A Shearwater Group plc Company

www.securenvoy.com

Sonicwall (NSV) Network Security Virtual Guide

SecurAccess Integration Guide

Version 1.0 – 10/18

Sonicwall NSV Integration Guide

Contents

1.1 Solution Summary

SecurEnvoy's SecurAccess MFA solution integrates with Sonicwall's (NSV) Network Security Virtual appliance through the use of RADIUS Server for authorisation and access control.

The software used for the integration process is listed below:

Sonicwall - SonicOS Enhanced 6.5.0.2-8v-37-211-66468e85
SecurEnvoy SecurAccess Release v9.3.502

1.2 Guide Usage

The information in this guide describes the configuration required for integration with SecurEnvoy and common to most deployments. It is important to note two things:

- Every organization is different and may require additional or different configuration.
- Some configuration may have other methods to accomplish the same task than those described.

1.3 Prerequisites

The following conditions are required to set up SecurEnvoy's MFA Solution:

- A SecurAccess MFA server installed, configured and working on a system with:
  - Windows Server 2003 or higher.
  - An LDAP or Lightweight Directory Service database of users

  Note: Please see SecurEnvoy's SecurAccess version 9.3 deployment guide on how to setup MFA server solution (On the www.securenvoy.com website)

- A Sonicwall Network Security virtual appliance running version 6.5.0.2 and above, (previous versions of Sonicwall may work but have not been tested with full functionality)

- This guide assumes that Sonicwall has been installed and previously configured to authenticate users with a username and password locally or via LDAP.

- Familiarity with the following technologies:
  - RADIUS configuration
  - Sonicwall NSV Administration Interface

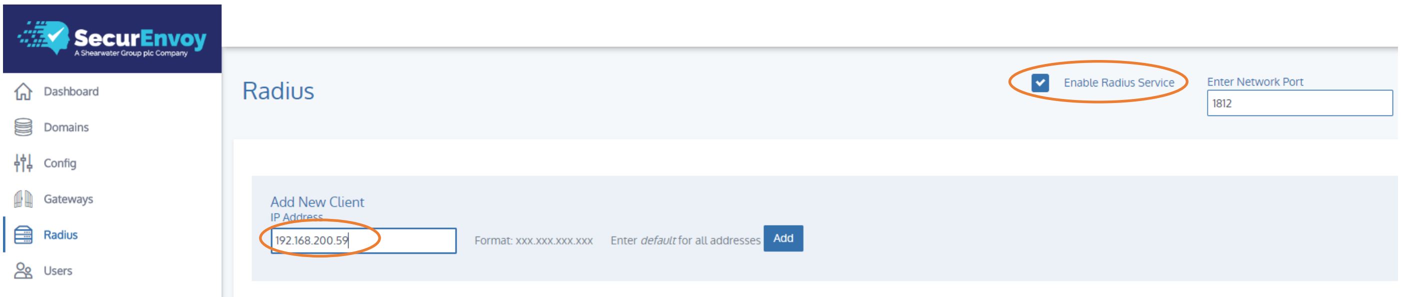
1.4 Authentication

The following section describes the steps required to configure the Sonicwall NSV appliance to authenticate users via RADIUS through the SecurEnvoy SecurAccess Solution.

1.41 Setup RADIUS - SecurAccess

Within the SecurAccess configuration, we will need to configure the Sonicwall appliance as an authorised RADIUS client.

- Navigate to RADIUS in the administrator dashboard.
- Ensure the RADIUS Service is enabled in the top right-hand side of the screen and make sure the port number is left as default 1812.
- Enter the internal IP address of the Sonicwall Appliance and click "Add"



