears.

- 3 Enable the **Save File** option and click **OK**.

The e-mail addresses are saved to a local `.csv` file.

## 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 From the Available Profiles panel on the **Profiles** tab, click on the alert profile you want to edit.

The Alert Profile Details page appears.

- 2 Click **Edit**.

The Edit Alert Profile page appears.

- 3 Click **New** in the SNMP Forwarding panel.

The *New SNMP* dialog box appears.

- 4 Type the **IP Address** of the SNMP proxy in the text box and click **Save**.

## Alerts Tab

The Alerts tab provides the following information about each alert that has been generated on your network:



<b>Severity</b>	Displays the severity of the alert.
<b>Location</b>	Displays the location where the event occurred.
<b>Reported Time</b>	The date and time when the event occurred.
<b>Description</b>	Provides a brief description of the event.
<b>Ack'd</b>	Indicates if the alert has been acknowledged.
<b>Source</b>	Displays the source of the alert.

This section provides information about the following tasks:

- [Acknowledging and Clearing Alerts](#)
- [Customizing Alerts Tab Functionality](#)

## Acknowledging and Clearing Alerts

When a new alert is generated, it appears in the Alerts tab and the Maps tab. In the Alerts tab, the alert is listed in the Current Alerts panel. In the Maps tab, the server location at which the alert was generated is outlined in the color of the most severe alert at that location.

Acknowledging the alert will remove the colored indicator from the map. If the Current Alerts panel begins to fill with alerts, you may want to remove acknowledged alerts that are no longer relevant.

**To acknowledge an alert:**

- From the Alerts tab, select the check boxes next to the alerts you want to acknowledge and click **Ack**.

-Or-

- From the Alerts tab, click **Ack All**.

**To clear alerts:**

- From the Alerts tab, select the check boxes next to the alerts you want to clear and click **Clear**.

-Or-

- From the Alerts tab, click **Clear All**.

All acknowledged alerts will be removed from the list. Alerts that were not marked as acknowledged will remain in the Current Alerts panel.



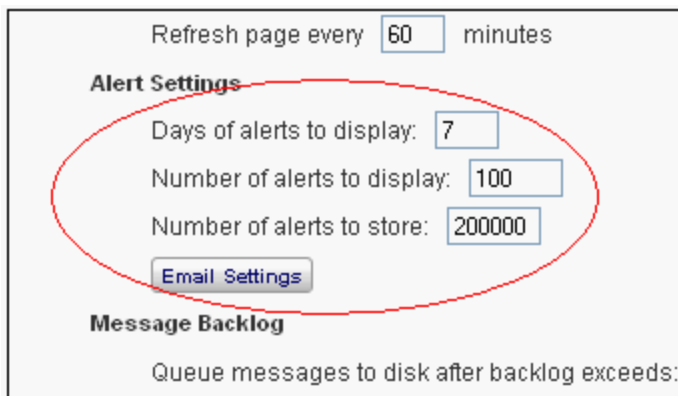
## Customizing Alerts Tab Functionality

The System Settings page allows you to configure the way the Alerts tab manages and displays alerts. You can configure the following settings:

- Number of days an alert is displayed in the Current Alerts panel.
- The number of alerts to display.
- Maximum number of alerts to store. Alerts are stored in the database on the Enterprise Server. This option is only available for administrative users.

To customize the Alerts tab functions:

- 1 Click **Tools > Settings**.
- 2 The System Settings page appears.



Refresh page every  minutes

**Alert Settings**

Days of alerts to display:

Number of alerts to display:

Number of alerts to store:

**Message Backlog**

Queue messages to disk after backlog exceeds:

*Alert Settings*

- 3 Under **Alert Settings**, use the **Days of alerts to display**, **Number of alerts to display**, and **Number of alerts to store** boxes to configure the alert settings.
- 4 Save your changes.

The Alerts tab will update to reflect your changes.



## 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 or infrastructure 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, infrastructure profiles, and mobile device groups. To access the Selection Criteria Builder, click the **Launch wizard** 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:

