Wavelink Avalanche Site Edition
Web Console User Guide

Version 5.0.1

asew-ug-501-20100824

Revised 24/8/2010

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

Email: sales@wavelink.com

Table of Contents

Chapter 1: Introduction

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

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

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

This section provides the following introductory information:

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

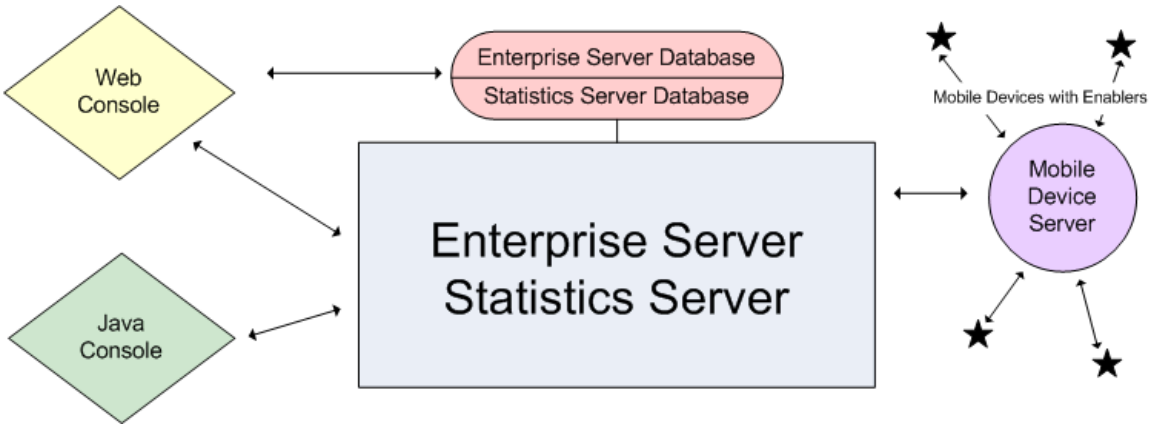
Managing Networks with Avalanche

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

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

Components of Avalanche

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



The primary components of Avalanche include:

- **Avalanche Java Console**. The Avalanche Java Console is your interface with wireless network components. With the Avalanche Console, you can manage and maintain everything from infrastructure device settings to mobile device software. The Java Console must be accessed from a computer where it has been installed.

- **Avalanche Web Console**. The Avalanche Web Console allows you to manage network components from any computer using an internet connection. It does not need to be installed.

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

- **Enterprise Server**. The Enterprise Server facilitates all communication between the Console, the distributed servers, and the enterprise database.

- **Statistics Server**. The Statistics Server collects statistical information from your devices and distributed servers for reporting purposes and stores information in the stats database.

- **Databases**. Avalanche databases store information about your network and devices. There are two databases for Avalanche. The enterprise database handles information such as managing device configuration. The stats database manages statistical information regarding the state of devices on your network.

- **Mobile Device Server**. The Mobile Device Server is server-side software responsible for communication between the Avalanche Console, enterprise and statistics servers, and your mobile devices.

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

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

Location Management: My Location and Sites

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

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

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

Getting Started

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

1. **Install Avalanche**. For more information on installing, refer to the Java Console help.

2. **Activate Mobile Device licenses for Avalanche**. You should activate the number of licenses based on the number of devices you want to manage. For more information on licensing, refer to the Java Console help.

3. **Configure profiles**. A profile allows you to manage configurations and settings centrally and then deploy those configurations to as many sites as necessary. In this way, you can update or modify multiple sites instead of manually changing

settings for each one. Avalanche provides network, scan to config, software, alert, Mobile Device Server, and mobile device profiles.

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

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

About This Document

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

This document makes the following assumptions:

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

This document uses the following typographical conventions:

`Courier New`	Any time you interact with the physical keyboard or type information into a text box that information appears in the `Courier New` text style. This text style is also used for any file names or file paths listed in the text. Examples: The default location is `C:\Program Files\Adobe\FrameMaker7.1.` Press `CTRL+ALT+DELETE`.
Bold	Any time this document refers to an option, such as descriptions of different options in a dialog box, that option appears in the **Bold** text style. This is also used for tab names and menu items. Examples: Click **Open** from the **File** Menu.
Italics	Any time this document refers to another section within the document, that section appears in the *Italics* text style. This style is also used to refer to the titles of dialog boxes. Examples: See *Components of Avalanche* on page 6 for more information. 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. These characteristics include creating profiles, assigning IP addresses, and monitoring network performance.

The Avalanche Console is traditionally accessed from a computer where the Console has been installed. This installed Console is the Java Console. However, using 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, and manage profiles and alerts.

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

This section contains the following topics for the Web Console:

- Launching the Avalanche Web Console
- Understanding the Web Console
- Viewing and Configuring System Settings

Launching the Avalanche Web Console

Using the Avalanche Web Console, you can configure and manage your wireless network. The Web Console does not need to be installed on each computer from which you want to access Avalanche. To access the Web Console, you will need:

- An internet browser, such as Internet Explorer or Firefox.
- An internet or LAN connection that can connect between the enterprise server and the computer from which you will be using the Web 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 did not perform a custom installation, the web components were installed automatically.

NOTE If you choose to use a certificate to create a secure connection, see *SSL Certificates* on page 128 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**.

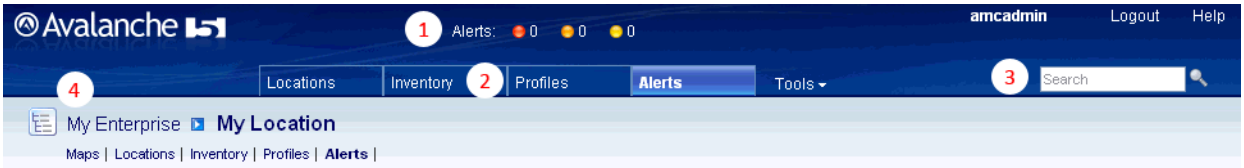
Avalanche is installed with a default login of *amcadmin* and password of *admin*.

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 context links. 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 region.

2. The management tabs provide access to inventories, alerts, and other properties of your enterprise. The **Tools** menu provides you with access to the Reports tool, scheduled tasks, Wavelink Remote Control, system support, information, and settings.

3. The search box allows you to search content in the Web Console.

4. The region navigation allows you to access information particular to a selected region. By selecting a region or location and then using the context links (underneath the name of the region), the information will be filtered to display only items pertinent to the selected region.

The rest of the page changes depending on which tab or context link you have selected, displaying panels with associated information.

This section gives details about the following areas:

- Management Tabs
- Region Navigation
- Panels
- Understanding Edit Mode

Management Tabs

The management tabs provide the user with available information relating to My Enterprise.

NOTE If you want to further filter the information displayed by location or site, use the context links to navigate.

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

- Maps

NOTE In Avalanche SE, **Maps** is only available as a context link.

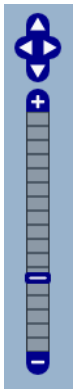
- Locations
- Inventory
- Profiles
- Alerts
- Tools Menu

Maps

From the Web Console map, you can view your location, the highest alert level associated with it, and the GPS position and history of your mobile devices.

You can filter the information displayed by region or location. Navigate to the desired region or location and use 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. When this option is enabled, My Enterprise, if it has a defined GPS location, will be displayed on the map.

Servers. When this option is enabled, My Location, if it has a defined GPS location, will be displayed on the map.

Sites. When this option is enabled, all sites that have defined GPS locations will be displayed on the map. You can view site-specific information in a callout box when you click on a site.

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.

To view the map on the Web Console:

- Click the Maps context link.

Locations

The **Locations** tab provides a panel with a summary of the location, a panel with details about any associated sites, and a panel of associated authorized users. For information on managing locations and sites with the Web Console, see *Location Management* on page 26.

Inventory

The **Inventory** tab provides panels listing mobile devices, the Mobile Device Server, and mobile device groups. You will only be able to see the devices, servers, and groups that are associated with My Enterprise.

Profiles

The **Profiles** tab provides panels listing applied and available profiles for the region. 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 regions and locations as necessary. The Applied Profiles panel displays the profiles that are currently applied to the selected region 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 region.

NOTE For information about specific profiles, see the Table of Contents. For information on applying a profile to a region or location, see *Assigning Profiles* on page 27.

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 region where they are assigned.

To change the priority of applied profiles:

1. In the Applied Profiles panel, click **Change Priority**.
2. The Change Priority page appears.
3. Reorder the profiles by dragging and dropping.
4. When you are done assigning priority, click **Save**.

Alerts

The **Alerts** tab provides a panel listing current alerts associated with your region. For information on viewing and acknowledging alerts, see *Using the Alerts Tab* on page 102.

Tools Menu

The **Tools** menu provides access to the Reports tool, scheduled tasks, Wavelink Remote Control, system support/information and settings. For tasks related to the Tools menu, see*Viewing and Configuring System Settings* on page 20.

Region Navigation

You can navigate to a specific location in your network and then display only the information applicable to that location by using the context links. By selecting a location and then using the context links, the Console will display only information pertinent to the selected location.

To navigate to a region or location to view:

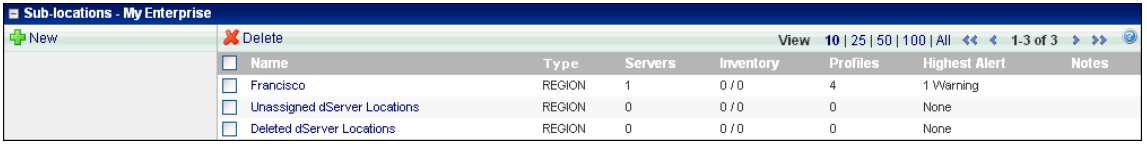
- Click the arrow to the right of the home location. A dialog box will appear, listing the available regions within the home region. Click the name of the region you want to navigate to.

  -Or-

- Click the tree view button to the left of the home location. The *Enterprise List* dialog box will appear, with tabs for a tree view or list of the available regions and locations. Using either the tree view or list, click the name of the region you want to navigate to.

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.



In the top left of the panel, the name of the panel is followed by the name of the region being displayed.

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-changing options. There is also a **Help** button that opens a window to a related help page.

To the left of the name of each item is a check box that allows you to select one or more items 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**.

Other tasks that can be performed in most panels include:

- Paging through Panels
- Sorting Columns

Paging through Panels

Some panels include large lists of information. By default, Avalanche 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.

Sorting Columns

Some of the columns in the panels give you the option of sorting the information in the list according to that column. You can sort a list according to column by clicking the header 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.

Understanding Edit Mode

Before you can edit a profile, device group, region properties, or server location properties, you must enter Edit Mode. While you are using Edit Mode, the item you are editing will be locked. While Edit Lock is engaged, no other user will be able to attempt to edit the configuration. Edit Lock has an automatic timeout, at which point you will be prompted in order to continue editing. If you do not respond to the prompt within the time configured, then your edit will be cancelled 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. For instructions on configuring these options, see the Java Console help.

Viewing and Configuring System Settings

From the Web Console, you can view system information and perform tasks related to managing the enterprise server. This section includes information on the following tasks:

- Viewing System Information
- Viewing the Audit Log
- Configuring General System Settings
- Configuring E-mail Settings

Viewing System Information

From the Web Console, you can view statistics about the enterprise server, Inforail, statistics server, and Mobile Device Server. 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 you 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.

Viewing the Audit Log

From the Web Console, you can view the audit log. The audit log collects information about actions performed from the Avalanche Console. As part of the data collection, the audit log includes the IP address of each Console that generated a logged event. Audit logging generates entries in the enterprise database. It can only be enabled and configured from the Java Console.

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

To view the audit log:

1 Click **Tools > Support**.

The System Information page appears.

2 Click **Audit Log**.

The Audit Log page appears.

3 Select the filter(s) 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 the checkbox next to the **Activity Type**.
- To filter events by username, enable **Username** and select the user from the drop-down list.

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

All events matching the filters appear in the list.

5 If you wish to delete all entries in the audit log, click **Clear Log**. This will delete the entries from the database.

Configuring General System Settings

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

To configure general system settings:

1 Click **Tools > Settings**.

The System Settings page appears.

2 If you want to configure the length of time before an inactive Web Console user is logged off, type the number of minutes in the text box under **Session Timeout**.

3 If you want to configure how many days an alert is displayed or how many alerts are stored in the database, type the appropriate numbers in the text boxes under **Alert Settings**.

4 If you want to configure the threshold for enterprise server messages allowed in the backlog, type the number of messages in the text box under **Message backlog**.

NOTE Any received messages beyond this threshold are stored in a file to disk until the backlog is reduced. Once the backlog is reduced, messages are pulled from the stored file back into the log.

---

5 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 enter 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 **Email Settings**.

The *Email Settings* dialog box appears.