Radius

☑ Enable Radius Service

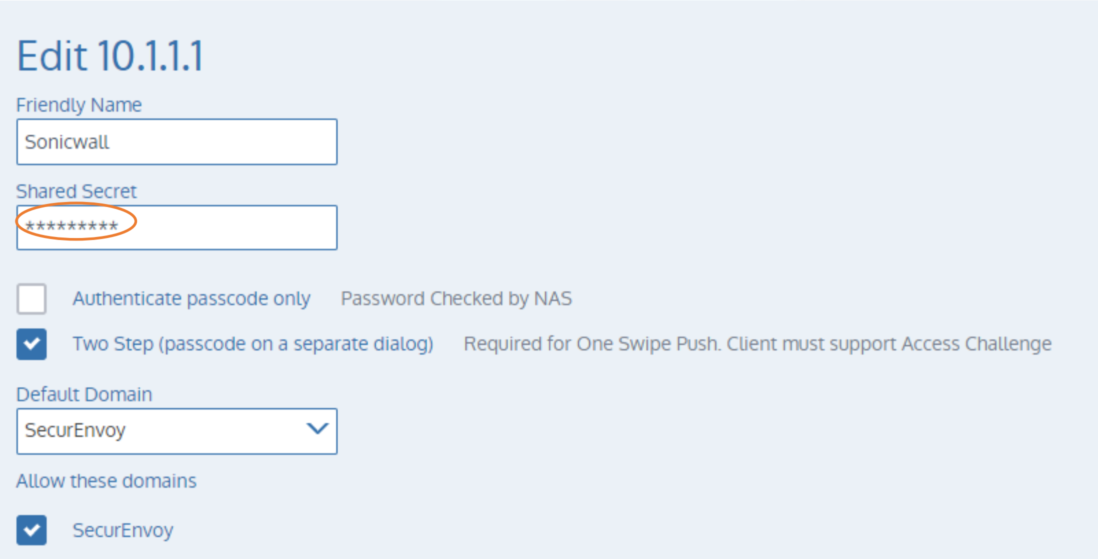
Enter Network Port: 1812

Add New Client

IP Address: 192.168.200.59

Format: xxx.xxx.xxx.xxx Enter *default* for all addresses

- Enter in a shared secret or common password and select the domains that will be authenticated against (if there is more than one domain configured in SecurAccess)
- Click Update



Edit 10.1.1.1

Friendly Name: Sonicwall

Shared Secret: *********

□ Authenticate passcode only Password Checked by NAS

☑ Two Step (passcode on a separate dialog) Required for One Swipe Push. Client must support Access Challenge

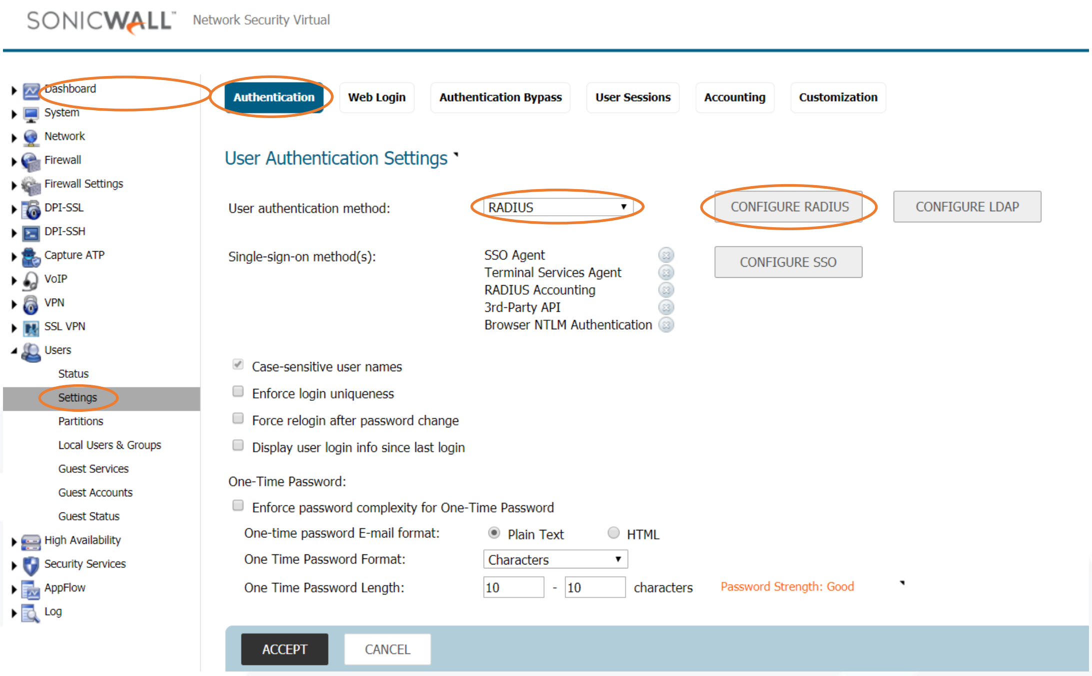
Default Domain: SecurEnvoy

Allow these domains

☑ SecurEnvoy

1.41 Setup RADIUS – Sonicwall

Navigate to Users\Settings within the Sonicwall NSV administration portal
select Authentication from the tabs and select RADIUS from the drop-down list to define the required configuration.



