# External authentication with Barracuda SSL VPN Authenticating Users Using SecurAccess Server by SecurEnvoy


| Contact information | | |
|---|---|---|
| SecurEnvoy | www.securenvoy.com | 0845 2600010 |
| | 1210 Parkview<br>Arlington Business Park<br>Theale<br>Reading<br>RG7 4TY | |
| Phil Underwood | Punderwood@securenvoy.com | |

**Barracuda SSl VPN (Radius) Integration Guide**

This document describes how to integrate a Barracuda SSL VPN appliance with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

The Barracuda SSL VPN appliance provides - Secure Remote Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Barracuda SSL VPN appliance), without the complication of deploying hardware tokens or smartcards.

Two-Factor authentication is provided by the use of your PIN and your Phone to receive the onetime passcode. This can be either via SMS, email or using a SecurEnvoy Soft Token installed upon the phone.

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into Microsoft's Active Directory and negates the need for additional User Security databases. SecurAccess consists of two core elements: a Radius Server and Authentication server. The Authentication server is directly integrated with LDAP or Active Directory in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing Microsoft password. Utilising the Windows password as the PIN, allows the User to enter their UserID, Windows password and One Time Passcode received upon their mobile phone. This authentication request is passed via the Radius protocol to the SecurEnvoy Radius server where it carries out a Two-Factor authentication. SecurEnvoy utilises a web GUI for configuration. All notes within this integration guide refer to this type of approach.

**The equipment used for the integration process is listed below:**

**Barracuda**
Barracuda SSL VPN appliance

**SecurEnvoy**
Windows 2008 server R2 64bit
IIS installed with SSL certificate (required for remote administration)
Active Directory installed or connection to Active Directory via LDAP protocol.

SecurAccess software release v5.4.503

**Index**



## 1.0 Pre Requisites

*It is assumed that the* Barracuda SSL VPN appliance *is setup and operational. An existing Domain user can authenticate using a Domain password and access applications, your users can access through SSL VPN using Domain accounts.*

*Securenvoy Security Server has a suitable account created that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and the Barracuda SSL VPN appliance, additional open ports will be required.*
***NOTE:*** *SecurEnvoy requires LDAP connectivity either over port 389 or 636 to the Active Directory servers and port 1645 or 1812 for RADIUS communication from the Barracuda SSL VPN appliance®.*

