

External Authentication with F5® APM Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	Merlin House Brunel Road Theale Reading RG7 4AB	
Phil Underwood	Punderwood@securenvoy.com	
Special thanks to Pranav Kumar of TSAvnet for F5 Integration	5 The Sterling Centre, Eastern Road, Bracknell, Berkshire, RG12 2PW	

1 Contents

1	Contents	2
2	F5® APM Integration Guide	3
3	Pre Requisites.....	4
4	Tokenless Authentication (All Types).....	4
4.1	Configuration of F5® APM	4
4.2	Configuration of SecurEnvoy	8
4.3	Test Logon (SSL VPN).....	9

2 F5® APM Integration Guide

This document describes how to integrate a F5® APM with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

F5® APM provides - Secure Application Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as F5® APM) 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 one time passcode, either by receiving a passcode via SMS, email or by using the Soft Token.

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into any LDAP directory server such as Microsoft's Active Directory and negates the need for additional User Security databases. SecurAccess 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 to the SecurEnvoy Security Server via the RADIUS protocol, where it carries out a Two-Factor authentication. It provides a seamless login into the corporate network environment by the remote User entering three pieces of information. SecurEnvoy utilises a web GUI for configuration, whereas the F5® APM Server environment uses a GUI application. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

F5® APM

Microsoft (for installation of SecurEnvoy Security Server)

Windows 2008 server

IIS installed with SSL certificate (required for management and remote administration)

Access to Active Directory with an Administrator Account

SecurEnvoy

SecurAccess software release v6.2.500

3 Pre Requisites

It is assumed that the F5® APM is setup and operational. It is also assumed that the 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 F5® APM, additional open ports will be required.

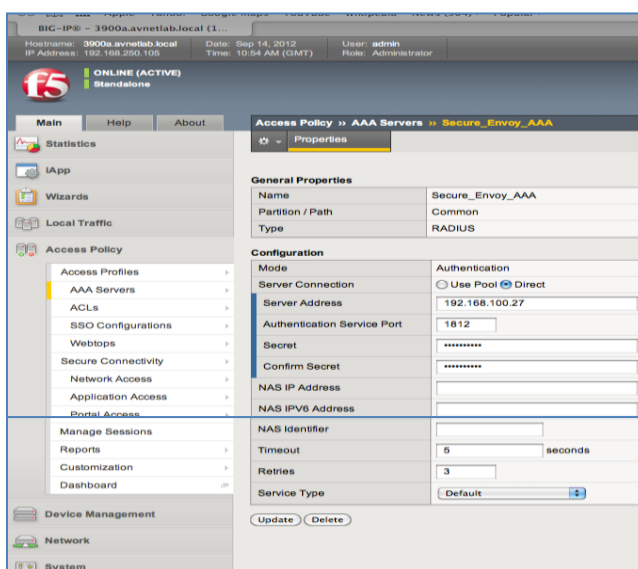
NOTE: SecurEnvoy requires LDAP connectivity either over port 389 or 636 to the Active Directory servers and port 1645 or 1812 for RADIUS communication from the F5® APM.

Only a single configuration is required, this will then support users with SMS sent via Pre-Load and Real Time as well as Soft Tokens, as F5® APM supports RADIUS (Challenge Response). Configuration in this guide refers to this type of approach.

