Authentication with Microsoft UAG SSL VPN

Using SecurAccess Server from SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Andy Kemshall	akemshall@securenvoy.com	

The equipment used for the integration process is listed below

Microsoft UAG

Microsoft UAG SSL VPN

SecurEnvoy Server

Windows 2008 server
IIS installed with SSL certificate (required for management and remote administration)
Access to Active Directory with an Administrator Account

SecurEnvoy Software

SecurAccess software release v6.1.501

Overview

This integration guide shows how to obtain the best possible end user experience by utilising "chained authentication" which leverages IAG's single sign-on capabilities. This setup requires two authentication servers, one for authenticating the Microsoft password and the other for authenticating the SecurEnvoy 6 digit SMS passcode. Thus the first authentication server is something you know your Microsoft Password and the second one is something you own, your mobile phone which together represents two factor authentication.

1. Pre Requisites

Microsoft IAG is already setup to authenticate a Microsoft password
(In this example the authentication server is referred to as "Domain Controller")

2. Setting up SecurEnvoy

Install the SecurEnvoy server

Use the default setting of "Windows Password is the PIN"

Setup a user for one time authentication.

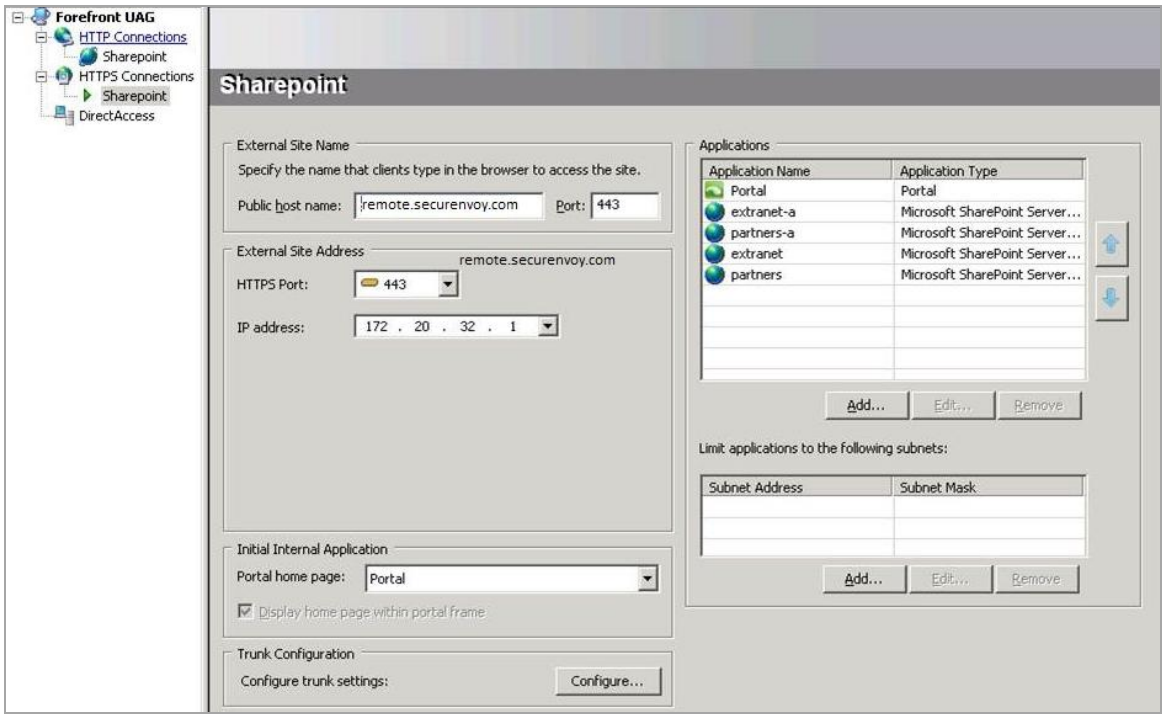
Select the "Radius" menu option and enter the UAG's IP Address, a shared secret (this can be any password you like) and select "Authenticate Passcode Only" option.



Click Update when complete.

3. Setting up SecurAccess in Microsoft UAG

Select an existing Trunk that you wish to authenticate, in this example "Sharepoint" under HTTPS connections.



Click "Configure trunk settings" under Trunk Configuration.

Select Authentication tab

Select Add and then select "Add" to add a new authentication server.

Select the Type as "**Radius**", enter the name "**SecurEnvoy**" and then enter the IP address of the SecurEnvoy server.