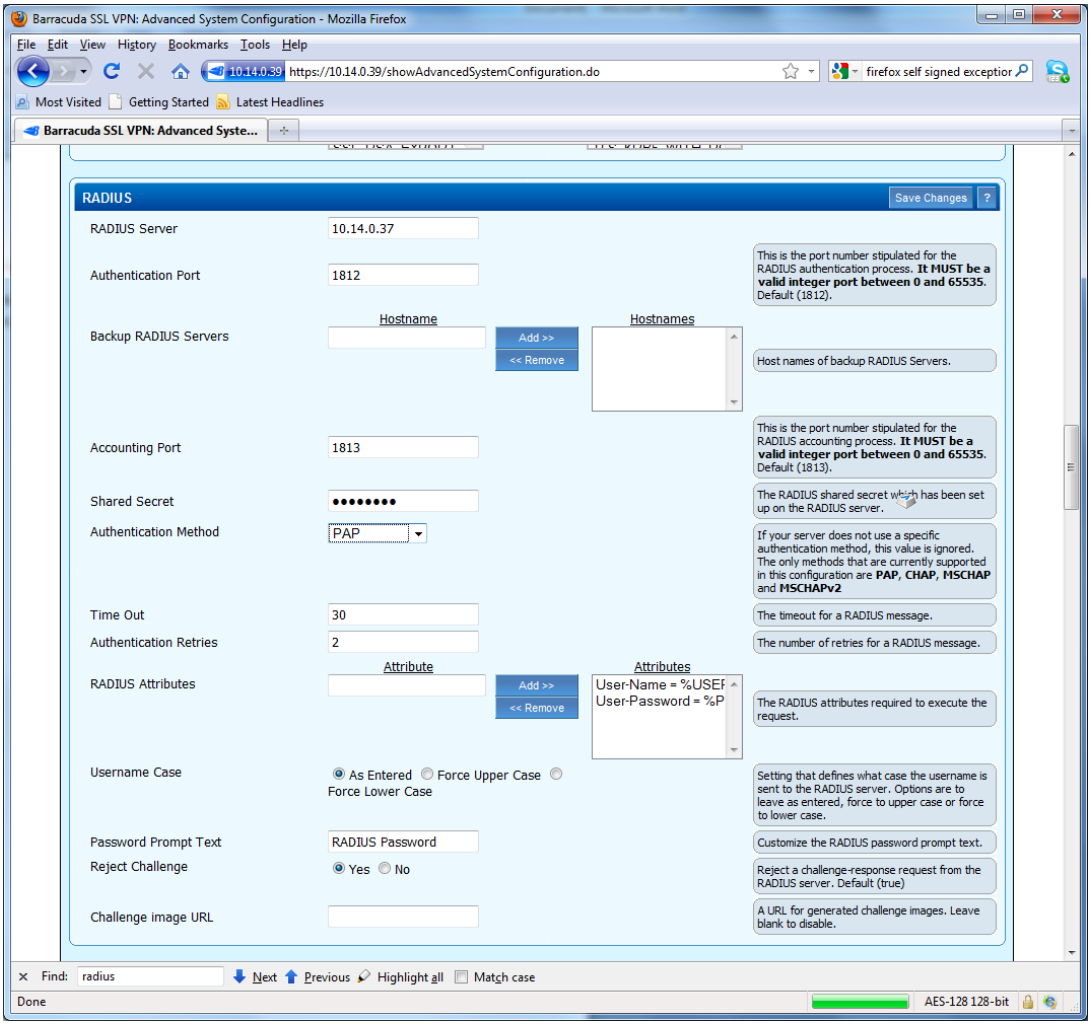
***NOTE:*** *Add radius profiles for each Barracuda SSL VPN appliance® that requires Two-Factor Authentication.*

## 2.0 Configuration of Barracuda SSL VPN

Configuring Barracuda SSL VPN to authenticate to SecurEnvoy RADIUS server
There are 3 steps involved, Configuring the RADIUS server settings, setting up a RADIUS authentication scheme, testing logon via RADIUS.

1. Log onto the SSL VPN and navigate to Advanced>Configuration.
2. In the RADIUS section, enter the correct values for the SecurEnvoy server.




Required settings:

RADIUS Server: the hostname or IP address of the SecurEnvoy server.

Authentication Port: normally 1812 unless this has been changed in the SecurEnvoy server.
Shared secret.

Authentication Method: PAP  Save these settings.

