Wavelink Avalanche CE Secure 1.1
User Guide

(for build 1.1.54 and later)

cesecure-ug-20090702

Revised 7/13/09

Copyright © 2009 by Wavelink Corporation All rights reserved.

Wavelink Corporation
6985 South Union Park Avenue, Suite 335
Midvale, Utah 84047
Telephone: (801) 316-9000
Fax: (801) 255-9699
Email: info@roisys.com
Website:http:\\www.wavelink.com

Email: sales@wavelink.com

No part of this publication may be reproduced or used in any form, or by any electrical or mechanical means, without permission in writing from Wavelink Corporation. This includes electronic or mechanical means, such as photocopying, recording, or information storage and retrieval systems. The material in this manual is subject to change without notice.

The software is provided strictly on an “as is” basis. All software, including firmware, furnished to the user is on a licensed basis. Wavelink grants to the user a non-transferable and non-exclusive license to use each software or firmware program delivered hereunder (licensed program). Except as noted below, such license may not be assigned, sublicensed, or otherwise transferred by the user without prior written consent of Wavelink. No right to copy a licensed program in whole or in part is granted, except as permitted under copyright law. The user shall not modify, merge, or incorporate any form or portion of a licensed program with other program material, create a derivative work from a licensed program, or use a licensed program in a network without written permission from Wavelink. The user agrees to maintain Wavelink’s copyright notice on the licensed programs delivered hereunder, and to include the same on any authorized copies it makes, in whole or in part. The user agrees not to decompile, disassemble, decode, or reverse engineer any licensed program delivered to the user or any portion thereof.

Wavelink reserves the right to make changes to any software or product to improve reliability, function, or design.

The information in this document is bound by the terms of the end user license agreement.

Table of Contents

Chapter 1: Introduction

This document provides information about the Wavelink CE Secure application.

This section provides the following information:

- Document Assumptions
- Document Conventions
- About Wavelink CE Secure
- Overview of Steps

Document Assumptions

This document assumes that the reader has the following:

- Knowledge of wireless networks and wireless networking protocols
- Knowledge of TCP/IP, including IP addressing, subnet masks, routing, BootP/DHCP, WINS, and DNS
- Knowledge of the mobile devices to which you will be deploying the CE Secure configurations
- Basic knowledge of HTML (not required)

Document Conventions

The following section contains information about text-formatting conventions in this manual.

Table 1-1 lists the text-formatting conventions that are used in this manual.

Convention	Description
`Courier New`	Any time you interact with the physical keyboard or type information into a text box that information appears in the `Courier New` text style. This text style is also used for any file names or file paths listed in the text. Examples: The default location is `C:\Program Files\Adobe\FrameMaker7.1.` Press `CTRL+ALT+DELETE`.
Bold	Any time this document refers to an option, such as descriptions of different options in a dialog box, that option appears in the **Bold** text style. This is also used for tab names and menu items. Examples: Click **Open** from the **File** Menu.
italics	Italicized text is used to indicate the name of an application, window or dialog box. For example: The *Update Utility* dialog box. The *Profile Manager* dialog box.

Table 1-1: *Text-Formatting Conventions*

About Wavelink CE Secure

Wavelink CE Secure is a stand-alone application delivered through Wavelink Avalanche (MC or SE) that provides security on Windows CE mobile devices.

Wavelink CE Secure prevents information from being exposed to unauthorized users by locking devices that have been out of network range for a specified period of time and adding a secure sign-on screen and data management capabilities to CE mobile devices.

The Wavelink CE Secure system consists of a mobile device client, security server, and security administrator. CE Secure provides secure authentication by interfacing with Active Directory services and utilizing security information stored in NT, Active Directory, and LDAP databases.

This section provides information on the following parts of CE Secure:

- **Client.** This part of CE Secure is loaded on the mobile device.
- **Server**. This part of CE Secure runs as a Windows service.
- **Configuration utility**. This part of CE Secure allows you to configure the way the CE Secure client and server function.

Client Features

The CE Secure client is configured using the CE Secure Config utility, and then loaded onto the mobile device. This section provides information about the features of the CE Secure client.

Logon Screen

CE Secure can be configured to display a logon screen when it is secured. The logon screen requires a user name, password and domain before CE Secure will unlock the device for normal use. CE Secure authenticates users against the CE Secure Authentication Service.

You can configure the secure logon screen to display under the following conditions:

- **Power on**. The logon screen displays when the device is powered on or rebooted.
- **Time change**. The logon screen displays if CE Secure is configured to Sync Clock with Agent upon Update. When this option is selected, Avalanche Console updates the time on the mobile device each time the mobile device connects to the Avalanche Console.
- **Lock-out period exceeded**. The logon screen displays when the device has been out of network range beyond the configured lock-out period.

Cached Credentials

When you successfully logon to the mobile device through the CE Secure logon screen, CE Secure stores the user id and password on the mobile device in a secure, encrypted form. Then, if the device ever moves beyond the scope of the network and cannot contact the authentication server, you can still logon to the mobile device using correct credentials. CE Secure verifies the logon information against the cached credentials and, if the information matches, unlocks the device. Cached credentials work after a warm boot of the mobile device, but do not survive a cold boot. If you cold boot the device, you need to return within network range, contact the authentication server and logon to unlock the mobile device.

Note: CE Secure only unlocks the mobile device using cached credentials if the CE Secure lockdown frequency has not been exceeded.

Admin Unlock

The Administrative Unlock facility (Admin Unlock) can be used under a the following conditions:

1. Your mobile device is locked, no network access is available and no cached credentials are stored.
2. CE Secure is being used without a logon facility. In such a mode, CE Secure will lock the device when it is outside of network range. Since there is no logon facility enabled, Admin Unlock may be used to temporarily unlock the device.

To perform the Admin Unlock you (or the mobile device user) must contact the CE Secure administrator and provide the unlock key displayed on the mobile device.

Using the unlock key from the mobile device, the CE Secure administrator generates the unlock code from the CE Secure Configuration utility in Avalanche Console. The user enters this unlock code on the mobile device, the device unlocks, and any encrypted data is decrypted.

For Admin Unlock to work properly, the shared secret on the mobile device must match the shared secret the CE Secure Admin is using to generate the unlock code. The default shared secret is Wavelink. You can configure this shared secret in the CE Secure Configuration utility.

Once unlocked, the device may re-lock if the **Auth Frequency** is set to something other than **Never**. This ensures that even if a device is unlocked, that it will re-lock automatically if it is still outside of network coverage after the defined interval.

Support Mode

You can enter the CE Secure support mode from most of the screens on the client. Support mode gives you some of functionality of the CE Secure Config utility, allowing you to encrypt, decrypt, and delete data on the mobile device. You can view screens, statistics, log files, and configuration data. The support mode also provides roaming information, access point information, and logon statistics.

Support mode should not be used in a production environment and is provided for authentication troubleshooting purposes.

Customized Screens

The CE Secure client is able to display screens for its different states, such as its locked state, for example. These screens may be customized through the CE Secure Configuration Manager. Text and images may be added so that the information displayed is relevant to your organization.

Server

The CE Secure server runs as a native Windows Service and determines if the mobile device is on a known and safe network. It authenticates the user id and password that are entered on the locked device. The server has configurable log levels and supports encrypted request and response sequences.

CE Secure Config Utility

The CE Secure Config utility is launched from the Avalanche Console. You configure both client parameters and server parameters from the CE Secure Config utility. This section provides information about the utilities you can configure.

CE Secure Auth Servers

You can enter a list of the IP addresses or servers with fully qualified domain names where the CE Secure authentication service is installed and running. This service is required regardless of whether authentication is enabled on the client. This is because the CE Secure Auth Server also provides licensing to the client.

Server Watch

CE Secure uses a variety of servers to operate. If authentication is enabled, then the CE Secure Auth Server is used to authenticate the client credentials when connected to the network. However, for CE Secure to determine when it is away from the network, you must provide a list of servers to which it will be able to connect when the network is present. Provide a list of these servers in the Server Watch dialog. There are three types of servers supported; those that respond to PING requests, those that respond to HTTP requests and those that respond to CE Secure authentication requests. Specify these servers in the format of:

ping://<server IP or name>

http://<server IP or name>

auth://<server IP or name>

Protected Files

Protected resources include files and directories you want to encrypt or delete after the device has been out of network range for a specified amount of time. CE Secure allows you to specify which files you want to encrypt and the time frame in which you want the files and directories to encrypt. You can also configure the time frame in which you want those files deleted. For files and directories located within the encrypted files and directories list that you do not want encrypted or deleted, you can list excluded files and directories which will not be encrypted or deleted.

Refer to *Chapter 4: Configuring CE Secure* on page 37 for more information.

Admin Unlock Code

The CE Secure Config utility generates the unlock code when you perform an Admin Unlock. For more information about generating the Admin Unlock code from the CE Secure Config utility, refer to *Performing an Admin Unlock* on page 60.

For Admin Unlock to work properly, the shared secret on the mobile device must match the shared secret the CE Secure Admin is using to generate the unlock code. You can configure this shared secret in the CE Secure Config utility.

Custom Screens

The CE Secure Configuration utility provides the ability to change the different screen states (such as the logon screen, waiting to decrypt screen etc.) with customized text and graphics. You are allowed to specify customized .jpg and .png format images as well as add your own text to reflect your own needs.

Overview of Steps

The following steps are an overview of installing and configuring CE Secure:

1. Create a new Software Profile for CE Secure in the Avalanche Console.

2. Import the CE Secure software package.

3. Install the CE Secure Authentication Service. (Your PC should be a member of the domain if domain authentication is required. You also need to install the CE Secure service with Domain Administrative Rights).

4. Add licenses for your CE Secure product.

5. Configure the CE Secure settings. It is critical to ensure that the CE Secure Authentication service has a known IP which is accessible to client devices.

6. Start the CE Secure server service.

7. Deploy the CE Secure applications and configurations to the mobile device. To do this you should be familiar with the Avalanche deployment mechanism which may require you to associate the Software Profile for CE Secure with your devices.

Chapter 2: Installing CE Secure

This section provides the following information:

- CE Secure System Requirements
- Installing the CE Secure Software Package in Avalanche
- Installing the CE Secure Service
- Starting, Stopping and Removing the CE Secure Service
- Removing CE Secure from Avalanche

CE Secure System Requirements

This section lists the client and server requirements for running CE Secure.

Client Requirements

- Pocket PC 2003, Windows Mobile 2003, Windows Mobile 5, 6.x
- CE .Net 4.2, CE 5.0
- 200 KB of disk space
- Wavelink Enabler 3.50-12 or later versions. Enabler 4.06-13 or later is required if being used with the Wavelink Certificate Manager.

NOTE Ensure the Enabler is configured to **Monitor for Updates** or **Monitor and launch Enabler**. If the Enabler is configured to **Do not monitor or launch Enabler**, CE Secure will not operate as designed. For details on configuring the Enabler, refer to *Avalanche Enabler User Guide*.

Server Requirements

- Windows 2000, Windows XP
- Wavelink Avalanche MC or SE 4.x or later running on hardware as specified in the Avalanche MC/SE data sheets.

Installing the CE Secure Software Package in Avalanche

CE Secure is deployed as an Avalanche software package and must be installed in Avalanche for configuration and deployment to mobile devices.

To install the CE Secure software package:

1 Obtain the CE Secure installation software package.

NOTE For information on obtaining the CE Secure installation software package, contact Wavelink Customer Service. Refer to*Appendix A: Wavelink Contact Information* on page 81.

2 Launch Avalanche Console.

3 From the Tree View, select **Software Profiles**. A list of Software Profiles displays in the pane on the right.

4 Select **Add Profile**.

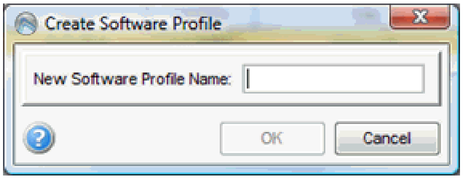


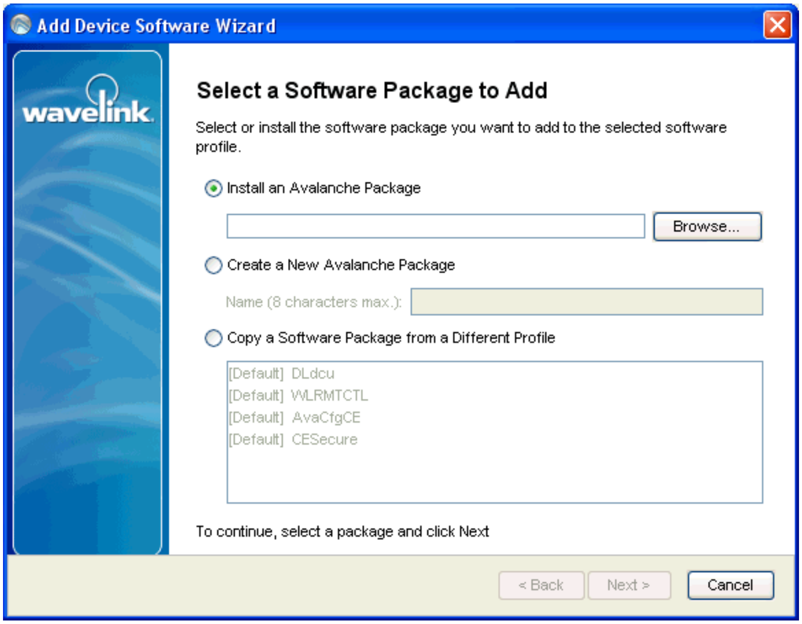
Figure 2-1. *Add Software Profile*

5 Enter a name for the profile and click **OK**.

6 From the **Software Profile List**, select the new profile.

7 Select the **Software Packages** tab and click **Add Package**.

The *Select Software Packages to Add* dialog box appears.



Select a Software Package to Add

Select or install the software package you want to add to the selected software profile.

● Install an Avalanche Package

○ Create a New Avalanche Package

Name (8 characters max.):

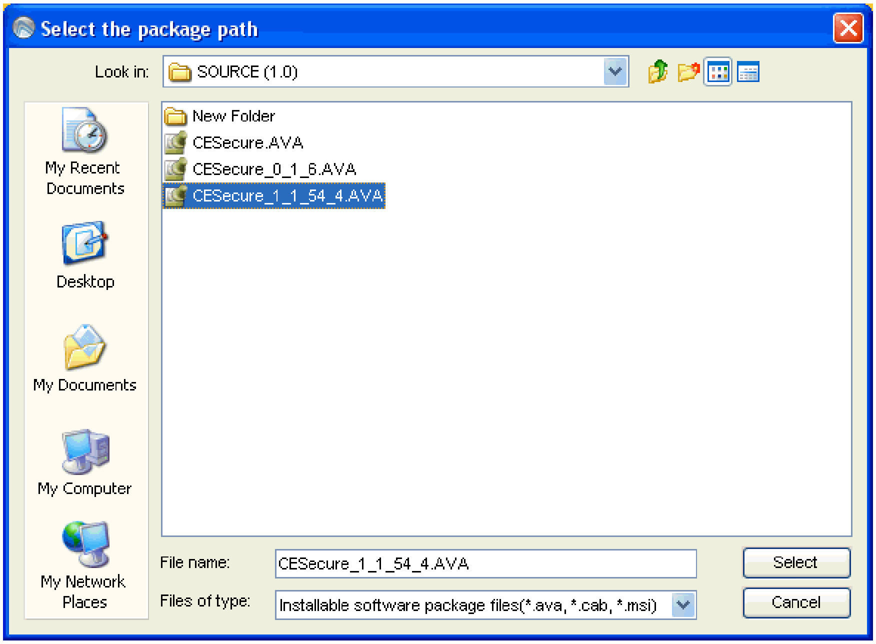
○ Copy a Software Package from a Different Profile

[Default] DLdcu
[Default] WLRMTCTL
[Default] AvaCfgCE
[Default] CESecure

To continue, select a package and click Next

Figure 2-2. *Select a Software Package to Add*

8 Click **Browse** and navigate to the CE Secure software package.



New Folder
CESecure.AVA
CESecure_0_1_6.AVA
CESecure_1_1_54_4.AVA

File name: CESecure_1_1_54_4.AVA

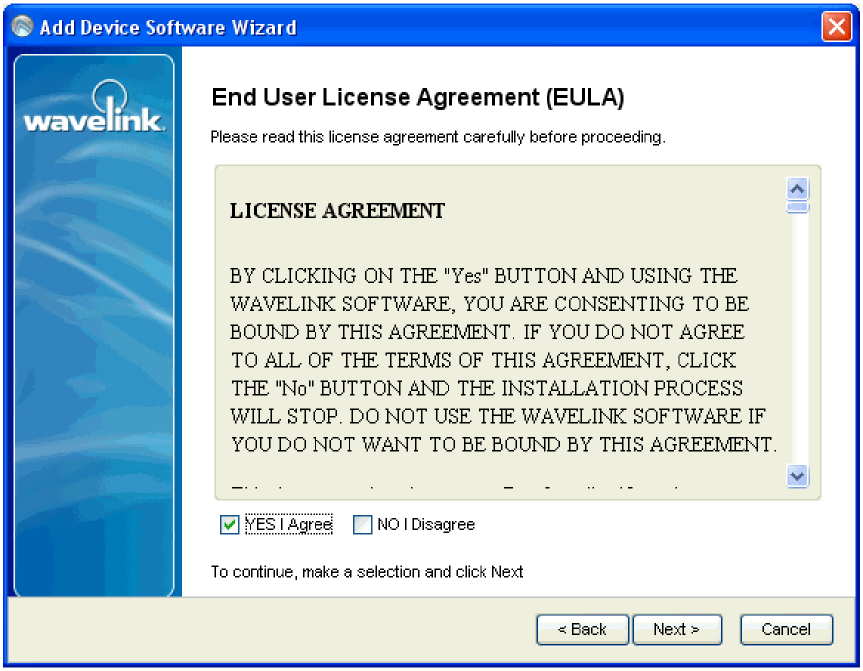
Files of type: Installable software package files(*.ava, *.cab, *.msi)

Figure 2-3. *Package Path*

9 Select the package and click **Select**.

10 In the *Add Device Software Wizard*. click **Next**.

The *License Agreement* dialog box appears.



