Avalanche SE

SITE EDITION

Avalanche Site Edition

Version 4.7

avse-ug-47-20080630

Revised 6/30/08

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

Email: sales@wavelink.com

Table of Contents

Chapter 1: Installing Avalanche SE

Avalanche SE is designed to operate on a wide variety of network configurations. However, system requirements must be met to ensure optimal performance. Review requirements before installing. This chapter provides information about the following:

- Installation Requirements
- Confirm that no firewalls (WinXP or external) will block any of the required ports for communication. (Refer to Appendix A for a list of ports required to run Avalanche SE).
- Importing Avalanche Manager Backup Files
- Activating Avalanche SE

Installation Requirements

The following table lists the installation requirements for Avalanche SE.

Item	Requirement
OS	Windows 2000 Server (SP 4), Windows 2000 Professional (SP 4), Windows 2003 Server (SP 2 or later), Windows XP (SP 2 or later)
Processor	Intel Pentium 4 Processor at 2.8 GHz (or equivalent)
Hard Drive	• 5 GB for Console • 10 GB for Mobile Device Server
RAM	• 1 GB for Console and Mobile Device Server
MISC	• Administrator login rights • Partition/Disk NTFS file system • JSE Runtime Environment 5.0 (automatically installed by the Avalanche installer if not already on your system • Shared file folder on the host system where the administrator has full control. • Administrative rights on the system.
RAPI	• Active Sync 3.7.1 or later • ActiveSync support connection • Serial port for serial connection

Before You Begin

Review the following before beginning the Avalanche SE installation:

- Confirm that any previous versions of Avalanche, Mobile Manager, Mobile Manager Enterprise, and PostgreSQL have been completely uninstalled, their directories removed and the Windows Services deleted.
- Confirm that no firewalls (WinXP or external) will block any of the required ports for communication. (Refer to Appendix A for a list of ports required to run Avalanche SE).

Installing Avalanche SE

When you install Avalanche SE (as a replacement for Avalanche Manager Site) you automatically create one local Location (My Location) on the machine to which you are installing Avalanche SE. A Mobile Device Server automatically installs to the local location.

The Avalanche install includes the following:

- PostgreSQL database
- Localized Java update
- License Server

To install Avalanche SE:

1 Download the Avalanche SE install.

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

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

The *Introduction* dialog box appears.

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

The *License Agreement* dialog box appears.

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

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

The *Organization Name* dialog box appears.

5 Enter the name of your organization and click **Next**.

6 This name will appear in the Avalanche SE Console, branding this version for your company.

The *Choose Destination Location* dialog box appears.

7 Click **Next** to accept the default installation folder, or click **Browse** to navigate to a folder of your choice. After you select an installation folder, click **Next** to continue the installation process.

Avalanche SE is installed on your system. The Setup program configures several internal components to run on your system. Once the installation is complete, you are immediately prompted to activate this installation of Avalanche SE for your network. For more information about activating Avalanche SE, refer to *Activating Avalanche SE* on page 11.

Importing Avalanche Manager Backup Files

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

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

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

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

To import a backup file:

1 Launch the Avalanche SE Console. (**Start menu > All Programs > Avalanche SE >Avalanche SE Console**)

2 From the **File Menu**, select **Import > Site Backup File**.

The *Import Data* dialog box appears.

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

A status dialog box appears as the file imports to the My Enterprise level.

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

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

The data from the backup file is imported to Avalanche SE and the database.

Migrated Components

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

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

Table 1-1: *Components Migrated from Avalanche Manager to Avalanche SE*

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

Table 1-1: *Components Migrated from Avalanche Manager to Avalanche SE*

Activating Avalanche SE

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

- Overview of Nodelocking
- Activating Avalanche SE Licenses
- Activating Remote Control and CE Secure Licenses

NOTE You do not need a license to configure and deploy Telnet Client packages. The Telnet Client is pre-licensed to communicate with Avalanche SE allowing you to deploy Telnet Client packages and configurations to your mobile devices without purchasing a license.

Overview of Nodelocking

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

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

Activating Avalanche SE Licenses

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

There are four methods of activating Avalanche SE licenses:

- Activating Automatically
- Activating Manually
- Importing a License

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

Activating Automatically

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

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

To activate Avalanche SE:

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

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

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

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

4 Click **Activate**.

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

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

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

Activating Manually

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

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

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

To manually activate a license:

1 Obtain the information needed for the product license.

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

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

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

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

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

6 Download the file to desired location.

7 Move `wavelink.lic` file to system with where Avalanche SE is installed.

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

Importing a License

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

To import a license:

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

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

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

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

Activating Remote Control and CE Secure Licenses

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

Refer to *Activating Automatically* on page 12, *Activating Manually* on page 13 and *Importing a License* on page 14 for steps to activate licenses.

Chapter 2: Avalanche SE Console

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

This section contains the following topics:

- Launching the Avalanche SE Console
- Understanding Avalanche SE Console
- Understanding Edit Mode
- Changing Console Preferences
- Avalanche SE Reporting Tool
- Using the Support Generator
- Using the Enabler Installation Tool

Launching the Avalanche SE Console

Launch the Avalanche SE Console from the **Programs** menu or from a shortcut.

To start the Avalanche SE Console:

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

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

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

   Avalanche SE is installed with a default user login of *amcadmin* and password of *admin*. Wavelink recommends you create a new password for this admin account once you log in. For information about changing passwords, refer to *Chapter 3: Managing User Accounts* on page 31.

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

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

5 Click **Connect**.

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

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

When your console contacts the Enterprise Server and your credentials are valid, the Avalanche SE Console appears.

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

Understanding Avalanche SE Console

The Avalanche SE Console consists of various tools to manage your wireless network. These tools are located in the Navigation Window, which also provides a tree view of the your enterprise, location, and mobile device groups. In addition, the Console contains tabs and tool bar options that provide you information regarding wireless network configuration and activity.

The Avalanche SE Console consists of the following areas:

- Tool Bar
- Quick Start Tab
- Alerts Tab
- Navigation Window/Profile Selection

Tool Bar

The following table provides information about each Tool Bar button.

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

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

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

Click this icon to open the Task Scheduler to perform backups.

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

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

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

Click this icon to launch the Avalanche SE Report Console.

Quick Start Tab

When you first launch the console, the **Quick Start** tab displays. This tab provides quick links to tasks you will perform to configure your enterprise. Each task is accompanied by a brief description which you can view by clicking the plus button. For detailed information and steps about each tasks, refer to the online help or the appropriate section in the documentation.

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

- Add Network Profiles. Use the prompts to create and begin configuring a network profile. FOr details about configuration options, refer to *Chapter 5: Managing Network Profiles* on page 51 for details.

- Add Device Software. Use the Add Device Software Wizard to guide you through creating a software profile or adding software packages. For details about using the wizard, refer to *Chapter 7: Managing Software Profiles* on page 85 for details.

- Tools (including Scan to Configure, Install Enablers and Check for Updates)

- Help and Support. Provides links to the Avalanche SE Help, Wavelink Support, and launches the Support Generator. For details about using the Support Generator, refer to *Using the Support Generator* on page 28.

If you do not want to display the **Quick Start,** you can disable the tab by selecting **View** > **Quick Start**. You can also disable the **Show Quick Start on Startup** check box located on the **Quick Start** tab. This ensures the **Quick Start** does not appear each time you launch the console.

Alerts Tab

The Alerts Tab displays alerts that occur on your wireless network in a table format. The table displays the following information about each alert:

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

Navigation Window/Profile Selection

The Navigation Window is a repository for profiles that may be configured and applied to your mobile devices. Profiles determine all aspects of device configuration, such as device network connectivity and software load. The Navigation Window also provides the My Enterprise view, which is a folder containing the mobile devices.

From the Navigation Window, you can access the following Profile Sets:

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

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

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

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

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

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

- **My Location and Sites**. My Location contains one Device Server that communicates with wireless devices. Sites are groups of mobile devices.

You can use the **Search** text box to locate profiles and sites in the console. Type in the name of the mobile device group or profile in the text box above the tree view. Click **Search**. The highlight will move to the first entry that matches the text you entered. The search is not case sensitive.If there are multiple matches, click **Search** until you reach the correct entry.

Understanding Edit Mode

Before you can edit profiles, you must enter edit mode. To use edit mode, you employ the following icons located in the toolbar:

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

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

Click **Save** to save configuration changes.

Consider the following directives regarding the use of Edit Mode:

- Edit mode is required to edit profiles, Location Properties, and Site Properties.
- You must select a profile, create a profile or highlight a location under My Enterprise to enable the Edit button.
- When you enter Edit Mode, the Navigation Window will not be available until you exit Edit Mode.
- If you add a new profile, you will need to click Edit Mode before you can continue configuration.

Changing Console Preferences

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

- Enable Checking for Updates
- Customizing Console Display

- Enabling Auto Assign Options
- Enabling Audit Logging
- Viewing Logged Activity
- Specifying the Backup Drive Location
- Configuring HTTP Proxy Connections
- Viewing the Enterprise Server Status
- Purging Statistics
- Changing Report Settings

Enable Checking for Updates

You can enable the Console to check for Avalanche updates each time it starts up. This option is enabled by default.

When you enable the option, a dialog box, displaying any devices whose Enablers are have updates available, appears each time you launch the console. The Enabler information is based on the information the device reported the last time it checked in. From the dialog box, you can click the **Download** link next to the device whose Enabler you want to update. The link will direct you to the Wavelink web page containing the update.

You can also access the update dialog box from the Help menu or from the Quick Start tab.

To enable checks:

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

   The *Preferences* dialog box appears.

2. In **Startup Settings**, enable the **Check for updates on startup** option.
3. Click **OK** to save your changes and close the *Preferences* dialog box.
4. The next time the Console is launched, it will check for additional software updates.

Customizing Console Display

You can configure the appearance of the Avalanche SE Console, including display size, position and default page view from the *Preferences* dialog box. You can also configure the manner in which the Alert Browser manages alerts.

To customize the console display:

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

The *Preferences* dialog box appears.

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

3 In **Alert Browser Settings**, use the text boxes to configure how many days an alert remains in the Alert Browser, the maximum number of alerts that can appear in the Alert Browser, and the maximum number of alerts to store.

NOTE Alerts are stored in the database on the Enterprise Server.

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

The Avalanche SE Console updates to reflect your changes.

Enabling Auto Assign Options

To enable auto-options:

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

The *Preferences* dialog box appears.

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

3 Enable the **Auto Assign Profiles** option to automatically assign all profiles and profile changes to **My Enterprise**.

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

Enabling Audit Logging

When you enable audit logging, you can specify what types of events you want the Console to log including:

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

The log file is stored in the default Avalanche SE location.

To enable audit logging:

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

The *Preferences* dialog box appears.

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

3 In **Audit Log**, activate the **Enable Audit Logging** checkbox.

4 Enable the events you want to record.

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

Viewing Logged Activity

If you enable audit logging for the Console, you can view the activity from the Console Activity Log. The log provides information based on the logging preferences you set for audit logging. You can view the date and time of the Console activity, the user activity, and description of the changes that occurred.

To view the Console activity:

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

Specifying the Backup Drive Location

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

For information about backing up your system, refer to the *Backing Up and Restoring Avalanche SE* document located on the Wavelink web site.

To specify a location:

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

The *Preferences* dialog box appears.

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

3 In the **Backup/Restore** section, enter the path where you want to save system backups.

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

Configuring HTTP Proxy Connections

If you are using an HTTP proxy for external Web site location connections, you must configure HTTP proxy settings to enable the city search performed during the Avalanche SE installation process.

To configure HTTP proxy settings:

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

The *Preferences* dialog box appears.

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

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

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

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

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

6 If you are using Basic Authentication for the HTTP proxy, type the **User Name** and **Password** in the appropriate text boxes. Otherwise, leave these boxes blank.

7 Click **OK** to save your changes.

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

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

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

Viewing the Enterprise Server Status

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

The following list describes the parameters and values displayed in the **eServer Status**:

- **Version**. Indicates the version of the eServer.
- **Build Number**. Indicates the build number of the eServer.
- **Installation Path**. Displays the installation location of the eServer.
- **Start Time**. Displays the last time the eServer was started.
- **Current Time**. Displays the current time.
- **Uptime**. Indicates how long the eServer has been running since the last start time.
- **Messages Received**. Displays the total number of messages the eServer has received.
- **Messages Sent**. Indicates the total number of messages the eServer has sent.
- **Spillover Enabled**. Indicates whether the memory spillover function is enabled (YES or NO).
- **Spillover Threshold**. Indicates the memory level before spillover takes effect.

- **Spillover Release**. Indicates the number of seconds before the spillover is released.
- **Blackout Mode**. Indicates if blackout mode is enabled.
  - **Off** indicates that blackout mode is not currently in use.
  - **Mobile Device Server** indicates that the server is in are in blackout mode.
- **Priority C0 - C2 Backlog** indicate the number of messages coming from consoles with C0 being the highest priority and C2 being the lowest priority.
- **Priority A0 - A2 Backlog** indicate the number of messages coming from the Mobile Device Server with priority A0 being the highest priority and A2 being the lowest priority.

To view the status::

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

The *eServer Console* dialog box appears.

2 In the **eServer Status** you can view the status of each property.

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

Purging Statistics

To prevent database and Enterprise Server inflation, you can configure the Enterprise Server to purge logged statistics. You can configure the following:

- **Purge Time**: Set the time of day you when you want to remove the statistics. This allows you to control the timing of the activity occurring on the Enterprise Server.
- **Number of Days to Keep**: Set the number of days you want to keep the statistics before removing them. Wavelink recommends setting the days to keep statistics fairly low as the statistics accumulate quickly and the purging process could take a very long time if there are too many statistics. The maximum number of days you can set is 30.

To configure purge settings:

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

The *eServer Console* dialog box appears.

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

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

Avalanche SE Reporting Tool

Avalanche SE features the Wavelink Avalanche SE Report Console, a reporting tool that allows you to build reports based on your location, sites or device groups. Before you can connect to the Report Console, you must install the reporting utility. Contact Wavelink Customer Service to obtain the installation package. For more information about using the reporting tool, refer to the *Wavelink Avalanche Reporting Tool Reference Guide*.

To connect to the Avalanche SE Report Console:

1 Install the Report Console utility.

2 Click the reporting tool icon in the toolbar.

Your web browser will connect to the Report Console.

Changing Report Settings

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

To change report settings:

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

The *Preferences* dialog box appears.

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

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

4 Enter the **Port number**.

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

Using the Support Generator

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

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

The Support Generator `.zip` files are saved to the installation location of Avalanche SE. The default location is `C:\Program Files\Wavelink\AvalancheSE\SUPPORT`. Once you create a `.zip` file, you can send the file to Wavelink Customer Service. Customer Service uses the `.zip` file to quickly diagnose the problem and provide a solution.

To use the Support Generator:

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

   The *Avalanche SE Support Generator* dialog box appears.

2. From the drop-down list, select the area of Avalanche SE where the problem is occurring.

3. In the **Processor** text box, enter your processor type.

4. In the **Installed RAM** text box, enter the amount of RAM you have installed.

NOTE You can not change the **Operating System** or **Free HDD Space** text boxes. These are populated by the support generator.

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

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

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

7 Click **Save**.

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

8 Make a note of the location and click **OK**.

9 Attach the `.zip` file to an e-mail and send the e-mail to `customerservice@wavelink.com`.

Using the Enabler Installation Tool

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

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

- Enabler installation packages on the machine where you are running the Console
- Mobile devices connected to the machine through Active Sync

To install an Enabler:

1 From the Quick Start tab, select the **Install Enabler** option.

The *Avalanche Enabler Install Selection* dialog box appears.

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

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

The *Enabler Configuration Tool* appears.

3 Once you configure the Enabler settings, use ActiveSync to send the Enabler to your connected mobile device.

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

Chapter 3: Managing User Accounts

Avalanche SE allows you to create different user accounts to designate users and assign specific privileges to those users. Upon installation of Avalanche SE, an Administrator account is created automatically. This account allows you to create new Administrator or Normal user accounts and restrict or allow administration of your wireless network.

NOTE Wavelink recommends that you create a new administrative user.

There are two types of user account permissions:

- **Regional Permissions**. These permissions are specific to the tasks and components of Avalanche SE. For each component you can grant read or read/write access. Read allows the user to view the configurations and settings for the component. Read/write allows the user to configure parameters and settings for the specified component. Regional permission users must also be assigned as authorized users to My Location or a site in the Navigation Window. Users that are assigned as authorized users for My Location or a site must be assigned at least one regional permission.

- **Profile Permissions**. These permissions allow the user complete global access to the specified profile. Administrators can grant read or read/write access for each type of profile. Read/write allows the user to manage all aspects of the profile, from configuration to application. Read allows the user to view the profile, but does not allow any editing.

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

- **None**. If you do not want a user to have access to any data, configurations or profiles, keep the access level at None. By default, all permissions are set to None.

- **Read/Write**. This level of access allows the user to access information and change configurations.

- **Read only**. This level of access allows the user to view the information, but does not allow the user to edit or configure any information.

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

- Software Admin

- Help Desk
- Network Admin

These user groups are set with a series of default permissions. You can modify the groups to suit your needs.

This chapter provides the following information about user accounts:

- Creating User Accounts
- Creating User Groups
- Assigning Regional Permissions
- Assigning Authorized Users
- Configuring Integrated Logon
- Changing Passwords

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 SE Console. You also assign permission levels to grant the user access to specific Enterprise and Mobile Device Server functionality.

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

- **Login**. This is the name the user will use to log in to the Avalanche SE Console.
- **Password**. This is the password that will grant access to the Avalanche SE Console. Passwords are case sensitive. The password has a 32 character limit.
- **Confirm Password**. You must confirm the password you assigned to the user.
- **First**. This is the first name of the user.
- **Last**. This is the last name of the user.

- **Type**. Select if the user is a Normal user or an Administrator. If the user is a Normal user, you will need to assign Regional or Profile permissions. If the user is an Administrator, the user will have access to the entire Console.
- **Description**. You can enter a description of the user or group.

To create a new account:

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

The *User Management* dialog box appears.

2 Click **Add**.

The *Add User or Group* dialog box appears.

3 Enter the information in the available text boxes.

NOTE The password is case sensitive.

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

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

The new account is now available and the user can log on to the Avalanche SE Console. The account is also distributed to the Mobile Device Server. If the user is set as a Normal user, that user will not have access to any areas of the Console until you assign permissions and permission levels to that user. For more information, refer to *Assigning Regional Permissions* on page 34.

Creating User Groups

You can divide users into groups, enabling you to grant the same permissions and access to several users at a time.