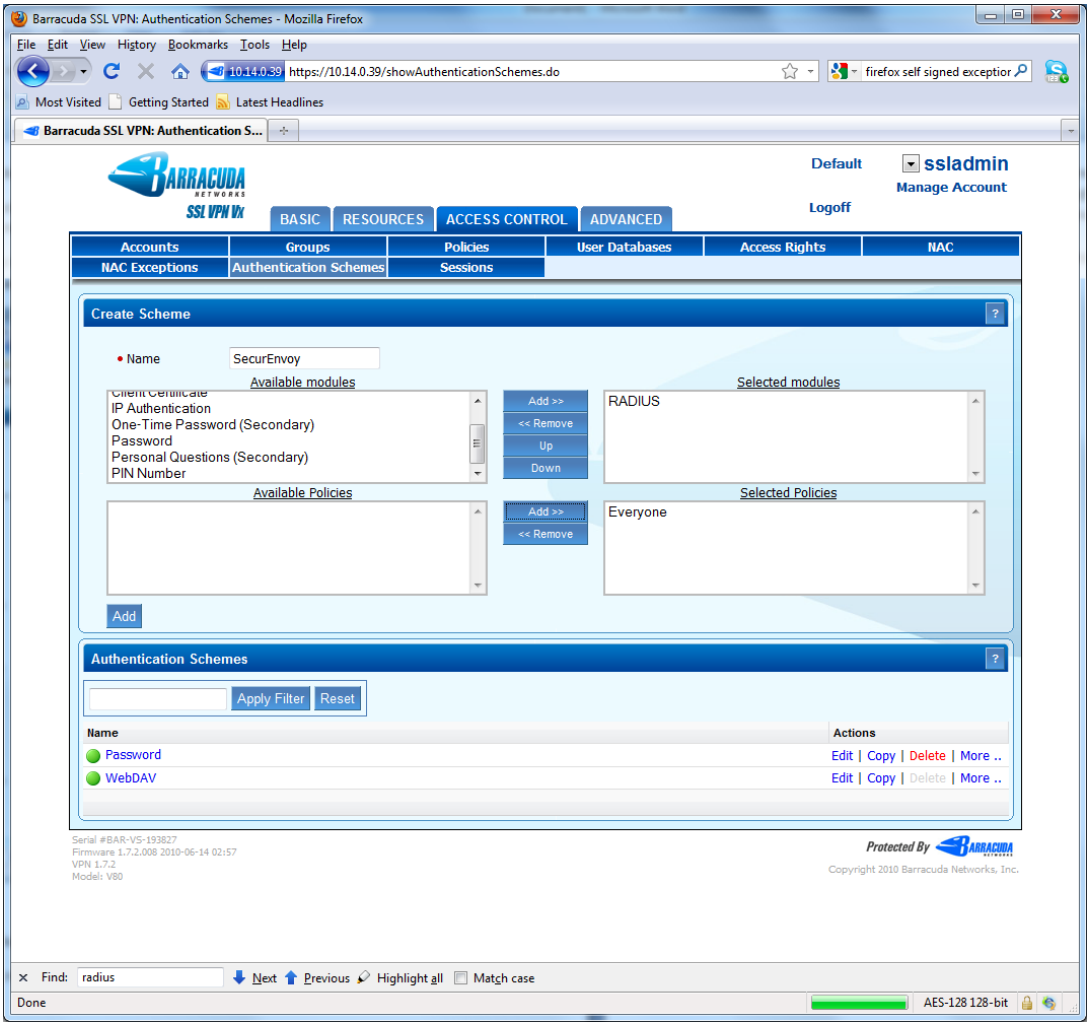
3. Navigate to Access Control>Authentication Schemes.