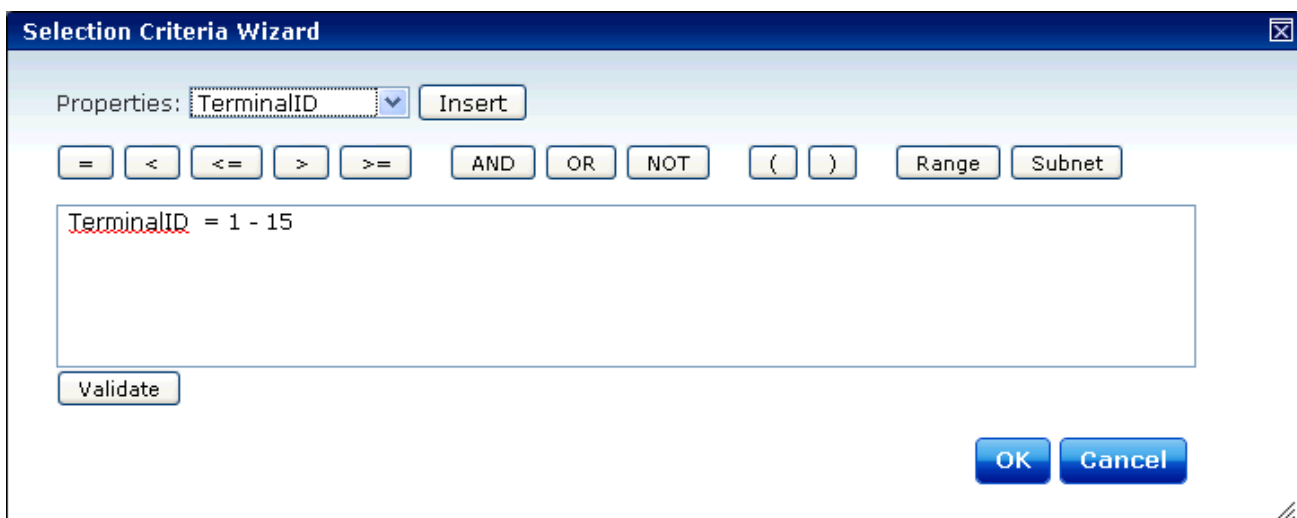
- Selection variables such as **ModelName** or **KeyboardName**. These variables determine the type of restriction placed on the package or profile. For example, by using a **ModelName** variable, you can restrict the package or profile to a specific class of mobile devices, based on their model numbers. 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**. 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: Avalanche Reports

The Avalanche Reports tool can help you organize information about the activity or status of devices or software on your network. These reports are generated from the information Avalanche stores in its database. You can create reports with an Avalanche template or you can create a custom report to display the desired information.

Before you can create a report, you must first configure the name, scope, output, and the time period to be included in the report. Then you can either generate the report immediately or schedule a time for the report to be generated. When a report is scheduled, it can be set to run once or on a recurring basis.

Click **Tools > Reports** to access the reports tool. The main page for the Reports tool has three panels:

- The Completed Reports panel displays the names of reports that have been completed. Once a report has been completed, you can view and save the results.
- The Scheduled Reports panel displays the names of reports that have been configured and scheduled.
- The Configured Reports panel displays the names of reports that have been configured.

The columns displayed in these panels include the following:

**Name** Displays the name of the report.

**Template** Displays the template used for the report.

**Location** Indicates the location or locations involved in the report.

**Result** Displays if the report ran successfully. If the report failed, this column displays the reason.

**Completed** Displays when the report was completed.

**Frequency** Displays how often the scheduled report will be run.

**Category** Displays the category to which the report belongs.

This section provides information about using the Reports tool, including:

- [Configuring Reports](#)
- [Generating and Scheduling Reports](#)
- [Creating Custom Reports](#)





## Configuring Reports

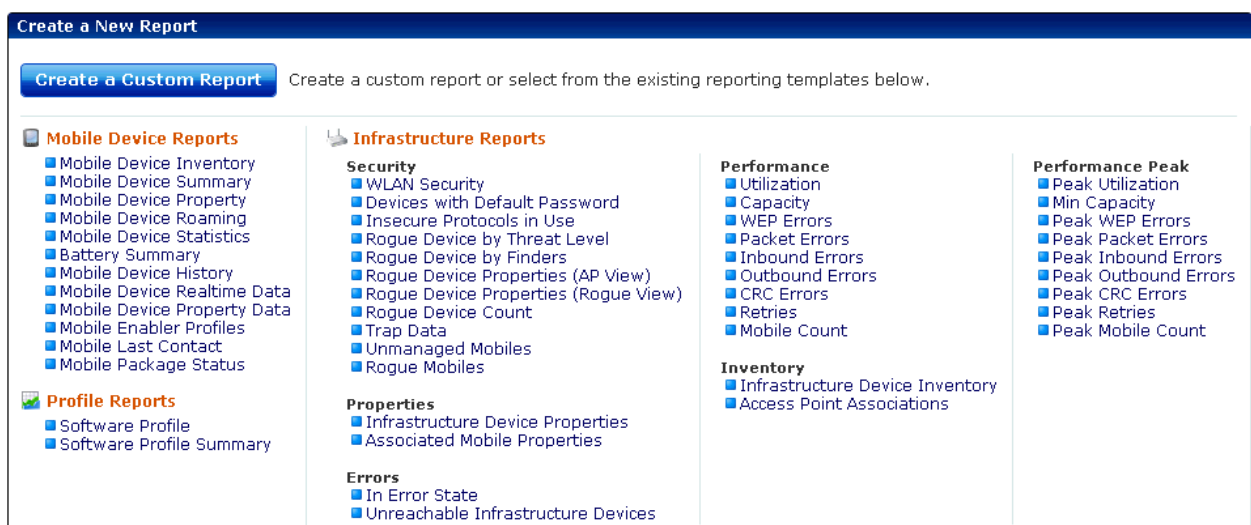
In order to create a report, you must first configure the name, scope, output, and the time period to be included in the report. Then you can either generate the report immediately or schedule a time for the report to be generated. When a report is scheduled, it can be set to run once or on a recurring basis.

