SecureW2 Client for Windows
User Guide

Version 3.1

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

Copyright © 2005 Alfa & Ariss

All rights reserved

Released: August 2005

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Alfa & Ariss (alfa-ariss.com/securew2.com).

Every effort has been made to ensure the accuracy of this manual. However, Alfa & Ariss makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Alfa & Ariss shall not be liable for any errors or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information of this document is subject to change without notice.

Trademarks
SecureW2 is a trademark of Alfa & Ariss.

Other product names mentioned in this manual may be trademarks or registered trademarks of their related companies and are the sole property of their respective manufacturers.

Table of Contents

Prerequisites

Currently the SecureW2 Client v3.x runs on the following (minimal) set-ups:

- Windows XP (Service Pack 1 recommended)
- Windows 2000 with Service Pack 4

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

The installation must be carried out by a user with Administrator privileges on the local computer.

To install the SecureW2 Client v3.x first make sure your computer meets the requirements shown above. The installation is then as follows:

1. Unzip the securew3xx.zip file to a temporary directory.
2. Double click on the SecureW2_3xx.exe file.
3. Follow the online instructions.
4. After the installation is complete, reboot the computer as instructed by the set-up.
5. To configure the SecureW2 Client please refer to the SecureW2 Users Guide.

Installation on Windows 2000

When installing on Windows 2000 make sure you have started the "Wireless Zero Config" service and set the startup-type to "Automatic".

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.

Uninstallation

Only users with Administrator privileges are able to remove the SecureW2 Client.

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

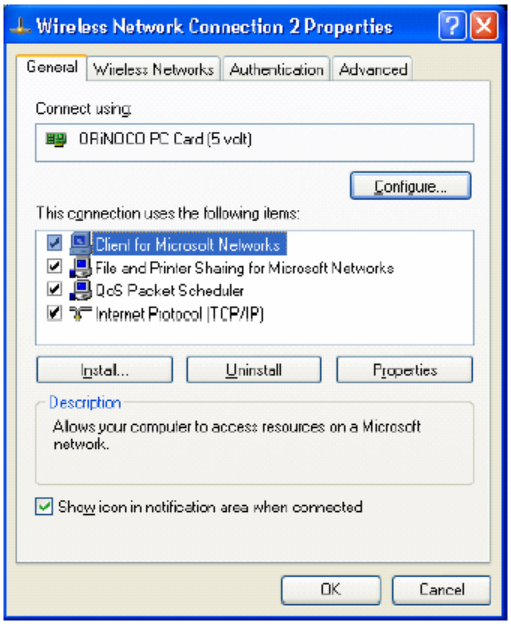
Configuring Windows

The SecureW2 Client v3.x module can be used for wired and wireless connections. The following section shows how to configure your wireless network adapter for 802.1X. For wired connections you can skip section this section and continue with the section

Configuring 802.1X for SecureW2 on page 10.

Configuring wireless settings

To configure a wireless adapter for 802.1X first open the "Network Connections" folder. Right-Click on your wireless adapter and select "Properties".



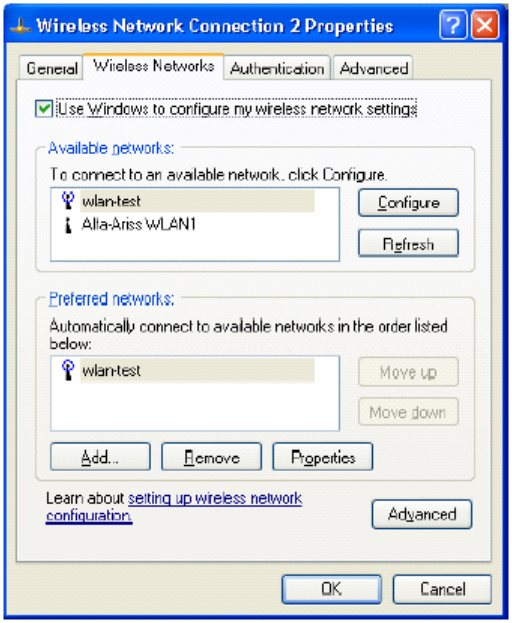
Make sure the "Show icon in notification area when connected" is selected.

