SecureW2 Client for Pocket PC
User Guide

Version 1.2

Released: August 2004

Table of Contents

Prerequisites

Before installing SecureW2 for Pocket PC, make sure your handheld runs Microsoft Pocket PC 2003 (Windows Mobile). If your handheld runs an older version, you may be able to upgrade to Pocket PC 2003. Contact your vendor for that matter.

If you will be using SecureW2 for **wireless** 802.1X authentication, make sure your wireless Ethernet card is 802.1X compatible by checking your vendor documentation.

Certificate Requirements

SecureW2 has the following requirements concerning certificates.

All certificates:

- Currently only RSA certificates are supported (all key sizes)
- The certificate must be time valid
- Revocation is not checked

All CA certificates:

- Must be installed in the "Trusted Root Certification Authority" store or similar ("ROOT") of the local computer.

TTLS Server certificate:

- Must be installed in the personal store ("My") of the local computer.

Installation

To install SecureW2, do the following:

1. Make sure your handheld is connected to your computer and that ActiveSync is installed and running.
2. Unzip the SecureW2_PPC2003_1xx.zip file to a temporary folder on your computer.
3. Double click on the SecureW2_PPC2003_1xx.exe file and follow the instructions of the installation program.

Once successfully installed, you can configure SecureW2.

Re-installation

If, for some reason, you wish to re-install SecureW2, make sure that no SecureW2 client configuration windows are open before running the installation program.

Un-installation

To uninstall SecureW2, simply use the "Remove Programs" application in the "Settings/System" folder on your handheld.

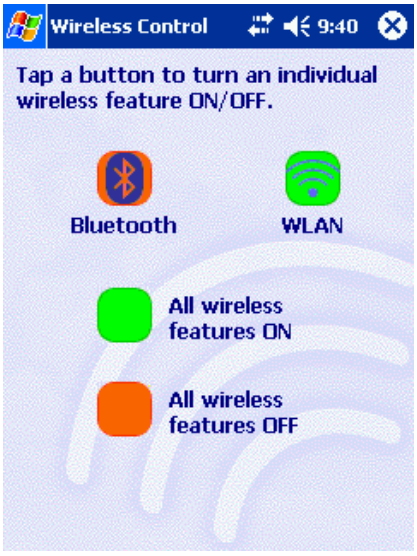
Configuring your handheld

Your handheld needs to be configured for wireless network access in order for SecureW2 to work correctly. This chapter guides you through the necessary steps involved.

Enabling the wireless adapter

Note: *the following is based on the built-in wireless adapter of the HP IPAQ 5550. Handhelds of other vendors might use slightly different methods.*

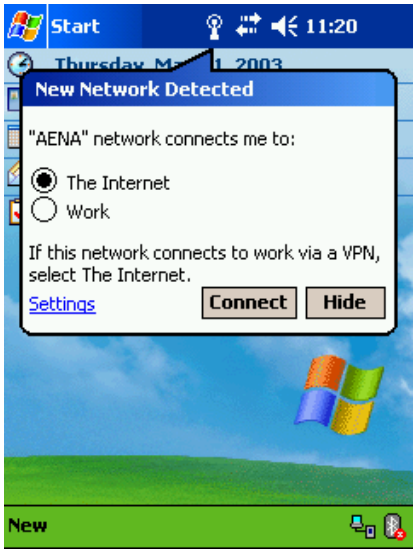
To enable the wireless adapter, start the wireless control application "iPAQ Wireless" located in the "Start menu".



Tap on the "WLAN" button in the "Wireless Control" window to enable the wireless adapter.
Close the window.

Configuring wireless settings

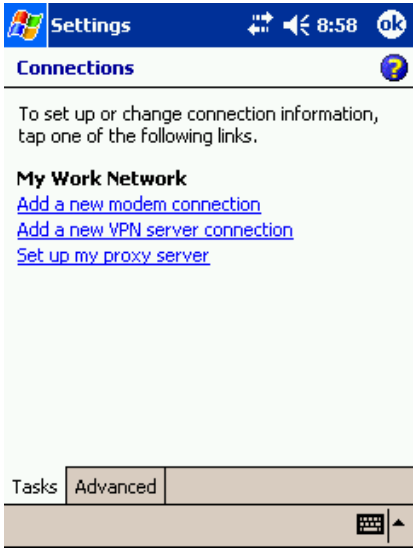
If your SSID/access point is not yet configured, you may see the following window.