This section includes instructions for configuring a report using a preexisting Avalanche template. For information on creating custom reports, see [Creating Custom Reports](#).

To configure a report with an Avalanche template:

- 1 Click **Tools > Reports**.
- 2 In the **Configured Reports** panel, click **New**.

The Create a New Report page appears.



Create a New Report page

- 3 Click on the desired template from the list of preexisting Avalanche report templates.
- 4 Depending on the template, the Reports tool will guide you through configuring the available options for the report. These will always include the name and output format, but may also include the scope or the time period to be included in the report. You may also choose to have a report sent to an e-mail recipient when it is generated.
  - **Scope.** You can configure the report to collect information from a specific location in the Avalanche navigation tree, or for some reports, for a specific infrastructure device.
  - **Name.** You must have a unique name for each configured report.



- **Output Format.** You can choose from three options how you want the report to appear: `.pdf`, `.xml`, or `.csv`.
- **Time.** You can set the report to include information from the past 24 hours, past week, or past month.

When you have completed the configuration, the report will appear in the Configured Reports panel on the Reports tool main page.

## Generating and Scheduling Reports

After a report has been configured, it can be generated immediately or scheduled for a specific time. When a report is scheduled, it can be set to run once or on a recurring basis. The configuration persists after the report has been run, so you can generate a report with the same name and configuration as often as desired.

To run a configured report:

- 1 Click **Tools > Reports**.
- 2 From the Configured Reports panel, enable the checkbox next to the report that you want to generate and click **Run Now**.

The report appears in the Completed Reports panel.

To schedule a report:

- 1 Click **Tools > Reports**.
- 2 From the Configured Reports panel, enable the checkbox next to the report that you want to generate and click **Schedule**.

The Schedule Reports page appears.

- 3 From the drop-down list, select how frequently you want the report to run.
- 4 Type the date and time you want the report to run in the text boxes. For the date, use a month/day/year format.
- 5 Click **Next**.
- 6 A summary of the report appears. Click **Done** to return to the Reports tool.

## Creating Custom Reports

The Reports tool allows you to create custom reports using information from your databases. In order to utilize custom reports, you must be familiar with SQL query statements.



---

**NOTE:** A custom report can include information from either one database or the other. You cannot create a custom report using tables from both the stats database and the enterprise database.

---

This section gives basic instructions on creating a custom report. For details about custom reporting, including the database tables and sample query statements, see the *Avalanche Custom Reporting Reference Guide* on the Wavelink Web site.

When you create a custom report, you can design a report that gathers and displays the information you need from a database.

To create a custom report:

1 Access the Reports tool.

2 From the Configured Reports panel, click **New**.

The Create a New Report panel appears.

3 Click **Create a Custom Report**.

The Create Reports panel appears.

4 Select the database from which you would like to report and click **Next**.

5 Select the database table on which you would like to report, and then enable the checkboxes for the columns which you want to include. Click **Next**.

A Summary page appears.

6 If you want to include information from a different table, click **Add Table**.

7 Use the **Where**, **Order By**, and **Group By** text boxes to create a SQL query statement that will return the desired information.

8 Type a **Report Name** in the text box and select the **Output Format** for the report. If you want the report to be e-mailed to a recipient when it is run, type the e-mail address in the **E-mail Report** text box. Click **Next**.

9 A summary of the report appears. Click **Done** to return to the Reports Tool page.

From the Reports page, you can run or schedule the report and view the report results.



## Chapter 16: 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.

---

**NOTE:** When using the Task Scheduler, use the **Next** and **Back** buttons provided in the wizard instead of the browser's buttons.

---

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:

**Start date.** The date the task will begin.

**Start time.** The time of day the task will begin.

**Run until complete.** When this option is selected, the task will run until it is complete.

**End date.** The date the task will end.

**End time.** The time of day the task will end.

**Use local time of server location.** 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:

**Start Time.** The time of day the event will begin.

**Use end time.** The time of day the event will end.



**Use local time of server location.** 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.

---

**NOTE:** Once Avalanche begins to send data to a location, it does not stop until all data is sent. This prevents a location from receiving only part of the information it needs. When an event's end time is reached, Avalanche completes any deployments that are in progress, but does not start sending data to any of the remaining locations.