4 Tokenless Authentication (All Types)

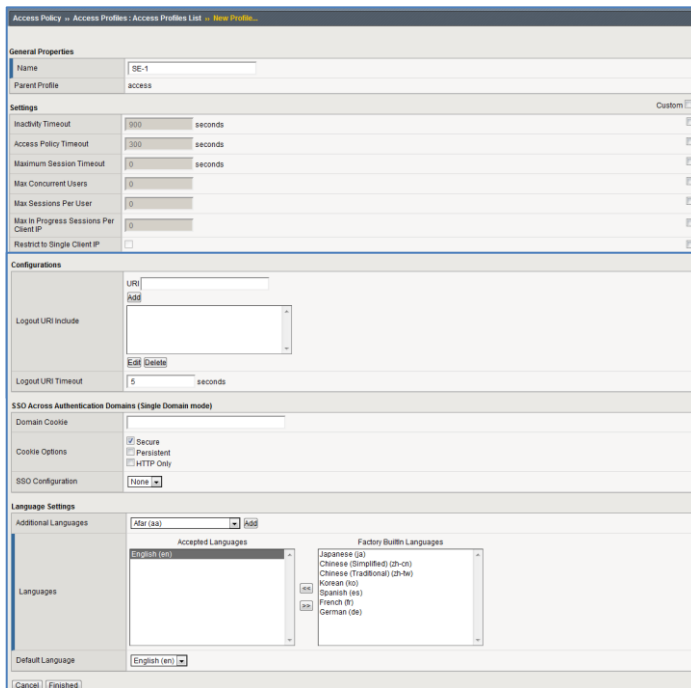
4.1 Configuration of F5® APM

1. Using a web browser log into the F5 APM
2. In Navigation pane, go to Access Policy – AAA servers – and select RADIUS
3. Enter details for the SecurEnvoy server (RADIUS)
 - a. Name
 - b. Set mode to authentication
 - c. Server connection set as Direct
 - d. Add SecurEnvoy server IP address
 - e. Set authentication port to 1812
 - f. Enter the shared secret (requires defining on SecurEnvoy server)
 - g. Set timeout to 10
 - h. Set retries to 1
 - i. Click Finish to complete

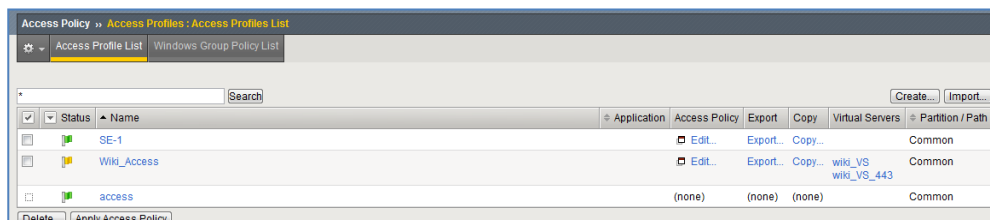


4. Now add the AAA server to an existing access-policy or in this example create a new profile.

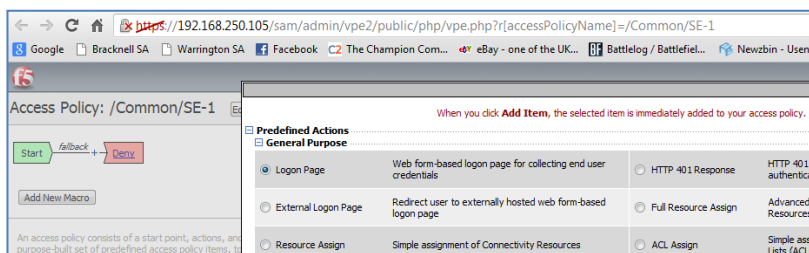
- a. Select new profile
- b. Assign a name
- c. Set Cookie options to Secure
- d. Assign Language to English
- e. Click finished to complete



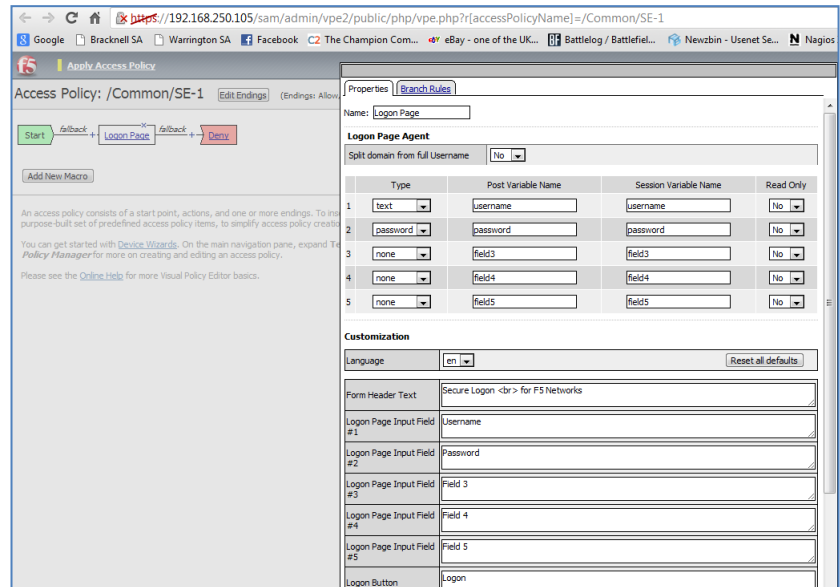
5. Navigate to the Access Profiles list, click the name of the profile you wish to add RADIUS authentication. In this example select the access policy named earlier (SE-1).



