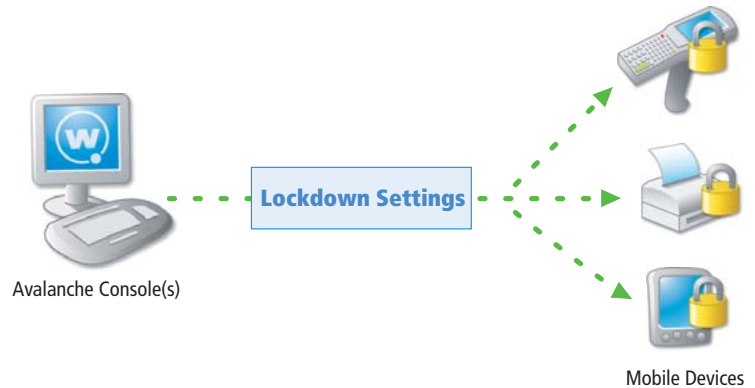


## Security for Windows CE mobile devices that provides protection for corporate data and systems.

Wavelink Avalanche CE Secure is a plug-in to Wavelink Avalanche that provides advanced user authentication and security on Windows CE™ mobile devices. With Avalanche CE Secure, administrators can reduce the risk that a lost or stolen mobile device will be used to compromise an organization's critical systems and data.

Wavelink Avalanche CE Secure provides administrators the ability to prevent critical data from being accessed or stolen by unauthorized users by locking mobile devices based on criteria defined by the administrator. Administrators can configure automatic device lockdown settings, such as when a mobile device is out of contact with an approved server, wireless network, or a combination of the two for a defined period of time. Avalanche CE Secure also provides easy-to-use administrative features and a fully configurable device-side user interface.



### Protect corporate data with user-authentication for mobile device

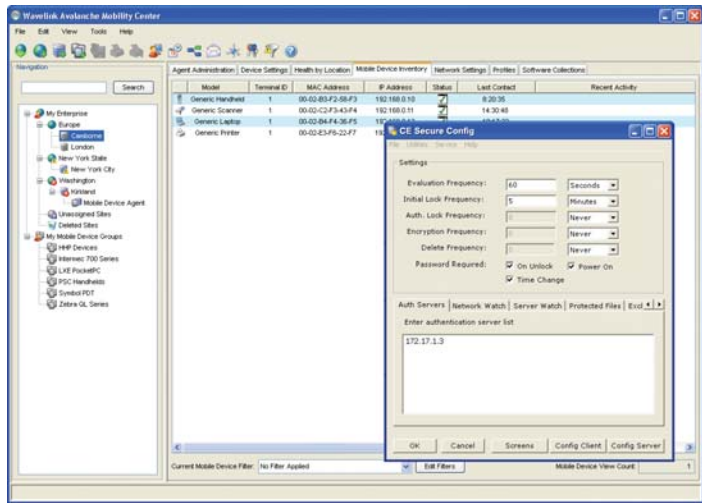
Wavelink Avalanche CE Secure provides an administrator the ability to present a login-page that requires a mobile device user to input an authorized username and password to gain access to the organization's applications and files on the mobile device. Wavelink Avalanche CE Secure can be configured to require a login when the mobile device is initially powered on or when the mobile device is rebooted. The administrator can customize the requirement for user login to include the instance when there is a time change on the mobile device or when an administrator defined lockout period has been exceeded. For temporary users, or for users that have forgotten their username and password, Wavelink Avalanche CE Secure provides administrators with the ability to generate an unlock code for a specific mobile device.

