



Wavelink Avalanche Site Edition
Web Console User Guide

Version 5.3

Revised 04/05/2012

Copyright © 2012 by Wavelink Corporation. All rights reserved.

Wavelink Corporation
10808 South River Front Parkway, Suite 200
South Jordan, Utah 84095
Telephone: (801) 316-9000
Fax: (801) 316-9099
Email: customerservice@wavelink.com
Web site: www.wavelink.com

No part of this publication may be reproduced or used in any form, or by any electrical or mechanical means, without permission in writing from Wavelink Corporation. This includes electronic or mechanical means, such as photocopying, recording, or information storage and retrieval systems. The material in this manual is subject to change without notice. The software is provided strictly on an “as is” basis. All software, including firmware, furnished to the user is on a licensed basis. Wavelink grants to the user a non-transferable and nonexclusive license to use each software or firmware program delivered hereunder (licensed program). Except as noted below, such license may not be assigned, sublicensed, or otherwise transferred by the user without prior written consent of Wavelink. No right to copy a licensed program in whole or in part is granted, except as permitted under copyright law. The user shall not modify, merge, or incorporate any form or portion of a licensed program with other program material, create a derivative work from a licensed program, or use a licensed program in a network without written permission from Wavelink. The user agrees to maintain Wavelink’s copyright notice on the licensed programs delivered hereunder, and to include the same on any authorized copies it makes, in whole or in part. The user agrees not to decompile, disassemble, decode, or reverse engineer any licensed program delivered to the user or any portion thereof. Wavelink reserves the right to make changes to any software or product to improve reliability, function, or design. The information in this document is bound by the terms of the end user license agreement.



Table of Contents

Chapter 1: Introduction	1
Components of Avalanche	1
Getting Started	3
About This Guide	4
Chapter 2: Avalanche Web Console	6
Launching the Avalanche Web Console	6
Understanding the Web Console	8
Management Tabs	9
Location Navigation	11
Panels	12
Editing Columns	13
Using Device Filters	14
Understanding Edit Mode	15
Console Tools	15
Viewing System Information	16
Configuring Audit Logging	16
Viewing the Audit Log	18
Configuring General System Settings	19
Configuring E-mail Settings	20
Setting a System Message	21
Creating Links in the Tools Menu	21
Checking for Available Updates	22
Installing Language Support	22
Chapter 3: Managing User Accounts	23
Creating User Accounts	24
Creating User Groups	25
Assigning User Permissions	26
Assigning Authorized Users	28
Assigning Authorized Users to Locations	28
Assigning Authorized Users to Profiles	28
Assigning Authorized Users to Mobile Device Groups	29
Configuring Integrated Logon	29
Removing User Accounts	30
Chapter 4: Location Management	31
Managing Group Locations	32
Applying Profiles to Locations	32
Editing Exclusions	33
Chapter 5: Managing Network Profiles	35
Creating Network Profiles	35



Configuring Scheduled Settings	36
Configuring WLAN IP Settings	37
Configuring WLAN Settings	38
Configuring WWAN Settings	42
Chapter 6: Managing Scan to Configure Profiles	44
Creating a Scan to Config Profile	44
Configuring a Scan to Config Profile	45
Adding Custom Properties for Scan to Config Profiles	45
Adding a Registry Key to a Scan to Config Profile	46
Printing Barcodes	47
Scanning Barcodes	47
Chapter 7: Managing a Mobile Device Server	48
Configuring a Mobile Device Server Profile	48
Mobile Device Server Profile General Configuration	49
Configuring Blackouts	53
Scheduling Profile-Specific Device Updates	54
Viewing Mobile Device Server Licensing Messages	55
Viewing Server Properties	56
Chapter 8: Managing Software Profiles	57
Creating Software Profiles	57
Managing Software Packages	58
Adding a Software Package	59
Building New Software Packages	60
Creating CAB or MSI Packages	62
Copying Software Packages	63
Configuring Software Packages with a Utility	63
Configuring Software Packages for Delayed Installation	64
Peer-to-Peer Package Distribution	65
Chapter 9: Managing Mobile Devices	68
Mobile Devices Panel	68
Viewing Mobile Device Details	69
Locating a Mobile Device	70
Locating a Device using Cell Tower Information	70
Viewing Location History	71
Configuring Mobile Device Properties	71
Creating Custom Properties	72
Creating Device-Side Properties	73
Editing Properties	73
Deleting Properties	74
Contacting the Mobile Device	74
Pinging Mobile Devices	74



Sending a Message to a Device User	75
Updating a Mobile Device	75
Chatting with a Device User	76
Wiping a Mobile Device	77
Chapter 10: Using Remote Control	78
Using the Remote Control Console	79
Changing the Username and Password	80
Synchronizing with the Avalanche License Server	80
Connecting to the Avalanche License Server	80
Configuring Server Options	81
Configuring Skin Settings for the Server	83
Managing Cell Carriers	83
Backing Up and Restoring the Remote Control Database	84
Viewing System Information	85
Configuring Connection Profiles	85
Configuring the Remote Control Client	86
Editing the Remote Control Package	86
Configuring Client Settings from the Mobile Device	89
Clearing Client Settings	91
Using a Mobile Device Profile for Remote Control Settings	91
Connecting to Mobile Devices	94
Connecting to a Mobile Device	94
Closing Remote Control Sessions	95
Standard Viewer Tasks	96
Accessing the File System	97
Creating New Folders	97
Copying Files to the PC	98
Copying Files to the Mobile Device	98
Manipulating Files on the Device	99
Pasting Text	99
Using the Registry Viewer	99
Creating New Registry Keys	100
Creating Key Values	100
Viewing Binary Data	101
Modifying Key Values	101
Editing Binary Data	102
Deleting Key Values	102
Exporting Registries	103
Comparing Registries	103
Using the Process Manager	104
Accessing the Log File	105
Viewing and Clearing Log Files	105
Configuring Logging	106



Viewing Device Information	107
Configuring Display and Capture Options	108
Setting Video Mode	109
Configuring Display Refresh Rates	109
Sizing the Mobile Device Display	110
Toggling Statistics	111
Using Device Skins	111
Recording Videos	112
Performing Screen Captures	113
Using Device Tools	114
Web Viewer Tasks	115
The Device Tab	115
Using the File Explorer	117
Using the Registry Explorer	118
Using the Process Manager	118
Viewing Device Information	119
Chapter 11: Managing Mobile Device Profiles	120
Configuring Device Wipe Folders	121
Editing Custom Properties for Mobile Device Profiles	122
Editing Registry Keys for a Mobile Device Profile	123
Adding a Registry Key to a Mobile Device Profile	123
Editing or Removing a Registry Key or Value	124
Remote Control Settings in a Mobile Device Profile	124
Configuring Mobile Device Profile Advanced Settings	127
Location Based Services	127
Geofence Areas	128
Regional Settings	129
Update Restrictions	129
Chapter 12: Managing Mobile Device Groups	130
Creating Mobile Device Groups	130
Sending Messages to Mobile Device Groups	131
Chapter 13: Managing Alert Profiles	132
Creating and Configuring Alert Profiles	132
Adding E-Mail Contacts	133
Adding SNMP Proxies	135
Alerts Tab	135
Acknowledging and Clearing Alerts	136
Customizing Alerts Tab Functionality	136
Chapter 14: Using Selection Criteria	138
Building Selection Criteria	138
Selection Variables	140



Operators	146
Chapter 15: Avalanche Reports	149
Configuring Reports	150
Generating and Scheduling Reports	151
Creating Custom Reports	152
Viewing Completed Reports	152
Chapter 16: Using the Task Scheduler	154
Backing Up the System	155
Restoring the System	156
Removing Completed Tasks	157
SSL Certificates for the Web Console	158
Configuring the Remote Control Server for SSL	167
Avalanche Services	176
Port Information	178
Uninstalling Avalanche	181
Wavelink Contact Information	182



Chapter 1: Introduction

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

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

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

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

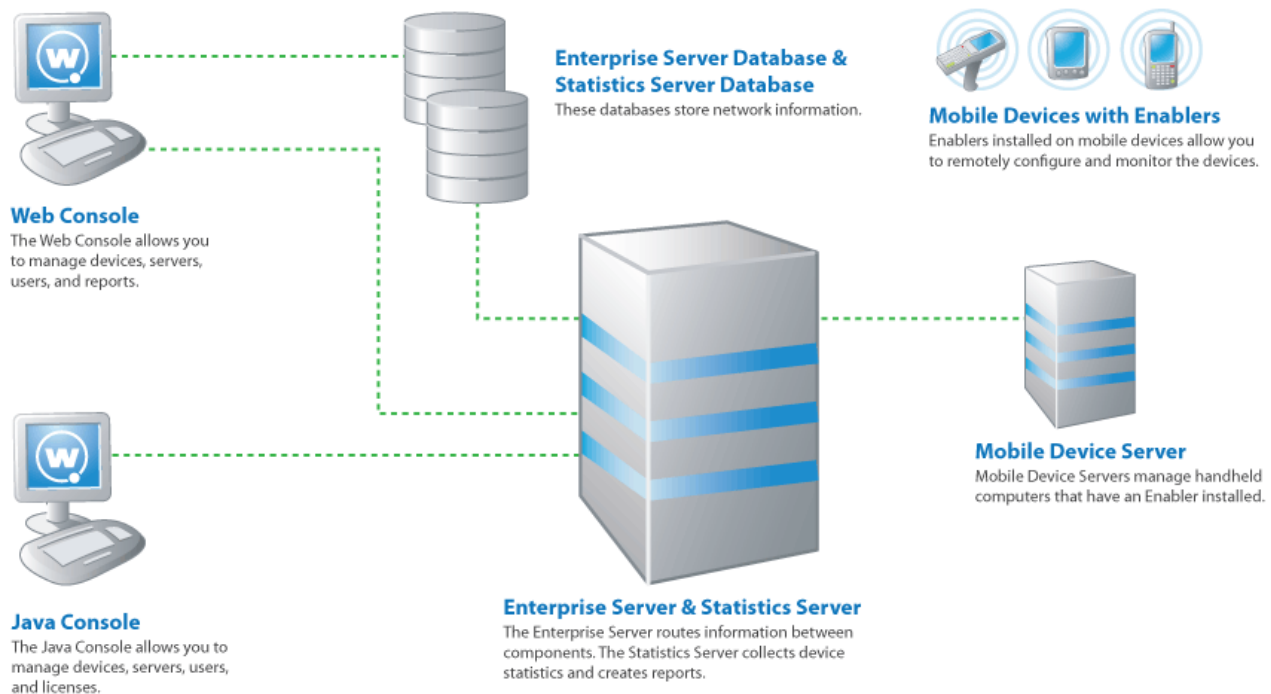
This section provides the following introductory information:

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

Components of Avalanche

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





The primary components of Avalanche include:

- **Avalanche Java Console.** The Avalanche Java Console gives you control over your wireless network components. With the Avalanche Console, you can manage and maintain everything from infrastructure device settings to mobile device software. The Java Console must be accessed from a computer where it has been installed.
- **Avalanche Web Console.** The Avalanche Web Console allows you to manage network components from any computer using an Internet connection and a web browser. 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 manages information and facilitates all communication between the Console, the mobile device server, and the Enterprise Server database.
- **Statistics Server.** The Statistics Server collects statistical information from your devices and device servers for reporting purposes and stores information in the Statistics Server database.



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

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

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

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

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

Getting Started

For best results in managing your Avalanche installation and configuration, Wavelink recommends performing the following steps in order:

- 1 **Install Avalanche.** For more information, see the *Installing Avalanche* paper on the Wavelink Web site.
- 2 **Activate Mobile Device licenses for Avalanche.** You should activate the number of licenses based on the number of devices you want to manage. For information on licensing, see the Java Console help.
- 3 **Create group locations.** Group locations are user-defined groups of devices that connect to the. For more information, see [Managing Group Locations](#) on page 32.
- 4 **Configure profiles.** A profile allows you to manage configurations and settings centrally and then deploy those configurations to as many locations as necessary. In this way, you



can update or modify multiple devices instead of manually changing settings for each one. Profiles must be enabled before being applied.

The following list provides information about each type of profile:

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

- 5 Assign profiles to locations.** You can assign configured profiles to locations from the Console. When you assign a profile to a location and perform a synchronization, the settings from the profiles are applied to the location and any associated devices. For more information, see [Applying Profiles to Locations](#) on page 32.
- 6 Configure Enablers.** Ensure that your mobile devices have Enablers installed, and configure the Enablers to connect to a mobile device server.

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

About This Guide

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

This help makes the following assumptions:



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

This help uses the following typographical conventions:

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

Examples:

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

Press `CTRL+ALT+DELETE.`

Bold Any time this guide refers to an option, such as descriptions of different options in a dialog box, that option appears in the **Bold** text style. This is also used for tab names and menu items.

Example:

Click **File > Open.**

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

Example:

The *Infrastructure Profiles* dialog box appears.



Chapter 2: Avalanche Web Console

You interact with your wireless network primarily using the Avalanche Console. The Avalanche Console allows you to control and monitor global characteristics of your wireless network, including network and device configuration and performance.

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

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

To access the Console, you will need:

- An Internet browser such as Internet Explorer, Firefox, or Chrome.
- An Internet connection between the Avalanche On Demand server and the computer where you will be using the Console.
- Each user who will use the Console to configure software packages must have a JRE installed.
- Each user who will upload software packages, e-mail lists, or floorplan images must have the latest version of a Flash browser plug-in.

This section contains the following topics about the Web Console:

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

Launching the Avalanche Web Console

To access the Web Console, you need:

- An Internet browser, such as Internet Explorer, Firefox, or Chrome.
- An Internet connection between the Avalanche enterprise server and the computer where you will be using the Console.



- The web components installed at the same location as the enterprise server. If you performed a custom installation, you should have selected the **Web Components** option to be installed. If you performed an enterprise installation, the web components were installed automatically.
- Each user who will use the Console to configure software packages must have a JRE installed locally.
- Each user who will upload software packages, e-mail lists, or floorplan images must have the latest version of a Flash browser plug-in.

NOTE: If you choose to use a certificate to create a secure connection between the browser and the server, see [SSL Certificates for the Web Console](#) on page 158 for information on launching the Web Console.

To access the Web Console from the Java Console:

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

The Web Console appears in your default browser.

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

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

- 3 Click **Connect**.

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

To access the Web Console from a web browser:

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

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

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

The User Login page appears.

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

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

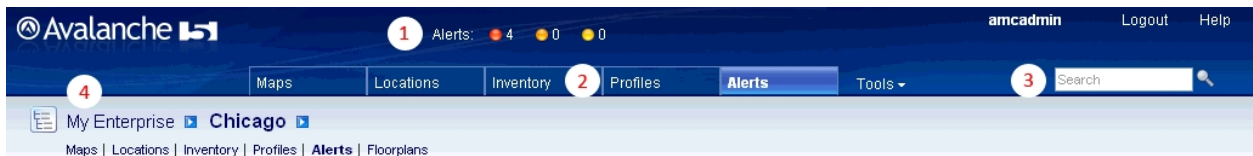
- 3 Click **Connect**.

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



Understanding the Web Console

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



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

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

NOTE: To refresh the information displayed on the page, press **F5**.

This section gives details about the following areas:

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



Management Tabs

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

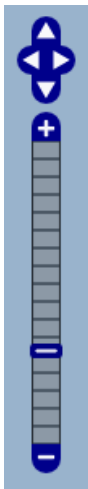
NOTE: If you want additional filtering by location, navigate to the location and then use the context links under the location name to navigate.

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

Maps Tab

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

The following options are available for configuring the map display:



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

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

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

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



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

Locations Tab

The **Locations** tab provides a panel with a summary of the location, a panel with details about any associated sub-locations, and a panel showing users authorized to manage the location. For information on managing locations with the Web Console, see [Location Management](#) on page 31.

Inventory Tab

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

Profiles Tab

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

NOTE: For information on applying a profile to a location, see [Applying Profiles to Locations](#) on page 32.

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

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



To change the priority of applied profiles:

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

The Change Priority page appears.

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

Alerts Tab

The **Alerts** tab provides a panel listing current alerts associated with your location. For information on acknowledging and clearing alerts, see [Acknowledging and Clearing Alerts](#) on page 136.

Tools Menu

The **Tools** menu provides access to the Reports tool, user management, audit logs, scheduled tasks, system information and settings. For tasks related to the Tools menu, see [Console Tools](#) on page 15.

Location Navigation

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

To navigate to a location to view:

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

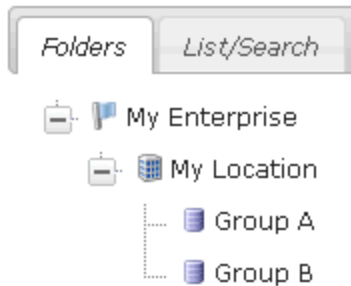
-Or-

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



Location View button





Folders tab of the Location View

Panels

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

Model Name	Terminal ID	MAC Address	IP Address	Sync State	Last Contact	Recent Activity
SYMMC75	HansenMC75	00-15-70-9B-FD-4C	10.22.168.177	✓	11/21/11 2:26 PM	Updated
SYMMC75	11	00-15-70-BF-95-7A	10.21.0.210	✓	11/15/11 3:42 PM	Updated
SYMMC3090	10	12-12-13-00-00-08	10.22.168.1	✓	11/21/11 4:30 PM	Updated

Mobile Devices panel

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

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

The top right of the panel contains options for displaying the information: how many items to display per page, and first/previous/next/last page options. There is also a **Help** button that opens a window to a related help page. Some panels that display information that may change also have a **Refresh Data** option in the top right corner, so you can manually refresh the information in the panel.

Some panels include large lists of information. By default, Avalanche generally displays the first ten items and then allows you to page through the rest of the list. You can change the number of items displayed per page, however, by clicking the preset number at the top of the panel. To page through the list, click the **First**, **Previous**, **Next**, and **Last** arrows.

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

NOTE: You can only delete one profile at a time.



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

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

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

Editing Columns

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

To edit the columns displayed:

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

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

- 2 To add a column, select the column you want to display from the Available Columns list and click **Add**.

The column name moves to the Selected Columns list.

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

The column name returns to the Available Columns list.

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

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

The columns are rearranged to reflect your modifications.

To display custom columns:

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

The *Modify Columns* dialog box appears.



- 2 Click **Add Custom**.

The *Add Custom Property* dialog box appears.

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

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

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

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

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

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

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

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

The columns are arranged to reflect your modifications.

Using Device Filters

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

To create a device filter:

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

The *Modify Filters* dialog box appears.

- 2 Click **New Filter**.

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

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

The *Selection Criteria Builder* dialog box appears, allowing you to create a filter based on a variety of device characteristics. For more information on using selection criteria, see [Using Selection Criteria](#) on page 138.

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

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



6 Click **Add New Filter**.

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

7 Click **Save Changes**.

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

To apply a device filter:

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

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

Understanding Edit Mode

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

Consider the following when using Edit Mode:

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

Console Tools

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

- [Viewing System Information](#)
- [Configuring Audit Logging](#)
- [Viewing the Audit Log](#)
- [Configuring General System Settings](#)
- [Configuring E-mail Settings](#)



- [Setting a System Message](#)
- [Creating Links in the Tools Menu](#)
- [Checking for Available Updates](#)
- [Installing Language Support](#)

Viewing System Information

From the Web Console, you can view statistics about the enterprise server, Inforail, statistics server, 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 your Avalanche installation. To manage licenses, use the Java Console.

Configuring Audit Logging

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

NOTE: For information on viewing actions in the audit log, see [Viewing the Audit Log](#) on page 18.

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

You can also archive the audit log at a specific time every day. When the information is archived, it is copied to a `.csv` file. The `.csv` file is stored in the same directory where backup files are stored. For information on configuring the backup file location, see the Java Console User Guide.

The following events can be configured for logging:

Deployment Package modifications	When a deployment package is modified.
Profile modification	When a profile is modified.



Device Commands	When one of the tools in the Device Details Tools panel is used.
Device Group modifications	When a device group is modified.
Group Location modifications	When a group location is modified.
Region Location modifications	When a region is modified.
Server Location modifications	When a server location is modified.
Profile Application modifications	When a profile is applied, excluded, or removed from a location.
Scheduled Event, Apply/Deploy Profiles	When an Apply/Deploy Profiles event has occurred.
Scheduled Event, Deploy/Update Servers	When a Deploy/Update Servers event has occurred.
Scheduled Event, System Backup	When a System Backup event has occurred.
Scheduled Event, System Restore	When a System Restore event has occurred.
Scheduled Event, Uninstall Server	When an Uninstall Server event has occurred.
Scheduled Event, Universal Deployment	When a scheduled Universal Deployment event has occurred.
Scheduled Event, Update Firmware	When an Update Firmware event has occurred.
User Logon/Logoff	When a user logs on or logs off the Avalanche Console.
User modifications	When a user account is modified.
VLACL modifications	When the VLACL is modified.
Console to Device Server Events	When servers are managed from the Console.

To enable audit logging:

- 1 Click **Tools > Settings**.

The System Settings page appears.



- 2 In the Audit Logging section, The Audit Logging Setting is displayed as either **Enabled** or **Disabled**. Click the setting to configure audit logging.
- 3 Enable the **Enable Audit Logging** check box.
- 4 If you want the audit log archived, enable **Enable Audit Log Archiving** and select the time of day (using a 24-hour clock) you want the log to be archived.
- 5 From the list, enable the events you want to record.
- 6 Click **Save**.

Viewing the Audit Log

The audit log collects information about actions performed from the Avalanche Console. As part of the data collection, the audit log tracks the username and IP address for each logged event, the date and time of the Console activity, and a description of the changes that occurred. Only an administrator user can configure and view the audit log.

NOTE: For information about enabling and configuring the audit log, see [Configuring Audit Logging](#) on page 16.

You must enable the audit log before you can view it. If desired, select criteria to filter the logged events so you can view the entire log or just a specific type of entry.

To view the audit log:

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

The Audit Log page appears.

- 2 Select the filter or filters you want to use:
 - To filter events by date, enable **Date Range** and use the calendar buttons to select the beginning and end dates.
 - To filter events by IP address, enable **IP Range** and enter the range of addresses you want to view.
 - To filter events by type, enable **Activity Type** and select the check boxes for the activities you want to view.
 - To filter events by username, enable **Username** and select the username from the drop-down menu.
- 3 Click **Apply Filters** to update the list according to your filter.

All events matching the filters appear in the list.



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

NOTE: You can also view the audit log from the System Settings page by clicking the **Audit Log** button.

Configuring General System Settings

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

NOTE: For information on configuring integrated logon for the Avalanche Console, see [Configuring Integrated Logon](#) on page 29.

To configure general system settings:

- 1 Click **Tools > Settings**.

The System Settings page appears.