End User License Agreement (EULA)

Please read this license agreement carefully before proceeding.

LICENSE AGREEMENT

BY CLICKING ON THE "Yes" BUTTON AND USING THE WAVELINK SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "No" BUTTON AND THE INSTALLATION PROCESS WILL STOP. DO NOT USE THE WAVELINK SOFTWARE IF YOU DO NOT WANT TO BE BOUND BY THIS AGREEMENT.

☑ YES I Agree ☐ NO I Disagree

To continue, make a selection and click Next

Figure 2-4. *License Agreement*

11 Click **YES, I agree** to agree to the software license agreement.

NOTE If you do not agree with the license agreement, you will not be able to complete installation.

The software package installs in the software profile you selected.

12 When the package has finished installing, click **Next**.

The *Configure Software Package* dialog box appears.

13 If you want to configure the package at this time, select from the list of available configuration utilities and click **Next.**

14 If you want to configure at a later time, click **Finish**.

Installing the CE Secure Service

Once you have installed the CE Secure package in Avalanche, you need to install CE Secure as a Windows Service. CE Secure is installed as a Windows Service to ensure CE Secure can always authenticate and license mobile clients, even when the Avalanche Console is not open.

The CE Secure Service can be installed most easily on the machine running the Avalanche Mobile Device Server, but can also be installed on any machine that can run the Avalanche Console. If you wish to install the CE Secure Authentication Server on the machine hosting the Avalanche Enterprise Server or Avalanche Mobile Device Server, launch the Avalanche Console from that system.

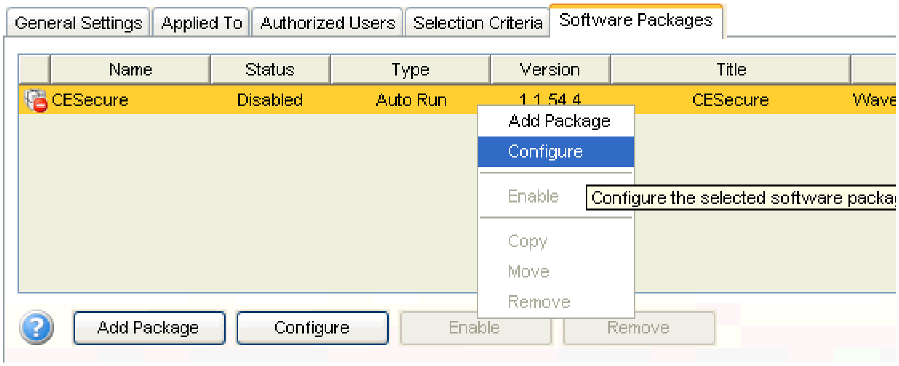
You install the CE Secure Service from the CE Secure software package configuration menu.

To install the CE Secure Service:

1 Ensure you have installed the CE Secure software package into the Avalanche Console.

2 Select the Software Profile containing the CE Secure software package.

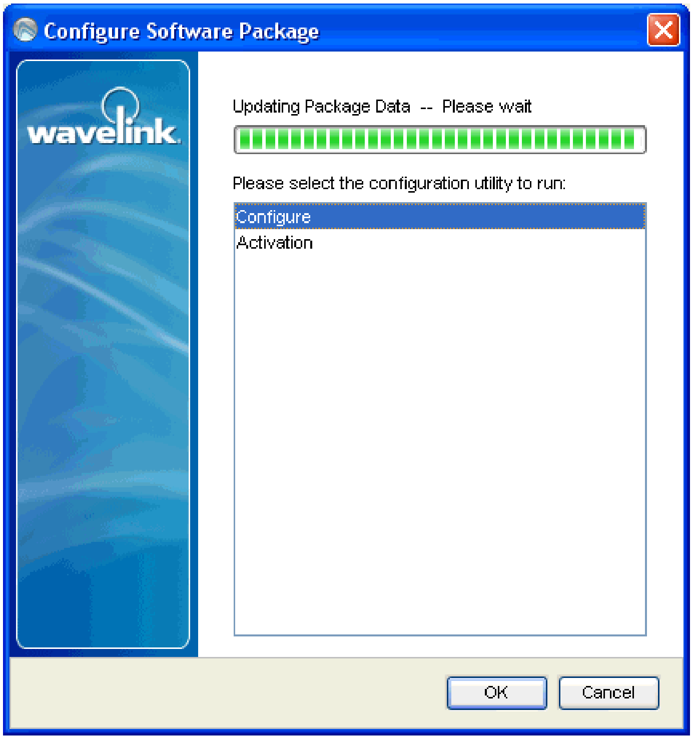
3 Select the CE Secure software package, right-click and select **Configure**.



	Name	Status	Type	Version	Title	
	CESecure	Disabled	Auto Run	1.1.54.4	CESecure	Wave

Figure 2-5. *Configure Software Packages*

The CE Secure configuration menu appears.



Configure Software Package

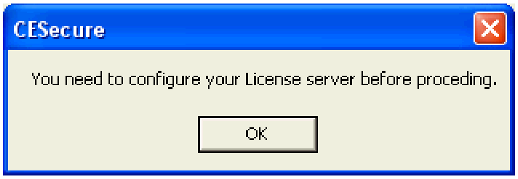
Updating Package Data -- Please wait

Please select the configuration utility to run:

Figure 2-6. *Configure Software Package Menu*

4 Select **Configure** and click **OK**.

A License Server message appears.



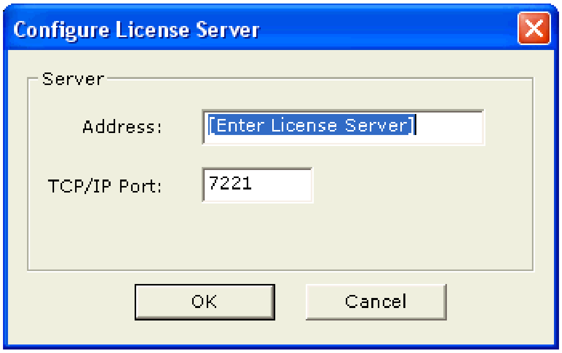
CESecure

You need to configure your License server before proceding.

Figure 2-7. *License Server Message*

5 Click **OK**.

The Configure License Server dialog box appears.



Configure License Server

Server

Address: [Enter License Server]

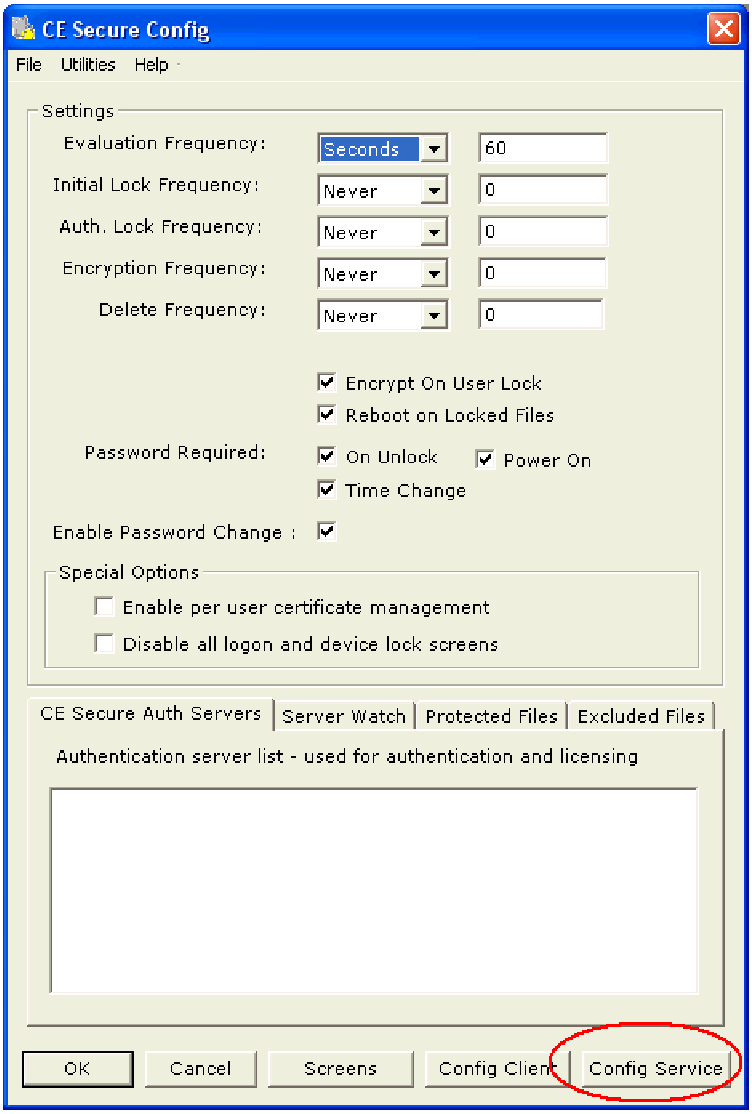
TCP/IP Port: 7221

Figure 2-8. *Configure License Server*

6 Enter the IP address of the server that will be used for the CE Secure Authentication Service and click **OK**.

NOTE The default TCP/IP Port is 7221. You can change this port if necessary.

The CE Secure Config utility appears.



Settings

Evaluation Frequency: Seconds 60

Initial Lock Frequency: Never 0

Auth. Lock Frequency: Never 0

Encryption Frequency: Never 0

Delete Frequency: Never 0

☑ Encrypt On User Lock

☑ Reboot on Locked Files

Password Required: ☑ On Unlock ☑ Power On

☑ Time Change

Enable Password Change : ☑

Special Options

☐ Enable per user certificate management

☐ Disable all logon and device lock screens

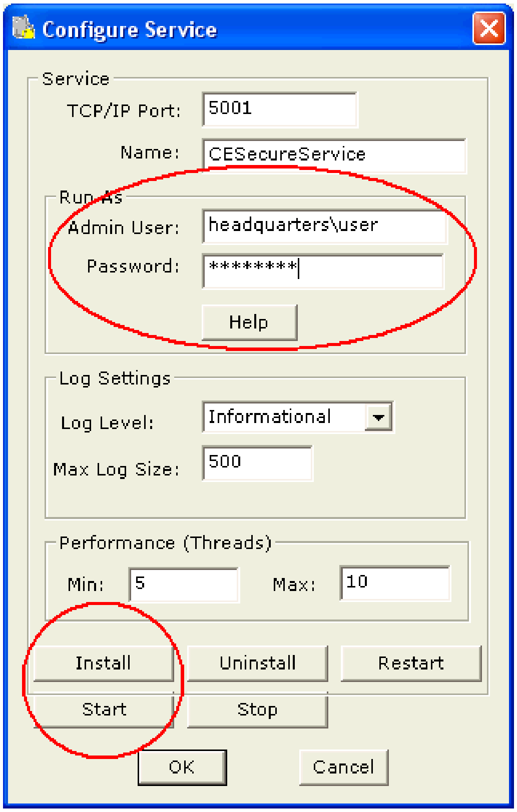
CE Secure Auth Servers | Server Watch | Protected Files | Excluded Files

Authentication server list - used for authentication and licensing

Figure 2-9. *Configuration Manager*

7 Click **Config Service**.

The *Configure Server* dialog box appears.



Configure Service

Service

TCP/IP Port: 5001

Name: CESecureService

Run As

Admin User: headquarters\user

Password: ********

Log Settings

Log Level: Informational

Max Log Size: 500

Performance (Threads)

Min: 5 Max: 10

Figure 2-10. *Configure Service*

8 In the **Run As** section, enter the **Admin User** in the form of `domain\username`.

9 Enter a **Password**.

NOTE The domain and username must have domain administrative rights. If they do not, some features such as password changes on the mobile device will fail to operate.

---

10 Once a domain administrative account is associated with the CE Secure Authentication Service, it may be installed. Click **Install** and then click **Start**.

The service is installed and started.

Starting, Stopping and Removing the CE Secure Service

The CE Secure service may be stopped, started, uninstalled or restarted as needed from the *Configure Service* dialog box (**CE Secure Config utility > Config Service**).

Removing CE Secure from Avalanche

To remove CE Secure completely you need to stop the CE Secure service, and then delete the software package from the **Software Profiles**. Once you delete the package from the Avalanche Console, you can then delete the orphan CE Secure package on the device. If you are using Avalanche MC, you must perform a Universal deployment before a removal action takes effect.

To delete the software package from the Management Console:

1 Right-click the CE Secure software package from the **Software Profile**.

2 Select **Configure Package > Config Service** and click **Stop Service**.

3 Click **Uninstall**.

The CE Secure Service is uninstalled.

4 Exit the CE Secure Config utility.

5 In the Avalanche Console, navigate to the software profile containing the CE Secure package.

6 Click **Edit** and then right-click the CE Secure software package in the **Software Packages** tab.

7 Click **Remove**.

The deleted package no longer appears in the console.

If you are using Avalanche MC, use the Task Manager to schedule a Universal Deployment. This ensures that the Avalanche Servers are informed of the pending package deletion.

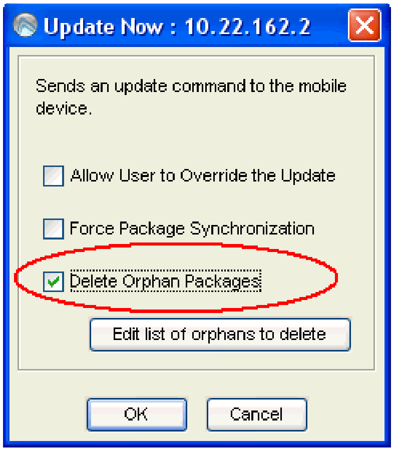
The CE Secure package on the mobile device is now an orphaned package and should be removed from the device..

To delete the orphaned CE Secure software package from a mobile device:

1 Ensure you have deleted the CE Secure software package from the Avalanche Console.

2 From the Mobile Device Inventory, right-click the mobile device and select **Update Now.**

The *Update Now* dialog box appears.



Sends an update command to the mobile device.

□ Allow User to Override the Update

□ Force Package Synchronization

☑ Delete Orphan Packages

Figure 2-11. *Delete Orphan Packages*

3 Select **Delete Orphan Packages** and click **OK**.

If you disabled the software package (but did not remove it), the status of the package will appear in the **Software Packages** tab as **Orphaned**.

The next time the mobile device checks in, CE Secure will be removed. You can also remove orphaned packages from Mobile Device Groups. Refer to Avalanche documentation for more information.

Chapter 3: Licensing

CE Secure requires a license for full functionality. You can access and configure the CE Secure Console without a license, but you will not be able to communicate with a mobile device.