To create a user group:

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

The *User Management* dialog box appears.

2 Click **Add**.

The *Add User or Group* dialog box appears.

3 Select the **User Group** option.

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

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

NOTE If you have not added any single users, the list box will be empty. Refer to *Creating User Accounts* on page 32 for information about creating users.

---

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

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

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

Your user group is created. Now you should assign it some permissions. For more information about assigning permissions, refer to *Assigning Regional Permissions* on page 34.

Assigning Regional Permissions

Regional Permissions are specific to My Location and sites. To have full permissions at My Location or a site, a user must be assigned the Regional Permissions in the User Management dialog box and then be assigned as an Authorized User to My Location or a specific site. Until you assign the user, Regional Permissions assigned in the *User Management* dialog box do not take effect.

NOTE The permissions are dependent on being assigned to My Location or a site. Each permission is only granted for the location to which the user is assigned. For information about assigning users to My Location or a site, refer to *Assigning Authorized Users to Locations* on page 38.

The following table describes the regional permissions:

Regional Permission	Read_Write	Read_Only
Alert Profile	Allows you to configure Alert profiles.	Allows you to view alerts that appear in the Alert Browser.
Deployment	Allows you to create and edit deployment packages and schedule deployments to the locations you are assigned.	Allows you to view recent deployments.
Enterprise Management	Allows you to view, manage, and configure all locations to which you are assigned in the My Enterprise tree. You must have other regional permissions assigned.	Allows you to view all configurations and settings.
Mobile Device Groups	Allows you to edit mobile device groups.	Allows you to view mobile device groups.
Mobile Devices	Allows you to manage the **Mobile Device Inventory** tab and gives you rights to all the mobile device functions in the Mobile Device Details such as ping and text.	Allows you to view the Mobile Device Inventory and mobile device properties.
Mobile Device Properties	Grants you access to the Mobile Device Details dialog box allowing you to create, edit, or delete properties on the mobile device.	Allows you to view the Mobile Device Details.
Remote Control	Allows you to use Remote Control. When you enable Read_Write functionality for Remote Control, Read_Only for Mobile Devices and Mobile Device Properties is automatically enabled. This grants you full access to use Remote Control. Also allows you to configure Remote Control Connection Profiles for particular devices.	Allows you to connect to Remote Control and view mobile devices. You cannot configure Remote Control Connection Profiles.
Network Profiles	Allows you to apply and remove Network Profiles.	Allows you to view assigned Network Profiles.
Scan to Config	Grants access to the Scan to Config utility and allows you to create, manage and maintain barcode profiles and custom properties.	Allows you to view the Scan to Config utility and current barcode profiles
Server Profiles: Mobile Device	Allows you to apply and remove Mobile Device Server Profiles.	Allows you to view assigned Mobile Device Server Profiles.

Table 3-1: *Regional Permissions Explained*

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

Table 3-1: *Regional Permissions Explained*

To assign regional permissions:

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

The *User Management* dialog box appears.

2 Select the user account to which you are assigning permissions.

3 Click **Edit**.

The *Edit User* dialog box appears.

4 Click the **Regional Permissions** tab.

5 Enable the checkbox next to each permission you want to grant the user. The user will not be able to access any functions that you leave unchecked. They will not be able to see the data or modify any conditions. The profile node or tab will be blank or inaccessible.

6 For each function that you enable, you must choose Read_Write or Read_Only. The default is set to READ_WRITE, which allows the user to view and modify any settings in the area where they have permission. READ_ONLY allows the user to view all the settings at that function, but the user can not modify any of the settings.

NOTE For each component in the Regional Permissions, you must assign the user to a location (My Location or a site). Until the user is assigned to a specific location, the user will have no access to the component.

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

Assigning Profile Permissions

Profile Permissions give you global access to each profile for which you are given permission. This means that if you have permissions for Alert Profiles, you can add, configure, modify and delete as many Alert Profiles as you like. However this does not give you permission to apply the profiles to any locations. You must be assigned to My Location to apply any profiles. This table describes each of the Profile Permissions:

Profile Permission	READ_WRITE	READ_ONLY
Alert Profiles	Allows you to create, edit and delete all alert profiles.	Allows you to view alert profiles and the settings associated with the profile. However you cannot modify the profiles in any way.
Mobile Device Groups	Allows you to create, configure, edit and delete mobile device groups.	Allows you to view mobile device groups and the settings associated with the groups.
Network Profiles	Allows you to create, configure, edit and delete network profiles.	Allows you to view existing network profiles and the settings associated with those profiles.
Server Profiles (Mobile Devices)	Allows you to create, configure, edit and delete mobile device profiles.	Allows you to view existing mobile device profiles and the associated settings.
Software Profiles	Allows you to create, configure, edit and delete software profiles.	Allows you to view existing software profiles and the associated settings.
Update Profiles	Allows you to create, configure, edit and delete software profiles.	Allows you to view existing update profiles and the associated settings.

Table 3-2: *Profile Permissions*

To assign user permissions:

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

The *User Management* dialog box appears.

2 Select the user account to which you are assigning permissions.

3 Click **Edit**.

The *Edit User* dialog box appears.

4 Click the **Profile Permissions** tab.

5 Enable the checkbox next to each function that you want this user to have permission to. The user will not be able to access any functions that you leave unchecked. They will not be able to see the data or modify any conditions. The profile node or tab will be blank or inaccessible.

6 For each function that you do enable, you have the option to select whether the permission type is Read_Write or Read_Only. The default is

sent to READ_WRITE, which allows the user to view and modify any settings in the area where they have permission. READ_ONLY allows the user to view all the settings at that function, but the user can not modify any of the settings.

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

Assigning Authorized Users

You must assign users configured with Regional Permissions to a location (My Location or a site) as an authorized user. If you do not configure the user to be an authorized user for a location, that user will not be able to manage any of the assigned Regional Permissions. Users that are Normal users but not configured to manage profiles can be assigned as authorized users for specific profiles.

Assigning Authorized Users to Locations

Locations refer to both the My Location object in the Navigation window and any sites you create under the My Location level. Once you assign a user a Regional Permission in the *User Management* dialog box, you must assign the user to a specific region. Until you assign a user to a region, the user does not have any permission to perform any Regional Permission tasks. When you assign a user to a region, that user has any Regional Permissions to all regions and Locations beneath the assigned region.

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

To assign users to locations:

1 Select the site or Location.

2 Select the **My Enterprise Properties** or **My Location Properties** tab.

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

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

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

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

Assigning Authorized Users to Profiles

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

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

To add an authorized user:

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

   The *Select Profile Admin User* dialog box appears.
3. From the list, select the user.
4. From the drop-down list select **READ_WRITE** or **READ_ONLY** permission for the user.
5. Click **OK**.

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

Configuring Integrated Logon

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

When you enable the integrated login, users with network logins can log on to the Avalanche SE 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 enabled the integrated logon feature, those users configured in the console will not be allowed to access the console. The only users allowed to access the console will be those that can log in to the network.

NOTE The default **amcadmin** account is able to login with or without integrated logon enabled.

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

To enable integrated logon:

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

The *User Management* dialog box appears.

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

3 Click **OK**.

4 Log out of the Avalanche SE Console.

Avalanche SE is now configured to recognized authenticated system users.

Changing Passwords

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

To change a password:

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

The *User Management* dialog box appears.

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

3 In the **Password For** section, click **Change Password**.

The *Change User Password* dialog box appears.

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

5 Retype the password to confirm it in the **Confirm New Password** text box.

6 Click **OK**.

7 Click **OK** again to return to the Avalanche SE Console.

The new password information is now available for the Avalanche SE Console. The password also distributed to any know Locations on the network.

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

Removing User Accounts

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

To delete a user account:

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

The *User Management* dialog box appears.

2 Select a user from the list.

3 Click **Remove**.

4 Confirm you want to remove the user account.

The deleted account is removed from the Avalanche SE Console. It is also removed from any known Locations on the network.

Chapter 4: Managing Locations and Sites

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

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

- Creating Sites
- Manually Assigning Profiles
- Monitoring the Mobile Device Server

Creating Sites

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

To create a site:

1. Right-click the My Location and click **Create Site**.

   The *Add Site* dialog box appears.

2. Enter a name for the site.
3. Use the Selection Criteria Builder to configure unique selection criteria for the site group.
4. When you are finished, click **OK**.

   A site appears under the Mobile Device Server.

Viewing Mobile Devices Within Sites

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

To view the mobile devices:

1. Select the site you want to view.

2 Select the **Mobile Device Inventory** tab.

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

Pinging Mobile Devices within Sites

You can ping the mobile devices in a site simultaneously if the devices are in range and running the Avalanche Enabler, an Avalanche-enabled application, or in some cases a configuration utility.

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

To ping mobile devices

1 Right-click the site from the Navigation Window.

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

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

Sending Messages to Sites

You can send the same message to all devices in a site simultaneously.

To send messages:

1 Right-click the site from the Navigation Window.

2 Select **Send Text Message** from the menu that appears.

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

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

5 Click **OK**.

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

Editing Site Properties

Site properties retrieve the common properties from all the devices in the site. You can then add, edit, and delete properties for the site.

The properties consist of user-defined properties. Properties can be used as selection variables in selection criteria to control which devices receive particular updates.

NOTE Refer to *Building Selection Criteria* on page 164 for related information.

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

To add a property to a mobile device group:

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

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

2. Click **Add Property**.

   The *Add Device Property* dialog box appears.

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

4. Enter the name of the property in the **Property Name** text box.

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

6. Click **OK**.

   The new property is added to the properties list.

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

To edit site properties:

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

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

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

The *Edit Device Property* dialog box appears.

3 Type the new property value.

4 Click **OK**.

The edited property appears in the list.

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

To delete site properties:

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

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

2 Select the property that you want to delete and click **Delete Property**.

3 Confirm that you want to delete the property.

The **Pending Value** column for the property displays the status of the property.

4 Click **OK** to remove the property and return to the Avalanche SE Console.

The property will be deleted after the next update.

Additional Site Functions

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

The additional options for sites are as follows:

Copy

Allows you to copy the site.

Delete

Allows you to delete the site.

Mark Orphan Packages for Deletion

Marks orphaned packages on the devices within the site for deletion.

Unmark Orphan Packages for Deletion

Unmarks orphan packages for deletion.

Update Now

Allows you to update all mobile devices within that site immediately.

Manually Assigning Profiles

Profiles are automatically assigned and applied at the My Enterprise level. If you want to apply profiles manually, you can disable the auto-assign option and then apply your profiles to My Enterprise or specific sites. The profiles are applied to the mobile devices based on selection criteria for the profile and the order in which the profiles are listed in the Console.

To disable auto assign:

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

2 From the dialog box that appears, select **Server**.

3 In the **Deployment Settings** section, disable the **Auto Assign Profiles** option.

4 Click **OK** to save your changes and return to the Console.

You can now manually assign profiles.

To assign a profile:

1 Select the site you where you want to apply the profile and click the **Site Properties** tab.

NOTE If you are applying the profile to My Enterprise, select My Enterprise and click **Properties**.

2 Click **Edit**.

3 Select the applicable profile tab and click **Add**.

The *Add Profile Application* dialog box appears.

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

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

5 Configure the other options based on the type of profile you are assigning.

6. Click **OK**.

   The profile is added.

7. Continue adding profiles, if desired.
8. Use the **Move Up** and **Move Down** buttons to assign the order in which the profiles are applied to mobile devices.
9. Save your changes.

   The assigned profiles are assigned to the selected locations.

Monitoring the Mobile Device Server

If you have installed Avalanche SE on a system and deployed a Mobile Device Server, you have the ability to start and stop the server from the Avalanche SE Console.

Stopping the Server

You can stop the server from the Navigation Window of the Avalanche SE Console.

To stop a server:

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

Starting the Server

You can restart the server from the Navigation Window of the Avalanche SE Console.

To restart the server:

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

Viewing Server Properties

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

To view Server properties:

- From the Navigation Window, right-click the Mobile Device Server and select **Mobile Device Server Properties**.

Chapter 5: Managing Network Profiles

Network profiles allow you to configure the following parameters for your wireless devices:

- **Network information.** You can set network information such as gateway addresses and subnet masks for mobile devices.
- **IP addresses**. You can select the method by which mobile devices receive their IP address assignments.
- **Security encryption and authentication.** You can select the types of encryption and authentication you want your wireless devices to use.
- **Epochs**. You can assign a specific time for a network profile change to take effect by creating a network Epoch.

This section contains the following topics:

- Creating Network Profiles
- Configuring Network Profile General Settings
- Viewing Where Network Profiles Are Applied
- Adding Network Profile Authorized Users
- Network Profile Selection Criteria
- Configuring Epoch Settings
- Network Profile Configuration Descriptions

Creating Network Profiles

A network profile allows you to control network settings for all devices meeting its selection criteria.

To create a network profile:

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

The *Input* dialog box appears.

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

The new network profile appears in the **Network Profile List**. The profile will not be applied to My Enterprise until you enable it. to apply it to your devices.

Once you have created a network profile, you can edit the settings. For a complete list of network profile settings, refer to the online help which provides descriptions for each configurable field.

Configuring Network Profile General Settings

In the **General Settings** tab, you can edit the network profile name, status, IP address pools, and enable or disable the profile. For a list of general network profile settings, refer to *Network Profile General Settings* on page 59.

This section provides information about the following tasks:

- Enabling a Network Profile
- Managing IP Address Pools

Enabling a Network Profile

You must enable network profiles before they can be applied to My Location or a site.

To enable a network profile:

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

The network profile is enabled and can be assigned to My Location or a site in the console.

Managing IP Address Pools

Network profiles allow you to assign IP addresses to your wireless devices from an IP address pool. You can create IP address pools for mobile devices. The IP address pool can contain either static addresses or dynamic addresses with a Server address mask.

To add addresses to an IP address pool:

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

2 Click **Edit**.

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

The *IP Address Pools* dialog box appears.

4 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)

5 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)

6 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

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

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

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

9 Save your changes.

To delete addresses from an IP address pool:

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

2 Click **Save**.

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

The *IP Address Pools* dialog box appears.

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

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

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

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

The addresses are deleted from the list.

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

8 Save your changes.

Viewing Where Network Profiles Are Applied

The **Applied To** tab in the network profile page allows you to see exactly where a profile is directly applied. You cannot change any of the information in this tab. If you need to apply a profile to a different location than what you see in the **Applied To** tab, you will need to access the My Location Properties tabs and assign the profiles there. For information, refer to *Manually Assigning Profiles* on page 47.

The **Applied To** tab displays the following information:

- **Parent Path**. The direct path back to My Enterprise.
- **Group.** The name of My Location or the Site where the profile is applied.
- **Selection Criteria**. Any selection criteria that is applicable at My Location or the site where the profile is applied.

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

To view:

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

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

3 Click the **Applied To** tab.

The tab displays the information for the selected network profile.

Adding Network Profile Authorized Users

The **Authorized Users** tab allows you to assign administrative privileges for a specified profile to a user that has Normal user rights and is not assigned permissions to profiles. This means that any user assigned as an authorized user to a network profile will have all administrative rights for that one profile. To add an authorized user you must have at least one user configured with Normal permissions.

To add an authorized user:

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

2 Click **Edit**.

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

The *Add Authorized User* dialog box appears.

4 From the user list, select the user.

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

6 Click **OK**.

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

Network Profile Selection Criteria

Selection criteria allows you to specify which devices the network profile manages. There are two types of selection criteria: mobile device and dynamic. Mobile device criteria define which mobile devices are managed by the profile. Dynamic selection criteria are defined by Avalanche SE and apply to a device's encryption and authentication support. For detailed information about creating selection criteria, refer to *Chapter 14: Selection Criteria* on page 163.

Configuring Epoch Settings

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

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

For a list of all available settings for an Epoch, refer to *Epochs Configuration Settings* on page 60.

This section provides information about the following tasks:

- Creating Epochs
- Wireless Settings

Creating Epochs

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

To create Epochs:

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

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

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

-Or-

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

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

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

4 Click **OK**.

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

5 Edit the network settings as desired.

6 Save your changes

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

Wireless Settings

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

For a list of available settings in the **Wireless Settings** tab, refer to *Wireless Settings Tab* on page 62.

This section provides information about the following:

- Encryption Methods
- Authentication Methods

Encryption Methods

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

WEP. WEP, or Wired Equivalent Privacy, is a protocol for encrypting wireless network communications. You secure your wireless network by creating either a 40- or 128-bit WEP key which is distributed to your devices. When WEP is enabled, a device can only communicate with other devices that share the same WEP key.

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

WPA2. WPA2 is similar to WPA but meets even higher standards for encryption security. In WPA2, encryption, key management, and message integrity are handled by CCMP (Counter mode CBC-MAC Protocol) instead of TKIP. WPA2 availability is dependent on some hardware types.

Authentication Methods

Avalanche SE supports Extensible Authentication Protocol (EAP) to ensure network security. There are five types of EAP and a pre-shared key option to configure. The availability of EAP authentication is dependent on hardware types. You also must have an Enabler on the mobile device that supports authentication. Contact Wavelink Customer Service to obtain an Enabler that supports authentication.

LEAP. (Lightweight Extensible Authentication Protocol) LEAP is available when you do not already have an encryption method selected. LEAP requires both client and server to authenticate and then creates a dynamic WEP key.

PEAP/MS-CHAPv2. (Protected Extensible Authentication Protocol combined with Microsoft Challenge Authentication Handshake Protocol) PEAP/MS-CHAPv2 is available when you are using encryption. It uses a public key certificate to establish a Transport Layer Security tunnel between the client and the authentication server.

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

EAP-FAST. (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling) EAP-Fast is available when you are using encryption. EAP-Fast uses protected access credentials and optional certificates to establish a Transport Layer Security tunnel.

TTLS. (Tunneled Transport Layer Security) TTLS is available when you are using encryption. TTLS uses public key infrastructure certificates (only on the server) to establish a Transport Layer Security tunnel.

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

Network Profile Configuration Descriptions

This section provides information about the network profile settings available in each region of the **Network Profiles** tab. This information includes descriptions of each option in the following regions:

- Network Profile General Settings
- Selection Criteria Settings
- Epochs Configuration Settings

Network Profile General Settings

The following table provides information about the network profile settings in the **General Settings** tab.

Field	Description
Name	Sets the name of the profile.
Status	Sets the status of the profile as either enabled or disabled.
IP Address Pools	Enables configuration of the IP address pools.
Manage Network Settings	Enables network settings management.
Manage Wireless Settings	Enables wireless settings management.
Override Manual Settings on Mobile Devices	Enables the profile to override the manual settings on mobile devices.