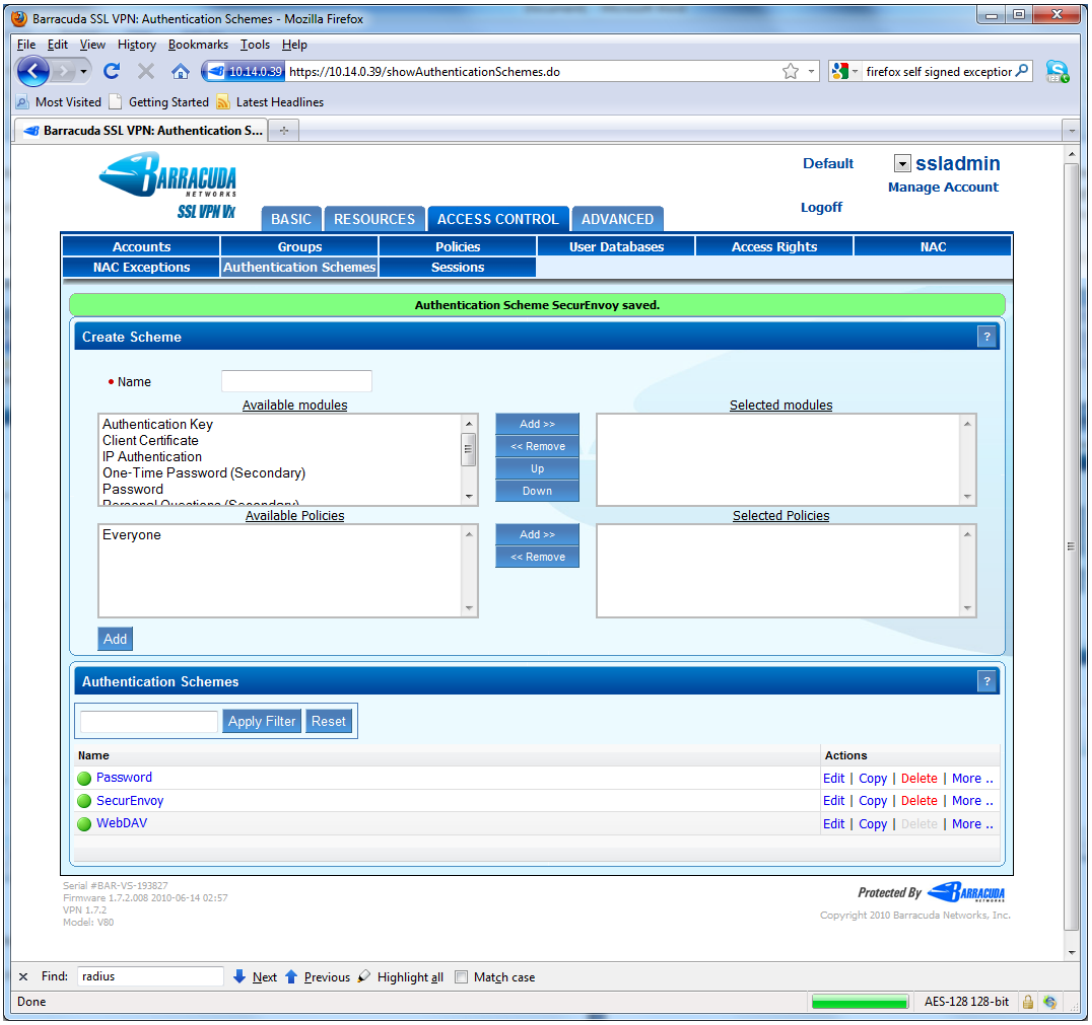
Create a new Authentication Scheme, give it a meaningful name (e.g RADIUS or SecurEnvoy).

Choose the RADIUS module as a minimum (you may also choose other modules if you require multi factor authentication).

Set which Policies in SSL VPN will have permission to log on using the RADIUS scheme.

Click Add

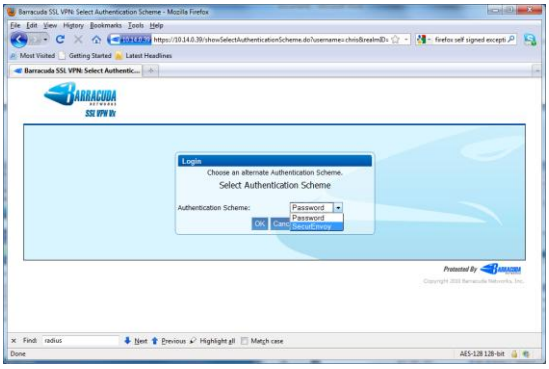




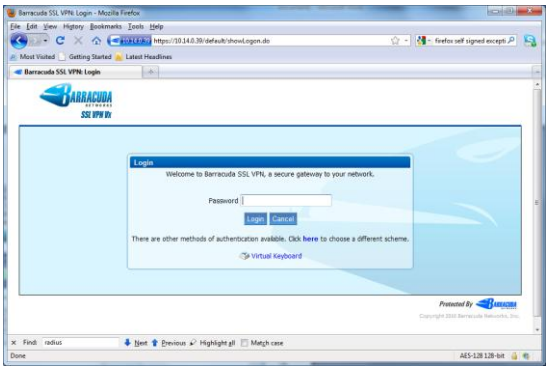

If you wish the RADIUS scheme to be the default option, increase its priority using More...>Increase Priority.

