

## Authentication with Microsoft IAG (Whale) SSL VPN

### Using SecurAccess Server from SecurEnvoy

Contact information		
SecurEnvoy	<a href="http://www.securenvoy.com">www.securenvoy.com</a>	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Andy Kemshall	<a href="mailto:akemshall@securenvoy.com">akemshall@securenvoy.com</a>	

The equipment used for the integration process is listed below

### **Microsoft IAG**

Microsoft IAG SSL VPN appliance  
Software Revision Version 3.7.0.0.14

### **SecurEnvoy Server**

Windows 2003 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 v4.1.501

### **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 called dev.com)

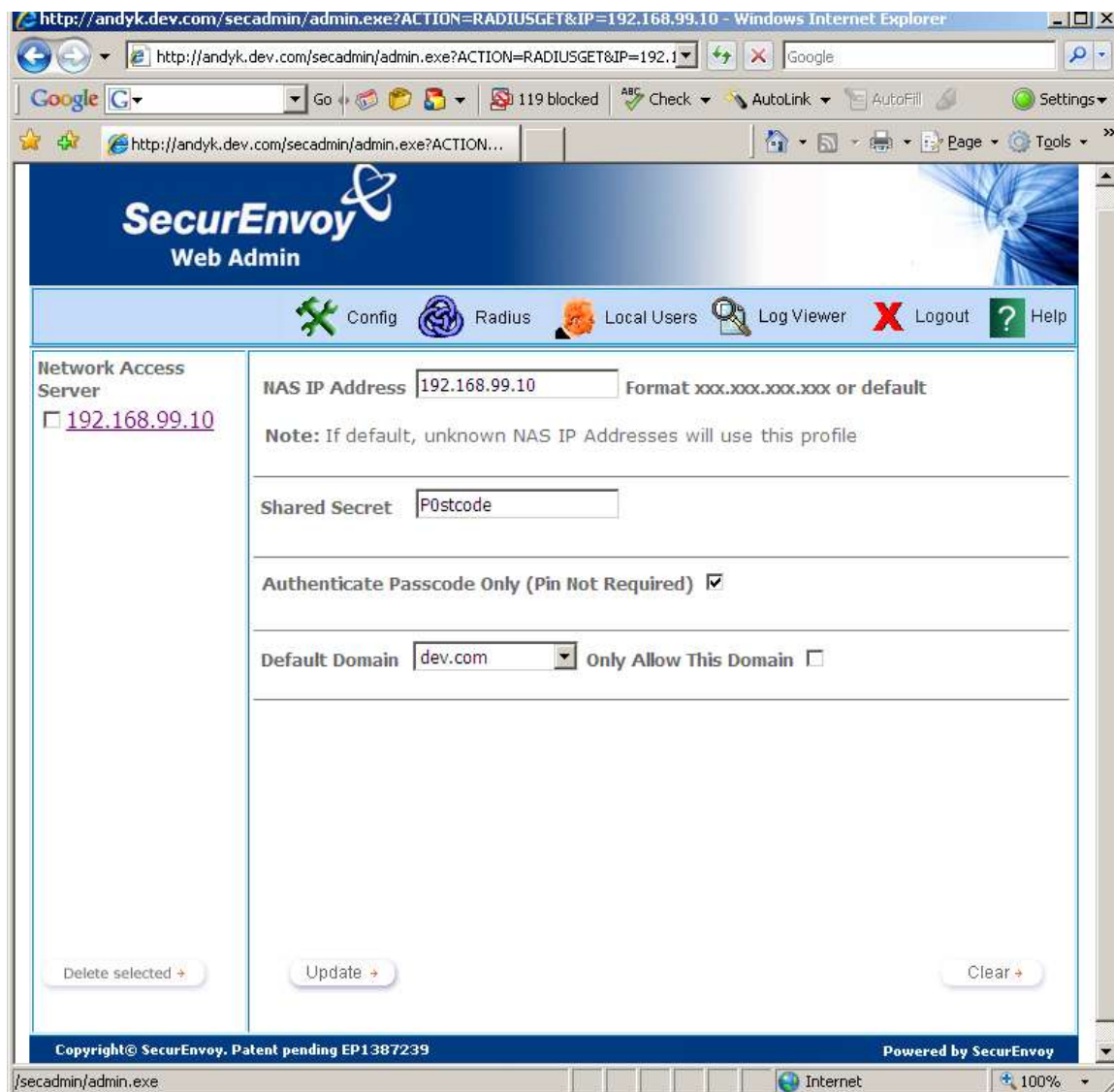
## 2. Setting up SecurEnvoy

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 IAG's IP Address, a shared secret (this can be any password you like) and select "Authenticate Passcode Only" option.



The screenshot shows the SecurEnvoy Web Admin interface in a Windows Internet Explorer browser. The page title is "SecurEnvoy Web Admin". The navigation menu includes "Config", "Radius", "Local Users", "Log Viewer", "Logout", and "Help". The "Radius" menu item is selected.