Table 5-1: *General Settings*

For more information about IP address pools, refer to *Managing IP Address Pools* on page 53.

Selection Criteria Settings

The following table provides information about the network profile settings in the **Selection Criteria** tab.

Field	Description
Mobile Device Selection Criteria	Defines which mobile devices the profile will manage.
Dynamic Selection Criteria	Defines the type of encryption a device must support in order to be managed by the network profile. These criteria cannot be configured by the user.

Table 5-2: *Selection Criteria*

For information about creating selection criteria, refer to *Building Selection Criteria* on page 164.

Epochs Configuration Settings

There are two tabs in the **Epochs** region: the **Network Settings** tab and the **Wireless Settings** tab. To edit the options in these tabs, the corresponding checkbox in the **General Settings** tab must be enabled.

This section provides information about the settings in the following tabs:

- Network Settings Tab
- Wireless Settings Tab

For information about creating, editing, and deleting Epochs, refer to *Configuring Epoch Settings* on page 56.

Network Settings Tab

The following table provides information about the settings available in the **Network Settings** tab in the **Epochs** region.

Field	Description
IP Address Assignment Region	

Table 5-3: *Network Settings Tab*

Mobile Devices	Sets the method by which IP addresses are assigned to mobile devices. **Manual Assignment.** The IP address is manually configured from the device. **IP Address Pool.** A mobile device is assigned an IP address from an IP address pool. For information on creating an IP address pool, refer to *Managing IP Address Pools* on page 53. **DHCP Server.** A mobile device is assigned an IP address by a DHCP server.
Mobile Device Settings Region	
Server Address	Provides mobile devices with the server address. You can either provide the address or use the value at My Location.
Use My Location Value	Sets the mobile device to use the mask/address value of My Location.
Gateway Address	Provides mobile devices with the gateway address.You can either provide the address or use the My Location value. The gateway address is the address for the node that handles traffic with devices outside the subnet.
Subnet Mask	Provides mobile devices with the subnet mask. You can either provide the address or use the My Location value. The subnet mask determines whether a packet's destination is on the subnet.
Domain Name System (DNS)	Enables a mobile device to access a DNS server. A Domain Name System translates hostnames/domain names to IP addresses.
Domain Name	Provides mobile devices with the name of the domain where they reside.
Primary DNS	Provides mobile devices with the IP address for a primary DNS.
Secondary DNS	Provides mobile devices with the IP address for a secondary DNS (used if the primary DNS is unavailable).
Tertiary DNS	Provides mobile devices with the IP address for a tertiary DNS (used if the primary and secondary DNS are unavailable).

Table 5-3: *Network Settings Tab*

Wireless Settings Tab

The following table provides information about the settings available in the **Network Settings** tab in the **Epochs** region.

Field	Description
SSID	Provides wireless devices with the SSID. The SSID is a service set identifier that only allows communication with devices sharing the same SSID.
Encryption	Sets the type of encryption used. The following options are available from the encryption drop-down list: **Use Profile/None.** Devices do not encrypt information. **WEP.** Wired Equivalent Privacy uses either a 40- or 128-bit WEP key which is distributed to your devices. **WEP Key Rotation.** WEP key rotation employs four keys which are automatically rotated at specified intervals. **WPA (TKIP).** Wi-Fi Protected Access uses Temporal Key Integrity Protocol (TKIP) to encrypt information and change the encryption keys as the system is used. **WPA2 (CCMP).** WPA2 meets higher standards for encryption by using CCMP (Counter mode CBC-MAC Protocol) instead of TKIP. For more information about the types of encryption available with Avalanche SE, refer to *Encryption Methods* on page 57.
Encryption Settings Region	The options in this region are based on the encryption type you selected from the Encryption drop-down list.

Table 5-4: *Wireless Settings Tab*

Field	Description
Authentication	Sets the type of authentication used. The options in this drop-down are based on the encryption type you selected in the Encryption drop-down list. Not all options will appear for each selection. **None.** No authentication type is used. **LEAP.** Lightweight Extensible Authentication Protocol is available when you do not already have an encryption method selected. **EAP.** Extensible Authentication Protocol is available when you have selected an encryption method. **Pre-Shared Key (PSK).** PSK is available when you have selected an encryption method. For more information about the types of authentication available with Avalanche SE, refer to *Authentication Methods* on page 58.

Table 5-4: *Wireless Settings Tab*

Field	Description
EAP Authentication The EAP options are only available when you select WEP, WPA (TKIP) or WPA (CCMP) from the **Encryption** drop-down list.	
EAP Type	Sets the type of EAP authentication used. **PEAP/MS-CHAPv2.** Protected Extensible Authentication Protocol combined with Microsoft Challenge Authentication Handshake Protocol uses a public key certificate to establish a Transport Layer Security tunnel. **PEAP/GTC.** Protected Extensible Authentication Protocol with Generic Token Card is similar to PEAP/MS-CHAPv2, but uses an inner authentication protocol instead of MS-CHAP. **EAP-FAST.** Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling uses protected access credentials and optional certificates to establish a Transport Layer Security tunnel. **TTLS.** Tunneled Transport Layer Security uses public key infrastructure certificates (only on the server) to establish a Transport Layer Security tunnel. For more information about the types of authentication available with Avalanche SE, refer to *Authentication Methods* on page 58.
Credentials	Sets the method for sending EAP credentials. **Prompt.** When the credentials are needed, the user is prompted with a dialog box to enter the information. **Fixed.** When the credentials are needed, the information is automatically sent without prompting the user.
Username	Sets the username for EAP credential authentication
Password	Sets the password for EAP credential authentication
Confirm	Confirms the password set for EAP credential authentication
Domain	Sets the domain name for EAP credential authentication
Include Windows logon domain with username	Includes the Windows logon domain with a username when using EAP credential authentication. This prevents authentication if the Windows logon has changed, even if the username is correct.

Table 5-4: *Wireless Settings Tab*

Field	Description
Pre-Shared Key (PSK) Authentication The PSK options are only available when you select WPA (TKIP) or WPA (CCMP) from the **Encryption** drop-down list.	
Use a 8-63 character pass phrase	Sets the PSK type as a pass phrase
Use a 64 character (256 Bit) hex key	Sets the PSK type as a hex key
(pre-shared key text box)	Sets the pre-shared key
Broadcast Key Rotation Interval	Sets the time interval at which the key is broadcast
LEAP Authentication The LEAP options are only available when you select WEP, WPA (TKIP) or WPA (CCMP) from the **Encryption** drop-down list.	
Credentials	Sets the method for sending EAP credentials. **Prompt.** When the credentials are needed, the user is prompted with a dialog box to enter the information. **Fixed.** When the credentials are needed, the information is automatically sent without prompting the user.
Username	Sets the username for EAP credential authentication
Password	Sets the password for EAP credential authentication
Confirm	Confirms the password set for EAP credential authentication
Domain	Sets the domain name for EAP credential authentication
Include Windows logon domain with username	Includes the Windows logon domain with a username when using EAP credential authentication. This prevents authentication if the Windows logon has changed, even if the username is correct.

Table 5-4: *Wireless Settings Tab*

Chapter 6: Managing the Mobile Device Server

The Mobile Device Server is server software that allows you to remotely manage and configure mobile devices. Avalanche SE allows you to manage the following software and network settings of the mobile devices operating on the network:

- **Administration Settings**. These settings include licensing, user files and terminal ID generation settings. Licenses for mobile devices are frequently redistributed, providing a great deal of flexibility in managing licenses. Within the Avalanche SE Console, these settings focus on when mobile device licenses are released from an inactive mobile device, allowing that license to move to a new device.

- **Connections**. Because mobile devices are frequently connected to cradles when they are not in use, the Mobile Device Server uses COM ports to automatically detect and manage cradled mobile devices. These settings allow you to decide which COM ports the Mobile Device Servers are allowed to use.

- **Security**. Avalanche SE includes several different authentication methods to prevent unauthorized mobile devices from accessing your network.

- **Scheduling Settings**. These settings include assigning times when the mobile devices should update and setting restrictions as to when the mobile devices should not update.

There is only one Mobile Device Server profile and this section provides information about the following tasks related to the server:

- Configuring Mobile Device Server Log Files
- Suppressing Mobile Device Server Statistics
- Configuring User Files
- Viewing Where Mobile Device Server Profiles Are Applied
- Mobile Device Server Profile Authorized Users
- Releasing Licenses
- Setting the Terminal ID

- Configuring Device Connections
- Enabling Secondary Server Support
- Configuring Server Updates
- Viewing Mobile Device Server Licensing Messages

Configuring Mobile Device Server Log Files

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

The log for the Mobile Device Server is stored as a text file in the `Wavelink\AvalancheSE\` subdirectory. (The default Avalanche installation path is `c:\Program Files\Wavelink\AvalancheSE`.)

You can set the log level to the following states:

- **Critical**. This level writes the least information to the log file, reporting only critical errors that have caused the Mobile Device Server service to crash.
- **Error**. This level writes errors that are caused by configuration and/or communication problems as well as Critical messages to the log file.
- **Warning**. This level writes Critical messages, Error messages, and indicates possible operational problems in the log file.
- **Info**. This level is the default logging level and the Wavelink-recommended setting. This logging level documents the flow of operation and writes enough information to the log file to diagnose most problems.
- **Debug**. This logging level writes large amounts of information to the log file that can be used to diagnose more serious problems.

NOTE Debug mode is not recommended in a production environment unless there is a problem to diagnose. Running in Debug mode consumes considerable CPU resources.

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

To configure logging settings:

1. From the **Mobile Device Server Profiles List**, select the profile you want to configure.
2. Click **Edit**.
3. From the **Logging Sensitivity** drop-down list, select the logging level you want Avalanche SE to report.
4. In the **Max Log Size** text box, specify the maximum size (in KB) the log file should write to before saving the file and beginning a new log.
5. Save your changes.

Suppressing Mobile Device Server Statistics

You can select to suppress both radio statistics and software profile data collection for the Mobile Device Server. This will prevent any data from being written to the software profile data table and radio statistics table in the database. This helps control the amount of information that the Enterprise Server stores. You do not have to suppress both sets of statistics. Consider how much data is being collected, how often the Enterprise Server removes the statistics, and the impact of the data across your bandwidth. This will ensure an educated decision on which options to enable.

To suppress statistics:

1. From the **Mobile Device Server Profiles List**, select the profile you want to configure.
2. Click **Edit**.
3. In the **General Settings** tab, enable **Suppress Radio Statistic Data Collection** and enable **Suppress Software Profile Data Collection**.
4. Click **Save**.

Configuring User Files

The User Files setting establishes the directory path that the Mobile Device Server uses to store retrievable user files. The path will be relative to the server installation location unless an absolute path is specified, beginning with a slash (/).

To configure the user files path:

1. From the **Mobile Device Server Profiles List**, select the profile you want to configure.
2. Click **Edit**.
3. Click the **Administration** tab.
4. In the **User Files** section, enter the file path name where you want to store retrievable files.
5. Save your changes.

   Servers are updated during the next deployment.

Viewing Where Mobile Device Server Profiles Are Applied

The **Applied To** tab in the network profile page allows you to see exactly where a profile is assigned. You can not change any of the information in this tab. If you need to apply a profile to a different location than what you see in the **Applied To** tab, you will need to access the **My Location Properties** tab and assign the profiles there. For information, refer to *Manually Assigning Profiles* on page 47.

The **Applied To** tab displays the following information:

- **Parent Path**. The direct path back to My Enterprise.
- **Group.** The name of My Location or the Site where the profile is applied.
- **Selection Criteria**. Any selection criteria that is applicable at My Location or the site where the profile is applied.

To view:

1. In the Navigation Window, select **Mobile Device Server Profiles**.

2 From **Mobile Device Server Profile List**, select the network profile you want to see.

3 Click the **Applied To** tab.

The tab displays the information for the selected network profile.

Mobile Device Server Profile Authorized Users

The **Authorized Users** tab allows you to assign administrative privileges for a specified profile to a user that has Normal user rights and is not assigned permissions to profiles. This means that any user assigned as an authorized user to a profile will have all administrative rights for that one profile.

To add an authorized user you must have at least one user configured with Normal permissions. For more information about creating users and assigning permissions, refer to *Chapter 3: Managing User Accounts* on page 31.

To add an authorized user:

1 In the **Mobile Device Server Profiles List**, select the desired profile.

2 Click **Edit**.

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

The *Add Authorized User* dialog box appears.

4 From the user list, select the user.

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

6 Click **OK**.

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

Releasing Licenses

You can conserve licenses by returning them to the unused pool when a device has not contacted a server after a period of time. You can configure the period of time which must elapse before the license is released. The minimum number of days is five.

To configure license release:

1. From the **Mobile Device Server Profiles List**, select the profile you want to configure.
2. Click **Edit**.
3. Click the **Device Administration** tab.
4. In the **Licensing** section, enable the **After** option and enter the number of days after which the license should be returned.
5. Save your changes.

   The Server is updated.

Setting the Terminal ID

The Mobile Device Server assigns each device a terminal ID the first time that the device communicates with Mobile Device Server. The number the Mobile Device Server selects is the lowest number available in a range of configured numbers. Alternately, you can use C-style format to configure your own specific terminal ID.

To configure the terminal ID settings:

1. From the **Mobile Device Server Profiles List**, select the profile you want to configure.
2. Click **Edit**.
3. Click the **Device Administration** tab.
4. In the **Terminal ID Generation** section, configure the lower and upper limits for the range of terminal IDs that the Mobile Device Server will assign to mobile devices.

Alternately, configure your own method using the **Generation template** text box.

Terminal ID lower bound Specify the lowest terminal ID that the Mobile Device Server will assign a mobile device.

Terminal ID upper bound Specify the highest terminal ID that the Mobile Device Server will assign a mobile device.

Generation template (optional) Use a C-style format to allow the Mobile Device Server to assign alphanumeric IDs.

Examples:

Seattle-%d (generates IDs such as Seattle-4)

Seattle-%05d (generates IDs such as Seattle-00004)

5 Save your changes.

The Server is updated with the changes.

Configuring Device Connections

This section provides information about configuring the mobile devices, including:

- Setting COM Ports
- Enabling the RAPI Gateway
- Configuring Connection Settings
- Enabling Encryption
- Enabling Authentication

Setting COM Ports

Mobile devices that are new to the network cannot be configured via wireless connection; instead, they must be initially configured when they are physically connected to the network through a cradle. You can configure Mobile Device Servers to automatically listen for mobile devices using the COM ports on the remote system.

Only one application on a host system can maintain ownership of a COM port. If the Mobile Device Server controls the COM ports on the host system, then no other application will be able to use them. Likewise, if another application on the host system (for example, Microsoft ActiveSync) has control of the COM ports, then the Mobile Device Server will not be able to use them.

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

To establish COM port settings:

1. From the **Mobile Device Server Profiles List**, select the profile you want to configure.

2. Click **Edit**.

3. Click the **Device Connections** tab.

4. In the **Serial Communication Settings (RS232)** section, configure the serial port options.

   - Select the **Do not reserve serial ports for device management** if you do not need serial ports to manage your mobile devices.

   - Select **Reserve COM1 and COM2** to reserve those two ports for Mobile Device communication on the Servers.

   - Select **Reserve a custom defined list of ports** and click **Add** to specify which ports you want to use to manage your mobile devices.

5. Save your changes.

   The Server is updated with the changes.

Enabling the RAPI Gateway

Avalanche SE allows you to use Microsoft ActiveSync connections that exist on the system hosting the Mobile Device Server. Avalanche SE can automatically detect these connections and create a gateway that allows you to use the connection to facilitate Avalanche communication between the Mobile Device Server and a mobile device. The communication medium over which the ActiveSync session has been established does not matter; the communication medium can be serial, USB, IrDA, or RF.

To enable the RAPI gateway:

1. From the **Mobile Device Server Profiles List**, select the profile you want to configure.
2. Click **Edit**.
3. In the **Device Connections** tab, enable the **Enable the RAPI Gateway** checkbox.
4. Save your changes.

   The Server is updated with the changes.

Configuring Connection Settings

If you have your Mobile Device Server Profile configured to use a secondary server when the primary server is unavailable, you can configure the manner in which your mobile devices attempt to connect to the secondary server. You can configure the following connection settings:

- **Override Connection Settings**. When you enable this option, the Mobile Device Server Profile settings will override any connection settings configured on the mobile device.
- **Server Connect Timeout**.This option configures the number of seconds the mobile device will wait between attempts to connect to its currently configured mobile device server.
- **Server Advance Delay**. This option configures the number of seconds prior to advancing to the next secondary server.

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

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

If the mobile device cannot connect to the secondary server after the set amount of time, it will attempt to connect to the next secondary server in the list. For information about configuring and ordering secondary servers, refer to *Enabling Secondary Server Support* on page 78.

To configure time out settings:

1 From the **Mobile Device Server Profiles List**, select the profile you want to configure.

2 Click **Edit**.

3 Click the **Device Connections** tab.

4 In the **Connections** setting section, enable the **Override Connection Settings** option.

5 Enter the number of seconds you want the mobile device to wait between connection attempts in the **Server Connect Timeout** text box.

6 Enter the number of seconds you want the mobile device to attempt to connect to the secondary server in the **Server Advance Delay**.

7 Save your changes.

Enabling Encryption

When you enable mobile device transport encryption, all TCP/IP communication between the Mobile Device Server and mobile devices will be encrypted.

To enable mobile device transport encryption:

1 From the **Mobile Device Server Profiles List**, select the profile you want to configure.

2 Click **Edit**.

3 In the **Security Settings** section, enable the **Enable Mobile Device Transport Encryption** option.

4 Save your changes.

Enabling Authentication

In conjunction with Access Control Lists and WEP security measures, Avalanche SE provides additional authentication methods for mobile devices. These options require that a mobile device first connect to the network through a serial connection before being able to roam the network wirelessly.

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

Mobile device authentication employs two options:

- **Enable Mobile Device Authentication**. This option forces mobile devices to connect to the network through a wired connection (such as a cradle) and receive an authentication key. When you enable this option, the Mobile Device 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.

- **Enable Server Authentication**. This option forces mobile devices to communicate with a single known Server. As with the **Enable Mobile Device Authentication** option, this option requires that mobile devices first connect to the network through a wired connection to receive information about the Server with which they are allowed to communicate. When you enable this option, the mobile device will challenge any Mobile Device 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.

NOTE Both of these options require mobile devices to connect to the network through a wired connection to receive authentication information. Proper planning is essential to ensure that all devices can connect to the wired network when these options are enabled—otherwise, these devices might be unable to connect to the network wirelessly.