---

The Task Scheduler allows you to perform the following tasks:

- [Performing a Server Synchronization](#)
- [Backing Up the System](#)
- [Restoring the System](#)



- [Removing Completed Tasks](#)

---

**NOTE:** Other tasks available from the Java Console include deploying servers, uninstalling servers, updating infrastructure firmware, and applying and deploying profiles. See the Java Console help for more information.

---

## Performing a Server Synchronization

Any time you make changes to profiles, settings or configurations in the Avalanche Console, perform a server synchronization to send all the changes to your servers. A server synchronization updates the settings for the selected location or locations.

To schedule a server synchronization:

- Click the **Schedule Sync** button to sync the currently selected location. Use the options in the Server Synchronization dialog box to set the time for the synchronization.

-Or-

- 1 Click **Tools > Sync Server**. The Schedule Task Wizard page appears.
- 2 From the **Task Type** drop-down list, select **Server Synchronization** and click **Next**.
- 3 To add a server location to the list, click **Add** and select the location from the list that appears.
- 4 When you are finished adding locations, click **Next**.

The 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 **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 > Schedule Backup**.

The Create A System Backup screen appears.

- 2 In the **Name of new backup** text box, enter an identifier for the system backup and click **Next**. This tag is used to select the correct file when restoring the system. It is not the same as the name of the zip file.

The Scheduling Options screen appears.

- 3 Determine when the event will occur and click **Next**.

The Review Your Task screen appears.

- 4 Review your task to ensure that it is correct and click **Finish**.

## 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 > Schedule Restore**.

The Restore A System Backup screen appears.

- 2 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 identifier tag.

The Review Your Task screen appears.



- 3 Review your task to ensure that it is correct and click **Finish**.
- 4 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 delete tasks individually.

To remove completed tasks:

- 1 Click **Tools > Scheduled Tasks**.

The Scheduled Tasks page appears.

- 2 In the Completed Tasks panel, select the check boxes next to the name of the tasks you want to delete from the list and click **Delete**.





## 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\AvalancheMC\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 Agent

C:\Program Files\Wavelink\MM\Program\AgentSvc.exe

This is an infrastructure server. The server is deployed to a server location.

### Wavelink Avalanche Service Manager (1 of 2)

C:\Program Files\Wavelink\MM\Program\WLAmcServiceManager.exe

The service manager starts and stops the infrastructure and mobile device servers. It is installed with a device server.

### Wavelink Avalanche Service Manager (2 of 2)

C:\Program Files\Wavelink\Avalanche\Service\WLAmcServiceManager.exe

The service manager starts and stops the mobile device servers and infrastructure servers. It is installed with a device server.

---

**NOTE:** The last Wavelink Avalanche Service Manager to be installed determines the path to the service.

---

### Wavelink Avalanche Enterprise Server

C:\Program Files\Wavelink\AvalancheMC\eserver.exe

This is the enterprise server.



## Wavelink Information Router

C:\Program Files\Wavelink\AvalancheMC\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\AvalancheMC\WLLicenseService.exe

The license server manages licensing. It is normally installed with the enterprise server.

## Wavelink Service Manager

C:\Program Files\Wavelink\MM\Program\svcmgr.exe

This service manager is used with the Infrastructure Site Tool to start and stop the infrastructure server. It is installed with the infrastructure server.

## Wavelink Stat Server Enterprise

C:\Program Files\Wavelink\AvalancheMC\StatServer.exe

The statistics server handles reports and device statistics. It is generally installed with the enterprise server.

## Wavelink TFTP Server

C:\Program Files\Wavelink\MM\Program\TftpSvc.exe

The TFTP server is installed with an infrastructure server.

## Wavelink Deployment

C:\Program Files\Wavelink\AvalancheMC\iserv.exe

The deployment server handles device server packages and their deployments. It is installed with the enterprise server.

## Wavelink Alerts

C:\Program Files\Wavelink\MM\Program\AlertSvc.exe

The alerts service manages alerts and runs local to an infrastructure 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 servers and infrastructure servers requesting licenses from the License Server. | 7221 | TCP     | Infrastructure Server, Mobile Device Server                                                     | Enterprise Server                                                         |
| InfoRail transmission of information between servers, consoles, databases.                    | 7225 | TCP     | Infrastructure Server, Mobile Device Server, Enterprise Server, Web and Java Console, databases | Infrastructure Server, 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](#).

