SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

Sonicwall (SMA) Secure Mobile Access Guide

SecurAccess Integration Guide

Version 1.1 – 06/22

Contents

1.1 SOLUTION SUMMARY 3

1.2 GUIDE USAGE 3

1.3 PREREQUISITES 3

1.4 AUTHENTICATION 4

1.41 SETUP RADIUS - SECURACCESS 4
1.41 SETUP RADIUS – SONICWALL 5
1.41 ASSIGN AUTHENTICATION SERVERS TO REALMS 6

1.5 CLIENT LOGON 7

1.51 CLIENTLESS SSL LOGIN 7
1.52 VPN CLIENT LOGIN 7

1.1 Solution Summary

SecurEnvoy's SecurAccess MFA solution integrates with Sonicwall's Secure Mobile Access appliance through the use of RADIUS Server for authorisation and access control.

The software used for the integration process is listed below:

Sonicwall SMA Release 12.4
SecurEnvoy SecurAccess Release v9.4.x

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 2012-r2 or higher.
  - An LDAP or Lightweight Directory Service database of users

  Note: Please see SecurEnvoy's SecurAccess version 9.4.x deployment guide on how to setup MFA server solution (*On the www,securenvoy.com website****)***
- A Sonicwall SMA virtual or physical appliance running version 12.4 and above.
- Sonicwall Connect client software installed/deployed on all clients that connect remotely to the appliance unless the Clientless solution will be used.
- This guide assumes that Sonicwall has been installed and previously configured to authenticate users with a username and password already.
- Familiarity with the following technologies:
  - RADIUS configuration
  - Sonicwall Administration Interface