- 2 Modify the settings as desired:
 - If you want to configure the length of time before an inactive Web Console user is logged off, or how often the page refreshes, type the number of minutes in the appropriate text box under **Web Settings**. The settings will only affect the Console for the user who configures them.
 - If you want to configure how many days an alert is displayed, how many alerts are displayed, or how many alerts are stored in the database, type the appropriate numbers in the text boxes under **Alert Settings**. The alert display settings will only affect the Console for the user who configures them. The **Number of alerts to store** option will only be available to administrators.
 - In the Edit Lock Control area, select **Enable Edit Lock Control** and set the **Edit Lock Timeout** and **Timeout Warning Tolerance**. If a user is editing an item (such as a profile), he has a limited amount of time to make and save his changes before the Edit Lock times out. When the Edit Lock times out, a prompt will appear asking if he wants to extend the Edit Lock. If he does not respond to the prompt, the Edit Lock will be canceled, changes will not be saved, and other users will be able to edit the item. The Edit Lock Timeout is the amount of time he has before the prompt appears, and the Timeout Warning Tolerance is the amount of time between when the prompt appears and when the Edit Lock is canceled.



- If you want to configure the maximum threshold for enterprise server messages allowed in the backlog, type the number of messages in the text box under **Message backlog**. If the spillover threshold is reached, the device servers are throttled and further messages are stored in a file to disk until the backlog is reduced. When device servers are throttled, they will no longer send device statistics updates to the enterprise server. After the backlog has been reduced, messages are pulled from the store file back into the log and the device servers are no longer throttled.
- If you want to enable or configure audit logging, click on the status and enable the desired options. For more information on audit logging, see [Configuring Audit Logging](#) on page 16.
- If you want to change the **Language** used in the Avalanche Console, use the drop-down list to select the desired option. This setting will only affect the Console for the user who configures it. You must have the language package installed in order to select a language other than English.

The language package can be downloaded from the Wavelink Web site. Install the language package on the same computer as the enterprise server and the installed language option will appear in the **Language** drop-down list. For instructions on installing a language package, see [Installing Language Support](#) on page 22.

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

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

Configuring E-mail Settings

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

To configure e-mail settings:

1 Click **Tools > Settings**.

The System Settings page appears.

2 Click the **Email Settings** button.

The *Email Settings* dialog box appears.

3 Type the location of the e-mail server you want Avalanche to use in the **E-Mail server** text box.

4 Type the **Username** and **Password** in the text boxes.



- 5 Type the address a reply should be sent to if an alert e-mail is replied to in the **Reply-to email address** text box.
- 6 Type the address the e-mails will appear from in the **From email address** text box.
- 7 Select the port Avalanche should use when contacting the e-mail server.
- 8 Click **Save** to save your changes.

Setting a System Message

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

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

- 1 Click **Tools > Settings**.

The System Settings page appears.

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

The message will be displayed for all Web Console users.

Creating Links in the Tools Menu

Add custom links in the **Tools** menu to provide easy access to other pages. When you create a link in the **Tools** menu, provide the text for the link and the URL to the desired page. Only an administrator will be able to perform this task.

To create a new link in the Tools menu:

- 1 Click **Tools > Settings**.

- 2 In the Custom Tools Links panel, click **Add**.

The *New Custom Tools Link* dialog box appears.

- 3 Type the name of the link that will appear in the Tools menu in the **Link Name** text box.
- 4 Type the full URL for the page in the **Link URL** text box. For example:

```
http://www.wavelink.com/
```

- 5 Click **Add** to close the dialog box.
- 6 Click **Save**.

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



Checking for Available Updates

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

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

To check for available software updates:

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

The Check for Avalanche Updates page appears.

- 2 Click **Check for Updates**.

The *Check for Updates* dialog box appears.

- 3 Click **Accept** to allow Avalanche to send system and device information to Wavelink.

- 4 Updates for installed software appear in the Available Updates panel. Click the link to download the new version.

Installing Language Support

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

To install an Avalanche language support pack:

- 1 Download the language support pack from the Wavelink web site.

- 2 Double-click the file to run the installer on the computer where Tomcat is running. (This is generally where the enterprise server is installed.)

The *InstallShield Wizard* appears.

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

- 4 The language support pack is installed. Click **Finish** to close the installer.

Once you have installed the language support, you can configure the Web Console on a per-user basis to use the desired language. For information on configuring the Web Console to use an installed language, see [Configuring General System Settings](#) on page 19.



Chapter 3: Managing User Accounts

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

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

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

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

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

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

This section provides the following information about user accounts:

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



Creating User Accounts

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

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

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

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

- Type** Select if the user is a Normal user or an Administrator. If the user is a Normal user, you will need to assign specific permissions. If the user is an Administrator, he will have access to the entire company.
- User Home** The portion of your network that the user will be assigned to. The user will only be able to access profiles and information for his assigned location.
- Description** A description of the user or group.
- Login** The name the user will use to log in to the Avalanche Console. The login is case sensitive. The following special characters are not allowed:
 ~ ! ^ * () + = | ? / < > , [] : ; { } \ " & space
- Password** The password that will grant access to the Avalanche Console. Passwords are case sensitive. The password has a 32-character limit.
- Confirm Password** You must confirm the password you assign to the user.
- First Name** The first name of the user.
- Last Name** The last name of the user.

To create a new account:

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

The User Management page appears.

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



- 3 The *Create User* dialog box appears. Click **User**.
- 4 The User Management page appears. Configure the settings for the user. **Login**, **Type**, **User Home**, **Password**, and **Confirm Password** are required fields.
- 5 Assign permissions now or an Administrator can modify permissions later.
- 6 Save your changes.

The new account is available. However, if a new user is set as a Normal user, that user will not have access to any areas of the Console until permissions are assigned to that user. For more information, see [Assigning User Permissions](#) on page 26.

Creating User Groups

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

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

- Software Admin
- Help Desk
- Network Admin

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

[To create a new user group:](#)

- 1 Click **Tools > User Management**.
The User Management page appears.
- 2 In the Users panel, click **New**.
- 3 The *Create User* dialog box appears. Click **User Group**.
The New User Group page appears.
- 4 Configure the settings and permissions for the group. **Group Name**, **Type**, and **User Home** are required fields.
- 5 In the Group User List panel, select the check boxes next to the names of the users who will be assigned to the user group.
- 6 Select the options in the Permissions panel to determine what users will have permissions for. Each user assigned to the group will have access for all group permissions as well as



the permissions assigned for his user account. For more information about permissions, see [Assigning User Permissions](#) on page 26.

- 7 Save your changes.

To view the users in a user group:

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

The User Management page appears.

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

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

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

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

The User Management page appears.

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

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

Assigning User Permissions

If you have an Administrator account, you have unlimited permissions and can assign and change permissions for Normal user accounts. When a Normal user account is assigned permissions to a functionality, that user has permissions for that specific functionality in his home location and any associated sub-locations. A user must have permissions for a location in order to view or edit the profiles, devices, or groups associated with the location.

Permissions can be assigned when a user is created, or from a specific location, profile, or mobile device group. This section describes the permissions available from the User Management page. For information on giving permissions to a user for a specific location, profile, or mobile device group, see [Assigning Authorized Users](#) on page 28.

The following table describes permissions that are available for profiles:

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



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

The following table describes permissions that are available for inventory:

Inventory		
Mobile Devices	View Only allows the user to view the mobile devices for assigned locations.	View/Manage allows the user to manage the mobile devices for assigned locations or mobile device groups.
Mobile Device Groups	View Only allows the user to view the mobile device groups and the devices they contain.	View/Edit allows the user to edit group properties for mobile device groups. A user must also have Mobile Devices permissions in order to view/edit the devices in a group.
Mobile Device Properties	View Only allows the user to view mobile device properties.	View/Edit allows the user to edit properties for mobile devices.
Remote Control	View Only allows the user to connect to a mobile device using Remote Control.	View/Edit allows the user to connect to a device using Remote Control or configure Remote Control connection profiles.

The following table describes the other permissions that are available:

Other		
Location Management	View Only allows the user to view location configurations and settings.	View/Edit allows the user to view, manage, and configure locations.



Other		
Synchronization	View Only allows the user to view recent and scheduled synchronizations.	View/Edit allows the user to create and deploy infrastructure or server packages, and initiate server synchronization.

Assigning Authorized Users

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

This section contains the following information:

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

Assigning Authorized Users to Locations

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

To assign a user to a location:

- 1 Navigate to the location and click the Locations context link.
- 2 In the Authorized Users panel, click **Assign**.
The *Authorized Users* dialog box appears.
- 3 Select the user/group from the drop-down list.
- 4 Click **Save**.

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

Assigning Authorized Users to Profiles

You can assign administrative privileges to a Normal user for a specific profile. If you want to give a Normal user permissions for all profiles of a specific type, see [Assigning User Permissions](#) on page 26.

To add or remove an authorized user:

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



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

Assigning Authorized Users to Mobile Device Groups

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

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

To add an authorized user:

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

The Mobile Device Group Details page appears.

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

The *New Authorized User* dialog box appears.

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

The user is added to the list of authorized users.

Configuring Integrated Logon

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

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



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

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

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

To enable integrated logon:

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

Avalanche is now configured to recognize authenticated system users.

Removing User Accounts

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

To delete a user account:

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

The User Management page appears.

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

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

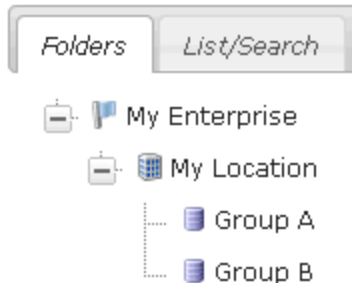


Chapter 4: Location Management

Avalanche uses locations in order to organize devices, users, and settings. Avalanche lets you organize devices in group locations to make them easier to manage. Locations are organized in the Location View, which can be accessed by clicking the Location View button:



Location View button



Folders tab of the Location View

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

Avalanche uses selection criteria to determine which devices belong to each group location. For example, if Group A has the selection criterion: `ModelName = ITCK30`, any Intermec CK30 devices automatically appear in the Group A inventory as well as the server location inventory. A device can belong to more than one group location concurrently.

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

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

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



Managing Group Locations

Group locations are groups of mobile devices that connect to the same server. Group locations allow increased flexibility for assigning different profiles at the same server location. A group location must be created in a server location where there is a mobile device server. Avalanche uses selection criteria to determine which devices belong to each group location.

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

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

To create a group location:

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

The New Group Location page appears.

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

A group location appears under the server location. The mobile devices meeting the specified selection criteria will be assigned to the group location. View the mobile devices in the group by selecting the group and then viewing the device inventory.

Applying Profiles to Locations

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



When you assign a profile to a location, it is also applied to any sub-locations and their devices. When this happens, the profile is said to be inherited. For information on excluding profiles that have been inherited, see [Editing Exclusions](#) on page 33.

Profiles are applied to the devices based on the selection criteria for the profile and the priority in which the profiles are listed in the Avalanche Console. Each profile can have selection criteria that define which devices can use the profile. A profile can be assigned additional selection criteria when it is applied to a location. This may be useful when a single location requires specialized or additional criteria. For information on selection criteria, see [Using Selection Criteria](#) on page 138.

For a general description of the types of profiles available, see [Getting Started](#) on page 3.

To apply a profile to a location:

- 1 Navigate to the location where you want to apply the profile and click the **Profiles** context link.
- 2 In the Available Profiles panel, select the check box next to the name of the profile you want to apply and click **Apply**.
- 3 Click **Apply** to apply the profile without deploying it. If you want to schedule a server synchronization for the location, click **Schedule Synchronization** and select the desired synchronization options.

NOTE: You can also apply a profile to a location from the Profile Details page. From the **Profiles** tab, click the name of the profile you want to apply. In the Applied Locations panel, click **New** and select the location you want to apply the profile to.

To view where a profile has been applied:

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

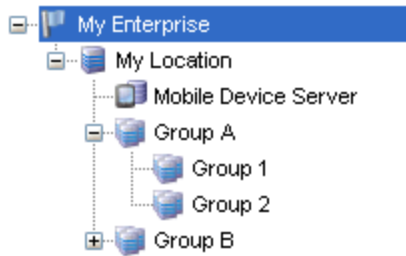
The home location for the profile appears in the profile details. You can also view the locations where the profile has been applied in the Applied Locations panel.

Editing Exclusions

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

For example:





Navigation Window

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

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

To exclude an inherited profile:

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

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

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



Chapter 5: Managing Network Profiles

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

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

The **Authorized Users** panel allows you to assign privileges for a profile to a user that does not have rights for that profile. This allows you to give a user permission for one specific profile, rather than all profiles of a specific type. Users that already have permission for the profile will not appear in the list of available users. For information about creating users and assigning permissions, see [Managing User Accounts](#) on page 23.

This section contains the following topics:

- [Creating Network Profiles](#)
- [Configuring Scheduled Settings](#)

Creating Network Profiles

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

To create a network profile:

- 1 From the **Profiles** tab, click **New Profile**.
- 2 The *New Profile* dialog box appears. Select **Network Profile**.
- 3 The New Profile Details page appears. Type a name for the profile in the **Name** text box.
- 4 If desired, enable the profile or set the profile to **Override manual settings on the mobile device**. If the profile is configured to override, it overrides any settings set from the device each time the device connects.
- 5 Click **Launch wizard** to use the Selection Criteria Builder to determine which devices the network profile manages. For details about using selection criteria, see [Using Selection Criteria](#) on page 138.
- 6 To add a mobile device IP address pool, click **Edit**.



The *IP Address Pools* dialog box appears.

- In the **Start** text box, type the lowest number you wish to include in your pool.

For example:

192.168.1.1 (for static addresses)

0.0.0.1 (for addresses with a Server address mask)

- In the **End** text box, type the highest number you wish to include in your pool.

For example:

192.168.1.50 (for static addresses)

0.0.0.50 (for addresses with a Server address mask)

- If you desire the addresses in the range to be masked with the Server address, enable the **Mask with server address** checkbox and enter the mask.

For example:

0.0.0.255

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

The available addresses and the mask will appear in the table to the left. This list will display all entered addresses.

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

- 7 If desired, type any **Notes** in the text box.
- 8 If you want the profile to manage WLAN IP, WLAN, or WWAN settings, enable the appropriate check box. When the boxes are enabled, the related panels appear below. For information on the options in these panels, see [Configuring Scheduled Settings](#) on page 36.
- 9 Click **Save**.

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

Configuring Scheduled Settings

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

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



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

This section contains information on the following configuration options:

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

Configuring WLAN IP Settings

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

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

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

Gateway Provides mobile devices with the address for the node that handles traffic with devices outside the subnet. You can provide the address, DNS name, or use the server location value.

Subnet Mask Provides mobile devices with the subnet mask. You can provide the address, DNS name, or use the server location value.

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

Domain Name Provides the domain name to 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.



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

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

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

The Network Profile Details page appears.

- 2 Click **Edit**.

The Edit Network Profile page appears.

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

The WLAN IP Settings panel appears.

- 4 Configure the WLAN IP settings as desired.

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

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

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

The Network Profile Details page appears.

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

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

- 4 Click **Save**.

The changes are applied at the scheduled time.

Configuring WLAN Settings

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

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



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

None. Devices do not encrypt information.

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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



To configure current WLAN settings:

- 1 From the Available Profiles panel on the **Profiles** tab, click on the network profile you want to edit.
- 2 The Network Profile Details page appears. Click **Edit**.
- 3 The Edit Network Profile page appears. Enable the **Manage WLAN** checkbox.
- 4 The WLAN Settings panel appears. Configure the WLAN settings as desired. If you select 128-bit WEP, WPA, or WPA2 encryption, you can enable the **Use authentication** check box to select the type of authentication to use.
 - If you select WEP keys, select either 40-bit or 128-bit key size and create the keys. The keys you enter must be in hex format. A 40-bit key should have 10 characters and a 128-bit key should have 26 characters. To change the value for one of the hex digits in a key, type a new value (using 0-9 and A-F) in the appropriate text box. An example of a 40-bit key would be: 5D43AB290F.
 - If you select WEP key rotation, choose the 40- or 128-bit key size, the starting date and time, rotation interval, and a passcode.
 - If you are using a pre-shared key with WPA or WPA2, type the passphrase or hex key in the **Key** text box. Use the **Broadcast key rotation interval** option to set how often the key is rotated.
 - If you select PEAP or TTLS authentication, enable the **Validate Server Certificate** check box to provide a path to the certificate.
 - If you select EAP_FAST, provide a path and password to a PAC (Protected Access Credential) file. This will provision devices with the PAC file.
 - If you are an authentication method, configure whether the **User Credentials** are **Prompt** (user is prompted when credentials are required) or **Fixed** (credentials are automatically sent when required).

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

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

To configure scheduled changes for WLAN settings:

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

The Network Profile Details page appears.

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



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

The changes are applied at the scheduled time.

Configuring WWAN Settings

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

Connection Name	A name for the connection.
Connection Type	There are two connection types available for your WWAN-enabled devices: APN (GPRS / EDGE / 3G). Provide a domain (Access Point Name) if you are using this type of connection. An example of an APN would be: wap.cingular Dial-Up. Type the number to be dialed by the modem. This does not correspond to the number of the device.
Credentials	Sets the Username , Password , and Domain credentials for the connection when they are necessary.
Custom Properties	This option allows you to add custom properties to the devices that receive this network profile. By clicking _ defined , you can add, edit, and delete properties and their values.
Enable TCP/IP header compression	Improves the performance of low-speed connections.
Enable software compression	Improves the performance of low-speed connections.
Activate phone as needed	Allows the Enabler to activate the device's phone if a WWAN connection is necessary.



Dial broadband connection as needed	Allows the Enabler to attempt a WWAN connection if a LAN connection cannot be established.
Public IP address for Avalanche Server	Provides the IP address of the enterprise server that is accessible from a WWAN. This is necessary if the device tries to contact the server when connecting from outside of the server's local network.

To configure current WWAN settings:

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

To configure scheduled changes for WWAN settings:

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

The Network Profile Details page appears.

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

The changes are applied at the scheduled time.



Chapter 6: Managing Scan to Configure Profiles

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

This section contains instructions for the following tasks:

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

Once you have configured your Scan to Config profile, you can apply that profile to any location in the Console. When you apply a profile to a location, the users who have permissions for that location can make changes as necessary. For more information about assigning Scan to Config profiles to a location, see [Applying Profiles to Locations](#) on page 32.

Creating a Scan to Config Profile

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

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

To create a Scan to Config profile:

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

The *New Profile* dialog box appears.

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

The New Profile Details page appears.

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

- 4 To encrypt the barcodes, type a passcode in the **Encryption Passcode** text box and confirm it in the **Confirm Passcode** text box. The passcode is used to encrypt the barcode data. The mobile device user must enter the same passcode when he scans the barcodes so that the



Enabler can decrypt the barcode data. If the user does not input the correct passcode at the device, then the barcode data is not decrypted and the scan registers as invalid.

- 5 Set the maximum barcode length. This defines how many characters are encoded in each barcode.
- 6 If you have already configured a network profile and want to use the settings from that profile, enable **Use settings from network profile** and select the network profile from the drop-down list. Enable **Use current profile setting** to use the current settings or, if the network profile has multiple scheduled settings, enable **Use scheduled profile change effective** and select the start time from the drop-down list.
- 7 If you want to set a static IP address for the device, enable **Assign static IP address** and type the **IP Address**, **Subnet mask** , and **Gateway** in the appropriate boxes.
- 8 If desired, type any notes in the **Notes** text box.
- 9 Click **Save**.

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

Configuring a Scan to Config Profile

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

The **Authorized Users** panel allows you to assign privileges for a profile to a user that does not have rights for that profile. This allows you to give a user permission for one specific profile, rather than all profiles of a specific type. Users that already have permission for the profile will not appear in the list of available users. For information about creating users and assigning permissions, see [Managing User Accounts](#) on page 23.

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

Adding Custom Properties for Scan to Config Profiles

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

To add a custom property:

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



- 2 Click **Edit**.
- 3 In the Properties panel, click **New**.
The *New Property* dialog box appears.
- 4 Type the **Name** and **Value** in the text boxes.
- 5 Select whether the property is a Device or Network property.

NOTE: Most properties will be device properties.

- 6 Click **Add**.
- 7 Click **Save**.

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

Adding a Registry Key to a Scan to Config Profile

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

To add a registry key:

- 1 From the **Profiles** tab, click on the name of the profile you want to configure.
The Profile Details page appears.
- 2 Click **Edit**.
- 3 The Edit Profile page appears.
- 4 In the Registry Keys panel, click **New**.
The *New Registry Entry* dialog box appears.
- 5 Select the **Root** from the drop-down list.
- 6 Type the name of the key in the **Key** text box.
- 7 Type the value entry of the key in the **Name** text box.
- 8 Enter the data for the value entry in the **Data** text box.
- 9 Select the **Type** of the value from the drop-down list.
- 10 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.



Printing Barcodes

Once you have created and configured a Scan to Config profile, print the set of barcodes for the profile. You can then scan the barcodes with a mobile device to change the network settings on that device. The Avalanche Web Console prints the barcodes to a .pdf file which you can save or send to a printer.

To print a Scan to Config profile as a barcode:

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

The Scan to Config Profile Details page appears.

- 2 Click **Print Barcodes**.

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

Scanning Barcodes

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

The barcodes are numbered and contain data that tell the device how many barcodes are in the set. This allows you to scan the barcodes out of sequence. Settings are applied after all the barcodes are scanned.

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 a Mobile Device Server

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

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

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

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

- [Configuring a Mobile Device Server Profile](#)
- [Viewing Mobile Device Server Licensing Messages](#)
- [Viewing Server Properties](#)

Configuring a Mobile Device Server Profile

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

See the following sections for information about configuring mobile device server profiles:

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

The **Authorized Users** panel allows you to assign privileges for a profile to a user that does not have rights for that profile. This allows you to give a user permission for one specific profile, rather than all profiles of a specific type. Users that already have permission for the profile will not appear in the list of available users. For information about creating users and assigning permissions, see [Managing User Accounts](#) on page 23.



Mobile Device Server Profile General Configuration

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

Server Security

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

Avalanche offers two options for encryption:

- Transport Encryption** Matches the level of encryption with the capacity of the mobile device. Communication between the mobile device server and mobile devices will be encrypted to the degree possible.
- Strict Transport Encryption** Uses AES encryption for information. Only Enablers that support AES encryption (Enabler 5.0 or newer) will be able to connect to the server when strict transport encryption is enabled.

Avalanche offers two options for authentication:

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

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

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



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

Server Resources

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

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

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

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

Terminal ID

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

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

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

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

Server Logging

A Mobile Device Server profile has the following logging settings:



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

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

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

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

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

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

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

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

License Return

A Mobile Device Server profile has the following licensing options:

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

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

Secondary Server

You can configure the following connection settings:



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

Device Statistics

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

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



Enable SMS Notification	Allows the Mobile Device Server to use SMS notification if a device cannot be reached by UDP packets. This option is only available for devices with a phone, and must also be configured on the device and at the enterprise server. For more information on enabling SMS notification, call Wavelink Customer Service.
Suppress GPS Data Collection	Causes the Mobile Device Server to discard GPS data collected from the devices without sending it to the enterprise server.
Suppress Radio Statistics Collection	Causes the Mobile Device Server to discard radio statistics data collected from the devices without sending it to the enterprise server.
Suppress Realtime Properties Data Collection	Causes the Mobile Device Server to discard realtime properties data collected from the devices without sending it to the enterprise server.
Suppress Software Inventory Collection	Causes the Mobile Device Server to discard software profile data collected from the devices without sending it to the enterprise server.

