Dell SonicWALL and SecurEnvoy Integration Guide

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	Merlin House Brunel Road Theale Reading RG7 4AB	
Tony Davis	tdavis@securenvoy.com	
Chris Payne	chris.payne@infinigate.co.uk	+44 845 4900 245

Table of Contents

Introduction

SSL VPN Integration Guide

This document describes how to integrate a Dell SonicWALL UTM appliance with SecurEnvoy's two-factor Authentication solution SecurAccess.

Dell SonicWALL UTMs include an optional SSL VPN module which provides secure remote access via an SSL encrypted session to internally hosted infrastructure such as file shares and applications.

SecurEnvoy SecurAccess provides two-factor, strong authentication for remote Access solutions such as a Dell SonicWALL SSL VPN, without the complication or cost of deploying hardware tokens or smartcards.

Two-Factor authentication is provided by the use of a PIN and a mobile phone to receive a passcode which can be delivered via SMS, email or using a smart phone soft token installed from phone vendor app stores. SecurEnvoy SecurAccess has been designed to be an easy to deploy and use technology for both administrator and user.

It integrates directly into Microsoft's Active Directory and negates the need for additional user security databases instead storing parameters in the directory schema. SecurAccess consists of two core elements: a RADIUS server to facilitate communication with solutions such as Dell SonicWALL SSL VPNs and an authentication server to authenticate attempts to login with Microsoft Active Directory.

SecurEnvoy SecurAccess can be configured in such a way that it can utilise users existing Microsoft password instead of a PIN. Taking advantage of this feature allows the users to enter their familiar username, password and one time passcode removing the need to also remember a PIN. This authentication request is passed via the RADIUS protocol to the SecurEnvoy SecurAccess server whereby authentication of the user and token takes place.

Environment Conditions

The equipment used for the integration process is listed below:

Dell SonicWALL UTM appliance with firmware version SonicOS Enhanced 5.9.0.4-127o. Licensed for SSL VPN Node/Users.

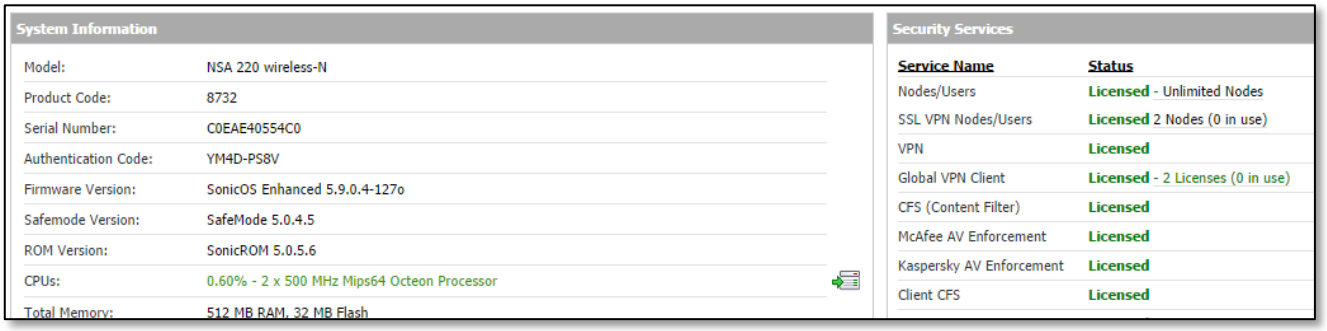

Figure 1 - Dell SonicWALL Version and Licensing

SecurEnvoy SecurAccess version 7.2.508 installed on a Windows Server 2008 R2 64-bit virtual machine. SecurAccess has been joined to an Active Directory domain and authenticates using LDAP. Tokens are delivered via SMS or soft token. RADIUS is enabled on default port TCP 1812.