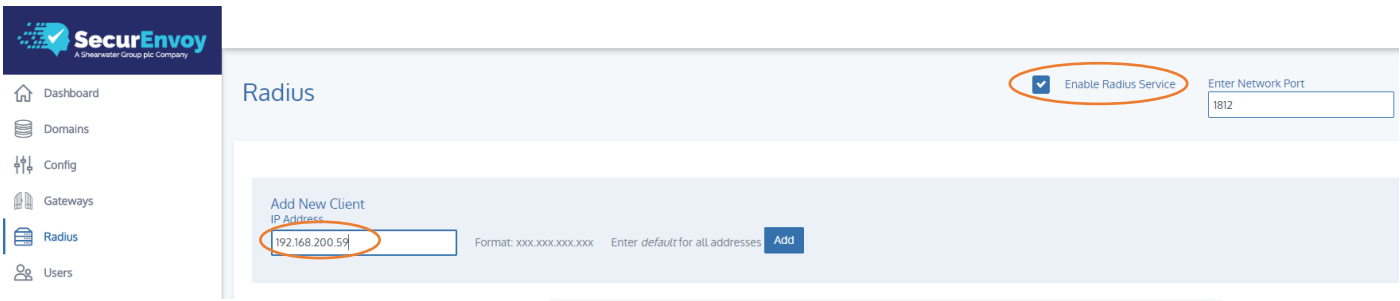
1.4 Authentication

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

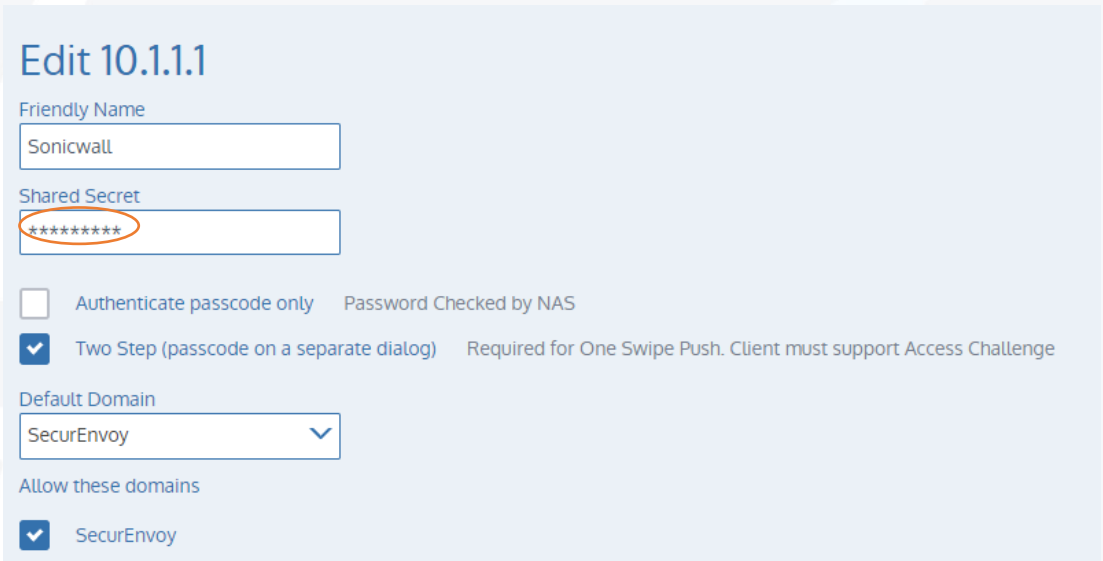
1.41 Setup RADIUS - SecurAccess

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"**



- 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**



1.41 Setup RADIUS – Sonicwall

Navigate to **System Configuration\Authentication Servers** within the Sonicwall administration portal.

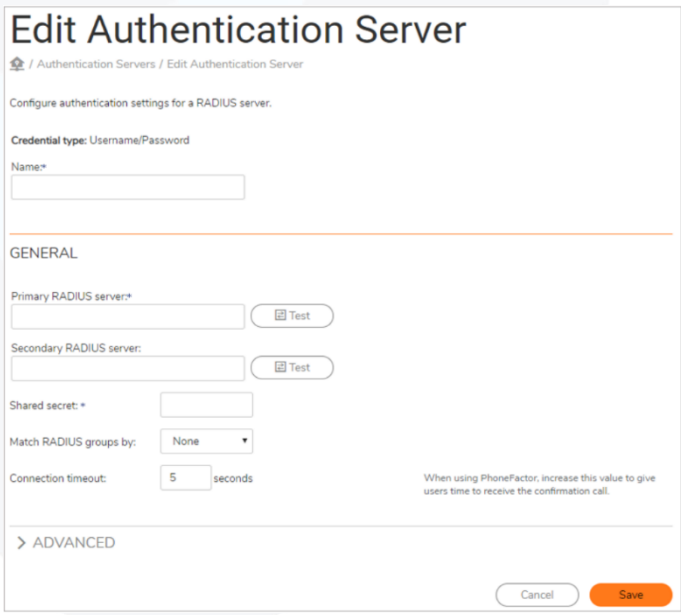
To configure RADIUS for user authentication:

1) Navigate to System Configuration > Authentication Servers.
2) Click New.
3) Under Authentication directory, click RADIUS.
4) Under Credential type, click Username/Password
5) Under the General section:
6) Radius Settings:
   - Name field: Type the name of the Securenvoy authenticating server.
   - Primary Radius server field: Enter the Primary Securenvoy server IP Address.
   - Secondary Radius server field: Enter the secondary Securenvoy server IP Address.
   - Shared secret: Enter matching Shared Secret.
   - Match Radius group by;
     - In the Match RADIUS groups by list, select the attribute containing the groups of which the user is a member. The value returned from RADIUS will be used in the group portion of the appliance access rule. There are three possible values:

RADIUS groups by	Description
None	Ignores the group attribute
Filterid attribute (11)	Matches against the FilterID attribute
Class attribute (25)	Matches against the Class attribute