Device Specific File Transfers

Directory for files uploaded from device When a package's .PPF file specifies that files are to be uploaded to Home, this option provides the path to Home on the machine local to the Mobile Device Server. If no path is specified, Home is defined as the Mobile Device Server installation directory.

Directory for files downloaded to device When a package's .PPF file specifies files that are to be downloaded from Home, this option provides the path to Home on the machine local to the Mobile Device Server. If no path is specified, Home is defined as the Mobile Device Server installation directory.

Configuring Blackouts

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

To create a blackout/exclusion window:

- 1 From the **Profiles** tab, click on the Mobile Device Server profile from the **Available Profile** panel.
- 2 The Mobile Device Server Profile Details page appears. 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.
- 4 The *New Blackout/Exclusion Window* dialog box appears. Type the start and end time of the blackout window. Enable the boxes for the days you want the blackout to apply and click **Save**.

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

Scheduling Profile-Specific Device Updates

From the Mobile Device Server profile, you can schedule profile-specific updates for your mobile devices. When you configure a Mobile Device Server update, you have the following options:

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



To schedule a profile-specific device update:

- 1 From the **Profiles** tab, click on the Mobile Device Server profile from the **Available Profile** panel.
- 2 The Mobile Device Server Profile Details page appears. Click **Edit**.
- 3 In the **Device Update Schedule** panel, click **New**.
- 4 The *New Device Server Update* dialog box appears. Select the event type. If you select **Recurring Event**, determine whether the update occurs on either a daily or weekly basis. If you select **Weekly** from this list, you must also select the day on which the update occurs.
- 5 Set the start date and time.

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

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

The update appears in the Device Update Schedule panel.

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

Viewing Mobile Device Server Licensing Messages

The Avalanche Console receives messages about license usage from the mobile device server. You can view these messages from the System Support page. A user must be an administrator to access this page.

To view licensing messages:

- 1 Click **Tools > Support**.
- 2 The System Support page appears. Next to **Mobile Device Server(s)**, click the **Details** button.
- 3 The *Mobile Device Servers* dialog box appears. Click the name of the server you want to view messages for.



The Mobile Device Server Details page appears.

Viewing Server Properties

You can view server properties from the Avalanche Console if you have permissions. 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.
- 2 In the Location Summary panel, click the **Details** button.

The Device Server Details page appears.



Chapter 8: Managing Software Profiles

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

This section contains the following topics:

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

Creating Software Profiles

Create software profiles to manage how and when software is distributed or updated on mobile devices. Associate software with a profile so that the software is distributed to the devices on a controlled basis.

Once a software profile has been created, you can edit the name, status, and selection criteria. You can also add software packages to the profile. For information on adding and configuring software packages, see [Managing Software Packages](#) on page 58.

Selection criteria determine which mobile devices receive the software profile. Only devices that meet the selection criteria for the software profile will receive the software associated with the profile. For information about creating selection criteria, see [Building Selection Criteria](#) on page 138.

The **Authorized Users** panel allows you to assign privileges for a profile to a user that does not have rights for that profile. This allows you to give a user permission for one specific profile, rather than all profiles of a specific type. Users that already have permission for the profile will not appear in the list of available users. For information about creating users and assigning permissions, see [Managing User Accounts](#) on page 23.

The home location for the profile is the location you have selected when you create the 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, enable the profile.
- 5 Click **Launch wizard** to use the Selection Criteria Builder to determine which devices the software profile will be applied to. For details about creating and using selection criteria, see [Using Selection Criteria](#) on page 138.
- 6 Click **Save**.

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

Managing Software Packages

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

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

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

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

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

Field	Description
Package Name	Displays the name of the software package.
Configure	Displays the date, time, and user for the most recent package configuration.
Status	Displays the enabled/disabled status of the software package.



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

This section includes the following information:

- [Adding a Software Package](#)
- [Building New Software Packages](#)
- [Creating CAB or MSI Packages](#)
- [Copying 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 and apply a software profile, add the software packages to that profile. Through the software profile you can configure the software package settings, enable the package, and then deploy the packages to specific mobile devices.

The Add Device Software Wizard allows you to add packages, enable packages, copy packages that have already been added to a different profile, or create custom software packages. Before



you create a custom package, ensure you know the location of all the files you want to include and ensure that the files are valid.

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

The following instructions provide information about adding an Avalanche package to a software profile. For information about building a new package, see [Building New Software Packages](#) on page 60.

To add a software package:

- 1 From the **Available Profiles** panel on the **Profiles** tab, click on the software profile you want to edit.
- 2 The Software Profile Details page appears. In the **Software Packages** panel, click **New**.
- 3 The Software Package Wizard appears. Select **Install an Avalanche package**.
- 4 Click **Select Package** to browse to the location of the software package. When you have selected the file, click **Open**.
- 5 In the Software Package Wizard, click **Next**.
- 6 A License Agreement appears. Accept the license agreement and click **Next**.
- 7 The package files will begin extracting locally. When the extraction is complete, click **Next**.
- 8 The Configure Software Package page appears. If desired, you can enable the package immediately.
- 9 Click **Finish** to complete the installation.

NOTE: If you want to enable a software package later, navigate to the software profile page and click **Disabled** in the Status column for the package you want to enable.

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

Building New Software Packages

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



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

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

Title A title for the package.

Vendor The package vendor.

Version The version number of the package.

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

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

Post Install Options Options for if the device will perform a warm boot or a cold boot after installation has completed, or if a program runs once installation is completed. When you select to run a program, the drop-down list will become active and you can select the program from your package to run. Post-install actions are optional.

To build a new package:

- 1 From the Available Profiles panel on the **Profiles** tab, click on the software profile you want to edit.
- 2 The Software Profile Details page appears. In the Software Packages panel, click **New**.
- 3 The Software Package Wizard appears. Select **Create a new Avalanche package** and type a name for the package in the text box.
- 4 Click **Next**.
- 5 The Specify the Files in the Ad Hoc Package page appears. Use the **Upload File** button to navigate to and select the file you want to add to the package and click **Add**.
- 6 The file is added to the list. Continue adding files as desired. When you have added all the files, click **Next**.
- 7 The Ad Hoc Package Options page appears. Configure the package options and click **Next**.
- 8 The Add Selection Criteria to the Ad Hoc Package page appears. If you want to configure selection criteria for the package, enable **Add Selection Criteria** and enter the information in the text box. By creating selection criteria for your package, only the devices which meet the selection criteria will receive the package.



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

9 Click **Next**.

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

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

11 Click **Finish** to complete the package.

Creating CAB or MSI Packages

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

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

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

2 The Software Profile Details page appears. In the Software Packages panel, click **New**.

3 The Software Package Wizard appears. Select **Install an Avalanche Package** and browse to the location of the `.CAB` or `.MSI` file.

4 Click **Next**.

5 The CAB or MSI File Options page appears. Type the name of the package.

6 If you want the package to be uninstalled once the program information is retrieved by the mobile device, enable **Remove after install**.

7 Click **Next**.

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

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

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



Copying Software Packages

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.
- 2 The Software Profile Details page appears. In the Software Packages panel, click **New**.
- 3 The Add Device Software page appears. 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 Click **Next** after the package has finished copying.
- 5 Choose whether the package is **Enabled** or **Disabled** and click **Finish**.

The package and its configuration are included in the target software profile.

Configuring Software Packages with a Utility

Some software packages come with configuration utilities that allow you to configure options before the packages are installed on a mobile device. These utilities can be accessed from the Avalanche Console. Configuration options will differ based on the software package. For details about configuring software packages, see the specific user guide for that product.

NOTE: If you do not have a current JRE installed locally, you must install it before you can 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.
- 2 The Software Profile Details page appears. In the Software Packages panel, click **Configure** for the software package you want to configure.

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

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



- 5 Select the utility you want to use and click **Launch Config**.
- 6 The utility is launched. Configure the package options as desired.

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

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

Configuring Software Packages for Delayed Installation

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

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.
- 2 The Software Profile Details page appears. In the Software Packages panel, click the name of the package you want to configure.
- 3 The Software Package Details page appears. Click **Edit**.
- 4 Configure the installation options as desired:
 - If you want to delay package activation until a specific date and time, enable the **Install date** option, click on the calendar button to select a date, and type the time in the provided text box.
 - To further delay the package installation after it has been activated, enable and configure the **Install delay** option. This will delay the installation of the package after it has been downloaded.
 - If you want the package to be activated during a certain time window, enable the **Install window** option and configure the hours during which the package will activate.
 - If you want the device user to have the option to override the software package installation delay, enable the **Allow device user to install on demand** checkbox. When



this option is selected, the user will be able to install the package as soon as it is downloaded.

- If you want to use the device for proxy package distribution, use the Use mobile device for proxy distribution of this package option. For more information on this option, see [Peer-to-Peer Package Distribution](#) on page 65.

5 Save your changes.

Peer-to-Peer Package Distribution

Peer-to-peer package distribution allows you to control bandwidth usage on your network by allowing a “package store” device to receive an update from the Mobile Device Server and then distribute the update to other mobile devices. If mobile devices cannot download an update from a package store device, they can contact the server directly.

Peer-to-peer package distribution has the following configuration options:

Option	Description
Enabled Cached Peer-to-Peer Package Distribution	Allows a package to be shared across multiple devices via peer-to-peer connections. When deployed to a package store device, the package will be available for other mobile devices from that package store device.
Do not allow non-Package Store Devices to begin updating until	Configures the time at which a non-package store device can contact a package store device to receive an update.
Do not allow server to update non-Package Store Devices until	Configures the time at which a non-package store device can contact the server to update and receive this package. Once the configured time is reached, the mobile devices will first attempt to contact a package store device to receive the update. If a package store device cannot be contacted or the connection times out, the device will then attempt to contact the server.

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



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

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



To configure peer-to-peer package distribution:

- 1 From the **Profiles** tab, click the name of the software profile with the package you want to configure.
- 2 The Software Profile Details page appears. In the Software Packages panel, click the name of the package you want to configure.
- 3 The Software Package Details page appears. Click **Edit**.
- 4 Configure the proxy distribution options as desired.
- 5 Save your changes.



Chapter 9: Managing Mobile Devices

This section provides information about the following mobile device topics:

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

Mobile Devices Panel

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

Model Name The model name of the mobile device.

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

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

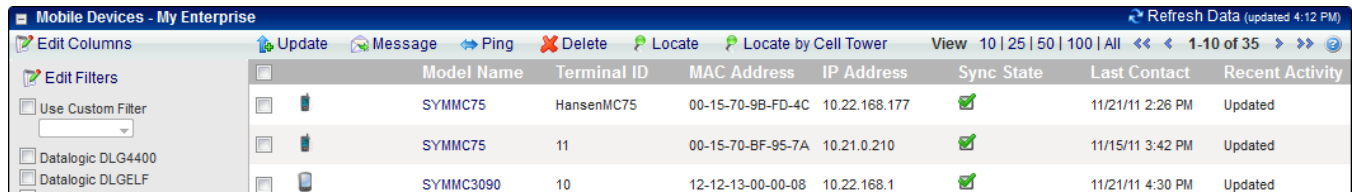
IP Address The Internet Protocol address assigned to the mobile device.

Sync State The synchronization 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`.





	Model Name	Terminal ID	MAC Address	IP Address	Sync State	Last Contact	Recent Activity
<input type="checkbox"/>	SYMMC75	HansenMC75	00-15-70-9B-FD-4C	10.22.168.177	<input checked="" type="checkbox"/>	11/21/11 2:26 PM	Updated
<input type="checkbox"/>	SYMMC75	11	00-15-70-BF-95-7A	10.21.0.210	<input checked="" type="checkbox"/>	11/15/11 3:42 PM	Updated
<input type="checkbox"/>	SYMMC3090	10	12-12-13-00-00-08	10.22.168.1	<input checked="" type="checkbox"/>	11/21/11 4:30 PM	Updated

Across the top of the panel are device tasks. You can select the checkbox to the left of the device name and then click the task (such as **Update** or **Delete**). When you use the **Update** command, a request is sent to the device that it contact the mobile device server and download any new settings.

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



For more information about options available for the Mobile Device Panel, see [Panels](#) on page 12.

Viewing Mobile Device Details

The Mobile Device Details page appears when you click on the name of a mobile device. It provides information about a specific mobile device and consists of the following areas:

- **Summary Information.** Provides a quick summary of device, health, signal strength and battery life information. The bars will display red, yellow, or green depending on the status of the battery, signal strength, and signal quality of the device. For advanced details, click the **Advanced** button. For information about the profiles applied for the device and their priority, click the **Profile Info** button.
- **Tools panel.** Provides tools for contacting and managing your device. For information on using the tools in this panel, see [Contacting the Mobile Device](#) on page 74.
- **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 71.
- **Packages panel.** Displays the packages installed on the device, their revision numbers, and reported status (whether the package has been installed, is pending, or the installation failed).
- **Device History panel.** Displays a history of Avalanche actions for the mobile device. This may include actions such as changing packages, editing properties, applying a profile, rebooting the device, or changing the Enabler configuration by a device user. This



information is only available for devices with 5.2 Enablers that are configured to report the events. (This can be configured on the Reporting tab of the Enabler Configuration Utility.)

- Applied Profiles panel. Displays the profiles that are applied to this device. You can filter the applied profiles by using the check boxes at the left of the panel.
- Installed Software panel. Displays the software installed on the mobile device.

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

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

Locating a Mobile Device

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

To view the location of a mobile device:

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

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

Locating a Device using Cell Tower Information

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

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

To locate a device using cell tower information:

- 1 Navigate to a location or mobile device group containing the device you want to locate.
- 2 Click the **Inventory** context link.



- 3 In the Mobile Devices panel, select the checkbox next to the name of the device you want to locate and click **Locate Cell Tower**.

An icon appears on the map displaying the location of the cell tower the device reported.

Viewing Location History

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. The statistics server only retains GPS information for the past 48 hours.

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

To view the location history of a mobile device:

- 1 Click the **Inventory** tab.
- 2 In the Mobile Devices panel, click the name of the device you want to view a history for.

The Device Details page appears.

- 3 In the Tools panel, click **Location History**.

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

Configuring Mobile Device Properties

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

NOTE: See [Building Selection Criteria](#) on page 138 for more information on using properties as selection variables.

You can view the properties for a specific mobile device by clicking on the name of the device from the **Inventory** tab.

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

Property The group the property belongs to.

Group



Data Type	Indicates if the value is configurable or snapshot. Configurable means that a user may change the value, and snapshot means that the property is updated by the device.
Name	The name of the property.
Value	The value of the property.
Pending Value	Indicates whether the property needs to be updated on the mobile device. If it needs to be updated, column will display the pending value in italics.

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

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

Creating Custom Properties

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

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

To create custom properties:

- 1 From the **Inventory** tab, click the name of the mobile device you want to configure.
The Mobile Device Details page appears.
- 2 In the Properties panel, click **New**.
The *New Mobile Device Property* dialog box appears.
- 3 Type the category to which you want to add the property in the **Property Group** text box.
- 4 Type the **Name** and **Value** of the property in the text boxes.
- 5 Click **Save**.
The property is added to the list in the Properties panel.



Creating Device-Side Properties

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

NOTE: The Avalanche Enabler sends device-side properties to the Enterprise Server; it does not collect the information. Users 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 panel on the Mobile Device Details page.

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

Editing Properties

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

Custom properties can be edited either for an individual mobile device, or using a mobile device profile or a Scan to Config profile. For information on using a profile to edit properties, see the section for that profile type.

To edit a property for a mobile device:

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

The Mobile Device Details page appears.

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

The *Edit Property* dialog box appears.

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

The new value downloads to the mobile device when it connects to the server. If the device has not yet received an updated property value, the pending value appears in the Pending Value column for the property.



Deleting Properties

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

To delete a property:

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

The Mobile Device Details page appears.

- 2 In the Properties panel, enable the check box to the left of the property.
- 3 Click **Delete**.

The property will be deleted from the mobile device.

Contacting the Mobile Device

This section provides information about connecting to a mobile device and viewing device location. The following tasks are available from the Mobile Device Details page.

- [Pinging Mobile Devices](#)
- [Sending a Message to a Device User](#)
- [Updating a Mobile Device](#)
- [Chatting with a Device User](#)
- [Wiping a Mobile Device](#)

NOTE: The Registry Explorer, File Explorer, and Process Manager icons available on the Mobile Device Details page are only available when the mobile device has a licensed Remote Control client.

Pinging Mobile Devices

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

To ping a mobile device:

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

The Mobile Device Details page appears.

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



The Status field displays the status of the ping request.

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

Sending a Message to a Device User

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

To send a message to a mobile device:

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

The Mobile Device Details page appears.

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

The *Send Message* dialog box appears.

- 3 Type a message in the text box.

- 4 Click **Send**.

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

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

Updating a Mobile Device

You can perform individual updates for mobile devices that are currently in range and running the Avalanche Enabler. This sends any pending profiles or properties to the device.

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

Allow User to Override the Update Gives the mobile device user the option to override the update.

Force Package Synchronization Forces the package to update on the device.

Delete Orphan Packages Removes orphan packages from the device. Edit the list of orphan packages to remove specific packages from the device.



NOTE: The rules that govern which mobile devices can receive a particular update are determined by the selection criteria. See [Building Selection Criteria](#) on page 138 for more information on building selection criteria.

To update a mobile device:

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

The Mobile Device Details page appears.

- 2 In the Tools panel, click **Update Now**.

The *Update Now* dialog box appears.

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

- 4 Click **Update Device(s)**.

The Status field displays the status of the update.

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

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

Chatting with a Device User

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

To initiate device chat:

- 1 From the Inventory tab, click the name of the device you want to chat with.

The Mobile Device Details page appears.

- 2 Click **Device Chat** in the Tools panel.

The *Mobile Device Chat* dialog box appears.

- 3 Type the message you want to send in the lower text box. When you press **Send** or **Enter**, the message is sent to the device and appears in the upper text box. The device user’s response will appear in the upper text box.

- 4 When you are finished, click **Close** to close the dialog box.



Wiping a Mobile Device

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

If there is more than one mobile device profile applied on the device, all of the Device Wipe folders for all of the applied profiles will be deleted during a device wipe. For information on configuring Device Wipe folders, see [Configuring Device Wipe Folders](#) on page 121.

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

To perform a remote device wipe:

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

The server sends a wipe command to the device.



Chapter 10: Using Remote Control

This section provides information about using the Remote Control Console, configuring the Remote Control package, and using the Remote Control Viewer after you are connected to a mobile device. The tasks detailed in this section assume you are connected to a mobile device and that you installed the Remote Control server. Before you use Remote Control, perform the following tasks:

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

When Remote Control is installed and licensed, perform the following tasks:

- [Using the Remote Control Console](#)
- [Configuring the Remote Control Client](#)
- [Connecting to Mobile Devices](#)



Using the Remote Control Console

The Remote Control Console allows you to configure options for connecting to Avalanche, configuring the client, downloading and using skins, and viewing system information.

Some Avalanche server information must be configured before you can connect a device or manage package options. When you finish installing Remote Control, the installation process will automatically launch a browser window, or you can navigate to the Remote Control Console using the browser's address bar.

Once you have completed the initial configuration, you can configure the following options from the Remote Control Console:

- [Changing the Username and Password](#)
- [Synchronizing with the Avalanche License Server](#)
- [Configuring Server Options](#)
- [Configuring Skin Settings for the Server](#)
- [Managing Cell Carriers](#)
- [Backing Up and Restoring the Remote Control Database](#)
- [Viewing System Information](#)
- [Configuring Connection Profiles](#)

To log in to the Remote Control Console:

- 1 From the computer where the Remote Control server is installed, click **Start > Programs > Remote Control 4.1 > Server Setup**.

-Or-

From the Avalanche Console, select the software profile that has the Remote Control package. When you click to configure the package, the *Configure Software Package* dialog box appears. Double-click **Server Configuration** in the list.

- 2 Log in using the username and password configured during installation.

The Remote Control Console appears.

NOTE: You can also access the Remote Control Console by opening a web browser and typing the URL in an address bar. If you have not configured SSL, the URL is: `http://<IP address or Domain Name>:1900/app/setup_logon.vm`. If you have configured SSL, use the URL provided in the SSL instructions.



Changing the Username and Password

The Remote Control Administrator user account is required to log in when you first configure the server from a web browser. The default username is *admin* and the default password is *admin*. Wavelink recommends you change at least one of these. You must log in using the account (or an Administrator Avalanche account) in order to change it.

After you have completed the initial configuration of Remote Control and provided the database address and password, use your Avalanche username and password to log in to Remote Control. Avalanche user permissions will be enforced. Only an Avalanche Administrator will be able to view the Setup or System menus.

To change the Remote Control Administrator username and password:

- 1 From the Remote Control Console, click **Password** in the System Menu.
- 2 Type the new username and password in the text boxes. When you change the password, you must type it a second time in the **Retype Password** text box to confirm that it is correct.
- 3 Click **Save**.

Synchronizing with the Avalanche License Server

Connecting to the Avalanche License Server

Remote Control must connect to the Avalanche license server in order to distribute licenses. The port 7221 should be unblocked between the Remote Control server and the Avalanche license server. The Avalanche license server is usually installed at the same location as the enterprise server. Configure the Avalanche server address for Remote Control after the server is installed from the Remote Control Console.

You can check to ensure the Remote Control server can contact the Avalanche license server from the Remote Control Console.

To configure the license server information from a web browser:

- 1 From the Remote Control Console, click **Licensing** in the System Menu.
- 2 Type the address of the Avalanche server in the **License Server** text box. The default **Port** for the license server is 7221.
- 3 Click **Verify** to check if Remote Control can contact the license server.
- 4 Click **Save**.



Configuring Server Options

The Remote Control web page allows you to configure the schedule that Remote Control uses to sync with Avalanche and the Wavelink skins repository. It also allows you to configure the e-mail gateway for Remote Control, the mail server (either POP3 or SMTP) credentials and log setting, the device timeout settings, and the VNC settings. If you have configured the Remote Control Clients to use encryption, enable encryption for the server on the **Encryption** tab.

The Server Setup page has the following options:

Wavelink Sync tab	
Enable Sync	Enables or disables the Remote Control synchronization with the Wavelink skins repository.
Schedule	Schedules when Remote Control syncs with the Wavelink skins repository. The default value means that Remote Control will sync daily at 1 AM. Use a cron expression format.
Skins Repository	The address for the Wavelink skins repository.
Wide Area tab	
Host	The DNS name of the mail server.
Mail From	The address that will appear in the From field of the e-mail.
POP3 Host	The DNS name of the POP3 host.
User	The user name for the POP3 server.
Password	The password for the POP3 server.
Pop Before SMTP	When this is enabled, Remote Control will try to use the POP3 server before it attempts SMTP.
User	The user name for the SMTP server.
Password	The password for the SMTP server.
Port	The port used by the SMTP server.
Use Auth	Determines if authentication credentials are sent to the outgoing mail server.