The main content area is titled "Network Access Server" and shows a list of servers. The server "192.168.99.10" is selected. The configuration details for this server are as follows:

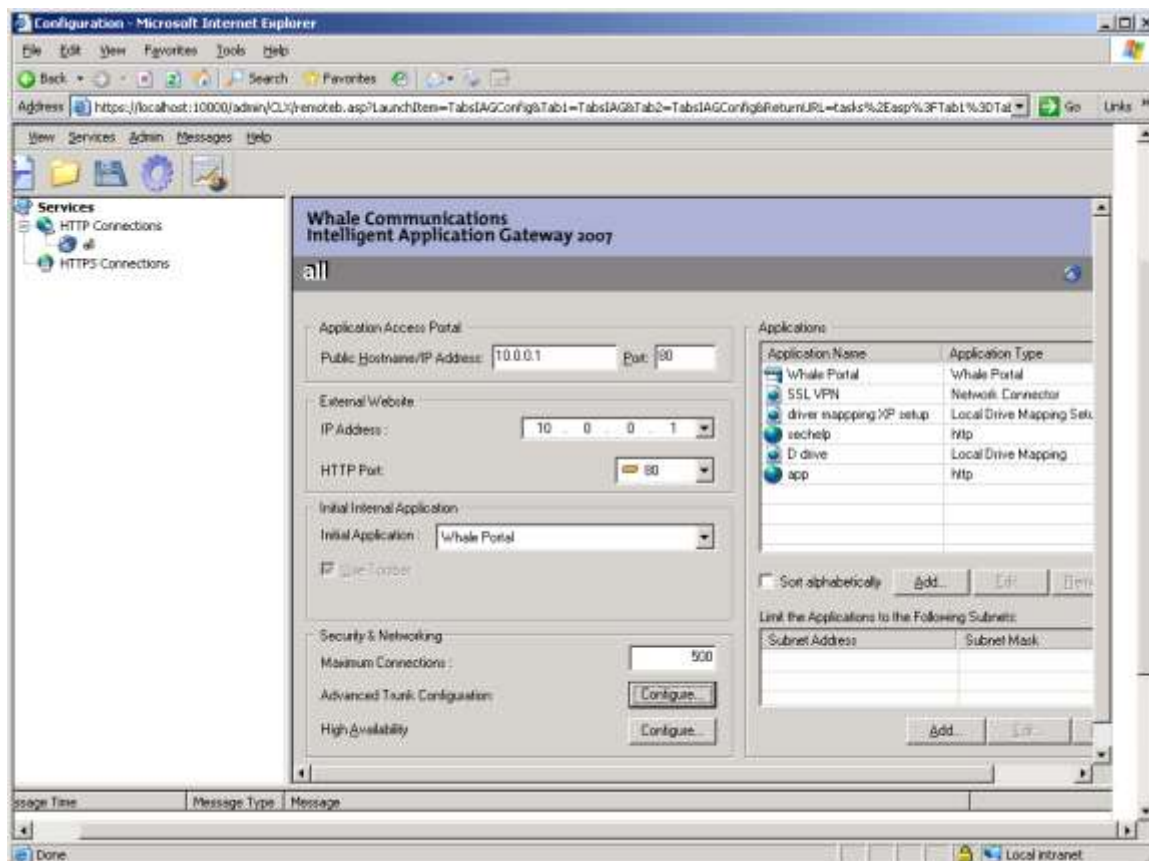
- NAS IP Address:** 192.168.99.10 (Format xxx.xxx.xxx.xxx or default)
- Note:** If default, unknown NAS IP Addresses will use this profile
- Shared Secret:** P0stcode
- Authenticate Passcode Only (Pin Not Required):**
- Default Domain:** dev.com (Only Allow This Domain: )

At the bottom of the configuration area, there are three buttons: "Delete selected +", "Update +", and "Clear +".

The footer of the page contains the text "Copyright© SecurEnvoy. Patent pending EP1387239" and "Powered by SecurEnvoy". The browser's status bar shows the path "/secadmin/admin.exe" and the zoom level "100%".

### 3. Setting up SecurAccess in Microsoft IAG

Select an existing Trunk that you wish to authenticate, in this example "All"



Click "Configure" under Advanced 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 SMS**” 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.

Select ok when complete.

Once complete highlight the SecurEnvoy Radius server and “click select”.