To authenticate mobile devices:

1 From the **Mobile Device Server Profiles List**, select the profile you want to configure.

2 Click **Edit**.

3 If you want to restrict mobile devices to communicate only with a single, known Server, set the following options in the **Device Communications** tab:

   - Enable the **Enable Server Authentication** checkbox.

- Set the administrative password for the Server in the *Change Server Auth Password* dialog box that appears.

4 If you want to force mobile devices to connect to the wired network and receive an authentication key before being allowed to roam the network wirelessly, set the following options in the **Device Communications** tab:

- Enable the **Enable Mobile Device Authentication** checkbox.
- Set the administrative password for the mobile device in the *Change Device Auth Password* dialog box that appears.

5 Save your changes.

Your server is updated.

Enabling Secondary Server Support

Avalanche SE allows you to configure Mobile Device Server profiles with secondary server support. This allows mobile devices to attempt to connect to a secondary Mobile Device Server if the primary server is not available. Mobile devices attempt to connect to the first server listed in the **Secondary Server** tab. If the device can not connect to that server, it will move down the server list until it is able to connect to a server. If the mobile device can not connect to any servers, it remains offline and an alert appears in the Alert Browser.

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

To add secondary servers:

1 From the **Mobile Device Server Profiles List**, select the default profile.

2 Click **Edit**.

3 Click the **Secondary Servers** tab.

4 Enable the **Enable Secondary Server Support** checkbox.

5 Click **Add**.

The *Add Secondary Server* dialog box appears.

6 Enter the host name or address of the secondary server.

7 Click **OK**.

The server is added to the list box.

8 Add as many secondary servers as you desire.

9 If you want to remove a server, select the server and click **Remove Server**.

10 Use the **Move UP** and **Move Down** buttons to set the order of the secondary servers.

NOTE Mobile devices connect to secondary servers in the order the servers are listed in the list box.

11 When you are finished adding secondary servers, save your changes.

Your Mobile Device Server Profile is now configured for secondary server support.

Configuring Server Updates

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

- **Scheduling Server Updates**. This option allows you to schedule when you want to update the Mobile Device Server software.
- **Configuring Update Restrictions**. This option allows you to assign dates and times when you do not want the server update to take place. You can also configure how many software updates can take place at the server at one time.

Scheduling Server Updates

The Avalanche SE Console allows you to update your Mobile Device Server software in a timely and efficient manner.

To schedule updates:

1 From the **Mobile Device Server Profiles List**, select the default profile.

2 Click **Edit**.

3 Click the **Update Schedule** and then **Add**.

4 In the **New Scheduled Update** section of the dialog box, select whether the event is a **One-Time** event or a **Recurring** event option.

5 If you select **Recurring Event** option, the **Recurring Period** lists become active. The first list allows you to determine whether the update occurs on either a daily or weekly basis. If you select **Weekly** from this list, the second list becomes active, allowing you to select the day on which the update occurs.

6 Configure the update start time by clicking the calendar button next to the **Start Time** text box. This button opens a calendar allowing you select the day and time on which the update begins.

7 If you want to establish an end time for this update, enable the **Use End Time** checkbox and select the date and time you want the update to end.

NOTE Selecting an end time is not required. This allows you to create events that recur indefinitely.

NOTE Once Avalanche SE begins to send data to My Location, it does not stop until all data is sent. This prevents My Location from receiving only part of the information it needs.

8 If you want the mobile device user to be able to override this update, enable the **Allow mobile device user to override the update** option.

9 If you want to remove any orphaned packages from the mobile device, enable the **Delete orphaned packages during the update** option.

As you update and modify the software installed on mobile devices, devices begin to acquire orphaned packages. Orphaned packages are parts of application files that no longer apply to applications on a mobile device. Packages will receive an orphaned status in the following cases:

- If a package has been deleted from the Avalanche SE Console.
- If a package is part of a software collection that has been disabled.
- If the package is disabled.

You can instruct the Mobile Device Server to delete any orphaned packages on mobile devices they manage.

10 If you want to synchronize the software packages, enable the **Force package synchronization during the update** option.

11 Click **OK** to close the dialog box and add the event to the **Scheduled Events** list.

The status bar indicates the settings you configured for the event. The first column represents whether the task is one-time or recurring. The second column indicates if you want the mobile device settings to override the date. The third column indicates if you selected to delete orphan packages. The fourth column indicates if you selected to synchronize the packages.

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

Configuring Update Restrictions

When you schedule updates for the Mobile Device Server, you might want to exclude specific dates and times. For example, you might want to prevent Avalanche SE from trying to update software during hours when your mobile devices are in use.

NOTE The dates and times you exclude from scheduling events apply to all events for the Mobile Device Server profile —you cannot set specific exclusion dates and times for each update.

To exclude dates and times from a scheduling event:

1 From the **Mobile Device Server Profiles List**, select the default profile.

2 Click **Edit**.

3 Click the **Update Restrictions** tab.

4 From the **Update Exclusion Window** section, enable the **Use a mobile device update exclusion window** option.

5 Using the **Prohibit updates between** lists, select the start and end times between which software updates should not occur.

6 Select the days during which these start and end times apply by enabling the check box next to the day.

For example, if you want to prevent software updates from occurring from 7:00 am to 7:00 pm from Monday through Friday, you would select 07:00 from the start time list, select 19:00 from the end time list, and enable the checkboxes for Monday, Tuesday, Wednesday, Thursday, and Friday.

7 If you want to allow any number of simultaneous updates, enable the **Allow unlimited simultaneous mobile device updates** option in the **Synchronization Exclusion Window** section.

-Or-

If you want to set the maximum number of simultaneous updates, disable the **Allow unlimited simultaneous mobile device updates** option and type the maximum number of simultaneous updates in the active text box.

Software updates require sending application package files to each mobile device. The amount of time needed to send these files depends on how large the application package files are. If you do not need to conserve bandwidth, you can allow unlimited simultaneous updates. If you want to conserve network bandwidth, you can set a maximum number of simultaneous updates that can occur.

NOTE The maximum number of simultaneous updates that you allow applies to all events for My Location or a site.

Viewing Mobile Device Server Licensing Messages

The Avalanche SE Console receives messaging licenses from the deployed Mobile Device Servers. You can view these messages from the *Server Licensing*

Messages dialog box. This dialog box provides information about My Location where the Server resides and displays licensing message.

To view licensing messages:

- From the **Tools** menu, select **Server License Messages**.

  The *dServer Licensing Messages* dialog box appears.

Chapter 7: Managing Software Profiles

A software profile is a configuration profile containing software packages. The software packages associated with the profile are installed on all devices meeting the selection criteria of the packages or profile. This chapter contains the following topics:

- Creating Software Profiles
- Managing Software Packages
- Software Profile Settings and Tables

Creating Software Profiles

When a mobile device matching the selection criteria is connected to Avalanche SE, Avalanche SE will download the software package(s) to the device. If no activation time is set, the package(s) will be installed immediately. If an activation time is set, the package(s) will be installed at the specified time. This section contains the following information:

- Adding Software Profiles
- Adding Software Profiles Using the Wizard
- Editing Software Profiles
- Viewing Where Software Profiles Are Applied
- Software Profile Authorized Users

Adding Software Profiles

You do not have to create a new profile to install software packages. You can use the default profile. However, if you want or need more organization for your packages, you can create additional profiles.

NOTE You can also create profiles using the Add Device Software Wizard that is launched from the **Quick Start** tab. Click the **Quick Start** tab and select **Add Device Software** to begin the wizard. For more information refer to Adding Software Profiles Using the Wizard

To add a software profile:

1 From the Navigation Window, select **Software Profiles**.

The **Software Profiles** tab appears.

2 Click **Add Profile**.

The *Input* dialog box appears.

3 Type the name of the new software profile and click **OK**.

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

The new profile is added to the **Software Profile List** and will be applied to My Enterprise.

Adding Software Profiles Using the Wizard

You can add software profiles from the software profiles tab or using the Add Device Software Wizard. The following steps are instructions for using the wizard.

To add a software profile:

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

The *Add Device Software Wizard* launches.

2 In the **Create a New Software Profile** text box, enter the name of the profile and then click **Next**.

Your software profile is created. The following steps in the wizard are optional. If you only want to create the profile and not configure any options, click **Finish**. Your profile appears in the software profiles tab. If you want to configure, continue with the wizard.

3 In the **Configure Software Profile** dialog that appears, you can enable the profile and configure selection criteria.

4 Click **Next**.

5 In the **Select a Software Package** to add, you can add, create or copy a package to the profile. For information about all these options refer to *Installing Software Packages* on page 90.

6 Click **Next**.

7 Enable and configure selection criteria for the packages you added to the profile.

8 Click **Finish**.

Your configured profile with the installed packages will appear in the Software Profiles tab.

Editing Software Profiles

Once a software profile has been created, you can edit the name, status, type, and selection criteria. For a complete list of software profile settings, see *Software Profile General Settings* on page 98.

This section contains information about the following:

- Enabling Software Profiles
- Software Profile Selection Criteria

Enabling Software Profiles

A software profile can have its status set to enabled or disabled. The profile must be enabled before you can apply it to mobile devices.

To enable a software profile:

1 In the **Software Profiles** tab, select the desired profile from the **Software Profile List**.

2 Click **Edit**.

3 In the **General Settings tab**, select the **Enabled** option to enable the profile.

4 Save your changes.

The profile status displays in the **Software Profile List** and the profile will be applied to My Enterprise.

Software Profile Selection Criteria

Selection criteria determine which mobile devices receive the software profile. For information about creating selection criteria for software profiles, refer to *Building Selection Criteria* on page 164.

Viewing Where Software Profiles Are Applied

The **Applied To** tab in the network profile page allows you to see exactly where (Location or site) the profile is applied. You can not change any of the information in this tab.

The **Applied To** tab displays the following information:

- **Parent Path**. The direct path back to My Enterprise.
- **Group.** The name of My Location or Site where the profile is applied.
- **Selection Criteria**. Any selection criteria that is applicable at My Location or the site where the profile is applied.

To view:

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

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

3 Click the **Applied To** tab.

The tab displays the information for the selected network profile.

Software Profile Authorized Users

The **Authorized Users** tab allows you to assign administrative privileges for a specified software profile to a user that has Normal user rights and is not assigned permissions to software profiles. This means that any user assigned as an authorized user to a software profile will have all administrative rights for that one software profile.

To add an authorized user you must have at least one user configured with Normal permissions. For more information about creating users and assigning permissions, refer to *Chapter 5: Managing User Accounts* on page 63.

To add an authorized user:

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

2 Click **Edit**.

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

The *Select Software Profile Admin User* dialog box appears.

4 From the drop-down list, select the user.

5 Click **OK**.

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

6 Save your changes and the profile will be applied to My Enterprise.

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 SE Console. Each software package is usually pre-assigned with default selection criteria.

Software packages can be one of the following package types:

- **Application packages**. These packages are added to the **Application** menu in the mobile device.

- **Support packages**. These packages contain updates to existing software packages or to the Avalanche Enabler. Support packages do not appear as new items under the **Application** menu of the mobile device.

- **Auto Run packages**. These packages automatically execute following a successful download. Like the support packages, auto run packages do not modify the **Application** menu. RF firmware upgrade packages are examples of auto packages.

- **Enabler Update Kits**. These packages allow for automatic updates to the Enablers installed on your devices. These packages are only used with a normal software profile, *not* with an Enabler software profile.

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

This section includes the following information:

- Installing Software Packages
- Configuring Software Packages Settings
- Configuring Software Packages for Delayed Installation

Installing Software Packages

Once you create a software profile or if you are using the default profile, you can install the software packages to that profile. Through the software profile you can configure the software package settings and then deploy the packages to specific mobile devices.

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

NOTE You can also install software packages using the Add Device Software Wizard launched from the **Quick Start** tab. Click the **Quick Start** tab and select **Add Device Software** to begin the wizard.

You can install packages or create custom software packages from the Avalanche SE Console using the Add Device Software Wizard. Before you create a custom package, ensure you know the location of all the files you want to include and ensure that the files are valid.You can perform the following tasks in the Add Device Software Package Wizard:

- **Install an Avalanche Package File**. Browse to the location on your machine where you store Avalanche package files.
- **Create a new package**. Build your own software package using files on the local machine.

- **Copy a package**. Copy an existing software package that is installed on Avalanche SE.

Using the Add Package wizard, you can also enable and configure the installed, created or copied software package.

Installing an Avalanche Software Package

Use the following steps to install an Avalanche software package. You must know the location on the local machine of the package.

To install an Avalanche software package:

1 Select the desired profile from the **Software Profiles List**.

2 In the **Software Packages** tab, click **Add Package**.

The *Create Software Package* dialog box appears.

3 Select **Add an Avalanche software package** and browse to the location of the software package.

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

A *License Agreement* dialog box appears.

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

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

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

7 If you want to configure your software package, double-click the configuration tool you want to launch.

8 When you are finished configuring, click **Next** to add another software package or **Finish** to complete the installation.

Building New Software Packages

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

To build a new package:

1. Select the desired profile from the **Software Profiles List**.
2. In the **Software Packages** tab, click **Add Package**.

   The *Create Software Package* dialog box appears.
3. Select **Create an ad hoc package**.
4. Enter a package name in the text box (limit eight characters) and click **Next**.

   The *Specify the Files* dialog box appears.
5. Click **Add** and browse to the location of the files you want to add to the package.
6. Select the files and click **Open**.

   The file path location appears in the text box.
7. Click **Next**.

   The *Ad Hoc Package Options* dialog box appears.
8. Configure the following options:

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

NOTE These settings are all optional unless you select to run a program. Then you are required to select which program you want to run.

9 Click **Next.**

The *Add Selection Criteria* dialog box appears.

10 If you want to configure Selection Criteria for the package, enable **Add Selection Criteria** and enter the information in the text box.

NOTE Configuring Selection Criteria is optional.

11 Click **Next**.

The package begins installing.

12 When the installation is complete, click **Next**.

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

13 If you want to configure your software package, double-click (or right-click) the configuration tool you want to launch.

14 When you are finished configuring, click **Next** to add another software package or **Finish** to complete the installation.

Copying a Software Package

From the Add Package wizard you can copy a previously installed software package. The wizard gives you the same functionality as right-clicking a software package in the software packages.

To copy a software package:

1 From **Software Profiles > Software Packages** tab, click **Add Package**.

The *Create Software Package* dialog box appears.

2 Select **Copy an already installed package**.

Any packages you have installed will appear in the text box.

3 Select which package you want to copy and click **Next**.

4 In the dialog box that appears, select the profile to which you want to copy the package or select **Create a new software profile** and enter a name for the profile.

5 Click **Next** and the package will copy to the software profile you selected or created.

6 When the copy is complete, click **Next**.

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

7 If you want to configure your software package, double-click (or right-click) the configuration tool you want to launch.

8 When you are finished configuring click **Next** to add another software package or **Finish** to complete the installation.

Configuring Software Packages Settings

Once a software package has been installed, you can perform several tasks, including:

- Configuring Software Packages
- Copying Software Packages
- Enabling Software Packages
- Moving Software Packages

Configuring Software Packages

Some software packages come with options that should be configured before the packages are installed on a mobile device. These options are configured from the Avalanche SE Console. Configuration options will differ based on the software package you are configuring.

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

To configure a software package:

1 Select the desired profile from the **Software Profiles List**.

2 From the **Installed Software Packages** section of the **Software Profiles** tab, select the package you want to configure.

3 Click **Configure**.

The *Configure Software Package* dialog box appears.

4 From the available list, edit the configuration options for the package.

NOTE Configuration details are specific to the type of software package. For details about configuring software packages, refer to the specific user's manual for that product.

5 When the options are configured, click **OK**.

The software package is configured and will apply to My Enterprise.

Copying Software Packages

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

To copy a software package:

1 Select the desired profile from the **Software Profiles List**.

2 Click **Edit**.

3 From the **Installed Software Packages** section of the **Software Profiles** tab, select the package you want to copy.

4 Click **Copy**.

The *Copy Software Package* dialog box appears.

5 From the drop-down list, select the profile you want to contain the software package and click **OK**.

The package is copied to the destination profile.

Enabling Software Packages

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

To enable a software package:

1. From the **Installed Software Packages** section of the **Software Profiles** tab, select the package you want to enable.
2. Click **Edit**.
3. Click **Enable**.
4. From the **File** menu, select **Save**.

   The profile's new status shows in the **Installed Software Packages**.

Moving Software Packages

A software package and its configuration can be moved from one software profile to another.

To move a software package:

1. From the **Installed Software Packages** section of the **Software Profiles** tab, select the package you want to move.
2. Click **Edit**.
3. Click **Move**.

   The *Move Software Package* dialog box appears.

4. Select the profile the package will be moved to from the drop-down list and click **OK**.

   The package is moved to the destination profile.

Configuring Software Packages for Delayed Installation

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

Delayed package installation provides flexible control over when you want the mobile device to install software packages.

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

Package activation is supported in Enabler version 4.1 and later.

To configure a software package for delayed installation:

1. From the **Installed Software Packages** section of the **Software Profiles** tab, select the package you want to configure.
2. Click **Edit**.
3. In the **Package Activation** section, enable the **Use an Activation Time** checkbox.
4. Click the **Calendar** button to select a date and time for the package to be installed on the device.

   The *Select a date and time* dialog box appears.
5. Select a date and time for the package installation and click **OK**.
6. If you want the device user to have the option to override the software package installation at the activation time, enable the **Allow Device User to Override** checkbox.

   If the user chooses to override the installation, they will be prompted to choose another time to install.
7. Save your changes.

Software Profile Settings and Tables

This section provides information about the settings and tables in the **Software Profiles** tab, including:

- Software Profile List
- Software Profile General Settings

- Installed Software Packages

Software Profile List

The **Software Profile List** displays information about your software profiles.

Field	Description
Name	Displays the name of the software profile.
Type	Displays the type of the software profile.
Status	Displays the enabled/disabled status of the software profile.
Selection Criteria	Displays the selection criteria used to apply the software profile.

Table 7-1: *Software Profile List*

Software Profile General Settings

The following table provides information about the software profile settings in the **General Settings tab**.

Field	Description
Name	Sets the name of the profile.
Status	Sets the status of the profile as either enabled or disabled.
Profile Type	Sets the type of the profile as either Normal or Enabler.

Table 7-2: *General Settings*

Installed Software Packages

The following table provide information about the **Installed Software Packages** region in the **Software Profiles** tab.

Field	Description
Name	Displays the name of the software package.
Status	Displays the enabled/disabled status of the software package.
Type	Displays the type of the software package.
Version	Displays the version of the software package.
Vendor	Displays the vendor associated with the software package.
Title	Displays the title of the software package.

