

How to configure SecureW2 Server



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: December 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.

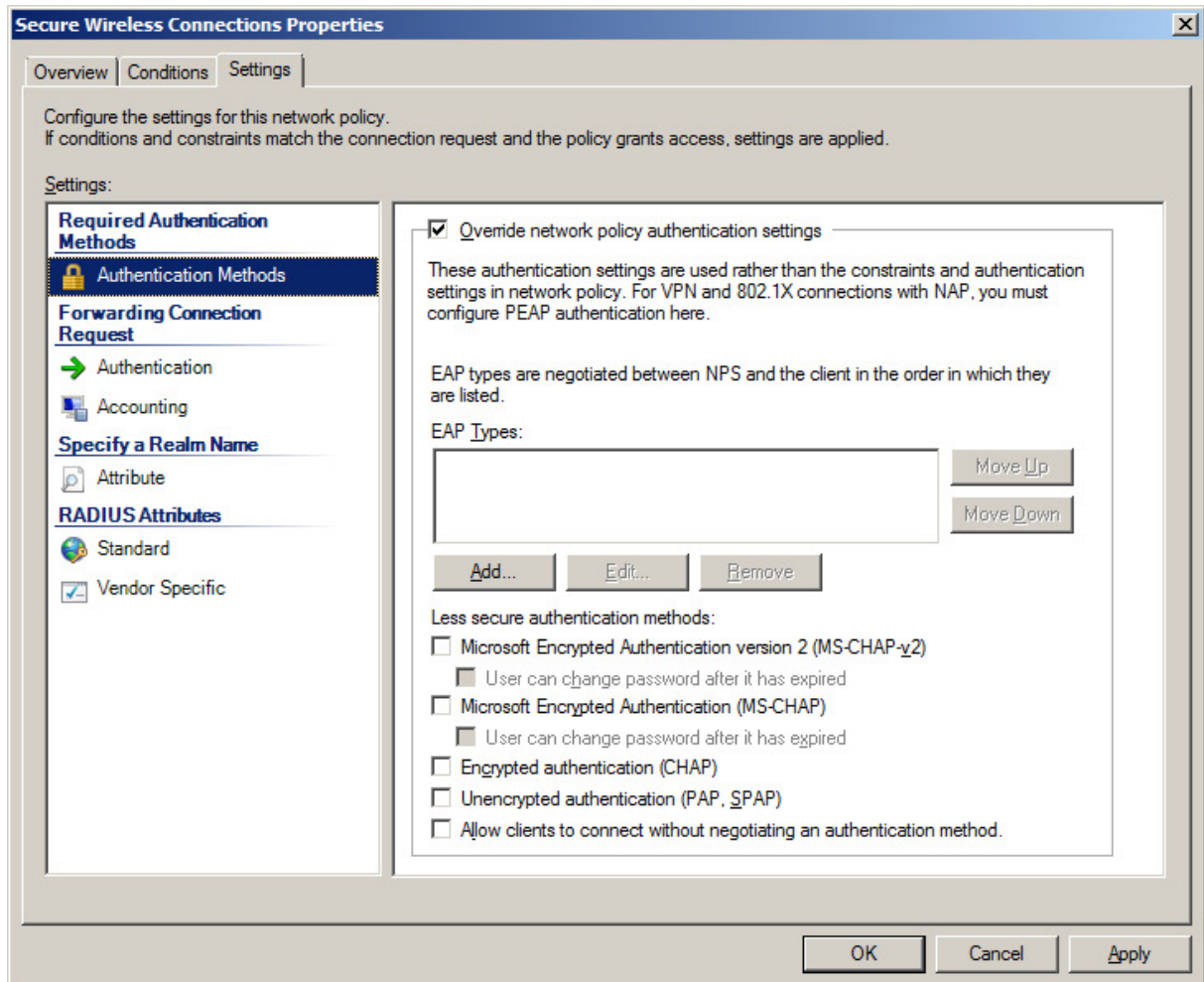
Other product names mentioned in this manual may be trademarks or registered trademarks of their related companies and are the sole property of their respective manufacturers.

1 Introduction

The following guide describes how to configure the SecureW2 Enterprise Server. This guide assumes that the reader is familiar with using and configuring the Microsoft Network Policy Server.

2 Network Policy Server (NPS)

The SecureW2 Enterprise Server runs as part of the Microsoft NPS server. It can be configured as an EAP TYPE in the “Authentication Methods” section of an NPS policy.



The SecureW2 Enterprise Server is listed as an EAP Type and can be added to the list of EAP Types by clicking on “Add...” and selecting the SecureW2 PEAP/TTLS or GTC method.

To configure the selected EAP Type simply select the EAP Type and click on “Edit...”, you will then be presented with the SecureW2 Enterprise Server Configuration.

3 Configuration

3.1 Certificate

The “Certificate” tab displays the server certificate that is currently being used to setup a secure TLS channel with the client.