3 Type the name or IP address of the **E-mail server**, the **Username** and **Password**, and the **Reply-to email address** in the provided text boxes.

4 Click **Save**.

Chapter 3: Managing User Accounts

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

There are two types of accounts: Administrator and Normal. An Administrator account can access and modify all the configurations in Avalanche. A Normal account is assigned to specific sites or profiles and is only authorized to view or make changes in his assigned areas.

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

NOTE Wavelink recommends that you create a new administrative user.

This chapter provides the following information about user accounts:

- Defining Permission Types
- Creating User Accounts
- Creating User Groups
- Assigning User Permissions
- Assigning Authorized Users

Defining Permission Types

There are two types of user account permissions:

- **Regional Permissions**. These permissions are specific to various tasks and components of Avalanche. For each component you can grant read or read/write access. Read allows the user to view the configurations and settings for the component. Read/write allows the user to configure parameters and settings for the specified component within his home region.
- **Profile Permissions**. These permissions allow the user complete global access to the specified profile. Administrators can grant read or read/write access for each

type of profile. Read/write allows the user to manage all aspects of the profile, from configuration to application. Read-only allows the user to view the profile, but does not allow any editing.

For details on each permission allowed, see *Assigning User Permissions* on page 25.

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

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

Creating User Accounts

Administrator accounts allow you to create new user accounts. A user account must be created from the Java Console. See the Java Console help for instructions on creating a new user account.

Creating User Groups

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

- Software Admin
- Help Desk
- Network Admin

These user groups are set with a series of default permissions. You can modify them to suit your needs. A user group must be created from the Java Console. See the Java Console help for instructions on creating a new user group.

Assigning User Permissions

If you have an Administrator account, you have unlimited permissions, and can assign and change permissions for Normal user accounts. Permissions must be configured from the Java Console. See the Java Console help file for instructions on assigning and changing multiple permissions.

Assigning Authorized Users

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

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

To add or remove an authorized user for a profile or group:

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

   -Or-

   From the **Inventory** tab, click on the name of the profile you want to configure.

2. Add or remove users as desired.

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

3. Click **Save**.

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

Chapter 4: Location Management

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

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

- Managing Sites
- Viewing Server Properties

Managing Sites

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

This section contains the following tasks for managing sites:

- Creating a Site
- Assigning Profiles
- Viewing Mobile Devices within Sites
- Editing Site Properties
- Additional Site Functions

Creating a Site

Creating sites allows flexibility in assigning profiles. A site must be created at My Location.

To create a site from the Web Console:

1. Navigate to My Location and click the **Locations** context link.
2. In the Sub-locations panel, click **New**.
3. Click **Site** in the *New Subordinate Location* dialog box that appears.

The New Site page appears.

4 Enter a name for the site.

5 Click **Launch Wizard** to use the Selection Criteria Builder to configure selection criteria for the site. For more information on using selection criteria, see *Using Selection Criteria* on page 104.

6 Enter any notes for the site in the provided **Notes** text box.

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

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

Assigning Profiles

Profiles are automatically assigned and applied at the My Enterprise level. If you want to apply profiles manually, you can disable the auto-assign option and then apply your profiles to My Enterprise or specific sites.

NOTE Disabling auto-assign must be done from the Java Console.

The profiles are applied to the mobile devices based on selection criteria for the profile and the order in which the profiles are listed in the Console.

To assign a profile to a site from the site page:

1 Navigate to the site.

2 Click the **Profiles** context link.

3 In the Available Profiles panel, enable the checkbox to the left of the profile(s) you want to apply and click **Apply**.

To assign a profile to a site from the profile page:

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

The profile details page appears.

2 In the Applied Locations panel, click **New**.

3 From the dialog box, select the site to which you want to assign the profile.

4 The site is added to the list of Applied Locations.

Viewing Mobile Devices within Sites

You can view the mobile devices that belong to an individual site from the **Inventory** tab of the Web Console.

To view the mobile devices:

- Navigate to the site for which you want to view mobile devices and click the **Inventory** context link.

  The mobile devices that belong to the site will appear in the Mobile Devices panel.

Editing Site Properties

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

NOTE Refer to *Building Selection Criteria* on page 105 for related information.

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

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

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

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

  The *Add Device Property* dialog box appears.

3 From the **Category** drop-down list, select **General** or **Custom** based on the property you are creating.

4 Enter the **Property Name** and **Property Value** in the provided text boxes.

5 Click **OK**.

The new property is added to the properties list.

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

Additional Site Functions

Sites allow you to more efficiently manage your mobile devices. These options are available from the Mobile Devices panel on the **Inventory** tab.

The additional options for sites are as follows:

Update	Allows you to update the selected mobile device(s) within that site immediately.
Message	Allows you to send a message to the device.
Ping	Allows you to ping the device.
Delete	Allows you to delete the device.
Locate	Allows you to plot the device on the map according the most recently reported GPS statistics. This option is only functional if the device(s) selected has reported GPS statistics.

Above the Mobile Device panel on the **Inventory** tab, there are two buttons: **Update Now** and **Send Message**. These buttons are global and not site-specific.

Viewing Server Properties

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

To view Server properties:

1 Navigate to My Location and click the **Locations** context link.

2 The Location Summary panel provides you with the status of the server, and whether the server is synchronized or in blackout. Click **Details** for more properties.

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.

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 all mobile devices meeting its selection criteria. General settings for a network profile include selection criteria for which devices apply the profile, IP address pools to assign addresses to mobile devices, and the ability to override the manual settings on the device. For information on configuring WLAN IP, WLAN, and WWAN, see *Configuring Scheduled Settings* on page 32.

To create a network profile from the Web Console:

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.

5 Click **Launch wizard** to use the Selection Criteria Builder to determine which devices the network profile manages. For details about creating and using selection criteria, refer to *Using Selection Criteria* on page 104.

6 To add a mobile device IP address pool, click **Edit**.

The *IP Address Pools* dialog box appears.

7 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)

8 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)

9 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

10 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.

NOTE If you want to delete addresses from the address pool, enable the checkbox to the left of the address and click **Delete**.

---

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

12 If desired, type any **Notes** in the text box.

13 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, see Configuring Scheduled Settings.

14 Click **Save**.

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

Configuring Scheduled Settings

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

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

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

This section contains information on the following configuration options:

- Configuring WLAN IP Settings
- Configuring WLAN Settings
- Configuring WWAN Settings
- Scheduled Profile Changes

Configuring WLAN IP Settings

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

Server Address — Provides mobile devices with the server address. You can provide the address, DNS name, or choose to **Use server address**. If you choose to use the server address, the mobile devices use the mask/address of the server to which the device connects.

NOTE If using a DNS name, click **Resolve** 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 choose to **Use server address**.

Subnet mask — Provides mobile devices with the subnet mask. You can provide the address, DNS name, or choose to **Use server address**.

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

Domain name — Provides the domain name for the devices.

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

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

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

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

To configure WLAN IP settings for a network profile:

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.

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

Encryption 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.

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

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

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

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

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

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 are using and what is supported by your Enabler and hardware. Authentication options include:

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

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

- **EAP_FAST/GTC**. (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling with Generic Token Card) EAP-FAST uses protected access credentials and optional certificates to establish a Transport Layer Security tunnel.
- **LEAP**. (Lightweight Extensible Authentication Protocol) LEAP requires both client and server to authenticate and then creates a dynamic WEP key.

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

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.

To configure 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 are using WEP keys, you must select either **40 Bit** or **128 Bit** key size, and create the keys. The keys you enter must be in hex format. A 40-bit key should have 10 characters and a 128-bit key should have 26 characters. To change the value for one of the hex digits in a key, type a new value (between 0-9 and A-F) in the appropriate text box. An example of a 40-bit key would be: 5D43AB290F.

- If you are using WEP key rotation, you must choose the 40 or 128 bit key size, the starting date and time, rotation interval, and a passcode.
- If you are using PEAP or TTLS authentication, you can enable the **Validate Server Certificate** option and provide a path to the certificate.
- If you are using EAP_FAST, you can provide a path to a PAC (Protected Access Credential) and the PAC password.
- If you are using an EAP method or LEAP, you can configure whether the **User Credentials** are **Prompt** (user is prompted when credentials are required) or **Fixed** (credentials are automatically sent when required).

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

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

Configuring WWAN Settings

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

Connection Name — A name for the connection.

Connection Type — There are two connection types available for your WWAN-enabled devices:

APN (GPRS / EDGE / 3G). Provide an Access Point Name if you are using a 3G connection. An example of an APN would be: wap.cingular

Dial-Up. The number to be dialed by the modem. This does not correspond to the number of the device.

Credentials — Provides the **Username**, **Password**, and **Domain**.

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

Enable TCP/IP header compression	Improves performance for low-speed connections.
Enable software compression	Improves performance for low-speed connections.
Activate phone as needed	Allows the Enabler to activate the device's phone if a WWAN connection is necessary.
Dial broadband connection as needed	Allows the Enabler to attempt a WWAN connection if a LAN connection cannot be established.
Public IP address for Avalanche Server	Provides the IP address of the enterprise server that is accessible from a WWAN. This is necessary if the device tries to contact the server when connected through a WWAN network outside of the server's local network.

To configure WWAN settings:

1. From the 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.

Scheduled Profile Changes

Scheduled settings allow you to change the settings for a network profile and apply those changes at a specific time. When you configure WLAN IP, WLAN, and WWAN settings, you can select the time you want those settings to become effective.

To schedule network profile changes:

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 Type the **Start Date** and **Time** in the text boxes, and configure the WLAN IP, WLAN, and WWAN settings for the epoch.

4 Click **Save**.

The scheduled network profile settings will come into effect at the date and time set for the epoch.

Chapter 6: Managing Scan to Configure Profiles

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

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

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

This section contains instructions for the following tasks:

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

Configuring Scan to Config Profiles

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

- Adding Scan to Config Profiles
- Editing Registry Keys for Scan to Config Profiles
- Editing Custom Properties for Scan to Config Profiles

Adding Scan to Config Profiles

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

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

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

NOTE WEP key rotation is not supported by 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.

5. Set the maximum length of the 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. Choose which epoch to use by enabling either **Use current profile settings** or **Use scheduled profile change effective** and selecting 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.

Editing Registry Keys for Scan to Config Profiles

You can add registry keys and values to a Scan to Config profile. When the profile is scanned by a device, those keys and values are added to the device's registry. You also have the option to edit or remove existing registry keys or values on the device's registry. 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
- Editing or Removing a Registry Key or Value

Adding a Registry Key

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

To add a registry key:

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

   The Scan to Config Profile Details page appears.

2. Click **Edit**.

   The Edit Scan to Config Profile page appears.

3. In the Registry Keys region, click **New**.

   The *New Registry Entry* dialog box appears.

4. Select the **Root Key** from the drop-down list.

5. Type the name of the new key in the **Key** text box.

6. Type the value of the key in the **Name** text box.

7. Enter the data for the value in the **Data** text box.

8. Select the **Type** of the value from the drop-down list.

9. Select **Create key** as the **Action**.

10. Click **Add** to add the registry key and value to the list.

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

To edit or remove a registry key value:

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 **Edit**.

The Edit Scan to Config Profile page appears.

3 In the Registry Keys region, click **New**.

The *New Registry Entry* dialog box appears.

4 Select the **Root Key** from the drop-down list.

5 Type the name of the key in the **Key** text box.

6 Type the value of the key in the **Name** text box.

7 Enter the data for the value 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**.

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

Editing 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 would be `location = Chicago`. Once a custom property has been applied to a device, you can use it as a selection criterion. You can apply custom properties to mobile devices through a Scan to Config profile.

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

This section contains information on the following tasks:

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

Adding a Custom Property

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

To add a custom property:

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

   The Scan to Config Profile Details page appears.

2. Click **Edit**.

   The Edit Scan to Config Profile page appears.

3. In the Device Properties region, click **New**.

   The *New Property* dialog box appears.

4. Type the category to which you want to add the property in the **Optional group** text box.

5. Type the **Property Name** and **Property Value** in the text boxes.

6. Select **Create property** as the **Action**.

7 Click **Save**.

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

Editing or Removing a Custom Property

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

To edit or remove a custom property:

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

The Scan to Config Profile Details page appears.

2 Click **Edit**.

The Edit Scan to Config Profile page appears.

3 In the Device Properties region, click **New**.

The *New Property* dialog box appears.

4 Type the category to which you want to add the property in the **Optional group** text box.

5 Type the **Property Name** and **Property Value** in the text boxes.

6 Select **Create property** as the **Action** if you are editing the property. Select **Delete property** as the **Action** if you are deleting the property.

7 Click **Save**.

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

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` which you can save or send to a printer.

To print 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**.

3. 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. This sends the configurations to the Enabler and updates the network profile.