Table 7-3: *Software Packages*

The **Installed Software Packages** region also includes the following regions:

- Package Activation
- Package Tracking
- Package Selection Criteria
- Package Distribution

Package Activation

The following table displays the software package options in the **Package Activation** region.

Field	Description
Use an Activation Time	Enables an activation time for the software package installation on the mobile device.
Activation Time	Sets the activation time for the software package installation on the mobile device.
Allow Device User to Override	Enables the device user to override the package installation at the time of activation.

Table 7-4:

Package Tracking

The following table displays the information included in the **Package Tracking** region.

Field	Description
Installation	Displays the date/time of package installation and the user who installed the package.
Last Configured	Displays the date/time of the last configuration and the user who performed the configuration.

Table 7-5: *Package Tracking*

Package Selection Criteria

Package selection criteria are determined by Avalanche SE. You cannot change the package selection criteria.

Package Distribution

The following table provides descriptions of the configuration options in the **Package Distribution** tab.

Field	Description
Enabled Cached Peer to Peer Package Distribution	Enable this option to allow the profile to be shared across multiple devices via peer to peer connections. When deployed to a mobile device, the profile will then be available for other mobile devices to receive the profile from that store mobile device.
Do Not Allow Non-Package Store Devices To Begin Updating Until	Enable this option to configure the time at which a non-package store mobile device can contact a package store device to update and receive this profile. A non-package store device refers to a mobile device that is not being used to update other mobile devices. Configuring the timing for profile updates allows you to control and conserve bandwidth.
Do not allow server to update non-Package Store Devices until	Enable this option to configure the time at which a non-package mobile device can contact the Mobile Device Server to update and receive this profile. Once the configured time is reached, the mobile devices will first attempt to contact a package store device to receive the update. If the a package store device cannot be contacted or the connection times out, the device will then attempt to contact the Mobile Device Server. A non-package store device refers to a mobile device that is not being used to update other mobile devices. Configuring the timing for profile updates allows you to control and conserve bandwidth.

The following table provides information about the results that will occur with the different configurations in the **Package Distribution** tab. The table assumes that the first option (**Enable Cached Peer to Peer Distribution**) is enabled. Emphasis is placed on the configurations which allow the mobile devices to receive the updates.T

If	Then Package Store Devices	And Non-Package Store Devices
Do Not Allow Non-Package Store Devices To Begin Updating Until is enabled and the configured time has not been reached (**Do Not Allow Server to Update Non-Package Store Devices Until** is not enabled).	*Can* contact the Mobile Device Server for updates at any time.	Cannot cannot contact any package store devices. Will attempt to contact the Mobile Device Server to receive the updates.
Do Not Allow Non-Package Store Devices To Begin Updating Until is enabled and the configured time has been reached (**Do Not Allow Server to Update Non-Package Store Devices Until** is not enabled).	*Can* contact the Mobile Device Server for updates at any time.	*Can* contact package store devices to update and receive the profile. If the device cannot contact a package store device, it will attempt to contact the Mobile Device Server.
Do Not Allow Non-Package Store Devices To Begin Updating Until is enabled and **Do Not Allow Server to Update Non-Package Store Devices Until** is enabled and the configured time has not been reached	*Can* contact the Mobile Device Server for updates at any time.	Cannot contact the Mobile Device Server for updates Cannot contact any package store devices

Table 7-6: *Configuration Results for Package Distribution*

If	Then Package Store Devices	And Non-Package Store Devices
Do Not Allow Non-Package Store Devices To Begin Updating Until is enabled and (**Do Not Allow Server to Update Non-Package Store Devices Until** is enabled and the configured time has been reached	*Can* contact the Mobile Device Server for updates at any time.	*Can* contact package store devices to receive updates If the device cannot contact a package store device or the connection times out, the device *can* contact the Mobile Device Server to receive updates.
No options are enabled	*Can* contact the Mobile Device Server for updates at any time	*Can* contact package store devices or Mobile Device Server for updates at any time

Table 7-6: *Configuration Results for Package Distribution*

Chapter 8: Managing Mobile Devices

This section provides information about the following mobile device topics:

- Mobile Device Inventory Tab
- Managing Device Filters
- Viewing Mobile Device Details
- Configuring Mobile Device Properties
- Software Inventory
- Controlling the Mobile Device
- Device Statistics

Mobile Device Inventory Tab

The **Mobile Device Inventory** tab lets you view all the devices (and device status) currently associated with Avalanche SE.

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

Device Name This column will display the friendly name of the mobile device. You can use the device name for filtering and selection criteria. If the friendly name is not available, the model name of the device will appear in brackets. You will not be able to use the model name for filtering or selection criteria.

Terminal ID The unique ID automatically generated by Avalanche SE.

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

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

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

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

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

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

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

Because the image data is transferred from the mobile device to the Mobile Device Server, to the Enterprise Server and finally to the Console, there may be a temporary delay in the display of the device images. No device images will display until the icons are available at the Console. Once the icons become available, they will display the next time the inventory list is loaded or refreshed. The icons will display in the *Mobile Device Details* dialog box the next time it opens.

Enablers that support this must make two icons available to the console. The large icon must be a `.png` image. It is recommended that the small icon be `.png` image as well. For more information about custom device icons, refer to *Using Custom Device Icons in Avalanche SE*, located on the Wavelink web site.

For information about modifying the columns in the **Mobile Device Inventory** tab, refer to the online help file included with the product.

Managing Device Filters

This section contains the following information:

- Creating Device Filters

- Applying Device Filters
- Deleting Device Filters

Creating Device Filters

To display specific devices in the **Mobile Device Inventory** tab, you must first create a new filter.

To create a filter:

1. From the **Mobile Device Inventory** tab, click **Edit Filters**.

   The *Modify Mobile Device Filters* dialog box appears.

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

3. Click the **Selection Criteria** button.

   The *Selection Criteria Builder* dialog box appears, allowing you to create a filter based on a variety of mobile device characteristics. See *Building Selection Criteria* on page 276 for more information.

4. When you are finished building a filter, click **OK** to return to the *Modify Mobile Device Filters* dialog box.

   The filter appears in the **Filter Expression** text box.

5. Click **Add Filter.**

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

6. Click **OK**.

   You can now select the filter from the **Current Mobile Device Filter** list located at the top of the **Mobile Device Inventory** tab.

Applying Device Filters

After you create device filters, you must apply them to the Mobile Device Inventory list. After the filter is applied, only the devices matching the selection criteria of the filter will appear in the Mobile Device Inventory list.

To apply filters:

1. Select the filter from the **Current Mobile Device Filter** list.

2 Click **Apply Filter**.

Deleting Device Filters

If you decide that a filter is no longer necessary, you can delete that filter from the Avalanche SE Console.

To delete a filter:

1 Select a filter from the **Current Mobile Device Filter** list.

2 Click **Edit Filter**.

The *Modifying Mobile Device Filters* dialog box appears.

3 In **Existing Filters**, select the filter you want to delete.

4 Click **Delete**.

Displaying Devices

The paging functionality displays the number of devices you select to view per page in the order Avalanche SE pulls those devices from database. If you attempt to page through a selected number of devices and have a device filter applied, you may not see all of your devices that match the filter. This is because Avalanche SE displays the first 25 or 50 devices, and then applies the filter. If there are devices in the list that do not match the filter, those devices are removed from the list. The next number of matching devices is not automatically pulled into the view. You will need to page through the list to view other filtered devices.

To configure device list paging:

1 From the **Number of Devices Per Page** drop-down list, select the number of devices you want to display.

2 Use the arrow keys to move forward and backward through the pages.

3 Use the refresh button to refresh the list of mobile devices.

Viewing Mobile Device Details

The *Mobile Device Details* dialog box provides device-specific information and consists of the following sections:

- **Summary**. This section provides a quick summary of device, health, and battery life information.

  The Health Data icon will display red, yellow or green depending on the health of the device. Health is based on several different things. The following provides information about the different states of the device:

  Green. If the device health icon reports a green status there are no issues with the device. Packages are installed. Battery level, signal strength, signal quality and disk space all meet the specified threshold.

  Yellow. If the device health icon reports a yellow status, it could mean any of the following:

  - The battery level has dropped below the minimum threshold (default 20% of battery life left). You can configure the threshold based on your requirements.
  - The signal strength or signal quality has dropped below the minimum threshold. Default is set at two bars.
  - There are software packages that are not completely installed (could be pending or currently installing).
  - The disk space has reached the minimum threshold. The program memory and flash memory (a defined flash drive location) both have a default of 5% threshold.

  Red. If the device health icon reports a red status, the device is in a critical state. This could mean any of the following:

  - The battery level has dropped below the minimum threshold (default 5% of battery life left).
  - The signal strength and signal quality have dropped to only one bar.
  - A software package has returned an error and cannot be installed.
  - The device is in danger of running out of disk space or there is no disk space left.

- **Activity**. This section provides current status information and the time and date the mobile device was last contacted.

- **Device Tabs**. This section provides access to the following tabs:
  - **General**. The **General** tab provides general network and wireless information about the device.
  - **Installed Software.** The **Installed Software** tab provides information about the software applications installed on the device. For details, refer to *Software Inventory* on page 112.
  - **Packages**. The **Packages** tab lists all the packages currently available for the device and the status of each package. You can view software packages and the current state of each software package associated with the mobile device.
  - **Properties**. The **Properties** tab lists the properties of the device and their values. This tab also allows you to add properties and values. For details about the tasks you can perform in the **Properties** tab, refer to *Configuring Mobile Device Properties* on page 108.
  - **Device Control**. The **Device Control** tab provides options for updating the mobile device, sending text messages, pinging the device, using Remote Control, and connecting to the Session Monitor. For details, refer to *Controlling the Mobile Device* on page 112.

To view Mobile Device Details:

- Right-click the mobile device you want to view and select **Mobile Device Details**.

Configuring Mobile Device Properties

Mobile device properties consist of pre-defined and user-defined properties. User-defined properties can be associated with individual mobile devices or with mobile device groups. Pre-defined properties are device-specific and dependent on the version of the Avalanche Enabler running on the mobile device. Properties can be used for selection criteria in addition to the selection variables. See *Building Selection Criteria* on page 276 for more information.

From the **Properties** tab, you can perform the following tasks:

- Viewing Properties
- Creating User-Defined Properties

- Creating Device-Side Properties
- Editing Properties
- Deleting Properties

Viewing Properties

You can view the properties associated with a specific mobile device.

To view the properties:

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

   The columns that appear in this dialog box are as follows:

Name The name of the property.

Value The value of the property.

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

Icon Indicates whether the property is static, snapshot, or configurable data.

Understanding Wireless Properties

Wireless properties are properties that the device reports and are then sent to the Enterprise Server. Any property with a `wles` prefix is considered a wireless property and will be saved to the database.

Understanding Real-Time Properties

Avalanche SE gathers real-time properties from the mobile devices it contacts. These statistics are reported to the Console every five minutes. They are not saved to the Mobile Device Server or the Enterprise Server.

Creating User-Defined Properties

Avalanche SE provides the ability to create user-defined properties on the mobile devices. These properties can then be used to build selection criteria for software updates.

You can add user-defined properties to individual mobile devices or to mobile device groups. When you add a property to a group, it is added to all mobile devices that are members of the group.

Once you create a custom property, you can then use that property in the **Mobile Device Inventory** tab.

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

To create user-defined properties:

1 From the **Mobile Device Inventory** tab, right-click the device you want to view and click **Mobile Device Details**.

2 Click the **Properties** tab.

3 Click **Add Property.**

4 From the drop-down list, select what type of property you want to add.

5 Type the name and the value of the property in the **Property Name** and **Property Value** text boxes.

6 Click **OK**.

The property is added to the list in the **Properties** tab under the chosen heading.

Creating Device-Side Properties

You have the ability to create property files on the mobile device and then use those files to collect device-specific information and display this information in the **Properties** tab.

A properties file is a plain-text file with an arbitrary or generic name followed by the `.prf` extension. The plain-text file contains key-value pairs that represent properties. The Avalanche Enabler reads the keyvalue pairs and transfers them to Avalanche SE as properties for the mobile device. These properties are displayed in the **Properties** tab of the *Mobile Device Details* dialog box.

A properties file must:

- Have a unique name
- Have a `.prf` extension
- Contain a vendor entry
- Contain only one unique key-value pair per line
- Mark supplemental, inconsequential text with the appropriate comment delimiters

Avalanche SE uses the vendor name to organize user-defined properties. The **Properties** tab in the *Mobile Device Details* dialog box displays the device-side properties that it has collected from the mobile device. Each property that displays is prefaced with the vendor name that is specified in the properties file from which Avalanche SE obtained the property. A period (.) separates the vendor name and the property.

For more information about creating device-side properties, please contact Wavelink Customer Service.

Editing Properties

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

User-defined properties can be edited either for a specific mobile device or for a group of devices using the group property editor.

To edit a property for a mobile device:

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

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

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

5 Click **OK**.

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

Deleting Properties

You can delete any configurable mobile device property from the selection criteria builder.

To delete a property:

1 From the **Mobile Device Inventory** tab, right-click the device you want to view and click **Mobile Device Details**.

2 Click the **Properties** tab.

3 Select the property that you want to delete and click **Delete Property**.

4 Click **OK**.

Software Inventory

This section provides information about the **Installed Software** tab. The **Installed Software** tab consists of two parts:

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

Controlling the Mobile Device

This section provides information about the following tasks that you can perform from the **Device Control** tab or by right-clicking the mobile device:

- Pinging Mobile Devices
- Sending Messages
- Updating the Mobile Device
- RAPI Gateways
- Using Remote Control
- Launching the Session Monitor

Pinging Mobile Devices

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

To ping the client:

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

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

Sending Messages

You can send a text-based message to clients that are currently in range and running the Avalanche Enabler, an Avalanche-enabled application or, in some cases, a configuration utility.

To send a message:

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

The *Send Text Message* dialog box appears.

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

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

6 Click **OK**.

The **Status** field in the **Activity** section displays the status of the text message request.

Updating the Mobile Device

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

NOTE The rules that govern which mobile devices can receive a particular update are determined by the selection criteria. See *Building Selection Criteria* on page 276 for more information.

To update a mobile device:

1 From the **Mobile Device Inventory** tab, right-click the device you want to view and click **Mobile Device Details**.

2 Click the **Device Control** tab.

3 Double-click the **Update Now** icon.

The *Update Now* dialog box appears.

4 Enable the **Allow User to Override the Update** option if you want to give the mobile device user the option to override the update.

5 Enable the **Force Package Synchronization** option if you want to force the package to update the device.

6 Enable the **Delete Orphan Packages** option if you want to remove orphan packages from the mobile device.

7 Click **OK**.

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

NOTE Many mobile devices incorporate a sleep function to preserve battery life. If a device is asleep, you must “wake” it before it can receive a “pushed” update from Avalanche SE. 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.

Deleting Mobile Devices

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

To delete mobile devices:

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

  The device is removed.

RAPI Gateways

Avalanche SE allows you to use Microsoft ActiveSync connections that exist on the system that hosts the Mobile Device Server. Avalanche SE can automatically detect these connections and create a gateway that allows you to use the connection to facilitate communication between the Mobile Device Server and a mobile device. The communication medium over which the ActiveSync session has been established does not matter; the communication medium can be serial, USB, IrDA, or RF.

Using Remote Control

Remote Control functionality is only available for devices that have a licensed Remote Control package installed in Avalanche SE. Remote Control is not functional, until you complete the following tasks:

1. Obtain and install the Remote Control software package.
2. License the Remote Control program.
3. Deploy the Remote Control software package to your mobile device.

Once deployed, you can use Remote Control. For detailed information about all tasks regarding Remote Control, including connecting to a mobile device and accessing various components of the device, refer to the *Wavelink Avalanche Remote Control User's Guide*.

Launching the Session Monitor

The Session Monitor utility allows you to view the Telnet Client on a mobile device from the Avalanche SE Console. The Session Monitor includes an override feature that can take control of the Telnet Client on the mobile device and a logging feature that creates a trace for Telnet sessions. To use the Session Monitor with Avalanche SE, you will need perform the following tasks:

- Obtain and install a Telnet 5.x (or later version) software package.
- Configure the Telnet Client software package.
- Deploy the Telnet Client to the mobile device.
- Launch the Telnet Client on the mobile device and then launch Session Monitor.

For detailed Telnet installation and configuration information, refer to the *Wavelink Telnet Client User's Guide*.

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

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

1. Ensure you have installed and configured a Telnet package.
2. Select My Location or a site from the Navigation Window.
3. Click the **Mobile Device Inventory** tab.
4. Right-click the device on which you want to launch the Session Monitor and select **Session Monitor** from the menu.

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

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

1 Ensure you have installed and configured a Telnet Client software package.

2 Select My Location or a site from the Navigation Window.

3 Click the **Mobile Device Inventory** tab.

4 Open the *Mobile Device Details* dialog box.

- Double-click the mobile device on which you want to launch session monitor.

-Or-

- Right-click the mobile device on which you want to launch session monitor and select **Mobile Device Details**.

5 Click the **Device Details** tab.

6 Double-click the **Session Monitor** icon.

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

Device Statistics

The Enabler collects various device statistics and writes them to a file for later upload to the Device Server. The following `_DEVPROP.PRF` properties have been defined to help configure the frequency of gathering and reporting statistics to the Device Server:

Reporting.Stats.Enabled	0-Disable, 1-Enable	Default-1
Reporting.Stats.GatherInterval	0-n, Expressed in minutes	Default-10 min.
Reporting.Stats.ReportInterval	0-n, Expressed in hours	Default-24 hours
Reporting.Stats.ReportFileSize	0-n, Expressed in KB units	Default-512 KB
Reporting.MinimumLinkSpeed	Expressed in KB/sec.	Default-188 KB/s

- **GatherInterval** is how often to take a snapshot of the statistics.

- **ReportInterval** is how often to have the file uploaded to the Device Server for reporting.

- If **GatherInterval** or **ReportFileSize** is set to 0, this has the effect of setting **Enabled** to 0.
- **MinimumLinkSpeed** is used to limit the upload to connections that meet the specified link speed only.
- **ReportFileSize** is used to limit the size of the statistics file on the device. Once this threshold is reached, the oldest records will be deleted to make room for new records to be added.

You can view the values for the preceding properties under **Reporting** in the **Properties** tab of the *Mobile Device Details* dialog box. See *Configuring Mobile Device Properties* on page 108 for related information.