## Infrastructure Server Outbound Ports

The following table provides a list of remote ports that the Infrastructure Server sends information to.

| Traffic Description                                                           | Port | UDP/TCP | Destination                  |
|-------------------------------------------------------------------------------|------|---------|------------------------------|
| SSH. Server manages device.                                                   | 22   | UDP/TCP | Infrastructure Device        |
| Telnet. Server manages device.                                                | 23   | UDP/TCP | Infrastructure Device        |
| SMTP. Server sends e-mail notifications.                                      | 25   | TCP     | SMTP Server                  |
| HTTP. Server manages device.                                                  | 80   | TCP     | Infrastructure Device        |
| SNMP. Server manages device; includes SNMP V3.                                | 161  | UDP/TCP | Infrastructure Device        |
| Communication between Infrastructure Server and Enterprise/Statistics Server. | 7225 | TCP     | Enterprise Server (InfoRail) |

## Infrastructure Server Inbound Ports

The following table provides a list of the ports that the Infrastructure Server listens on.

| Traffic Description                                                                | Port | UDP/TCP | Source                               |
|------------------------------------------------------------------------------------|------|---------|--------------------------------------|
| TFTP. Firmware upgrades.                                                           | 69   | UDP     | Infrastructure Device                |
| SNMP traps and VLACL information.                                                  | 162  | UDP     | Infrastructure Device                |
| IAPP. Discovery of Proxim APs.                                                     | 2313 | UDP     | Proxim APs                           |
| RPC. Infrastructure Site Tool initiates authentication with Infrastructure Server. | 7200 | TCP     | Infrastructure Site Tool             |
| Alerts service connects to Infrastructure Server.                                  | 7205 | TCP     | Infrastructure Server (always local) |
| Alerts service authenticates with Infrastructure Site Tool.                        | 7210 | TCP     | Infrastructure Site Tool             |



| Traffic Description                                                       | Port | UDP/TCP | Source                   |
|---------------------------------------------------------------------------|------|---------|--------------------------|
| Infrastructure Site Tool starts/stops Infrastructure Server.              | 7211 | TCP     | Infrastructure Site Tool |
| Communication between Infrastructure Site Tool and Infrastructure Server. | 7212 | UDP     | Infrastructure Site Tool |
| Alerts service normal data communication.                                 | 7213 | UDP     | Infrastructure Site Tool |
| Infrastructure Server authentication with Infrastructure Site Tool.       | 7215 | UDP     | Infrastructure Site Tool |

## 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       |



## Supported Firmware

Avalanche is not packaged with any firmware files. You must obtain supported firmware from the manufacturer and then import the files into Avalanche.

The following table lists the vendor, hardware and firmware versions supported in Avalanche.

| Vendor | Hardware | Supported Versions |
|--------|----------|--------------------|
| Aruba  | 3200*    | 5.0.3.2            |
|        |          | 3.4.2.6            |
|        | 3400*    | 5.0.3.2            |
|        |          | 3.4.2.6            |
| Avaya  | AP-3     | 2.5.2              |
|        |          | 2.4.11             |
|        |          | 2.4.5              |
|        |          | 2.3.3              |
|        |          | 2.3.2              |
|        |          | 2.3.2              |
|        | AP-4/5/6 | 2.5.2              |
|        |          | 2.4.11             |
|        |          | 2.4.5              |
|        |          | 2.3.3              |
|        |          | 2.3.2              |
|        |          | 2.3.2              |
| AP-8   | 2.5.2    |                    |
|        | 2.4.11   |                    |



---

| <b>Vendor</b> | <b>Hardware</b> | <b>Supported Versions</b>                                                                                                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco         | 1100 IOS        | 12.3.8-JED1<br>12.3-8JED<br>12.3-8JEC3<br>12.3-8JEC<br>12.3-8JEB1<br>12.3-8JEB<br>12.3-8JEA3<br>12.3-8JEA2<br>12.3-8JEA1<br>12.3-8JEA<br>12.3-8JA<br>12.3-7JA3<br>12.3-7JA<br>12.3-4JA<br>12.3-2JA<br>12.3-2JA2<br>12.2-15JA<br>12.2-13JA3<br>12.2-13JA1<br>12.2-11JA1 |





---

| <b>Vendor</b> | <b>Hardware</b> | <b>Supported Versions</b> |
|---------------|-----------------|---------------------------|
|               | 1130            | 12.4.21a-JY               |
|               |                 | 12.4.21a-JA1              |
|               |                 | 12.4.10b-JDA3             |
|               |                 | 12.4.10b-JA               |
|               |                 | 12.4-3gJA1                |
|               |                 | 12.4-3gJA                 |
|               |                 | 12.3-8JEA3                |
|               |                 | 12.3-8JEA2                |
|               |                 | 12.3-11JA4                |
|               |                 | 12.3-11JA1                |
|               |                 | 12.3-8JEB                 |
|               |                 | 12.3-8JEA1                |
|               |                 | 12.3-8JEA                 |
|               |                 | 12.3-8JA                  |
|               |                 | 12.3-7JA3                 |
|               |                 | 12.3-7JA                  |
|               |                 | 12.3-4JA                  |
|               |                 | 12.3-2JA                  |
|               |                 | 12.3-2JA2                 |