CE Secure licensing is based on a per-mobile device. This means that CE Secure can manage one mobile device for each license.

Licenses do not expire. Once a license is granted to a device, it is perpetual and permanently allocated from the license pool. Once the license pool is exhausted, please contact Wavelink to obtain more licenses.

This chapter provides the following licensing information:

- Types of Licenses
- Wavelink License Server
- Activating CE Secure Licenses
- Changing the License Server
- Verifying Licenses
- Explaining License Checks
- Example Licensing Screens

Types of Licenses

CE Secure requires one CE Secure license for each mobile device to which you want to connect. To obtain CE Secure licenses, please contact Wavelink Customer Service.

There are two types of licenses you can purchase for CE Secure:

- Base Licenses
- Maintenance Licenses

Base Licenses

A base license authorizes you to the version of CE Secure that you purchased and any builds associated with that version. For example, if you purchased a CE Secure 1.1 license, then you are entitled to use 1.1- xx Avalanche builds. If you want to use the features available in later builds (such as 1.2 onwards), then you must either buy a 1.2 base license for your mobile devices, or you must purchase a maintenance license for your 1.1 devices. A Base license provides for minor upgrades and code changes, but does not allow major upgrades and updates to CE Secure. Base licenses do not expire.

Maintenance Licenses

A maintenance license allows you to upgrade CE Secure when new major versions of CE Secure become available. For example, a maintenance license allows you to upgrade from CE Secure 2.x to CE Secure 3.x. Maintenance licenses are valid only through a specific date. After the expiration date, if you attempt to upgrade CE Secure, it will revert to operating in demo mode.

Wavelink License Server

License Server is a Wavelink application that runs on a host system and as part of Avalanche software packages. The License Server is responsible for supplying licenses to mobile devices that are using CE Secure.

The License Server is a service that starts automatically and includes functionality for CE Secure with Avalanche 4.0 and later. If, you are using an older version of Avalanche, please contact Wavelink Customer Service to request information about obtaining the CE Secure License Server Update patch for Avalanche 3.x.

The License Server operates on port 7221. For the License Server to function properly, this port needs to be open or not blocked by firewall.

Installing the License Server

The License Server is installed as a service and starts automatically.

To install the License Server:

1 Obtain the License Server installation file.

2 Double-click the `.exe` file to begin installation.

3 Use the InstallShield Wizard to complete the installation.

The License Server is installed as a service on your machine.

Activating CE Secure Licenses

After you install the CE Secure software package (refer to *Installing the CE Secure Software Package in Avalanche* on page 14), you are asked to activate it with a valid license code. This code uses a technique called nodelocking, in which CE Secure is licensed only for a specific computer/mobile device 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 CE Secure 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.

This section provides the following information about activating your CE Secure license:

- Launching the CE Secure License Activator
- Activating Demo Mode
- Activating CE Secure Licenses

Launching the CE Secure License Activator

Wavelink provides a license Activator packaged with Avalanche MC and with the CE Secure package. You can access the Activator to install licenses for CE Secure.

Launching the Activator in Avalanche MC

You can launch the activator from the **Start** menu or from the CE Secure software package if you are using Avalanche.

To launch the activator for Avalanche:

- Select **Start > Programs > Wavelink Avalanche> Activate**.

  -Or-

- Right-click the CE Secure software package in the Software Profile tab and select **Configure**. From the drop-down list, select **Activation**.

NOTE For more information about Avalanche, refer to the *Wavelink Avalanche MC (or SE) User Guide*.

Activating CE Secure

When you activate CE Secure, a license file called `wavelink.lic` is installed on your system. This file provides the information the product needs to operate. There are three methods of activating your CE Secure license:

- Activating Automatically
- Activating Manually
- Importing a License

Activating Automatically

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

When you use the automatic activation method, Avalanche connects with a secure Wavelink web site to verify your license and nodelock, and a license file is sent to your host system.

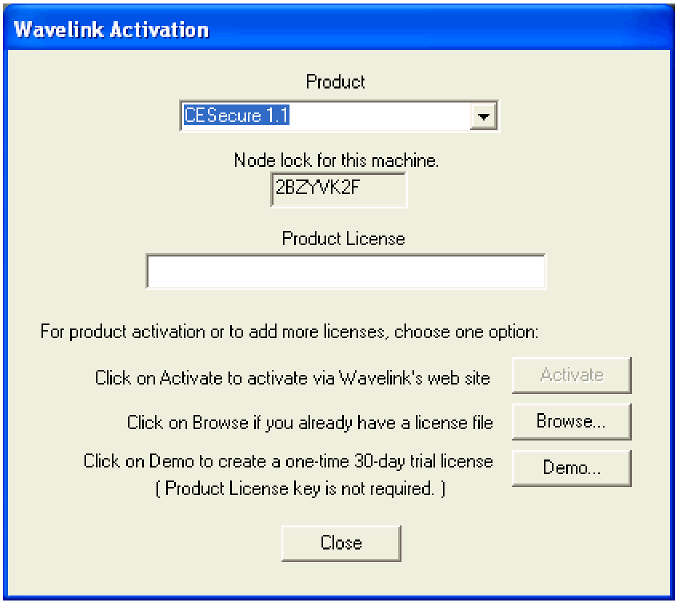
The license file called `wavelink.lic` is installed on your system, which provides the information the product needs to operate.

To activate CE Secure:

1 Obtain the CE Secure product licensing code from Wavelink**.**

NOTE You receive this information in an e-mail from Wavelink upon purchasing Wavelink CE Secure. Contact Wavelink Customer Service if you have not received this e-mail.

2 Access the Activator.



Wavelink Activation

Product

CESecure 1.1

Node lock for this machine.

2BZYVK2F

Product License

For product activation or to add more licenses, choose one option:

Click on Activate to activate via Wavelink's web site

Click on Browse if you already have a license file

Click on Demo to create a one-time 30-day trial license
(Product License key is not required.)

Figure 3-1. *Wavelink Activator*

3 From the **Product** drop-down list, select **CE Secure**.

4 Type your license number in the **Product License** text box.

5 Click **Activate**.

The Activator 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, specifying your licensing information and asking if you want to save the information.

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

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:

- **NodeLock for the machine**. You can get this information from the Activator dialog box.

- **Product License**. You can get this information from the e-mail you received from Wavelink upon purchasing CE Secure.
- **E-mail Address**. You need a valid e-mail address. This is where the license file will be sent.

To activate CE Secure:

1 Gather the information needed to license CE Secure.

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

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

4 Select which Wavelink Product you are activating.

5 Enter your registration information in the **Registration** region. (This step is optional.)

6 Enter a valid e-mail address.

7 Click **Activate License**.

When you click **Activate License**, the Wavelink activation server verifies the information you entered and then e-mails the `wavelink.lic` file to the e-mail address you entered.

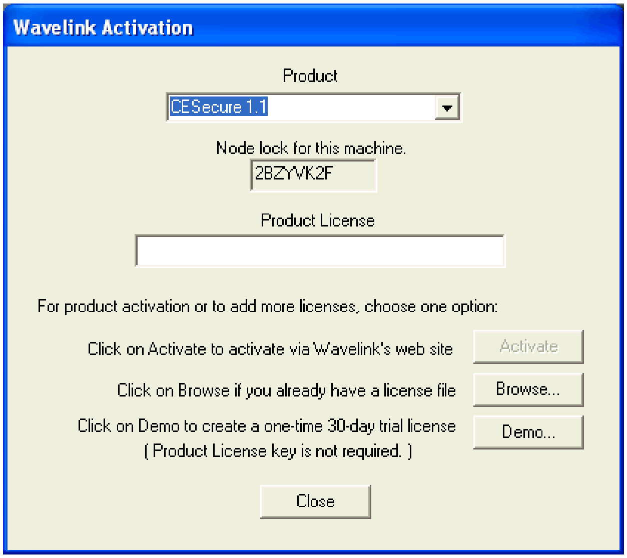
8 Check your e-mail to ensure you received the `wavelink.lic` file and then follow the steps to import a license file.

Importing a License

If you already have a license file for CE Secure or you have received the `wavelink.lic` file using the manual activation method, you can activate the license by importing it into the Activator.

To import a license:

1 Access the Activator.



Wavelink Activation

Product: CESecure 1.1

Node lock for this machine.: 2BZYVK2F

Product License

For product activation or to add more licenses, choose one option:

Click on Activate to activate via Wavelink's web site

Click on Browse if you already have a license file

Click on Demo to create a one-time 30-day trial license
(Product License key is not required.)

Figure 3-2. *Wavelink Activation*

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 Demo Mode

If you are installing CE Secure for demonstration purposes, you can run the product in demo mode. Demo mode gives you full CE Secure functionality on two mobile devices for 30 days.

To activate demo mode:

1 Access the Activator.

The *Wavelink Activation* dialog box appears.

2 Click **Demo**.

CE Secure will run in demo mode for up to 30 days.

Generating a License Manually

If for some reason the mobile device is unable to obtain a license for CE Secure, you can generate a license manually. This may happen if there is no active connection to the authentication/license server. When you generate a license code, CE Secure obtains a valid license code from the License Server and reserves it for use with your mobile device.

You can only generate a license manually after you have configured CE Secure and downloaded it to your mobile device. For detailed information, refer to *Chapter 4: Configuring CE Secure* on page 37 and *Deploying CE Secure to the Mobile Device* on page 57.

To generate a license manually:

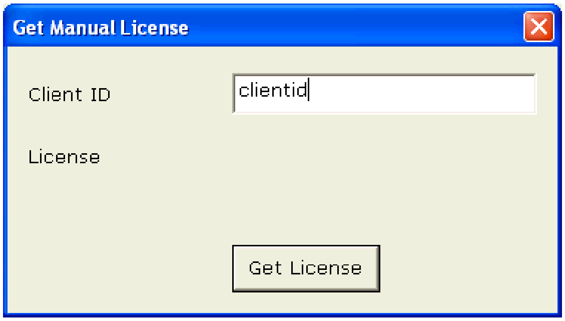
1 From the *CE Secure Logon* screen on the mobile device, click **Register Manually**.

The *Register Manually* screen appears.

2 Make note of the **Client ID**.

3 From the CE Secure Config utility on your PC, select **Utilities > Licensing > Generate License Manually.**

The *Generate License* dialog box appears.



Get Manual License

Client ID: clientid

License

Figure 3-3. *Generate Unlock Code*

4 In the **Client ID** text box, enter the **Client ID** displayed in the *CE Secure Register Manually* screen on the mobile device.

5 Click **Get License**.

A license code displays.

6 Enter the license in the **License** text box on the mobile device.

NOTE If the virtual keyboard is not displayed on the CE Secure Logon screen, click the **Keyboard** button

7 Click **Register**.

The device will authenticate the information and license CE Secure for this mobile device.

Changing the License Server

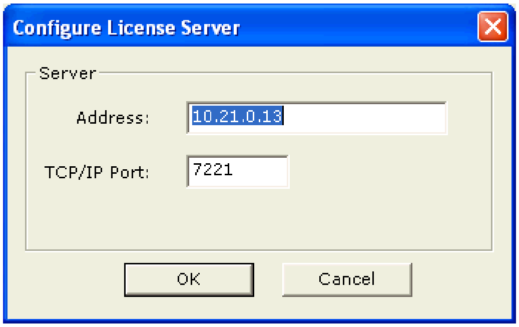
You can change the License Server and port number from the **Licenses** tab of the CE Secure Config utility. For details about launching the CE Secure Config utility, refer to *Chapter 4: Configuring CE Secure* on page 37.

To change the License Server:

1 Launch the CE Secure Config utility.

2 Select **Utilities > Licensing > Configure**.

The *Configure License Server* dialog box appears.



Address: 10.21.0.13

TCP/IP Port: 7221

Figure 3-4. *Configure License Server*

3 In the **Address** text box, enter the IP address of the License Server you want to use.

4 In the **TCP/IP Port** text box, enter the port number on which you want the License Server to run.

5 Click **OK** to save your changes and return to the CE Secure Config utility.

Verifying Licenses

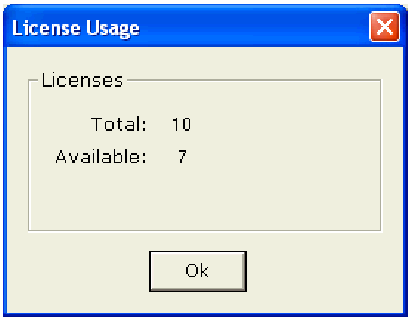
From the CE Secure Config utility, you can compare the total number of CE Secure licenses with the number of licenses available.

To verify licenses:

1 Launch the CE Secure Config utility.

2 Select **Utilities > Licensing > Usage**.

The *License Usage* dialog box appears.



Total: 10
Available: 7

Figure 3-5. *Verifying Connections*

In the **Licenses** region, you can view your total number of licenses in use compared to your total available licenses.

Explaining License Checks

This section provides information about how CE Secure operates when attempting to obtain or check licensing.

CE Secure performs license checks upon each evaluation interval. Therefore, CE Secure is constantly ensuring it can contact the License Server and obtain a license. The following table describes the license check method. In these instances, CE Secure has never been licensed.

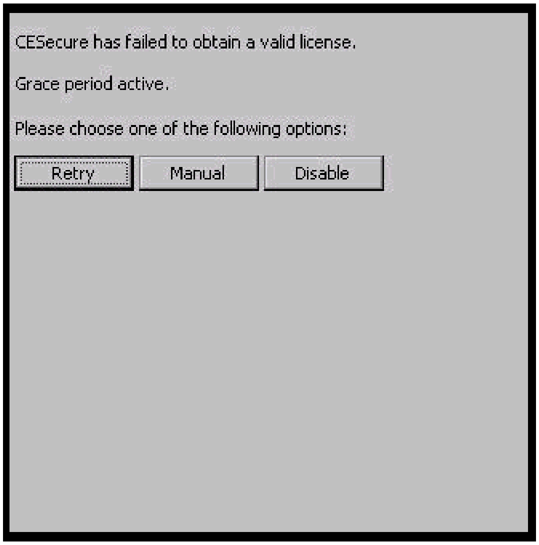
If	Then
The mobile device can contact the License Server but there are no available licenses	CE Secure notifies the user that it can not obtain any licenses and terminates.
The mobile device can contact the License Server and there are available licenses	No license dialog box appears and the CE Secure functions as normal.

Table 3-1: *If CE Secure Has Never Been Licensed*

Example Licensing Screens

This section provides information about the licensing screens in CE Secure.

The first line in the CE Secure Licensing dialog box indicates that CE Secure has failed to obtain a license. The second line provides the status message. This status message changes depending on the circumstances of the device and the reason it failed to license.



CESecure has failed to obtain a valid license.

Grace period active.

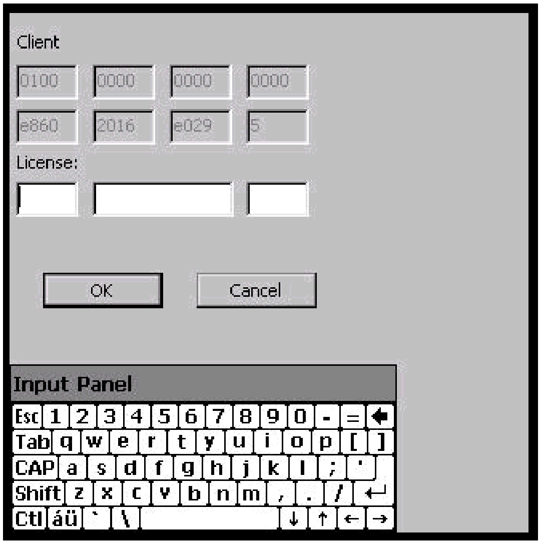
Please choose one of the following options:

Figure 3-6. *CE Secure Licensing*

You can then select the following options:

- **Retry**. When you push this button, the CE Secure attempts to contact the License Server or obtain a license again.

- **Manual**. When you push this button, the *Enter License Manually* dialog box appears. Use the **Client** code listed in this dialog box to obtain a License from your License Server administrator. Enter the license in the available text boxes and click **OK**.



Client

0100 0000 0000 0000

e860 2016 e029 5

License:

OK
Cancel
Input Panel
Esc 1 2 3 4 5 6 7 8 9 0 - =
Tab q w e r t y u i o p [ ]
CAP a s d f g h j k l ; '
Shift z x c v b n m , . /
Ctl áü ` \ ↓ ↑ ← →

Figure 3-7. *Enter LIcenses Manually Dialog Box*

- **Disable**. This button disables the license checks for 24 hours when you are in a grace period.