The Enabler will also inventory all installed software packages and (for WindowsCE) all `.eve` files on the device. Since this can be a time consuming operation, the inventory collection is done in the background. Unlike device statistics, the frequency is not configurable. Every 24 hours a new software inventory file is created. The following `_DEVPROP.PRF` properties are used to configure inventory collection:

Reporting.Software.Enabled	0-Disable, 1-Enable	Default-1
Reporting.MinimumLinkSpeed	Expressed in KB/sec.	Default-188 KB/s

Chapter 9: Managing Mobile Device Groups

To better organize your wireless network, you can use the Avalanche SE Console to create collections of mobile devices, called mobile device groups. These groups allow you to manage multiple devices simultaneously, using the same tools available for managing individual mobile devices. Mobile devices can be members of multiple mobile device groups.

The topics in this section include:

- Creating Mobile Device Groups
- Adding Mobile Device Group Authorized Users
- Pinging Mobile Devices within Mobile Device Groups
- Sending Messages to Mobile Device Groups
- Editing Properties for Mobile Device Groups
- Additional Mobile Device Group Functions

Creating Mobile Device Groups

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

If you disable a mobile device group, the group is removed. This section provides information about creating static groups and dynamic groups.

Creating Static Mobile Device Groups

A static mobile device group is essentially a snapshot of all the mobile devices in your inventory that match a set of configured selection criteria.

When you create a static group, you configure the selection criteria for the group to determine which devices you want to add to the group. Avalanche SE retrieves those devices currently listed in the Mobile Device Inventory list that have properties matching the selection criteria.

If a new device with properties that match the selection criteria for that mobile device group connects to the Avalanche SE Console, it will not automatically be placed in the mobile device group. You will need to manually add any new devices to the group. For information about manually assigning a mobile device to a group, refer to *Adding Devices to Static Mobile Device Groups* on page 120.

To create a static device group:

1 Right-click the **Mobile Device Groups** node in the Navigation Window and select **New Mobile Device Group.**

The *New Mobile Device Group* dialog box appears.

2 Type a name for the group.

3 To enable the group, select **Enabled** from the drop-down list.

4 Enable the **Static** option.

5 Click **OK**.

The group appears below the **Mobile Device Groups** icon.

Adding Devices to Static Mobile Device Groups

Once you create a static mobile device group, you can configure the selection criteria for that group and then add devices with properties matching that selection criteria to the group.

To add mobile devices to a static mobile device group:

1 From the Navigation Window, select the static group.

2 Right-click and select **Properties**.

The *Mobile Device Group Properties* dialog box appears.

3 Click the **Selection Criteria** button to open the Selection Criteria Builder and then create your selection criteria.

-Or-

Manually type selection criteria into the text box.

For information about building selection criteria, refer to *Building Selection Criteria* on page 164.

4 When you have finished creating the selection criteria, click **Add Matching Devices to Group**.

Avalanche SE locates the matching devices that currently exist in the Mobile Device Inventory list and adds them to the group.

Removing Devices from Static Mobile Device Groups

You cannot remove individual mobile devices from a static group. If you want to make changes to a static mobile device group, you must first remove all current devices from the group. Next, modify the selection criteria as desired, and add the appropriate mobile devices back into the group.

Creating Dynamic Mobile Device Groups

When you create a dynamic group, you configure the selection criteria for the group to determine which devices you want to add to the group. Avalanche SE retrieves those devices currently listed in the Mobile Device Inventory list that have properties matching the selection criteria. If a new device that has properties matching the selection criteria for that mobile device group connects to the Avalanche SE Console, that device is automatically placed in the mobile device group. Therefore, dynamic mobile device groups can be constantly adding and removing mobile devices based on the selection criteria assigned to that group.

To create a dynamic device group:

1 Right-click the **Mobile Device Groups** node in the Navigation Window and select **New Mobile Device Group.**

The *New Mobile Device Group* dialog box appears.

2 Type a name for the group.

3 To enable the group, select **Enabled** from the drop-down list.

4 Enable the **Dynamic** option.

5 Click the **Selection Criteria** button to open the Selection Criteria Builder.

-Or-

Manually type selection criteria into the text box.

For information about building selection criteria, refer to *Building Selection Criteria* on page 164.

6 Click **OK**.

Avalanche SE locates the matching devices that currently exist in the Mobile Device Inventory list and adds them to the group.

Adding Mobile Device Group Authorized Users

The **Authorized Users** tab allows you to assign administrative privileges to for a specified mobile device group to a user that has Normal user rights and is not assigned permissions to group. This means that any user assigned as an authorized user to a group will have all administrative rights for that one group.

To add an authorized user you must have at least one user configured with Normal permissions, but that does not have global permission for the profile. Users that have permission for the mobile device groups will not appear in the Authorized User list.

For information about creating users and assigning permissions, refer to *Chapter 3: Managing User Accounts* on page 31.

To add a user:

1 Right-click a device group in the Navigation Window and select **Properties.**

The *Mobile Device Group* dialog box appears.

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

The *Add Authorized User* dialog box appears.

3 From the list, select the user.

4 From the drop-down list, select the level of permission.

5 Click **OK**.

The user is added to the list box and retains permissions for the mobile device group, based on the assigned level.

Pinging Mobile Devices within Mobile Device Groups

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

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

To ping mobile devices within device groups:

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

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

Sending Messages to Mobile Device Groups

You can use mobile device groups to send messages to users. This allows you to send the same message to multiple devices simultaneously.

To send messages to device groups:

1. Right-click the group from the Navigation Window.
2. Select **Send Text Message** from the menu that appears.

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

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

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

Editing Properties for Mobile Device Groups

Mobile device group properties retrieve the common properties from all the devices in the group. You can then add, edit, and delete properties for mobile device groups.

Mobile device group properties consist of user-defined properties. Properties can be used as selection variables in selection criteria to control which devices receive particular updates.

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

To add a property to a mobile device group:

1 Right-click on a mobile device group and select **Edit Device Properties**.

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

2 Click **Add Property**.

The *Add Device Property* dialog box appears.

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

4 Enter the name of the property in the **Property Name** text box.

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

6 Click **OK**.

The new property is added to the properties list.

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

To edit a mobile device group property:

1 Right-click on a mobile device group and select **Edit Device Properties**.

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

2 Select the property that you want to edit and click **Propert**y.

The *Edit Device Property* dialog box appears.

3 Type the new property value.

4 Click **OK**.

The edited property appears in the list.

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

To delete a mobile device group property:

1 Right-click on a mobile device group and select **Edit Device Properties**.

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

2 Select the property that you want to delete and click **Delete Propert**y.

3 Confirm that you want to delete the property.

The Pending Value column for the property displays the status of the property.

4 Click **OK** to remove the property and return to the Avalanche SE Console.

The property will be deleted after the next update.

Additional Mobile Device Group Functions

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

The additional options for mobile device groups are as follows:

Enable/Disable	Allows you to enable or disable the group.
Copy	Allows you to copy the group.
Delete	Allows you to delete the group.

Rename	Allows you to rename the group.
Mark Orphan Packages for Deletion	Marks orphaned packages on the devices within the group for deletion.
Unmark Orphan Packages for Deletion	Unmarks orphan packages for deletion.
Update Now	Allows you to update all mobile devices within that group immediately.

Chapter 10: Managing Alerts

You can manage network alerts in Avalanche SE using alert profiles. Alerts refer to activity that occurs on a wireless device and ways to respond to those alerts. For example, a network alert might be generated if a Server goes offline or if a new Infrastructure device is discovered. Alert profiles allow you to specify what type of network events generate alerts and where alerts are sent when those events occur.

This chapter provides information about the following topics:

- Managing Alert Profiles
- Creating Contact Lists
- Creating Proxy Pools
- Using the Alert Browser

Managing Alert Profiles

There are three types of alert profiles:

- **Default Alert Profiles**. The default alert profile consists of preset alerts and is deployed as part of the Mobile Device Server deployment package. These alerts provide information about the Mobile Device Server only. You do not need to create a new location alert profile for the Mobile Device Server. However if you want to receive notifications through e-mail or a proxy, you must create a Normal alert profile configured with events that match the default profile events. You can modify the default alert profile to your preference.

- **Site Alert Profiles**. Site alert profiles are deployed to the location and contain a list of events that will generate alerts. When an event that matches the site alert profile is generated, an alert is sent to the Enterprise Server or configured proxy server. You can assign as many Site alert profiles to a location as you desire. Each Site alert profile deployed to a location adds to the existing alert profiles at the location. If you have duplicate alerts configured in profiles, the server will just receive one alert.

- **Normal Alert Profiles**. Normal alert profiles reside at the Avalanche SE enterprise level. These profiles determine when notification of an alert should be sent to the e-mail addresses or proxy. When an alert is generated at the location level by either the default alert profile or the location alert profile, that alert is sent to the Enterprise Server. If the alert matches the Normal alert profile, Avalanche SE sends an alert notification to the e-mail addresses assigned to that alert profile or forwards the alert to a proxy computer. If no alerts generated at the location match the Normal alert profile, no e-mail is sent. Each Normal alert profile deployed to a location adds to the existing alert profiles at the location. If you have duplicate alerts configured in the profile, you will receive two separate notifications at either the e-mail address or proxy.

This section provides the following alert-related task information:

- Creating Alert Profiles
- Enabling Alert Profiles
- Configuring Alert Profiles
- Removing Alert Profiles
- Removing Alert Profiles

Creating Alert Profiles

When you create an alert profile, you specify the profile as a Site alert profile or a Normal alert profile.

Site alert profiles are configured with a list of events that will generate an alert. These profiles are then deployed to a location (My Enterprise, My Location or a site). When an event matching the alert profile occurs, an alert is generated and sent to the Avalanche SE Console. Site alert profiles cannot be configured to send alert notifications to e-mail addresses. You must create a Normal alert profile to receive e-mail notification of alerts. However, you can view Site alerts in the **Alerts** tab in the Avalanche SE Console.

Normal alert profiles reside at the Enterprise Server level. These profiles exist to send notification of alerts to selected e-mail addresses. To receive e-mail notification of any alerts generated by the Site alert profile, you must create a Normal alert profile that contains events matching those listed in the Site alert profile. Your Normal alert profile must also contain events matching those listed in the default alert profile if you want to receive e-mail notification for any alerts generated by the default alert profile.

You do not need to deploy Normal alert profiles.

To create an alert profile:

1 From the Navigation Window, select the Alert Profiles node.

The **Alert Profiles** tab appears.

2 In the **Alert Profiles** region, click **Add Profile**.

The *Input* dialog box appears.

3 Type a name for the alert profile in the **New Alert Profile Name** text box.

4 Click **OK**.

The new alert profile appears in the **Alert Profile List**.

5 In the **General Settings tab**, select whether this profile is a **Normal** alert profile or a **Site** alert profile.

6 From the **File** menu, select **Save.**

Enabling Alert Profiles

An alert profile can have an enabled or disabled status. You must enable an alert profile before you can assign that profile to a location.

To enable an alert profile:

1 From the **Alert Profiles List**, select the alert profile you want to enable.

2 Click **Edit**.

3 In the **General Settings** tab, select the **Enabled** option.

4 From the **File** menu, select **Save.**

The alert profile is enabled and can be assigned to a location and deployed.

Viewing Where Alert Profiles Are Applied

The **Applied To** tab in the network profile page allows you to see the locations to which a selected profile is directly applied You can not change any of the information in this tab.

The **Applied To** tab displays the following information:

- **Parent Path**. The direct path back to the My Enterprise region.
- **Group.** The name of the location (My Enterprise, My Location or specific sites).
- **Selection Criteria**. Any selection criteria that is applicable where the profile is applied.

To view:

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

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

3 Click the **Applied To** tab.

The tab displays the information for the selected network profile.

Configuring Alert Profiles

Once you create an alert profile, you need to assign which alerts should be generated based on events taking place at the locations. If you do not assign any specific alerts, you will continue to receive alerts based on the default profile that is packaged with the Server deployment package. If you configure an alert profile and then assign that profile to a location, the new alert profile overwrites the existing default alert profile at the locations. Once the default alert profile is overwritten, you can assign more than one alert profile to a location. The alert profiles assigned will not overwrite each over. Instead, each alert profile generates alerts based on the events assigned to that profile.

You can also specify which e-mail address should be notified when an event matching a selected alert occurs and assign proxies from the proxy pool to the alert profile. For information about creating a contact list or a proxy pool, refer to *Creating Contact Lists* on page 138 and *Creating Proxy Pools* on page 141.

To configure an alert profile:

1 In the **Alert Profile List**, select the profile to which you are assigning alerts.

2 Click **Edit**.

3 In the **Profiled Alerts** region, enable any alert that you want to include in this alert profile.

4 If you want to receive an e-mail when a specified event takes place, enable any e-mail addresses in the **Profiled Contacts** list.

NOTE The **Profiled Contacts** list is only available for Normal alerts. For information about creating the **Profiled Contacts** list, refer to *Creating Contact Lists* on page 138.

5 If you want to forward alerts that occur to a proxy address, enable the proxy address in the **Profiled Proxies** list.

NOTE The **Profiled Proxies** list is only available for Normal alerts. For information about creating the **Profiled Proxies** list, refer to *Creating Proxy Pools* on page 141.

6 Save your changes.

Your alert profile is configured to notify the server when any of those selected alerts occur.

Alert Profile Authorized Users

The **Authorized Users** tab allows you to assign administrative privileges for a specified profile to a user that has Normal user rights and is not assigned permissions to profiles. This means that any user assigned as an authorized user to a profile will have all administrative rights for that one profile.

To add an authorized user you must have at least one user configured with Normal permissions, but not that does not have global permission for the profile. Users that have permission for the profile, will not appear in the Authorized User list.

For information about creating users and assigning permissions, refer to *Chapter 3: Managing User Accounts* on page 31.

To add an authorized user:

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

2 Click **Edit**.

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

The *Add Authorized User* dialog box appears.

4 From the list, select the user.

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

6 Click **OK**.

The user is added to the list box and retains permissions for Alert Profiles, based on the assigned level.

Removing Alert Profiles

If you determine that an alert profile is unnecessary, you can delete it from the Avalanche SE Console. When you remove a profile from the console, devices that are assigned to that profile retain those settings until you assign a new alert profile to the device.

To remove an alert profile:

1 From the **Alert Profiles List**, select the profile you want to remove and click **Remove Profile.**

2 Confirm that you want to remove the profile.

The profile is removed from the **Alert Profiles List**.

3 From the **File** menu, select **Save.**

Creating Contact Lists

Each Normal alert profile can use one or more e-mail addresses to inform you when a specified event occurs. If you want the Avalanche SE Console to notify you of an alert by e-mail, you must create a contact list. Contacts are available for Normal alert profiles only.

When you create your contact list, you add any e-mail addresses for which you want to receive alerts to the list. Your entire contact list is available for every Normal alert profile. When you configure Normal alert profiles, you can select which addresses you want to receive alerts from that alert profile.

To create a contact list:

1 From the **Alert Profile List**, select the profile you want to configure.

2 Click **Edit**.

3 In the **Profiled Contacts** tab, select **Edit Contacts**.

The *Contact Manager* dialog box appears.

This dialog box allows you to add e-mail addresses, import an e-mail address list, and delete obsolete addresses.

4 Type the name of an SMTP e-mail server in the **E-mail Server** text box, such as `mail.company.com`.

5 To verify the validity of the e-mail server, click **Test Server**.

Avalanche SE attempts to contact the e-mail server and displays a dialog box informing you if it was successful or not.

6 Type an e-mail address in the **Response E-mail Address** text box, such as `itdept@company.com`.

Any replies to alert notification e-mails are sent to this e-mail address.

7 Add any e-mail addresses to which you want alert notification e-mails sent, such as `jsmith@widget.com`.

- To add an e-mail address, click **Add** and type the appropriate information in the *Contact Information* dialog box. Click **OK**.

The address appears in the **Available Contacts** list.

8 Repeat the preceding steps until you are finished adding e-mail addresses.

9 Click **OK**.

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

NOTE The contact list only applies to Normal alert profiles.

10 Save your changes.

Importing E-mail Addresses

You can add e-mail addresses to the **Profiled Contacts** list by importing a comma-delimited `.csv` file that was exported from Microsoft Outlook.

To import e-mail addresses:

1 From the **Alerts Profile List**, select the profile you want to configure.

2 Click **Edit.**

3 In the **Profiled Contacts** tab, select **Edit Contacts**.

The *Contact Manager* dialog box appears.

4 Click **Import**.

An *Open* dialog box appears.

5 Select the `.csv` file that contains the e-mail addresses that you want to import.

6 Click **Open**.

The e-mail addresses contained in the text file appear in the **Available Contacts** list.

7 Click **OK**.

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

Removing Contacts

You can delete e-mail addresses from the **Profiled Contacts** list when you no longer need those addresses. When you delete an address from the contact list, that address no longer receives the alerts.

To remove a contact:

1 Ensure you are in Edit Mode.

2 In the **Profiled Contacts** tab, select **Edit Contacts**.

The *Contact Manager* dialog box appears.

3 In the **Available Contacts** region, select the e-mail address you want to remove from the list.

4 Click **Remove**.

5 Confirm that you want to delete the e-mail address.

The e-mail address is removed from the list.

6 Click **OK** to return to the **Profile Contacts** tab.

Creating Proxy Pools

The Avalanche SE Console allows you to set one or more proxies for an alert profile. When you set a proxy, the console automatically forwards the alert to the IP address of the proxy, enabling you to integrate Avalanche SE with your existing network management tools. To use proxies with alert profiles you must create a proxy pool. Proxies are available to Normal alert profiles only.

To add proxies to the proxy pool:

1 Select the profile you want to configure.

2 Click **Edit**.

3 In the **Profiled Proxies** tab, select **Edit Proxies**.

The *Proxy Pool Manager* dialog box appears.

4 Click **Add**.

The *Add Proxy Address* dialog box appears.

5 In the **Proxy Address** text box, enter the IP address and click **OK**.

The address appears in the **Available IP Addresses** list box.

6 Repeat the predating steps until you are finished adding proxy addresses.

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

Any proxy addresses you added appear in the **Profiled Proxies** list box.

Deleting Proxies

If a proxy is no longer necessary, you can delete that proxy from the pool.

To delete a proxy:

1 Ensure you are in Edit Mode.

2 In the **Profiled Proxies** tab, select **Edit Proxies**.

The *Proxy Pool Manager* dialog box appears.

3 Select the IP address of the proxy from the **Available Proxy Addresses** list.

4 Click **Delete**.

5 Confirm that you want to delete the proxy.

Avalanche SE deletes the proxy from the list.