Option	Description
View Certificate	Select this option to view the current server certificate.
Change Certificate	Select this option to add or change the server certificate.

Select “Change Certificate” to select a server certificate.

NOTE: The certificate must be installed in the local computer root certificate store

3.2 Authentication

The “Authentication” tab is used to configure which types of inner authentication the SecureW2 Enterprise Server supports. PAP is supported by TTLS, EAP is supported by both TTLS and PEAP. The EAP authentication methods list contains the supported EAP methods. The order in the list is the order in which the SecureW2 Server will negotiate the EAP method requested by the client.



Option	Description
Authentication methods	
Allow PAP authentication	Select this option to allow PAP authentication
Allow EAP authentication	Select this option to allow EAP authentication, this will enable the “EAP authentication methods” list.
EAP authentication methods	
Add	Add a new EAP method to the list
Configure	Configure a selected EAP method
Remove	Remove a selected EAP method from the list
Prefer (Up)	Move an EAP method higher in the list
Prefer (Down)	Move an EAP method lower in the list

3.3 Database

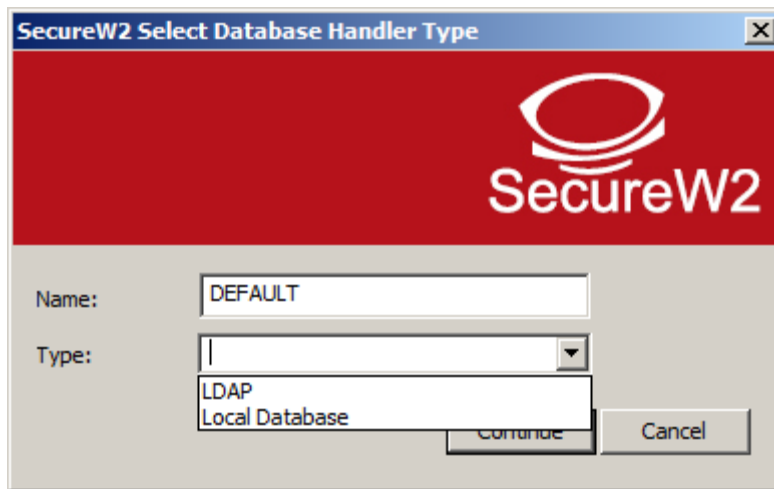
The SecureW2 Enterprise Server supports a number of database backends. This is configured by adding the appropriate database handlers to the list in the “Database” tab. The order in the list is the order in which the database handlers are called during identification and authentication. If a database handler fails the next in the list is called.



Option	Description
Add	Add a Database handler to the list
Configure	Configure a Database handler
Remove	Remove a Database handler from the list
Prefer (Up)	Move a Database Handler higher in the list
Prefer (Down)	Move a Database Handler lower in the list

3.3.1 Adding a Database handler

To add a database handler simply select “Add” in the “Database” tab.



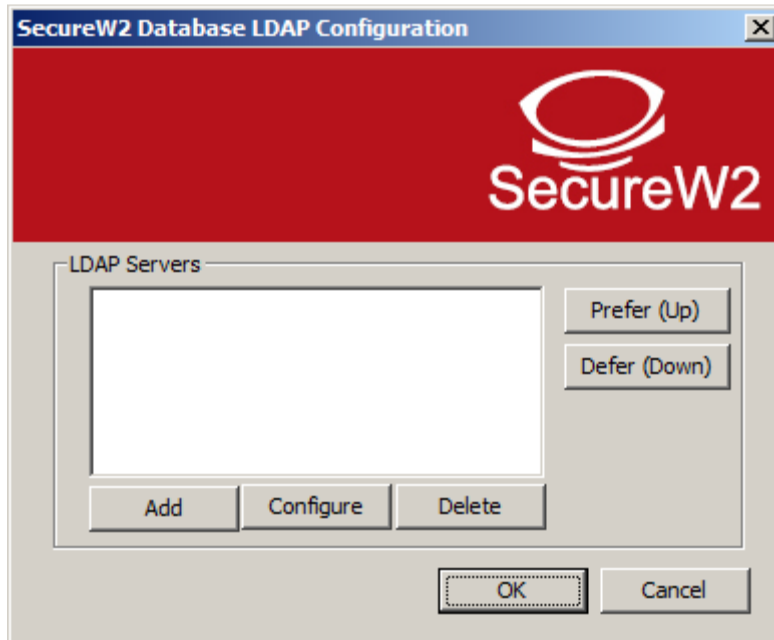
In the Select dialog select the “Type” of database handler you wish to add. The “Name” value is used to identify the database handler in the list (For example, “Primary LDAP”, “Secondary LDAP”).

3.3.2 Local Database Handler

The local database handler utilizes the Microsoft built-in LSA mechanism. If the NPS is part of an Active Directory it will use this as the user database backend. If the NPS is standalone it will use the local user accounts. This database handler does not require any additional configuration.

