

How to configure SecureW2



Disclaimer

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 © 2009 SecureW2 B.V.

All rights reserved

Released: Juli 2009

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 SecureW2 B.V.

Every effort has been made to ensure the accuracy of this manual. However, SecureW2 makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. SecureW2 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 SecureW2 B.V.

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.

1 SecureW2 TTLS and PEAP Configuration

1.1 Profile

SecureW2 uses profiles to configure the TTLS and PEAP methods. This window allows you to create, edit and delete profiles as you wish.



Option	Description
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.
<p>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.</p>	

1.2 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.

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.

1.2.1 Connection



In this tab you can specify connection settings:

Option	Description
Use alternate outer identity	Allows the use of a different outer identity.
Use anonymous outer identity	Sets the outer identity to an anonymous identity. If for example the username entered in the user credentials window is: useramer@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.

1.2.2 Certificates



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.

Option	Description
Trusted Root CA	This selection box contains the certificate authorities currently trusted by SecureW2.
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	Select this option to allow SecureW2 to verify the

server name	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".
-------------	---

NOTE: If you leave the Trusted Root CA empty you will receive a warning stated that SecureW2 will use the default Microsoft certificate trust to verify the certificates.

1.2.3 Authentication



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

Option	Description
Select Authentication Method	This drop down box let's you select the inner authentication used by SecureW2. Currently you have two choices: 1. PAP (username password) 2. 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.

1.2.4 User Account

Enterprise Client - DEFAULT

SecureW2

Connection | Certificates | Authentication | User account

Prompt user for credentials

Username:

Password:

Domain:

Use this account to logon computer

Advanced OK Cancel

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

Option	Description
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.

1.3 Advanced Configuration



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

Option	Description
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".
The options Server certificate must be installed on local computer and Check For Microsoft Key extension will only work if the option Verify Server Certificate is enabled in the Connection tab.	
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	When this option is selected the SecureW2 client

address after authentication	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.
------------------------------	--

1.4 Connecting to the Network

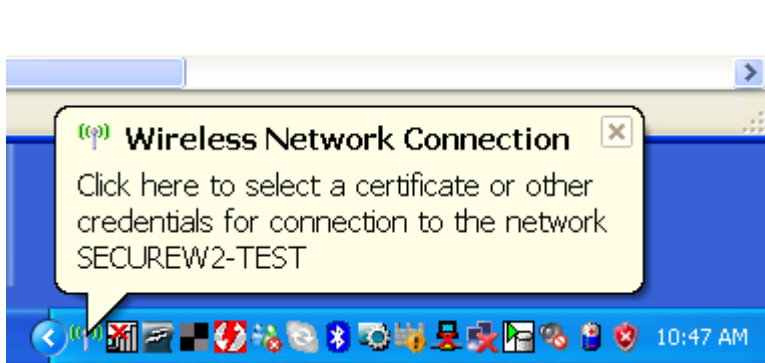
As soon as you have configured SecureW2, the authentication procedure for connecting to the network will start automatically.

1.4.1 Windows XP and Vista User Interface

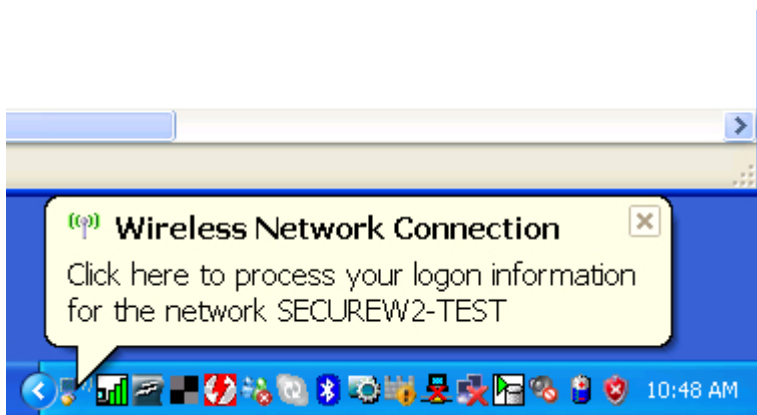
Windows XP and Vista use a specific user interface in which, before a user can interact, the user must first click on an “Information pop-up” in the bottom-right hand side of the screen. Simply click anywhere in the “Information pop-up” and the actual interaction window will appear in which the user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

IMPORTANT: Make sure the “Show icon in notification area when connected” is selected in the adapter properties. This will allow the Wired and Wireless Zero Config to interact with the user when needed.

1. When the user needs to enter his/her credentials:




2. When the “Unknown server” (See section 2.2 Unknown Server) window is to be displayed:



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

<i>Option</i>	<i>Description</i>
Install All Certificates	Installs all displayed certificates as trusted.
Install Certificate	Installs the selected certificate as trusted.
View Certificate	Lets you examine a certificate.