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

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

To scan the configuration:

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

   The *Scan Configuration* dialog box appears.

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

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

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

Chapter 7: Managing the Mobile Device Server

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

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

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

- Configuring Mobile Device Server Profile Settings
- Viewing Mobile Device Server Details

Configuring Mobile Device Server Profile Settings

Mobile Device Server profiles are used to manage your Mobile Device Servers. This section provides information on the following elements associated with creating a Mobile Device Server profile:

- Server Security
- Server Resources
- License Return
- Device Specific File Transfers
- Terminal ID
- Server Logging
- Device Statistics

- Communications Restrictions
- Scheduling Profile-Specific Device Updates
- Mobile Device Server Profile Authorized Users
- Creating a Mobile Device Server Profile

Server Security

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

Avalanche offers two options for encryption:

- **Transport Encryption**. When you enable transport encryption, Avalanche will match the level of encryption with the capacity of the mobile device. TCP/IP communication between the Mobile Device Server and mobile devices will be encrypted to the degree possible.
- **Strict Transport Encryption**. When you enable strict transport encryption, Avalanche will use AES encryption for information. Only devices that support AES encryption (Enabler 5.0 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**. This option requires mobile devices to connect to the network through a wired connection (such as a cradle) and receive an authentication key. When you enable this option, the Mobile Device Server will challenge any device attempting to connect to the Server for a password. If the mobile device does not have the correct password, the Mobile Device Server will not allow a TCP/IP connection.

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

- **Server Authentication**. This option forces mobile devices to communicate with a single known server. Mobile devices must first connect to the network through a wired connection to receive information about the server with which they are allowed to communicate. When you enable this option, the mobile device will challenge any Mobile Device Server attempting contact for a password. If the

Mobile Device Server does not have the correct password, the mobile device will not allow a TCP/IP connection.

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

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

Server Resources

You can configure Mobile Device Servers to automatically listen for mobile devices using the serial ports on a remote system. Only one application on a host system can maintain ownership of a serial port. If the Mobile Device Server controls the serial ports on the host system, then no other application will be able to use them. Likewise, if another application on the host system (for example, Microsoft ActiveSync) has control of the serial ports, then the Mobile Device Server will not be able to use them.

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

You can also restrict the number of devices that can update concurrently. These details can be configured from the Mobile Device Server Profile Details page.

License Return

From the Mobile Device Server Profile Details page, you can configure the return of licenses to the unused pool when a device has not contacted a server after a period of time. The period of time which must elapse before the license is released can be configured. The minimum number of days is five.

Secondary Server

Avalanche allows you to configure Mobile Device Server profiles with secondary server support. This allows mobile devices to attempt to connect to a secondary Mobile Device Server if the primary server is not available. Mobile devices attempt to connect to the servers in the Secondary Server List. If the device cannot connect to the first server on the list, it will move to the next server on the list until it is able to

connect to a server. If the mobile device can not connect to any servers, it remains offline and an alert appears in the Alert Browser.

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

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

You can configure the following settings:

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

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

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

Device Specific File Transfers

From the Mobile Device Server Profile Details page, you can configure where package files are stored. There are two storage directories that can be configured:

- **Directory for file uploaded to 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 file downloaded from 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.

Terminal ID

The Mobile Device Server assigns each device a terminal ID the first time that the device communicates with Mobile Device Server. The number the Mobile Device Servers selects is the lowest number available in a range of numbers configured from the Mobile Device Server Profile Details page.

You can also configure your own alphanumeric terminal ID range. Use a C-style format to create a generation template. For example, `Seattle-%d` would generate IDs such as `Seattle-4`, and `Seattle-%05d` would generate IDs such as `Seattle-00004`.

Server Logging

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

You can set the log function to the following levels:

- **Critical**. This level writes the least information to the log file, reporting only critical errors that have caused the Mobile Device Server to crash.

- **Error**. This level writes errors that are caused by configuration and/or communication problems as well as and Critical messages to the log file.

- **Warning**. This level writes Critical messages, Error messages, and indicates possible operational problems in the log file.

- **Info**. This level is the default logging level. This logging level documents the flow of operation and writes enough information to the log file to diagnose most problems.

- **Debug**. This logging level writes large amounts of information to the log file that can be used to diagnose problems.

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

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

Device Statistics

From the Mobile Device Server Profile Details page, you can configure whether mobile devices upload statistics, inventory, and properties to the Mobile Device Server. The options include:

- **Device Chat Timeout**. This option sets the amount of time in minutes that both the device and the server will wait before dropping a chat session.

- **Device Comeback Delay**. This option sets the amount of time in minutes that the mobile device will wait before trying to reconnect to the Mobile Device Server after a connect rejection (i.e., if the device tried to connect during an exclusion window).

- **Enable Device Caching**. This option enables mobile devices to download software package files from other mobile devices on the same subnet instead of from the Mobile Device Server. Device caching reduces the demands on the Mobile Device Server during software package synchronization. For information about implementing device caching, call Wavelink Customer Support.

- **Enable Persistent Connection**. This option causes each device to create a persistent TCP connection with the Mobile Device Server. This ensures

communication in an environment where UDP packets cannot reliably be transmitted between the server and the device.

- **Enable SMS Notification**. This option allows the Mobile Device Server to use SMS notification if a device cannot be reached by UDP packets. This option is only available for devices with a phone, and must also be configured on the device and at the enterprise server. For more information on enabling SMS notification, call Wavelink Customer Service.

- **Suppress GPS Data Collection**. When this option is enabled, the Mobile Device Server will discard GPS data collected from the devices rather than transmitting it to the enterprise server.

- **Suppress radio statistics collection**. When this option is enabled, the Mobile Device Server will discard radio statistics data collected from the devices rather than transmitting it to the enterprise server.

- **Suppress software inventory collection**. When this option is enabled, the Mobile Device Server will discard software profile data collected from the devices rather than transmitting it to the enterprise server.

- **Suppress real-time properties collection**. When this option is enabled, the Mobile Device Server will discard realtime properties data collected from the devices rather than transmitting it to the enterprise server.

Communications Restrictions

To allow you more control over bandwidth usage, Avalanche uses communication restrictions. During a server-to-server blackout, the Mobile Device Server is not allowed to communicate with the Enterprise Server. During a device-to-server exclusion, 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 region.

   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.

5 Click **OK**.

Scheduling Profile-Specific Device Updates

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

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

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

individually rather than consulting the meta-file, which 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 region.

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

6 If desired, enable the **Stop if not completed by** option. Set the stop date and time.

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

7 Enable the other update options as desired.

8 Click **Save**.

The update appears in the Device Update Schedule region.

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

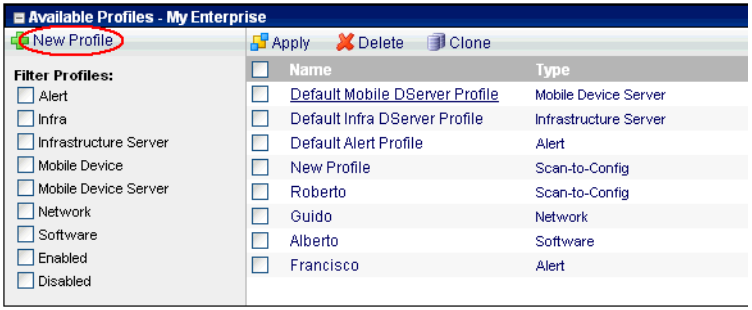
Mobile Device Server Profile Authorized Users

For information on adding an authorized user for the Mobile Device Server profile, see *Assigning Authorized Users* on page 25.

Creating a Mobile Device Server Profile

To create a Mobile Device Server profile:

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



The *New Profile* dialog box appears.

2 Select **Mobile Device Server 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 options as desired.

6 Click **Save**.

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

Viewing Mobile Device Server Details

The Web Console allows you to view details about your mobile device servers. You can view the server version, time started, status, and information about licensing and serial ports. receives licensing messages from the deployed Mobile Device Servers.

To view details of a Mobile Device Server:

1. From the Web Console, click **Tools > Support**.

   The System Information page appears.

2. Next to **Mobile Device Server(s)**, click **Details**. From the list that appears, click the name of the server for which you want to view details.

3. The Mobile Device Server Details page appears. This page displays the server version, start time, status, and information about current licenses and serial ports.

4. If you want to view the licensing messages associated with the server, click **License Messages**.

Chapter 8: Managing Software Profiles

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

This section contains the following topics:

- Creating a Software Profile
- Managing Software Packages

Creating a Software Profile

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

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, you can 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, refer to *Using Selection Criteria* on page 104.
6. Click **Save**.
7. The software profile is created and can be configured and assigned to a region or location.

Managing Software Packages

A software package is a collection of application files that are installed on a mobile device. The package also 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 install and configure the software packages associated with that software profile. You can enable the package, configure how the package is activated and distributed, and use the package utilities to configure it.

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.
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: • **Control.** An internally used package specific to the Avalanche Console. A network profile is an example of a control package. • **Application.** These packages install an application which can be run from the Application Menu screen on the mobile device. An example of an application package is the Telnet Client. • **Support.** These packages deliver files and do not add new items to the Application Menu screen on the mobile device. An example of a support package is a package that updates an existing file. • **Auto Run.** These packages automatically run after download but do not appear in the mobile device's application list. An Enabler Update Kit is an example of an auto run package.
Version	Displays the version of the software package.

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

Adding 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.

You can add packages, copy packages from another profile, or create custom software packages from the Web Console. Before you create a custom package, ensure you know the location of all the files you want to include.

You can also enable and configure the software package. The following instructions provide information about adding an existing Avalanche package to a software profile. For information about building a new package refer to *Building New Software Packages* on page 62.

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** and browse to the location of the software package.

4 Select the file and click **Next.**

A License Agreement appears.

5 Accept the license agreement and click **Next**.

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

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

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

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

Building New Software Packages

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

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**.

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

5 Browse to the location of the file(s) 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 following options:

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

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

8 Click **Next**.

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

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

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

10 Click **Next**.

11 The 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.

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

Installing CAB or MSI Packages

You can use Avalanche to push `.cab` or `.msi` files to your mobile devices. When you copy a `.cab` file onto a device, 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 Enter the name of the package (limit: eight characters).

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 is copied.

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 the name of the package you want to enable.

The Software Package Details page appears.

3 Click **Edit**.

4 Enable the **Enabled** checkbox.

5 Click **Save**.

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. Each time you use package configuration utilities, the utility and current settings are downloaded to the local machine where you are working, and then the settings are saved to the Enterprise Server database.

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.

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 from the list and click **OK**.

4 The *Configure Software Package* dialog box appears and the package utility is downloaded. Click **Next**.

5 From the list, select the configuration utility you want to run and click **Launch Config**.

6 The utility is launched. Configure the package options as desired.

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.

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.

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

5 Save your changes.

Peer-to-Peer Package Distribution

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

Peer-to-peer package options are set for each package, rather than for the software profile. The following table provides descriptions of the configuration options on the Web Console for peer-to-peer package distribution:

Field	Description
Use mobile device for proxy distribution of this package	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 proxy device.
Only distribute to proxy devices until	Enable this option to configure the time at which a non-proxy device can contact a proxy device to receive an update. A non-proxy device refers to a mobile device that is not being used to update other mobile devices.
Enforce proxy distribution until	Enable this option to configure the time at which a non-proxy 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 proxy device to receive the update. If a proxy device cannot be contacted or the connection times out, the device will then attempt to contact the Server.

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

If	Then Proxy Devices	And Non-proxy Devices
Only distribute to proxy devices until is enabled and the configured time has not been reached (**Enforce proxy distribution until** is not enabled)	*Can* contact the Server for updates at any time.	Cannot contact any proxy devices. Will attempt to contact the Server to receive updates.
Only distribute to proxy devices until is enabled and the configured time has been reached (**Enforce proxy distribution until** is not enabled)	*Can* contact the Server for updates at any time.	*Can* contact proxy devices to update and receive the profile. If the device cannot contact a proxy device, it will attempt to contact the Server.
Only distribute to proxy devices until is enabled and **Enforce proxy distribution until** is enabled and the configured time has not been reached	*Can* contact the Server for updates at any time.	Cannot contact the Server for updates. Cannot contact any proxy devices.
Only distribute to proxy devices until is enabled and **Enforce proxy distribution until** is enabled and the configured time has been reached	*Can* contact the Server for updates at any time.	*Can* contact proxy devices to receive updates. If the device cannot contact a proxy device or the connection times out, the device *can* contact the Server to receive updates.
No options are enabled	*Can* contact the Server for updates at any time.	*Can* contact proxy devices or Server for updates at any time.

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 Click **Save**.