Debug Mail Session	Enables or disables a Remote Control log for sending mail.
Timeouts tab	
TCP	How long to wait (in milliseconds) before the TCP connection request times out.
Send UDP Requests	If the server will attempt to use UDP to request the device to connect.
UDP	How long to wait (in milliseconds) before the UDP connection request times out.
SMS	How long to wait (in milliseconds) before the SMS connection request times out.
Web Session	The length of time (in seconds) before the connection to the Remote Control Console will time out.
VNC tab	
Quality	The quality of the Remote Control display. This is on a scale of 1-100, where 100 is the best quality and 1 is the worst quality.
Device Refresh	How often the device screen is refreshed during a Remote Control session.
Viewer Refresh	How often the viewer screen is refreshed during a Remote Control session.
Alt Server tab	
Use Alternate Server	Specifies that the Remote Control Console should be launched using a local server address. This option only needs to be enabled when the server address in the Client Settings is a publicly available IP address. (For example, if the device is using a WWAN address.)
Server Address	The local Remote Control server address to use for launching the Remote Control Console.
Encryption tab	
Use Encryption	Configures the server to use AES encryption.
Passphrase	The passphrase to use for encryption. This can include ASCII characters and be up to 64 characters long.



	<p>NOTE: The Client and Server BOTH must be configured with the same passphrase for encryption to work. For information on configuring the Client with encryption, see Editing the Remote Control Package on page 86.</p>
--	--

To configure server options from the Remote Control web page:

- 1 Launch the Remote Control Console using the username configured during installation.
- 2 Click **Server Setup** in the System Menu.
- 3 Configure the settings as needed.
- 4 Click **Save**.

Configuring Skin Settings for the Server

The Remote Control web page allows you to enable automatic skin synchronization, view available skins, or download skins from the Wavelink server.

To enable automatic skin synchronization:

- 1 From the Remote Control Console, click **Skins** in the System Menu.
- 2 Click the **Auto Sync** tab.
- 3 Select **Yes** from the drop-down menu and click **Update**.

To view the skins available on your computer:

- 1 From the Remote Control Console, click **Skins** in the System Menu.
- 2 Click the **Available** tab.
- 3 Select the brand name to view all skins for that brand, or click **Expand** in the top right corner to view all skins for all brands.

To download skins:

- 1 From the Remote Control Console, click **Skins** in the System Menu.
- 2 Click the **Download** tab.
- 3 Select the brand name to view all skins for that brand, or click **Expand** in the top right corner to view all skins for all brands. When you find the skin you want, click **Download**.

Managing Cell Carriers

If you are using an e-mail gateway for SMS messages, select a default cellular provider for the messages to be sent through. If your carrier is not in the list, you can add it.



NOTE: If you have some devices that use a different carrier, you can configure the carrier on a per-device basis from the Remote Control Client.

To select your cellular provider for SMS messages:

- 1 From the Remote Control Console, click **Carriers** in the System Menu.
- 2 Use the **Default** drop-down menu to select your provider.
- 3 If your carrier is not in the list, click **Add New**.
- 4 Type the **Name**, **Email Address**, and the **Max Length** of the text message in the text boxes and click **Update**. The carrier will be added to the list.

NOTE: For examples of the e-mail address format, you can view the details of carriers that have already been configured.

Backing Up and Restoring the Remote Control Database

Remote Control maintains its own database of device information separate from the Avalanche databases. The Remote Control web page allows you to back up and restore the Remote Control database. Database backups can be exported to another system for storage or for redundancy.

To back up the Remote Control database:

- 1 From the Remote Control Console, click **Backup** in the System Menu.
- 2 Click **Backup**.
- 3 A backup is created locally.

To restore a Remote Control database backup:

- 1 From the Remote Control Console, click **Backup** in the System Menu.
- 2 In the Restore area, select the backup that you want to restore. Click **Restore**.

To export or import a backup file:

- 1 From the Remote Control Console, click **Backup** in the System Menu.
- 2 If you want to export a backup file to store it somewhere else, select the backup file from the list and click **Download**. When you are prompted to save or open the file, save it to the desired location.

-Or-

If you want to import a backup file that was stored somewhere else, click **Browse**. Use the dialog box to navigate to and select the file. Click **Upload**. The file will be added to the list of available backups.



Viewing System Information

The System Info section on the Remote Control web page allows you to view the server run time, a list of connected devices, the license server information, and local resources.

To view the system information:

- 1 From the Remote Control web page, click **System Info** in the System Menu.
- 2 Select the tabs across the top to view different information.

Configuring Connection Profiles

Connection profiles allow you to define the skin displayed when a user connects to a device using Remote Control. They are configured from the Remote Control Console.

The following options are available when configuring a connection profile:

Name The name of the connection profile.

Use as default When this option is enabled, the current profile is used as the default when you establish a connection.

If you want to establish a connection using a profile other than the default profile, you can set the profile from the viewer while you are connected.

Show skin Displays a skin when you are connected to a device. When this option is enabled, the server is set to **Autodetect** and Remote Control will use device information to display the correct skin.

NOTE: If Remote Control settings are configured in a mobile device profile, the mobile device profile will override these connection profile settings.

To configure the connection settings:

- 1 From the Remote Control Console, click **Profiles** in the User Menu.
- 2 Select the connection profile from the Profiles list, or click **Add New** to create a new profile.
- 3 Configure the options as desired in the Details box.
- 4 Click **Save**.



Configuring the Remote Control Client

The Remote Control Client is configured from the Avalanche Console. After the package is added to a software profile, use the configuration tools in the package to modify the Remote Control Client or connect to the Remote Control Console. For information on launching the Remote Control Console from the package, see [Using the Remote Control Console](#) on page 79.

The package can also be configured so that the Client can be configured from the device after it is installed. If the device user configures the Client, the user at the Avalanche Console still has the option to clear the settings.

Certain Remote Control settings can also be configured from an Avalanche mobile device profile. When you configure Remote Control settings using a mobile device profile, the profile settings will override other Remote Control settings.

This section provides information on the following topics:

- [Editing the Remote Control Package](#)
- [Configuring Client Settings from the Mobile Device](#)
- [Clearing Client Settings](#)
- [Using a Mobile Device Profile for Remote Control Settings](#)

Editing the Remote Control Package

Once the Remote Control server is installed and the package added to a software profile, you can configure the Remote Control Client with the server address, connection method, the logging level, and other client options.

The following options are available when configuring the Remote Control package:

Connection Type	Select to use either TCP/IP or ActiveSync to connect to mobile devices.
Server ID	The ID for the server. This only needs to be modified if there are multiple Remote Control Servers.
Server Address	The DNS name or IP address of the Remote Control Server.
Server Port	The port the Remote Control Server listens on.



Connection Policy	<p>Select how Remote Control notifies the mobile device user that Remote Control is establishing a connection.</p> <ul style="list-style-type: none">• Silent indicates that the user will not be notified.• Notify indicates that the user will see a text window on his device letting him know that a connection has been established.• Prompt-Allow will provide the user with a prompt to allow or deny the connection. If the user does not respond, the connection will be allowed.• Prompt-Deny will provide the user with a prompt to allow or deny the connection. If the user does not respond, the connection will be denied.
Policy Time	<p>Select how long the notification or prompt will be displayed. If you selected Prompt-Allow or Prompt-Deny, this is the number of seconds Remote Control will wait before establishing or denying the connection.</p>
Password	<p>A password to require Remote Control users to provide a password before connecting to a mobile device.</p>
Log Level	<p>This is for the client log stored on the device. Logging levels include:</p> <ul style="list-style-type: none">• Critical. Indicates errors that cause Remote Control to fail to start.• Error. Indicates errors that are caused by configuration and/or communication problems.• Informational. Documents the flow of operation.• Warning. Indicates possible operational problems.• Debug. Used to diagnose program malfunctions or communication problems.
Maximum Size	<p>Configure the maximum size that the log file can reach before creating a new log file. New log files do not override previous log files.</p>
Use Encryption	<p>Configures the client to use AES encryption.</p>



Passphrase	The passphrase to use for encryption. This can include ASCII characters and be up to 64 characters long.
	<hr/> <p>NOTE: The Client and Server BOTH must be configured with the same passphrase for encryption to work. For information on configuring the Server for encryption, see Configuring Server Options on page 81</p> <hr/>
Client Sleep While Connected	Allows the mobile device to enter sleep mode while connected to Remote Control. If you do not enable this option, Remote Control will not allow the mobile device to enter sleep mode while connected.
Allow Client Configuration	Grants client configuration control to the mobile device user. This allows the user to configure the Remote Control client from the mobile device. When the mobile device user has configuration control, any changes you make in the Client Settings tab from the Remote Control Console will not deploy to the device. To regain Client Configuration setting control from the Remote Control Console, you must disable this option and redeploy the settings to the mobile device.
Disable Client Exit	When this option is enabled, the mobile device user cannot exit the Remote Control application.
Client Pre-connect to Server	Configures the device to always pre-connect to the Remote Control Server.
Client Connect on ActiveSync	When this option is enabled, the device will attempt to connect to the server when it is cradled.
Corporate Connection	This determines if VPN or port forwarding will be used by the mobile device connecting to your server. <ul style="list-style-type: none"> • If this option is enabled, the mobile device uses a VPN connection to connect to the server. • If this option is disabled, the mobile device uses an Internet connection to connect to the server.

To edit the Remote Control package from the Java Console:

- 1 From the **Profiles** tab, select the software profile that has the Remote Control package.
- 2 In the Software Packages list, select the Remote Control package and click **Configure**.

The *Configure Software Package* dialog box appears.

- 3 Select **Client Configuration** from the list and click **Launch**.



The *Remote Control Client Configuration* dialog box appears.

- 4 Configure the options as desired.
- 5 Click **OK** to save your changes and return to the Java Console.

To edit the Remote Control package from the Web Console:

- 1 From the **Profiles** tab, click on the name of the software profile that has the Remote Control package.

The Software Profile Details page appears.

- 2 From the Software Package panel, click **Configure** for the Remote Control package.

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

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

The *Remote Control Client Configuration* dialog box appears.

- 6 Configure the options as desired.
- 7 Click **OK** to return to the *Configure Software Package* dialog box.
- 8 Click **Next** to save your changes.
- 9 Click **Finish** to return to the Web Console.

Configuring Client Settings from the Mobile Device

Before you can configure client settings from the mobile device, you must enable the **Allow Client Configuration** option from the Remote Control Console (in the **Client** tab of the Client Setup page). This allows the mobile device user to configure the connection type, policy notification, password, and whether the device is allowed to sleep while connected. If you disable the **Allow Client Configuration** option, the mobile device user will not be allowed to access the client information on the mobile device.

For more information about enabling the **Allow Client Configuration** option and the configurations available, see [Editing the Remote Control Package](#) on page 86.



NOTE: Once you have configured the options from the device, the client will no longer accept configuration changes from Avalanche. In order to push settings to the device from Avalanche again, you should disable the **Allow Client Configuration** option or use the [Clearing Client Settings](#) on page 91 option.

The following settings are configurable from the device:

Connection Type Select to use either TCP/IP or ActiveSync to connect to mobile devices.

Type

Policy Select how Remote Control notifies the mobile device user that Remote Control is establishing a connection.

Silent indicates that the user will not be notified.

Notify indicates that the user will see a text window on his device letting him know that a connection has been established.

Prompt-Allow will provide the user with a prompt to allow or deny the connection. If the user does not respond, the connection will be allowed.

Prompt-Deny will provide the user with a prompt to allow or deny the connection. If the user does not respond, the connection will be denied.

Policy Seconds Select how long the notification or prompt will be displayed. If you selected **Prompt-Allow** or **Prompt-Deny**, this is the number of seconds Remote Control will wait before establishing or denying the connection.

Password A password to require Remote Control users to provide a password before connecting to a mobile device.

Allow Sleep while connected Allows the mobile device to enter sleep mode while connected to Remote Control. If you do not enable this option, Remote Control will not allow the mobile device to enter sleep mode while connected.

To configure client settings from the mobile device:

- 1 Launch the Remote Control application on the mobile device.
- 2 Tap **File > Configure**.

The *Configure* dialog box appears.



NOTE: If the **Allow Client Configuration** option is not enabled from the Remote Control Console, the *Not Available* dialog box appears. The device user will not be able to access client settings.

- 3 Configure the settings as desired.
- 4 Click **OK**.

The Remote Control client is updated with the new settings.

Clearing Client Settings

You can clear all client configuration settings using the **Clear Client Settings** option in the Standard Viewer. When you select this option, all your client configurations are removed, including anything that was configured on the mobile device. This option is useful if you have enabled the **Allow Client Configuration** option.

To clear client settings:

- From the Standard Viewer, click **Tools > Clear Client Settings**.

Using a Mobile Device Profile for Remote Control Settings

Configure Remote Control settings for a device by using a mobile device profile. The mobile device profile allows you to configure the following options for the Remote Control client:

Connection Policy Select how Remote Control notifies the mobile device user that Remote Control is establishing a connection.

Silent indicates that the user will not be notified.

Notify indicates that the user will see a text window on his device letting him know that a connection has been established.

Prompt-Allow will provide the user with a prompt to allow or deny the connection. If the user does not respond, the connection will be allowed.

Prompt-Deny will provide the user with a prompt to allow or deny the connection. If the user does not respond, the connection will be denied.

Policy Time The length of time that the notification or prompt will be displayed. If you selected **Prompt-Allow** or **Prompt-Deny**, this is the number of seconds Remote Control will wait before establishing or denying the session.



Log Level	<p>This is for the client log stored on the device. Logging levels include:</p> <p>Critical. Indicates errors that cause Remote Control to fail to start.</p> <p>Error. Indicates errors that are caused by configuration and/or communication problems.</p> <p>Informational. Documents the flow of operation.</p> <p>Warning. Indicates possible operational problems.</p> <p>Debug. Used to diagnose program malfunctions or communication problems.</p>
Maximum Size	Configure the maximum size that the log file can reach before creating a new log file. New log files do not override previous log files.
Client Sleep While Connected	Allows the mobile device to enter sleep mode while connected to Remote Control. If you do not enable this option, Remote Control will not allow the mobile device to enter sleep mode while connected.
Allow Client Configuration	Grants client configuration control to the mobile device user. This allows the user to configure the Remote Control client from the mobile device. When the mobile device user has configuration control, any changes you make in the Client Settings tab from the Remote Control Console will not deploy to the device. To regain Client Configuration control from the Remote Control Console, disable this option and redeploy the settings to the mobile device.
Disable Client Exit	When this option is enabled, the mobile device user cannot exit the Remote Control application.
Client Pre-connect to Server	Configures the device to always pre-connect to the Remote Control Server.
Client Connect on ActiveSync	When this option is enabled, the device will attempt to connect to the server when it is cradled.
Corporate Connection	<p>This determines if VPN or port forwarding will be used by the mobile device connecting to your server.</p> <ul style="list-style-type: none"> • If this option is enabled, the mobile device uses a VPN connection to connect to the server. • If this option is disabled, the mobile device uses an Internet connection to connect to the server.

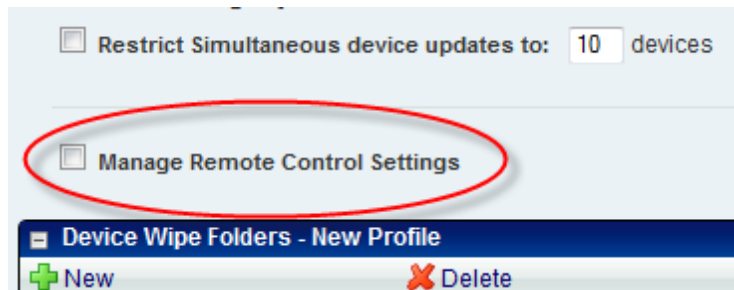


Show Skin Displays a skin when you are connected to a device. When this option is enabled, select the skin you want to use from the drop-down menu. If you choose **Autodetect**, Remote Control will use device information to display the correct skin.

NOTE: When you configure Remote Control settings using a mobile device profile, the profile settings will override other Remote Control settings.

To configure Remote Control settings using a mobile device profile:

- 1 Log in to the Avalanche Web Console.
- 2 From the **Profiles** tab, click the name of the mobile device profile you want to configure.
The Mobile Device Profile Details page appears.
- 3 Enable the **Manage Remote Control Settings** option.



Mobile Device Profile Details

- 4 In the Remote Control Settings panel, configure the options as desired.
- 5 Save your changes.



Connecting to Mobile Devices

After you configure the client and server settings, deploy the Remote Control client to the mobile device. Once the mobile device has the client installed, and you have added Remote Control licenses through Avalanche, you can create Remote Control connection sessions. A connection session is when the mobile device is connected to Remote Control, allowing you to view and control the mobile device.

The Remote Control Client has an option to preconnect. When preconnect is enabled, the mobile device will automatically connect to the Remote Control Server without receiving a connection request. Then, when a user begins a connection session, the session begins quickly and easily because the device is already connected to the server. You can enable or disable preconnect from the Remote Control Console.

When you have initiated a connection session, the device appears in a Remote Control Viewer. If you launch the viewer from the Avalanche Web Console, the connection session will appear in the Web Viewer. If you launch from the Avalanche Java Console or the Remote Control Console, the connection session will appear in the Standard Viewer.

NOTE: Device skins are not supported in the Web Viewer. They may appear, but they won't have any functionality.

This section provides information about the following Remote Control connection tasks:

- [Connecting to a Mobile Device](#)
- [Closing Remote Control Sessions](#)
- [Standard Viewer Tasks](#)
- [Web Viewer Tasks](#)

Connecting to a Mobile Device

A connection session can be initiated from the Avalanche Java Console or the Avalanche Web Console.

When you initiate a connection session, the computer you are connecting from sends a request to the Remote Control Server. If the device is preconnected (has already established a connection to the server), the server connects the viewer to the device. If the device is not preconnected, the server requests the device to connect back to the server, and when the device responds the server connects the viewer to the device. Alternately, the Standard Viewer may try to connect to the device directly without routing traffic through the server. This option is only available when the device and viewer are on the same LAN.



NOTE: If the device is not configured to preconnect, the device user can manually preconnect by opening the Remote Control Client and tapping **File > Connect to Server**.

To connect to a device from the Avalanche Java Console:

- From the **Mobile Device Inventory** tab, right-click the name of the device and select **Remote Control** from the context menu.

-Or-

- From the *Mobile Device Details* dialog box, click the **Device Control** tab and then double-click **Remote Control**.

The *WLRemoteControl* dialog box appears while the viewer attempts to contact the device. When the Remote Control session has been initiated, the Standard Viewer appears. Clicking within the Standard Viewer sends the mouse click to the connected device. Typing on the physical keyboard sends the key commands to the mobile device.

To connect to a device from the Avalanche Web Console:

- 1 From the **Inventory** tab, click on the name of the device you want to connect to.

The Mobile Device Details page appears.

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

The Remote Control Web Viewer appears while the viewer attempts to contact the device. While the device is not connected, only the **Status** and **Edit Device** options will be available in the Available Commands panel. When the Remote Control session has been initiated, other commands will appear. Click **View** to open the device view and interact with the device.

Closing Remote Control Sessions

When you close the window that the Standard Viewer appears in, the session is disconnected. The following are alternate methods to disconnect a connection session.

To close a connection session:

- From the Standard Viewer, select **File > Exit**.

-Or-

- From the Web Viewer, click **Disconnect** in the Available Commands panel.



Standard Viewer Tasks

This section provides information about using Remote Control once you are connected to a mobile device. The tasks detailed in this section assume you are connected to a mobile device.

NOTE: There are two different Viewer interfaces, depending on how you initiated the Remote Control connection. If you launched from the Avalanche Java Console, Remote Control will use the Standard Viewer. If you launched from the Avalanche Web Console, Remote Control will use the Web Viewer. You cannot connect to a device with both the Standard Viewer and the Web Viewer at the same time.

This section contains tasks for working from the Standard Viewer. For information on working from the Web Viewer, see [Web Viewer Tasks](#) on page 115.

Once you connect to a mobile device, the Standard Viewer offers a variety of tools and configuration options. The Standard Viewer has the following tabs:

- **Device.** From this tab you can view the mobile device and perform operations on the mobile device. Clicking within the Standard Viewer sends the mouse click to the connected device. Typing on the keyboard sends the key commands to the mobile device.
- **File System.** From this tab you can access the file system on the mobile device. For detailed information about tasks you can perform in the File System tab, see [Accessing the File System](#).
- **Registry Viewer.** The Registry Viewer allows you to view and edit the registry on the mobile device. For detailed information about the Registry Viewer, see [Using the Registry Viewer](#).
- **Processes.** The Process Manager provides a view of the processes that are currently running on the mobile device. For detailed information, see [Using the Process Manager](#).
- **Access Log.** The Remote Control logging feature stores information about the current connection session of Remote Control. For detailed information, see [Accessing the Log File](#).
- **Device Info.** The **Device Info** tab provides information about the mobile device to which you are connected. For details about this tab, see [Viewing Device Information](#).

The Standard Viewer has the following toolbar buttons:



Record. Begins to record a video.



Stop Record. Stops a video recording.





Camera. Takes a picture of the current mobile device screen.



Toggle Skin. Toggles whether a skin for the device is displayed or not.



Refresh. Refreshes the mobile device screen.



Zoom in. Zooms in on the mobile device display.



Zoom out. Zooms out on the mobile device display.



Autoscale. Automatically scales the mobile device display to fit the size of the window you have open.



Set Video Mode. Allows you to set the video mode to **Standard** or **Image**.

This section also provides information about the following Standard Viewer tasks:

- [Configuring Display and Capture Options](#)
- [Using Device Tools](#)

Accessing the File System

You can access the File Explorer of the mobile device using the Standard Viewer. This enables you to perform tasks and operations in the File Explorer on the mobile device from your Remote Control connection session. Access the File Explorer by opening the Standard Viewer clicking the **File System** tab. You can also access the File System from the *Avalanche Mobile Device Details* dialog box. Click the **Device Control** tab and then double-click the **File System** icon.

This section provides information about the following tasks from the Standard Viewer:

- [Creating New Folders](#)
- [Copying Files to the PC](#)
- [Copying Files to the Mobile Device](#)
- [Manipulating Files on the Device](#)
- [Pasting Text](#)

Creating New Folders

You can create and name directories on the device using the File Explorer.



To create a new folder on the device from the Standard Viewer:

- 1 Click on the **File System** tab.
- 2 Navigate to the location where you want to create the new folder.
- 3 Right-click and select **New**.
The folder is created in the selected location.
- 4 Right-click the new folder and select **Rename Folder**.
- 5 Type the name of the folder.

Copying Files to the PC

You can copy files from the mobile device to the PC.