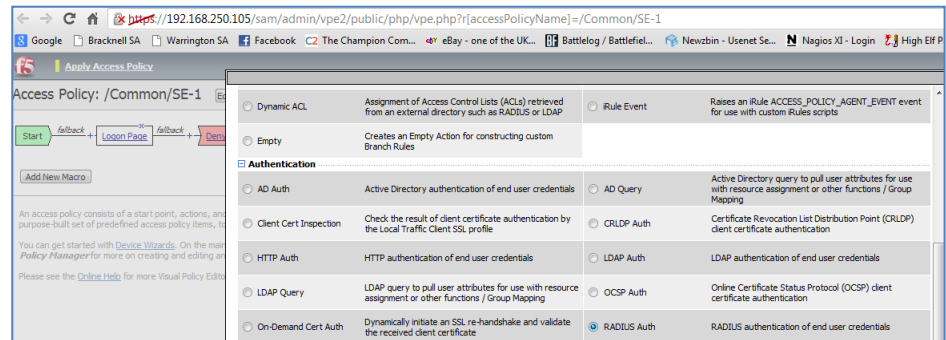
6. Click the edit access policy for SE-1
 a. Then select Add New Macro, the following screen is shown.



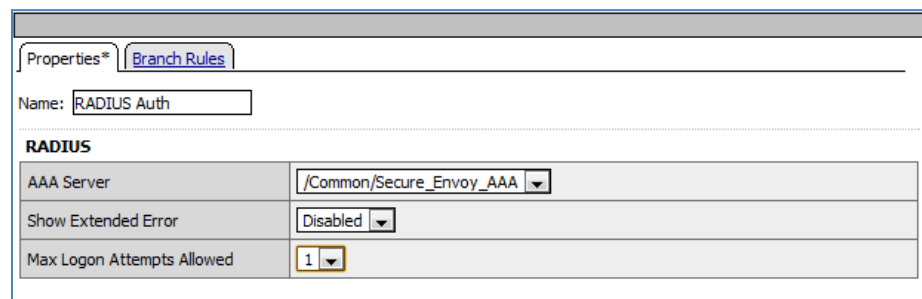
- b. Continue through the Macro, the following screen is shown for the Logon Page



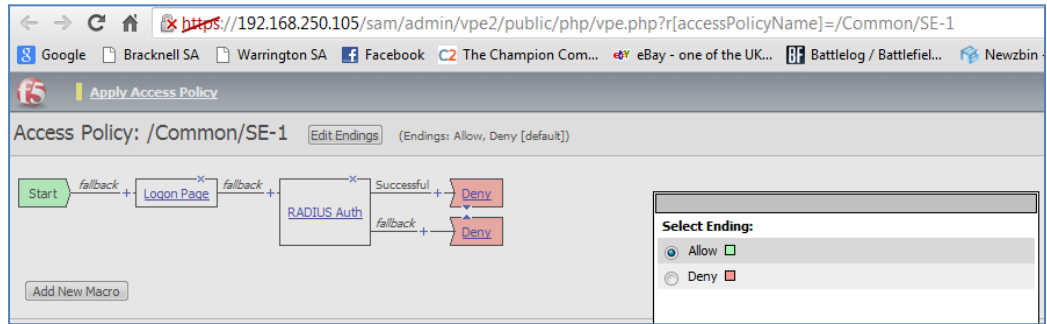
- b. Continue through the Macro, the following screen is for setting authentication, select RADIUS auth



- c. Continue through the Macro, the following screen is for selecting the RADIUS server



- d. Continue through the Macro, the following screen is to set the logic for authentication

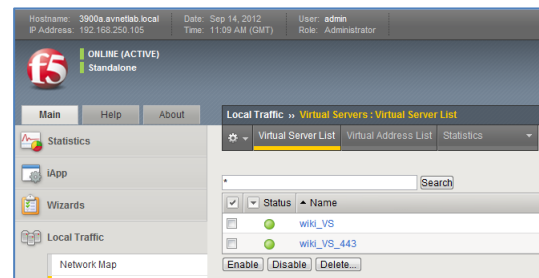


e. Once complete, the logic should look like the screenshot below

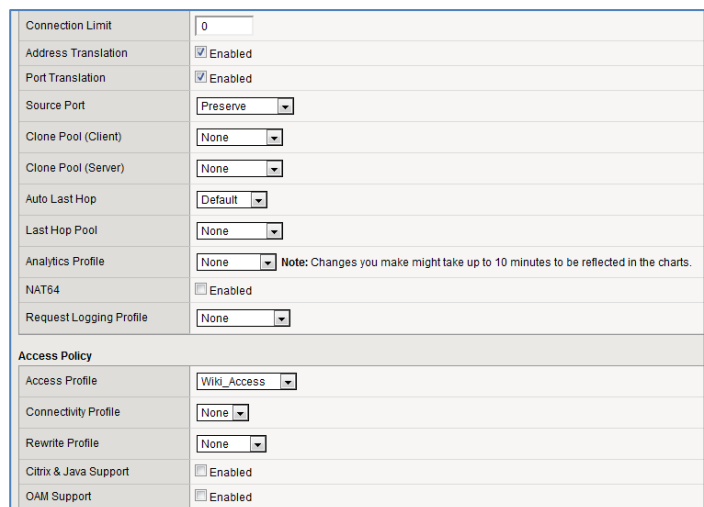


f. Navigate to Virtual servers (Create virtual server as per F5 guides)