In Windows XP you must use the Windows XP wireless client to configure your wireless network adapter. In Windows 2000 you must use the client software provided with your wireless Ethernet card, as there is no standard wireless client. Please refer to the manual for your wireless network adapter for more information on how to configure for 802.1X.

The following steps show how to configure your adapter using the Windows wireless client in XP. Windows 2000 users can skip this section.

Using Windows XP to configure your wireless adapter

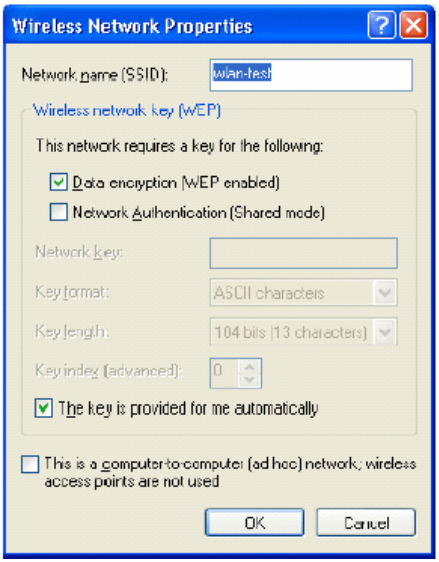
Select the "Wireless Networks" tab.



Make sure the "Use Windows to configure my wireless network settings" is selected.

The "Available networks" box shows the available access points. Select the one you wish to connect to and click on "Configure".

You are now presented with the "Wireless Network properties" window.



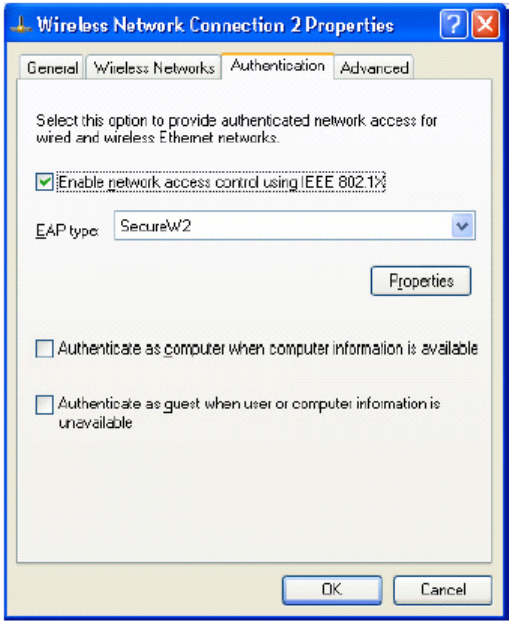
Here you can configure the basic wireless setting for your adapter. If you wish to use 802.1x you must configure the adapter to use Data encryption (WEP). To do this select "Data encryption (WEP enabled)" and "The key is provided for me automatically".

When configured, the access-point will appear in the "Preferred networks" box as shown in the Wireless Networks tab.

Configuring 802.1X for SecureW2

To use the SecureW2 Client you must enable 802.1x for the wired/wireless adapter. To enable 802.1x select the "Authentication" tab in the "Wireless properties" window, see the Wireless properties window.

> ***NOTE:*** *The location of the "Authentication" tab can differ between different versions of Windows. In Windows XP and Windows 2000 the "Authentication" tab is located in the "Wireless properties" window, see the Wireless properties window. In Windows XP Service Pack 1 and higher the "Authentication" tab is located in the "Wireless Network" window, see the Wireless Network Properties window.*



Select "Enable network access control using IEEE 802.1X". You can now select the "EAP type" from the pull down menu.