To copy files to the PC using the Standard Viewer:

- 1 Click on the **File System** tab.
- 2 Select the file or folder you want to copy to the PC. From the **Files** menu, select **Copy to PC**.

-Or-

Right-click the file you want to copy and select **Copy to PC**.

The *Browse for Folder* dialog box opens.

- 3 Navigate to the location where you want to save the file.
- 4 Click **OK**.

The folder is copied to the selected location.

Copying Files to the Mobile Device

You can copy files from the machine running Remote Control and place them in the File Explorer of a connected mobile device.

To copy files to the mobile device using the Standard Viewer:

- 1 Click on the **File System** tab.
- 2 Navigate to where you want to place the file.
- 3 From the **Files** menu, select **Copy to Remote**.

The *Open* dialog box appears.

- 4 Locate the file that you want to copy to the mobile device and click **Open**.

The *Sending Files Status* dialog box appears. The files are copied to the selected location.



- 5 Once the file transfer is complete, click **OK**.

NOTE: You can also drag files directly from the PC and drop them into the File Explorer.

Manipulating Files on the Device

From the File Explorer, you can run, open, view or delete files located on the mobile device. You can run any file with an `.exe` extension.

To run/open/view/delete a file on the mobile device from the Standard Viewer:

- 1 Click on the **File System** tab.
- 2 Using the tree view, navigate to the location of the file.
- 3 Right-click the file and select the desired option.
 - If you are running a program, the program opens on the mobile device.
 - If you are opening a file, the file appears on the mobile device.
 - If you are viewing a file, the file appears on the PC.
 - If you are deleting a file, the file is removed from the list.
- 4 Click the **Device** tab to view the mobile device screen.

Pasting Text

Remote Control allows you to copy and paste text from the PC to the mobile device. Only textual information can be copied and pasted. For example, you could copy text from a text editor on the PC to Pocket Word on the mobile device. Both text editors must be open.

Use the **Paste to device** command to paste information from the PC to the mobile device.

To copy and paste information using the Standard Viewer:

- 1 Open a text editor on both PC and the mobile device.
- 2 From the text editor on your PC, select the text to be copied and pasted.
- 3 Right-click and select **Copy**.
- 4 In the Standard Viewer, select **Edit > Paste to device**.

The text appears in the text editor on the mobile device.

Using the Registry Viewer

From the **Registry Viewer** tab in the Standard Viewer, you can browse and view the registry of a connected mobile device. Access the device's registry from the Standard Viewer by clicking the **Registry Viewer** tab. You can also access the Registry Viewer through the *Mobile*



Device Details dialog box. Click the **Device Control** tab and then double-click the Registry Viewer icon.

This section provides information about the following Registry Viewer tasks:

- [Creating New Registry Keys](#)
- [Creating Key Values](#)
- [Viewing Binary Data](#)
- [Modifying Key Values](#)
- [Editing Binary Data](#)
- [Deleting Key Values](#)
- [Exporting Registries](#)
- [Comparing Registries](#)

Creating New Registry Keys

From the **Registry Viewer** tab, you can create new registry keys on the mobile device.

[To create a new registry key using the Standard Viewer:](#)

- 1 Open the Registry Viewer.
- 2 Navigate to where you want to create a new key.
- 3 Right-click and select **New Key**.
A **New Key** folder appears.
- 4 Right-click the **New Key** folder and select **Rename**.
- 5 Name the folder.

Creating Key Values

You can create String, Binary, DWORD, and Multi-String values in the mobile device registry.

[To create key values using the Standard Viewer:](#)

- 1 Open the Registry Viewer.
- 2 Navigate to where you want to create a new key.
- 3 Right-click and from the menu that appears, select the key value you want create.
The value appears in the file list box.



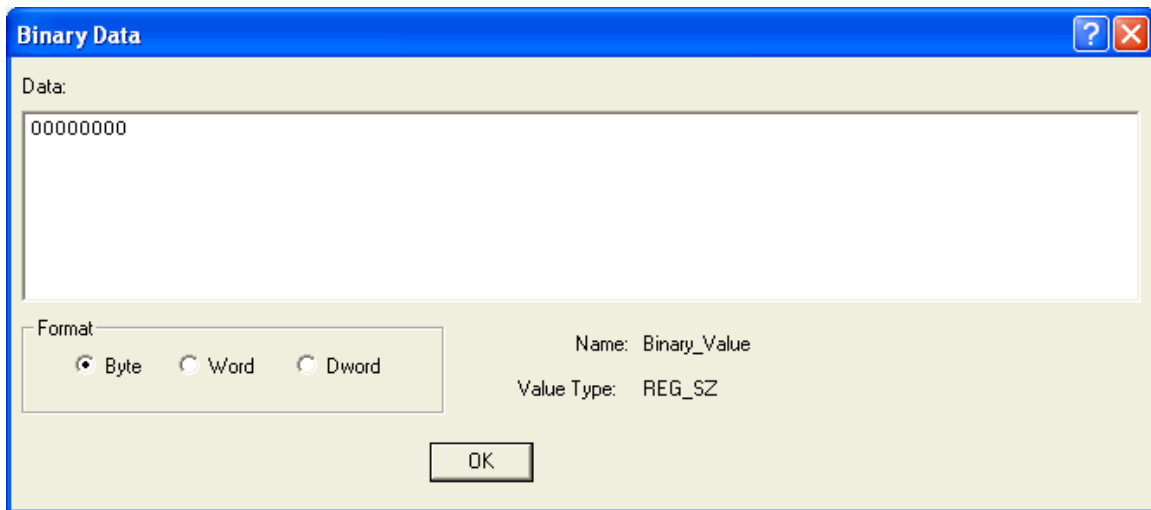
Viewing Binary Data

For any registry key, you can display the binary data for that key.

To view binary data using the Standard Viewer:

- 1 Open the Registry Viewer.
- 2 Navigate to the location of the key you want to view.
- 3 Right-click the key and select **Display Binary Data**.

The *Binary Data* dialog box appears.



Binary Data

- 4 Use the options in the Format area to display the data in **Byte**, **Word** or **Dword** format.
- 5 Click **OK** when you are finished.

Modifying Key Values

You can modify key values in the **Registry Viewer** tab of the Standard Viewer.

To modify key values using the Standard Viewer:

- 1 Click the **Registry Viewer** tab.
- 2 Navigate to the location of the key you want to edit.
- 3 Right-click the key and select **Modify**.

A dialog box appears according to what type of key you are modifying.

- If you are modifying a String or Binary value, the *Edit String* dialog box appears.
- If you are modifying a DWORD key value, the *Edit DWORD Value* dialog box appears.



- If you are modifying a Multi-String value, the *Edit Multi-String* dialog box appears.
- 4 Using the configuration options available in each dialog box, edit the key value.
 - 5 Click **OK** when you are finished.

The key value is modified.

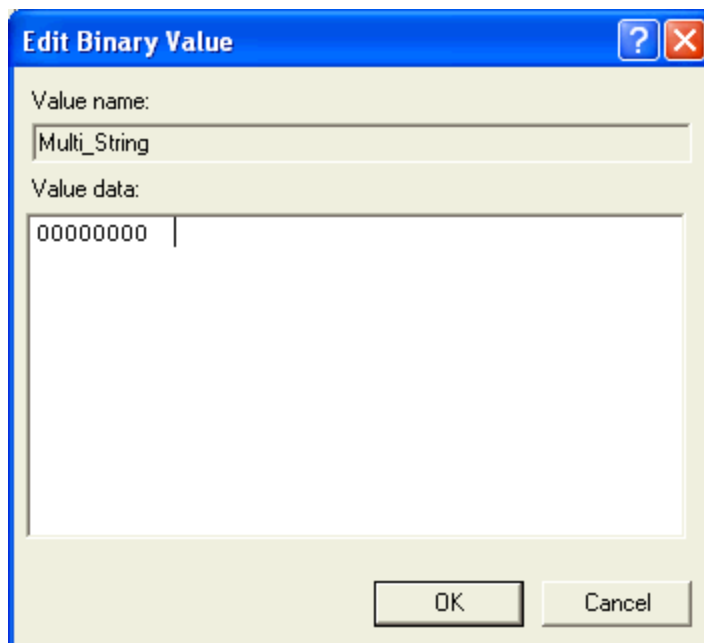
Editing Binary Data

You have the ability to modify the binary data of each type of key value in the **Registry Viewer** tab of the Standard Viewer.

To modify binary data using the Standard Viewer:

- 1 Click the **Registry Viewer** tab.
- 2 Navigate to the location of the key you want to modify.
- 3 Right-click the key and select **Modify Binary Data**.

The *Edit Binary Value* dialog box appears.



Edit Binary Value

- 4 In the **Value data** text box, edit the binary value as desired.
- 5 Click **OK** when you are finished.

Deleting Key Values

You can delete registry key values that you no longer need.



To delete key values using the Standard Viewer:

- 1 Click the **Registry Viewer** tab.
- 2 Navigate to the location of the key you want to delete.
- 3 Right-click the key and select **Delete**.

A dialog box appears asking you to confirm that you want to delete this key value.

- 4 Click **Yes** if you want to permanently delete the value.

The key value is removed from the registry.

Exporting Registries

You can export registries from the mobile device and save them as `.xml` files on your computer.

To export a registry using the Standard Viewer:

- 1 Click the **Registry Viewer** tab.
- 2 Navigate to the location of the registry you want to export.
- 3 From the **File** menu, select **Export**.

A *Save As* dialog box appears.

- 4 Navigate to the location where you want to save the registry.
- 5 Name the registry and click **Save**.

The registry is saved as an `.xml` file.

Comparing Registries

There are two methods you can use to compare registries:

- You can compare the registry on a mobile device to a registry you have saved and exported.
- You can compare the registry of one device to another device after establishing a second connection session.

To compare registries from the Standard Viewer:

- 1 Click the **Registry Viewer** tab.
- 2 From the **File** menu, select **Compare**.

A dialog box appears.





- 3 If you are comparing it to a saved registry, select the **Existing Registry** option and click **OK**. In the dialog box that appears, navigate to the location of the registry to which you want to compare and click **Open**.

-Or-

If you are comparing it to the registry of another device, select **Another Device** and click **OK**. In the dialog box that appears, specify the connection type and IP address for the second device and click **OK**.

A *Registry Compare* dialog box appears displaying the existing registry file.

- 4 When you are finished comparing registries, close the *Registry Compare* dialog box.

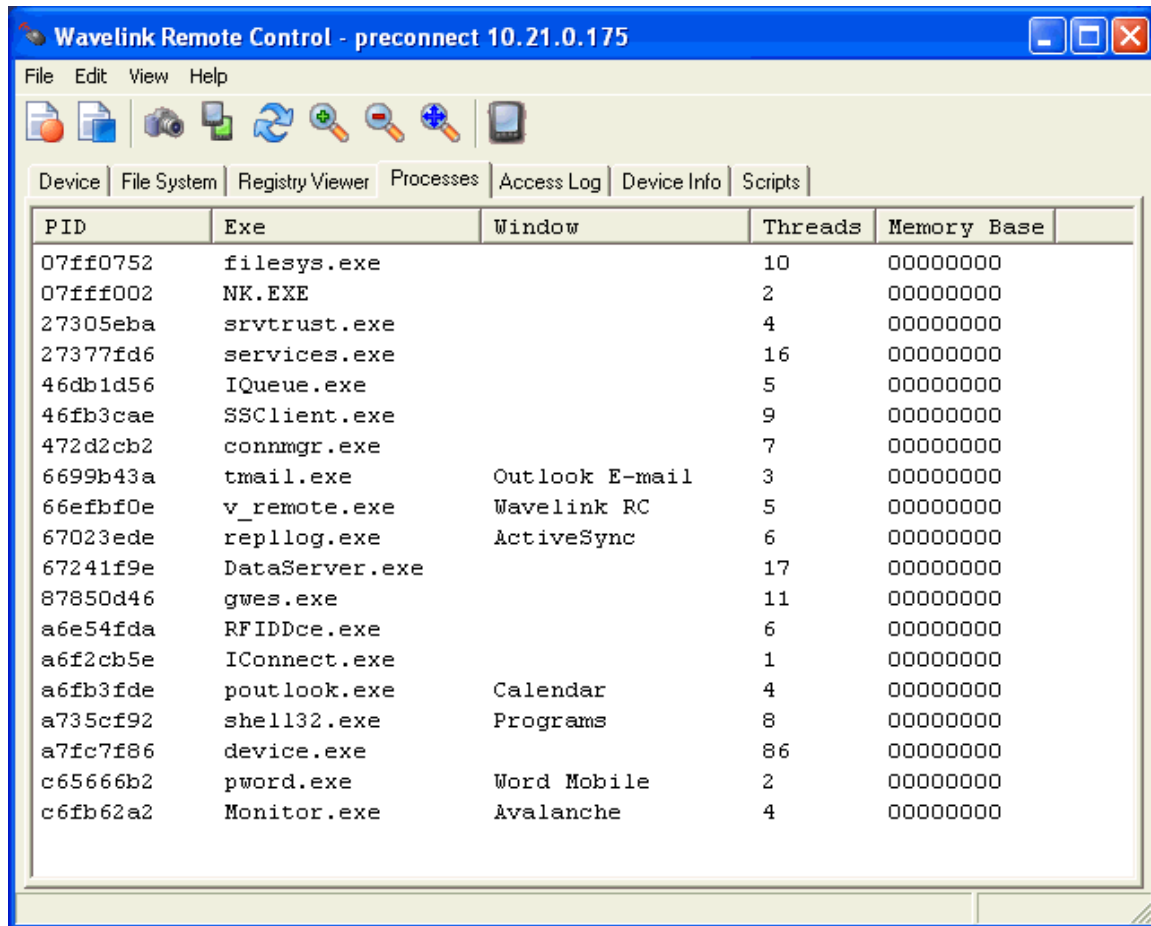
Using the Process Manager

The **Processes** tab in the Standard Viewer allows you to view the processes that are currently running on the mobile device. You have the option to activate or kill (end) any of the processes. Activating a process brings that process to the foreground of the device screen. Killing a process stops the process.

To use the Process Manager:

- 1 Click the **Processes** tab.





Process Manager

2 Select a process and right-click to **Activate** or **Kill** that process.

Accessing the Log File

The Remote Control logging feature stores information about the connection sessions for Remote Control.

This section provides information about the following logging options:

- [Viewing and Clearing Log Files](#)
- [Configuring Logging](#)

Viewing and Clearing Log Files

You can view the log file for a current Remote Control session from the **Access Log** tab. If you need to delete the information that displays in the log file, you can clear the entire file. When you select to clear the log file, the entire log in the **Access Log** tab is removed. You cannot select individual items to clear.



To clear the log file:

- 1 Click the **Access Log** tab.
- 2 From the **Edit** menu, select **Clear Log**.

-Or-

Right-click within the log and select **Clear Log**.

The **Access Log** tab clears.

Configuring Logging

Remote Control supports the following log levels:

- **Critical.** This level writes the least information to the log file, reporting only critical errors that cause a process to abort.
- **Error.** This level writes Error messages and Critical messages to the log file.
- **Warning.** This level writes Critical messages, Error messages, and Warning messages to the log file.
- **Informational.** This level writes enough information to the log file to diagnose most problems.
- **Debug.** This logging level writes large amounts of information to the log file that can be used to diagnose more serious problems.

You can change the logging for a particular connection session through the *Configure* dialog box located in the Standard Viewer.

To change the logging configuration:

- 1 Click the **Access Log** tab.
- 2 From the **File** menu, select **Configure**.

The *Configure* dialog box appears.

- 3 In the Logging area, select the log level from the **Level** drop-down menu.
- 4 Enter the maximum size you want the log level to reach in the **Max Size** text box.
- 5 Click **OK**.

The *Configuration Data Change* dialog box appears. This dialog box indicates that you changed something from the original profile configuration.



- If you want to use your updated changes, but do not want to update the configuration file, select the **Use New Configuration** option.
- If you want to use your updated changes and update the configuration file to reflect those changes, select the **Use New Configuration and Update config file** option.

6 Click **OK**.

The new logging information is applied.

NOTE: You can also set up the logging configuration when you configure the Client. For more information, see [Editing the Remote Control Package](#) on page 86.

Viewing Device Information

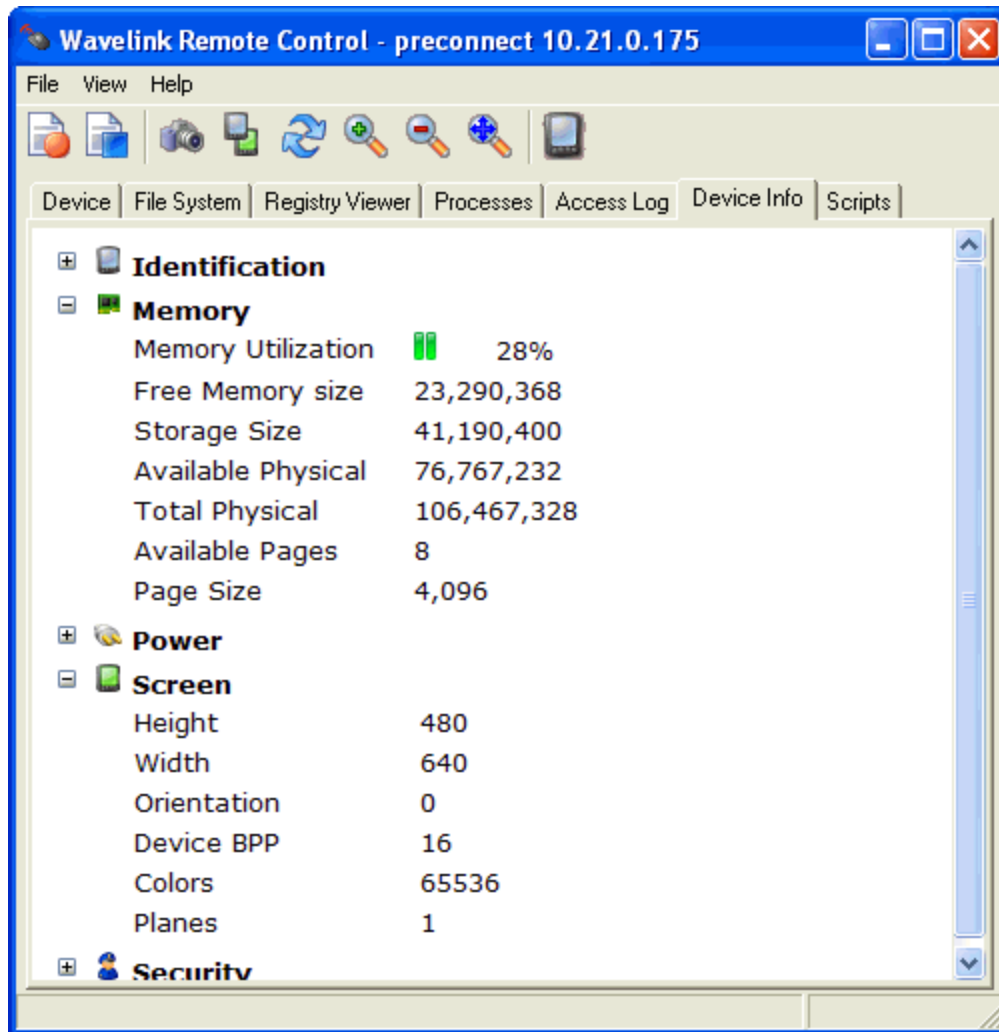
The **Device Info** tab in the Standard Viewer provides information about the mobile device to which you are connected. This information includes:

- Identification, including OEM information and the operating system versions.
- Memory, including the amount of free memory left on the device and storage space.
- Power, including information about the battery level and charging status of the mobile device.
- Screen, including information about the screen size and orientation.
- Security, including password information.

To view device information:

- From the Standard Viewer, click the **Device Info** tab.





Device Info

Configuring Display and Capture Options

When you create a Remote Control connection session, you can configure the following display and capture options:

- [Setting Video Mode](#)
- [Configuring Display Refresh Rates](#)
- [Sizing the Mobile Device Display](#)
- [Toggling Statistics](#)
- [Using Device Skins](#)
- [Recording Videos](#)
- [Performing Screen Captures](#)



Setting Video Mode

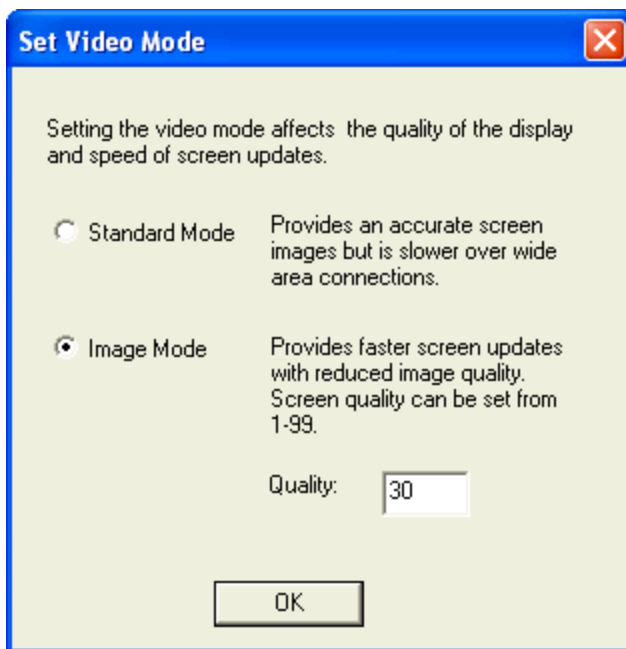
You can set two types of video mode depending on how you want the mobile device screen to appear and how fast you want the program to run.

- **Standard Mode.** This mode provides the clearest, most accurate screen images. However the refresh rate is slower over wide area connections.
- **Image Mode.** This mode provides faster screen updates with reduced image quality. You can set the screen display quality from one - 99 based on preference.

To set video mode:

- 1 From the Standard Viewer, click the Video Mode icon.

The *Set Video Mode* dialog box appears.



Set Video Mode

- 2 Select the video mode you want to use and click **OK**.

Configuring Display Refresh Rates

You can configure the rate at which Remote Control refreshes the mobile device screen display. The refresh rate can range from 1 to 17 frames per second. Your selection is dependent on the speed of the mobile device and the communication method you are using. Select the best setting for your usage that does not impact the mobile device CPU too heavily and allows for reasonable screen updates.



NOTE: You can also configure the refresh rate option when you configure the Client. For more information, see [Editing the Remote Control Package](#) on page 86.

To configure the refresh rate:

- 1 From the Standard Viewer, click **File > Configure**.

The *Configure* dialog box appears.

- 2 From the **Refresh Rate** drop-down list, select the rate at which you want the screen display to refresh.
- 3 Click **OK**.

The *Configuration Data Change* dialog box appears. This dialog box indicates that you changed something from the original profile configuration.

- If you want to use your updated changes, but do not want to update the configuration file, select the **Use New Configuration** option.
- If you want to use your updated changes and would like to update the configuration file to reflect those changes, select the **Use New Configuration and Update config file** option.