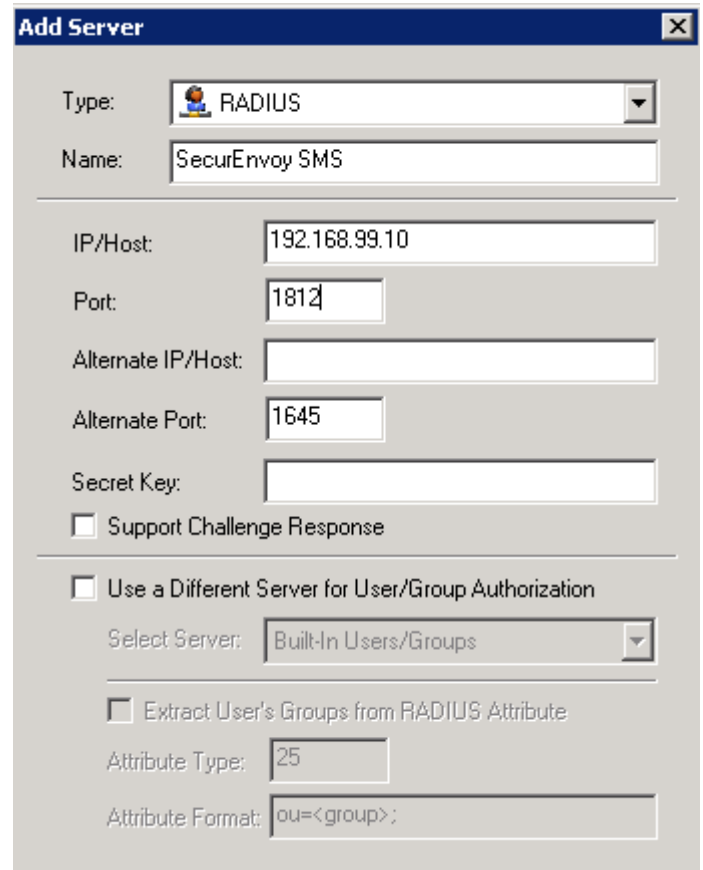
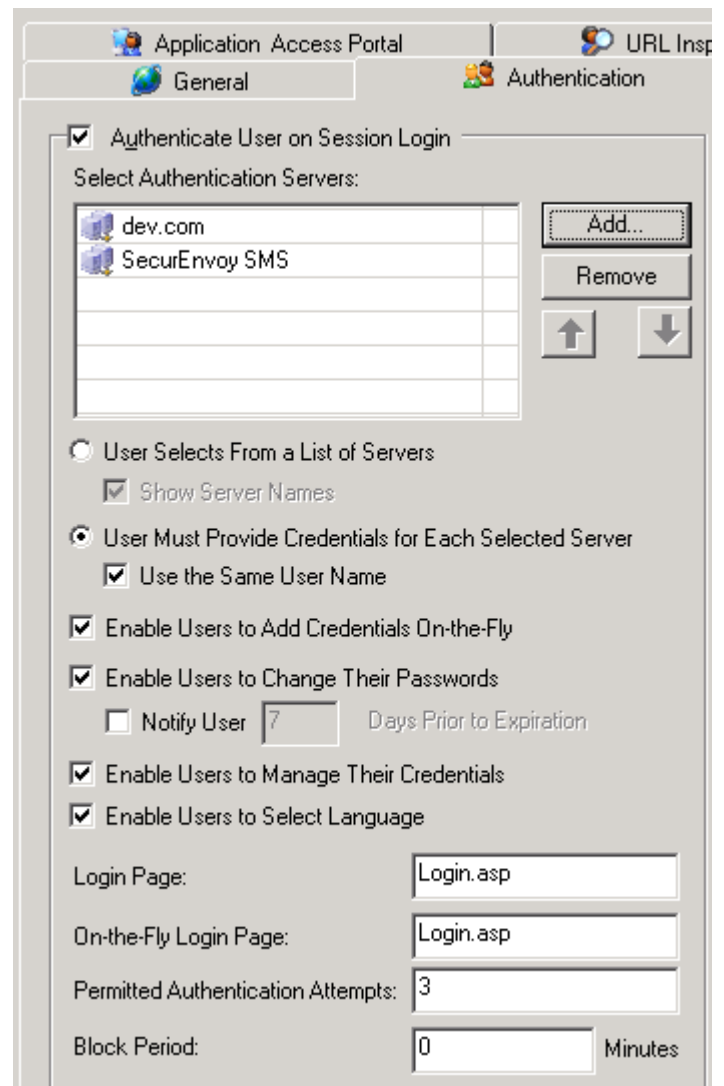
To enforce “Chained Authentication”, Click the radial button “User must provide credentials for each selected server”

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 dev.com).

Server Name	Server Type
dev.com	
SecurEnvoy SMS	

## 4. Testing Authentication

Connect to the URL of the IAG's configured trunk

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

Enter the Microsoft Password in the xxx Password field (in this example dev.com)

Enter the 6 digit SMS passcode from the users mobile phone into the "SecurEnvoy SMS Password" field



The screenshot shows a web browser window with the title "Whale Communications" and the URL "www.whalecommunications.com". The page content includes a header with "Microsoft Internet Explorer" and "This site is protected by the Intelligent Application Gateway". Below the header, the text "Please provide the following:" is followed by four input fields: "User Name:", "dev.com Password:", "SecurEnvoy SMS Password:", and "Language:" (with a dropdown menu set to "English (default)"). A red-bordered warning box contains the text: "You are accessing this site from a computer running Microsoft Windows XP, Service Pack 2 (SP2) or higher. Internet Explorer is configured by default to block popups. In order to be able to receive inactive lineout notifications and other warnings from this site, it is recommended that you configure your browser to allow popups from this site." Below the warning box are two buttons: "Submit" and "Reset". At the bottom, there is a footer with the text: "This site is intended only for authorized users. If you encounter any problems with this site please contact your system administrator at [administrator@server.com](mailto:administrator@server.com)".

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