Chapter 9: Managing Mobile Devices

This section provides information about the following mobile device topics:

- Mobile Devices Panel
- Mobile Device Details Page

Mobile Devices Panel

The Mobile Devices panel on the Inventory page shows a set of mobile devices based on the currently selected region or 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.
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**.

Above the Mobile Device panel on the **Inventory** tab, there are two buttons: **Update Now** and **Send Message**. These buttons are global and not site-specific. They allow you to update all mobile devices, or send a message to all mobile devices.

You can also customize the columns in the **Mobile Device Inventory** tab to display according to your preference.

This section provides information about the following tasks:

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

Inventory Paging

The Mobile Devices panel allows you to select how many devices you want to appear in the panel at a time.

To configure inventory paging:

1. From the top right corner of the Mobile Devices region, select the number of devices you want to display.
2. Use the arrow keys to move forward and backward through the pages.

Displaying Custom Mobile Device Icons

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

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

Deleting Mobile Devices

You can delete mobile devices from the Mobile Devices panel. This removes the device from the list and releases the license that mobile device was using.

To delete mobile devices:

1. In the Mobile Devices panel, select the check box next to the device(s) you want to delete.

2 Click **Delete**.

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

Editing Columns

The Web Console allows you to control which columns appear in the Mobile Devices panel and the order in which they display.

To edit the columns displayed:

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

The *Modify Columns* dialog box appears.

Column headers listed in the Available Columns list are headers that do not currently display in the panel. Column headers listed in the Selected Columns list are those that currently display in the panel.

2 From the Available Columns list, select which column you want to display and click **[>]**.

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 **[<]**.

The column name returns to the Available Columns list.

4 Use **Move Up** and **Move Down** 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.

Adding Custom Columns

If you have created custom properties for your mobile devices, you can display them in a column in the Mobile Devices panel.

For details about creating custom properties, refer to *Creating Custom Properties* on page 81.

To display columns for custom properties:

1. In the Mobile Device region on the **Inventory** tab, click **Modify Columns**.

   The *Modify Columns* dialog box appears.

2. Click **Add Custom**.

   The *Add Custom Property* dialog box appears.

3. From the **Property Key** drop-down list, select the custom property you want to add as a column.

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

5. From the **Data Type** drop-down list, select the data type for this property.

6. In the **Tool tip** text box, type the name of the tool tip you want to display.

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 **[>]** to move the property to the Selected Columns list.

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

   The columns are arranged to reflect your modifications.

Managing Device Filters

You can filter which devices are displayed in the Mobile Devices panel by applying mobile device filters. When a filter is applied, only the devices meeting the criteria associated with that filter will be displayed.

Avalanche automatically creates a filter for each model of device that it is managing. These filters appear to the left of the inventory list. You can also create your own filters by using selection criteria.

This section contains the following information:

- Editing Custom Device Filters
- Applying Device Filters

Editing Custom Device Filters

You can create a filter for the Mobile Devices panel, so that the panel only displays the devices meeting the defined selection criteria. Custom filters can also be deleted from the Modify Filters page.

To create a filter:

1. In the Mobile Devices panel, click **Edit Filters**.

   The Modify Filters page appears.

2. Enter a name for the new filter in the **Filter Name** text box.

3. Click the **Launch Wizard** button.

   The *Selection Criteria Wizard* dialog box appears, allowing you to create a filter based on a variety of mobile device characteristics. See *Building Selection Criteria* on page 105 for more information on building selection criteria.

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

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

5. Click **Add Filter**.

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

6. Click **Save**.

   You can now select the filter from the **Use Custom Filter** drop-down list located in the Mobile Devices panel.

Applying Device Filters

Device filters can be applied in the Mobile Devices panel. When the filter is applied, only the devices matching the selection criteria of the filter will appear in the Mobile Devices panel.

You can have multiple model filters selected at one time.

To apply a filter:

- Enable the check box next to the model filter you want to apply.

  -Or-

7 From the Mobile Devices panel, enable **Use Custom Filter** option and select the filter from the drop-down list.

Mobile Device Details Page

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 regions:

- **Summary Information**. This region provides a quick summary of device, health, signal strength and battery life information. The Health Data 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.
- **Tools** panel. Provides tools for contacting and managing your device. For information on using the tools in this panel, see *Contacting a Mobile Device* on page 76.
- **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* on page 80.
- **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.
- **Alerts** panel. Displays any current alerts associated with the mobile device.

To view mobile device details:

- In the Mobile Devices panel on the **Inventory** tab, click the name of the device for which you want to view details.

Contacting a Mobile Device

This section provides information about the following tasks that you can perform from the Tools panel on the Mobile Device Details page:

- Sending Messages
- Pinging a Mobile Device

- Updating a Mobile Device
- Locating a Device
- Locating a Device using Cell Tower Information
- Viewing Location History

Sending Messages

You can 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 Text Message* dialog box appears.

3. Type a message in the **Text Message** field.

4. Enable the **Provide Audible Notification** option if you want a sound to play when the mobile device receives the message.

5. Click **OK**.

   The Status field in the Activity region 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**.

Pinging a Mobile Device

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 device you want to ping in the Mobile Devices panel.

2 The Mobile Device Details page appears.

3 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**.

Updating a Mobile Device

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

NOTE The rules that govern which mobile devices can receive a particular update are determined by the selection criteria. See *Building Selection Criteria* on page 105 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.

- Enable the **Allow User to Override the Update** option if you want to give the mobile device user the option to override the update.
- Enable the **Force Package Synchronization** option if you want to force the package to update the device.
- Enable the **Delete Orphan Packages** option if you want to remove orphan packages from the mobile device.

- Click **Edit list of orphans to delete** if you want to select which orphan packages you want to remove.

3 Click **Update Device(s)**.

The Status field displays the status of the update.

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

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

Locating a Device

From the Web Console, 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 with its GPS details in a callout box. 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.

3 Click **Locate**.

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 region 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 region, 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**.

   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.

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

NOTE Refer to *Building Selection Criteria* on page 105 for more information on using properties as selection variables.

From the Properties panel of the Mobile Device Details page, you can perform the following tasks:

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

Viewing Properties

You can view the properties associated with a specific mobile device being managed by Avalanche.

To view the properties:

- From the **Inventory** tab, click the device you want to view properties for in the Mobile Devices panel.

  The Mobile Device Detail page appears.

The following list describes the columns that appear in the Properties panel:

Property Group	The group the property belongs to.
Data Type	Indicates if the value is configurable or snapshot.
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, the column will display the pending value in italics.

Creating Custom Properties

From the Web Console, you can create custom properties on the mobile devices. These properties can then be used to build selection criteria for software updates or a filter.

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 the Java Console help.

To create custom properties:

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

   The Mobile Device Details page appears.

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

   The *New Property* dialog box appears.

3. Type the category to which you want to add the property in the **Group (optional)** text box.

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

5. Select **Create property** as the **Action**.

6. Click **Add and 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.

Deleting Properties

You can delete any configurable mobile device property 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**.

4. The property will be deleted from the mobile device.

Chapter 10: Mobile Device Profiles

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

- Creating and Configuring Mobile Device Profiles
- Mobile Device Profile Authorized Users
- Editing Registry Keys for Mobile Device Profiles
- Editing Custom Properties for Mobile Device Profiles
- Configuring Mobile Device Profile Advanced Settings

Creating and Configuring Mobile Device Profiles

When you create a mobile device profile, you can enable it, and define orphan package removal and selection criteria.

To configure mobile device profile general settings:

1. If you are creating a new mobile device profile, click **New Profile** in the Available Profiles panel and click **Mobile Device Profile** from 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. Select **Enabled** if you want to enable the profile.

3. If you want to restrict which mobile devices use the profile, click **Launch wizard** to use the Selection Criteria Builder to create selection criteria for the profile. For more information on using the Selection Criteria Builder, see *Using Selection Criteria* on page 104.

4. If there is a package you want removed from the devices when it becomes orphaned, click the **__ defined** link by the **Orphan package removal** option. In the *Orphan Packages Removal List* dialog box, type the name of the package in the text

box and click **Add**. To delete a package from the list, click the **Delete** icon to the left of the package name. Click **Save** to save your changes and close the dialog box.

5 If desired, type any notes in the **Notes** text box.

6 If you want the mobile devices to communicate with a specific server, type the address of the server in the **Server Address** text box.

7 If you want to enable SMS notifications, enable the **Enable SMS Notification** check box.

8 If you want to **Force Package Synchronization** when the devices connect, enable the check box.

9 If you want to **Restrict simultaneous device updates**, enable the check box and the set the maximum number of devices that can update simultaneously.

Click **Save** to save your changes.

Mobile Device Profile Authorized Users

You can add authorized users for all mobile device profiles or enable a user for a specific mobile device profile. For information on adding an authorized user, see *Managing User Accounts* on page 23.

Editing Registry Keys for Mobile Device Profiles

You can add registry keys and values to a mobile device profile. The keys and values are then deployed to the devices where that profile is applied. You also have the option to edit or remove existing registry keys or values on the devices where the profile is applied. You must know the name and location of the key in order to edit or remove it.

This section contains information on the following tasks:

- Adding a Registry Key
- Removing a Registry Key

Adding a Registry Key

You can add registry keys to a mobile device profile. These keys will be added to the device when the profile is deployed to the mobile devices.

To add a registry key:

1. From the **Profiles** tab, click the name of the mobile device profile you want to configure.
2. The Mobile Device Profile Details 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 parent **Key** in the text box.
6. Enter a **Name** and **Data** for the key and its value.
7. Select **Create Key** as the **Action**.
8. Click **Add and Save**.

   The key is added to the profile and will be added on the mobile device when it receives the profile.

Removing a Registry Key

You can remove an existing registry key on a mobile device through a mobile device profile. You must know the name of the key/value in order to remove it.

To remove a registry key:

1. From the **Profiles** tab, click the name of the mobile device profile you want to configure.
2. The Mobile Device Profile Details 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 parent **Key** in the text box.

6 Enter a **Name** and **Data** for the key and its value.

7 Select **Delete key** as the **Action**.

8 Click **Add and Save**.

The key deletion action is added to the profile.

Editing Custom Properties for Mobile Device Profiles

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

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

This section contains information on the following tasks:

- Adding a Custom Property
- Removing a Custom Property

Adding a Custom Property

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

To add a custom property:

1 From the **Profiles** tab, click the name of the mobile device profile you want to configure.

2 The Mobile Device Profile Details page appears.

3 In the Properties panel, click **New**.

The *New Property* dialog box appears.

4 If you want the property to belong to a specific group, type the name of the group in the **Optional group** text box.

5 Type the **Property Name** and **Property Value** in the text boxes.

6 Select **Create property** as the **Action**.

7 Click **Add and Save**.

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

Removing a Custom Property

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

To remove a custom property:

1 From the **Profiles** tab, click the name of the mobile device profile you want to configure.

2 The Mobile Device Profile Details page appears.

3 In the Properties panel, click **New**.

The *New Property* dialog box appears.

4 Type the name of the **Optional Group** to which the property currently belongs in the text box.

5 Type the current **Property Name** and **Value** in the text boxes.

6 Select **Delete property** as the **Action**.

7 Click **Add and Save**.

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

Configuring Mobile Device Profile Advanced Settings

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

- Location Based Services
- Geofence Areas
- Regional Settings
- Update Restrictions

Location Based Services

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

- **Enable location-based services**. Enables GPS reporting for devices using the selected mobile device profile.
- **Reporting interval**. Determines how often the device reports its GPS statistics to the Mobile Device Server.
- **Report location using cell towers**. Uses information from nearby cell towers to establish the location of the device.
- **Report location using GPS**. Uses GPS coordinates to establish the location of the device.
- **GPS acquisition timeout**. Determines how often the device checks its GPS coordinates.
- **Prompt user to initiate GPS acquisition**. Prompts the mobile device user to ask if Avalanche should be allowed to collect and report location-based data. This prompt will appear when the Enabler is launched.
- **Notify user after __ consecutive GPS failures**. Provides a notification to the mobile device user after the device has failed to acquire GPS coordinates the specified number of times.

To configure location-based services:

1. From the **Profiles** tab, click the name of the mobile device profile you want to configure.
2. The Mobile Device Profile Details page appears.
3. In the Other Settings panel, configure the options as desired.
4. Save your changes.

Geofence Areas

A geofence is a virtual perimeter defined by GPS coordinates. You can configure a geofence area for your mobile devices. 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 Home area.

To configure a geofence area:

1. From the **Profiles** tab, click the name of the mobile device profile you want to configure.
2. The Mobile Device Profile Details page appears.
3. Click **Edit**.
4. In the Geofence Areas panel, click **New**.

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

3. Enable the **Manage time zone** check box and select the time zone from the drop-down menu.

4. Enable the **Automatically adjust clock for Daylight Savings Time** if you want the devices to switch over automatically.