Chapter 4: Configuring CE Secure

You configure CE Secure settings from the CE Secure Config utility. This section provides information about the following CE Secure configuration tasks:

- Accessing the CE Secure Config Utility
- Configuring Administrator Settings
- Configuring Client Options
- Configuring Service Settings

Accessing the CE Secure Config Utility

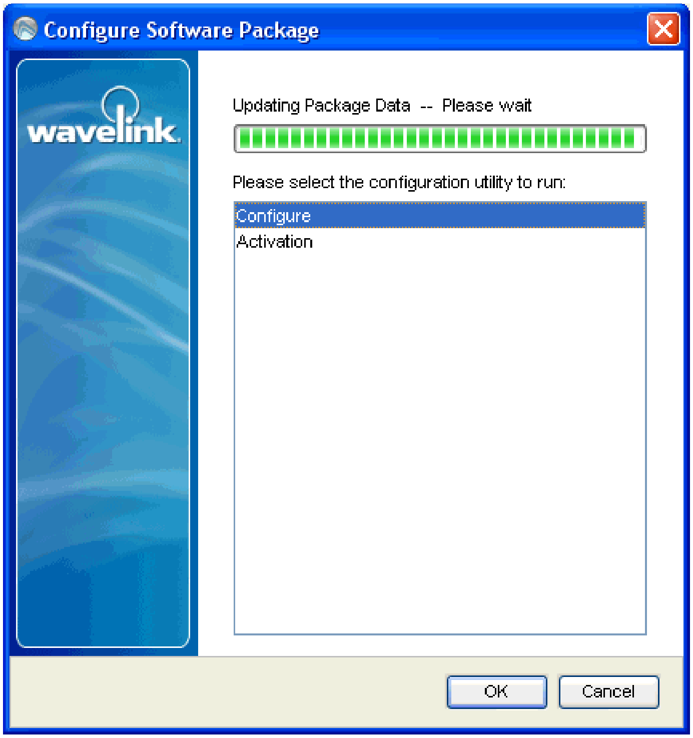
Use the CE Secure Config utility to configure all CE Secure settings. You can access CE Secure Config from the Avalanche console.

NOTE The CE Secure Config utility may also be referred to as the Configuration Manager.

To access the CE Secure Config utility:

1. From the **Software Profiles List** select the software profile to which CE Secure was installed.
2. From the **Software Packages** tab, right-click the CE Secure package and select **Configure**.

   The *Configure Software Package* dialog box appears.



Configure Software Package

Updating Package Data -- Please wait

Please select the configuration utility to run:

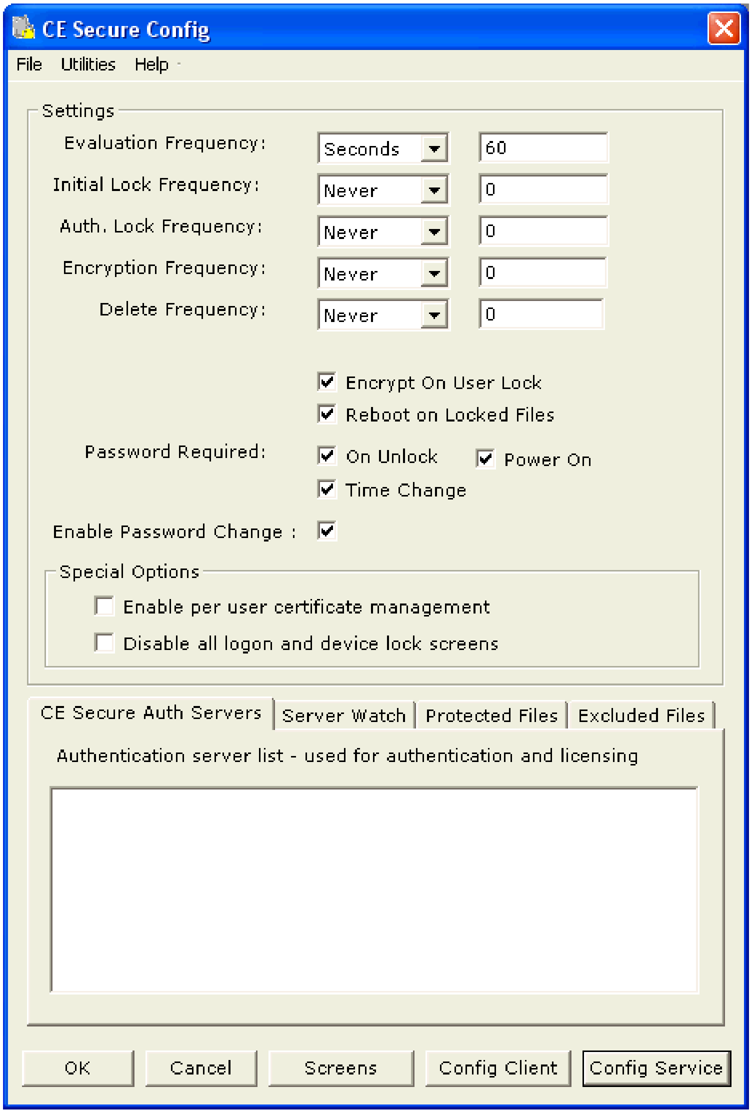
Configure

Activation

Figure 4-1. *Configure Software Package*

3 From the menu, select **Configure** and click **OK**.

The CE Secure Config utility appears.



Settings

Evaluation Frequency: Seconds 60

Initial Lock Frequency: Never 0

Auth. Lock Frequency: Never 0

Encryption Frequency: Never 0

Delete Frequency: Never 0

☑ Encrypt On User Lock

☑ Reboot on Locked Files

Password Required: ☑ On Unlock ☑ Power On

☑ Time Change

Enable Password Change : ☑

Special Options

□ Enable per user certificate management

□ Disable all logon and device lock screens

CE Secure Auth Servers | Server Watch | Protected Files | Excluded Files

Authentication server list - used for authentication and licensing

Figure 4-2. *CE Secure Config Utility*

Configuring Administrator Settings

The Administrator Settings are the settings found in the CE Secure Config utility. The CE Secure Config utility contains two areas of configuration, the lockdown settings and the configuration tabs. This section provides the following information:

- Configuring the CE Secure Lockdown Settings
- Configuring Information in the Configuration Tabs

Configuring the CE Secure Lockdown Settings

Use the lockdown settings to configure when and under what circumstances you want the mobile device to lock. Once the device is locked, the device either needs to be brought back into range of the network and/or the user must enter valid credentials.

To configure CE Secure lockdown settings:

1. Determine under what circumstances you want the mobile device to lock.
2. In the **Settings** section of the CE Secure Config utility, enter the frequency of each lock option.

NOTE By default, the CE Secure lockdown settings are configured to never lock, encrypt files, or delete files.

The following is a list of the CE Secure lockdown settings you can configure.

Evaluation Frequency This is the frequency with which CE Secure checks the **Server check** list to ensure it is in a safe state.

Initial Lock Frequency Specify how long the mobile device can be out of contact with the networks and/or servers listed in the Network and Server Watch tabs before initiating lockdown mode. .

Auth. Lock Frequency Once the device is outside of the network (and is in a vulnerable state), it may be unlocked by using cached credentials or by using the administrative unlock facility. However, if this option is selected, it will lock again after the defined period expires, if the device is unlocked and away from the network.

Encryption Frequency Specify the time that must expire before CE Secure will encrypt specified files on the mobile device when the device is beyond the scope of the network (cannot contact the servers listed in the Server Watch tabs).

Delete Frequency

Specify the time that must expire before the CE Secure will delete specified files from the mobile device when the device is beyond the scope of the network (cannot contact the servers listed in the Server Watch tabs). .

Encrypt on User Unlock

Enable this option if you want CE Secure to encrypt Protected Files upon a user unlock from the mobile device.

Reboot on Locked Files

Enable this option if you want CE Secure to reboot the mobile device when trying to encrypt Protected Files.

This option will reboot the mobile device if one of the Protected Files is in use when CE Secure begins to encrypt Protected Files. Because the file is open, CE Secure can not encrypt it. When the device reboots, the file will close and CE Secure is able to encrypt the files.

Password Required: On Unlock

Enable this option if you want to require a login (User ID and Password) to unlock the device when the device is locked.

If this option is enabled, CE Secure requires a valid User ID and Password to unlock the mobile device in any locked circumstance (whether you are within the range of the network or not). When this option is enabled, CESecure does not automatically unlock the mobile device if the device returns within network range, but requires a valid User ID and Password to login and unlock the mobile device.

If the On Unlock option is disabled and the device moves beyond the scope of the network, the Admin Unlock screen displays. If you return within network range and have not attempted to log on to the mobile device (by accessing the Logon screen), CE Secure will automatically unlock the mobile device. If you return with network range and have attempted to logon to the mobile device, CE Secure will not automatically unlock the mobile device. You will need a valid User ID and Password to unlock the device.

Password Required: Power On

Enable this option if you want to require a user id and password to unlock the mobile device after the device is rebooted or powered on.

Password Required: Time Change

Enable this option if you want to require a user id and password to unlock the mobile device after a time change.

Enable Password Change

If Active Directory requires that the end-user change their password at the next logon, then this facility allows them to do this from the mobile device.

Enable Per User Certificate Management	This facility is used when CE Secure is used in conjunction with the Wavelink Certificate Manager. Please refer to the Certificate Manager documentation for more information.
Disable all logon and device lock screens	If you are only using CE Secure to provision 802.1X certificates using the Wavelink Certificate Manager and do not wish to have any form of logon or file protection capabilities, select this option.

Configuring Information in the Configuration Tabs

Use the CE Secure configuration tabs to perform the following tasks:

- Configuring CE Secure Authentication Servers
- Configuring Servers to Monitor
- Adding Protected Files
- Adding Excluded Files

Configuring CE Secure Authentication Servers

Use the **CE Secure Auth Servers** tab in the CE Secure Config utility to enter the IP addresses of the authentication servers where the authentication and licensing service is installed and running. The authentication servers listed verify user id and password information entered in CE Secure on a locked mobile device.

To configure the Authentication servers:

1. From the CE Secure Config utility, select the **CE Secure Auth Servers** tab.
2. Enter the IP addresses of the servers you want to use as authentication servers.

   This tab must be populated with at least one CE Secure Service IP address. This is the service through which the CE Secure client obtains its license.

Configuring Servers to Monitor

Use the **Server Watch** tab to enter the host names of the servers you want to monitor. These are servers that the device may encounter. If the mobile device is not within the scope of the network (cannot contact a network, a server, or both), CE Secure locks the device after the lock frequency expires.

If you enter a server in the **Server Watch** tab, CE Secure must be able to contact one server to remain within the scope of the network and unlocked upon expiration of the lock frequency. Servers can be entered into the **Server Watch** tab using the following formats:

- `auth://<host>`
- `ping://<host>`
- `http://<url>`

You can enter hosts using dotted IP addresses (192.168.1.1) or by name (www.wavelink.com).

To configure servers:

1 From the CE Secure Config utility, select the **Server Watch** tab.

2 Enter the IP addresses of the servers you want the mobile device to contact.

Adding Protected Files

Use the Protected Files tab to enter the file path for any files or directories you want encrypted or deleted once the device has been out of network range for the specified amount of time. For information about configuring the encryption or deletion time, refer to *Configuring the CE Secure Lockdown Settings* on page 40. These files and directories are decrypted when the user unlocks the mobile device by logging in or performing an Admin Unlock.

To add files to the Protected Files tab:

1 From the CE Secure Config utility, select the **Protected Files** tab.

2 Enter the file path names of any files and directories you want encrypted or deleted after the device has been out of network range.

Adding Excluded Files

Use the **Excluded Files** tab to enter the file path for files and directories you want to exclude from the Protected files list. These files and directories will not be encrypted or deleted if the device goes out of network range. Excluded Files are files and directories that may be included within the **Protected Files** path but that you want to exclude from being encrypted or deleted.

To add files to the Excluded Files tab:

1 From the CE Secure Config utility, select the **Excluded Files** tab.

2 Enter the file path names of any files and directories you want to exclude from the **Protected Files** list.

Configuring Client Options

You can configure the following client settings from the CE Secure Config utility:

- **Stop ActiveSync**. Enable this option if you want to stop ActiveSync upon device lock. The system will warn you if you have selected this option because once selected, the only way of communicating with the device will be over the network and, therefore, it must have a valid connection.

- **Disable Hardware Keys**. Enable this option if you want to disable the vendor specific device keys (shortcut keys) upon a device lock.

- **Keep Current User in Registry.** Enable this option to leave the current user login ID in the registry for any local program to access. This can be used to aid single sign-on.

- **Show Last Logon Information**. Enable this option to cache the user ID and domain and display it at the login screen when the device locks. This simplifies the login process since only a password needs to be supplied.

- **Show Support Mode**. Enable this option to display a diagnosis button on the client. The Diagnosis button (labeled Support Mode) also enables you to quit the CE Secure application. This should only be used for troubleshooting.

- **Show SIP Button.** Enable this option to display the client keyboard **Toggle** button. On devices without a touch screen you may wish to hide the keyboard toggle, since no Soft Input Panel (SIP) can be displayed. In cases where you have both SIP capable and non-SIP capable devices, create two Software Profiles – one with **Show SIP Button** enabled and another with it disabled.

- **Enable Advanced AP.** Enables a password protected API on the client to share password information. Refer to *Appendix B: Avalanche Advanced Properties* on page 83 for more information.

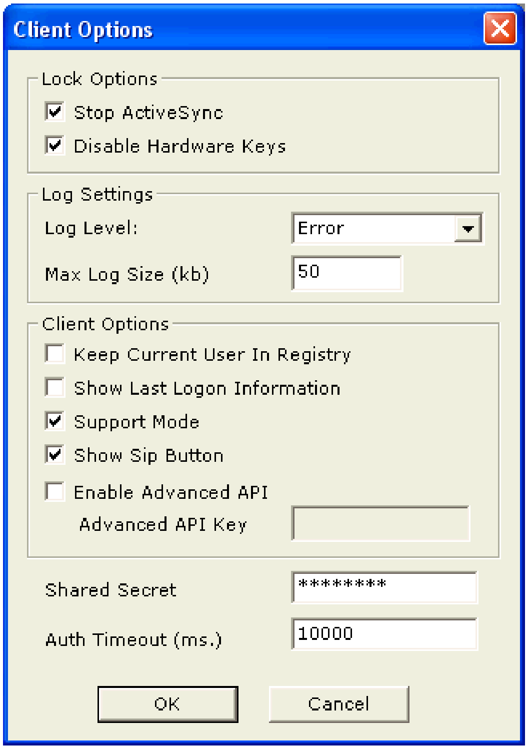
- **Shared Secret**. This is the secret used as the basis for performing administrative unlocks with keys.

- **Auth Timeout**. This is the amount of time the client gives the CE Secure authentication service to respond before another authentication attempt is made.

To configure lock options:

1 From the CE Secure Config utility, click **Config Client**.

The *Client Options* dialog box appears.



Client Options

Lock Options

☑ Stop ActiveSync

☑ Disable Hardware Keys

Log Settings

Log Level: Error

Max Log Size (kb) 50

Client Options

☐ Keep Current User In Registry

☐ Show Last Logon Information

☑ Support Mode

☑ Show Sip Button

☐ Enable Advanced API

Advanced API Key

Shared Secret ********

Auth Timeout (ms.) 10000

Figure 4-3. *Client Lock Options*

2 Configure the desired settings and then click **OK**.

Upon deployment or the next time a mobile device checks in, the device will receive the updated client settings.