3.3.3 LDAP Database Handler

The LDAP database handler uses (multiple) LDAP server as a user database backend. Up to 5 LDAP servers can be defined. The order in the list is the order in which the LDAP servers are queried. If an LDAP server query fails the next in the list is tried until the LDAP server query succeeds.



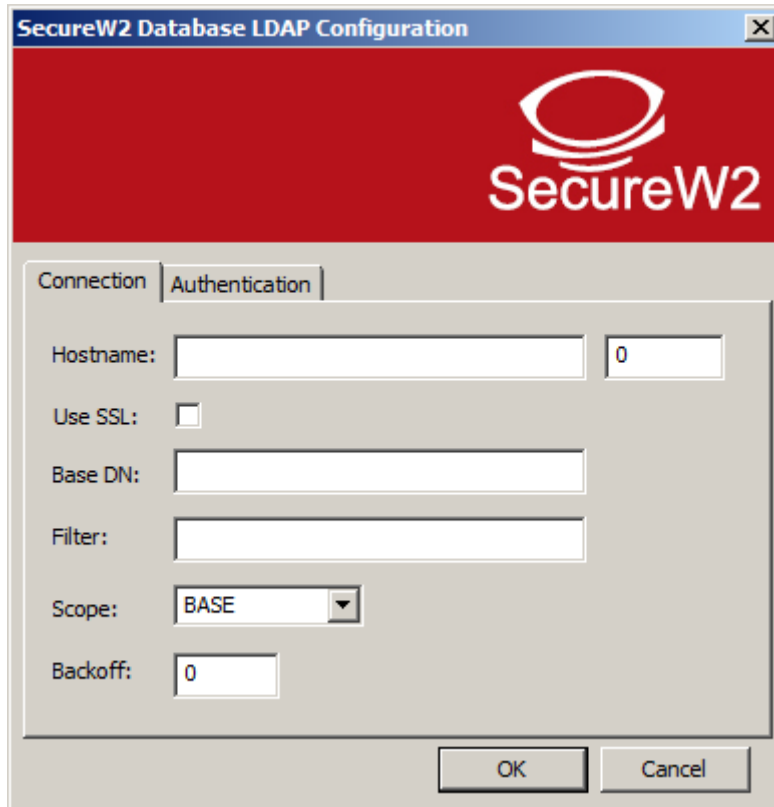
Option	Description
Add	Add an LDAP Server to the list
Configure	Configure an LDAP Server
Remove	Remove an LDAP Server from the list
Prefer (Up)	Move an LDAP Server higher in the list
Prefer (Down)	Move an LDAP Server lower in the list

3.3.3.1 LDAP Server Configuration

The LDAP Server Configuration is used to specify the connection and authentication parameters of an LDAP Server.

3.3.3.1.1 Connection

The “Connection” tab contains the information for connecting to the LDAP Server.



The screenshot shows a dialog box titled "SecureW2 Database LDAP Configuration" with a red header containing the SecureW2 logo. The "Connection" tab is selected. The dialog contains the following fields and controls:

- Hostname: A text input field followed by a port number input field containing "0".
- Use SSL: A checkbox that is currently unchecked.
- Base DN: A text input field.
- Filter: A text input field.
- Scope: A dropdown menu currently set to "BASE".
- Backoff: A text input field containing "0".

At the bottom of the dialog are "OK" and "Cancel" buttons.

Option	Description
Hostname	Enter the dns name/ip address and port number of the LDAP server
Use SSL	Specify whether SSL is to be used to secure the LDAP connection
Base DN	The base DN in which the query is executed
Filter	Specify a possible search filter for the query. To use the username in the filter use %s. For example: cn=%s
Scope	Scope of the query. Options are “BASE”, “ONE”, “SUBTREE”.
Backoff	The number of seconds an LDAP server should not be used after a query failed.

3.3.3.1.2 Authentication

The authentication tab contains the credentials to be used to connect to the LDAP Server.



The screenshot shows a dialog box titled "SecureW2 Database LDAP Configuration". The window has a red header with the SecureW2 logo. Below the header, there are two tabs: "Connection" and "Authentication", with "Authentication" being the active tab. The main area contains two input fields: "Auth DN:" and "Password:". At the bottom of the dialog, there are "OK" and "Cancel" buttons.

Option	Description
Auth DN	The authentication DN to be used for the query. For example: cn=admin,dc=test,dc=com
Password	The password belonging to the authentication DN

3.4 Advanced

The “Advanced” tab contains certain options to change the more advanced feature of the SecureW2 Enterprise Server.



Option	Description
PAP/MSCHAPv2 authentication	
Ignore EAP realm	Configure an LDAP Server
Convert EAP realm to Windows domain	Remove an LDAP Server from the list
Session resumption (quick connect)	
Enable session resumption (quick connect)	This enables Session resumption (quick connect).
Maximum time between two sessions	The maximum numbers of hours a previous authentication session is valid.