5. Save your changes.

Update Restrictions

To allow you more control over bandwidth usage, Avalanche uses blackout windows. During a device-to-server restriction, 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.

4. Click **Save**.

Chapter 11: Managing Mobile Device Groups

To better organize your wireless network, you can use the Web Console to create collections of mobile devices, called mobile device groups. These groups allow you to manage multiple devices simultaneously, using the same tools available for managing individual mobile devices. Mobile device groups can include devices from the entire network, regardless of the location of the device. Each mobile device can be a member of multiple mobile device groups.

The topics in this chapter include:

- Creating Mobile Device Groups
- Adding Mobile Device Group Authorized Users
- Sending Messages to Mobile Device Groups
- Locating Devices in a Mobile Device Group

Creating Mobile Device Groups

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

- **Dynamic Mobile Device Groups**. When you create a dynamic group, you configure the selection criteria for the devices you want to belong to the group. Avalanche retrieves devices currently listed in the Mobile Device Inventory list that match the selection criteria. If a new device that matches the selection criteria for that mobile device group connects to Avalanche, it is automatically placed in the mobile device group. Therefore, dynamic mobile device groups will continuously add and remove mobile devices based on the selection criteria, without continued management.

- **Static Mobile Device Groups**. A static mobile device group contains all the mobile devices in your inventory that match a set of configured selection criteria.You configure the selection criteria when the group is created, and then the devices currently in the Mobile Device Inventory that match the selection criteria are added to the group.

After the group has been created, any further changes must be done manually. If a new device matching the selection criteria for a static mobile device group connects to the Avalanche Console, it will not automatically be added to the mobile device group.

This section contains the following information:

- Creating a Mobile Device Group
- Adding Devices to a Static Group
- Removing Devices from a Static Group

Creating a Mobile Device Group

When you create a mobile device group, you can make it dynamic or static. Devices will be added to the group if they match the specified selection criteria.

To create a mobile device group from the Web Console:

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.

Adding Devices to a Static Group

A static mobile device group does not change when the device inventory changes. If you want to add devices to a static group, you must do it manually.

To add devices to a static group:

1. Click the **Inventory** tab.

2 In the Mobile Device Groups panel, click the name of the group you want to modify.

The Mobile Device Group page appears.

3 In the Mobile Devices panel, click **Add**.

4 The Selection Criteria Builder launches, and you can create selection criteria for the devices you want to add to the group.

NOTE The selection criteria do not need to match the selection criteria that were specified when the group was created.

5 When you are finished defining selection criteria, click **OK**.

The devices matching the new selection criteria will be added to the group, but none of the devices already in the group will be compared with the selection criteria. Devices already in the group will stay in the group unless removed manually.

Removing Devices from a Static Group

You can manually delete devices from a static mobile device group after they have been added. You cannot use selection criteria to remove devices from a static group.

To remove devices from a static group:

1 Click the **Inventory** tab.

2 In the Mobile Device Groups panel, click the name of the group you want to modify.

The Mobile Device Group page appears.

3 In the Mobile Devices panel, select the check box to the left of the name of the device(s) you want to remove from the group.

4 Click **Remove**.

The device is removed from the group.

Adding Mobile Device Group Authorized Users

You can add authorized users for all mobile device groups or enable a user for a specific mobile device group. For information on adding an authorized user, see *Managing User Accounts* on page 23.

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. Navigate to the Home location of the mobile device group you want to send a message to.
2. Click the Inventory context link.
3. In the Mobile Device Groups panel, click the name of the group you want to send a message to.

   The Mobile Device Group page appears.
4. In the Mobile Devices panel, enable the check box to the left of the name of the devices you want to send a message to.
5. Click **Message**.

   The *Send Message* dialog box appears.
6. 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.

Locating Devices in a Mobile Device Group

From the Web Console, 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 with its GPS details in a callout box. You can view location from either the Mobile Devices panel on the **Inventory** tab or from the Mobile Device Group Details page.

To view the location of a mobile device in a mobile device group:

1 Click the **Inventory** tab.

2 In the Mobile Device Group panel, click the name of the mobile device group containing the device you want to locate.

The Mobile Device Group Details page appears.

3 In the Mobile Devices panel, select the check box next to the device you want to locate.

NOTE If you select more than one device, Avalanche will display only the first selected device on the list.

4 Click **Locate**.

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.

Chapter 12: Managing Alert Profiles

You can manage alerts in Avalanche using alert profiles. An alert profile gives you options for configuring what events generate an alert and who is notified when an alert is generated. Examples of what might generate an alert might be if a server goes offline or if a new mobile device is discovered.

This chapter provides information about the following topics:

- Managing Alert Profiles
- Using the Alerts Tab

Managing Alert Profiles

Alert profiles can be configured according to what events you want to generate an alert and if alerts should be forwarded to a proxy or e-mail account. A default alert profile is created when Avalanche is installed and is automatically applied to a Mobile Device Server. The default profile can be modified according to your preferences.

This section provides the following alert-related tasks:

- Creating Alert Profiles
- Editing Alert Profiles
- Importing and Exporting E-mail Addresses
- Alert Profile Authorized Users

Creating Alert Profiles

Alert profiles are configured with a list of events that will generate an alert. These profiles are then deployed to the Server Locations. When an event on the list occurs, an alert is generated and sent to the Avalanche Console. If the profile is configured for forwarding the alert to e-mail recipients or a proxy, the Console forwards the alert.

The settings that can be configured for an alert profile include:

Email Settings — If you plan to use an SMTP server, you must enter the name or address of the server, a username and password, and a reply-to e-mail address.

Email Recipients — Each alert profile can notify one or more e-mail addresses when specified events occur. If you want the Avalanche Console to notify you of an alert by e-mail, you must add the e-mail address to the **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 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.

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.

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 Settings**, **Email Recipients**, **SNMP Forwarding**, and **Available Alerts**.

   - To set the SMTP server settings, click **Email Settings** at the top right of the New Profile Details page.

   - To add an e-mail recipient, click **New** in the Email Recipients panel.

NOTE You must have the SMTP server settings configured if you want to send alert e-mails.

- To add an SNMP address, click **Add** 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 region or location.

Editing Alert Profiles

You can edit the details of an existing alert profile. You can configure the enabled status, notes, e-mail settings, proxy recipients, and the events that generate alerts.

To edit an alert profile:

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 Edit the details as desired.

- To set the SMTP server settings, click **Email Settings** at the top of the New Profile Details page.
- To add an e-mail recipient, click **New** in the Email Recipients panel.
- To add an SNMP address, click **Add** in the SNMP Forwarding panel.
- To delete an e-mail recipient or SNMP proxy, enable the checkbox next to it and click **Delete** at the top of the appropriate panel.

- To add or delete events, 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 in the list.

4 Click **Save** to return to the Alert Profile Details page.

Once you have finished editing the alert profile, it must be deployed before the changes will be applied.

Importing and Exporting E-mail Addresses

You can add e-mail addresses to the **Email Recipients** list of an alert profile by importing a comma-delimited `.csv` file (for example, one exported from Microsoft Outlook). Also, once you have created a mailing list, you can export it as a `.csv` file.

This section contains instructions for the following tasks:

- Importing E-mail Addresses
- Exporting E-mail Addresses

Importing E-mail Addresses

You can add e-mail addresses to the **Email Recipients** list of an alert profile by importing a comma-delimited `.csv` file (for example, one exported from Microsoft Outlook).

To import e-mail addresses:

1 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**.

The file name appears in the **Upload Email Recipients** text box.

6 Click **Save**.

The contacts display in the **Profiled Contacts** list.

Exporting E-mail Addresses

You can export e-mail addresses from the **Email Recipients** list of an alert profile to a `.csv` file.

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**.

Figure 12-1. *Email Recipients panel on the Alert Profile Details page*

The *Opening EmailExport.csv* dialog box appears.

3 Click **OK**.

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

Alert Profile Authorized Users

You can add authorized users for all alert profiles or enable a user for a specific alert profile. For information on adding an authorized user, see *Managing User Accounts* on page 23.

Using the Alerts Tab

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

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

This section provides information about the following tasks:

- Acknowledging Alerts
- Clearing Alerts
- Customizing Alerts Tab Functionality

Acknowledging Alerts

When a new alert appears in the **Alerts** tab, the Server Location at which the alert was generated is outlined in the Map view in the color of the most severe alert at that location. To stop this, you must acknowledge the alert.

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**.

Clearing Alerts

When the Alert Browser begins to fill with alerts, you may want to remove acknowledged alerts that are no longer relevant.

To clear alerts:

- 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.
- Maximum number of alerts to store. Alerts are stored in the database on the Enterprise Server.

To customize the Alerts tab functions:

1 Click **Tools > Settings**.

  The System Settings page appears.

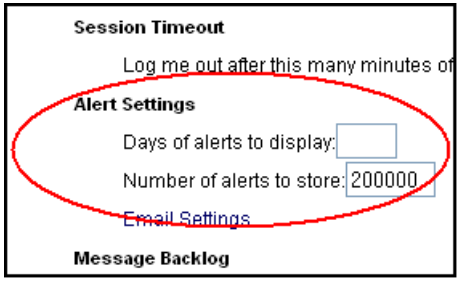


Figure 12-2. *Alert Settings on the System Settings page*

2 Under **Alert Settings**, use the **Days of alerts to display** and **Number of alerts to store** boxes to configure the alert settings.

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

  The **Alerts** tab will update to reflect your changes.

Chapter 13: Using Selection Criteria

Selection criteria are sets of rules which you can apply to individual software collections and individual network profiles. These criteria define which mobile devices will receive designated updates. For a software collection, the selection criteria determine which mobile devices can receive the software packages contained in the collection. For a network profile, the selection criteria determine which mobile devices can receive the settings contained in the profile.

Additional selection criteria are typically built into the software packages themselves, further restricting the distribution of the package. The built-in selection criteria associated with a particular software package are set by Wavelink or the third-party application developer and, once created, they cannot be modified.

A selection criteria string is a single expression (much like a mathematical expression) that takes a set of variables corresponding to different aspects of a mobile device and compares them to fixed values. The syntax includes parentheses and boolean operators to allow for flexible combination of multiple variables.

Additionally, if you want to set criteria but only want to match part of the expression you can use an asterisk [*] as a wildcard to represent single or multiple characters.

NOTE Asterisks are not allowed in property names or values because the symbol denotes a wildcard.

Selection criteria are compiled into internal formats that can be efficiently interpreted by the distributed servers. Most of the profile-related criteria also need to be translated into database SQL/HQL queries in order to build device inventories. The database interfaces used by Avalanche put a length limit on the generated SQL expressions which can be exceeded when selection criteria get too complex. Selection criteria containing more than 150 expressions have a good chance of exceeding database-imposed limits.

To reduce the size and complexity of selection criteria, the user should make use of the range and wildcard capabilities built into the selection criteria language.

You can use the selection criteria builder to build a valid selection criteria string. You can also use the selection criteria builder to test the selection criteria string on specific mobile devices that appear in the **Mobile Device Inventory** tab.

This section provides the following information:

- Building Selection Criteria
- Building Custom Properties
- Selection Variables
- Operators

Building Selection Criteria

You can access the Selection Criteria Builder from several different places in the Web Console, including: network profiles, software profiles, and mobile device groups. Access the Selection Criteria Builder by clicking the **Launch wizard** button.

NOTE Selection criteria also apply to software packages; however, you cannot edit software package selection criteria in Avalanche.

In the Selection Criteria Builder, you can build the selection criteria string by selecting or typing string elements one element at a time. The string elements include:

- Selection variables such as **ModelName** or **KeyboardName**. These variables determine the type of restriction placed on the package or profile. For example, by using a **ModelName** variable, you can restrict the package or profile to a specific class of mobile devices, based on their model numbers. You may use any property that you have assigned a device as a selection criterion variable.
- Operators such as AND (&), and OR (|) that are used to assign a value to a selection variable or to combine multiple variables.

NOTE Parentheses are recommended when multiple operators are involved. Nesting of parentheses is allowed.

- Actual values that are assigned to a selection variable. For example, if you assign a value of 6840 to a **ModelName** variable by building the string `ModelName = 6840`, then you will restrict packages or profiles to model 6840 mobile devices.

To build selection criteria:

1. Access the Selection Criteria Builder by clicking the **Launch wizard** button.

2 From the drop-down list, select a property and click **Insert Property**.

NOTE For information about properties, see *Selection Variables* on page 107.

3 Click one of the operator buttons.

NOTE For more information about operators, see *Operators* on page 114.

4 Type a value for the source property that you selected.

5 For each additional element you want to add to the selection criteria string, repeat the preceding steps.

NOTE Due to the potential complexity of long selection criteria strings, it is recommended that you limit the selection criteria to 20 selection variables or less.

6 Click **Validate**.

The Selection Criteria Builder will indicate whether the selection criteria expression is valid.