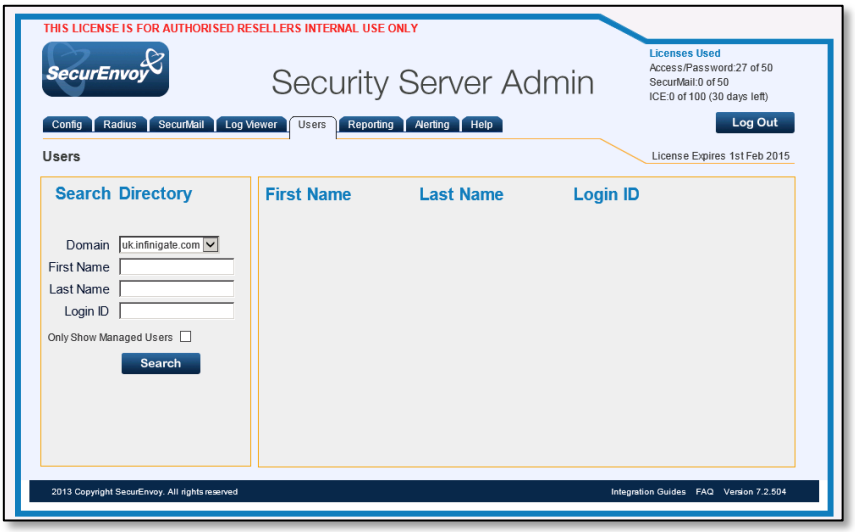

Figure 2 - SecurEnvoy SecurAccess Version and Licensing

Configuration

Prerequisites

It is assumed that the Dell SonicWALL UTM appliance is setup and SSL VPN is operational. An existing domain user can authenticate using a Domain password and access applications.

SecurEnvoy SecurAccess has a suitable account created that has read and write privileges to Active Directory.

SecurEnvoy SecurAccess requires LDAP connectivity either over ports TCP 389 or TCP 636 to the Active Directory servers and ports TCP/UDP 1645 or TCP/UDP 1812 for RADIUS communication from the Dell SonicWALL UTM appliance.

Configuring SecurEnvoy SecurAccess

1. Open and log into the SecurAccess web administration interface.

2. Select the **RADIUS** tab.

3. Enter the IP address of the Dell SonicWALL appliance into the **NAS IP Address field** and a shared secret into the **Shared Secret** field.

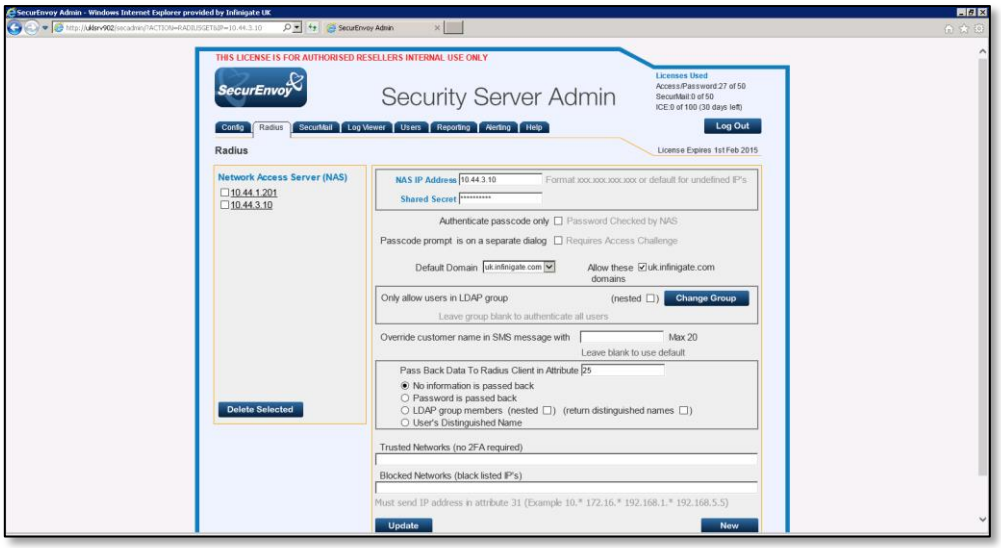

Figure 3 - Configuring SecurAccess RADIUS Settings

4. In this scenario as we will be combining the password and passcode for authentication, un-tick the option **Passcode Prompt is on a Separate Dialog.**

5. Press the **Update** button to save the changes.

Configuring the Dell SonicWALL appliance

1. Launch the Dell SonicWALL web based admin interface.

2. From the left menu pane, expand **Users** and select **Settings**.

3. Select under **User Authentication Method** select **RADIUS + Local Users** from the drop down menu. Note that is recommended that a local user option is available as a back door for admins in the unlikely event that there is an issue with RADIUS communications.