6 Click **OK** to return to the **Alerts Profile** tab.

Using the Alert Browser

The **Alerts** tab contains the Alert Browser. The browser is a table overview of the alerts that occur on your wireless network. It provides the following information about each alert:

Ack	Allows you to acknowledge that you have seen the alert.
Alert	Displays the type of alert.
Date	The time and date when the alert occurred.
Description	Provides a brief description of the alert.

Acknowledging Alerts

- In the **Alert** tab, enable the checkbox next to the alert you want to acknowledge.

  -Or-

  To acknowledge all alerts in the list, click **Acknowledge All**.

Clearing Alerts

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

To clear alerts:

1 Acknowledge any alerts you want to clear by marking the checkbox next to the alert.

2 Click **Clear All**.

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

Customizing Alert Browser Functionality

In the *Preferences* dialog box, you can configure the way the Alert Browser manages and displays alerts. You can configure the following settings:

- Number of days an alert remains in the Alert Browser
- Maximum number of alerts that are listed in the Alert Browser
- Maximum number of alerts to store. Alerts are stored in the database on the Enterprise Server.

To customize the Alert Browser functions:

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

The *Preferences* dialog box appears.

2 In the **Alert Browser Settings**, use the text boxes to configure the alert specific settings.

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

The Alarm Browser will update to reflect your changes.

Alert Profile Descriptions

The following tables provide a list of the settings and the description of those settings.

- Alert Profile List
- Alert Profile General Settings

Alert Profile List

The Alert Profile List displays information about your software profiles.

Field	Description
Name	Displays the name of the alert profile.
Status	Sets the status of the profile as either enabled or disabled.
Site	Indicates if the alert is a Site alert. If YES, the alert is a Site alert. If NO, the alert is a Normal alert.
Alerts	Displays the number of Profiled Alerts that are assigned to the profile.
Contacts	Displays the number of contacts in the contact list that are assigned to receive notifications from this alert profile.
Proxies	Displays the number of proxies that are assigned to receive notification from this alert profile.

Table 10-1: *Software Profile List*

Alert Profile General Settings

The following table provides information about the software profile settings in the **General Settings** tab.

Field	Description
Name	Sets the name of the alert profile.

Table 10-2: *General Settings*

Field	Description
Status	Sets the status of the profile as either enabled or disabled.
Type	Sets the type of the profile as either Normal or Site. Site alert profiles are deployed to the locations and contain a list of events that will generate alerts. When an event that matches the Site alert profile is generated, an alert is sent to the Avalanche SE server or configured proxy server. You can assign as many Site alert profiles to a location as you desire. Each Site alert profile deployed to a location adds to the existing alert profiles at the location. If you have duplicate alerts configured in profiles, the server will just receive one alert. Normal alert profiles reside at the Avalanche SE enterprise level. These profiles determine when notification of an alert should be sent to the e-mail addresses or proxy. When an alert is generated at a location by either the default alert profile or the Site alert profile, that alert is sent to the Avalanche SE server. If the alert matches the Normal alert profile, Avalanche SE sends an alert notification to the e-mail addresses assigned to that alert profile or forwards the alert to a proxy computer. If no alerts generated at the location match the Normal alert profile, no e-mail is sent. Each Normal alert profile deployed to a location adds to the existing alert profiles at the location. If you have duplicate alerts configured in the profile, you will receive two separate notifications at either the e-mail address or proxy

Table 10-2: *General Settings*

Chapter 11: Managing Update Profiles

You can control mobile device updates at a more granular level by creating Update Profiles. Update Profiles are intended to decrease traffic by restricting specific mobile devices from contacting the Mobile Device Server during assigned times. These assigned times are called Exclusion Windows. Exclusion Windows are scheduled periods of time when your mobile devices are not authorized to contact the Mobile Device Server. Once applied, the Update Profile regulates when and which mobile devices can contact the Mobile Device Server for updates.

To conserve bandwidth and increase compliance for critical software updates, you can create separate Update Profiles that are applicable to different groups of mobile devices. Use selection criteria to create Update Profiles that specify when certain mobile devices can contact the Mobile Device Server.

You can improve the performance, responsiveness, and reliability of the update process by optimizing the schedule of the updates. The best way to schedule and apply Update Profiles varies depending on many factors including the number of mobile devices attempting to contact each Mobile Device Server and your bandwidth capabilities.

Similar Exclusion Windows can be configured in the Mobile Device Server Profile. However, Exclusion Windows from the Mobile Device Server Profile do not include the selection criteria functionality and the option to schedule Exclusion Windows at different times on different days.

NOTE The dates and times you exclude from scheduling events apply to all events. You cannot set specific exclusion dates and times for each update. However, you can configure activation for specific software packages from a Software Profile. For more information, refer to *Chapter 7: Managing Software Profiles* on page 85.

This chapter includes the following topics:

- Adding Update Profiles
- Configuring Update Profile General Settings
- Adding Update Profiles Authorized Users
- Scheduling Exclusion Windows

- Applying Selection Criteria

Adding Update Profiles

Create separate Update Profiles based on when you want your mobile devices to contact the Mobile Device Server.

To add an update profile:

1. From the Navigation Window, select **Update Profiles**.
2. In the **Update Profile List**, click **Add**.

   An *Input* dialog box appears.
3. Enter a name for the update profile.
4. Click **OK**.

Configuring Update Profile General Settings

Update Profile general settings include options to enable or disable the profile and set the number of simultaneous updates that can occur at the Mobile Device Server. Consider how your bandwidth speed may be affected before configuring this setting.

To configure general settings:

1. Select the update profile you want to configure.
2. Click **Edit**.
3. In the **General Settings**, enable the profile.
4. Enable the profile.
5. If you want to allow any number of simultaneous updates, enable the **Allow unlimited simultaneous mobile device updates** option in the **Synchronization Exclusion Window**.

   -Or-

If you want to set the maximum number of simultaneous updates, disable the **Allow unlimited simultaneous mobile device updates** option and type the maximum number of simultaneous updates in the active text box.

6 Save your changes.

Viewing Where Update Profiles Are Applied

The **Applied To** tab in the network profile page allows you to see exactly where the profile is applied. You cannot change any of the information in this tab. If you need to apply a profile to a different location than what you see in the **Applied To** tab, you will need to access the **Properties** tab and assign the profiles there. The **Applied To** tab displays the following information:

- **Parent Path**. The direct path back to the My Enterprise region.
- **Group.** The location where the profile is applied.
- **Selection Criteria**. Any selection criteria that is applicable where the profile is applied.

To view:

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

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

3 Click the **Applied To** tab.

The tab displays the information for the selected network profile.

Adding Update Profiles Authorized Users

The **Authorized Users** tab allows you to assign administrative privileges for a specified profile to a user that has Normal user rights and is not assigned global permissions to profiles. This means that any user assigned as an authorized user to a profile will have all administrative rights for that one assigned profile.

To add an authorized user you must have at least one user assigned to Normal permissions, but not that does not have global permission for the profile. Users that already have permission for the profile will not appear in the Authorized User list.

For information about creating users and assigning permissions, refer to *Chapter 3: Managing User Accounts* on page 31.

To add an authorized user:

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

2 Click **Edit**.

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

The *Add Authorized User* dialog box appears.

4 From the list, select the user.

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

6 Click **OK**.

The user is added to the list box and retains permissions for Update Profiles, based on the assigned level.

Scheduling Exclusion Windows

Exclusion windows allow you to schedule times when mobile devices are not allowed to contact the Mobile Device Server.

To schedule exclusion windows:

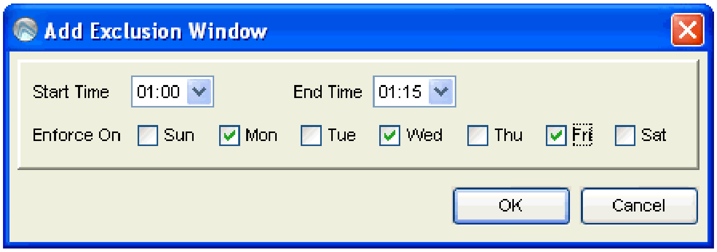
1 Select the update profile for which you are scheduling an exclusion window.

2 Click **Edit**.

3 Select the **Exclusion Window** tab.

4 Click **Add Exclusion Windows**.

The *Add Exclusion Window* dialog box appears.



Start Time 01:00 End Time 01:15

Enforce On □ Sun ☑ Mon □ Tue ☑ Wed □ Thu ☑ Fri □ Sat

Figure 11-1. *Add Exclusion Window*

5 Use the **Start Time** and **End Time** drop-down lists to schedule the time of the exclusion window.

6 Enable the days of the week that you would like to schedule the exclusion window.

7 Click **OK**.

The exclusion window appears in the **Weekly View** and **Daily View** of the **Exclusion Window** tab.

8 Save your changes.

Editing Exclusion Windows

Once you have created an exclusion window, you can edit the configuration from the **Weekly View** and **Daily View** sections of the **Exclusion Window** tab.

To edit exclusion windows:

1 Ensure you are in Edit Mode.

1 In the **Weekly View**, select the day of the week you want to modify.

2 In the **Daily View**, click and hold the exclusion window marker.

3 Drag the marker to the time you want to schedule.

4 Save the profile.

Applying Selection Criteria

You can use selection criteria to selectively configure which mobile devices receive the Update Profile. Mobile devices with properties that match the section criteria configured in the profile will receive the profile. For details about Selection Criteria and the operators to use, refer to *Chapter 14: Selection Criteria* on page 163.

Chapter 12: Using Scan to Configure

Avalanche SE allows you to create scan to config profiles (barcode profiles) that are configured with network profile settings. You can then print the profiles as barcodes and use a mobile device to scan them. The information from the scanned barcodes is stored in the Avalanche profile on the Enabler. You can create as many barcode profiles as you need and save them in the *Scan to Config* dialog box in the Avalanche SE Console.

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

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

This section contains instructions for the following tasks:

- Configuring Barcode Profiles
- Printing Barcodes
- Scanning Barcodes

Configuring Barcode Profiles

When you create a barcode profile, you can perform the following tasks:

- Adding Barcode Profiles
- Configuring Network Settings
- Creating Custom Properties
- Editing Barcode Profiles
- Deleting Barcode Profiles

Adding Barcode Profiles

You can create as many different barcode profiles as you need. The profiles appear in the **Barcode Profiles** list box in the *Scan To Config Profile* dialog box. Once you have configured your the network settings for the profile, you can print the barcodes and then use a wireless device to scan the barcode and set the network settings for that device.

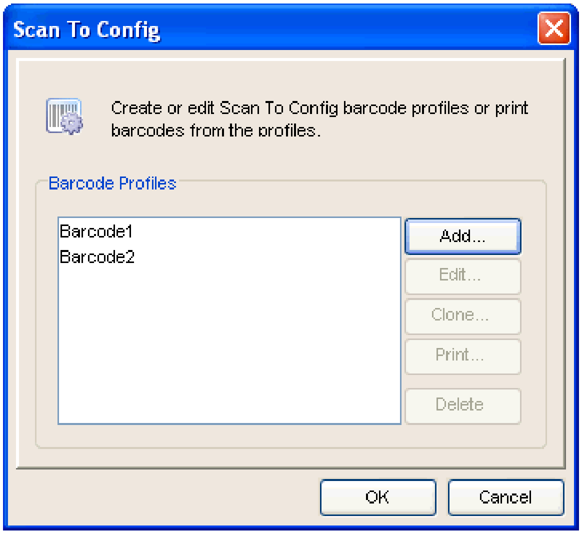
When you create a barcode profile, you can also configure a passcode for that profile. The passcode is used to encrypt the barcode data. The mobile device user must enter the same passcode when they are using scan to configure so that the Enabler can decrypt the barcode data when it is scanned. If the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

To create a barcode profile:

1 From the **Tools** menu, select **Scan To Config**.

NOTE You can also access the Scan to Config utility from the **Quick Start** tab.

The *Scan To Config* dialog box appears.



Create or edit Scan To Config barcode profiles or print barcodes from the profiles.

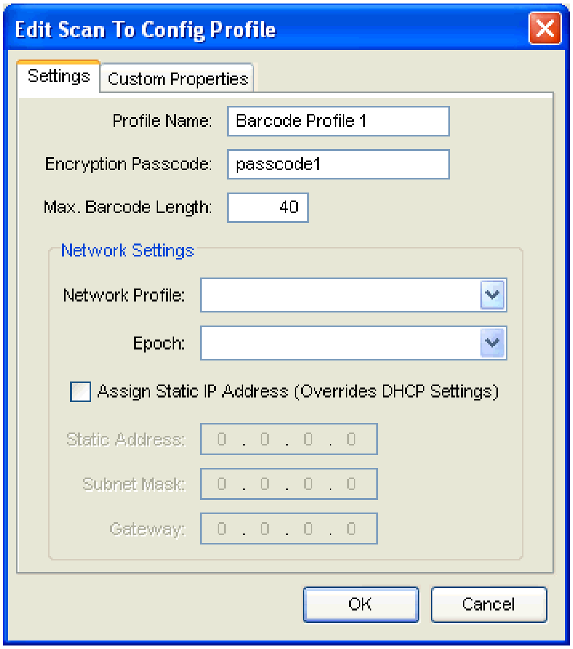
Barcode Profiles

Barcode1
Barcode2

Figure 12-1. *Scan To Config*

2 Click **Add**.

The *Edit Scan To Config Profile* dialog box appears.



Profile Name: Barcode Profile 1

Encryption Passcode: passcode1

Max. Barcode Length: 40

Network Profile:

Epoch:

□ Assign Static IP Address (Overrides DHCP Settings)

Static Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Gateway: 0 . 0 . 0 . 0

Figure 12-2. *Edit Scan To Config Profile*

3 In the **Profile Name** text box, type the name of the profile.

4 In the **Passcode** text box, type the name of the encryption passcode you are going to use (optional).

5 In the **Max. Barcode Length**, type number of characters you want the barcodes to be (1 - 40 characters).

6 Click **OK**.

The barcode profile is added to the **Barcode Profiles** list.

Configuring Network Settings

You can configure the settings of a barcode profile from the *Edit Scan To Config Profile* dialog box.

You need to have created at least one network profile that you can apply to this barcode profile. If you have not created any network profiles, refer to *Creating Network Profiles* on page 51 for information about creating them.

When a mobile device scans the barcode, the mobile device receives the network settings configured within that barcode.

NOTE WEP key rotation is not supported.

To configure the settings:

1 From the **Tools** menu, select **Scan To Config**.

The *Scan To Config* dialog box appears.

2 Select the profile you want to configure settings for and click **Edit**.

The *Edit Scan To Config Profile* dialog box appears.

3 From the **Network Profile** drop-down list, select the network profile you want to use for this barcode profile.

For information about creating network profiles, refer to *Creating Network Profiles* on page 51.

NOTE IP pools are not supported. You must specify enable DHCP in the network profile or enable DHCP.

---

4 If the network profile you selected contains epochs, you can select which epoch you want to use.

5 If you want to manually assign a static IP address, subnet mask, and gateway, enable the **Assign Static IP Address** option.

Assigning this information overrides any DHCP settings.

6 Configure the settings.

7 Click **OK**.

The profile is updated with the configured network settings.

Creating Custom Properties

Custom properties allow you to define specific properties that you want applied to the mobile device. These properties are configured into the barcode profile, and then printed out in the barcodes. When the mobile device scans the barcode, the properties are placed on the mobile device. Custom properties are one way of refining selection criteria for mobile devices.

You can perform the following tasks associated with custom properties:

- Adding Custom Properties
- Editing Custom Properties
- Deleting Custom Properties

Adding Custom Properties

When you add a custom property, that property is included in the information created in the barcode. When you scan the barcode with a mobile device, the custom property is placed on the mobile device along with the network profile. Custom properties must be created individually for each barcode profile.

You can create either device-specific properties or network-specific properties. A device property adds properties in the device properties section on the mobile device and can be used with selection criteria related to that device.

A network property allows custom properties to be configured for the network adapter on the device. This allows flexibility for network management features that may be supported on a particular device.

To add a custom property:

1 From the **Tools** menu, select **Scan To Config**.

The *Scan To Config* dialog box appears.

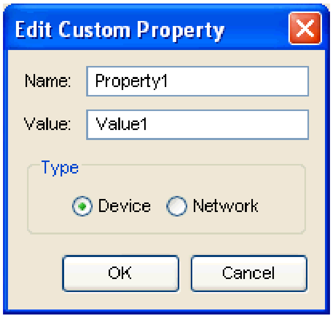
2 Select the profile to which you want to add a custom property and click **Edit**.

- If you have not created a barcode profile, click **Add**.

The *Edit Scan To Config Profile* dialog box appears.

3 Select the **Custom Properties** tab and click **Add**.

The *Edit Custom Property* dialog box appears.



Name: Property1

Value: Value1

Type

● Device ○ Network

Figure 12-3. *Edit Custom Property*

4 In the **Name** text box, enter the name of the custom property.

5 In the **Value** text box, enter the value for the property.

6 Select whether this property is a device-specific property or a network-specific property.

7 Click **OK**.

The new property is added to the list box for that specific barcode.

8 Click **OK** again to return to the *Scan to Config* dialog box.

Editing Custom Properties

You can edit any custom property in the list box.

To edit a custom property:

1 From the **Tools** menu, select **Scan To Config**.

The *Scan To Config* dialog box appears.

2 Select the profile for which you want to edit a property and click **Edit**.

3 From the **Custom Properties** tab, select the property you want to modify.

4 Click **Edit**.

The *Edit Custom Properties* dialog box appears.

5 Make the desired changes.

6 Click **OK**.

The updated property appears in the list box.

Deleting Custom Properties

You can remove any custom properties that are no longer applicable to the barcode profile.

To remove a custom property:

1 From the **Tools** menu, select **Scan To Config**.

The *Scan To Config* dialog box appears.

2 Select the profile for which you want to remove a property and click **Edit**.

3 From the **Custom Properties** tab, select the property you want to remove.

4 Click **Remove**.

The property is removed from the list box and will not be configured into the barcode profile.

Editing Barcode Profiles

You can edit any of the barcode profiles you create.

To edit a barcode profile:

1 From the **Tools** menu, select **Scan to Config.**

The *Scan To Config* dialog box appears.

2 From the **Barcode Profiles** list box, select the barcode profile you want to modify.

3 Click **Edit**.

4 Make the desired changes.

5 Click **OK**.

You can print the modified barcode profile and update your mobile devices.

Deleting Barcode Profiles

If you no longer need a barcode profile, you can remove it from the barcode profile list.

To delete a barcode profile:

1 From the **Tools** menu, select **Scan to Config**.

The *Scan To Config* dialog box appears.

2 From the **Barcode Profiles** list box, select the barcode profile you want to remove.

3 Click **Delete**.

The profile is removed from the list box and no longer available.