7 Click **OK** to close the *Selection Criteria Builder* dialog box.

Building Custom Properties

You can build custom properties to use in your selection criteria.

To build custom properties:

1 From the Selection Criteria Builder, select **New Property**.

The *Add Custom Property* dialog box appears.

2 Enter the name for the custom property and click **OK**.

The new property is added to the drop-down list.

Selection Variables

Selection criteria are based on the use of selection variables. In some cases, selection variables are mobile device properties, such as the Terminal ID.

You can place numbers and strings directly in the selection criteria string, with or without quotes.

NOTE Selection criteria strings are case sensitive.

For example, the following selection criteria strings are all valid:

```
ModelName=6840
ModelName = 6840
ModelName=”6840”
```

The following Palm emulation selection criteria string is valid:

```
Series = S
```

While the following are not:

```
series = s
Series = s
```

Long strings are also supported as selection criteria. For example, the following string is valid:

```
Series = 3 | (MAC = 00-A0-F8-27-B5-7F | MAC = 00-A0-F8-80-3D-4B |
MAC = 00-A0-F8-76-B3-D8 | MAC = 00-A0-F8-38-11-83 | MAC = 00-A0-F8-
10-24-FF | MAC = 00-A0-F8-10-10-10)
```

Selection variables for the selection criteria string are as follows:

`Columns` The number of display columns the mobile device supports. The possible value range is 1 – 80.

Example:

```
Columns > 20
```

`EnablerVer` Predefined Enabler version number.

Values with decimals must be surrounded by double quote marks.

EnablerVer = “3.10-13”

`IP` IP address of the mobile device(s).

Enter all IP addresses using dot notation. IP addresses can be written in three ways:

- Direct comparison with a single IP address. For example, `IP = 10.1.1.1`.
- Comparison with an arbitrary address range. For example, `IP = 10.1.1.5 – 10.1.1.15` (This can also be written as `IP = 10.1.1.5 – 15`.)
- Comparison with a subnet. This is done by supplying the network number along with the subnet mask or CIDR value. For example,
  `IP = 10.1.1.0/255.255.255.0`
  Using CIDR notation, this can also be written as
  `IP = 10.1.1.0/24`

`KeyboardCode` A number set by the device manufacturer and used internally by the BIOS to identify the keyboard type.

Supported values include:

`0` = 35-Key
`1` = More than 35 keys and WSS1000
`2` = Other devices with less than 35 keys

Example:

```
KeyboardCode = 0
```

`KeyboardName`

A value indicating which style of keyboard the mobile device is using (46key, 35key, etc.). This selection variable is not valid for CE devices.

Supported values include:

```
35KEY
46KEY
101KEY
TnKeys
```

Example:

```
KeyboardName = 35KEY
```

`Last Contact`

The parser for the LastContact property is unique because it not only allows specifying absolute time stamps, but also relative ones, forcing their constant reevaluation as the time-base changes.

Examples of time-stamp formats:

mm/dd/yyyy

`LastContact = “12/22/2005”` (All day)

HH:MM mm/dd/yyyy

`LastContact = “23:15 12/22/2005”` (All minute long, 24 hour notation)

hh:mm AP mm/dd/yyyy

`LastContact = “11:15 PM 12/22/2005”`

Also range-forms of the above

The relative format uses an offset from the current time.

`<offset>M`

`LastContact = 60M` (60 minutes in the past)

`<offset>H`

`Last Contact = 1H` (one hour in the past, the whole hour)

`<offset>D`

`Last Contact = 1D` (one day in the past, the whole day)

Also range-forms of the above

Special syntax allows inverted ranges from the range form to reduce the amount of confusion.

`LastContact=7D-1M`

`MAC`

MAC address of the mobile device.

Enter any MAC addresses as a string of hexadecimal digits. Dashes or colons between octets are optional. For example:

```
MAC = 00:A0:F8:85:E8:E3
```

`ModelName`

The standard model name for a mobile device. This name is often a number but it can be alphanumeric. Examples include 6840, 3940, and 4040. If the model number is unknown, it might appear in one of the views when the mobile device is selected.

A few of the supported values include:

`1040, 1740, 1746, 1840, 1846, 2740, 2840, 3140, 3143, 3540, 3840, 3843, 3940, 4040, 5040, 6140, 6143, 6840, 6843, 6940, 7240, 7540, 7940, 8140, 8940, PTC960, TR1200, VT2400, WinPC, WT2200, 7000CE,` HHP7400, MX1, MX2, MX3, VX1, iPAQ, iPAD, Falcon, ITCCK30, ITC700

Example:

```
ModelName = 6840
```

`ModelCode`

A number set by the device manufacturer and used internally by the BIOS to identify the hardware.

Supported values include:

`1`= LRT 38xx/LDT
`2` = VRC39xx/69xx
`3` = PDT 31xx/35xx
`4` = WSS1000
`5` = PDT 6800
`6` = PDT 6100

Example:

```
ModelCode <= 2
```

This matches all 38xx, 39xx, and 69xx devices.

`OSVer`	Predefined property designated by the Enabler. Values with decimals in them must be surrounded by double quote marks. `OSVer = “4.20”`
`OS Type`	Predefined property designated by the Enabler. `OSType = PocketPC`
`Processor`	Predefined property designated by the Enabler. `Processor = ARM`
`ProcessorType`	Predefined property designated by the Enabler. `ProcessorType = xScale`
`Assigned IP`	IP address of the mobile device. Enter all IP addresses using dot notation. IP addresses can be written in three ways: • Direct comparison with a single IP address. For example, `IP = 10.1.1.1`. • Comparison with an arbitrary address range. For example, `IP = 10.1.1.5 – 10.1.1.15` (This can also be written as `IP = 10.1.1.5 – 15`.) • Comparison with a subnet. This is done by supplying the network number along with the subnet mask or CIDR value. For example, `IP = 10.1.1.0/255.255.255.0`. Using CIDR notation, this can also be written as `IP = 10.1.1.0/24`.

`Series`

The general series of a device. This is a single character: '3' for Symbol '3000' series mobile devices, '7' for Symbol '7000' series mobile devices, etc.

Supported values include:

`3` = DOS 3000 Series
`P` = DOS 4000 and 5000 Series
`7` = DOS 7000 Series
`T` = Telxon devices
`C` = CE devices
`S` = Palm devices
`W` = Windows machines
D = PSC and LXE DOS devices

Example:

```
Series = 3
```

`Rows`

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:

any
ip
serial

`Terminal ID` The unique ID for the mobile device that Avalanche generates. The initial terminal ID is 1, and the values increment as needed.

Example:

```
Terminal ID = 5
```

NOTE You can redefine terminal IDs for mobile devices as needed. If you are using terminal IDs in a workstation ID, the value must not exceed the character limit for the host. Typically, hosts support 10 characters.

`@exists` Enables the user to check for the existence of a property. The `@exists` function name is case-sensitive and can only be used with an EQ or NE operator.

Example:

```
@exists ne some.property
```

```
@exists ==Some.property & Some.property =
“value”
```

Operators

All selection criteria strings are evaluated from left to right, and precedence of operations is used when calculating the selection criteria. When more than one operator is involved, you must include parentheses in order for the selection criteria string to be evaluated properly.

For example:

```
(ModelName=3840) or ((ModelName=6840) and (KeyboardName= 46Key))
```

The proceeding selection criteria string states that either 3840 mobile devices, regardless or keyboard type, or 46Key 6840 mobile devices will receive the software package.

You may use the symbol of the operator (!, &, |, etc.) in a selection criterion, or you may use the letter abbreviation (NOT, AND, OR, etc.). If you use the letter abbreviation for the operator, then you must use uppercase letters. Spaces around

operators are optional, and you can use the wildcard [*] for left wildcard constants and right wildcard constants.

Operators use the following precedence:

1 Parentheses

2 OR operator

3 AND operator

4 NOT operator

5 All other operators

The following operators can be used along with any number of parentheses to combine multiple variables.

`NOT (!)` Binary operator that negates the boolean value that follows it.

```
! (KeyboardName = 35Key) & (Rows = 20)
```

All mobile devices receive the software package except for those with both 20 rows and 35Key keyboards.

`AND (&)` Binary operator that results in TRUE if and only if the expressions before and after it are also both TRUE.

Example:

```
(ModelName=3840) | ((ModelName=6840) &
(KeyboardName= 46Key))
```

`OR (|)` Binary operator that results in TRUE if either of the expressions before and after it are also TRUE.

```
(ModelName =6840) | (ModelName = 3840)
```

6840 and 3840 mobile devices can receive the software package.

`EQ (=)` Binary operator that results in TRUE if the two expressions on either side of it are equivalent.

Example:

```
ModelName = 6840
```

`NE (!=)` Not equal to.

Example:

ModelName != 6840

Targets all non-6840 mobile devices.

`>` Binary operator that results in TRUE if the expression on the left is greater than the expression on the right.

Example:

```
Rows > 20
```

`<` Binary operator that results in TRUE if the expression on the left is less than the expression on the right.

Example:

```
Rows < 21
```

`>=` Binary operator that results in TRUE if the expression on the left is greater than or equal to the expression on the right.

Example:

```
Rows >= 21
```

`<=` Binary operator that results in TRUE if the expression on the left is less than or equal to the expression on the right.

Example:

```
Rows <= 20
```

(*) Wildcard operator.

Wildcard expressions should be quoted and must be used with either an EQ or NE operator.

`Keyboardname = “35*”` - Tail is the wildcard

`Keyboardname = “*35”` - Head is the wildcard

`Keyboardname = “*”` - Entire constant is the wildcard

You can also use wildcards for IP addresses.

```
IP = 10.20.*.*
```

This would be equivalent to 10.20.0.0-10.20.255.255. A wildcard address must contain all four octets and can only be used with either the EQ or the NE operator.

Chapter 14: Using the Task Scheduler

The Task Scheduler enables you to schedule system backups, and allows you to restore a backup copy when necessary. This section provides information on the following tasks:

- Backing Up the System
- Restoring the System

Backing Up the System

This section provides information about using the Task Scheduler to backup the Avalanche system. When you are using a PostgreSQL database, Avalanche provides the capability to backup and restore all your Avalanche information. You should back up the system regularly. If for any reason Avalanche files are deleted or corrupted, you will be able to restore them from the backup files. When you back up Avalanche, the database information and software collections are both saved in a zip file.

NOTE If you are attempting to back up your system on a Linux operating system, Wavelink recommends you perform the back up manually.

To back up the system:

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

   The Scheduled Task Wizard page appears.

2. From the **Task Type** drop-down list, select **System Backup** and click **Next**.

   The *Create A System Backup* screen appears.

3. 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.

4. Determine when the event will occur.

   - If you want the event to occur immediately, select the **Perform the task now** option.

- If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.
- If you want the event to occur on a regular basis, select the **Schedule a recurring event for the task** option.

5 Click **Next**.

6 If you selected the **Schedule a one-time event** for the task option, the *Schedule One-Time Task* screen appears.

Within this screen, you can set the following parameters for the event:

- Select the start date and time for the event.
- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **Use end time** option and then select the date and time for the event. If the event is not finished by this date and time, Avalanche will generate an alert.
- If you want the start and end time for this event to be based on the local time for the server location, enable the **Use local time of server location** option. Otherwise, the start and end times are based on the local time for the enterprise server.

7 If you selected the **Schedule a recurring event** option, the *Schedule Recurring Task* screen appears.

Within this screen, you can set the following parameters for this event:

- Select the start time for the event.
- Determine when you want the event to end. If you want the event to end after a specified amount of time, select the **Use end time** option and then select the end time for the event. If the event is not finished by this time, Avalanche will generate an alert.
- If you want the start and end time for this event to be based on the local time for the server location, enable the **Use local time of server location** option. Otherwise, start and end times are based on the local time for the enterprise server.

- Set the **Task Frequency**. You can set whether the event occurs daily, weekly, or monthly. The task frequency options will change depending on which of these you have selected.
- Set the **Range of recurrence** for the event. This will determine when you want this event schedule to be effected.

8 Click **Next**.

The *Review Your Task* screen appears.

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

The *Task Scheduled* dialog box appears.

10 Click **Schedule another task** to schedule a new event, or click **Done**.

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 > Scheduled Tasks**.

The Scheduled Task Wizard page appears.

2 From the **Task Type** drop-down list, select **System Restore** and click **Next**.

The *Restore A System Backup* screen appears.

3 Select the system backup you wish to restore and click **Next**.

- Select **Restore the most recent system backup** to restore Avalanche to the latest backup file.
- Select **Restore by path** to specify the file name and path of the desired system backup.

NOTE The default file path is:

```
C:\Program Files\Wavelink\AvalancheSE\backup
```

- Select **Restore selected** to choose the desired system backup according to the identifier tag.