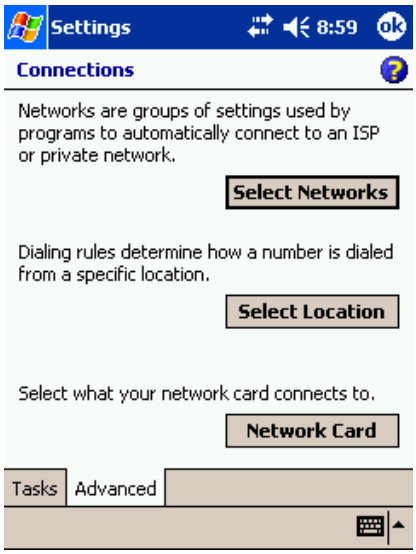
Tap on the "Hide" button to continue.

Tap on the connection icon located next to the sound control to see the "Connectivity" window.

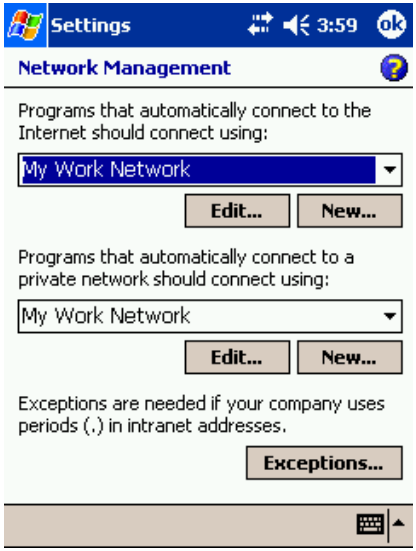
Tap on the "Settings" link to continue. The "Connections" window will pop up.



In the "Connections" window, select the "Advanced" tab.



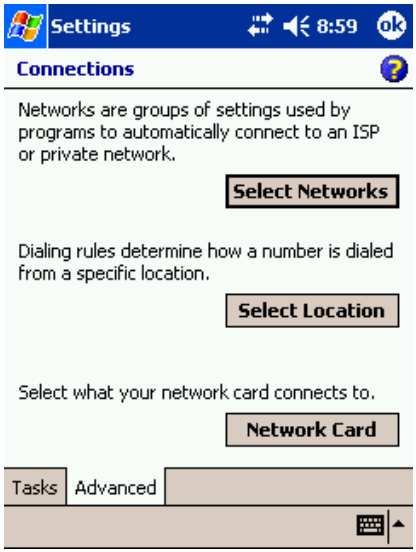
In the "Advanced" tab, tap on the "Select Networks" button. The "Network Management" window will pop up.



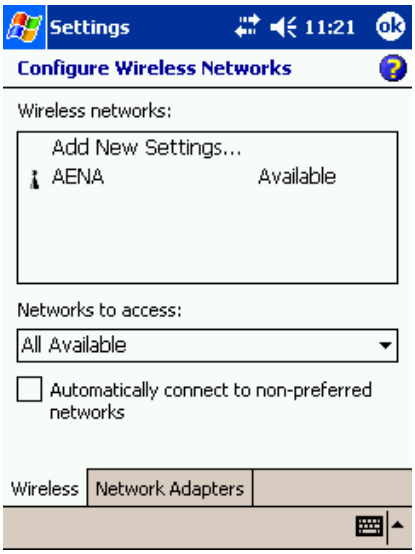
Select "My Work Network" profile for both private and Internet connections.

If you have changed these settings to fit your own network configuration, please select or create a profile that has the option “This network connects to the Internet” turned off.

Tap on OK to continue.



In the “Advanced” tab, tap on the “Network Card” button.
The "Configure Wireless Networks” window will pop up.