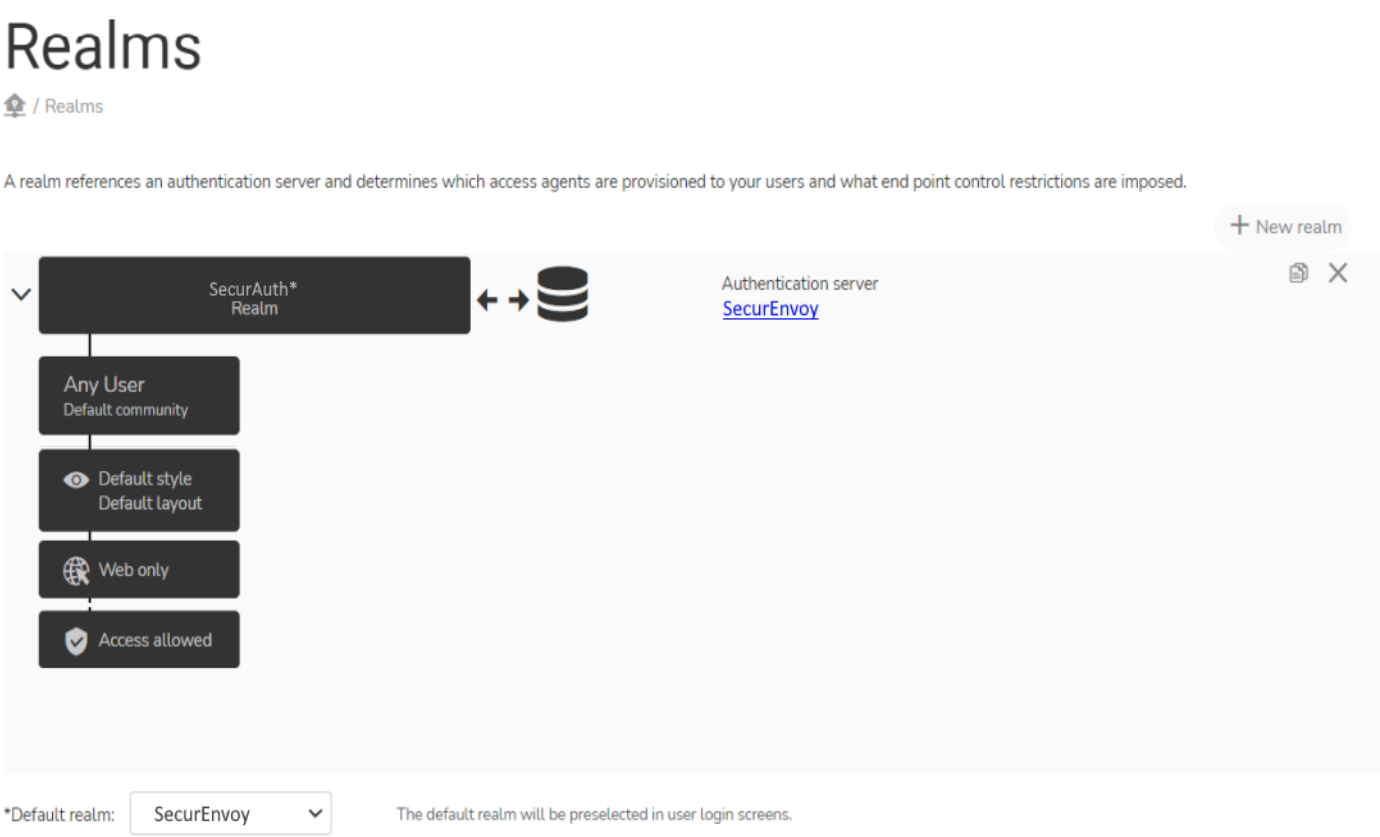
   - Connection timeout: 20 – 30 seconds

7) In the Primary RADIUS server field, type the host name or IP address of your primary RADIUS server. If your RADIUS server is listening on a port other than 1645 (the (the well-known port for RADIUS), you can specify a port number as a colon-delimited suffix (:<port number>).