The *Review Your Task* screen appears.

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

The *Task Scheduled* dialog box appears.

5 Click **Schedule another task** to schedule a new event, or click **Done**.

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.

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

- Accessing the Reports Tool
- Configuring Reports
- Generating Reports
- Creating Custom Reports
- Exporting Reports

Accessing the Reports Tool

You can access the Reports tool through the Avalanche Web Console.

The main page for the Reports tool has three panels:

- **Completed Reports**. This panel displays the names of reports that have been completed.
- **Scheduled Reports**. This panel displays the names of reports that have been configured and scheduled.
- **Configured Reports**. This panel displays the names of reports that have been configured.

The columns displayed in these panels are as follows:

Name	Displays the name of the report.
Template	Displays the template used for the report.
Location	Indicates the location(s) involved in the report.
Completed	Displays when the report was completed.
Frequency	Displays how frequently the scheduled report will be run.
Category	Displays the category to which the report belongs.

To access the Reports tool:

1 Access the Web Console.

2 Click **Tools > Reports**.

The Reports tool main page appears.

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* on page 126.

To configure a report with an Avalanche template:

1 In the Configured Reports panel, click **New**.

The Create a New Report page appears.

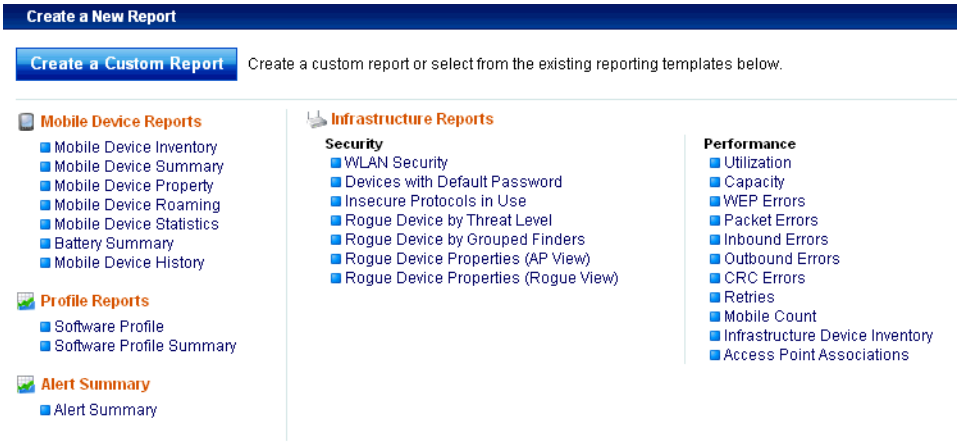


Figure 15-1. *Create a New Report page*

2 Click on the desired template from the list of preexisting Avalanche report templates.

3 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.

- **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`.
- **Scope**. You can configure the report to collect information from a specific location, region, or device group in Avalanche.
- **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 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.

This section includes instructions for the following:

- Running a Report
- Scheduling a Report

Running a Report

After a report has been configured, you can generate it at any time. 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. From the Configured Reports panel, enable the checkbox next to the report that you want to generate.
2. Click **Run Now**.

   The report appears in the Completed Reports panel.

Scheduling a Report

After a report has been configured, you can schedule it to run at a specific time.

To schedule a report:

1. Access the Reports tool.
2. From the Configured Reports panel, enable the checkbox next to the report that you want to generate.
3. Click **Schedule**.

   The Schedule Reports page appears.
4. From the drop-down list, select how frequently you want the report to run.
5. Type the date and time you want the report to run in the text boxes. For the date, use a mm/dd/yyyy format.

6 Click **Next**.

7 A summary of 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**. When you are finished adding tables, click **Next**.

7 Type a **Report Name** in the text box and select the **Output Format** for the report. Click **Next**.

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

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

Exporting Reports

All reports can be exported and saved for future use.

To export a report:

1 Access the Reports tool.

2 From the Reports Now Available panel, select the desired folder.

3 Click the View icon to the right of the desired report.

The report appears in the browser window.

4 Select **File > Save As**.

5 Navigate to the desired location and click **Save**.

The report is saved to the location you selected.

Appendix A: SSL Certificates

The Avalanche Web Console uses Hypertext Transfer Protocol (http) by default, which is not encrypted. If you want your information to be encrypted, you can configure Avalanche to use https with an SSL certificate instead.

If you intend to use Avalanche with an SSL certificate for a secure connection, you have the options of purchasing a certificate through a third-party Certificate Authority (such as Verisign), or creating a self-signed certificate.

NOTE If you create a self-signed certificate, web browsers will not initially recognize the certificate and will display warning messages that the site is not trusted. They may require you to make an exception in order to connect to the enterprise server. The connection will be encrypted, however.

This section contains instructions for the following tasks:

- Implementing a Certificate from a Certificate Authority
- Implementing a Self-Signed Certificate

Implementing a Certificate from a Certificate Authority

You can choose to use Avalanche with a certificate from a Certificate Authority. Note that the following instructions are based upon acquiring a certificate through the certificate authority, Verisign. The steps may vary somewhat when using another certificate authority vendor.

Wavelink strongly recommends that you backup the keystore file, the actual certificate file, the intermediate certificate, the certificate request, and the server.xml document after you have implemented your certificate. This would include the following files:

- `amckeystore.keystore`
- `[your certificate].cer`
- `intermediateCA.cer`
- `certreq.csr`
- `server.xml`

This section contains the following tasks for obtaining an SSL certificate from a certificate authority:

- Creating a Keystore
- Generating the Certificate Signing Request
- Importing an Intermediate Certificate
- Importing a Certificate
- Activating SSL for Tomcat
- Accessing the Web Console over a Secure Connection
- Troubleshooting

Creating a Keystore

To create a keystore for the certificate, use the keytool.exe utility. You will need to provide a Common Name (domain name), organizational unit, organization, city, state, and country code. You will also need to provide a keystore name and passwords for the keystore and alias. These are arbitrary, but should be noted for future reference.

To generate a keystore for the certificate:

1. From a command line, navigate to:
   `[Avalanche installation directory]\JRE\Bin`
2. Use the command:
   `keytool -genkey -alias amccert -keyalg RSA -keystore amckeystore.keystore`
3. At the prompt **Enter keystore password**, type the keystore password. When prompted, re-enter the password.
4. At the prompt **What is your first and last name**, type the Common Name.

NOTE The Common Name (domain name) you enter should be one that your company owns. Add a DNS entry if needed to resolve this computer to the Common Name.

5 At the prompts, enter your organizational unit, organization, city, state, and the country code.

6 When you are prompted to review your information, type `yes` to confirm that it is correct. If you type `no`, you will be guided through the prompts again.

7 At the prompt **Enter key password for <amccert>**, type a password to use for the alias. If you want to use the same password for the alias as you used for the keystore, press `Return`.

An example of generating a keystore:

```
Enter keystore password: avalanche

Re-enter new password: avalanche

What is your first and last name?
[Unknown]: avaself.wavelink.com

What is the name of your organizational unit?
[Unknown]: Engineering

What is the name of your organization?
[Unknown]: Wavelink Corporation

What is the name of your City or Locality?
[Unknown]: Midvale

What is the name of your State or Province?
[Unknown]: Utah

What is the two-letter country code for this unit?
[Unknown]: US

Is CN=avaself.wavelink.com, OU=Engineering, O=Wavelink Corporation,
L=Midvale, ST=Utah, C=US correct?
[no]:  yes

Enter key password for <amccert>
(RETURN if same as keystore password):
```

Generating the Certificate Signing Request

Once you have created the keystore, you can use the keytool.exe utility to generate a certificate signing request (`certreq.csr`) file to send to a certificate authority.

To generate a certificate signing request:

1 From a command line, navigate to:
`[Avalanche installation directory]\JRE\Bin`

2 Use the command:
```
keytool -certreq -keyalg RSA -alias amccert -file certreq.csr
-keystore "C:\Program Files\Wavelink\AvalancheMC\JRE\bin\
amckeystore.keystore"
```

3 Enter your keystore password.

When you apply to a certificate authority for an SSL web server certificate, you will need to submit the `certreq.csr` file. This file should be created in the `C:\Program Files\Wavelink\AvalancheMC\JRE\bin` folder.

Importing an Intermediate Certificate

When you acquire an intermediate certificate from your certificate authority, import it into the keystore. You may need to copy the contents of the intermediate certificate to a text editor and save the file as `intermediateCA.cer`. This file must be saved in the `[Avalanche installation directory]\JRE\bin` directory before you can import it.

To import an intermediate certificate:

1 From a command line, navigate to:
`[Avalanche installation directory]\JRE\bin`

2 Use the command:
```
keytool -import -alias intermediateCA -keystore "[Avalanche
installation directory]\JRE\bin\amckeystore.keystore"
-trustcacerts -file intermediateCA.cer
```

NOTE In this command, the filename `intermediateCA.cer` is used. If your intermediate certificate has a different name, use it instead.

3 Enter your keystore password.

The intermediate certificate is added to the keystore.

Importing a Certificate

Once you have received your certificate, you need to import it into the keystore. Your certificate will probably come as a file with the extension `.cer` or in the body of an e-mail. If it comes in the body of an e-mail, copy the contents to a text editor and save the file with a `.cer` extension. This file must be saved in the `[Avalanche installation directory]\JRE\bin` directory before you can import it.

To import a certificate:

1 From a command line, navigate to:
`[Avalanche installation directory]\JRE\bin`

2 Use the command:
```
-import -alias amccert -keystore  "C:\Program Files\Wavelink\
AvalancheMC\JRE\bin\amckeystore.keystore" -trustcacerts -file
ava-wavelink-com.cer
```

NOTE As an example, `ava-wavelink-com.cer` is used as the filename. Replace this filename with the name of your certificate.

3 Enter your keystore password.

The certificate is added to the keystore.

Activating SSL for Tomcat

Once you have generated a certificate, you must activate SSL for Tomcat. You must modify the `server.xml` file and then restart the Tomcat server.

To activate SSL for Tomcat:

1 Navigate to
`[Avalanche Install location]\WebUtilities\tomcat\conf`
and open the `server.xml` file with a text editor such as Notepad.

2 Find
```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
   maxThreads="150" scheme="https" secure="true" clientAuth="false"
   sslProtocol="TLS" />
```

3 Remove the comment markers so that the section is not commented out.

4 Modify the section to contain the following information:

```
<Connector port="8443"
   protocol="org.apache.coyote.http11.Http11NioProtocol" SSLEnabled="true"
   maxThreads="150" scheme="https" secure="true" clientAuth="false"
   sslProtocol="TLS" keystoreFile="C:\Program Files\Wavelink\AvalancheMC\
   JRE\bin\amckeystore.keystore" keystorePass="[keypass]"/>
```

Where `[keypass]` is the keystore password you entered when creating the certificate. For the above example, this would be `avalanche`.

```
keystorePass="avalanche"
```

NOTE If you are not using port 443 for any other applications, you can change the connector port to 443. Changing the port to 443 will allow you to access the Web Console without entering the port within the URL.

5 Save your changes to the file.

6 Restart the Apache Tomcat for Wavelink service.

Accessing the Web Console over a Secure Connection

Once you have generated a certificate, activated SSL for Tomcat, and restarted the Tomcat server, you can access the Web Console over a https connection.

To access the Web Console over a secure connection:

- In the address field of your browser, type:

  `https://<Your Domain Name>:8443/AvalancheWeb`

  -Or-

- If you changed the connector port to 443, type:

  `https://<Your Domain Name>/AvalancheWeb`

Troubleshooting

To troubleshoot issues connecting to the Apache Tomcat server using SSL after changes are made, go to `C:\Program Files\Wavelink\AvalancheMC\WebUtilities\Tomcat\logs` to find Catalina Tomcat logs.

NOTE You need to stop the Tomcat service to get all the log messages.

Example log file: `catalina.2010-02-24.log`

Implementing a Self-Signed Certificate

These instructions explain how to generate a self-signed certificate in the Apache Tomcat environment. If you choose not to use a Certificate Authority, you can still use a https connection to connect to the Web Console by creating your own certificate.

NOTE Internet browsers will not recognize a self-signed certificate as legitimate and will display warnings before allowing you access.

NOTE Wavelink strongly recommends backing up `server.xml` and `selfsignkeystore.keystore` when you have implemented a self-signed certificate.

This section contains the following tasks for implementing a self-signed certificate:

- Generating a Certificate
- Activating SSL for Tomcat
- Accessing the Web Console over a Secure Connection
- Troubleshooting

Generating a Certificate

To create a self-signed certificate, use the keytool.exe utility. You will need to provide a Common Name (domain name), organizational unit, organization, city, state, and country code when creating your certificate. You will also need to provide a keystore name and passwords for the keystore and alias. These are arbitrary, but should be noted for future reference.