This window shows all the SSIDs that your wireless adapter has either found or is configured for. Either Tap on the SSID you are going to configure SecureW2 for or select "Add New Settings…" to add an SSID (if the SSID is for example not broadcasted).

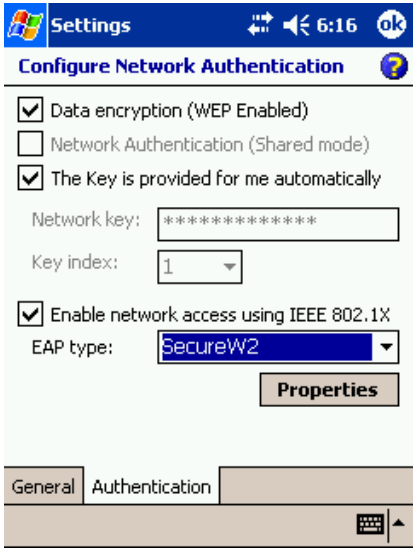
The "Configure Wireless Network" window will now pop up.

If you are adding new settings, enter the name of the SSID in the "Network Name" input field.

Select "Work".

> ***NOTE:*** *When "Work" has been selected this means that the profile "My Work Network" profile is active when the wireless adapters connects. As shown previously we have selected the "My Work Network" profile for private and Internet connections allowing the wireless adapter connection to be used for both.*

Select the "Authentication" tab.
The "Configure Network Authentication" window will pop up.



Make sure the configuration is as shown in the picture above. Then tap on the "Properties" button and you will be presented with the SecureW2 configuration window.

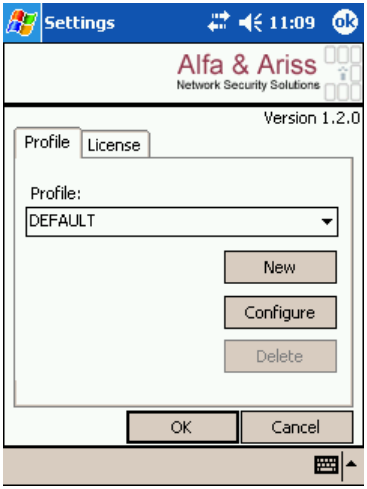
SecureW2 Client Configuration

SecureW2 Profiles

The main SecureW2 Client configuration window is built up out of two tabs:

- **Profile** in which you can manage your profiles
- **License** in which you install or verify your license

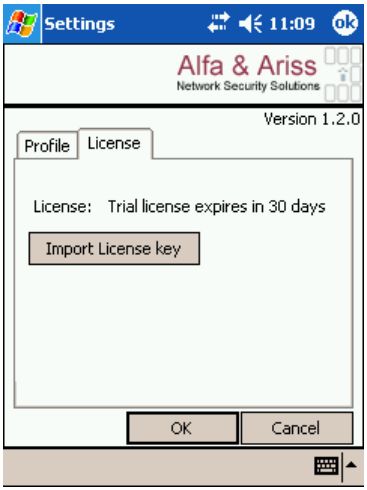
Managing your Profiles



SecureW2 2 uses profiles to configure the client. This window allows you to create, edit and delete profiles as you wish.

Profile	This drop down box lets you select the current profile for this connection.
New	Tap on this button to create a new profile.
Configure	Tap on this button to configure the profile currently selected in the drop down box.
Delete	Tap on this button to delete the profile currently selected in the drop down box.

Configuring your License



The License tab shows the current status of your license. Tapping on "Import License key" button to import your SecureW2 license. You will be presented with a window in which you can select your license file. The status will then show if the import was successful or not.

SecureW2 Profile Configuration

SecureW2 uses profiles to configure for connections. In this window, you can manage your profiles.