Select "SecureW2" as the "EAP type" and click on "Properties".

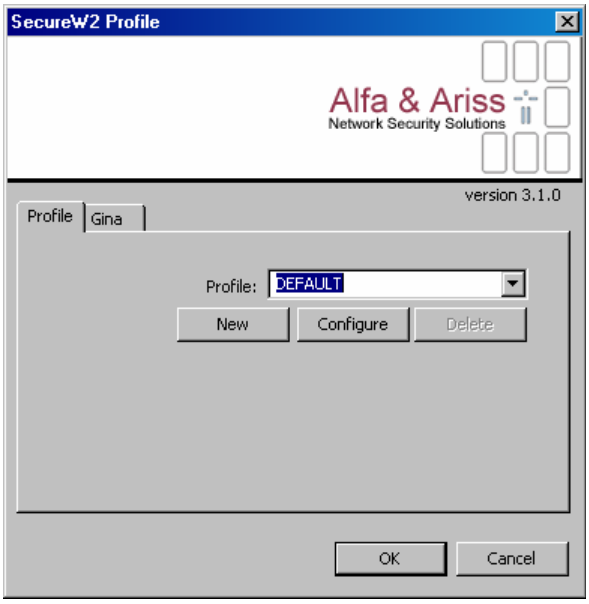
SecureW2 Client Configuration

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

- **Profile** in which you can create, configure or delete a profile.
- **Gina** in which you configure the SecureW2 Gina

> ***NOTE:*** *Administrative users have full access to all options displayed. Non-administrators not able to select the Gina Tab.*

Managing your Profiles



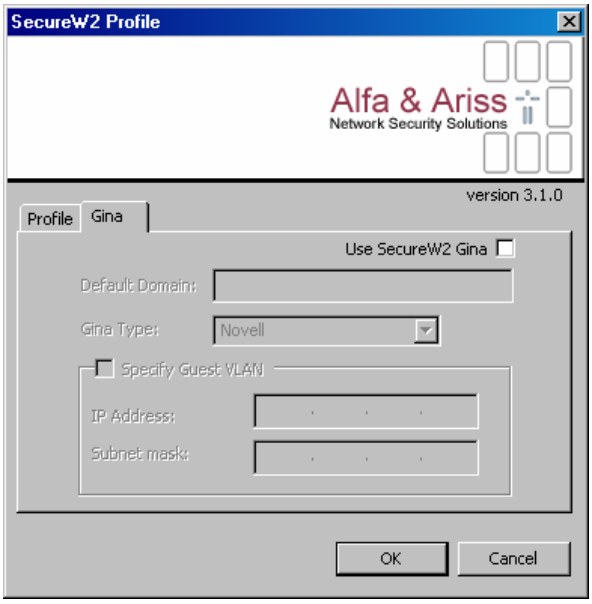
SecureW2 3.x uses profiles to configure the client. This window allows you to create, edit and delete profiles as you wish.

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.

> ***NOTE:*** *Administrative users have full access to all options displayed. Non-administrators are only able to configure the selected profile. They cannot create, select or delete a profile.*

SecureW2 Gina



Use SecureW2 Gina

Enables the SecureW2 Gina functionality.

Default Domain

Enter the default domain you wish to use while authenticating using the Gina interactive logon credentials.

Gina Type

Select the type of Gina that is required. Currently only Novell is supported.

Specify Guest VLAN

Enables the use of the VLAN functionality. When configured the SecureW2 Gina will only perform 802.1X if the IP Address of the adapter matches the configured IP and Subnet mask.

IP Address

Enter the IP Address of the Guest VLAN.

Subnet mask

Enter the Subnet mask of the Guest VLAN.

SecureW2 Profile Configuration

After creating a new profile or when you wish to configure an existing profile you will be presented with the "SecureW2 Profile Configuration" window.

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.