---

| Vendor | Hardware | Supported Versions |
|--------|----------|--------------------|
|        | 1200     | 12.05              |
|        |          | 12.04              |
|        |          | 12.03T             |
|        |          | 12.02T1            |
|        |          | 12.01T1            |
|        |          | 11.56              |
|        |          | 11.42T             |



---

| <b>Vendor</b> | <b>Hardware</b> | <b>Supported Versions</b> |
|---------------|-----------------|---------------------------|
|               | 1200 IOS        | 12.3.8-JED1               |
|               |                 | 12.3-8JED                 |
|               |                 | 12.3-8JEC3                |
|               |                 | 12.3-8JEC                 |
|               |                 | 12.3-8JEB1                |
|               |                 | 12.3-8JEA3                |
|               |                 | 12.3-8JEA2                |
|               |                 | 12.3-8JEB                 |
|               |                 | 12.3-8JEA1                |
|               |                 | 12.3-8JEA                 |
|               |                 | 12.3-8JA                  |
|               |                 | 12.3-7JA3                 |
|               |                 | 12.3-7JA                  |
|               |                 | 12.3-4JA                  |
|               |                 | 12.3-2JA                  |
|               |                 | 12.3-2JA2                 |
|               |                 | 12.2-15JA                 |
|               |                 | 12.2-13JA3                |
|               |                 | 12.2-13JA4                |
|               |                 | 12.2-13JA1                |
|               |                 | 12.2-11JA1                |



---

| <b>Vendor</b> | <b>Hardware</b> | <b>Supported Versions</b>                                                                                                                                               |
|---------------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco         | 1240            | 12.4.21a-JA1<br>12.4.10b-JDA3<br>12.4.10b-JA<br>12.4-3gJA1<br>12.4-3gJA<br>12.3-8JEA3<br>12.3-8JEA2<br>12.3-11JA4<br>12.3-11JA1<br>12.3-8JEB<br>12.3-8JEA1<br>12.3-8JEA |



---

| <b>Vendor</b> | <b>Hardware</b> | <b>Supported Versions</b>                                                                                                                                                                                               |
|---------------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | 1310BR          | 12.4.21a-JY<br>12.4.21a-JA1<br>12.4.10b-JDA3<br>12.4.10b-JDA2<br>12.4.10b-JA<br>12.4.3g-JA1<br>12.3-8JEA3<br>12.3-8JEA2<br>12.3-11JA4<br>12.3-11JA1<br>12.3-8JEB<br>12.3-8JEA1<br>12.3-8JEA<br>12.2(15)JA<br>10.4-3g-JA |
|               | 340 AP          | 12.05<br>12.04<br>12.03T<br>12.02T1<br>12.01T1<br>11.23T<br>11.10T1                                                                                                                                                     |



---

| <b>Vendor</b> | <b>Hardware</b> | <b>Supported Versions</b>                                           |
|---------------|-----------------|---------------------------------------------------------------------|
|               | 350 AP          | 12.05<br>12.04<br>12.03T<br>12.02T1<br>12.01T1<br>11.23T<br>11.10T1 |
|               | 350 Bridge      | 12.05<br>12.04<br>12.03T<br>12.02T1<br>12.01T1<br>11.23T<br>11.10T1 |



| Vendor          | Hardware        | Supported Versions                                                                                                                                                     |
|-----------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 350 IOS         | 12.3-8JEA3<br>12.3-8JEA2<br>12.3-8JEA1<br>12.3-8JEA<br>12.3-8JA<br>12.3-7JA3<br>12.3-7JA<br>12.3-4JA<br>12.3-2JA<br>12.3-2JA2<br>12.2-15JA<br>12.2-13JA2<br>12.2-13JA1 |
|                 | 4402*           | 5.2.178.0                                                                                                                                                              |
| Dell            | TrueMobile 1170 | 2.2.2                                                                                                                                                                  |
| HP              | ProCurve 520wl  | 2.4.5<br>2.1.2                                                                                                                                                         |
| Meru            | MC1000*         | 3.6-111                                                                                                                                                                |
| Motorola/Symbol | AP-3020         | 04.02-19                                                                                                                                                               |
|                 | AP-4121         | 02.70-12<br>02.70-06<br>02.52-13<br>02.51-23                                                                                                                           |