Configuring Client Logging

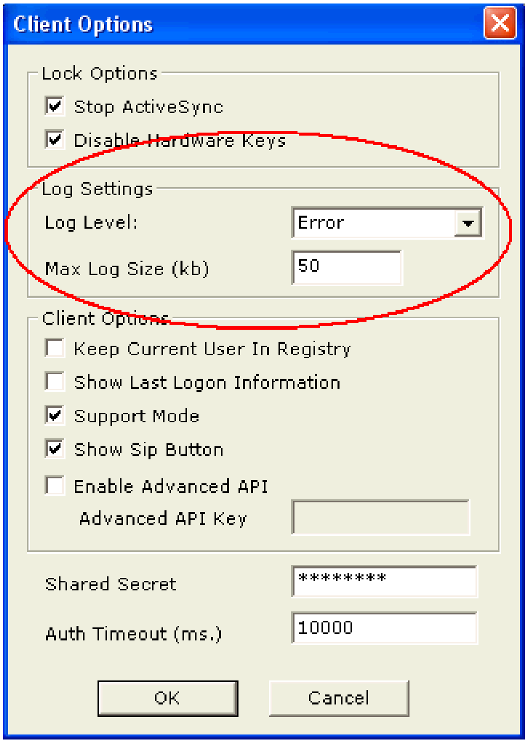
You can create log files for client and server information. The log file can be viewed from any plain text editor.

The client log is stored on the client with the default name CE Secure.log. The back versions of the CE Secure log files are stored with a 1-5 suffix. When a new log file is stored, all files are moved down one level: for example, CE Secure.log becomes CE Secure.log1 and CE Secure.log1 becomes CE Secure.log2, etc. No more than five log files are saved. Once there are five log files, CE Secure.log5 is deleted upon the creation of the next log file. New log files are created when the mobile device reboots or if a new CE Secure configuration is downloaded.

To configure the client log level:

1 From the CE Secure Config utility, click **Config Client**.

The *Client Options* dialog box appears.



Client Options

Lock Options

☑ Stop ActiveSync

☑ Disable Hardware Keys

Log Settings

Log Level: Error

Max Log Size (kb) 50

Client Options

☐ Keep Current User In Registry

☐ Show Last Logon Information

☑ Support Mode

☑ Show Sip Button

☐ Enable Advanced API

Advanced API Key

Shared Secret ********

Auth Timeout (ms.) 10000

Figure 4-4. *Client Log Settings*

2 From the **Log Level** drop-down menu, select the level at which you want to store client information.

3 In the **Max Log Size** text box, enter the maximum size you want the log level to reach before CE Secure creates a new file.

4 If you are finished configuring the client, click **OK** to return to the CE Secure Config utility.

NOTE If the log file exceeds the maximum log size, a new log file will be created automatically.

Configuring Service Settings

You can configure the service settings from the CE Secure Config utility..

This section provides the following information:

- Configuring Service Options
- Configuring the Service Log

Configuring Service Options

These options allow you to configure the TCP/IP port and performance threads for the service.

NOTE If you change the TCP/IP port, you need to stop and then restart the CE Secure service for the changes to take effect. For details on starting and stopping the CE Secure service, refer to *Starting, Stopping and Removing the CE Secure Service* on page 23.

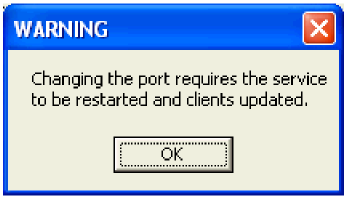
To configure server options:

1 From the CE Secure Config utility, click **Config Server.**

The *Configure Service* dialog box appears.

2 In the **Services** region, click in the **TCP/IP Port** text box.

A *WARNING* dialog box appears.



WARNING

Changing the port requires the service to be restarted and clients updated.

Figure 4-5. *WARNING Dialog Box*

NOTE If you change the TCP/IP port, you need to stop and then restart the CE Secure server for the changes to take effect.

3 Click **OK** and enter the **TCP/IP Port**.

4 In the **Performance** region, enter the minimum number of threads in the **Min Threads** text box.

5 In the **Performance** region, enter the maximum number of threads in the **Max. Threads** text box.

NOTE It is recommended that you only change the **Performance Thread**s settings under the direction of Wavelink Customer Support.

6 If you are finished configuring the server, click **OK** to return to the CE Secure Config utility.

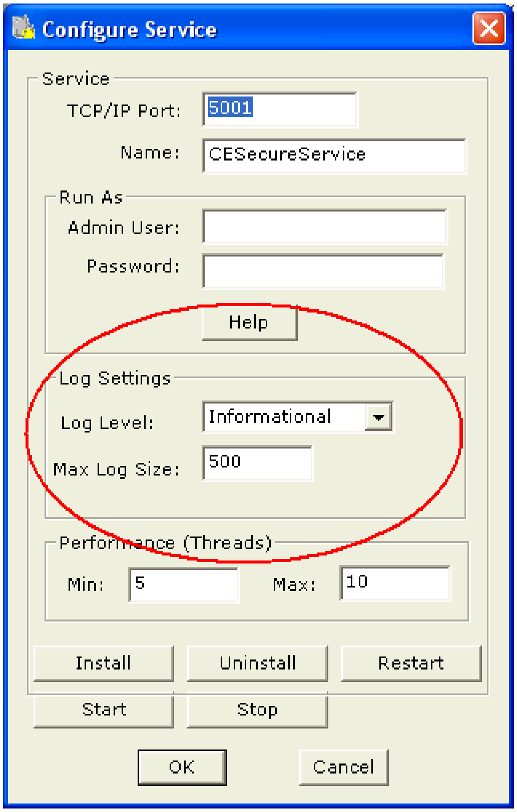
Configuring the Service Log

You can create log files for client and server information. The log file can be viewed from any plain text editor.

The server log is stored on the server with the default name CE SecureServer.log. The back versions of the CE SecureServer log files are stored with a 1-5 suffix. When a new log file is stored, all files are moved down one level, for example CE SecureServer.log becomes CE SecureServer.log1 and CE SecureServer.log1 becomes CE SecureServer.log2, etc. No more than five log files are saved. Once there are five log files, CE SecureServer.log5 is deleted upon the creation of the next log file. New log files are created when the mobile device reboots or if a new CE Secure configuration is downloaded

To configure the server log:

1 From the CE Secure Config utility, click **Config Server**.



TCP/IP Port: 5001
Name: CESecureService
Admin User:
Password:
Log Level: Informational
Max Log Size: 500
Min: 5
Max: 10

Figure 4-6. *Configure Service*

2 From the **Log Level** drop-down menu, select the level at which you want to log client information.

3 In the **Max Log Size** text box, enter the maximum size you want the log level to reach before CE Secure creates a new file.

NOTE If your log file exceeds the maximum log file, a new log file will be created automatically.

4 Click **OK** to return to the CE Secure Config utility.

Server Configuration Options

The following is a list of the Server Options configuration options:

TCP/IP

Enter the TCP/IP port. Both the client and the server use this port.

Min Threads

Enter the minimum number of performance threads.

Threads provide the ability to tune the server for certain performance scenarios. The threads available at any given time directly correspond to the number of simultaneous requests that can be processed.

NOTE These fields should only be changed under the direction of Wavelink Customer Support.

Max Threads

Enter the maximum number of performance threads.

Threads provide the ability to tune the server for certain performance scenarios. The threads available at any given time directly correspond to the number of simultaneous requests that can be processed.

NOTE These fields should only be changed under the direction of Wavelink Customer Support.

Log Level

Select from the drop-down list the level at which you would like to log information from the server.

Logging levels include:

- Critical. Indicates errors that cause CE Secure to fail to start.
- Errors. Indicates errors that are caused by configuration and/or communication problems.
- Warning. Indicates possible operational problems.
- Info. Documents the flow of operation.
- Debug. Used to diagnose program malfunctions or communication problems.

Max Log Size

Enter the maximum log size you want stored. Once this size is reached, CE Secure creates a new log file. The last five log files are stored on the mobile device.

Default: 500 kb

Chapter 5: Customizing Client Screens

This section provides information about customizing client screens in CE Secure.

- Overview of Customizing Screens
- Accessing the Display Configuration Utility
- Adding Images

Overview of Customizing Screens

CE Secure allows you to customize all the screens that appear on the CE Secure client on the device. You can customize screens using the Display Configuration utility. Both text and graphics may be added to the device screens as needed.

The following is an overview of the steps to create customized CE Secure client screens:

1. Access the Display Configuration utility.
2. Add images that you want to display on your screens to the image dialog box.
3. Select the screen you want to customize from the coordinating tabs.
4. Enter text and images in the **Header**, **Message**, and **Footer** tabs to customize the header, message, and footer sections of the screens.

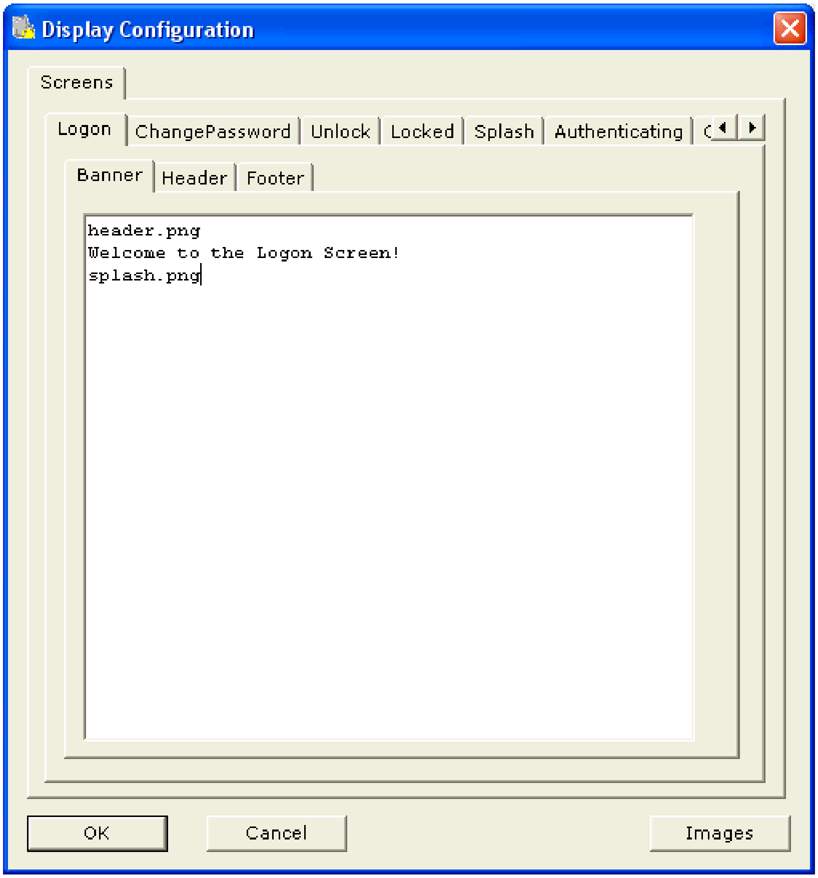
Accessing the Display Configuration Utility

The Display Configuration utility allows you to customize the different CE Secure screens.

To access the Display Configuration utility:

1. Access the CE Secure Config utility.
2. Click **Screens .**

   The Display Configuration utility opens.



```
header.png
Welcome to the Logon Screen!
splash.png
```

Figure 5-1. *Display Configuration Utility*

Banner, Header, and Footer Tabs

Using plain text you can enter text in the **Banner**, **Header**, and **Footer** tabs to customize the look of the banner, header and footer of the selected screen. Use the **Banner** tab to enter the file name to be used as a banner. This may be a `.png` or `.jpg` file. Ensure that the dimensions of the file will fit your target device.

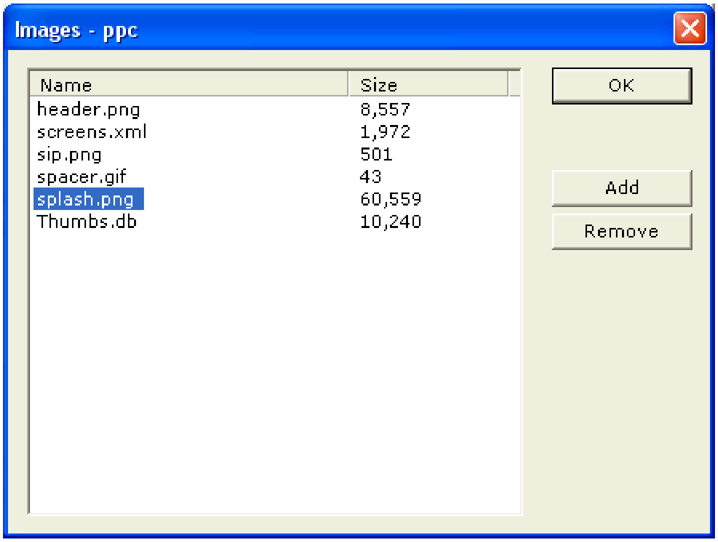
Adding Images

When you want to use images to customize your client screens you need to add the image file to the *Images* dialog box. You can use any image that has been added to the *Images* dialog box on any of the custom screens. Once the image has been added to the *Images* dialog box, you can type the name of that image in the text boxes to place that image on the selected screen.

To add an image:

1 From the Display Configuration utility, click **Images**.

The *Images* dialog box opens.



Name	Size
header.png	8,557
screens.xml	1,972
sip.png	501
spacer.gif	43
splash.png	60,559
Thumbs.db	10,240

Figure 5-2. *Images Dialog Box*

2 Click **Add** and navigate to the location of and select the image you want to add.

3 Click **Open**.

The image name will be added to the image list. This image is now available to use in your code.

Chapter 6: Common CE Secure Tasks

This section provides the information about common tasks you can perform using Wavelink CE Secure, including:

- Deploying CE Secure to the Mobile Device
- Unlocking the Mobile Device
- Performing User Lock on the Mobile Device
- Protecting Files

NOTE The Enabler on the mobile device must be configured to **Monitor for Updates** or **Monitor and launch Enabler**. If the Enabler is configured to **Do not monitor or launch Enabler**, CE Secure will not work.

The Enabler on the mobile device must also have the **Check for updates at start up** option enabled. If this option is not enabled and the mobile device is cold booted, the time clock on the mobile device will be inaccurate and CE Secure will not actively monitor for the authentication server.

For details about configuring these options in the Enabler, refer to the *Wavelink Enabler User's Guide*.

Deploying CE Secure to the Mobile Device

Once you have configured CE Secure in Avalanche, you can send the CE Secure client and the configurations to the mobile device. The first time you deploy CE Secure to the mobile device, the device will lock and require a logon or an Admin Unlock to unlock.

If you are using Avalanche MC, you will need to assign the software profile to the regions and locations you want to receive CE Secure and then perform a Universal Deployment (**Tools > Task Scheduler**) to send the software profile settings to your regions and locations. If you are using Avalanche SE, the profile will be automatically applied to My Enterprise and the devices will receive the profile settings upon the scheduled update or device next check in. For more information, refer to your *Avalanche User Guide*.

The following steps provide information about updating a single mobile device at a time.

To deploy CE Secure to the mobile device:

1. Complete CE Secure configurations in the CE Secure Config utility and click **OK**.
2. Save the changes to the software profile.
3. From the Mobile Device Inventory in Avalanche, right-click the device to which you want to send the CE Secure configuration
4. Select **Update Now (Disallow User Override)** or **Update Now (Allow User Override)**.

NOTE Update Now (Allow User Override) allows the user to postpone the CE Secure package installation.

The CE Secure package and the configurations will be sent to the mobile device.

Unlocking the Mobile Device

A mobile device will lock under any of the following circumstances depending on how CE Secure is configured:

- **Power on.** When the device is powered on or rebooted.
- **Time change.** If the time changes on the device or the time on the device is different than the time on the Avalanche Console.
- **Lock-out period exceeded.** When the device has been out of network range beyond the configured lock-out period.
- **Encryption period exceeded.** When the device reaches the encryption time out and CE Secure begins encrypting data on the device.
- **Deletion period exceeded.** When the device reaches the delete time-out and CE Secure begins deleting data on device.

When a mobile device locks, you will see the *Device Locked* screen for approximately three seconds. Then the *Logon* screen appears.

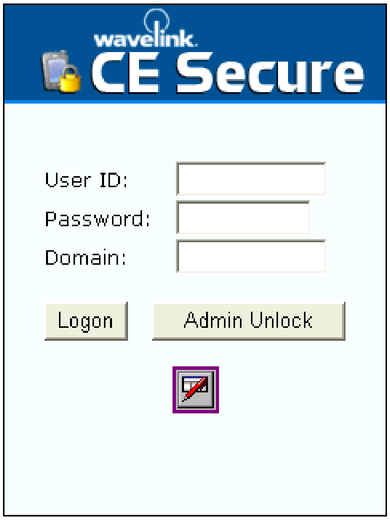


Figure 6-1. *CE Secure Logon Screen*

From the *Logon* screen, there are two ways to unlock a mobile device:

- Logging on to the Mobile Device
- Performing an Admin Unlock

NOTE If you have trouble keeping your mobile device unlocked, check the CE Secure Config utility on the server or the config *Viewer* in the *CE Secure Support* screen on the mobile to determine the circumstances under which CE Secure was configured to lock. For information about the configuring CE Secure, refer to *Chapter 4: Configuring CE Secure* on page 37. For information about viewing the Config Viewer, refer to *Using the CE Secure Support Mode Options* on page 69.