- 4 Click **OK**.

Sizing the Mobile Device Display

While you are viewing a device, you can configure the size of the mobile device display to scale from .5x - 4x. There is also an auto-scale option that will fit the display to the size of the window you have open.

NOTE: You can also configure scale setting when you configure the Client. For more information, see [Editing the Remote Control Package](#) on page 86.

To change the display scale:

- From the **View** Menu, select **Scale** and then the size you want the display to be.
- Or-
- Use the **Zoom In**, **Zoom Out**, or **Autoscale** toolbar options to adjust the size of the display.

To set the scale for the profile:

- 1 From the **File** menu, select **Configure**.

The *Configure* dialog box appears.

- 2 From the **Scale** drop-down list, select the size of the mobile device display.
- 3 Click **OK**.



The *Configuration Data Change* dialog box appears. This dialog box indicates that you changed something from the original profile configuration.

- If you want to use your updated changes, but do not want to update the device configuration file, select the **Use New Configuration** option.
- If you want to use your updated changes and update the configuration file to reflect those changes, select the **Use New Configuration and Update config file** option.

4 Click **OK**.

The device will appear as the size you selected.

Toggling Statistics

You can display connection statistics at the bottom of the Standard Viewer. The statistics include bytes sent, bytes received, the number of keys pressed during the session, and the number of mouse clicks during the session.

To toggle statistics:

- 1 Click the **Device** tab.
- 2 From the **View** menu, select **Toggle Statistics**.

Using Device Skins

From the Standard Viewer, you can toggle between a selected skin and the default view (no skin). To use skins, you must enable the **Show Skin** option when you are configuring the Client or from the *Configure* dialog box in the Standard Viewer.

If you did not enable the **Show Skin** option when you configured the Client, you can configure the connection to display skins from the Standard Viewer.

NOTE: For information on how to enable the **Show Skin** option, see [Editing the Remote Control Package](#) on page 86.

Once you enable the **Show Skin** option, Remote Control displays the skin for the connected mobile device. You can toggle the skin to display or not display from the **Device** tab in the Standard Viewer.

To enable the **Show Skin** option:

- 1 From the **File**, select **Configure**.
The *Configure* dialog box appears.
- 2 Enable the **Show Skin** option.
- 3 Select which skin to display from the **Skin** drop-down list.
- 4 Click **OK**.



The *Configuration Data Change* dialog box appears. This dialog box indicates that you changed something from the original profile configuration.

- If you want to use your updated changes, but do not want to update the configuration file, select the **Use New Configuration** option.
- If you want to use your updated changes and would like to update the configuration file to reflect those changes, select the **Use New Configuration and Update config file** option.

5 Click **OK**.

The skin image appears in the **Device** tab of the *Standard Viewer*.

To toggle skins:

- 1 Select the **Device** tab in the Standard Viewer.
- 2 From the **View** menu, select **Toggle Skin**.

-Or-

Click the **Toggle Skin** icon in the Standard Viewer toolbar.

Recording Videos

You can record a video of your Remote Control session for training or demonstration purposes. First, you must enable AVI as the recording method. You can select the AVI recording method from the *Configure* dialog box in the Standard Viewer. You can play the AVI file using any program compatible with the AVI video file format, such as Windows Media Player.

To display the cursor while recording:

- 1 From the **File** menu, select **Configure**.

The *Configure* dialog box appears.

- 2 If you want the cursor to display in the AVI video, enable the **Show Cursor** option.
- 3 Click **OK**.

The *Configuration Data Changed* dialog box appears. This dialog box indicates that you changed something from the original profile configuration.

- If you want to use your updated changes, but do not want to update the configuration file, select the **Use New Configuration** option.
- If you want to use your updated changes and update the configuration file to reflect those changes, select the **Use New Configuration and Update config file** option.

4 Click **OK**.



The new recording information is applied.

To record the AVI file:

- 1 In the Standard Viewer, click the Record toolbar icon.

The *Save As* dialog box appears.

- 2 Name the file and click **Save**.

The *Video Compression* dialog box opens.

- 3 Configure the compression options and click **OK**.

- 4 From the **Device** tab in the Standard Viewer, perform the actions on the mobile device that you want to record.

- 5 Click the Stop Record toolbar icon when you are finished.

The AVI file is saved in the directory specified.

Performing Screen Captures

When you are connected to a mobile device through a Remote Control session, you can capture screen images from the mobile device.

Before you can take screen captures using Remote Control, you must select the method by which you want to capture the screen image. You can capture screen shots using three different methods:

- **File.** Use this option to save the image to a specified file. Once you capture the screen image, you can specify where you want to save the file.
- **Clipboard.** Use this option to place the image on the clipboard.
- **One-click.** Use this option to click once and send the screen capture to a previously specified file format. The file format must be chosen in the *Configure* dialog box. The file name will be automatically created based on the current time and date.

You can configure screen capture methods from the Standard Viewer. You can also configure screen capture methods when you configure the Client. For more information, see [Editing the Remote Control Package](#) on page 86.

To configure the screen capture method:

- 1 In the Standard Viewer, select **File > Configure**.

The *Configure* dialog box opens.

- 2 In the Screen Capture area, select the method you want to use when performing screen captures.

- 3 Click **OK**.



The *Configuration Data Change* dialog box appears. This dialog box indicates that you changed something from the original profile configuration.

- If you want to use your updated changes, but do not want to update the configuration file, select the **Use New Configuration** option.
- If you want to use your updated changes and update the configuration file to reflect them, select the **Use New Configuration and Update config file** option.

4 Click **OK**.

The screen capture method you configured is now enabled.

To perform a screen capture:

- 1 In the **Device** tab, navigate to the screen view of the device you want to capture.
- 2 Click the Camera toolbar icon.

The image is saved according to the screen capture method you configured in the *Configure* dialog box.

Using Device Tools

When you are connected to a device, Remote Control has several tools to help you control the device. These tools include:

- **Soft Reset.** Forces a warm boot on the device. When you reset the device, the Remote Control connection is terminated.
- **Suspend.** Puts the mobile device in a suspended (sleep) state. When you suspend the device, the Remote Control connection is terminated.
- **Clearing Client Settings.** Clears changes to the Remote Control settings that the device user may have set.

To use the device tools:

- 1 Click the **Device** tab.
- 2 From the **Tools** menu, select the tool you want to use.

If you select **Soft Reset** or **Suspend**, the connection session is terminated.

If you select **Clearing Client Settings**, any Remote Control settings changed by the device user are reset.



Web Viewer Tasks

This section provides information about using the Remote Control Web Viewer once you are connected to a mobile device. The tasks detailed in this section assume you are connected to a mobile device. For information about creating a connection session, see [Connecting to Mobile Devices](#) on page 94.

NOTE: There are two different Viewer interfaces, depending on how you initiated the Remote Control connection. If you launched from the Avalanche Java Console, Remote Control will use the Standard Viewer. If you launched from the Avalanche Web Console, Remote Control will use the Web Viewer. You cannot connect to a device with both the Standard Viewer and the Web Viewer at the same time.

This section contains tasks for working from the Web Viewer. For information on working from the Standard Viewer, see [Standard Viewer Tasks](#) on page 96.

Once you connect to a mobile device, Remote Control offers a variety of functionality, tools and configuration options. The Web Viewer has the following tabs:

- **Device.** For information on tasks performed from the **Device** tab, see [The Device Tab](#).
- **Files.** The **Files** tab allows you to view and modify the files on the device. You can run, open, download, rename, or delete files. For information on tasks performed from the **Files** tab, see [Using the File Explorer](#).
- **Registry.** The **Registry** tab allows you to view and modify the device registry. For information on tasks performed from the **Registry** tab, see [Using the Registry Explorer](#).
- **Processes.** The **Processes** tab allows you to view, kill, and activate processes on the device. For information tasks performed from the **Processes** tab, see [Using the Process Manager](#).
- **Device Info.** The **Device Info** tab provides information on the device ID, memory, power, screen, and security. You cannot change any of the information from this tab. For details on the information available on this tab, see [Viewing Device Information](#).
- **Scripts.** The **Scripts** tab allows you to create scripts in JavaScript to run on your device using Remote Control. For more information on how to use the Script Editor, see the *Remote Control Scripting Reference Guide* on the Wavelink web site.

NOTE: Skins may be displayed in the Web Viewer, but they will not be functional.

The Device Tab

The **Device** tab in the Web Viewer allows you to interact with the device and view its access history and logs. You can also perform tasks such as a reboot or device sync. The tab has four



panels:

Device Description Panel

The Device Description panel on the Web Viewer **Device** tab provides information about the device you are connected to, a thumbnail of the current display on the device, and buttons for updating or refreshing the thumbnail. Device information may include:

Status	The connection status of the device.
OEM Info	OEM info as reported by the device.
Server Address	Address for the Avalanche Mobile Device Server.
Ava Term ID	Terminal ID assigned to the device by Avalanche.
Last Seen	Last time the device was connected to.
Description	Device description set in Remote Control Console.
IP Address	IP address of the mobile device.
Phone Number	Phone number for the device.
Carrier	Carrier for the device's phone service.

Available Commands Panel

The following commands are performed from the Available Commands panel on the **Device** tab:

View	Opens a real-time view of the device in a new tab or window.
Status	Displays information about the connection status. When you click Status , the <i>Device Status</i> dialog box appears. This dialog box allows you to refresh the status of the device, disconnect, reboot, or ping the device, or display the Remote Control Client interface on the device.
Edit Device	Allows you to edit the device description details, including the phone number, carrier, name and description.
Disconnect	Disconnects the device from the Remote Control session.
Reboot	Performs a warm boot of the device. The connection session is terminated.
Suspend	Sends the device into a suspended (sleep) state. The connection session is terminated.



Text Message	Sends an SMS text message to the mobile device.
Device Sync	Sends an SMS message to the device requesting it to connect to the Avalanche Mobile Device Server.

Device Log Panel

The Device Logs panel displays Remote Control logged activity for the device. This includes the time of the activity, the user who performed the action, whether the action was successful, and possible additional information.

Access History Panel

The Access History Panel displays Remote Control connection history for the device. This includes the time of the activity, the user who attempted to connect, the IP address the Avalanche user connected from, and the access type for the connection.

Using the File Explorer

You can access the File Explorer of the mobile device from your PC during your Remote Control connection session. This enables you to view, copy, rename, or delete files and perform tasks on the mobile device.

To use the File Explorer:

- 1 From the Avalanche Web Console, navigate to the Mobile Device Details page and click **File Explorer**.

-Or-

After you have established a Remote Control session with the device, click the **Files** tab in the Web Viewer.

- 2 Use the folder icons to navigate to the desired file.
 - When you select the file, the file information appears in a panel above the File Explorer, and you have the options to **Run**, **Open**, **Download** the file from the mobile device, **Rename**, or **Delete**.
 - To copy a file to the device, navigate to the location you want the file stored and click **Upload File**. When the Uploading Files area appears, click **Browse** to find the file you want to copy to the device. After selecting the file, click **Upload**.
 - Use the **Add Directory** and **Delete Directory** options to change the file structure.

Remote Control will make the changes on the device as you perform the desired tasks.



Using the Registry Explorer

From the **Registry** tab in the Web Viewer, you can view and edit the registry of a connected mobile device.

To view and edit the registry:

- 1 From the Avalanche Web Console, navigate to the Mobile Device Details page and click **Registry Explorer**.

-Or-

After you have established a Remote Control session with the device, click the **Registry** tab in the Web Viewer.

- 2 Use the tree view to navigate to the registry key you want to view or edit.
 - If you are adding or deleting a registry key, click **Add Key** or **Delete Key** at the top of the panel.
 - If you are editing a current value, select the name of the key and the Editing Registry Value panel appears. Make changes as desired and click **Save**.
 - If you are adding a value, click **Add New Value** and the Adding Registry Value panel appears. Make changes as desired and click **Save**.

Remote Control will make the changes on the device as you perform the desired tasks.

Using the Process Manager

The **Processes** tab in the Web Viewer allows you to view the processes that are currently running on the mobile device. You have the option to activate or kill (end) any of the processes. Activating a process brings that process to the front of any other programs running on the mobile device. Killing a process stops the process.

To use the Process Manager:

- From the Avalanche Web Console, navigate to the Mobile Device Details page and click **Process Manager**.

-Or-

- After you have established a Remote Control session with the device, click the **Processes** tab in the Web Viewer.
 - To kill a process, select it from the list and click **Kill**.
 - To activate a process, select it from the list and click **Activate**.

Remote Control will make the changes on the device as you perform the desired tasks.



Viewing Device Information

The **Device Info** tab in the Web Viewer provides information about the mobile device to which you are connected. This information includes:

- Identification, including OEM information and the operating system versions.
- Memory, including the amount of free memory left on the device and storage space.
- Power, including information about the battery level and charging status of the mobile device.
- Screen, including information about the screen size and orientation.
- Security, including password information.

To view device information:

- After you have established a connection, click the **Device Info** tab in the Web Viewer.



Chapter 11: Managing Mobile Device Profiles

You can use a mobile device profile to change settings on your mobile devices, as well as add, change, and remove custom properties and registry keys. It also allows you to configure Remote Control for devices that have a Remote Control client installed.

A mobile device profile has the following general options:

Enabled	Enables or disables the profile.
Home location	Sets the home location for the profile.
Mobile device selection criteria	Determines which devices the profile is applied to. For information on selection criteria, see Using Selection Criteria on page 138.
Orphan Package Removal	Removes packages that have been orphaned from the device. A package is considered orphaned if it has been deleted from the Avalanche Console, if the software profile it belongs to has been disabled, or if the package has been disabled. Orphaned packages must be listed by name. Orphaned packages must be listed by name. Orphan package removal will only happen once, when the profile is first applied.
Notes	Any notes for the profile.
Set Server Address	Specifies the address of a specific mobile device server you want the devices to connect to.
Enable SMS Notification	Allows SMS messages to be sent to the device from the Avalanche Console.
Force Package Synchronization	Synchronizes each file of each package on the device without checking the meta-file, which provides information about the state of the files. When the option is not enabled, the server checks the meta-file, and then synchronizes only the files that have been altered or do not match.
Restrict simultaneous device updates	Limits the number of devices using the profile that are allowed to update simultaneously. This may be useful if there is a particular update that will take significant bandwidth or time. Restrict how many devices receive that update at a time so that other functions aren't affected.
Authorized Users	The Authorized Users panel allows you to assign privileges for a profile to a user that does not have rights for that profile. This allows you to give a user permission for one specific profile, rather than all profiles of a specific type. Users that already have permission for the profile will not appear in the list of available users. For information about creating users and assigning permissions, see Managing User Accounts on page 23.



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

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

To create and configure a mobile device profile from the Profiles tab:

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

-Or-

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

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

Configuring Device Wipe Folders

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

To configure device wipe folders:

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

The Mobile Device Profile Details page appears.

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

The *Device Wipe Folder* dialog box appears.

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

If the server is unable to contact the device using a TCP/IP connection, it will attempt to send the wipe command using SMS. When the device's Enabler receives the command, it



will delete all files in the specified folders and force the device to reboot. If any of the selected files were in use, the Enabler will try again to delete them after the reboot.

For information on performing a device wipe after the mobile device profile has been deployed, see [Wiping a Mobile Device](#) on page 77.

Editing Custom Properties for Mobile Device Profiles

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

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

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

To add a custom property:

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

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

To edit or remove a custom property from the device:

- 1 From the **Profiles** tab, click on the name of the profile you want to configure.
- 2 Click **Edit**.
- 3 In the Properties panel, click **New**.
The *New Property* dialog box appears.
- 4 Type the **Group**, **Name**, and **Value** in the text boxes. If you are editing the property, this is the new value for the property.



- 5 If you are editing the value of the property, select **Create property**. If you want to remove the property from the device, select **Delete property**.
- 6 Click **Save**.

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

Editing Registry Keys for a Mobile Device Profile

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

This section contains information on the following tasks:

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

Adding a Registry Key to a Mobile Device Profile

When you add registry keys and values to a mobile device profile, they are added to the device registry when the profile is applied.

To add a registry key:

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

The Profile Details page appears.

- 2 Click **Edit**.

- 3 The Edit Profile page appears.

- 4 In the Registry Entries panel, click **New**.

The *Registry Key Entry* dialog box appears.

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

- 6 Type the name of the key in the **Key** text box.

- 7 Type the value entry of the key in the **Name** text box.

- 8 Enter the data for the value entry in the **Data** text box.

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

- 10 Select **Create key** as the **Action**.



- 11 Click **Add** to add the registry key and value to the list.
- 12 When you are done, click **Save**.

The key and value are saved to the profile.

Editing or Removing a Registry Key or Value

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

To edit or remove a registry key or value:

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

The Profile Details page appears.

- 2 Click **Edit**.

The Edit Profile page appears.

- 3 In the **Registry Entries** panel, click **New**.

The *New Registry Entry* dialog box appears.

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

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

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

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

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

- 9 If you are editing the key or key value, select **Create key** as the **Action**. If you are deleting the key or key value, select **Delete key**.

- 10 Click **Save**.

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

Remote Control Settings in a Mobile Device Profile

Configure Remote Control settings for a device by using a mobile device profile. The mobile device profile allows you to configure the following options for the Remote Control client:



Connection Type	The method the device should use to connect to the Remote Control Server.
Server Address	The IP address or DNS name of the Remote Control server.
Server Port	The port the Remote Control server listens on for device connections.
Server ID	An identifying name for a Remote Control server.
Connection Policy	Select how Remote Control notifies the mobile device user that Remote Control is establishing a connection. Silent indicates that the user will not be notified. Notify indicates that the user will see a text window on his device letting him know that a connection has been established. Prompt-Allow will provide the user with a prompt to allow or deny the connection. If the user does not respond, the connection will be allowed. Prompt-Deny will provide the user with a prompt to allow or deny the connection. If the user does not respond, the connection will be denied.
Policy Time	The length of time that the notification or prompt will be displayed. If you selected Prompt-Allow or Prompt-Deny , this is the number of seconds Remote Control will wait before establishing or denying the session.
Log Level	This is for the client log stored on the device. Logging levels include: Critical. Indicates errors that cause Remote Control to fail to start. Error. Indicates errors that are caused by configuration and/or communication problems. Informational. Documents the flow of operation. Warning. Indicates possible operational problems. Debug. Used to diagnose program malfunctions or communication problems.
Maximum Size	Configure the maximum size that the log file can reach before creating a new log file. New log files do not override previous log files.
Password	When a password is set, the users are required to provide the password before they can connect to a remote device.



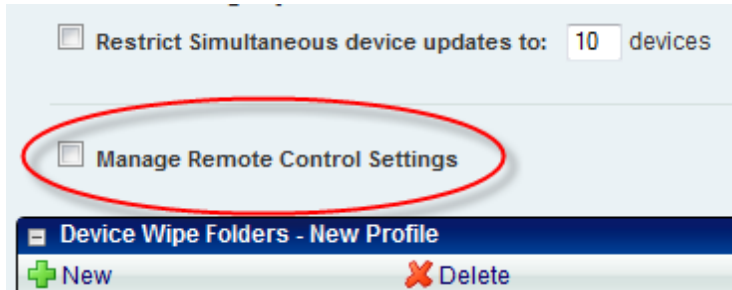
Client Sleep While Connected	Allows the mobile device to enter sleep mode while connected to Remote Control. If you do not enable this option, Remote Control will not allow the mobile device to enter sleep mode while connected.
Allow Client Configuration	Grants client configuration control to the mobile device user. This allows the user to configure the Remote Control client from the mobile device. When the mobile device user has configuration control, any changes you make in the Client Settings tab from the Remote Control Console will not deploy to the device. To regain Client Configuration setting control from the Remote Control Console, you must disable this option and redeploy the settings to the mobile device.
Disable Client Exit	When this option is enabled, the mobile device user cannot exit the Remote Control application.
Client Pre-connect to Server	Configures the device to always pre-connect to the Remote Control Server.
Client Connect on ActiveSync	When this option is enabled, the device will attempt to connect to the server when it is cradled.
Corporate Connection	This determines if VPN or port forwarding will be used by the mobile device connecting to your server. <ul style="list-style-type: none">• If this option is enabled, the mobile device uses a VPN connection to connect to the server.• If this option is disabled, the mobile device uses an Internet connection to connect to the server.
Show Skin	Displays a skin when you are connected to a device. When this option is enabled, select the skin you want to use from the drop-down menu. If you choose Autodetect , Remote Control will use device information to display the correct skin.

NOTE: When you configure Remote Control settings using a mobile device profile, the profile settings will override other Remote Control settings.

To configure Remote Control settings using 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 Remote Control Settings** option.





Mobile Device Profile Details

- 3 In the Remote Control Settings panel, configure the options as desired.
- 4 Save your changes.

Configuring Mobile Device Profile Advanced Settings

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

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

Location Based Services

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

Enable location-based services Enables GPS reporting for devices using the selected mobile device profile.

Reporting interval Determines how often the device reports its GPS statistics to the Mobile Device Server.

Report location using cell towers Uses information from nearby cell towers to establish the location of the device.

Report location using GPS Uses GPS coordinates to establish the location of the device.



GPS acquisition timeout	Determines how often the device checks its GPS coordinates.
Prompt user to initiate 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 _ 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.
The Mobile Device Profile Details page appears.
- 2 In the Other Settings panel, configure the options as desired.
- 3 Save your changes.

Geofence Areas

A geofence is a virtual perimeter defined by GPS coordinates. Geofence areas are displayed when you use the Locate function to locate your devices on the map. When you configure a geofence area and define it as the Home area, Avalanche can generate an alert when devices report a GPS position that is outside of the defined area.

To configure a geofence area:

- 1 From the **Profiles** tab, click the name of the mobile device profile you want to configure.
The Mobile Device Profile Details page appears.
- 2 Click **Edit**.
- 3 In the Geofence Areas panel, click **New**.
The *Add Geofence* dialog box appears.
- 4 Type a name for the area in the **Name** text box.
- 5 If you want the area to be a home area, enable the **Home** check box.
- 6 Enter the start and end latitude and longitude for the geofence. The start point should be the southwest corner of your area, and the end point should be the northeast.
- 7 Click **Save**.
The area is added to the list.



Regional Settings

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

To change the regional settings of a mobile device profile:

- 1 From the **Profiles** tab, click the name of the mobile device profile you want to configure.
The Mobile Device Profile Details page appears.
- 2 Enable the **Manage regional settings** check box and select the region from the drop-down list.
- 3 Enable the **Manage time zone** check box and select the time zone from the drop-down list.
- 4 Save your changes.

Update Restrictions

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

To create an update restriction:

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

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

- 4 Save your changes.



Chapter 12: Managing Mobile Device Groups

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

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

You can add authorized users for all mobile device groups or enable a user for a specific mobile device group. For information on adding an authorized user, see [Assigning Authorized Users to Mobile Device Groups](#) on page 29.