4. Press the **Configure RADIUS…** button.

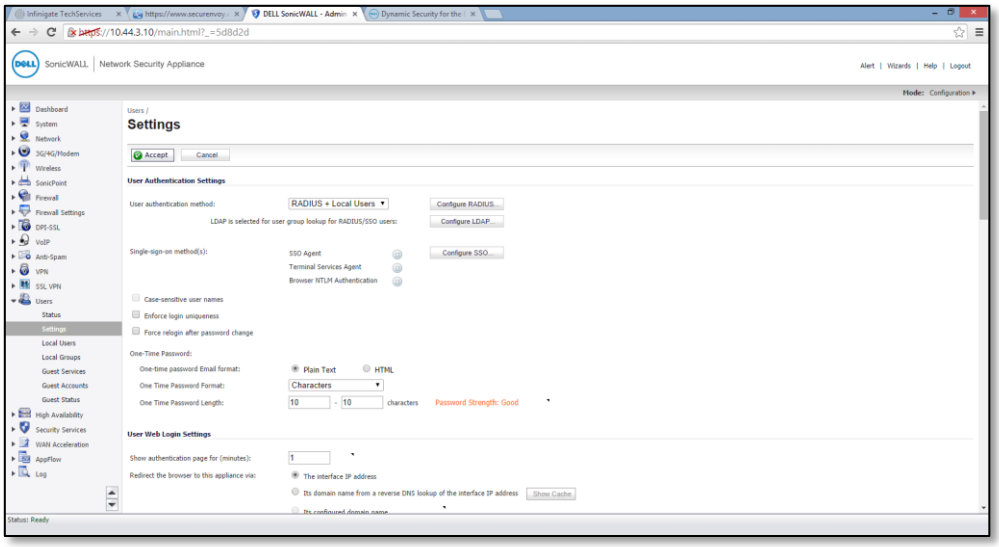

Figure 4 - Enabling RADIUS Authentication on Dell SonicWALL

5. Set the **Global RADIUS Settings** to 10 seconds timeout and 1 retry.

6. Set **IP address**, **shared secret** (the same shared secret which was entered into the SecurAccess interface) and **port** used to communicate with the SecurEnvoy SecurAccess Server.

7. A secondary SecurEnvoy SecurAccess server can be added for resilience.

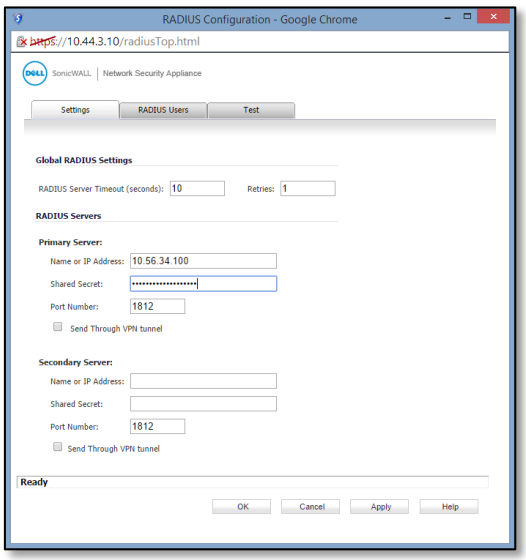

Figure 5 - Configuring SonicWALL RADIUS Settings

8. To test the configuration, select the **Test** tab.

9. Enter the test accounts username in **User** field and the password plus passcode in **Password** field. Press the **Test** button to complete the test and review the results.

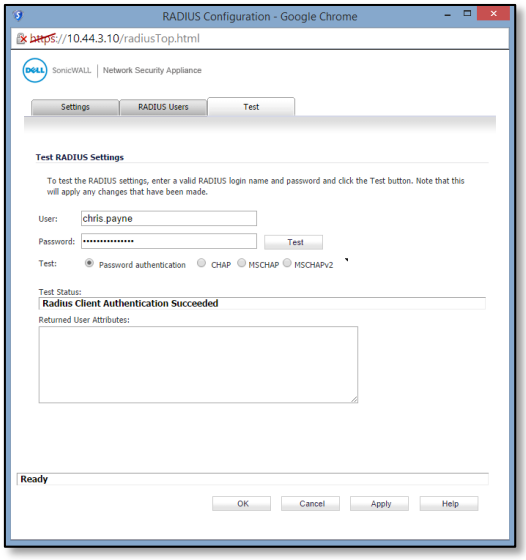

Figure 6 - Successful SonicWALL RADIUS Test

Testing

Logging into Dell SonicWALL SSL VPN

1. Open the Dell SonicWALL SSL VPN site in a web browser.

2. Enter the test user's username in the **Username** field and the users password followed by the passcode in the **Password** field.