Logging on to the Mobile Device

When the device is locked, you can log on to the mobile device from the CE Secure Logon screen by entering a user id, password, and domain name. This logon information is the same logon information as your CE Secure server logon. For example, if the CE Secure service is installed on your Windows machine, you use the same Windows login information to log on to the device locked by CE Secure.

During the log on process, the client contacts the authentication server that you configured in the Auth Servers tab of the CEConfig dialog box to validate the user credentials entered. For more information on configuring authentication servers, refer to *Configuring CE Secure Authentication Servers* on page 42. If the validation is successful, this information is cached on the device so the user can log on when the authentication server is not available.

To log on to the mobile device:

1 If the virtual keyboard is not displayed on the CE Secure Logon screen, click the Keyboard button.

2 Using the virtual keyboard, enter the **User ID**.

3 Enter the **Password**.

4 Enter the **Domain Name**.

5 Click **Logon**.

If the information validates against the authentication server, the device unlocks.

Performing an Admin Unlock

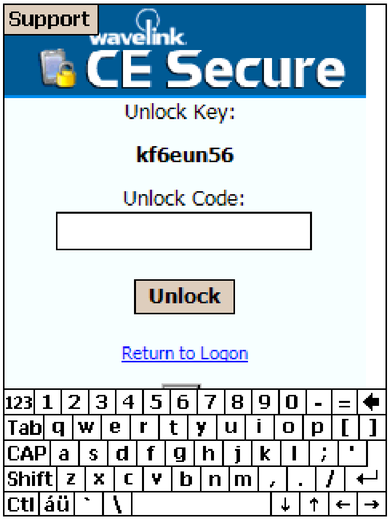
Administrators can perform an Admin Unlock to unlock the device without being within the scope of the network or using the user id and password.

NOTE For Admin Unlock to work properly, the shared secret on the mobile device must match the shared secret the CE Secure Admin is using to generate the unlock code.

To perform an Admin Unlock:

1 From the *CE Secure Logon* screen, click **Admin Unlock**.

The *Unlock Key* screen appears.



Unlock Key:

kf6eun56

Unlock Code:

Unlock
Return to Logon
123 1 2 3 4 5 6 7 8 9 0 - =
Tab q w e r t y u i o p [ ]
CAP a s d f g h j k l ; '
Shift z x c v b n m , . /
Ctl áü ` \ ↓ ↑ ← →

Figure 6-2. *Unlock Key*

2 Make note of the **Unlock Key**.

3 From the CE Secure Config utility, select **Utilities > Generate Unlock Key**.

The *Generate Unlock Code* dialog box appears.

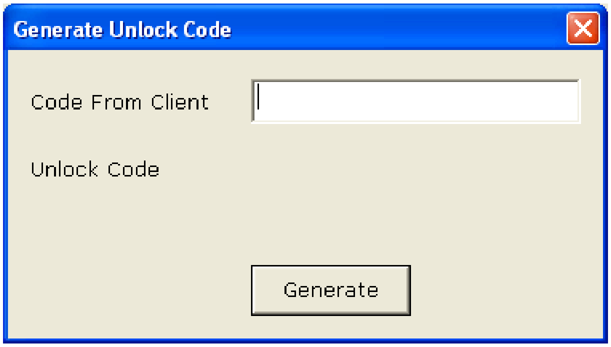
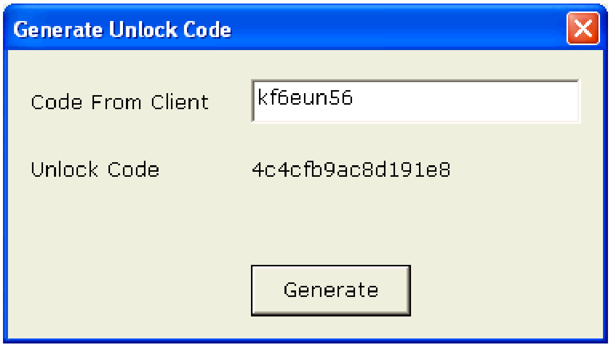


Figure 6-3. *Generate Unlock Code*

4 In the **Code From Client** text box, enter the **Unlock Key** displayed on the *CE Secure Unlock Key* screen.

5 Click **Generate**.

The unlock code displays.



Generate Unlock Code

Code From Client: kf6eun56

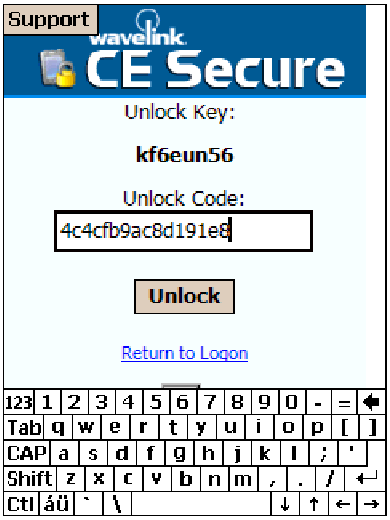
Unlock Code: 4c4cfb9ac8d191e8

Figure 6-4. *Generate Unlock Code*

6 Enter the unlock code in the **Unlock Code** text box on the mobile device.

NOTE If the virtual keyboard is not displayed on the CE Secure Logon screen, click the Keyboard button

---



Unlock Key:

kf6eun56

Unlock Code: 4c4cfb9ac8d191e8

Unlock
Return to Logon
123 1 2 3 4 5 6 7 8 9 0 - =
Tab q w e r t y u i o p [ ]
CAP a s d f g h j k l ; '
Shift z x c v b n m , . /
Ctl áü ` \ ↓ ↑ ← →

Figure 6-5. *Unlock Screen on the Mobile Device*

7 Click **Unlock**.

The device will authenticate the information, unlock the mobile device, and decrypt any encrypted files.

Performing User Lock on the Mobile Device

CE Secure provides a method to lockdown the mobile device from the mobile device called a User Lock. This feature is useful in situations where you want to lock the mobile device without waiting for the lock frequency to expire. When you perform a User Lock on the mobile device, the device locks, and, if the device is configured to encrypt the Protected Files, files are encrypted. For more information on protecting files and configuring files to be encrypted, refer to *Protecting Files* on page 64.

NOTE If you User Lock your mobile device, but remain within the scope of the network, the Delete Frequency timer does not start and your files will not be deleted. If you User Lock the mobile device and move beyond the scope of the network (or if you are already beyond the scope of the network), the Delete Frequency timer begins. If the Deletion Frequency expires while in User Lock mode and you are beyond the scope of the network, your encrypted files will be deleted.

This section provides information about configuring CE Secure to encrypt files upon a User Lock and performing a User Lock from the mobile device.

To configure CE Secure to encrypt files upon a User Lock:

1 Access the CE Secure Config utility.

2 In the lock settings region, enable **Encrypt On User Lock** option.

   - Alternatively, if you are configuring the device to not encrypt files upon a User Lock, disable the **Encrypt On User Lock** option.

3 Click **OK** to save the configuration changes.

4 In the Mobile Device Inventory in the Avalanche Console, right-click the device you want to update and select **Update Now (Disallow User Override)** or **Update Now (Allow User Override)**.

   The mobile device updates with the CE Secure Configuration changes.

To perform a User Lock on the mobile device:

- From the mobile device **Start** menu, select **CE Secure**.

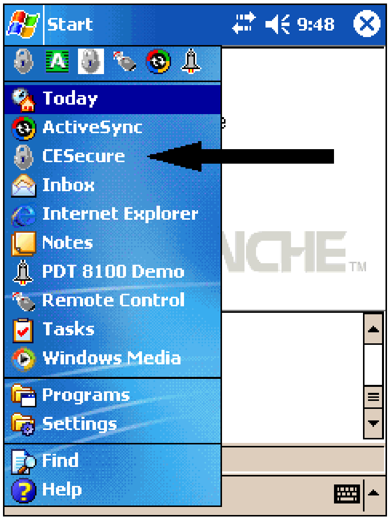


Figure 6-6. *CE Secure User Lock Option*

If configured to do so, the mobile device will encrypt the Protected Files and then lock.

Protecting Files

Protected Files include files, directories, and data that you want encrypted or deleted once the device has been out of network range for a specified amount of time. When the mobile device is unlocked or returns within network range, files are decrypted. This section provides information about configuring which files are protected and the way the files are protected. For more information refer to *Adding Protected Files* on page 43.

To configure protected files:

1. From the CE Secure Config utility, click the Protected Files tab.
2. Enter the path names for those files and directories you want to encrypt or delete after a specified amount of time.
3. Click the Excluded Files tab.

4 If there are any files or directories within the path names you entered in the **Protected Files** tab that you do not want encrypted or deleted, enter those path names.

5 From the Settings region of the CE Secure Config utility, enter the **Encryption Frequency** and select the measure of time from the drop-down men.

6 Enter the **Delete Frequency** and select the measure of time from the drop-down menu.

7 Click **OK**.

8 From the Mobile Device Inventory, right-click the mobile device to which you want to send the CE Secure configuration and select **Update Now (Disallow User Override)** or **Update Now (Allow User Override)**.

The configurations are sent to the mobile device.

NOTE CE Secure does not wait for the **Encryption Frequency** to expire when you perform a User Lock. Therefore, these files will be encrypted immediately upon a User Lock. For more information about User Lock, refer to *Performing User Lock on the Mobile Device* on page 63.

Chapter 7: Using CE Secure Support Mode

CE Secure provides a support mode that allows administrators to access CE Secure client screens, view data and log information, and perform other administrative functions from the mobile device. CE Secure support mode must be enabled from the configuration utility.

This chapter provides the following information:

- Enabling CE Secure Support Mode
- Accessing Support Mode on the Mobile Device
- Using the CE Secure Support Mode Options

Enabling CE Secure Support Mode

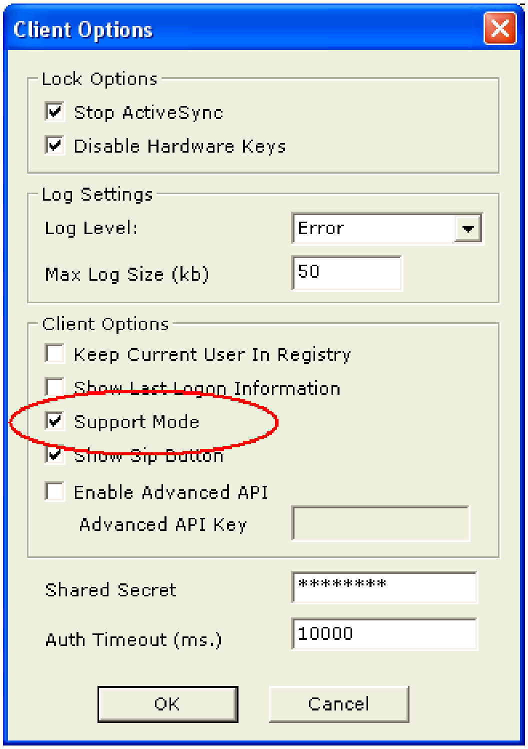
Support mode is not enabled by default in CE Secure. It is recommended that you enable support mode for administrative or trouble-shooting purposes only.

To enable Support Mode:

1 Access the CE Secure Config utility and click **Config Client**.

The *Client Options* dialog box appears.

2 Enable the **Support Mode** option and click **OK.**



Client Options

Lock Options

☑ Stop ActiveSync

☑ Disable Hardware Keys

Log Settings

Log Level: Error

Max Log Size (kb) 50

Client Options

□ Keep Current User In Registry

□ Show Last Logon Information

☑ Support Mode

☑ Show Sip Button

□ Enable Advanced API

Advanced API Key

Shared Secret ********

Auth Timeout (ms.) 10000

Figure 7-1. *Support Mode Option*

3 Deploy the updated configuration to the mobile device.

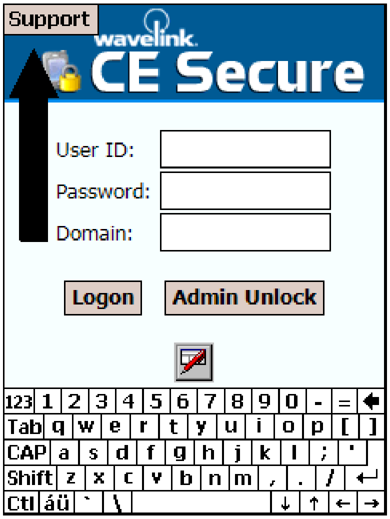
The **Support** button is now available on the CE Secure client screens.

Accessing Support Mode on the Mobile Device

Once you enable support mode in the CE Secure Config utility and deploy the updated configuration to the mobile device, you can access the support mode. A **Support** button is available in the upper-left corner the CE Secure client screens.

To access support mode:

- From one of the CE Secure client screens, click the **Support** button located in the upper-left corner of the screen.



User ID:

Password:

Domain:

Figure 7-2. *Support Mode on the Mobile Device*

Using the CE Secure Support Mode Options

The *CE Secure Support* screen information for support and troubleshooting. The screen is divided into the following regions:

- Show Screen
- Protected Files
- SIP (Soft Input Panel)
- View
- Active Sync
- Hardware Keys
- Hide
- Exit Program

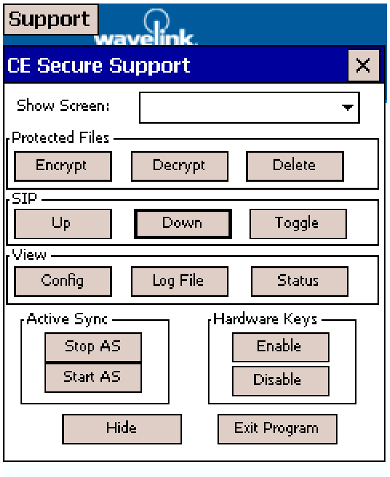


Figure 7-3. *CE Secure Support Screen*

This section provides detailed information about the functions you can perform from the *CE Secure Support* screen regions on the mobile device.

Show Screen

The **Show Screen** drop-down list allows you select and view any of the client screens. This is useful when you create custom client screens and want to verify the appearance of each screen on the mobile device.

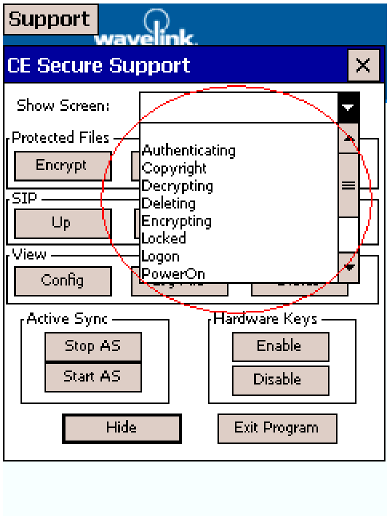


Figure 7-4. *Show Screen*

When you click a screen name, the screen appears and displays until you click the **Support** button to return to the CE Secure screen. The **Show Screens** feature is for viewing client screens only. You cannot modify the screens or enter information.

Protected Files

The **Encrypt**, **Decrypt**, and **Delete** buttons allow you to encrypt, decrypt, or delete the protected files on the mobile device.

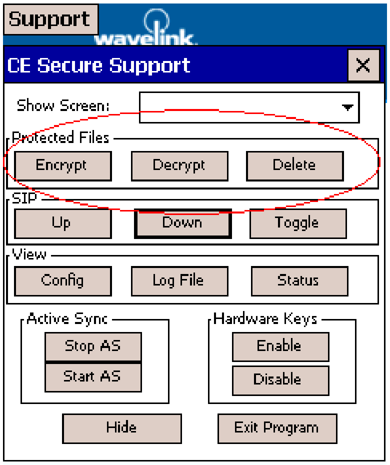


Figure 7-5. *Protected Files Buttons*

The protected files are those files entered in the **Protected Files** tab in the CE Secure Config utility. You cannot select which files to encrypt or decrypt from the support screen. For more information on configuring protected files, refer to *Protecting Files* on page 64.