g. Select the correct Virtual server



h. Apply access policy to virtual server



4.2 Configuration of SecurEnvoy

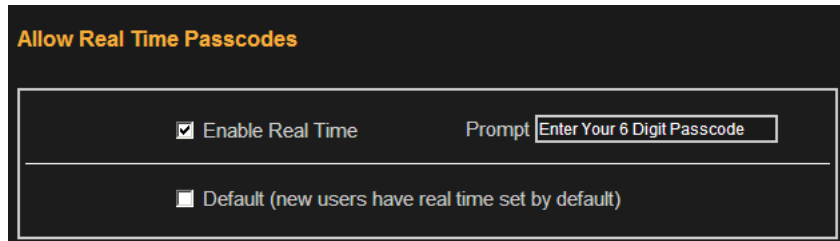
Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

To Support Pre-Load and Real-Time SMS as well as Soft Tokens the following configuration is required.

Go to Config-Real Time Passcodes

Enable the checkbox

Click Update to complete



Allow Real Time Passcodes

Enable Real Time Prompt

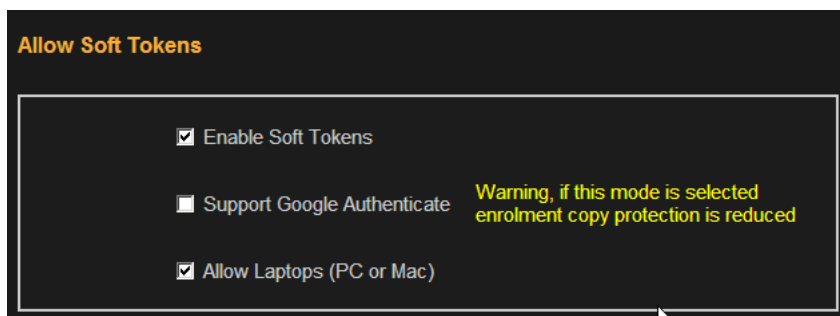
Default (new users have real time set by default)

Go to Config-Soft Tokens

Enable Soft Tokens

Enable PC Soft Tokens (If Required)

Click Update to complete



Allow Soft Tokens

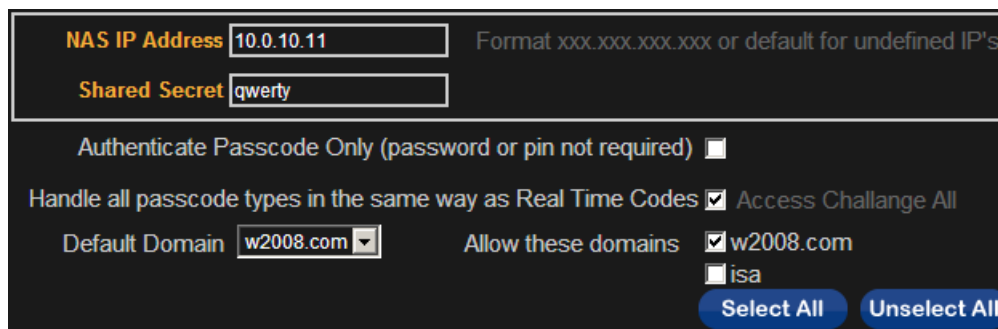
Enable Soft Tokens

Support Google Authenticate **Warning, if this mode is selected enrolment copy protection is reduced**

Allow Laptops (PC or Mac)

Click the **"Radius"** Button

Enter IP address and Shared secret for each F5® APM that wishes to use **SecurEnvoy** Two-Factor authentication.



NAS IP Address Format xxx.xxx.xxx.xxx or default for undefined IP's

Shared Secret

Authenticate Passcode Only (password or pin not required)

Handle all passcode types in the same way as Real Time Codes Access Challenge All

Default Domain Allow these domains w2008.com isa

Click checkbox "Handle all passcodes in the same way as Real Time"

Click **"Update"** to confirm settings.

Click **"Logout"** when finished. This will log out of the Administrative session.

4.3 Test Logon (SSL VPN)

Navigate to the relevant URL for the SSL VPN e.g. <https://remote.office.com>

User enters their Domain UserID and password,
Click "Logon"



f5

Secure Logon
for F5 Networks

Username

Password

Logon

User is then prompted for their 6 digit
Passcode.

Click "Logon" to complete the logon.



f5

Enter Your 6 Digit Passcode

Logon