After creating a new profile or when you wish to configure an existing profile, you will be presented with the "SecureW2 Profile Configuration" window. This window is built up out of four tabs:

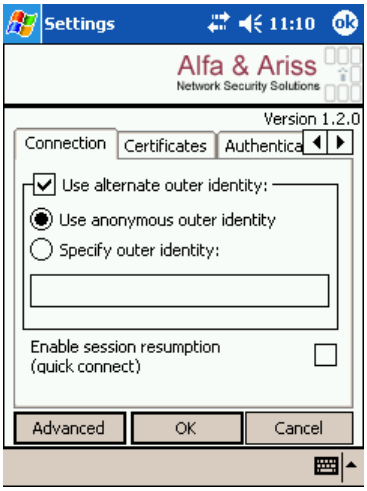
- **Connection** in which you specify connection settings
- **Certificates** in which you specify how you wish to handle certificates of network authentication servers you connect to
- **Authentication** in which you specify how you wish to authenticate
- **User account** in which you specify how the user will present his/her credentials.

Further more it is possible to access the advanced options by clicking on the "Advanced" button in the bottom left corner of the Profile tab.

For more information on the advanced options, see Advanced Configuration on page 20.

Configuring your Connection

In this tab you specify how you wish to handle certificates of network authentication servers that you connect to.



Use alternate outer identity

Allows the use of a different outer identity.

By default the username used to setup the secure tunnel (Outer Identity) and the username used for the actual authentication (Inner Identity) are the same. Selecting this gives you the following two options:

Use anonymous outer identity

Sets the outer identity to an anonymous identity. If for example the username entered in the user credentials window is: username@domain, selecting this option sets the outer identity to anonymous@domain.

Specify outer identity

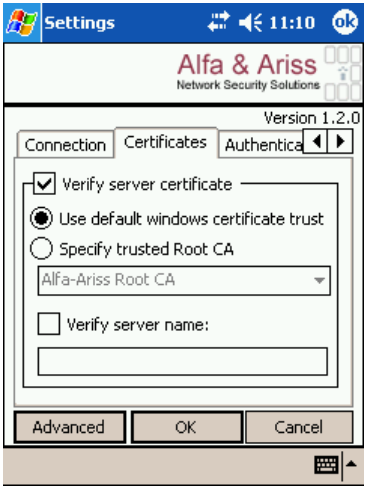
This allows you to specify the Outer Identity that is to be used during authentication.

Enable session resumption (quick connect)

Once a user has successfully been authenticated it is possible to use session resumption whenever the user's session times out or if a user has roamed to another access point.

Configuring Certificate Handling

In this tab you specify how you wish to handle certificates of network authentication servers that you connect to.



Verify server certificate

Select this option if you want the SecureW2 Client to verify the certificate of the remote server that will carry out the authentication.

> ***NOTE:*** *The certificate will be verified using the certificate trust of the local computer.*

Use default windows certificate trust

Select this to use the default windows certificate trust.

Trusted Root Authority

This list box allows you to control the way SecureW2 verifies the server certificate chain. The box shows a list of all the Trusted Root CA certificates that have been installed on the Local Computer. By selecting a Root CA you will restrict SecureW2 to connect only to server that has certificates issued by this CA.

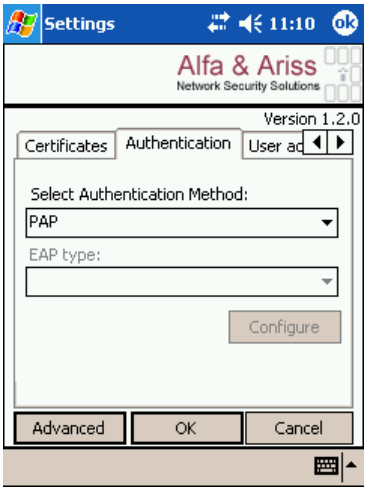
Verify server name

Select this option to allow SecureW2 to verify the Common Name in the certificate of the authenticating server.

By specifying "domain.com" SecureW2 will connect to all servers with a Common Name ending in "domain.com".

Configuring Authentication

In this tab, you configure how you wish to authenticate when connecting to the network.