SIP (Soft Input Panel)

The **Up**, **Down**, and **Toggle** buttons allow you to display the virtual keyboard (**Up**), hide the virtual keyboard (**Down**) or toggle the keyboard display (**Toggle**).

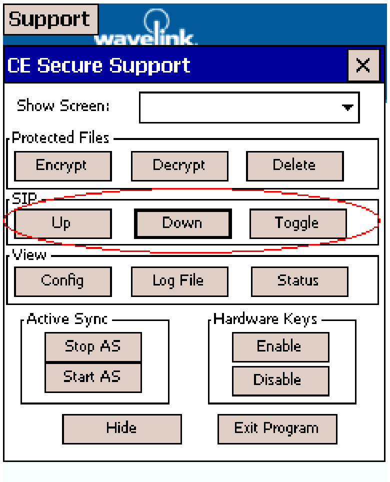


Figure 7-6. *SIP Buttons*

View

The View region of the *CE Secure Support* screen provides allows you to view the following:

- Config
- Log File
- Status

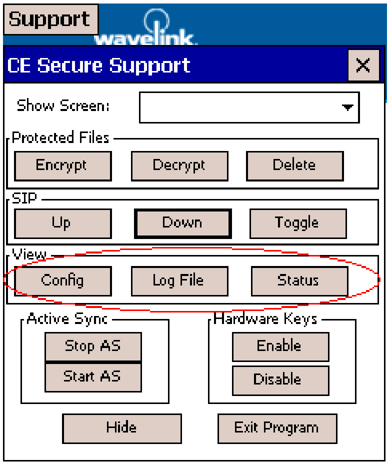
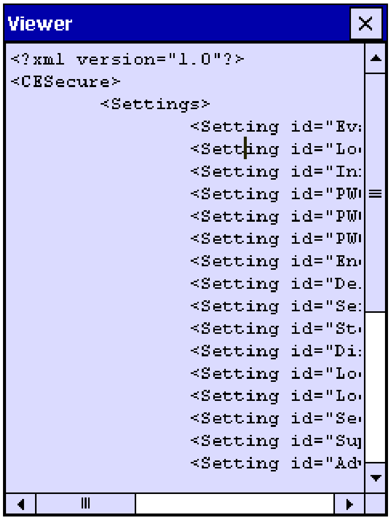


Figure 7-7. *View Buttons*

Config

When you click the `Config` button the config *Viewer* appears.



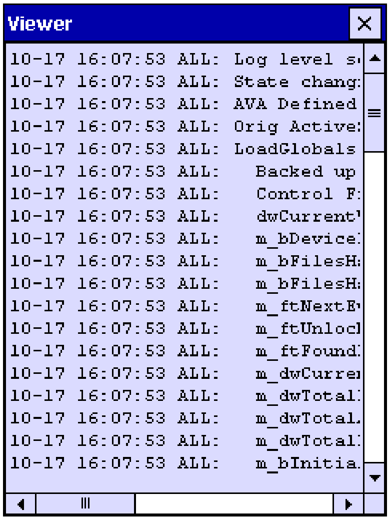
```
<?xml version="1.0"?>
<CESecure>
        <Settings>
                <Setting id="Ev
                <Setting id="Lo
                <Setting id="In
                <Setting id="PW
                <Setting id="PW
                <Setting id="PW
                <Setting id="En
                <Setting id="De
                <Setting id="Se
                <Setting id="St
                <Setting id="Di
                <Setting id="Lo
                <Setting id="Lo
                <Setting id="Se
                <Setting id="Su
                <Setting id="Ad
```

Figure 7-8. *Config Viewer*

This screen allows you to view all CE Secure settings that are configured in the CE Secure Config utility. You cannot change any configurations from this screen. Configuration changes must be made in Avalanche and deployed to the device. For more information, refer to *Chapter 4: Configuring CE Secure* on page 37. Click the **X** to return to the *CE Secure Support* screen.

Log File

When you click the **Log File** button, the log *Viewer* appears.



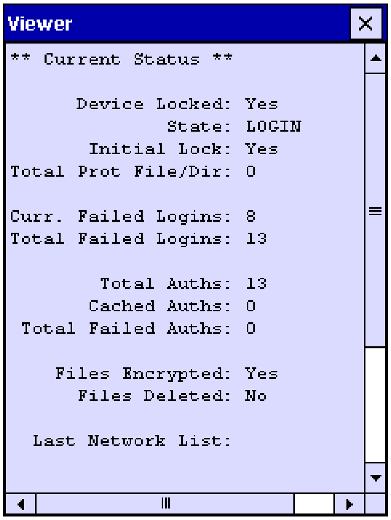
```
10-17 16:07:53 ALL: Log level s
10-17 16:07:53 ALL: State chang
10-17 16:07:53 ALL: AVA Defined
10-17 16:07:53 ALL: Orig Active
10-17 16:07:53 ALL: LoadGlobals
10-17 16:07:53 ALL:   Backed up
10-17 16:07:53 ALL:   Control F
10-17 16:07:53 ALL:   dwCurrent
10-17 16:07:53 ALL:   m_bDevice
10-17 16:07:53 ALL:   m_bFilesH
10-17 16:07:53 ALL:   m_bFilesH
10-17 16:07:53 ALL:   m_ftNextE
10-17 16:07:53 ALL:   m_ftUnloc
10-17 16:07:53 ALL:   m_ftFound
10-17 16:07:53 ALL:   m_dwCurre
10-17 16:07:53 ALL:   m_dwTotal
10-17 16:07:53 ALL:   m_dwTotal
10-17 16:07:53 ALL:   m_dwTotal
10-17 16:07:53 ALL:   m_bInitia
```

Figure 7-9. *Log Viewer*

This screen allows you to view the CE Secure client log file. Click the **X** to return to the *CE Secure Support* screen.

Status

When you click the **Status** button, the status *Viewer* appears.



```
** Current Status **

      Device Locked: Yes
              State: LOGIN
       Initial Lock: Yes
Total Prot File/Dir: 0

Curr. Failed Logins: 8
Total Failed Logins: 13

        Total Auths: 13
       Cached Auths: 0
 Total Failed Auths: 0

    Files Encrypted: Yes
      Files Deleted: No

  Last Network List:
```

Figure 7-10. *Status Viewer*

From this screen you can view statistics of the CE Secure client and the mobile device. Click the **X** to return to the *CE Secure Support* screen.

Active Sync

You can use the **Stop AS** and **Start AS** buttons to stop and start an Active Sync connection.

NOTE You can only start an ActiveSync connection if there is a physical connection between the mobile device and the server.

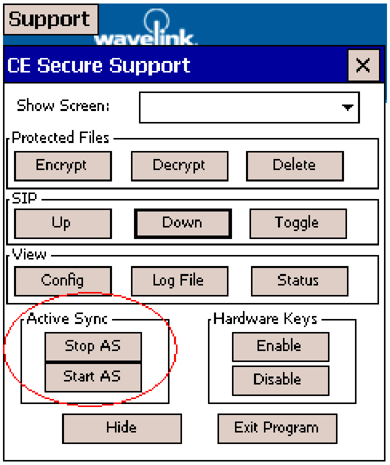


Figure 7-11. *Active Sync Buttons*

Hardware Keys

You can use the **Enable** and **Disable** buttons to enable and disable the hardware keys on the mobile device.

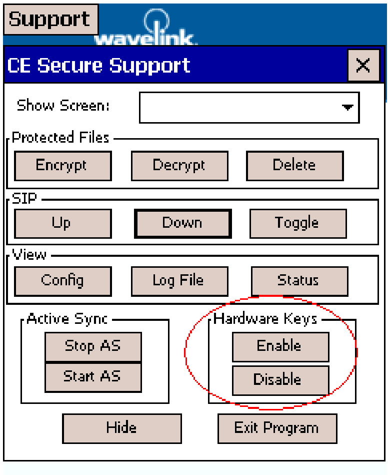


Figure 7-12. *Hardware Key Buttons*

Hide

The **Hide** button hides the *CE Secure Support* screen.

Exit Program

The **Exit Program** button exits you from *CE Secure Support* screen and unlocks the mobile device. The device does not need to be within the scope of the network and you do not need to enter a valid User ID and Password to unlock the mobile device when you use the **Exit Program** button.

Appendix A: Wavelink Contact Information

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

Email: customerservice@wavelink.com

Phone: USA and Canada: 1-888-697-WAVE (9283) ext.2 or 1.801.316.9000 ext.2
Outside USA and Canada: +800 WAVELINK (9283-5465) ext.2

Days: Monday-Friday, except national holidays in the U.S.

Hours: 7:00 AM MT to 7:00 PM MT

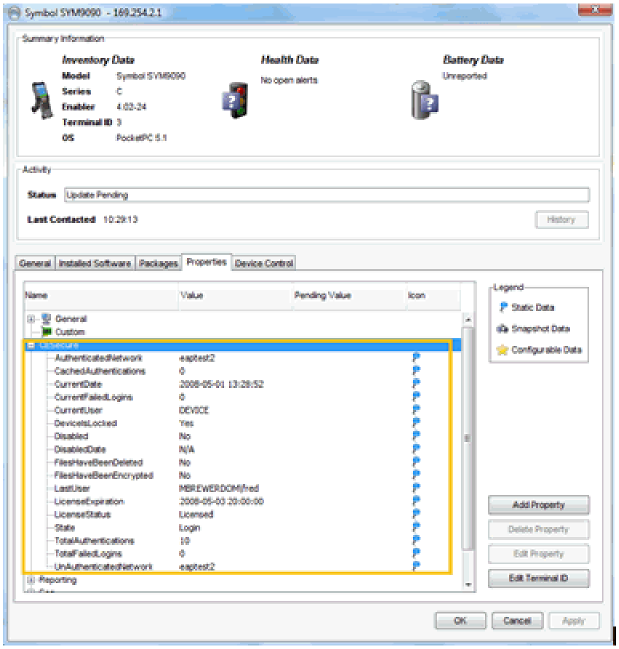
Appendix B: Avalanche Advanced Properties

This appendix provides information about the following topics:

- CE Secure Device Properties
- Property Definitions and Usage
- Using Device Properties in Mobile Device Groups
- New Registry Entry for Device Resident Application
- Certificate Management in CE Secure
- Cached User Information on Device Logon Screen
- Secure Password and Advanced Functions API
- Security Defaults for CE Secure Manager

CE Secure Device Properties

Every device managed by Avalanche provides static and real-time properties that are reported to the Enterprise Server on each check-in period. This is enhanced with additional data for CE Secure.



Inventory Data

Model	Symbol SYM9090
Series	C
Enabler	4.02-24
Terminal ID	3
OS	PocketPC 5.1

Health Data

No open alerts

Battery Data

Unreported

Status: Update Pending

Last Contacted: 10:29:13

Name	Value	Pending Value	Icon
General			
Custom			
CESecure			
AuthenticatedNetwork	eaptest2		
CachedAuthentications	0		
CurrentDate	2008-05-01 13:28:52		
CurrentFailedLogins	0		
CurrentUser	DEVICE		
DeviceIsLocked	Yes		
Disabled	No		
DisabledDate	N/A		
FilesHaveBeenDeleted	No		
FilesHaveBeenEncrypted	No		
LastUser	MBREWERDOM\fred		
LicenseExpiration	2008-05-03 20:00:00		
LicenseStatus	Licensed		
State	Login		
TotalAuthentications	10		
TotalFailedLogins	0		
UnAuthenticatedNetwork	eaptest2		
Reporting			

Figure 1. *Properties Tab*

The 17 properties can be used by the Mobile Device Groups system in a number of ways to determine factors, such as where a user is currently logged in, or to find a device that has an unusual number of failed login attempts.

An asterisk (*) indicates the separately licensed.

Property Definitions and Usage

The properties, when using with Mobile Device Groups, must be prefixed with "CESecure", for example, "LastUser" would become "CESecure.LastUser". Also, some of the properties listed below reflect conditions which occur when the device is away from an 802.11 network and have been enacted. For these to be reported correctly, either the device must come back in to contact with the 802.11 network or the properties should be reported by another means, such as wireless WAN.

The following table displays the definitions and data types for the properties:

Property	Definition
AuthenticatedNetwork	The SSID for the network that will be used for any users associated with the device when used in combination with 802.1X and the Wavelink Certificate Manager. The type is STRING.
CachedAuthentications	CE Secure is able to provide authenticated logins to a device even when access to Active Directory is unavailable. This field provides the count for the number of users for which cached authentications are available. The type is an INTEGER.
CurrentDate	The current date as reported by the client in the format of YYYY-MM-DD HH:MM:SS. The type is a STRING.
CurrentFailedLogins	The number of failed login attempts for the current login screen. This number is reset once a login is successfully completed. The type is an INTEGER.
CurrentUser	Provides the identity of the currently logged in user with their domain in the format of: <DOMAIN> \ <USERID> If device certificates only are being used, this field will show "DEVICE". The type is a STRING.
DeviceIsLocked	Specifies whether the device is currently displaying the logon screen. The values are a STRING and will reflect "Yes" or "No".
Disabled	Specifies if the device has initiated its lock-down sequence. The values are a STRING and will reflect "Yes" or "No".
DisabledDate	The time that the disable event occurs in the STRING format of YYYY-MM-DD HH:MM:SS.
FilesHaveBeenDeleted	Refers to files you have configured to delete if the device be away from the network for an extended period. If this condition has occurred, this field, which is a STRING will show "Yes". Otherwise it displays "No".

Property	Definition
FilesHaveBeenEncrypted	Refers to Encrypted Files. Encrypted Files are files you have specified to be deleted if the device is away from the network for an extended period of time. Data type is STRING with “Yes” and “No” being the possibilities.
LastUser	The last logged in user in the format of STRING and <domain> / <username>
LicenseExpiration	CE Secure clients will check-in periodically to retrieve a new license. If the License Server is not available, the client enters a Grace Period. This field shows the time at which the client must have renewed its license before the Grace Period is entered. The format is STRING in the form of YYYY-MM-DD HH:MM:SS.
LicenseStatus	If a license is currently active, this STRING field will show “Licensed”. If the license has been revoked, it will show “Unlicensed”.
State	Displays the status of the client. This is a STRING field. “Login” shows that the login screen is currently active. This field can be used to identify all devices which are currently active.
TotalAuthentications	Displays the total number of successful authentications that have occurred on this device. This is an INTEGER.
TotalFailedLogins	The total number of failed login attempts to the device. This is an INTEGER.
UnAuthenticatedNetwork	The SSID for the network that is to be used when a user is logged out or when device certificates are employed. This is a STRING.

Using Device Properties in Mobile Device Groups

Because device-side properties are being populated into the Avalanche MC Enterprise database, queries may be made via the Mobile Device Groups to provide granular information about certain criteria.

For example, groups may be made to track specific events. The types of events are configurable using a regular expression comparison engine (see below). This allows the administrator to find out customized information, such as:

- Tracking which device an individual user is currently using
- Identify all devices that are secured onto a specific network and/or in use
- Identify devices that have experienced excessive login attempts
- Find devices that have previously been in distress and have erased or encrypted their data
- Identify usage patterns for devices by identifying how many authorized parties have been provisioned for a device
- A combination of the above using any of the fields mentioned in the properties list, including those from other aspects of the device

To configure the Mobile Device Groups, the administrator must first right-click **Mobile Device Groups** in the Navigation Window and create a new group. Refer to the following example or to your Avalanche User Guide for more information about creating Mobile Device Groups.

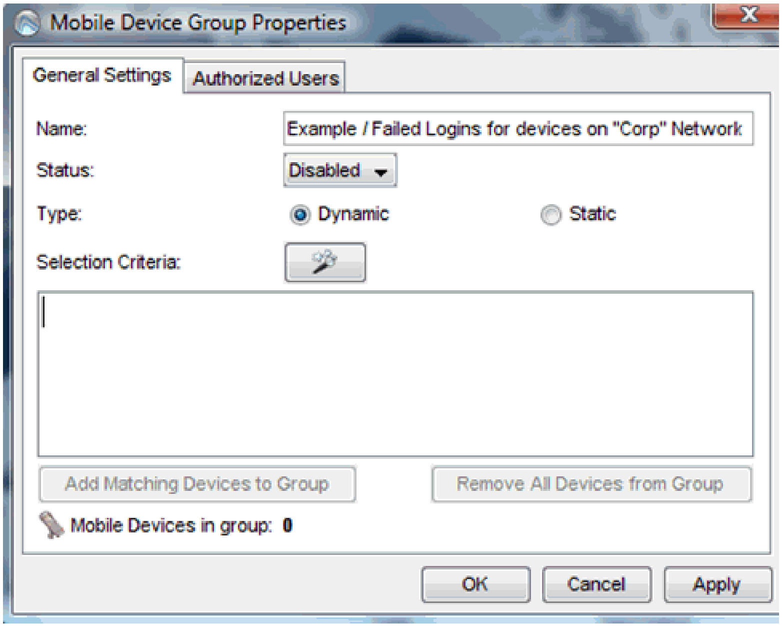
Mobile Device Groups Example

In the following example, a set of criteria will be created to show all devices that have had excessive login attempts and are present on the corporate network using the SSID of "corp".