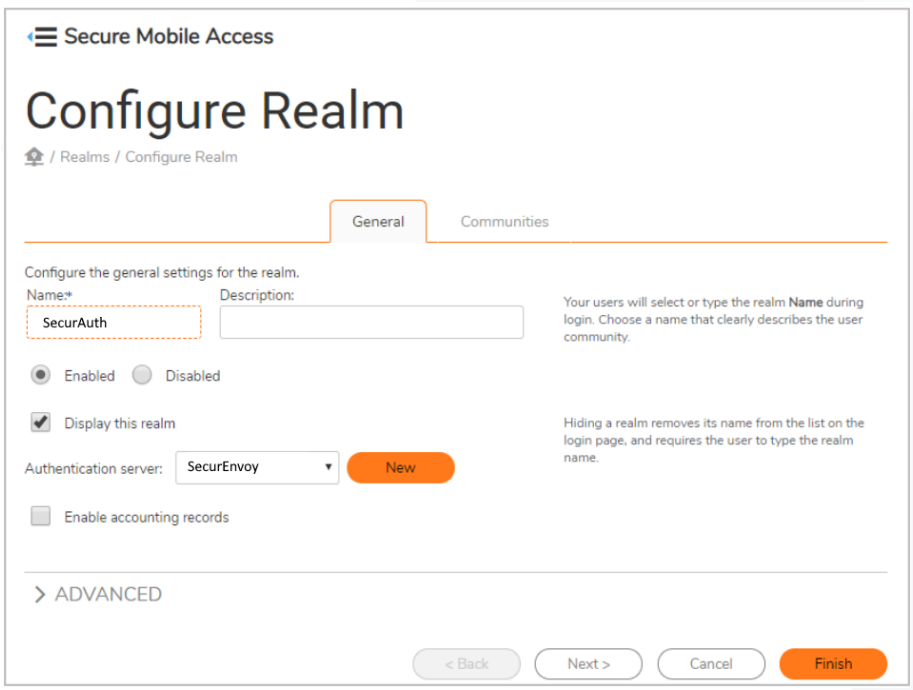


1.41 Assign Authentication Servers to Realms

Navigate to **User Access\Realms** and select your existing Realm which is likely to have local or AD authentication set.

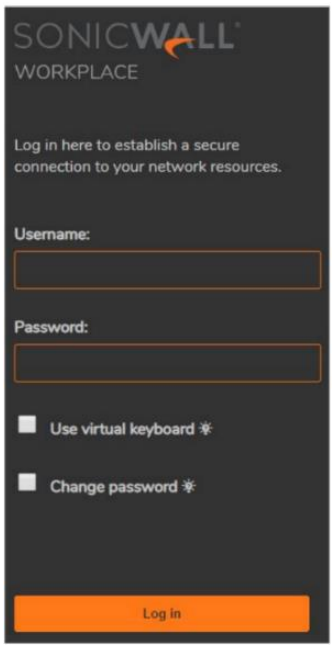


Within the Realm, select the Radius Authentication Servers configured in the previous section, from the drop-down list and click **Save**



1.5 Client Logon

1.51 Clientless SSL Login



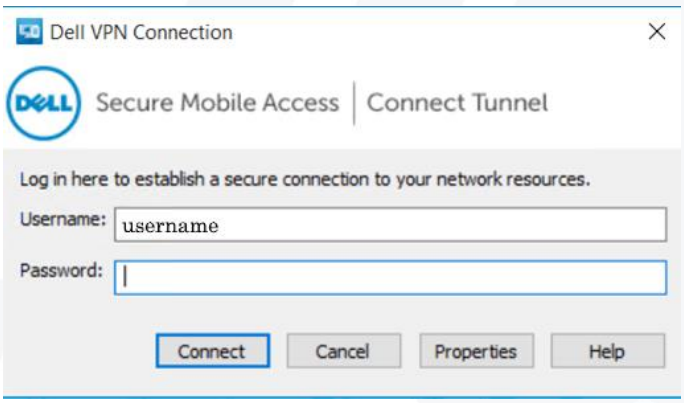
The following section describes the login process and demonstrates what will be presented back to the user.