User Authentication Settings

User authentication method: RADIUS

Single-sign-on method(s): SSO Agent, Terminal Services Agent, RADIUS Accounting, 3rd-Party API, Browser NTLM Authentication

☑ Case-sensitive user names
☐ Enforce login uniqueness
☐ Force relogin after password change
☐ Display user login info since last login

One-Time Password:

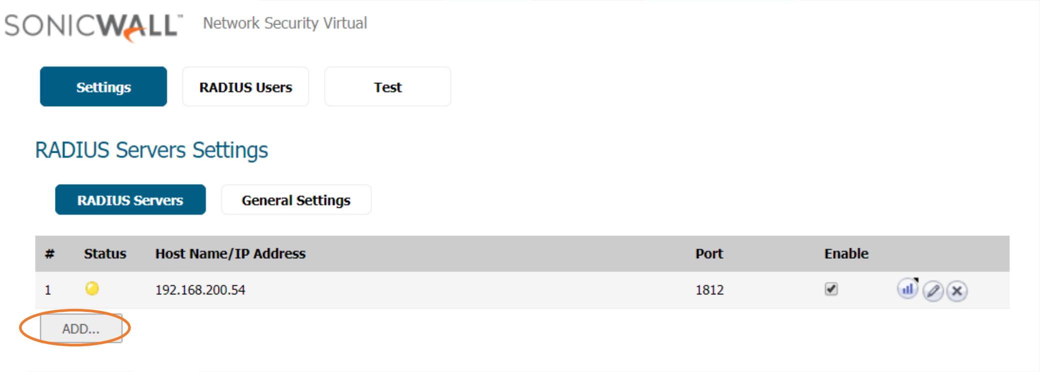
☐ Enforce password complexity for One-Time Password

One-time password E-mail format: ● Plain Text ○ HTML

One Time Password Format: Characters

One Time Password Length: 10 - 10 characters Password Strength: Good

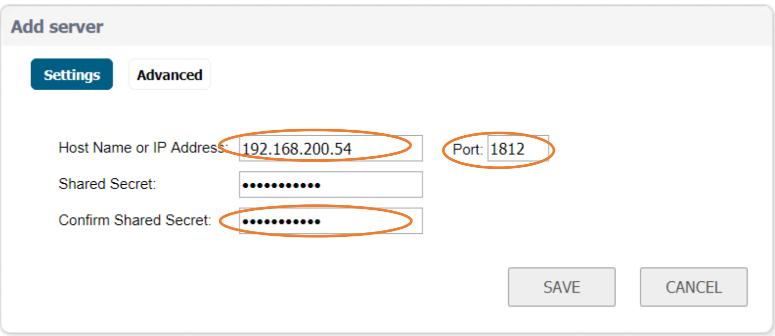
Select Configure RADIUS from the configuration, which will present a new web window as follows.



RADIUS Servers Settings

#	Status	Host Name/IP Address	Port	Enable
1	●	192.168.200.54	1812	☑

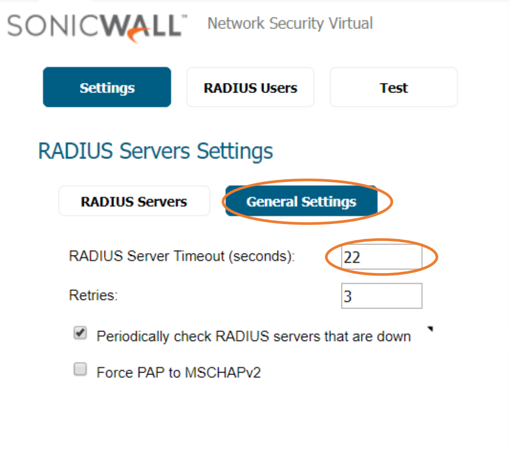
Click ADD to define a new RADIUS server



Host Name or IP Address: 192.168.200.54 Port: 1812
Shared Secret: ●●●●●●●●●●●
Confirm Shared Secret: ●●●●●●●●●●●

Once presented with the Add Server dialogue box, enter the IP address of the SecurAccess server and the shared Secret key defined earlier in the guide.
Please make sure the Port is defined as 1812 or identical to the RADIUS port configured previously.