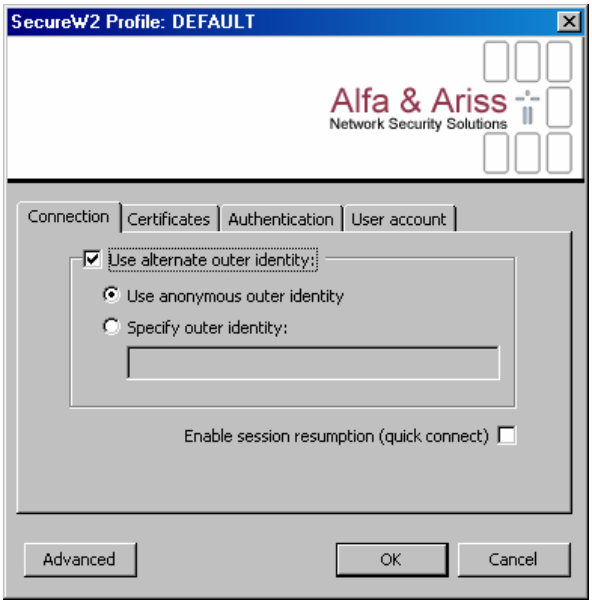
> ***NOTE:*** *Non-Administrative users can only access the "User account" tab.*

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 the upcoming heading **Advanced configuration**.

Configuring your Connection

In this tab you can specify connection settings.



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.

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

Specify outer identity

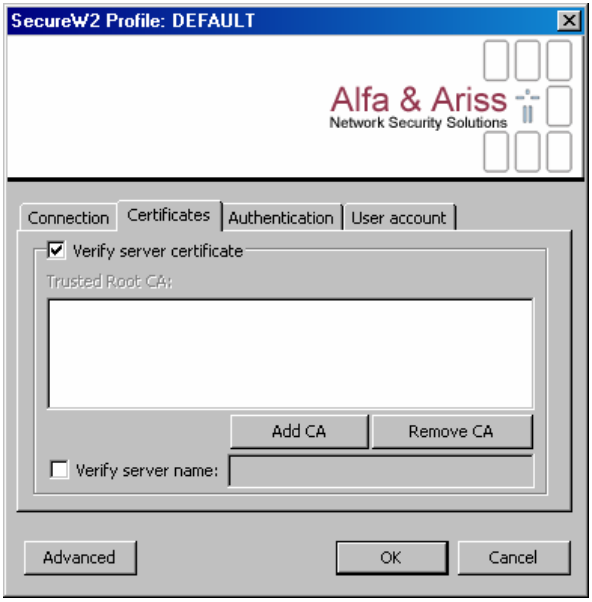
This allows you to specify the Outer Identity that is to be used during authentication.

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.*

Trusted Root CA

This selection box contains the certificate authorities currently trusted by SecureW2. To add an remove certificates use the following options:

Add CA

When you select this option a dialog box is shown with the current certificate authorities installed on the local computer. Select the appropriate ca and click on OK. The certificate authority will now appear in the selection box "Trusted Root CA"

Remove CA

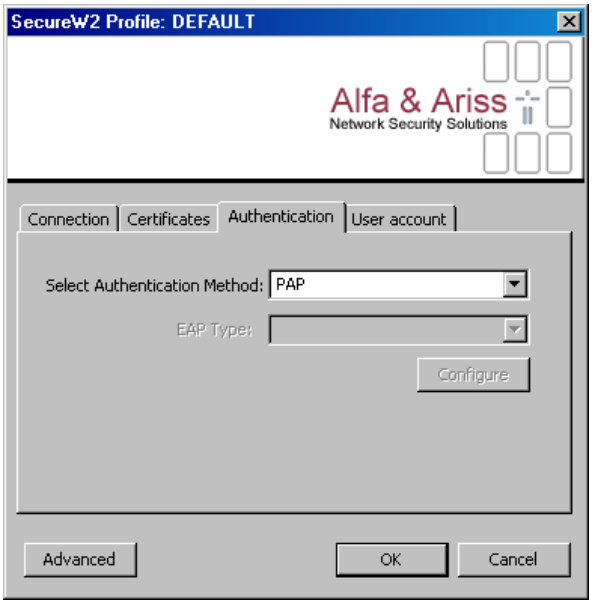
When you select this option the highlighted certification authority will be removed from the selection box "Trusted Root CA".