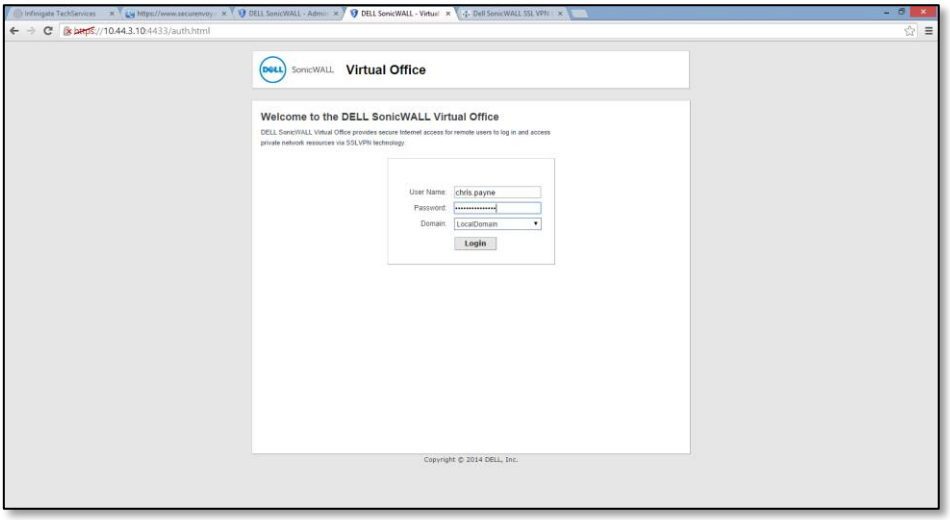

Figure 7 - Logging into the Dell SonicWALL SSL VPN Portal

3. Press the Login button to continue.

4. You should now be logged into the Dell SonicWALL SSL VPN service.

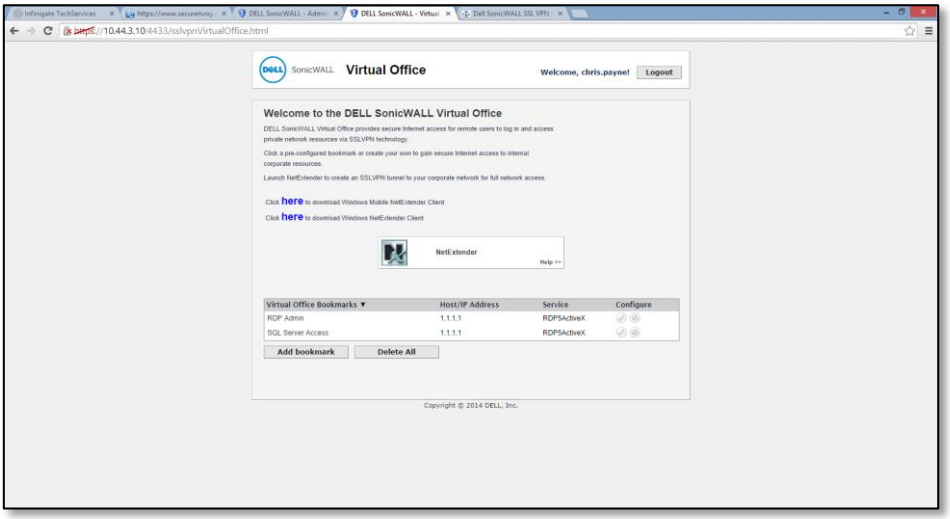

Figure 8 - Logged into the Dell SonicWALL SSL VPN Portal

Further Information

Administration Guides

For further information or advice on custom configuration of either SecurEnvoy SecurAccess of Dell SonicWALL UTM appliances please visit the vendor's websites.

http://www.securenvoy.com

http://www.sonicwall.com

Version History

Version	Details	Name	Date
1.0	First Version.	Chris Payne	18/09/2014