### Multiple lock-down options to protect against a lost or stolen mobile device

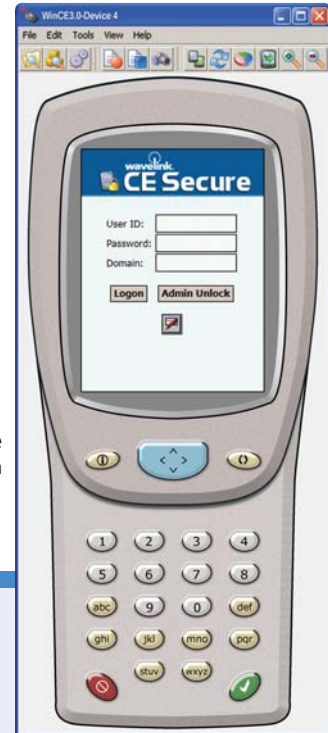
Sometimes a mobile device can be misplaced or lost, compromising mobile data and/or the network before an administrator can act to remove the device's access to valuable company data and applications. Wavelink Avalanche CE Secure helps administrators to protect an organizations critical applications and data by providing an administrator a flexible model for defining when a mobile device should lock down. With Wavelink Avalanche CE Secure, administrators can define when a mobile device is operating in a "secure" state by defining an approved wireless network, an approved server address, or a combination of the two. If a mobile device does not access an approved network or server after a set period of time, or if there is a time change on the mobile device, the mobile device can be locked down or critical data can be encrypted or deleted as defined by the administrator.

### Fully configurable device-side user-interface provides customized messaging and presentation options

The Wavelink Avalanche CE Secure device-side user interface is completely configurable by the administrator. With Avalanche CE Secure, the administrator can easily customize splash screen, images, style sheets and even send specific messaging to end users.



Avalanche Console with CE Secure dialog



Secure Mobile Device Login

## Key Features

The following provides a list of the Avalanche CE Secure lockdown settings you can configure:

**Evaluation Frequency** - Specify how often Avalanche CE Secure should verify that the mobile device is in an approved state.

**Initial Lock Frequency** - Specify how much time will pass before the mobile device's state will be verified before implementing lockdown mode. A device is deemed "not validated" when it cannot contact a defined network server or a defined wireless network.

**Authentication Lock Frequency** - Specify how much time until a device that is not validated (but has been unlocked once) will lock again.

**Encryption Frequency** - Specify when Avalanche CE Secure will encrypt specified files on the mobile device when the device not validated.

**Delete Frequency** - Specify when the mobile device will delete specified files from the mobile device when the device not validated.

**Password Required** - Select if you want to require a password to gain access to the mobile device after the following instances:

- Time change
- Device reboot or power on
- Device unlock

**Customizable Device-side User Interface** - Wavelink Avalanche CE Secure provides an interactive HTML-based screen designer where you can customize client-side screens.

**Easily Manage Protected Files** - Easily manage the circumstances in which a mobile device encrypts or deletes files upon lock down. Avalanche CE Secure allows an administrator the ability to specify which files should be encrypted or deleted as well as the time frame in which the files should be encrypted or deleted.

**Avalanche CE Secure Authentication** - Wavelink Avalanche CE Secure provides secure authentication by interfacing with Active Directory services utilizing security stored in NT, Active Directory, HTTP and LDAP databases.

## Avalanche CE Secure System Requirements

### Mobile Device Client Requirements:

This part of CE Secure is loaded on the mobile device.  
Compatibility: Pocket PC 2003, CE .NET 4.2 and 56 KB of storage  
Requires Avalanche Enabler 3.50-12

### Server Requirements:

This part of Avalanche CE Secure runs as a Windows™ service.  
Requirements: Windows 2000 or Windows XP, and Wavelink Avalanche Manager

### Supported Devices:

visit [www.wavelink.com/wavelink/avalanche/cesecure.aspx](http://www.wavelink.com/wavelink/avalanche/cesecure.aspx)



11335 NE 122nd Way, Suite 200 Kirkland, WA 98034 USA  
Sales and Support: 1-888-697-WAVE (9283)  
International: +1-425-823-0111 UK/EMEA: +44-870-351-8564  
[WWW.WAVELINK.COM](http://WWW.WAVELINK.COM)