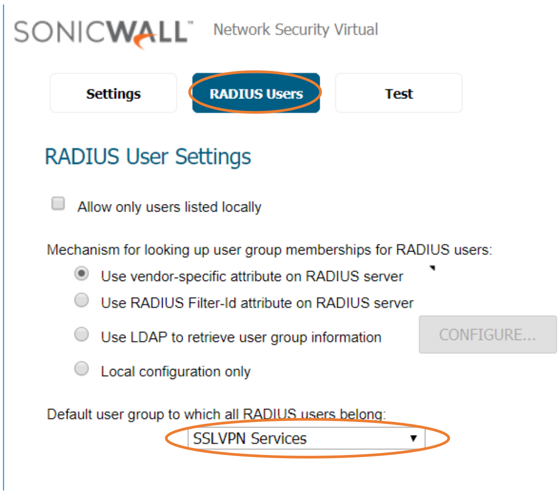
Click SAVE to continue



RADIUS Server Timeout (seconds): 22
Retries: 3
☑ Periodically check RADIUS servers that are down
□ Force PAP to MSCHAPv2

We will now need to increase the RADIUS timeout by selecting the General Settings tab and increasing the timeout to 22 seconds (increase of 3 seconds above SecurEnvoy's default 19 Second timeout)

To finalise the RADIUS configuration, we will allocate the RADIUS server to the SSL VPN profile. Select RADIUS Users from the tabs and make sure the Default user group selected is SSL VPN Services



RADIUS User Settings

☐ Allow only users listed locally

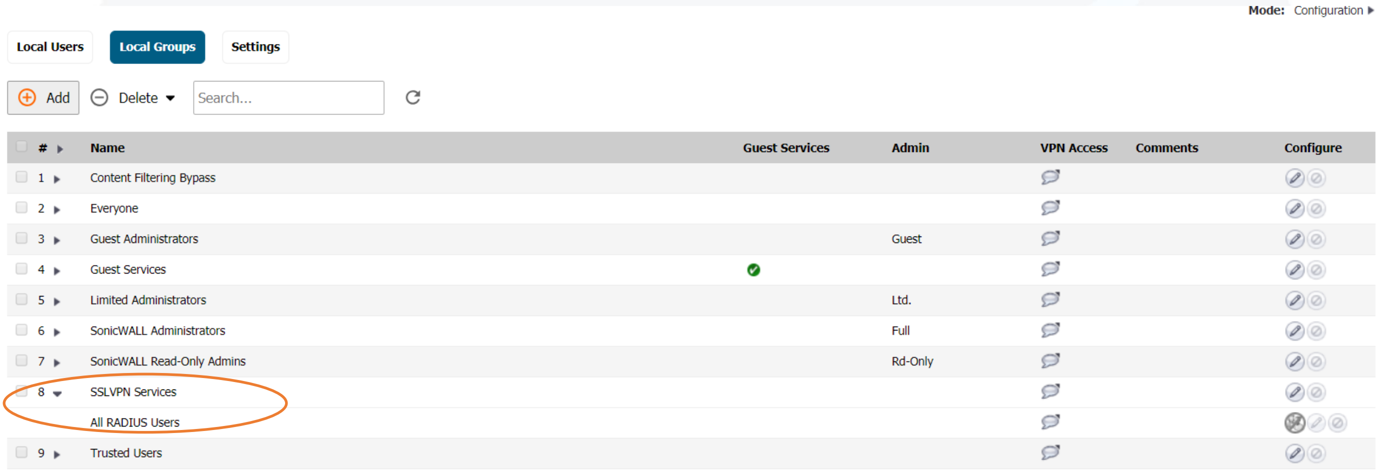
Mechanism for looking up user group memberships for RADIUS users:

- ● Use vendor-specific attribute on RADIUS server
- ○ Use RADIUS Filter-Id attribute on RADIUS server
- ○ Use LDAP to retrieve user group information CONFIGURE...
- ○ Local configuration only

Default user group to which all RADIUS users belong: SSLVPN Services ▾

Click Apply, then OK to return to the authentication Tab.