Printing Barcodes

Once you have created and configured a barcode profile, you can print that profile. The profile prints as a set of barcodes in random order. You can then use a mobile device to scan the barcodes. The barcode will assign the configured network settings to the mobile device.

To print a barcode:

1 From the **Tools** menu, select **Scan to Config**.

The *Scan To Config* dialog box appears.

2 From the **Barcode Profiles** list box, select the barcode profile you want to print.

3 Click **Print**.

The barcode profile is printed as a set of barcodes.

Scanning Barcodes

To deploy the network configurations to the mobile device, you must open the *Scan Configuration* dialog box from the Enabler on the mobile device. Use the mobile device to scan each barcode in any order. This sends the configurations to the Enabler and updates the Avalanche profile.

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

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

To scan the configuration:

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

The *Scan Configuration* dialog box appears.

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

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

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

Chapter 13: Performing System Backups

You can perform the following system backup tasks from the Task Scheduler:

- Backing Up the System
- Restoring the System

Backing Up the System

When you back up Avalanche SE, the database information and software collections are both saved in a zip file. The Scheduled Task Wizard provides the capability to backup and restore your entire system. You should back up the system regularly, and also when uninstalling Avalanche SE. If for any reason Avalanche SE files are deleted or corrupted, you will be able to restore them from the backup files.

NOTE If PostgreSQL is not installed in the Wavelink directory, backup and restore functionality will fail.

To back up the system:

1 Select **Task Schedule** from the **Tools** menu.

The *Task Schedule* dialog box appears.

2 Click **Add**.

The *Select A Task* dialog box appears.

3 Select **System Backup** from the **Task Type** list and click **Next**.

The *Create A System Backup* dialog box appears.

4 In the **Tag Name** text box, enter a name for the system backup and click **Next**.

NOTE The tag is an identifier that can be used to select the correct file when restoring the system. The tag is not the same as the name of the zip file.

The *Select Scheduling Options* dialog box appears.

5 Determine when the event will occur.

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

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

- If you want the event to occur on a regular basis, select the **Schedule a recurring event for the task** option.

6 Click **Next**.

7 If you selected the **Schedule a one-time event** for the task option, the *Schedule the Time Window* dialog box appears.

- Within this dialog box, you can set the following parameters for the event:

- Select the start date and time for the event.

- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **Use end time** option and then select the date and time for the event. If the event is not finished by this date and time, Avalanche SE will generate an alert.

- If you want the start and end time for this event to be based on the local time for My Location, enable the **Use Location's Local Time** option. Otherwise, the start and end times are based on the local time for the Avalanche SE Console.

8 If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

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

- Select the start time for the event.

- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **Use end time** option and then select the end date and time for the event. If the event is not finished by this date and time, Avalanche SE will generate an alert.

- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.
- If you want the start and end time for this event to be based on the local time for My Location, enable the **Use Location's Local Time** option. Otherwise, start and end times are based on the local time for the Avalanche SE Console.

9 Click **Next**.

The *Review Your Task* dialog box appears.

10 Review your task to ensure that it is correct and click **Next**.

The *Task Scheduled* dialog box appears.

11 Click **Next** to schedule a new event, or click **Finish** to return to the *Task Schedule* dialog box.

The task is added to the **Scheduled and Recurring Tasks** list. The task will run according to its schedule, and once it has completed, it will move to the **Successfully Completed Tasks** list.

Restoring the System

Once the system information has been saved, you can use the Task Scheduler to restore the information to Avalanche SE.

You cannot restore a system backup from a previous version of Avalanche SE. The backup version must match the Avalanche SE version. If you attempt to restore a system backup from a previous version of Avalanche SE, the restoration will fail.

NOTE If there is any information in the system that was not backed up, it will be replaced when the system is restored.

NOTE If PostgreSQL is not installed in the Wavelink directory, backup and restore functionality will fail.

To restore the system:

1 Select **Task Schedule** from the **Tools** menu.

The *Task Schedule* dialog box appears.

2 Click **Add**.

The *Select A Task* dialog box appears.

3 Select **Restore System** from the **Task Type** list and click **Next**.

The *Restore A System Backup* dialog box appears.

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

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

NOTE The default file path is `C:\Program Files\Wavelink\AvalancheSE\backup`

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

The *Select Scheduling Options* dialog box appears.

5 Determine when the event will occur and click **Next**.

- If you want the event to occur immediately, select the **Perform task now** option.
- If you want the event to occur at some point in the future, select the **Schedule a one-time event for the task** option.

- If you want the event to occur on a regular basis, select the **Schedule a recurring event for the task** option.

6 Click **Next**.

7 If you selected the **Schedule a one-time event** for the task option, the *Schedule the Time Window* dialog box appears.

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

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

8 If you selected the **Schedule a recurring event** option, the *Configure Task Recurrence* dialog box appears.

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

- Select the start time for the event.
- Determine when you want the event to end. If you want the event to end only after the deployment is complete, select the **Run until complete** option. If you want the event to end after a specified amount of time, select the **Use end time** option and then select the end date and time for the event. If the event is not finished by this date and time, Avalanche SE will generate an alert.
- Set the frequency of the event. You can set whether the event occurs daily, weekly, or monthly.
- Set the start and end dates for the event.

- If you want the start and end time for this event to be based on the local time for My Location, enable the **Use Location's Local Time** option. Otherwise, start and end times are based on the local time for the Avalanche SE Console.

9 Click **Next**.

The *Review Your Task* dialog box appears.

10 Review your task to ensure that it is correct and click **Next**.

The *Task Scheduled* dialog box appears.

11 Click **Next** to schedule a new event, or click **Finish** to return to the *Task Schedule* dialog box.

The task is added to the **Scheduled and Recurring Tasks** list. The task will run according to its schedule, and once it has completed, it will move to the **Successfully Completed Tasks** list.

Chapter 14: Selection Criteria

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

Additional selection criteria is typically associated with the software packages themselves, further restricting the distribution of the package, but package criteria is built into the package at the time of its creation.

NOTE The selection criteria associated with a particular software package is set by Wavelink or the third-party application developer and, once created, the criteria associated with a package cannot be modified.

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

By default, the selection criteria string for a software collection or a network profile is empty, which allows all packages within the collection - or all settings within the profile - to download to all mobile devices. You can modify this criteria at any time.

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

This section provides information on the following tasks:

- Building Selection Criteria
- Selection Variables
- Operators

Building Selection Criteria

You can access the Selection Criteria Builder from several different places in the Avalanche SE Console, including: Network Profiles, Software Profiles, and Mobile Device Groups.

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

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

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

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

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

To build selection criteria:

1. Access the Selection Criteria Builder.
2. From the drop-down list, select a source property and click **Insert Property**.

NOTE For information about source properties, see *Selection Variables* on page 165.

3 Select one of the operator buttons.

NOTE For more information about operators, see *Operators* on page 173.

---

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

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

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

---

6 Click **Validate**.

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

7 Click **OK** to return to the Selection Criteria Builder.

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

Building Custom Properties

You can build custom properties to use in your selection criteria

To build custom properties:

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

The *Add Custom Property* dialog box appears.

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

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

Selection Variables

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

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

NOTE Selection criteria strings are case sensitive.

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

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

The following Palm emulation selection criteria string is valid:

```
Series = S
```

While the following is not:

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

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

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

Selection variables for the selection criteria string are as follows:

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

Example:

```
Columns > 20
```

`EnablerVer` Predefined property designated by the Enabler.

Values with decimals must be surrounded by double quote marks.

EnablerVer = “3.10-13”

`IP`

IP address of the mobile device.

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

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

`KeyboardCode`

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

Supported values include:

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

Example:

```
KeyboardCode = 0
```

`KeyboardName`

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

Supported values include:

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

Example:

```
KeyboardName = 35KEY
```

`Last Contact`

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

Examples of time-stamp formats must be quoted.

- mm/dd/yyyy

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

- HH:MM mm/dd/yyyy

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

- hh:mm AP mm/dd/yyyy

  `LastContact = “11:15 PM 12/22/2005”`

- Plus range-forms of the above

The relative format uses an offset from the current time.

- <offset>M

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

- <offset>H

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

- <offset D>

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

- Plus range forms of the above

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

- `LastContact=7D-1M`

`MAC`

MAC address of the mobile device.

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

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

`ModelName`

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

A few of the supported values include:

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

Example:

```
ModelName = 6840
```

`ModelCode`

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

Supported values include:

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

Example:

```
ModelCode <= 2
```

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

`OSVer`

Predefined property designated by the Enabler. Values with decimals in them must be surrounded by double quote marks.

```
OSVer = "4.20"
```

`OS Type`

Predefined property designated by the Enabler.

```
OSType = PocketPC
```

`Processor`

Predefined property designated by the Enabler.

```
Processor = ARM
```

`ProcessorType`

Predefined property designated by the Enabler.

```
ProcessorType = xScale
```

`Assigned IP`

IP address of the mobile device.

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

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

`Series`

The general series of a device.

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 = Any other DOS devices

Example:

```
Series = 3
```

`Rows`

The number of display rows the mobile device supports. The possible value range is 1 to 25.

Example:

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

This example matches all mobile devices with 20 rows, except those with 35-key keyboards.

`Syncmedium`

The type of synchronization medium for the mobile device to use.

Supported values include:

SyncMedium=any
SyncMedium=ip
SyncMedium=serial

`Terminal ID`

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

Example:

```
Terminal ID = 5
```

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

Operators

All selection criteria strings are evaluated from left to right, without operator precedence. When more than one operator is involved, you must include parentheses in order for the selection criteria string to be evaluated properly.

For example:

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

NOTE Spaces around operators are optional.

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

You may use the symbol of the operator (!, &, |, etc.) in a selection criteria, or you may use the letter abbreviation (NOT, AND, OR, etc.). If you use the letter abbreviation for the operator, then you must format the letter abbreviation in all upper-case letters.

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

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

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

All mobile devices with 20 rows receive the software packages within the collection except for those with 35Key keyboards.

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

Example:

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

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

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

Both 6840 and 3840 mobile devices can receive the software packages.

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

Example:

```
ModelName = 6840
```

`NE (!=)` Not equal to.

Example:

ModelName != 6840

The selection criteria targets all non-6840 mobile devices.

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

Example:

```
Rows > 20
```

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

Example:

```
Rows < 21
```

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

Example:

```
Rows >= 21
```

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

Example:

```
Rows <= 20
```

Operators use the following precedence:

1. Parenthesis
2. OR operator
3. AND operator
4. NOT operator
5. All other operators

Appendix A: Port Information

The tables in this appendix provide information about the ports used in Avalanche SE. The tables include:

- Enterprise Server Ports
- Mobile Device Server Ports
- Remote Control Ports

NOTE All ports are inbound ports that must be opened in the firewall.

Enterprise Server Ports

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

Port	Description	Port Type
5432	Avalanche SE JDBC (Internal Use, facilitates communication between the Enterprise Server and PostgreSQL database.	TCP
7221	Avalanche SE License Server	TCP
7226	InfoRail Service IR to IR router port	TCP
7225	InfoRail Service	TCP
5002	AMC Wavelink Authentication Service	TCP
1899	Remote Control Communication	TCP
5001	CE Secure Authentication Service	TCP

Mobile Device Server Ports

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

Port	Description	Port Type
1777	Mobile Device Server MU Protocol Service	TCP/UDP

Remote Control Ports

The table lists the Remote Control component that the port is open on, the port number and the way the port is used on that component.

Components	Ports	Port Use
Remote Control Server	TCP 1899	Listens for mobile devices requesting pre-connect status
	TCP 1900	Listens to establish the connection from the Remote Control Viewer to a pre-connected device or from the Remote Control Viewer to the server
Device	TCP 1899	Listens for direct connection from the Remote Control Viewer
	UDP 1903	Listens for discovery messages
License Server	TCP 7221q	Listens for license requests from the Remote Control Server

Appendix B: Avalanche SE Services

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

Services List

Wavelink Authentication Service AMC

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

Enterprise Server

Apache Tomcat

C:\Program Files\Apache Software Foundation\Tomcat 5.5\bin\tomcat5.exe

Enterprise Server

Wavelink Alerts

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

Mobile Device Server

Wavelink Avalanche MC Service Manager

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

Mobile Device Server

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

Wavelink Avalanche Agent

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

Mobile Device Server

Wavelink Avalanche Enterprise Service

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

Enterprise Server

Wavelink Deployment

C://Program Files//Wavelink//AvalancheMC\IServ.exe

Mobile Device Server

Wavelink Information Router

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

Enterprise Server

Wavelink License Server

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

Enterprise Server

Glossary

ActiveSync A synchronization program developed by Microsoft. It allows a mobile device synchronize with the machine running Avalanche SE.

Administrator User Accounts Users assigned as Administrator Accounts have unlimited permissions, and can assign and change permissions for Normal user accounts.

Alert Profile A collection of traits that define a response to a specific network or statistical alert. Typically, an alert profile consists of the alert being monitored and either an e-mail address or proxy computer to which the alert is forwarded.

Authorized Users Authorized users are users that have permission to access assigned areas of the console and the ability to perform certain tasks.

Avalanche SE Console The Avalanche SE Console is the graphical user interface (GUI) where you manage your Mobile Device Server, profiles and devices.

Blackout Window A period of time when the Mobile Device Servers are not allowed to contact the Enterprise Server, eliminating heavy bandwidth and allowing control the flow of device connections to the Enterprise Server. Also referred to as Enterprise Server Connection.

CE Secure A Wavelink plug-in that provides advanced user authentication and security on Windows CE mobile devices.

Client A mobile device with an installed Avalanche Enabler, which allows the client to communicate with a Mobile Device Server and to be configured and managed through Avalanche SE.

Default Profile A profile that the Mobile Device Server automatically assigns to network mobile devices. The Mobile Device Server applies these default profiles to any devices discovered that are not assigned to a profile.

Device Filters Device filters allow you to display specific mobile devices in the Mobile Device Inventory based on selection criteria.

DHCP
Dynamic Host Configuration Protocol. An IP service that allows DHCP clients to automatically obtain IP parameters from a DHCP server.

DNS
Domain Name System. A service that provides host name-to-IP address mapping.

Enabler
The software installed on a mobile device that allows it to be managed by Avalanche SE.

Enterprise Server
The Enterprise Server is the platform that manages communication and collaboration between the components of Avalanche SE.

Enterprise Server Connections
See Blackout Window.

Epochs
An epoch consists of a collection of network settings and configured times in which the settings for a network profile changes. Epochs can be created for each configured network profile. Most network profile settings can be managed by Epochs.

ESSID
Extended Service Set ID. The identifier of an extended service set for devices that are participating in an infrastructure mode wireless LAN.

Exclusion Windows
Exclusion Windows are scheduled periods of time when your mobile devices are not authorized to contact the Mobile Device Server to conserve bandwidth and increase compliance for critical software updates. Exclusion Windows are configured through Update Profiles.

Mobile Device
A hand-held or vehicle-mounted device, such as a scan gun or PDA, that travels with a user as they conduct daily operations.

Mobile Device Server
The Mobile Device Server consists of server side software packages that facilitate communication between the mobile devices and the Enterprise Server.

Mobile Device Server Profile
Mobile Device Server Profiles allow you to define device configuration settings for the Mobile Device Server. Once you have configured a Mobile Device Server Profile you can apply that profile to your location.

Mobile Device Groups
Groupings of mobile devices with similar characteristics defined by selection criteria.

My Locations This is the location on your network where you want to manage mobile devices. A Mobile Device Server is installed at this location.

Network Profile A collection of settings that allow you to download network parameters such as IP addresses, the ESSID, and WEP encryption keys to the mobile device over a serial or wireless connection.

Nodelock The process in which a Wavelink license is bound to a specific computer on a network. The Wavelink licensing process uses an algorithm to combine a product serial number and a computer system's node to generate a unique license number for product authorization.

Normal User Accounts Users assigned as Normal users do not have access to any component of Avalanche SE until assigned specific permissions.

Orphan Packages A software package that has been deployed to a client through Avalanche SE, but has been disabled or is not recognized by the Server. You must orphan a software package before you can use Avalanche SE to delete it from the client.

Ping An IP service that is used to test IP connectivity. Part of the ICMP service.

Profile A collection of configuration settings that can be applied to multiple devices simultaneously.

Ports Ports are typically used to map data to a particular process running on a computer.

PostgreSQL A powerful, open source relational database system packaged with Avalanche SE

Profile Permissions Profile permissions provide global access to each profile you are given permission for. Does not allow permission to apply the profiles to any locations until you are assigned Regional Permissions for a location.

RAPI A connection to the RAPI (Microsoft ActiveSync) interface on a host system. Avalanche uses the Local Gateway to perform updates and to install Avalanche Enablers to mobile devices. RAPI support is only available for ActiveSync versions pervious to version 4.0.

Regional Permissions

Provide access to specific to regions. To have full permissions at a region, a user must be assigned the Regional Permission in the User Management dialog box and then be assigned as an Authorized User to the specific region. See Authorized User.

Remote Control

A Wavelink plug-in that allows you to remotely view and manage mobile devices.

Scan to Configure

The ability to configure barcode profiles that contain network profile settings. You can then print the profiles as barcodes and scan the barcodes with a mobile device running an Enabler 3.5 (or later versions). The information configures the network profile of the mobile device.

Secondary Servers

If configured and assigned, secondary servers allow mobile devices to attempt to connect to a secondary Mobile Device Server if the primary server is not available.

Selection Criteria

A collection of parameters that define which mobile devices receive specific software updates.

Selection Variables

The basis for selection criteria. In some cases, selection variables are mobile device properties.

Software Packages

The collection of files that reside on the mobile device for a particular application. These files include any support utilities used to configure or manage the application from the Avalanche SE Console.

Software Profiles

A logical grouping of software packages maintained and managed by the Avalanche SE.

SSID

Service Set Identifier. A unique name, up to 32 characters long, that is used to identify a wireless LAN. The SSID is attached to wireless packets and acts as a password to connect to a specific BSS or ESS.

Task Scheduler

The Task Scheduler provides the means to perform system back ups.

Telnet

A TCP/IP utility used for terminal emulation, which allows a client to connect and interact with a remote host system.

Terminal ID

The identification number of a specific (physical) terminal or workstation on the network.

Update Profiles Update Profiles decrease traffic by restricting specific mobile devices from contacting the Mobile Device Server during assigned times using Exclusion Windows. See also, Exclusion Windows.

User Account A login name and password used by an individual to access the Administrator. User accounts are assigned permission levels.

WEP Wired Equivalent Privacy. An encryption standard for wireless networks that provides the equivalent security of a wired connection for wireless transmissions.

Index