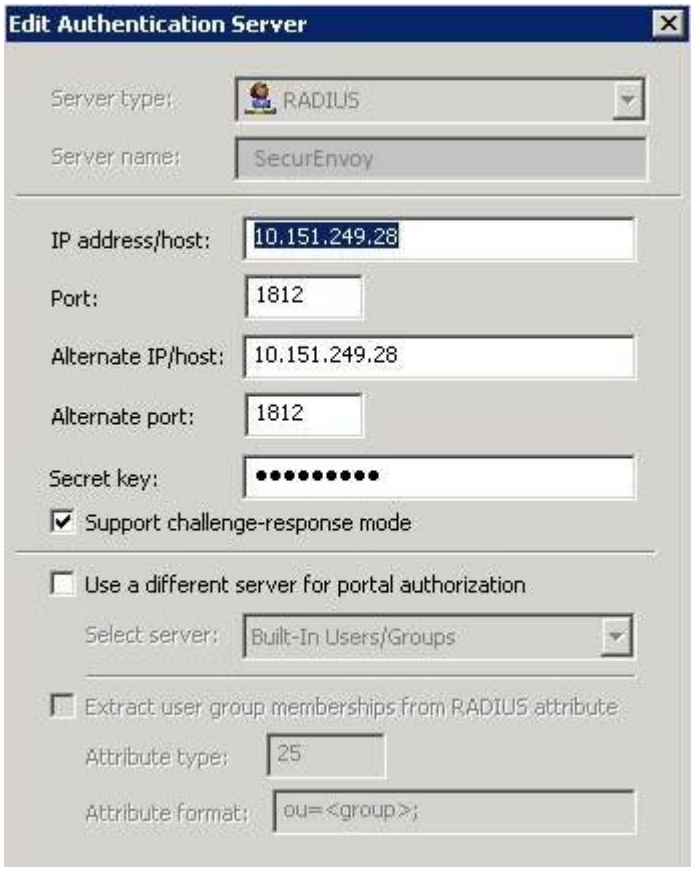
Set port to **1812**,

Enter the same shared secret as set in section 2.

If you have installed a second SecurEnvoy server then enter this as the alternate IP/Host and change the Alternate port to 1812.

If you require to use "Real time delivery" of passcodes enable the checkbox "Support challenge-response mode".

Select ok when complete.



Once complete highlight the SecurEnvoy Radius server and "click select".

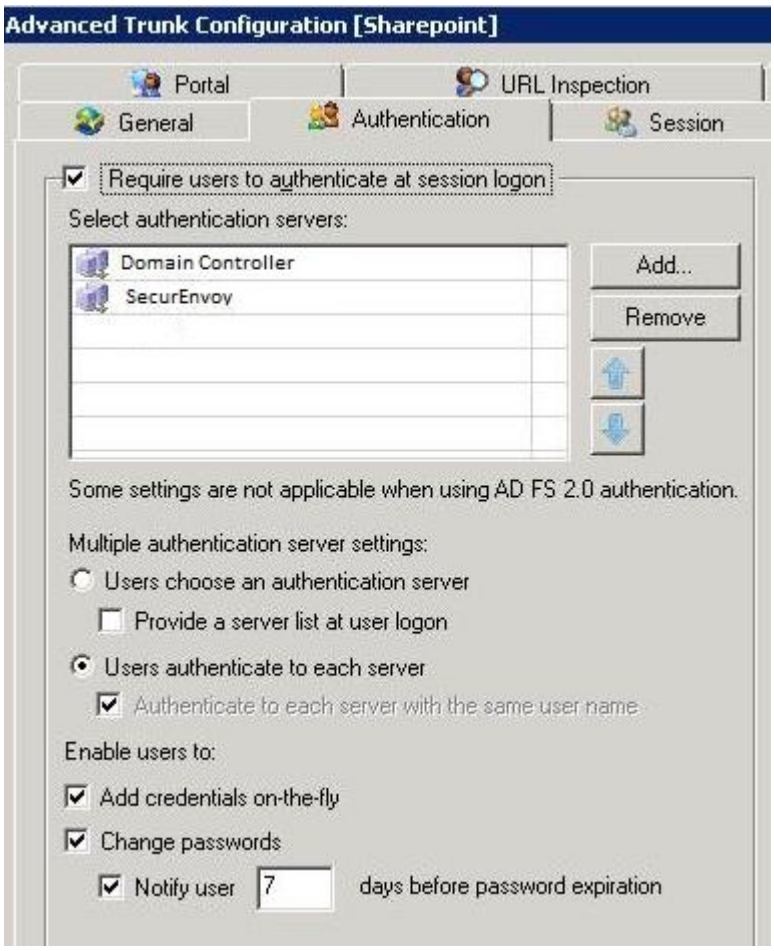
To enforce "Chained Authentication", Click the radial button "User must provide credentials for each selected server"

Also make sure the "Use the same username is checked.

Click "Ok" to submit changes

On the main console click activate configuration to submit changes.

If application single sign-on is required setup this up to use the Microsoft password authentication server (in this example it is referred to as Domain Controller).



4. Testing Authentication

Connect to the URL of the UAG's configured trunk

Enter a user name that has been configured for two factor authentication.

Enter the Microsoft Password in the xxx Password field.

Enter the 6 digit SMS passcode from the user's mobile phone into the "SecurEnvoy SMS Password" field.



You should be successfully authenticated and have the next required one time code sent to this users mobile phone.