Verify server name

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

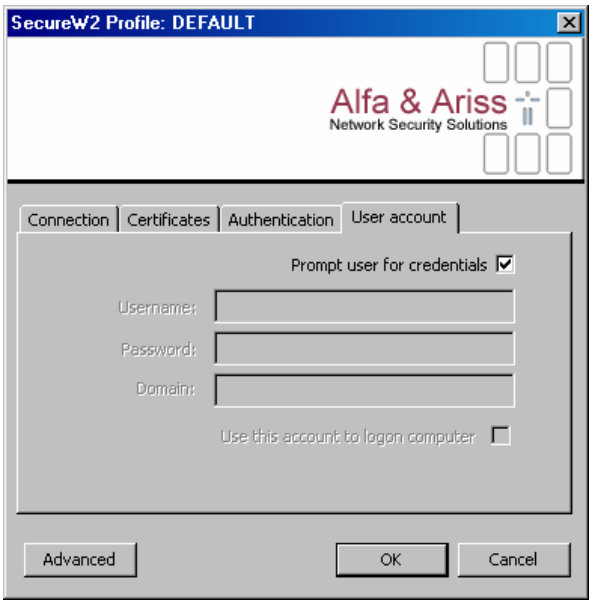
When you select EAP as the inner authentication type this drop down box will be enabled. It shows the current EAP modules installed on the device from you may choose to use as the inner authentication.

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

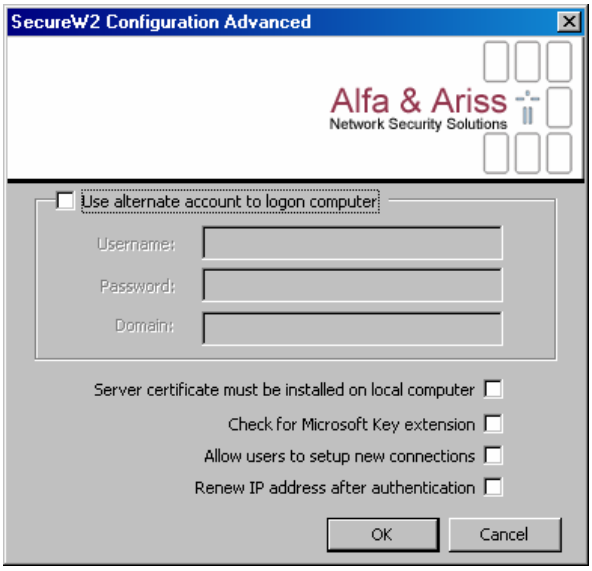
When this option is selected the user is prompted to enter his or her credentials during the authentication sequence.

Use this account to logon computer

When this option is selected the user credentials will also be used to logon the computer during start up.

Advanced Configuration

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



Use alternate account to logon computer

When this option is selected the credentials entered in the fields "Username", "Password" and "Domain" are used to authenticate the connection when the system itself wants to setup a 802.1X connection.

Server certificate must be installed on local computer

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

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 (meaning install 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.

Renew IP address after authentication

When this option is selected the SecureW2 client will try to renew the adapters IP address after successful authentication.