Click Accept to make sure the configuration is written to the device



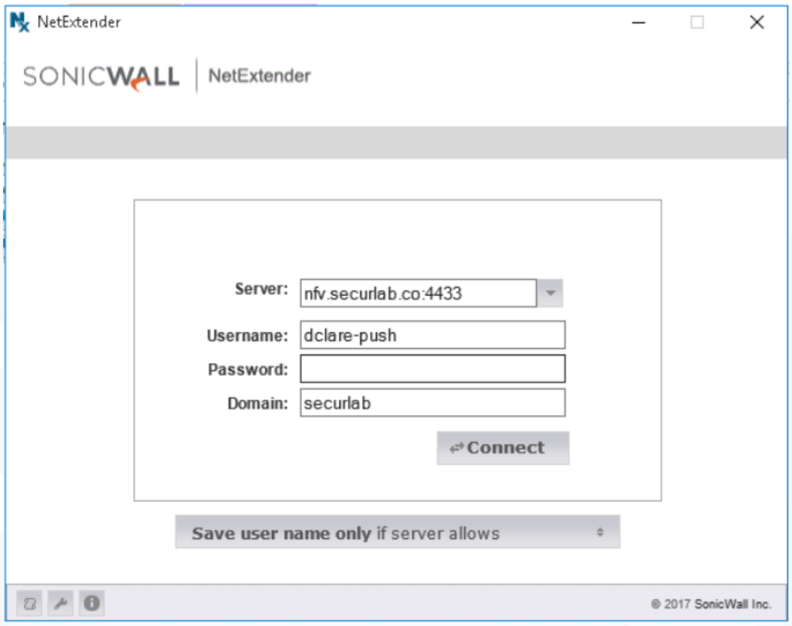
☐	#	Name	Guest Services	Admin	VPN Access	Comments	Configure
☐	1 ▸	Content Filtering Bypass					
☐	2 ▸	Everyone					
☐	3 ▸	Guest Administrators		Guest			
☐	4 ▸	Guest Services	✓				
☐	5 ▸	Limited Administrators		Ltd.			
☐	6 ▸	SonicWALL Administrators		Full			
☐	7 ▸	SonicWALL Read-Only Admins		Rd-Only			
☐	8 ▾	SSLVPN Services					
		All RADIUS Users					
☐	9 ▸	Trusted Users					

It is possible to check that the RADIUS configuration has been assigned to the SSL VPN Services by selecting the Local Groups TAB and expanding the SSL VPN Services section.

1.5 Client Logon

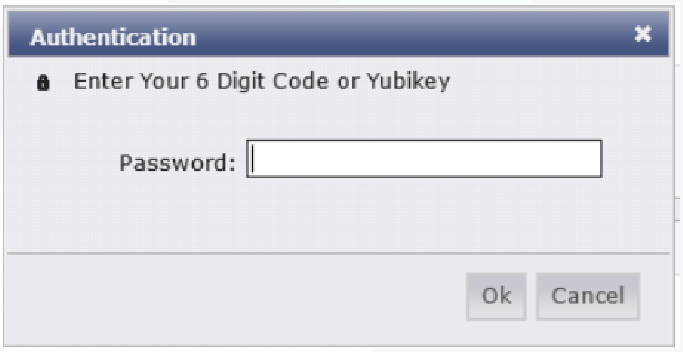
The following section describes the login process for the Sonicwall NSV NetExtender client and demonstrates what will be presented back to the user.

- Click on the NetExtender client and enter the server name or IP and port if not already completed from previous configuration (Local User or LDAP Config)
- Enter in your username from Active Directory or Local Directory Service account
- Enter your domain password and SSL domain and click Connect



Server: nfv.securlab.co:4433
Username: dclare-push
Password:
Domain: securlab
Save user name only if server allows

If not presented with a PUSH notification, when prompted, enter the 6-digit token or Yubikey token and click ok



Enter Your 6 Digit Code or Yubikey

Password:

Please Reach Out to Your Local SecurEnvoy Team...

UK & IRELAND

The Square, Basing View
Basingstoke, Hampshire
RG21 4EB, UK

Sales

E sales@SecurEnvoy.com
T 44 (0) 845 2600011

Technical Support

E support@SecurEnvoy.com
T 44 (0) 845 2600012

EUROPE

Freibadstraße 30,
81543 München,
Germany

General Information

E info@SecurEnvoy.com
T +49 89 70074522

ASIA-PAC

Level 40 100 Miller Street
North Sydney
NSW 2060

Sales

E info@SecurEnvoy.com
T +612 9911 7778

USA - West Coast

Mission Valley Business Center
8880 Rio San Diego Drive
8th Floor San Diego CA 92108

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA - Mid West

3333 Warrenville Rd
Suite #200
Lisle, IL 60532

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA – East Coast

373 Park Ave South
New York,
NY 10016

General Information

E info@SecurEnvoy.com
T (866)777-6211

SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

SecurEnvoy HQ, Octagon Point, 5 Cheapside, St Paul's, London, EC2V 6AA E: info@SecurEnvoy.com T: 44 (0) 845 2600010
Company No. 04866711 VAT Number GB 862076128