- Browse to your Sonicwall SMA Workspace Login Screen
- Enter in your username from Active Directory or Local Directory Service account
- Enter your domain password and click **Login In**

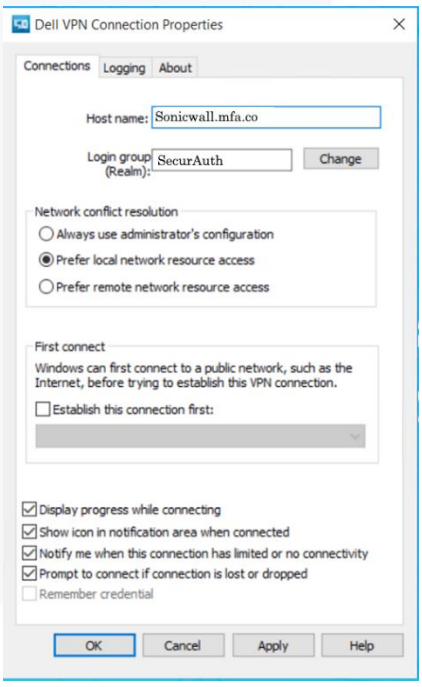
When prompted, enter the 6-digit passcode and click **ok**

1.52 VPN Client Login

Load the Secure Mobile Access client and select **Properties**

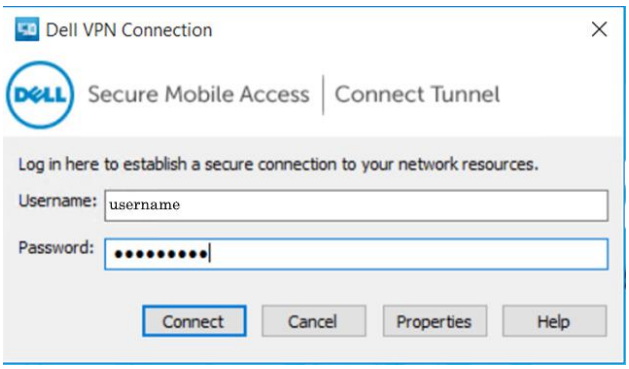


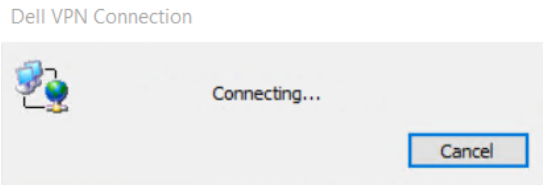
On presentation of the properties of the client, make sure that the **hostname** or **IP address** of the External interface of the Sonicwall SMA is set, along with the **Login Group Realm** (Configured under the authentication section.
Click **Apply** and close the dialogue.



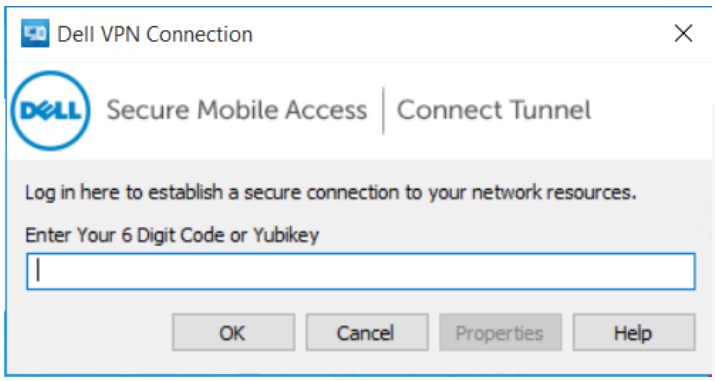
The following section describes the login process and demonstrates what will be presented back to the user.

- Enter in your username from Active Directory or Local Directory Service account
- Enter your domain password and click **Connect**





When prompted, enter the 6-digit token or yubikey token and click **ok**



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