Inner authentication type

This drop down box let's you select the inner authentication used by SecureW2. Currently you have two choices

- PAP (username password)
- EAP (SecureW2 will use another EAP module to authenticate the user)

EAP Type

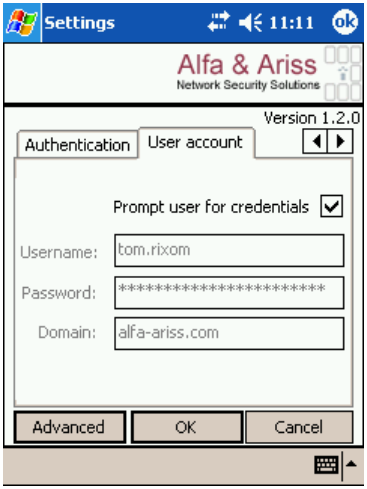
When you select EAP as the inner authentication type this drop down box will be enabled. It shows the current EAP modules installed on the device from you may choose to use as the inner authentication.

Configure

If an inner EAP module is configurable you can use this button to configure the selected inner EAP module.

Configuring your User Account

In this tab, you configure how the user will present her/his credentials when connecting.

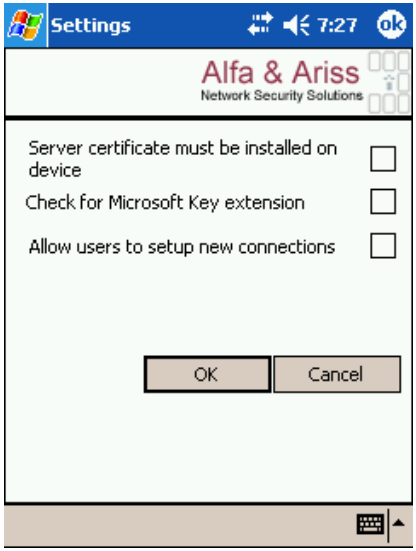


Prompt user for credentials

When this option is selected the user is prompted to enter his or her credentials during the authentication sequence.

Advanced Configuration

In this window, you configure the advanced options of SecureW2.



Server certificate must be installed on device

When this option is selected the certificate of the server must be installed in the certificate store of the device.

Check for Microsoft Key extension

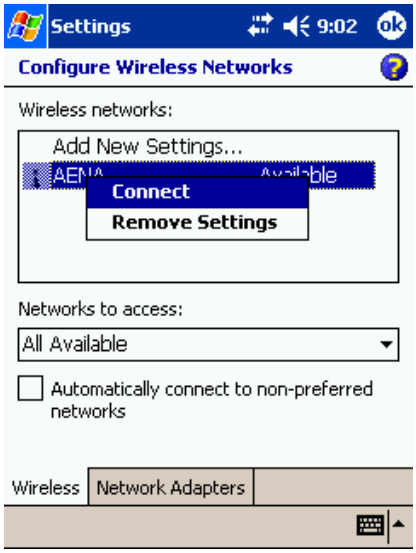
When this option is selected the certificate of the server must have the Enhanced Key Usage: **Server Authentication**.

Allow users to setup new connections

Select this option to allow users to setup new connections. By default users are not allowed to setup new connections (in other words, installing unknown certificates). This is to prevent hackers from trying to trick users into connecting to their access point by inserting a certificate that appears to be from the user's organization.

Connecting to the Network

As soon as you have configured SecureW2, the authentication procedure for connecting to the network will start automatically.



However, to force connection, simply tab and hold down the stylus on the appropriate SSID in the "Configure Wireless Networks" window. Select "Connect" when the menu shows.

Depending on your profile, SecureW2 might prompt you for your credentials. Otherwise, connecting and authenticating will be automatically executed.

Unknown Server

The first time you connect to an authentication server and the server certificate is not trusted; SecureW2 will pop up the "Unknown server" window.

NOTE: *The "Unknown Server" window will only appear if the option "Allow users to setup new connections" is selected.*

This shows the certificate hierarchy in which the unknown server certificate resides. This window will only pop up if you have selected **Verify server certificate** in the certificate handling options of SecureW2.
Before you can connect to the server all the certificates in the chain must be trusted. To trust a certificate is must be installed onto the device.


Indicates a trusted certificate


Indicates a certificate is not trusted

Install All Certificates

Installs all displayed certificates as trusted.

Install Certificate

Installs the selected certificate as trusted.