4. Test logon.
   On the SSL VPN login page, you enter your username and click Login

You will see 'There are other methods of authentication available'. Click on click here and then choose the RADIUS authentication scheme

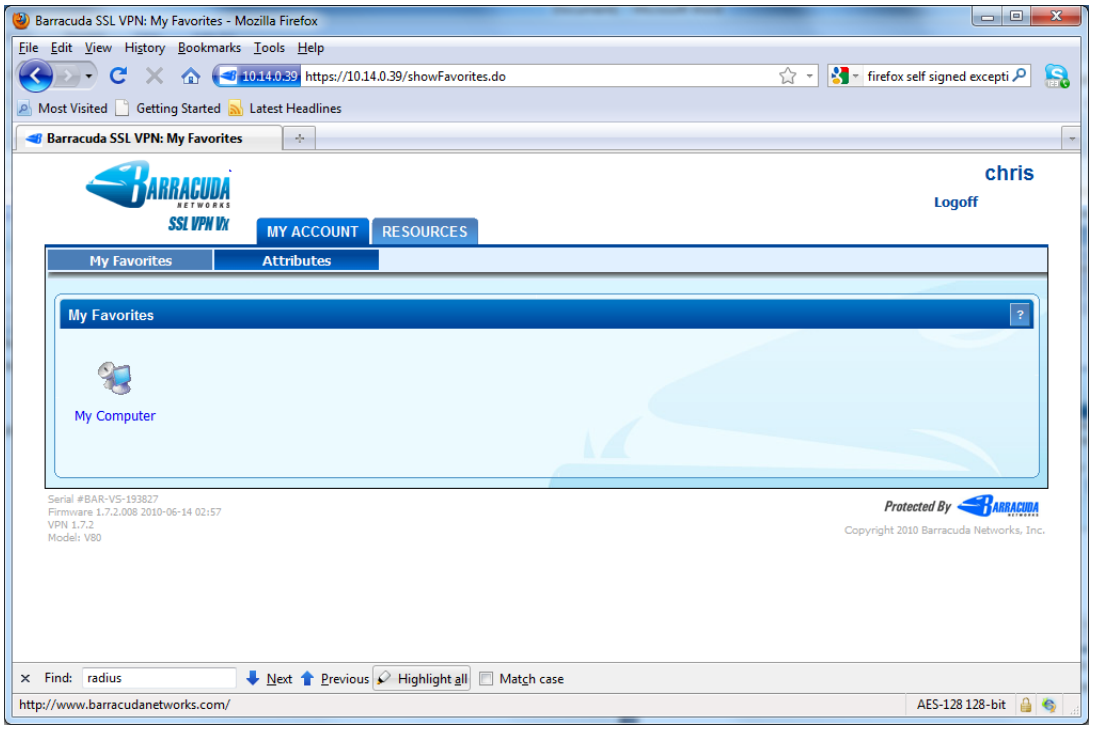


Click OK. (Note that you do not have to do this stage if you remove the default Password authentication from the Authentication Schemes page



Now enter your SecurEnvoy passphrase (normally your AD password combined with your 6 digit passphrase). Click Login.

You should now be logged onto your SSL VPN:



## 3.0 Configuration of Real time SMS passcodes

NOTE: If you wish to use the Real Time SMS delivery of passwords, then there is one extra setting required. Log on to SSL VPN as ssladmin and navigate to Advanced>Configuration. In the RADIUS section, set Reject Challenge to No:

This setting is set to Yes by default as some RADIUS servers do not seem to adhere very well to the RADIUS RFC for the challenge part of the protocol.

## 4.0 Configuration of SecurEnvoy

To help facilitate an easy to use environment, SecurEnvoy can be set up to only authenticate the passcode component as both authentication servers that are required to authenticate a remote user.

SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent to the user's mobile phone, via SMS, email or generated by the Soft Token.

Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

1. Click the **"Radius"** Button
2. Enter IP address and Shared secret for each Barracuda SSL VPN appliance that wishes to use **SecurEnvoy** Two-Factor authentication.


3. Press Update
4. Now Logout