---

| <b>Vendor</b> | <b>Hardware</b> | <b>Supported Versions</b>                                                                                                                                                                                                                    |
|---------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | AP-4131         | 03.95-04<br>03.94-15a<br>03.93-00<br>03.92-21<br>03.70-77<br>03.70-46a<br>03.50-26<br>03.50-18                                                                                                                                               |
|               | AP-5131         | 2.3.2.0-008R<br>2.3.1.0-004R<br>2.3.0.0-019R<br>2.2.2.0-001R<br>2.2.1.0-007R<br>2.2.0.0-023R<br>2.1.1.0-001R<br>2.1.0.1-003R<br>2.1.0.0-030R<br>2.0.0.0-045R<br>1.1.2.0-005R<br>1.0.1.0-004R<br>1.1.0.0-045R<br>1.0.0.0-188R<br>1.1.1.0-020R |





| <b>Vendor</b>          | <b>Hardware</b> | <b>Supported Versions</b>                                                                                                                                                                    |
|------------------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Motorola/Symbol</b> | AP 5181         | 2.3.2.0-008R<br>2.3.1.0-004R<br>2.3.0.0-019R<br>2.2.2.0-001R<br>2.2.1.0-007R<br>2.2.0.0-023R<br>2.1.1.0-001R<br>2.1.0.1-003R<br>2.1.0.0-030R<br>2.0.0.0-045R<br>1.1.2.0-005R<br>1.1.1.0-020R |
|                        | AP 7131         | 4.1.2.0-012R<br>4.1.1.0-017R<br>4.1.0.0-072R<br>4.0.3.0-010R<br>4.0.2.0-003R<br>4.0.1.0-019R<br>4.0.0.0-057R<br>3.2.2.0-005R<br>3.2.1.0-012R<br>3.2.0.0-067R<br>3.0.2.0-028R<br>3.0.0.0-039R |



---

| <b>Vendor</b> | <b>Hardware</b> | <b>Supported Versions</b> |
|---------------|-----------------|---------------------------|
|               | RFS 7000        | 4.3.3.0-004R              |
|               |                 | 4.3.2.0-012R              |
|               |                 | 4.3.1.0-016R              |
|               |                 | 4.3.0.0-059R              |
|               |                 | 4.2.1.0-005R              |
|               |                 | 4.2.0.0-024R              |
|               |                 | 4.1.0.0-042R              |
|               |                 | 4.0.2.0-001R              |
|               |                 | 4.0.1.0-005R              |
|               |                 | 4.0.0.0-067R              |
|               |                 | 1.3.2.0-010R              |
|               |                 | 1.3.1.0-003R              |
|               |                 | 1.3.0.0-029R              |
|               |                 | 1.2.0.0-040R              |
|               |                 | 1.1.1.0-003R              |
|               |                 | 1.1.0.0-038R              |
|               |                 | 1.0.1.0-012R              |



---

| <b>Vendor</b> | <b>Hardware</b> | <b>Supported Versions</b>                                                                                                                                                                                                    |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | RFS 6000        | 4.3.3.0-004R<br>4.3.2.0-012R<br>4.3.1.0-016R<br>4.3.0.0-059R<br>4.2.1.0-005R<br>4.2.0.0-024R<br>4.1.0.0-042R<br>4.0.2.0-001R<br>4.0.1.0-005R<br>4.0.0.0-067R<br>3.3.2.0-010R<br>3.3.0.0-029R<br>3.2.0.0-040R<br>3.1.0.0-024R |
|               | RFS 4000*       | 4.3.0.0-059R<br>4.3.2.0-012R<br>4.3.3.0-004R                                                                                                                                                                                 |



| <b>Vendor</b>          | <b>Hardware</b> | <b>Supported Versions</b> |
|------------------------|-----------------|---------------------------|
| <b>Motorola/Symbol</b> | WS 2000         | 2.4.5.0-006R              |
|                        |                 | 2.4.4.0-001R              |
|                        |                 | 2.4.3.0-020R              |
|                        |                 | 2.4.1.0-005R              |
|                        |                 | 2.4.0.0-023R              |
|                        |                 | 2.3.2.0-003R              |
|                        |                 | 2.3.1.0-012R              |
|                        |                 | 2.3.0.0-035R              |
|                        |                 | 2.3.0.0-034R              |
|                        |                 | 2.2.3.0-020R              |
|                        |                 | 2.2.2.0-003R              |
|                        |                 | 2.2.1.0-018R              |
|                        |                 | 2.2.0.0-021R              |
|                        |                 | 2.1.1.0-009R              |
|                        |                 | 2.1.0.0-035R              |
|                        |                 | 2.0.0.0-036R              |
|                        |                 | 1.5.0.0-216r              |
|                        |                 | 1.0.10.08                 |
|                        | WS 5000         | 1.2.0.39o                 |
|                        |                 | 1.2.0.39f                 |
| 1.1.4.30f              |                 |                           |
| 1.1.4.30SP1            |                 |                           |