The topics in this section include:

- [Creating Mobile Device Groups](#)
- [Viewing Devices in a Mobile Device Group](#)
- [Sending Messages to Mobile Device Groups](#)

Creating Mobile Device Groups

Mobile device groups allow you to group devices together based on selection criteria you configure. You can create dynamic or static groups. In both group types, new devices can be added to the group based on changes to the selection criteria.

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

When a new device that matches the selection criteria for a dynamic mobile device group connects to the Avalanche Console, it is automatically placed in the mobile device group. Dynamic mobile device groups will continually add and remove mobile devices based on the selection criteria, without further management.

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

When a new device matching the selection criteria for a static mobile device group connects to the Avalanche Console, it will **not** automatically be placed in the mobile device



group. To modify a static mobile device group, modify the selection criteria as desired and add the mobile devices to the group. You cannot remove individual mobile devices from a static group.

The home location for the group is the location that is selected when the group is created.

To create a mobile device group:

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

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

Sending Messages to Mobile Device Groups

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

To send messages to device groups:

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

The *Send Message* dialog box appears.

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

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



Chapter 13: Managing Alert Profiles

Manage alerts in Avalanche using alert profiles. An alert profile gives you options for configuring what network events generate an alert and who is notified when an alert is generated. A server going offline or a completed synchronization are examples of alert events.

This section provides information about the following topics:

- [Creating and Configuring Alert Profiles](#)
- [Alerts Tab](#)

Creating and Configuring Alert Profiles

Alert profiles are configured with a list of events that will generate an alert. These profiles are then deployed to the servers. When an event on the list occurs, an alert is 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 **Authorized Users** panel allows you to assign privileges for a profile to a user that does not have rights for that profile. This allows you to give a user permission for one specific profile, rather than all profiles of a specific type. Users that already have permission for the profile will not appear in the list of available users. For information about creating users and assigning permissions, see [Managing User Accounts](#) on page 23.

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

Email Recipients Each alert profile can notify one or more e-mail addresses when specified events occur. If you want the Avalanche Console to send notification by e-mail, you must add the e-mail address to the Email Recipients list for that profile. The entire contact list will receive e-mails for all alerts generated by that profile.

SNMP Forwarding The Avalanche Console allows you to set one or more proxy hosts for an alert profile. When you add a proxy to a profile, the Console automatically forwards all alerts for that profile to the IP address of the proxy, enabling you to integrate Avalanche with your existing network management tools.

Available Alerts Avalanche provides a list of events that will generate alerts. You can choose events from this list when you create an alert profile.

See the following sections for additional information on configuring alert profiles:

- [Adding E-Mail Contacts](#)



- [Adding SNMP Proxies](#)

To create an alert profile:

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

The *New Profile* dialog box appears.

- 2 Select **Alert Profile**.

The New Profile Details page appears.

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

- 4 If desired, enable the profile or type any notes in the **Notes** text box.

- 5 Configure the **Email Recipients**, **SNMP Forwarding**, and **Available Alerts**.

NOTE: You must have the SMTP server settings configured if you want to send alert e-mails. For information on configuring the SMTP server settings, see [Configuring E-mail Settings](#) on page 20.

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

The alert profile is created and configured, and can be assigned to a location.

Adding E-Mail Contacts

Each alert profile can notify one or more e-mail addresses when related events occur. If you want the Avalanche Console to notify you of an alert by e-mail, add the e-mail address to the Profiled Contacts list for that profile. The entire contact list will receive e-mails for all alerts generated by that profile.

NOTE: You must configure the e-mail settings before Avalanche will send e-mails when alerts are generated. For information on configuring e-mail settings, see [Configuring E-mail Settings](#) on page 20.

A list of e-mail addresses in a comma-delimited `.csv` file (for example, one exported from Microsoft Outlook) can be imported in order to add multiple e-mail addresses at a time. You



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

To add an e-mail contact:

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

The Alert Profile Details page appears.

- 2 Click **Edit**.

The Edit Alert Profile page appears.

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

The *Add Email Recipient* dialog box appears.

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

The contact appears in the Email Recipient panel.

To import e-mail addresses:

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

The Alert Profile Details page appears.

- 2 Click **Edit**.

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

The *Import Email Recipients* dialog box appears.

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

- 5 Click **Open**.

- 6 Click **Save**.

The contacts appear in the Email Recipients panel.

Click **Save**.

To export e-mail addresses:

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

The Alert Profile Details page appears.



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

- Or -

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

The *Opening EmailExport.csv* dialog box appears.

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

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

Adding SNMP Proxies

The Avalanche Console allows you to set one or more SNMP proxies for an alert profile. When you add a proxy to a profile, the Console automatically forwards all alerts for that profile to the IP address of the proxy, enabling you to integrate Avalanche with your existing network management tools.

To add an SNMP proxy:

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

The Alert Profile Details page appears.

- 2 Click **Edit**.

The Edit Alert Profile page appears.

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

The *New SNMP* dialog box appears.

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

Alerts Tab

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

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

Acknowledging and Clearing Alerts

When a new alert is generated, it appears in the Alerts tab and the Maps tab. In the Alerts tab, the alert is listed in the Current Alerts panel. In the Maps tab, the server location at which the alert was generated is outlined in the color of the most severe alert at that location. Acknowledging the alert will remove the colored indicator from the map. If the Current Alerts panel begins to fill with alerts, remove acknowledged alerts that are no longer relevant.

[To acknowledge an alert:](#)

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

[To clear alerts:](#)

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

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

Customizing Alerts Tab Functionality

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

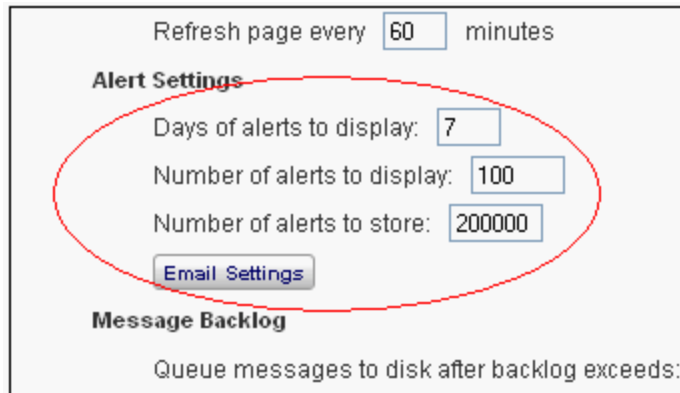
- Number of days an alert is displayed in the Current Alerts panel.
- The number of alerts to display.



- Maximum number of alerts to store. Alerts are stored in the database on the Enterprise Server. This option is only available for administrative users.

To customize the Alerts tab functions:

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



Refresh page every minutes

Alert Settings

Days of alerts to display:

Number of alerts to display:

Number of alerts to store:

[Email Settings](#)

Message Backlog

Queue messages to disk after backlog exceeds:

Alert Settings

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

The Alerts tab will update to reflect your changes.



Chapter 14: Using Selection Criteria

Selection criteria are sets of rules which you can apply to profiles or devices. The rules are generally device properties such as the model name or OS type. These criteria define which mobile devices receive a profile or are added to a group. For example, set a profile so that it is only applied to Hand Held 7400 devices by using the criterion:

```
ModelName = HHP7400
```

After the profile is enabled and applied to a location, it is distributed to devices in the location that meet the selection criterion.

If you want to set criteria but only want to match part of the expression, use an asterisk (*) as a wildcard to represent single or multiple characters. A hyphen (-) can be used to indicate a range of numbers. You can also use parentheses and boolean operators for flexible combination of multiple variables. These options can reduce the size and complexity of selection criteria.

NOTE: The database interfaces used by Avalanche put a length limit on SQL expressions. Selection criteria containing more than 150 expressions have a good chance of exceeding the limits. Wavelink recommends limiting selection criteria to 20 selection variables or less.

Additional selection criteria are typically built into each software package to restrict the distribution of the package to devices that can use it. The built-in selection criteria associated with a software package are set by the package developer and cannot be modified after the package has been created.

The selection criteria builder provides a list of operators and preset selection variables, and also allows you to add custom properties as selection variables. Use the selection criteria builder to build valid selection criteria.

This section provides the following information:

- [Building Selection Criteria](#)
- [Selection Variables](#)
- [Operators](#)

Building Selection Criteria

You can access the Selection Criteria Builder from several different places in the Avalanche Console, including network profiles, software profiles, and mobile device groups. To access the Selection Criteria Builder, click the **Launch wizard** button.

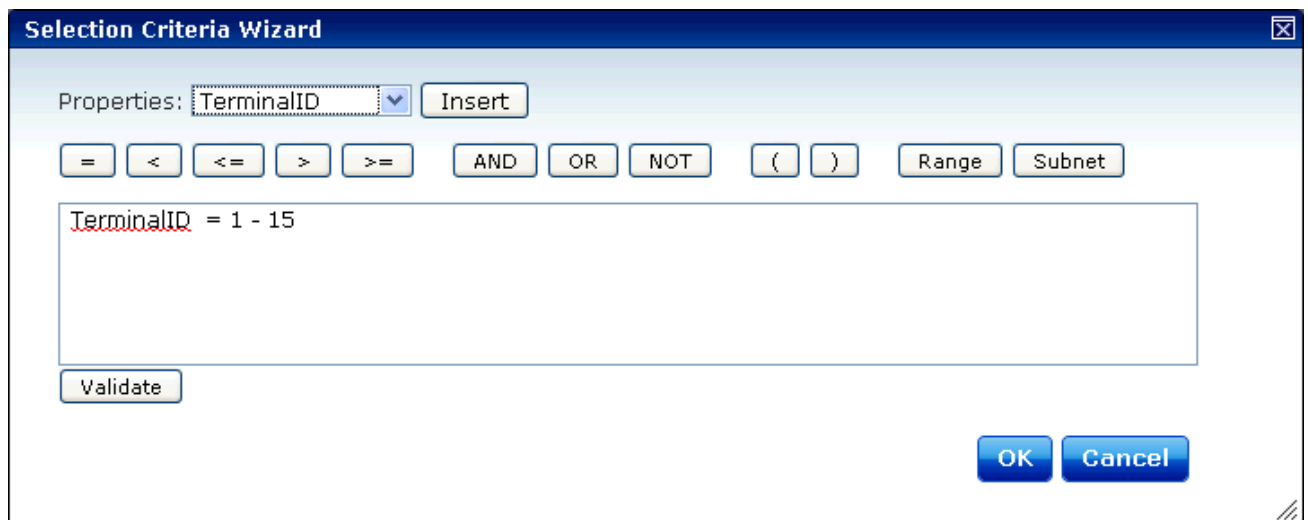


In the Selection Criteria Builder, you can build the selection criteria string by selecting or typing string elements one element at a time. The string elements include:

- Selection variables such as **ModelName** or **KeyboardName**. Avalanche comes with a default list of variables, or you can add custom properties as selection variables.
- Operators such as AND (&) and OR (|) that are used to assign a value to a selection variable or to combine multiple variables. Parentheses are recommended when multiple operators are involved. Nesting of parentheses is allowed.
- Actual values that are assigned to a selection variable. For example, if you assign a value of 6840 to a **ModelName** variable by building the string `ModelName = 6840`, then you will restrict packages or profiles to model 6840 mobile devices.

To build selection criteria:

- 1 Access the Selection Criteria Builder.



Selection Criteria Builder

- 2 From the drop-down list, select a property and click **Insert**. For information about properties, see [Selection Variables](#) on page 140.
- 3 Select one of the operator buttons. For more information about operators, see [Operators](#) on page 146.
- 4 Type a value for the property that you selected.
- 5 For each additional element you want to add to the selection criteria string, repeat the preceding steps.

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



6 Click **Validate** to see if Avalanche accepts the criteria as valid.

Using profiles, you can add custom properties to your devices. These custom properties or properties already existing on the device can be used for selection criteria. In order to use a property as a selection variable, add the property to the Selection Criteria Builder.

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

Selection Variables

Selection criteria are based on the use of selection variables. Some selection variables are preset, or you can create your own from custom properties.

You can place numbers and strings directly in the selection criteria string with or without quotes. Selection criteria strings are case sensitive.

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

```
ModelName=6840
ModelName = 6840
ModelName="6840"

Series = S
```

While these are not:

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

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

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

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

The following table lists the preset selection variables:

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

Example:

```
Columns > 20
```



- EnablerVer** Enabler version number. Values with decimals must be surrounded by double quote marks.
- EnablerVer = "3.10-13"
- IP** IP address of the mobile devices.
- 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 The 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 last time the device contacted a server. The parser for the LastContact property allows specifying absolute time stamps or relative ones.

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" (All minute long, 12-hour notation)

- 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)

- Range-forms of the above, including inverted ranges

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. Device details often display the model name.

A few of the supported values include:

```
1040, 1740, 1746, 1840, 1846, 2740, 2840, 3140, 3143,  
3540, 3840, 3843, 3940, 4040, 5040, 6140, 6143, 6840,  
6843, 6940, 7240, 7540, 7940, 8140, 8940, PTC960,  
TR1200, VT2400, WinPC, WT2200, 7000CE, HHP7400, MX1,  
MX2, MX3, VX1, iPAQ, iPAD, Falcon, ITCK30, ITC700
```

Example:

```
ModelName = 6840
```

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

Supported values include:

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

Example:

```
ModelCode <= 2
```

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

OSVer The OS version as reported by the Enabler. Values with decimals in them must be surrounded by double quote marks.

```
OSVer = "4.20"
```

OS Type The OS type as reported by the Enabler.

```
OSType = PocketPC
```

Processor The processor as reported by the Enabler.

```
Processor = ARM
```



ProcessorType The processor type as reported 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 used by the mobile device.

Supported values include:

```
any
ip
serial
```

Terminal ID The unique ID for the mobile device generated by Avalanche or assigned by a user. The initial terminal ID is 1, and the values increment as needed. You can redefine terminal IDs for mobile devices as needed. If you are using terminal IDs in a workstation ID, the value must not exceed the character limit for the host. Typically, hosts support 10 characters.

Example:

```
Terminal ID = 5
```

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

Example:

```
@exists ne some.property
@exists ==Some.property & Some.property = "value"
```

Operators

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

For example:

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

This states that both 3840 mobile devices (regardless of keyboard type) and 6840 mobile devices with a 46-key keyboard will be included.

You may use the symbol of the operator (!, &, |, etc.) in the selection criteria or the letter abbreviation (NOT, AND, OR, etc.). If you use the letter abbreviation for the operator, then you must use uppercase letters. Spaces around operators are optional, and you can use the wildcard character [*] for left wildcard constants and right wildcard constants.

Operators use the following precedence:



- 1 Parentheses
- 2 OR operator
- 3 AND operator
- 4 NOT operator
- 5 All other operators

The following operators can be used along with 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 15: Avalanche Reports

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

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

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

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

The columns displayed in these panels include the following:

Name Displays the name of the report.

Template Displays the template used for the report.

Location Indicates the location or locations involved in the report.

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

Completed Displays when the report was completed.

Frequency Displays how often the scheduled report will be run.

Category Displays the category to which the report belongs.

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

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



Configuring Reports

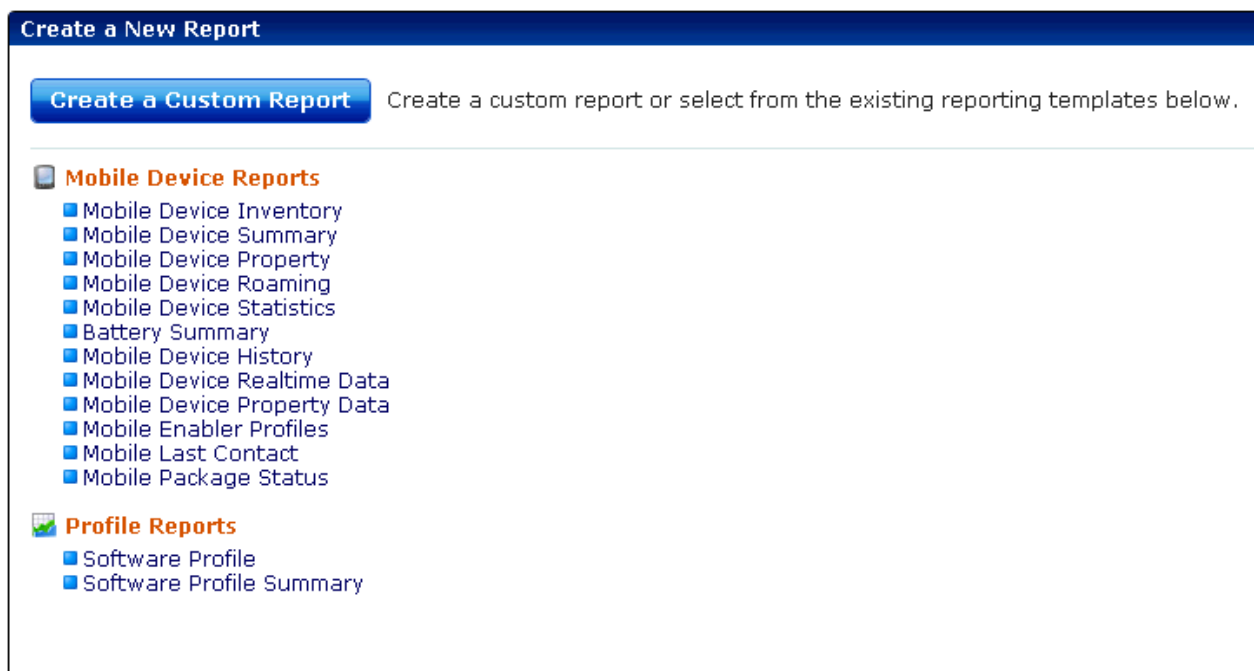
In order to create a report, you must first configure the name, scope, output, and the time period to be included in the report. Then you can either generate the report immediately or schedule a time for the report to be generated. When a report is scheduled, it can be set to run once or on a recurring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

This section includes instructions for configuring a report using a preexisting template. For information on creating custom reports, see [Creating Custom Reports](#) on page 152.

To configure a report with an Avalanche template:

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

The Create a New Report page appears.



Create a New Report page

- 3 Click on the desired template from the list of preexisting Avalanche report templates.
- 4 Depending on the template, the Reports tool will guide you through configuring the available options for the report. These will always include the name and output format, but may also include the scope or the time period to be included in the report. You may also choose to have a report sent to an e-mail recipient when it is generated.



- **Scope.** Configure the report to collect information from a specific location in the Avalanche navigation tree.
- **Name.** Create a unique name for each configured report.
- **Output Format.** Choose the file format for the report results: `.pdf`, `.xml`, or `.csv`.
- **Time.** Set the report to include information from the past 24 hours, past week, or past month.

NOTE: You cannot use a PDF output for reports with a scope of more than 1000 mobile devices — it will not run. The PDF generated would be too large. For a Mobile Device Property report, the maximum device limit for PDF is 250. If you want to run a report for a larger number of devices, it must be in CSV or XML format.

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

Generating and Scheduling Reports

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

To run a configured report:

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

The report appears in the Completed Reports panel.

To schedule a report:

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

The Schedule Reports page appears.

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



- 6 A summary of the report appears. Click **Done** to return to the Reports tool.

Creating Custom Reports

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

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.

To create a custom report:

- 1 Access the Reports tool.
- 2 From the Configured Reports panel, click **New**.
- 3 The Create a New Report panel appears. Click **Create a Custom Report**.
- 4 The Create Reports panel appears. 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**.
- 6 A Summary page appears. If you want to include information from a different table, click **Add Table**.
- 7 Use the **Where**, **Order By**, and **Group By** text boxes to create a SQL query statement that will return the desired information.
- 8 Type a **Report Name** in the text box and select the **Output Format** for the report. If you want the report to be e-mailed to a recipient when it is run, type the e-mail address in the **E-mail Report** text box. Click **Next**.
- 9 A summary of the report appears. Click **Done** to return to the Reports Tool page.

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

Viewing Completed Reports

View completed reports from the Reports page. Depending on the format, you can view a report in the browser or download the file for offline use.



To view completed reports:

- 1 Click **Tools > Reports**.
- 2 In the Completed Reports panel, click the name of the report you want to view. If the report is PDF or XML format, it will appear in the browser. If the report is CSV, you will be prompted to open the file with a suitable program.

-Or-

Right-click the name of the report and select **Save As** to save the file locally.



Chapter 16: Using the Task Scheduler

The Task Scheduler enables you to schedule network management activities for your locations. This allows you to specify which locations receive the changes and implement changes during periods of low network activity. You can schedule activities such as backing up or restoring the database.

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

Scheduling options for the Task Scheduler include:

Perform the task now Runs the task immediately.

Schedule a one-time event for the task Performs the task once at the scheduled time. This selection allows you to configure the following options:

Start date. The date the task will begin.

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

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

End date. The date the task will end.

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

Use local time of server location. Uses the time local to the specified server(s) rather than the local time of the enterprise server.

Schedule a recurring event for the task Performs the task repeatedly at the scheduled times. This selection allows you to configure the following options:

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

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

Use local time of server location. Uses the time local to the specified server(s) rather than the local time of the enterprise server.

Daily. The task is performed daily. When Daily is selected, you can also configure the following options:



Every weekday. Runs the scheduled task every day Monday - Friday.

Every weekend. Runs the scheduled task every Saturday and Sunday.

Weekly. The task is performed on a weekly basis. When **Weekly** is selected, you can also configure the following options:

Run every __ week(s) on. This option allows you to configure whether the task is run weekly or at a longer interval. For example, if you want the task to run every other Saturday, type 2 in the text box and enable the **SAT** checkbox.

[days of the week]. These check boxes allow you to specify which days of the week the task is performed.

Monthly. The task is performed on a monthly basis. When **Monthly** is selected, you can also configure the following option:

Run on the __ day, every __ month(s). This option allows you to set the day of the month to run the task, and how many months apart the task should be run.

Start date. Specifies the date the task should begin running.

No end date. When this option is selected, the task will continue repeating indefinitely.

End by. When this option is selected, the task will no longer run after the specified date.

The Task Scheduler allows you to perform the following tasks:

- [Backing Up the System](#)
- [Restoring the System](#)
- [Removing Completed Tasks](#)

Backing Up the System

This section provides information about using the Task Scheduler to back up the Avalanche system. Backup and restore functionality is available when you are using PostgreSQL



databases installed at the same location as the Enterprise Server. When you back up Avalanche, the enterprise database information and software packages are saved in a zip file.

You should back up the system regularly. If for any reason Avalanche files are deleted or corrupted, you will be able to restore them from the backup files.

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

To back up the system:

- 1 Click **Tools > Schedule Backup**.

The Create A System Backup screen appears.

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

The Scheduling Options screen appears.

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

The Review Your Task screen appears.

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

Restoring the System

If you have created a system backup using the Task Scheduler, you can use the Task Scheduler to restore the information to Avalanche.

You cannot restore a system backup from a previous version of Avalanche. The backup version must match the Avalanche version. If you attempt to restore a system backup from a previous version of Avalanche, the restoration will fail.

NOTE: If you are attempting to restore the system on a Linux operating system, Wavelink recommends you perform the restoration manually.