To generate a self-signed certificate:

1 From a command line, navigate to:
`[Avalanche installation directory]\JRE\Bin`

2 Use the command:
`keytool -genkey -alias amcselfcert -keyalg RSA -keystore selfsignkeystore.keystore`

3 At the prompt **Enter keystore password**, type the keystore password. When prompted, re-enter the password.

4 At the prompt **What is your first and last name**, type the Common Name.

NOTE The Common Name (domain name) you enter should be one that your company owns. Use a DNS entry if needed to resolve this computer to the Common Name.

---

5 At the prompts, enter your organizational unit, organization, city, state, and the country code.

6 When you are prompted to review your information, type `yes` to confirm that it is correct. If you type `no`, you will be guided through the prompts again.

7 At the prompt **Enter key password for <amcselfcert>**, type a password to use for the alias. If you want to use the same password for the alias as you used for the keystore, press `Return`.

An example of generating a self-signed certificate:

```
Enter keystore password: avalanche

Re-enter new password: avalanche

What is your first and last name?
[Unknown]: avaself.wavelink.com

What is the name of your organizational unit?
[Unknown]: Engineering

What is the name of your organization?
[Unknown]: Wavelink Corporation

What is the name of your City or Locality?
[Unknown]: Midvale
```

```
What is the name of your State or Province?
[Unknown]: Utah

What is the two-letter country code for this unit?
[Unknown]: US

Is CN=avaself.wavelink.com, OU=Engineering, O=Wavelink Corporation,
L=Midvale, ST=Utah, C=US correct?
[no]:  yes

Enter key password for <amcselfcert>
(RETURN if same as keystore password):
```

Activating SSL for Tomcat

Once you have generated a certificate, you must activate SSL for Tomcat. You must modify the server.xml file and then restart the Tomcat server.

To activate SSL for Tomcat:

1. Navigate to `[Avalanche Install location]\WebUtilities\tomcat\conf` and open the `server.xml` file with a text editor such as Notepad.

2. Find
```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
   maxThreads="150" scheme="https" secure="true"
   clientAuth="false" sslProtocol="TLS" />
```

3. Remove the comment markers so that the section is not commented out.

4. Modify the section to contain the following information:
```
<Connector port="8443"
   protocol="org.apache.coyote.http11.Http11NioProtocol" SSLEnabled="true"
   maxThreads="150" scheme="https" secure="true" clientAuth="false"
   sslProtocol="TLS" keystoreFile="C:\Program Files\Wavelink\AvalancheMC\
   JRE\bin\selfsignkeystore.keystore" keystorePass="[keypass]"/>
```

   Where `[keypass]` is the keystore password you entered when creating the certificate. For the above example, this would be `avalanche`.

   `keystorePass=”avalanche”`

NOTE If you are not using port 443 for any other applications, you can change the connector port to 443. Changing the port to 443 will allow you to access the Web Console without entering the port within the URL.

5 Save your changes to the file.

6 Restart the Apache Tomcat for Wavelink service.

Accessing the Web Console over a Secure Connection

Once you have generated a certificate, activated SSL for Tomcat, and restarted the Tomcat server, you can access the Web Console over a https connection.

To access the Web Console over a secure connection:

- In the address field of your browser, type:

  `https://<Your Domain Name>:8443/AvalancheWeb`

  -Or-

- If you changed the connector port to 443, type:

  `https://<Your Domain Name>/AvalancheWeb`

Troubleshooting

To troubleshoot issues connecting to the Apache Tomcat server using SSL after changes are made, go to `C:\Program Files\Wavelink\AvalancheMC\WebUtilities\Tomcat\logs` to find Catalina Tomcat logs.

NOTE You need to stop the Tomcat service to get all the log messages.

Example log file: `catalina.2010-02-24.log`

Appendix B: Avalanche Services

This appendix lists all of the Avalanche services. Under each service title, you'll find the file path where the service is located and which type of server (Enterprise Server, Statistics Server or Mobile Device Server) uses the service.

Wavelink Authentication Service

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

Enterprise Server

Apache Tomcat

C:\Program Files\Wavelink\AvalancheMC\WebUtilities\Tomcat\bin\tomcat6.exe

Enterprise Server

Wavelink Alerts

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

Mobile Device Server

Wavelink Avalanche Service Manager

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

Mobile Device Server

Wavelink Avalanche Agent

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

Mobile Device Server

Wavelink Avalanche Enterprise Server

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

Enterprise Server

Wavelink Information Router

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

Enterprise Server

Wavelink License Server

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

Enterprise Server

Wavelink Stat Server Enterprise

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

Stats Server

Wavelink Deployment

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

Enterprise Server

Appendix C: Port Information

This appendix provides information about the ports used in Avalanche SE. The information provided includes:

- Database Ports
- Enterprise Server Ports
- Mobile Device Server Ports
- Wavelink Products Used with Avalanche

NOTE Except where noted, the ports listed are all inbound ports.

Database Ports

When Avalanche is installed with the default database (PostgreSQL), the default port for database communication is 5432.

Enterprise Server Ports

The following table provides a list of ports that the Enterprise Server uses.

Port	Description	Port Type
5002	Wavelink Authentication Service	TCP
7221	Avalanche License Server	TCP
7225	InfoRail Service	TCP
7226	InfoRail Service IR-to-IR router port	TCP
8009	Tomcat AJP for integrating with Apache httpd	TCP
8080	Tomcat HTTP	TCP

NOTE The Enterprise Server also listens on 8443 for a Tomcat connection with an SSL certificate. You can change this to 443 in the `server.xml` file if no other program is using 443.

Mobile Device Server Ports

The following table provides a list of the ports that the Mobile Device Server uses.

Port	Description	Port Type
1777	Protocol Service	TCP/UDP
1778	Services persistent connections to mobile devices	TCP

Wavelink Products Used with Avalanche

The following table provides a list of the ports that are used by Wavelink products often used in conjunction with Avalanche.

Port	Product	Port Type
1899	Remote Control	TCP
1900	Remote Control	TCP
5001	CE Secure	TCP

Appendix D: Wavelink Contact Information

If you have comments or questions regarding this product, please contact Wavelink Customer Service.

E-mail Wavelink Customer Support at: CustomerService@wavelink.com

For customers within North America and Canada, call the Wavelink Technical Support line at 801-316-9000 (option 2) or 888-699-9283.

For international customers, call the international Wavelink Technical Support line at +800 9283 5465.

For Europe, Middle East, and Africa, hours are 9 AM - 5 PM GMT.

For all other customers, hours are 7 AM - 7 PM MST.

Glossary

ActiveSync	A synchronization program developed by Microsoft. It allows a mobile device synchronize with the machine running Avalanche.
Administrator User Accounts	Users assigned as Administrator Accounts have unlimited permissions, and can assign and change permissions for Normal user accounts.
Alert Profile	A collection of traits that define a response to a specific network or statistical alert. Typically, an alert profile consists of the alerts being monitored and either an e-mail address or proxy computer to which the alert is forwarded.
Authorized Users	Authorized users are users that have permission to access assigned areas of the Console and the ability to perform certain tasks. Administrator users have access to all areas and tasks in their Home region; Normal users must be assigned to specific areas or tasks in order to view or perform them.
Avalanche Console	The Avalanche Console is the graphical user interface (GUI) where you manage your Servers, profiles and devices. The Java Console must be installed on a computer, but the Web Console can be accessed from any Web browser that can connect to your enterprise server.
Blackout Window	A period of time when the Mobile Device Servers and Infrastructure Servers are not allow to contact the Enterprise Server, eliminating heavy bandwidth and allowing control the flow of device connections to the Enterprise Server.

CE Secure	A Wavelink plug-in that provides advanced user authentication and security on Windows CE mobile devices.
Client	A mobile device with an installed Avalanche Enabler. The Enabler allows the client to communicate with a Server and to be configured and managed through Avalanche.
Default Profile	A profile that the Servers automatically assign to network infrastructure or mobile devices. The Servers apply these default profiles to any devices discovered that are not assigned to a profile.
Device Filters	Device filters allow you to display specific mobile devices in the Mobile Device Inventory based on selection criteria.
DHCP	Dynamic Host Configuration Protocol. An IP service that allows DHCP clients to automatically obtain IP parameters from a DHCP server.
DNS	Domain Name System. A service that provides hostname-to-IP address mapping.
Enabler	The software installed on a mobile device that allows Avalanche to manage it.
Enterprise Server	The Enterprise Server is the service that manages communication and collaboration between the components of Avalanche.
Epochs	An epoch consists of a collection of network settings and configured times in which the settings for a network profile changes. Epochs can be created for each configured network profile. Most network profile settings can be managed by Epochs.

ESSID	Extended Service Set ID. The identifier of an extended service set for devices that are participating in an infrastructure mode wireless LAN.
Exclusion Windows	Exclusion Windows are scheduled periods of time when your mobile devices are not authorized to contact the Mobile Device Server to conserve bandwidth and increase compliance for critical software updates. Exclusion Windows are configured through the Mobile Device Server profile.
Filters	Device filters allow you to display specific devices in the Inventory based on selection criteria.
Geofence	A virtual perimeter defined by GPS coordinates. When a mobile device that is assigned a geofence area leaves that area, Avalanche will display an alert.
Home Region	Each user must be assigned a home region. He will only be allowed to access information for his home region and any associated sub-regions or locations.
Java Console	The Console is the graphical user interface (GUI) where you manage your Servers, profiles and devices. The Java Console must be installed on a computer. See also Web Console.
Mobile Device	A hand-held or vehicle-mounted device, such as a scan gun or PDA, that travels with a user as he conducts daily operations.
Mobile Device Server	The Mobile Device Server consists of server side software packages that facilitate communication between the mobile devices and the Enterprise Server.
Mobile Device Server Profile	Mobile Device Server profiles allow you to define device configuration settings for the mobile device Server.

Mobile Device Groups	A mobile device group consists of mobile devices with similar characteristics. These groups are defined by selection criteria.
Network Profile	A collection of settings that allow you to download network parameters such as IP addresses, the ESSID, and encryption and authentication settings to devices over a serial or wireless connection.
Normal User Accounts	Users assigned as Normal users do not have access to any component of Avalanche until assigned permissions.
Orphan Packages	A software package that has been deployed to a client through Avalanche, but has been disabled or is not recognized by the Server. You must orphan a software package before you can use Avalanche to delete it from the client.
Ping	An IP service that is used to test IP connectivity. Part of the ICMP service.
Profile	A collection of configuration settings that can be applied to multiple regions/ locations simultaneously.
Ports	Typically used to map data to a particular process running on a computer.
PostgreSQL	A powerful, open source relational database system packaged with Avalanche.
Profile Permissions	Provide global access to each profile you are given permission for. Does not allow permission to apply the profiles to any regions until you are assigned Regional Permissions for a region.

Regional Permissions	Provide access to specific to regions. To have full permissions at a region, a user must be assigned the Regional Permission in the User Management dialog box and then be assigned as an Authorized User to the specific region. See Authorized User.
Remote Control	A Wavelink plug-in that allows you to remotely view and perform tasks on mobile devices.
Scan to Configure	The ability to configure barcode profiles that contain network profile settings. You can then print the profiles as barcodes and scan the barcodes with a mobile device with an Enabler version 3.5 or later. The Enabler configures the network settings on the mobile device.
Secondary Servers	If configured and assigned, secondary servers allow mobile devices to attempt to connect to a secondary Mobile Device Server if the primary server is not available.
Selection Criteria	Parameters that can be used for filters, profile or package management, or device group definition.
Selection Variables	The basis for selection criteria. In some cases, selection variables are mobile device properties.
Software Packages	The collection of files that reside on the mobile device for a particular application. These files include any support utilities used to configure or manage the application from the Avalanche Console.
Software Profiles	A logical grouping of software packages maintained and managed by the Avalanche.

SSID	Service Set Identifier. A unique name, up to 32 characters long, that is used to identify a wireless LAN. The SSID is attached to wireless packets and acts as a password to connect to a specific LAN.
Task Scheduler	The Task Scheduler provides the means to deploy Servers, send updates, and perform system backups.
Telnet	A TCP/IP utility used for terminal emulation, which allows a client to connect and interact with a remote host system.
Terminal ID	The identification number of a specific (physical) terminal or workstation on the network.
User Account	A login name and password used by an individual to access the Console. A user can have Administrator or Normal permissions.
Web Console	The Avalanche Console is the graphical user interface (GUI) where you manage your Servers, profiles and devices. The Web Console can be accessed from any Web browser that can connect to your enterprise server and allows you to manage and view reports and floorplans.
WEP	Wired Equivalent Privacy. An encryption standard for wireless networks that provides the equivalent security of a wired connection for wireless transmissions.

Index

N

O

P

R

S

T

U

W