> ***IMPORTANT:*** *Use only if necessary. This option is only applicable to setups where the DHCP renewal is not working correctly. Do NOT use in normal circumstances.*

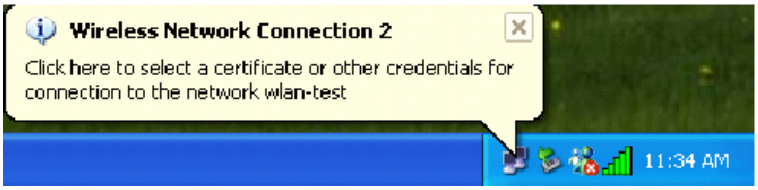
Connecting to the Network

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

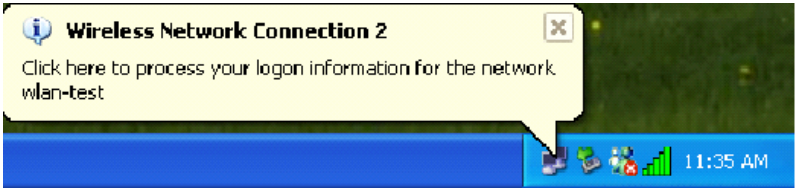
Windows XP User Interface

Windows XP uses a specific user interface in which, before a user can interact, the user must first click on an "Information pop-up" in the bottom-right hand side of the screen. Simply click anywhere in the "Information pop-up" and the actual interaction window will appear in which the user may for example enter a username. There are two types of "Information pop-up" used during the 802.1x authentication.

When the user needs to enter his/her credentials:

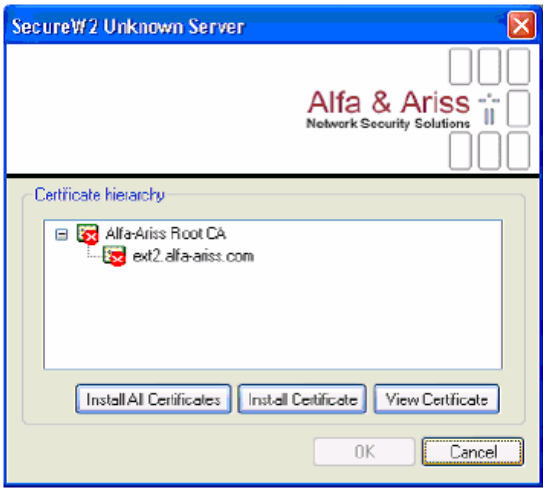


When the "Unknown server" (See section 2.2 Unknown Server) window is to be displayed:



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.

View Certificate

Lets you examine a certificate.

Miscellaneous

Event Logging

The SecureW2 Client uses the standard Windows Event Logger for logging. To view the SecureW2 Event Log simply use the standard Windows Event Viewer (Located under "START", "SETTINGS","ADMINISTRATIVE TOOLS","EVENT VIEWER"). All events are placed in the "Application Log".

Enabling domain logon

It is possible to configure the SecureW2 Client so that there is IP connectivity at the start-up of Windows. This makes things as Windows Domain Logon and Novell Network Logon possible. To achieve this, make sure that the SecureW2 is configured in a way that requires no user interaction. This means that the option "Prompt user for credentials" must NOT be selected and the Username, Password and optional Domain field are filled in correctly.

Furthermore if the "Verify server certificate" option is also selected, make sure that the certificate chain of the server is correctly installed.

Trouble shooting

If you are having problems connecting please verify that the authentication was successful. You can do this by opening the "Network Connections" folder. If the authentication was successful then the wireless adapter should show the text "Authentication succeeded". If not it could be because of the following:

- Incorrect username/password/domain, make sure these are correct.
- WEP is not enabled when using a wireless connection, if authentication is successful and you still cannot get any IP activity make sure you have selected 'wireless' as the connection type in the configuration of SecureW2.

Known problems

- It is possible that when not using computer credentials the user might be prompted multiple times to authenticate. Use the first window to enter your credentials and close the rest.
- When logging on to the machine while SecureW2 has not been configured or has been miss-configured it can take a while before the network connection comes up.
- If you use the "Connect to Wireless Network" window to connect to an access point, there is a known bug in the Microsoft 802.1x client, which could result in a "double" authentication. If you wish to (re-) connect it is best to disable/enable the adapter.