To restore the system:

- 1 Click **Tools > Schedule Restore**.

The Restore A System Backup screen appears.

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

- Select **Restore the most recent system backup** to restore Avalanche to the latest backup file.



- Select **Restore by path** to specify the file name and path of the desired system backup.
- Select **Restore selected** to choose the desired system backup from the list according to the identifier tag.

The Review Your Task screen appears.

- 3 Review your task to ensure that it is correct and click **Finish**.
- 4 Restart the enterprise server, statistics server, and Tomcat service after the files are restored. If Avalanche is installed on a Windows OS, this is done from the Windows Services list. For the specific names of the services, see [Avalanche Services](#) on page 176.

Removing Completed Tasks

When the Task Scheduler has completed an event, that event appears in the **Completed Tasks** list. By default the Task Scheduler is set to retain all completed tasks in the list. You can delete tasks individually.

To remove completed tasks:

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

The Scheduled Tasks page appears.

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



SSL Certificates for the Web Console

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

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

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

Self-signed certificates may also limit some functionality depending on the Flash plug-in for your browser. This would affect uploading software packages, e-mail lists, or floorplan images using the Web Console.

This section contains instructions for the following tasks:

- [Implementing a Certificate from a Certificate Authority](#)
- [Implementing a Self-Signed Certificate](#)

Implementing a Certificate from a Certificate Authority

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

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

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

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

- [Creating a Keystore](#)



- [Generating the Certificate Signing Request](#)
- [Importing an Intermediate Certificate](#)
- [Importing a Certificate](#)
- [Activating SSL for Tomcat](#)
- [Accessing the Web Console over a Secure Connection](#)
- [Troubleshooting](#)

Creating a Keystore

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

[To generate a keystore for the certificate:](#)

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

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

- 5 At the prompts, enter your organizational unit, organization, city, state, and the country code.
- 6 When you are prompted to review your information, type `yes` to confirm that it is correct. If you type `no`, you will be guided through the prompts again.
- 7 At the prompt **Enter key password for <amccert>**, type a password to use for the alias. If you want to use the same password for the alias as you used for the keystore, press Return.

[An example of generating a keystore:](#)

```
Enter keystore password: avalanche
```

```
Re-enter new password: avalanche
```



```
What is your first and last name?[Unknown]: avaself.wavelink.com
What is the name of your organizational unit?[Unknown]: Engineering
What is the name of your organization?[Unknown]: Wavelink Corporation
What is the name of your City or Locality?[Unknown]: Midvale
What is the name of your State or Province?[Unknown]: Utah
What is the two-letter country code for this unit?[Unknown]: US

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

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

Generating the Certificate Signing Request

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

To generate a certificate signing request:

- 1 From a command line, navigate to:
`[Avalanche installation directory]\JRE\Bin`
- 2 Use the command:
`keytool -certreq -keyalg RSA -alias amccert -file certreq.csr
-keystore "[Avalanche installation
directory]\JRE\bin\amckeystore.keystore"`
- 3 Enter your keystore password.

When you apply to a certificate authority for an SSL web server certificate, you will need to submit the `certreq.csr` file. This file should be created in the `[Avalanche installation directory]\JRE\bin` folder.

Importing an Intermediate Certificate

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

To import an intermediate certificate:

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



- 2 Use the command:

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

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

- 3 Enter your keystore password.

The intermediate certificate is added to the keystore.

Importing a Certificate

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

To import a certificate:

- 1 From a command line, navigate to:

```
[Avalanche installation directory]\JRE\bin
```
- 2 Use the command:

```
keytool -import -alias amccert -keystore "[Avalanche installation directory]\JRE\bin\amckeystore.keystore" -trustcacerts -file ava-wavelink-com.cer
```

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

- 3 Enter your keystore password.

The certificate is added to the keystore.

Activating SSL for Tomcat

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

To activate SSL for Tomcat:

- 1 Navigate to

```
[Avalanche Install location]\WebUtilities\tomcat\conf
```

and open the `server.xml` file with a text editor such as Notepad.



2 Find

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

3 Remove the comment markers so that the section is not commented out.**4 Modify the section to contain the following information:**

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

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

```
keystorePass="avalanche"
```

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

5 Save your changes to the file.**6 Restart the Apache Tomcat for Wavelink service.**

Accessing the Web Console over a Secure Connection

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

To access the Web Console over a secure connection:

- In the address field of your browser, type:

```
https://[Your Domain Name]:8443/AvalancheWeb
```

-Or-

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

```
https://[Your Domain Name]/AvalancheWeb
```



Troubleshooting

To troubleshoot issues connecting to the Apache Tomcat server using SSL after changes are made, go to

```
[Avalanche installation directory]\WebUtilities\Tomcat\logs
```

to find Catalina Tomcat logs.

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

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

Implementing a Self-Signed Certificate

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

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

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

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

- [Generating a Certificate](#)
- [Activating SSL for Tomcat](#)
- [Accessing the Web Console over a Secure Connection](#)
- [Troubleshooting](#)

Generating a Certificate

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

To generate a self-signed certificate:

- 1 From a command line, navigate to:

```
[Avalanche installation directory]\JRE\Bin
```



- 2 Use the command:
`keytool -genkey -alias amcselfcert -keyalg RSA -keystore selfsignkeystore.keystore`
- 3 At the prompt **Enter keystore password**, type the keystore password. When prompted, re-enter the password.
- 4 At the prompt **What is your first and last name**, type the Common Name.

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

- 5 At the prompts, enter your organizational unit, organization, city, state, and the country code.
- 6 When you are prompted to review your information, type `yes` to confirm that it is correct. If you type `no`, you will be guided through the prompts again.
- 7 At the prompt **Enter key password for <amcselfcert>**, type a password to use for the alias. If you want to use the same password for the alias as you used for the keystore, press Return.

An example of generating a self-signed certificate:

```
Enter keystore password: avalanche
Re-enter new password: avalanche
What is your first and last name?[Unknown]: avaself.wavelink.com
What is the name of your organizational unit?[Unknown]: Engineering
What is the name of your organization?[Unknown]: Wavelink Corporation
What is the name of your City or Locality?[Unknown]: Midvale
What is the name of your State or Province?[Unknown]: Utah
What is the two-letter country code for this unit?[Unknown]: US
Is CN=avaself.wavelink.com, OU=Engineering, O=Wavelink Corporation,
L=Midvale, ST=Utah, C=US correct?[no]: yes
Enter key password for <amcselfcert> (RETURN if same as keystore
password):
```

Activating SSL for Tomcat

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



To activate SSL for Tomcat:

1 Navigate to

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

2 Find

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

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

4 Modify the section to contain the following information:

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

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

```
keystorePass="avalanche"
```

NOTE: If you are not using port 443 for any other applications, you can change the connector port to 443. Changing the port to 443 will allow you to access the Web Console without typing the port as part of the URL.

5 Save your changes to the file.

6 Restart the Apache Tomcat for Wavelink service.

Accessing the Web Console over a Secure Connection

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

To access the Web Console over a secure connection:

- In the address field of your browser, type:

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

-Or-

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



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

Troubleshooting

To troubleshoot issues connecting to the Apache Tomcat server using SSL after changes are made, go to

```
[Avalanche installation directory]\WebUtilities\Tomcat\logs
```

to find Catalina Tomcat logs.

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

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



Configuring the Remote Control Server for SSL

The Remote Control Server can be configured to use SSL for connections between the server and a browser, so when you use the Remote Control Console, the connection is encrypted. It also encrypts connections between the viewer and the server. In order to use SSL, you must have a certificate and a private key.

If you intend to use Remote Control with an SSL certificate for a secure connection, you can either purchase a certificate through a third-party Certificate Authority (such as Verisign) OR create a self-signed certificate.

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

To configure Remote Control for SSL, complete one of the following tasks:

- [Implementing a Certificate from a Certificate Authority](#)
- [Implementing a Self-Signed Certificate](#)

Implementing a Certificate from a Certificate Authority

You can use Remote Control with a certificate from a Certificate Authority. Remote Control requires that the certificate be imported into the Java keystore. The steps may vary depending on the certificate authority vendor.

Wavelink strongly recommends that you backup the keystore and certificate files after you have implemented your certificate.

The steps provided below use the Java keytool utility. The following tasks are necessary to implementing an SSL certificate from a certificate authority:

- [Creating a Keystore](#)
- [Generating the Certificate Signing Request](#)
- [Importing the Certificate](#)
- [Configuring Remote Control to Use SSL](#)
- [Accessing the Remote Control Console over a Secure Connection](#)
- [Configuring the Package with the Server Address](#)



Creating a Keystore

To create a keystore for the certificate, use the `keytool.exe` utility. You will need to provide a domain name (Common 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 should be noted for future reference.

To generate a keystore for the certificate:

- 1 From a command line, navigate to:

```
[RC installation directory]\jre\bin
```

where `[RC installation directory]` is the directory where Remote Control is installed.

- 2 Use the command:

```
keytool -genkey -alias rcselfcert -keyalg RSA -keystore 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 domain name. The domain name you enter should be the domain name for the server where Remote Control is installed. Wavelink recommends using the fully qualified domain name unless you plan to use a wildcard certificate.

NOTE: Remote Control will not function if the domain name on the certificate is incorrect.

- 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 <rcselfcert>**, press `Return` to use the same password for the key.
- 8 The certificate and keystore are created.

An example of generating a keystore:

```
Enter keystore password: avalanche
Re-enter new password: avalanche
What is your first and last name?[Unknown]: domain.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=domain.wavelink.com, OU=Engineering, O=Wavelink Corporation,
L=Midvale, ST=Utah, C=US correct?[no]: yes
Enter key password for <rcselfcert>(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:

```
[Remote Control installation directory]\jre\bin
```

- 2 Use the command:

```
keytool -certreq -keyalg RSA -alias rcselfcert -file certreq.csr
-keystore "[Remote Control installation
directory]\JRE\bin\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 `[Remote Control installation directory]\jre\bin` folder.

Importing the Certificate

When you acquire your certificate and any intermediate certificates from the certificate authority, import them into the keystore. Depending on the format of the files, you may need to convert them to a format that the keystore will recognize. Copy the file or files to the `[Remote Control installation directory]\JRE\bin` directory before you import.

NOTE: If you generated the CSR from the computer where Remote Control is installed, the keystore will already have the private key. If you need to import the private key to a different keystore or if you need to combine the certificate file and intermediate certificates, use a tool such as OpenSSL to convert the files to a single file in PKCS12 format before importing the file to the keystore.

To import a certificate:

- 1 From a command line, navigate to:

```
[Remote Control installation directory]\JRE\bin
```



- 2 Use the command:

```
keytool -import -alias amccert -keystore keystore -trustcacerts -  
file example.cer
```

NOTE: As an example, `example.cer` is used as the filename. Replace this with the name of your certificate file.

- 3 Enter your keystore password.

The certificate is added to the keystore. After you have imported the certificate, copy the keystore file (named `keystore`) to the `Remote Control 4.1\cfg` directory.

Configuring Remote Control to Use SSL

Once you have generated a certificate, configure Remote Control with the keystore information. Modify the `server.properties` file and then restart the Remote Control server. If you do not want the password in clear text, obfuscate the password using the provided instructions.

NOTE: The properties file is case-sensitive.

To activate SSL for Remote Control:

- 1 Navigate to:

```
[RC Install location]\cfg
```

and open the `server.properties` file with a text editor such as Notepad.

- 2 If the key password and the keystore password are the same, insert the following lines:

```
Web.HTTP.Enable = 0  
Web.HTTPS.Enable = 1  
Web.SSL.KeyPassword = [password]  
Web.SSL.KeyStore = cfg/keystore  
Web.SSL.MaxIdleTime = 60000  
Web.SSL.Port = 8900
```

Where `[password]` is the password for both the key and keystore.

Or, if the key password and keystore password are different, insert the following lines:

```
Web.HTTP.Enable = 0  
Web.HTTPS.Enable = 1  
Web.SSL.KeyPassword = [key password]  
Web.SSL.Password = [keystore password]  
Web.SSL.KeyStore = cfg/keystore
```



```
Web.SSL.MaxIdleTime = 60000
Web.SSL.Port = 8900
```

Where [key password] and [keystore password] are your passwords for the key and keystore.

- 3 Save your changes to the file.
- 4 Restart the Remote Control service.

To obfuscate a password:

- 1 From a command line, navigate to:

```
[Remote Control installation location]\lib
```

- 2 Use the command:

```
java.exe -cp jetty-6.1.24.jar;jetty-util-6.1.24.jar
org.mortbay.jetty.security.Password [password]
```

where [password] is the password you want obfuscated.

The command will generate an obfuscated password that begins `OBF:.` Use the entire line as a password in the `server.properties` file. For example:

```
Web.SSL.KeyPassword = OBF:1vgt1t331vg1
```

Accessing the Remote Control Console over a Secure Connection

Once you have imported the certificate, copied the keystore file to the Remote Control `cfg` directory, and configured and restarted Remote Control, you can access the Console over a `https` connection.

To access the Remote Control Console over a secure connection:

- In the address field of your browser, type:

```
https://<Domain Name>:8900/app/setup_logon.vm
```

Configuring the Package with the Server Address

In order to connect to a device after configuring the server to use SSL, you must configure the Remote Control package with the new server port and protocol.

NOTE: This document provides instructions on configuring the package from the Java Console. The task can also be accomplished from the Web Console.

To configure the package with the server address:

- 1 On the **Profiles** tab, select the software profile that has the Remote Control package.



- 2 From the Software Packages area of the **Software Profile** tab, select the package and click **Configure**. The *Configure Software Package* dialog box appears.
- 3 From the available list, double-click **Server Location**. The *Remote Control Server Location* dialog box appears.
- 4 In the Server text box, type the address and port for the Remote Control server, including the https protocol. For example:

```
https://servername.headquarters.yourcompany.com:8900
```
- 5 Click **OK**.

The software package is ready for synchronization.

Implementing a Self-Signed Certificate

These instructions explain how to generate and use a self-signed certificate for Remote Control. 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 may not recognize a self-signed certificate as trusted and display warnings before allowing you access.

Wavelink strongly recommends backing up the server configuration and keystore files after you have implemented a self-signed certificate.

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

- [Generating a Certificate](#)
- [Configuring Remote Control to Use SSL](#)
- [Accessing the Remote Control Console over a Secure Connection](#)
- [Configuring the Package with the Server Address](#)

Generating a Certificate

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

To generate a self-signed certificate:

- 1 From a command line, navigate to:

```
[RC installation directory]\jre\bin
```



where `[RC installation directory]` is the directory where Remote Control is installed.

- 2 Use the command:

```
keytool -genkey -alias rcselfcert -keyalg RSA -keystore 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 domain name. The domain name you enter should be the domain name for the server where Remote Control is installed. Wavelink recommends using the fully qualified domain name unless you plan to use a wildcard certificate.

NOTE: Remote Control will not function if the domain name on the certificate is incorrect.

- 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 <rcselfcert>**, press `Return` to use the same password for the key.
- 8 The certificate and keystore are created. Copy the keystore file (named `keystore`) to the Remote Control 4.1/cfg directory.

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]: domain.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=domain.wavelink.com, OU=Engineering, O=Wavelink Corporation,
L=Midvale, ST=Utah, C=US correct?[no]: yes
Enter key password for <rcselfcert>(RETURN if same as keystore
password):
```



Configuring Remote Control to Use SSL

Once you have generated a certificate, configure Remote Control with the keystore information. Modify the `server.properties` file and then restart the Remote Control server. If you do not want the password in clear text, obfuscate the password using the provided instructions.

NOTE: The properties file is case-sensitive.

To activate SSL for Remote Control:

- 1 Navigate to

```
[RC Install location]\cfg
```

and open the `server.properties` file with a text editor such as Notepad.

- 2 If the key password and the keystore password are the same, insert the following lines:

```
Web.HTTP.Enable = 0
Web.HTTPS.Enable = 1
Web.SSL.KeyPassword = [password]
Web.SSL.KeyStore = cfg/keystore
Web.SSL.MaxIdleTime = 60000
Web.SSL.Port = 8900
```

Where `[password]` is the password for both the key and keystore.

Or, if the key password and keystore password are different, insert the following lines:

```
Web.HTTP.Enable = 0
Web.HTTPS.Enable = 1
Web.SSL.KeyPassword = [key password]
Web.SSL.Password = [keystore password]
Web.SSL.KeyStore = cfg/keystore
Web.SSL.MaxIdleTime = 60000
Web.SSL.Port = 8900
```

Where `[key password]` and `[keystore password]` are your passwords for the key and keystore.

- 3 Save your changes to the file.
- 4 Restart the Remote Control service.

To obfuscate a password:

- 1 From a command line, navigate to:

```
[Remote Control installation location]\lib
```



- 2 Use the command:

```
java.exe -cp jetty-6.1.24.jar;jetty-util-6.1.24.jar  
org.mortbay.jetty.security.Password [password]
```

where [password] is the password you want obfuscated.

- 3 The command will generate an obfuscated password that begins `OBF:.` Use the entire line as a password in the `server.properties` file. For example:

```
Web.SSL.KeyPassword = OBF:1vgt1t331vg1
```

Accessing the Remote Control Console over a Secure Connection

Once you have generated a certificate, copied the keystore file to the Remote Control `cfg` directory, and configured and restarted Remote Control, you can access the Console over a `https` connection.

To access the Remote Control Console over a secure connection:

- In the address field of your browser, type:

```
https://<Domain Name>:8900/app/setup_logon.vm
```

Configuring the Package with the Server Address

In order to connect to a device after configuring the server to use SSL, you must configure the Remote Control package with the new server port and protocol.

NOTE: This document provides instructions on configuring the package from the Java Console. The task can also be accomplished from the Web Console.

To configure the package with the server address:

- 1 On the **Profiles** tab, select the software profile that has the Remote Control package.
- 2 From the Software Packages area of the **Software Profile** tab, select the package and click **Configure**. The *Configure Software Package* dialog box appears.
- 3 From the available list, double-click **Server Location**. The *Remote Control Server Location* dialog box appears.
- 4 In the Server text box, type the address and port for the Remote Control server, including the `https` protocol. For example:

```
https://servername.headquarters.yourcompany.com:8900
```

- 5 Click **OK**.

The software package is ready for synchronization.



Avalanche Services

This is a list all of the Avalanche services. Under each service title, you'll find the file path where the service is located for a default installation and which server the service is associated with.

Apache Tomcat for Wavelink

C:\Program Files\Wavelink\Avalanche\WebUtilities\Tomcat\bin\tomcat7.exe

The Tomcat server is responsible for making the Web Console available. It is normally installed with the Enterprise Server.

Wavelink Authentication Service AMC

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

The authentication server authenticates users when your system is configured to use SecurePlus or integrated logon. It is installed with the Enterprise Server.

Wavelink Avalanche Service Manager

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

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

Wavelink Avalanche Enterprise Server

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

This is the enterprise server.

Wavelink Information Router

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

The inforail service handles messages between servers and databases. It is normally installed with the enterprise server.

Wavelink License Server

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

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

Wavelink Stat Server Enterprise

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



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

Wavelink Avalanche Agent

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

This is the mobile device server.



Port Information

This section provides information about the ports used in Avalanche MC.

Database Inbound Ports

The databases listen on different ports depending on the database management system you are using (PostgreSQL, Oracle, or Microsoft SQL Server) and whether the database administrator has changed the port number. The following table lists the default port for each database management system. Be sure to configure Avalanche and your network with the correct port number.

The standard Avalanche installation uses a PostgreSQL database management system.

Database Management System	Default Port	UDP/TCP	Source
PostgreSQL	5432	TCP	Enterprise Server, Statistics Server, Web Console
Oracle	1521	TCP	Enterprise Server, Statistics Server, Web Console
MS SQL Server	1433	TCP	Enterprise Server, Statistics Server, Web Console

Enterprise/Statistics Server Ports

The following table provides a list of ports that the Enterprise and Statistics Server use to communicate. The Tomcat server is usually installed local to the Enterprise Server.

Traffic Description	Port	UDP/TCP	Source	Destination
LDAP user verification.	389	TCP	Enterprise Server	LDAP server
Active Directory user verification.	5002	TCP	Enterprise Server	Active Directory server
Mobile device server requesting licenses from the License Server.	7221	TCP	Mobile Device Server	Enterprise Server



Traffic Description	Port	UDP/TCP	Source	Destination
InfoRail transmission of information between servers, consoles, databases.	7225	TCP	Mobile Device Server, Enterprise Server, Web and Java Console, databases	Mobile Device Server, Statistics Server, databases
InfoRail talking to itself.	7226	TCP	Local traffic	Local traffic
Web Console requesting information.	8080	TCP	Web Console	Tomcat server

NOTE: If you use an SSL certificate, the Tomcat server listens on 8443 for a connection. You can change this to 443 in the `server.xml` file if no other program is using 443. For more information on changing the port for a Web Console connection, see [SSL Certificates for the Web Console](#) on page 158.

Mobile Device Server Ports

The following table provides a list of the ports that the Mobile Device Server uses to communicate with the Enabler installed on a mobile device.

Traffic Description	Port	UDP/TCP
Protocol Service. Traffic between the server and the Enabler.	1777	UDP/TCP
MUV3. Services persistent connections to mobile devices.	1778	TCP

SecurePlus and Remote Control Ports

SecurePlus (known in earlier versions as CE Secure) uses port 5001 (TCP). The following table provides a list of the ports that are used by Wavelink Avalanche Remote Control.

Usage	Port	Type	RC Server	Console/Viewer	RC Client
Contacting a mail server (Optional)	25 ¹ 110 ²	TCP	Out	N/A	N/A
Device Connection ³	1899	TCP	In/Out	Out	In/Out

¹For SMTP.

²For POP3.

³For Avalanche On Demand or WAN connections, this port must be forwarded from the public IP to the internal server address.



Usage	Port	Type	RC Server	Console/ Viewer	RC Client
Server Control	1900	TCP	In	Out	N/A
Status Checks	1903	UDP	Out	Out	In
Avalanche License Server	7221	TCP	Out	N/A	N/A
Avalanche Tomcat Server	8080	TCP	Out	N/A	N/A



Uninstalling Avalanche

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

When you uninstall Avalanche, you are given the option to uninstall the PostgreSQL database as well. If you select to uninstall Avalanche and the PostgreSQL database, all components of Avalanche and the database will be removed. If you select to uninstall Avalanche but leave the database, the `\db` folder located in the default installation directory will remain on your system. (The default location is `C:\Program Files\Wavelink\AvalancheMC\db`.)

The uninstall utility will not remove a Remote Control Server. Remote Control components have separate utilities for uninstallation. For more information, see the *Remote Control User Guide*.

If you uninstall and reinstall the enterprise server (on the same system) without uninstalling the device servers, the device servers are automatically discovered and appear in the **Unassigned Server Locations** region. If you install the enterprise server on a different system, device servers are not auto-discovered.

To uninstall Avalanche:

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

-Or-

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

The *Uninstall Wizard* appears.

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

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



Wavelink Contact Information

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

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

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.