1 From the *Mobile Device Group Properties* dialog box, create a dynamic or static group.

   A dynamic group will automatically add devices as and when the devices meet the criteria.

   A static group will show a list of devices which meet the criteria at the point in time when the group was created.


Mobile Device Group Properties
General Settings
Authorized Users
Add Matching Devices to Group
Remove All Devices from Group
OK
Cancel
Apply

Name: Example / Failed Logins for devices on "Corp" Network

Status: Disabled

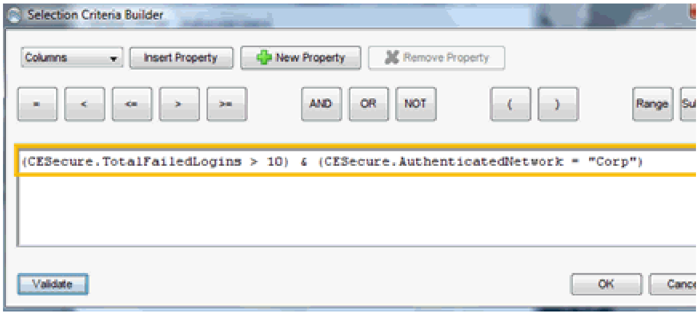
Type: ● Dynamic ○ Static

Selection Criteria:

Mobile Devices in group: 0

Figure 1-1. *Mobile Device Group Properties*

2 Configure a regular expression in Selection Criteria to compare the “TotalFailedLogins” against 10 and the SSID from the “AuthenticatedNetwork” property.



```
(CESecure.TotalFailedLogins > 10) & (CESecure.AuthenticatedNetwork = "Corp")
```

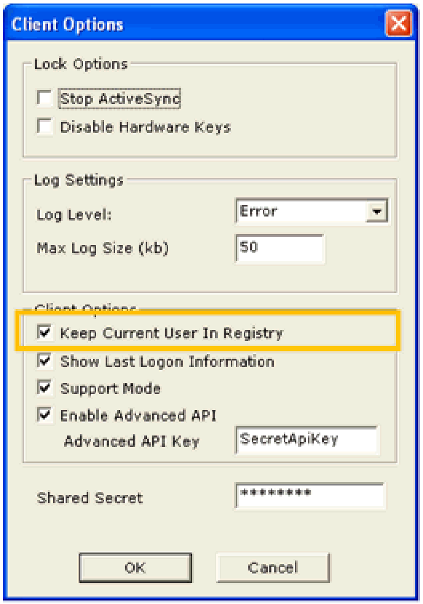
Figure 1-2. *Selection Criteria Builder*

3 If both criteria are met, the Mobile Device Group listing will show all relevant devices.

New Registry Entry for Device Resident Application

Programs that reside on the device can take advantage of new registry keys which are populated. These keys allow for a more streamlined process for logging in because the username and domain information may be populated into another application automatically by just reading a special registry key.

To enable this option, the administrator must access the CE Secure Config utility, select **Client Options** and then enable **Keep Current User In Registry**.



Lock Options

□ Stop ActiveSync

□ Disable Hardware Keys

Log Settings

Log Level: Error

Max Log Size (kb) 50

Client Options

☑ Keep Current User In Registry

☑ Show Last Logon Information

☑ Support Mode

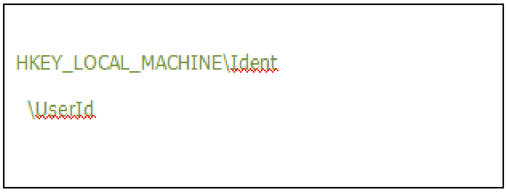
☑ Enable Advanced API

Advanced API Key SecretApiKey

Shared Secret ********

Figure 1-3. *Key Current User in Registry*

Once this is configured, the following registry key will be updated each time the CE Secure user is modified.

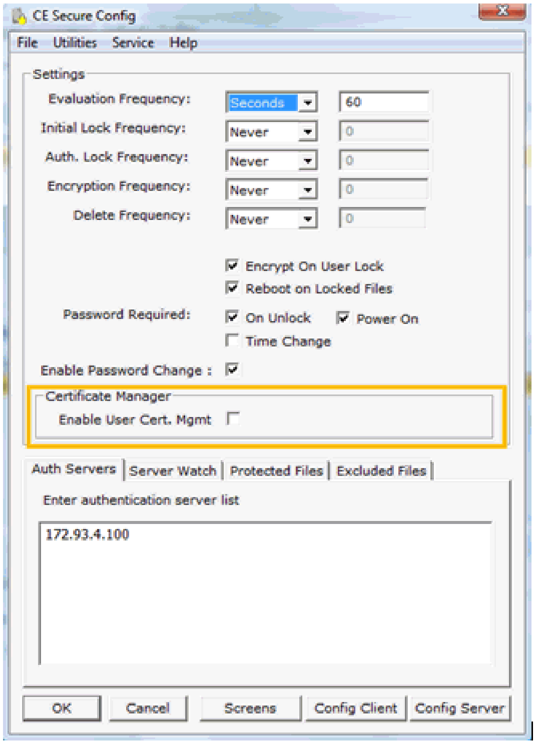


```
HKEY_LOCAL_MACHINE\Ident
 \UserId
```

Figure 1-4. *UserID Registry Key*

Certificate Management in CE Secure

If CE Secure is used in combination with the Wavelink Certificate Manager, CE Secure is able to provide each user provisioned for the device with an individual certificate. This certificate is then used to authenticate them to an 802.1X / EAP-TLS network.



Settings

Evaluation Frequency: Seconds 60

Initial Lock Frequency: Never 0

Auth. Lock Frequency: Never 0

Encryption Frequency: Never 0

Delete Frequency: Never 0

☑ Encrypt On User Lock

☑ Reboot on Locked Files

Password Required: ☑ On Unlock ☑ Power On

□ Time Change

Enable Password Change : ☑

Certificate Manager

Enable User Cert. Mgmt □

Auth Servers | Server Watch | Protected Files | Excluded Files

Enter authentication server list

172.93.4.100

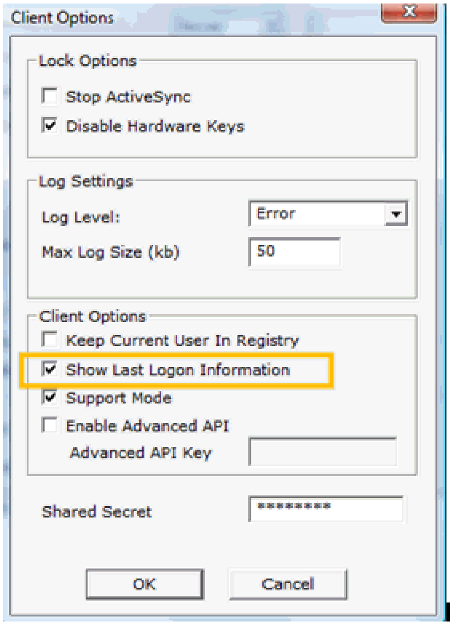
Figure 1-5. *Certificate Manager Options*

This option cannot be used without the Certificate Manager and additional licenses in support for certificate management may also be necessary.

Cached User Information on Device Logon Screen

A common issue with devices that are often laid down or turned off in normal operation is the that a somewhat lengthy login process needs to be reattempted when the device is needed again.

This would normally consist of a username, a domain and a password. This may optionally be reduced to just the password because the username and domain can be pre-populated when the **Show Last Logon Information** is enabled.



Client Options

Lock Options

☐ Stop ActiveSync

☑ Disable Hardware Keys

Log Settings

Log Level: Error

Max Log Size (kb) 50

Client Options

☐ Keep Current User In Registry

☑ Show Last Logon Information

☑ Support Mode

☐ Enable Advanced API

Advanced API Key

Shared Secret ********

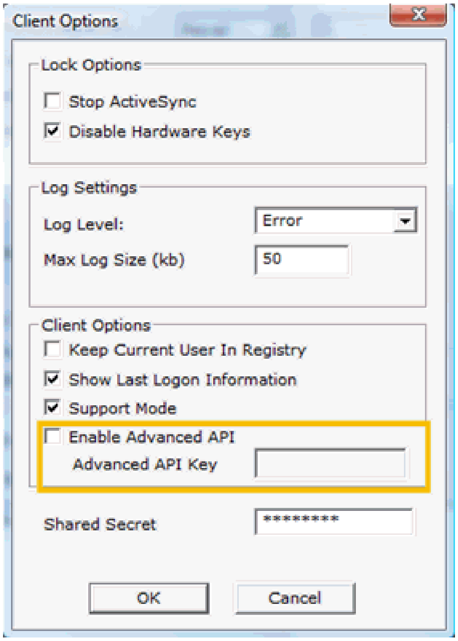
Figure 1-6. *Show Last Logon Information*

The **Show Last Logon Information** will pre-populate the login display with the last user that was successfully authenticated. The end-user need only enter their password to resume operation.

Secure Password and Advanced Functions API

CE Secure supports a programmatic API so other programs can interface with CE Secure on the mobile device. These functions are sensitive in nature and are restricted to only authorized client utilities.

First, the administrator must enable the option in the CE Secure Config utility. Once this option is enabled, the Advanced API key should be filled in with a secret shared key.



Client Options

Lock Options

☐ Stop ActiveSync

☑ Disable Hardware Keys

Log Settings

Log Level: Error

Max Log Size (kb) 50

Client Options

☐ Keep Current User In Registry

☑ Show Last Logon Information

☑ Support Mode

☐ Enable Advanced API

Advanced API Key

Shared Secret *********

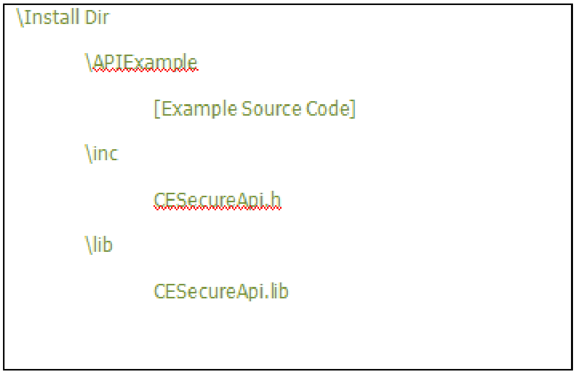
Figure 1-7. *Enable Advanced API*

This key should only be provisioned to trusted client applications and is used in an application program to gain access to advanced API functions as described. In essence, the API is authenticated.

Also, a CE Secure Advanced API SDK is available from Wavelink upon request.

CESecure API Overview

The CESecure API is provided as a linkable Windows library which include files. The contents of the installation are as follows:



```
\Install Dir
        \APIExample
                [Example Source Code]
        \inc
                CESecureApi.h
        \lib
                CESecureApi.lib
```

Figure 1-8. *API Contents*

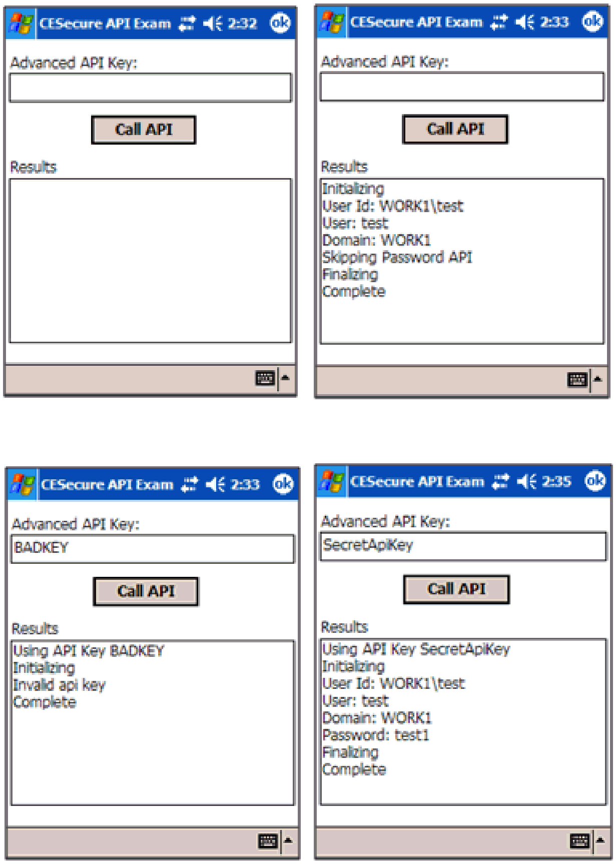
Standard API functions with explanative function names are as follows:

- cesecure_Initialize
- cesecure_Finalize
- cesecure_GetCurrentUser
- cesecure_GetUserFromUserId
- cesecure_GetDomainFromUserId
- cesecure_GetLastErrorMessage

Advanced API function include:

- cesecure_GetCurrentPassword

Typical Application Example



```
Initializing
User Id: WORK1\test
User: test
Domain: WORK1
Skipping Password API
Finalizing
Complete
```

Advanced API Key: BADKEY

```
Using API Key BADKEY
Initializing
Invalid api key
Complete
```

Advanced API Key: SecretApiKey

```
Using API Key SecretApiKey
Initializing
User Id: WORK1\test
User: test
Domain: WORK1
Password: test1
Finalizing
Complete
```

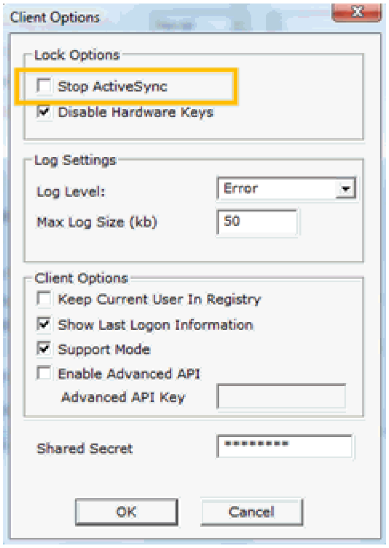
Figure 1-9. *Examples*

Security Defaults for CE Secure Manager

Some of the defaults in CE Secure promote high security, but at the same time can present pitfalls if they are not properly understood or configured.

Stop Active Sync

One of the security options is the **Stop Active Sync**. This highly secure option prevents unauthorized personnel from gaining access to a device via the Active Sync cradle and it is active as soon as it is provisioned.



Client Options

Lock Options

☐ Stop ActiveSync

☑ Disable Hardware Keys

Log Settings

Log Level: Error

Max Log Size (kb) 50

Client Options

☐ Keep Current User In Registry

☑ Show Last Logon Information

☑ Support Mode

☐ Enable Advanced API

Advanced API Key

Shared Secret *********

Figure 1-10. *Stop ActiveSync*

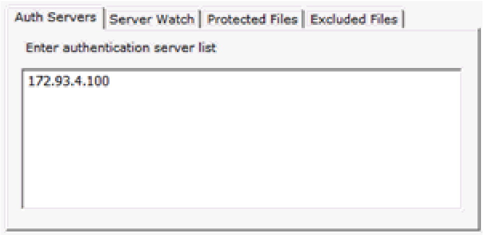
Before this option is enabled, administrators must ensure that the wireless configuration, Active Directory configuration and (where used) user assignment are configured correctly.

Without correct provisioning, a device may end up locking out unauthorized users from the device via the screen and Active Sync, even though the connection and authentication to Active Directory has not been tested.

When an administrator exits the CE Secure Config utility, a warning is displayed to inform them when this option is not set.

Authentication Server

Furthermore, the provisioning of the Authentication Server is now being checked to warn users when a vital field is missing.



Enter authentication server list

172.93.4.100

Figure 1-11. *Auth Servers*

To authenticate users against Active Directory, this field must not be empty.

Now, if the administrator exits the CE Secure configuration manager without making an entry, a warning is made

Index