---

| <b>Vendor</b> | <b>Hardware</b> | <b>Supported Versions</b>                                                                                                                                                                 |
|---------------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | WS 5000 v1.2+   | 2.1.5.0-003R<br>2.1.4.0-001R<br>2.1.3.0-010R<br>2.1.2.0-010R<br>2.1.1.0-006R<br>2.1.0.0-029R<br>2.0.0.0-034R<br>1.4.3.0-012R<br>1.4.2.0-005R<br>1.4.1.0-014R<br>1.2.5.0-022R<br>1.1.4.30f |
|               | WS 5100 v1.4+   | 2.1.5.0-003R<br>2.1.4.0-001R<br>2.1.3.0-010R<br>2.1.2.0-010R<br>2.1.1.0-006R<br>2.1.0.0-029R<br>2.0.0.0-034R<br>1.4.3.0-012R<br>1.4.2.0-005R<br>1.4.1.0-014R                              |



---

| <b>Vendor</b> | <b>Hardware</b> | <b>Supported Versions</b>                                                                                                                                                    |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | WS 5100 v3.0+   | 3.3.3.0-006R<br>3.3.2.0-010R<br>3.3.1.0-003R<br>3.3.0.0-029R<br>3.2.0.0-040R<br>3.1.0.0-045R<br>3.0.4.0-004R<br>3.0.3.0-003R<br>3.0.2.0-008R<br>3.0.1.0-145R<br>3.0.0.0-267R |
| <b>Proxim</b> | 2000            | 2.5.5<br>2.5.3<br>2.5.2<br>2.4.11<br>2.4.5<br>2.4.4<br>2.3.3<br>2.3.1<br>2.2.2                                                                                               |



---

| <b>Vendor</b> | <b>Hardware</b> | <b>Supported Versions</b> |
|---------------|-----------------|---------------------------|
|               | 4000            | 4.0.12                    |
|               |                 | 4.0.3                     |
|               |                 | 4.0.2                     |
|               |                 | 4.0.0                     |
|               |                 | 3.7.0                     |
|               |                 | 3.6.3                     |
|               |                 | 3.4.0                     |
|               |                 | 3.2.1                     |
|               |                 | 3.1.0                     |
|               |                 | 2.6.0                     |
|               |                 | 2.5.2                     |
|               |                 | 2.4.11                    |
|               |                 | 2.4.10                    |
|               | 4900            | 4.0.12                    |
|               |                 | 4.0.9                     |
|               |                 | 4.0.3                     |
|               |                 | 4.0.2                     |
|               |                 | 4.0.0                     |
|               |                 | 3.7.0                     |
|               |                 | 3.6.3                     |
|               |                 | 3.4.0                     |
|               |                 | 3.2.1                     |
|               |                 | 3.1.0                     |



---

| Vendor   | Hardware        | Supported Versions                                                                                        |
|----------|-----------------|-----------------------------------------------------------------------------------------------------------|
|          | 600             | 2.5.5<br>2.5.3<br>2.5.2<br>2.4.11<br>2.4.5<br>2.4.4<br>2.3.3<br>2.3.1<br>2.2.2                            |
|          | 700             | 4.0.12<br>4.0.3<br>4.0.2<br>4.0.1<br>4.0.0<br>3.7.0<br>3.6.6<br>3.4.0<br>3.2.1<br>3.1.0<br>2.6.0<br>2.5.2 |
| SYSTIMAX | AirSPEED AP 541 | 2.6.0<br>2.5.2                                                                                            |





| Vendor | Hardware        | Supported Versions       |
|--------|-----------------|--------------------------|
|        | AirSPEED AP 542 | 2.6.0<br>2.5.2<br>2.4.11 |

\* These models are supported using a Extended Device Support script available from Wavelink. You must import the EDS script before Avalanche can manage these devices. To obtain an EDS script, contact Wavelink Customer Support. For more information on importing an EDS script, see Importing an Infrastructure Device Support File.

## Transitional Firmware

Transitional firmware refers to the rare cases when a particular firmware version is required when updating to a newer revision of firmware.

For example, when updating the WS5100 v1.4+ to a WS5100 v3.0+, you must first be on the 2.1.1.0-006R firmware, and then update to 3.0.0.0-267R. Once the update to 3.0.0.0-267R is completed, you may then update to any 3.x.x firmware.

Transitional firmware versions are fully supported in Avalanche.

The following is a list of transitional firmware:

|                               |                              |
|-------------------------------|------------------------------|
| <b>Cisco 350 AP</b>           | 12.2-13JA1                   |
| <b>Cisco 1200</b>             | 12.2-11JA1                   |
| <b>Motorola/Symbol WS2000</b> | 2.0.0.0-036R                 |
| <b>Motorola/Symbol WS5000</b> | 1.1.4.30SP1                  |
| <b>Motorola/Symbol WS5100</b> | 2.1.1.0-006R<br>3.0.0.0-267R |



## 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.

